Cisco Application Policy Infrastructure Controller エンタープライズ モジュール構成ガイド リリース 1.0.x

初版：2015 年 11 月 02 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/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

はじめに vii

対象読者 vii

表記法 viii

関連資料 ix

マニュアルの入手方法およびテクニカル サポート x

概要 1

Cisco Application Policy Infrastructure Controller エンタープライズ モジュールについて 1

Cisco APIC-EM GUI の概要 4

デバイスおよびホストの検出 9

検出について 9

デバイスおよびホスト検出を理解する 11

ワイヤレス LAN コントローラの検出を理解する 12

検出の使用 13

CDP を使用した検出の実行 13

IP アドレス範囲を使用した検出の実行 16

検出の停止と開始 19

検出の削除 20

検出結果を理解する 20

デバイスおよびホストの管理 25

デバイス インベントリの管理 25

デバイス テーブル ビューのフィルタリング 32

デバイス レイアウト ビューの変更 33

デバイス ロールの変更 34

デバイスの削除 36

タグの追加および削除 36

タグの削除 38

ロケーション タグの追加または削除 40
ロケーション マーカーの追加および削除 41
ロケーション マーカーの追加 41
ロケーション マーカーの削除 44
ホスト インベントリの管理 45
ホスト テーブル ビューの変更 47
ユーザおよびロールの管理 49
ロールベース アクセス コントロールについて 49
ユーザ ロールについて 49
管理者ロール 50
オブザーバ ロール 51
インストーラ ロール 51
ユーザおよびドメイン 52
AAA について 52
認証および承認 52
Cisco APIC-EM のリソースと権限 52
アカウンティング（Accounting） 54
パスワードの変更 54
ユーザおよびロールの設定 56
ユーザの追加 57
ユーザの削除 58
ユーザ情報の表示と編集 59
ユーザ アクセス ステータスの表示 59
ユーザ ログの確認 60
アプリケーションの管理 63
シスコのネットワーク プラグ アンド プレイ 63
シスコ インテリジェント WAN（IWAN） 64
トポロジ 67
トポロジ ツールバー 68
トポロジのアイコン 71
デバイス データの表示 73
デバイス集約 74

[トポロジ（Topology）] ウィンドウのデバイスの集約 74
[トポロジ（Topology）] ウィンドウでのデバイスの集約解除 75
トポロジ構造の設定 76
トポロジ レイアウトの保存 79
保存されたトポロジ レイアウトを開く 79
[トポロジ（Topology）] ウィンドウでのデバイス ロールの変更 80
デバイスおよびホストの検索 81
デバイスへのタグの適用 82
タグ付きデバイスの表示 83
パス トレースの実行 84
パス トレースについて 84
パス トレースのサポート 87
パス トレース プロトコルおよびネットワーク接続 87
パス トレースの実行 94
パス トレースの結果の理解 95
API マニュアルの確認 99
Cisco APIC-EM API マニュアルについて 99
サポートされる HTTPS メソッドおよび一般構造 102
共通の外部 RESTful サービス HTTP 応答コード 103
Cisco APIC-EM API のテスト 105

はじめに

- 対象読者，vii ページ
- 表記法，viii ページ
- 関連資料，ix ページ
- マニュアルの入手方法およびテクニカル サポート，x ページ

対象読者

このマニュアルは、Cisco Application Policy Infrastructure Controller エンタープライズ モジュール（Cisco APIC-EM）を設定および維持する経験豊富なネットワーク管理者を対象としています。Cisco APIC-EMGUI を理解し、ネットワーク内で接続されたデバイスおよびホストを管理して、ネットワーク デバイスを介してパス トレースを実行するために、このコンフィギュレーション ガイドを使用します。

Cisco APIC-EM に関する追加情報については、次のガイドを参照してください。

- インストール、展開、確認、およびトラブルシューティングに関する情報を含むCisco APIC-EM自体に関する情報については、『*Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*』を参照してください。
- コントローラのGUIを初めて使用することに関する詳細については、『*Cisco APIC-EM Quick Start Guide*』を参照してください。

（注） Cisco Application Policy Infrastructure Controller エンタープライズ モジュール（Cisco APIC-EM）は、このコンフィギュレーション ガイド内では コントローラとも呼ばれます。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
^ または Ctrl	^ 記号と Ctrl は両方ともキーボードの Control（Ctrl）キーを表します。たとえば、**^D** または **Ctrl+D** というキーの組み合わせは、Ctrl キーを押しながら D キーを押すことを意味します（ここではキーを大文字で表記していますが、小文字で入力してもかまいません）。
bold フォント	コマンド、キーワード、およびユーザが入力するテキストは、**bold** フォントで記載されます。
イタリック体	ドキュメント名、新規用語または強調する用語、値を指定するための引数は、*italic* フォントで記載されます。
`courier` フォント	システムが表示する端末セッションおよび情報は、`courier` フォントで記載されます。
`太字の courier` フォント	**`太字の Courier`** フォントは、ユーザが入力しなければならないテキストを示します。
[x]	角カッコの中の要素は、省略可能です。
...	構文要素の後の省略記号（3つの連続する太字ではないピリオドでスペースを含まない）は、その要素を繰り返すことができることを示します。
|	パイプと呼ばれる縦棒は、一連のキーワードまたは引数の選択肢であることを示します。
[x | y]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
{x | y}	どれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	角カッコまたは波カッコが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。

表記法	説明
<>	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システムプロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

読者への警告の表記法

このマニュアルでは、読者への警告に次の表記法を使用しています。

（注） 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

ヒント 「問題解決に役立つ情報」です。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

ワンポイント アドバイス 時間を節約する方法です。ここに紹介している方法で作業を行うと、時間を短縮できます。

警告 IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger.You are in a situation that could cause bodily injury.Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.警告文 1071

SAVE THESE INSTRUCTIONS

関連資料

- Cisco APIC-EM のドキュメンテーション：
  - *Release Notes for the Cisco Application Policy Infrastructure Controller Enterprise Module*

- *Cisco APIC-EM Quick Start Guide*（コントローラの GUI から直接アクセス可能）
- *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*
- *Cisco Application Policy Infrastructure Controller* エンタープライズ モジュール構成ガイド
- *Cisco Application Policy Infrastructure Controller Enterprise Module Hardware Installation Guide*
- *Open Source Used In Cisco APIC-EM*

• Cisco APIC-EM 用 Cisco IWAN のドキュメンテーション：

- *Release Notes for Cisco IWAN*
- *Release Notes for Cisco Intelligent Wide Area Network (Cisco IWAN)*
- *Software Configuration Guide for Cisco IWAN on APIC-EM*
- *Open Source Used in Cisco IWAN and Cisco Network Plug and Play*

• Cisco APIC-EM 用シスコ ネットワーク プラグ アンド プレイのドキュメンテーション：

- *Release Notes for Cisco Network Plug and Play*
- *Solution Guide for Cisco Network Plug and Play*
- *Configuration Guide for Cisco Network Plug and Play on Cisco APIC-EM*
- *Cisco Open Plug-n-Play Agent Configuration Guide*
- *Mobile Application User Guide for Cisco Network Plug and Play*

（注） ノースバウンド REST API によってコントローラと対話する独自のアプリケーションの開発については、developer.cisco.com/site/apic-em の Web サイトを参照してください。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手、Cisco Bug Search Tool（BST）の使用、サービス要求の送信、追加情報の収集の詳細については、『*What's New in Cisco Product Documentation*』を参照してください。このドキュメントは、http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html から入手できます。

『*What's New in Cisco Product Documentation*』では、シスコの新規および改訂版の技術マニュアルの一覧を、RSS フィードとして購読できます。また、リーダー アプリケーションを使用して、コンテンツをデスクトップに配信することもできます。RSS フィードは無料のサービスです。

第 1 章

概要

- Cisco Application Policy Infrastructure Controller エンタープライズ モジュールについて，1 ページ
- Cisco APIC-EM GUI の概要，4 ページ

Cisco Application Policy Infrastructure Controller エンタープライズ モジュールについて

Cisco Application Policy Infrastructure Controller - エンタープライズ モジュール（APIC-EM）は、企業ネットワーク（アクセス、キャンパス、WAN、ワイヤレス）用の Cisco SDN コントローラです。

プラットフォームは、コア ネットワークの自動化ソリューションを駆動するオープン ノースバウンド REST API を使用する複数のアプリケーション（SDN アプリケーション）をホストします。また、さまざまなサウスバウンド プロトコルもサポートしています。そのため、お客様の環境に導入済みの各種ネットワーク デバイスと通信し、新規および既存の環境のいずれにも SDN の利点を広めることができます。

Cisco APIC-EM プラットフォームは、キャンパス、ブランチ、WAN のインフラストラクチャ全体における有線およびワイヤレス両方のエンタープライズ ネットワークをサポートします。次の利点があります。

- オープン API を使用して、インテリジェントかつオープンで、プログラム可能なネットワークを構築する
- 高度な自動化によって、時刻、リソースとコストを節約する
- ビジネス インテント ポリシーを動的なネットワーク設定に変換する
- ネットワーク全体の自動化と制御の一元化を実現する

次の表では、Cisco APIC-EM の機能と利点について説明します。

表 *1*：***Cisco APIC*** エンタープライズ モジュールの機能と利点

機能	説明
ネットワーク情報データベース（NIDB）	Cisco APIC-EM はネットワークを定期的にスキャンし、ITの「唯一の正しい情報源」を作成します。このインベントリは、すべてのネットワークデバイスを含み、また企業ネットワーク全体を抽象化します。
ネットワーク トポロジの可視化	Cisco APIC-EM は、ネットワーク デバイスを自動的に検出し、詳細なデバイスレベルのデータを使用して物理トポロジにマッピングします。ネットワークのトラブルシューティングにもこのインタラクティブな機能を使用できます。
シスコのプラグ アンド プレイ アプリケーション	シスコのネットワーク プラグ アンド プレイ ソリューションは、シスコのエンタープライズ ポートフォリオ全体に広がる統合型ソリューションです。シスコ ルータ、スイッチ、ワイヤレス アクセス ポイントにわたって、顧客に、非常に安全、スケーラブル、シームレスな統合ゼロタッチ導入エクスペリエンスを提供します。
シスコ インテリジェント WAN （IWAN）アプリケーション	個別にライセンス付与される APIC-EM 用の IWAN アプリケーションは、シンプルなビジネス ポリシーで IWAN ネットワーク プロファイルのプロビジョニングを簡略化します。IWAN アプリケーションは、ハイブリッドな WAN リンクの優先パスに関して、アプリケーションまたはアプリケーションのグループによってビジネス レベル設定を定義します。この機能では、接続によるアプリケーションエクスペリエンスによって、それ以外では非アクティブまたはバックアップリンクを使用することでコストを節約します。
公開キー インフラストラクチャ（PKI）サーバ	Cisco APIC-EM では、信頼マネージャ サービスに統合された PKI サーバを提供します。また、IWAN アプリケーションなどのアプリケーション向けの PKI X.509 証明書の発行、更新、失効のライフサイクル管理を自動化します。この機能によって、IWAN アプリケーションでは、ネットワークで信頼を確立し、保持するプロセスを大幅に簡素化します。

機能	説明
パス トレース アプリケーション	パストレースアプリケーションによって、ネットワークのビジネスアプリケーションから取得されたフローの検査および質問を自動化してネットワークの問題を解決することができます。
ハイ アベイラビリティ（HA）	完全なデータの一貫性を保つ N+ 1 冗長モードでハイ アベイラビリティと拡張性を実現します。すべてのノードは、パフォーマンスとロードシェアリングを最適化するために、アクティブ-アクティブ モードで稼働します。
バックアップと復元	Cisco APIC-EM は、コントローラ GUI からのデータベース全体の完全なバックアップと復元をサポートします。

Cisco APIC-EM GUI の概要

Cisco APIC-EM にログインすると、[ホーム（Home）] ページが表示されます。

図 *1*：*[*ホーム（*Home*）*]* ページ

コールアウト番号	[名前（Name）]	説明
1	[ナビゲーション（Navigation）] ペイン	IWAN およびネットワーク プラグ アンド プレイなどの Cisco APIC-EM 機能と追加のアプリケーションにアクセスできます。
2	ウィンドウ	機能またはアプリケーション インターフェイスが表示される領域。[ナビゲーション（Navigation）] ペインのオプションをクリックすると、対応するウィンドウが開きます。
3	**グローバル** ツールバー	API マニュアル、設定、および通知などのツールにアクセスできる領域。**グローバル** ツールバーのアイコンの詳細については、以下のグローバル ツールバー オプションの表を参照してください。
4	フィードバック リンク	Cisco APIC-EM 機能およびその GUI を使用してエクスペリエンスに関する入力を行い、改善案を表示できるフォームにリンクします。

[ナビゲーション（Navigation）] ペインのオプション

[ナビゲーション（Navigation）] ペインは、主要な Cisco APIC-EM 機能にアクセスするためのオプションを提供します。

表 *2*：*[ナビゲーション（Navigation）]* ペインのオプション

アイコン	[名前（Name）]	説明
	ナビゲーションの非表示/再表示（Hide/Unhide Navigation）	[ナビゲーション（Navigation）] ペインを非表示にする、または再表示することができます。
	Home	システム要件およびサポートされるプラットフォームに関する情報を表示します。
	検出	ネットワークのデバイスおよびホストをスキャンするための検出オプションを設定できます。
	デバイス インベントリ（Device Inventory）	インベントリ データベースへのアクセスを提供します。ここでは、ネットワークで検出されたデバイスについての表形式の情報を表示、フィルタ処理、およびソートすることができます。

アイコン	[名前（Name）]	説明
	トポロジ	物理的なレイヤ 2 およびレイヤ 3 のネットワークのグラフィカル表示を表示します。
	ホスト インベントリ（Host Inventory）	インベントリ データベースへのアクセスを提供します。ここでは、ネットワークで検出されたホストについての表形式の情報を表示、フィルタ処理、およびソートすることができます。ユーザは使用できる 3 つのステータス（アクティブ、非アクティブ、および削除）の 1 つにすることができます。
	IWAN	ネットワーク全体の設定、サイトのプロビジョニング、アプリケーション ポリシーの設定をすることができます。
	パス トレース（Path Trace）	コントローラは、ネットワークで検出されたデバイスからプロトコルおよび他のタイプのデータを確認および収集し、このデータを使用して 2 つのホストまたはレイヤ 3 インターフェイス間のパスを計算することができます。
	[ネットワークプラグアンドプレイ（Network Plug and Play）]	ネットワークデバイスのリモート導入アプリケーションにアクセスできます。

グローバル ツールバーのオプション

グローバル ツールバーは、他のシステムの機能にアクセスしてシステム通知を表示することができます。

表 *3*：グローバル ツールバーのオプション

アイコン	オプション	説明
	API	ノースバウンド REST API の自動生成されたドキュメントを表示します。

アイコン	オプション	説明
	システム通知（System Notifications）	システム通知ビューを開きます。このビューは、システム通知に関する情報を提供します。たとえば、ソフトウェアの更新またはセキュリティ証明書の更新についての通知がこのウィンドウに表示されます。各通知には、簡単な説明とクリックした場合に（追加の操作を行うことができる）通知の送信元の Cisco APIC-EM UI ウィンドウを開くアイコンが含まれます。
	アプリケーション通知（Application Notifications）	アプリケーション通知ビューを開きます。赤色の四角は、まだレビューされていない通知を示します。青色の四角は、通知がないか、または通知がありレビュー済みであることを示します。各通知は、リストの上部に最近に発生した順に表示されます。各通知には、簡単な説明と、クリックした場合に通知の送信元の Cisco APIC-EM アプリケーションを開くアイコンが含まれます。 （注） 現在開いているウィンドウ（アプリケーション）のイベントだけに通知するように設定することもできます。現在のウィンドウ（たとえば、[検出の通知のみ表示（Show only notifications for Discovery）]）の通知ビューのリンクをクリックすることによって、そのアプリケーションに発生するイベントに対する通知を制限します。

アイコン	オプション	説明
	管理機能（Administrative Functions）	Cisco APIC-EM またはユーザに固有の機能を実行できるウィンドウを開きます。 • Cisco APIC-EM 機能： ◦設定（Settings）：ユーザアカウント、検出クレデンシャル、ネットワーク設定およびその他のセキュリティとメンテナンス設定などのコントローラ設定を設定できます。 ◦ログ（Logs）：コントローラのサービス ログを検索できます。 • ユーザ機能： ◦パスワードの変更（Change Password）：自分のパスワードを変更できます。 ◦ログアウト（Sign Out）：Cisco APIC-EM をログアウトします。

第 2 章

デバイスおよびホストの検出

- 検出について，9 ページ
- 検出の使用，13 ページ

検出について

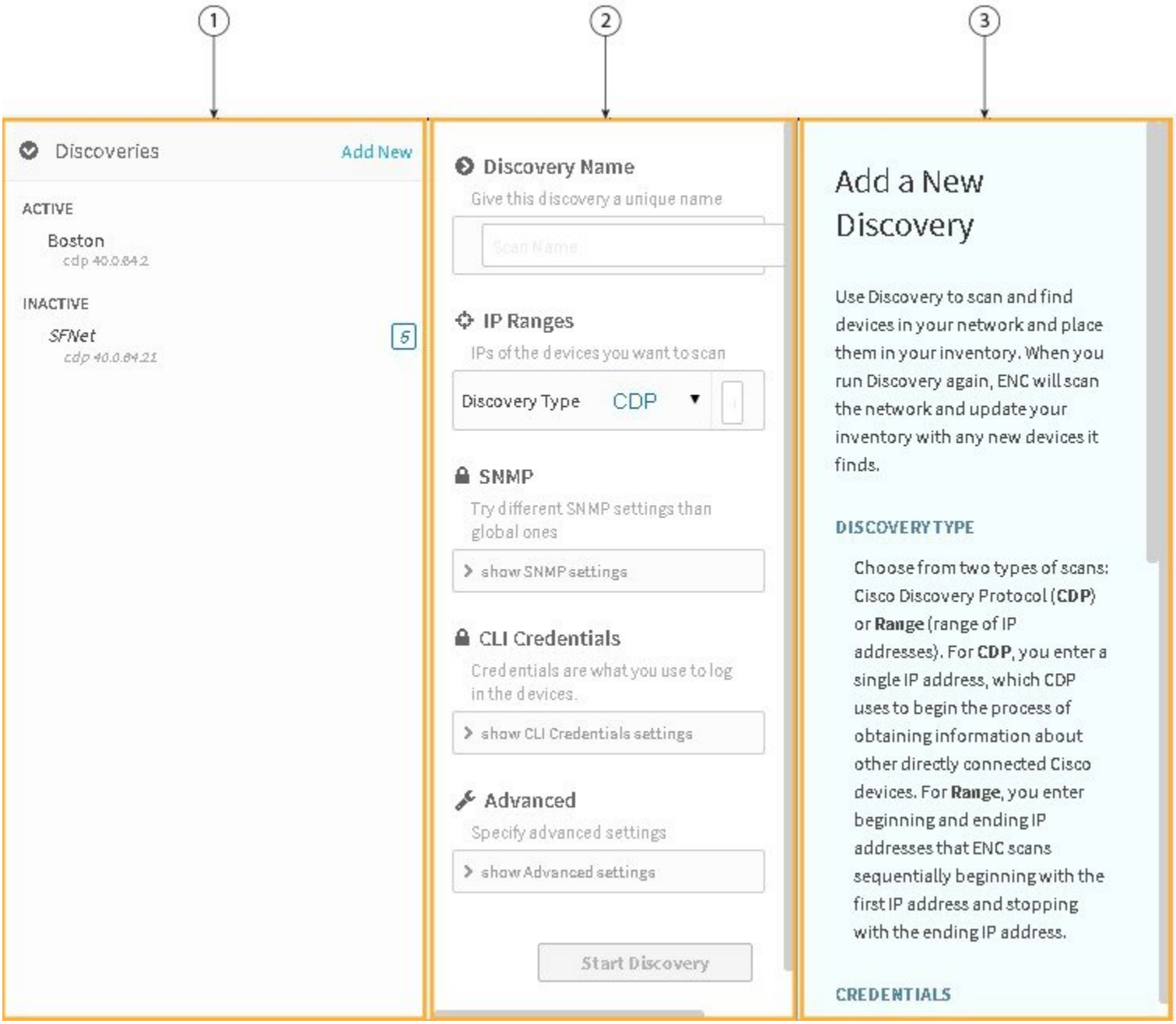
検出機能は、ネットワークのデバイスおよびホストをスキャンし、Cisco APIC-EM データベースを取得する情報とともに読み込みます。これを行うには、検出機能ができるだけネットワークのデバイスの多くに到達して、できるだけ多くの情報を収集できるようにするために、ネットワークに関する情報をコントローラに通知する必要があります。

検出機能は、次のプロトコルとメソッドを使用して、ネットワークに関する情報を取得します。

- Cisco Discovery Protocol（CDP）
- コミュニティベースの簡易ネットワーク管理プロトコル バージョン 2 （SNMPv2c）
- 簡易ネットワーク管理プロトコル バージョン 3 （SNMPv3）
- Link Layer Discovery Protocol（LLDP）
- IP デバイス トラッキング（IPDT）：IPDT はコントローラによってすべてのデバイスに対して自動的に有効になります。この設定では、権限は検出時にコントローラに付与される必要があります。
- LLDP-MED：IP 電話および可能性のあるいくつかのサーバが LLDP Media Endpoint Discovery を使用して検出されます。

[ナビゲーション（Navigation）]ペインで検出機能にアクセスするには、[検出（Discovery）]をクリックします。[検出（Discovery）] ウィンドウが開きます。

図 *2*：*[*検出（*Discovery***）*]*ウィンドウ**



番号付きコールアウト	[名前（Name）]	説明
1	[検出（Discovery）] ペイン	検出に使用するメソッドおよび IP アドレスとともに、作成された検出スキャンの名前を表示します。リストは、アクティブおよび非アクティブの検出の間で分割されます。 成功したスキャン（検出および認証されたデバイス）では、検出されたデバイスの数が検出名の右側のボックスに表示されます。失敗したスキャンでは、ボックスまたは検出されたデバイスの数が表示されません。 [検出（Discovery）] ペインで、検出名をクリックすると、[検出の詳細（Discovery Details）] ペインと [デバイスの詳細（Device Details）] ペインの情報が表示されます。
2	[検出の詳細（Discovery Details）] ペイン	検出、検出の状態、検出されたデバイスの数を実行するために使用された検出パラメータの詳細を提供します。このペインのボタンで、[開始（Start）]、[停止（Stop）]、および [削除（Delete）] の検出が可能です。
3	内部ツール ガイド	検出の設定方法に関するガイダンスを提供します。

デバイスおよびホスト検出を理解する

Cisco APIC-EM はデバイスおよびホストを検出し、検出結果をデバイスおよびホストのインベントリ データベースに入力します。

デバイスおよびホストを検出するには、SNMPv2c クレデンシャルまたは SNMPv3 クレデンシャル、SNMPv2c クレデンシャルまたは SNMPv3 クレデンシャルの両方を設定する必要があります（ネットワークによります）。SNMPv2 の場合、SNMP 読み取りコミュニティ クレデンシャルのみ必須です。

CLI クレデンシャルも必須です。デバイスの設定ファイルにアクセスするには、CLI クレデンシャルを設定します。

これらのクレデンシャルは、次の Cisco APIC-EM GUI の 2 つの異なる場所で設定できます。

- [設定（Settings）] > [検出クレデンシャル（Discovery Credentials）] ウィンドウ：ネットワークのすべてまたはほとんどのサービスに共通している場合、このウィンドウに SNMP および CLI クレデンシャルを設定します。これらのクレデンシャルは、グローバル クレデンシャルと呼ばれます。
- [検出（Discovery）] ウィンドウ：デバイスを迅速に検出する場合、または大部分のデバイスがネットワーク接続されている一般的な SNMP および CLI クレデンシャルを持たず、[設定（Settings）]> [検出クレデンシャル（Discovery Credentials）] ウィンドウに設定されたデバイ

スを必要とする場合は、このウィンドウの SNMP および CLI クレデンシャルを設定します。これらのクレデンシャルは、例外のクレデンシャルと呼ばれます。

ワイヤレス LAN コントローラ（WLC）には検出するための追加の設定要件があります。詳細については、ワイヤレス LAN コントローラの検出を理解する，（12 ページ）を参照してください。

ワイヤレス LAN コントローラの検出を理解する

Cisco APIC-EM は、複数の Cisco ワイヤレス LAN コントローラ（WLC）から SNMP トラップを受け入れます。SNMP トラップはホスト インベントリのデータベースを更新するのに使用されます。Cisco APIC-EM がトラップ レシーバで、WLC が拡張トラップを Cisco APIC-EM に送信するため、WLC 設定が必要です。

次の WLC は、SNMP トラップを有効にする必要があります。

- Cisco シリーズ 2504 ワイヤレス LAN コントローラ
- Cisco シリーズ 5508 ワイヤレス LAN コントローラ
- Cisco シリーズ 8510 ワイヤレス LAN コントローラ
- Cisco Wireless Service Module 2（WiSM2）

