



Cisco APIC 開始ガイド、リリース 6.0(x)

初版：2022年6月17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](http://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)



目次

はじめに :	Trademarks iii
--------	-----------------------

第 1 章	新機能と更新情報 1
	新規および変更情報 1

第 2 章	初期設定 3
	次の手順については、以下を参照してください 3
	Cisco APIC での設定のための簡略化されたアプローチ 4
	BIOS のデフォルト パスワードの変更 4
	APIC について 5
	Cisco APIC のセットアップ 5
	アクティブ APIC とスタンバイ APIC のセットアップ 9
	APIC コントローラの IPv6 管理アドレスのプロビジョニング 15
	GUI へのアクセス 16
	REST API へのアクセス 18
	NX-OS スタイル CLI へのアクセス 18
	端末から NX-OS スタイル CLI へのアクセス 19
	GUI から NX-OS スタイル CLI へのアクセス 19
	オブジェクト モデル CLI へのアクセス 20

第 3 章	APIC GUI の概要 23
	GUI の概要 23
	メニュー バーおよびサブメニュー バー 24
	メニュー バーのタブ 25

[System] タブ	25
[Tenants] タブ	26
[Fabric] タブ	26
[Virtual Networking] タブ	27
[Admin] タブ	27
[Operations] タブ	27
[Apps] タブ	27
[インテグレーション (Integrations)] タブ	27
メニュー バーのツール	28
検索	28
Multi-Site Manager の起動	28
フィードバック	28
アラート	28
ツール	29
ヘルプ	29
マイ プロファイルの管理	30
ナビゲーション ウィンドウ	31
[Work] ペイン	32
作業ウィンドウの共通ページ	32
インターフェイスのカスタマイズ	33
APIC GUI の命名	33
CLI または GUI へのログイン バナーを追加する	34
単一ブラウザ セッション管理	34
導入の警告とポリシーの利用情報	34
ポートのグラフィカル設定	35
GUI 内の API 交換の表示	36
GUI アイコン	39
障害、統計情報、およびヘルス レベルのアイコン	40

第 4 章	ファブリックの初期化とスイッチの検出	41
	ファブリックの初期化	41

ファブリックの初期化について	41
ファブリック トポロジ (例)	41
マルチ階層ファブリック トポロジ (例)	43
外部ロータブル サブネットの交換	45
スイッチの検出	47
APIC によるスイッチ検出	47
APIC クラスタによるスイッチ登録	47
スイッチ ロールの考慮事項	47
GUI を使用した未登録スイッチの登録	48
GUI を使用したディスカバリ前のスイッチの追加	50
スイッチ検出の自動ファームウェア更新	52
APIC からのスイッチ検出の検証とスイッチ管理	53
GUI を使用した登録スイッチの検証	53
ファブリック トポロジの検証	53
GUI を使用したファブリック トポロジの検証	53
VM 管理でのアンマネージド スwitchの接続	54
メンテナンス モード	54
メンテナンス モード	54
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	56
GUI を使用してスイッチを挿入し、動作モードにする	56
Cisco NX-OS から Cisco ACI POAP への自動変換	57
Cisco NX-OSからCisco ACI POAPへの自動変換について	57
Cisco NX-OS から Cisco ACI POAP への自動変換の注意事項と制限事項	57
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	58
Cisco Nexus 9000 スwitchの安全な消去	60
Cisco Nexus 9000 スwitchの安全な消去について	60
GUI を使用した Cisco Nexus 9000 スwitchのユーザー データの安全な消去	60
GUI を使用して Cisco Nexus 9000 モジュラ スwitch 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	61
スウィッチの CLI を使用して Cisco Nexus 9000 スwitchからユーザー データを安全に消去する	61

第 5 章	Cisco APIC クラスタの管理	63
	APIC クラスタの概要	63
	Cisco APIC Cluster のクラスタの拡大	63
	Cisco APIC クラスタの縮小	64
	クラスタ管理の注意事項	64
	APIC クラスタ サイズの拡大	65
	APIC クラスタのサイズ縮小	66
	クラスタでの Cisco APIC コントローラの交換	67
	GUI を使用した APIC クラスタの拡大	68
	GUI を使用した APIC クラスタの縮小	69
	Cisco APIC コントローラのコミッショニングとデコミッショニング	70
	GUI を使用したクラスタの Cisco APIC のコミッショニング	70
	GUI を使用したクラスタでの Cisco APIC コントローラのデコミッショニング	70
	クラスタ内の APIC のシャットダウン	71
	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	71
	クラスタ内、apic のパフォーマンスを元に戻す方法	72
	Cold Standby	72
	Cold Standby について (Cisco APIC クラスタ用)	72
	GUI を使用した Cold Standby ステータスの確認	74
	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	74

