初回セットアップ ウィザード

この章は、次の項で構成されています。

初回セットアップ ウィザードについて

初回セットアップ ウィザードを使用して、Cisco APIC の初回セットアップを実行します。

- GUI を使用して Cisco APIC に初めてログインすると、初回セットアップ ウィザードが自動的に表示されます。
- Cisco APIC リリース 4.2(3) 以降では、  GUI ウィンドウの右上隅にある [システムツール（System Tools）] アイコン（Cisco APIC）をクリックし、**[APIC_release_number の新機能（What's New in *APIC_release_number*）]** を選択すると、初期設定ウィザードにアクセスできます。

[APIC へようこそ（Welcome to APIC）] ウィンドウが表示され、この特定のリリースに含まれる新機能に関する情報が示されます。

初回セットアップ ウィザードにアクセスするには、ウィンドウの右下にある **[初回セットアップの開始（Begin First Time Setup）]** または **[初回セットアップの確認（Review First Time Setup）]** をクリックします。**[基本の設定（Let's Configure the Basics）]** ウィンドウが表示され、Cisco APIC の設定に使用できる個々のページへのリンクが示されます。

少なくとも 1 つの BGP ルートリフレクタを含む初期設定が完了すると、**[サマリを続行（Proceed to Summary）]** ボタンが有効になります。設定のサマリータイルを表示するには、このボタンをクリックします。追加のタイルが **[以下がお望みですか（You Might want to ...）]** 見出しの下に表示されます。. これらの追加トピックはオプションですが、推奨されます。

次の項では、このウィンドウから使用できる各初期設定ページの詳細について説明します。

[Fabric Membership（ファブリック メンバーシップ）]

[ファブリック メンバーシップ（Fabric Membership）] ウィンドウを使用して、ACI ファブリックによって検出されたリーフおよびスパイン スイッチを登録します。ボックスに記載されているシリアル番号を使用して、リーフ スイッチとスパイン スイッチをファブリックに手動で追加することもできます。

（注） 少なくとも 2 つのリーフ スイッチと 2 つのスパイン スイッチを登録することを推奨します。初回セットアップ ウィザードを進めるには、少なくとも 1 つのリーフ スイッチと 1 つのスパイン スイッチを登録する必要があります。

[ファブリック メンバーシップ（Fabric Membership）] ウィンドウには、次の 2 つのセクションがあります。

- **検出済み**：このセクションでは、新しく検出されたが未登録のスイッチについて説明します。これらのノードのノード ID は 0 で、IP アドレスはありません。
- **登録済み**：このセクションでは、ACI ファブリックに登録されているすべてのスイッチに関する情報を提供します。

次のいずれかの方法でスイッチを登録できます。

- スイッチが **[検出済み（Discovered）]** セクションに表示されている場合は、そのスイッチの横にある **[登録（Register）]** ボタンをクリックして、**[ファブリック ノード メンバーの作成（Create Fabric Node Member）]** ウィンドウを開きます。この場合、**[ポッド ID（Pod ID）]** フィールドと **[シリアル番号（Serial Number）]** フィールドは **[ファブリック ノード メンバーの作成（Create Fabric Node Member）]** ウィンドウに自動的に入力されます。
- スイッチが **[検出済み（Discovered）]** セクションに表示されない場合は、[アクション（Action）] アイコン（ ）をクリックし、ドロップダウン リストから **[ファブリック ノード メンバーの作成（Create Fabric Node Member）]** を選択します。

[ファブリック ノード メンバーの作成（Create Fabric Node Member）] ウィンドウで、次の情報を入力します。

フィールド	設定
ポッド ID	ノードが存在するポッドを特定します。
シリアル番号（Serial Number）	必須：新しいスイッチのシリアル番号を入力します。

