ACI ファブリックの Nexus Dashboard Orchestrator の Cisco APIC サイトの準備

リリース 4.3.x

目次

ポッド プロファイルとポリシー グループ

各サイトの APIC には、ポッド ポリシー グループを持つポッド プロファイルが 1 つ必要です。サイトにポッド ポリシー グループがない場合は、作成する必要があります。通常、これらの設定はすでに存在していて、ファブリックを最初に展開したときに設定したとおりになっているはずです。

1. サイトの APIC GUI にログインします。
2. ポッド プロファイルにポッド ポリシー グループが含まれているかどうかを確認します。

   [ファブリック（**Fabric**）**]** **>** **[**ファブリック ポリシー（**Fabric Policies**）**]** **>** **[**ポッド（**Pods**）**]** **>** **[**プロファイル（**Profiles**）**]** **>** **[**ポッド プロファイルのデフォルト（**Pod Profile default**）**]** に移動します。

3. 必要であれば、ポッド ポリシー グループを作成します。
   a. **[**ファブリック（**Fabric**）**]** **>** **[**ファブリック ポリシー（**Fabric Policies**）**]** **>** **[**ポッド（**Pods**）**]** **>** **[**ポリシー グループ（**Policy Groups**）**]** に移動します。
   b. **[**ポリシー グループ（**Policy Groups**）**]** を右クリックし、**[**ポッド ポリシー グループの作成（**Create Pod Policy Groups**）**]** を選択します。
   c. 適切な情報を入力して、**[**送信（**Submit**）**]** をクリックします。
4. 新しいポッド ポリシー グループをデフォルトのポッド プロファイルに割り当てます。
   a. **[**ファブリック（**Fabric**）**]** **>** **[**ファブリック ポリシー（**Fabric Policies**）**]** **>** **[**ポッド（**Pods**）**]** **>** **[**プロファイル（**Profiles**）**]** **>** **[**ポッド プロファイルのデフォルト（**Pod Profile default**）**]** に移動します。
   b. デフォルトのプロファイルを選択します。
   c. 新しいポッド ポリシー グループを選択し、**[**更新 **(Update)]** をクリックします。

すべての APIC サイトのファブリック アクセス ポリシーの設定

APIC ファブリックを Nexus Dashboard Orchestrator に追加し、Nexus Dashboard Orchestrator により管理できるようにするには、サイトごとに設定することが必要な、ファブリック固有の多数のアクセス ポリシーがあります。

ファブリック アクセス グローバル ポリシーの設定

このセクションでは、Nexus Dashboard Orchestrator に追加し、管理する前に、APIC サイトごとに作成する必要があるグローバル ファブリック アクセス ポリシーの設定について説明します。

1. サイトの APIC GUI に直接ログインします。
2. メイン ナビゲーション メニューから、**[**ファブリック（**Fabric**）**]** > **[**アクセス ポリシー（**Access Policies**）**]** を選択します。

   サイトを Nexus Dashboard Orchestrator に追加するには、いくつかのファブリックポリシーを設定する必要があります。APIC の観点からは、ベアメタル ホストを接続していた場合と同様に、ドメイン、AEP、ポリシー グループ、およびインターフェイス セレクタを構成することができます。同じマルチサイト ドメインに属するすべてのサイトに対して、スパイン スイッチ インターフェイスをサイト間ネットワークに接続するための同じオプションを構成する必要があります。

3. VLAN プールを指定します。

   最初に設定するのは、VLAN プールです。レイヤ 3 サブインターフェイスは VLAN 4 を使用してトラフィックにタグを付け、スパインスイッチをサイト間ネットワークに接続します。

   a. 左側のナビゲーション ツリーで、**[**プール（**Pools**）**]** > **[VLAN]** を参照します。

   b. **[VLAN]** カテゴリを右クリックし、**[VLAN** プールの作成（**Create**

      VLAN Pool）**]** を選択します。**[VLAN** プールの作成（**Create**

      VLAN Pool）**]** ウィンドウで、次の項目を指定します。

      - [名前（name）] フィールドで、VLAN プールの名前（たとえば、msite）を指定します。
      - [**Allocation Mode (**割り当てモード**)**]の場合は、[スタティック割り当て(Static Allocation)]を指定します。
      - [**Encap** ブロック**(Encap Blocks)**] の場合は、単一の VLAN 4 だけを指定します。両方の **[Range**（範囲）**]** フィールドに同じ番号を入力することによって、単一の VLAN を指定できます。

4. 接続可能アクセス エンティティ プロファイル (AEP) を作成します。

   a. 左側のナビゲーションツリーで、**[**グローバル ポリシー（**Global Policies**）**]** > **[**接続可能なアクセス エントリ プロファイル（**Attachable Access Entity Profiles**）**]** を参照します。

   b. **[**アタッチ可能なアクセス エンティティ プロファイル（**Attachable Access Entry Profiles**）**]** カテゴリを右クリックして、**[**アタッチ可能なアクセス エンティティ プロファイルの作成（**Create Attachable Access Entity Profiles**）**]** を選択します。

      [接続可能アクセス エンティティ プロファイルの作成（Create Attachable Access Entity Profiles）] ウィンドウで、AEP の名前（例: msite-aep）を指定します。

c. [次へ（**Next**）] をクリックして [送信（**Submit**）]します。

インターフェイスなどの追加の変更は必要ありません。

5. ドメインを設定します。
設定するドメインは、このサイトを追加するときに、Nexus Dashboard Orchestratorから選択するものになります。

a. 左のナビゲーション ツリーで、[物理的 ドメインと外部ドメイン（**Physical and External Domains**）] > [外部ルーテッド ドメイン（**External Routed Domains**）] を参照します。

b. [外部ルーテッド ドメイン（**External Routed Domains**）] カテゴリを右クリックし、[レイヤ **3** ドメインの作成（**Create Layer 3 Domain**）] を選択します。[レイヤ **3** ドメインの作成（**Create Layer 3 Domain**）]ウィンドウで、次の項目を指定します。

- [名前（**Name**）] フィールドで、ドメインの名前（たとえば、msite-l3）を指定します。
- 関連付けられている接続可能エンティティ プロファイルの場合は、ステップ 4で作成した AEP を選択します。
- **VLAN** プールの場合は、ステップ 3で作成した VLAN プールを選択します。

c. [送信（Submit）] をクリックします。

セキュリティ ドメインなどの追加の変更は必要ありません。

次に行う作業：

グローバル アクセス ポリシーを設定した後も、[ファブリック アクセス インターフェイス ポリシーの構成（Configuring Fabric Access Interface Policies）] の説明に従って、インターフェイス ポリシーを追加する必要があります。

ファブリック アクセス インターフェイス ポリシーの設定

始める前に：

ファブリックの APIC では、「ファブリック アクセス グローバル ポリシー」の説明に従って、VLAN プール、AEP、および ドメインなどのグローバル ファブリック アクセス ポリシーを構成しておく必要があります。

このセクションでは、各 APIC サイトの Nexus Dashboard Orchestrator で行わなければならないファブリック アクセス インターフェイスの設定について説明します。

1. サイトの APIC GUI に直接ログインします。
2. メイン ナビゲーション メニューから、[ファブリック（**Fabric**）] > [アクセス ポリシー（**Access Policies**）] を選択します。

前の項で構成した VLAN、AEP、およびドメインに加えて、サイト間ネットワーク (ISN) に接続するファブリックのスパイン スイッチ インターフェイスに対してインターフェイス ポリシーを作成します。

3. スパイン ポリシー グループを設定します。

a. 左ナビゲーション ツリーで、[インターフェイス ポリシー（**Interface Policy**）] >[ポリシー グループ（**Policy Groups**）] > [スパイン ポリシー グループ（**Spine Policy Groups**）] を参照します。

これは、ベアメタル サーバを追加する方法と類似していますが、リーフ ポリシー グループの代わ

りにスパイン ポリシー グループを作成する点が異なります。

b. [スパイン ポリシー グループ（**Spine Policy Groups**）] カテゴリーを右クリックして、[スパイン アクセス ポート ポリシー グループの作成（**Create Spine Access Port Policy Group**）] を選択します。

[スパイン アクセス ポリシー グループの作成（**Create Spine Access Port Policy Group**）] ウィンドウで、以下のとおり指定します。

- [名前（**Name**）] フィールドで、ポリシー グループの名前を指定します。たとえば Spine1-PolGrp です。
- [リンク レベル ポリシー（**Link Level Policy**）] フィールドで、スパイン スイッチと ISN の間のリンク ポリシーを指定します。
- **[CDP** ポリシー **(CDP Policy)]** の場合、CDP を有効にするかどうかを選択します。
- [アタッチ済みエンティティ プロファイル（**Attached Entity Profiel**）]で、前の項で構成した AEP を選択します。たとえば msite-aep です。

c. [送信（Submit）] をクリックします。

セキュリティ ドメインなどの追加の変更は必要ありません。

4. スパイン プロファイルを設定します。

a. 左ナビゲーション ツリーで、[インターフェイス ポリシー（**Interface Policies**）] > [ポリシー グループ（**Profiles**）] > [スパイン ポリシー グループ（**Spine Profiles**）] を参照します。

b. [プロファイル（**Profiles**）] カテゴリを右クリックし、[スパイン インターフェイス プ

ロファイルの作成（**Create Spine Interface Profile**）] を選択します。[スパイン イン

ターフェイス プロファイルの作成（**Create Spine Interface Profile**）] ウィンドウで、

次のとおり指定します。

- [名前（**name**）] フィールドで、プロファイルの名前（Spine1-ISNなど）を指定します。
- [インターフェイス セレクタ（**Interface Selectors**）]で、**+** 記号をクリックして、ISN に接続されるスパイン スイッチ上のポートを追加します。次に、[スパイン アクセス ポート セレクターの作成（**Create Spine Access Port Selector**）] ウィンドウで、次のように指定します。
  - [名前（**Name**）] フィールドで、ポート セレクタの名前を指定します（Spine1-ISN など）。
  - [インターフェイス **ID**（**Interface IDs**）] で、ISN に接続するスイッチ ポートを指定します（5/32 など）。
  - [インターフェイス ポリシー グループ **(Interface Policy Group)]** に、前の手順で作成したポリシー グループを選択します (例: Spine1-PolGrp)。

  それから、**[OK]** をクリックして、ポート セレクタを保存します。

c. [送信（**Submit**）] をクリックして、スパイン インターフェイス プロファイルを保存します。

5. スパイン スイッチ セレクター ポリシーを設定します。

a. 左ナビゲーション ツリーで、[スイッチ ポリシー（**Switch Policies**）] > [プロファイル（**Profiles**）] > [スパイン プロファイル（**Spine Profiles**）] を参照します。

b. [スパイン プロファイル（**Spine Profiles**）] カテゴリを右クリックし、[スパ

イン プロファイルの作成（**Create Spine Profile**）**]** を選択します。**[**スパイン インターフェイス プロファイルの作成（**Create Spine Interface Profile**）**]** ウィンドウで、次のように指定します。

- **[**名前 **(name)]** フィールドに、プロファイルの名前を指定します (例: Spine1)。
- **[**スパイン セレクタ（**Spine Selectora**）**]** で、**+** をクリックしてスパインを追加し、次の情報を入力します。
  - **[**名前 **(name)]** フィールドで、セレクタの名前を指定します (例: Spine1) 。
  - **[**ブロック **(Blocks)]** フィールドで、スパイン ノードを指定します (例: 201)。

c. **[**更新 **(Update)]** をクリックして、セレクタを保存します。

d. **[**次へ **(Next)]** をクリックして、次の画面に進みます。

e. 前の手順で作成したインターフェイス プロファイルを選択します。

例：Spine1-ISN。

f. **[**完了 **(Finish)]** をクリックしてスパイン プロファイルを保存します。

リモート リーフ スイッチを含むサイトの設定

Multi-Site アーキテクチャはリモート リーフスイッチを持つ {FabricControllerShortName} サイトをサポートします。次のセクションでは、Nexus Dashboard Orchestrator がこれらのサイトを管理できるようにするために必要な注意事項、制限事項、および設定手順を説明します。

リモート リーフの注意事項と制限事項

Nexus Dashboard Orchestrator により管理されるリモート リーフをもつ APIC サイトを追加する場合、次の制約が適用されます。

- Cisco APIC をリリース 4.2(4) 以降にアップグレードする必要があります。
- このリリースでは、物理リモート リーフ スイッチのみがサポートされます
- -EX および -FX 以降のスイッチのみが、マルチサイトで使用するリモートリーフスイッチとしてサポートされています。
- リモートリーフは、IPN スイッチを使用しないバックツーバック接続サイトではサポートされていません
- 1 つのサイトのリモート リーフ スイッチで別のサイトの L3Out を使用することはできません。
- あるサイトと別のサイトのリモート リーフ間のブリッジ ドメインの拡張はサポートされていません。

また、Nexus Dashboard Orchestrator でサイトを追加して管理するには、その前に次のタスクを実行する必要があります。

- 次の項で説明するように、リモート リーフの直接通信を有効にし、サイトの {FabricControllerShortName} でルータブル サブネットを直接構成する必要があります。
- リモート リーフ スイッチに接続しているレイヤ 3 ルータのインターフェイスに適用されている DHCP リレー設定で、Cisco APIC ノードのルーティング可能な IP アドレスを追加する必要があります。

  各 APIC ノードのルーティング可能なIP アドレスは、APIC GUI の **System > Controllers > <controller-name>** のルーティング可能な **IP** フィールドに表示されます。

リモート リーフ スイッチのルーティング可能なサブネットの設定

1 つ以上のリモート リーフ スイッチを含むサイトを Nexus Dashboard Orchestrator に追加するには、その前に、リモート リーフ ノードが関連付けられているポッドのルーティング可能なサブネットを設定する必要があります。

1. サイトの {FabricControllerShortName} GUI に直接ログインします。
2. メニュー バーから、[ファブリック（**Fabric**）] > [インベントリ（**Inventory**）] を選択します。
3. [ナビゲーション (Navigation)] ウィンドウで、[ポッド ファブリック セットアップ ポリシー **(Pod Fabric Setup Policy)**] をクリックします。
4. メイン ペインで、サブネットを設定するポッドをダブルクリックします。
5. [ルータブル サブネット（**Routable Subnets**）] エリアで、[**+**] 記号をクリックしてサブネットを追加します。
6. [**IP**] と [予約アドレス数（**Reserve Address Count**）] を入力し、状態を [アクティブ（Active）] または [非アクティブ（Inactive）] に設定してから、[更新（**Update**）] をクリックしてサブネットを保

存します。

ルーティング可能なサブネットを設定する場合は、 /22~/29の範囲のネットマスクを指定する必要があります。

7. [送信（**Submit**）] をクリックして構成を保存します。

リモート リーフ スイッチの直接通信の有効化

1 つ以上のリモート リーフ スイッチを含むサイトを Nexus Dashboard Orchestrator に追加するには、その前に、そのサイトに対して直接リモート リーフ通信を設定する必要があります。リモートリーフ直接通信機能に関する追加情報については、*Cisco APIC レイヤ 3 ネットワーク コンフィギュレーション ガイド*を参照してください。ここでは、Multi-Site との統合に固有の手順とガイドラインの概要を説明します。

リモート リーフ スイッチの直接通信を有効にすると、スイッチは新しいモードでのみ機能します。

1. サイトの {FabricControllerShortName} に直接ログインします。
2. リモート リーフ スイッチの直接トラフィック転送を有効にします。
   a. メニュー バーから、[システム（**System**）] > [システムの設定（**System Settings**）] に移動します。
   b. 左側のサイドバーのメニューから [ファブリック全体の設定（**Fabric Wide Setting**）] を選択します。
   c. [リモート リーフ 直接トラフィック転送（**Enable Remote Leaf Direct Traffice Forwarding**）] チェックボックスをオンにします。

   有効にした後は、このオプションを無効にすることはできません。

   d. [送信（**Submit**）] をクリックして変更を保存します。

Cisco Mini ACI ファブリック

Cisco Multi-Site は、追加の設定を必要とせずに、一般的なオンプレミス サイトとして Cisco Mini ACI ファブリックをサポートします。ここでは、Mini ACI ファブリックの概要について説明します。このタイプのファブリックの導入と設定に関する詳細情報は、*『Cisco Mini ACI ファブリックおよび仮想 APIC』*に記述されています。

Cisco ACI リリース 4.0(1) では、小規模導入向けに Mini ACI ファブリックが導入されました。Mini ACI ファブリックは、1つの物理 APIC と、仮想マシンで実行される 2 つの仮想 APIC（vAPIC）で構成される [CiscoAPICShortName] クラスタで動作します。これにより、APIC クラスタの物理的なフットプリントとコストが削減され、ACI ファブリックを、物理的な設置面積や初期コストのために、フルスケールの ACI インストールが実用的でないような、ラック スペースや初期予算が限られたシナリオ（コロケーション施設やシングルルームデータセンターなど）に導入できるようになります。

