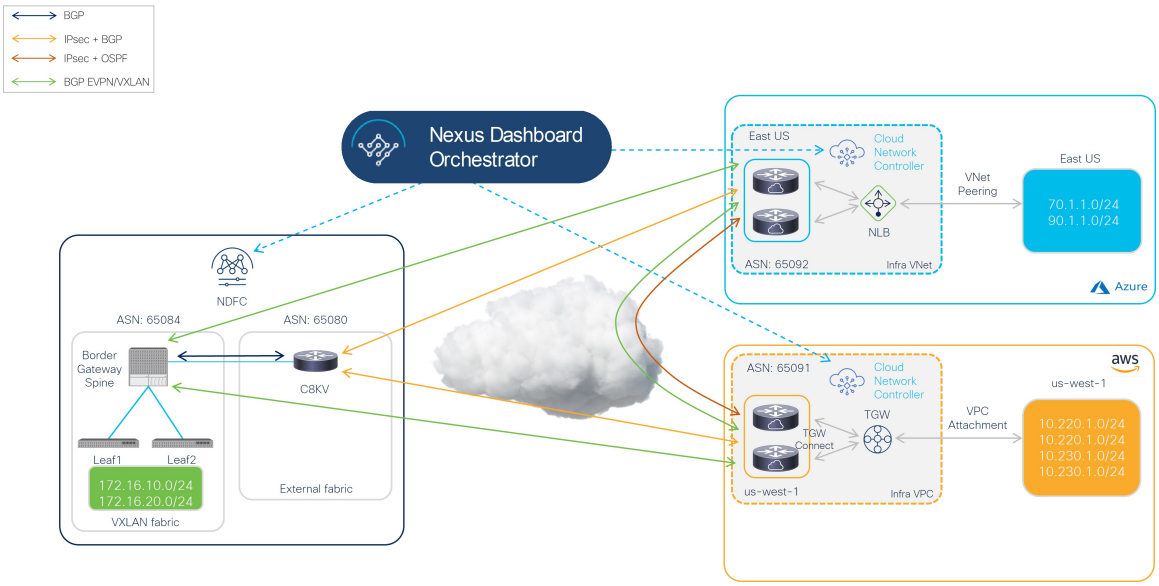
ハイブリッド クラウドとマルチクラウド接続展開のインフラ構成を設定する

- ハイブリッド クラウドとマルチクラウド接続展開のインフラ構成のトポロジ例 （1 ページ）
- オンプレミス NDFC ファブリックを設定 （3 ページ）
- クラウド サイト上のクラウド ネットワーク コントローラを展開します （21 ページ）
- NDFC とクラウド サイトを ND と NDO に導入準備する （36 ページ）
- Complete サイト間の接続 NDFC と クラウド サイトの間 （44 ページ）

ハイブリッドクラウドとマルチクラウド接続展開のインフラ構成のトポロジ例

次の図は、ハイブリッドクラウドおよびマルチクラウド接続の展開のインフラ構成に使用できる、サポートされているトポロジの 1 つを示しています。

図 *1:*



このドキュメントの手順では、IPsec（マルチクラウド）でサポートされるトポロジのオプション1に基づく特定のユース ケースとしてこのトポロジを使用し、このトポロジのユース ケースに特化したハイブリッド クラウド接続オプションを構成する方法について説明します。

この展開手順では、IPsec を使用してマルチクラウド接続を構成し、これらのハイブリッド クラウド接続エリアのそれぞれで特定の構成を行います。全体的な構成手順は次のとおりです。

- NDFC のインストール

  詳細については、次を参照します：

  - *Cisco Nexus* ダッシュボード ファブリック コントローラのインストールとアップグレード ガイド、リリース 12.1.2 以降
  - *Cisco NDFC-Fabric* コントローラ 構成ガイドリリース 12.1.2 以降
  - *Cisco Nexus* ダッシュボード ファブリック コントローラ導入ガイド、リリース 12.1.2 以降

- 初期設定：
  - オンプレミス NDFC ファブリックの設定
  - Cisco Cloud ネットワーク コントローラのインスール
  - クラウド サイトの設定
  - NDO のインストール
  - NDO を使用したハイブリッド クラウド接続の設定
- テナントとスキーマの展開：

- ユース ケース 1：ストレッチ VRF（VRF 内）
- ユース ケース 2：ルートリーク（VRF 間）

オンプレミス NDFC ファブリックを設定

このセクションでは、2 つのオンプレミス NDFC ファブリックを設定します：

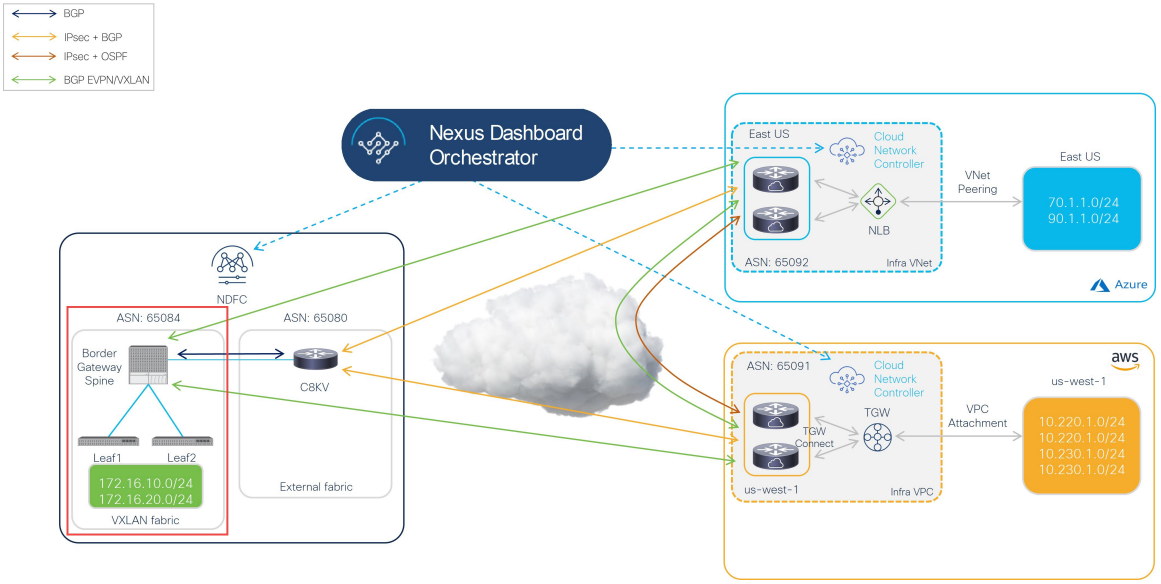
- NDFC VXLAN ファブリック
- NDFC 外部ファブリック

次のセクションの手順を実行して、2 つのオンプレミス NDFC ファブリックを設定します。

NDFC VXLAN ファブリックを作成

この手順では、下で強調表示されているトポロジ例の一部を構成します。

図 *2:*



VXLAN ファブリックには、オンプレミス ファブリックとクラウド サイト間の VXLAN マルチサイト接続を構築するために使用される 1 つ以上のボーダー ゲートウェイ（BGW）デバイスが含まれている必要があります。

次のセクションの手順を実行して、NDFC VXLAN ファブリックを構成します。

NDFC VXLAN ファブリックを作成

ステップ 1 NDFC がインストールされている Nexus ダッシュボードにログインします。

ステップ 2 NDFC アカウントにログインします。

ステップ 3 **[ローカルエリアネットワーク（LAN）]** > **[ファブリック（ファブリック）]** に移動します。
[LAN ファブリック（LAN Fabrics）] ウィンドウが表示されます。

ステップ 4 **[アクション（Actions）]** > **[ファブリックの作成（Create Fabric）]** をクリックします。
[ファブリックの作成（Create Fabric）] ウィンドウが表示されます。

ステップ 5 `Easy_Fabric` テンプレートを使用して、NDFC VXLAN ファブリックの作成プロセスを開始します。

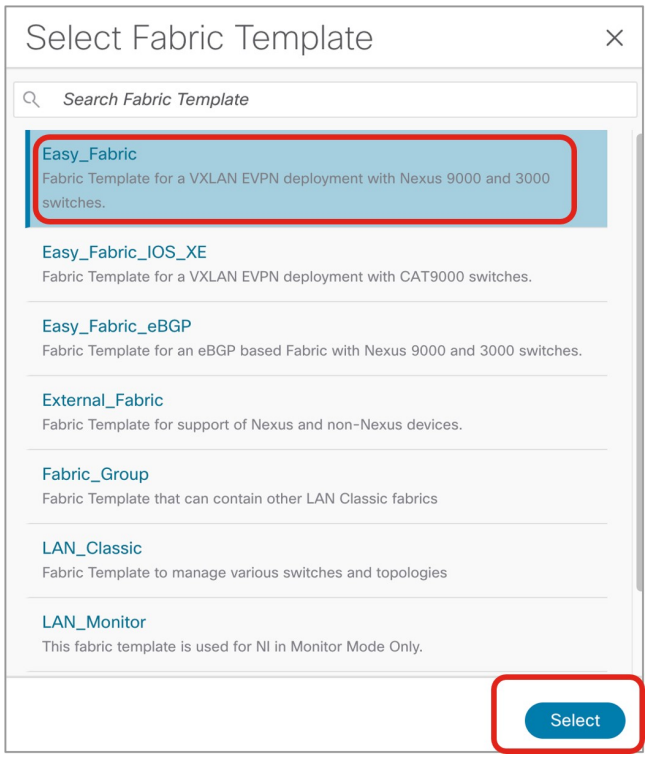
a) **[ファブリック名（Fabric Name）]** フィールドに NDFC VXLAN ファブリックの名前を入力します。

b) **[テンプレートを選ぶ（Pick a Template）]** エリアで、**[テンプレートを選択（Choose Template）]** します。
[ファブリック テンプレートの選択（Select Fabric Template）] ウィンドウが表示されます。

c) `Easy_Fabric` テンプレートを見つけてクリックします。

d) [選択（Select）] をクリックします。

図 *3:*



ステップ 6 必要な一般的な VXLAN ファブリック パラメータ構成を完了します。

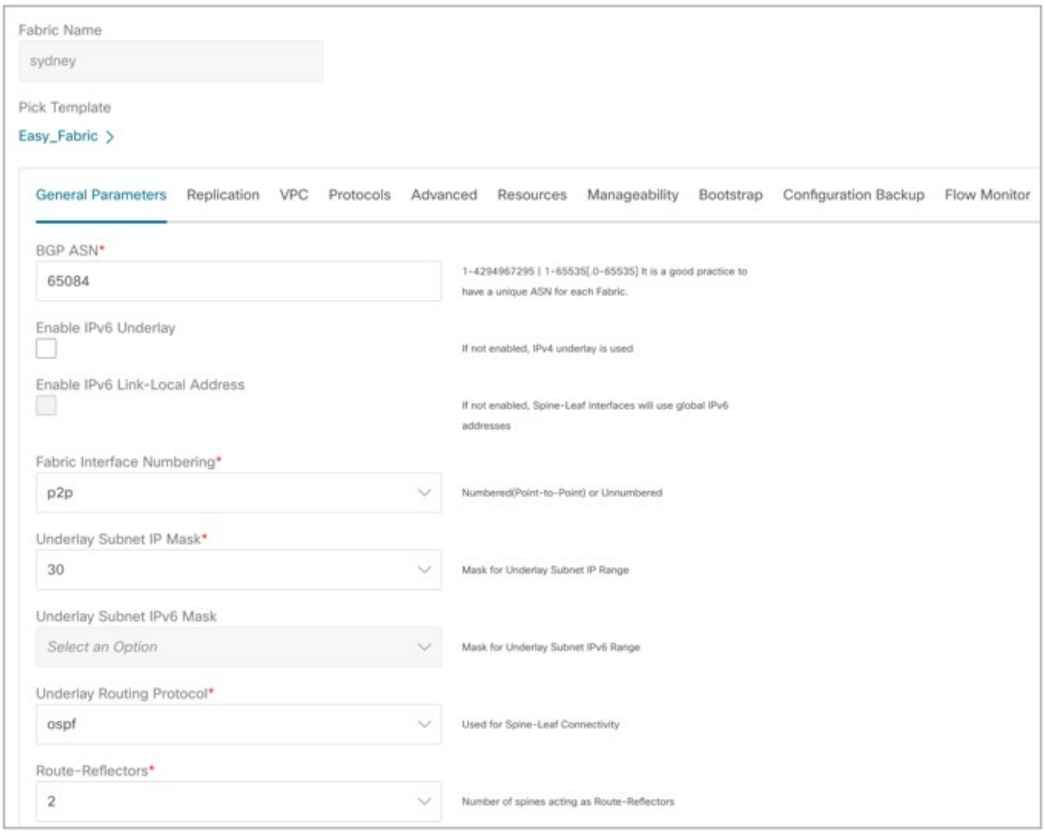
`Easy_Fabric` テンプレートの次のパラメーター タブに入力する必要がありますが、このハイブリッド クラウド トポロジのユース ケースに固有のパラメーターは含まれていません。

- 一般的なパラメータ
- **Replication**
- **VPC**
- **Protocols**

通常どおり、これらのパラメータ タブで VXLAN ファブリック構成を完了します。詳細については、*[Cisco Nexus ダッシュボード ファブリック コントローラ導入ガイド（Cisco Nexus Dashboard Fabric Controller Deployment Guide）]*、リリース 12.1.2 以降を参照します。

たとえば、トポロジ例の情報を使用すると、**[一般パラメータ（General Parameters）]** ページの **[BGP ASN]** フィールドに `65084` と入力します。

図 *4*:



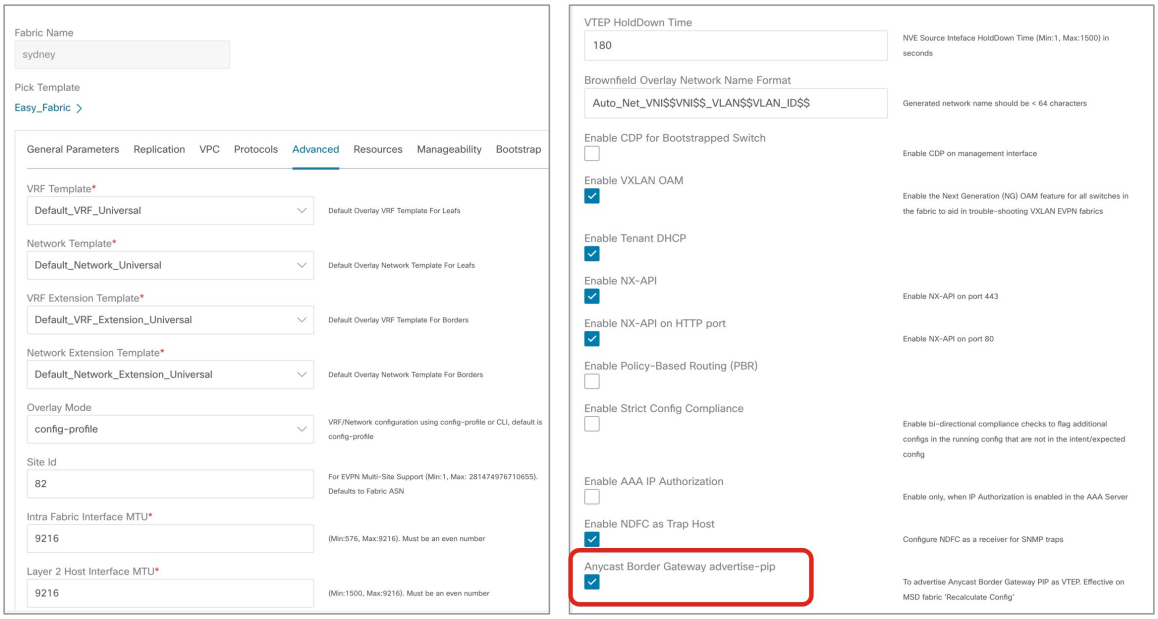
ステップ *7* **[詳細（Advanced）]** パラメータ タブで、このハイブリッド クラウド トポロジのユース ケースに特に必要な構成を行います。

- **[エニーキャスト ボーダー ゲートウェイの advertise-pip（Anycast Border Gateway advertise-pip）]** フィールドを見つけ、ボックスをオンにしてこのオプションを有効にします。これにより、エニーキャスト ボーダー ゲートウェイ PIP が VTEP としてアドバタイズされます。

  これは、サイト間でレイヤー 3 のみの接続（レイヤー 2 拡張機能がないなど）が確立されている場合に必要です。これは、ハイブリッドクラウドおよびマルチクラウドの展開に常に当てはまります。

- 通常どおり、**[詳細（Advanced）]**パラメータ タブで残りの構成を完了します。

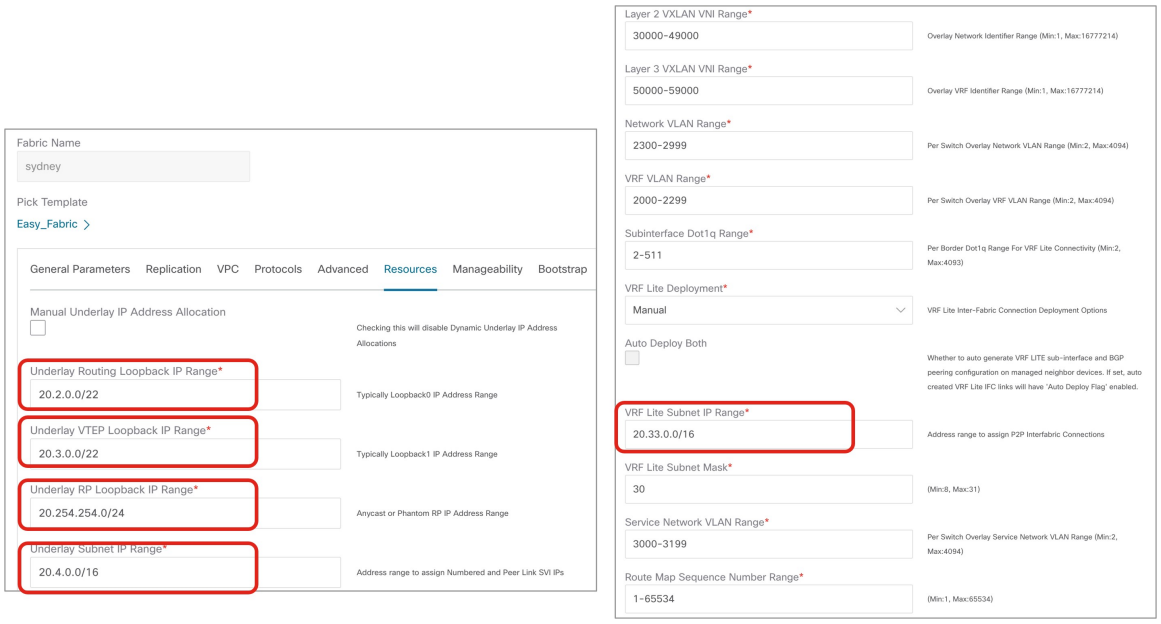
図 *5*:



ステップ 8 **[情報技術（Resources）]** パラメータ タブをクリックし、このページに必要な値を入力します。

- このハイブリッド クラウドのユース ケース専用に、次のフィールドに適切な情報を入力します。
  - **[アンダーレイ ルーティング ループバック IP 範囲（Underlay Routing Loopback IP Range）]**：通常、これは loopback0 の IP アドレス範囲です。
  - **[アンダーレイ VTEP ループバック IP 範囲（Underlay Routing Loopback IP Range）]**：通常、これは loopback1 の IP アドレス範囲です。
  - **[アンダーレイ VTEP ループバック IP 範囲（Underlay RP Loopback IP Range）**：エニーキャストまたはファントム ランデブー ポイント（RP）IP アドレスの範囲.
  - **[アンダーレイ サブネット IP 範囲（Underlay Subnet IP Range）]**：アドレス範囲ピア リンク SVI IP アドレスの番号付されたものを割り当てする。
  - **[VRF Lite サブネット IP 範囲（VRF Lite Subnet IP Range）]**：P2P ファブリック間接続を割り当てるアドレス範囲。
- 通常どおり、**[情報技術（Resources）]**パラメータ タブで残りの構成を完了します。

図 *6 :*



ステップ 9 [管理性] および [ブートストラップ パラメータ] タブで、必要な一般的な VXLAN ファブリック パラメータ設定を完了します。

[管理性（Manageability）]および**[ブートストラップ（Bootstrap）]**パラメータ タブの構成を完了する必要がある場合がありますが、これらには、このハイブリッドクラウド トポロジのユース ケースに固有のパラメータは含まれていません。

ステップ 10 **[構成バックアップ（Configuration Backup）]** パラメータ タブをクリックし、**[毎時のファブリック バックアップ（Hourly Fabric Backup）]** フィールドのチェックボックスをオンにして、その機能を有効にします。

通常どおり、**[構成バックアップ（Configuration Backup）]**パラメータ タブで残りの構成を完了します。

ステップ 11 VXLAN ファブリックの**[ファブリックを作成（Create Fabric）]** ウィンドウで必要な構成を完了したら、**[保存（Save）]** をクリックします。
[LAN ファブリック（LAN Fabrics）] ウィンドウに戻り、作成したばかりのVXLAN ファブリックが表示されます。

次のタスク

VXLAN ファブリックにスイッチを追加し、VXLAN ファブリックへのスイッチの追加 （7 ページ）に記載されている手順を使用して、スイッチに必要な役割を設定します。

VXLAN ファブリックへのスイッチの追加

この手順では、スイッチを VXLAN ファブリックに追加し、スイッチに必要な役割を設定します。

始める前に

NDFC VXLAN ファブリックを作成 （4 ページ）で提供されている手順を使用して、NDFC VXLAN ファブリックを作成します。

ステップ 1 **[ローカル エリア ネットワーク（LAN）ファブリック（LAN Fabrics）]** ウィンドウで、作成したばかりの VXLAN ファブリックをクリックします。

ファブリックの**[概要（Overview）]** ウィンドウが表示されます。

（注） 次の手順では、NDFC がスイッチを検出できるようにするために必要な情報を手動で入力する方法について説明します。代わりに、管理 IP アドレス、デフォルト ルートとスイッチに構成済みの発見されなければならないスタート アップ構成などの特定のパラメータが既にない場合に便利な NDFC の Power On Auto Provisioning（POAP）機能を使用することもできます。POAP は、ネットワークに初めて展開されるデバイスに構成ファイルをインストールするプロセスを自動化し、手動構成を実行せずにデバイスを起動できるようにします。POAP の詳細については、「外部ファブリックおよびローカルエリア ネットワーク（LAN）クラシック ファブリックでのインバンド POAP 管理」および「NDFC でのインバンド POAP を使用した VXLAN ファブリックのゼロ タッチ プロビジョニング」を参照してください。

ステップ 2 **[アクション（Actions）]** > **[スイッチを追加（Add Switches）]** をクリックします。
[スイッチの追加（Add Switches）] ウィンドウが表示されます。

ステップ 3 スイッチを検出するために必要な情報を追加します。

- シード IP、ユーザー名、パスワードなど、スイッチを検出するために必要な情報をこのページに入力します。
- スイッチの既存の構成を保持するかどうかを決定します。
  - これが既存の構成をスイッチに保持するブラウンフィールド展開の場合は、**[構成を保持（Preserve Config）]** チェックボックスをオンにして、それらの既存の設定を保持します。
  - これがグリーンフィールド展開の場合は、**[構成を保持（Preserve Config）]** チェックボックスをオフにして、スイッチの構成をクリーンアップします。

ステップ 4 **[スイッチの検出（Discover Switches）]** をクリックします。

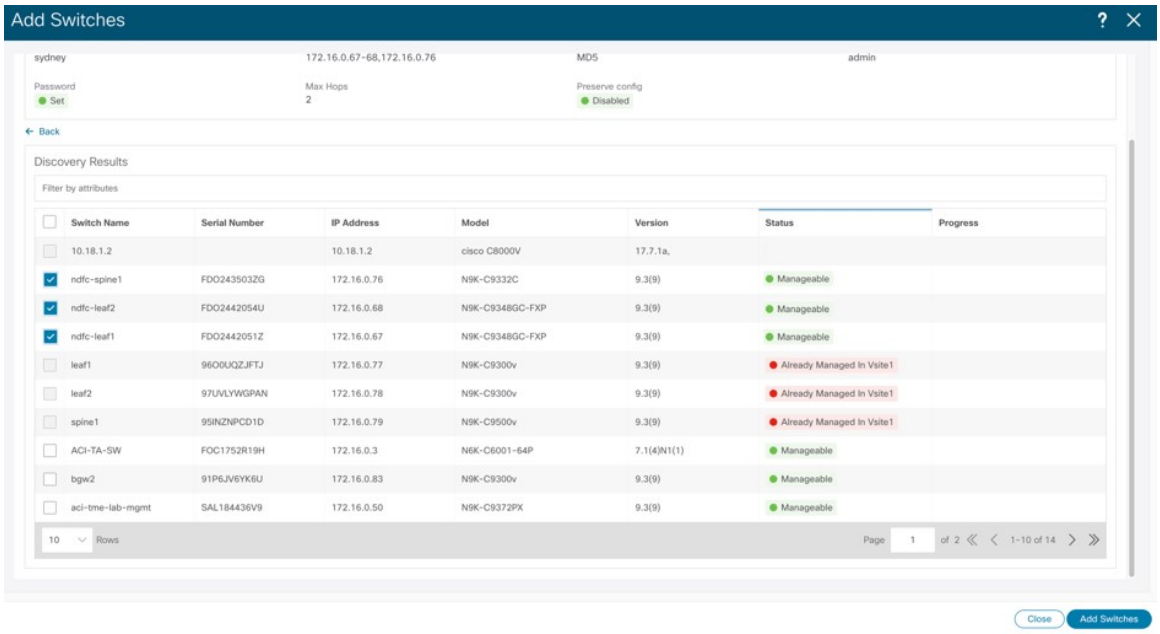
表示される確認ポップアップ ウィンドウで **[確認（Confirm）]** をクリックします。

ステップ 5 スイッチが検出されたら、スイッチを NDFC VXLAN ファブリックに追加します。

[発見結果（Discovery Results）] エリアで、適切なスイッチを選択します（該当する各スイッチの横にあるボックスをクリックします）。

例として、次の図は、ファブリックに追加される 2 つのリーフ スイッチと 1 つのスパイン スイッチを示しています。

図 *7:*



ステップ 6 **[スイッチの追加（Add Switches）]** をクリックします。

（注） **[構成を保持（Preserve Config）]** オプションがオンになっている場合、スイッチは NDFC VXLAN ファブリックに追加された後に再起動します。

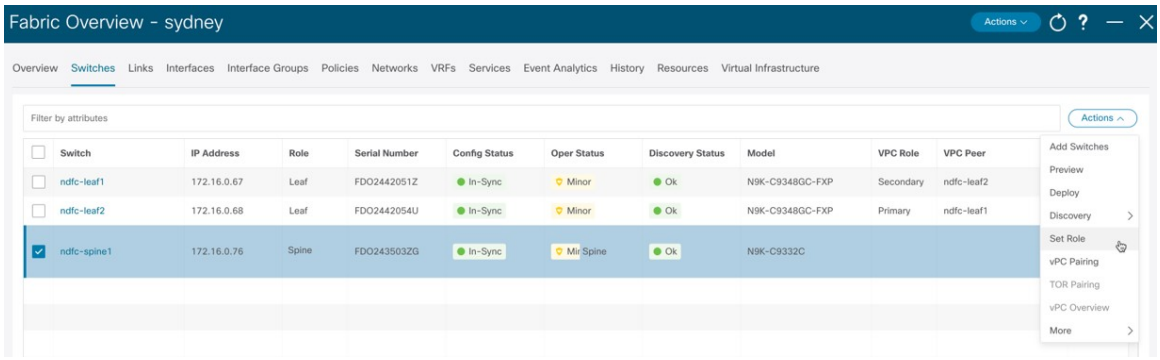
ステップ 7 適切なスイッチの役割を[ボーダー ゲートウェイ スパイン（Border Gateway Spine）]に設定します。

これらの手順例では、1 つのスパイン スイッチがスパイン スイッチとボーダー ゲートウェイ スパイン スイッチの二重の役割を果たしているため、これらの手順例では、スパイン スイッチの役割をボーダー ゲートウェイ スパイン スイッチに変更します。ただし、ご使用の環境では、2 つの別個のスイッチがあり、1 つはスパイン スイッチの役割を持ち、もう 1 つはボーダー ゲートウェイの役割を持っている場合があります。

a) NDFC VXLAN ファブリック概要ウィンドウ の**[スイッチ（Switches）]** タブをクリックします。このファブリックに追加されたスイッチが表示されます。

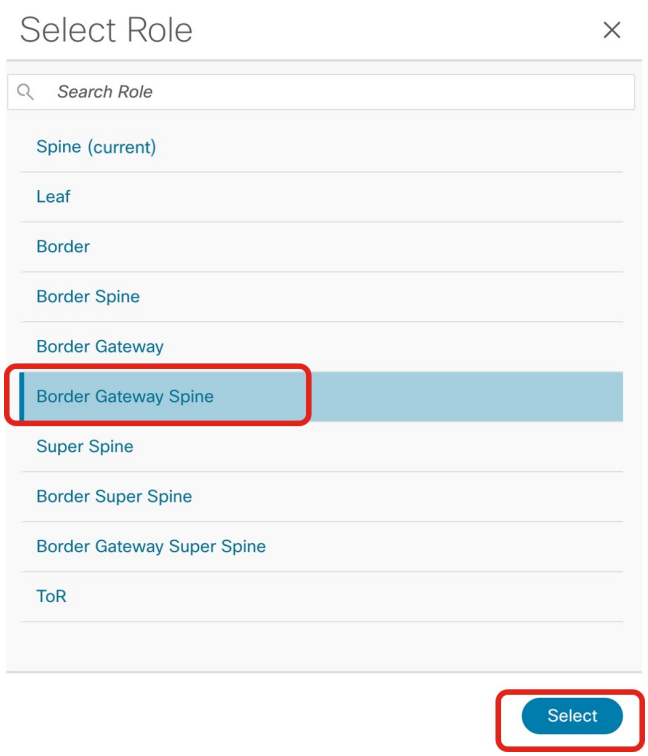
b) スパイン スイッチの横にあるボックスをクリックしてそのスイッチを選択し、**[アクション（Actions）] > [役割を設定（Set Role）]**をクリックします。