フィールド	設定
ノード ID（Node ID）	必須：100 以上の数字を入力します。最初の 100 ID は、APIC アプライアンス ノードのために予約されています。 （注） リーフ ノードとスパイン ノードには異なる数字をつけることをお勧めします。たとえば、100の範囲の番号リーフ(例：101、102) と 200 の範囲の番号スパイン (例：201、202)。 （注） ノード ID が割り当てられた後は、更新できません。ノードが **[登録済みノード (Registered Nodes)]** タブ表に追加された後、表の行を右クリックし、**[ノードとラック名の編集 (Edit Node and Rack Name)]** を選択してノードを更新できます。
Switch Name	leaf1 または spine3 などのノード名。
ノードタイプ（Node Type）	割り当てられたノードの役割を選択します。次のオプションがあります。 • **leaf** 必要に応じて、次のボックスのいずれかをオンにします。 • **リモート** • **仮想** • **階層 2 リーフ** • **spine** 必要に応じて、次のボックスをオンにします。 • **仮想** • **unknown**

[ファブリック ノード メンバーの作成（Create Fabric Node Member）] ウィンドウで情報を入力したら、**[送信（Submit）]** をクリックし、**[ファブリック メンバーシップ（Fabric Membership）]** で **[続行（Continue）]** をクリックして、初回セットアップ ウィザードの次のウィンドウに進みます。

管理

[アウトオブバンド管理（Out of Band Management）] ウィンドウを使用して、アウトオブバンド（OOB）ネットワークに接続するリーフ スイッチ、スパイン スイッチ、および APIC ノードの管理インターフェイス IP アドレスを設定します。複数のノードを選択して、IP アドレスの割り当てを開始します。

（注） 初回セットアップ ウィザードは、アウトオブバンド管理用にまだ設定されていないノードの設定に役立ちます。

次のフィールドにゲートウェイのアドレスを入力すると、検出されたノードごとに IP アドレスが自動的に提案されます。

- **IPv4 ゲートウェイ**：アウトオブバンド管理を使用した外部ネットワークへの通信用のIPv4 デフォルト ゲートウェイ アドレス。
- **IPv6 ゲートウェイ**：アウトオブバンド管理を使用した外部ネットワークへの通信用のIPv6 デフォルト ゲートウェイ アドレス。

[属性によるフィルタ（Filter by attributes）] 領域では、検出されたノードを属性でフィルタ処理できます。アウトオブバンド管理用に設定するために選択したノードを変更する場合は、**[編集（Edit）]** をクリックします。

[保存する（Save）] をクリックし、初期セットアップ ウィザードの次のウィンドウに進みます。

vPC ペア

[セットアップ - vPC ペア（Setup - vPC Pairs）] ウィンドウは、ファブリック ポリシー ノード エンドポイントを使用してグループのメンバー ノードを明示的に構成するために使用します。

[属性によるフィルタ（Filter by attributes）] 領域で、属性によって vPC ペアをフィルタリングできます。vPC ペアを設定するために選択した vPC ペアを変更する場合は、**[編集（Edit）]** をクリックします。

vPC ペア中央ペインで、**[アクション（Actions）]** ドロップダウン リストを展開し、**[vPC リーフ スイッチ ペアの作成（Create vPC Leaf Switch Pair）]**、**[vPC リーフ スイッチ ペアの削除（Delete vPC Leaf Switch Pair）]**、**[すべてダウンロード（Download All）]**、または **[オブジェクト ストア ブラウザで開く（Open in Object Store Browser）]** を選択します。

[保存する（Save）] をクリックし、初期セットアップ ウィザードの次のウィンドウに進みます。

BGP

BGP ウィンドウを使用して、ACI ファブリックのルート リフレクタを設定し、マルチプロトコル BGP（MP-BGP）を使用してファブリック内に外部ルートを配布します。ACI ファブリックのルート リフレクタを有効にすると、外部ネットワークへの接続を設定できます。

（注） ルートリフレクタとして設定するスパインスイッチを選択します。初回セットアップウィザードを進めるには、少なくとも1つのルートリフレクタを設定する必要があります。このウィンドウのテーブルにスパインスイッチが表示されない場合は、スイッチが正しいタイプで登録されているか、APIC によって検出されていることを確認します。