付録 A :	CLI を使用している Cisco APIC の設定	77
	Cisco APIC クラスタの設定	77
	クラスタ管理の注意事項	77
	CLI を使用した、クラスタ内の Cisco APIC の交換	78
	CLI を使用してスタンバイ apic 内でアクティブな APIC 経由でスイッチング	79
	CLI を使用して Cold Standby ステータスを確認する	80
	ファブリックの初期化とスイッチの検出	80
	スイッチの検出	80
	CLI を使用した未登録スイッチの登録	80

CLI を使用したディスカバリ前のスイッチの追加	81
グレースフル挿抜 (GIR) モード	81
CLI を使用してメンテナンス モードにスイッチを移行する	81
CLI を使用して操作モードにスイッチを挿入する	82

付録 B :

REST API を使用した Cisco APIC の設定	83
Cisco APIC クラスタの設定	83
REST API を使用した APIC クラスタの拡大	83
REST API を使用した APIC クラスタの縮小	83
REST API を使用してアクティブ APIC とスタンバイ APIC を切り替える	84
ファブリックの初期化とスイッチの検出	84
スイッチの検出	84
REST API を使用した未登録スイッチの登録	84
REST API を使用したディスカバリ前のスイッチの追加	85
グレースフル挿抜 (GIR) モード	86
REST API を使用して、メンテナンス モードにスイッチを削除	86
REST API を使用した操作モードへのスイッチの挿入	86



第 1 章

新機能と更新情報

この章は、次の内容で構成されています。

- [新規および変更情報 \(1 ページ\)](#)

新規および変更情報

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(1) の新機能および変更された機能に関する情報

機能	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。これらの各領域には、ネットワークアーキテクチャや設計の詳細など、ユーザー固有の情報と、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、返品承認 (RMA) によっ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 (60 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 (3 ページ)
- Cisco APIC での設定のための簡略化されたアプローチ (4 ページ)
- BIOS のデフォルトパスワードの変更 (4 ページ)
- APIC について (5 ページ)
- Cisco APIC のセットアップ (5 ページ)
- GUI へのアクセス (16 ページ)
- REST API へのアクセス (18 ページ)
- NX-OS スタイル CLI へのアクセス (18 ページ)
- オブジェクトモデル CLI へのアクセス (20 ページ)

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

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。

-
- 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、CIMC 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 ポートを通じてローカルで 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となります。
- 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、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 2: 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。

名前	説明	デフォルト値
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「 <i>Deploying APIC Cluster Connectivity to the Fabric Over a Layer 3 Network</i> 」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	<p>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</p> <p>(注) Cisco APIC での使用専用はこの 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。</p>	
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	<p>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。</p> <p>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ができます。</p>	<p>225.0.0.0/15</p> <p>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。</p>
アウトオブバンド管理用の IPv4/IPv6 アドレス	<p>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。</p> <p>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。</p>	—
デフォルト ゲートウェイの IPv4/IPv6 アドレス	<p>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</p>	—

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。 <ul style="list-style-type: none"> • 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 3: 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

名前	説明	デフォルト値
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。
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 での使用専用はこの 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
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。 <ul style="list-style-type: none"> • 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): 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]: 172.23.142.29/21
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: 3914
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

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): 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: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

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は参照してください、 *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

