ファブリック プロビジョニング

この章の内容は、次のとおりです。

ファブリック プロビジョニング

Ciscoアプリケーションセントリック インフラストラクチャ（ACI）の自動化とセルフプロビジョニングにより、従来のスイッチング インフラストラクチャに勝るこれらの操作上のメリットがもたらされます。

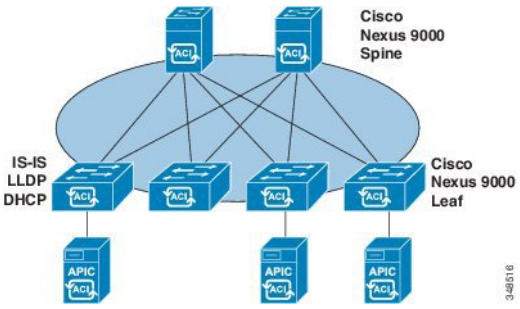
- クラスタ化され論理的に一元化されたが物理的に分散されている APIC では、ファブリック全体にポリシー、ブートストラップおよびイメージ管理が提供されます。

- APIC 起動トポロジの自動検出、自動設定、およびインフラストラクチャ アドレッシングでは、次の業界標準のプロトコルが使用されます。Intermediate System-to-Intermediate System（IS-IS）、リンク層検出プロトコル（LLDP）、ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）。
- APIC では、シンプルで自動化されたポリシーベースのプロビジョニングとアップグレードのプロセス、および自動イメージ管理が提供されます。
- APIC では、スケーラブルな設定管理が提供されます。 ACI のデータセンターは非常に規模が大きい場合があるため、スイッチまたはインターフェイスを個別に設定すると、スクリプトを使用しても十分に拡張しません。 APIC ポッド、コントローラ、スイッチ、モジュール、およびインターフェイス セレクタ（すべて、範囲、特定のインスタンス）により、ファブリック全体の対称設定が可能になります。 対称設定を適用するには、管理者がインターフェイス コンフィギュレーションを単一のポリシー グループに関連付けるスイッチ プロファイルを定義します。

スタートアップ検出と設定

クラスタ化された APIC コントローラでは、ファブリックに DHCP、ブートストラップ コンフィギュレーションおよびイメージ管理が提供され、自動化された起動およびアップグレードが可能になります。 次の図は、スタートアップ検出を示します。

図 *1*：スタートアップ検出の設定



Cisco Nexus ACI ファブリック ソフトウェアは ISO イメージとしてバンドルされ、管理コンソールを通じて Cisco APIC サーバにインストールできます。 Cisco Nexus ACI Software ISO には、Cisco APIC イメージ、リーフ ノードのファームウェア イメージ、スパイン ノードのファームウェア イメージ、デフォルトのファブリック インフラストラクチャ ポリシーおよび操作に必要なプロトコルが含まれます。

ACI ファブリックのブートストラップ シーケンスは、すべてのスイッチで出荷時にインストールされたイメージによってファブリックが起動されると開始されます。 ACI ファームウェアと APIC を実行する Cisco Nexus 9000 シリーズ スイッチは、ブート プロセスに予約済みのオーバーレイを使用します。 このインフラストラクチャ スペースはスイッチ上でハードコードされています。 APIC はデフォルトのオーバーレイを通じてリーフに接続できます。または、ローカルで有効な ID を使うことができます。

ACI ファブリックはインフラストラクチャ スペースを使用します。インフラストラクチャ スペースはファブリック内でセキュアに隔離され、ここですべてのトポロジディスカバリ、ファブリック管理、インフラストラクチャアドレッシングが行われます。 ファブリック内の ACI ファブリック管理コミュニケーションは、内部のプライベート IP アドレスを通じてインフラストラクチャ スペース内で行われます。 このアドレッシング方式によって、APIC はクラスタ内のファブリック ノードおよび他の Cisco APIC コントローラとの通信を行えます。 APIC は、Link Layer Discovery Protocol（LLDP）ベースの検出プロセスを使用してクラスタ内の他の Cisco APIC コントローラの IP アドレスとノード情報を検出します。

次に、APIC クラスタ検出プロセスについて説明します。

- Cisco ACI の各 APIC は、内部のプライベート IP アドレスを使用してクラスタ内の ACI ノードおよび他の APIC と通信します。 APIC は、LLDP ベースの検出プロセスを通じてクラスタ内の他の APIC コントローラの IP アドレスを検出します。
- APIC は、APIC ID から APIC IP アドレスと APIC の Universally Unique Identifier（UUID）にマッピングを提供するアプライアンス ベクトル（AV）を維持します。 最初に、各 APIC がローカルの IP アドレスで満たされた AV から開始し、他のすべての APIC スロットが不明としてマークされます。
- スイッチの再起動後、リーフのポリシー要素（PE）が APIC からその AV を取得します。 スイッチはその後、この AV をすべてのネイバーにアドバタイズし、ローカル AV とネイバーの AV 間の不一致をローカル AV のすべての APIC にレポートします。

このプロセスを使用して、APIC はスイッチを介して ACI の他の APIC コントローラについて学習します。 クラスタ内のこれらの新しく検出された APIC コントローラを検証した後、APIC コントローラはローカル AV を更新して、スイッチを新しい AV でプログラミングします。 その後、スイッチはこの新しい AV のアドバタイズを開始します。 このプロセスは、すべてのスイッチが同一の AV を持ち、すべての APIC コントローラが他のすべての APIC コントローラの IP アドレスを認識するまで継続します。

ACI ファブリックは、APIC に直接接続しているリーフ ノードから順にカスケード式に起動されます。 LLDP およびコントロール プレーン IS-IS コンバージェンスは、このブート プロセスと並行して行われます。 ACI ファブリックは LLDP および DHCP ベースのファブリック検出機能を使用して、ファブリック スイッチ ノードの検出、インフラストラクチャの VXLAN トンネル エンドポイント（VTEP）アドレスの割り当て、スイッチへのファームウェアのインストールを自動的に行います。 この自動プロセスの前に、Cisco APIC コントローラ上で最小限のブートストラップ設定を行う必要があります。

クラスタ管理のガイドライン

APIC クラスタは複数の APIC コントローラで構成され、ACI ファブリックに対する統合されたリアルタイムモニタリング、診断および構成管理機能がオペレータに提供されます。最適なシステム パフォーマンスを確保するには、次のガイドラインに従って APIC クラスタに変更を加えてください。

