



## Cisco NX-OS のハイブリッドクラウド接続展開

初版：2023 年 1 月 31 日

最終更新：2023 年 4 月 17 日

### シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>





## Trademarks

---

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at:

<http://www.cisco.com/go/softwareterms>. Cisco product warranty information is available at

<http://www.cisco.com/go/warranty>. US Federal Communications Commission Notices are found here

<http://www.cisco.com/c/en/us/products/us-fcc-notice.html>.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and-if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com go trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)





## 目次

---

|        |                       |
|--------|-----------------------|
| はじめに : | <b>Trademarks</b> iii |
|--------|-----------------------|

---

|       |                   |
|-------|-------------------|
| 第 1 章 | <b>新機能と更新情報</b> 1 |
|       | 新機能と更新情報 1        |

---

|         |   |
|---------|---|
| 第 1 部 : | <b>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</b> 3 |
|---------|---|

---

|       |                             |
|-------|-----------------------------|
| 第 2 章 | <b>概要</b> 5                 |
|       | ハイブリッドクラウド接続のコンポーネントを理解する 5 |
|       | ハイブリッドクラウド接続を構築 7           |
|       | 用語 10                       |
|       | 前提条件 13                     |
|       | 注意事項と制約事項 13                |
|       | 関連資料 14                     |

---

|       |                                      |
|-------|--------------------------------------|
| 第 3 章 | <b>サポートされるトポロジ</b> 15                |
|       | [Connection] のオプション 15               |
|       | IPsec (シングルクラウド) でサポートされるトポロジ 16     |
|       | IPsec (マルチクラウド) でサポートされるトポロジ 21      |
|       | IPsec なしでサポートされているトポロジ (シングルクラウド) 25 |
|       | IPsec なしでサポートされるトポロジ (マルチクラウド) 29    |

---

|       |  |
|-------|--|
| 第 4 章 | <b>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</b> 35 |
|       | 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 35       |

|   |     |
|---|-----|
| オンプレミス NDFC ファブリックを設定                       | 37  |
| NDFC VXLAN ファブリックを作成                        | 37  |
| NDFC VXLAN ファブリックを作成                        | 38  |
| VXLAN ファブリックへのスイッチの追加                       | 41  |
| NDFC 外部ファブリックを構成                            | 45  |
| NDFC 外部ファブリックを作成                            | 46  |
| オンプレミス Cisco Catalyst 8000V を外部ファブリックに追加    | 49  |
| 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            | 55  |
| 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            | 56  |
| AWS の詳細設定で必要なパラメータを構成します                    | 57  |
| AWS のリージョン管理の必要なパラメータを構成します                 | 58  |
| 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          | 63  |
| Azure の詳細設定で必要なパラメータを構成します                  | 63  |
| Azure のリージョン管理で必要なパラメーターを構成する               | 65  |
| NDFC とクラウドサイトを ND と NDO に導入準備する             | 70  |
| Complete サイト間の接続 NDFC とクラウドサイトの間            | 78  |
| 必要なコントロールプレーン構成を完了する                        | 78  |
| 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 | 80  |
| 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              | 87  |
| VXLAN ファブリック サイトのマルチサイト VIP を定義します。         | 89  |
| IPsec デバイスを VXLAN ファブリック サイトにマップする          | 90  |
| 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   | 92  |
| 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    | 94  |
| 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             | 97  |
| 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    | 99  |
| Nexus ダッシュボード オーケストレータの構成を展開                | 102 |

---

第 II 部 :           **使用例 107**

---

第 5 章           **テナントを展開 109**

    テナントを展開 109

---

|       |                              |
|-------|------------------------------|
| 第 6 章 | ストレッチされた VRF ユース ケース 117     |
|       | ストレッチされた VRF ユース ケースについて 117 |
|       | ストレッチされた VRF ユース ケースの構成 118  |

---

|       |  |
|-------|--|
| 第 7 章 | ルート リークの使用例 155                        |
|       | ルート リークの使用例について 155                    |
|       | 必要なテンプレートの構成 157                       |
|       | オンプレミス サイトテンプレートの構成 157                |
|       | Azure サイトテンプレートの構成 166                 |
|       | AWS サイトテンプレートの構成 172                   |
|       | ルートリークの設定 177                          |
|       | Azure VRF から NDFC VRF へのルート リークの構成 177 |
|       | Azure VRF から AWS VRF へのルート リークの構成 179  |
|       | AWS VRF から NDFC VRF へのルート リークの構成 182   |
|       | AWS VRF から Azure VRF へのルート リークの構成 184  |
|       | NDFC VRF から AWS VRF へのルート リークの構成 186   |
|       | NDFC VRF から Azure VRF へのルート リークの構成 188 |
|       | 構成の確認 191                              |





# 第 1 章

## 新機能と更新情報

---

- [新機能と更新情報 \(1 ページ\)](#)

## 新機能と更新情報

次の表は、この最新リリースまでの主な変更点の概要を示したものです。ただし、今リリースまでの変更点や新機能の一部は表に記載されていません。

| リリースバージョン         | 特長                 | 説明                 |
|-------------------|--------------------|--------------------|
| NDFC リリース 12.1.2e | このユースケースドキュメントの初版。 | このユースケースドキュメントの初版。 |





## 第 1 部

# 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

- [概要 \(5 ページ\)](#)
- [サポートされるトポロジ \(15 ページ\)](#)
- [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を設定する \(35 ページ\)](#)





## 第 2 章

### 概要

- [ハイブリッドクラウド接続のコンポーネントを理解する \(5 ページ\)](#)
- [ハイブリッドクラウド接続を構築 \(7 ページ\)](#)
- [用語 \(10 ページ\)](#)
- [前提条件 \(13 ページ\)](#)
- [注意事項と制約事項 \(13 ページ\)](#)
- [関連資料 \(14 ページ\)](#)