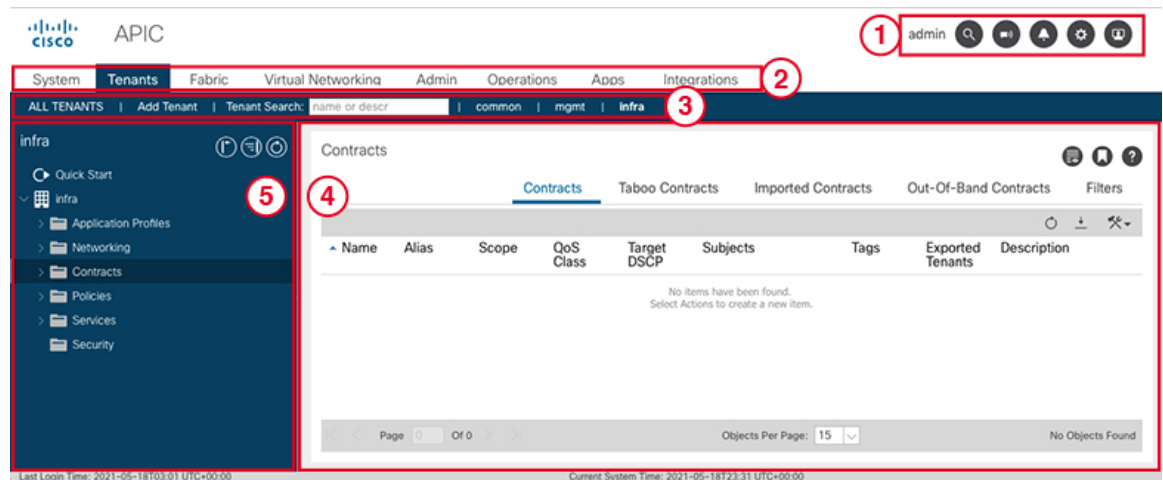
この章は、次の内容で構成されています。

- [GUI の概要 \(23 ページ\)](#)
- [メニューバーおよびサブメニューバー \(24 ページ\)](#)
- [ナビゲーション ウィンドウ \(31 ページ\)](#)
- [\[Work\] ペイン \(32 ページ\)](#)
- [インターフェイスのカスタマイズ \(33 ページ\)](#)
- [単一ブラウザセッション管理 \(34 ページ\)](#)
- [導入の警告とポリシーの利用情報 \(34 ページ\)](#)
- [ポートのグラフィカル設定 \(35 ページ\)](#)
- [GUI 内の API 交換の表示 \(36 ページ\)](#)
- [GUI アイコン \(39 ページ\)](#)

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 \(24 ページ\)](#)
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 \(24 ページ\)](#)
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 \(24 ページ\)](#)
4. 作業ウィンドウ: [\[Work\] ペイン \(32 ページ\)](#)
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 \(31 ページ\)](#)

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 \(36 ページ\)](#) 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
<i>username</i>	現在ログインしているローカル ユーザの名前。
	検索 (28 ページ)
	Multi-Site Manager の起動 (28 ページ)
	フィードバック (28 ページ)
	アラート (28 ページ)
	ツール (29 ページ)
	ヘルプ (29 ページ)
	マイ プロファイルの管理 (30 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ク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クなどのため)。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、アカウント機能、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。

[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спек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 \(36 ページ\)](#) を参照してください。
- **Start Remote Logging** — ログ情報 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** : 一般的な 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した後 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します。 [導入の警告とポリシーの利用情報 \(34 ページ\)](#) 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 \(34 ページ\)](#)」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 \(34 ページ\)](#) 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が、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] ウィ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 を配置できるようにサイトで許可を設定する必要があります。サイトの所有者が `x-frame-option` を `deny` または `sameorigin` に設定すると、URL がポイントしているサイトは表示されません。

ステップ 4 [送信 (Submit)] をクリックします。

単一ブラウザセッション管理

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

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

導入の警告とポリシーの利用情報

Deployment Warning Settings を構成することにより、他のリソースやポリシーに影響を及ぼす可能性のあるポリシーを変更または削除した際に、ポリシーの使用情報が自動的に表示される

ようにすることができます。ポリシーの利用情報では、ユーザが現在変更または削除しているポリシーがどのリソースおよびポリシーを使用しているかをユーザが確認することができます。テーブルには、特定のポリシーを使用するノード、およびこのポリシーを使用するほかのポリシーが表示されます。デフォルトでは、利用情報は、ユーザがポリシーを変更しようとするたびにダイアログボックス内に表示されます。また、いつでも画面下部の **Show Usage** ボタンをクリックして同じ情報を表示できます。

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

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

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

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

ポートのグラフィカル設定

APIC GUI は、ファブリックのリーフスイッチ上でポート、ポートチャネル、および仮想ポートチャネルを設定し、ダイナミックブレイ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。ブレイ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切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** : 適切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спек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спек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спек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 4: APIC GUI に頻繁に表示されるアイコン

アイコン	説明
	検索 (28 ページ)
	アラート (28 ページ)
	マイ プロファイルの管理 (30 ページ)
	ツール (29 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 5: APIC GUI に表示される障害の重大度レベル

アイコン	説明
	クリティカル：このアイコンは、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、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、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 \(41 ページ\)](#)
- [スイッチの検出 \(47 ページ\)](#)
- [メンテナンス モード \(54 ページ\)](#)
- [Cisco NX-OS から Cisco ACI POAP への自動変換 \(57 ページ\)](#)
- [Cisco Nexus 9000 スイッチの安全な消去 \(60 ページ\)](#)