図 *8*:



c) **[ロールの選択（Select Role）]** リストで [ボーダー ゲートウェイ スパイン（Border Gateway Spine）] ロールを見つけて選択し、**[選択（Select）]** をクリックします。

図 *9*:



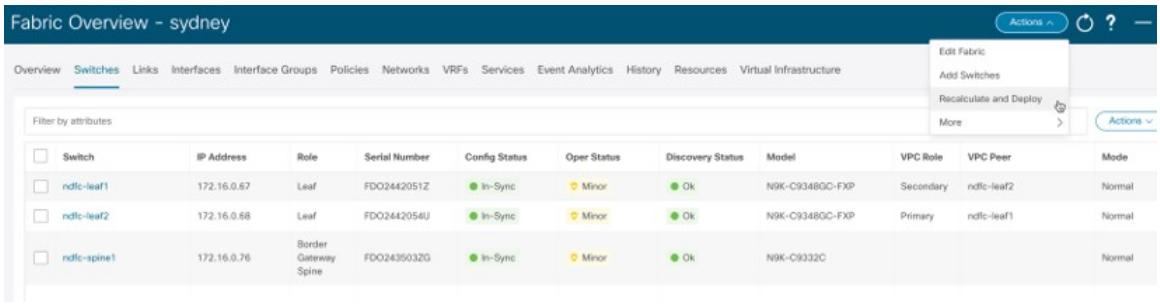
ステップ 8 **[ローカル エリア ネットワーク（LAN）]**>**[ファブリック（Fabrics）]**に移動し、作成したNDFC VXLAN ファブリックを選択します。

NDFC VXLAN ファブリックの **[概要（Overview）]** ページが表示されます。

ステップ 9 **[スイッチ（Switches）]** タブをクリックして、追加したスイッチが正しく表示されることを確認します。

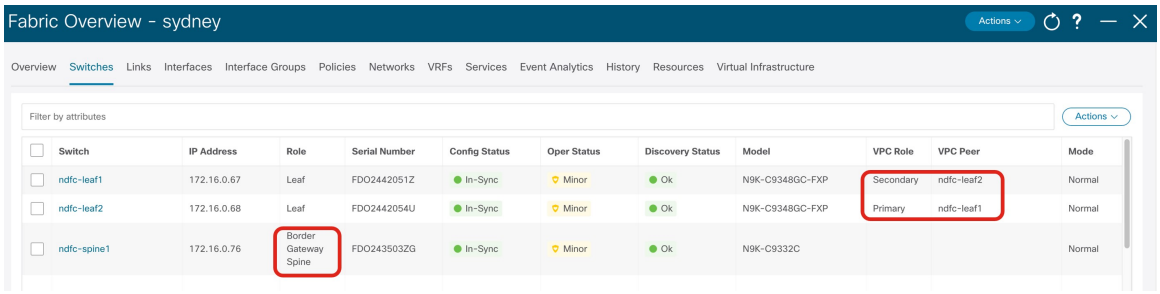
ステップ 10 **[アクション（Actions）]** > **[再計算と展開（Recalculate and Deploy）]**をクリックします。

図 *10 :*



前述のように、これらの手順では、1 つのスパイン スイッチがスパイン スイッチとボーダー ゲートウェイ スパイン スイッチの二重の役割を果たしているため、以下に示すように、これらの手順例ではスパイン スイッチの役割をボーダー ゲートウェイ スパイン スイッチに変更しました。これらの手順例では、次の図に示すように、vPC ペアも 2 つのリーフ スイッチにすでに構成されています。vPC ペアの構成の詳細については、*Cisco NDFC-Fabric* コントローラ構成ガイド リリース 12.1.2e 以降を参照してください。

図 *11 :*



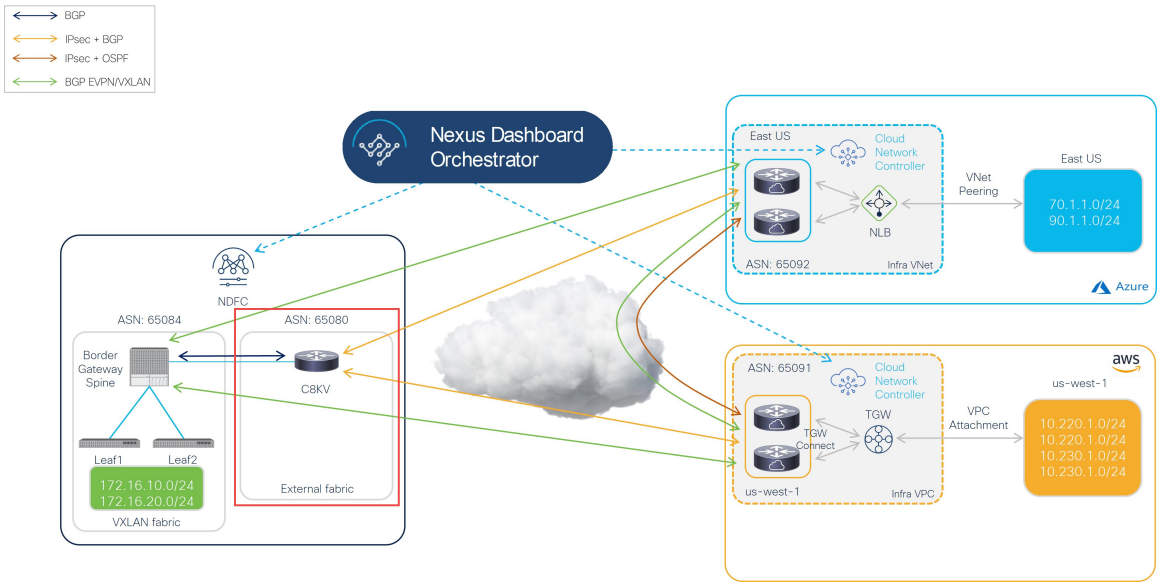
次のタスク

NDFC 外部ファブリックを構成 （11 ページ）で提供されている手順を使用して、NDFC 外部ファブリックを設定します。

NDFC 外部ファブリックを構成

この手順では、下で強調表示されているトポロジ例の一部を構成します。下の図の例およびユース ケースの手順全体では、Cisco Catalyst 8000V が外部ファブリックの IPsec デバイスとして使用されていますが、IPsec をサポートし NDFC によって管理されていれば（たとえば、ASR 1000 および Catalyst 8000V）、外部ファブリックにはさまざまなタイプのデバイスが存在する可能性があります。

図 *12 :*



NDFC 管理の外部ファブリックには、1 つ以上の IPsec デバイスが含まれています。IPsec デバイスは、インターネット (パブリック) を介して、または直接接続（AWS）や ExpressRoute（Azure）などのプライベート接続によってクラウド ネットワークに接続できます。パブリック インターネットを使用してクラウドサイトに接続する場合、オンプレミスの IPsec デバイスとクラウド サイトの Catalyst 8000V の間に IPsec トンネルが確立されます。

次のセクションの手順を実行して、NDFC 外部ファブリックを構成します。

NDFC 外部ファブリックを作成

始める前に

これらの手順に進む前に、NDFC VXLAN ファブリックを作成 （4 ページ） に提供されている手順を完了してください。

ステップ 1 まだログインしていない場合は、NDFC アカウントにログインします。

ステップ 2 **[ローカルエリアネットワーク（LAN）]** > **[ファブリック（ファブリック）]** に移動します。

ステップ 3 **[アクション（Actions）]** > **[ファブリックの作成（Create Fabric）]** をクリックします。
[ファブリックの作成（Create Fabric）] ウィンドウが表示されます。

ステップ 4 `External_Fabric` テンプレートを使用して、外部ファブリックを作成するプロセスを開始します。

`External_Fabric` テンプレートは、Nexus および Catalyst 8000V などの非 Nexus デバイスを使用して従来の LAN ファブリックを構築するために使用されます。

a) **[ファブリック名（Fabric Name）]** フィールドに外部ファブリックの名前を入力します。

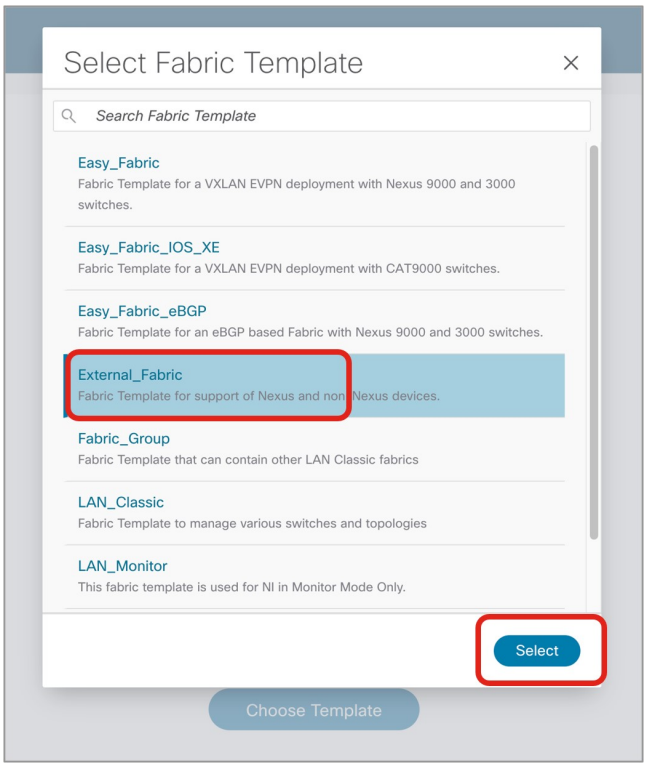
b) **[テンプレートを選ぶ（Pick a Template）]** エリアで、**[テンプレートを選択（Choose Template）]** します。

[ファブリック テンプレートの選択（Select Fabric Template）] ウィンドウが表示されます。

c) `External_Fabric` テンプレートを見つけてクリックします。

d) [選択（Select）] をクリックします。

図 *13 :*



ステップ 5 **[一般パラメータ（General Parameters）]** タブで、このハイブリッド クラウド トポロジのユース ケースに特に必要な構成を行います。

- **BGP ASN** フィールドで、BGP ASN を定義します。

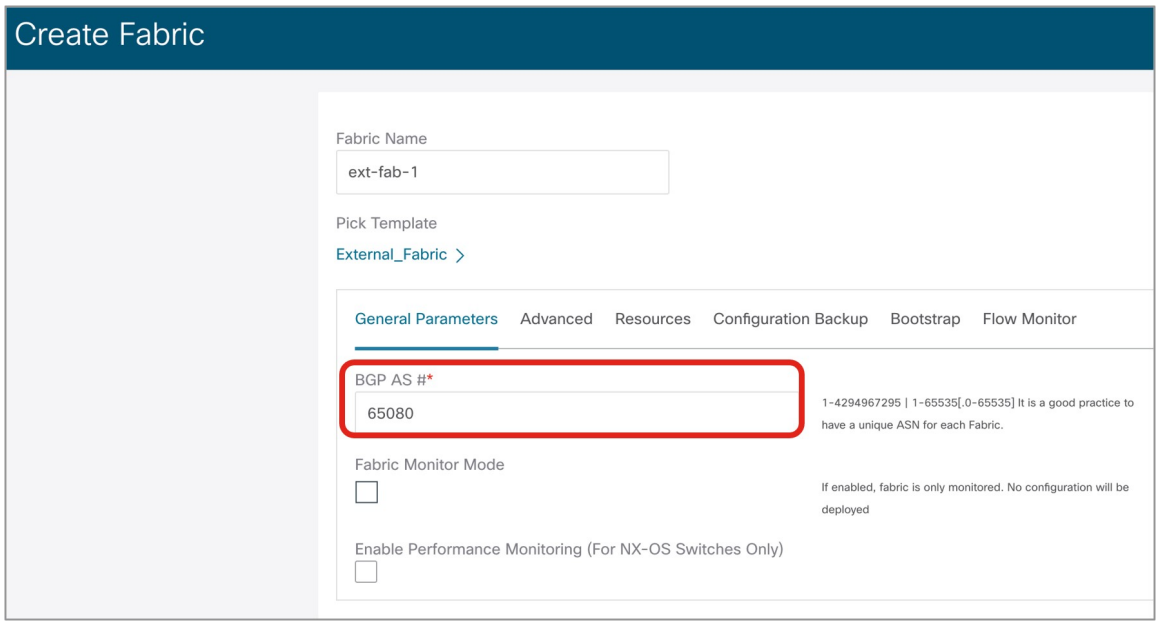
  たとえば、トポロジ例の情報を使用すると、このユース ケースの **BGP ASN** フィールドに `65080` と入力します。

- 外部ファブリックをモニタリングするかどうかを決定します。

  - オンプレミスの IPSec デバイスを NDFC で管理する場合は、**[ファブリック モニタ モード（Fabric Monitor Mode）]** フィールドの横にあるボックスをオフにして、このオプションの選択を解除します。

  - オンプレミスの IPsec デバイスが NDFC（Cisco 以外のサードパーティ ファイアウォールなど) によって管理されない場合、ファブリックが監視のみされる場合は、**[ファブリック モニタ モード（Fabric Monitor Mode）]** フィールドの横にあるチェックボックスをオンにします。

図 *14 :*



ステップ 6 必要な一般的な外部ファブリック パラメータ設定を完了します。

`External_Fabric` テンプレートの次のパラメーター タブに入力する必要がありますが、このハイブリッド クラウド トポロジのユース ケースに固有のパラメーターは含まれていません。

- **詳細設定**
- **関連資料**
- **コンフィギュレーションのバックアップ**
- **ブートストラップ**
- **Flow Monitor**

たとえば、**[構成バックアップ（Configuration Backup）]**パラメータ タブで、**[時間単位のファブリック バックアップ（Hourly Fabric Backup）]** フィールドのボックスをチェックして、その機能を有効にすることができます。

詳細については、*[Cisco Nexus ダッシュボード ファブリック コントローラ導入ガイド（Cisco Nexus Dashboard Fabric Controller Deployment Guide）]*、リリース 12.1.2 以降を参照します。

ステップ 7 外部ファブリックの **[ファブリックを作成（Create Fabric）]** ウィンドウで必要な構成を完了したら、**[保存（Save）]** をクリックします。
[LAN ファブリック（LAN Fabrics）] ウィンドウに戻り、作成したばかりの外部ファブリックが表示されます。

次のタスク

オンプレミスの Cisco Catalyst 8000V を外部ファブリックに追加し、オンプレミス Cisco Catalyst 8000V を外部ファブリックに追加 （15 ページ）で提供されている手順を使用して必要なロールを設定します。

オンプレミス Cisco Catalyst 8000V を外部ファブリックに追加

次の手順に従って、オンプレミスの Cisco Catalyst 8000V を外部ファブリックに追加し、Cisco Catalyst 8000V に必要な役割を設定します。

始める前に

NDFC 外部ファブリックを作成 （12 ページ）で提供されている手順を使用して、NDFC 外部ファブリックを作成します。

ステップ 1 **[ローカル エリア ネットワーク（LAN）ファブリック（LAN Fabrics）]** ウィンドウで、作成したばかりの外部ファブリックをクリックします。

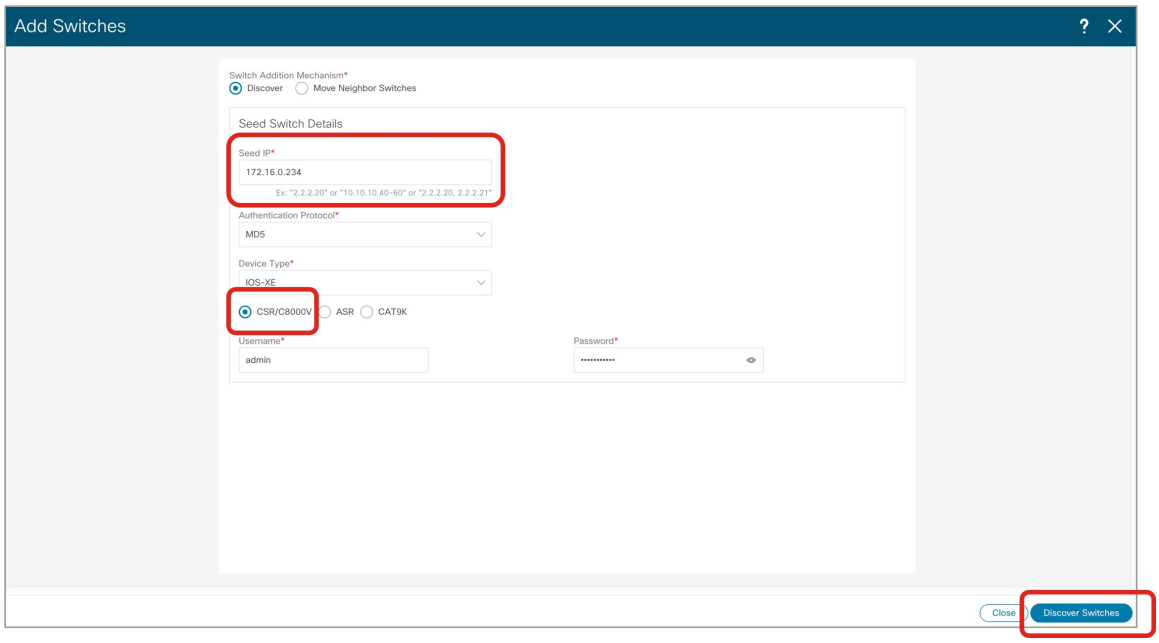
ファブリックの**[概要（Overview）]** ウィンドウが表示されます。

ステップ 2 **[アクション（Actions）]** > **[スイッチを追加（Add Switches）]** をクリックします。
[スイッチの追加（Add Switches）] ウィンドウが表示されます。

ステップ 3 Cisco Catalyst 8000V を検出するために必要な情報を追加し、**[スイッチを発見（Discover Switches）]** をクリックします。

- Cisco Catalyst 8000V の**[シード IP（Seed IP）]** フィールドに必要な情報を入力します。
- **[デバイス タイプ（Device Type）]** フィールド内で `IOS-XE`を選択します。
- `[デバイス タイプ（Device Type）]` フィールドが表示されたら、その下にある **[CSR/C8000V]** オプションを選択します。

図 *15 :*



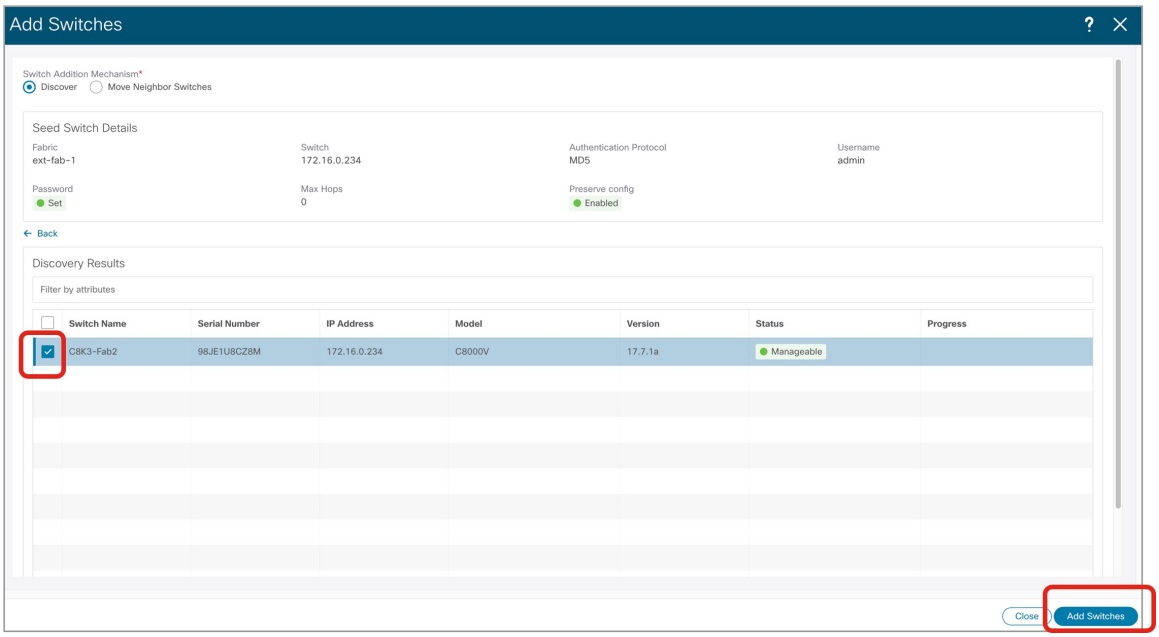
ステップ 4 **[スイッチの検出（Discover Switches）]** をクリックします。

表示される確認ポップアップ ウィンドウで **[確認（Confirm）]** をクリックします。

ステップ 5 Cisco Catalyst 8000V が検出されたら、Cisco Catalyst 8000V を外部ファブリックに追加します。

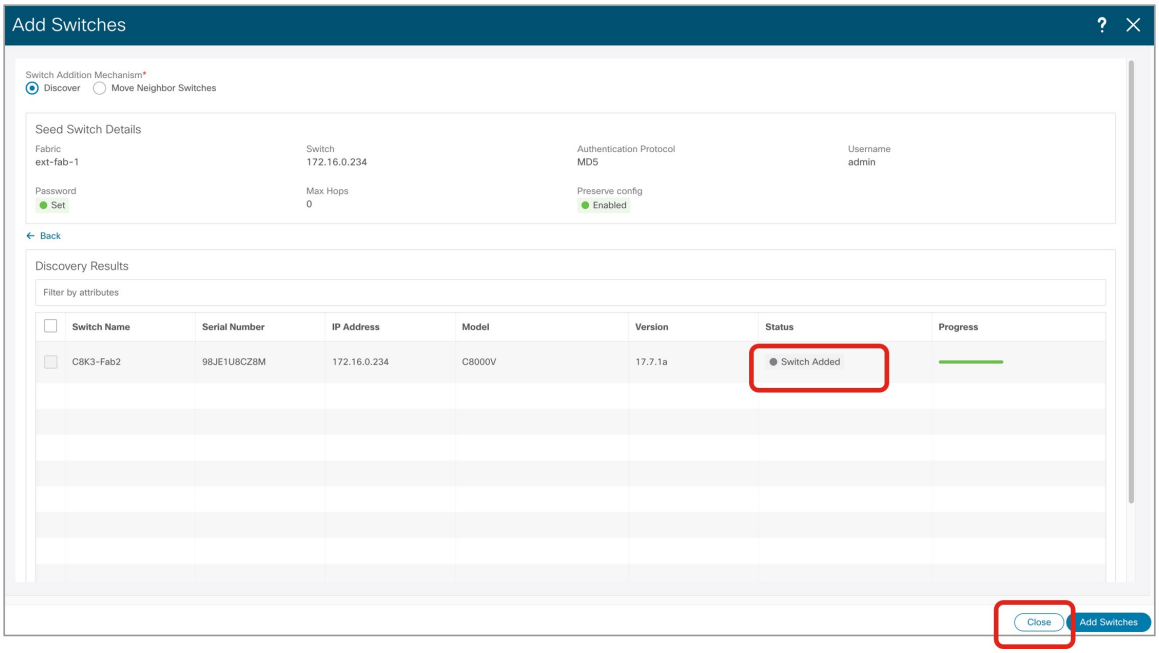
[発見結果（Discovery Results）] エリアで、Cisco Catalyst 8000V を選択し（Cisco Catalyst 8000V の隣のボックスをクリック）、**[スイッチを追加（Add Switches）]** をクリックします。

図 *16 :*



ステータスが **[スイッチが追加されました（Switch Added）]** に変わります。**[閉じる（Close）]** をクリックしてウィンドウを閉じます。

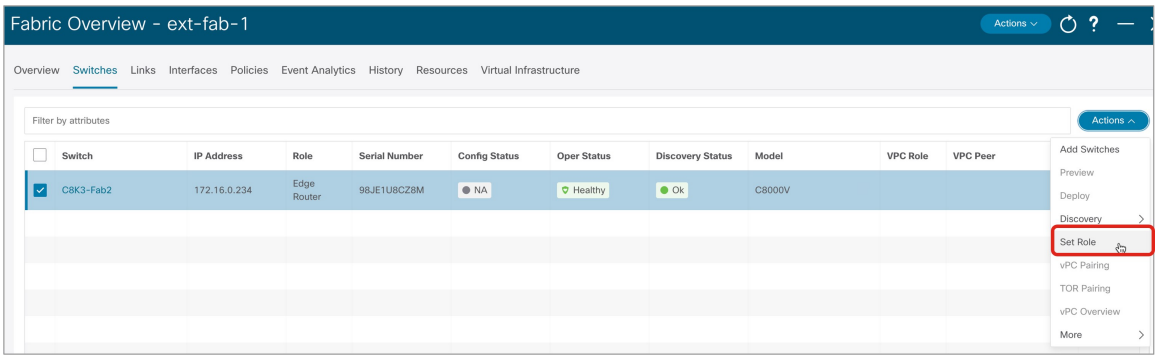
図 *17 :*



ステップ 6 Cisco Catalyst 8000V の役割を[コア ルータ（Core Router）]に設定します。

a) Cisco Catalyst 8000V の横にあるボックスをクリックしてそのルータを選択し、**[アクション（Actions）]**> **[セット ロール（Set Role）]**をクリックします。

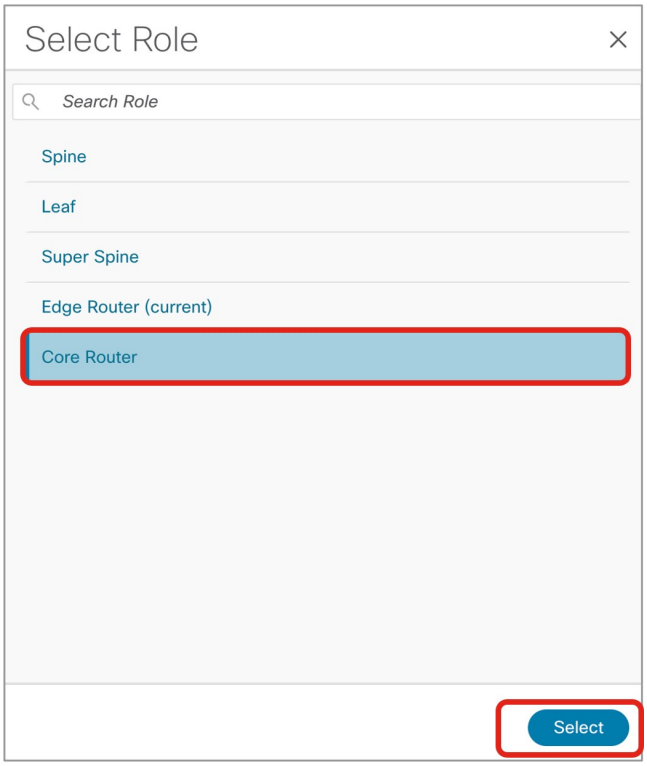
図 *18 :*



b) **[ロールの選択（Select Role）]** リストで `[コア ルータ（Core Router）]` ロールを見つけて選択し、**[選択（Select）]** をクリックします。

NDFC が BGP プロトコルを自動的に有効にするように、すべての Catalyst 8000V を `[コア ルータ（Core Router）]` ロールに設定する必要があります。

図 *19 :*

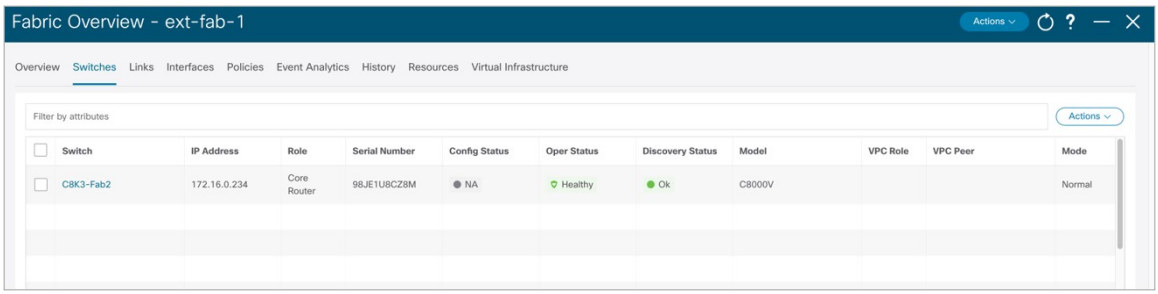


ステップ 7 **[ローカル エリア ネットワーク（LAN）]** > **[ファブリック（Fabrics）]** に移動し、作成した外部ファブリックを選択します。

外部ファブリックの **[概要（Overview）]** ページが表示されます。

ステップ 8 **[スイッチ（Switches）]** タブをクリックして、追加した Cisco Catalyst 8000V が正しく表示されることを確認します。

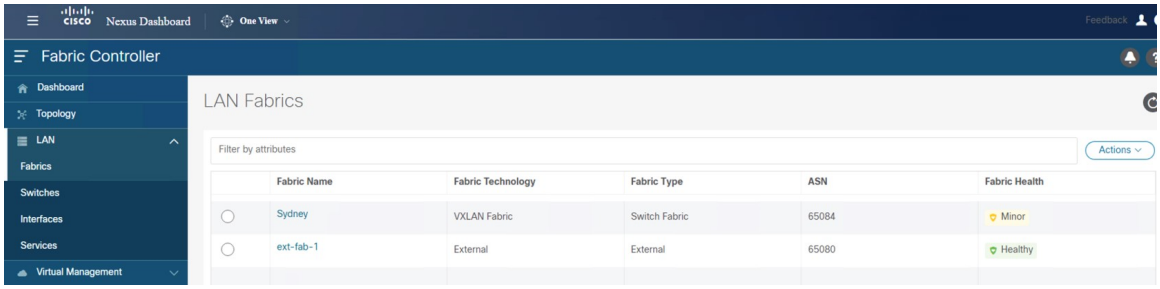
図 *20 :*



ステップ 9 **[アクション（Actions）]** > **[再計算と展開（Recalculate and Deploy）]**をクリックします。

プロセスのこの時点で、**[ローカル エリア ネットワーク（LAN）]** > **[ファブリック（Fabrics）]**に移動すると表示されるように、VXLAN と外部ファブリックは NDFC で構成されます。