（注） クラスタへの変更を開始する前に、必ずその状態を確認してください。 クラスタに対して計画した変更を実行するときは、クラスタ内のすべてのコントローラが正常である必要があります。 クラスタ内の 1 つ以上の APIC コントローラが正常でない場合は、先に進む前にその状況を修復してください。 APIC クラスタの健全性の問題の解決に関する詳細については、『*Cisco APIC Troubleshooting Guide*』を参照してください。

クラスタを管理する場合、次の一般的ガイドラインに従ってください。

- 現在はクラスタ内にない APIC からのクラスタ情報は無視してください。その情報からは正確なクラスタ情報は提供されません。
- クラスタ スロットには、APIC シャーシ ID が含まれます。 スロットを設定すると、割り当てられたシャーシ ID の APIC を解放するまでそのスロットは使用できません。
- APIC ファームウェア アップグレードが進行中の場合は、それが完了し、クラスタが十分に適合するまで待機してからクラスタに他の変更を加えます。

APIC クラスタ サイズの拡大

APIC クラスタ サイズを拡大するには、次のガイドラインに従ってください。

- クラスタの拡大がファブリックのワークロードの要求に影響しないときに、クラスタの拡大を予定します。
- ハードウェア インストレーション ガイドの手順に従って、新しい APIC コントローラを準備します。 PING テストでインバンド接続を確認します。
- クラスタの目標サイズを既存のクラスタ サイズ コントローラ数に新規コントローラ数を加えた数になるように増やします。 たとえば、既存のクラスタ サイズ コントローラの数が 3 で、3 台のコントローラを追加する場合は、新しいクラスタの目標サイズを 6 に設定します。すべての新しいコントローラがクラスタに含まれるまで、クラスタはそのサイズを一度に 1 台のコントローラずつ順を追って増やしていきます。

  （注） 既存の APIC コントローラが利用できなくなった場合、クラスタの拡張は停止します。 クラスタの拡大を進める前に、この問題を解決します。

- 各アプライアンスの追加時に APIC が同期しなければならないデータ量に応じて、拡張の完了に必要な時間はアプライアンスごとに 10 分を超える場合があります。 クラスタが正常に拡大すると、APIC の運用サイズと目標サイズが同じになります。

  （注） APIC がクラスタの拡大を完了するまでは、クラスタに追加の変更をしないようにします。

クラスタでの APIC コントローラの交換

APIC コントローラを交換するには、次のガイドラインに従ってください。

- 交換する APIC コントローラの ID 番号をメモします。
- 交換する APIC コントローラを解放します。

（注） 交換を行う前に APIC コントローラを解放しないと、クラスタが交換コントローラを吸収できなくなります。

- ハードウェア インストレーション ガイドの手順に従って交換 APIC コントローラを段階分けします。 PING テストでインバンド接続を確認します。
- 交換コントローラを APIC クラスタに追加する場合、以前使用した APIC コントローラの ID 番号を交換 APIC コントローラに割り当てます。 APIC は、交換コントローラをクラスタと同期します。

（注） 既存の APIC コントローラが使用できなくなると、クラスタの同期が停止します。 クラスタの同期を進める前に、この問題を解決します。

- コントローラの交換時に APIC が同期しなければならないデータ量に応じて、交換の完了に必要な時間は交換コントローラごとに 10 分を超える場合があります。 交換コントローラとクラスタとの同期が成功すると、APIC の操作サイズとターゲット サイズは変化がありません。

（注） クラスタに追加の変更を加える前に、APIC がクラスタの同期を完了することを許可します。

- ファブリックのワークロードの要求がクラスタの同期に影響されないときに、APIC コントローラの交換をスケジューリングします。
- UUID とファブリックのドメイン名は、再起動後に APIC コントローラに保持されます。 ただし、工場出荷時状態に戻す再起動ではこの情報は削除されます。 APIC コントローラをファブリックから別のファブリックに移動する場合、そのようなコントローラを別の ACI ファブリックに追加する前に、工場出荷時状態に戻す再起動を実行する必要があります。

APIC クラスタのサイズ縮小

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

（注） 縮小したクラスタから APIC コントローラを解放し、電源オフする正しい手順を実行しないと、予期しない結果を招く可能性があります。 認識されていない APIC コントローラをファブリックに接続されたままにしないでください。

- クラスタ サイズを小さくすると、残りの APIC コントローラの負荷が増大します。 クラスタの同期がファブリックのワークロードの要求に影響しないときに、APIC コントローラ サイズの縮小を予定します。
- クラスタの目標サイズを新たな低い値に減らします。 たとえば、既存のクラスタ サイズが 6 で、3 台のコントローラを削除する場合は、クラスタの目標サイズを 3 に減らします。
- 既存のクラスタ内でコントローラ ID の番号が最大のものから、APIC コントローラを 1 台ずつ、解放、電源オフ、接続解除し、クラスタが新規の小さい目標サイズになるまで行います。

  各コントローラを解放および削除するごとに、APIC はクラスタを同期します。
- 既存の APIC コントローラが使用できなくなると、クラスタの同期が停止します。 クラスタの同期を進める前に、この問題を解決します。
- コントローラの削除の際に APIC が同期すべきデータの量により、各コントローラの解放とクラスタの同期を完了するために要する時間は、コントローラごとに 10 分以上になる可能性があります。

（注） クラスタに追加の変更を行う前に、必要な解放手順全体を完了し、APIC がクラスタの同期を完了できるようにしてください。

ファブリック インベントリ

ポリシー モデルには、すべてのノードおよびインターフェイスを含むファブリックの完全なリアルタイムインベントリが含まれます。 このインベントリ機能により、プロビジョニング、トラブルシューティング、監査、およびモニタリングを自動化できます。

Cisco ACI のファブリック スイッチの場合は、ファブリック メンバーシップのノード インベントリに、ノード ID、シリアル番号および名前を識別するポリシーが含まれます。 サードパーティのノードは、管理対象外のファブリック ノードとして記録されます。 Cisco ACI のスイッチは自動的に検出することができ、またはポリシー情報をインポートできます。 ポリシー モデルは、ファブリック メンバー ノードのステータス情報も保持します。

ノードのステータス	状態
Unknown	ポリシーが存在しません。 すべてのノードにはポリシーが必要で、ポリシーがない場合はメンバ ノードのステータスは不明となります。