次の表に、WLC での設定が必要なオブジェクト ID と SNMP トラップを指定します。

トラップ名	OID
ciscoLwappDot11ClientAssocTrap	1.3.6.1.4.1.9.9.599.0.9
ciscoLwappDot11ClientDeAuthenticatedTrap	1.3.6.1.4.1.9.9.599.0.10
ciscoLwappDot11ClientMovedToRunStateNewTrap	1.3.6.1.4.1.9.9.599.0.11
ciscoLwappDot11ClientMobilityTrap	1.3.6.1.4.1.9.9.599.0.12

次の設定は、上記の SNMP トラップを有効にするために設定する必要があります。

- config trapflags client enhanced-802.11-associate enable
- config trapflags client enhanced-802.11-deauthenticate enable
- config trapflags client enhanced-authentication enable
- config trapflags client enhanced-802.11-stats enable

（注） WLC の SNMP トラップを設定するときは、SNMP トラップの宛先 IP アドレスとしての Cisco APIC-EM の IP アドレスが設定されていることを確認してください。

検出の使用

CDP を使用した検出の実行

CDP を使用して検出を実行できます。

検出の実行中に、以下のアクションを実行できます。

- [検出（Discovery）] ペインで [新規追加（Add New）] をクリックして新しい検出を作成する。
- [検出（Discovery）] ペインで検出名を選択し、[検出の詳細（Discovery Details）] ペインで [停止（Stop）] をクリックすることにより、アクティブな検出を停止する。
- [検出（Discovery）] ペインで検出名を選択し、[検出の詳細（Discovery Details）] ペインで [開始（Start）] をクリックすることにより、非アクティブな検出を開始する。
- [検出（Discovery）] ペインで検出名を選択し、[検出の詳細（Discovery Details）] ペインで [削除（Delete）] をクリックすることにより、検出を削除する。

はじめる前に

管理者権限が必要です。ユーザ権限に関する詳細については、ユーザおよびロールの管理, （49 ページ）を参照してください。

検出対象のデバイスで CDP を有効にする必要があります。

ステップ 1 [ナビゲーション（Navigation）] ペインで、[検出（Discovery）] をクリックします。
[検出（Discovery）] ウィンドウが表示されます。

ステップ 2 （任意） [検出名（Discovery Name）] フィールドに、この検出の一意の名前を入力します。

ステップ 3 [IP 範囲（IP Ranges）] 領域で、次の手順を実行します。

a) [検出タイプ（Discovery Type）] フィールドで、[CDP] を選択します。

b) [IP アドレス（IP Address）] フィールドに、検出スキャンの開始点として使用する Cisco APIC-EM の IP アドレスを入力します。

ステップ 4 [SNMP] 領域で、検出するデバイスによって使用されている SNMP バージョンの 1 つまたは両方を設定します。
以下のガイドラインと、表に記載されている情報を使用して、フィールドに正しい値を入力するために役立ててください。

- コントローラでは複数の SNMP クレデンシャル設定がサポートされますが、5 個より多いクレデンシャル セット（グローバルまたは除外、SNMPv2c または SNMPv3 のクレデンシャル）を設定すると、エラー メッセージが表示されます。

- 検出およびインベントリへの入力が正常に行われるためには、SNMP 読み取り専用（RO）コミュニティ ストリングが必要です。SNMP RO コミュニティ ストリングが指定されていない場合、ベストエフォートとして、デフォルトの SNMP RO コミュニティ ストリング「public」を使用して検出が実行されます。

表 *4*：*SNMPv2c*

フィールド	説明
読み取りコミュニティ（Read Community）	SNMP の読み取り専用（RO）または読み取り/書き込み（RW）のコミュニティ ストリング。 このフィールドに設定する SNMP コミュニティ ストリングは、この特定の検出にのみ使用されます。保存可能なすべての検出で使用できるデフォルトの SNMP コミュニティ ストリングをセットアップするには、[設定（Settings）] > [検出クレデンシャル（Discovery Credentials）] の順にクリックします。 （注） ネットワーク デバイスの検出を有効にするには、ネットワーク デバイスの IP ホスト アドレスをクライアント アドレスとして設定します。
書き込みコミュニティ（Write Community）	SNMP の読み取り専用（RO）または読み取り/書き込み（RW）のコミュニティ ストリング。

（注） 選択内容に応じて、特定の [SNMPv3] 設定オプションは使用できる場合も使用できない場合もあります。

表 *5*：*SNMPv3*

フィールド	説明
[ユーザ名（Username）]	SNMPv3 設定に関連付けられるユーザ名。
[モード（Mode）]	SNMP メッセージが必要とするセキュリティ レベル、およびメッセージの認証が必要かどうかを指定します。次のいずれかのモードを選択します。 • noAuthNoPriv：認証または暗号化を実行しないセキュリティ レベル • AuthNoPriv：認証は実行するが、暗号化を実行しないセキュリティ レベル • AuthPriv：認証と暗号化両方を実行するセキュリティ レベル

フィールド	説明
認証タイプ（Auth Type）	使用する認証タイプを指定します。 • SHA：ハッシュ ベースのメッセージ認証コード（HMAC）、セキュア ハッシュ アルゴリズム（SHA）に基づく認証 • MD5：ハッシュ ベースのメッセージ認証コード（HMAC）、Message Digest 5（MD5）アルゴリズムに基づく認証 • なし（None）：認証を行いません。
認証パスワード（Auth Password）	SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。
プライバシー タイプ（Privacy Type）	プライバシー タイプを指定します。 • DES：データ暗号規格（DES）の 56 ビット暗号化、および暗号ブロック連鎖（CBC）DES（DES-56）標準に基づいて認証します。 • AES128：暗号ブロック連鎖（CBC）モード AES を暗号化に使用します。 • なし（None）：プライバシーなし。
プライバシー パスワード（Privacy Password）	SNMPv3 プライバシー パスワードは、DES 暗号化または AES128 暗号化をサポートするデバイスと交換するメッセージの暗号化に使用する秘密キーの生成に使用されます。

表 *6*：*SNMP* のプロパティ

フィールド	説明
接続タイムアウト (秒)（Connection Timeout (in Seconds)）	デバイスとの接続を確立する際、タイムアウトするまでコントローラが待機する秒数。有効な値は 5 ～ 120 秒（5 秒単位）です。
再試行回数（Retry Count）	デバイスへの接続試行回数。有効な値は 0 ～ 4 回の試行です。

ステップ 5 [CLI クレデンシャル（CLI Credentials）] 領域で、Cisco APIC-EM で検出するデバイスのフィールドにユーザ名、パスワード、およびイネーブル パスワードを入力します。
パスワードとイネーブルパスワードはセキュリティ上の理由から暗号化されており、設定を表示した際に見ることはできません。

検出クレデンシャルは、ネットワーク内のシスコ デバイスを認証および検出するために Cisco APIC-EM によって使用される既存のデバイス クレデンシャルです。Cisco APIC-EM では、共通検出クレデンシャルと除外検出クレデンシャルという 2 つのタイプの検出クレデンシャルがサポートされます。

（注） 検出スキャンごとに 1 セットのみの検出クレデンシャルに限定されますが、ネットワーク内のシスコ デバイスすべてを認証し、検出するために、異なるクレデンシャルを使って複数の検出スキャンを実行できます。

ステップ 6 （任意） [詳細設定（Advanced）] 領域で、Cisco APIC-EM がデバイスへの接続に使用するプロトコルを設定します。
デフォルトでは、Cisco APIC-EM は以下のプロトコルを使用します。

- SSH
- Telnet

スキャンからプロトコルを削除するには、プロトコル名をクリックします。プロトコルの横にあるチェックマークが消え、プロトコルはディスプレイから徐々に消えます。

デバイスへの接続に使用されるプロトコルの順序をカスタマイズするには、選択したプロトコルを一覧内の目的の位置にドラッグ アンド ドロップします。

ステップ 7 [検出の開始（Start Discovery）] をクリックします。
[検出（Discoveries）] ウィンドウにスキャンの結果が表示されます。

[検出の詳細（Discovery Details）] ペインに、ステータス（アクティブまたは非アクティブ）および検出設定が表示されます。 [検出デバイス（Discovery Devices）] ペインに、選択されたディスカバリで検出されたデバイスのホスト名、IP アドレス、およびステータスが表示されます。

IP アドレス範囲を使用した検出の実行

IP アドレス範囲を使用してデバイスを検出できます。
検出の実行中に、以下のアクションを実行できます。

- [検出（Discovery）] ペインで [新規追加（Add New）] をクリックして新しい検出を作成する。
- [検出（Discovery）] ペインで検出名を選択し、[検出の詳細（Discovery Details）] ペインで [停止（Stop）] をクリックすることにより、アクティブな検出を停止する。
- [検出（Discovery）] ペインで検出名を選択し、[検出の詳細（Discovery Details）] ペインで [開始（Start）] をクリックすることにより、非アクティブな検出を開始する。
- [検出（Discovery）] ペインで検出名を選択し、[検出の詳細（Discovery Details）] ペインで [削除（Delete）] をクリックすることにより、検出を削除する。

はじめる前に

管理者権限が必要です。ユーザ権限に関する詳細については、ユーザおよびロールの管理, （49 ページ）を参照してください。

ステップ 1 [ナビゲーション（Navigation）] ペインで、[検出（Discovery）] をクリックします。
[検出（Discovery）] ウィンドウが表示されます。

ステップ 2 （任意） [検出名（Discovery Name）] フィールドに、この検出の一意の名前を入力します。

ステップ 3 [IP 範囲（IP Ranges）] 領域で、次の手順を実行します。

a) [検出タイプ（Discovery Type）] フィールドで、検出スキャン タイプの [範囲（Range）] を選択します。

b) [IP アドレス（IP Address）] フィールドに、検出されるデバイスの最初と最後の IP アドレス（IP 範囲）を入力し、[追加（Add）] をクリックします。
検出スキャンに対して、単一の IP アドレス範囲または複数の IP アドレスを入力できます。

c) 追加の IP アドレスを IP アドレス フィールドに入力し、[追加（Add）] をクリックします。

ステップ 4 [SNMP] 領域で、ネットワーク内のデバイスによって使用されている SNMP バージョンの 1 つまたは両方を設定します。
次のガイドラインと、以下の表に記載されている情報を使用して、フィールドに正しい値を入力してください。

- コントローラでは最大 5 つの SNMP クレデンシャル設定がサポートされます。
- 検出およびインベントリへの入力が正常に行われるためには、SNMP 読み取り専用（RO）コミュニティ ストリングが必要です。ただし、*SNMP RO* コミュニティ ストリングが指定されていない場合、ベストエフォートの検出スキャンとして、デフォルトの *SNMP RO* コミュニティ ストリング「*public*」を使用して検出が実行されます。

表 *7* : *SNMPv2c*

フィールド	説明
読み取りコミュニティ（Read Community）	SNMP の読み取り専用（RO）または読み取り/書き込み（RW）のコミュニティ ストリング。 このフィールドに設定する SNMP コミュニティ ストリングは、この特定の検出にのみ使用されます。保存可能なすべての検出で使用できるデフォルトの SNMP コミュニティ ストリングをセットアップするには、[設定（Settings）] > [検出クレデンシャル（Discovery Credentials）] の順にクリックします。 （注） ネットワーク デバイスの検出を有効にするには、ネットワーク デバイスの IP ホスト アドレスをクライアント アドレスとして設定します。
書き込みコミュニティ（Write Community）	SNMP の読み取り専用（RO）または読み取り/書き込み（RW）のコミュニティ ストリング。

（注） 選択内容に応じて、特定の [SNMPv3] 設定オプションは使用できる場合とできない場合があります。

表 *8*：*SNMPv3*

フィールド	説明
[ユーザ名（Username）]	SNMPv3 設定に関連付けられるユーザ名。
[モード（Mode）]	SNMP メッセージが必要とするセキュリティ レベル、およびメッセージの認証が必要かどうかを指定します。次のいずれかのモードを選択します。 • noAuthNoPriv：認証または暗号化を実行しないセキュリティ レベル • AuthNoPriv：認証は実行するが、暗号化を実行しないセキュリティ レベル • AuthPriv：認証と暗号化両方を実行するセキュリティ レベル
認証タイプ（Auth Type）	使用する認証タイプを指定します。 • SHA：ハッシュ ベースのメッセージ認証コード（HMAC）、セキュア ハッシュ アルゴリズム（SHA）に基づく認証 • MD5：ハッシュ ベースのメッセージ認証コード（HMAC）、Message Digest 5（MD5）アルゴリズムに基づく認証 • なし（None）：認証を行いません。
認証パスワード（Auth Password）	SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。
プライバシー タイプ（Privacy Type）	プライバシー タイプを指定します。 • DES：データ暗号規格（DES）の 56 ビット暗号化、および暗号ブロック連鎖（CBC）DES（DES-56）標準に基づいて認証します。 • AES128：暗号ブロック連鎖（CBC）モード AES を暗号化に使用します。 • なし（None）：プライバシーなし。
プライバシー パスワード（Privacy Password）	SNMPv3 プライバシー パスワードは、DES 暗号化または AES128 暗号化をサポートするデバイスと交換するメッセージの暗号化に使用する秘密キーの生成に使用されます。

表 *9* : ***SNMP*** のプロパティ

フィールド	説明
接続タイムアウト(秒)（Connection Timeout (in Seconds)）	デバイスとの接続を確立する際、タイムアウトするまでコントローラが待機する秒数。有効な値は 5 ～ 120 秒（5 秒単位）です。
再試行回数（Retry Count）	デバイスへの接続試行回数。有効な値は 0 ～ 4 回の試行です。

ステップ 5 [CLI クレデンシャル（CLI Credentials）] 領域で、検出するデバイスについての除外ユーザ名、パスワード、およびイネーブル パスワードを入力します。最大 5 つの CLI クレデンシャルを追加できます。

（注） パスワードとイネーブル パスワードはセキュリティ上の理由から暗号化されており、設定を表示した際に見ることはできません。

（注） 検出スキャンごとに 1 セットのみの検出クレデンシャルに限定されますが、ネットワーク内のシスコ デバイスすべてを認証し、検出するために、異なるクレデンシャルを使って複数の検出スキャンを実行できます。

ステップ 6 （任意） [詳細設定（Advanced）] 領域で、Cisco APIC-EM がデバイスへの接続に使用するプロトコルを設定します。

デフォルトでは、Cisco APIC-EM は以下のプロトコルを使用してデバイスに接続します。

- SSH
- Telnet

スキャンからプロトコルを削除するには、プロトコル名をクリックします。プロトコルの横にあるチェックマークが消え、プロトコルはビューから徐々に消えます。

接続に使用されるプロトコルの順序をカスタマイズするには、プロトコルを一覧にドラッグアンドドロップします。

ステップ 7 [検出の開始（Start Discovery）] をクリックします。

[検出（Discoveries）] ウィンドウにスキャンの結果が表示されます。

[検出の詳細（Discovery Details）] ペインに、ステータス（アクティブまたは非アクティブ）および検出設定が表示されます。 [検出デバイス（Discovery Devices）] ペインに、選択されたディスカバリで検出されたデバイスのホスト名、IP アドレス、およびステータスが表示されます。

検出の停止と開始

進行中の検出を停止してから再起動することができます。

はじめる前に

管理者権限が必要です。ユーザ権限に関する詳細については、ユーザおよびロールの管理, （49 ページ）を参照してください。

ステップ 1 [ナビゲーション（Navigation）] ペインで、[検出（Discovery）] をクリックします。
[検出（Discovery）] ウィンドウが表示されます。

ステップ 2 アクティブな検出を停止するには、次の手順を実行します。

a) [検出（Discovery）] ペインで、検出を選択します。
b) [検出の詳細（Discovery Details）] ペインで、[停止（Stop）] をクリックします。
c) [OK] をクリックして、検出を停止することを確認します。

ステップ 3 非アクティブな検出を再起動するには、次の手順を実行します。

a) [検出（Discovery）] ペインで、検出を選択します。
b) [検出の詳細（Discovery Details）] ペインで、[開始（Start）] をクリックします。

検出の削除

アクティブまたは非アクティブに関係なく、検出を削除できます。

はじめる前に

管理者権限が必要です。ユーザ権限に関する詳細については、ユーザおよびロールの管理, （49 ページ）を参照してください。

ステップ 1 [ナビゲーション（Navigation）] ペインで、[検出（Discovery）] をクリックします。
[検出（Discovery）] ウィンドウが表示されます。

ステップ 2 [検出（Discovery）] ペインで、削除する検出を選択します。

ステップ 3 [検出の詳細（Discovery Details）] ペインで、[削除（Delete）] をクリックします。

ステップ 4 [OK] をクリックして、検出を削除することを確認します。

検出結果を理解する

[検出（Discovery）] ウィンドウは、選択したスキャンに関する情報を表示します。[検出（Discovery）] ウィンドウに、[ナビゲーション（Navigation）] ペインからアクセスするには、[検

出（Discovery）] をクリックします。[検出結果（Discovery Results）] ウィンドウには、3 つのメイン ペインがあります。

（注） 表示する [検出結果（Discovery Results）] ウィンドウには、少なくとも 1 つの検出スキャンを作成しておく必要があります。

図 *3* : *[*検出結果（***Discovery Results***）*]* ウィンドウ

コールアウト番号	[名前（Name）]	説明
1	[検出（Discovery）] ペイン	検出に使用するメソッドおよびIPアドレスとともに、作成された検出スキャンの名前を表示します。リストは、アクティブおよび非アクティブの検出の間で分割されます。 成功したスキャン（検出および認証されたデバイス）では、検出されたデバイスの数が検出名の右側のボックスに表示されます。失敗したスキャンでは、ボックスまたは検出されたデバイスの数が表示されません。 [検出（Discovery）] ペインで、検出名をクリックすると、[検出の詳細（Discovery Details）] ペインと [デバイスの詳細（Device Details）] ペインの情報が表示されます。
2	[検出の詳細（Discovery Details）] ペイン	検出、検出の状態、検出されたデバイスの数を実行するために使用された検出パラメータの詳細を提供します。このペインのボタンで、[開始（Start）]、[停止（Stop）]、および [削除（Delete）] の検出が可能です。
3	[デバイス（Devices）] ペイン	スキャン中に見つかったデバイスのホスト名、IPアドレス、および状態を表示します。

第 3 章

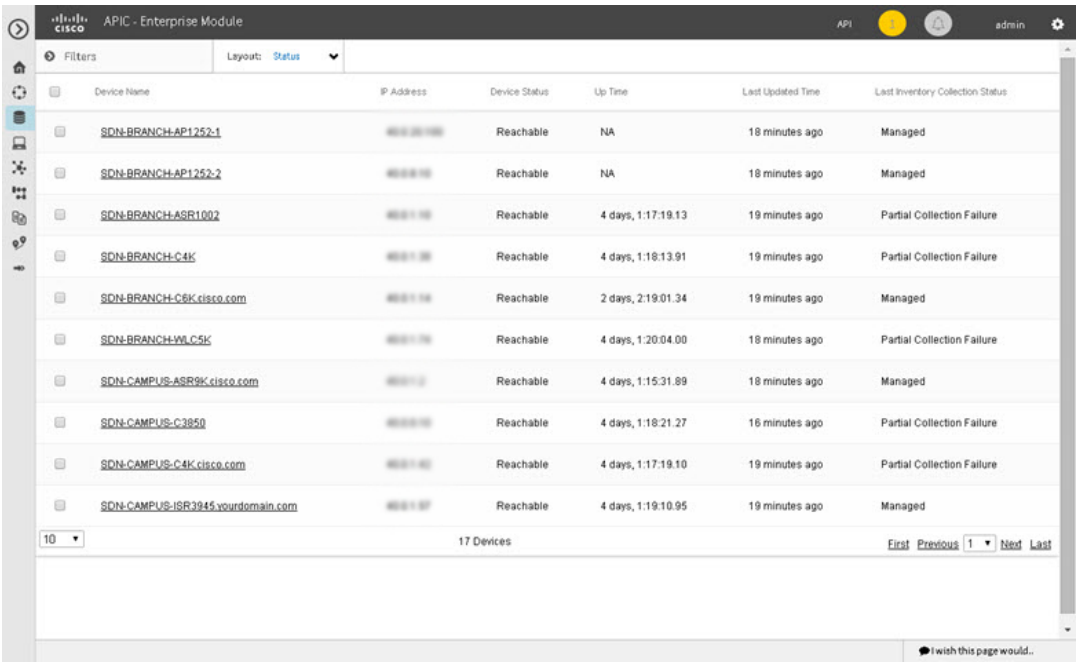
デバイスおよびホストの管理

- デバイス インベントリの管理，25 ページ
- ホスト インベントリの管理，45 ページ

デバイス インベントリの管理

[デバイスインベントリ（Device Inventory）] ウィンドウに、検出スキャンの結果が表示されます。[検出（Discovery）] ウィンドウに、[ナビゲーション（Navigation）] ペインからアクセスするには、[デバイス インベントリ（Device Inventory）] をクリックします。[デバイス インベントリ（Device Inventory）] ウィンドウが表示されます。

図 *4* : *[デバイス インベントリ（Device Inventory）]* ウィンドウ



（注） 表示される情報は、選択したレイアウトによって異なります。

最初の検出後、ネットワーク デバイスは 30 分ごとにポーリングされます。ポーリングはデバイス、リンク、ホスト、およびインターフェイスごとに実行されます。アクティブ状態が一日未満のデバイスのみが表示されます。これによって、古いデバイス データが表示されないようにします。500 個のデバイスのポーリングに約 20 分かかります。

コールアウト番号	[名前（Name）]	説明
1	[デバイスの選択（Device Selection）] チェックボックス	タスクを実行するデバイスを選択します。
2	フィルタ（Filters）	名前別、ロケーション タグ別、IP アドレス別でテーブルに表示されるデバイスを選択的にスクリーニングできます。
3	レイアウト（Layout）	次の 3 つの定義済みレイアウト、またはカスタマイズしたレイアウトから選択できます。 • ステータス（Status）：レイアウトでは、デバイス名、IP アドレス、デバイスの状態、稼動時間、最終更新時間が表示されます。 • ハードウェア（Hardware）：レイアウトでは、デバイス名、IP アドレス、デバイス ファミリ、プラットフォーム、シリアル番号、MAC アドレス、ロール、および IOS/ファームウェアのバージョンとコンフィギュレーション ファイルへのリンクが表示されます。 • タギング（Tagging）：レイアウトでは、デバイス名、IP アドレス、MAC アドレス、デバイス ロール、ロケーション、およびタグが表示されます。

[デバイス インベントリ（Device Inventory）] テーブルの下で、テーブルに表示されるデバイス数（10、25、50、100）を調整できます。[最初（First）]、[前（Previous）]、[次（Next）]、[最後（Last）]、またはページ番号をクリックして、テーブル間を移動します。

[デバイス インベントリ（Device Inventory）] テーブルに、検出された各デバイスに関する次の情報が表示されます。[構成（Config）] カラムを除く、すべてのカラムではソートをサポートします。カラム ヘッダーをクリックすると、行が昇順にソートされます。カラム ヘッダーを再度クリックすると、行が降順にソートされます。

表 *10*：デバイス インベントリ（***Device Inventory***）

デバイス インベントリ（**Device Inventory**）	説明
デバイスの状態（Device Status）	デバイスの状態。 • 接続中（Connecting）：コントローラがデバイスに接続しています。 • 認証済み（Authenticated）： ◦ 検出済み（Discovered）：コントローラがデバイスに接続し、CLIを使用してシスコ コマンドを実行できます。 ◦ 失敗（Failure）：コントローラがデバイスに接続しましたが、CLIを使用してシスコ コマンドを実行できません。この状態は通常、デバイスがシスコ デバイスではないことを示します。 • 認証失敗（Authentication Failed）：コントローラがデバイスに接続しましたが、どのタイプのデバイスであるか判断できません。このデバイスの状態も通常は、デバイスがシスコ デバイスではないことを示します。 • 到達不能（Not reachable）：コントローラがデバイスに接続できません。 （注） ディスカバリ要求の前にクレデンシャルが提供されていない場合に、デバイスの状態が「到達不能」と表示されます。正しいクレデンシャルを提供した上で新しく検出を実行する必要があります。

デバイス インベントリ（**Device Inventory**）	説明
デバイス名（Device Name）	デバイスの名前。[デバイス概要（Device Overview）] ダイアログボックスに次の情報を表示するには、デバイス名をクリックします。 • デバイス シリアル番号（Device serial number） • デバイスの IP アドレス（Device IP address） • MAC アドレス • Cisco OS バージョン（Cisco OS version） • 使用可能時間（Up time） • 製品 ID • ベンダー（Vendor） • メモリ サイズ（Memory size） （注） インベントリが 30 分以上更新されていないデバイスに対して、デバイス名が赤色で表示されます。 [デバイス概要（Device Overview）] ダイアログボックスには、次のインターフェイスデータを含む [インターフェイス（Interfaces）] タブも含まれます。 • 状態（Status）：アップまたはダウン。 • インターフェイス名（Interface Name）：インターフェイスの名前。 • MACアドレス（MAC Address）：インターフェイスの MAC アドレス。
MAC アドレス（MAC Address）	デバイスの MAC アドレス。
[IPアドレス（IP Address）]	デバイスの IP アドレス。
IOS/ファームウェア（IOS/Firmware）	現在デバイス上で実行されている Cisco IOS ソフトウェア。
プラットフォーム	シスコ製品の部品番号。
シリアル番号（Serial Number）	シスコ デバイスのシリアル番号。