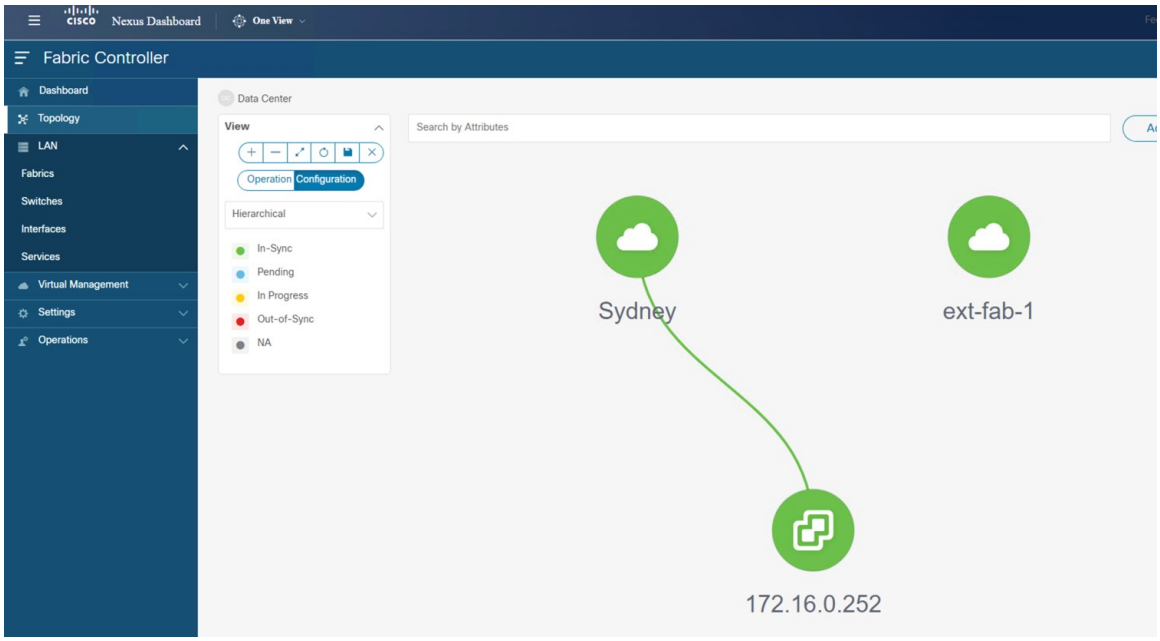
図 *21 :*



[トポロジ（Topology）] ビューを使用して、プロセスのこの時点で次の構成を決定することもできます：

- VXLAN と外部ファブリックの間にまだ接続がないこと：

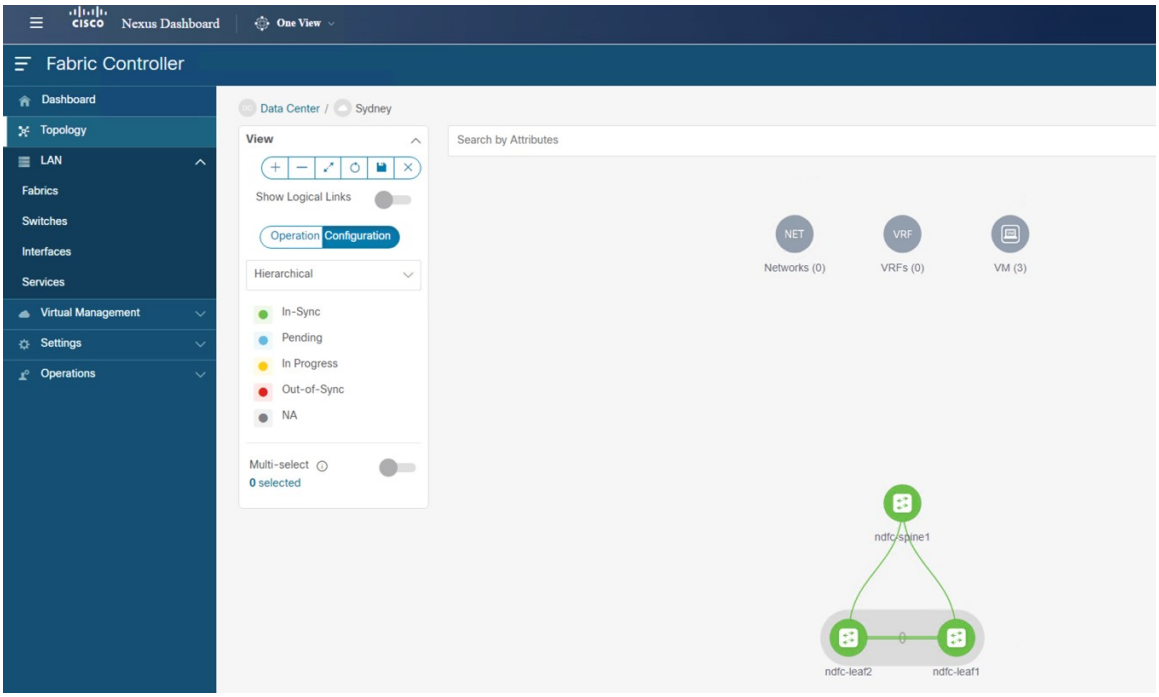
図 *22 :*



この NDFC では VMM ビジュアライザ機能が有効になっているため、IP アドレスが 172.16.0.252 の vCenter アイコンがトポロジ ビューに表示されます。VMM 機能の詳細については、*Cisco NDFC-Fabric コントローラ 構成ガイド*の仮想インフラストラクチャ マネージャの章を参照してください。

- VXLAN ファブリックにネットワークまたは VRF がまだ作成されていないこと：

図 *23 :*



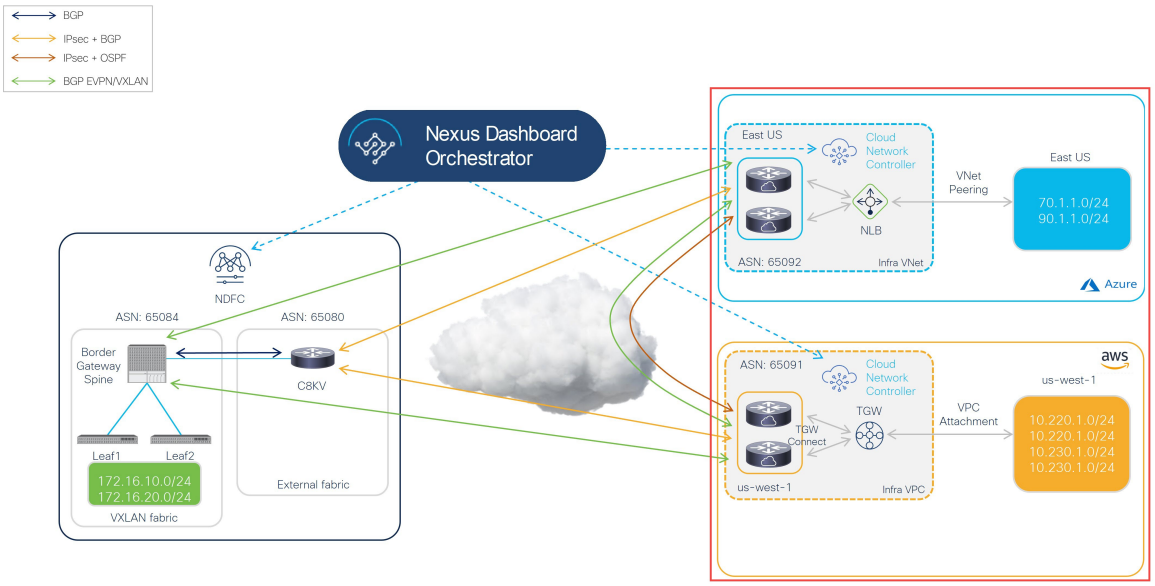
次のタスク

クラウド サイト上のクラウド ネットワーク コントローラを展開します （21 ページ）で提供されている手順を使用して、クラウド サイトにクラウド ネットワーク コントローラを展開します。

クラウド サイト上のクラウド ネットワーク コントローラを展開します

このセクションでは、下で強調表示されているトポロジ例の一部を構成します。

図 *24 :*



ハイブリッド クラウド トポロジの例に基づいて、これらの手順では、クラウド ネットワーク コントローラを介して 2 つのクラウド サイト（AWS および Azure クラウド サイト）をセットアップすることを想定しています。したがって、これらの手順全体で次のドキュメントを参照します。

- *AWS* インストール ガイド、リリース *25.1*（*x*）以降の *Cisco* クラウド ネットワーク コントローラ
- *AWS* ユーザー ガイド、リリース *25.1*（*x*）以降の *Cisco* クラウド ネットワーク コントローラ
- *Azure* インストール ガイド、リリース *25.1*（*x*）以降の *Cisco* クラウド ネットワーク コントローラ
- *Azure* ユーザー ガイド、リリース *25.1*（*x*）以降の *Cisco* クラウド ネットワーク コントローラ

以下のセクションの手順を実行して、クラウド ネットワーク コントローラをクラウド サイトに展開します。

AWS クラウド サイトのクラウド ネットワーク コントローラを展開

これらのセクションの手順に従って、AWS クラウド サイトにクラウド ネットワーク コントローラを展開します。

AWS の詳細設定で必要なパラメータを構成します

このセクションでは、この例のハイブリッドクラウドトポロジ専用に、**[クラウドネットワーク コントローラのセットアップ（Cloud Network Controller Setup）]** ページの **[詳細設定（Advanced Settings）]** エリアで、AWS クラウド サイトに必要な構成を行います。

[Azure インストール ガイドの Cisco クラウド ネットワーク コントローラ（Cisco Cloud Network Controller for AWS Installation Guide）]の「Configuring Cisco Cloud Network Controller Using the Setup Wizard」の章に記載されている手順を使用しますが、**[クラウド ネットワーク コントローラ 設定（Cloud Network Controller Setup）]** ページには、この例のハイブリッド クラウド トポロジの場合のために具体的に構成する必要がある 2 つのエリアがあることに注意してください：

- **コントラクトベースのルーティング（Contract-based routing）**：クラウド ネットワーク コントローラは、次の 2 種類のモードをサポートしています。
  - 契約ベースのルーティング
  - ルート マップベースのルーティング

  契約ベースのルーティングとは、EPG 間の契約が VRF 間のルーティングを駆動することを意味しますが、このタイプの契約ベースのルーティングは NDFC では使用できないため、この特定の例のハイブリッド クラウド トポロジでは、契約ベースのルーティングをオフにして、代わりにルート マップ ベースのルーティングを使用します。詳細については、AWS ユーザー ガイドの Cisco クラウド ネットワーク コントローラ、リリース 25.1（x）以降の「ルーティング ポリシー」および「グローバル Inter-VRF ルート リーク ポリシー」セクションを参照してください。
- **クラウド ネットワーク コントローラのアクセス権限**：デフォルトでは、クラウド ネットワーク コントローラにはルーティングとセキュリティのアクセス権限があります。つまり、クラウド ネットワーク コントローラはネットワークを自動化できるだけでなく、クラウド上のセキュリティ グループを自動化および構成することもできます。クラウド ネットワーク コントローラがセキュリティ グループを自動化して構成する場合、EPG と契約も構成する必要があります。ただし、EPG と契約は、ルーティングの自動化のみが必要な NDFC エンド ユーザーには適用されません。NDO および NDFC とうまく統合するには、**クラウド ネットワーク コントローラのアクセス権限**オプションを**ルーティングのみ**に設定する必要があります。

ステップ 1 AWS の Cisco Cloud Network Controller にログインします。

ステップ 2 この例のハイブリッド クラウド トポロジ用に、1 番目のクラウド サイトである AWS クラウド サイトをセットアップするプロセスを開始します。

AWS インストールガイドの Cisco クラウド ネットワーク コントローラ、リリース 25.1（x）以降の最初の数章には、このハイブリッド クラウド トポロジのユース ケースに固有ではない一般的な情報が含まれているため、そのドキュメントのこれらの章の手順を完了してから、ここに戻ります：

- 概要

- Cisco クラウド ネットワーク コントローラのインストールの準備
- Cisco Cloud Network Controller のクラウド形成テンプレート情報の構成

ステップ 3 Cisco Cloud Network Controller GUI で、インテントアイコン（）をクリックし、**[Cloud Network Controller セットアップ（Cloud Network Controller Setup）]** を選択します。

[基本を構成しましょう（Let's Configure the Basics）] ページが表示されます。

ステップ 4 **[詳細設定（Advanced Settings）]** エリアを探し、**[構成の編集（Edit Configuration）]** をクリックします。

ステップ 5 **[詳細設定（Advanced Settings）]** ページで、次の構成を設定します。

- **[契約に基づいたルーティング（Contract Based Routing）]**：ボックスがオフになっていることを確認します (この機能が有効になっていないことを確認します)。これにより、契約ベースのルーティングが無効になり、代わりにルート マップ ベースのルーティングが使用されます。
- **クラウド ネットワーク コントローラのアクセス権限**：**[ルーティングのみ（Routing Only）]** オプションを選択します。

ステップ 6 [保存して続行（Save and Continue）] をクリックします。

[基本を構成しましょう（Let's Configure the Basics）]ページに戻ります。

次のタスク

AWS のリージョン管理の必要なパラメータを構成します （24 ページ） の手順を実行します。

AWS のリージョン管理の必要なパラメータを構成します

このセクションでは、この例のハイブリッド クラウド トポロジー専用に、**[クラウド ネットワーク コントローラ（Cloud Network Controller Setup）]**のセットアップ ページの**[リージョン管理（Region Management）]** エリアで AWS クラウド サイトに必要な構成を行います。

始める前に

AWS の詳細設定で必要なパラメータを構成します （23 ページ） に挙げられている手順を完了します。

ステップ 1 **[リージョン管理（Region Management）]** エリアを探して適切なボタンをクリックします。

クラウド ネットワーク コントローラを初めてセットアップする場合は **[開始（Begin）]** をクリックし、以前にこのクラウド ネットワーク コントローラでリージョン管理を既に構成している場合は **[構成の編（Edit Configuration）]** をクリックします。

ステップ 2 AWS トランジット ゲートウェイを有効化

普段、Transit Gateway を使用して、リージョン内および TGW ピアリングがサポートされているリージョン間の接続に VPN トンネルを使用しないようにします。詳細については、ドキュメント「*AWS トラン*

ジット ゲートウェイまたは *AWS* トランジット ゲートウェイ コネクトを使用した *VPC* 間の帯域幅の増加」を参照してください。

特に、このハイブリッド クラウド トポロジのユース ケースの例では、**[トランジット ゲートウェイの使用（Use Transit Gateway）]** エリアで、**[有効化（Enable）]** の横にあるチェックボックスをクリックして AWS Transit Gateway を使用します。これにより、以降の手順で TGW Connect を有効にするために必要なハブ ネットワークを追加できます。

ステップ 3 **[管理するリージョン（Regions to Manage）]** 領域で、Cisco Cloud Network Controller のホーム リージョンが選択されていることを確認します。

Cisco Cloud ネットワーク コントローラを AWS に最初に展開したとに選択したリージョンは、ホーム リージョンであり、このページで既に選択されいているはずです。これは、Cisco Cloud Network Controller が展開されるリージョン（Cisco Cloud Network Controller によって管理されるリージョン）で、[リージョン（Region）]列に「`Cisco Cloud Network Controller`」というテキストが表示されます。

ステップ 4 Cisco クラウド ネットワーク コントローラ で追加のリージョンを管理します。他のリージョンで Inter-VPC 通信と Hybrid-Cloud、Hybrid Multi-Cloud、または Multi-Cloud 接続を行うように Cisco Catalyst 8000Vs を展開する場合は、追加のリージョンを選択します。

Cisco Catalyst 8000V は、Cisco Cloud Network Controller が導入されているホーム リージョンを含む、最大 4 つのリージョンにハイブリッド クラウドおよびマルチクラウド接続を提供できます。

ステップ 5 リージョンにローカルにクラウド ルータを展開するには、そのリージョンの **Catalyst 8000Vs** チェックボックスにチェック マークをつけるためにクリックします。

Catalyst 8000V が展開されているリージョンが少なくとも 1 つ必要です。ただし、このページで複数のリージョンを選択した場合は、選択したすべてのリージョンに Catalyst 8000V を設定する必要はありません。

ステップ 6 AWS トランジット ゲートウェイ統計を使用する場合は、1 つ以上のリージョンの **[TGW 統計（TGW Stats）]** 列のボックスをオンにします。

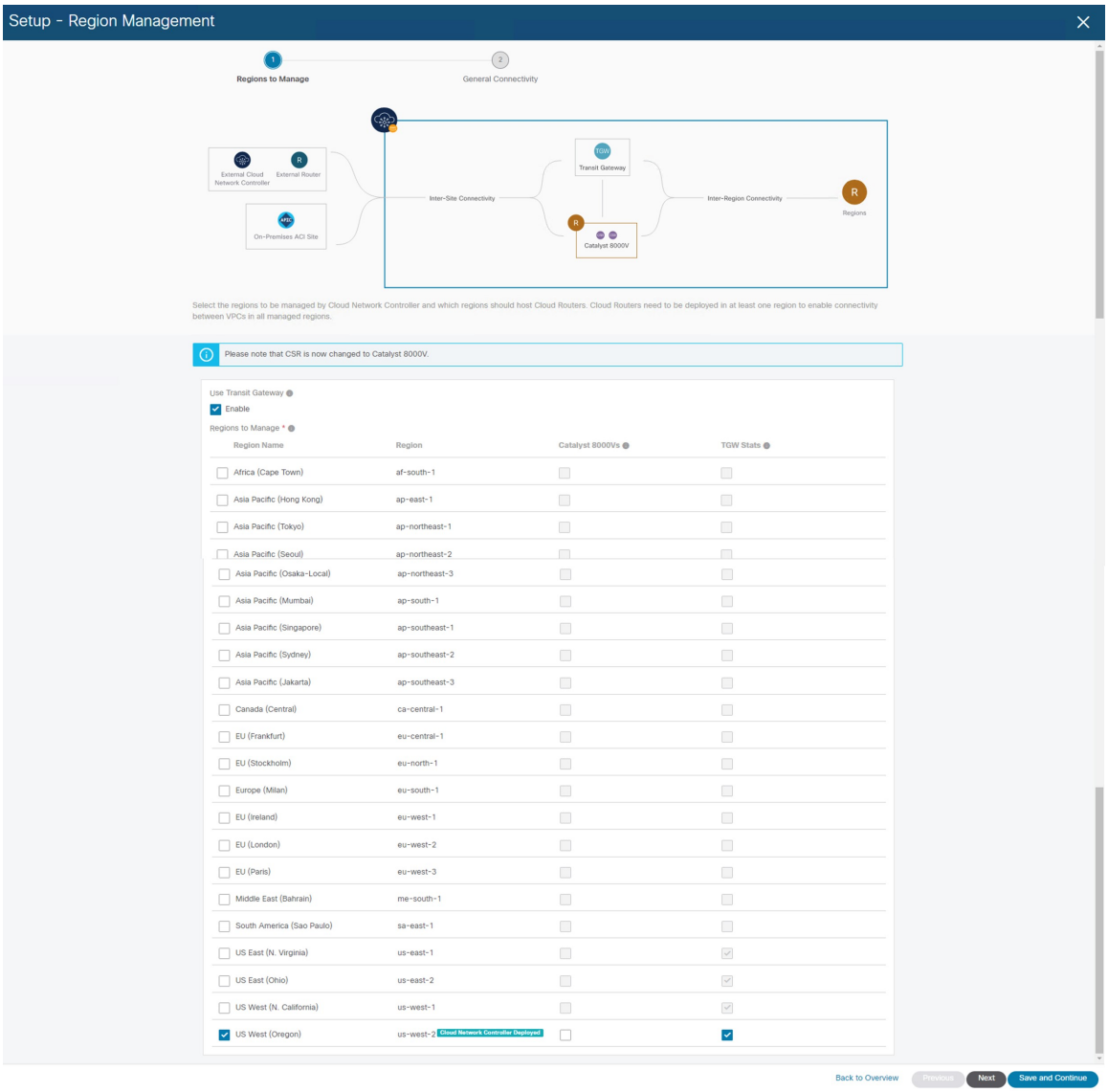
チェックボックスをオンにすると、指定したリージョンのインフラ テナントの AWS トランジット ゲートウェイ トラフィック統計の収集が有効になります。

（注） AWS トランジット ゲートウェイの統計情報を収集するには、フロー ログを作成する必要もあります。*AWS* ユーザー ガイド の *Cisco* クラウド *APIC* リリース 25.1（x）以降の「Cisco Cloud APIC Statistics」の章の「Enabling VPC Flow Logs」セクションを参照してください。

特に、この例のハイブリッド クラウド トポロジのユース ケースでは、次のようになります。

- 米国東部（バージニア北部）リージョンと米国西部（北カリフォルニア）リージョン（us-east-1 および us-west-1 リージョン）の隣のチェック ボックスにチェック マークを付けます。
- Cisco クラウド ネットワーク コントローラ ホーム リージョンの **Catalyst 8000V** および **TGW Stats** 列のチェック ボックスにチェック マークを付けます。

図 *25 :*



ステップ 7 適切なリージョンをすべて選択したら、ページの下部にある[Next]をクリックします。

[General Connectivity]ページが表示されます。

ステップ 8 **[一般接続（General Connectivity）]** ページで必要な構成を行います。

詳細については、*[AWS 設置ガイドの Cisco クラウド ネットワーク コントローラ（Cisco Cloud Network Controller for AWS Installation Guide）]*リリース 25.1（x）以降のセットアップウィザードを使用した Cisco Cloud Network Controller の構成の章を参照してください。

特に、このハイブリッド クラウド トポロジのユース ケースの例では、次の手順の手順を使用してハブ ネットワークを追加します。

Cisco クラウド ネットワーク コントローラ では、2 つ以上の AWS Transit Gateway の集合を**[ハブ ネットワーク（hub network）]**と呼びます。ハブ ネットワークは、VRF のネットワーク分離を提供します。VRF のグループをハブ ネットワークに接続して、VRF のグループを他のハブ ネットワークに接続されている他の VRF から分離することができます。ハブ ネットワークは、リージョンごとに少なくとも 2 つの AWS Transit Gateway を作成します。

ステップ 9 **[ハブ ネットワーク（Hub Network）]** 領域で、**[ハブ ネットワークの追加（Add Hub Network）]** をクリックします。

[ハブ ネットワークの追加（Add Hub Network）] ウィンドウが表示されます。

ステップ 10 **[名前（Name）]** フィールドにハブ ネットワークの名前を入力します。

ステップ 11 [BGP Autonomous System Number] フィールドに、AWS でゼロを入力して番号を選択するか、各ハブネットワークの値を 64512 ー 65534 の範囲で入力し、フィールドの横にあるチェック マークをクリックします。

たとえば、ハイブリッド クラウド トポロジの例の情報を使用すると、このフィールドに `65091` と入力します。

ステップ 12 AWS Transit Gateway Connect 機能を有効にする場合は、**[TGW Connect]** フィールドで **[有効化（Enable）]** の横のチェック ボックスをクリックします。

このハイブリッド クラウド トポロジのユース ケースの例では、AWS Transit Gateway Connect 機能を有効にします。詳細については、*AWS* トランジット ゲートウェイまたは *AWS* トランジット ゲートウェイ コネクトを使用した *VPC* 間の帯域幅の増加 を参照してください。

ステップ 13 **[CIDR]** 領域で、**[Add CIDR]** をクリックします。

これは、AWS トランジット ゲートウェイ接続 CIDR ブロックで、トランジット ゲートウェイ側の接続ピア IP アドレス（GRE 外部ピア IP アドレス）として使用されます。

a) **[Region（リージョン）]** フィールドで、**[リージョンを選択（Select Region）]** をクリックして適切なリージョンを選択します。

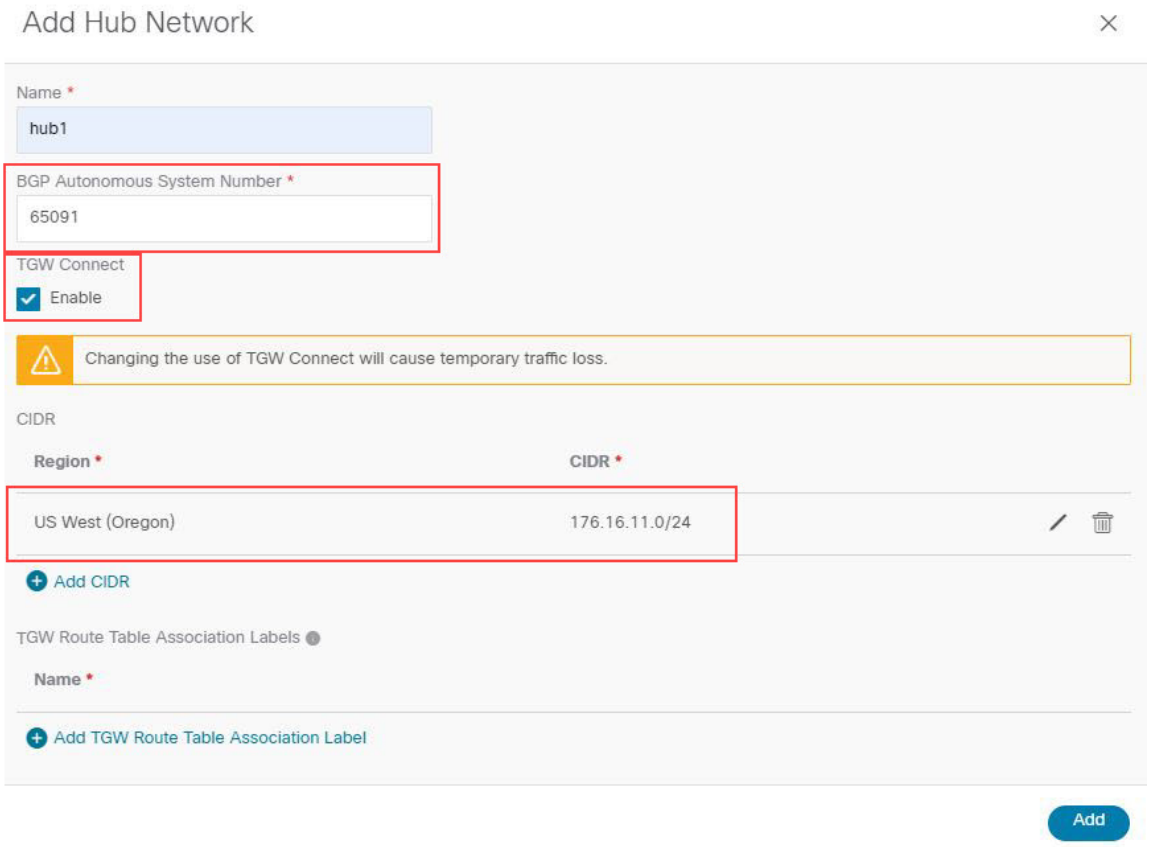
b) **CIDR** フィールドに、中継ゲートウェイ側の接続ピア IP アドレスとして使用される CIDR ブロックを入力します。

図 *26 :*

c) この CIDR ブロックのこれらの値を受け入れるには、チェック マークをクリックします。

d) AWS トランジット ゲートウェイ接続機能を使用するすべての管理対象リージョンに対して、これらの管理対象リージョンのそれぞれに使用する CIDR ブロックを追加します。

図 *27 :*



ステップ 14 通常どおりに残りの構成を完了します。

- **[一般接続（General Connectivity）]**ページの残りの構成を通常どおりに完了し、**[保存して続行（Save and Continue）]** をクリックします。
- 通常どおり、**[スマート ライセンス（Smart Licensing）]** ページで必要な設定を完了します。

詳細については、[AWS 設置ガイドの Cisco クラウド ネットワーク コントローラ（Cisco Cloud Network Controller for AWS Installation Guide）]リリース 25.1（x）以降のセットアップウィザードを使用した Cisco Cloud Network Controller の構成の章を参照してください。

プロセスのこの時点で、Cisco クラウド ネットワーク コントローラの最初のクラウド サイト（この例のハイブリッド クラウド トポロジでは AWS クラウド サイト）の基本設定が完了しました。次の手順に進んで、Cisco クラウド ネットワーク コントローラの 2 番目のクラウド サイト（この例のハイブリッド クラウド トポロジでは、Azure クラウド サイト）の基本構成を完了します。

ステップ 15 必要に応じて、AWS の Direct Connect を構成します。

Catalyst 8000V ルータからクラウド ネットワークへの接続にプライベート接続が必要な場合は、直接接続を構成します。AWS 用の 直接接続 の構成については、[AWS ユーザー ガイドの Cisco クラウド ネット

ワーク コントローラ（Cisco Cloud Network Controller for AWS User Guide]リリース 25.1（x）以降を参照してください。

次のタスク

Azure クラウド サイトのクラウド ネットワーク コントローラを展開 （29 ページ）で提供されている手順を使用して、2 番目のクラウドサイト（Azure クラウドサイト）にクラウドネットワーク コントローラを展開します。

Azure クラウド サイトのクラウド ネットワーク コントローラを展開

これらのセクションの手順に従って、Azure クラウド サイトにクラウド ネットワーク コントローラを展開します。

Azure の詳細設定で必要なパラメータを構成します

このセクションでは、この例のハイブリッドクラウドトポロジ専用に、**[クラウド ネットワーク コントローラのセットアップ（Cloud Network Controller Setup）]** ページの **[詳細設定（Advanced Settings）]** エリアで、Azure クラウド サイトに必要な構成を行います。