ノードのステータス	状態
Discovering	ノードが検出されていることを示す一時状態。
Undiscovered	ノードにはポリシーがありますが、ファブリックで提示されたことはありません。
Unsupported	ノードは Cisco のスイッチですが、サポートされていません。 たとえば、ファームウェアのバージョンが ACI のファブリックと互換性がありません。
Decommissioned	ノードはポリシーとして検出されましたが、ユーザがこれを無効にしました。ノードを再びイネーブルにすることができます。
Inactive	ノードが到達不能です。 検出されましたが、現在アクセスできません。 たとえば、電源がオフになっているか、ケーブルが切断されている可能性があります。
Active	ノードはファブリックのアクティブ メンバです。

無効のインターフェイスは、管理者によってブラックリスト化されたものや、APICが異常を検出するため取り除かれたものである可能性があります。 リンク ステート異常の例を次に示します。

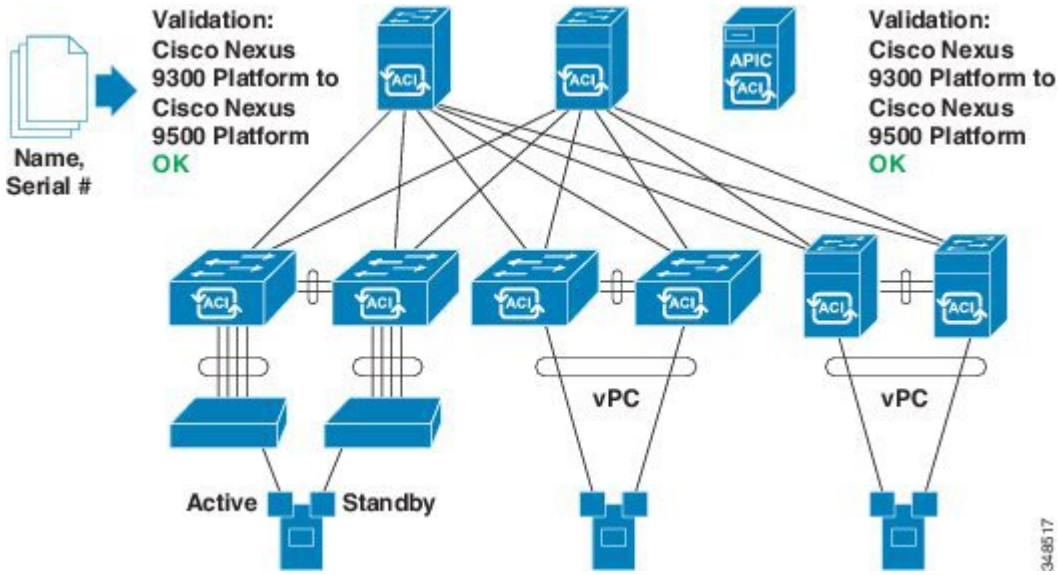
- スパインに接続されているスパイン、リーフに接続されているリーフ、リーフアクセス ポートに接続されているスパイン、非ACIノードに接続されているスパイン、または非ACIデバイスに接続されているリーフ ファブリック ポートなどの配線の不一致。
- ファブリック名の不一致。 ファブリック名は各 ACI ノードに保存されます。 工場出荷時のデフォルト状態に戻されることなくノードが別のファブリックに移動される場合、ファブリック名が保持されます。
- UUID の不一致によって APIC がノードをディセーブルにします。

（注） 管理者がAPICを使用してスパインのすべてのリーフ ノードをディセーブルにすると、スパインへのアクセスを回復するためにスパインの再起動が必要です。

プロビジョニング

APIC プロビジョニング方式により、適切な接続を通じて ACI ファブリックが自動的に起動します。 次の図は、ファブリックのプロビジョニングを示します。

図 *2*：ファブリック プロビジョニング



Link Layer Discovery Protocol（LLDP）ディスカバリが隣接するすべての接続を動的に学習した後、これらの接続は緩やかなルールに照らし合わせて検証できます。たとえば、「LEAF can connect to only SPINE-L1-*」または「SPINE-L1-* can connect to SPINE-L2-* or LEAF」などと指定できます。ルールに一致しないものが見つかった場合は、エラーが発生して接続がブロックされます。 また、接続に注意が必要であることを示すアラームが作成されます。 Cisco ACI ファブリックの管理者は、テキスト ファイルからすべてのファブリック ノードの名前とシリアル番号を APIC にインポートすることができ、または APIC GUI、コマンドライン インターフェイス（CLI）または API を使用してシリアル番号を自動的に検出し、名前をノードに割り当てることをファブリックに許可できます。

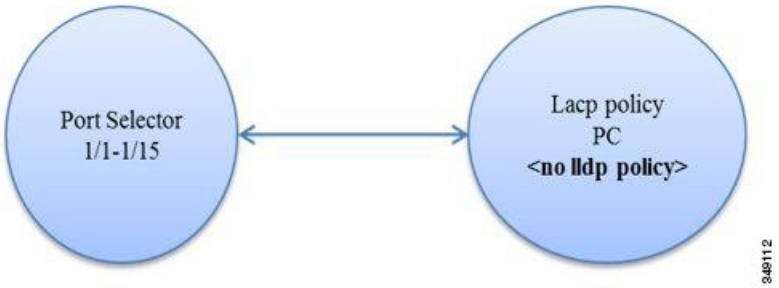
デフォルト ポリシー

APICデフォルト ポリシー値の初期値は、スイッチにロードされる具象モデルから取得されます。ファブリックの管理者は、デフォルト ポリシーを変更できます。 デフォルト ポリシーは、次の複数の目的に使用されます。

1 ファブリックの管理者がモデル内のデフォルト値を上書きできます。

2 管理者が明示ポリシーを提供しない場合、APIC はデフォルトのポリシーを適用します。 管理者はデフォルトのポリシーを作成でき、管理者が明示ポリシーを提供しない限り、APIC はそのポリシーを使用します。

図 *3*：デフォルト ポリシー



たとえば、管理者が行うアクションまたは行わないアクションに応じて、APIC は次を実行します。

- 管理者が選択したポートに対して LLDP ポリシーを指定しないため、APIC はポート セレクタに指定されたポートに対しデフォルトの LLDP インターフェイス ポリシーを適用します。
- 管理者がポート セレクタからポートを削除すると、APIC はそのポートにデフォルト ポリシーを適用します。 この例では、管理者がポート 1/15 をポート セレクタから削除すると、そのポートはポート チャネルの一部ではなくなり、APIC はそのポートにすべてのデフォルト ポリシーを適用します。