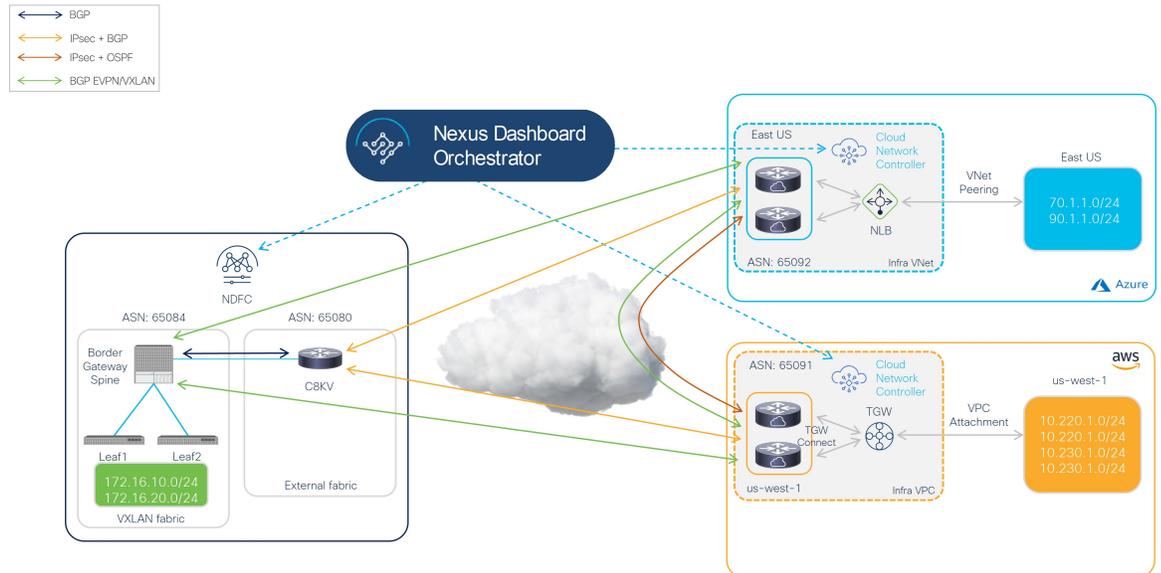
## ハイブリッドクラウド接続のコンポーネントを理解する

このドキュメントでは、Cisco Nexus ダッシュボード ファブリック コントローラ (NDFC) によって管理される Cisco Nexus 9000 NX-OS ベースのファブリックと Cisco クラウドネットワーク コントローラ (CNC) によって管理されるパブリッククラウドサイトを備えた、Cisco Nexus ダッシュボード オーケストレータ (NDO) によって強化された Cisco ハイブリッドクラウド ネットワーキング ソリューションの導入手順について説明します。

Cisco Nexus Dashboard Orchestrator (NDO) ベースのハイブリッドクラウドソリューションは、オンプレミス ネットワークとクラウド ネットワーク間のシームレスな接続を提供します。このソリューションは、NDFC を使用してオンプレミスの VXLAN ベースのファブリックとオンプレミスの Cisco Catalyst 8000V を管理しますが、クラウド サイト (AWS または Microsoft Azure) は Cisco Cloud Network Controller (CNC) によって管理されます。NDO は、オンプレミス サイトとクラウド サイト間、および 2 つ以上のクラウド サイト間の接続を調整するために使用されます。VXLAN は、サイト間にオーバーレイ トンネルを構築するために使用されます。

次の図は、これらのコンポーネントを使用したハイブリッドクラウド接続のトポロジ例を示しています。詳細については、「[サポートされるトポロジ \(15 ページ\)](#)」を参照してください。

図 1:



このトポロジ例では、NDFCが管理するオンプレミスサイトにAWSおよびAzureクラウドサイトへの安全な接続が設定されています。そこではインフラ VPC/VNet の上の Cisco Catalyst 8000Vは、オンプレミスデータセンターから来るそしてオンプレミスデータセンターへ向かう全てのトラフィックのクラウドゲートウェイの役割があります。

ボーダーゲートウェイ (BGWs) でもある、様々なオンプレミス VXLAN EVPN サイトのシームレス Layer-2/Layer-3 DCI 拡張をサポートするオンプレミスサイト上で、パブリッククラウドへ Layer-3 拡張もサポートします。

クラウド内の BGW と Cisco Catalyst 8000V 間のコントロールプレーンには BGP-EVPN が使用され、データプレーンには VXLAN が使用されます。

前の図に示すように、Cisco Hybrid クラウドネットワークングソリューションは次のコンポーネントで構成されています。

- **Cisco Nexus ダッシュボード オーケストレータ (NDO)** : NDO は、セントラルポリシーコントローラとして働き、様々な NDFC インスタンスに管理されている複数のオンプレミスファブリックに渡ってポリシーを管理します。そして、各クラウドサイトは、自分の Cisco クラウドネットワークコントローラに抽象化されます。NDO は Nexus ダッシュボード上のサービスとして実行されます。Nexus ダッシュボードは、VMware ESXi、Linux KVM、Amazon Web Services、または Microsoft Azure で実行される物理アプライアンスまたは仮想マシンのクラスターとして展開できます。以前にバージョン間サポートが導入されているため、NDO は、異なるソフトウェアバージョンを実行している Cisco クラウドネットワークコントローラを管理できます。
- **[Cisco Nexus ダッシュボードファブリックコントローラ (NDFC)]** : NDFC は、LAN、VXLAN、SAN、および Cisco IP Fabric for Media (IPFM) ファブリックを構築するためのネットワーク自動化およびオーケストレーションツールです。NDFC は、物理クラスターまたは仮想クラスターのいずれかである Nexus ダッシュボードクラスター上でサービスとして実行されます。ハイブリッドクラウドネットワークングソリューションの場合、

NDFCはオンプレミスのVXLANファブリックとオンプレミスのCisco Cloud Router (Catalyst 8000V) を管理します。

- **オンプレミス VXLAN ファブリック** : オンプレミス VXLAN ファブリックは、NDFC によって管理される Nexus 90000/3000 スイッチで構築されています。ファブリックには、オンプレミス サイトとクラウド サイト間の VXLAN マルチサイト オーバーレイ トンネルの開始と終了を担当する 1 つ以上のボーダー ゲートウェイ (BGW) デバイスが必要です。NDFC には、VXLAN ファブリックを作成するための事前に作成されたテンプレートがあります。このドキュメントでは、VXLAN ファブリックに External\_Fabric テンプレートを使用しています。
- **オンプレミスの Cisco Cloud Router (CCR)** : CCR は、オンプレミスの VXLAN ファブリックとクラウド サイト間の到達可能性を提供するために使用されます。CCR は、パブリックインターネットまたはプライベート接続 (AWS Direct Connect や Azure ExpressRoute など) を使用してクラウド サイトへの接続を提供します。オンプレミスの CCR は、事前に構築された External\_Fabric テンプレートを使用して NDFC によって管理され、コア ルーター ロールを割り当てる必要があります。

Cisco Catalyst 8000V は、Cisco ハイブリッドクラウド ネットワーキング ソリューションのオンプレミス CCR として使用されます。

- **Cisco クラウド ネットワーク コントローラ (CNC)** : Cisco クラウド ネットワーク コントローラは、サポートされているパブリッククラウド上で仮想インスタンスとして実行され、パブリッククラウド内の自動接続、ポリシー変換、およびワークロードのさらなる可視性を提供します。Cisco クラウド ネットワーク コントローラは、NDO から受け取ったすべてのポリシーを変換し、それらをクラウドネイティブの構造、AWS の VPC やセキュリティグループや Microsoft Azure の VNet などにプログラムします。Cisco Cloud Network Controller は、AWS Marketplace や Azure Marketplace などのパブリッククラウドマーケットプレイスを通じて展開されます。
- **Cisco Catalyst 8000V** : Cisco Catalyst 8000V は、パブリッククラウドプラットフォームの重要なコンポーネントです。Cisco Catalyst 8000V は、オンプレミスサイトおよびパブリッククラウドプラットフォームへのサイト間通信に使用されます。さらに、Cisco Catalyst 8000V は、オンプレミスのクラウド接続と、さまざまなクラウドプロバイダー間の接続 (たとえば、Azure から AWS) に使用されます。