AWS クラウド サイトに対して行ったのと同じ構成を Azure クラウド サイトに対して行います。

[Azure インストール ガイドの Cisco クラウド ネットワーク コントローラ（Cisco Cloud Network Controller for Azure Installation Guide）]の「Configuring Cisco Cloud Network Controller Using the Setup Wizard」の章に記載されている手順を使用しますが、**[クラウド ネットワーク コントローラ 設定（Cloud Network Controller Setup）]** ページには、この例のハイブリッド クラウド トポロジの場合のために具体的に構成する必要がある 2 つのエリアがあることに注意してください：

- **コントラクトベースのルーティング（Contract-based routing）**：クラウド ネットワーク コントローラは、次の 2 種類のモードをサポートしています。
  - 契約ベースのルーティング
  - ルート マップベースのルーティング

  契約ベースのルーティングとは、EPG 間の契約が VRF 間のルーティングを駆動することを意味しますが、このタイプの契約ベースのルーティングは NDFC では使用できないため、この特定の例のハイブリッド クラウド トポロジでは、契約ベースのルーティングをオフにして、代わりにルート マップ ベースのルーティングを使用します。詳細については、AWS ユーザー ガイドの Cisco クラウド ネットワーク コントローラ、リリース 25.1（x）以降の「ルーティング ポリシー」および「グローバル Inter-VRF ルート リーク ポリシー」セクションを参照してください。
- **クラウド ネットワーク コントローラのアクセス権限**：デフォルトでは、クラウド ネットワーク コントローラにはルーティングとセキュリティのアクセス権限があります。つま

り、クラウド ネットワーク コントローラはネットワークを自動化できるだけでなく、クラウド上のセキュリティ グループを自動化および構成することもできます。クラウドネットワーク コントローラがセキュリティ グループを自動化して構成する場合、EPG と契約も構成する必要があります。ただし、EPG と契約は、ルーティングの自動化のみが必要な NDFC エンド ユーザーには適用されません。NDO および NDFC とうまく統合するには、**クラウド ネットワーク コントローラのアクセス権限**オプションを**ルーティングのみ**に設定する必要があります。

始める前に

AWS クラウド サイトのクラウド ネットワーク コントローラを展開 （22 ページ）で提供されている手順を使用して、最初のクラウド サイト（AWS クラウド サイト）にクラウド ネットワーク コントローラを展開します。

ステップ 1 Azure の Cisco クラウド ネットワーク コントローラにログインします。

ステップ 2 この例のハイブリッド クラウド トポロジ用に、2 番目のクラウド サイトである Azure クラウド サイトをセットアップするプロセスを開始します。

Azure インストールガイドの Cisco クラウド ネットワーク コントローラ、リリース 25.1（x）以降の最初の数章には、このハイブリッド クラウド トポロジのユース ケースに固有ではない一般的な情報が含まれているため、そのドキュメントのこれらの章の手順を完了してから、ここに戻ります：

- 概要
- Cisco クラウド ネットワーク コントローラのインストールの準備
- Azure での Cisco Cloud Network Controller の展開

ステップ 3 Cisco Cloud Network Controller GUI で、インテント アイコン（）をクリックし、**[Cloud Network Controller セットアップ（Cloud Network Controller Setup）]** を選択します。

[基本を構成しましょう（Let's Configure the Basics）] ページが表示されます。

ステップ 4 **[詳細設定（Advanced Settings）]** エリアを探し、**[構成の編集（Edit Configuration）]** をクリックします。

ステップ 5 **[詳細設定（Advanced Settings）]** ページで、次の構成を設定します。

- **[契約に基づいたルーティング（Contract Based Routing）]**：ボックスがオフになっていることを確認します (この機能が有効になっていないことを確認します)。これにより、契約ベースのルーティングが無効になり、代わりにルート マップ ベースのルーティングが使用されます。
- **クラウド ネットワーク コントローラのアクセス権限**：**[ルーティングのみ（Routing Only）]** オプションを選択します。

ステップ 6 [保存して続行（Save and Continue）] をクリックします。

[基本を構成しましょう（Let's Configure the Basics）]ページに戻ります。

次のタスク

Azure のリージョン管理で必要なパラメーターを構成する （31 ページ） の手順を実行します。

Azure のリージョン管理で必要なパラメーターを構成する

このセクションでは、この例のハイブリッド クラウド トポロジー専用に、**[クラウド ネットワーク コントローラ（Cloud Network Controller Setup）]**のセットアップ ページの**[リージョン管理（Region Management）**エリアで Azure クラウド サイトに必要な構成を行います。

始める前に

Azure の詳細設定で必要なパラメータを構成します （29 ページ） の手順を実行します。

ステップ 1 **[リージョン管理（Region Management）**エリアを探して適切なボタンをクリックします。

クラウド ネットワーク コントローラを初めてセットアップする場合は **[開始（Begin）]** をクリックし、以前にこのクラウド ネットワーク コントローラでリージョン管理を既に構成している場合は **[構成の編（Edit Configuration）]** をクリックします。

ステップ 2 **[内部ネットワークの接続（Connectivity for Internal Network）]** エリア内の **[仮想ネットワーク ピアリング（Virtual Network Peering）]**が自動的に有効化されていることを検証します。

グローバル レベルの VNet ピアリングは、**[内部ネットワークの接続（Connectivity for Internal Network）]** エリアで設定されます。これにより、Cisco Cloud Network Controller レベルで VNet ピアリングが有効になり、CCR を使用してすべてのリージョンに NLB が展開されます。リリース5.1（2）以降では、グローバルレベルのVNetピアリングはデフォルトで有効になっており、無効にすることはできません。詳細については、*[Azure 向け Cloud APIC の VNet ピアリングを構成する（Configuring VNet Peering for Cloud APIC for Azure）]*を参照してください。

ステップ 3 **[管理するリージョン（Regions to Manage）]** 領域で、Cisco Cloud Network Controller のホーム リージョンが選択されていることを確認します。

Cisco Cloud ネットワーク コントローラを AWS に最初に展開したとに選択したリージョンは、ホーム リージョンであり、このページで既に選択されいているはずです。これは、Cisco Cloud Network Controller が展開されるリージョン（Cisco Cloud Network Controller によって管理されるリージョン）で、[リージョン（Region）]列に「`Cisco Cloud Network Controller`」というテキストが表示されます。

（注） Azure VNet ピアリングは自動的に有効化されているので、Cisco クラウド ネットワーク コントローラ ホーム リージョンの **Catalyst 8000Vs** カラムのボックスがチェックを既にされていない場合、チェックする必要があります。

ステップ 4 Cisco クラウドネットワーク コントローラ で追加のリージョンを管理します。他のリージョンで Inter-VNet 通信と Hybrid-Cloud、Hybrid Multi-Cloud、または Multi-Cloud 接続を行うように Cisco Catalyst 8000Vs を展開する場合は、追加のリージョンを選択します。

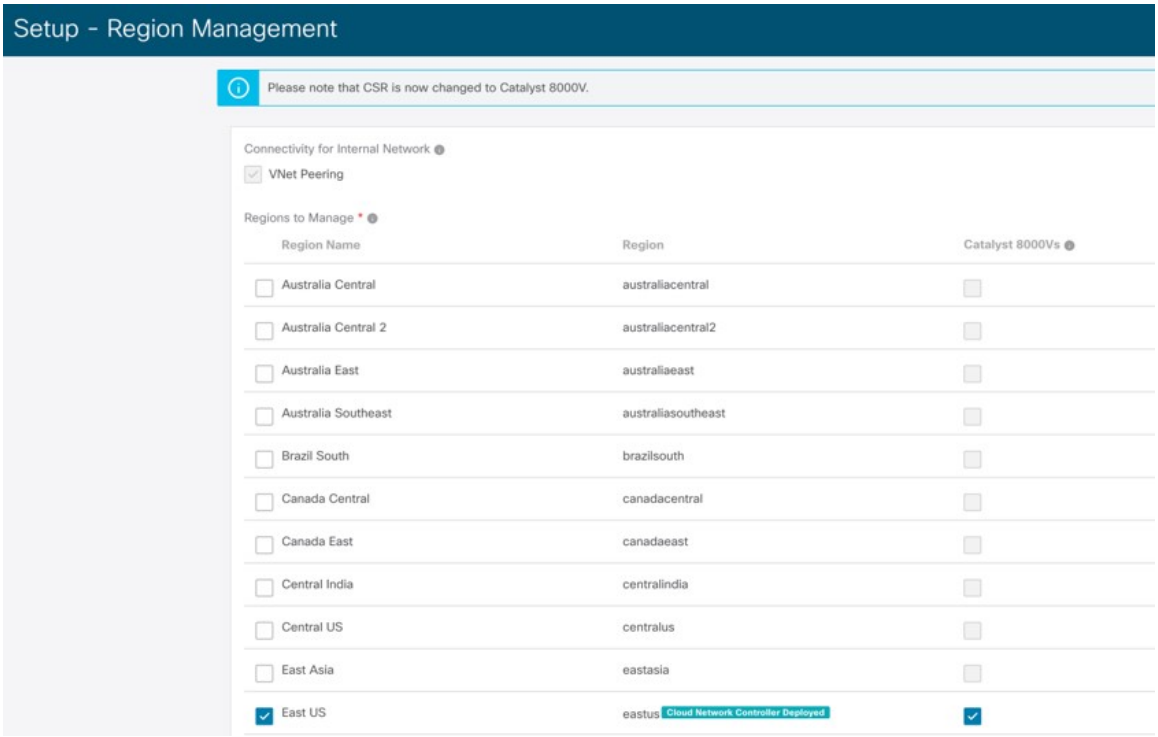
Cisco Catalyst 8000V は、Cisco Cloud Network Controller が導入されているホーム リージョンを含む、最大 4 つのリージョンにハイブリッド クラウドおよびマルチクラウド接続を提供できます。

ステップ 5 リージョンにローカルにクラウド ルータを展開するには、そのリージョンの **Catalyst 8000Vs** チェック ボックスにチェック マークをつけるためにクリックします。

Catalyst 8000V が展開されているリージョンが少なくとも 1 つ必要です。ただし、このページで複数のリージョンを選択した場合は、選択したすべてのリージョンに Catalyst 8000V を設定する必要はありません。

特に、このハイブリッド クラウド トポロジのユース ケースの例では、Cisco クラウド ネットワーク コントローラ ホーム リージョンの **Catalyst 8000V** 列のチェック ボックスにチェック マークを付けます。

図 *28 :*



ステップ 6 適切なリージョンをすべて選択したら、ページの下部にある[Next]をクリックします。

[General Connectivity]ページが表示されます。

ステップ 7 **[一般接続（General Connectivity）]** ページで必要な構成を行います。

詳細については、*[Cisco Cloud Network Controller for Azuru 設置ガイド（Cisco Cloud Network Controller for Azure Installation Guide）]* リリース 25.1（x）以降のセットアップウィザードを使用した Cisco Cloud Network Controller の構成の章を参照してください。

特に、このハイブリッドクラウドトポロジのユース ケースの例では、次の手順の手順を使用して、Cisco Catalyst 8000V に対して次の設定を行います。

ステップ 8 **[全般（General）]** エリアの **[クラウド ルータのサブネット プール（Subnet Pools for Cloud Routers）]** フィールドで、Catalyst 8000V のサブネットを追加する場合は、**[クラウド ルータのサブネット プールの追加（Add Subnet Pool for Cloud Routers）]** をクリックします。

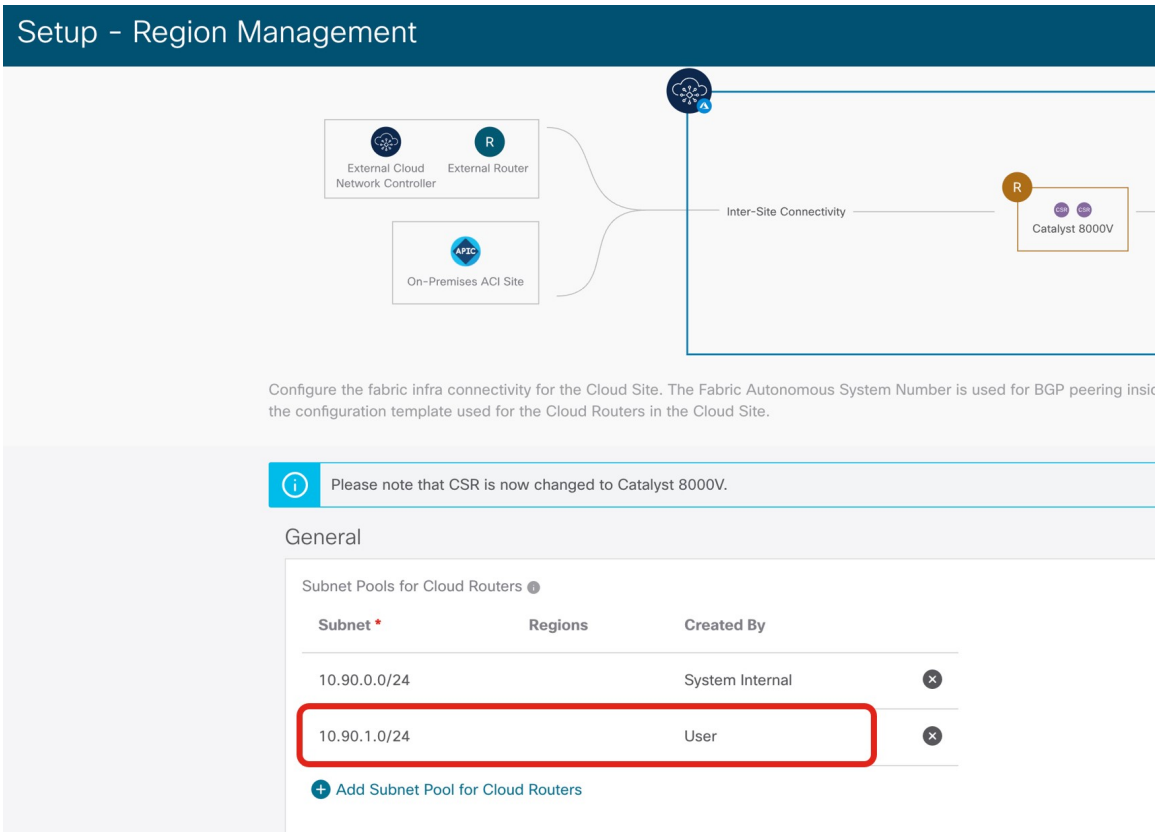
最初のサブネットプールが自動的に入力されます（System Internalとして表示）。このサブネットプールのアドレスは、Cisco Cloud Network Controller で管理する必要がある追加のリージョンのリージョン間接続に使用されます。このフィールドに追加するサブネットプールは、マスク/24の有効なIPv4サブネットである必要があります。

次の状況では、この手順で Catalyst 8000V のサブネットを追加します。

- Cisco Cloud Network Controller ホーム リージョンに Catalyst 8000V を展開している場合は、自動的に生成される[システム内部（System Internal）]サブネット プールに加えて、1 つのサブネット プールを追加します。
- 前のページで Cisco Cloud Network Controller により管理対象となる追加のリージョンを選択した場合：
  - 管理対象リージョンごとに 2ー4 の Catalyst 8000V を持つすべての管理対象リージョンに *1* つのサブネットプールを追加します（このページの**[リージョンごとのルータの数（Number of Routers Per Region）]** フィールドに**2**、**3**、または **4** を入力した場合）。
  - 管理対象リージョンごとに 5 つ以上の Catalyst 8000V があるすべての管理対象リージョンに *2* つのサブネットプールを追加します（このページの **[リージョンごとのルータの数（Number of Routers Per Region）]** フィールドに **5ー8** を入力した場合）。

特に、このハイブリッド クラウド トポロジのユース ケースの例では、サブネット エントリとして `10.90.1.0/24` を使用してサブネット プールを 1 つ追加します。

図 *29 :*

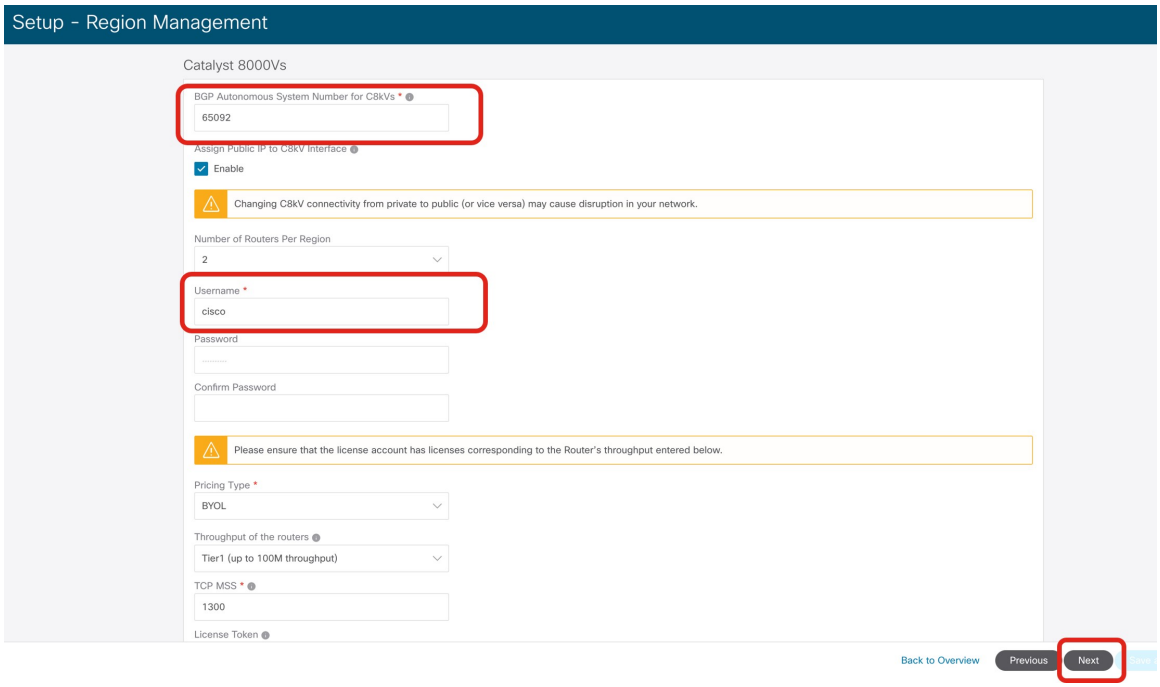


ステップ 9 **Catalyst 8000V** エリアの **[C8kVs の BGP 自律システム番号（BGP Autonomous System Number for C8kVs）]** フィールドに、このサイトに固有の BGP 自律システム番号（ASN）を入力します。

BGP自律システム番号は1ー65534の範囲で指定できます。追加の制限は、*[Cisco Cloud Network Controller for Azuru 設置ガイド（Cisco Cloud Network Controller for Azure Installation Guide）]*リリース 25.1（x）以降のセットアップウィザードを使用した Cisco クラウド ネットワーク コントローラの構成の章を参照してください。

具体的には、このハイブリッド クラウド トポロジのユース ケースの例では、**[C8kV の BGP 自律システム番号（BGP Autonomous System Number for C8kVs）]**フィールドに 65092 を入力します。

図 *30 :*



ステップ 10 **[次へ（Nexr）]** をクリックし、通常どおりに残りの構成を完了します。

- **[一般接続（General Connectivity）]** ページの残りの構成を通常どおりに完了し、**[保存して続行（Save and Continue）]** をクリックします。
- 通常どおり、**[スマート ライセンス（Smart Licensing）]** ページで必要な設定を完了します。

詳細については、*[Cisco Cloud Network Controller for Azuru 設置ガイド（Cisco Cloud Network Controller for Azure Installation Guide）]* リリース 25.1（x）以降のセットアップウィザードを使用した Cisco Cloud Network Controller の構成の章を参照してください。

ステップ 11 必要に応じて、Azure の ExpressRoute を構成します。

Catalyst 8000V ルータからクラウドネットワークへの接続にプライベート接続が必要な場合は、ExpressRoute を構成します。Azure 用の ExpressRoute の構成については、*[Azure ユーザー ガイドの Cisco クラウド ネットワーク コントローラ（Cisco Cloud Network Controller for Azure User Guide]* リリース 25.1（x）以降を参照してください。

次のタスク

NDFC とクラウド サイトを ND と NDO に導入準備する （36 ページ） で提供されている手順を使用して、NDFC 管理サイト（VXLAN ファブリック、外部ファブリック、およびクラウド サイト）を Nexus ダッシュボード（ND）および Nexus ダッシュボード オーケストレータ（NDO）にオンボードします。

NDFC とクラウド サイトを ND と NDO に導入準備する

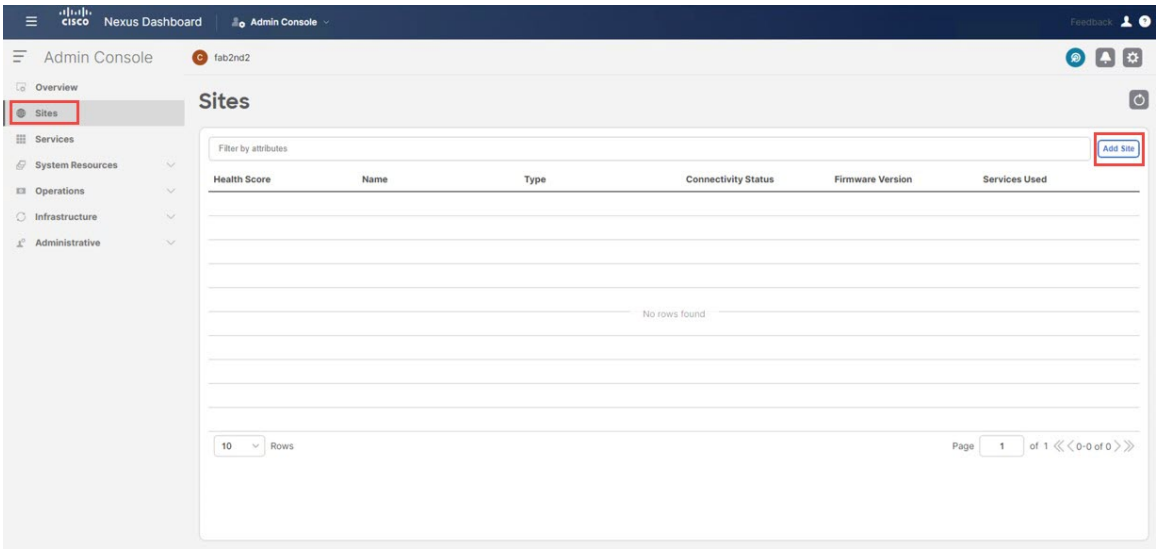
始める前に

- NDFC VXLAN ファブリックを作成（4ページ）で提供されている手順を使用して、NDFC VXLAN ファブリックを作成します。
- NDFC 外部ファブリックを作成 （12 ページ）で提供されている手順を使用して、NDFC 外部ファブリックを作成します。
- AWS クラウド サイトのクラウド ネットワーク コントローラを展開 （22 ページ）で提供されている手順を使用して、最初のクラウド サイトにネットワーク クラウド コントローラを展開します。
- Azure クラウド サイトのクラウド ネットワーク コントローラを展開 （29 ページ）で提供されている手順を使用して、2番目のクラウドサイトにネットワーク クラウドコントローラを展開します。

ステップ 1 Nexus Dashboard Orchestrator（NDO）を使用して Nexus Dashboard（ND）クラスタにログインします。

ステップ 2 Nexus ダッシュボードで、**[サイト（Sites）]** > **[サイトを追加（Add Site）]** をクリックします。

図 *31 :*



[サイトの追加（Add Site）] ページが表示されます。

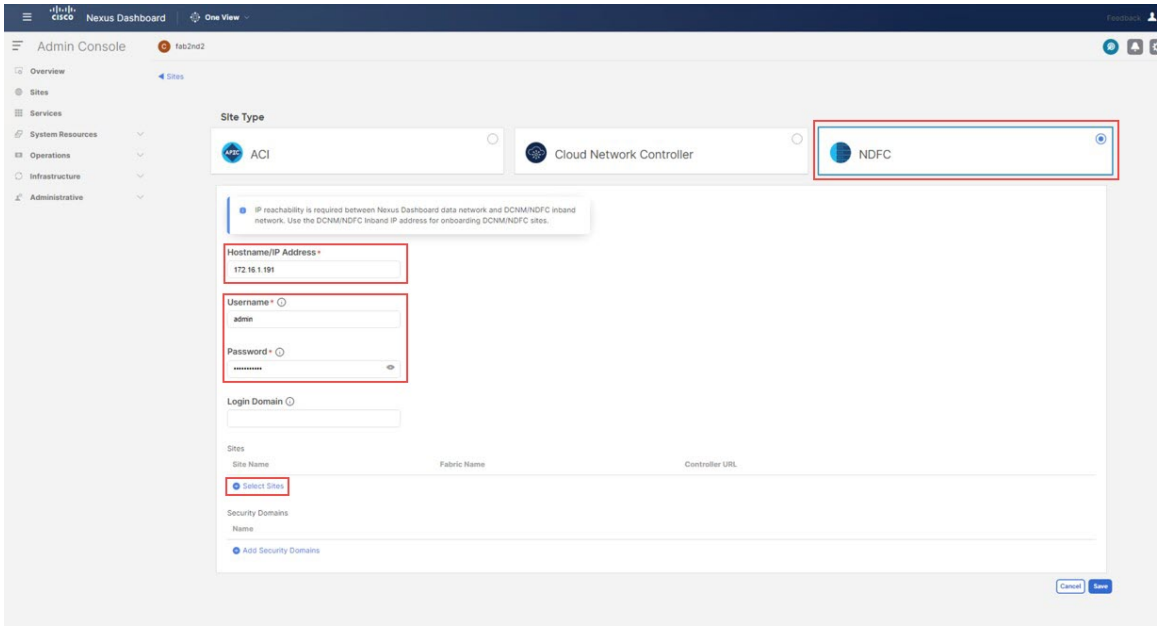
ステップ 3 **[サイトの追加（Add Site）]** ページの **[NDFC]** ボックスをクリックします。

ステップ 4 NDFC サイトを追加するために必要な情報を入力します。

- **[ホスト名/IP アドレス（Hostname/IP Address）]**フィールド内で NDFC のデータ インターフェイス IP アドレスを入力します。
- [ユーザー名（Username）] および [パスワード（Password）] フィールドに、NDFC のユーザー名とパスワードログイン情報を入力します。

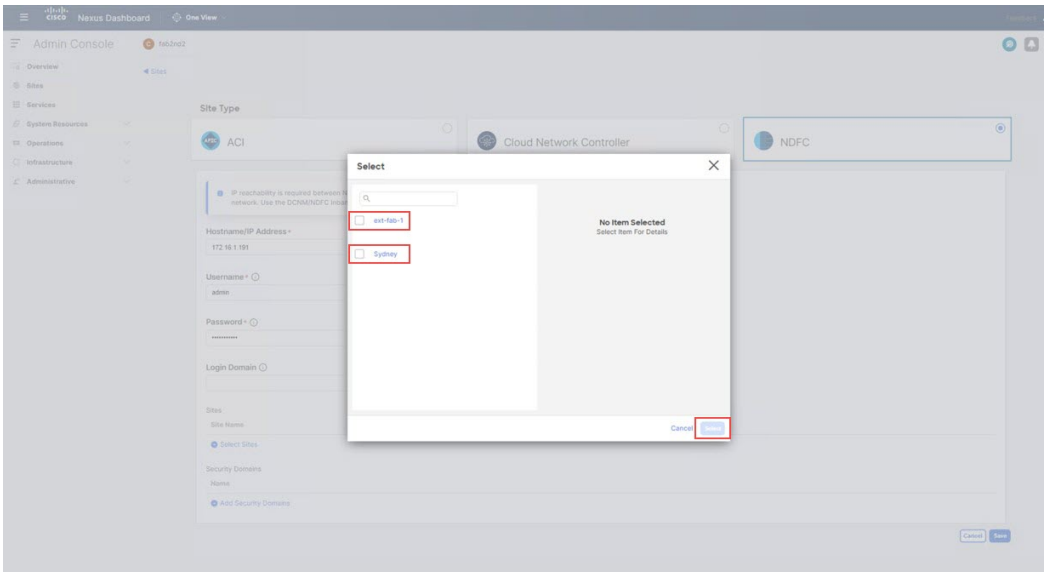
ステップ 5 **[サイトの選択 (Select Sites)]** をクリックします。

図 *32*:



ステップ 6 以前に追加した 2 つの NDFC サイト（VXLAN ファブリックと外部ファブリック サイト）の横にあるボックスをクリックし、**[選択（Select）]** をクリックします。

図 *33 :*

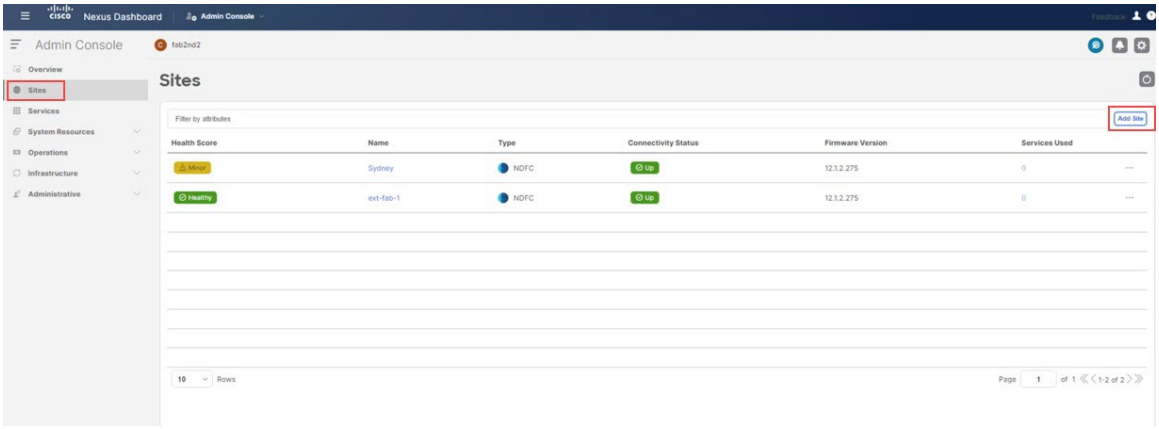


[サイトの追加（Add Site）] ページに戻ります。

ステップ 7 Nexus ダッシュボードの **[サイトの追加（Add Site）]** ページに 2 つの NDFC サイト（VXLAN ファブリックと外部ファブリック サイト）が正しく表示されていることを確認し、**[保存（Save）]** をクリックします。