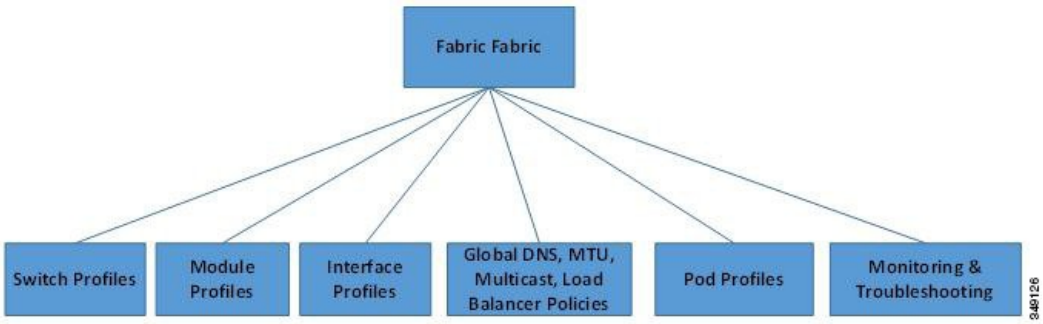
ACI ファブリックをアップグレードした場合、デフォルト値が新しいリリースで変更されても既存のポリシーのデフォルト値が保持されます。 ノードが APIC に初めて接続されると、ノードはそれ自体をすべてのデフォルト ポリシーをノードにプッシュする APIC に登録します。 デフォルト ポリシーでのすべての変更がノードにプッシュされます。

ファブリック ポリシーの概要

ファブリック ポリシーは、内部のファブリック インターフェイスの操作を管理し、スパインおよびリーフ スイッチを接続するさまざまな機能、プロトコル、およびインターフェイスの設定を可能にします。ファブリックの管理者権限を持つ管理者は、要件に応じて新しいファブリック ポリシーを作成できます。 APIC では、管理者はファブリック ポリシーを適用するポッド、スイッチ

およびインターフェイスを選択できます。次の図は、ファブリックのポリシーモデルの概要を示します。

図 *4*: ファブリック ポリシーの概要



ファブリック ポリシーは、次のカテゴリにグループ化されます。

- スイッチ プロファイルは、設定するスイッチとスイッチの設定ポリシーを指定します。
- モジュール プロファイルは、設定するスパイン スイッチ モジュールとスパイン スイッチの設定ポリシーを指定します。
- インターフェイス プロファイルは、設定するファブリック インターフェイスとインターフェイスの設定ポリシーを指定します。
- グローバル ポリシーは、DNS、ファブリック MTU のデフォルト、マルチキャスト ツリー、およびファブリック全体で使用するロード バランサの設定を指定します。
- ポッド プロファイルは、日時、SNMP、協調キー サーバ（COOP）、IS-IS、およびボーダー ゲートウェイ プロトコル（BGP）のルート リフレクタ ポリシーを指定します。
- モニタリングおよびトラブルシューティングのポリシーは、モニタする対象、しきい値、障害とログの処理方法、および診断方法を指定します。

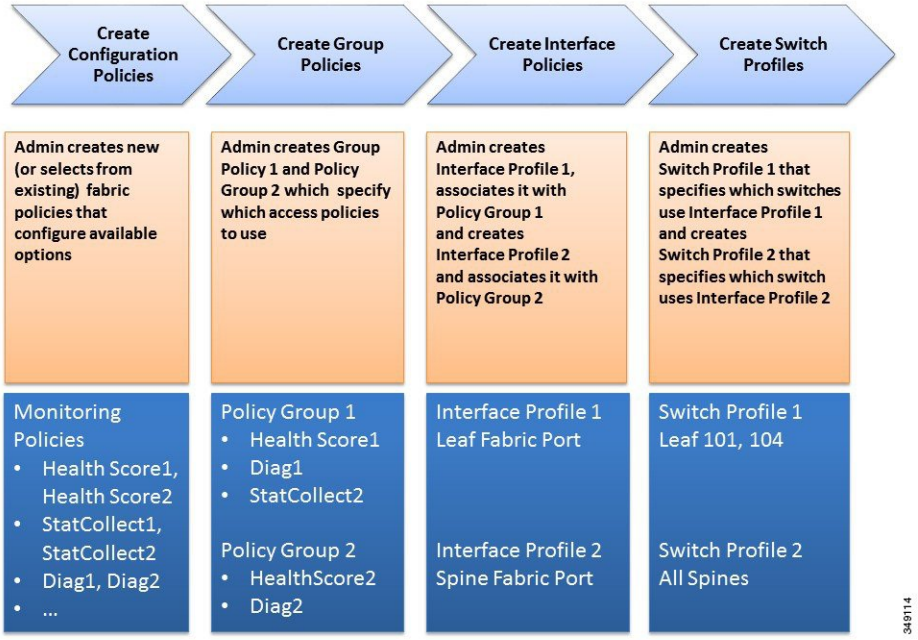
ファブリック ポリシーの設定

ファブリック ポリシーは、スパインおよびリーフ スイッチに接続するインターフェイスを設定します。ファブリック ポリシーは、モニタリング（統計情報収集および統計情報のエクスポート）、トラブルシューティング（オンデマンド診断と SPAN）、IS-IS、協調キー サーバ（COOP）、SNMP、ボーダー ゲートウェイ プロトコル（BGP）のルート リフレクタ、DNS、またはネットワーク タイム プロトコル（NTP）などの機能をイネーブルにできます。

ファブリック全体で設定を適用するには、管理者がポリシーの定義済みグループをスイッチ上のインターフェイスに単一段階で関連付けます。 このようにして、ファブリック上の多数のインターフェイスを一度に設定できます。1 個のポートを一度に設定することはスケーラブルではあ