## ハイブリッドクラウド接続を構築

このセクションでは、ハイブリッドクラウド接続を構築するために使用されるプロセスについて説明します。

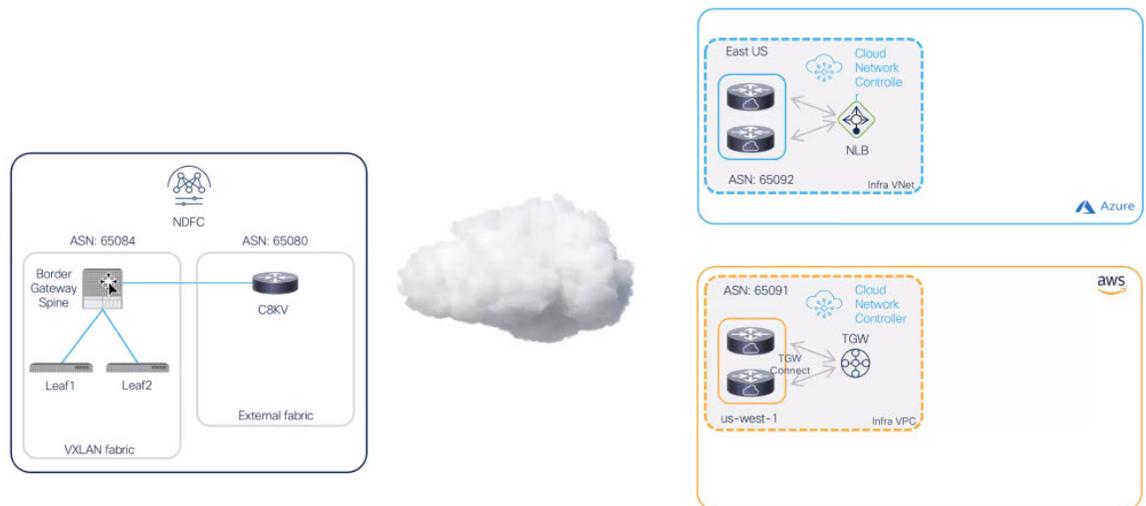
- [開始点 \(8 ページ\)](#)
- [アンダーレイ レイヤーの構築 \(8 ページ\)](#)
- [オーバーレイの構築 \(9 ページ\)](#)

## 開始点

次の図は、ハイブリッドクラウド接続の開始点を示しています。ここでは、[ハイブリッドクラウド接続のコンポーネントを理解する \(5 ページ\)](#) で説明されているさまざまな部分があります：

- Nexus ダッシュボードファブリック コントローラ (NDFC) のファブリック：
  - オンプレミスの VXLAN ファブリック
  - 外部ファブリック
- 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クラウドサイト (AWS および Azure)

図 2:

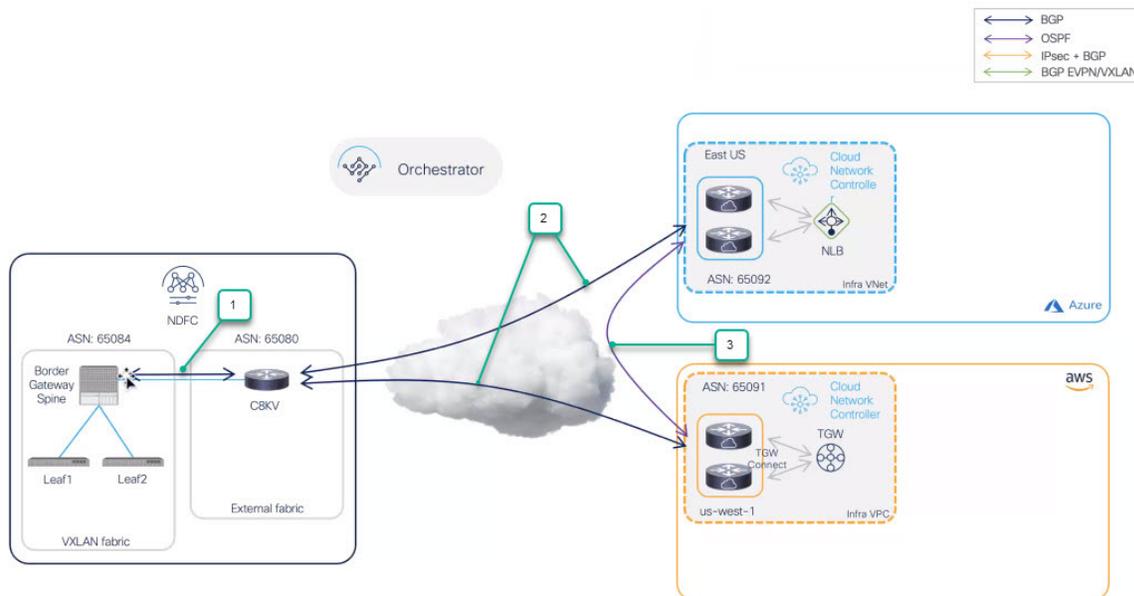


## アンダーレイ レイヤーの構築

次に、後でアンダーレイがどのように構築されるかを示します。

1. まず、VXLANファブリックのボーダーゲートウェイスパインスイッチと外部ファブリックの Cisco Catalyst 8000V の間に BGP 接続が確立されます。
2. 次に、BGP ピアリングを使用して、外部ファブリックのオンプレミス Cisco Catalyst 8000V とクラウドサイトの各クラウドルータ間のアンダーレイ接続を確立します。
3. 最後に、OSPF はクラウドサイト間でクラウド間アンダーレイ接続に使用されます。

図 3:

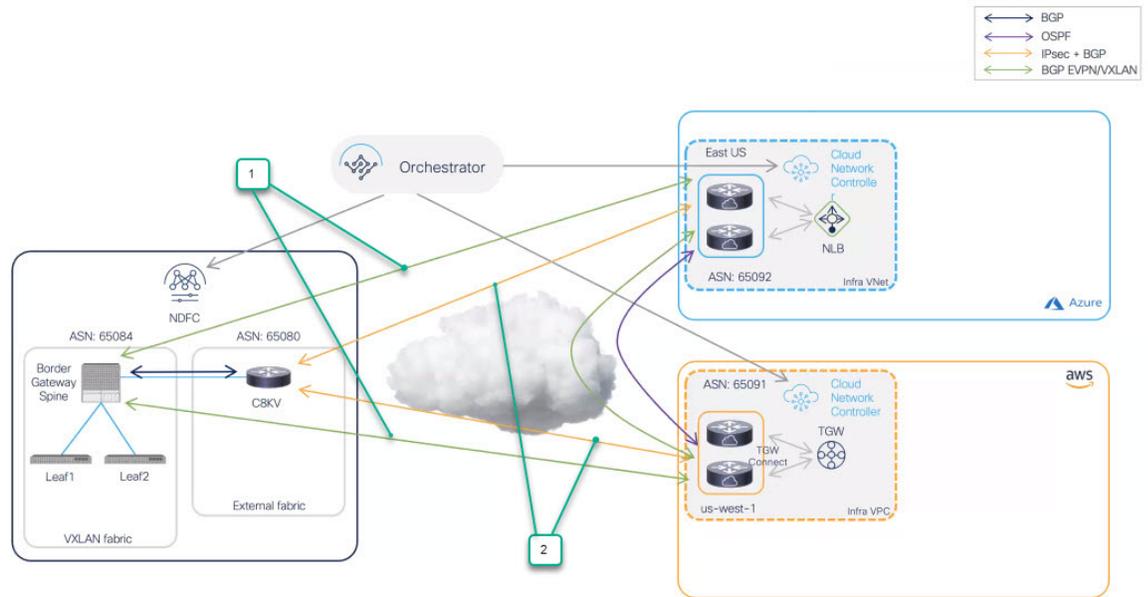


### オーバーレイの構築

最後に、前の手順で確立されたアンダーレイ接続の上に VXLAN マルチサイトオーバーレイを確立する方法を示します：

1. VXLAN マルチサイトが確立されます。これは、VXLAN ファブリックのボーダー ゲートウェイ スパイニングスイッチから始まり、クラウドサイトの Cisco Catalyst 8000V で終了します。
2. 接続タイプとしてパブリック インターネットを選択した場合、IPsec と OSPF を使用して NDFC VXLAN ファブリック サイトとクラウドサイトの間を接続します。