ステップ 8 Nexus ダッシュボードで、最初のクラウドサイトを追加するために**[サイト（Sites）]** > **[サイトを追加（Add Site）]** もう一度をクリックします。

図 *34 :*

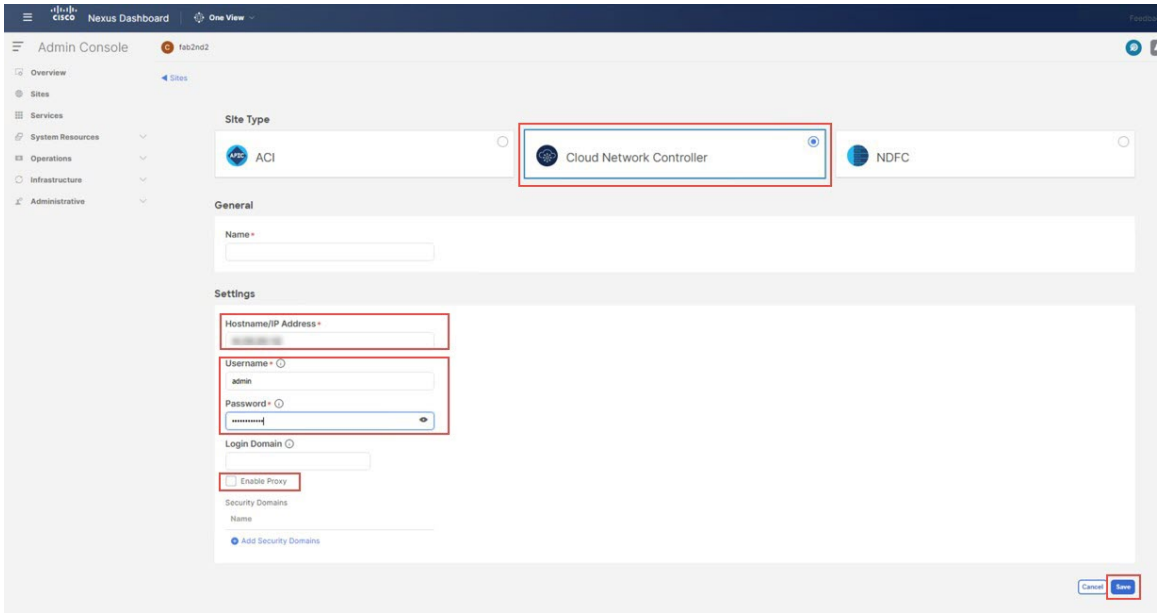


[サイトの追加（Add Site）] ページが表示されます。

ステップ 9 **[サイトの追加（Add Site）]** ページで **[クラウド ネットワーク コントローラ（Cloud Network Controller）]** ボックスをクリックし、必要な情報を入力して最初のクラウド サイト（この例のトポロジでは AWS サイト）を追加します。

- **[ホスト名/IP アドレス（Hostname/IP Address）]** フィールドに、最初のクラウド サイトのクラウド ネットワーク コントローラ（CNC）の IP アドレスを入力します。
- **[ユーザー名（Username）]** と **[パスワード（Password）]** フィールドに、最初のクラウドサイトのクラウド ネットワーク コントローラ（CNC）のユーザー名とパスワードのログイン情報を入力します。
- クラウド ネットワーク コントローラ（CNC）の場合、CNC がプロキシを通して到達可能ならば、**[プロキシを有効化（Enable Proxy）]** プロキシは、Nexus Dashboard のクラスタ設定ですでに設定されている必要があります。プロキシが管理ネットワーク経由で到達可能な場合は、プロキシIPアドレスに対して静的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。

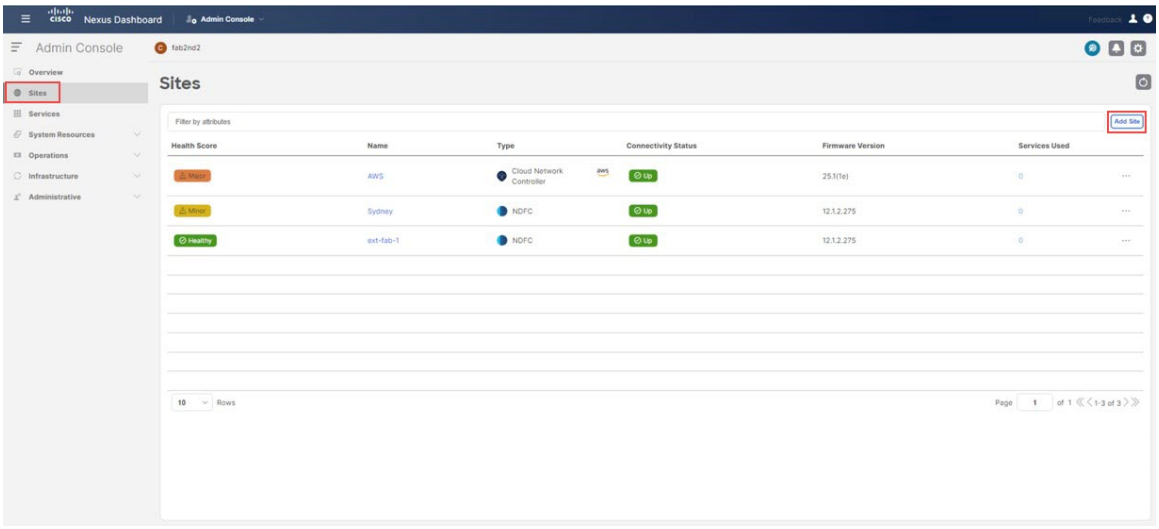
図 *35 :*



ステップ 10 [保存 (Save)] をクリックして、最初のクラウド サイトを追加します。

ステップ 11 Nexus ダッシュボードで、2 番目のクラウドサイトを追加するために**[サイト（Sites）]** > **[サイトを追加（Add Site）]** もう一度をクリックします。

図 *36 :*

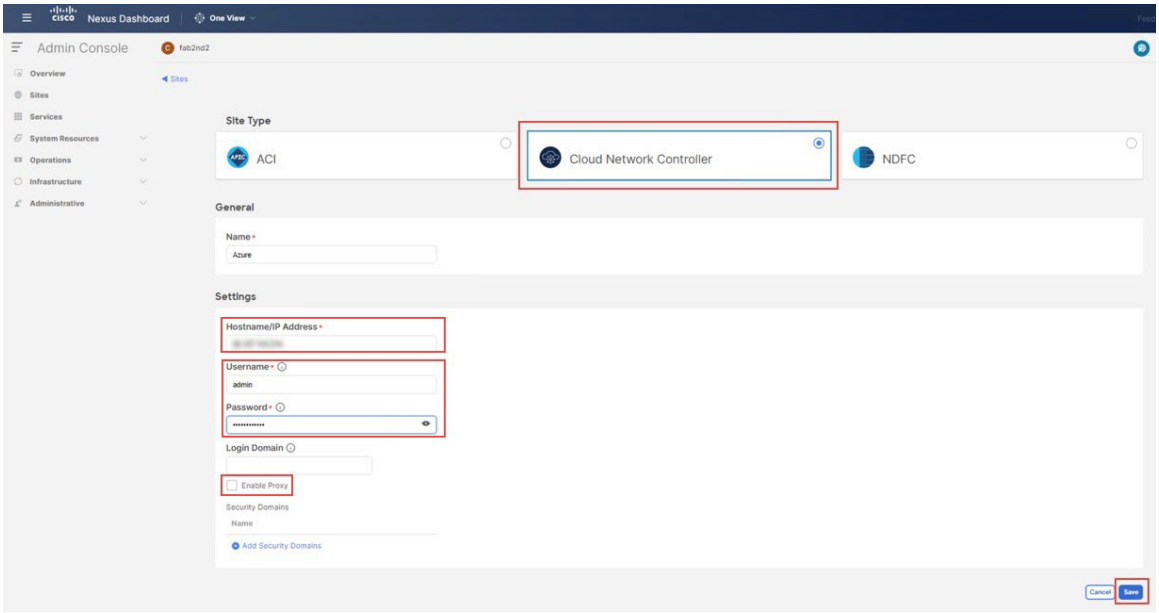


[サイトの追加（Add Site）] ページが表示されます。

ステップ 12 **[サイトの追加（Add Site）]** ページで **[クラウド ネットワーク コントローラ]** ボックスをクリックし、必要な情報を入力して、2 番目のクラウドサイト（このトポロジ例の Azure サイト）のクラウドネットワーク コントローラ（CNC）を追加します。

前の一連の手順を繰り返します。今度は、2 番目のクラウドサイトのクラウドネットワーク コントローラ（CNC）の **[ホスト名/IP アドレス（Hostname/IP Address）]**、**[ユーザー名（Username）]**、および **[パスワード（Password）]** フィールドに必要な情報を入力し、2 番目のクラウドの CNC の場合は **[プロキシを有効にする（Enable Proxy）]** をクリックします。サイトはプロキシ経由で到達可能です。

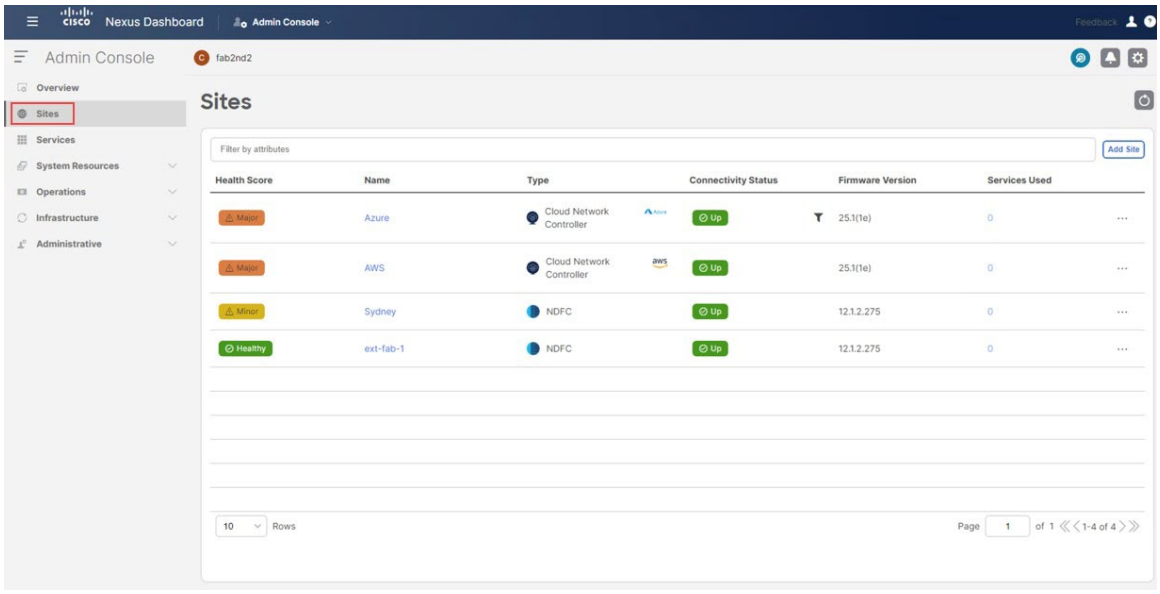
図 *37 :*



ステップ 13 Nexus ダッシュボードで**[サイト（Sites）]**をクリックし、4 つのサイトが正しく表示されていることを確認します。

- NDFC の 2 つのサイト（VXLAN ファブリックと外部ファブリック サイト）
- クラウド ネットワーク コントローラが展開されたクラウド サイト（この例のハイブリッド クラウド トポロジでは、AWS および Azure クラウド サイト）

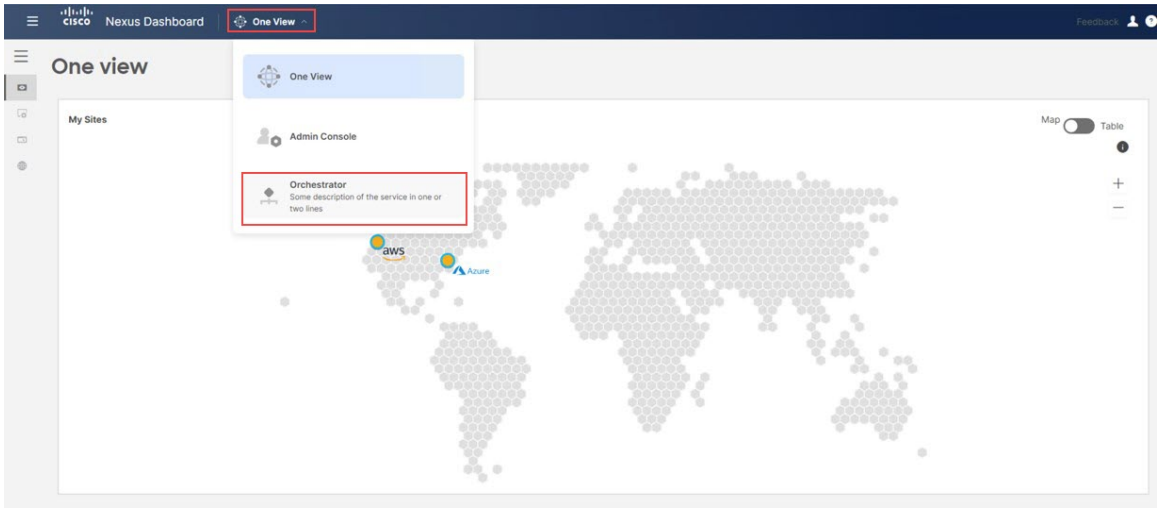
図 *38 :*



ステップ 14 Nexus ダッシュボード オーケストレータ（NDO）にアクセスします。

Nexus ダッシュボードで、ウィンドウの上部にある **[一つの表示（One View）]** > **[オーケストレータ（Orchestrator）]**をクリックします。

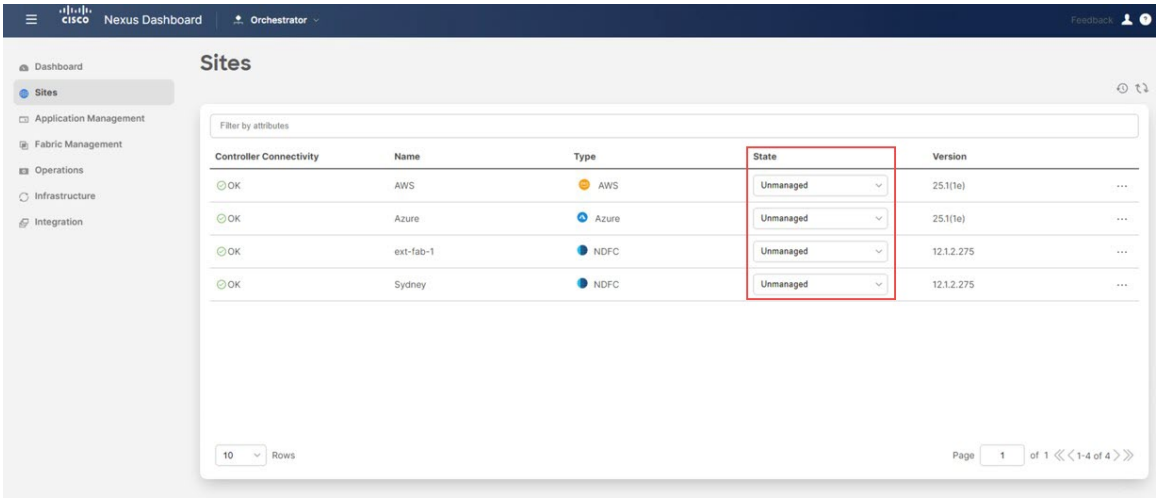
図 *39 :*



ステップ 15 NDO で、**[サイト（Sites）]** をクリックします。

ND で追加した 4 つのサイトが表示されますが、**[管理対象外（Unmanaged）]**の状態で表示されます。

図 *40 :*

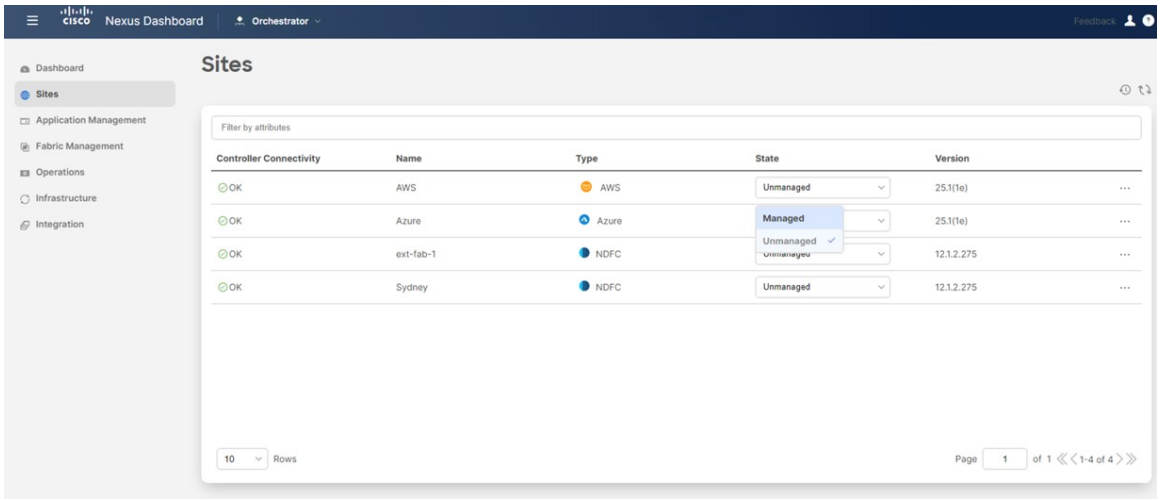


ステップ 16 NDO から、4 つのサイトを管理します。

NDO の各サイトに対して次の手順を実行します。

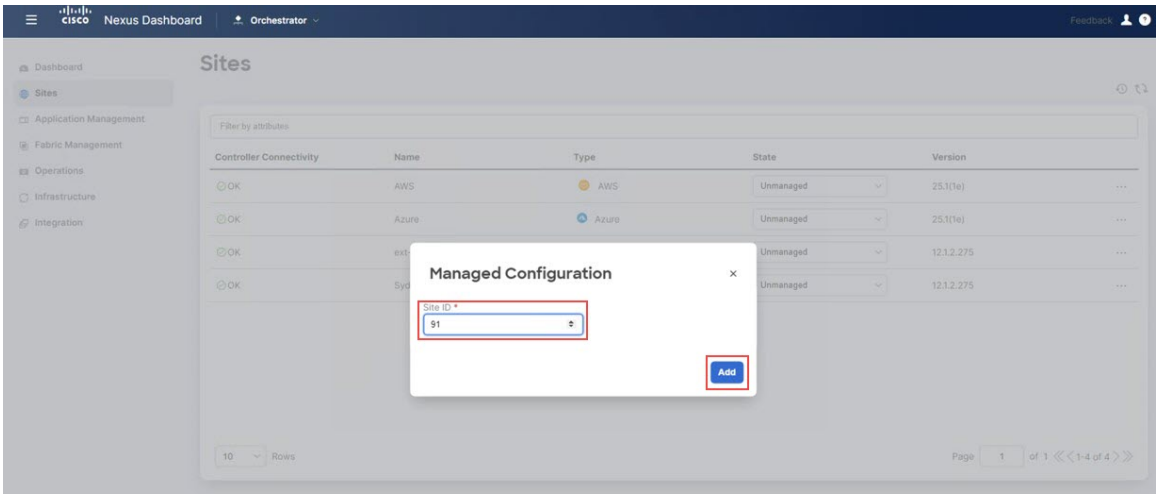
a) NDO にリストされている最初のサイトの **[状態（State）]** 列で、状態を **[管理対象外（Unmanaged）]** から **[管理対象（Managed）]** に変更します。

図 *41 :*



b) この特定のサイトに固有のサイト識別子（この NDO を通じて管理されている他のサイトのサイト識別子と競合しないサイト識別子）を指定し、**[追加（Add）]** をクリックします。

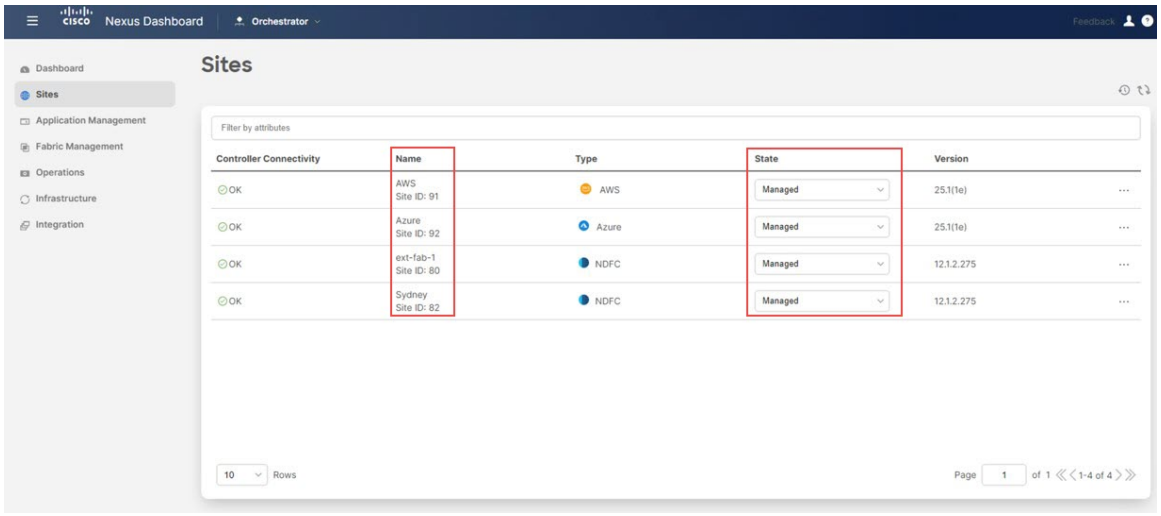
図 *42 :*



c) NDO の残りのサイトに対してこれらの手順を繰り返して、各サイトを**[管理対象（Managed）]** 状態に変更し、各サイトに一意のサイト ID を提供します。

次の図は、4 つのサイトすべて（2 つの NDFC サイトと 2 つのクラウド サイト）の例を示しており、状態が **[管理対象（Managed）]** に変更され、各サイトに一意のサイト ID が提供されています。

図 *43 :*



次のタスク

Complete サイト間の接続 NDFC と クラウド サイトの間 （44 ページ）に記載されている手順を使用して、NDFC とクラウド サイト間のサイト間接続を完了します。

Complete サイト間の接続 NDFC と クラウド サイトの間

次のセクションの手順に従って、NDFC とクラウド サイト間のサイト間接続を完了します。

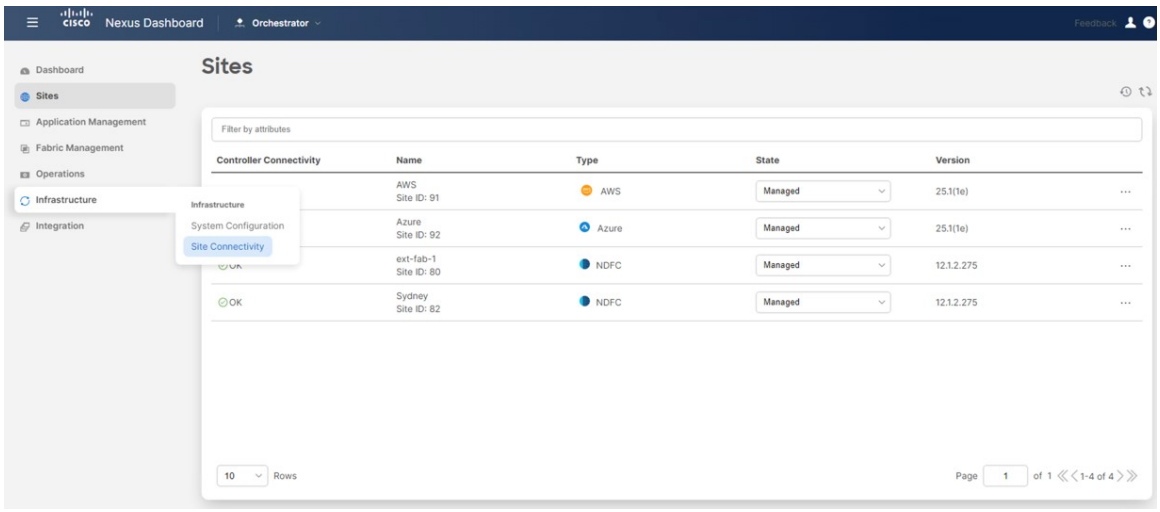
必要なコントロール プレーン構成を完了する

始める前に

NDFC とクラウド サイトを ND と NDO に導入準備する （36 ページ）で提供されている手順を使用して、ND および NDO で NDFC およびクラウド サイトをオンボードします。

ステップ 1 NDO 内で、**[インフラストラクチャ（Infrastructure）] > [サイト接続（Site Connectivity）]**に移動します。

図 *44 :*



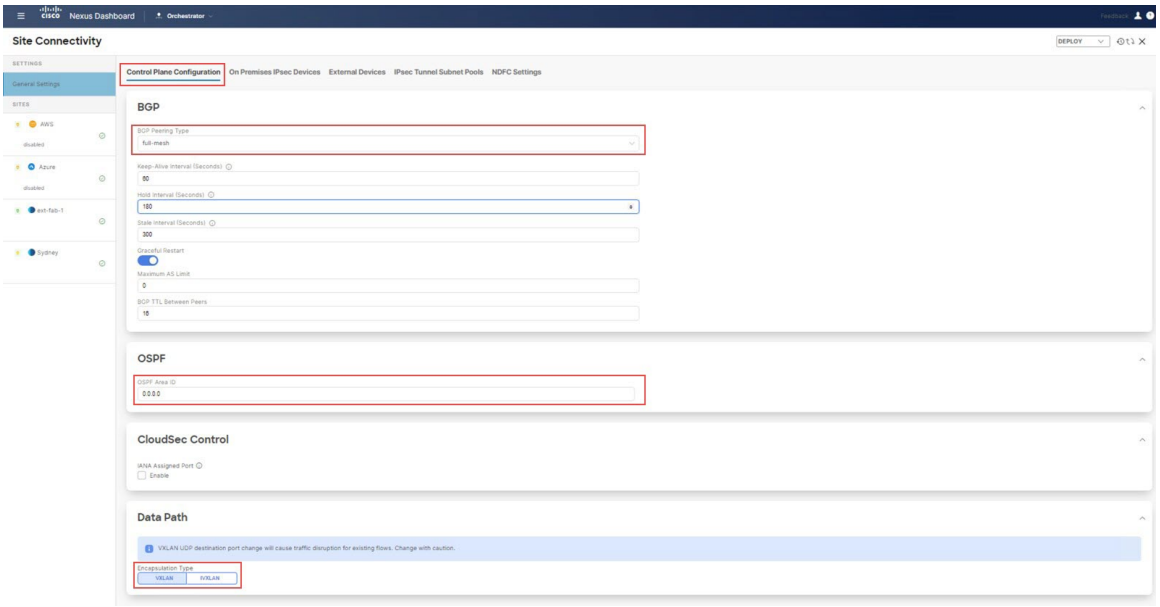
この時点で、世界地図にサイトが表示されますが、サイト間にリンクはありません。つまり、この時点ではサイト間に接続がありません。

図 *45 :*

ステップ 2 **[サイト接続（Site Connectivity）]** ウィンドウの右上のエリアで、**[構成（Configure）]** をクリックします。**[一般設定（General Settings）]** エリアの **[サイト接続（Site Connectivity）]** ウィンドウが表示されます。

ステップ 3 **[一般設定（General Settings）]** エリアで、**[コントロール プレーン構成（Control Plane Configuration）]** タブをクリックし、このページで必要な構成を行います。

図 *46 :*



BGP はオンプレミスとクラウド サイト間のアンダーレイ接続に使用され、OSPF はクラウド間のアンダーレイ接続に使用されることに注意してください。

（注） これらの一般的な BGP 設定は、アンダーレイ接続とオーバーレイ接続の両方での BGP の使用に適用され、オーバーレイ ピアリングにのみ適用される次のステップの **[BGP ピアリング タイプ（BGP Peering Type）]** オプションを除き、通常は変更しないでください。

ステップ 4 オンプレミスとクラウド サイト間のオーバーレイ接続の場合、**BGP** エリアの **[BGP ピアリング タイプ（BGP Peering Type）]** フィールドで、**[フルメッシュ（full-mesh）]** または **[ルート サーバー（route-server）]** のいずれかを選択します。

フル メッシュまたはルート サーバー接続を使用するトポロジを確認するには、サポートされるトポロジを参照してください。

この特定のユース ケースでは、IPsec（マルチクラウド）でサポートされるトポロジ の オプション 1 トポロジに基づいて展開を構成しているため、このユース ケースでは **[フルメッシュ（full-mesh）]** を選択します。

ステップ 5 必要に応じて、**BGP** エリアで残りのパラメータを定義します。

ステップ 6 クラウド間アンダーレイ接続の場合、**OSPF** エリアで、**[OSPF エリア識別子（OSPF Area ID）]** フィールドに適切な値を入力します。

2 つのクラウド サイト間のアンダーレイ ルーティングは OSPF を使用するため、この構成はクラウド間接続に必要です。この例では、このフィールドに OSFP エリア識別子`0.0.0.0` を入力します。

ステップ 7 **[データ パス（Data Path）]** で、**[カプセル化タイプ（Encapsulation Type）]** エリアを見つけて、**[VXLAN]** を選択します。