[BGP] ウィンドウで、ルート リフレクタとして使用するスパイン スイッチの横にあるボックスをオンにし、**[自律システム番号（Autonomous System Number）]** フィールドにこのスパイン スイッチの ASN を入力します。**[保存して続行（Save and Continue）]** をクリックし、初期セットアップ ウィザードの次のウィンドウに進みます。

DNS

DNS ウィンドウを使用して、リーフ スイッチ、スパイン スイッチ、および APIC ノードが DNS 名を照会できるように DNS サーバと検索ドメインを設定します。OOB 接続は DNS 通信に使用されます。

（注） 初回セットアップ ウィザードは、**デフォルト**の DNS ポリシーで DNS サーバと DNS ドメインを設定します。

DNS サーバを設定するには、[DNS サーバ（DNS Servers）] 領域で **[+]** をクリックし、次の情報を入力します。

- **アドレス**：プロバイダ アドレスを入力します。
- **希望**：優先するプロバイダとしてこのアドレスが必要な場合は、チェックボックスをオンにします。
- **ステータス**：設定要求のステータスを提供します。

[更新（Update）] をクリックし、必要に応じてこのプロセスを繰り返して追加の DNS サーバを設定します。

検索ドメインを設定するには、[ドメインの検索（Search Domains）] 領域で **[+]** をクリックし、次の情報を入力します。

- **名前**：ドメイン名（cisco.com）を入力します。
- **デフォルト**：チェックボックスをオンにして、このドメインをデフォルトドメインにします。デフォルトとして指定できるドメイン名は 1 つだけです。
- **ステータス**：設定要求のステータスを提供します。

[更新（Update）] をクリックし、必要に応じてこのプロセスを繰り返して追加の検索ドメインを設定します。

[DNS サーバ（DNS Servers）] テーブルまたは [ドメインの検索（Search Domains）] テーブルからエントリを削除するには、削除するエントリを選択し、そのテーブルのゴミ箱アイコンをクリックします。

[保存して続行（Save and Continue）] をクリックし、初期セットアップ ウィザードの次のウィンドウに進みます。

NTP

NTP ウィンドウを使用してタイムゾーンを設定し、リーフ スイッチ、スパイン スイッチ、および APIC ノードを有効な時刻源に同期するように NTP サーバを割り当てます。OOB 接続は NTP 通信に使用されます。

（注） 初期セットアップ ウィザードは、**デフォルト**の NTP ポリシーでサーバを設定します。

[表示形式（Display Format）] 領域で、**[local]** をクリックして日付と時刻をローカル タイムゾーン形式で表示するか、**[utc]** をクリックして日付と時刻を UTC タイムゾーン形式で表示します。デフォルトは **[local]** です。

上記で **[local]** を選択した場合は、[タイムゾーン（Time Zone）] 領域で、ドロップダウン矢印をクリックしてドメインのタイムゾーンを選択します。ドロップダウン メニュー領域に入力して、ドロップダウン オプションをフィルタリングすることもできます。デフォルトは **[協定世界時（Coordinated Universal Time）]** です。

NTP サーバを設定するには、[NTP サーバ（NTP Servers）] 領域で **[+]** をクリックし、次の情報を入力します。

- **ホスト名/IPAddress**：NTP サーバのホスト名と IP アドレスを入力します。
- **希望**：複数のプロバイダーを作成する場合は、最も信頼できる NTP 時刻源の **[希望（Preferred）]** チェックボックスをオンにします。
- **ステータス**：設定要求のステータスを提供します。

[更新（Update）] をクリックし、必要に応じてこのプロセスを繰り返して追加の NTP サーバを設定します。

NTP サーバ テーブルからエントリを削除するには、削除するエントリを選択し、そのテーブルのゴミ箱アイコンをクリックします。

[保存して続行（Save and Continue）] をクリックし、初期セットアップ ウィザードの次のウィンドウに進みます。

プロキシ

[プロキシ（Proxy）] ウィンドウを使用して、HTTP または HTTPS プロキシ ポリシーを構成します。設定すると、一部の Cisco Cloud Application Policy Infrastructure Controller（APIC）機能、