図 4:



## 用語

このマニュアルでは、次の用語を使用します。

| 用語         | 略語  | 定義  |
|------------|-----|---|
| ボーダーゲートウェイ | BGW | NDFC 簡単ファブリック (VXLAN EVPN ファブリックなど) でサポートされているスイッチロールの1つ。BGWは、オンプレミスファブリック間のレイヤー2/レイヤー3 DCI 接続と、パブリッククラウドサイトへのレイヤー3 接続 (ハイブリッドクラウド接続など) を拡張するために使用されます。 |

| 用語           | 略語  | 定義  |
|--------------|-----|---|
| コア ルータ       |     | <p>NDFC 外部ファブリックでサポートされる役割の1つ。</p> <p>コア ルータは、一方の側で VXLAN EVPN ファブリックと、もう一方の側でクラウドサイトの Catalyst 8000V とのレイヤ 3 接続（アンダーレイ）を確立するために使用されます。</p>                                     |
| 直接接続         |     | <p>AWS クラウドで使用されます。AWS 直接接続は、ネットワークを AWS に直接リンクして、一貫した低遅延のパフォーマンスを提供するクラウドサービスです。</p>   |
| ExpressRoute |     | <p>Azure クラウドで使用されます。Azure ExpressRoute を使用して、Azure データセンターとオンプレミスまたはコロケーション環境のインフラストラクチャとの間にプライベート接続を作成できます。</p>   |
| サイト間ネットワーク   | ISN | <p>オンプレミスの VXLAN ファブリック間、およびパブリッククラウド（「アンダーレイ」とも呼ばれる）と、オンプレミスの VXLAN ファブリックをインターコネクトするために使用されるレイヤー 3 インフラストラクチャ。そのため、ISN には、インターネットまたは直接接続および ExpressRoute 専用回線を含めることもできます。</p> |

| 用語            | 略語        | 定義  |
|---------------|-----------|---|
| IP セキュリティ ルータ | IPSec ルータ | オンプレミス サイトとクラウド サイト Cisco クラウド ネットワーク コントローラの間で IPsec 接続を確立するには、インターネット プロトコル セキュリティ (IPsec) 対応の ルータが必要です。  |
| ルーティング サーバ    | RS        | <p>コントロールプレーン ノードは、オンプレミスの BGW デバイス間の EVPN 隣接関係 (アジャセンシー) の確立を容易にするために使用され、それらすべての間にフルメッシュ ピアリングを作成する必要性を軽減します。ルート サーバは BGP プロトコルを実行し、2 つ以上の BGP ピア間でルートを渡すために使用されます。</p> <p>ルート サーバ機能は、iBGP セッションに従来使用されていた「ルータリフレクタ」機能に相当する eBGP です。必要な BGP ピアリングの数を減らすのに役立ちます。</p> |
| 仮想ネットワーク      | VNet      | <p>Azure クラウドで使用されます。Azure Virtual Network (VNet) は、Azure のプライベート ネットワークの基本的な構成要素です。VNet を使用すると、Azure 仮想マシン (VM) などのさまざまな種類の Azure 情報技術が、相互、インターネット、およびオンプレミス ネットワークと安全に通信できます。</p> <p>クラウド ネットワーク コントローラに関連して、クラウド ネットワーク コントローラの VRF は Azure の VNet にマッピングされます。</p> |

| 用語           | 略語  | 定義   |
|--------------|-----|--|
| 仮想プライベートクラウド | VPC | <p>AWS クラウドで使用されます。Amazon 仮想プライベートクラウド (VPC) は、お客様が定義する仮想ネットワークで AWS の情報技術を起動できるようにします。この仮想ネットワークは、お客様自身のデータセンターで運用されている可能性がある従来型のネットワークとよく似ているだけでなく、AWS の拡張可能なインフラストラクチャを活用するというメリットがあります。</p> <p>クラウドネットワークコントローラに関連して、クラウドネットワークコントローラの VRF は AWS の VPC にマッピングされます。</p> |

## 前提条件

次のソフトウェアバージョンが必要です。

- Cisco Nexus ダッシュボード (ND) バージョン 2.3.1c 以降 (物理または仮想クラスタ)
- Cisco Nexus ダッシュボードファブリックコントローラ (NDFC) バージョン 12.1.2e 以降
- Cisco Nexus ダッシュボードオーケストレータ (NDO) バージョン 4.1 (1) 以降
- AWS サイトおよび Microsoft Azure サイト用の Cisco クラウドネットワークコントローラ (CNC) バージョン 25.1 (1e) 以降

## 注意事項と制約事項

以下は、ハイブリッドクラウド接続ソリューションを展開するときに理解する必要がある特定のガイドラインと制限事項です。

- 現在、各 Cisco クラウドネットワークコントローラは、AWS および Azure クラウドで最大 16 のリージョンを管理できます。16 を超えるリージョンを管理する場合は、追加の Cisco クラウドネットワークコントローラを展開する必要があります。詳細については、[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](#)または[Azure インス](#)

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「サイト、リージョン、および CCR の数の制限について」セクションを参照してください。

## 関連資料

Cisco ハイブリッドクラウド ネットワーキング ソリューションを構成するコンポーネントのドキュメントは、次の場所にあります：

- [Cisco Nexus ダッシュボード オーケストレータ \(NDO\) ドキュメント](#)
- [Cisco Nexus ダッシュボード ファブリック コントローラ \(NDFC\) ソリューション](#)
- [Cisco クラウド ネットワーク コントローラ \(CNC\) ドキュメント](#)
- [Cisco キャタリスト 8000V ドキュメント](#)
- [Amazon Web Services \(AWS\) ドキュメント](#)
- [Microsoft Azure ドキュメント](#)



## 第 3 章

# サポートされるトポロジ

- [Connection] のオプション (15 ページ)
- IPsec (シングルクラウド) でサポートされるトポロジ (16 ページ)
- IPsec (マルチクラウド) でサポートされるトポロジ (21 ページ)
- IPsec なしでサポートされているトポロジ (シングルクラウド) (25 ページ)
- IPsec なしでサポートされるトポロジ (マルチクラウド) (29 ページ)