デフォルトでは、NDO は、オンプレミス ファブリックに基づく NDFC のハイブリッド クラウドのデータ プレーンで標準規格 VXLAN を使用します。もう 1 つのオプションは iVXLAN です。これは、ACI サイトのハイブリッド クラウド接続を構築するときに使用する必要があります（ACI は iVXLAN を使用するため）。

次のタスク

オンプレミス IPsec デバイス と IPSec トンネル サブネット プールを追加 （46 ページ） の手順を実行します。

オンプレミス IPsec デバイス と IPSec トンネル サブネット プールを追加

このセクションでは、オンプレミスの IPsec デバイス（NDFC 外部ファブリック サイトの Cisco Catalyst 8000V）を追加し、IPsec トンネル プールを構成します。

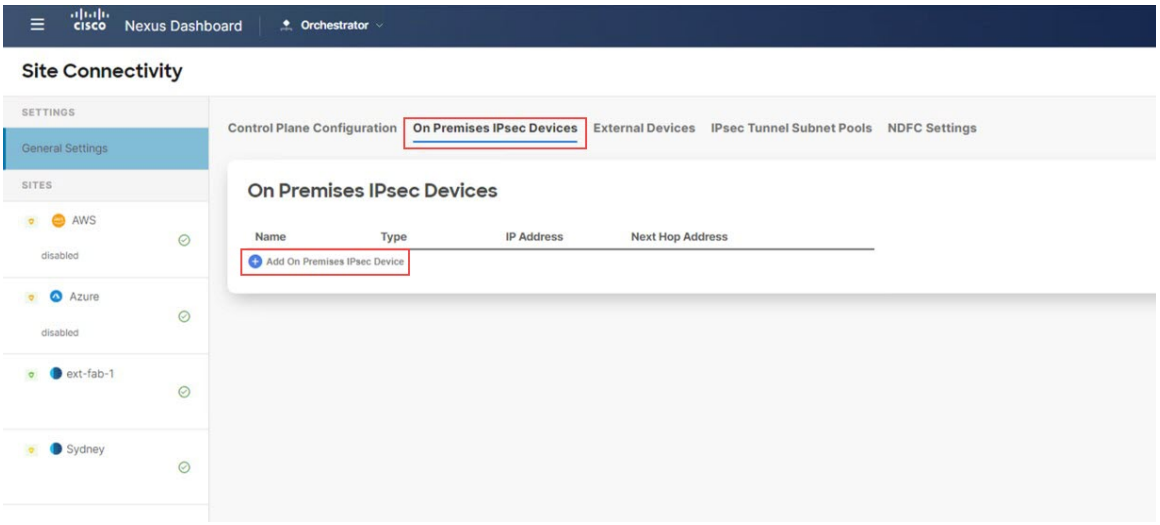
始める前に

必要なコントロール プレーン構成を完了する （44 ページ） の手順を実行します。

ステップ 1 同じ **[一般設定（General Settings）]** ページで、**[オン プレミス IPsec デバイス（On Premises IPsec Devices）]** タブをクリックします。

ステップ 2 **[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。

図 *47 :*



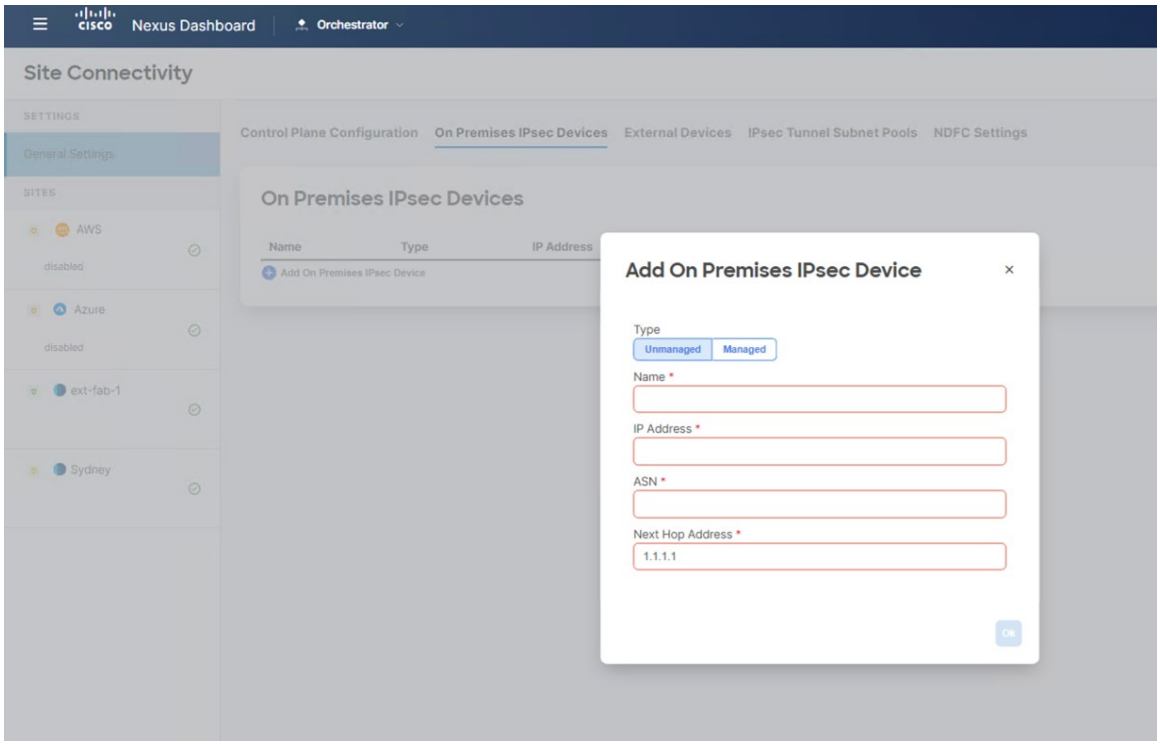
[オン プレミス IPsec デバイスを追加（Add On Premises IPsec Device）] ページが表示されます。

ステップ 3 **[タイプ（Type）]** フィールドで、**[非管理（Unmanaged）]** または **[管理（Managed）]** を選択します。

オンプレミスの IPsec デバイスでは、**[非管理（Unmanaged）]**と**[管理（Managed）]**管理対象の両方のオプションがサポートされています。

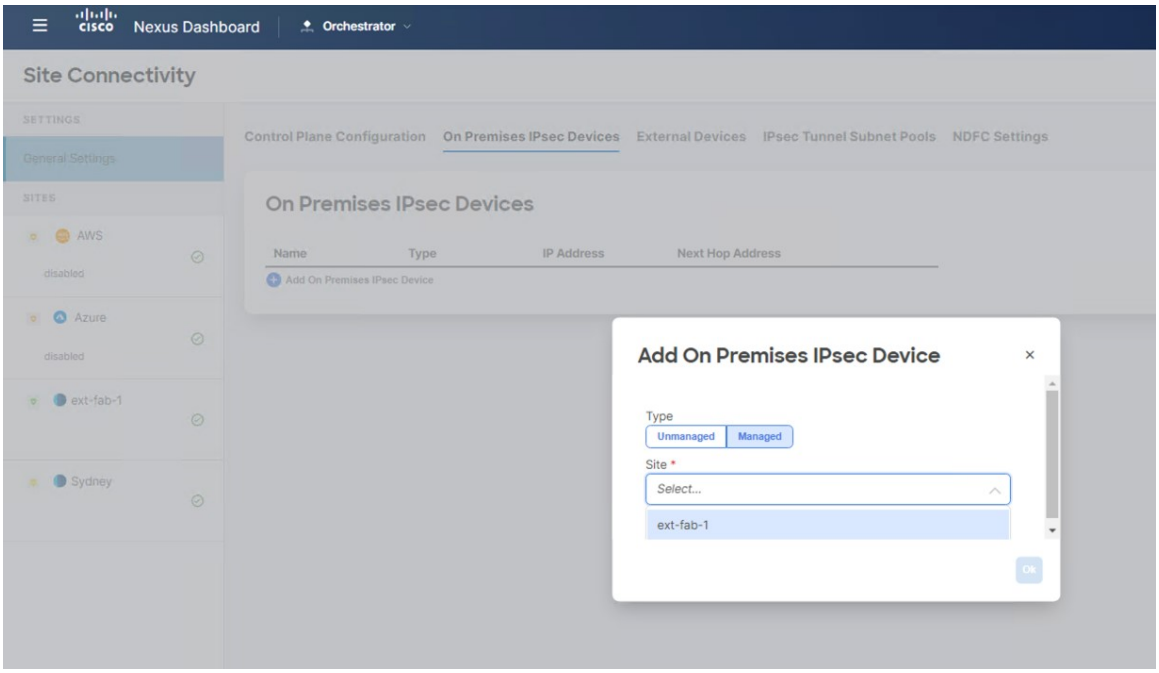
- オンプレミスの IPsec デバイスに対して **[管理対象外（Unmanaged）]** オプションを選択した場合は、**[名前（Name）]**、**[IP アドレス（IP Address）]**、**[ネクスト ホップ アドレス（Next Hop Address）]** など、この管理対象外のオンプレミス IPsec デバイスに必要な情報を入力する必要があります。オンプレミスの IPsec デバイスが NDFC で管理されていない場合 (そのデバイスが NDFC でサポートされていないか、サードパーティのデバイスである場合)、**[管理対象外（Unmanaged）]** を使用します。次に、NDO は、管理対象外の IPsec デバイスに必要な構成を生成します。これをダウンロードして、オンプレミスの IPsec デバイスに手動で適用できます。

図 *48 :*



- オンプレミスの IPsec デバイスに対して**[管理対象（Managed）]** オプションを選択すると、**[サイト（Site）]** フィールドが **[管理対象（Managed）]** オプションの下に表示されます。**[サイト（Site）]** フィールドで使用できるサイトは、NDFC で構成された外部ファブリックについて NDO が NDFC からプルする情報に基づいています。

図 *49 :*



管理対象のオンプレミス IPsec デバイスを備えた NDFC 外部ファブリックを選択します。この場合、選択したサイトに基づいて、**ASN** フィールドが自動的に入力されます。

このユース ケースの例では、オンプレミスの IPsec デバイスのタイプとして **[管理対象（Managed）]** を選択します。

a) **[デバイス（Device）]** フィールドで、この展開に使用するオンプレミスの IPsec デバイスを選択します。

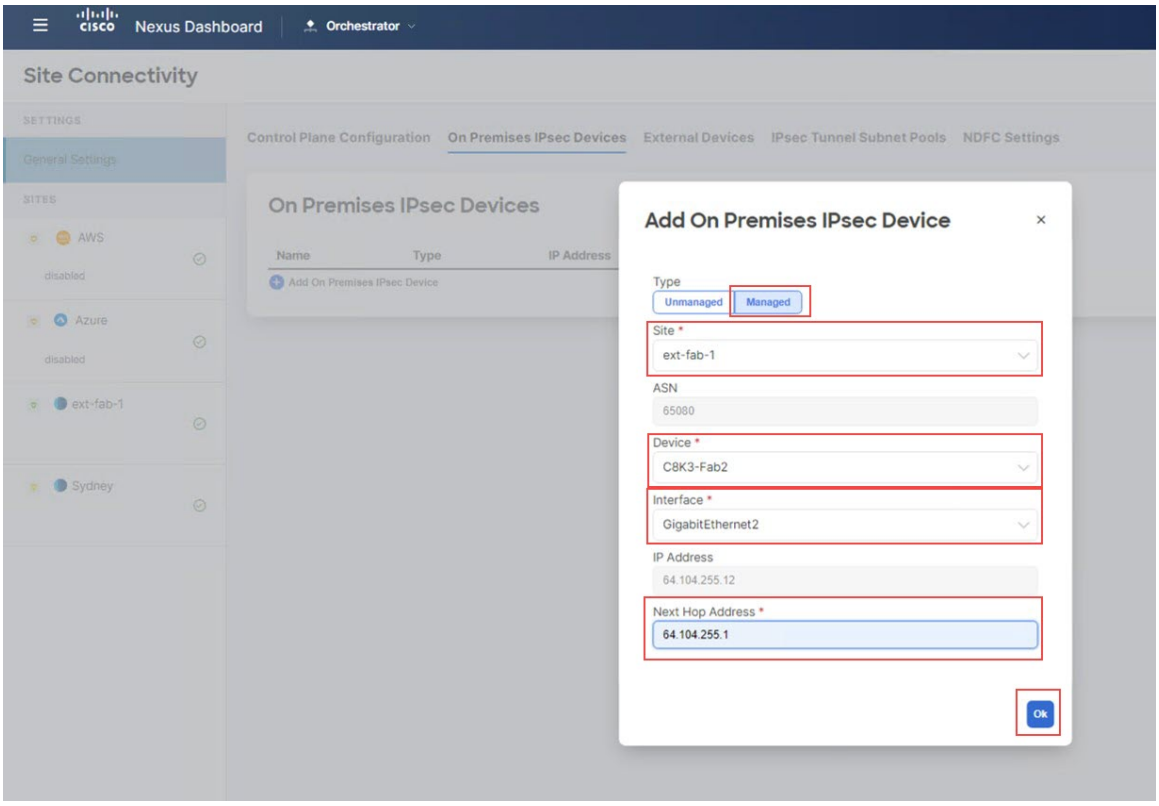
[デバイス（Device）] フィールドで使用できるデバイスは、上で選択した NDFC サイトで構成されたオンプレミスの IPsec デバイスについて、NDO が NDFC からプルする情報に基づいています。**[デバイス（Device）]** フィールドで選択したオンプレミスの IPsec デバイスに基づいて、**ASN** フィールドが自動的に入力されます。

b) **[インターフェイス（Interface）]** フィールドで、オンプレミスの IPsec デバイスに使用する適切なインターフェイスを選択します。

このインターフェースの **[IP アドレス（IP Address）]** フィールドは、**[インターフェイス（Interface）]** フィールドで選択したインターフェースに基づいて自動的に入力されます。

c) **[ネクスト ホップ アドレス（Next Hop Address）]** フィールドに、IPsec で構成するルートに使用するアドレスを入力します。

図 *50 :*



ステップ 4 **[オンプレミス IPsec デバイスを追加（Add On Premises IPsec Device）]** ページで必要な情報の入力が完了したら、**Ok** をクリックします。

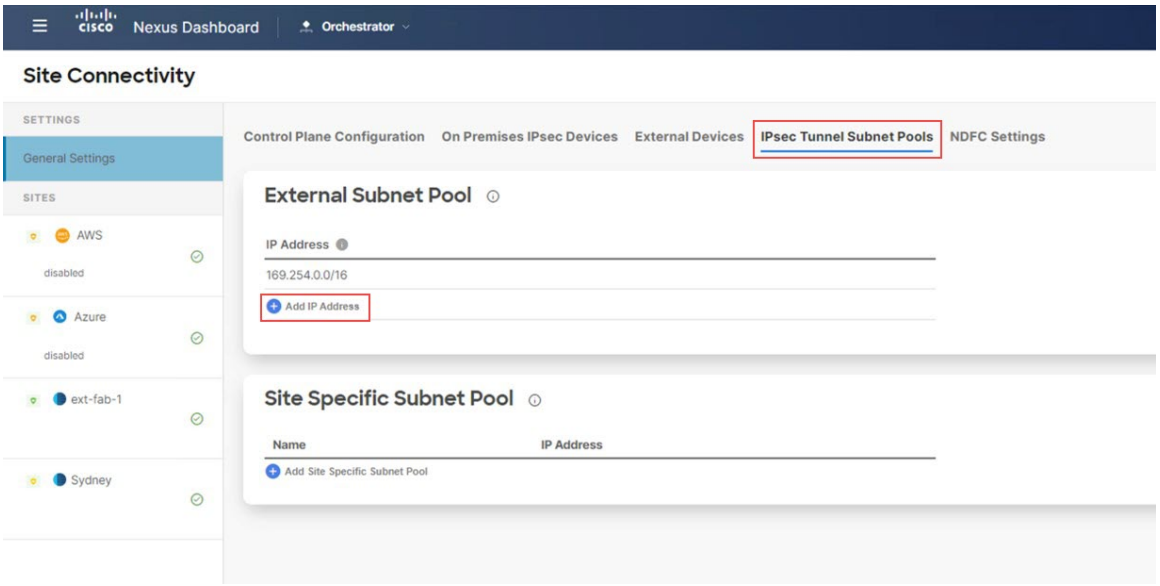
[オンプレミス IPsec デバイス（On Premises IPsec Device）] ページに戻ります。このページには、構成されたオンプレミスの IPsec デバイスが表示されています。

ステップ 5 IPsec トンネル サブネット プールを構成するために**[IPSec トンネル サブネット プール（IPsec Tunnel Subnet Pools）]** タブをクリックします。

クラウド トンネルの IP 割り当てには、**[IPSec トンネル サブネット プール（IPsec Tunnel Subnet Pools）]** の情報が必要です。

ステップ 6 **[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）]** をクリックします。

図 *51 :*

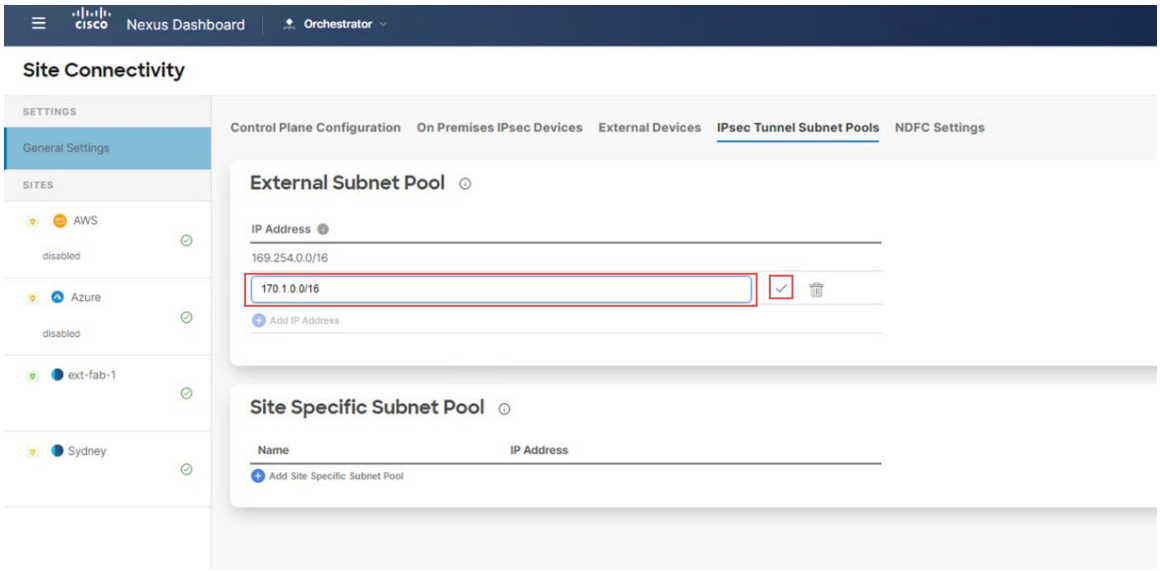


ステップ 7 IPsec トンネルに使用する IP サブネット プールを入力します。

IPsec トンネルのパブリックまたはプライベート IP アドレスを使用して、IP サブネット プールを定義します。これは、オンプレミスの外部デバイスと Cisco Catalyst 8000V の間、およびクラウド サイトに展開された Cisco Catalyst 8000V の間の IPsec トンネル アドレスの IP アドレスのプールです。

- IPsec トンネルごとに /30 サブネットが必要です。
- プール サイズは、すべての IPsec トンネルに対応できる必要があります。
- 許可される最小プール サイズは 512 アドレス（/23 サブネット）です。
- 環境内の他の IP アドレスと重複しない IP アドレスの範囲（パブリックまたはプライベート）を使用します。

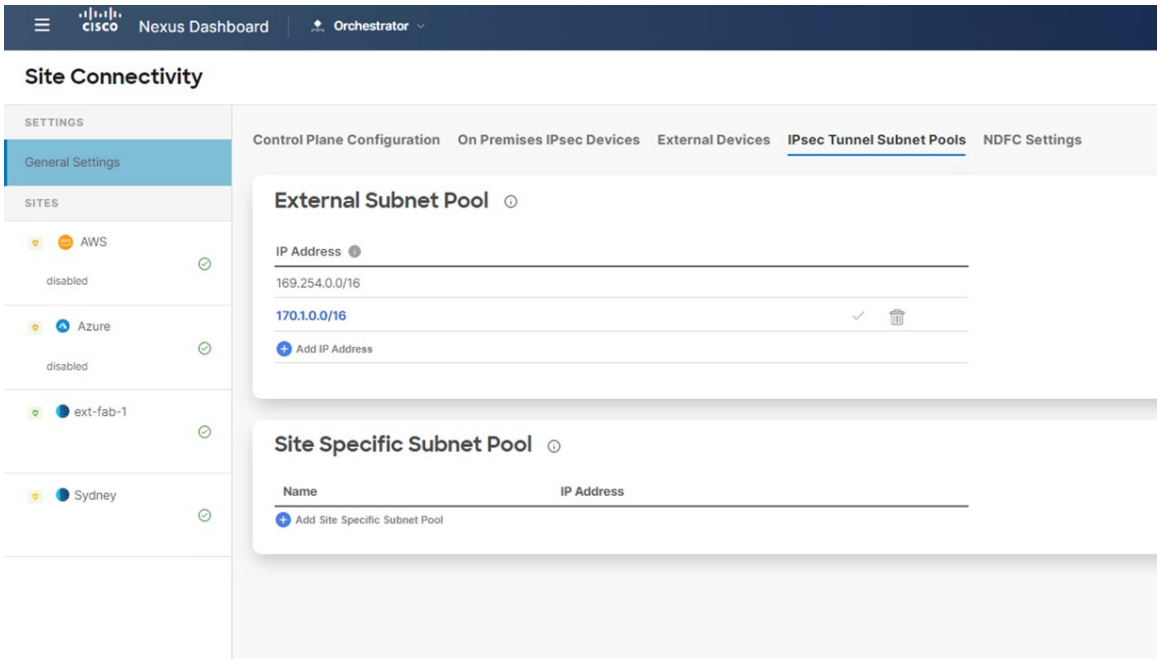
図 *52 :*



ステップ 8 チェックボックスをクリックして、入力した IP サブネット プールを受け入れます。

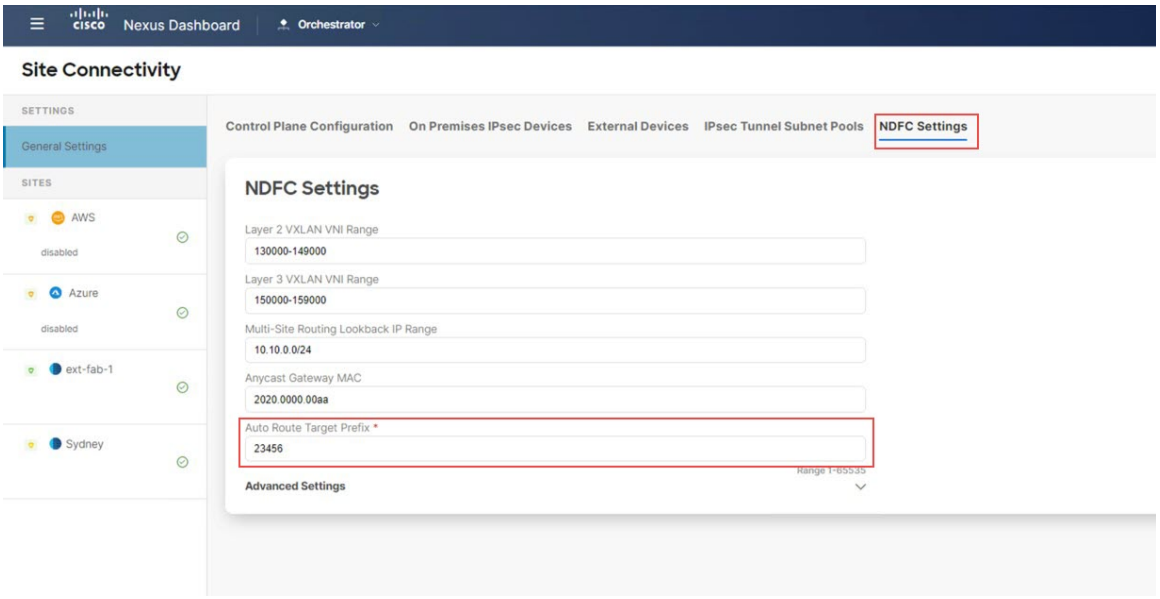
[外部サブネット プール（External Subnet Pool）]エリアの下に IP サブネット プールが表示されます。

図 *53 :*



ステップ 9 必要に応じて、**[NDFC 設定（NDFC Settings）]** タブをクリックし、**[自動ルート ターゲット プレフィックス（Auto Route Target Prefix）]**に必要な情報を入力します。

図 *54 :*



NDO の NDFC 設定では、ルート ターゲット生成のルート ターゲット プレフィックスが NDFC のデフォルト値 23456 に設定されています (クラウド ネットワーク コントローラーにはこの設定に対して異なる値があります)。したがって、重複を避けるために必要な場合、この値は **[自動ルート ターゲット プレフィックス（Auto Route Target Prefix）]** フィールドで変更できます。このフィールドに値を設定すると、NDO は NDO によってこの値を NDFC にプッシュできます。

次のタスク

NDFC 外部ファブリック内の外部デバイスのポートを追加する （53 ページ） の手順を実行します。

NDFC 外部ファブリック内の外部デバイスのポートを追加する

このセクションでは、NDFC外部ファブリックの外部デバイスに必要なポートを追加して構成します。これらは、コア ルータを BGW ノードに接続するインターフェイスです。

始める前に

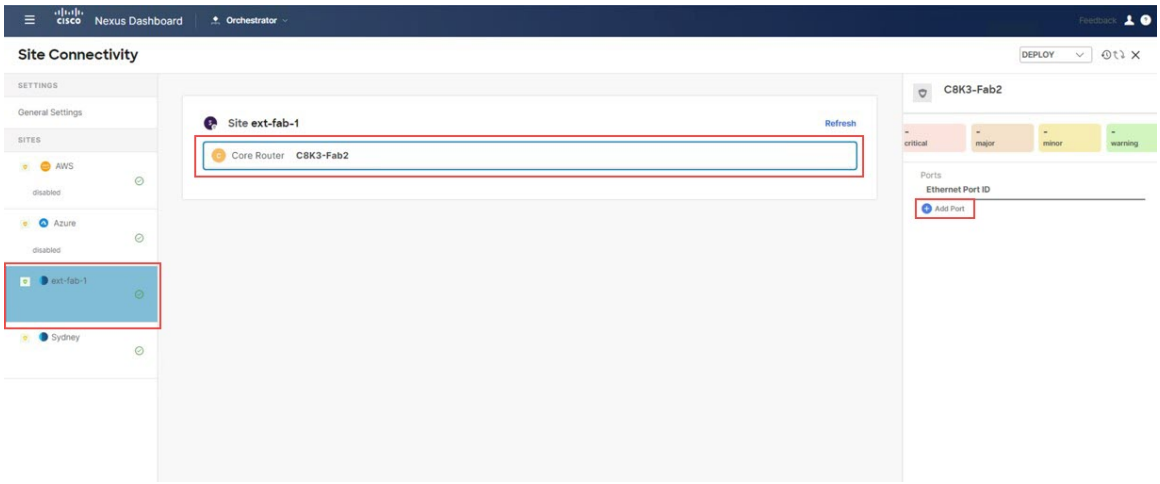
オンプレミス IPsec デバイス と IPSec トンネル サブネット プールを追加 （46 ページ） の手順を実行します。

ステップ 1 **[一般設定：サイト（General Settings: Sites）]** の下の左側のウィンドウで、NDFC 外部ファブリック（この例では ext-fab-1 サイト）をクリックします。

ステップ 2 中央のペインで、NDFC 外部ファブリックの最初の外部デバイスをクリックします。

ステップ 3 右側のペインで **[ポートを追加（Add Port）]** をクリックします。

図 *55 :*

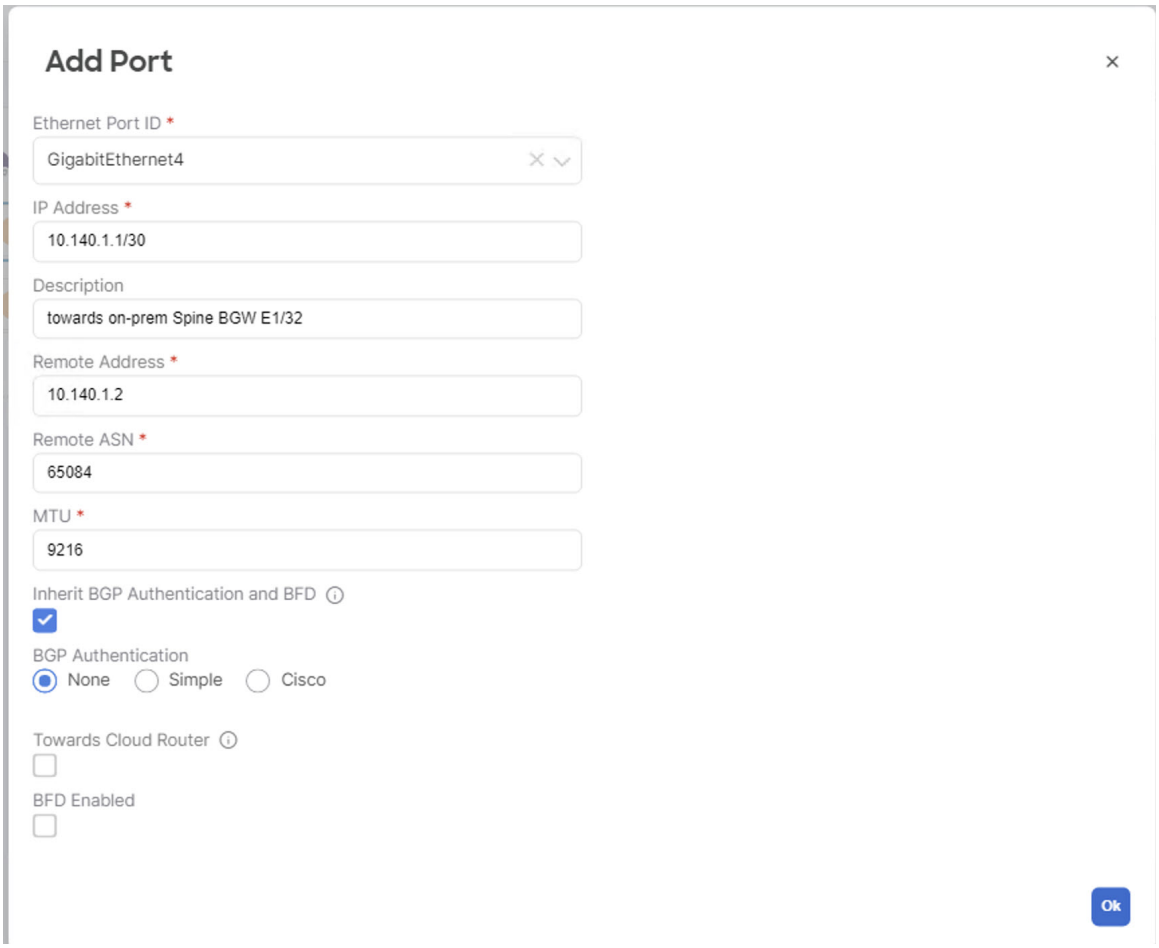


ステップ 4 IP アドレス、リモート IP アドレス、リモート ASN など、ポート構成に必要な情報を入力します。

（注） **[クラウド ルータに向かう（Towards Cloud Router）]** オプションは、ハブ サイトのボーダー ゲートウェイにのみ適用されます。次の理由により、このウィンドウでこのオプションを有効にしません。