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。

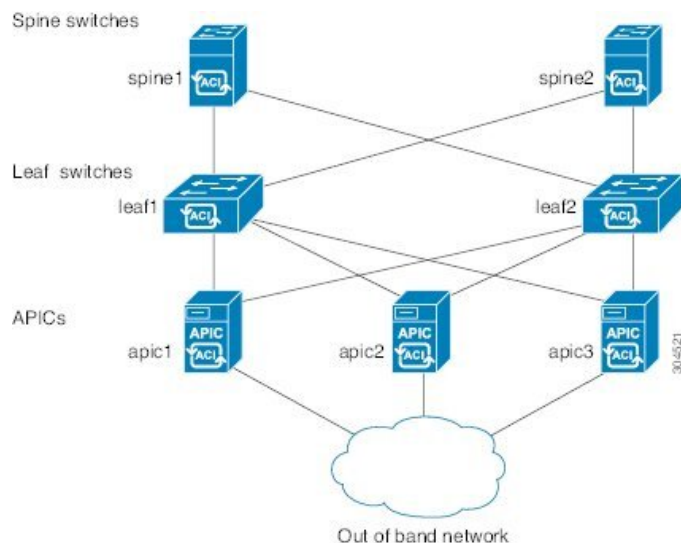
ファブリック トポロジ (例)

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。

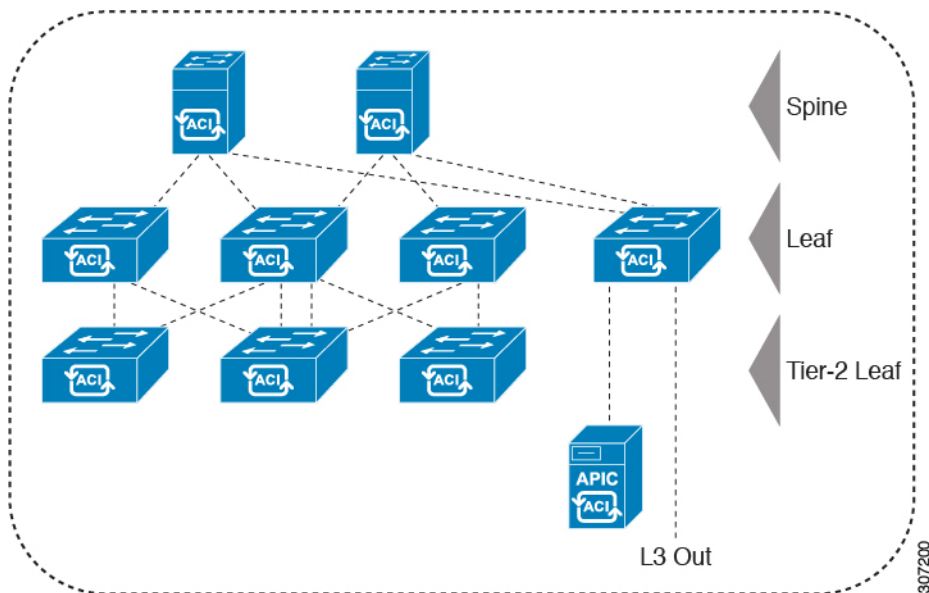
マルチ階層トポロジでは、リーフスイッチには最初にスパインスイッチへのアップリンク接続と、階層 2 リーフスイッチへのダウンリンク接続があります。トポロジ全体を ACI ファブリックにするには、階層 2 リーフ ファブリック ポートに接続されているリーフスイッチ上のすべてのポートが、ファブリックポートとして設定されている必要があります (まだデフォルトのファブリックポートを使用していない場合)。APIC が階層 2 リーフスイッチを検出した後、階層 2 リーフ上のダウンリンクポートをファブリックポートに変更し、中間レイヤリーフ上のアップリンクポートに接続できます。



- (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 6: 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-Gbps	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