デバイス インベントリ（**Device Inventory**）	説明
使用可能時間（Up Time）	デバイスが起動してから、稼働している時間。
構成	CLI の **show running-config** コマンドの出力と同様の設定情報を表示するには、[表示（View）] をクリックします。 （注） この機能は、アクセス ポイントとワイヤレス LAN コントローラではサポートされていないため、これらのデバイス タイプに対して設定データは返されません。
デバイス ロール（Device Role）	スキャンプロセス中に、検出された各デバイスに割り当てられているロール。デバイス ロールは、ネットワーク内での役目と配置に従って、デバイスを識別およびグループ分けするために使用されます。コントローラがデバイス ロールを確認できない場合、デバイス ロールは不明と設定されます。 （注） ネットワーク トポロジが変更されるのに従い、コントローラはデバイス ロールを変更できますが、デバイス ロールを手動で変更する場合は、そのロールはネットワーク トポロジの変更に伴い変更されません。 必要に応じて、このカラムのドロップダウン リストを使用して、割り当てられたデバイス ロールを変更することができます。次のデバイス ロールを使用できます。 • 不明 • アクセス（Access） • コア • ディストリビューション（Distribution） • ボーダー ルータ（Border Router）

デバイス インベントリ（**Device Inventory**）	説明
参照先	1 つのデバイスに適用できるロケーションは 1 つのみです。ロケーション情報は APIC-EM コントローラでのみ保持されます。デバイスに適用されるロケーションはデバイス自体から入手することはできません。APIC-EM ロケーションは、いくつかのデバイスがサポートする「シビックロケーション」プロパティではありません。トポロジビューでロケーションを作成したり使用することはできません。そのため、ロケーションをホストに接続することはできず、トポロジビューのロケーションを検索することはできません。ロケーションは、デバイスに適用できる特定のタイプのタグです。タグは属性に基づいてデバイスのグループ化を有効にします。 [ロケーション（Location）] ウィンドウを開くには、このカラムで [追加（Add）] をクリックします。このウィンドウで既存または新規のロケーションのいずれかを追加できます。 また、デバイスにワールド マップの地理的なマーカーを追加することもできます。デバイスに地理的マーカーを追加するには、次の手順を実行します。 • [マーカーの追加（Add Marker）] をクリックして、マーカーアイコンをワールドマップのロケーションに移動します。 • ワールド マップのロケーションに正確な座標を設定するには、[座標の設定（Set Coordinates）] をクリックします。 • ワールド マップからマーカーを削除するには、[マーカーの削除（Remove Marker）] をクリックします。 ワールド マップを、[トポロジ（Topology）] ウィンドウで表示するには、[マップ（Map）] アイコンをクリックします。 （注） ロケーション タグはデバイスごとに 1 つだけ適用できます。

デバイス インベントリ（**Device Inventory**）	説明
タグ	特定するため、または同じ属性を持つ他のデバイスとグループ化するためにデバイスに割り当てる属性。たとえば、プラットフォーム ID、Cisco IOS リリース、またはロケーションに基づいて、タグを作成してデバイスをグループ化できます。 [タグ（Tag）] カラムの数字は、そのデバイスに適用されたタグの数を示します。 [タグ（Tag）] ダイアログボックスを開くには、このカラムの数値または [追加（Add）] をクリックします。既存のタグを追加するか、新しいタグを作成できます。 （注） ロケーション タグとデバイス タグの両方を同時に使用することができます。 （注） 全体的にタグを削除するには、まず接続しているデバイスからタグを削除します。
最終更新時間（Last Updated Time）	デバイスが最後にスキャンされ、コントローラ データベースが更新された日付と時刻。
デバイス ファミリ（Device Family）	関連するデバイス グループ。 • シスコ インターフェイスおよびモジュール • ルータ • スイッチおよびハブ • サードパーティ デバイス • サポート対象外のシスコ デバイス • ワイヤレス コントローラ
デバイス シリーズ（Device Series）	デバイスのシリーズ番号（たとえば、Cisco Catalyst 4500 シリーズ スイッチ）。
平均更新頻度（Average Update Frequency）	デバイスが更新される平均間隔（単位：分）。デフォルトでは、デバイスは 25 分おきにポーリングされます。

デバイス インベントリ（Device Inventory）	説明
最終インベントリ収集ステータス（Last Inventory Collection Status）	デバイス最終検出のスキャン状態。 • 管理対象（Managed）：デバイスが完全に管理されている状態にあります。 • 部分的な収集の失敗（Partial Collection Failure）：デバイスが部分的に収集された状態であり、すべてのインベントリ情報が集められませんでした。 • 到達不能（Unreachable）：デバイス接続の問題が原因で、デバイスが到達できず、インベントリ情報を集められませんでした。この状態は定期的に収集される際に発生することがあります。 • 誤ったクレデンシャル（Wrong Credentials）：デバイス クレデンシャルがデバイスをインベントリに追加した後に変更された場合、この状態が表示されます。 • 進行中（In Progress）：インベントリ収集が実行されています。

関連トピック

デバイス ロールの変更, （34 ページ）
タグの追加および削除, （36 ページ）
複数のデバイスへのタグの追加または削除
ロケーション タグの追加または削除, （40 ページ）
ロケーション マーカーの追加, （41 ページ）

デバイス テーブル ビューのフィルタリング

[デバイス（Devices）] テーブルに表示されるデバイスを、デバイス名、ロケーション、および IP アドレスでフィルタリングできます。

はじめる前に

[ナビゲーション（Navigation）] ペインで [デバイス インベントリ（Device Inventory）] をクリックして、[デバイス インベントリ（Device Inventory）] ウィンドウにアクセスします。

ステップ 1 [デバイス インベントリ（Device Inventory）] ツールバーで、[フィルタ（Filters）] をクリックします。
以下のフィルタが表示されます。

- デバイス名（Device Name）
- デバイス ロケーション（Device Location）
- Device IP Address（デバイス IP アドレス）

ステップ 2 選択したフィルタのフィールドに適切な値を入力します。
たとえば、[デバイスの IP アドレス（Device IP Address）] フィルタに IP アドレスを入力します。

（注） IP アドレスや他のフィールドに入力するときに、コントローラにより自動入力値が提示されます。いずれかの推奨値を選択するか、または IP アドレスの入力を完了します。

（注） これらのフィルタにワイルドカード（アスタリスク）を使用することもできます。文字列値の先頭、末尾、または中間にアスタリスクがある値を入力できます。

ステップ 3 プラス（+）アイコンをクリックして、フィルタを実行します。
[デバイス（Devices）] テーブルに表示されるデータは、フィルタ選択に従って自動的に更新されます。

ステップ 4 （省略可能）フィルタで必要な場合、上記の手順に従って 1 つ以上のフィルタを追加します。

（注） フィルタごとに複数の値でフィルタリングすることも、複数の異なるフィルタ タイプでフィルタリングすることもできます。

ステップ 5 [x] アイコンをクリックしてフィルタ フィールドを閉じ、元の [デバイス（Devices）] テーブル表示に戻ります。

次の作業

[デバイス インベントリ（Device Inventory）] ウィンドウに表示される更新された情報を確認します。ネットワーク構成で必要な場合は、[デバイス（Devices）] テーブル ビューに表示されるカラムを変更します。

デバイス レイアウト ビューの変更

さまざまなレイアウト ビューを選択、またはネットワーク内のデバイスのレイアウト ビューをカスタマイズすることにより、[デバイス（Devices）] テーブルに表示される情報を変更できます。

はじめる前に

[ナビゲーション（Navigation）] ペインで [デバイス インベントリ（Device Inventory）] をクリックして、[デバイス インベントリ（Device Inventory）] ウィンドウにアクセスします。

ステップ 1 [デバイス インベントリ（Device Inventory）] ツールバーでで、レイアウト オプションを選択します。次のレイアウト オプションを使用できます。

- ステータス（Status）：アップ タイム、更新頻度、更新回数などの一般的なデバイス ステータス情報を表示します。
- ハードウェア（Hardware）：IOS/ファームウェア、シリアル番号、デバイス ロールなどのハードウェア情報を表示します。
- タギング（Tagging）：デバイス ロール、場所、タグなどのタギング情報を表示します。
- カスタマイズ（Customize）：独自のレイアウトを作成するために選択できるオプションのリストを表示します。

特定のレイアウトを選択した後、[デバイス（Devices）]テーブル内の情報が新しい表示に合わせて調整されます。

ステップ 2 特定のレイアウトをカスタマイズするには、[カスタマイズ（Customize）]および目的の表示オプションを選択します。

（注） 表示オプションは、オプションがオンであることを示すチェックマークのオンとオフで切り替わります（テーブルに表示）。

選択後、新しいカラムが [デバイス（Devices）] テーブルに追加され、リストで選択したオプションのチェック マークが青色に変わります。

次の作業

[デバイス インベントリ（Device Inventory）] ウィンドウに表示される更新された情報を確認します。ご使用のネットワーク構成で必要な場合、次のカラムを調整します。

- デバイス ロール
- 参照先
- タグ

デバイス ロールの変更

スキャン プロセス中、コントローラは、検出された各デバイスにロールを割り当てます。デバイス ロールは、ネットワークにおける責任と配置に従ったデバイスの識別とグループ化に使用されます。

デバイスは、以下のいずれかのロールを持つことができます。

- 不明：デバイス ロールが不明です。
- アクセス：デバイスはネットワークのアクセス レイヤまたは第 1 階層/エッジに配置され、必要なタスクを実行します。
- ボーダー ルータ：デバイスはボーダー ルータで必要なタスクを実行します。
- ディストリビューション：デバイスはネットワークのディストリビューション レイヤに配置され、必要なタスクを実行します。
- コア：デバイスはネットワークのコアに配置され、必要なタスクを実行します。

デバイス ロールは、[デバイス インベントリ（Device Inventory）] ウィンドウで変更できます。

（注） デバイス ロールは、[トポロジ（Topology）] ウィンドウでも変更できます。[トポロジ（Topology）] ウィンドウでのデバイス ロールの変更，（80 ページ）を参照してください。

はじめる前に

デバイス ロールを変更するには、[デバイス インベントリ（Device Inventory）] ウィンドウにアクセスします。

（注） 次の手順を実行するには、管理者権限が必要です。Cisco APIC-EM を使用してタスクを実行するために必要なユーザ権限の詳細については、第4章「ユーザおよびロールの管理」を参照してください。

ステップ 1 [ナビゲーション（Navigation）] ペインで、[デバイス インベントリ（Device Inventory）] をクリックします。
[デバイス インベントリ（Device Inventory）] ウィンドウが表示されます。

ステップ 2 [デバイス インベントリ（Device Inventory）] ツールバーで、[レイアウト（Layout）] ドロップダウン リストからいずれかのオプションを選択します。
有効なオプションは、[ハードウェア（Hardware）] 、[タギング（Tagging）] 、または [カスタマイズ（Customize）]>[デバイス ロール（Device Role）] です。テーブルが更新され、[デバイス ロール（Device Role）] のカラムが含まれています。

ステップ 3 変更するデバイスを見つけ、[デバイス ロール（Device Role）] カラムでドロップダウン リストから新しいロールを選択します。
有効な選択肢は、[不明（Unknown）] 、[アクセス（Access）] 、[コア（Core）] 、[ディストリビューション（Distribution）] 、または [ボーダー ルータ（Border Router）] です。

次の作業

必要に応じて、[デバイス インベントリ（Device Inventory）] ウィンドウで他のデバイスのロールを変更します。

関連トピック

デバイス インベントリの管理, （25 ページ）

デバイスの削除

[デバイス インベントリ（Device Inventory）] ウィンドウで、Cisco APIC-EM データベースからデバイスを削除できます。

はじめる前に

管理者権限を持っていることを確認します。ユーザ権限に関する詳細については、ユーザおよびロールの管理, （49 ページ）を参照してください。

Cisco APIC-EM の検出機能を使用してネットワークがスキャンされ、デバイス インベントリ データベースに入力されていることを確認します。

ステップ 1 [ナビゲーション（Navigation）] ペインで、[デバイス インベントリ（Device Inventory）] をクリックします。
[デバイス インベントリ（Device Inventory）] ウィンドウが表示されます。

ステップ 2 削除するデバイスの横にあるチェックボックスをクリックします。
ツールバーが開きます。

（注） ツールバーが開いた後で、その他のチェックボックスをクリックして複数のデバイスを選択することも、リストの上部にあるチェックボックスをクリックしてすべてのデバイスを選択することもできます。

ステップ 3 開いたツールバーで、[削除（Delete）] をクリックします。

タグの追加および削除

デバイス タグは属性に基づいてデバイスをグループ化することができます。たとえば、プラットフォーム ID、Cisco IOS リリース、またはロケーションに基づいてタグを追加してデバイスをグループ化できます。

（注） 単一のデバイスに複数のタグを設定できます。同様に、複数のデバイスに適用できる単一のタグもあります。

[デバイス インベントリ（Device Inventory）] ウィンドウのデバイスに対してタグを追加したり、削除できます。

はじめる前に

（注） 管理者権限が必要です。ユーザ権限に関する詳細については、ユーザおよびロールの管理，（49 ページ）を参照してください。

ステップ 1 [ナビゲーション（Navigation）] ペインで、[デバイス インベントリ（Device Inventory）] をクリックします。
[デバイス インベントリ（Device Inventory）] ウィンドウが表示されます。

ステップ 2 [デバイス インベントリ（Device Inventory）] ツールバーで、ドロップダウン リストから [レイアウト（Layout）] > [タギング（Tagging）] の順に選択します。
テーブルが更新され、他のカラムに加えて、[タグ（Tag）] カラムが表示されます。

ステップ 3 タグを適用するか削除するデバイスの名前の左側にあるチェックボックスをオンにします。複数のデバイスを選択できます。
[ロケーションの設定（Set Location）] と [タグの追加（Add Tag）] ドロップダウン ボタンが表示されます。

（注） 1 つのデバイスのみに対してタグを追加するか削除する場合は、目的のデバイスの [タグ（Tag）] カラムの番号をクリックします。このアクションにより、[複数デバイス タギング（Multiple Device Tagging）] ダイアログボックスが表示されます。ステップ 5 に進みます。

ステップ 4 [タグの追加（Add Tag）] をクリックします。
[複数デバイス タギング（Multiple Device Tagging）] ダイアログボックスが表示されます。

ステップ 5 次のいずれかを実行します。

- タグを適用します。

a) [使用可能なタグ（Available Tags）] リストから、選択したデバイスに適用するタグをクリックします。タグがデバイスに適用されると、[適用済みタグ（Applied Tags）] リストに表示されます。

b) タグがリストにない場合は、タグの名前を入力し、[新しいタグの追加（+New Tag）] をクリックします。
[使用可能なタグ（Available Tags）] リストに新しいタグが表示されます。前の手順に戻り、タグを適用します。

c) [x] をクリックして、ダイアログボックスを閉じます。

- タグを削除します。

a) [適用済みタグ（Applied Tags）] リストで、選択したデバイスから削除するタグの横にある [ゴミ箱（Trash can）] アイコンをクリックします。

（注） 少なくとも 1 つのデバイスにタグが適用されている場合、[適用済みタグ（Applied Tags）] リストに入力されています。[適用済みタグ（Applied Tags）] リストには、各タグが適用されているデバイスの数、またはすべてのデバイスに適用されているかどうかが表示されます。

デバイスおよび [適用済みタグ（Applied Tags）] リストからタグが削除されます。

b) [x] をクリックして、ダイアログボックスを閉じます。

次の作業

ネットワーク構成で必要な場合は、他のデバイスのタグを追加または削除します。

関連トピック

デバイス インベントリの管理, （25 ページ）

タグの削除

タグを削除する前に、すべてのデバイスからそのタグを削除する必要があります。[デバイス インベントリ（Device Inventory）] ウィンドウまたは[トポロジ（Topology）] ウィンドウで、コントローラからタグを削除できます。この手順では、[デバイス インベントリ（Device Inventory）] ウィンドウでタグを削除する方法を示します。

はじめる前に

[ナビゲーション（Navigation）] ペインで [デバイス インベントリ（Device Inventory）] をクリックして、[デバイス インベントリ（Device Inventory）] ウィンドウにアクセスします。

（注） 管理者権限が必要です。ユーザ権限に関する詳細については、ユーザおよびロールの管理, （49 ページ）を参照してください。

手順の概要

1. [ナビゲーション（Navigation）] ペインで、[デバイス インベントリ（Device Inventory）] をクリックします。
2. [デバイス インベントリ（Device Inventory）] ツールバーで、ドロップダウン リストから [レイアウト（Layout）] > [タギング（Tagging）] の順に選択します。
3. タグを削除するデバイスの名前の左側にあるチェックボックスをクリックします。複数のデバイスを選択できます。
4. [タグの追加（Add Tag）] をクリックします。
5. [適用済みタグ（Applied Tags）] リストで、選択したデバイスから削除するタグの横にある [ゴミ箱（Trash can）] アイコンをクリックします。
6. [使用可能なタグ（Available Tags）] リストで、コントローラから削除するタグの横にある [ゴミ箱（Trash can）] アイコンをクリックします。
7. [OK] をクリックして削除を実行します。
8. [x] をクリックして、ダイアログボックスを閉じます。

手順の詳細

ステップ 1 [ナビゲーション（Navigation）] ペインで、[デバイス インベントリ（Device Inventory）] をクリックします。
[デバイス インベントリ（Device Inventory）] ウィンドウが表示されます。

ステップ 2 [デバイス インベントリ（Device Inventory）] ツールバーで、ドロップダウン リストから [レイアウト（Layout）] > [タギング（Tagging）] の順に選択します。
テーブルが更新され、他の情報に加えて、[タグ（Tag）] カラムが表示されます。

ステップ 3 タグを削除するデバイスの名前の左側にあるチェックボックスをクリックします。複数のデバイスを選択できます。
[ロケーションの設定（Set Location）] ボタンと [タグの追加（Add Tag）] ボタンが [デバイス インベントリ（Device Inventory）] ツールバーに表示されます。

（注） 1 つのデバイスからのみタグを除去および削除する場合は、目的のデバイスの [タグ（Tag）] カラムの番号をクリックすることもできます。このアクションにより、[複数デバイス タギング（Multiple Device Tagging）] ダイアログボックスが表示されます。ステップ 5 に進みます。

ステップ 4 [タグの追加（Add Tag）] をクリックします。
[複数デバイス タギング（Multiple Device Tagging）] ダイアログボックスが表示されます。

ステップ 5 [適用済みタグ（Applied Tags）] リストで、選択したデバイスから削除するタグの横にある [ゴミ箱（Trash can）] アイコンをクリックします。

（注） 少なくとも 1 つのデバイスにタグが適用されている場合、[適用済みタグ（Applied Tags）] リストに入力されています。[適用済みタグ（Applied Tags）] リストには、各タグが適用されているデバイスの数、またはすべてのデバイスに適用されているかどうかが表示されます。

デバイスおよび [適用済みタグ（Applied Tags）] リストからタグが削除されます。

ステップ 6 [使用可能なタグ（Available Tags）] リストで、コントローラから削除するタグの横にある [ゴミ箱（Trash can）] アイコンをクリックします。
確認用のダイアログボックスが表示されます。

ステップ 7 [OK] をクリックして削除を実行します。
[使用可能なタグ（Available Tags）] リストからタグが削除されます。削除が失敗した場合は、そのタグがまだデバイスに割り当てられている可能性があります。これらのデバイスからタグを削除してから、再度タグを削除してみます。

ステップ 8 [x] をクリックして、ダイアログボックスを閉じます。

次の作業

ネットワーク構成で必要な場合は、他のデバイスのタグを追加または削除します。

ロケーション タグの追加または削除

ロケーション タグは、ロケーションの属性に基づいてデバイスのグループ化を有効にします。

[デバイス（Devices）] テーブルのデバイスに対してロケーションを追加または削除します。

はじめる前に

[デバイス（Devices）]テーブルのデバイスに対してロケーションを追加または削除するには、[デバイス インベントリ（Device Inventory）] ウィンドウにアクセスします。

（注） 次の手順を実行するには、管理者権限が必要です。Cisco APIC-EM を使用してタスクを実行するために必要なユーザ権限の詳細については、第4章「ユーザおよびロールの管理」を参照してください。

ステップ 1 [デバイス（Devices）]テーブルの上部にある [レイアウト（Layout）] フィールドから [タギング（Tagging）] を選択するか、または [カスタマイズ（Customize）] を選択し、ドロップダウン リストから [ロケーション（Location）] を選択します。
[デバイス（Devices）] テーブルは [ロケーション（Location）] カラムを含めるようにディスプレイを調整します。

ステップ 2 [デバイス（Devices）] テーブルで [ロケーション（Location）] カラムを見つけます。

ステップ 3 [ロケーション（Location）] カラム内でロケーションの追加または削除をする特定のデバイスを見つけます。

ステップ 4 デバイスにロケーションを追加するには、デバイスの [ロケーション（Location）] カラムで [追加（Add）] をクリックすると、[ロケーション（Location）] ウィンドウが表示されます。

[ロケーション（Location）] ウィンドウは [現在運用可能なロケーション（Available Locations）] と [適用済みロケーション（Applied Location）] に分けられます。

ステップ 5 （省略可能）[現在運用可能なロケーション（Available Locations）] カラムに新しいロケーションを追加するには、デバイスのロケーションを入力し、このウィンドウで [新しいロケーションの追加（+ New Location）] ボタンをクリックします。
新しいロケーションが [現在運用可能なロケーション（Available Locations）] カラムに表示されます。

ステップ 6 デバイスにそのロケーションを追加するには、[現在運用可能なロケーション（Available Locations）] カラムの既存のロケーションをクリックします。新しいロケーションが [適用済みロケーション（Applied Location）] カラムに移動します。

（注） 既存のロケーションを削除するには、[適用済みロケーション（Applied Location）] カラムのロケーションの左側にある [ゴミ箱（trash can）] アイコンをクリックします。ロケーションが [現在運用可能なロケーション（Available Locations）] カラムに移動します。

ステップ 7 デバイスに新しいロケーションを保存する場合は、[ロケーション（Location）] ウィンドウの右上にある [X] アイコンをクリックします。

次の作業

ネットワーク設定の必要に応じて、他のデバイスに対して他のロケーションを追加または削除します。

関連トピック

デバイス インベントリの管理, （25 ページ）
ロケーション マーカーの追加, （41 ページ）

ロケーション マーカーの追加および削除

デバイスにロケーションタグを追加する以外に、ワールドマップにデバイスの地理的位置を表すロケーション マーカーを追加できます。これらのマーカーは、[トポロジ（Topology）] ウィンドウに表示できます。

ロケーション マーカーの追加

[デバイス ウィンドウ（Device Inventory）] ウィンドウのデバイスにロケーション マーカーを追加できます。

はじめる前に

管理者権限が必要です。

デバイスにすでにロケーション タグを追加しています。

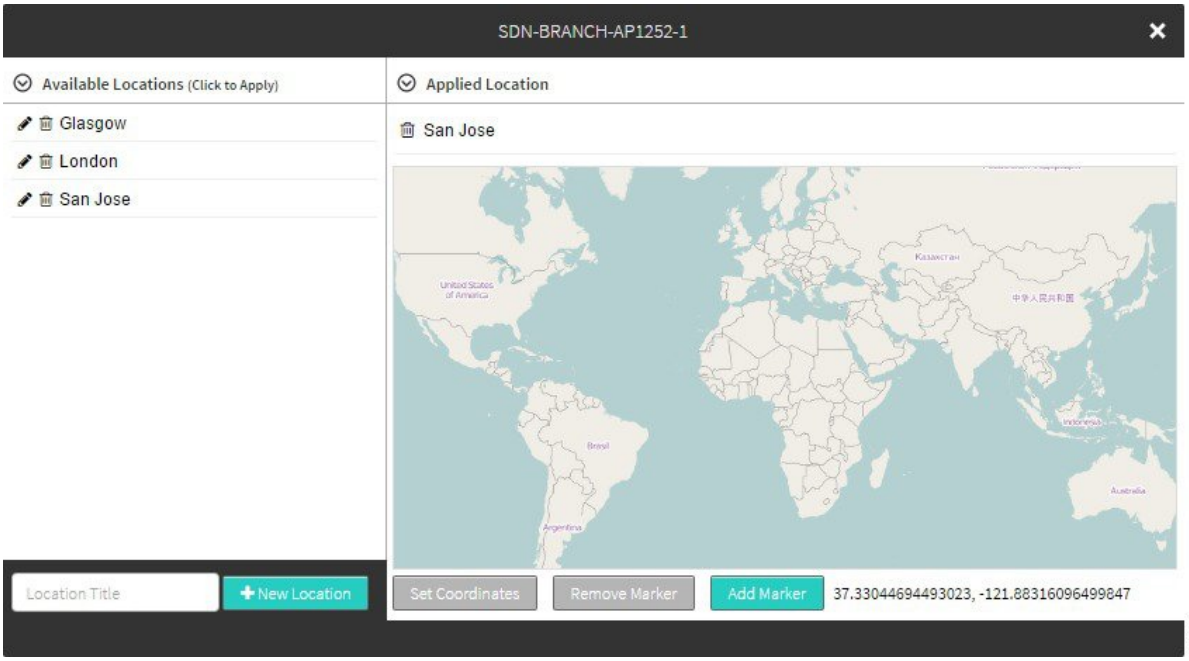
ステップ 1 [ナビゲーション（Navigation）] ペインで、[デバイス インベントリ（Device Inventory）] をクリックします。
[デバイス インベントリ（Device Inventory）] ウィンドウが表示されます。