- この導入例に使用しているトポロジは、ハブサイトを使用していないのでのこ導入例に**[クラウド ルータに向かう（Towards Cloud Router）]** をイネーブル化しません。
- IPsec（マルチクラウド）でサポートされるトポロジのオプション 3のようなハブ サイトを使用するトポロジを構成していた場合でも、そのハブサイトトポロジのNDFC外部ファブリックの外部デバイスに対して、このページでこのオプションを有効にしません。代わりに、NDFC VXLAN ファブリック内の BGW スパイン デバイスにポートを追加する （58 ページ）で説明されているように、NDFC VXLAN ファブリックの BGW スパイン デバイスのページでこのオプションを有効にします。

図 *56 :*



ステップ 5 完了したら、**[OK]** をクリックします。

ステップ 6 残りの外部デバイスに対してこの手順を繰り返します。

次のタスク

VXLAN ファブリック サイトのマルチサイト VIP を定義します。 （55 ページ） の手順を実行します。

VXLAN ファブリック サイトのマルチサイト VIP を定義します。

このセクションでは、VXLAN ファブリック サイトのマルチサイト VIP を定義します。

始める前に

NDFC 外部ファブリック内の外部デバイスのポートを追加する （53 ページ） の手順を実行します。

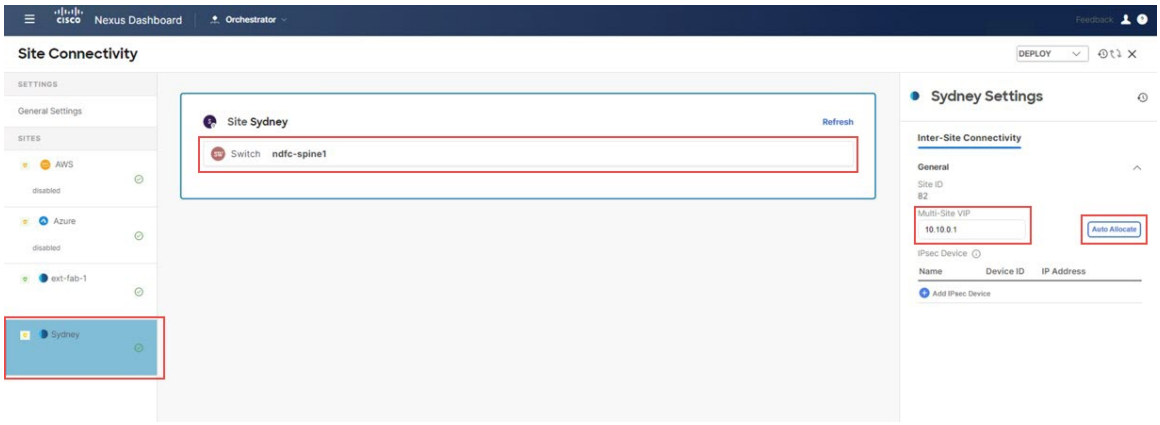
ステップ 1 **[一般設定：サイト（General Settings: Sites）]** の下の左側のペインで、NDFC VXLAN ファブリック サイトをクリックします。

ステップ 2 中央のペインで、スパイン デバイスをクリックします。

ステップ 3 右側のペインの **[サイト間接続（Inter-Site Connectivity）]** で、**[マルチサイト VIP（Multi-Site VIP）]** フィールドにマルチサイト VIP を定義します。

[自動割り当て（Auto Allocate）] をクリックするか、マルチサイト VIP の IP アドレスを明示的に定義できます。

図 *57 :*



次のタスク

IPSec デバイスを VXLAN ファブリック サイトにマップする （56 ページ） の手順を実行します。

IPSec デバイスを VXLAN ファブリック サイトにマップする

このセクションでは、IPsec デバイスを VXLAN ファブリック サイトにマッピングします。

始める前に

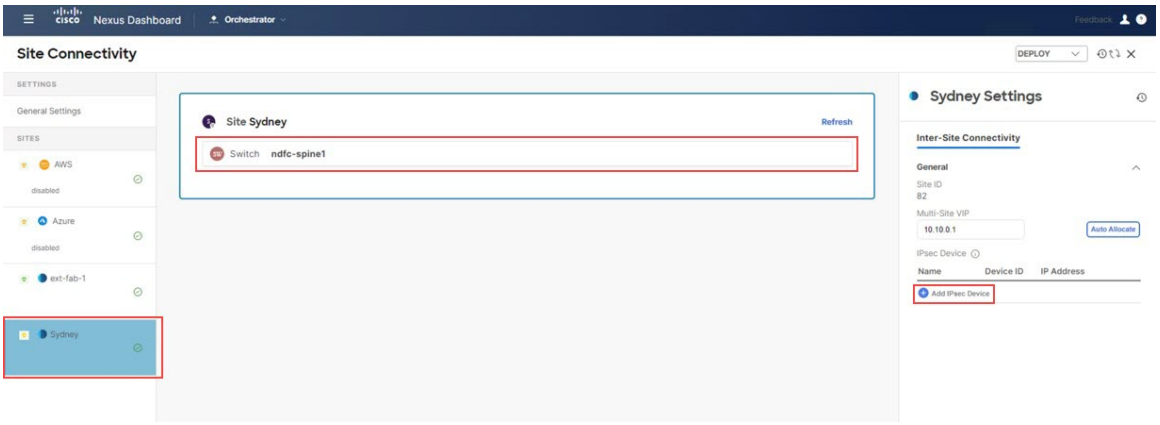
VXLAN ファブリック サイトのマルチサイト VIP を定義します。 （55 ページ） の手順を実行します。

ステップ 1 **[一般設定：サイト（General Settings: Sites）]** の下の左側のペインで、NDFC VXLAN ファブリック サイトをクリックします。

ステップ 2 中央のペインで、スパイン デバイスをクリックします。

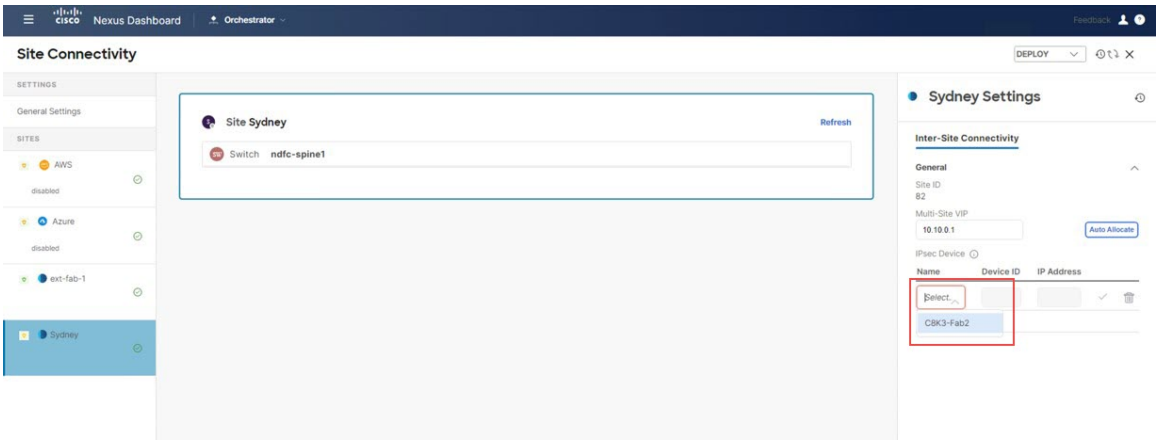
ステップ 3 右側のペインの **[サイト間接続（Inter-Site Connectivity）]** で、**[IPsec デバイスの追加（Add IPsec Device）]** をクリックします。

図 *58 :*



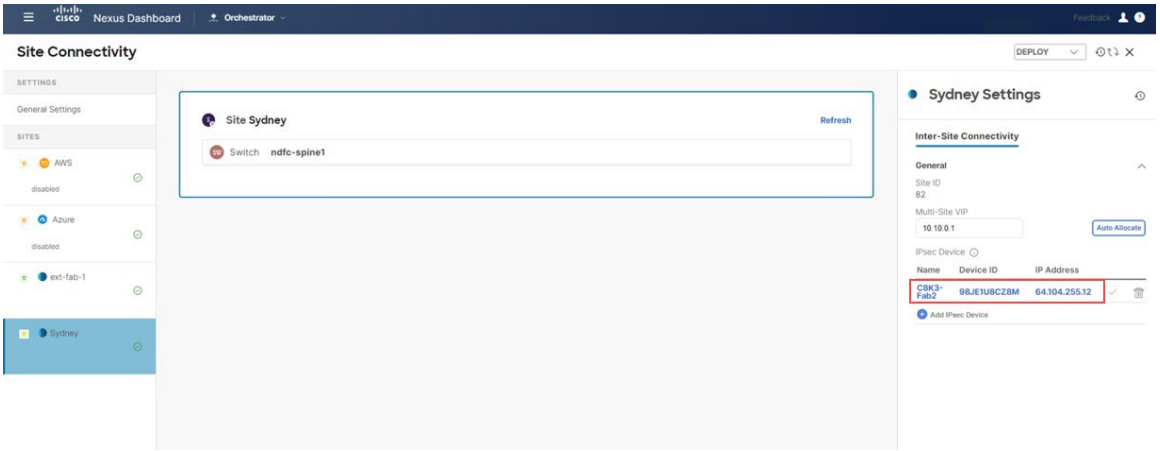
ステップ 4 **[選択（Select）]** をクリックして、適切な IPsec デバイスを選択します。

図 *59 :*



これで、オンプレミスの IPsec デバイスが VXLAN ファブリック サイトにマップされました。

図 *60 :*



ステップ 5 NDFC VXLAN サイトをクラウド サイトに接続するために使用されるオンプレミスの IPsec デバイス（Cisco Catalyst 8000V）ごとに、この手順を繰り返します。

次のタスク

NDFC VXLAN ファブリック内の BGW スパイン デバイスにポートを追加する （58 ページ） で提供されている手順を使用して、コア ルータ（Cisco Catalyst 8000V）に接続する BGW スパイン デバイスのポートを構成します。

NDFC VXLAN ファブリック内の BGW スパイン デバイスにポートを追加する

このセクションでは、オンプレミスの IPsec デバイスに面する NDFC VXLAN ファブリックの BGW スパイン デバイスに必要なポートを追加して構成します。

始める前に

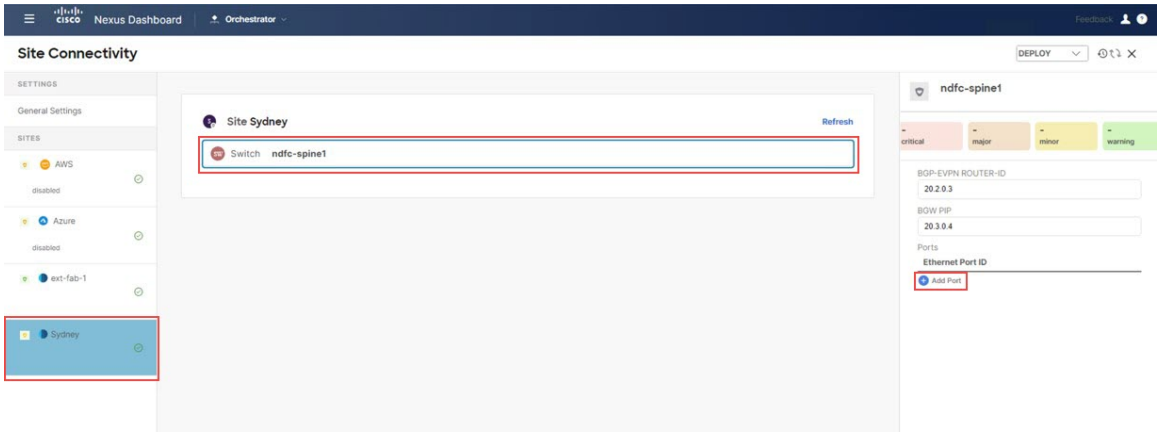
IPSec デバイスを VXLAN ファブリック サイトにマップする （56 ページ） の手順を実行します。

ステップ 1 **[一般設定：サイト（General Settings: Sites）]** の下の左側のペインで、NDFC VXLAN ファブリック サイトをクリックします。

ステップ 2 中央のペインで、スパイン デバイスをクリックします。

ステップ 3 右側のペインで **[ポートを追加（Add Port）]** をクリックします。

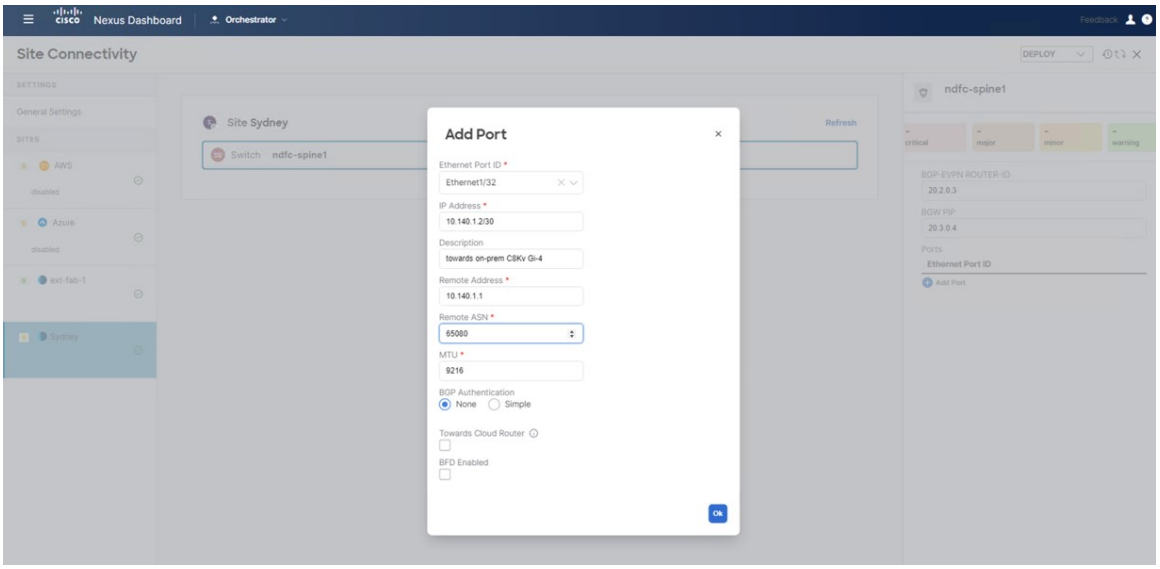
図 ***61 :***



ステップ 4 必要な情報をこのページに入力します。

このページでポート パラメータを定義します。

図 *62 :*



- **[イーサネット ポート識別子（Ethernet Port ID）]** フィールドで、オンプレミスの Cisco Catalyst 8000V の方を向いているインターフェイスを選択します。
- **[IP アドレス（IP Address）]** フィールドに、このインターフェイスの IP アドレスを入力します。これらの手順の後半で、Nexus ダッシュボード オーケストレータ は、VXLAN ファブリックに存在する BGW スパイン スイッチで、このインターフェイスのこの IP アドレスを構成します。
- **[リモート アドレス（Remote Address）]** フィールドに、オンプレミスの IPsec デバイスのギガビット 4 インターフェイスの IP アドレスを入力します。
- **[リモート ASN（Remote ASN）]** フィールドに、オンプレミスの IPsec デバイスの ASN を入力します。たとえば、このユース ケースの例では、オンプレミスの IPsec デバイスの ASN として `65080` を入力します。

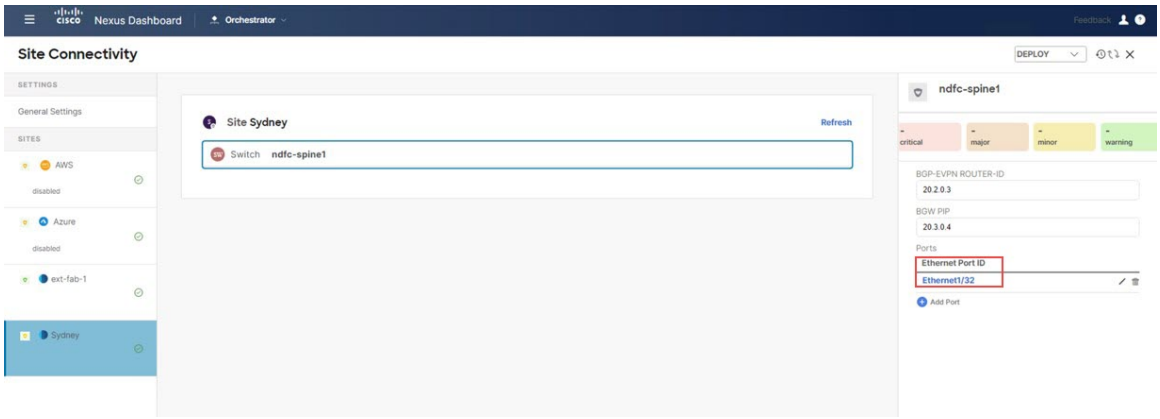
（注） **[クラウド ルータに向かう（Towards Cloud Router）]** オプションは、オンプレミス ハブ サイトのボーダー ゲートウェイにのみ適用されます。IPsec（マルチクラウド）でサポートされるトポロジのオプション 3などのハブ サイトを使用しているトポロジでは、このオプションを有効にする必要があります。

この導入例に使用しているトポロジは、ハブ サイトを使用していないのでのこ導入例に**[クラウド ルータに向かう（Towards Cloud Router）]** をイネーブル化しません。

ステップ 5 [OK] をクリックします。

BGW スパイン デバイスのポートが NDFC VXLAN ファブリックに追加されました

図 *63 :*



次のタスク

1 つ目のクラウド サイトを NDFC VXLAN ファブリック サイトに接続する （60 ページ） の手順を実行します。

1 つ目のクラウド サイトを NDFC VXLAN ファブリック サイトに接続する

このセクションでは、1 番目のクラウド サイトを NDFC VXLAN ファブリック サイトに接続します。

始める前に

NDFC VXLAN ファブリック内の BGW スパイン デバイスにポートを追加する （58 ページ） の手順を実行します。

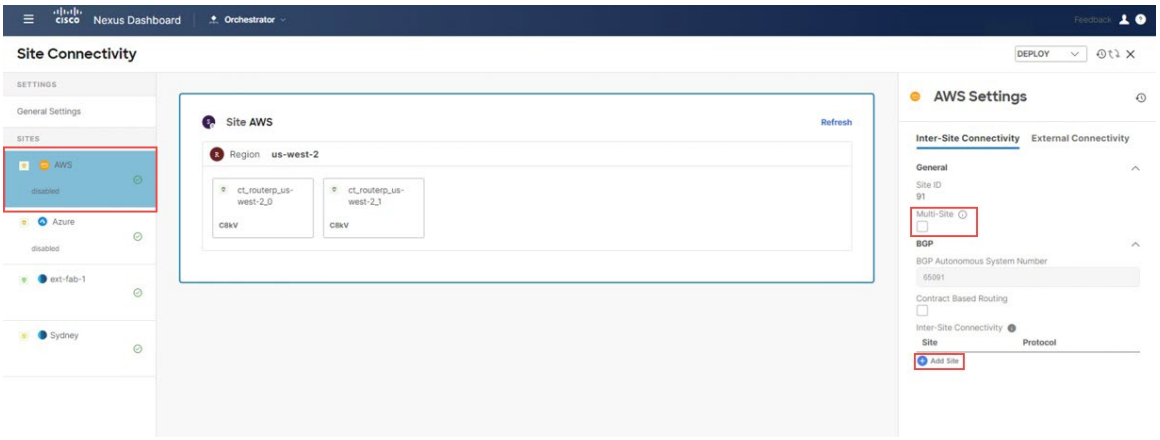
ステップ 1 **[一般設定：サイト（General Settings: Sites）]** の下の左側のペインで、最初のクラウド サイト（AWS サイトなど）をクリックします。

ステップ 2 右側のペインで、**[サイト間接続（Inter-Site Connectivity）]** をクリックし、**[マルチサイト（Multi-Site）]** の下にあるチェックボックスをオンにして、その機能を有効にします。

この機能は、サイト間に VXLAN マルチサイト オーバーレイ トンネルを構築するために必要です。

ステップ 3 右側のペインで **[サイトの追加（Add Site）]** をクリックします。

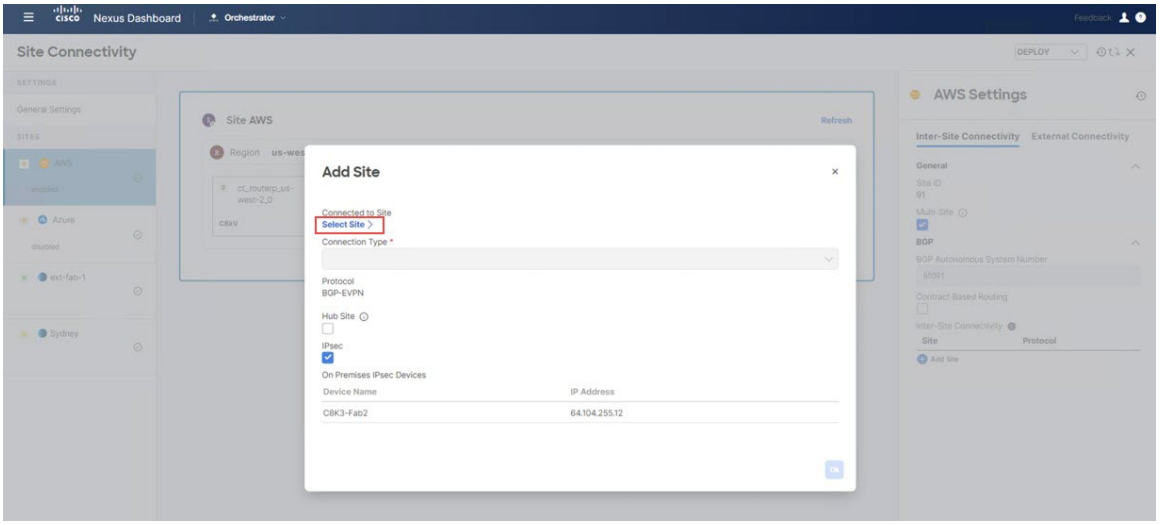
図 *64 :*



[サイトの追加（Add Site）] ページが表示されます。

ステップ 4 **[サイトの追加（Add Site）]** ページ内で**[サイトを選択（Select a Site）]**をクリックします。

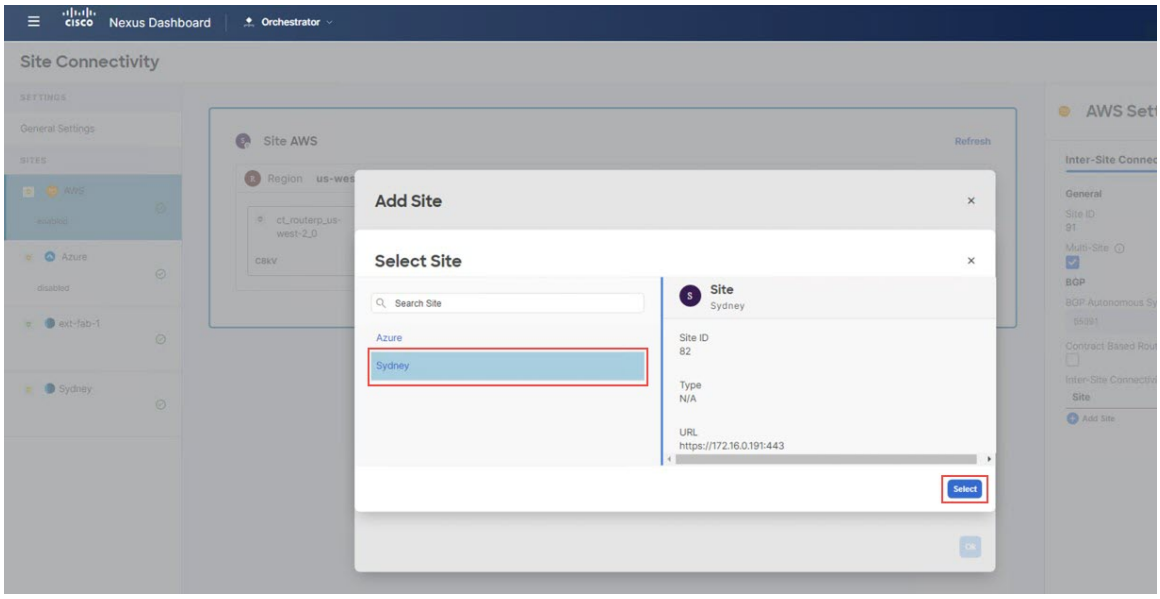
図 *65 :*



[サイトを選択（Select a Site）] ページが表示されます。

ステップ 5 NDFC VXLAN ファブリック (この例ではシドニー サイト) を選択し、**[選択（Select）]** をクリックします。

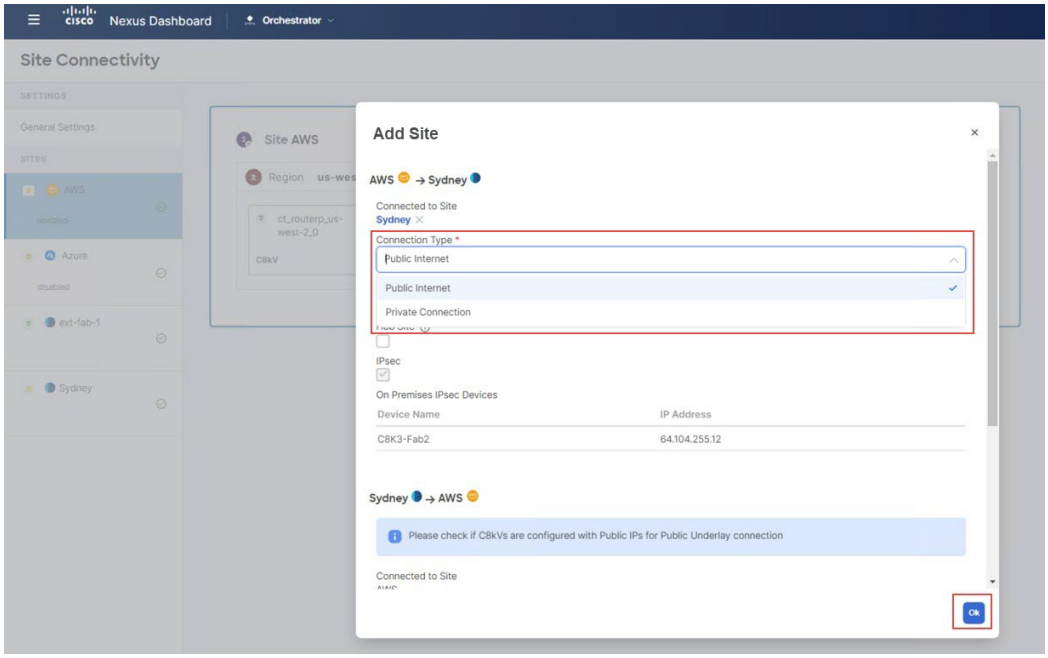
図 *66 :*



[サイトの追加（Add Site）] ページに戻ります。

ステップ 6 **[サイトの追加（Add Site）]** ページの **[接続タイプ（Connection Type）]** フィールドで、1 番目のクラウド サイトから NDFC VXLAN ファブリック サイトに使用する接続のタイプを選択します。

図 *67 :*



[パブリック インターネット（Public Internet）]を選択するか、AWS で直接接続または Azure で ExpressRoute を使用している場合は**[プライベート接続（Private Connection）]**を選択できます。

- オンプレミス サイトでは**[パブリック インターネット（Public Internet）]**と**[プライベート接続（Private Connection）]**の両方のオプションを使用できますが、クラウド サイトでは**[パブリック インターネット（Public Internet）]**接続オプションのみを使用できます。
- IPsec は、**[パブリック インターネット（Public Internet）]**接続タイプでは必須であり、その接続タイプでは自動的に有効になりますが、**[プライベート接続（Private Connection）]**タイプでは IPsec はオプションです。

（注） IPsec（マルチクラウド）でサポートされるトポロジのオプション 3などのハブ サイトを使用しているトポロジでは、**[ハブ サイト（Hub Site）]**オプションを有効にする必要があります。