次の図に、物理 APIC と 2 つの仮想 APIC（vAPIC）を備えた [CiscoACIShortName2] ファブリックの例を示します。

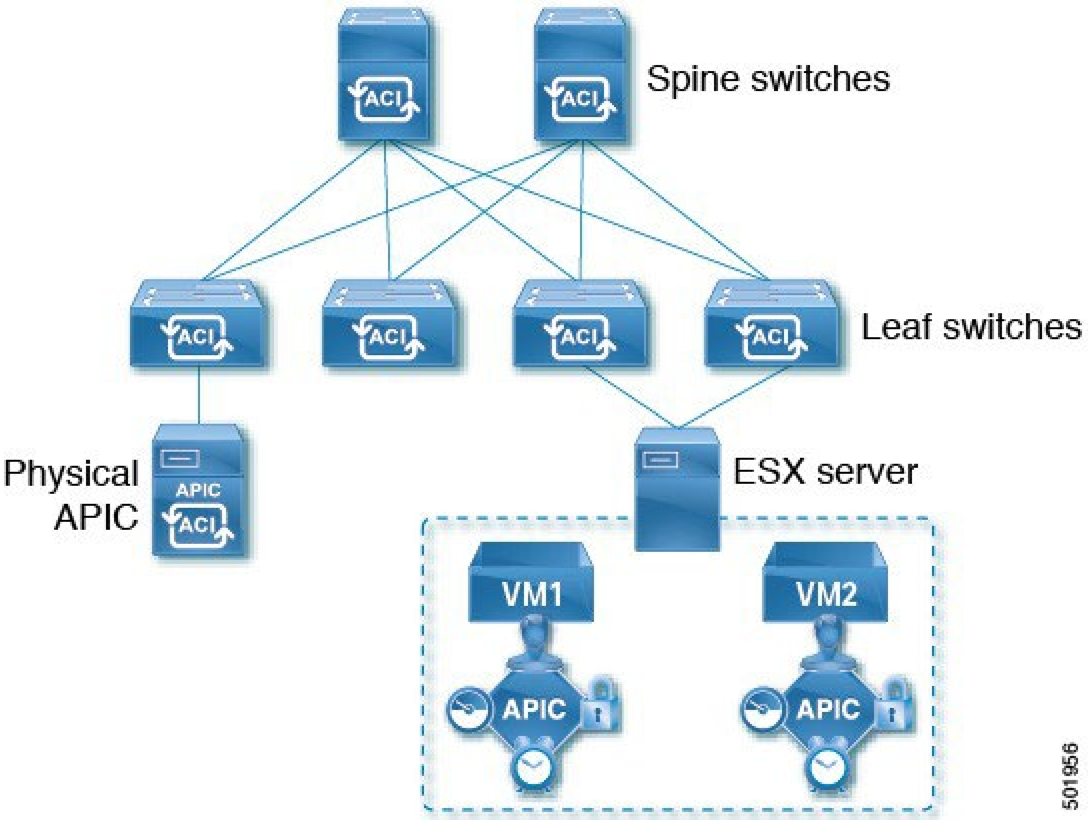


図 1. Cisco Mini ACI ファブリック

サイトの追加と削除

Cisco NDO と APIC の相互運用性のサポート

Cisco Nexus Dashboard Orchestrator（NDO）では、すべてのサイトで特定のバージョンの APIC を実行する必要はありません。各サイトの APIC クラスタと NDO 自体は、Nexus Dashboard Orchestrator サービスがインストールされている Nexus ダッシュボードにファブリックをオンボードできる限り、相互に独立してアップグレードし、混合動作モードで実行することができます。そのため、常に Nexus Dashboard Orchestrator の最新リリースにアップグレードしておくことをお勧めします。

ただし、1 つまたは複数のサイトで APIC クラスタをアップグレードする前に NDO をアップグレードすると、新しい NDO の機能の一部が、以前の APIC リリースでまだサポートされていないという状況が生じ得ることに注意してください。この場合、各テンプレートでチェックが実行され、すべての設定済みオプションがターゲットサイトでサポートされていることを確認します。

このチェックは、テンプレートを保存するか、テンプレートを展開するときに実行されます。テンプレートがすでにサイトに割り当てられている場合、サポートされていない設定オプションは保存されません。テンプレートがまだ割り当てられていない場合は、サイトに割り当てることができますが、サイトがサポートしていない設定が含まれている場合は、スキーマを保存したり展開したりすることはできません。

サポートされていない設定が検出されると、エラーメッセージが表示されます。例: *この APIC サイト バージョン<site version>は、NDO ではサポートされていません。 この<feature>に必要な最小バージョンは<required-version>以降です。*

次の表に、各機能と、それぞれに必要な最小限の APIC リリースを示します。

次の機能の一部は以前の Cisco APICリリースでサポートされていますが、リリース 4.2(4) は Nexus Dashboard にオンボードして、このリリースの N Dashboard Orchestrator で管理できる最も古いリリースです。

機能	最小バージョン
ACI マルチポッドのサポート	リリース 4.2(4)
サービス グラフ (L4 ~ L7 サービス)	リリース 4.2(4)
外部 EPG	リリース 4.2(4)
ACI 仮想エッジ VMM のサポート	リリース 4.2(4)
DHCP Support	リリース 4.2(4)
整合性チェッカー	リリース 4.2(4)
vzAny	リリース 4.2(4)
ホストベースのルーティング	リリース 4.2(4)
CloudSec 暗号化	リリース 4.2(4)
レイヤ 3 マルチキャスト	リリース 4.2(4)
OSPF の MD5 認証	リリース 4.2(4)
EPG 優先グループ	リリース 4.2(4)
サイト内 L3Out	リリース 4.2(4)

機能	最小バージョン
QoS の優先順位	リリース 4.2(4)
コントラクト QoS 優先順位	リリース 4.2(4)
シングル サインオン（SSO）	リリース 5.0(1)
マルチキャスト ランデブー ポイント（RP）のサポート	リリース 5.0(1)
AWS および Azure サイトのトランジット ゲートウェイ（TGW）サポート	リリース 5.0(1)
SR-MPLS サポート	リリース 5.0(1)
クラウド ロードバランサ 高可用性ポート	リリース 5.0(1)
UDR を使用したサービスグラフ（L4-L7 サービス）	Release 5.0(2)
クラウドでのサードパーティ デバイスのサポート	Release 5.0(2)
クラウド ロードバランサのターゲット接続モード機能	Release 5.1(1)
Express Route 経由で到達可能な非 ACI ネットワークの Azure でのセキュリティおよびサービス挿入サポート	Release 5.1(1)
CSR プライベート IP サポート	Release 5.1(1)
Azure のクラウド ネイティブ サービスの ACI ポリシー モデルと自動化の拡張	Release 5.1(1)
Azure の単一 VNET 内での複数の VRF サポートによる柔軟な セグメンテーション	Release 5.1(1)
|Azure PaaS および サードパーティ サービスのプライベート リンク自動化	Release 5.1(1)
ACI-CNI を使用した Azure での OpenShift 4.3 IPI	Release 5.1(1)
クラウド サイト アンダーレイの設定	リリース 5.2(1)

Cisco ACI サイトの追加

始める前に：

- この章の前の項で説明したように、オンプレミスの ACI サイトを追加する際には、各サイトの APIC でサイト固有の構成を完了している必要があります。
- 追加するサイトの 1 つ以上がリリース 4.2(4) 以降を実行していることを確認する必要があります。

ここでは、Cisco Nexus Dashboard GUI を使用して Cisco APIC または Cloud Network Controller サイトを追加し、そのサイトを Cisco Nexus Dashboard Orchestrator で管理できるようにする方法について説明します。

1. Cisco Nexus Dashboard にログインして **[**管理コンソール（**Admin Console**）**]**を開きます。
2. 左のナビゲーション メニューから **[**操作（**Operate**）**]** を選択し、**[**サイト（**Site**）**]**をクリックします。
3. **[**サイトの追加（**Add Site**）**]** を選択し、情報を提供します。
   a. **[**サイト タイプ（**Site Type**）**]** で、追加する ACI ファブリックのタイプに応じて **[ACI]** または

[Cloud Network Controller] を選択します。

b. コントローラ情報を入力します。

- ACI ファブリックを現在管理している APIC コントローラについて、**[**ホスト名**/IP** アドレス（**Host Name/IP Address**）**]**、**[**ユーザー名（**User Name**）**]**、および **[**パスワード（**Password**）**]** を入力する必要があります。

  APIC ファブリックでは、Cisco Nexus Dashboard Orchestrator サービスのみでサイトを使用する場合、APIC のインバンドまたはアウトオブバンド IP アドレスを指定できます。Cisco Nexus Dashboard Insights でもサイトを使用する場合は、インバンド IP アドレスを指定する必要があります。

- Cisco APIC によって管理されるオンプレミス ACI サイトの場合、このサイトを Cisco Nexus Insights などのデイ 2 オペレーション アプリケーションで使用する場合は、追加する Cisco Nexus Dashboard をファブリックに接続するために使用するインバンド **EPG** 名も指定する必要があります。それ以外の場合、このサイトを Cisco Nexus Dashboard Orchestrator でのみ使用する場合は、このフィールドを空白のままにすることができます。

- Cloud Network Controller サイトの場合、プロキシ経由でクラウド サイトに到達できる場合は、**[**プロキシを有効（**Enable Proxy**）**]**にします。

  プロキシは、Cisco Nexus Dashboard のクラスタ設定ですでに構成されている必要があります。管理ネットワーク経由でプロキシに到達できる場合は、プロキシIPアドレス用のスタティック管理ネットワーク ルートも追加する必要があります。プロキシとルートの構成の詳細については、お使いのリリースの Nexus Dashboard ユーザー ガイドを参照してください。

c. **[**保存（**Save**）**]** をクリックして、サイトの追加を終了します。

現在、サイトは Cisco Nexus ダッシュボードで使用できますが、次の手順で説明するように、Cisco Nexus Dashboard Orchestrator 管理のため有効にする必要があります。

4. 追加する任意の ACI または、Cloud Network Controller サイトに対して前の手順を繰り返します。

5. Cisco Nexus Dashboard の **[**サービス（**Services**）**]** ページから、Cisco Nexus Dashboard Orchestrator サービスを開きます。

   Cisco Nexus Dashboard ユーザーのログイン情報を使用して自動的にサインインします。

6. Cisco Nexus Dashboard Orchestrator GUI でサイトを管理します。

   a. 左のナビゲーションメニューから [サイト（Sites）] を選択します。

   b. メインペインで、NDOで管理する各ファブリックの **[**状態（**State**）**]** を [非管理対象（`Unmanaged`）] から [管理対象（`Managed`）] に変更します。

   サイトを管理するときは、サイトごとに一意のサイト ID を指定する必要があります。

サイトの削除

始める前に：

削除するサイトに関連付けられているすべてのテンプレートが展開されていないことを確認する必要があります。

ここでは、Cisco Nexus Dashboard Orchestrator GUI を使用して 1 つ以上のサイトのサイト管理を無効にする方法について説明します。サイトは Cisco Nexus Dashboard に残ります。

1. Cisco Nexus Dashboard Orchestrator GUI を開きます。

   Cisco Nexus Dashboard の **[**サービス カタログ（**Service Catalog**）**]** から NDO サービスを開きます。Cisco Nexus Dashboard ユーザーのログイン情報を使用して自動的にサインインします。

2. すべてのテンプレートからサイトを削除します。

   サイトを管理解除して Cisco Nexus Dashboard から削除する前に、関連付けられているすべてのテンプレートからサイトを削除する必要があります。

   a. **[**構成（**Configure**）**] > [**テナント テンプレート（**Tenant Template**）**] [**アプリケーション（**Applications**）**]** に移動します。

   b. サイトに関連付けられた 1 つ以上のテンプレートを含む **[**スキーマ（**Schema**）**]** をクリックします。

   c. **[**概要（**Overview**）**]** ドロップダウンから、削除するサイトに関連付けられているテンプレートを選択します。

   d. **[**アクション（**Actions**）**]** ドロップダウンから、**[**サイトの追加/削除（**Add/Remove Sites**）**]** を選択し、削除するサイトのチェックを外します。

      これにより、このテンプレートを使用してこのサイトに展開された構成が削除されます。

      ストレッチされていないテンプレートの場合、代わりに **[**アクション（**Actions**）**] > [**サイトの関連付けを解除（**Dissociate Sites**）**]** を選択して、テンプレートによってサイトに展開された構成を保持することを選択できます。このオプションを使用すると、NDO によって展開された構成を保持できますが、それらのオブジェクトを NDO から管理することはできなくなります。

   e. このスキーマおよび他のすべてのスキーマで管理解除するサイトに関連付けられているすべてのテンプレートについて、この手順を繰り返します。

3. サイトのアンダーレイ構成を削除します。

   a. 左のナビゲーション メニューから 、**[**構成（**Configure**）**] > [**サイト間接続（**Site To Site Connectivity**）**]** を選択します。

   b. メイン ペインにある **[**構成（**Configure**）**]** をクリックします。

   c. 左のサイドバーで、管理対象から外すサイトを選択します。

   d. **[**詳細の表示（**View Details**）**]** をクリックして、サイト設定をロードします。

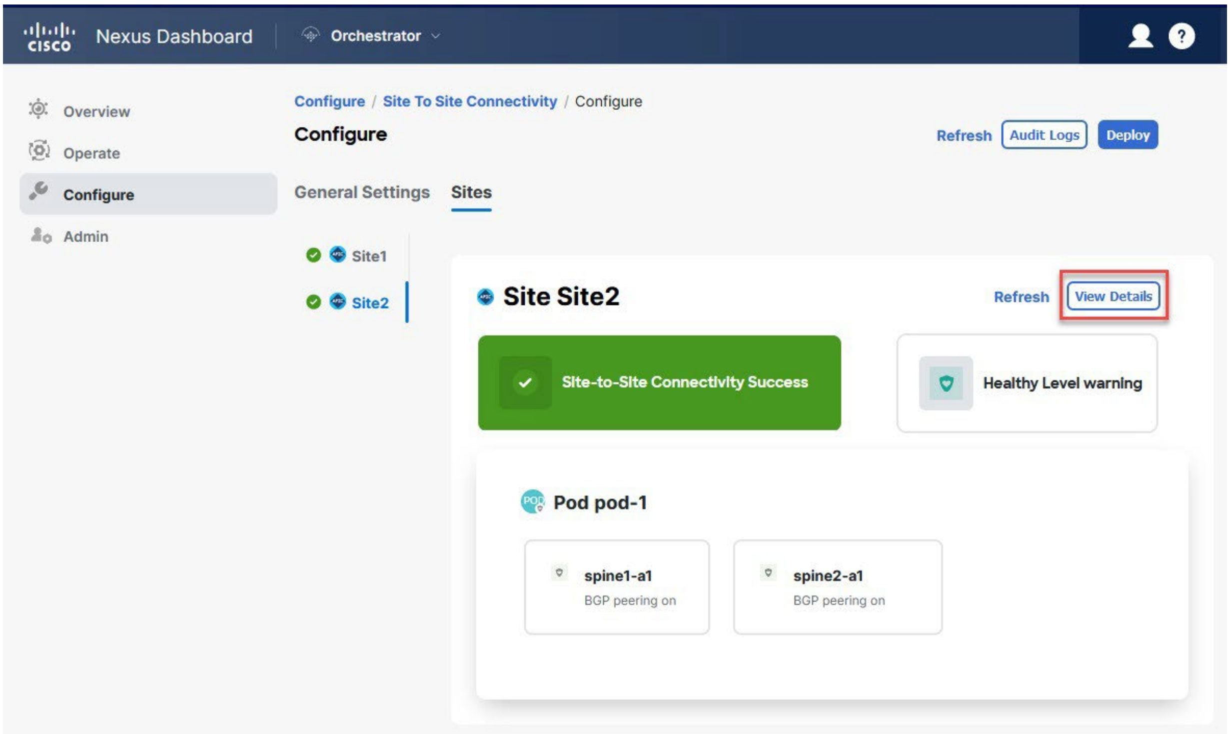


図 2 [構成（Configure）] > [サイト間接続（Site to Site Connectivity）] > [サイト（Site）] > [詳細の表示（View Details）]

e. 右側のサイドバーの [サイト間接続（**Inter-Site Connectivity**）] タブで、[マルチサイト（**Multi-Site**）] チェックボックスを無効にします。これにより、このサイトと他のサイト間の EVPN ピアリングが無効になります。

f. [展開する（**Deploy**）] をクリックして、変更をサイトに展開します。

4. Cisco Nexus Dashboard Orchestrator GUI で、サイトを無効にします。

a. 左のナビゲーションメニューから [サイト（**Sites**）] を選択します。

b. メイン ペインで、非管理対象に設定したいサイトに対して [状態（**State**）] を [非管理対象（Unmanaged）] から [管理対象（Managed）] に変更します。

サイトが 1 つ以上の展開されたテンプレートに関連付けられている場合、それらのテンプレートを展開解除するまで、その状態を [非管理対象（Unmanaged）] に変更することはできません。

5. Cisco Nexus Dashboard からサイトを削除します。

このサイトを管理したり、他のアプリケーションで使用したりする必要がなくなった場合は、Cisco Nexus Dashboard からもサイトを削除できます。

このサイトは、Cisco Nexus Dashboard クラスタにインストールされているどのサービスでも使用されないようにしてください。

a. 上部のナビゲーション バーで [ホーム（**Home**）] アイコンをクリックして、Cisco Nexus Dashboard GUI に戻ります。

b. Cisco Nexus Dashboard GUI の左側のナビゲーション メニューから、[操作（**Operate**）] > [サイト（**Sites**）] を選択します。

c. 削除するサイトを1つ以上選択します。

d. メイン ペインの右上にある [アクション（**Actions**）] > [サイトの削除（**Delete Site**）] をクリックします。

e. サイトのサインイン情報を入力し、**[OK]** をクリックします。
   Cisco Nexus Dashboard からサイトが削除されます。

ファブリック コントローラへの相互起動

Cisco Nexus Dashboard Orchestrator は現在、ファブリックのタイプごとにいくつかの構成オプションをサポートしています。追加の多くの構成オプションでは、ファブリックのコントローラに直接サインインする必要があります。

NDO の **[**操作（**Operate**）**]** > **[**サイト（**Sites**）**]** 画面から特定のサイト コントローラの GUI にクロス起動するには、サイトの横にあるアクション（**[...]**）メニューを選択し、**[**ユーザー インターフェイスで開く（**Open in user interface**）**]** をクリックします。クロス起動は、ファブリックのアウトオブバンド（OOB）管理IPで動作します。

Cisco Nexus Dashboardとファブリックで同じユーザーが構成されている場合、Cisco Nexus Dashboard ユーザーと同じサインイン情報を使用して、ファブリックのコントローラに自動的にログインします。一貫性を保つために、Cisco Nexus Dashboard とファブリック全体で共通のユーザーによるリモート認証を構成することを推奨します。

インフラ一般設定

インフラ設定ダッシュボード

[構成（Config）] > [サイト間の接続（Site To Site Connectivity）] ページでは、Cisco Nexus Dashboard Orchestrator 展開のすべてのサイトと、サイト間接続の概要が表示され、次の情報が含まれています