主に Cisco Intersight 接続などのインターネット アクセスを必要とする機能が、HTTP または HTTPS プロキシを介してトラフィックを送信します。詳細については、*Cisco APIC* システム管理設定ガイドを参照してください。

グローバル設定

[グローバル設定（Global Configurations）] ウィンドウを使用して、特定のエリアを設定します。これは、Cisco Application Centric Infrastructure（ACI）ファブリックの初回セットアップ中のベスト プラクティスとして推奨されます。**[OK]** をクリックします。次の領域を設定する準備ができたら、

- サブネット チェック （7 ページ）
- ドメイン検証 （8 ページ）
- 再配布されたルートの中間システムから中間システム （8 ページ）
- IP エージングの管理状態 （8 ページ）
- 不正なエンドポイントの制御 （8 ページ）
- COOP グループポリシー （9 ページ）

（注） このウィンドウの一部の設定は、[Fabric Wide Setting Policy]ページ（[System] [System Settings] [Fabric-Wide Settings]）で設定できる[Subnet Check]および[Domain Validation]の設定など、初回セットアップ後に設定できます。>>ただし、初回セットアップ後にこれらの設定を行うと、他の既存の設定で問題が発生する可能性があります。たとえば、**[ファブリック全体の設定ポリシー（Fabric Wide Setting Policy）]** ページで **[サブネット チェックの適用（Enforce Subnet Check）]** および **[ドメイン検証の適用（Enforce Domain Validation）]** の設定を有効にすると、インターフェイスまたはEPGにスタティックに割り当てられたポートに適切なポリシーチェーンがない場合、設定済みの L3Out 接続が切断される可能性があります。

サブネット チェック

この機能では、ある VRF で設定されたサブネットの外、つまり他のすべての VRF では、IP アドレス学習が無効になります。

この機能は、Cisco ACI () が IP アドレスをデータ プレーンからエンドポイントとして学習した場合、VRF インスタンス レベルでサブネットのチェックを適用します。このオプションをオンにすると、ファブリックは、ブリッジ ドメインで構成されたもの以外のサブネットからの IPアドレスを学習しなくなります。この機能は、このようなシナリオで、ファブリックがエンドポイント情報を学習しないようにします。

[適用（Enforce）] の横にあるチェックボックスをオンにして、サブネット チェック機能を有効にします。

ドメイン検証

この機能は、スタティック パスが追加されているが、ドメインが EPG に関連付けられていない場合に検証チェックを実行します。

有効な場合、スタティック パスが EPG に追加されているときに検証チェックが実行され、パスが EPG に関連付けられているドメインの一部であるか判断します。このポリシーの適用範囲は、ファブリック全体です。を設定した後、ポリシーは起動に各リーフ スイッチにプッシュされます。

[適用（Enforce）] の横のチェックボックスをオンにして、ドメイン検証機能を有効にします。これは強く推奨されています。

再配布されたルートの中間システムから中間システム

これは、IS-IS にすべてインポートされたルートに使用されている IS-IS メトリックです。このオプションで 64（最大）未満のメトリック（63 など）を設定すると、Cisco ACI では新しいスパインでルーティング コンバージェンスが達成されるまで、スイッチは安定したスパインからのルートを優先できます。

[IS-IS メトリック（IS-IS metric）] フィールドに適切な値を入力します。

IP エージングの管理状態

このポリシーを有効にすると、Cisco ACI では各 IP アドレスを個別に追跡し、未使用のアドレスを効率的にエージング アウトできます。それ以外の場合、未使用の IP アドレスは、ベース MAC アドレスが期限切れになるまで学習されたままになります。これはリモート エンドポイントには影響しません。