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)
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TEP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 秒以上待つてから、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 natable
```

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

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

- a) 表示されているシリアル番号を確認し、どのスイッチを追加するか決定します。
- b) 次の設定を実行または編集します。

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

フィールド	設定
ロール (Role)	<p>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。</p> <ul style="list-style-type: none"> • spine • leaf • virtualleaf • virtualspine • リモート リーフ • 層-2-leaf <p>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。</p>
ラック名	<p>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。</p>

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)	<p>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。</p> <p>(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)。</p> <p>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。</p>
Switch Name	leaf1 または spine3 などのノード名。
ノードタイプ (Node Type)	<p>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。</p> <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • Is Virtual：ノードが仮想であることを指定します。 • unknown <p>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。</p>
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。

フィールド	設定
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 \(48 ページ\)](#) 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。

スイッチ検出の自動ファームウェア更新

[Auto Firmware Update on Switch Discovery (スイッチ検出で自動ファームウェア更新)] が有効な場合、APIC では次のシナリオで新しいスイッチのファームウェアを自動的に更新します。

- 新しいノード ID で新規スイッチ検出
- 既存のノード ID でスイッチ交換
- 既存のノードの初期化と再検出

Cisco APIC リリース 5.1(1) 以前のリリースで、この機能は [ブートスクリプトバージョン検証の強制 (Enforce Bootscript Version Validation)] と呼ばれ、[管理 (Admin)] > [ファームウェア (Firmware)] > [インフラストラクチャ (Infrastructure)] > [ノード (Nodes)] に存在していました。Cisco APIC リリース 5.1(1) で、この機能は名前が変更され、現在の場所に移動しました。

- 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)] > [自動ファームウェア更新 (Auto Firmware Update)] に移動します。
- ステップ 2** [スイッチ検出で自動ファームウェア更新 (Auto Firmware Update on Switch Discovery)] チェックボックスをオンにそて、この機能を有効にします。
- ステップ 3** [デフォルトファームウェアバージョン (Default Firmware Version)] ドロップダウンリストで新しいスイッチを更新するために、ターゲットファームウェアバージョンを選択します。

(注) 交換シナリオなど新規スイッチのノード ID が [管理 (Admin)] > [ファームウェア (Firmware)] の下にあるファームウェア更新の一部である場合、新規スイッチは更新グループで指定されたターゲットバージョンに更新されます。もしくは、この手順で指定されたデフォルトのファームウェアバージョンに更新されます。

選択された [デフォルトのファームウェアバージョン (Default Firmware Version)] が「any」の場合、この機能ではファームウェア更新グループの一部ではない ID を持つ新規スイッチのファームウェアを更新しません。ファームウェア更新グループの一部であるノード ID を持つ新規スイッチは、更新グループで指定されたターゲットバージョンに更新されます。

ステップ 4 [送信 (Submit)] をクリックします。

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witch 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witch 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witch 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。

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を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 内でアダプタイズ、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、 **acdiag 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ン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 ACI POAP 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 デバイスに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。
- 製品ID (PID) に -EX、-FX、-GX、またはそれ以降のサフィックスがないノードはサポートされません。
- 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。

スイッチ検出時の自動ファームウェア更新で、NX-OSノードが指定されたCisco ACIイメージで起動するまで待ちます。Cisco ACIイメージを使用してノードが起動すると、ノードは通常の新しいCisco ACIスイッチと同様に[登録保留中のノード (Nodes Pending Registration)] タブに表示されます。その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の実行できます。

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 \(63 ページ\)](#)
- [Cisco APIC Cluster のクラスタの拡大 \(63 ページ\)](#)
- [Cisco APIC クラスタの縮小 \(64 ページ\)](#)
- [クラスタ管理の注意事項 \(64 ページ\)](#)
- [GUI を使用した APIC クラスタの拡大 \(68 ページ\)](#)
- [GUI を使用した APIC クラスタの縮小 \(69 ページ\)](#)
- [Cisco APIC コントローラのコミッションとデコミッション \(70 ページ\)](#)
- [クラスタ内の APIC のシャットダウン \(71 ページ\)](#)
- [Cold Standby \(72 ページ\)](#)

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があるすべての 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。拡張プロセスは稼働中のクラスタ 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、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従ってください。



- (注) 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。

クラスタを管理する場合、次の一般的ガイドラインに従ってください。

- 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。

ここでは、次の内容について説明します。

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 インストール 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

APIC クラスタのサイズを縮小し、クラスタから削除された APIC コントローラを解放するには、次のガイドラインに従います。



(注) 縮小したクラスタから APIC コントローラを解放し、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 APIC コントローラをファブリックに接続されたままにしないでください。

- クラスタサイズを小さくすると、残りの APIC コントローラの負荷が増大します。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、APIC コントローラサイズの縮小を予定します。