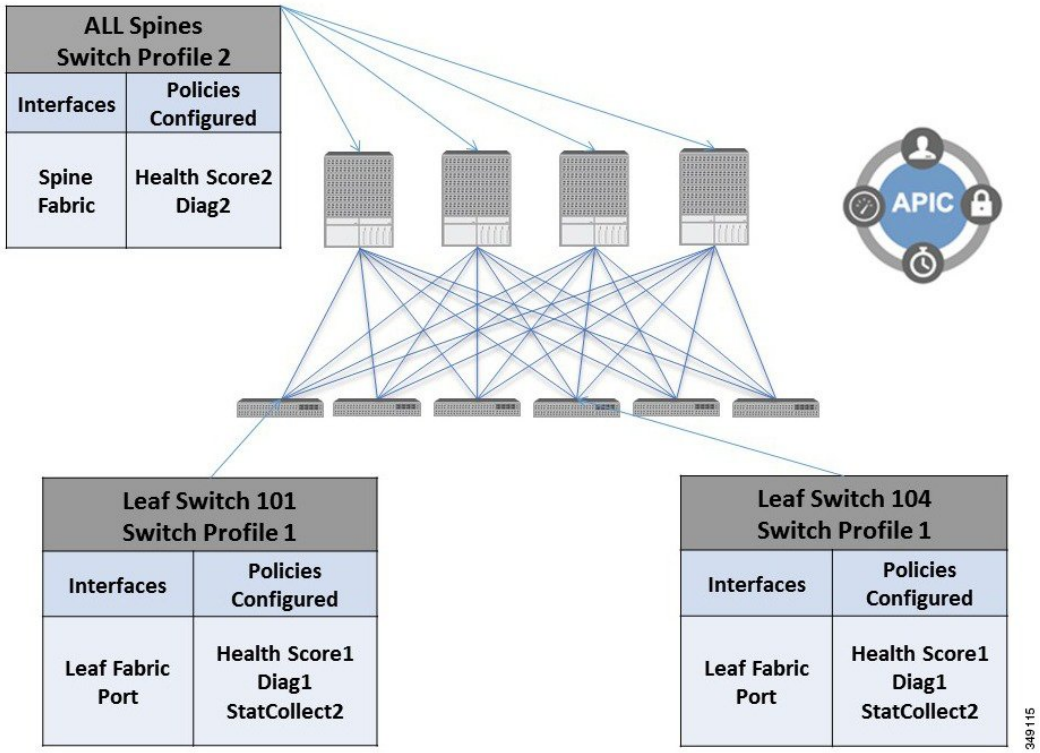
りません。 次の図は、ACI ファブリックを設定するプロセスがどのように動作するかを示します。

図 *5*：ファブリック ポリシーの設定プロセス



次の図は、ACI ファブリックにスイッチ プロファイル 1 およびスイッチ プロファイル 2 を適用した結果を示します。

図 *6* : ファブリック スイッチ ポリシーのアプリケーション



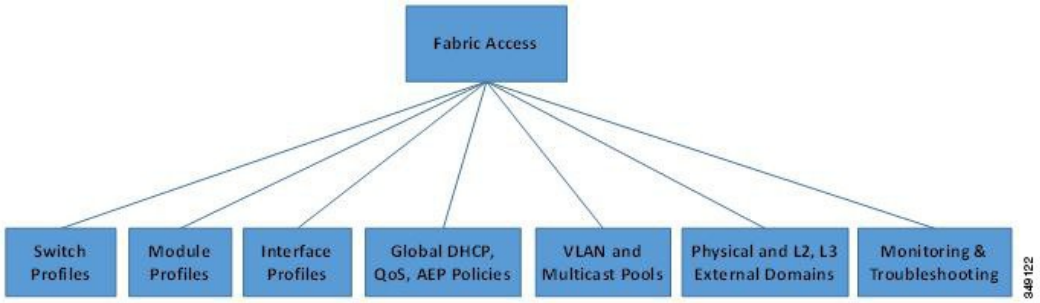
インフラストラクチャと範囲を組み合わせることにより、管理者はスケーラブルな方法でファブリック構成を管理することができます。 これらの設定は、REST API、CLI、または GUI を使用して実行できます。 GUI 内の [Quick Start Fabric Interface Configuration] ウィザードでは、そのようなポリシーの実行に必要な基盤となるオブジェクトが自動的に作成されます。

アクセス ポリシーの概要

アクセスポリシーは、仮想マシンコントローラおよびハイパーバイザなどのデバイスに接続する外向きインターフェイス、ホスト、ネットワーク接続ストレージ、ルータ、またはファブリックエクステンダ（FEX）インターフェイスを設定します。アクセスポリシーにより、ポートチャネルおよび仮想ポート チャネル、Link Layer Discovery Protocol（LLDP）、Cisco Discovery Protocol（CDP）、または Link Aggregation Control Protocol（LACP）などのプロトコル、および統計情報

収集、監視、および診断などの機能の設定が可能になります。 次の図は、アクセス ポリシー モデルの概要を示します。

図 7: アクセス ポリシー モデルの概要



アクセス ポリシーは、次のカテゴリにグループ化されます。

- スイッチ プロファイルは、設定するスイッチとスイッチの設定ポリシーを指定します。
- モジュール プロファイルは、設定するリーフ スイッチのアクセス カードおよびアクセス モジュールとリーフ スイッチの設定ポリシーを指定します。
- インターフェイス プロファイルは、設定するアクセス インターフェイスとインターフェイスの設定ポリシーを指定します。
- グローバル ポリシーにより、ファブリック全体に使用できる DHCP、QoS、および接続可能アクセスエンティティ（AEP）のプロファイル機能の設定が可能になります。 AEP プロファイルは、リーフ ポートの大規模セットでハイパーバイザ ポリシーを展開するためのテンプレートを提供し、仮想マシン管理（VMM）のドメインと物理ネットワーク インフラストラクチャを関連付けます。 また、レイヤ 2 およびレイヤ 3 の外部ネットワークの接続にも必要となります。
- プールは、VLAN、VXLAN およびマルチキャスト アドレス プールを指定します。 プールは、VMM などの複数のドメインおよびレイヤ 4 ～ レイヤ 7 のサービスで消費できる共有リソースです。 プールは、トラフィックのカプセル化 ID の範囲を表します（たとえば、VLAN ID、VNID、マルチキャスト アドレスなど）。
- 物理および外部ドメイン ポリシーには、次のものが含まれます。
  - 外部ブリッジド ドメインのレイヤ 2 ドメイン プロファイルには、ファブリックに接続されたブリッジド レイヤ 2 ネットワークが使用するポートおよび VLAN の仕様が含まれます。
  - 外部ルーテッド ドメインのレイヤ 3 ドメイン プロファイルには、ファブリックに接続されたルーテッド レイヤ 3 ネットワークが使用するポートおよび VLAN の仕様が含まれます。
  - 物理ドメイン ポリシーには、テナントまたはエンドポイント グループで使用されるポートや VLAN などの物理インフラストラクチャの仕様が含まれます。