有効な場合、IP エージング ポリシーは、エンドポイント上の未使用の Ip アドレスをエージングします。この状況では、IP エージング ポリシーは、エンドポイントの IP アドレスを追跡する ARP 要求 (IPv4) とネイバー要請（IPv6）を送信します。応答が指定されていない場合、ポリシーは未使用の IPs アドレスをエージングします。

このフィールドのオプションは次のとおりです。

- **無効**：**デフォルト設定。 Cisco APICでは、IP エージング ポリシーを無視します。**
- **有効**：Cisco APIC は IP エージング ポリシーを監視します。

この機能を有効にすることを強くお勧めします。

不正なエンドポイントの制御

不正なエンドポイントは、リーフ スイッチを頻繁に攻撃し、異なるリーフ スイッチ ポートにパケットを繰り返し挿入し、802.1Q タグを変更し（エンドポイントの移動をエミュレート）、その結果、IP アドレスと MAC アドレスが異なる EPG とポートで迅速に学習されます。誤設定により頻繁に IP アドレスと MAC アドレスが変更 (移動する) されることになります。

不正エンドポイント制御機能は、この脆弱性に対処します。このポリシーを有効にすると、Cisco ACI で不正なエンドポイントを検出して削除できます。

このフィールドのオプションは次のとおりです。

- **無効**：デフォルト設定。Cisco APIC は、不正なエンドポイント制御ポリシーを無視します。
- **有効**：Cisco APIC は、不正エンドポイント制御ポリシーを監視します。

この機能を有効にすることを強くお勧めします。

[不正 EP 検出間隔（Rogue EP Detection Interval）]、**[不正 EP 検出倍数係数（Rogue EP Detection Multiplication Factor）]**、**[保持間隔（Hold Interval）]** などの不正エンドポイント制御の追加設定は、**[エンドポイント制御（Endpoint Controls）]** パネルから使用できます。**[エンドポイント制御（Endpoint Controls）]** パネルにアクセスするには、メニューバーで **[システム（System）]** > **[システム設定（System Settings）]** > **[エンドポイント制御（Endpoint Controls）]** をクリックし、**[不正 EP 制御（Rogue EP Control）]** タブをクリックします。

次に、**[エンドポイント制御（Endpoint Controls）]** ウィンドウの **[不正 EP 制御（Rogue EP Control）]** タブのフィールドの有効なデフォルト設定を示します。

- **不正 EP 検出間隔**：有効な値は 0 ー 65535 秒です。デフォルト値は 60 です。
- **不正 EP 検出倍数係数**：有効な値は 2 ー 65535 です。デフォルト値は4です。
- **保持時間**：5.2(1) および 5.2(2) リリースでは、有効な値は 1800 ー 3600 秒です。5.2(3) リリース以降、有効な値は 300 ー 3600 秒です。デフォルト値は 1800 です。

COOP グループポリシー

マッピング情報（ロケーションおよび ID）をスパイン プロキシに伝達するために、Council of Oracles Protocol（COOP）を使用します。リーフ スイッチは、Zero Message Queue（ZMQ）を使用して、エンドポイントアドレス情報をスパイン スイッチ「Oracle」に転送します。スパイン ノードで実行している COOP によって、すべてのスパイン ノードがエンドポイントの一貫したコピーと、マッピング データベースの場所情報を保持していることを確認します。

COOP プロトコルは、次の 2 つの ZMQ 認証モードをサポートします。

- **互換性タイプ**：デフォルト設定。COOP は、メッセージ転送のために MD5 認証および非認証 ZMQ 接続の両方を受け入れます。

（注） Cisco APIC は、COOP の MD5 パスワードとして使用されるトークンを管理します。このトークンは、Cisco APIC 1 時間ごとに自動的にローテーションされます。このトークンは表示できません。

- **厳密タイプ**：COOP は MD5 認証 ZMQ 接続のみを許可します。

COOP グループ ポリシーの **[厳密タイプ（Strict Type）]** 設定を強く推奨します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。