- 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。
- 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 ID の番号が最大のものから、APIC コントローラを 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、APIC はクラスタを同期します。



(注) クラスタから APIC コントローラをデコミッションした後に、電源をオフにし、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。

- 既存の 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。

- コントローラの削除の際に 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、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 コントローラのデコミッション \(70 ページ\)](#) 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 のコミッションング \(70 ページ\)](#) 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るため、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

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。

拡大したいクラスタ内にある [apic_controller_name] 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 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、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) 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 [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 6** クラスタに追加するすべての 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、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 7** 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

- 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

- 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 コントローラのデコミッション

- 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。

特記事項

- 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路でスイッチします。
 - 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 クラスター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 (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))]** がオンになっている場合、スタンバイ (新しいアクティブ) APIC は元のスタンバイ OOB 管理 IP アドレスを保持します。
- **[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：
 - アクティブな APIC が 1 つだけ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、古いアクティブ Cisco APIC の OOB 管理 IP アドレスを使用します。
 - 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 APIC の OOB 管理 IP アドレスを使用しようとしませんが、アクティブな APIC の OOB 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 OOB 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 OOB 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 OOB 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 OOB 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) APIC OOB 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、クラスターのマイノリティ状態を解除する必要があることに注意してください。

- 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。

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 経路でスイッチング

スタンバイ apic 内でアクティブな APIC 経路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（74 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。
-

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



付録 **A**

CLI を使用している Cisco APIC の設定

- [Cisco APIC クラスタの設定 \(77 ページ\)](#)
- [ファブリックの初期化とスイッチの検出 \(80 ページ\)](#)

Cisco APIC クラスタの設定

クラスタ管理の注意事項

Cisco Application Policy Infrastructure Controller (APIC) クラスタは複数の Cisco APIC コントローラで構成され、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従ってください。



- (注) 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。

クラスタを管理する場合、次の一般的ガイドラインに従ってください。

- 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せす。
- 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。

ここでは、次の内容について説明します。

CLI を使用した、クラスタ内の Cisco APIC の交換



- (注)
- クラスタの管理の詳細については、[クラスタ管理の注意事項](#) を参照してください。
 - APIC を交換すると、パスワードは必ずクラスタから同期されます。APIC 1 を交換するときには、パスワードの入力を求められますが、そのパスワードはクラスタ内の既存のパスワードを優先して無視されます。APIC 2 または 3 を交換するときには、パスワードの入力は求められません。

始める前に

APIC を交換する前に、交換用 APIC が、交換する APIC と同じファームウェアバージョンを実行していることを確認します。バージョンが同じでない場合は、開始する前に代替 APIC のファームウェアを更新する必要があります。異なるバージョンを実行して 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。

ステップ 1 交換する APIC を特定します。

ステップ 2 **acdiag avread** コマンドを使用して、交換する APIC の設定の詳細を確認します。

ステップ 3 **controller controller-id decommission** コマンドを使用して APIC をデコミッションします。

(注) APIC を解放すると、APIC ID とシャーシ ID のマッピングが削除されます。通常、新しい APIC には、異なる APIC ID があるので、クラスタに新しい APIC を追加するにはこのマップを削除する必要があります。

ステップ 4 新しい APIC をコミッションする手順は、次のとおりです。

- a) ファブリックから古い APIC を切断します。
- b) ファブリックに交換 APIC を接続します。

新しい APIC コントローラが、[未認可コントローラ (Unauthorized Controllers)] リストの APIC GUI メニュー[システム (System)]>[コントローラ (Controllers)]>[apic_controller_name]>[ノードで確認するクラスタ (Cluster as Seen by Node)] に表示されます。

- c) **controller controller-id commission** コマンドを使用して新しい APIC をコミッションします。
- d) 新しい APIC を起動します。
- e) クラスタの残りの部分に新しい APIC 情報が伝播するまでに数分かかります。

新しい APIC コントローラが、[Active Controllers] リストの APIC GUI メニュー[システム (System)]>[コントローラ (Controllers)]>[apic_controller_name]>[ノードで確認するクラスタ (Cluster as Seen by Node)] に表示されます。

CLI を使用してスタンバイ apic 内でアクティブな APIC 経由でスイッチング

スタンバイ apic 内でアクティブな APIC 経由でスイッチするには、次の手順を使用します。

ステップ 1 **replace-controller replace ID** 番号 バックアップ シリアル番号

スタンバイ APIC でアクティブな APIC に置き換えられます。

例 :