ステップ 2 [デバイス インベントリ（Device Inventory）] ツールバーで、ドロップダウン リストから [レイアウト（Layout）] > [タギング（Tagging）] の順に選択します。
テーブルが更新され、他のカラムに加えて、[ロケーション（Location）] カラムが表示されます。

ステップ 3 （省略可能）特定のロケーション タグを持つデバイスを表示するには、[デバイス インベントリ（Device Inventory）] ツールバーで、[フィルタ（Filters）] をクリックし、[デバイス ロケーション（Device Location）] フィールドにロケーション タグを入力し、[+] アイコンをクリックします。

ステップ 4 [ロケーション（Location）] カラムからロケーションをクリックします。
[ロケーション（Location）] ダイアログボックスが表示され、デバイスの名前が上部に示されます。[適用済みロケーション（Applied Locations）] リストにロケーション タグが表示されます。

図 *5*：*[ロケーション（Location）]* ウィンドウ

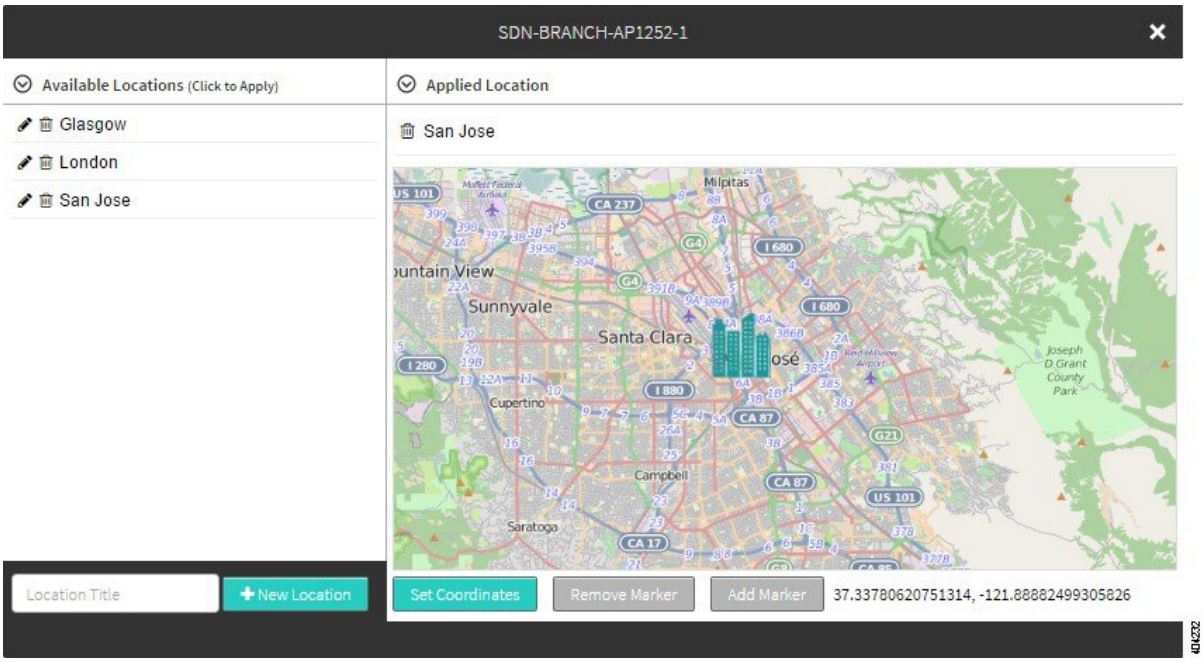


ステップ 5 （省略可能）マップに詳細なロケーションを取得するにはマップをドラッグしてズームします。

ステップ 6 マップにロケーション マーカーを追加するには、[マーカーの追加（Add Marker）] をクリックします。

ステップ 7 マップの特定のロケーションにマーカーをドラッグします。

図 *6*：ロケーション マーカーの配置



ステップ 8 マーカーの座標を設定するには、[座標の設定（Set Coordinates）] をクリックします。

ステップ 9 [X] をクリックして、ダイアログボックスを閉じます。

（注） さらにロケーションマーカーを追加するには、[ロケーション（Location）] ダイアログボックスを閉じ、[ロケーション（Location）] カラムで別のロケーションをクリックします。現在の [ロケーション（Location）] ダイアログボックスで別のロケーションを選択すると、そのロケーションが現在選択されているデバイスに適用されます。

次の作業

ロケーションのすべてにロケーション マーカーを追加します。

マップにロケーション マーカーを表示するには、[トポロジ（Topology）] ウィンドウにアクセスします。

関連トピック

デバイス インベントリの管理，（25 ページ）
トポロジ
トポロジのアイコン，（71 ページ）

Topology Toolbar

ロケーション マーカーの削除

[デバイス インベントリ（Device Inventory）] ウィンドウのデバイスからロケーション マーカーを削除できます。

はじめる前に

管理者権限が必要です。

ロケーション マーカーがすでに追加されている必要があります。

ステップ 1 [ナビゲーション（Navigation）] ペインで、[デバイス インベントリ（Device Inventory）] をクリックします。
[デバイス インベントリ（Device Inventory）] ウィンドウが表示されます。

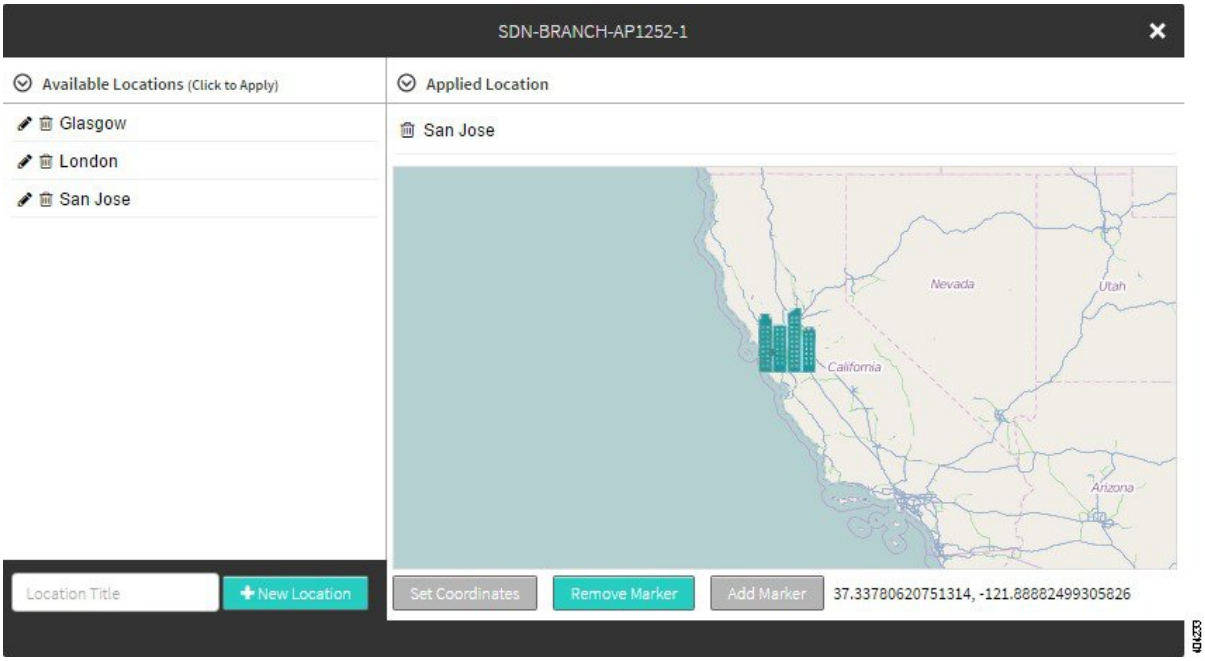
ステップ 2 [デバイス インベントリ（Device Inventory）] ツールバーで、ドロップダウン リストから [レイアウト（Layout）] > [タギング（Tagging）] の順に選択します。
テーブルが更新され、他のカラムに加えて、[ロケーション（Location）] カラムが表示されます。

ステップ 3 （省略可能）特定のロケーション タグを持つデバイスを表示するには、[デバイス インベントリ（Device Inventory）] ツールバーで、[フィルタ（Filters）] をクリックし、[デバイス ロケーション（Device Location）] フィールドにロケーション タグを入力し、[+] アイコンをクリックします。

ステップ 4 目的のデバイスについて、[ロケーション（Location）] カラムのロケーションをクリックします。

[ロケーション（Location）] ダイアログボックスが表示され、デバイスの名前が上部に示されます。[適用済みロケーション（Applied Locations）] リストにロケーション タグが表示されます。

図 7：***[ロケーション（Location）]ウィンドウ***



ステップ 5 [マーカーの削除（Remove Marker）] ボタンをクリックします。

ステップ 6 [X] をクリックして、ダイアログボックスを閉じます。

（注） さらにロケーションマーカーを追加するには、[ロケーション（Location）] ダイアログボックスを閉じ、[ロケーション（Location）] カラムで別のロケーションをクリックします。現在の [ロケーション（Location）] ダイアログボックスで別のロケーションを選択すると、そのロケーションが現在選択されているデバイスに適用されます。

ホストインベントリの管理

[ホストインベントリ（Host Inventory）] ウィンドウには、ネットワークで検出されたホストとユーザが表示されます。

ホストインベントリを表示するには、[ナビゲーション（Navigation）] ペインの [ホストインベントリ（Host Inventory）] をクリックします。[ホストインベントリ（Host Inventory）] ウィンドウが開き、ネットワークで検出されたホストが一覧表示されます。次の表に、インベントリのホストについて表示される情報を示します。

（注） 表に表示されるホスト数（10、25、50、100）を制限するには、またはホストのグループ（最初、前、次、最後、または1-3）を一度に表示するには、[ホストインベントリ（Host Inventory）] テーブルの下にあるフィルタを使用します。

図 *8*：*[ホスト インベントリ（Host Inventory）]* ウィンドウ

表 *11*：ホスト インベントリ（*Host Inventory*）

ホスト インベントリ（Host Inventory）	説明
ホスト名（Host Name）	ホストの名前。
ホスト MAC アドレス（Host MAC address）	ホストの MAC アドレス。
ホスト IP アドレス（Host IP address）	ホストの IP アドレス。
ホスト タイプ（Host Type）	ホストのタイプ（有線またはワイヤレス）。
接続されたネットワーク デバイスの IP アドレス（Connected Network Device IP Address）	ホストに接続されているデバイスの IP アドレス。
接続されたインターフェイス名（Connected Interface Name）	デバイスが接続されているインターフェイスの名前。たとえば、GigabitEthernet1/0/24。

関連トピック

ホスト テーブル ビューの変更，（47 ページ）

ホスト テーブル ビューの変更

[ホスト（Hosts）]チェックリストにアクセスして表示するデータを選択することにより、[ホスト（Hosts）] テーブルに表示される情報を変更できます。

はじめる前に

[ホスト（Hosts）] テーブルに表示される情報を変更するために、[ホスト インベントリ（Host Inventory）] ウィンドウにアクセスします。

ステップ 1 [ホストインベントリ（Host Inventory）]チェックリストにアクセスするには、[ホストインベントリ（Host Inventory）] ウィンドウの [ホスト（Hosts）] テーブルの左上にある [ホイール（Wheel）] アイコンの上にカーソルを合わせます。
[ホイール（Wheel）] アイコンの上にカーソルを合わせると、[ホスト（Hosts）] チェックリストが表示されます。

ステップ 2 リストの該当するボックスをオンにして、[ホスト（Hosts）]テーブルに表示する情報を選択します。たとえば、[ホスト（Hosts）]テーブルにホスト タイプ（有線または無線）を表示する場合は、リストで [ホスト タイプ] をオンにして選択します。

ステップ 3 外側の任意の場所をクリックすることで、[ホストインベントリ（Host Inventory）]チェックリストを閉じます。

次の作業

[ホスト インベントリ（Host Inventory）] ウィンドウに表示される更新された情報を確認します。

関連トピック

ホスト インベントリの管理, （45 ページ）

第 4 章

ユーザおよびロールの管理

- ロールベース アクセス コントロールについて，49 ページ
- ユーザ ロールについて，49 ページ
- AAA について，52 ページ
- パスワードの変更，54 ページ
- ユーザおよびロールの設定，56 ページ

ロールベース アクセス コントロールについて

Cisco APIC-EM はロールベース アクセス コントロール（RBAC）をサポートします。RBAC は、ユーザ ロールに基づいてユーザのコントローラ アクセスを制限または承認する方法です。ロールは、コントローラのユーザの権限を定義します。権限がユーザに直接割り当てられることはないため、個々のユーザ権限の管理では、適切なロールを Cisco APIC-EM GUI へのアクセスが必要なユーザに割り当てることが主な作業になります。

ユーザ ロールについて

最初に Cisco APIC-EM を展開するときに、設定ウィザードはユーザ名とパスワードの入力が求められます。この最初のユーザには、コントローラの完全な管理（読み書き）権限が与えられ、他のユーザのユーザ アカウントを作成できます。

（注） 管理ロールを持つユーザのみが、ユーザの作成とユーザ ロールの割り当てをすることができます。

ユーザは、実行が許可される機能を決定する次のロールを割り当てられます。

- 管理者（ROLE_ADMIN）：ユーザおよびアカウントを追加または削除する機能を含む、すべての Cisco APIC-EM リソースに対する完全な管理者権限を提供します。詳細については、管理者ロール，（50 ページ） を参照してください。

（注） 管理者（ROLE_ADMIN）権限を持つユーザを少なくとも 2 人設定することを強くお勧めします。万一、1 人のユーザがロックされるか、またはパスワードを忘れた場合、この状況から回復できる管理者権限を持つ別のユーザがいます。

- オブザーバ（ROLE_OBSERVER）：主に読み取り専用権限を Cisco APIC-EM に提供します。詳細については、オブザーバ ロール，（51 ページ） を参照してください。
- インストーラ（ROLE_INSTALLER）：インストーラはシスコのプラグ アンド プレイ モバイル アプリケーションを使用して、リモートで APIC-EM コントローラにアクセスし、デバイスを展開して状態を表示することができます。インストーラは、Cisco APIC-EM GUI に直接アクセスできなくなります。

  詳細については、インストーラ ロール，（51 ページ） を参照してください。

管理者ロール

管理者ロールを持つユーザには、ユーザとアカウントを追加または削除する機能を含む、すべての Cisco APIC-EM リソースに対する完全な管理者権限があります。管理者ロール（ROLE_ADMIN）を持つユーザは、次のタスクを実行できます。

- （既存のパスワードにより）自分のパスワードを変更します。
- 管理者（ROLE_ADMIN）またはオブザーバ（ROLE_OBSERVER）権限を持つ新しいユーザを作成します。
- ユーザのロールと範囲を持つ他のすべてのユーザを表示します。
- 自分のロールを含む他のユーザ ロールを編集します。
- それらのロールを含むユーザを削除します。

管理者は直接 GUI の別のユーザ パスワードを変更することはできませんが、管理者は削除してから GUI を使用して新しいパスワードでユーザを再作成できます。

管理者ロールで使用可能な特定のリソースの詳細については、Cisco APIC-EM のリソースと権限，（52 ページ） を参照してください。

（注） セキュリティ上の理由から、パスワードは、どのユーザに対しても（管理者権限を持つユーザに対してさえも）、表示されません。

（注） 管理者（ROLE_ADMIN）権限を持つユーザを少なくとも 2 人設定することを強くお勧めします。万一、1 人のユーザがロックされるか、またはパスワードを忘れた場合、この状況から回復できる管理者権限を持つ別のユーザがいます。

オブザーバ ロール

オブザーバ ロールは、Cisco APIC-EM に読み取り専用の権限を提供します。オブザーバ ロール（ROLE_OBSERVER）を割り当てられたユーザは、（既存のパスワードにより）自分のパスワードを変更できます。

次のタスクを実行できます。

- ロールまたは範囲の編集
- ロールまたは範囲の削除
- 自身のパスワードの表示
- デバイス インベントリのデバイスのリストを表示します。

オブザーバ ロールで使用可能な特定のリソースの詳細については、Cisco APIC-EM のリソースと権限, （52 ページ） を参照してください。

（注） セキュリティ上の理由から、パスワードは、どのユーザに対しても（管理者権限を持つユーザに対してさえも）、表示されません。

インストーラ ロール

インストーラ ロール（ROLE_INSTALLER）が割り当てられているユーザは、シスコ プラグ アンド プレイ モバイル アプリケーションを使用して、Cisco APIC-EM にリモートでアクセスし、次の機能を実行することができます。

- デバイスのステータスを表示します。
- デバイスの展開をトリガーします。

インストーラは、Cisco APIC-EM GUI に直接アクセスできません。

（注） セキュリティ上の理由から、パスワードは、どのユーザに対しても（管理者権限を持つユーザに対してさえも）、表示されません。

ユーザおよびドメイン

ネットワークで異なるドメイン（ネットワークまたはサブネットワーク）に複数のユーザを作成できます。ユーザごとに異なるドメインの異なるロールを持つことができます。たとえば、ユーザは、ネットワーク A にオブザーバ ロールおよびネットワーク B に管理者ロールを持つことができます。

AAA について

認証および承認

ユーザとロールは認証および承認のプロセスに従います。

Cisco APIC-EM を使用して、コントローラ用の各リソースが操作にマッピングされ、各操作はユーザに必要な権限にマッピングされます。すべての REST API がコントローラの認証プロセスによって保護されます。これらへのアクセスを許可するリソースおよびロールについては、Cisco APIC-EM のリソースと権限, （52 ページ） を参照してください。

（注） ユーザ ロールおよびその権限によっては、特定の Cisco APIC-EM の GUI の機能が表示されません。GUI にロール動作（たとえば、管理者、インストーラ、オブザーバ）を並べて表示するには、複数の Chrome ブラウザか Chrome ブラウザの匿名モードのいずれかを使用する必要があります。タブを使用する単一の Chrome ブラウザにロール動作を並べて表示することはできません。

Cisco APIC-EM のリソースと権限

次の表では、各 Cisco APIC-EM リソースに必要なロール権限について説明します。

（注） ロールおよびその権限によっては、特定の Cisco APIC-EM GUI の機能が表示されません。GUI のロール動作（たとえば、管理者およびオブザーバ）を並べて表示するには、複数のブラウザかブラウザの匿名モードのいずれかを使用する必要があります。タブを使用する単一のブラウザにロール動作を並べて表示することはできません。

表 *12*：*Cisco APIC-EM* のリソースと権限

リソース	ロール権限
検出：スキャン	• 管理者（Administrator）

リソース	ロール権限
インベントリ：デバイス クレデンシャルを使用したインベントリ リストの取得	• 管理者（Administrator）
インベントリ：タグの追加	• 管理者（Administrator） • オブザーバ
インベントリ：デバイス ロールの作成	• 管理者（Administrator） • オブザーバ
インベントリ：タグを追加してデバイス ロールを作成すること以外の操作	• 管理者（Administrator） • オブザーバ
ロールベース アクセス コントロール：ユーザおよびセキュリティ ロールの作成および削除	• 管理者（Administrator） • オブザーバは所有するパスワードを表示および変更できます。
ファイル サービス	• 管理者（Administrator）
ホスト	• 管理者（Administrator） • オブザーバ
タスク ID	• 管理者（Administrator） • オブザーバ
テレメトリ	• 管理者（Administrator） • オブザーバ
トポロジ	• 管理者（Administrator） • オブザーバ

リソース	ロール権限
Path Analysis（Path Analysis）	• 管理者（Administrator） • オブザーバ

アカウンティング（Accounting）

管理者は、認証されたセッションのログの内容にアクセスできます。ユーザ、操作、API に関する次の情報は、セキュリティまたはトラブルシューティングのログでキャプチャされます。

- ノースバウンド API アクセス データ
- ユーザ名での認証の成功またはすべてのメソッドにおける失敗

関連トピック

ユーザ ログの確認，（60 ページ）

パスワードの変更

Cisco APIC-EM へのログインに使用するパスワードを変更できます。

（注） 自身のパスワードだけを変更できます。別のユーザのパスワードを変更するには、管理者権限が必要です。パスワードの変更では、ユーザをコントローラ データベースから削除してから、新しいパスワードを使用して新規ユーザとしてそのユーザを再作成します。

[パスワードの変更（Change Password）] ウィンドウで提供されるパスワード ジェネレータ、または以下のガイドラインを使用して、安全なパスワードを作成できます。

以下の 4 つのクラスのうち少なくとも 3 つのクラスの文字を含む 8 文字以上のパスワードを作成します。

- 大文字のアルファベット
- 小文字のアルファベット
- 数字
- 特殊文字：スペース文字、または以下のいずれかの文字（または文字の組み合わせ）

  ! @ # $ % ^ & * ( ) - = + _ { } [ ] \\ | ; : " ' , < . > ? / :: #! ./;; >> << () **

複雑なパスワードに加えて、ユーザ名からセキュリティ上の脆弱性が生じないようにする必要があります。セキュリティ上の脆弱性が生じる可能性があるユーザ名を回避するには、以下の規則に従います。

- すべてのユーザが一意のユーザ名とパスワードを持っている必要があります。
- 管理者のログインとパスワードの使用をユーザに許可しないでください。

セキュリティ上の脆弱性が生じないようにするために、パスワードを作成するときにCisco APIC-EMパスワード ポリシーに従うことをお勧めします。詳細については、『*Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*』を参照してください。

ステップ 1 **グローバル** ツールバーで、[設定（Settings）] アイコンをクリックします。
[設定（Settings）] ウィンドウが表示されます。

ステップ 2 [設定（Settings）] ウィンドウの [ナビゲーション（Navigation）] ペインで、[パスワードの変更（Change Password）] をクリックします。
[パスワードの変更（Change Password）] ウィンドウが表示されます。

ステップ 3 [パスワードの変更（Change Password）] ウィンドウで、以下のフィールドに適切な値を入力します。

- ユーザ名（Username）：デフォルトでこのフィールドに表示されるユーザ名。
- 現在のパスワード（Current Password）：現在のパスワード。
- 新しいパスワード（New Password）：新しいパスワード。独自のパスワードを作成します。または、より強力なパスワードを作成する場合は、[生成（Generate）] をクリックし、シード フレーズを入力し、[生成（Generate）] をクリックします。生成されたパスワードは、[パスワードの適用（Apply Password）] をクリックすることにより適用できます。または、新しいパスワードの入力前または入力後に、生成されたパスワード（またはその一部）をコピーして貼り付けることができます。

  （注） パスワード ジェネレータを使用してより強力なパスワードを作成することを強くお勧めします。

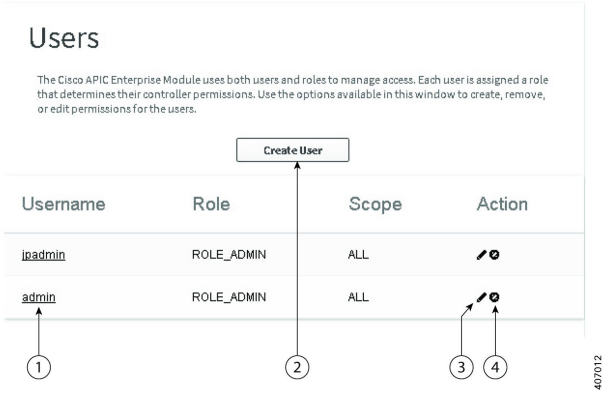
- 新しいパスワードの確認（Confirm New Password）：確認のために新しいパスワードを再度入力。

ステップ 4 終了したら、[更新（Update）] をクリックして、新しいパスワードを更新して保存します。
パスワード変更をキャンセルする場合は、[キャンセル（Cancel）] をクリックします。

ユーザおよびロールの設定

[ユーザ（Users）] ウィンドウに、**グローバル** ツールバーからアクセスするには、[設定（Settings）] アイコン をクリックします。その後、[設定（Settings）] ウィンドウの [ナビゲーション（Navigation）] ペインから、[ユーザ（Users）] をクリックします。