- モニタリングおよびトラブルシューティングのポリシーは、モニタする対象、しきい値、障害とログの処理方法、および診断方法を指定します。

アクセス ポリシーの設定

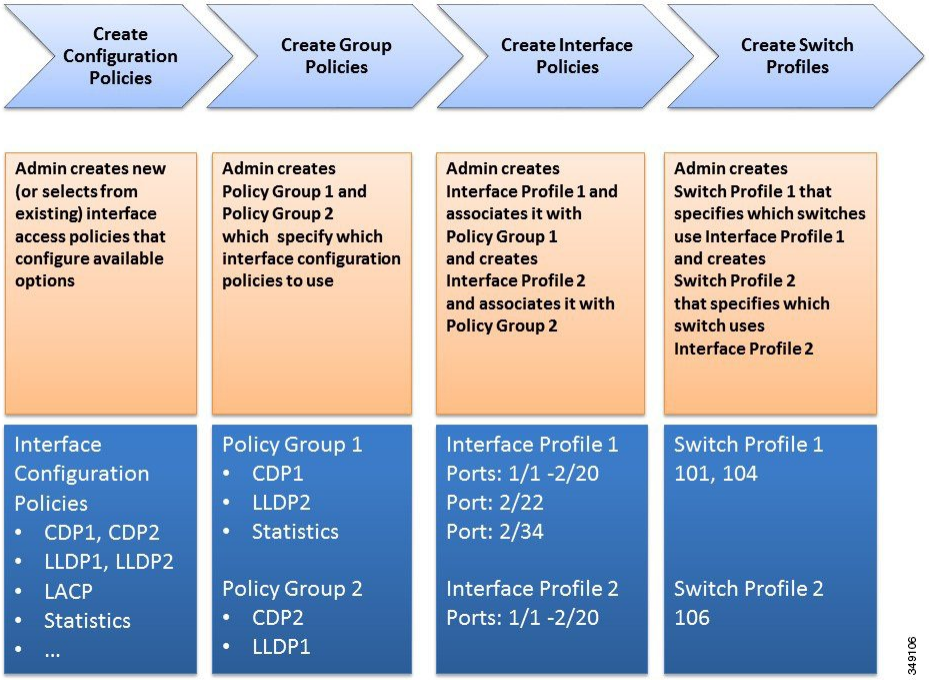
アクセス ポリシーは、スパイン スイッチに接続していない外向きインターフェイスを設定します。 外向きインターフェイスは、仮想マシン コントローラなどの外部デバイス、ハイパーバイザ、ホスト、ルータ、またはファブリック エクステンダ（FEX）と接続します。 アクセス ポリシーにより、管理者はポート チャネルおよび仮想ポート チャネル、LLDP、CDP、LACP などのプロトコル、モニタリングや診断などの機能を設定することができます。 スイッチインターフェイス、ポートチャネル、仮想ポートチャネル、およびインターフェイス速度の変更に関するサンプルの XML ポリシーを付録 C「アクセス ポリシーの例」に示します。

（注） テナント ネットワーク ポリシーがファブリックのアクセス ポリシーと別に設定される一方で、テナント ポリシーが依存する基盤となるアクセス ポリシーが整わないとテナント ポリシーはアクティブ化されません。

潜在的に多数のスイッチ間で設定を適用するためには、管理者は、単一のポリシー グループのインターフェイス コンフィギュレーションを関連付けるスイッチ プロファイルを定義します。 このようにして、ファブリック上の多数のインターフェイスを一度に設定できます。 スイッチプロ

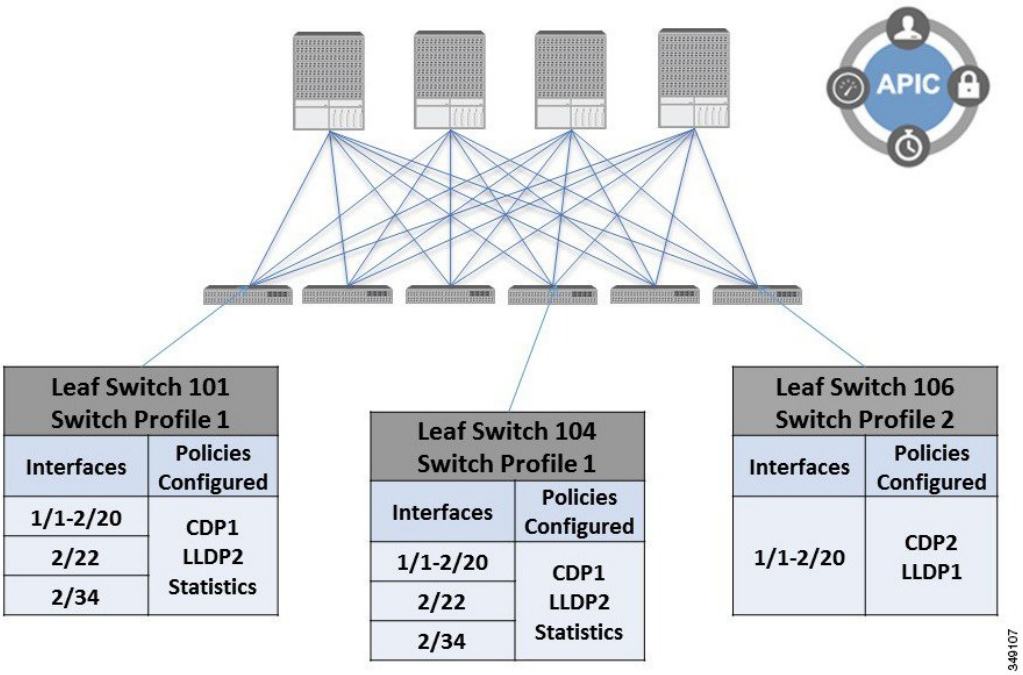
ファイルには、複数のスイッチに対する対称設定や一意の特殊用途設定を含めることができます。次の図は、ACI ファブリックへのアクセス設定のプロセスを示します。

図 *8*：アクセス ポリシーの設定プロセス



次の図は、ACI ファブリックにスイッチ プロファイル 1 およびスイッチ プロファイル 2 を適用した結果を示します。

図 *9*: アクセス スイッチ ポリシーの適用



インフラストラクチャと範囲を組み合わせることにより、管理者はスケーラブルな方法でファブリック構成を管理することができます。 これらの設定は、REST API、CLI、または GUI を使用して実行できます。 GUI 内の [Quick Start Interface]、[PC]、[VPC Configuration] ウィザードでは、そのようなポリシーの実行に必要な基盤となるオブジェクトが自動的に作成されます。