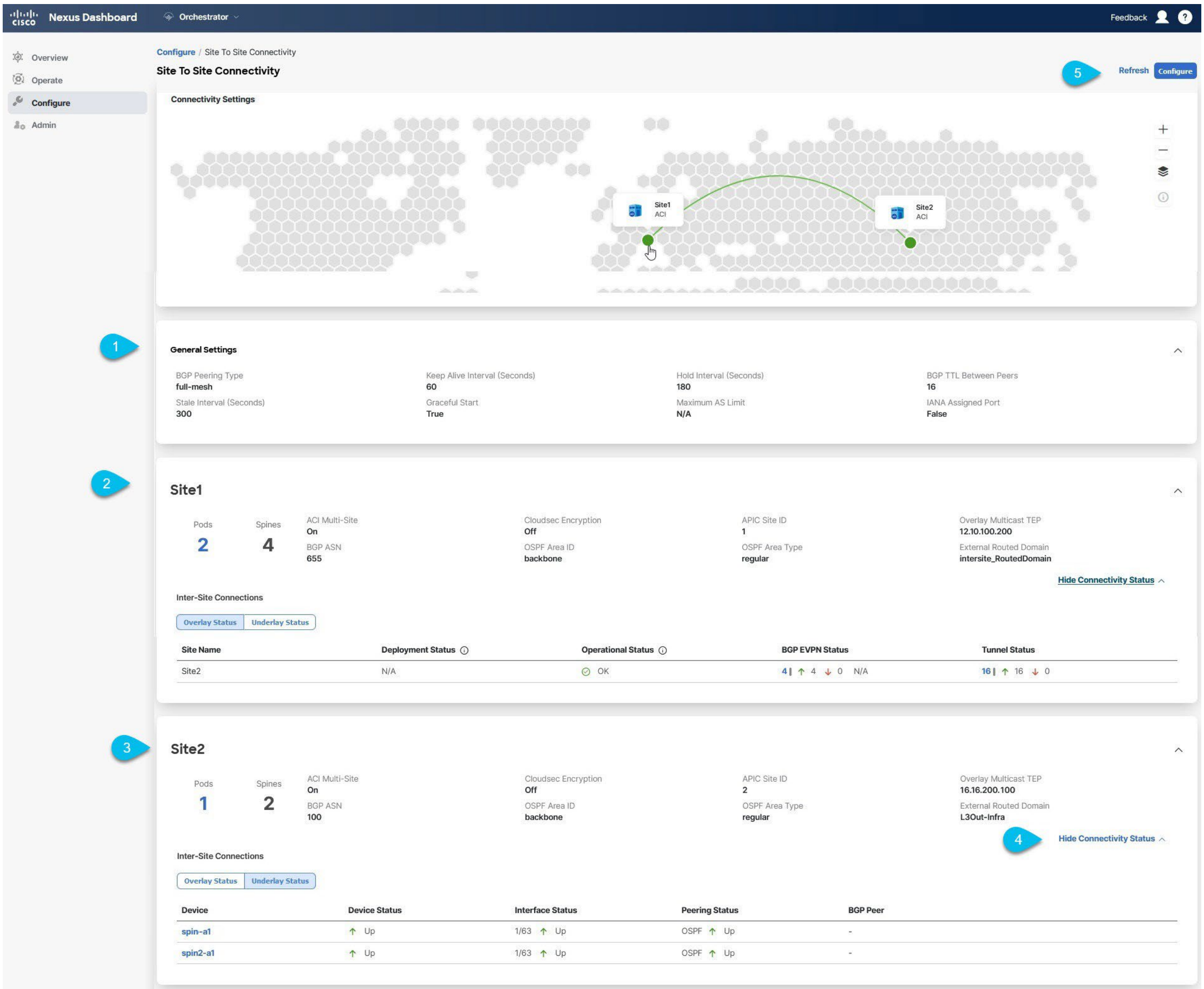


図 3. インフラ設定の概要

1. **[一般設定（General Settings）]** タイルには、BGP ピアリング タイプとその構成に関する情報

   が表示されます。詳細については、次のセクションで説明します。

2. **[オンプレミス（On-Premises）]** タイルには、ポッドとスパイン スイッチの数、OSPF 設定、およびオーバーレイ IP とともに、マルチサイト ドメインの一部であるすべてのオンプレミス サイトに関する情報が表示されます。

   サイト内のポッドの数を表示する **[ポッド（Pods）]** タイルをクリックすると、各ポッドのオーバーレイ ユニキャスト TEP アドレスに関する情報を表示できます。

   これについては、「Cisco APIC サイトのインフラの構成」で詳しく説明されています。

3. **[クラウド（Cloud）]** タイルには、マルチサイト ドメインの一部であるすべてのクラウド サイトに関する情報と、リージョン数および基本的なサイト情報が表示されます。

これについては、「Cisco クラウド ネットワーク コントローラ ファブリックのインフラの構成」を参照してください。

4. [接続ステータスの表示（**Show Connectivity Status**）] をクリックして、特定のサイトのサイト間接続の詳細を表示できます。
5. [構成（**Configure**）] ボタンを使用して、サイト間接続構成に移動できます。これについては、次の項で詳しく説明します。

次のセクションでは、全般的なファブリック インフラ設定を行うために必要な手順について説明します。ファブリック固有の要件と手順は、管理するファブリックの特定のタイプに基づいて、次の章で説明します。

インフラの設定を進める前に、前のセクションで説明したようにサイトを設定して追加する必要があります。

加えて、スパイン スイッチの追加や削除、またはスパイン ノード識別子の変更などのインフラストラクチャの変更には、一般的なインフラの構成手順の一部として、「ファブリック接続情報の更新」に記載されているような、Cisco Nexus Dashboard Orchestrator のファブリック接続情報の更新が必要です。

パーシャル メッシュ サイト間接続

Nexus Dashboard Orchestrator が管理するすべてのサイトから他のすべてのサイトへのサイト間接続を構成するフル メッシュ接続に加えて、このリリースではパーシャル メッシュ構成もサポートしています。パーシャル メッシュ構成では、他のサイトへのサイト間接続を持たないスタンドアロン モードでサイトを管理したり、サイト間構成をマルチサイト ドメイン内の他のサイトのサブセットのみに制限したりできます。

Nexus Dashboard Orchestrator リリース 3.6(1) より前では、サイト間のサイト間接続が構成されていなくても、サイト間でテンプレートを拡張し、他のサイトに展開された他のテンプレートからポリシーを参照でき、それらのサイト間のサイト間接続が構成されていなくても、サイト間で動作しない意図したトラフィック フローが発生します。

リリース 3.6(1) 以降、Orchestrator では、それらのサイト間のサイト間接続が適切に構成および展開されている場合にのみ、（他のサイトに展開されている）他のテンプレートからテンプレートとリモート参照ポリシーを 2 つ以上のサイト間で拡張できます。

次のセクションで説明するように、Cisco APIC および Cisco Cloud Network Controller サイトのサイト インフラストラクチャを構成する場合、サイトごとに、他のどのサイト インフラストラクチャ接続を確立するかを明示的に選択し、その構成情報のみを提供できます。

パーシャル メッシュ接続のガイドライン

パーシャル メッシュ接続を構成するときは、次のガイドラインを考慮してください。

- パーシャル メッシュ接続は、2 つのクラウド サイト間、またはクラウドとオンプレミスのサイト間

  でサポートされています。すべてのオンプレミス サイト間で完全なメッシュ接続が自動的に確立さ

  れます。

- パーシャル メッシュ接続は、BGP-EVPN または BGP-IPv4 プロトコルを使用してサポートされています。

  ただし、テンプレートのストレッチは、BGP- EVPN プロトコルを使用して接続されているサイトに対してのみ許可されることに注意してください。BGP-IPv4 を使用して 2 つ以上のサイトを接続してい

る場合、それらのサイトのいずれかに割り当てられたテンプレートは、1 つのサイトにのみ展開できます。

インフラの設定: 一般設定

ここでは、すべてのサイトの一般的なインフラ設定を構成する方法について説明します。

> 次の設定には、すべてのサイトに適用されるものと、特定のタイプのサイト（Cloud Network Controller サイトなど）に必要なものとがあります。各サイト固有のサイト ローカル設定に進む前に、インフラ一般設定で必要なすべての設定を完了していることを確認します。

1. Cisco Nexus Dashboard Orchestrator の GUI にログインします。
2. 左のナビゲーション メニューから 、[構成（**Configur**）] > [サイト間接続（**Site To Site Connectivity**）] を選択します。
3. メイン ペインにある [構成（**Configure**）] をクリックします。
4. 左側のサイドバーで、[一般設定（**General Settings**）] を選択します。
5. [コントロール プレーン構成（**Control Plane Configuration**）] を指定します。
   a. [コントロール プレーン構成（**Control Plane Configuration**）] タブを選択します。
   b. [**BGP** ピアリング タイプ（**Bgp Peering Type**）] を選択します。

      - [フルメッシュ（full-mesh）]：各サイトのすべてのボーダー ゲートウェイ スイッチは、リモート サイトのボーダー ゲートウェイ スイッチとのピア接続を確立します。

        [フルメッシュ（full-mesh）] 構成では、Cisco Nexus Dashboard Orchestrator は ACI 管理ファブリックのスパイン スイッチと NDFC 管理ファブリックのボーダー ゲートウェイを使用します。

      - [ルートリフレクタ（route-reflector）]：route-reflector オプションを使用すると、各サイトが MP-BGP EVPN セッションを確立する 1 つ以上のコントロール プレーン ノードを指定できます。ルート リフレクタ ノードを使用すると、NDO によって管理されるすべてのサイト間で MP-BGP EVPN フル メッシュ隣接関係が作成されなくなります。

        ACIファブリックの場合、[ルート リフレクタ（route-reflector）] オプションは、同じ BGP ASN の一部であるファブリックに対してのみ有効です。

   c. [キープアライブ間隔（秒）（**Keepalive Interval**（**Seconds**））] フィールドに、

      キープアライブ間隔を秒単位で入力します。デフォルト値を維持することを推奨し

      ます。

   d. [保留間隔（秒）（**Hold Interval**（**Seconds**））] フィールドに、保留

      間隔を秒単位で入力します。デフォルト値を維持することを推奨します。

   e. [失効間隔（秒）（**Stale Interval**（**Seconds**））] フィールドに、失

      効間隔を秒単位で入力します。デフォルト値を維持することを推奨

      します。

   f. [グレースフル ヘルパー（**Graceful Helper**）] オプションをオンにするかどうかを選択します。
   g. [**AS** 上限（**Maximum AS Limit**）] を入力します。

デフォルト値を維持することを推奨します。

h. **[**ピア間の **BGP TTL**（**BGP TTL Between Peers**）**]** を入力します。
デフォルト値を維持することを推奨します。

i. **[OSPF** エリア **ID**（**OSPF Area ID**）**]** を入力します。

Cloud Network Controller サイトがない場合、このフィールドは UI に表示されません。これは、

オンプレミス IPN ピアリングのためにクラウド サイトで使用される OSPF エリア ID です。

j. (オプション) CloudSec 暗号化の **[IANA** 割り当てポート（**IANA Assigned Port**）**]**を有効にします。

デフォルトでは、CloudSec は独自の UDP ポートを使用します。このオプションを使用すると、サイト間の CloudSec 暗号化に公式の IANA 予約ポート 8017 を使用するように CloudSec を構成できます。

IANA 予約ポートは、リリース 5.2(4) 以降を実行している Cisco APIC サイトでサポートされています。
この設定を変更するには、すべてのサイトで CloudSec を無効にする必要があります。メッセージの添付ファイルを取得する場合は、
IANA 予約ポートを有効にしたいものの、すでに 1 つ以上のサイトで CloudSec 暗号化を有効にしている場合は、いったんすべてのサイトで CloudSec を無効にし、[IANA 予約 UDP ポート（IANA Reserve UDP Port）] オプションを有効にしてから、
必要なサイトで CloudSec を再度有効にします。

CloudSec を構成するための詳細情報と手順については、*『ACI ファブリック用のNexus Dashboard Orchestrator 構成ガイド（Nexus Dashboard Orchestrator Configuration Guide for ACI Fabrics）』*の「CloudSec 暗号化」の章を参照してください。

6. **[IPN** デバイス（**IPN Devices**）**]** 情報を入力します。

オンプレミスとクラウド サイト間のサイト間接続を設定する予定がない場合は、この手順をスキップできます。

後のセクションで説明するように、オンプレミスとクラウド サイト間のサイト アンダーレイ接続を構成する場合は、クラウド CSR への接続を確立するオンプレミス IPN デバイスを選択する必要があります。これらの IPN デバイスは、オンプレミス ファブリックの構成画面で使用可能になる前に、ここで定義する必要があります。詳細は「インフラの構成：オンプレミスのファブリック設定」に記載されています。

a. **[**オンプレミス **IPsec** デバイス（**On Premises IPsec Devices**）**]** タブを選択します。

b. **[+**オンプレミス **IPsec** デバイスを追加（**+Add On-Premises IPsec Device**）**]** をクリックします。

c. デバイスが **[**管理対象外（**Unmanaged**）**]** か **[**管理対象（**Managed**）**]** かを選択し、デバイス

情報を提供します。これは、デバイスが NDFC によって直接管理されるかどうかを定義します。

- **[**管理対象（**Managed**）**]** IPN デバイスには、シンプルにデバイスの **[**名前（**Name**）**]** と **[IP** アドレス（**IP Address**）**]** を入力してください。

  指定した IP アドレスは、IPN デバイスの管理 IP アドレスではなく、クラウド CSR からのトンネル ピア アドレスとして使用されます。

- **[**管理対象（**Managed**）**]** IPN デバイスの場合、デバイスが入っているNDFC の **[**サイト

（**Site**）**]** を選択し、
そのサイトから [デバイス（Device）] を選択します。

次に、インターネットに接続しているデバイスの **[**インターフェイス（**Interface**）**]** を選択し、インターネットに接続しているゲートウェイの IP アドレスである **[**ネクスト ホップ（**Next Hop**）**]** IP アドレスを指定します。

d. チェック マーク アイコンをクリックして、デバイス情報を保存します。
e. 追加する IPN デバイスについて、この手順を繰り返します。

7. **[**外部デバイス（**External Devices**）**]** 情報を入力します。

Cloud Network Controller サイトがない場合、このタブは UI に表示されません。

Multi-Site ドメインに Cloud Network Controller サイトがない場合、またはクラウド サイトとブランチ ルータまたはその他の外部デバイス間の接続を設定する予定がない場合は、この手順をスキップできます。

次の手順では、クラウド サイトからの接続を設定するブランチ ルータまたは外部デバイスに関する情報を指定する方法について説明します。

a. **[**外部デバイス（**External Devices**）**]** タブを選択します。

このタブは、Multi-Site ドメインに少なくとも 1 つのクラウドサイトがある場合にのみ使用できます。

b. **[**外部デバイスの追加（**Add External Device**）**]** をクリックします。

[外部デバイスの追加（**Add External Device**）**]** ダイアログが開きます。

c. デバイスの **[**名前（**Name**）**]**、**[IP** アドレス（**IP Address**）**]**、および **[BGP** 自律システム番号（**BGP Autonomous System Number**）**]** を入力します。

指定した IP アドレスは、デバイスの管理 IP アドレスではなく、Cloud Network Controller の CSR からのトンネル ピア アドレスとして使用されます。接続は、IPSec を使用してパブリック インターネット経由で確立されます。

d. チェック マーク アイコンをクリックして、デバイス情報を保存します。
e. 追加する IPN デバイスについて、この手順を繰り返します。

すべての外部デバイスを追加したら、次の手順を完了して、IPSec トンネル サブネット プールにこれらのトンネルに割り当てられる内部 IP アドレスを指定します。

8. **[IPsec** トンネル サブネット プール（**IPsec Tunnel Subnet Pools**）**]** 情報を入力します。

Cloud Network Controller サイトがない場合、このタブは UI に表示されません。ここで指定できる

サブネットプールには、次の 2 つのタイプがあります。

- **[**外部サブネット プール（**External Subnet Pool**）**]**：クラウド サイトの CSR と他のサイト（クラウドまたはオンプレミス）間の接続に使用されます。

  これらは、Cisco Nexus Dashboard Orchestrator によって管理される大規模なグローバル サブネット プールです。Orchestrator は、これらのプールからより小さなサブネットを作成し、サイト間 IPsec トンネルと外部接続 IPsec トンネルで使用するサイトに割り当てます。

  1 つ以上のクラウド サイトから外部接続を有効にする場合は、少なくとも 1 つの外部サブネット

プールを提供する必要があります。

- **[**サイト固有のサブネット プール（**Site-Specific Subnet Pool**）**]**：クラウド サイトの CSR と外部デバイス間の接続に使用されます。

  これらのサブネットは、外部接続 IPsec トンネルが特定の範囲内にあることが必要な場合に定義できます。たとえば、外部ルータに IP アドレスを割り当てるために特定のサブネットがすでに使用されており、それらのサブネットを NDO およびクラウド ファブリックの IPsec トンネルで引き続き使用する場合です。これらのサブネットは Orchestrator によって管理されず、各サブネットはサイト全体に割り当てられ、外部接続 IPsec トンネルにローカルで使用されます。

  名前付きサブネット プールを指定しない場合でも、クラウド サイトの CSR と外部デバイス間の接続を構成すると、外部サブネット プールが IP 割り当てに使用されます。.