図 *9*：*[ユーザ（Users）]* ウィンドウ



番号付きコールアウト	[名前（Name）]	説明
1	実際のユーザ名	ユーザの現在のアクセス ステータスを表示します。
2	ユーザの作成	新規ユーザを追加できます。 1
3	編集（Edit）	ユーザ ロールの設定を変更できます。他の設定は変更できません。 2

番号付きコールアウト	[名前（Name）]	説明
4	削除（Delete）	ユーザを Cisco APIC-EM データベースから削除します。削除されたユーザはコントローラにログインできなくなります。[3]

1 この機能を実行するには、管理者（ROLE_ADMIN）としてログインする必要があります。
2 この機能を実行するには、管理者（ROLE_ADMIN）としてログインする必要があります。
3 この機能を実行するには、管理者（ROLE_ADMIN）としてログインする必要があります。

ユーザの追加

管理者ロール（ROLE_ADMIN）を持つユーザだけがユーザを Cisco APIC-EM に追加できます。

（注） ユーザ情報（クレデンシャル）は、コントローラ上のローカルデータベースに保存されます。

（注） 管理者（ROLE_ADMIN）権限を持つユーザを少なくとも 2 人設定することを強くお勧めします。万一、1 人のユーザがロックされるか、またはパスワードを忘れた場合、この状況から回復できる管理者権限を持つ別のユーザがいます。

はじめる前に

管理者（ROLE_ADMIN）である必要があります。

ステップ 1 **グローバル** ツールバーで、[設定（Settings）] アイコンをクリックします。
[設定（Settings）] ウィンドウが表示されます。

ステップ 2 [設定（Settings）] ウィンドウの [ナビゲーション（Navigation）] ペインで、[ユーザ（Users）] をクリックします。
ユーザに関する以下の情報が表示された [ユーザ（Users）] ウィンドウが表示されます。

- ユーザ名（Username）：ユーザに割り当てられているユーザ名。
- ロール（Role）：APIC-EM 内のユーザの権限を定義するロール。有効なロールは、ROLE_ADMIN、ROLE_OBSERVER、または ROLE_INSTALLER です。
- 範囲（Scope）：アクセスをユーザに許可するドメインまたはテナント。
- アクション（Actions）：ユーザ情報の編集またはユーザの削除を行うためのアイコン。

ステップ 3 [ユーザの作成（Create User）] をクリックします。

ステップ 4 [ユーザの作成（Create User）] ダイアログボックスで、新しいユーザのユーザ名、パスワード（2 回）、およびロールを入力します。範囲は、デフォルトで [範囲すべて（SCOPE ALL）] に設定されます。

ステップ 5 [追加（Add）] をクリックします。
新しいユーザが [ユーザ（Users）] ウィンドウに表示されます。

関連トピック

ユーザおよびロール

ユーザの削除

管理者ロール（ROLE_ADMIN）を持つユーザは、Cisco APIC-EM からユーザを削除できます。

はじめる前に

管理者（ROLE_ADMIN）である必要があります。

ステップ 1 **グローバル** ツールバーで、[設定（Settings）] アイコンをクリックします。
[設定（Settings）] ウィンドウが表示されます。

ステップ 2 [設定（Settings）] ウィンドウの [ナビゲーション（Navigation）] ペインで、[ユーザ（Users）] をクリックします。
ユーザに関する以下の情報が表示された [ユーザ（Users）] ウィンドウが表示されます。

- ユーザ名（Username）：ユーザに割り当てられているユーザ名。
- ロール（Role）：APIC-EM 内のユーザの権限を定義するロール。有効なロールは、ROLE_ADMIN、ROLE_OBSERVER、または ROLE_INSTALLER です。
- 範囲（Scope）：アクセスをユーザに許可するドメインまたはテナント。
- アクション（Actions）：ユーザ情報の編集またはユーザの削除を行うためのアイコン。

ステップ 3 削除するユーザを見つけ、[アクション（Actions）] カラムで [削除（Delete）] アイコンをクリックします。
ユーザは、Cisco APIC-EM データベースから削除され、コントローラにはアクセスできません。

（注） デフォルトの管理ユーザは削除できません。Cisco APIC-EM では、コントローラにログインできる管理者が少なくとも 1 人必要です。

関連トピック

ユーザおよびロール

ユーザ情報の表示と編集

管理者ロール（ROLE_ADMIN）ユーザは、ユーザ設定とロールを表示および変更できます。

（注） ユーザ情報（クレデンシャル）は、コントローラ上のローカルデータベースに保存されます。

はじめる前に

管理者（ROLE_ADMIN）である必要があります。

ステップ 1 **グローバル** ツールバーで、[設定（Settings）] アイコンをクリックします。
[設定（Settings）] ウィンドウが表示されます。

ステップ 2 [設定（Settings）] ウィンドウの [ナビゲーション（Navigation）] ペインで、[ユーザ（Users）] をクリックします。
ユーザに関する以下の情報が表示された [ユーザ（Users）] ウィンドウが表示されます。

- ユーザ名（Username）：ユーザに割り当てられているユーザ名。
- ロール（Role）：APIC-EM 内のユーザの権限を定義するロール。有効なロールは、ROLE_ADMIN、ROLE_OBSERVER、または ROLE_INSTALLER です。
- 範囲（Scope）：アクセスをユーザに許可するドメインまたはテナント。
- アクション（Actions）：ユーザ情報の編集またはユーザの削除を行うためのアイコン。

ステップ 3 ユーザの情報を編集する場合は、[アクション（Actions）] カラムで [編集（Edit）] アイコンをクリックします。
ユーザ名と範囲はデフォルトで設定されているため、それらの設定を変更することはできません。ただし、ロール設定は変更できます。有効なロールは、ROLE_ADMIN、ROLE_OBSERVER、または ROLE_INSTALLER です。

ステップ 4 ユーザ情報の編集が終了したら、[更新（Update）] をクリックします。

関連トピック

ユーザおよびロール

ユーザ アクセス ステータスの表示

Cisco APIC-EM へのユーザのアクセス ステータスを表示できます。

はじめる前に

管理者（ROLE_ADMIN）である必要があります。

ステップ 1 **グローバル** ツールバーで、[設定（Settings）] アイコンをクリックします。
[設定（Settings）] ウィンドウが表示されます。

ステップ 2 [設定（Settings）] ウィンドウの [ナビゲーション（Navigation）] ペインで、[ユーザ（Users）] をクリックします。
ユーザに関する以下の情報が表示された [ユーザ（Users）] ウィンドウが表示されます。

- ユーザ名（Username）：ユーザに割り当てられているユーザ名。
- ロール（Role）：APIC-EM 内のユーザの権限を定義するロール。 有効なロールは、ROLE_ADMIN、ROLE_OBSERVER、または ROLE_INSTALLER です。
- 範囲（Scope）：アクセスをユーザに許可するドメインまたはテナント。
- アクション（Actions）：ユーザ情報の編集またはユーザの削除を行うためのアイコン。

ステップ 3 ユーザの現在のアクセス ステータスを表示するには、個々のユーザ名（リンク）をクリックします。
[ユーザ ステータス（User Status）] ダイアログボックスが開き、以下の情報が表示されます。

- [ユーザ名（Username）]
- アカウント ステータス（Account status）：ロック、またはロック解除
- アカウント ロック有効期限（Account Locked Expiration）：ユーザ アカウントがロック解除されるまでの時間

管理者である場合、[ロック解除（Unlock）] をクリックしてユーザ アカウントをロック解除できます。

（注） コントローラへのユーザアクセスに対するパスワードポリシーの設定方法については、『*Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*』を参照してください。

ステップ 4 ユーザ情報の表示または編集が終了したら、[閉じる（Close）] をクリックします。

ユーザ ログの確認

Elastic Service Platform（Grapevine）開発者コンソールを使用して、ユーザ ログを確認できます。

（注） 上級ユーザのみが、開発者コンソールを使用してここで説明する手順を実行することをお勧めします。

はじめる前に

Cisco APIC-EM が正常に導入され、動作している必要があります。

ステップ 1 コンソールの [概要（Overview）] ウィンドウにリストされている各サービスのステータスを確認します。各サービスは正方形として表されます。緑色の正方形はアクティブなサービスインスタンスを表し、赤色の正方形は障害のあるインスタンスまたは処理に失敗したインスタンスを持つサービスを表しています。色がない正方形は、非アクティブ サービス（開始されたインスタンスも実行中のインスタンスもない）を表しています。

ステップ 2 コンソールの [概要（Overview）] ウィンドウ内の各サービスのバージョンを確認します。バージョンは、リストされている各サービスのヘッダーにあります。

ステップ 3 特定のアクティブなサービスインスタンス（緑色の正方形アイコン）をクリックし、ウィンドウの下部にある**インスタンス** ログを参照することにより、サービス ログを確認します。

ステップ 4 ログ内でキーワード USER-ACCOUNTING を検索します。
これらのログ エントリ タイプについて以下のデータが表示されます。

- 日付とタイムスタンプ
- ユーザ名：Administrator、Installer、または Observer
- ユーザ名：Administrator、Installer、または Observer
- API
- アクション：GET、POST、PUT、または DELETE の各メソッド
- 成功または失敗

（注） **grep** コマンドを使用してログ内のキーワードを検索することもできます。

次の作業

ログ内のユーザデータを確認したら、ユーザアクティビティのトラブルシューティングに進みます。

開発者コンソールでの作業が完了したら、[ログアウト（Logout）] をクリックします。

関連トピック

アカウンティング（Accounting），（54 ページ）

第 5 章

アプリケーションの管理

- シスコのネットワーク プラグ アンド プレイ，63 ページ
- シスコ インテリジェント WAN（IWAN），64 ページ
- トポロジ，67 ページ
- パス トレースの実行，84 ページ

シスコのネットワーク プラグ アンド プレイ

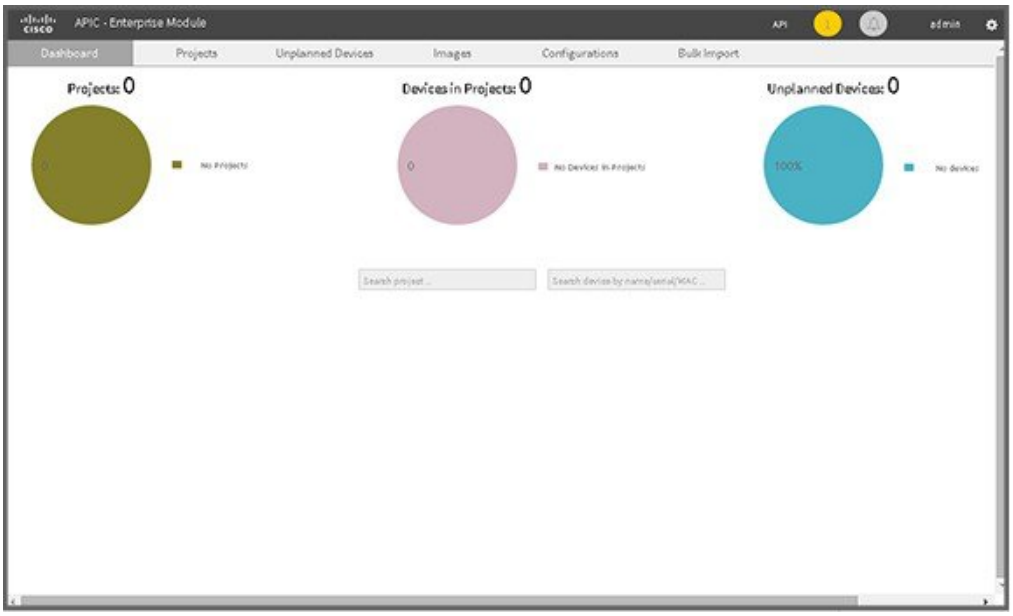
シスコのネットワーク プラグ アンド プレイ アプリケーションは、シスコのルータ、スイッチ、ワイヤレス アクセス ポイントのゼロデイ導入に対してシンプルでセキュアなソリューションです。シスコのネットワーク プラグ アンド プレイ アプリケーションによって、ユーザは必要なイメージ、設定、およびその他の詳細を指定してデバイスを事前プロビジョニングできます。デバイス インストーラがシスコ ネットワーク デバイスをインストールして起動すると、デバイスは自動的に DHCP または DNS を使用する Cisco APIC-EM コントローラを検出します。検出プロセスが完了したら、シスコのネットワーク プラグ アンド プレイ アプリケーションが事前設定情報のデバイスをプロビジョニングします。デバイスが事前設定されていない場合、Cisco APIC-EM を検出して接続した後、シスコのネットワーク プラグ アンド プレイ アプリケーションで計画されていないデバイスとして表示されます。シスコのネットワーク プラグ アンド プレイ アプリケーションを使用して、計画されていないデバイスを要求し、新しい設定および Cisco IOS イメージで設定することができます。Cisco APIC-EM は、PnP をサポートするシスコ デバイスにイメージとコンフィグレーション ファイルを安全におよび自動で提供することによってネットワーク デバイスのプロビジョニングを簡素化する組み込み型プラグ アンド プレイ（PnP）プロトコル サーバをサポートします。PnP サーバは、PnP サポート対象のシスコ デバイスにインストールされている Cisco PnP エージェントと通信します。

ネットワーク プラグ アンド プレイ ダッシュボード ページから、サイト展開のステータスを確認できます。また、[プロジェクト（Projects）] リンクを使用した新しいサイトの定義を開始したり、[未計画のデバイス（Unplanned Devices）] リンクを使用して要求されていないデバイスを表示したりすることもできます。

シスコのネットワーク プラグ アンド プレイの設定手順については、シスコのネットワーク プラグ アンド プレイに関するマニュアルを参照してください。

（注） PnP アプリケーションがコントローラ上で有効になり、プロキシ ゲートウェイが PnP 対応デバイスとコントローラ間の DMZ に存在する場合、プロキシ ゲートウェイの証明書をインポートする必要があります。詳細については、『Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide』を参照してください。

図 *10*：シスコのネットワーク プラグ アンド プレイ ダッシュボード



シスコ インテリジェント WAN（IWAN）

シスコ インテリジェント WAN（IWAN）は、運用コストを削減しながら、IT にすべての接続で優れたユーザ エクスペリエンスを提供します。また、IWAN は、IT 運用を管理タスクを自動化しながら、ソフトウェアベースのコントローラ モデルによって簡素化し、より迅速で、より正常に展開します。

シスコ IWAN アプリケーションは、APIC-EM を使用して、1 つのシステムにネットワーク デバイスを抽象化してネットワークの複雑さを削除し、アプリケーションとサービスの展開を高速化するためのインフラストラクチャの集中型プロビジョニングを提供します。

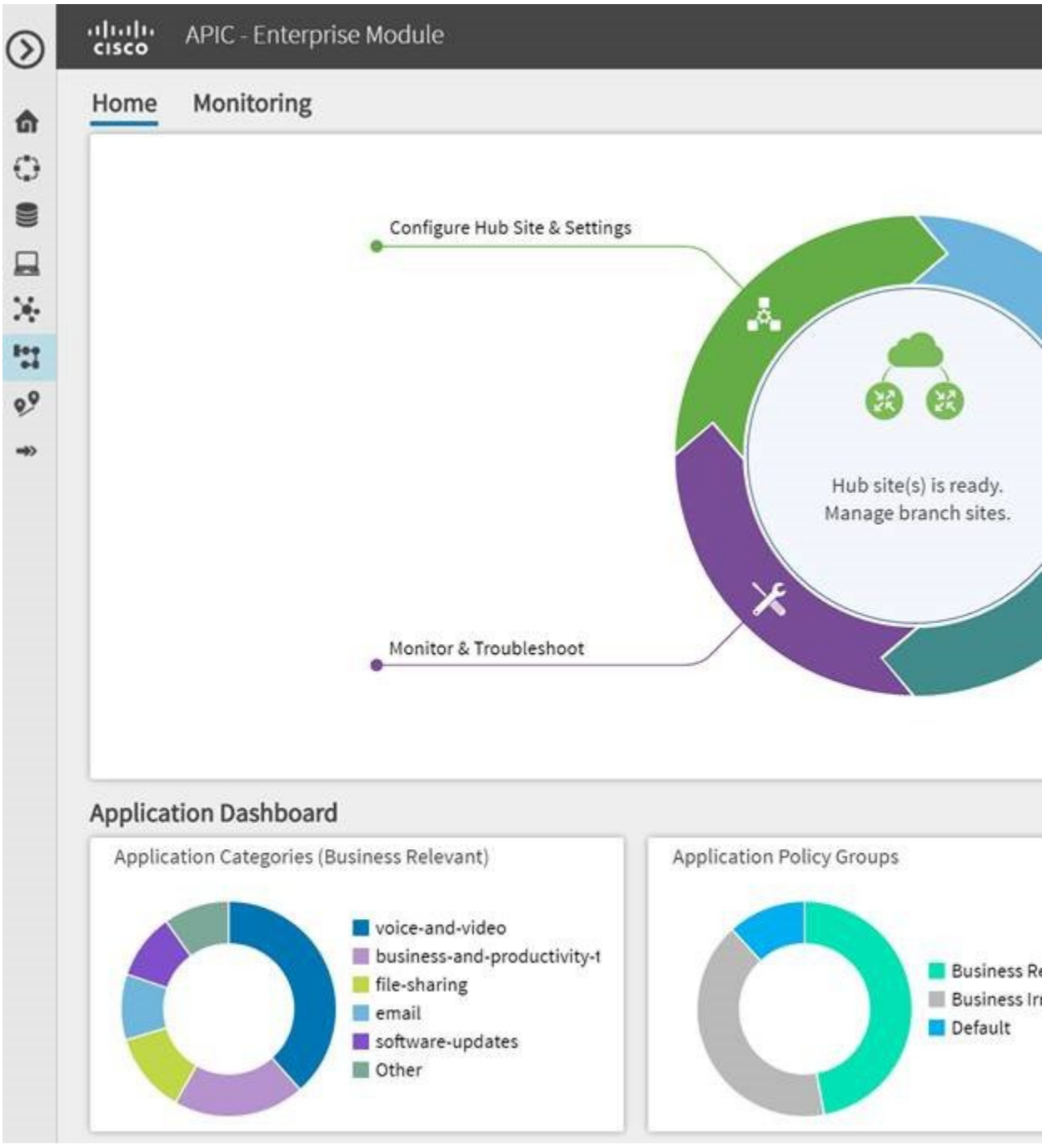
APIC-EM を使用する シスコ IWAN アプリケーションは、ビジネス ポリシーとアプリケーション ルールに基づいてアプリケーション中心のアプローチを使用してブランチに Software Defined Networking を拡張します。これは、ネットワーク全体に分散的に適用される IT 集中管理を提供します。

IWAN ダッシュボード ページから、ネットワーク全体を設定し、サイトをプロビジョニングし、アプリケーション ポリシーを設定できます。

シスコ IWAN ネットワークの設定手順については、シスコ IWAN に関するマニュアルを参照してください。

（注） IWANアプリケーションがコントローラ上で有効になり、プロキシ ゲートウェイがネットワーク デバイスとコントローラ間の DMZ に存在する場合、プロキシ ゲートウェイ証明書をインポートする必要があります。詳細については、『Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide』を参照してください。

図 *11*：*IWAN* ダッシュボード



トポロジ

[トポロジ（Topology）] ウィンドウはネットワークのグラフィック ビューを表示します。設定した検出設定を使用して、Cisco APIC-EM は、デバイスを検索し、デバイス レベルの詳細データを使用して物理トポロジにマッピングします。

[トポロジ（Topology）] ウィンドウにアクセスするには、[ナビゲーション（Navigation）] ペインの [トポロジ（Topology）] をクリックします。[トポロジ（Topology）] ウィンドウが表示されます。

さらに、物理トポロジの上部にあるレイヤ 2 および 3 のトポロジを自動可視化することにより、設計計画および簡素化されたトラブルシューティングを詳細に表示できます。

レイヤ 2 トポロジの場合、コントローラは、[トポロジ（Topology）] ウィンドウに表示するために、ネットワーク内に設定された VLAN を検出します。レイヤ 3 トポロジの場合、コントローラは、[トポロジ（Topology）] ウィンドウに表示するために、ネットワーク内で最近設定および使用されているものによってレイヤ 3 トポロジ（OSPF、IS-IS など）のすべての形式を検出します。

（注） 個々のデバイス設定が取得され、ネットワーク情報ベース（NIB）に保存されます。

デバイス アイコンをクリックすると、そのデバイスに関する情報が提供されます。

（注） ホスト間のパスやネットワーク デバイスを通過するパスに関する詳細については、パス トレース機能を使用します。このアプリケーションにアクセスするには、[ナビゲーション（Navigation）] ペインの [パス トレース（Path Trace）] をクリックします。

トポロジ ツールバー

トポロジ ツールバーは、[トポロジ（Topology）] ウィンドウの上部にあります。

図 *12*：トポロジ ツールバー

[トポロジ（Topology）]ウィンドウのツールバーを使用して、次のトポロジ ビューにアクセスし、次のタスクを実行できます。

- トポロジの検索：[トポロジ（Topology）] ウィンドウでホストまたはデバイスを検索します。ホスト名、デバイス名、デバイス タイプ、または IP アドレスを入力し、表示される結果リストからホストまたはデバイスを選択します。ホストまたはデバイスを結果リストからクリックすると、[トポロジ（Topology）] ウィンドウは、そのホストまたはデバイスを表示するためにシフトします。
- ズームイン/アウト：[トポロジ（Topology）] ウィンドウの表示を調整します。メニューバーの [+]（プラス）アイコンをクリックして、ネットワークのホストおよびデバイスの表示を最大化します。メニュー バーの [-]（マイナス）アイコンをクリックして、ネットワークのホストおよびデバイスの表示を最小化します。

（注） また、マウスのスクロール ホイールを使用してズームインとズームアウトすることもできます。

- トポロジ構造の設定：[フィルタ（Filters）]オプションを表示して、トポロジの構造を変更します。

（注） 詳細については、第 3 章「アプリケーションの管理」の「トポロジ構造の設定」を参照してください。

- ドラッグして選択：「ドラッグして選択」するための機能を切り替えたり、複数のデバイスを選択するためにデバイスを Shift + クリックします。
- 集約の切り替え：デバイスの集約を有効または無効にします。集約はデフォルトで有効になっています。
- 色分けの切り替え：異なる色または単一の色のデバイスアイコンの表示を切り替えます。色分けはデフォルトで有効になっています。
- マップ ビュー ：**トポロジ** マップ ビューにアクセスします。ネットワークの物理的ロケーションのグラフィカル表示でネットワーク トポロジを表示するには、このアイコンをクリックします。

（注） このアイコンは、[デバイス インベントリ（Device Inventory）] ウィンドウからデバイスのロケーション マーカーを追加した場合に表示されます。

- ソート：[トポロジ（Topology）] ウィンドウ内のホストとデバイスをソートします。次の方法を使用してホストまたはデバイスをソートするには、このアイコンをクリックします。

次の表では、各ソートがどのように機能するかについて説明します。

ランダム（Random）	[トポロジ（Topology）] ウィンドウのデバイスおよびホストはランダムに表示されます。これはデフォルト ビューです。

タイプ ロール別	デバイスおよびホストは次の順にソートされます。 • クラウド • ルータ • WLC • スイッチ（Switch） • Access Point; アクセス ポイント • 有線 • ワイヤレス 上記のソートされた各項目は次の順にソートされます。 • ボーダー ルータ • コア • Distribution • アクセス（Access）
タイプ ブロック別	TBD
タイプ ブロック接続別	TBD
タイプ ブロック接続別	TBD

- タグ：使用可能なタグを表示します。各タグをクリックすると、[トポロジ（Topology）]ウィンドウでこのタグを持つデバイスが強調表示されます。
- レイヤ：レイヤ 2 およびレイヤ 3 のオプションを表示します。
  - L2：[レイヤ 2 （Layer 2）] フィールドをクリックし、ドロップダウン メニューから VLAN またはキーワードでレイヤ 2 のデフォルト ビューの 1 つを選択することによって、ネットワークのレイヤ 2 ビューにアクセスします。

    （注） ドロップダウン メニューから管理項目を選択して、管理ネットワークのビューにアクセスすることもできます。

  - L3：キーワードでトポロジ ビューに表示するには、[レイヤ 3 （Layer 3）] フィールドをクリックし、レイヤ3タイプを選択することによって、ネットワークのレイヤ3ビューにアクセスします。次のレイヤ 3 タイプのビューを利用できます。

- Intermediate System-to-Intermediate System （IS-IS） ：IS-IS ルーティング プロトコルを使用して、接続されたデバイスを表示します。
- Open Shortest Path First （OSPF） ：OSPF ルーティング プロトコルを使用して、接続されたデバイスを表示します。
- Static-Route：スタティック ルート設定を使用して、接続されたデバイスを表示します。

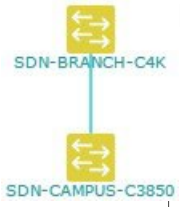
（注） デフォルトのレイヤ 3 ビューは上記のビューすべてです。

- 保存：[現在のレイアウトの保存（Save Current Layout）]（現在のレイアウト、デバイスの集約、およびラベルの保存）および [保存したレイアウトの読み込み（Load Saved Layout）]（前に保存したレイアウト、デバイスの集約とラベルの読み込み）オプションを表示します。