```
apic1#replace-controller replace 2 FCH1804V27L
Do you want to replace APIC 2 with a backup? (Y/n): Y
```

ステップ 2 **replace-controller reset ID** 番号

アクティブなコントローラのステータスをリセットが失敗します。

例 :

CLI を使用して Cold Standby ステータスを確認する

```
apic1# replace-controller reset 2
Do you want to reset failover status of APIC 2? (Y/n): Y
```

CLI を使用して Cold Standby ステータスを確認する

APIC の **show controller** ステータスを確認するには、管理者として APIC にログインして、Cold Standby show controller Cold Standby コマンドを入力します。

```
apic1# show controller
Fabric Name       : vegas
Operational Size  : 3
Cluster Size     : 3
Time Difference   : 496
Fabric Security Mode : strict
```

ID	Pod	Address	In-Band IPv4	In-Band IPv6	OOB IPv4	OOB IPv6
		Version	Flags	Serial Number	Health	
1*	1	10.0.0.1	0.0.0.0	fc00::1	172.23.142.4	
		fe80::26e9:b3ff:fe91:c4e0	2.2(0.172)	crva- FCH1748V0DF	fully-fit	
2	1	10.0.0.2	0.0.0.0	fc00::1	172.23.142.6	
		fe80::26e9:bf8f:fe91:f37c	2.2(0.172)	crva- FCH1747V0YF	fully-fit	
3	1	10.0.0.3	0.0.0.0	fc00::1	172.23.142.8	
		fe80::4e00:82ff:fead:bc66	2.2(0.172)	crva- FCH1725V2DK	fully-fit	
21~		10.0.0.21		----- FCH1734V2DG		

Flags - c:Commissioned | r:Registered | v:Valid Certificate | a:Approved | f/s:Failover fail/success
 (*) Current (~) Standby

ファブリックの初期化とスイッチの検出

スイッチの検出

CLI を使用した未登録スイッチの登録

この手順を使用して、CLI を使用して [ファブリック メンバーシップ (Fabric Membership)] 作業ウィンドウの [保留中ノードの登録 (Nodes Pending Registration)] タブからスイッチを登録します。



- (注) この手順は、「CLIを使用したディスカバリ前のスイッチの追加」と同じです。コマンドを実行すると、システムはノードが存在するかどうかを判断し、存在しない場合はそのノードを追加します。ノードが存在する場合、システムにより登録されます。

手順

	コマンドまたはアクション	目的
ステップ 1	<code>[no] system switch-id serial-number switch-id name pod id role leaf node-type tier-2-leaf</code>	スイッチを保留中の登録リストに追加します。

CLI を使用したディスカバリ前のスイッチの追加

この手順を使用して、CLI を使用して [ファブリック メンバーシップ (Fabric Membership)] 作業ウィンドウの [保留中ノードの登録 (Nodes Pending Registration)] タブにスイッチを追加します。



- (注) この手順は、「CLIを使用した未登録スイッチの登録」と同じです。コマンドを実行すると、システムはノードが存在するかどうかを判断し、存在しない場合はそのノードを追加します。ノードが存在しない場合、システムにより登録されます。

`[no] system switch-id serial-number switch-id name pod id role leaf node-type tier-2-leaf`

スイッチを保留中の登録リストに追加します。

グレースフル挿抜 (GIR) モード

CLI を使用してメンテナンス モードにスイッチを移行する

CLI を使用してメンテナンス モードにスイッチを移行するには、次の手順を使用します。



- (注) スイッチがメンテナンス モード中の場合、スイッチの CLI 「show」 コマンドでは、前面パネル ポートがアップ状態であり、BGP プロトコルがアップ状態かつ実行中であることを示します。インターフェイスは実際にシャットダウンされ、BGP のその他すべての隣接関係がダウンしますが、表示されているアクティブ状態でデバッグが可能です。

`[no]debug-switch node_id or node_name`

CLI を使用して操作モードにスイッチを挿入する

メンテナンス モードにスイッチを移行します。

CLI を使用して操作モードにスイッチを挿入する

この手順を使って、スイッチを CLI を使用している動作モードに挿入します。

[no]no debug-switch *node_id or node_name*

動作モードにスイッチを挿入します。



付録 **B**

REST API を使用した Cisco APIC の設定

- [Cisco APIC クラスタの設定 \(83 ページ\)](#)
- [ファブリックの初期化とスイッチの検出 \(84 ページ\)](#)

Cisco APIC クラスタの設定

REST API を使用した APIC クラスタの拡大

クラスタは、実際のサイズを目標サイズに合わせます。目標サイズが実際のサイズよりも大きい場合、クラスタ サイズが拡大します。

ステップ 1 APIC クラスタのサイズを拡大するために目標のクラスタ サイズを設定します。

例 :

```
POST
https://<IP address>/api/node/mo/uni/controller.xml
<infraClusterPol name='default' size=3/>
```

ステップ 2 クラスタに追加する APIC コントローラを物理的に接続します。

REST API を使用した APIC クラスタの縮小

クラスタは、実際のサイズを目標サイズに合わせます。目標サイズが実際のサイズより小さい場合、クラスタ サイズは縮小します。

ステップ 1 APIC クラスタのサイズを縮小するため、目標のクラスタ サイズを設定します。

例 :

```
POST
https://<IP address>/api/node/mo/uni/controller.xml
<infraClusterPol name='default' size=1/>
```

REST API を使用してアクティブ APIC とスタンバイ APIC を切り替える

ステップ2 クラスタ縮小のための APIC1 上の APIC3 の解放

例 :