  両方のサブネット プールの最小マスク長は /24 です。

1 つ以上の外部サブネット プール*を追加するには：

a. **[IPsec** トンネル サブネット プール（**IPsec Tunnel Subnet Pools**）**]** タブを選択します。

b. **[**外部サブネット プール（**External Subnet Pool**）**]** エリアで、**[+ IP**アドレスの追加（**+Add IP Address**）**]** をクリックして、1 つ以上の外部サブネット プールを追加します。

   このサブネットは、以前の Cisco Nexus Dashboard Orchestrator リリースでサイト間接続用に Cloud Network Controller で以前に構成した、オンプレミス接続に使用されるクラウド ルータの IPsec トンネル インターフェイスとループバックに対処するために使用されます。

   サブネットは、他のオンプレミス TEP プール と重複してはなりません。
   サブネットには /16 と /24 の間のネットワークが必要で、0.x.x.x または 0.0.x.x で始めることはできません。たとえば、30.29.0.0/16 のようにします。

c. チェックマーク アイコンをクリックして、サブネット情報を保存します。

d. 追加するサブネット プールについて、これらのサブステップを繰り返します。

1 つ以上のサイト固有のサブネット プールを追加するには：

a. **[IsSec** トンネル サブネット プール（**IsSec Tunnel Subnet Pools**）**]** タブを選択します。

b. **[**サイト固有のサブネット プール（**Site-Specific Subnet Pools**）**]** エリアで、**[+ IP** アドレスの追加（**+Add IP Address**）**]** をクリックして、1 つ以上の外部サブネット プールを追加します。

   [名前付きサブネット プールの追加（**Add Named Subnet Pool**）**]** ダイアログが開きます。

c. サブネットの **[**名前（**Name**）**]** を入力します。

   後ほど、サブネットプールの名前を使用して、IP アドレスを割り当てるプールを選択できます。

d. **[+ IP** アドレスの追加（**+ Add IP Address**）**]** をクリックして、1 つ以上のサブネット プールを追加します。

   サブネットには /16 と /24 の間のネットワーク マスクが必要で、0.x.x.x または 0.0.x.x で始めることはできません。たとえば、30.29.0.0/16 のようにします。

e. チェックマーク アイコンをクリックして、サブネット情報を保存します。

   同じ名前付きサブネット プールに複数のサブネットを追加する場合は、この手順を繰り返します。

f. **[**保存（**Save**）**]** をクリックして、名前付きサブネット プールを保存します。
g. 追加する名前付きサブネット プールについて、これらのサブステップを繰り返します。

次に行う作業：

全般的なインフラ設定を構成した後も、管理するサイトのタイプ（ACI、Cloud Network Controller、または NDFC）に基づいて、サイト固有の構成に関する追加情報を指定する必要があります。次の項で説明する手順に従って、サイト固有のインフラストラクチャ設定を行います。

Cisco APIC サイトのインフラの設定

サイト接続性情報の更新

スパインの追加や削除、またはスパイン ノードの ID 変更などのインフラストラクチャへの変更が加えられた場合、Multi-Site ファブリック接続サイトの更新が必要になります。このセクションでは、各サイトの APIC から直接最新の接続性情報を取得する方法を説明します。

1. Cisco Nexus Dashboard Orchestrator の GUI にログインします。
2. 左のナビゲーション メニューから 、**[**構成（**Config**）**] > [**サイト間接続（**Site To Site Connectivity**）**]** を選択します。
3. メイン ペインの右上にある **[**構成（**Configure**）**]** をクリックします。
4. 左側のペインの **[**サイト（**Sites**）**]** の下で、特定のサイトを選択します。
5. メイン ウィンドウで、APIC からファブリック情報を取得するために **[**更新（**Refresh**）**]** ボタンをクリックします。
6. （オプション）オンプレミス サイトの場合、廃止されたスパイン スイッチノードの設定を削除する場合は、**[**確認（**Confirmation**）**]** ダイアログでチェックボックスをオンにします。

   このチェックボックスを有効にすると、現在使用されていないスパイン スイッチのすべての設定情報がデータベースから削除されます。

7. 最後に、**[**はい（**Yes**）**]** をクリックして確認し、接続情報をロードします。

   これにより、新しいスパインや削除されたスパインを検出し、すべてのサイトに関連したファブリックの接続を APIC からインポートし直します。

インフラの設定: オンプレミス サイトの設定

ここでは、オンプレミス サイトにサイト固有のインフラ設定を構成する方法について説明します。

1. Cisco Nexus Dashboard Orchestrator の GUI にログインします。
2. 左のナビゲーション メニューから 、**[**構成（**Configur**）**] > [**サイト間接続（**Site To Site Connectivity**）**]** を選択します。
3. メイン ペインの右上にある **[**構成（**Configure**）**]** をクリックします。
4. 左側のペインの **[**サイト **(Sites)]** の下で、特定のオンプレミス サイトを選択します。
5. **[**詳細の表示（**View Details**）**]** をクリックして、サイト設定をロードします。

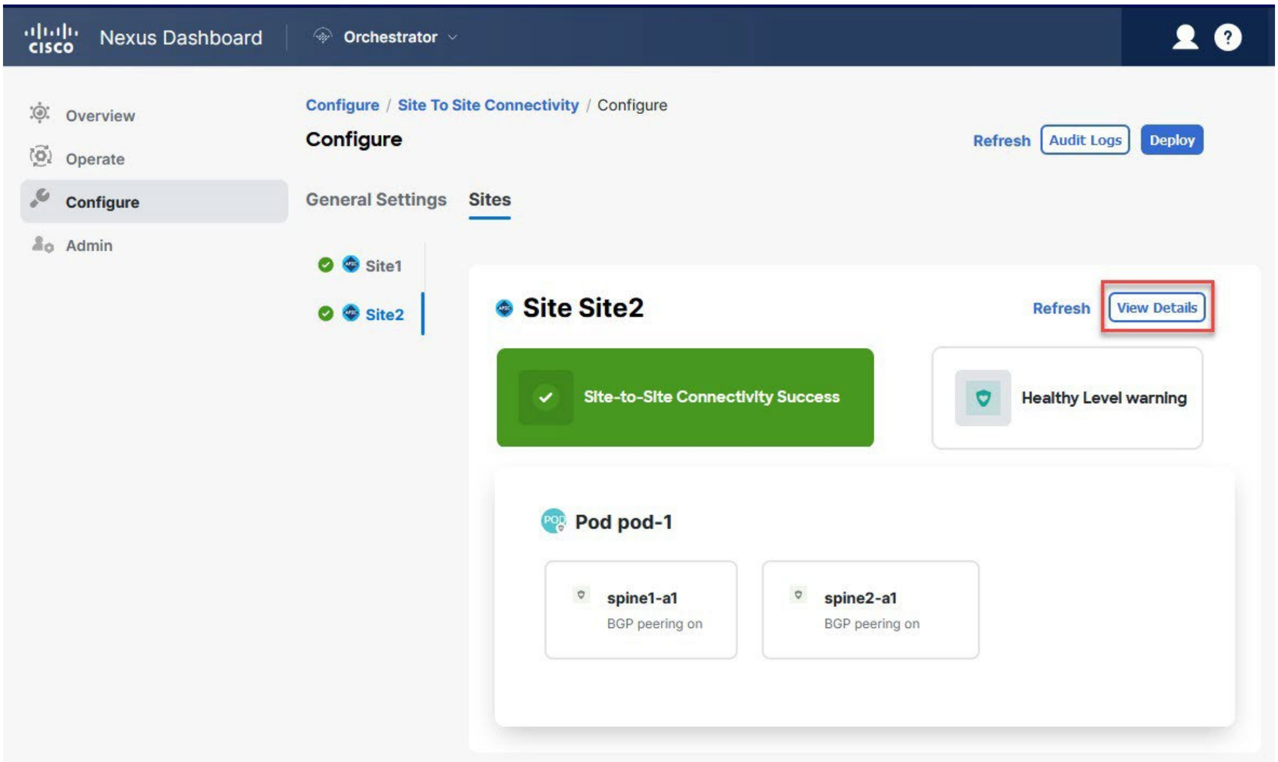


図 4 [構成（Configure）] > [サイト間接続（Site to Site Connectivity）] > [サイト（Site）] > [詳細の表示（View Details）]

6. [サイト間接続（**Inter-Site Connectivity**）] 情報を入力します。

   a. 右側の [**<Site>** 設定（**<Site> Settings**）] ペインで、[マルチサイト（**Multi-Site**）] ノブを有効にします。

      これは、オーバーレイ接続がこのサイトと他のサイト間で確立されるかどうかを定義します。

   b. (オプションｎ) [**CloudSec** 暗号化（**CloudSec Encryption**）] ノブを有効にして、サイトを暗号化します。

      CloudSec 暗号化は、サイト間トラフィックの暗号化機能を提供します。この機能の詳細については、*Cisco Multi-Site Configuration Guide* の「Infrastructure Management」の章を参照してください。

   c. [オーバレイ マルチキャスト **TEP**（**Overlay Multicast TEP**）] を指定します。

      このアドレスは、サイト間の L2 BUM および L3 マルチキャスト トラフィックのために使用されます。この IP アドレスは、単一のポッドまたはマルチポッド ファブリックであるかどうかには関わりなく、同じファブリックの一部であるすべてのスパイン スイッチに展開されます。

      このアドレスは、元のファブリックの [インフラ（infra）] TEP プールのアドレス空間または 0.x.x.x の範囲から取得することはできません。

   d. [**BGP** 自律システム番号（**BGP Autonomous System Number**）] を指定します。

   e. （オプション）[**BGP** パスワード (**BGP Password**)] を指定します。

   f. [**OSPF** エリア **ID**（**OSPF Area ID**）] を入力します。

      サイトと IPN 間のアンダーレイ接続に OSPF プロトコルを使用する場合は、次の設定が必要です。代わりに BGP を使用する場合は、この手順を省略できます。BGP アンダーレイの構成は、「Configuring Infra: Spine Switches」で説明されているように、ポート レベルで行われます。

   g. ドロップダウン リストから、[**OSPF** エリア タイプ（**OSPF Area Type**）] を選択します。サイト

と IPN 間のアンダーレイ接続に OSPF プロトコルを使用する場合は、次の設定が必要です。代わりに BGP を使用する場合は、この手順を省略できます。BGP アンダーレイの構成は、「Configuring Infra: Spine Switches」で説明されているように、ポート レベルで行われます。

OSPF エリアタイプは、次のいずれかになります。

- nssa
- 通常(regular)

h. サイトの OSPF ポリシーを設定します。

サイトと IPN 間のアンダーレイ接続に OSPF プロトコルを使用する場合は、次の設定が必要です。代わりに BGP を使用する場合は、この手順を省略できます。BGP アンダーレイの構成は、「Configuring Infra: Spine Switches」で説明されているように、ポート レベルで行われます。

既存のポリシー（たとえば msc-ospf-policy-default）をクリックして修正することも、[+ポリシー追加（**+Add Policy**）] をクリックして新しい OSPF ポリシーを追加することもできます。それから、[ポリシーの追加/更新（**Add/Update Policy**）] ウィンドウで、以下を指定します。

- [ポリシー名（**Policy Name**）] フィールドにポリシー名を入力します。
- [ネットワーク タイプ（**Network Type**）] フィールドで、[ブロードキャスト（broadcast）]、[ポイントツーポイント（point-to-point）]、または [未指定（unspecified）] のいずれかを選択します。デフォルトは [ブロードキャスト（broadcast）] です。
- [優先順位（**Priority**）] フィールドに、優先順位番号を入力します。デフォルト値は 1 です。
- [インターフェイスのコスト（**Cost of Interface**）] フィールドに、インターフェイスのコストを入力します。デフォルト値は 0 です。
- [インターフェイス制御（**Interface Controls**）] ドロップダウン リストから、以下のいずれかを選択します。
  - サブネットをアドバタイズ**(advertise-subnet)**
  - **BFD**
  - **MTU**を無視**(mtu-ignore)**
  - パッシブパーティシペーション**(passive-participation)**
- [**Hello** 間隔（秒）（**Hello Interval（Seconds）**）] フィールドに、hello 間隔を秒単位で入力しますデフォルト値は 10 です。
- [**Dead** 間隔（秒）（**Dead Interval（Seconds）**）] フィールドに、dead 間隔を秒単位で入力します。デフォルト値は 40 です。
- [再送信間隔（秒）（**Retransmit Interval（Seconds）**）] フィールドに、再送信間隔

を秒単位で入力します。デフォルト値は 5 です。

- [転送遅延（秒）（Transmit Delay（Seconds））] フィールドに、遅延を秒

単位で入力します。デフォルト値は 1 です。

i. （オプション）[外部ルート ドメイン（**External Routed Domain**）] ドロップダウンから、使用するドメインを選択します。

Cisco APIC GUI で作成した外部ルータ ドメインを選択します。詳細については、APIC リリースに特定の『Cisco APIC レイヤ 3 ネットワーク構成ガイド（Cisco APIC Layer 3 Networking Configuration Guide）』 を参照してください。

j. （オプション）サイトの [**SDA** 接続（**SDA Connectivity**）]を有効にします。

サイトが SDA ネットワークに接続されている場合は、[**SDA** 接続（**SDA Connectivity**）] ノブを有効にして、[外部ルーテッド ドメイン（**External Routed Domain**）]、[**VLAN** プール（**VLAN Pool**）]、および [**VRF Lite IP** プール範囲（**VRF Lite IP Pool Range**）] の情報を提供します。

サイトの SDA 接続を有効にする場合は、『*ACI ファブリックの Cisco マルチサイト構成ガイド*』の「SDA 使用例」の章で説明されている追加構成を行う必要があります。

k. （オプション）サイトの [**SR-MPLS** 接続（**SR-MPLS Connectivity**）]を有効にします。

サイトが MPLS ネットワークを介して接続されている場合には、[**SR-MPLS** 接続性（**SR-MPLS Connectivity**）] ノブを有効にして、セグメント ルーティング グローバル ブロック（SRGB）の範囲を指定します。

セグメント ルーティング グローバル ブロック（SRGB）は、ラベル スイッチング データベース（LSD）でセグメント ルーティング（SR）用に予約されているラベル値の範囲です。これらの値は SR 対応ノードへのセグメント識別子（SID）として割り当てられ、ドメイン全体でグローバルな意味を持ちます。

デフォルトの範囲は 16000 ~ 23999 です。

サイトのMPLS接続を有効にする場合は、『*ACI ファブリックの Cisco マルチサイト 構成ガイド*』の「SR-MPLS 経由で接続されたサイト」の章で説明されている追加構成を行う必要があります。

7. オンプレミスとクラウド サイト間のサイト間接続を構成します。

オンプレミス サイトとクラウド サイトの間にサイト間接続を作成する必要がない場合（たとえば、導入にクラウドのみまたはオンプレミス サイトのみが含まれる場合）は、この手順をスキップします。

オンプレミスとクラウド サイト間のアンダーレイ接続を構成する場合は、Cloud Network Controller の CSR がトンネルを確立する IPN デバイスの IP アドレスを指定し、クラウド サイトのインフラ設定を行う必要があります。

a. [**+IPN** デバイスの追加（**+Add IPN Device**）] をクリックして、IPNデバイスを指定します。

b. ドロップダウンから、前に定義した IPN デバイスのいずれかを選択します。

IPN デバイスは、次のリンク で説明さ　れ　ているように、[**General** 設定] > [**IPN Devices**] リストですでに定義されている必要があります。https://www-author3.cisco.com/c/en/us/td/docs/dcn/ndo/4x/articles- 431/nexus-dashboard-orchestrator-aci-preparing-cisco-apic-sites-431.html#_configuring_infra_general_settings_2Configuring Infra: General Settings]。

c. クラウド サイトのサイト間接続を構成します。

クラウド サイトからこのオンプレミス サイトへの以前に構成された接続はすべてここに表示されますが、追加の構成は、「Cisco クラウド ネットワーク コントローラ ファブリックのインフラの構成」の説明に従ってクラウド ファブリック側から行う必要があります。

次に行う作業：

必要なサイト間接続情報をすべて設定しましたが、まだサイトにプッシュされていません。「インフラ 構成の展開」の説明に従って、設定を展開するする必要があります。

インフラの設定: ポッドの設定

このセクションでは、各サイトでポッド固有の設定を行う方法について説明します。

1. Cisco Nexus Dashboard Orchestrator の GUI にログインします。
2. 左のナビゲーション メニューから 、**[**構成（**Configur**）**]** > **[**サイト間接続（**Site To Site Connectivity**）**]** を選択します。
3. メイン ペインの右上にある **[**構成（**Configure**）**]** をクリックします。
4. 左側のペインの **[**サイト（**Sites**）**]** の下で、特定のサイトを選択します。
5. メイン ウィンドウで、ポッドを選択します。
6. 右の **[**ポッドのプロパティ（**Pod Properties**）**]** ペインで、ポッドについてオーバーレイ ユニキャスト TEP を追加できます。

   この IP アドレスは、同じポッドの一部であるすべてのスパイン スイッチに展開され、レイヤ 2 およびレイヤ 3 ユニキャスト通信用の VXLAN カプセル化トラフィックの送信と受信に使用されます。

7. **[+TEP** プールの追加（**+Add TEP Pool**）**]** をクリックして、ルーティング可能な TEP プールを追加します。

   外部ルーティング可能な TEP プールは、IPN 経由でルーティング可能な IP アドレスのセットを APIC ノード、スパイン スイッチ、および境界リーフ ノードに割り当てるために使用されます。これは、マルチサイト アーキテクチャを有効にするために必要です。

   以前に APIC でファブリックに割り当てられた外部 TEP プールは、ファブリックが Multi-Site ドメインに追加されると、NDO によって自動的に継承され、GUI に表示されます。

8. サイトの各ポッドに対してこの手順を繰り返します。

インフラの設定: スパイン スイッチ

このセクションでは、Cisco Multi-Site のために各サイトのスパイン スイッチを設定する方法について説明します。スパイン スイッチを設定する場合、各サイトのスパインと ISN 間の接続を設定することで、Multi-Site ドメイン内のサイト間のアンダーレイ接続を効果的に確立できます。

リリース 3.5(1) より前は、OSPF プロトコルを使用してアンダーレイ接続が確立されていました。一方、このリリースでは、OSPF、BGP（IPv4 のみ）、または混合プロトコルを使用できます。混合とは、一部のサイトではサイト間アンダーレイ接続に OSPF を使用し、一部のサイトでは BGP を使用することです。両方ではなく OSPF または BGP のいずれかを設定することを推奨します。両方のプロトコルを設定した場合には、BGP が優先され、OSPF はルート テーブルにインストールされません。