トポロジのアイコン

次のアイコンが [トポロジ（Topology）] ウィンドウに表示されます。

アイコン	ネットワーク要素	説明
	クラウド	外部ネットワークの表示。
	ホスト	ホストのホスト名または IP アドレスを表示します。
	ルータ	デバイス名を表示します。
	スイッチ（Switch）	デバイス名を表示します。

アイコン	ネットワーク要素	説明
	アクセス ポイント（Access Point）	デバイス名を表示します。
	ワイヤレス LAN コントローラ	デバイス名を表示します。
	集約されたデバイス	集約されたデバイスの数およびデバイス タイプを表示します。 （注） 異なるデバイス タイプが集約された場合、集約されたデバイスの数だけが表示されます。
	ロケーション マーカー	デバイス名を表示します。デバイス アイコンが背景としてロケーション マーカーと一緒に表示されます。 （[デバイス インベントリ（Device Inventory）] ウィンドウから）デバイスにロケーション マーカーを追加し、[ナビゲーション（Navigation）] ペインの [トポロジ（Topology）] をクリックするかトポロジ ツールバーの [マップ（Map）] ボタンをクリックすると、トポロジ マップ ビューが表示されます。マップ ビューは、ロケーション マーカーを配置する場所を示します（たとえば、サンノゼ、ロンドン）。マップでロケーション マーカーをクリックし、その場所（サンノゼなど）のトポロジを表示します。 異なるロケーション マーカー（ロンドンなど）を使用するデバイスは、背景としてロケーション マーカーで表示されます。
	[リンク（Links）]	デバイス間の行。 接続されたデバイスに関する情報を表示するには、リンクをクリックします。 （注） リンクの一部はデバイスの集約のために非表示になります。

関連トピック

デバイスへのタグの適用
デバイス データの表示
デバイスおよびホストの検索, （81 ページ）
トポロジ構造の設定, （76 ページ）

集約されたデバイス ラベルの変更
デバイスからのタグの削除
タグ付きデバイスの表示
ロケーション マーカーの追加, （41 ページ）
[トポロジ（Topology）] ウィンドウのデバイスの集約, （74 ページ）
トポロジ構造の設定, （76 ページ）
トポロジ

デバイス データの表示

特定のデバイスのデータを [トポロジ（Topology）] ウィンドウに表示できます。デバイス データを表示すると、デバイス間のネットワーク接続問題のトラブルシューティングに役立ちます。

（注） [トポロジ（Topology）] ウィンドウでアクセスできるデバイス データには、[デバイス インベントリ（Device Inventory）] ウィンドウでもアクセスできます。

以下のデバイス データを使用できます。

- ロケーション（選択したデバイスのアイコンにロケーション マーカーの背景がある場合、ロケーション情報が表示されます。そのロケーション マーカーを共有するデバイスのトポロジを表示するには、[ロケーション（Location）] リンクをクリックします）。
- タイプ（Type）
- デバイス ロール（デバイス ロールの変更方法については、デバイス ロールの変更, （34 ページ） を参照）。
- IP アドレス
- MAC アドレス
- OS（オペレーティング システム）
- Software version
- ポート
  - ギガビット イーサネット ポート
  - 10 ギガビット イーサネット ポート
  - 管理ポート
- VLAN（存在する場合）
- 接続数
- 接続されたデバイスのリスト（各接続デバイスのデバイス タイプ（アイコン）と接続数が表示されます。接続されたデバイスをクリックすると、そのデバイスの詳細が表示されます）。

- タグ（Tags）

ステップ 1 [ナビゲーション（Navigation）] ペインで、[トポロジ（Topology）] をクリックします。
[トポロジ（Topology）] ウィンドウが表示されます。

（注） [デバイス インベントリ（Device Inventory）] ウィンドウからデバイスのロケーション マーカーを追加した場合は、トポロジマップ ビューが表示されます。その場所のトポロジを表示するには、ロケーション マーカーをクリックします。

ステップ 2 特定のデバイスのデータを表示するには、[トポロジ（Topology）] ウィンドウでそのデバイスをクリックします。

ステップ 3 集約されたデバイスのリストを表示するには、次の手順を実行します。

a) [トポロジ（Topology）] ウィンドウで、[集約されたデバイス（aggregated devices）] アイコンをクリックします。

b) [デバイスの詳細（Device Details）] ペインで、デバイスデータを表示する各デバイスの [詳細（Details）] リンクをクリックします。

c) 集約されたデバイスのリストに戻るには、[集約結果（Aggregated Results）] リンクをクリックします。

次の作業

ネットワーク内のその他のデバイスのデータを選択して確認するか、または以下のようなタスクを実行します。

- 選択したグループの集約または集約解除
- デバイス名と IP アドレスを使用したデバイスの検索
- ネットワーク内のデバイスへのタグの適用
- デバイス ロールの変更

デバイス集約

Cisco APIC-EM デバイス集約機能を使用して、デバイスが [トポロジ（Topology）] ウィンドウに表示される方法を調整します。この機能は、ネットワークのナビゲーションと管理性を向上させます。

[トポロジ（Topology）] ウィンドウのデバイスの集約

[トポロジ（Topology）] ウィンドウでグループにデバイスを集約したりグループから集約解除できます。

はじめる前に

Cisco APIC-EM の検出機能を使用してネットワークをスキャンし、データベースのデバイスおよびホスト インベントリに入力します。

ネットワーク設定内のデバイスを視覚的にグループ化および組織化する方法を決定します。

ステップ 1 [ナビゲーション（Navigation）] ペインで [トポロジ（Topology）] をクリックします。
[トポロジ（Topology）] ウィンドウが表示されます。

（注） [デバイス インベントリ（Device Inventory）] ウィンドウからデバイスのロケーション マーカーを追加した場合は、トポロジ マップ ビューが表示されます。その場所のトポロジを表示するには、ロケーション マーカーをクリックします。

ステップ 2 デバイスの集約を有効にするには、[集約の切り替え（Toggle Aggregation）] アイコンをクリックします。

（注） デバイスの集約はデフォルトでは有効になっています。

ステップ 3 別のデバイス アイコンにデバイス アイコンをドラッグ アンド ドロップします。
デバイス アイコンが集約されたデバイスのアイコンに変わります。集約されたデバイスのアイコンの詳細については、トポロジのアイコン，（71 ページ） を参照してください。

（注） また、複数のデバイスは、[複数選択（Multiselect）] アイコンをクリック、目的のデバイス上にマウスをドラッグ、[選択の集約（Aggregate Selected）] リンクをクリックすることによって、選択できます。

関連トピック

トポロジ
トポロジのアイコン，（71 ページ）
Topology Toolbar

[トポロジ（Topology）] ウィンドウでのデバイスの集約解除

はじめる前に

Cisco APIC-EM の検出機能を使用してネットワークをスキャンし、データベースのデバイスおよびホスト インベントリに入力します。

ネットワーク設定内のデバイスを視覚的にグループ化および組織化する方法を決定します。

ステップ 1 [ナビゲーション（Navigation）] ペインで、[トポロジ（Topology）] をクリックします。
[トポロジ（Topology）] ウィンドウが表示されます。

（注） [デバイス インベントリ（Device Inventory）] ウィンドウからデバイスのロケーション マーカーを追加した場合は、トポロジ マップ ビューが表示されます。その場所のトポロジを表示するには、ロケーション マーカーをクリックします。

ステップ 2 [集約されたデバイス（aggregated devices）] アイコンをクリックします。
集約されたデバイスのリストが表示されます。

ステップ 3 一覧から、集約されたデバイスから削除する各デバイスの [集約解除（Disaggregate）] リンクをクリックします。
デバイスが一覧と [集約されたデバイス（aggregated devices）] アイコンから削除されます。集約されたデバイス ラベルと [集約されたデバイス（aggregated devices）] アイコンは、デバイス数を反映するように更新されます。

トポロジ構造の設定

3 つのデフォルトのトポロジ レイアウトから選択できます。また、トポロジ グラフ全体のサイズや個々の要素を区切る間隔などの詳細設定を使用してこれらのレイアウトを変更することもできます。

はじめる前に

Cisco APIC-EM の検出機能を使用してネットワークをスキャンし、データベースのデバイスおよびホスト インベントリに入力します。

ステップ 1 [ナビゲーション（Navigation）] ペインで、[トポロジ（Topology）] をクリックします。
[トポロジ（Topology）] ウィンドウが表示されます。

（注） [デバイス インベントリ（Device Inventory）] ウィンドウからデバイスのロケーション マーカーを追加した場合は、トポロジ マップ ビューが表示されます。その場所のトポロジを表示するには、ロケーション マーカーをクリックします。

ステップ 2 [トポロジ（Topology）] ツールバーで、[フィルタ（Filters）] アイコンをクリックします。

ステップ 3 ドロップダウン リストからフィルタを選択します。使用可能なオプションは、[ブランチ（Branch）]、[接続（Connections）] 、または [デバイスとロール（Device & Role）] です。

ステップ 4 各フィルタの表示方法を設定するには、[詳細ビュー（Advanced View）] ボタンをクリックします。基本ビューに戻るには、[基本ビュー（Basic View）] ボタンをクリックします。

フィルタ	基本ビュー（**Basic View**）	詳細ビュー（**Advanced View**）
エンタープライズ	構造化された接続階層ビューにデバイスアイコンを配置します（上から下）。	デバイス タイプ（Device type）：スライダを使用して、デバイス タイプに基づいてデバイス アイコン間のスペースを調整します。 クラウド中心 X（cloud-centralizeX）：オン（デフォルト）になっている場合、デバイス アイコンは X 軸を中心として配置されます。 オフになっている場合、デバイス アイコンは X 軸に沿って配置されます。 デバイス ロール（Device role）：スライダを使用して、デバイス ロールに基づいてデバイス アイコン間のスペースを調整します。 ブランチ（Branch）：スライダを使用して、ブランチ間のスペースを調整します。 ノード オーバーラップ（Node overlap）：スライダを使用して、ノード間のスペースを調整します。 有線集約（aggregate-WIRED）：オンになっている場合（デフォルト）、有線ホストが集約されます。 オフになっている場合、有線ホストは集約解除されます。 無線集約（aggregate-WIRELESS）：オンになっている場合（デフォルト）、無線ホストが集約されます。 オフになっている場合、無線ホストは集約解除されます。 （注） デバイス アイコンの表示方法（水平または垂直）を変更するには、各スライダの横にあるドロップダウンから[x] または [y] を選択します。

フィルタ	基本ビュー（**Basic View**）	詳細ビュー（**Advanced View**）
接続	接続数（最小から最大の順）に基づいて左から右の順にデバイスアイコンを整列します。 （注） 集約されたデバイスは、このビューでは集約解除されます。	接続（Connections）：スライダを使用して、接続間のスペースを調整します。 ノードオーバーラップ（Node overlap）：スライダを使用して、ノード間のスペースを調整します。 中心 Y（centralizeY）：オン（デフォルト）になっている場合、デバイス アイコンは Y 軸を中心として配置されます。オフになっている場合、デバイス アイコンは Y 軸に沿って配置されます。 （注） デバイスアイコンの表示方法（水平または垂直）を変更するには、各スライダの横にあるドロップダウンから[x]または [y] を選択します。
タイプとロール（Type and Role）	デバイス タイプ（クラウド、ルータ、WLC、スイッチ、アクセス ポイント、有線、無線）とロール（ボーダールータ、コア、ディストリビューション、ホスト、およびアクセス）に基づいて上から下の順にデバイス アイコンを配置します。 （注） 集約されたデバイスは、このビューでは集約解除されます。	デバイス タイプ（Device type）：スライダを使用して、デバイスタイプに基づいてデバイス アイコン間のスペースを調整します。 デバイス ロール（Device role）：スライダを使用して、デバイス ロールに基づいてデバイス アイコン間のスペースを調整します。 ノードオーバーラップ（Node overlap）：スライダを使用して、ノード間のスペースを調整します。 中心 X（centralizeX）：オン（デフォルト）になっている場合、デバイス アイコンは X 軸を中心として配置されます。オフになっている場合、デバイス アイコンは X 軸に沿って配置されます。 （注） デバイスアイコンの表示方法（水平または垂直）を変更するには、各スライダの横にあるドロップダウンから[x]または [y] を選択します。

次の作業

現在のレイアウトを保存するか、または以前に保存したレイアウトをロードします。詳細については、トポロジ レイアウトの保存, （79 ページ）および保存されたトポロジ レイアウトを開く, （79 ページ）を参照してください。

関連トピック

トポロジ
トポロジのアイコン, （71 ページ）
Topology Toolbar
トポロジ
トポロジのアイコン, （71 ページ）
Topology Toolbar

トポロジ レイアウトの保存

後で開いて表示できるように、トポロジ レイアウトを保存できます。

はじめる前に

管理者ロールの権限が必要です。

検出を使用してネットワークをスキャンし、デバイスおよびホスト インベントリがデータベースに入力されている必要があります。

ステップ 1 [ナビゲーション（Navigation）] ペインで、[トポロジ（Topology）] をクリックします。
[トポロジ（Topology）] ウィンドウが表示されます。

ステップ 2 [トポロジ（Topology）] ツールバーで、[保存（Save）] アイコンをクリックします。

ステップ 3 [トポロジ タイトル（Topology Title）] フィールドにトポロジの名前を入力し、[新規保存（Save as New）] をクリックします。

ステップ 4 [OK] をクリックして保存を確認します。
トポロジが保存され、名前がダイアログボックスの上部に表示されます。

保存されたトポロジ レイアウトを開く

以前に保存したトポロジ レイアウトを開くことができます。

はじめる前に

管理者ロールの権限が必要です。

検出を使用してネットワークをスキャンし、デバイスおよびホスト インベントリがデータベースに入力されている必要があります。

トポロジ レイアウトが保存されている必要があります。

ステップ 1 [ナビゲーション（Navigation）] ペインで、[トポロジ（Topology）] をクリックします。
[トポロジ（Topology）] ウィンドウが表示されます。

ステップ 2 [トポロジ（Topology）] ツールバーで、[保存（Save）] アイコンをクリックします。
保存されたトポロジ レイアウトのリストが表示されたダイアログボックスが開きます。

ステップ 3 開くトポロジ レイアウトの [フォルダ（Folder）] アイコンをクリックします。

ステップ 4 [OK] をクリックして確認します。
[トポロジ（Topology）] ウィンドウにトポロジ レイアウトが開きます。

[トポロジ（Topology）] ウィンドウでのデバイス ロールの変更

スキャンプロセス中、検出された各デバイスにデバイス ロールが自動的に割り当てられます。デバイス ロールは、ネットワークにおける責任と配置に従ったデバイスの識別とグループ化に使用されます。

デバイスは、Cisco APIC-EM 内の以下のいずれかのロールを持つことができます。

- 不明：デバイス ロールが不明です。
- アクセス：デバイスはアクセス レイヤまたは第 1 階層/エッジに配置され、必要なタスクを実行します。
- ボーダー ルータ：デバイスはボーダー ルータで必要なタスクを実行します。
- ディストリビューション：デバイスはディストリビューション レイヤに配置され、必要なタスクを実行します。
- コア：デバイスはコアに配置され、必要なタスクを実行します。

デバイスを選択してデバイス データを表示すると、デバイス ロールを変更できます。

（注） デバイス ロールは、[デバイス インベントリ（Device Inventory）] ウィンドウでも変更できます。

はじめる前に

Cisco APIC-EM の検出機能を使用してネットワークをスキャンし、データベースのデバイスおよびホスト インベントリに入力します。

ステップ 1 [ナビゲーション（Navigation）] ペインで、[トポロジ（Topology）] をクリックします。
[トポロジ（Topology）] ウィンドウが表示されます。

（注） [デバイス インベントリ（Device Inventory）] ウィンドウからデバイスのロケーション マーカーを追加した場合は、トポロジマップ ビューが表示されます。その場所のトポロジを表示するには、マップ上のロケーション マーカーをクリックします。

ステップ 2 [トポロジ（Topology）] ウィンドウで特定のデバイスをクリックして選択します。

ステップ 3 [ロール（Role）] ドロップダウン リストからロール（[アクセス（Access）]、[コア（Core）]、[ディストリビューション（Distribution）]、または [ボーダー ルータ（Border Router）]）を選択します。

ステップ 4 （省略可能）その他のデバイスを選択し、デバイス ロールを変更します。

ステップ 5 [トポロジ（Topology）] ツールバーで [フィルタ（Filters）] アイコンをクリックします。

ステップ 6 （省略可能）ドロップダウン リストからフィルタを選択します。使用可能なオプションは、[ブランチ（Branch）]、[接続（Connections）]、または [デバイスとロール（Device & Role）] です。

ステップ 7 フィルタ タイプの右側にある更新ボタンをクリックして、デバイス ロールをすべて更新します。
[トポロジ（Topology）] 構造が更新され、変更されたデバイス ロールが表示されます。

デバイスおよびホストの検索

Cisco APIC-EM 検索機能を使用して、ネットワーク内の特定のホストまたはデバイスを探します。この機能は、任意の文字列値を使用してネットワークを検索することができます。特定のホストまたはデバイスを迅速に探すには、検索フィールドで以下の値を使用します。

- デバイスまたはホストの名前
- 集約ラベル
- IP アドレス
- デバイス ロール
- デバイス タイプ（Device Type）

（注） 検索機能では、フラグメント化された結果がサポートされます。たとえば、検索フィールドに **12** と入力すると、1 と 2 を含む IP アドレスまたはデバイス名を持つデバイスに関する結果が取得されます（.12、.120、.102、10.20、1-switch2 など）。

はじめる前に

Cisco APIC-EM の検出機能を使用してネットワークをスキャンし、データベースのデバイスおよびホスト インベントリに入力します。

検索用にネットワーク内で使用される文字列値を決定します。

ステップ 1 [ナビゲーション（Navigation）] ペインで [トポロジ（Topology）] をクリックします。
[トポロジ（Topology）] ウィンドウが表示されます。

（注） [デバイス インベントリ（Device Inventory）] ウィンドウからデバイスのロケーション マーカーを追加した場合は、トポロジ マップ ビューが表示されます。その場所のトポロジを表示するには、マップ上のロケーション マーカーをクリックします。

ステップ 2 [トポロジ（Topology）] ツールバーで、[トポロジの検索（Search Topology）] フィールドにキーワードを入力します。
入力を開始すると、コントローラは入力候補のリストを表示します。

（注） 検索フィールドで [x] をクリックして、検索キーワード フィールドと結果をクリアすることができます。

ステップ 3 検索結果のデバイスをクリックすると、そのデバイスとリンクが [トポロジ（Topology）] ウィンドウで強調表示されます。デバイスを再度クリックすると、そのデバイスの詳細データが表示されます。

ステップ 4 見つかったホストまたはデバイスのプロビジョニングまたはトラブルシューティング タスクに進みます。

次の作業

その他の文字列値を使用してネットワーク内のその他のホストまたはデバイスを検索するか、または以下のようなその他のタスクを実行します。

- 特定のデバイスのデータの表示
- ネットワーク内のデバイスへのタグの適用

関連トピック

トポロジ
トポロジのアイコン，（71 ページ）
Topology Toolbar

デバイスへのタグの適用

単一の属性を持つネットワーク内のデバイスに関連付けるために Cisco APIC-EM タグ機能を使用します。タグは、属性に基づいてデバイスのグループ化を有効にすることもできます。たとえば、タグを作成し、プラットフォーム ID、Cisco IOS リリース、またはロケーションに基づいて、デバイスをグループ化するために使用できます。

[トポロジ（Topology）] ウィンドウのネットワーク内のデバイスにタグを適用するには、次の手順を実行します。

（注） ホストにタグを適用するとサポートされません。

はじめる前に

次のタスクが実行済みである必要があります。

- Cisco APIC-EM の検出機能を使用してネットワークをスキャンし、データベースのデバイスおよびホスト インベントリに入力します。
- ネットワーク内のデバイスに適用するのに使用するタグを確認します。

ステップ 1 [ナビゲーション（Navigation）] ペインで、[トポロジ（Topology）] をクリックします。
[トポロジ（Topology）] ウィンドウが表示されます。

ステップ 2 タグ付けするデバイスをクリックします。複数のデバイスを選択するには、[複数選択（Multiselect）] アイコンをクリックします。複数選択機能の使用方法の詳細については、トポロジのアイコン，（71 ページ） を参照してください。

（注） 選択したデバイスの選択を解除するには、選択したデバイスの外側をクリックします。

[デバイス情報（Device Information）] ダイアログボックスが表示されます。

ステップ 3 [デバイス タギング（Device Tagging）] をクリックします。
[デバイス タギング（Device Tagging）] ダイアログボックスが表示されます。

ステップ 4 [使用可能なタグ（Available Tags）] カラムから、選択したデバイスに適用するタグをクリックします。目的のタグが存在しない場合は、次の手順に従って作成することができます。

a) [タグ タイトル（Tag Title）] フィールドにタグの名前を入力します。
b) [新しいタグの追加（+New Tag）] をクリックします。

ステップ 5 タギングが完了したら、[x] をクリックして、このダイアログボックスを閉じます。

ステップ 6 タグ付けしたデバイスの 1 つをクリックしてタギングを確認できます。
[デバイス情報（Device Information）] ダイアログボックスが、デバイスに適用されるタグの合計数と名前とともに [タグ（Tags）] フィールドに表示されます。

タグ付きデバイスの表示

[トポロジ（Topology）] ウィンドウにタグ付きデバイスを表示するには、次の手順を実行します。

はじめる前に

次のタスクが実行済みである必要があります。

- ネットワーク上のデバイスを検出し、デバイスおよびホスト インベントリ データベースに入力する。
- [デバイス インベントリ（Device Inventory）] または [トポロジ（Topology）] ウィンドウを使用したタグの作成と適用。

ステップ 1 [ナビゲーション（Navigation）] ペインで、[トポロジ（Topology）] をクリックします。
[トポロジ（Topology）] ウィンドウが表示されます。

（注） [デバイス インベントリ（Device Inventory）] ウィンドウからデバイスのロケーション マーカーを追加した場合は、トポロジマップ ビューが表示されます。その場所のトポロジを表示するには、ロケーション マーカーをクリックします。

ステップ 2 [トポロジ（Topology）] ツールバーで、[タグ（Tags）] をクリックします。
タグ選択ボックスが表示されます。

ステップ 3 タグに関連付けられているデバイスを識別するには、タグをクリックします。デバイスを通常の表示に戻すには、タグを再度クリックします。
タグは色分けされているため、タグをクリックすると、それに関連付けられているデバイスの周囲に同じ色の円が描画されます。

（注） 複数のタグを一度にクリックできます。最初に表示するように選択したタグはデバイスの周囲の最も内側の円であり、次のタグは次の円、というように続きます。

ステップ 4 タグ選択ボックスを閉じるには、[トポロジ（Topology）] ツールバーで [タグ（Tags）] アイコンをクリックします。

パス トレースの実行

パス トレースについて

パス トレースでは、ネットワークで検出されたデバイスからプロトコルやその他のタイプのデータをコントローラで確認および収集し、このデータを使用して 2 つのホスト間またはレイヤ 3 インターフェイスとの間のパスを計算します。パス トレースアプリケーションを使用して、ネットワーク全体のさまざまなデバイス間に分散されているトラフィック パスをモニタし、デバッグできます。

ネットワークの 2 つのノード間でパス トレースを実行することにより、これらのタスクを実行します。2 つのノードは、有線ホスト、ワイヤレス ホスト、レイヤ 3 インターフェイスの組み合わ

せにできます。また、パス トレースの接続を確立するためにコントローラが使用するプロトコルとして、TCP または UDP を指定できます。

パス内のすべてのノードで、コントローラがデバイスとパスに関する情報をレポートします。たとえば、ノードの検出にレイヤ 2 プロトコルが使用されている場合、コントローラは、パスがスイッチド パスであることをレポートし、それに [スイッチド（Switched）] というラベルを付けます。検出されたデバイスで行われたロード バランシングの判断をコントローラが検出すると、パスが ECMP パスであることをレポートし、それに [ECMP] というラベルを付けます。パス トレースは、デバイスおよびパスに関する次の情報を確認できます。