```
POST
https://<IP address>/api/node/mo/topology/pod-1/node-1/av.xml
<infraWiNode id=3 adminSt='out-of-service'>
```

ステップ3 クラスタ縮小のための APIC1 上の APIC2 の解放

例 :

```
POST
https://<IP address>/api/node/mo/topology/pod-1/node-1/av.xml
<infraWiNode id=2 adminSt='out-of-service'>
```

REST API を使用してアクティブ APIC とスタンバイ APIC を切り替える

REST API を使用してアクティブな APIC とスタンバイ APIC を切り替えるには、この手順を使用します。

アクティブ APIC とスタンバイ APIC を切り替えます。

URL for POST: `https://ip address/api/node/mo/topology/pod-initiator_pod_id/node-initiator_id/av.xml`
 Body: `<infraWiNode id=outgoing_apic_id targetMbSn=backup-serial-number/>`
 where `initiator_id` = id of an active APIC other than the APIC being replaced.
`pod-initiator_pod_id` = pod ID of the active APIC
`backup-serial-number` = serial number of standby APIC

例 :

```
https://ip address/api/node/mo/topology/pod-1/node-1/av.xml
<infraWiNode id=2 targetMbSn=FCH1750V00Q/>
```

ファブリックの初期化とスイッチの検出

スイッチの検出

REST API を使用した未登録スイッチの登録

この手順を使用して、REST API を使用して [ファブリックメンバーシップ (Fabric Membership)] 作業ウィンドウの [保留中ノードの登録 (Nodes Pending Registration)] タブからスイッチを登録します。



- (注) この手順は、「REST API を使用したディスカバリ前のスイッチの追加」と同じです。コードを適用すると、システムはノードが存在するかどうかを判断し、存在しない場合はそのノードを追加します。ノードが存在しない場合、システムにより登録されます。

スイッチ説明を追加します。

例 :

```
POST
https://<IP address>/api/policymgr/mo/uni.xml

<!-- /api/policymgr/mo/uni.xml -->
<polUni>
<ctrlrInst>
  <fabricNodeIdentPol>
    <fabricNodeIdentP nodeType="tier-2-leaf" podId="1" serial="XXXXXXXXX"
      name="tier-2-leaf-leaf1" nodeId="101"/>
  </fabricNodeIdentPol>
</ctrlrInst>
</polUni>
```

REST API を使用したディスカバリ前のスイッチの追加

この手順を使用して、REST API を使用して [ファブリックメンバーシップ (Fabric Membership)] 作業ウィンドウの [保留中ノードの登録 (Nodes Pending Registration)] タブにスイッチを追加します。



- (注) この手順は、「REST API を使用した未登録スイッチの登録」と同じです。コードを適用すると、システムはノードが存在するかどうかを判断し、存在しない場合はそのノードを追加します。ノードが存在しない場合、システムにより登録されます。

スイッチ説明を追加します。

例 :

```
POST
https://<IP address>/api/policymgr/mo/uni.xml

<!-- /api/policymgr/mo/uni.xml -->
<polUni>
<ctrlrInst>
  <fabricNodeIdentPol>
    <fabricNodeIdentP nodeType="tier-2-leaf" podId="1" serial="XXXXXXXXX"
      name="tier-2-leaf1" nodeId="101"/>
  </fabricNodeIdentPol>
```

```
</ctrlrInst>
</polUni>
```

グレースフル挿抜 (GIR) モード

REST API を使用して、メンテナンス モードにスイッチを削除

REST API を使用して、メンテナンス モードにスイッチを削除するのには、次の手順を使用します。

メンテナンス モードにスイッチを削除します。

例 :

```
POST
https://<IP address>/api/node/mo/uni/fabric/outofsvc.xml
```

```
<fabricOOServicePol
  descr=""
  dn=""
  name="default"
  nameAlias=""
  ownerKey=""
  ownerTag="">
  <fabricRsDecommissionNode
    debug="yes"
    dn=""
    removeFromController="no"
    tDn="topology/pod-1/node-102"/>
</fabricOOServicePol>
```

REST API を使用した操作モードへのスイッチの挿入

REST API を使用して操作モードにスイッチを挿入するには、次の手順を使用します。

操作モードにスイッチを挿入します。

例 :

```
POST
https://<IP address>/api/node/mo/uni/fabric/outofsvc.xml
```

```
<fabricOOServicePol
  descr=""
  dn=""
  name="default"
  nameAlias=""
  ownerKey=""
  ownerTag="">
  <fabricRsDecommissionNode
```



```
    debug="yes"  
    dn=""  
    removeFromController="no"  
    tDn="topology/pod-1/node-102"  
    status="deleted"/>  
</fabricOOServicePol>
```

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。

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。