1. Cisco Nexus Dashboard Orchestrator の GUI にログインします。

2. 左のナビゲーション メニューから 、[構成（Config）] > [サイト間接続（Site To Site Connectivity）] を選択します。
3. メイン ペインの右上にある [構成（Configure）] をクリックします。
4. 左側のペインの [サイト（Sites）] の下で、特定のオンプレミス サイトを選択します。
5. メイン ペインで、ポッド内のスパイン スイッチを選択します。
6. 右側の [<スパイン> 設定 (Settings)] ペインで、[+ ポート追加(Add Port)] をクリックします。
7. [ポートの追加（Add Port）] ウィンドウで、アンダーレイの接続情報を入力します。

   IPN 接続用に APIC で直接構成されているポートがインポートされ、リストに表示されます。NDO から設定する新しいポートについては、次の手順を使用します。

   a. 次の一般情報を指定します。

      - [イーサネット ポート ID（Ethernet Port ID）] フィールドに、ポ

        ート ID、たとえば 1/29 を入力します。これは、IPN への接続に使

        用されるインターフェイスです。

      - [IP アドレス（IP Address）] フィールドに、IP アドレス/ネットマスクを入力します。

        Orchestrator によって、指定された IP アドレスを持ち、指定されたポートを使用する、VLAN 4 のサブインターフェイスが作成されます。

      - [MTU] フィールドに、サーバの MTU を入力します。MTU を 9150B に構成する [継承（inherit）] を指定するか、576 ～ 9000 の値を選択します。

        スパイン ポートの MTU は、IPN 側の MTU と一致させる必要があります。

8. アンダーレイ プロトコルを選択します。

   a. アンダーレイ接続に OSPF プロトコルを使用する場合は、[OSPF] を有効にします。

      代わりに、アンダーレイ接続に BGP プロトコルを使用する場合は、この部分をスキップし、次のサブステップで必要な情報を入力します。

      - [OSPF] を [有効（Enabled）] に設定します。

        OSPF 設定が使用可能になります。

      - [OSPF ポリシー（OSPF Policy）] ドロップダウンで、「インフラの構成：オンプレミス サイト設定」で構成したスイッチの OSPF ポリシーを選択します。

        OSPF ポリシーの OSPF 設定は、IPN 側と一致させる必要があります。

      - [OSPF 認証（OSPF Authentication）] では、[なし（none）] または以下のいずれかを選択します。
        - MD5
        - シンプル
      - [BGP] を [無効（Disabled）] に設定します。

   b. アンダーレイ接続に BGP プロトコルを使用する場合は、[BGP] を有効にします。
      アンダーレイ接続に OSPF プロトコルを使用しており、前のサブステップですでに設定している場

合は、この部分をスキップします。

次の場合、BGP IPv4 アンダーレイはサポートされません。

- マルチサイト ドメインに 1 つ以上の Cloud Network Controller サイトが含まれている場合、オンプレミスからオンプレミス、およびオンプレミスからクラウド サイトの両方のサイト間アンダーレイ接続に OSPF プロトコルを使用する必要があります。
- いずれかのファブリックの WAN 接続に GOLF（ファブリック WAN のレイヤ 3 EVPN サービス）を使用している場合。

上記の場合、スパインに展開された Infra L3Out で OSPF を使用する必要があります。

- **[OSPF]** を [無効（Disabled）] に設定します。

  両方ではなく OSPF または BGP のいずれかを設定することを推奨します。両方のプロトコルを設定した場合には、BGP が優先され、OSPF はルート テーブルにインストールされません。ISN デバイスとの EBGP 隣接関係だけがサポートされるからです。

- **[BGP]** を [有効（Enabled）] に設定します。

  BGP 設定が使用可能になります。

- [ピア **IP**（**Peer IP**）] フィールドに、このポートの BGP ネイバーの IP ア

  ドレスを入力します。BGP アンダーレイ接続では、IPv4 IP アドレスのみ

  がサポートされます。

- [ピア **AS** 番号（**Peer AS Number**）] フィールドに、BGP ネイバーの自律システム（AS）番号を入力します。

  このリリースでは、ISN デバイスとの EBGP 隣接関係のみがサポートされます。

- **[BGP** パスワード（**BGP Password**）] フィールドに、BGP ピア パスワードを入力します。
- 必要に応じて追加のオプションを指定します。
  - [双方向フォワーディング検出（Bidirectional Forwarding Detection）]：双方向フォワーディング検出（BFD）プロトコルを有効にして、このポートと IPN デバイスの物理リンクの障害を検出します。
  - [管理状態（Admin State）]：ポートの管理状態を有効に設定します。

9. IPN に接続するすべてのスパイン スイッチおよびポートに対してこの手順を繰り返します。

Cisco Cloud Network Controller サイトのインフラの構成

クラウド サイト接続性情報の更新

CSR やリージョンの追加や削除などのインフラストラクチャの変更には、Multi-Site ファブリック接続サイトの更新が必要です。このセクションでは、各サイトの APIC から直接最新の接続性情報を取得する方法を説明します。

1. Cisco Nexus Dashboard Orchestrator の GUI にログインします。
2. 左のナビゲーション メニューから 、[構成（**Config**）**] > [**サイト間接続（**Site To Site Connectivity**）] を選択します。
3. メイン ペインの右上にある **[**構成（**Configure**）**]** をクリックします。
4. 左側のペインの [サイト（**Sites**）**]** の下で、特定のサイトを選択します。
5. メイン ウィンドウで **[**更新（**Refresh**）**]** ボタンをクリックして、新規または変更された CSR およびリージョンを検出します。
6. 最後に、**[**はい（**Yes**）**]** をクリックして確認し、接続情報をロード

   します。これにより、新規または削除された CSR およびリージョン

   が検出されます。

7. **[**展開（**Deploy**）**]** をクリックして、クラウドサイトの変更を、接続している他のサイトに伝達します。

   クラウド サイトの接続を更新し、CSR またはリージョンが追加または削除された後、インフラ構成を展開して、そのクラウド サイトへのアンダーレイ接続がある他のサイトが更新された構成を取得する必要があります。

インフラの設定**:** クラウド サイトの設定

ここでは、Cloud Network Controller サイト固有のインフラ設定を構成する方法について説明します。

1. Cisco Nexus Dashboard Orchestrator の GUI にログインします。
2. 左のナビゲーション メニューから 、**[**構成（**Config**）**] > [**サイト間接続（**Site To Site Connectivity**）**]** を選択します。
3. メイン ペインの右上にある **[**構成（**Configure**）**]** をクリックします。
4. 左側のペインの [サイト **(Sites)]** の下で、特定のクラウド サイトを選択します。
5. **[**詳細の表示（**View Details**）**]** をクリックして、サイト設定をロードします。

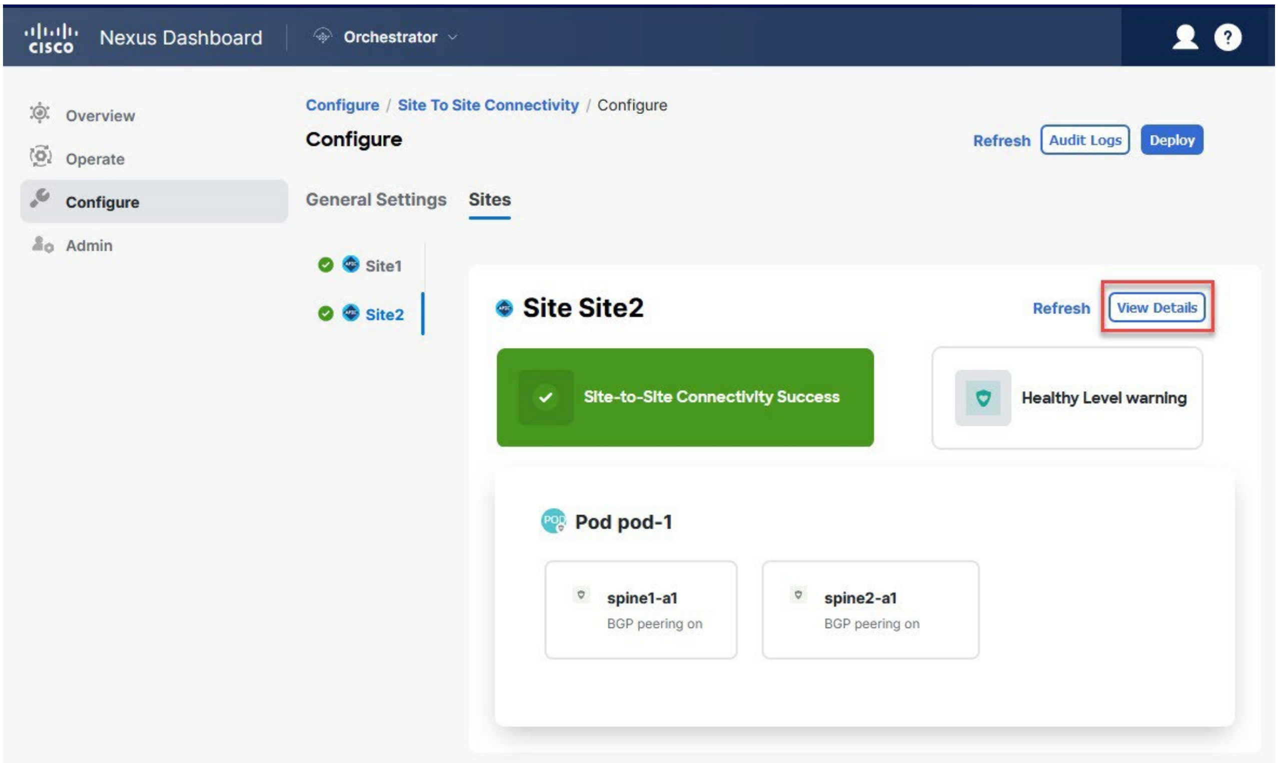


図 5 [構成（Configure）] > [サイト間接続（Site to Site Connectivity）] > [サイト（Site）] > [詳細の表示（View Details）]

6. [サイト間接続（**Inter-Site Connectivity**）] 情報を入力します。

   a. 右側の **[<Site>** 設定（**<Site> Settings**）**]** ペインで、**[**サイト間接続（**Inter-Site Connectivity**）**]** タブを選択します。

   b. [マルチサイト（**Multi-Site**）] ノブを有効にします。

   これは、オーバーレイ接続がこのサイトと他のサイト間で確立されるかどうかを定義します。

   オーバーレイ構成は、次の手順で説明するようにアンダーレイ サイト間接続が確立されていないサイトにはプッシュされません。

   c. （オプション）**[BGP** パスワード **(BGP Password)]** を指定します。

7. サイト固有の [サイト間接続（**Inter-Site Connectivity**）**]** 情報を入力します。

   a. クラウド サイトの右側のプロパティ サイドバーで、[サイトの追

   加（**Add Site**）] をクリックします。[サイトの追加（**Add**

   Site）**]** ウィンドウが表示されます。

   b. **[**サイトへの接続（**Connected to Site**）**]** で、**[**サイトの選択（**Select a Site**）**]** をクリックし、構成しているサイト (たとえば、[Site1]) からの接続を確立するサイト (たとえば、[Site2]) を選択します。

   リモート サイトを選択すると、[サイトの追加（**Add Site**）**]** ウィンドウが更新され、両方向の接続、つまり [Site1] > [Site2] および **[Site1]** > **[Site2]** が反映されます。

   c. **[Site1]** > **[Site2]** エリアで、**[**接続タイプ（**Connection Type**）**]** ドロップダウンから、サイト間の接続のタイプを選択します。

   次のオプションを使用できます。

- [パブリック インターネット（Public Internet）]：2 つのサイト間の接続は、インターネットを介して確立されます。

  このタイプは、任意の 2 つのクラウド サイト間、またはクラウド サイトとオンプレミス サイト間でサポートされます。
- [プライベート接続（Private Connection）]：2 つのサイト間のプライベート接続を使用して接続が確立されます。

  このタイプは、クラウド サイトとオンプレミス サイトの間でサポートされます。

- [クラウド バックボーン（Cloud Backbone）]`：クラウド バックボーンを使用して接続が確立されます。

  このタイプは、Azure-to-AzureやAWS-to-AWSなど、同じタイプの 2 つのクラウド サイト間でサポートされます。

複数のタイプのサイト（オンプレミス、AWS、Azure）がある場合、サイトの異なるペアは異なる接続タイプを使用できます。

d. これら 2 つのサイト間の接続に使用する [プロトコル（**Protocol**）] を選択します。

BGP-EVPN 接続を使用している場合は、オプションで **IPSec** を有効にして、使用する Internet Key Exchange (IKE) プロトコルのバージョンを選択できます。構成に応じて、IKEv1（バージョン 1）または IKEv2 (バージョン 1) です。

- [パブリック インターネット（Public Internet）] 接続の場合、IPsec は常に有効です。
- [クラウド バックボーン（Cloud Backbone）] 接続の場合、IPsec は常に無効です。
- プライベート接続の場合、IPsec は有効または無効にすることができます。

代わりに **BGP-IPv4** 接続を使用する場合は、構成しているクラウド サイトからのルート リーク構成に使用される外部 VRF を提供する必要があります。

[Site1] > [Site2] の接続情報が提供された後、**[Site2] > [Site1]** エリアは、反対方向の接続情報を反映します。

e. **[**保存（**Save**）**]** をクリックして、サイト間の接続構成を保存します。

[Site1] から [Site2] への接続情報を保存すると、[Site2] から [Site1] へのリバース接続が自動的に作成されます。これは、他のサイトを選択し、右側のサイドバーにある [サイト間接続（**Inter-site Connectivity**）] 情報を選択することで確認できます。

f. 他のサイトのサイト間接続を追加するには、この手順を繰り返します。

[Site1] から [Site2] へのアンダーレイ接続を確立すると、リバース接続が自動的に行われます。

ただし、[Site1] から [Site3] へのサイト間接続も確立する場合は、そのサイトに対してもこの手順を繰り返す必要があります。

8. [外部接続（**External Connectivity**）] 情報を入力します。

NDO によって管理されていない外部サイトまたはデバイスへの接続を設定する予定がない場合は、この手順をスキップできます。

外部接続のユース ケースの詳細な説明は、 *「Nexus Dashboard Orchestrator を使用したクラウド CSR からの外部接続の設定」 ドキュメントで入手できます。*

a. 右側の [<Site> 設定（<Site> Settings）] ペインで、[外部接続（External Connectivity）] タブを選択します。

b. [外部接続の追加（Add External Connectivity）] をクリックします。
   [外部接続の追加（Add External Connectivity）] ダイアログが開きます。

c. [VRF] ドロップダウンから、外部接続に使用する VRF を選択します。

   これは、クラウド ルートをリークするために使用される VRF です。[リージョン（Regions）] セクションには、この構成を適用する CSR を含むクラウド リージョンが表示されます。

d. [外部デバイス（External Devices）] セクションの [名前（Name）] ドロップダウンから、外部デバイスを選択します。

   これは、一般的なインフラストラクチャ構成時に [一般設定（General Settings）] > [外部デバイス（External Devices）] リストに追加した外部デバイスであり、 インフラ の構成：一般設定（Configuring Infra: General Settings）

e. [トンネル IKE バージョン (Tunnel IKE Version)] ドロップダウンから、クラウド サイトの CSR と外部デバイス間の IPSec トンネルの確立に使用する IKE バージョンを選択します。

f. （オプション）[トンネル サブネット プール（Tunnel Subnet Pool）] ドロップダウンから、名前付きサブネット プールのいずれかを選択します。

   名前付きサブネット プールは、クラウド サイトの CSR と外部デバイス間の IPSec トンネルに IP アドレスを割り当てるために使用されます。ここで 名前付き サブネット プールを指定しない場合、外部 サブネット プールが IP 割り当てに使用されます。

   外部デバイス接続用の専用サブネット プールを提供することは、特定のサブネットがすでに外部ルータに IP アドレスを割り当てるために使用されています。それらのサブネットを NDO およびクラウド サイトの IPSec トンネルに引き続き使用する場合に役立ちます。

   この接続に特定のサブネット プールを提供する場合は、[インフラの構成：一般設定（Configuring Infra: General Settings）] の手順に従ってあらかじめ作成しておく必要があります。

g. （オプション）[事前共有キー（Pre-Shared Key）] フィールドに、トンネルの確立に使用するカスタム キーを入力します。

h. 必要に応じて、同じ外部接続（同じ VRF ）に対して追加する外部デバイスについて、前のサブステップを繰り返します。

i. 必要に応じて、追加の外部接続（異なる VRF ）に対してこの手順を繰り返します。

   CSR と外部デバイス間のトンネルエンドポイントには 1 対 1 の関係があるため、異なる VRF を使用して追加の外部接続を作成できますが、同じ外部デバイスに追加の接続を作成することはできません。

次に行う作業：

必要なサイト間接続情報をすべて設定しましたが、まだサイトにプッシュされていません。「インフラ 構成の展開」の説明に従って、構成を展開するする必要があります。

Cloud Network Controller サイトのダウンタイムからの回復

クラウド ネットワーク コントローラ（以前の Cloud APIC）インスタンス/VM が NDO によって管理され

ているときに何らかの理由でダウンすると、そのクラウド サイトに関連付けられている既存のテンプレートを展開解除または削除できない場合があります。この場合、NDO でサイトを強制的に管理解除しようとすると、サイトが回復した場合でも、古い構成および展開エラーが発生する可能性があります。

この状態から回復するには：

1. 新しいクラウド ネットワーク コントローラ サイトを起動し、クラウド サイトを再登録します。

    a. NDOにログインします。

    b. 管理コンソールを開きます。

    c. **[**操作（**Operate**）**] > [**サイト（**Sites**）**]** ページに移動します。

    d. 再展開したサイトの隣にあるアクション **[(...)]** メニューから、**[**サイトの編集（**Edit Site**）**]**を選択します。

    e. [サイトを再登録する（Reregister site）] チェックボックスをチェックします。

    f. 新しいサイトの詳細を提供します。

        サイトの新しいパブリック IP アドレスとサインイン資格情報を提供する必要があります。

    g. *[保存（Save）]* をクリックして、サイトを再登録します。

    サイトの接続ステータスが UP と表示されると、NDO のサイト IP も更新され、新しいサイトは「管理」状態になります。

2. スキーマごとに以前に展開されたテンプレートを展開解除します。

    a. NDOにログインします。

    b. **[**構成（**Configure**）**]** に移動し、**[**テナント テンプレート（**Tenant Template**）**] > [**アプリケーション（**Applications**）**]** を選択します。

    c. テンプレートが展開されているスキーマをクリックします。

    d. **[**テンプレート プロパティ（**Template Properties**）**]** の横にある **[**アクション（**Actions**）**]** メニューから、**[**テンプレートの展開解除（**Undeploy Template**）**]** を選択し、テンプレートが正常に展開解除されるまで待ちます。