スケジューラ

スケジュールにより、設定のインポート/エクスポートまたはテクニカルサポートの収集などの操作を 1 つ以上の指定した時間帯に発生させることができます。

スケジュールには、一連のタイムウィンドウ（オカレンス）が含まれます。 これらのウィンドウは、1 回だけ発生させるか、または毎週指定した日時に繰り返し発生させることができます。 期間や実行するタスクの最大数などのウィンドウで定義されているオプションにより、スケジュール設定されたタスクの実行時期が決定されます。 たとえば、最大時間長またはタスク数に達したため特定のメンテナンス時間帯に変更を展開できない場合、この展開は次のメンテナンス時間に持ち越されます。

各スケジュールは、APIC が 1 つまたは複数のメンテナンス時間帯に入っているかどうか、定期的に確認します。 入っている場合、スケジュールはメンテナンスポリシーで指定された制限に対し適切な展開を実行します。

スケジュールには、スケジュールに関連付けられたメンテナンス時間帯を決定する 1 つ以上のオカレンスが含まれています。 オカレンスは次のいずれかになります。

- [One Time Window]：一度だけ行うスケジュールを定義します。 これらの時間帯は、その時間帯の最大時間長まで、または時間帯の中で実行可能なタスクの最大数に達するまで継続されます。
- [Recurring Window]：繰り返すスケジュールを定義します。 この時間帯は、タスクの最大数に達するまで、または時間帯に指定された日の終わりに達するまで継続します。

ファームウェアのアップグレード

APIC 上のポリシーは、ファームウェア アップグレード プロセスの次の項目を管理します。

- 使用するファームウェアのバージョン。
- シスコから APIC リポジトリへのファームウェア イメージのダウンロード。
- 互換性の適用。
- アップグレードするもの：
  - スイッチ
  - APIC
  - 互換性カタログ
- アップグレードを実行する時期。
- 障害の処理方法（再試行、一時停止、無視など）。

各ファームウェアイメージには、サポートされるタイプおよびスイッチモデルを識別する互換性カタログが含まれます。 APICは、ファームウェアイメージ、スイッチタイプ、およびそのファームウェアイメージを使用することを許可されるモデルのカタログを保持しています。デフォルトの設定では、互換性カタログに適合しない場合、ファームウェアの更新が拒否されます。

イメージ管理を実行する APIC には、互換性カタログ、APIC コントローラのファームウェア イメージおよびスイッチ イメージのイメージ リポジトリがあります。 管理者は、イメージ ソース ポリシーを作成することで外部 HTTP サーバまたは SCP サーバから新しいファームウェア イメージを APIC イメージ リポジトリにダウンロードできます。

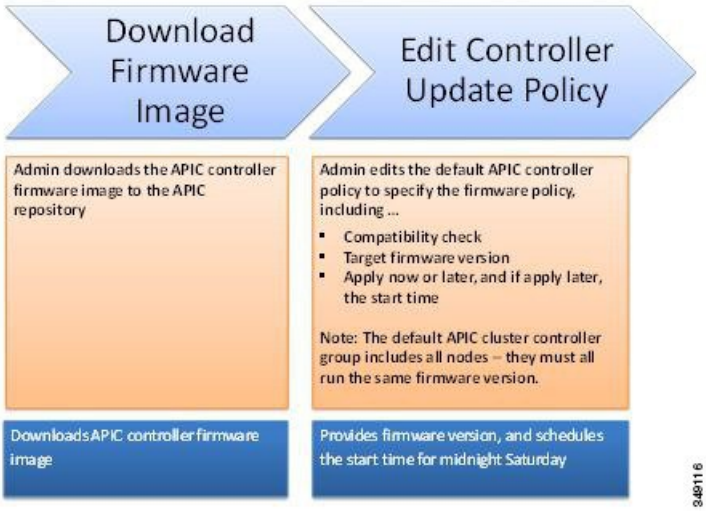
APIC 上のファームウェア グループ ポリシーは、必要なファームウェア バージョンを定義します。

メンテナンス グループ ポリシーは、ファームウェアをアップグレードする時期、アップグレードするノード、および障害の処理方法を定義します。 また、メンテナンス グループ ポリシーは、同時にアップグレードできるノードのグループを定義して、それらのメンテナンス グループをスケジュールに割り当てます。 ノード グループ オプションには、すべてのリーフ ノード、すべてのスパイン ノード、またはファブリックの一部であるノードのセットが含まれます。

APIC コントローラのファームウェア アップグレード ポリシーは、クラスタ内のすべてのノードに常に適用されますが、アップグレードは常に一度に 1 つのノードに実行されます。 APIC GUI により、ファームウェア アップグレードに関するリアルタイムのステータス情報が提供されます。

次の図は、APIC クラスタ ノードのファームウェア アップグレードのプロセスを示します。

図 *10* : *APIC* クラスタ コントローラのファームウェア アップグレードのプロセス



APICは、次のようにこのコントローラのファームウェアアップグレードポリシーを適用します。

- コントローラのクラスタ アップグレードは、土曜日の深夜に開始されます。
- システムは、既存のファームウェアの互換性を確認し、新しいファームウェアイメージで提供される互換性カタログに従って、新しいバージョンにアップグレードします。
- アップグレードは、クラスタ内のすべてのノードがアップグレードされるまで、一度に 1 個のノードずつ行われます。

（注） APIC はノードの複製クラスタであるため、中断は最小限に抑えるべきです。管理者は、APIC のアップグレードのスケジューリングを検討する場合、システムの負荷を意識する必要があります。

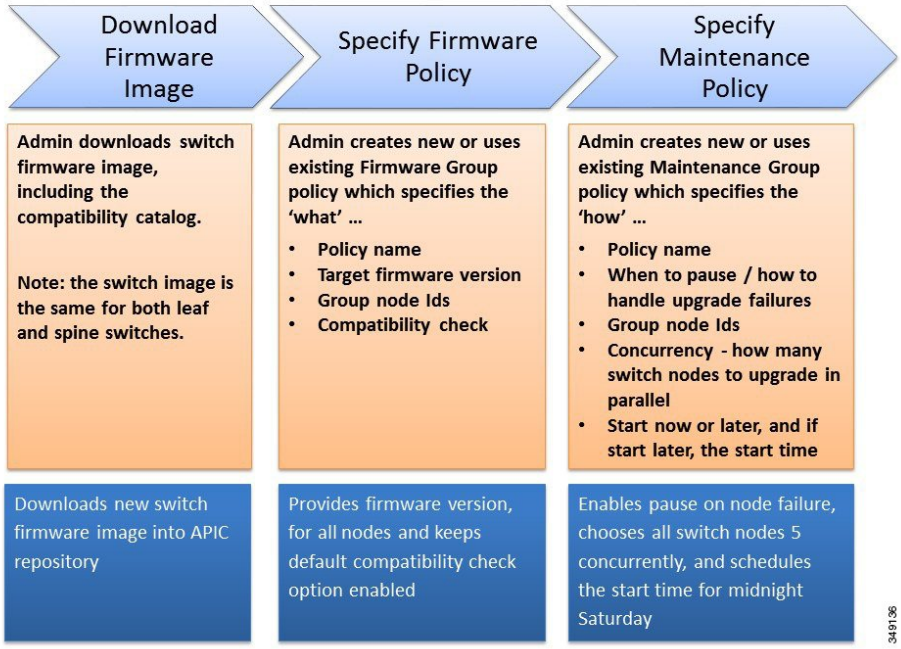
- APIC を含む ACI ファブリックは、アップグレードが進行中でも動作し続けます。