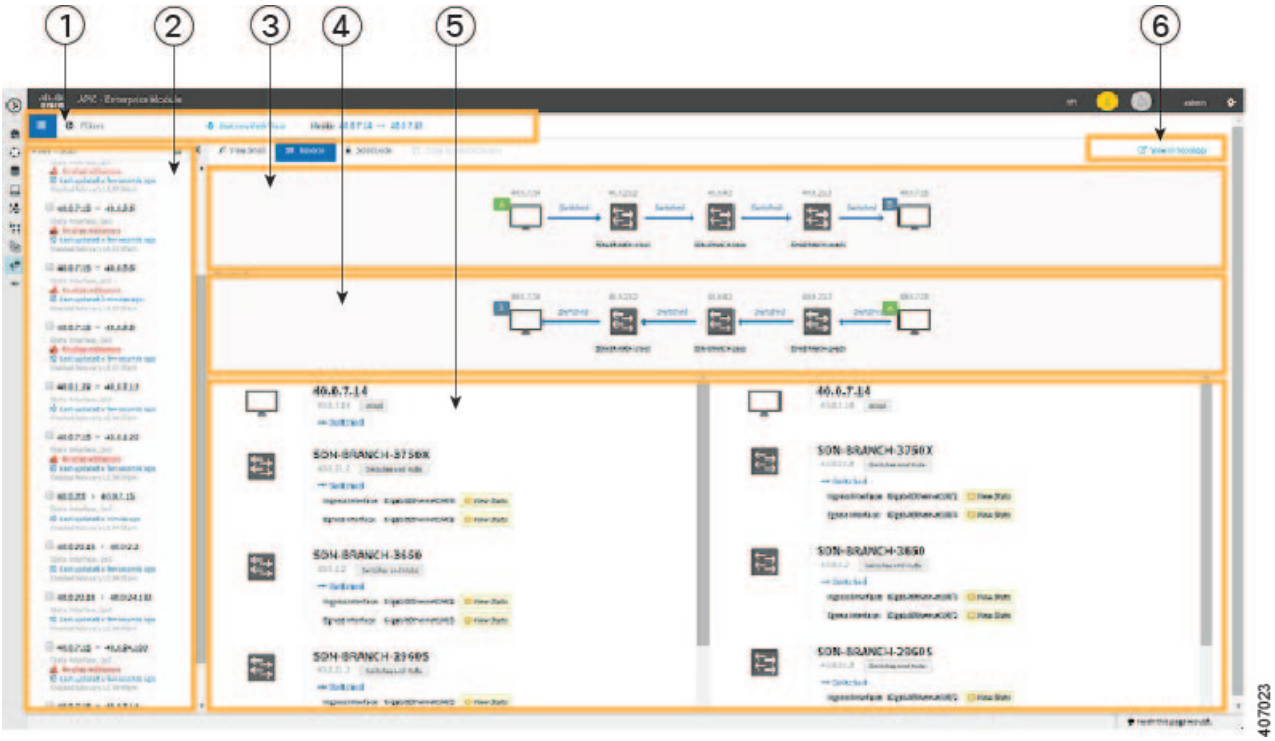
- HSRP
- SVI
- レイヤ 2
- レイヤ 2 ポート チャネル
- レイヤ 3 ルーティング プロトコル
- ECMP/TR
- NetFlow
- SVI での ECMP
- サブインターフェイス
- EIGRP
- レベル 3 再帰ループ

パス トレース内の不明なデバイスであるノード（通常はシスコ以外のデバイス）について、コントローラは、最後の既知のシスコ デバイスから（ホストの送信元 IP から）、次のネイバー シスコデバイス（宛先の送信元IPのこともある）までの不明なデバイス間のパスを計算します。不明なデバイスについて収集された IP アドレス データは、このネイバー シスコ デバイスからコントローラに送信され、トレース パスが計算されます。不明なデバイスは疑問符（?）としてコントローラの GUI に表示されます。

（注） 特定の状況では、パス トレースは、2 つ（または複数）のデバイス間を流れることがあります。どのデバイスが実際にパストレースのフローを受信したかを確認するために、コントローラはNetFlow コンフィギュレーションおよびデバイスに関するレコードを読み取ります（存在する場合）。デバイスからこのデータを読み取ることで、コントローラは実際のパスの可能性を判断できます。

パス トレースを実行するには、[ナビゲーション（Navigation）] ペインから [パス トレース（Path Trace）] をクリックします。[パス トレース（Path Trace）] ウィンドウが開きます。

図 *13* : *[パス トレース（Path Trace）]* ウィンドウ



コールアウト番号	[名前（Name）]	説明
1	ツールバー	[トレース結果のグラフィカル表示（Trace Results Graphical Display）] に表示されるパス トレースに対して作用するツールが含まれています。
2	**トレース結果のグラフィカル表示（Trace Results Graphical Display）**	パス トレースのグラフィカル表現を示します。
3	**トレース結果の詳細（Trace Results Details）**	パス上のデバイスに関する詳細情報を表示します。
4	**元のトレースの結果（Original Trace Results）**	送信元ホストから宛先ホストへのパス トレースを表示します。

コールアウト番号	[名前（Name）]	説明
5	**結果の反転（Reverse Results）**	宛先ホストから送信元ホストへの逆順のパス トレースを表示します。
[6]	[トポロジに表示（View in Topology）] ボタン	[トポロジ（Topology）] ウィンドウにトレース結果を表示します。 （注） トレース結果は、[パス トレース（Path Trace）] ウィンドウを終了すると保持されません。[トポロジに表示（View in Topology）] をクリックし、[トポロジ（Topology）] ウィンドウにトレース結果を表示してから [パス トレース（Path Trace）] ウィンドウに戻ると、前に表示していたトレース結果は表示されなくなります。

関連トピック

パス トレースの実行, （94 ページ）

パス トレースのサポート

Cisco APIC-EM は、物理的な接続、およびパス内でデバイスが使用するプロトコルに基づいて、キャンパス ネットワークと WAN ネットワークの両方に対するパス トレースの計算を実行できます。具体的には、Cisco APIC-EM は次のネットワーキング環境を通じてパス トレースをサポートします。

- キャンパス/データセンターからキャンパス/データセンターへ
- キャンパス/データセンターからブランチへ
- ブランチからキャンパス/データセンターへ
- ブランチからブランチへ

（注） 選択したホストまたはインターフェイスに対してコントローラがパス トレースを完了できない場合は、部分的なトレースの結果が表示されます。

パス トレース プロトコルおよびネットワーク接続

次の表に、Cisco APIC-EM パス トレースでサポートされるデバイス プロトコル、およびネットワーク接続（物理、ワイヤレス、仮想）を示します。

（注） プラットフォームおよびシナリオごとのプロトコル、ワイヤレス、および AP サポートの詳細については、『*Release Notes for the Cisco Application Policy Infrastructure Controller Enterprise Module*』を参照してください。

表 *13*：パス トレースのサポートされるデバイス プロトコルとネットワーク接続

サポートされるデバイス プロトコルおよびネットワーク接続	説明
ボーダー ゲートウェイ プロトコル（BGP）	ネットワークでBGPを使用すると、コントローラの GUI を通じて所定のアプリケーション フローに対するパス トレースを表示できます。ユーザは、特定のアプリケーションが使用している正確なパスを特定できます。 このパス トレース計算で使用されるデータは検出プロセス中に取得され、コントローラのデータベース内に保存されて最新に保たれます。
等コスト マルチ パス（ECMP）	ネットワークでECMPルーティングのストラテジーを使用すると、コントローラのGUIを通じて所定のアプリケーション フローに対するパス トレースを表示できます。ユーザは、特定のアプリケーションが使用している正確なパスを特定できます。 このパス トレース計算に使用されるデータは、パス計算の要求時にネットワーク デバイスを通じて生成されるオンデマンド クエリを通じて取得されます。 （注） パス トレース セグメント内のデバイス間で ECMP が使用されると、コントローラの GUI に表示されます。
ホットスタンバイ ルータ プロトコル（HSRP）	ネットワーク内でHSRPが使用されると、コントローラは所定のセグメントに対するHSRPのアクティブ ルータを自動的に検索し、パス トレースのための適切なパスを計算します。 このパス トレース計算で使用されるデータは検出プロセス中に取得され、コントローラのデータベース内に保存されて最新に保たれます。

サポートされるデバイス プロトコルおよびネットワーク接続	説明
Intermediate System-to-Intermediate System（IS-IS）プロトコル	ネットワークで IS-IS を使用する際は、コントローラの GUI を通じて所定のアプリケーション フローに対するパス トレースを表示できます。ユーザは、特定のアプリケーションが使用している正確なパスを特定できます。 このパス トレース計算で使用されるデータは検出プロセス中に取得され、コントローラのデータベース内に保存されて最新に保たれます。
レイヤ 3 転送インターフェイス	コントローラは、2 つのレイヤ 3 転送インターフェイス間、またはレイヤ 3 転送インターフェイスとホスト間のパス トレースを実行できます。

サポートされるデバイス プロトコルおよびネットワーク接続	説明
MPLS-VPN（WAN）	コントローラは、ブランチ間で接続された、プロバイダー管理の MPLS-VPN サービスに対するパス トレース サポートを提供します。このタイプのパス トレースでサポートされるデバイスには、次のものがあります。 • Cisco ASR 1000 Series Aggregation Services Router • Cisco ASR 9000 Series Aggregation Services Router • Cisco Integrated Services Routers（ISR）G2 すべてのカスタマー エッジ（CE）ルータで NetFlow が有効になっており、ホストとルータ間でトラフィックが流れている必要があります。 （注） 上記のサポート対象のデバイスは、[デバイスインベントリ（Device Inventory）] の [デバイスロール（Device Role）] について [ボーダー ルータ（Border Routers）] としてタグ付けされます。サポートされる上記のデバイスは、パス トレースの実行時にボーダー ルータとしてタグ付けしておく必要があります。 このパス トレース計算に使用されるデータは、パス計算の要求時にネットワーク デバイスを通じて生成されるオンデマンド クエリを通じて取得されます。
Open Shortest Path First プロトコル（OSPF）	ネットワークで OSPF を使用する際は、コントローラの GUI を通じて所定のアプリケーション フローに対するパス トレースを表示できます。ユーザは、特定のアプリケーションが使用している正確なパスを特定できます。 このパス トレース計算で使用されるデータは検出プロセス中に取得され、コントローラのデータベース内に保存されて最新に保たれます。

サポートされるデバイス プロトコルおよびネットワーク接続	説明
物理的な接続（イーサネット、Serial over SONET、および Packet over SONET（PoS））	所定のアプリケーション フローに対するパス トレースは、イーサネット、Serial over SONET、および Packet over SONET を介して表示できます。 このパス トレース計算で使用されるデータは検出プロセス中に取得され、コントローラのデータベース内に保存されて最新に保たれます。
スパニングツリー プロトコル（STP）	コントローラは、スパニング ツリー プロトコル（STP）のレイヤ 2 サポートを提供します。 このパス トレース計算で使用されるデータは検出プロセス中に取得され、コントローラのデータベース内に保存されて最新に保たれます。
スタティック ルーティング	ネットワークでスタティック ルーティングを使用する際は、コントローラの GUI を通じて所定のアプリケーション フローに対するパス トレースを表示できます。ユーザは、特定のアプリケーションが使用している正確なパスを特定できます。 このパス トレース計算で使用されるデータは検出プロセス中に取得され、コントローラのデータベース内に保存されて最新に保たれます。
仮想接続：レイヤ 2 ポート チャネル	ネットワーク内で仮想接続（レイヤ 2 ポート チャネル）を使用する際は、所定のアプリケーション フローに対するパス トレースが表示されます。仮想インターフェイス（ポート チャネル）を介してパス トレースが表示され、ユーザはアプリケーションに対するエンドツーエンドのパスを確認できます。
仮想接続：VLAN/SVI	ネットワーク内で仮想接続（VLAN/SVI）を使用する際は、所定のアプリケーション フローに対するパス トレースが表示されます。パス トレースが表示され、ユーザはアプリケーションに対するエンドツーエンドのパスを確認できます。 このパス計算で使用されるデータは検出プロセス中に取得され、コントローラのデータベース内に保存されて最新に保たれます。

サポートされるデバイス プロトコルおよびネットワーク接続	説明
ワイヤレス	コントローラは、Control and Provisioning of Wireless Access Points（CAPWAP）、802.11、およびモビリティに対するパス トレース サポートを提供します。 ワイヤレス ネットワーク要素を使用する際は、所定のアプリケーション フローに対するパス トレースが表示されます。ユーザは、特定のアプリケーションが使用している正確なパスを認識します。 （注） パス トレース中にCAPWAPまたはモビリティ トンネリング（ローミング用）のいずれかが検出されると、それがコントローラのGUIに表示されます。 このパス計算で使用されるデータは検出プロセス中に取得され、コントローラのデータベース内に保存されて最新に保たれます。
等コスト マルチパス/トレース ルート（ECMP/TR）	ネットワーク内でECMP/TRを使用する際は、コントローラのGUIを通じて所定のアプリケーション フローに対するパス トレースを表示できます。ユーザは、特定のアプリケーションが使用している正確なパスを特定できます。 このパス トレース計算で使用されるデータは、デバイスをポーリングすることによってオンデマンドで取得されます。ECMPでパス トレースを実行すると、要求されたタプルについてのCisco Express Forwarding（CEF）による検索がデバイスでオンデマンドで実行されます。パス トレースにおいてパス内に多数の未定義または管理対象外のデバイスが検出されると、最後の既知または管理対象のCiscoデバイスからオンデマンドでパス トレースが実行され、そのトレース ルート結果の最初の既知または管理対象のCiscoデバイスからパス計算が再開されます。パス トレースを使用して検出された未定義または管理対象外のホップは、未定義のデバイスとして、IPアドレスとともにパスに追加されます。

サポートされるデバイス プロトコルおよびネットワーク接続	説明
NetFlow	ネットワークで Netflow を使用する際は、コントローラの GUI を通じて所定のアプリケーション フローに対するパス トレースを表示できます。ユーザは、特定のアプリケーションが使用している正確なパスを特定できます。 宛先に複数のボーダールータがあると、実際の入力ボーダールータを見つけるためにデバイスの Netflow キャッシュが使用されます。これらのデバイスの Netflow レコードが、所定のタプルについて、オンデマンドで照合されます。ボーダー ルータ上に Netflow を設定する必要があります。Netflow が設定されていない場合、入力インターフェイスを見つけるためにトレースルートが使用されますが、これは正確でない場合があります。
サブ インターフェイス	ネットワーク内でサブインターフェイスを使用する際は、所定のアプリケーションフローに対するパス トレースが表示されます。2 つのサブインターフェイス間のパス トレースが表示され、ユーザはアプリケーションに対するエンドツーエンドのパスを視覚化できます。
Enhanced Interior Gateway Routing Protocol（EIGRP）	ネットワークで EIGRP を使用すると、コントローラの GUI を通じて所定のアプリケーションフローに対するパストレースを表示できます。ユーザは、特定のアプリケーションが使用している正確なパスを特定できます。 このパス トレース計算で使用されるデータは検出プロセス中に取得され、コントローラのデータベース内に保存されて最新に保たれます。

サポートされるデバイス プロトコルおよびネットワーク接続	説明
レイヤ 3 の再帰ルックアップ	ネットワークでレイヤ 3 の再起ルックアップを使用すると、コントローラの GUI を通じて所定のアプリケーション フローに対するパス トレースを表示できます。ユーザは、特定のアプリケーションが使用している正確なパスを特定できます。最大 3 つの再起ルックアップがサポートされます。 このパス トレース計算で使用されるデータは検出プロセス中に取得され、コントローラのデータベース内に保存されて最新に保たれます。

パス トレースの実行

ネットワーク内の 2 つのノード間のパス トレースを実行できます。2 つのノードは、2 つのホストまたはレイヤ 3 インターフェイス、あるいはその両方の場合があります。

（注） パス トレース アプリケーションでは、精度に関する通知（パーセント数が含まれた赤色のボックス）が表示されます。ノードまたはパス セグメントに表示される精度に関する通知は、パスを決定するために使用される情報に基づいたパスの精度レベルを示します。精度に関する通知をクリックすると、そのパス トレースの精度を向上させるために実行する提案が表示されます。これらの提案を使用してパス上のデバイス設定を調整し、2 回目のトレースを実行してより正確な結果を得ることができます。

はじめる前に

検出機能を使用してネットワークをスキャンし、データベースのデバイスおよびホスト インベントリを入力します。

コントローラがデバイスに SSH または Telnet アクセスできることを確認します。

ステップ 1 [ナビゲーション（Navigation）] ペインで、[パス トレース（Path Trace）] をクリックします。
[パス トレース（Path Trace）] ウィンドウが表示されます。

ステップ 2 [ソース IP（Source IP）] フィールドに、最初のホストまたはレイヤ 3 転送インターフェイスの IP アドレスを入力します。
コントローラによって認識されるホストの現在のリストを確認するには、[ホスト インベントリ（Host Inventory）] テーブルを表示します。

デバイスのレイヤ 3 転送インターフェイスをリスト表示するには、デバイス名または IP アドレスの後にコロン「：」を付けて入力します。デバイス上の IP アドレスを持つすべてのインターフェイスが表示されます。

ステップ 3 [宛先 IP（Destination IP）] フィールドに、2 番目のホストまたはレイヤ 3 転送インターフェイスの IP アドレスを入力します。
コントローラによって認識されるホストの現在のリストを確認するには、[ホスト インベントリ（Host Inventory）] テーブルを表示します。

デバイスのレイヤ 3 転送インターフェイスをリスト表示するには、デバイス名または IP アドレスの後にコロン「：」を付けて入力します。デバイス上の IP アドレスを持つすべてのインターフェイスが表示されます。

ステップ 4 （任意） [ソース ポート（Source Port）] フィールドに、最初のホストのポート番号を入力します。

ステップ 5 （任意） [宛先ポート（Destination Port）] フィールドに、2 番目のホストのポート番号を入力します。

ステップ 6 （任意） [プロトコル（Protocol）] フィールドで、レイヤ 4 パス トレース プロトコルのドロップダウン メニューから [tcp] または [udp] を選択します。

ステップ 7 [トレース（Trace）] をクリックします。
パス トレースの出力を確認します。詳細については、パス トレースの結果の理解, （95 ページ）を参照してください。

ステップ 8 パス トレースを [トポロジ（Topology）] ウィンドウで表示するには、次の手順を実行します。[トポロジに表示（View in Topology）] をクリックします。
ネットワークのパス トレースが強調表示された状態で [トポロジ（Topology）] ウィンドウが開きます。
[トポロジ（Topology）] ウィンドウの詳細については、トポロジ, （67 ページ） を参照してください。

（注） デバイスのロケーション マーカーを追加した場合は、ロケーション マーカーがトポロジ マップに表示されます。その場所のトポロジを表示するには、ロケーション マーカーをクリックします。

関連トピック

パス トレースについて, （84 ページ）

パス トレースの結果の理解

パス トレースを実行すると、コントローラは [パスの結果（Path Results）] ペインに結果を表示します。

ツールバー

[パスの結果（Path Results）] ペインの上部にあるツールバーには、パス トレースの表示を調整するボタンがあります。

縮小表示（View Small）	トレース パスの詳細を大きく表示できるよう、トレース パスのグラフィックを最小化します。
逆方向の表示（Show Reverse）	ホストの送信先 IP からホストの送信元 IP のトレース パスのグラフィックを表示します。 逆方向パス トレースのグラフィックは、元のパス トレースのすぐ下に表示されます。 逆方向パス トレースの詳細は、元のパス トレースの詳細の右に表示されます。
スクロール ロック（Scroll Lock）	パス トレースおよび逆方向パス トレース詳細ウィンドウのスクロールをロックします。（[逆方向の表示（Show Reverse）] が有効になっている場合に使用できます。）
重複するデバイスの表示（Show Duplicate Devices）	パス トレース内の重複するデバイスを表示/非表示します。
トポロジに表示（View in Topology）	[トポロジ（Topology）] ウィンドウを開き、ネットワーク トポロジのパス トレースの結果を強調表示します。[トポロジ（Topology）] ウィンドウの使用方法の詳細については、トポロジ, （67 ページ）を参照してください。

（注） トレースの結果に応じて、上記の一部のボタンはグレーで表示され使用できない場合があります。

トレース結果のグラフィカル表示

コントローラはパス方向、およびパスが通過するデバイスとネットワークをグラフィカルに表示します。次の情報も表示されます。

- 送信元と宛先間のパス トレース上のホストとデバイス（IP アドレスを含む）。
- リンク情報ソース（Link Information Source）：デバイス間のパスの発信元が [スイッチド（Switched）]、[STP]、[ECMP]、[ルーテッド（Routed）]、[トレース ルート（Trace Route）]、または他の送信元タイプであるかどうか。

（注） パス トレースが長く、多くのデバイスが含まれている場合、パス トレースの各デバイスをクリックして、そのデバイスに焦点を当てるように GUI の表示を調整します。その後、そのデバイスからビューを上下にスクロールできます。

トレース結果の詳細

パス トレースで各デバイスについて表示される詳細情報を確認します。

IP	デバイスの IP アドレス
タイプ（Type）	有線デバイスまたはワイヤレス デバイス（アクセス ポイント、スイッチ、またはルータ）。
リンクの送信元（Link Source）	パス内の 2 つのデバイス（デバイス A とデバイス B）およびパスの方向がデバイス A からデバイス B であると仮定すると、ネットワーク構成に応じて次のリンク情報の送信元タイプが表示される場合があります。 • BGP：リンクはデバイス A に設定された BGP ルートに基づきます。 • ECMP：リンクは Cisco Express Forwarding（CEF）のロード バランシングの決定に基づきます。 • EIGRP：リンクはデバイス A に設定された EIGRP ルータに基づきます。 • 接続（Connected）：デバイス B はデバイス A に直接接続されています。 • VLAN 間ルーティング（InterVlan Routing）：パスがデバイス B に切り替えられるデバイス A に SVI 設定があります。 • ISIS：リンクはデバイス A に設定された IS-IS ルートに基づきます。 • NetFlow：リンクはデバイス A で送信元と宛先について収集された NetFlow レコードに基づきます。 • OSPF：リンクはデバイス A に設定された OSPF ルートに基づきます。 • スタティック（Static）：リンクはスタティック ルートに基づきます。 • スイッチド（Switched）：リンクはレイヤ 2 VLAN 転送に基づきます。 • トレース ルート（Trace Route）：リンクはトレース ルートに基づきます。 • 有線（Wired）：デバイス A はデバイス B に接続された有線ホストです。 • 無線（Wireless）：デバイス A はデバイス B（アクセス ポイント）に接続されたワイヤレス ホストです。

トンネル（Tunnels）	CAPWAP データ（ワイヤレス）またはモビリティ トンネリング （注） コントローラは関連デバイス周辺のパス トレース CAPWAP トンネルのグラフィック ビューを表示します。ズームインまたはズームアウトしてビューを自動調整できます。
入力インターフェイス（Ingress interface）	パス トレースのデバイスの入力インターフェイス（物理または仮想）。 たとえば、物理入力インターフェイスは [GigabitEthernet1/0/1]、仮想入力インターフェイスは [GigabitEthernet1/3 [Vlan1]] となります。
出力インターフェイス（Egress interface）	パス トレースのデバイスの出力インターフェイス（物理または仮想）。 たとえば、物理インターフェイスは [GigabitEthernet1/0/2]、仮想入力インターフェイスは [GigabitEthernet1/4 [Vlan2]] となります。
精度の注記（Accuracy note）	デバイス間のセグメントのパス トレースについて不確実な点がある場合、このセグメントの計算されたパスの精度に関する注記がパーセンテージで表示されます。

第 6 章

API マニュアルの確認

- Cisco APIC-EM API マニュアルについて，99 ページ
- Cisco APIC-EM API のテスト，105 ページ

Cisco APIC-EM API マニュアルについて

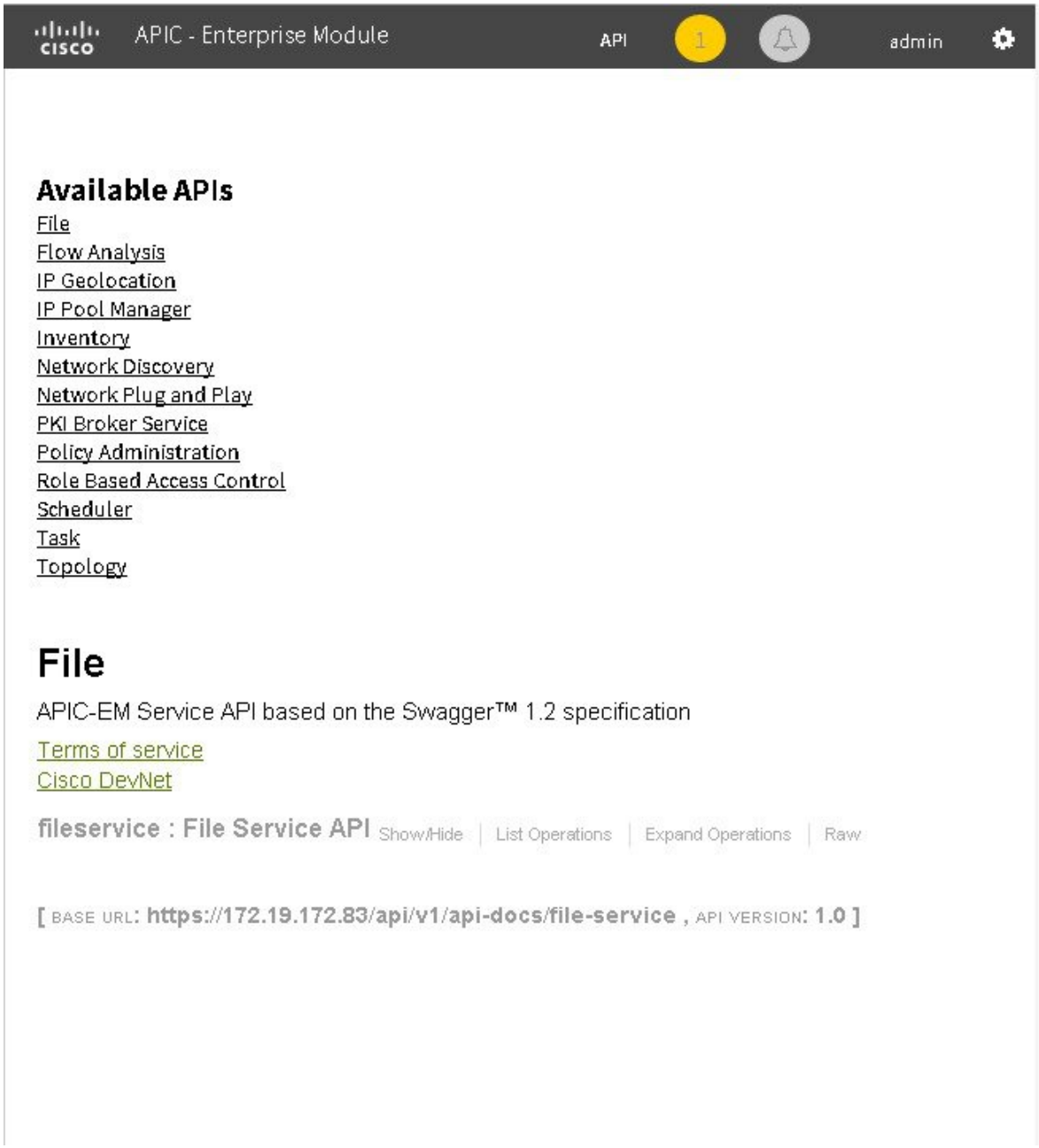
Cisco APIC-EM コントローラは、インタラクティブな、ノースバウンド Representational State Transfer（REST）API マニュアルを提供します。REST API マニュアルを使用して、大規模なネットワーク管理システムを持つコントローラを統合し、ネットワークの管理に役立てることができます。