3. サイトのインフラ構成を更新して、新しい Cisco Catalyst 8000V スイッチが NDO に追加されるようにします。

    a. **[**構成（**Configure**）**]** に移動して **[**サイト間接続（**Site To Site Connectivity**）**]** を選択します。

    b. 画面右上の **[**構成（**Configure**）**]** をクリックします。

    c. **[**サイト（**Sites**）**]** パネルでクラウド サイトを選択し、**[**更新（**Refresh**）**]** をクリックします。

    d. 画面の右上にある **[**展開（**Deploy**）**]** をクリックし、すべてのサイトが正常に展開されるまで待ちます。

4. このクラウド ネットワーク コントローラ サイトに関連付けられているすべてのテンプレートを再展開します。

    a. **[**アプリケーション（**Applications**）**]** タブで **[**構成（**Configure**）**] > [**テナント テンプレート（**Tenant Templates**）**]** に移動します。

    b. 以前に展開されていないテンプレートを使用してスキーマをクリックします。

    c. **[**サイトに展開（**Deploy to Sites**）**]** をクリックし、テンプレートが展開されるまで待ちます。

ACI サイト向けのインフラ設定の展開

インフラ設定の展開

ここでは、各 APIC サイトにインフラ設定を展開する方法について説明します。

1. メイン ペインの右上にある**[展開（Deploy）]** をクリックして、構成を展開します。

   オンプレミスまたはクラウドサイトのみを設定した場合は、**[展開 (Deploy)]** をクリックしてインフラ設定を展開します。

   ただし、オンプレミスとクラウド サイトの両方がある場合は、次の追加オプションを使用できます。

   - [展開 & IPN デバイス構成ファイルをダウンロード（Deploy & Download IPN Device config files）]：オンプレミスの **APIC** サイトとクラウド ネットワーク コントローラ サイトの両方に構成をプッシュし、オンプレミスとクラウド サイト間のエンドツーエンド インターコネクトを有効にします。

     さらに、このオプションでは、IPN デバイスから Cisco クラウド サービス ルータ（CSR）への接続できるようにするための設定情報を含む zip ファイルをダウンロードします。すべてまたは一部の設定ファイルのどちらをダウンロードするかを選択できるようにするための、フォローアップ画面が表示されます。

   - **[展開 & IPN** デバイス構成定ファイルをダウンロード **(Deploy & Download IPN Device config files):]** 両方の Cloud Network Controller サイトに構成をプッシュし、クラウド サイトと外部デバイス間のエンドツーエンド インターコネクトを有効にします。

     さらに、このオプションでは、外部デバイスから、自分のクラウドサイトに展開された Cisco クラウド サービス ルータ（CSR）へ接続できるようにするための、設定情報を含む zip ファイルをダウンロードします。すべてまたは一部の設定ファイルのどちらをダウンロードするかを選択できるようにするための、フォローアップ画面が表示されます。

   - [IPN デバイス設定ファイルのみをダウンロード (Download IPN Device config files only):] 構成情報を含む **zip** ファイルをダウンロードします。これは、**IPN** デバイスから **Cisco Cloud Services Router**（**CSR**）への接続を、構成を展開することなく可能にするために用いるものです。
   - [外部デバイス設定ファイルのみをダウンロード (Download External Device config files only):] 構成情報を含む **zip** ファイルをダウンロードします。これは、外部デバイスから **Cisco Cloud Services Router**（**CSR**）への接続を、構成を展開することなく可能にするために用いるものです。

2. 確認ウィンドウで **[**はい **(Yes)]** をクリックします。

   [展開が開始されました。個々のサイトの展開ステータスメッセージについては、左側のメニューを参照してください（Deployment started, refer to left menu for individual site deployment status）] というメッセージにより、インフラ構成の展開が開始されたことが示されます。左側のペインのサイト名の横に表示されるアイコンで、各サイトの進行状況を確認できます。

次に行う作業：

インフラ オーバーレイとアンダーレイの構成設定が、すべてのサイトのコントローラとクラウド CSR に展開されます。残った最後の手順では、「ファブリック接続情報の更新」で説明するように、IPN デバイスをクラウド CSR のトンネルを使用して設定します。

オンプレミスとクラウド サイト間の接続の有効化

オンプレミス サイトまたはクラウド サイトのみがある場合は、このセクションをスキップできます。

ここでは、オンプレミス APIC サイトと Cloud Network Controller サイト間の接続を有効にする方法について説明します。

デフォルトでは、Cisco Cloud Network Controller は冗長 Cisco Cloud サービス ルータ 1000v のペアを展開します。この項の手順では、2つのトンネルを作成します。1つはオンプレミスの IPsec デバイスからこれらの各 Cisco Cloud サービス ルータ 1000v 対する IPsec トンネルです。複数のオンプレミス IPsec デバイスがある場合は、各オンプレミスデバイスの CSR に同じトンネルを設定する必要があります。

次の情報は、オンプレミスの IPsec ターミネーション デバイスとして Cisco Cloud サービス ルータ 1000v のコマンドを提供します。別のデバイスまたはプラットフォームを使用している場合は、同様のコマンドを使用します。

1. クラウド サイトに導入された CSR とオンプレミスの IPsec ターミネーション デバイスとの間の接続を有効にするために必要な必要な情報を収集します。

   「Deploying Infra Configuration」の手順の一部として、Nexus Dashboard Orchestrator の **[IPN** デバイス設定ファイルの展開とダウンロード **(Deploy&Download IPN Device config files)]** オプションまたは **[IPN** デバイス設定ファイルのダウンロード **(IPN Device config files only)]** オプションを使用して、必要な設定の詳細を取得できます。

2. オンプレミスの IPsec デバイスにログインします。
3. *最初_の* CSR のトンネルを構成します。

   最初の CSR の詳細は、Nexus Dashboard Orchestrator からダウンロードした ISN デバイスのコンフィギュレーションファイルで確認できますが、次のフィールドには、特定の展開の重要な値が示されます。

   - *<first-csr-tunnel-ID>*：このトンネルに割り当てる一意のトンネル ID です。
   - *<first-csr-ip-address>*：最初の CSR の 3 番目のネットワーク インターフェイスのパブリ

     ック IP アドレスです。トンネルの宛先は、アンダーレイ接続のタイプによって異なります。

     - アンダーレイがパブリック インターネット経由の場合、トンネルの宛先はクラウド ルータ インターフェイスのパブリック IP です。
     - アンダーレイがプライベート接続（AWS の DX や Azure の ER など）を介している場合、トンネルの宛先はクラウド ルータ インターフェイスのプライベート IP です。
   - *<first-csr-preshared-key>*：最初の CSR の事前共有キーです。
   - *<onprem-device-interface>* は、Amazon Web Services に展開された Cisco Cloud サービス ルータ 1000v への接続に使用されるインターフェイスです。
   - *<onprem-device-ip-address>* は、Amazon Web Services に展開された Cisco Cloud サービス ルータ 1000v への接続に使用される *<interface>* インターフェイスです。
   - *<peer-tunnel-for-onprem-IPsec-to-first-CSR>*：最初のクラウド CSR に対してオンプレミスの IPsec デバイスのピア トンネル IP アドレスとして使用されます。
   - *<process-id>* ：OSPF プロセス ID です。

- *<area-id>*：OSPF エリア ID です。

次の例は、Nexus Dashboard Orchestrator リリース 3.3(1) および Cloud Network Controller リリース 5.2(1) 以降でサポートされている IKEv2 プロトコルを使用したサイト間接続設定を示しています。IKEv1 を使用している場合は、NDO からダウンロードした IPN 設定ファイルの外観が若干異なる場合がありますが、原則は同じです。

+

```
crypto ikev2 proposal ikev2-proposal-default encryption
    aes-cbc-256 aes-cbc-192 aes-cbc-128 integrity
    sha512 sha384 sha256 sha1
    group 24 21 20 19 16 15 14 2
exit

crypto ikev2 policy ikev2-policy-default
    proposal ikev2-proposal-default
exit

crypto ikev2 keyring key-ikev2-infra:overlay-1- <first-csr-tunnel-id>_____
    peer peer-ikev2-keyring
        address  <first-csr-ip-address>_____
        pre-shared-key  <first-csr-preshared-key>_____
    exit
exit

crypto ikev2 profile ikev2-infra:overlay-1- <first-csr-tunnel-id>_____
    match address local interface <onprem-device-interface>_____
    match identity remote address  <first-csr-ip-address> _____255.255.255.255
    identity local address  <onprem-device-ip-address>_____
    authentication remote pre-share
    authentication local pre-share
    keyring local key-ikev2-infra:overlay-1- <first-csr-tunnel-id>_____
    lifetime 3600
    dpd 10 5 on-demand
exit

crypto ipsec transform-set infra:overlay-1- <first-csr-tunnel-id>_____esp-gcm 256
    mode tunnel
exit

crypto ipsec profile infra:overlay-1- <first-csr-tunnel-id>_____
    set pfs group14
    set ikev2-profile ikev2-infra:overlay-1- <first-csr-tunnel-id>_____
    set transform-set infra:overlay-1- <first-csr-tunnel-id>_____
exit
```

```
interface tunnel 2001
    ip address <peer-tunnel-for-onprem-IPsec-to-first-CSR> 255.255.255.252 ip
    virtual-reassembly
    tunnel source  <onprem-device-interface>_____
    tunnel destination <first-csr-ip-address>_____
    tunnel mode ipsec ipv4
    tunnel protection ipsec profile infra:overlay-1- <first-csr-tunnel-id>_____
    ip mtu 1400
    ip tcp adjust-mss 1400
    ip ospf  <process-id>_____area <area-id>_____
    no shut
exit
```

+

```
crypto ikev2 proposal ikev2-proposal-default encryption aes-
    cbc-256 aes-cbc-192 aes-cbc-128 integrity sha512
    sha384 sha256 sha1
    group 24 21 20 19 16 15 14 2
exit

crypto ikev2 policy ikev2-policy-default proposal
    ikev2-proposal-default
exit

crypto ikev2 keyring key-ikev2-infra:overlay-1-2001 peer
    peer-ikev2-keyring
        address 52.12.232.0
        pre-shared-key 1449047253219022866513892194096727146110
    exit
と入力
し、終
了しま
す。

crypto ikev2 profile ikev2-infra:overlay-1-2001
    ! Please change GigabitEthernet1 to the appropriate interface match
    address local interface GigabitEthernet1
    match identity remote address 52.12.232.0 255.255.255.255 identity local
    address 128.107.72.62
    authentication remote pre-share authentication
    local pre-share
    keyring local key-ikev2-infra:overlay-1-2001
    lifetime 3600
    dpd 10 5 on-demand exit
```

```
crypto ipsec transform-set infra:overlay-1-2001 esp-gcm 256 mode
    tunnel
exit

crypto ipsec profile infra:overlay-1-2001 set
    pfs group14
    set ikev2-profile ikev2-infra:overlay-1-2001
    set transform-set infra:overlay-1-2001
exit

! これらのトンネルインターフェイスは、オンプレミスデバイスとクラウドルータ間のポイン
トツーポイント接続を確立します
! トンネルの宛先は、アンダーレイ接続のタイプによって異なります。
! 1）アンダーレイがインターネット経由の場合、トンネルの接続先はクラウド ルータ インタ
ーフェイスのパブリック IP です。
! 2）アンダーレイがプライベート経由の場合、トンネルの接続先はクラウド ルータ インター
フェイスのプライベート IP です。
     AWS 上の DX やAWS 上の ER などの接続

interface tunnel 2001
    ip address 5.5.1.26 255.255.255.252
    ip virtual-reassembly
    ! GigabitEthernet1を適切なインターフェイス トンネルの送信元
    GigabitEthernet1 に変更してください
    tunnel destination 52.12.232.0
    tunnel mode ipsec ipv4
    tunnel protection ipsec profile infra:overlay-1-2001 ip
    mtu 1400
    ip tcp adjust-mss 1400
    ! Please update process ID according with your configuration ip
    ospf 1 area 0.0.0.1
    no shut
exit
```

4. 2 番目、および設定する必要があるその他の CSR について、これらの手順を繰り返します。
5. オンプレミスの IPsec デバイスでトンネルがアップしていることを確認します。

   現在のステータスを表示するには、次のコマンドを使用します。両方のトンネルがアップとして表示されていない場合は、この項の手順で入力した情報を確認して、問題が発生している可能性がある場所を確認します。両方のトンネルがアップとして表示されるまで、次のセクションに進まないでください。

```
ISN_CSR# show ip interface brief | include Tunnel
Interface              IP-Address      OK? Method Status              Protocol
```

```
Tunnel1000          30.29.1.2      YES manual up                 *up*
Tunnel1001          30.29.1.4      YES manual up                 *up*
```

サイトのアップグレード

概要

> この機能は、Cisco APIC サイトでのみサポートされます。Cisco クラウド ネットワーク コントローラ または Cisco NDFC ファブリックではサポートされていません。

Cisco マルチサイトを導入する際に、各サイトの APIC クラスタおよびスイッチ ノード ソフトウェアをサイト レベルで個別に管理する必要がありました。Multi-Site ドメイン内のサイトの数が増えると、リリースのライフ サイクルとアップグレードは、リリースと機能の互換性のために手動で調整および管理する必要があるため、複雑になる可能性があります。

Cisco Nexus ダッシュボード オーケストレータは、すべてのサイトのソフトウェア アップグレードを単一のポイントから管理できるワークフローを提供します。複数のサイト管理者がソフトウェア アップグレードを手動で調整する必要がなく、アップグレードに影響する可能性のある、潜在的な問題を把握できます。

[管理（Admin）] > [ソフトウェア管理（**Software Management**）**]** に移動して、サイトのアップグレード画面にアクセスできます。このページには 4 つのタブがあります。このセクションと次のセクションで説明します。

[概要（Overview）] タブには、Multi-Site ドメイン内のサイトと、展開されている、または展開の準備ができているファームウェア バージョンに関する情報が表示されます。[サイト ファームウェア（Sites Firmware）] サービスは、5 分ごとにサイトをポーリングして、アップグレード ポリシーの最新のステータスなどの新しいデータまたは変更されたデータを探します。メイン ペインの右上隅にある **[**更新（**Refresh**）**]** ボタンをクリックすると、手動で更新をトリガーできます。

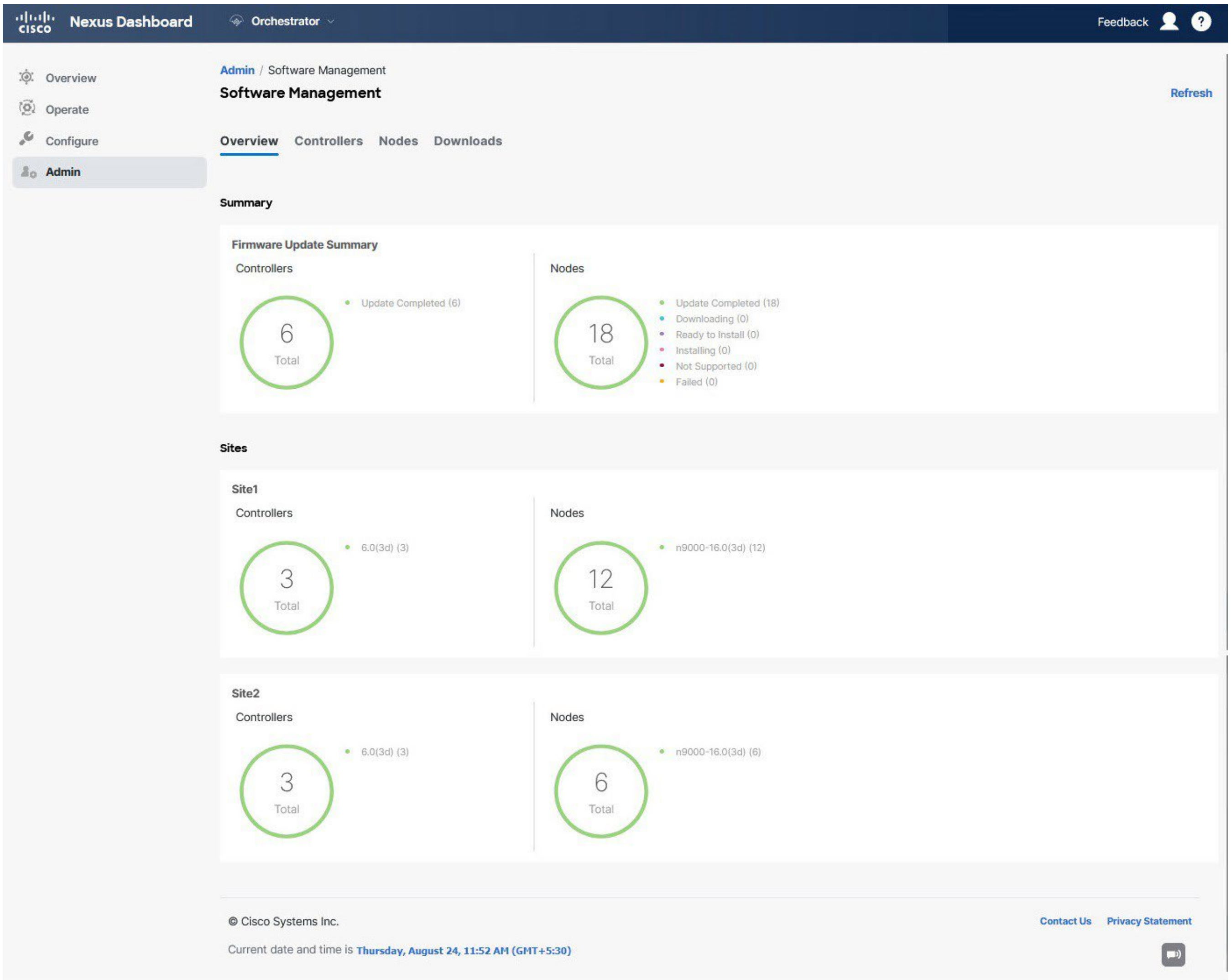


図 6 サイトのファームウェアの概要

ページは次の 3 つの領域に分かれています。

- [ファームウェア アップデートの概要（**Firmware Update Summary**）]：Cisco APIC およびスイッチ ファームウェアを含む、マルチサイト ドメイン内のすべてのサイトに存在するファームウェア イメージの全体的な概要を提供します。