## [Connection] のオプション

Cisco ハイブリッドクラウド ネットワーキング ソリューションでは、次の接続オプションを使用できます：

- **[IPsec 付き (With IPsec)]** : オンプレミスのデータセンターからクラウドへの接続がパブリック インターネットを介している場合、安全なチャネルを確立するために IPsec トンネルが必要です。この場合、ボーダー ゲートウェイ (BGW) は、ASR 1000 または、Cisco Catalyst 8000V などのオンプレミス IPsec-capable デバイスに接続されます。このデバイスは、クラウド内の Catalyst 8000V との IPsec トンネルを確立します。オンプレミスの BGW は、この「IPsec で保護されたアンダーレイ」を利用して、クラウド内の Catalyst 8000V で VXLAN トンネルを構築できます。
- **[IPsec 抜き (Without IPsec)]** : BGW が直接接続 (AWS) または、ExpressRoute (Azure) を使用してパブリック クラウドに接続されている場合、IPsec を有効にするのはオプションです。この場合、オンプレミスの VXLAN EVPN データセンターとそれらの専用回線上の Cisco Catalyst 8000V との間で VXLAN 接続が採用されます。

次のセクションでは、これらの接続オプションのいずれかを使用して使用できる、サポートされているトポロジに関する詳細情報を提供します。

- IPsec (シングルクラウド) でサポートされるトポロジ (16 ページ)
- IPsec (マルチクラウド) でサポートされるトポロジ (21 ページ)
- IPsec なしでサポートされているトポロジ (シングルクラウド) (25 ページ)
- IPsec なしでサポートされるトポロジ (マルチクラウド) (29 ページ)

## IPsec (シングルクラウド) でサポートされるトポロジ

次の表は、オンプレミス サイトとオンプレミスとクラウド サイトの間で BGP EVPN コントロールプレーンの隣接関係を確立する方法と、オンプレミス サイトと1つのクラウド サイト間のアンダーレイ接続を確立するために IPsec を利用する方法を示しています。



(注) 次の各図は、簡単な例を表示します。実際のシナリオでは、各ロールにデバイスが重複で展開されている可能性があります。

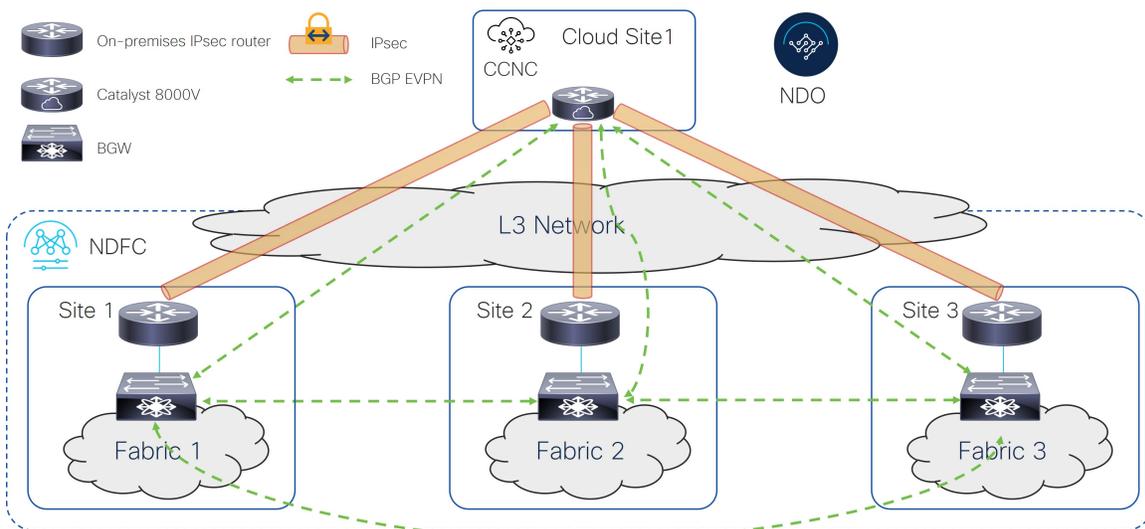
| オンプレミスの間の BGP EVPN | クラウド サイトへの BGP EVPN と IPsec      |                                  |   |
|--------------------|----------------------------------|----------------------------------|---|
|                    | フルメッシュ                           | バフ サイトのみを通して                     | <ul style="list-style-type: none"> <li>• BGP EVPN からクラウド サイトへ: フルメッシュ</li> <li>• クラウド サイトへの IPsec: 共有 IPsec ルーター経由のみ</li> </ul> |
| フルメッシュ             | <a href="#">オプション 1 (16 ページ)</a> | <a href="#">オプション 3 (18 ページ)</a> | <a href="#">オプション 5 (20 ページ)</a>  |
| ルーティング サーバ付き       | <a href="#">オプション 2 (17 ページ)</a> | <a href="#">オプション 4 (19 ページ)</a> | 該当なし  |

### オプション1

次の図は、IPsec を使用してシングルクラウド接続の例を示しています。

- 全てのオンプレミスサイトにある BGW ノードは、フルメッシュ BGP EVPN 隣接関係 (アジャセンシー) を間に確立させます。
- クラウドサイトの Cisco Catalyst 8000V は、各オンプレミスサイトに展開されたコア ルータと IPsec トンネルを確立し、オンプレミスサイトのすべての BGW デバイスとフルメッシュ BGP EVPN 隣接関係 (アジャセンシー) 全てのを確立します。

図 5:



## オプション 2

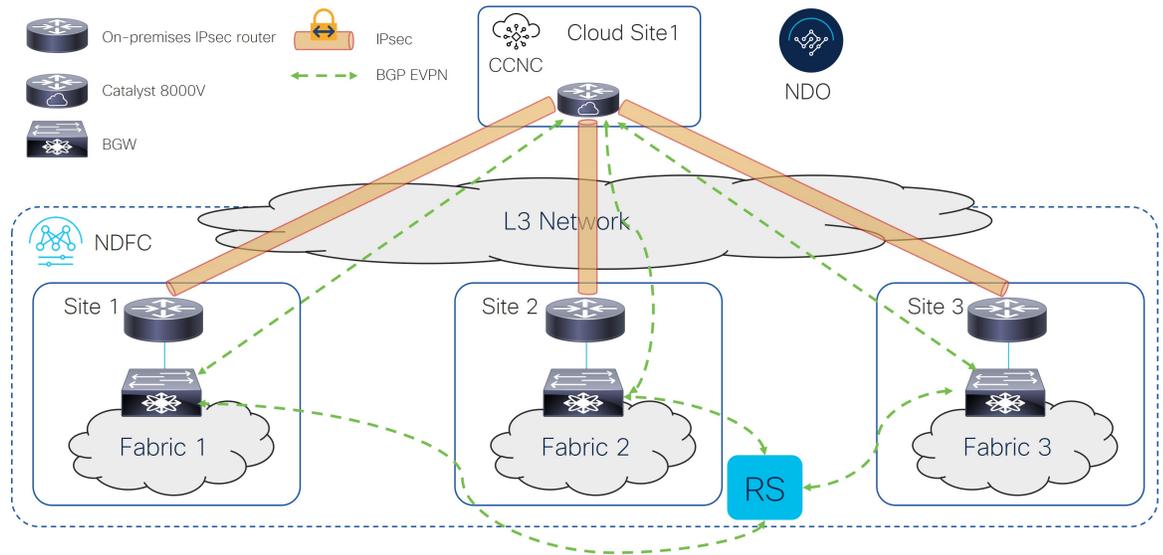
次の図は、IPsec を使用してシングルクラウド接続の例を示しています。

- BGW ノードは、全てのオンプレミスサイトに EVPN 隣接関係 (アジャセンシー) と一緒にルートサーバー (RS) コントロールプレーンノードを確立します。
- クラウドサイトの Cisco Catalyst 8000V は、各オンプレミスサイトに展開されたコアルータとフルメッシュ IPsec トンネルを確立し、オンプレミスサイトのすべての BGW デバイスと BGP EVPN 隣接関係 (アジャセンシー) 全てのを確立します。