（注） コントローラはアップグレードをランダムに実行します。 各APICコントローラは、アップグレードに約 10 分かかります。 コントローラ イメージがアップグレードされると、クラスタからドロップされ、クラスタ内の他のAPICコントローラが動作中に新しいバージョンで再起動します。 コントローラが再起動すると、クラスタに再び参加します。 その後、クラスタが収束し、次のコントローラ イメージがアップグレードを開始します。 クラスタがすぐに収束せず、完全に適合しない場合は、クラスタが収束し完全に適合するまでアップグレードは待機します。 この期間中、「Waiting for Cluster Convergence」メッセージが表示されます。

- コントローラ ノードのアップグレードが失敗すると、アップグレードが一時停止し、手動による介入が行われるまで待機します。

次の図は、すべての ACI ファブリック スイッチ ノードのファームウェアをアップグレードするプロセスがどのように動作するかを示します。

図 *11*：スイッチ ファームウェアのアップグレード プロセス



APIC は、次のようにこのスイッチ アップグレード ポリシーを適用します。

- APIC は、アップグレードを土曜日の深夜に開始します。
- システムは、既存のファームウェアの互換性を確認し、新しいファームウェア イメージで提供される互換性カタログに従って、新しいバージョンにアップグレードします。

- アップグレードは、すべての指定されたノードがアップグレードされるまで、一度に 5 個のノードずつ行われます。

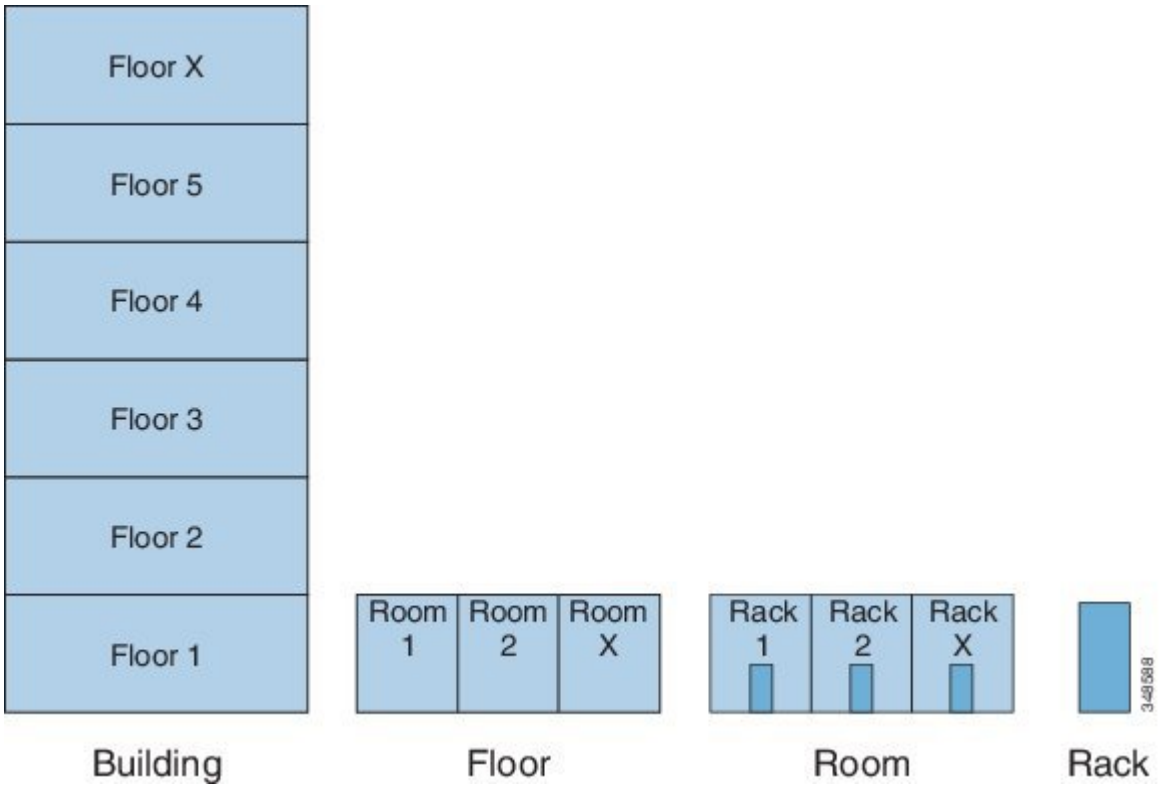
（注） ファームウェアのアップグレードにより、スイッチがリブートします。リブートにより数分間スイッチの操作が中断される場合があります。

- スイッチ ノードのアップグレードが失敗すると、アップグレードが一時停止し、手動による介入が行われるまで待機します。

Geolocation

管理者は、位置情報ポリシーを使用して、データセンター施設内の ACI ファブリック ノードの物理ロケーションをマッピングします。 次の図は、位置情報マッピング機能の例を示します。

図 *12*：*Geolocation*



たとえば、単一の部屋でのファブリック展開の場合は、管理者がデフォルトのルーム オブジェクトを使用して、スイッチの物理ロケーションに一致する 1 つ以上のラックを作成します。 大規模な展開の場合、管理者は 1 つ以上のサイト オブジェクトを作成できます。 各サイトには、1 つ以上の建物を含めることができます。 各建物には、1 つ以上のフロアがあります。 各フロアには 1

つ以上の部屋があり、各部屋には 1 つ以上のラックがあります。 最後に、各ラックは 1 つ以上のスイッチに関連付けることができます。