  イメージのタイプごとに、各状態のイメージ数を含む、固有の情報が表示されます。

  - 完了（Completed）：イメージは現在、コントローラまたはスイッチに展開されています。
  - ダウンロード中（Downloading）（スイッチノードのみ）：イメージはスイッチ ノードにダウンロード中です。
  - インストールの準備完了（Ready to Install）（スイッチノードのみ）：イメージはスイッチノードに正常にダウンロードされ、インストールの準備ができています。
  - インストール中（Installing）：コントローラまたはスイッチノードに現在イメージを展開中です。
  - 未サポート（Not Supported）：リリース 4.2(5) より前のリリースなど、リモート ファームウェア アップグレードをサポートしていないイメージ。

- [サイト固有の情報（**Site-specific information**）]：ページの追加のセクションには、個々のサイトに関する情報が表示されます。これには、現在展開されているソフトウェアのバージョンと、コントローラまたはノードの数が含まれます。

注意事項と制約事項

Cisco Nexus Dashboard Orchestrator からファブリック アップグレードを実行する場合、次の制限が適用されます。

- 「Upgrade and Downgrading the Cisco APIC and Switch Software」（『Cisco APIC *Installation*、*Upgrade*、*and Downgrade Guide*』）に記載されている Cisco APIC アップグレード プロセスに固有のガイドライン、推奨事項、および制限事項を確認し、それに従う必要が あります。
- Cisco Nexus Dashboard Orchestrator を Cisco Nexus Dashboard に展開する必要があります。

  サイトのアップグレード機能は、VMware ESXのNDO導入では使用できません。また、『*Cisco APIC インストール、アップグレード、 ダウングレード ガイド*』に記載されている標準のアップグレード手順に従う必要があります。

- ファブリックは、Cisco APIC リリース 4.2(5) 以降を実行している必要があります。

  以前の APIC リリースを実行しているファブリックは、アップグレード ワークフロー中に選択できません。『*Cisco APIC Installation, Upgrade, and Downgrade Guide* 』*に記載されている標準のアップグレード手順に従います*。

- サイトのアップグレードは、これらのファブリックを管理するサイト管理者と調整することを推奨します。潜在的な問題が発生した場合は、トラブルシューティングのためにコントローラまたはスイッチ ノードにアクセスする必要があります。
- アップグレード プロセスの途中でファブリック スイッチ ノードが非アクティブ（inactive）状態になった場合（たとえば、ハードウェアまたは電源障害）、プロセスは完了できません。この間、ノード アップグレード ポリシーを削除または変更することはできません。これは、NDO がノードがダウンしたか、または単にアップグレードのリブート中かを区別できないためです。

  この問題を解決するには、非アクティブ ノードを APIC から手動でデコミッションする必要があります。この時点で、NDO アップグレード ポリシーは変更を認識し、失敗（failed）ステータスを返します。その後、NDO のアップグレード ポリシーを更新してスイッチを削除し、アップグレードを再実行できます。

コントローラとスイッチ ノードのファームウェアをサイトにダウンロードする

アップグレードを実行する前に、コントローラとスイッチ ソフトウェアをファブリック内のすべてのサイト コントローラにダウンロードする必要があります。次の手順を完了すると、後でダウンロードしたイメージを使用してアップグレード プロセスを開始できます。

1. Cisco Nexus Dashboard Orchestrator にログインします。
2. ファームウェア ダウンロードをセットアップします。

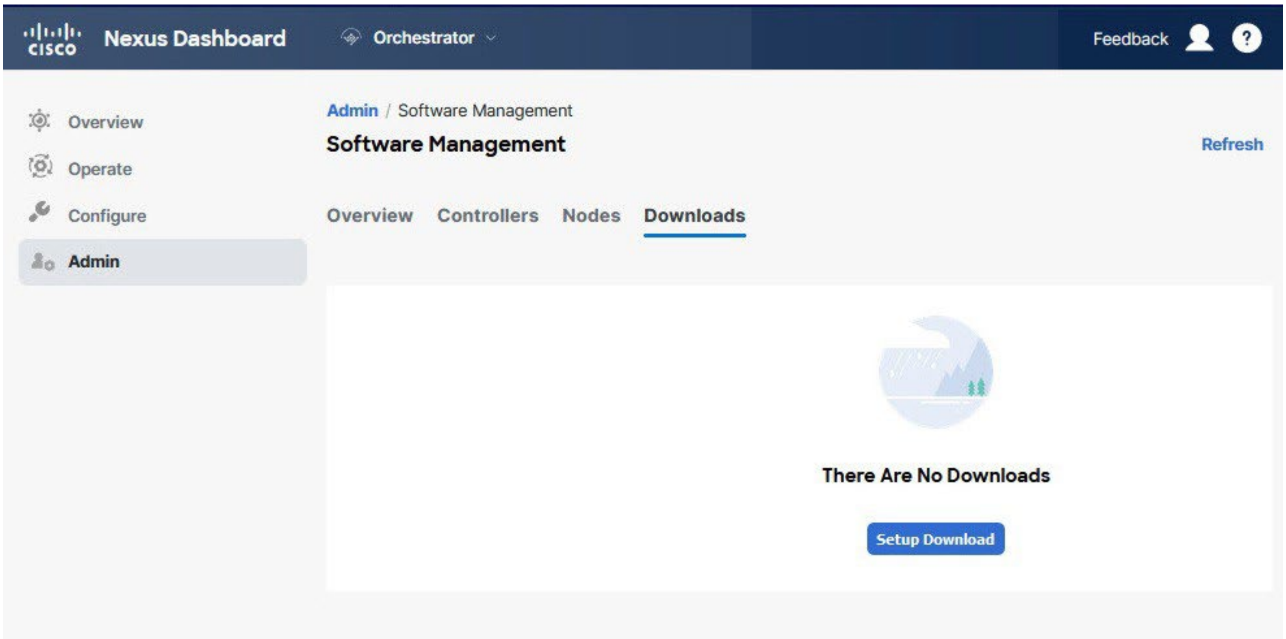


図 7 サイト ファームウェア更新

a. 左のナビゲーション ペインから [管理（**Admin**）] > [ソフトウェア管理（**Software Management**）] を選択します。

b. メイン ウィンドウで [ダウンロード（**Downloads**）] タブを選択します。

c. [ダウンロードのセットアップ（**Setup Downloads**）] タブをクリックします。

以前に 1 つ以上ダウンロードをセットアップしていた場合は、代わりに、メインペインの右上にある [ダウンロードのセットアップ（**Setup Downloads**）] ボタンをクリックします。

[イメージを **APIC** へダウンロード（**Download Image to APIC**）] 画面が表示されます。

3. サイトを選択します。

ここで選択したすべてのサイトの Cisco APIC にイメージがダウンロードされます。

a. [サイトの選択 (**Select Sites**)] をクリックします。

b. [サイトの選択（**Select Sites**）] ウィンドウで、1 つ以上のサイトをオンにし、[追加して閉じる（**Add and Close**）] をクリックします。

c. [次へ（Next）] をクリックして続行します。

4. 詳細を入力します。

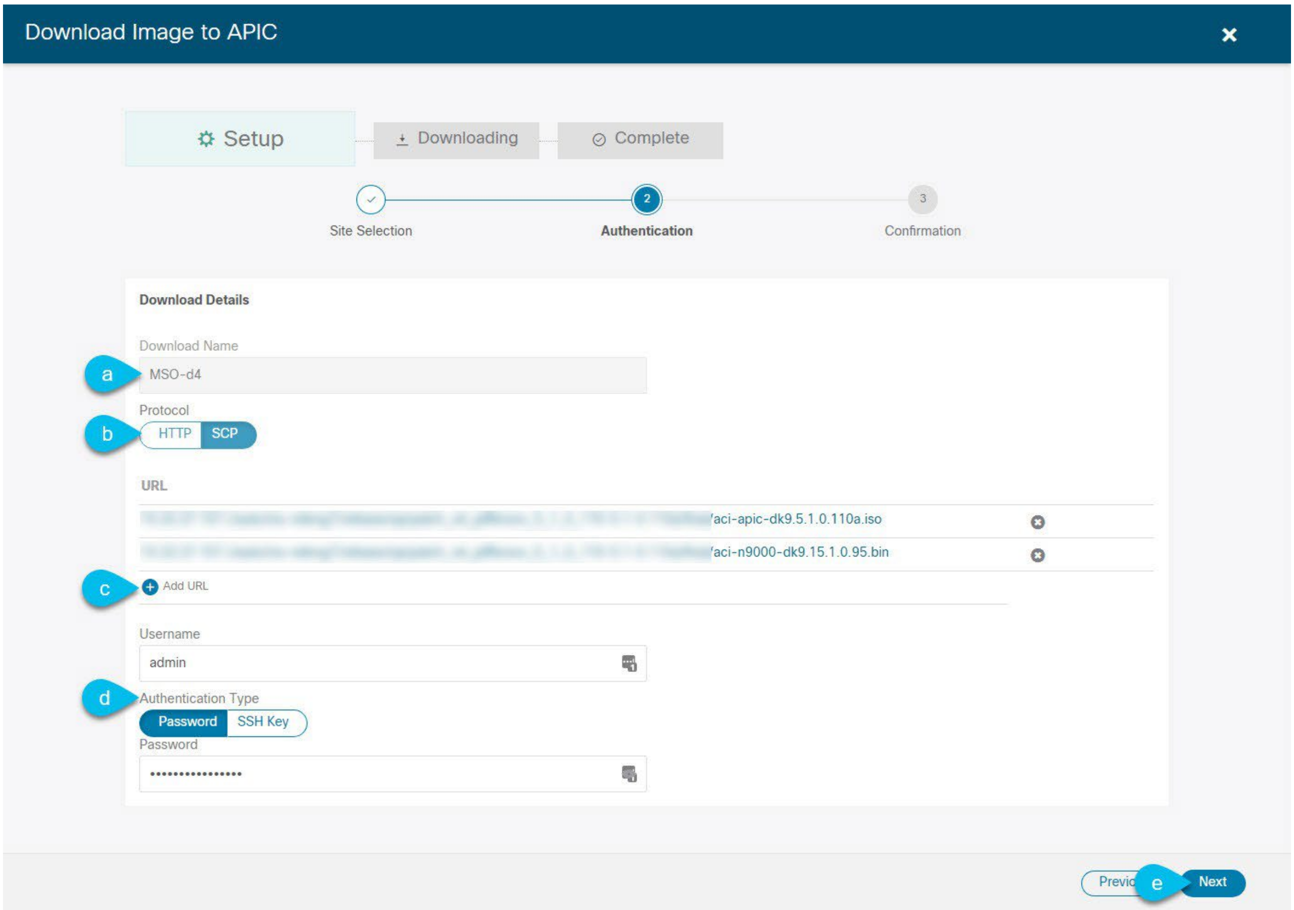


図 8 詳細

a. [名前（**Name**）] を入力します。

ダウンロードを追跡するためのわかりやすい名前を指定します。

b. プロトコルを選択します。

HTTP または SCP 経由でイメージをダウンロードすることを選択できます。

c. [**+ URL**の追加（**+ Add URL**）] をクリックして、1 つ以上のイメージの場所を指定します。

APIC とスイッチ ファームウェア イメージの両方を提供できます。

d. **SCP** を選択した場合は、認証情報を入力します。サインインする [ユーザー名（**Username**）]（admin など）を入力する必要があります。[認証タイプ **(Authentication Type)**] を選択します。

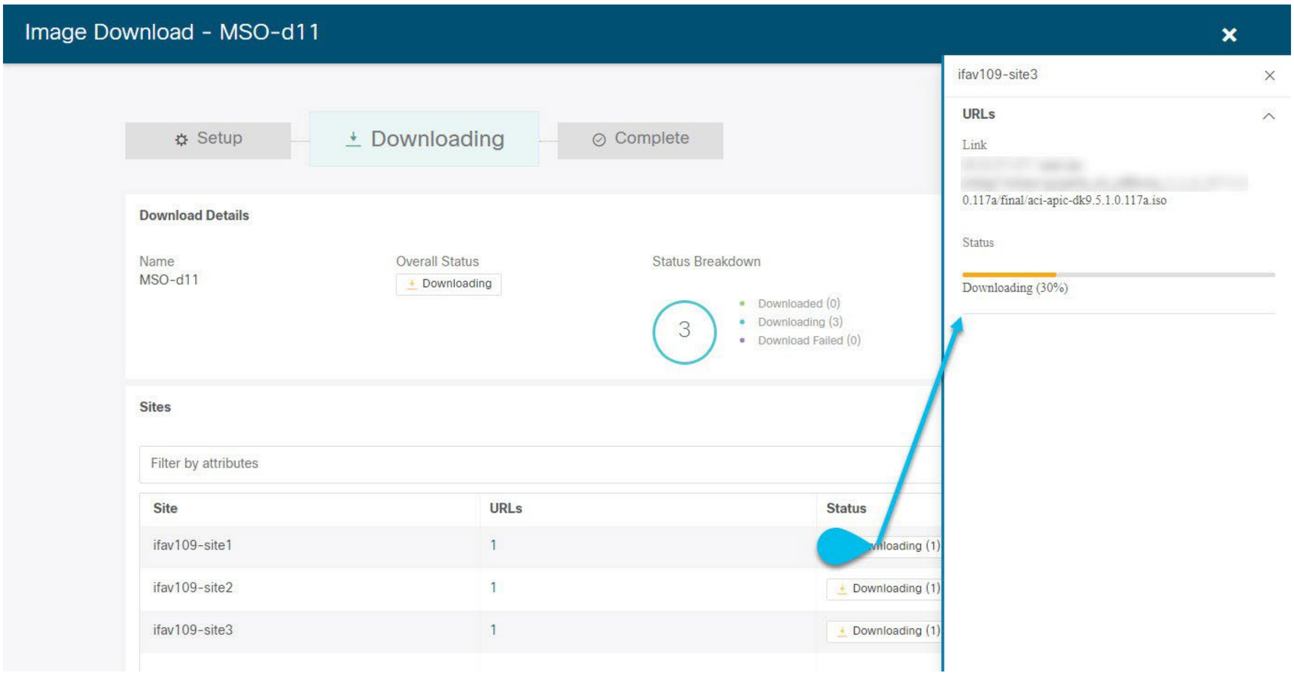
- パスワード認証の場合は、前に指定したユーザー名のパスワードを入力します。
- **SSH** キー認証の場合は、**SSH** キーと **SSH** キー パスフレーズを入力する必要があります。

e. [次へ（Next）] をクリックして続行します。

5. 確認画面で情報を確認し、[送信（**Submit**）] をクリックして続行します。

表示される [ダウンロード中（**Downloading**） 画面で、イメージのダウンロードのステータスを確認できます。

ステータスをクリックして、進行状況の詳細を表示することもできます。



すべてのダウンロードが完了すると、[完了 **(Completed)**] 画面に移行します。[ダウンロード（**Downloading**）] 画面で待機する必要はありません。前の手順で指定したダウンロード名をクリックすると、[ダウンロード（**Downloads**）] タブからいつでも戻ることができます。

コントローラのアップグレード

ここでは、サイトの APIC クラスタのソフトウェア アップグレードを設定する方法について説明します。

1. Cisco Nexus Dashboard Orchestrator にログインします。
2. APIC クラスタのアップグレードをセットアップします。

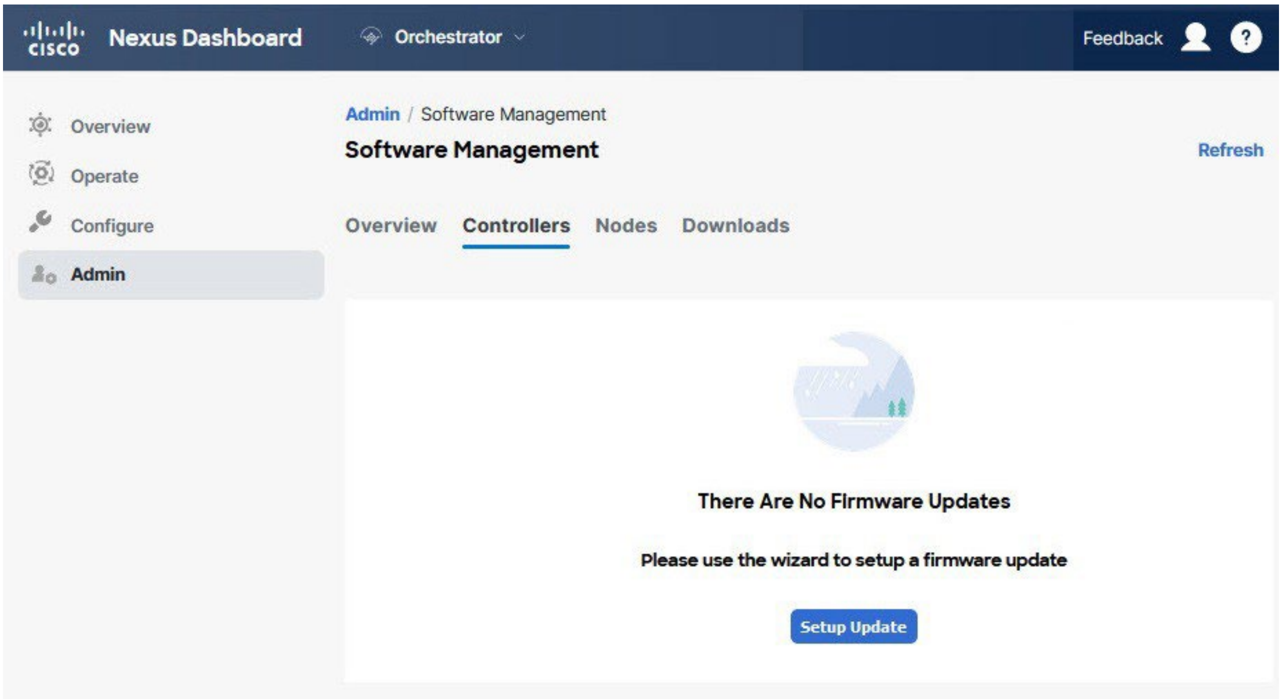


図 9. コントローラのアップグレード

a. 左のナビゲーション ペインから **[**管理（**Admin**）**] > [**ソフトウェア管理（**Software Management**）**]** を選択します。

b. メインウィンドウで **[**コントローラ（**Controllers**）**]** タブを選択します。

c. **[**更新のセットアップ（**Setup Update**）**]** タブをクリックします。

以前に 1 つ以上の更新を設定している場合は、代わりにメイン ペインの右上にある **[**更新のセットアップ **(Setup Update)]** ボタンをクリックします。