（注） コントローラは、ルートのサービス カタログにインストールしたサービスに基づいてノースバウンド REST API マニュアルを表示します。

グローバル ツールバーからノースバウンド REST API マニュアルにアクセスするには、[API] をクリックします。

（注） REST API マニュアルは、Swagger 1.2 仕様に基づいています。

図 *14* : *[API]* ウィンドウ



インタラクティブなノースバウンド REST API マニュアルでは、次の内容を提供します。

- ノースバウンド REST API のサービスの条件および Cisco Developer Community の Web サイトに関する次の情報へのリンクは、次のとおりです。
  - 利用規約（Terms of Service）：API が置かれているサーバにアクセスするための利用規約を確認します。
  - Cisco DevNet：Cisco Developer Community の Web サイトにアクセスします。 この Web サイトは、開発者情報、コミュニティ フォーラム、開発者サンドボックスなどの開発者向けのサポートを提供します。
- コントローラによって使用され、アプリケーションによって構成された、サポートされているノースバウンド REST API に関するリストは、次のとおりです。
  - ファイル
  - IP プール マネージャ
  - ネットワーク プラグ アンド プレイ サービス
  - ポリシー管理
  - ロール ベース アクセス コントロール
  - スケジューラ
  - タスク
  - トポロジ

（注） アクティブなサービスが実行されているアプリケーションのみが、メニューリストに表示されます。

- それぞれのノースバウンド REST API でサポートされているメソッドのリストは、次のとおりです。
  - GET：リソースを取得します。
  - POST：リソースを作成します。
  - PUT：リソースの状態を変更または更新します。
  - DELETE：リソースを削除します。
- API のメソッドは、次のとおりです。
  - 表示/非表示（Show/Hide）：API でサポートされているメソッド（GET、POST、PUT、および DELETE）を表示するか非表示にします。
  - 操作の表示（List Operations）：API でサポートされているメソッド（GET、POST、PUT、および DELETE）を表示します。

- 操作の展開（Expand Operations）：以下のような、API のメソッドの展開ビューを表示します。
  - 実装上の注意事項（Implementation Notes）：実装の詳細など、ノースバウンド REST API についての簡単な説明です。
  - 応答クラス（Response Class）：モデル ビュー、モデル スキーマ ビュー、応答コンテンツ タイプです。
  - パラメータ（Parameters）：パラメータ、説明、パラメータ タイプ、データ型の定義（文字列、整数、またはモデル）、およびテストの入力フィールドです（必要な場合）。
  - エラー ステータス コード（Error Status Codes）：HTTP ステータス コードと原因の定義。

- 未処理のコンテンツ：外部の Swagger UI （ユーザが用意）の未処理のコンテンツを提供して、ノースバウンド REST API にアクセスします。コンテンツはテキスト ファイル形式で提供されます。

ノースバウンド REST API に関する理解を深めるために、サンプルのメソッドを実行し、結果の出力を取得できます。詳細については、Cisco APIC-EM API のテスト，（105 ページ）を参照してください。

関連トピック

Cisco APIC-EM API の確認とテスト
共通の外部 RESTful サービス HTTP 応答コード，（103 ページ）

サポートされる HTTPS メソッドおよび一般構造

次の表では、Cisco APIC-EM でサポートされる HTTPS メソッドおよび構造について説明します。

HTTPS メソッド タイプ	構造
GET	Get メソッド タイプで次の値を使用します。 • /noun • /noun/count • /noun/{start}/{end} • /noun/{noun-id}
POST	複製リソース、または次の応答を送信した場合、POST メソッド タイプは、409 応答コードを返します。 {"response":"id-of-created-resource"}

HTTPS メソッド タイプ	構造
PUT	PUT メソッド タイプは次の応答を返します。 {"response":"message-about-attributes-that-changed"}
DELETE	DELETE メソッド タイプは、失敗した場合 404 応答コード、または次の応答を返します。 {"response":"message-about-deletion"}

次は、Cisco APIC-EM でサポートされる HTTPS メソッドの一般的なガイドラインです。

- 各メソッドは 1 つのリソースの操作として使用されます
- 各リソースは 1 つの名詞で表示されます（例：ネットワーク デバイス、リンク、インターフェイス、ホスト）
- リソースは、ID 番号ごとに（名前ごとではない） HTTPS メソッドで参照されます
- Get API によって返されるエントリの最大数は 500 です（デフォルト）。API は、1 つのコールに 500（デフォルト）を超えるエントリは提供しません。
- すべてのリソースでの CRUD （作成、読み取り、更新、削除）操作は、1 つの API コールでは許可されません。

共通の外部 RESTful サービス HTTP 応答コード

外部 RESTful サービスは、以下で説明されているように共通の HTTP 応答コードを返します。応答ヘッダーで返されるステータス コードに加えて、各応答には、要求の性質に応じて、（JSON ファイル形式の）追加のコンテンツがある場合があります。

表 *14*：成功（*2xx*）コード

状態コード	説明
200 OK	要求は成功しました。結果は応答本文に含まれています。
201 Created	POST/PUT 要求が処理され、新しいリソースが作成されました。リソースに関する情報は、応答本文にあります。
202 Accepted	要求が受け入れられて処理されましたが、処理が完了していません。
204 No Content	要求は成功しましたが、コンテンツが戻りませんでした。
206 部分的な内容	GET 要求は範囲ヘッダーを含み、サーバは範囲に一致する部分的な内容を返しました。

表 *15* : クライアント エラー（*4xx*）コード

状態コード	説明
400 不正な要求	クライアントがサーバが理解できない要求をしました（たとえば、要求構文が正しくない）。
401 未認証	要求に含まれるクライアントの認証クレデンシャルが欠落しているか、または無効です。
403 禁止	サーバは認証クレデンシャルを認識しますが、この要求を実行するためのクライアントが承認されません。
404 Not Found	クライアントは存在しないシステムに対して要求を行いました。
409 競合	ターゲット リソースは競合状態です（たとえば、複数のユーザによって編集されているリソースの編集の競合）。後で要求を再試行すると成功する場合があります。
415 サポートされないメディアタイプ	クライアントは、サーバがサポートしない形式の要求本文を送信しました（たとえば、JSON だけを受け入れるサーバに対する XML）。

表 *16* : サーバ エラー（*5xx*）コード

状態コード	説明
500 Internal Server Error	サーバは要求を処理できませんでした。
501 実装されない	サーバは要求を処理するために必要な機能を完了していません。
503 Service Unavailable	サービスは（一時的に）利用できません。

関連トピック

Cisco APIC-EM API の確認とテスト
Cisco APIC-EM API マニュアルについて，（99 ページ）

Cisco APIC-EM API のテスト

はじめる前に

[API] ウィンドウで、Cisco APIC-EM ノースバウンド REST API をテストできます。

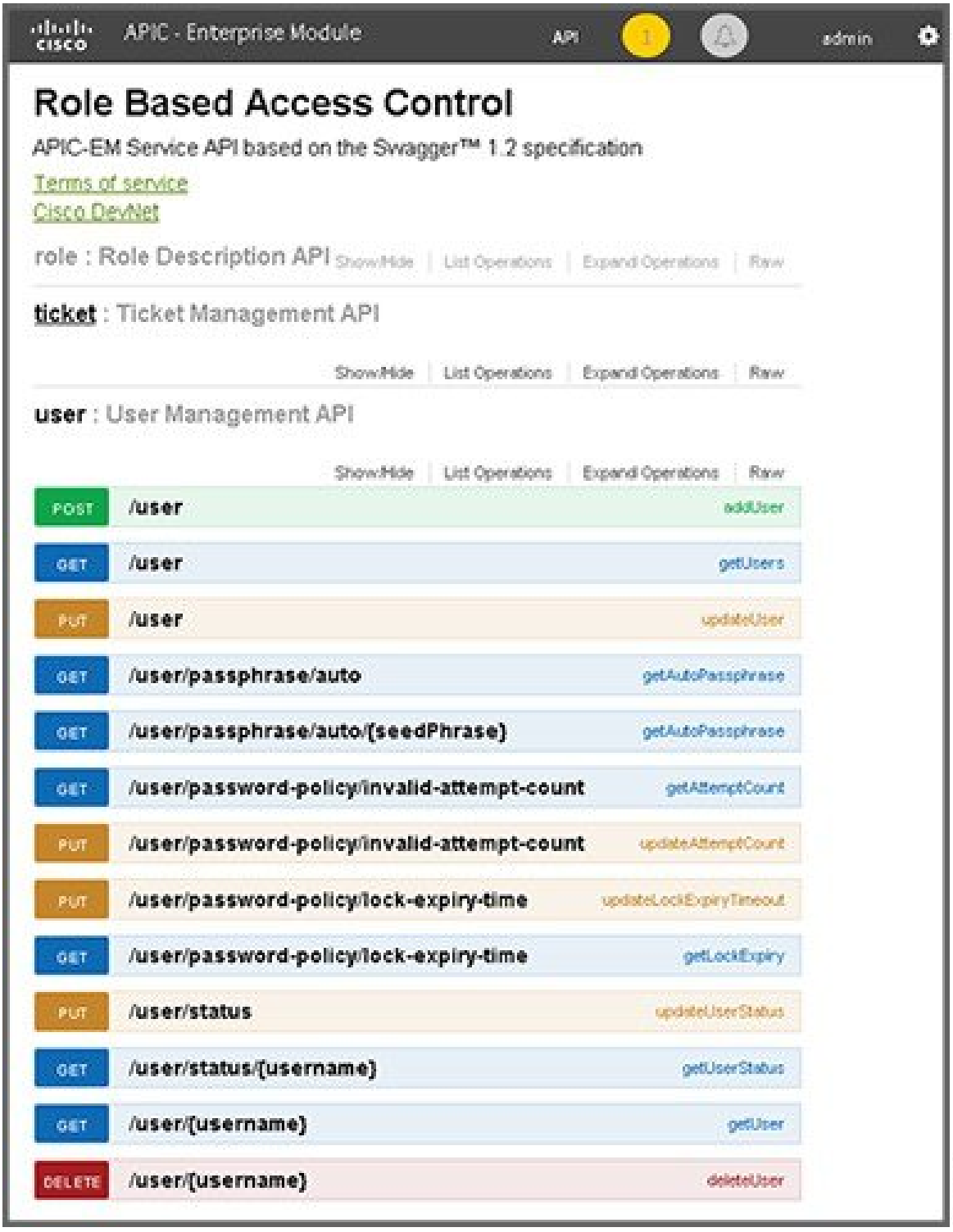
ステップ 1 [グローバル（Global）] ツールバーで、[API] をクリックします。

ステップ 2 使用可能な API のリストから、API を選択します。
たとえば、[ロールベース アクセス コントロール（Role Based Access Control）] API を選択します。

ステップ 3 ロールベース アクセス コントロール API のリストから、サポートされているメソッドを表示する対象の API を選択します。

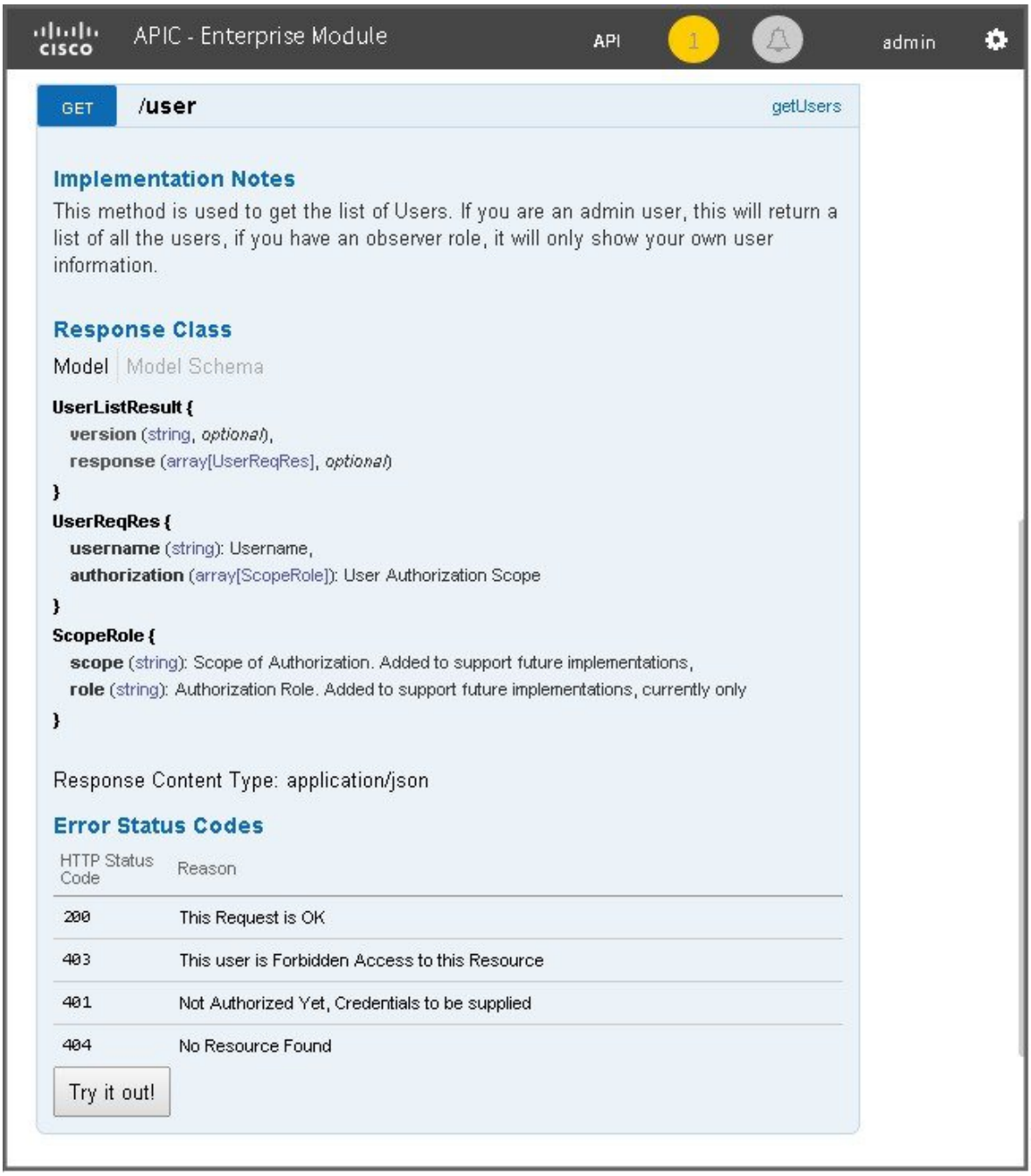
たとえば、[ユーザ（user）] API を選択します。

図 *15*：ユーザ管理 *API* でサポートされるメソッド


APIC - Enterprise Module
API
admin
Role Based Access Control
APIC-EM Service API based on the Swagger™ 1.2 specification
Terms of service
Cisco DevNet
role : Role Description API Show/Hide | List Operations | Expand Operations | Raw
ticket : Ticket Management API
Show/Hide | List Operations | Expand Operations | Raw
user : User Management API
Show/Hide | List Operations | Expand Operations | Raw
POST /user addUser
GET /user getUsers
PUT /user updateUser
GET /user/passphrase/auto getAutoPassphrase
GET /user/passphrase/auto/{seedPhrase} getAutoPassphrase
GET /user/password-policy/invalid-attempt-count getAttemptCount
PUT /user/password-policy/invalid-attempt-count updateAttemptCount
PUT /user/password-policy/lock-expiry-time updateLockExpiryTimeout
GET /user/password-policy/lock-expiry-time getLockExpiry
PUT /user/status updateUserStatus
GET /user/status/{username} getUserStatus
GET /user/{username} getUser
DELETE /user/{username} deleteUser

ステップ 4 [操作の展開（Expand Operations）] をクリックします。

図 *16* : *getUsers API* の展開ビュー



ステップ 5 各拡張 API メソッド ウィンドウの下部にある [試行（Try it out!）] ボタンをクリックすることにより、API をテストします。

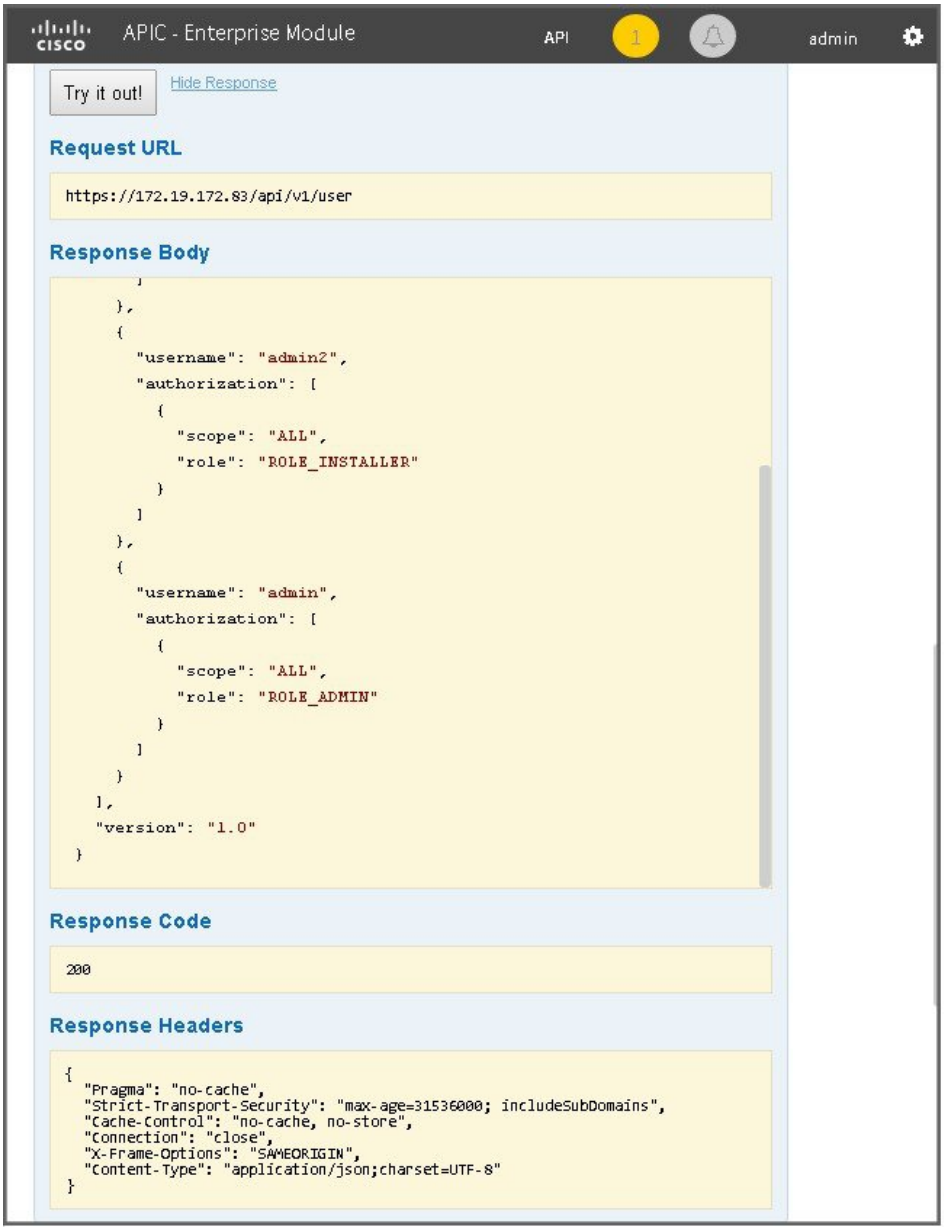
（注） API をテストする前に、いずれかの必須コンテンツ フィールドにコンテンツを入力します。

たとえば、[GET /user] に対して [試行（Try it out!）] ボタンをクリックし、以下の出力を確認します。

- 要求 URL（Request URL）：適切なメソッド（GET、POST、PUT、DELETE）に関して作成され、コントローラに送信される要求 URL を表示します。
- 応答本文（Response Body）：要求 URL に対する応答の例を表示します。
- 応答コード（Response Code）：応答例のエラー ステータス コードを表示します。

- 応答ヘッダー（Response Header）：応答ヘッダー：RESTful サービスによって返される応答を表示します。使用されている特定の HTTP ヘッダーが表示されます。

図 *17*：***getUsers API*** の出力



索 引

A

API 4
API マニュアル 99

C

Cisco APIC-EM 1
　概要 1

G

GUI の概要 4

H

HTTPS メソッド 102

I

Intermediate System-to-Intermediate System。参照先： IS-IS
inventory 45
　ホスト 45
IS-IS 71, 87
　トポロジ 71
　パス トレース 87
IWAN 4

O

Open Shortest Path First プロトコル（OSPF） 87
OSPF 71

P

Packet Over SONET（POS） 87

R

RBAC 49, 54
　アカウンティング 54

S

Static-Route 71

U

user 52, 54, 57, 58, 59
　password 54
　アクセス 59
　ユーザ情報の表示 59
　権限 52
　削除 58
　追加 57

い

インストーラ 51
インベントリ 25
　デバイス 25

お

オブザーバ 51

し

シスコのネットワーク プラグ アンド プレイ 4

す

スタティック ルーティング 87
スパニングツリー プロトコル（STP） 87

た

タグ 36, 38
　削除 36, 38
　追加 36

て

デバイス インベントリ 4, 25
　IOS 25
　MAC アドレス 25
　ウィンドウ 25
　シリアル番号 25
　タグ 25
　デバイス ファミリ 25
　デバイス ロール 25
　デバイスの状態 25
　デバイス名（Device Name） 25
　プラットフォーム 25
　最終更新時間 25
　参照先 25
　使用可能時間（Up Time） 25
　設定（Configuration） 25
　平均更新頻度 25
デバイス テーブル 25, 32, 33
　ビューの変更 33
　フィルタリング 32
デバイス ロール 34, 80

と

トポロジ 4, 68, 70, 71, 74, 75, 76, 79, 80, 81, 83
　L2 70
　L3 70
　アイコン 71
　ウィンドウ 68
トポロジ (続き)
　タグ 83
　ツールバー 68
　デバイス ロール 80
　検索 81
　構造の設定 76
　集約 74
　集約解除 74, 75
　保存 79

の

ノースバウンド REST API 99
ノースバウンド REST API マニュアル 105

は

パス トレース 84, 87, 94
　プロトコル 87
パスワードの変更 4

ふ

フィードバック 4
プラグ アンド プレイ 4

ほ

ボーダー ゲートウェイ プロトコル（BGP） 87
ポート チャネル 87
ホスト インベントリ 4, 45
　ウィンドウ 45
ホスト テーブル 45, 47
　filters 45
　ビューの変更 47
ホットスタンバイ ルータ プロトコル（HSRP） 87

ゆ

ユーザ ログ 60
ユーザおよびドメイン 52

ろ

ロール 50, 51
　オブザーバ 51
　管理者 50
ログアウト 4
ロケーション タグ 40
ロケーション マーカー 41, 44
　削除 44
　追加 41

わ

ワイルドカード文字 33