この導入例に使用しているトポロジは、ハブ サイトを使用していないのでのこ導入例に**[ハブ サイト（Hub Site）]**オプションをイネーブル化しません。

ステップ 7 このページでの構成が完了したら、**[OK]**をクリックします。

次のタスク

1 つ目のクラウド サイトを2 つ目のクラウド サイトに接続する （63 ページ） の手順を実行します。

1 つ目のクラウド サイトを2 つ目のクラウド サイトに接続する

このセクションでは、最初のクラウド サイトを 2 つ目のクラウド サイトに接続します。

始める前に

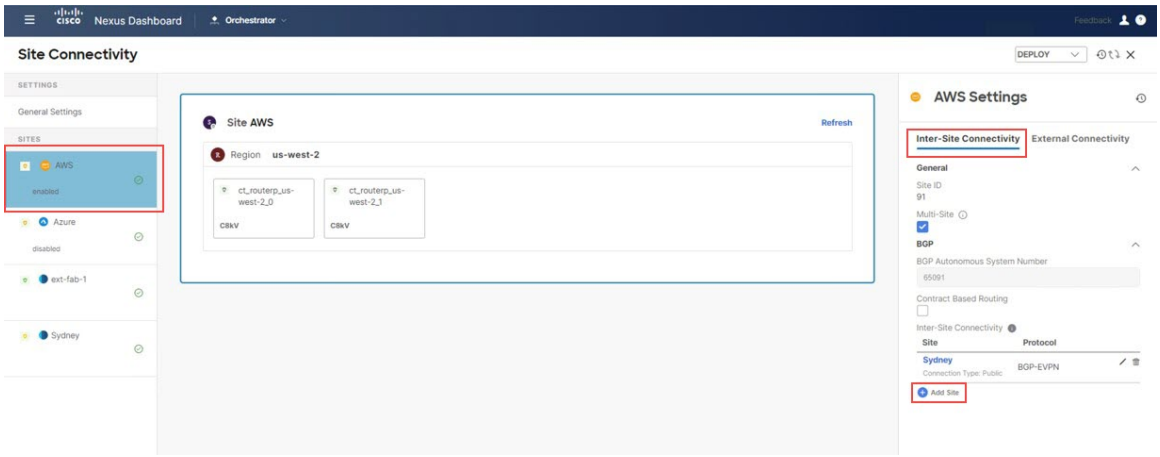
1 つ目のクラウド サイトを NDFC VXLAN ファブリック サイトに接続する （60 ページ） の手順を実行します。

ステップ 1 **[一般設定：サイト（General Settings: Sites）]**の下の左側のペインで、最初のクラウド サイト（AWS サイトなど）をクリックします。

ステップ 2 右側のウィンドウで、**[サイト間の接続（Inter-Site Connectivity）]**をクリックします。

ステップ 3 右側のペインで**[サイトの追加（Add Site）]**をクリックします。

図 *68 :*



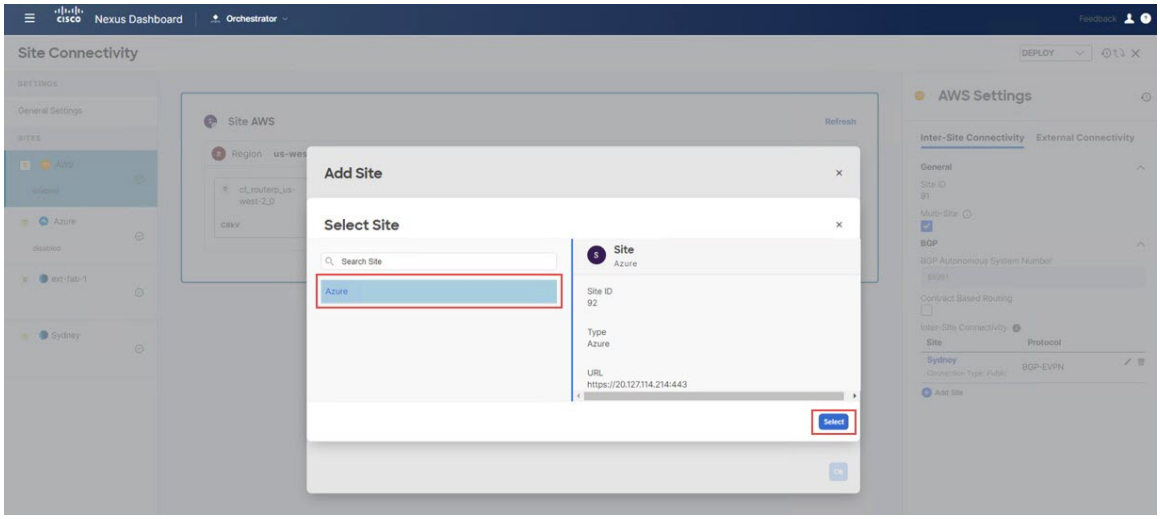
[サイトの追加（Add Site）] ページが表示されます。

ステップ 4 **[サイトの追加（Add Site）]** ページ内で**[サイトを選択（Select a Site）]**をクリックします。

[サイトを選択（Select a Site）] ページが表示されます。

ステップ 5 2 番目のクラウド サイト（たとえば、Azure クラウド サイト）を選択し、**[選択（Select）]** をクリックします。

図 *69 :*



[サイトの追加（Add Site）] ページに戻ります。

ステップ 6 **[サイトの追加（Add Site）]** ページページの **[接続タイプ（Connection Type）]** フィールドで、最初のクラウド サイトから 2 番目のクラウド サイトに使用する接続のタイプを選択します。

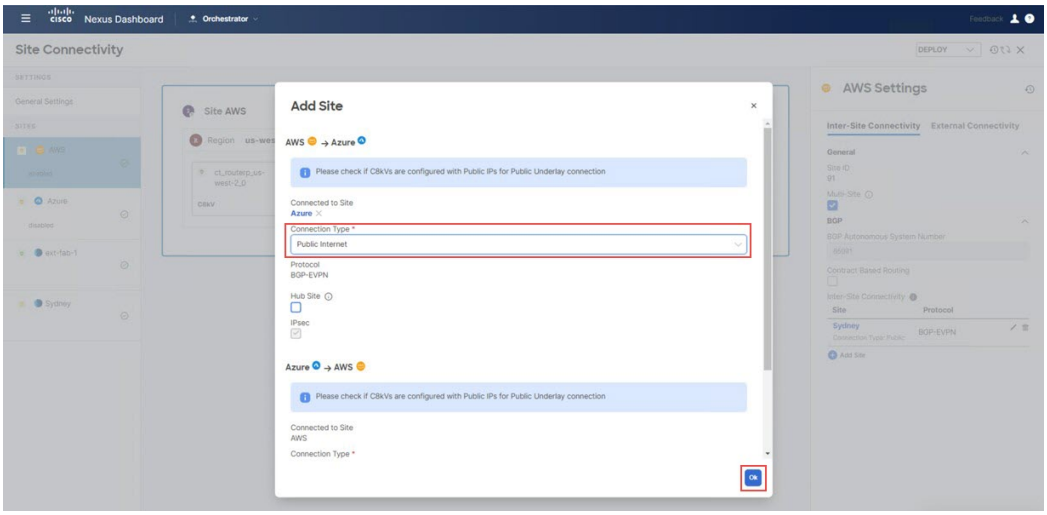
一部のタイプのクラウド間接続では、次のオプションを使用できます。

- **パブリック インターネット**

- クラウド バックボーン

クラウドバックボーンを使用して、同じプロバイダーのクラウドサイト間の接続を確立できます（たとえば、1 つのクラウド ネットワーク コントローラによって管理される AWS サイト 1 と 2 番目のクラウド ネットワーク コントローラによって管理される AWS サイト 2）。ただし、次の図に示すように、異なるクラウド プロバイダーのサイト間（AWS から Azure など）では、**パブリック インターネット**が唯一のオプションです。

図 *70 :*



パブリック インターネット 接続タイプが選択されている場合、**IPsec** オプションは必須であり、その接続タイプでは自動的に有効になりますが、**クラウド バックボーン タイプ** では IPsec はオプションです。

（注） トポロジが **ハブ サイト** を使用している場合でも、クラウド間接続のハブ サイト オプションを有効にしません (その場合、クラウド サイトと NDFC VXLAN ファブリック サイト間の接続を構成するときに **ハブ サイト** オプションを有効にします)。

ステップ 7 このページでの構成が完了したら、**[OK]** をクリックします。

次のタスク

2 つ目のクラウド サイトを NDFC VXLAN ファブリック サイトに接続する （65 ページ） の手順を実行します。

2 つ目のクラウド サイトを NDFC VXLAN ファブリック サイトに接続する

このセクションでは、2 番目のクラウド サイトを NDFC VXLAN ファブリック サイトに接続します。

このセクションの手順は、前のセクションで実行した手順と基本的に同じです。ここで、次のことを行います。

- 最初のクラウド サイトを 1 つ目のクラウド サイトを NDFC VXLAN ファブリック サイトに接続する （60 ページ） の NDFC VXLAN ファブリック サイトに接続しました。
- 最初のクラウド サイトを 1 つ目のクラウド サイトを2 つ目のクラウド サイトに接続する （63 ページ） の 2 番目のクラウド サイトに接続しました。

このセクションでは、2 番目のクラウド サイトを NDFC VXLAN ファブリック サイトに接続します。1 つ目のクラウド サイトを2 つ目のクラウド サイトに接続する （63 ページ） 内のAWS と Azure 間の接続は既に構成されているため、2 番目のクラウド サイト（Azure）から AWS への接続を構成する必要はありません。その接続は前のセクションで既に構成されているためです。

始める前に

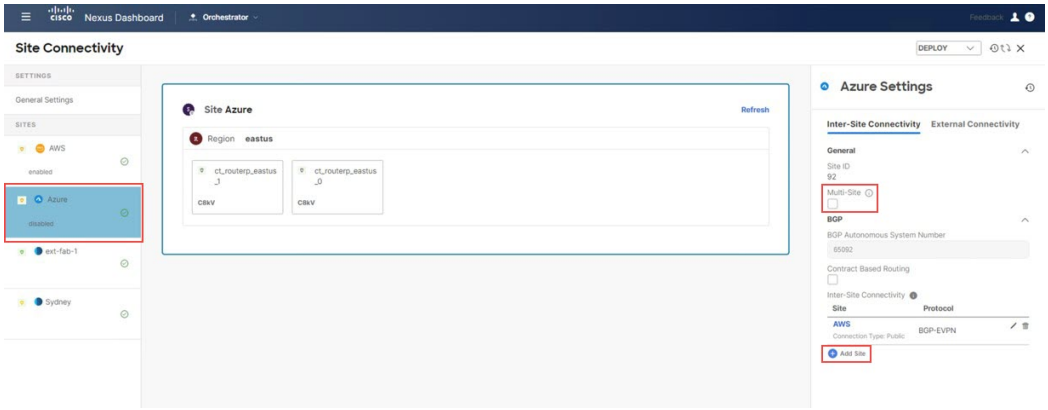
1 つ目のクラウド サイトを2 つ目のクラウド サイトに接続する （63 ページ） の手順を実行します。

ステップ 1 **[全般設定: サイト（General Settings: Sites）]** の下の左側のウィンドウで、2 番目のクラウドサイト（Azure サイトなど）をクリックします。

ステップ 2 右側のペインで、**[サイト間接続（Inter-Site Connectivity）]** をクリックし、**[マルチサイト（Multi-Site）]** の下にあるチェックボックスをオンにして、その機能を有効にします。

ステップ 3 右側のペインで **[サイトの追加（Add Site）]** をクリックします。

図 *71 :*



[サイトの追加（Add Site）] ページが表示されます。

ステップ 4 **[サイトの追加（Add Site）]** ページ内で**[サイトを選択（Select a Site）]**をクリックします。

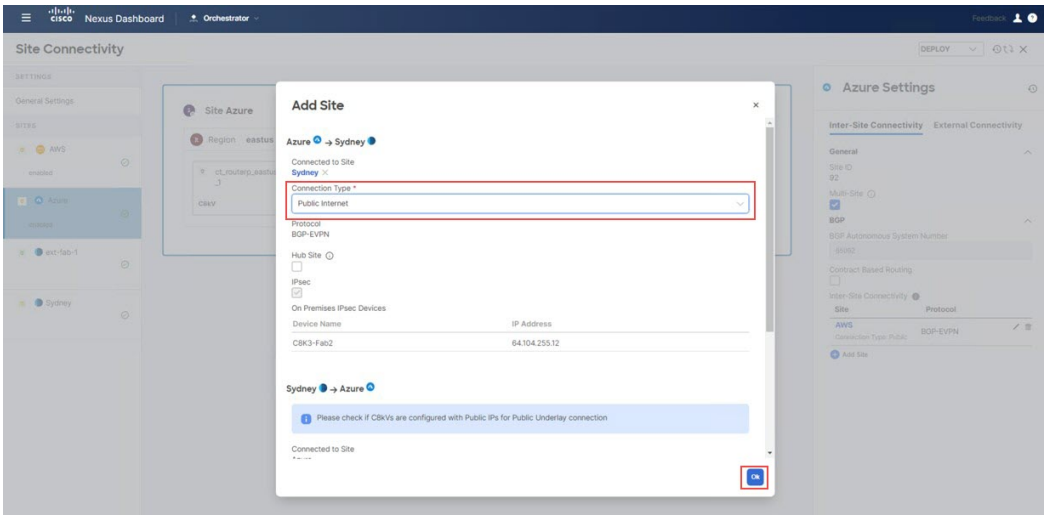
[サイトを選択（Select a Site）] ページが表示されます。

ステップ 5 NDFC VXLAN ファブリック (この例ではシドニー サイト) を選択し、**[選択（Select）]** をクリックします。

[サイトの追加（Add Site）] ページに戻ります。

ステップ 6 **[サイトの追加（Add Site）]** ページの **[接続タイプ（Connection Type）]** フィールドで、2 番目のクラウド サイトから NDFC VXLAN ファブリック サイトに使用する接続のタイプを選択します。

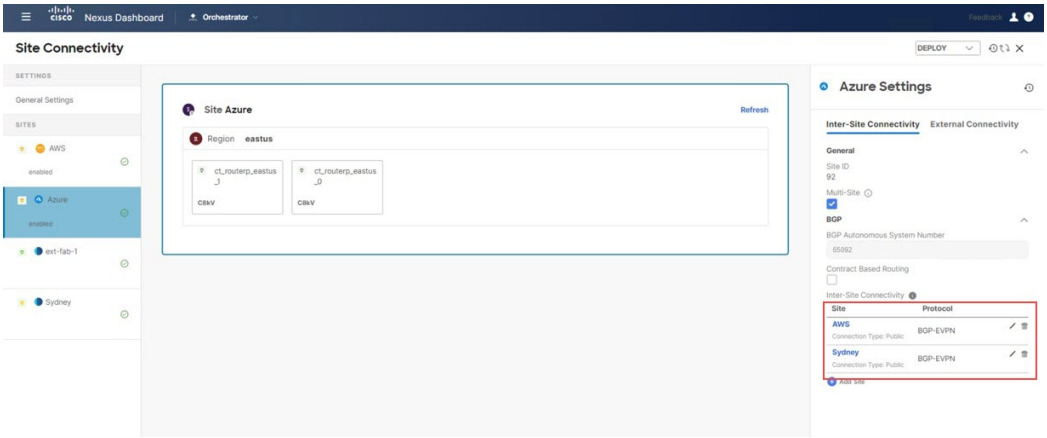
図 *72 :*



ステップ 7 このページでの構成が完了したら、**[OK]** をクリックします。

構成されたサイトが表示されます。

図 *73 :*



次のタスク

Nexus ダッシュボード オーケストレータの構成を展開 （68 ページ） の手順を実行します。

Nexus ダッシュボード オーケストレータの構成を展開

このセクションでは、Nexusダッシュボード オーケストレータ（NDO）に構成を展開します。

始める前に

2 つ目のクラウド サイトを NDFC VXLAN ファブリック サイトに接続する （65 ページ） の手順を実行します。

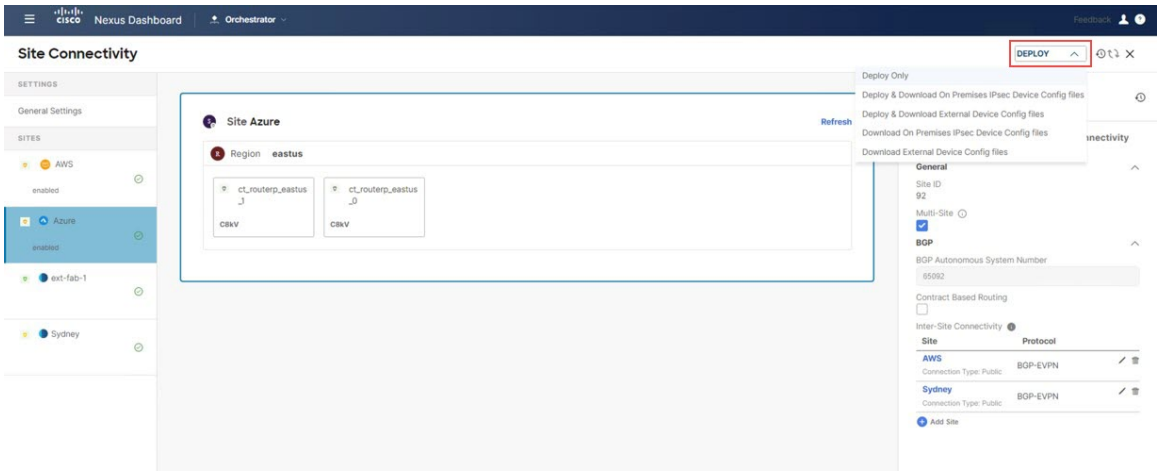
ステップ 1 NDO で構成を展開します。

- オンプレミス IPsec デバイス と IPSec トンネル サブネット プールを追加 （46 ページ）でオンプレミス IPsec デバイスの **[管理対象外（Unmanaged）]** オプションを選択した場合は、ページの右上にある **[展開（Deploy）]** > **[展開して外部デバイス構成ファイルをダウンロード（Deploy & Download External Device Config files）]**をクリックします。

  このオプションにより、オンプレミス IPsec デバイスの構成に使用する必要な構成情報を含む zip ファイルがダウンロードされます。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。

- オンプレミス IPsec デバイス と IPSec トンネル サブネット プールを追加 （46 ページ）でオンプレミス IPsec デバイスの **[管理対象（Managed）]** オプションを選択した場合は、ページの右上にある**[展開（Deploy）]** > **[展開（Deploy）]**をクリックします。

図 *74 :*



ステップ 2 **[確認（Confirmation）]** ウィンドウで、**[はい (Yes)]** をクリックします。

この時点で、NDO は次のことを行います。

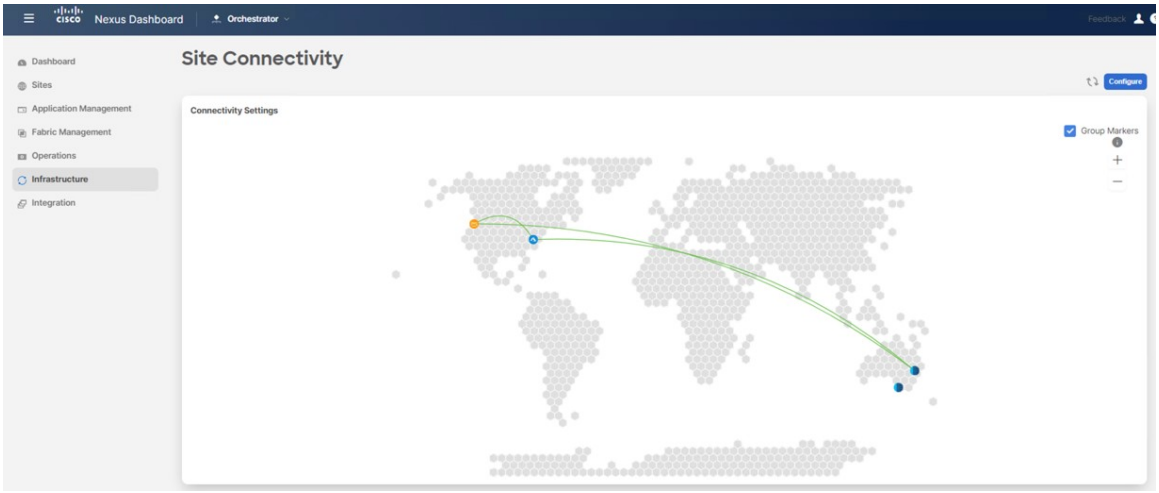
- クラウド ネットワーク コントローラを介して NDFC およびクラウド サイト（AWS および Azure）との通信を開始して、IPsec トンネルを自動化します。
- Azure Catalyst 8000V と AWS Catalyst 8000V の間で OSPF を構成します。

- BGW スパイン スイッチ、オンプレミス IPsec デバイス、および Azure Catalyst 8000V および AWS Catalyst 8000V 間の eBGP を構成します。
- サイト間の BGP-EVPN ピアリング セッションを確立します。

ステップ 3 NDO で構成が正しく行われたことを確認します。

- 左側のナビゲーション バーで**[インフラストラクチャ（Infrastructure）]** > **[サイト接続（Site Connectivity）]**をクリックし、**[接続設定（Connectivity Settings）]** エリアでサイト間の接続を確認します。

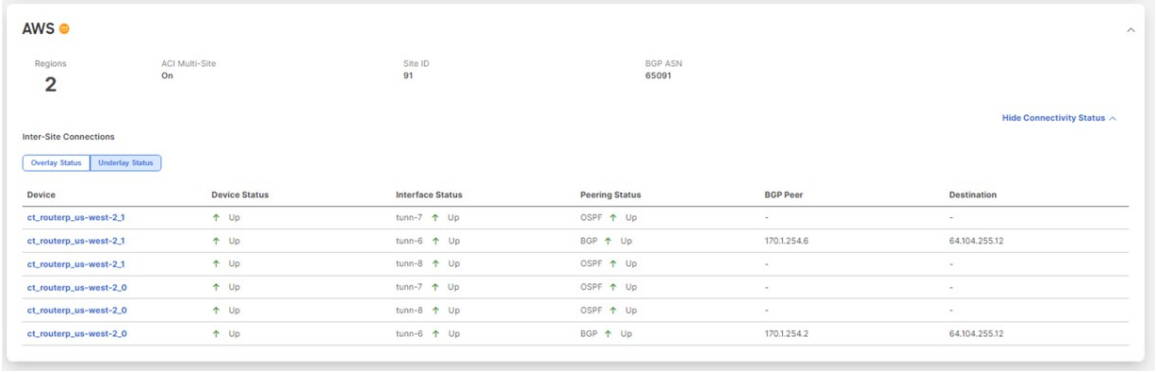
図 *75*:



- 同じページで、最初のクラウド サイト（AWS サイトなど）のエリアまで下にスクロールし、**[接続ステータスを表示（Show Connectivity Status）]** をクリックしてから、**[サイト間接続（Inter-Site Connections）]** エリアで **[アンダーレイ ステータス（Underlay Status）]** をクリックして、アンダーレイ ステータスを確認します。

  この例では、最初のクラウド サイト（AWS）に 2 つの Cisco Catalyst 8000V があり、2 番目のクラウド サイト（Azure）にある 2 つの Cisco Catalyst 8000V と、2 番目のクラウド サイト（Azure）にある 1 つの Cisco Catalyst 8000V に IPsec トンネルがあるため、6 つの IPsec トンネルがあります。オンプレミスの外部ファブリック。

図 *76*:



- 2 番目のクラウド サイト（Azure サイトなど）のエリアまでスクロール ダウンし、**[接続ステータスの表示（Show Connectivity Status）]** をクリックしてから、**[サイト間接続（Inter-Site Connections）]** エリアで **[アンダーレイ ステータス（Underlay Status）]** をクリックして、アンダーレイのステータスを確認します。

  この例では、6 つの IPsec トンネルがあります。これは、2 番目のクラウド サイト（Azure）に 2 つの Cisco Catalyst 8000V があり、最初のクラウド サイト（AWS）にある 2 つの Cisco Catalyst 8000V と、オンプレミスの外部ファブリック。

図 *77*:

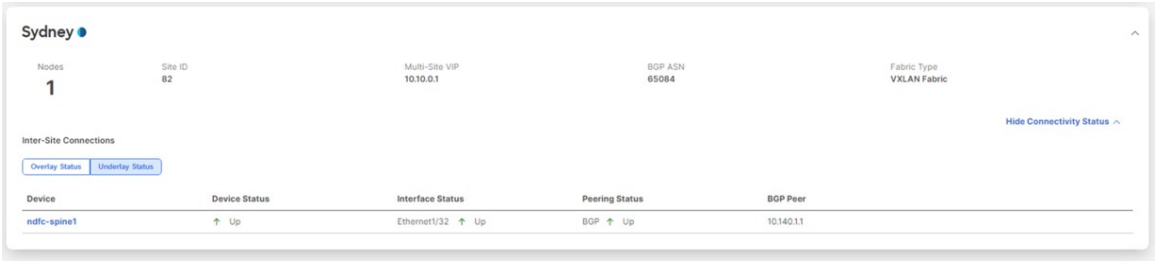
- NDFC 外部ファブリック サイトのエリアまでスクロール ダウンし、**[接続ステータスの表示（Show Connectivity Status）]** をクリックしてから、**[サイト間接続（Inter-Site Connections）]** エリアで **[アンダーレイ ステータス（Underlay Status）]** をクリックして、アンダーレイのステータスを確認します。

  外部ファブリックの機能は、オンプレミスの IPsec デバイスから VXLAN ファブリックおよびクラウド サイトへのアンダーレイの到達可能性を提供することです。アンダーレイ プロトコルは eBGP を使用します。

- NDFC VXLAN ファブリック サイトのエリアまでスクロール ダウンし、**[接続ステータスの表示（Show Connectivity Status）]** をクリックしてから、**[サイト間接続（Inter-Site Connections）]** エリアで **[アンダーレイ ステータス（Underlay Status）]** をクリックして、アンダーレイ ステータスを確認します。

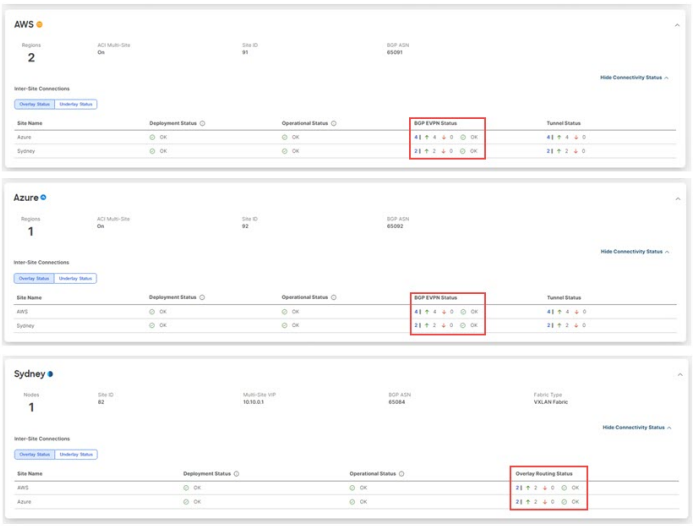
  アンダーレイ ステータスは、BGW スパイン スイッチとオンプレミス IPsec デバイス間の eBGP セッション ステータスを示します。

図 *78 :*



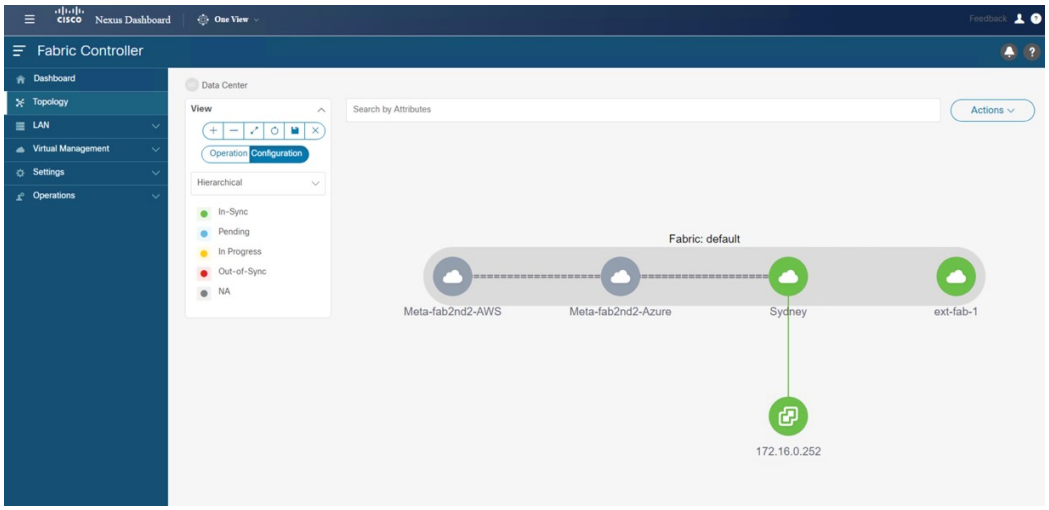
- これらの各画面で、**[オーバーレイ ステータス（Overlay Status）]** をクリックして、それぞれのオーバーレイ ステータスを確認します。

図 *79 :*



- NDFC 画面に戻り、**[トポロジ（Topology）]** 画面でハイブリッド クラウド接続を確認します。次の例では、NDFC VXLAN ファブリック サイト（シドニー サイト）が 1 番目と 2 番目のクラウド サイト（AWS および Azure クラウド サイト）に接続されていることがわかります。

図 *80 :*


Nexus Dashboard
One View
Feedback
Fabric Controller
Dashboard
Topology
LAN
Virtual Management
Settings
Operations
Data Center
View
Operation
Configuration
Hierarchical
In-Sync
Pending
In Progress
Out-of-Sync
NA
Search by Attributes
Actions
Fabric: default
Meta-fab2nd2-AWS
Meta-fab2nd2-Azure
Sydney
ext-fab-1
172.16.0.252

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。