[サイト ファームウェアの更新のセットアップ（**Setup Site Firmware Update** ）**]** 画面が開きます。

3. アップグレードの詳細を入力します。

a. **[**名前（**Name**）**]** を入力します。

これは、いつでもアップグレードの進行状況を追跡するために使用できる、コントローラのアップグレード ポリシー名です。

b. **[**サイトの選択 **(Select Sites)]** をクリックします。

[サイトの選択（**Select Sites**）**]** ウィンドウが表示されます。

c. **[**サイトの選択（**Select Sites**）**]** ウィンドウで、1 つ以上のサイトをオンにし、**[**追加して閉じる（**Add and Close**）**]** をクリックします。

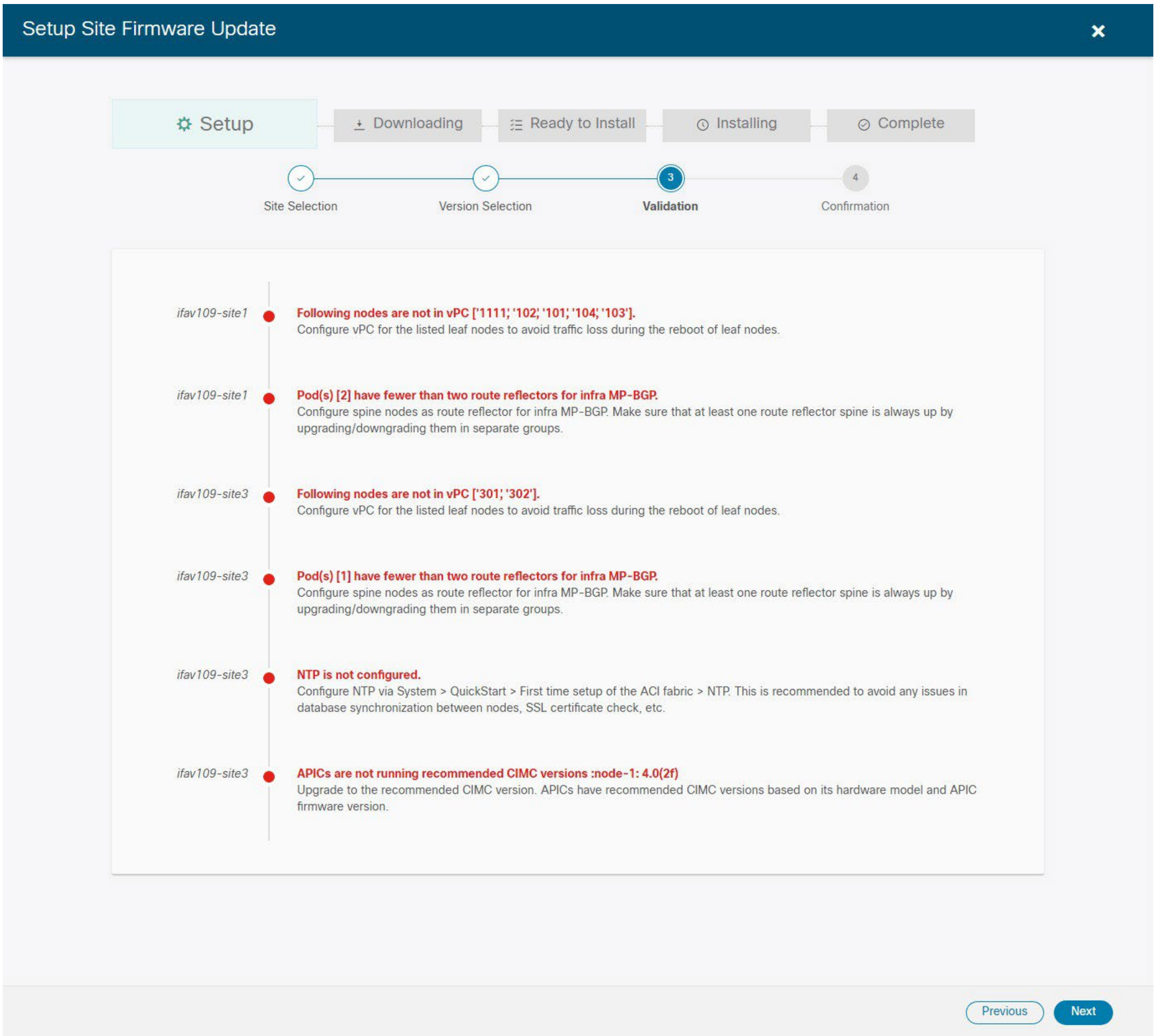
d. [次へ（Next）] をクリックして続行します。

4. **[**バージョンの選択（**Version Selection**）**]** 画面で、アップロードしたファームウェア バージョンを選択し、**[**次へ（**Next**）**]** をクリックします。

ここで使用可能にするためには、ファームウェアをサイトにダウンロードする必要があります。前のセクションで設定したダウンロードが正常に完了したものの、ここでイメージを使用できない場合は、**[**ファブリック ファームウェアの更新のセットアップ（**Setup Fabric Firmware Update**）**]** 画面を閉じ、**[**管理（Admin）] > [ソフトウェア管理（Software Management）]
> [概要（**Overview**）**]** タブに戻り、[更新（Refresh）] ボタンをクリックして、使用可能な最新情報をリロードします。それからファブリックのアップグレード手順をもう一度開始します。

5. **[**確認（**Validation**）**]** 画面で情報を確認し、**[**次へ（**Next**）**]** をクリックします。

障害がないことを確認し、アップグレードに影響する可能性がある追加情報を確認します。



6. [確認（**Confirmation**）] 画面で情報を確認し、[送信（**Submit**）] をクリックしてアップグレードを開始します。
7. [インストールの準備完了（**Ready to Install**）] 画面で、[インストール（**Install**）] をクリックします。

   アップグレード プロセス中に NDO からサイトへの接続が失われると、GUI には、接続が失われる前の、アップグレードの最新の既知ステータスが表示されます。接続が再確立されると、アップグレードのステータスが更新されます。接続が失われた後、メイン ペインの右上にある [更新（**Refresh**）] ボタンをクリックすると、手動で更新できます。

ノードのアップグレード

ここでは、サイトのスイッチ ノードのソフトウェア アップグレードを設定する方法について説明します。

1. Cisco Nexus Dashboard Orchestrator にログインします。
2. スイッチ ノードのアップグレードをセットアップします。

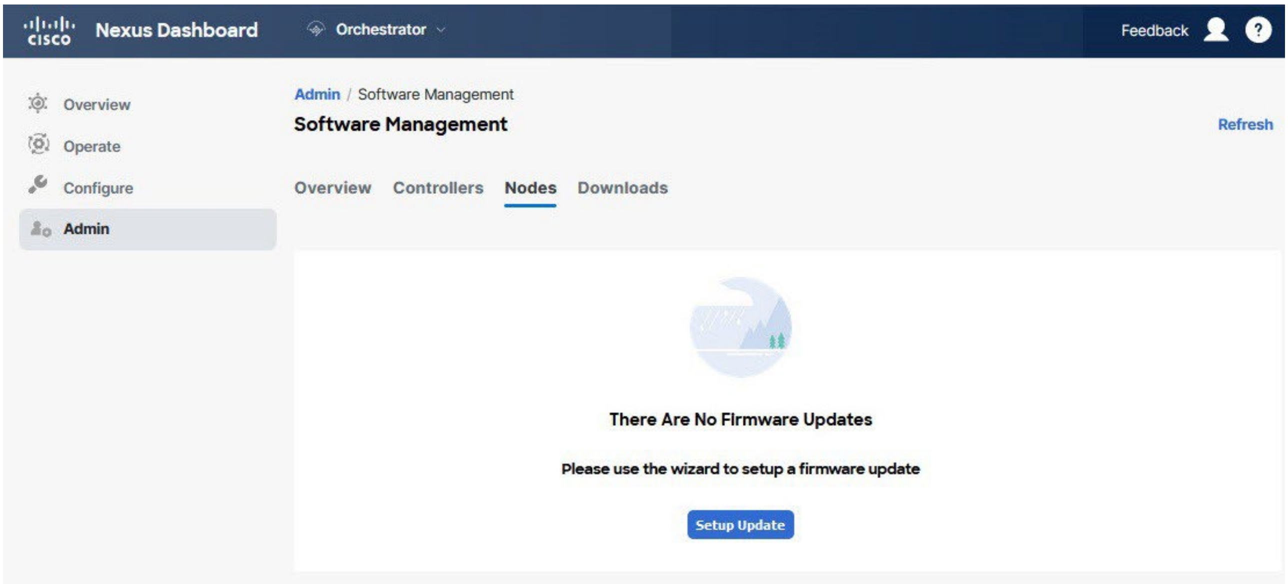


図 10 スイッチ ノードのアップグレード

a. 左のナビゲーション ペインから [管理（**Admin**）] > [ソフトウェア管理（**Software Management**）] を選択します。

b. メイン ウィンドウで [ノード（**Node**）] タブを選択します。

c. [更新のセットアップ（**Setup Update**）] タブをクリックします。

以前に 1 つ以上の更新を設定している場合は、代わりにメイン ペインの右上にある [更新のセットアップ **(Setup Update)**] ボタンをクリックします。

[ノード ファームウェアの更新のセットアップ（**Setup Node Firmware Update** ）] 画面が開きます。

3. アップグレードの詳細を入力します。

a. [名前（**Name**）] を入力します。

これは、いつでもアップグレードの進行状況を追跡するために使用できるアップグレード ポリシー名です。

b. [ノードの選択 **(Select Nodes)**] をクリックします。

[ノードの選択（**Select Nodes**）] ウィンドウが表示されます。

c. サイトを選択し、そのサイトのスイッチノードを選択して、[追加して閉じる **(Add and Close)**] をクリックします。

一度に 1 つのサイトからスイッチノードを追加できます。他のサイトからスイッチを追加する場合は、この手順を繰り返します。image::503324.jpg[,width=720]

d. 他のサイトのノードについて、前のサブステップを繰り返します。

e. [次へ（Next）] をクリックして続行します。

4. [バージョンの選択（**Version Selection**）] 画面で、アップロードしたファームウェア バージョンを選択し、[次へ（**Next**）] をクリックします。

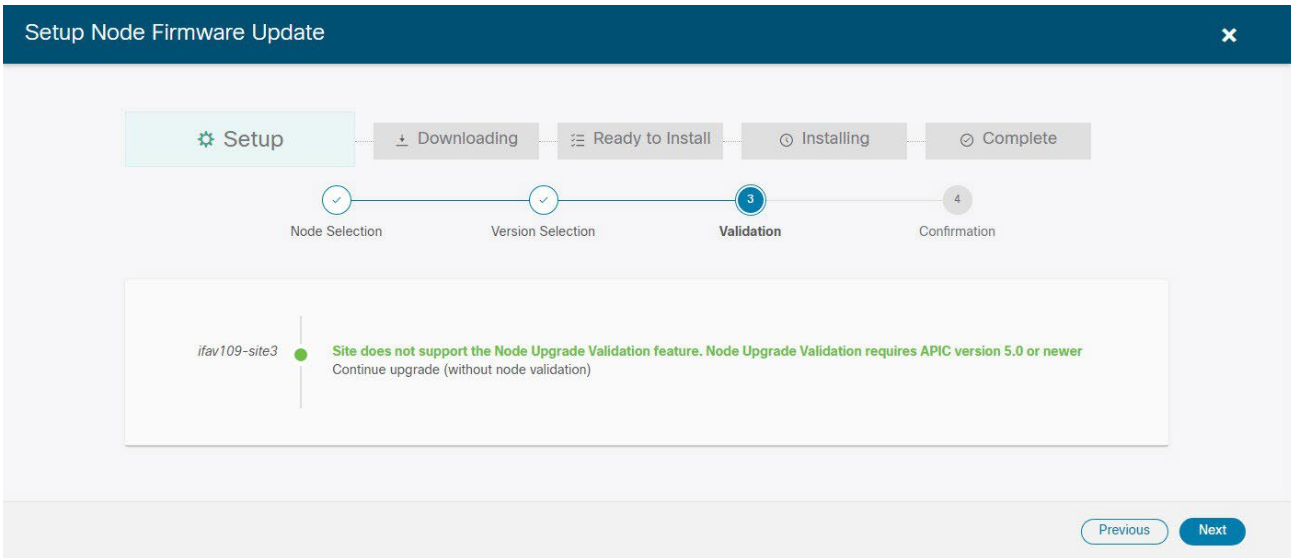
ここで使用可能にするためには、ファームウェアをサイトにダウンロードする必要があります。前のセクションで設定したダウンロードが正常に完了したものの、ここでイメージを使用できない場合は、[ファブリック ファームウェアの更新のセットアップ（**Setup Fabric Firmware Update**）] 画面を閉

じ、[管理（**Admin**）] > [ソフトウェア管理（**Software Management**）]
> [ノード（**Nodes**）] タブに戻り、[更新（Refresh）] ボタンをクリックして、使用可能な最新情報をリロードします。それからファブリックのアップグレード手順をもう一度開始します。

5. [検証（**Validation**）] 画面で、障害が発生していないことを確認し、[次へ（**Next**）] をクリックします。

   障害がないことを確認し、アップグレードに影響する可能性がある追加情報を確認します。

   リリース 5.0(1) より前のリリースを実行しているサイトは、ノードの検証をサポートしていません。
   そのため 、NDO からのアップグレードを開始する前に、サイトのAPICでスイッチノードの障害を確認することをお勧めします。



6. [確認（**Confirmation**）] 画面で情報を確認し、[送信（**Submit**）] をクリックします。

   これにより、選択したすべてのノードにイメージが事前にダウンロードされます。ダウンロードが完了すると、画面が [インストール準備完了（**Ready to Install**）] に遷移し、次の手順に進むことができます。

7. （オプション）[詳細設定 **(Advanced Settings)**]を変更します。

   詳細オプションを変更する前に、 Upgrade and Downgrading the Cisco APIC and Switch Software （Cisco APIC *Installation*、*Upgrade*、and Downgrade Guide) で説明されている*Cisco APIC アップグレードプロセスのガイドライン*、推奨事項、および制限事項を確認してください。

   [インストールの準備完了（**Ready to Install**）] 画面で、[詳細設定（**Advanced Settings**）] メニューを開いて追加のオプションを表示できます。

   - [互換性チェックを無視（**Ignore Compatibility Check**）]：デフォルトでは、このオプションは [いいえ（No）] に設定され、互換性チェックが有効になっています。システムの現在実行中のバージョンから指定された新しいバージョンへのアップグレードパスがサポートされているかどうかが確認されます。

     [互換性チェックを無視 (Ignore Compatibility Check)] フィールドで [はい (Yes)] にして互換性チェック機能を無効にした場合、システムでサポートされていないアップグレードが実行されるリスクがあり、システムが利用できない状態になる可能性があります。

   - [グレースフル チェック（**Graceful Check**）]：デフォルトでは、このオプションは [いいえ（No）]` に設定されています。アップグレード プロセスでのアップグレード実行前には、どのス

イッチもグレースフル挿入/取り外し（GIR）モードにされません。

このオプションを有効にすると、アップグレードの実行中にノードをグレースフルに（GIRを使用して）ダウンさせることができ、アップグレードによるトラフィック損失が減少します。

- [実行モード（**Run Mode**）]：デフォルトでは、このオプションは [失敗時に続行（Continue on Failure）] に設定されており、ノードのアップグレードが失敗すると、次のノードに進みます。または、このオプションを [失敗時に一時停止 (Pause on Failure)]に設定すると、いずれかのノードのアップグレードが失敗した場合にアップグレード プロセスを停止できます。

8. [失敗（Failed）] とマークされたノードをアップグレードから削除します。

   アップグレードポリシーに、ファームウェアのダウンロードに失敗した 1 つ以上のノードが含まれている場合、アップグレードを続行できません。[失敗（Failed）]ステータスにカーソルを合わせると、詳細情報と失敗の理由が表示されます。

   アップグレードからノードを削除するには、[インストールの準備完了（**Ready to Install**）] 画面の [アップデートの詳細を編集（**Edit Update Details**）] のリンクをクリックします。
   画面に戻ります。

9. [インストール（**Install**）] をクリックしてアップグレードを開始します。

   アップグレード プロセス中に NDO からサイトへの接続が失われると、GUI には、接続が失われる前の、アップグレードの最新の既知ステータスが表示されます。接続が再確立されると、アップグレードのステータスが更新されます。接続が失われた後、メイン ペインの右上にある [更新（**Refresh**）] ボタンをクリックすると、手動で更新できます。

初版：2024 年 3 月 1 日
最終更新日：2024 年 3 月 1 日

米国本社
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax：408 527-0883