(注) 現在、ルートサーバコントロールノードと Cisco Catalyst 8000V をピアリングすることはサポートされていません。

図 6:

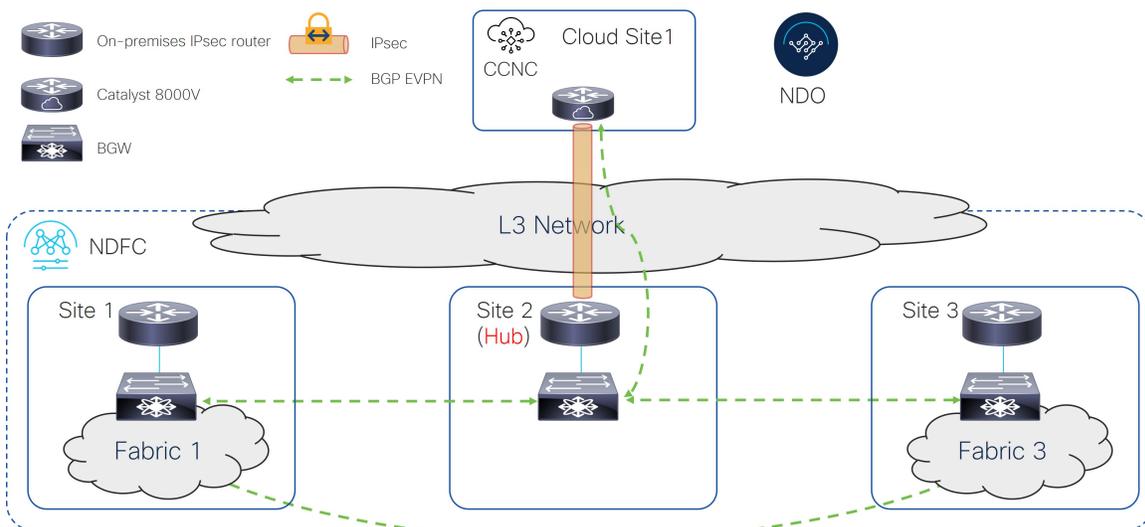


### オプション3

次の図は、IPsec を使用してシングルクラウド接続の例を示しています。

- 全てのオンプレミスサイトにあるBGWノードは、フルメッシュBGPEVPN隣接関係（アジャセンシー）を間に確立させます。
- クラウドサイトのCisco Catalyst 8000Vは、特定のオンプレミスハブサイトに展開されたコアルータとのみIPsecトンネルを確立し、ハブサイトのBGWデバイスとのみBGPEVPN隣接を確立します。
- サイト2（Cisco Catalyst 8000VがEVPNに現れる）内で展開されたBGWは、後ろにファブリックを持つことはできません。オンプレミスとクラウドサイトの間でプレフィックスを交換するためののみ使用されます。

図 7:



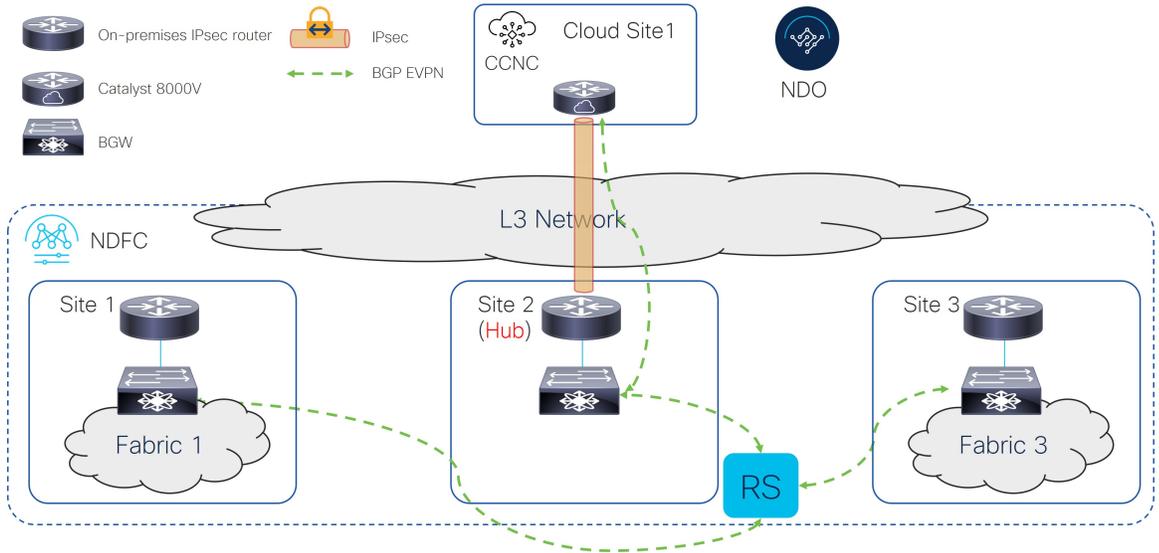
#### オプション 4

次の図は、IPsec を使用してシングルクラウド接続の例を示しています。

- BGW ノードは、全てのオンプレミスサイトに EVPN 隣接関係（アジャセンシー）と一緒にルートサーバーコントロールプレーンノードを確立します。
- クラウドサイトの Cisco Catalyst 8000V は、特定のオンプレミスハブサイトに展開されたコアルータとのみ IPsec トンネルを確立し、ハブサイトの BGW デバイスとのみ EVPN 隣接を確立します。
- サイト 2（Cisco Catalyst 8000V が EVPN に現れる）内で展開された BGW は、後ろにファブリックを持つことはできません。オンプレミスとクラウドサイトの間でプレフィックスを交換するためにのみ使用されます。

IPsec (シングルクラウド) でサポートされるトポロジ

図 8:

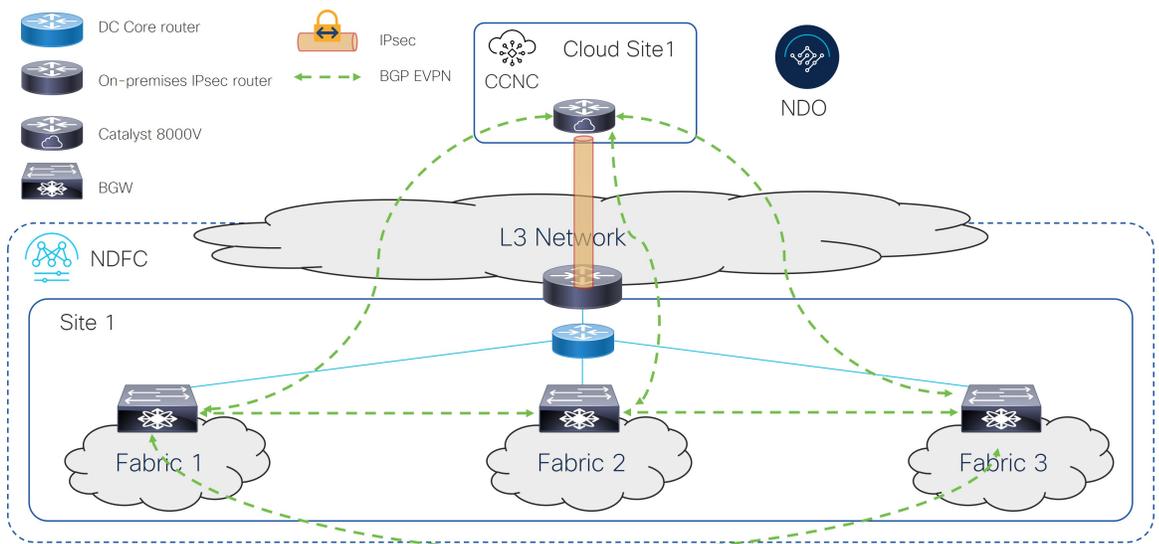


オプション5

次の図は、IPsec を使用してシングルクラウド接続の例を示しています。

- 全てのオンプレミスサイトにあるBGW ノードは、フルメッシュEVPN 隣接関係 (アジャセンシー) を間に確立させます。
- クラウドサイトの Cisco Catalyst 8000V は、オンプレミス サイトのすべてのBGW デバイスとのフルメッシュ BGP EVPN 隣接関係を確立します。
- クラウドサイトへの IPsec 接続は、共有 IPsec ルータのみを介して行われます。

図 9:



## IPsec (マルチクラウド) でサポートされるトポロジ

次の表は、オンプレミス サイトとオンプレミスとクラウドサイトの間で BGP EVPN コントロールプレーンの隣接関係を確立する方法と、オンプレミス サイトと複数のクラウドサイト間のアンダーレイ接続を確立するために IPsec を利用する方法を示しています。



(注) 次の各図は、簡単な例を表示します。実際のシナリオでは、各ロールにデバイスが重複で展開されている可能性があります。

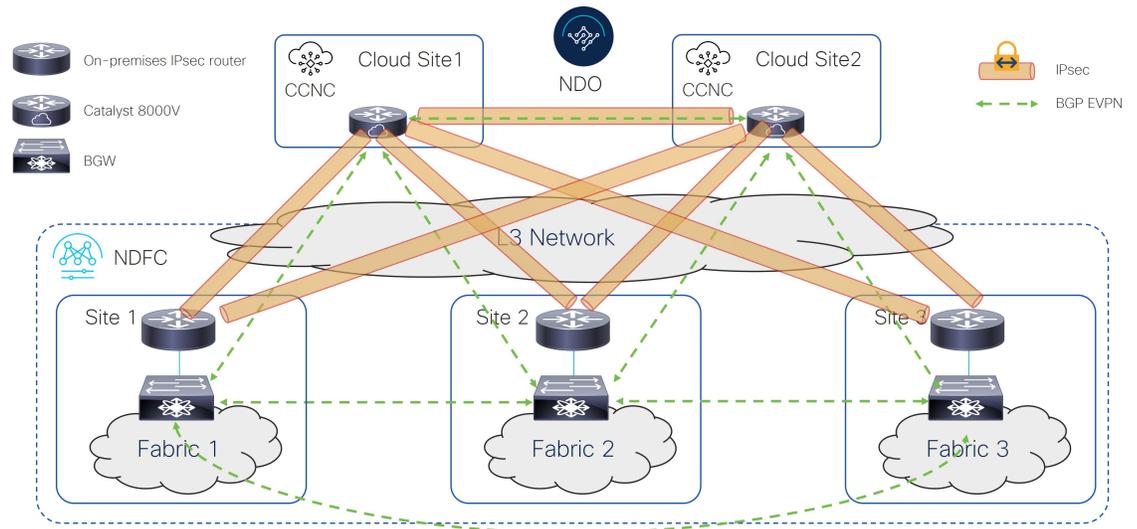
| オンプレミスの間の BGP EVPN | クラウドサイトへの BGP EVPN と IPsec       |                                  |  | クラウドサイト間の BGP EVPN と IPsec |
|--------------------|----------------------------------|----------------------------------|--|----------------------------|
|                    | フルメッシュ                           | バフ サイトのみを通して                     | <ul style="list-style-type: none"> <li>• BGP EVPN からクラウドサイトへ：フルメッシュ</li> <li>• IPsec からクラウドサイトへ：ハブサイト経由のみ</li> </ul> |                            |
| フルメッシュ             | <a href="#">オプション 1 (21 ページ)</a> | <a href="#">オプション 3 (23 ページ)</a> | <a href="#">オプション 5 (24 ページ)</a>   | フルメッシュ                     |
| ルーティングサーバ付き        | <a href="#">オプション 2 (22 ページ)</a> | <a href="#">オプション 4 (23 ページ)</a> | 該当なし   |                            |

### オプション 1

次の図は、IPsec を使用したマルチクラウド接続の例を示しています。

- 全てのオンプレミスサイトにある BGW ノードは、フルメッシュ BGP EVPN 隣接関係 (アジャセンシー) を間に確立させます。
- クラウドサイトの Cisco Catalyst 8000V は、各オンプレミスサイトに展開されたコア ルータと IPsec トンネルを確立し、オンプレミスサイトのすべての BGW デバイスとフルメッシュ EVPN 隣接関係 (アジャセンシー) 全てのを確立します。
- 異なるクラウドサイトの Cisco Catalyst 8000V は、フルメッシュ IPsec トンネルとそれらの間の EVPN 隣接を確立します。

図 10:

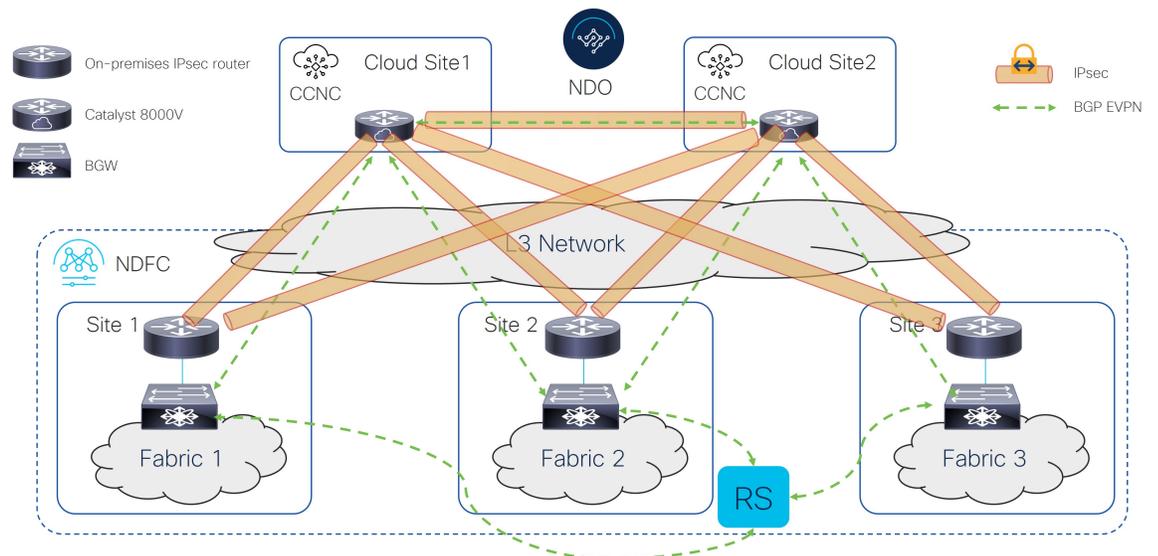


## オプション 2

次の図は、IPsec を使用したマルチクラウド接続の例を示しています。

- BGW ノードは、全てのオンプレミスサイトに EVPN 隣接関係 (アジャセンシー) と一緒にルートサーバーコントロールプレーン ノードを確立します。
- クラウドサイトの Cisco Catalyst 8000V は、各オンプレミスサイトに展開されたコアルータと IPsec トンネルを確立し、オンプレミスサイトのすべての BGW デバイスとフルメッシュ BGP EVPN 隣接関係 (アジャセンシー) 全てのを確立します。
- クラウドルータは、ハブサイトの BGW と BGP EVPN をピアリングします。

図 11:

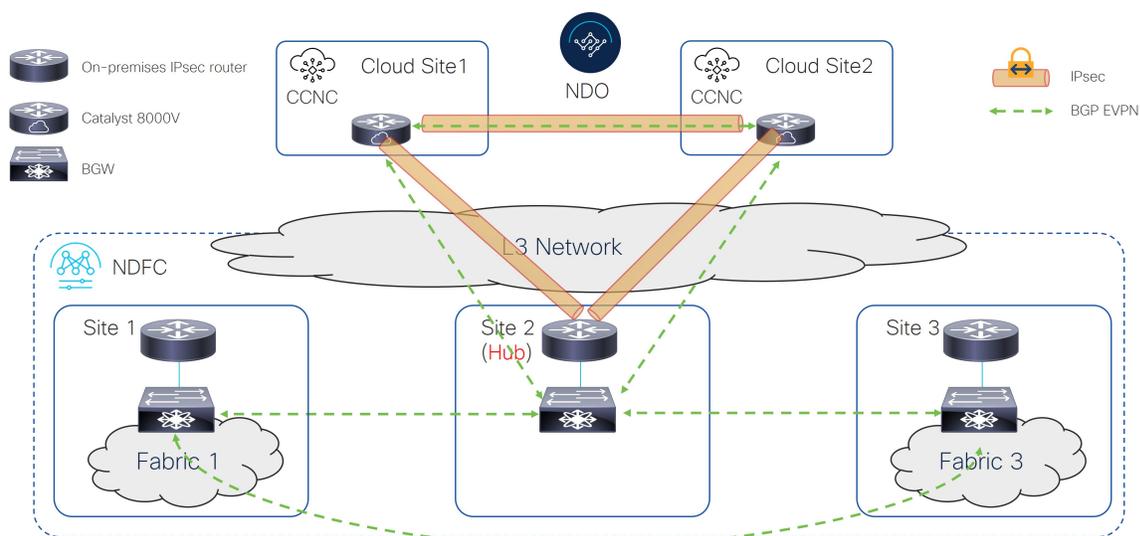


### オプション3

次の図は、IPsecを使用したマルチクラウド接続の例を示しています。

- 全てのオンプレミスサイトにあるBGWノードは、フルメッシュEVPN隣接関係（アジャセンシー）を間に確立させます。
- クラウドサイトのCisco Catalyst 8000Vは、特定のオンプレミスハブサイトに展開されたコアルータとのみIPsecトンネルを確立し、ハブサイトのBGWデバイスとのみEVPN隣接を確立します。
- 異なるクラウドサイトのCisco Catalyst 8000Vは、フルメッシュIPsecトンネルとそれらの間のEVPN隣接を確立します。
- サイト2（Cisco Catalyst 8000VがEVPNに現れる）内で展開されたBGWは、後ろにファブリックを持つことはできません。オンプレミスのとクラウドサイトとの間のプレフィックスの交換のみに使用されています。

図 12:



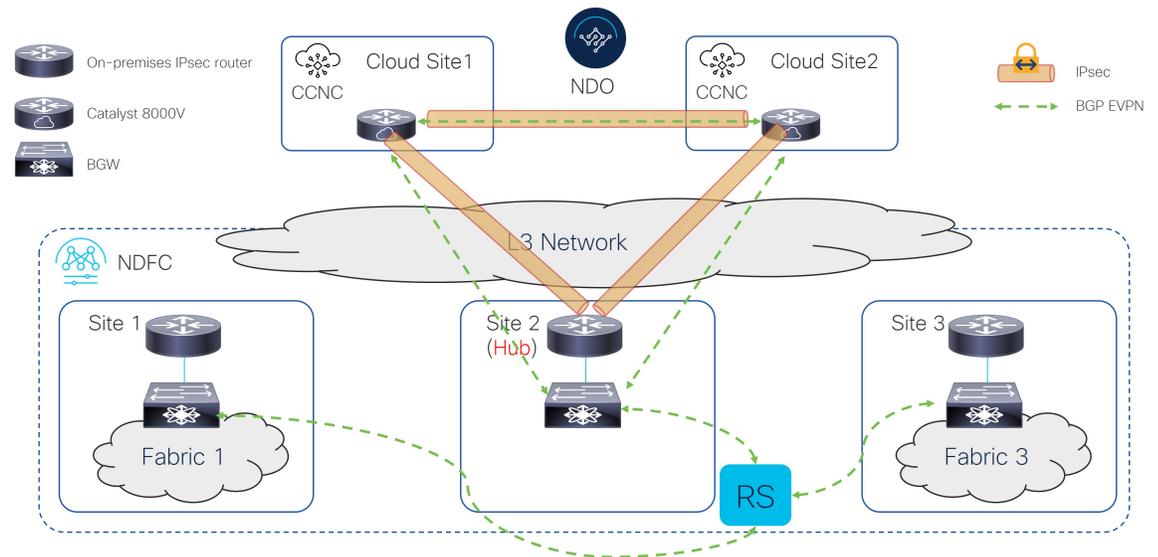
### オプション4

次の図は、IPsecを使用したマルチクラウド接続の例を示しています。

- BGWノードは、全てのオンプレミスサイトにEVPN隣接関係（アジャセンシー）と一緒にルートサーバーコントロールプレーンノードを確立します。
- クラウドサイトのCisco Catalyst 8000Vは、特定のオンプレミスハブサイトに展開されたコアルータとのみIPsecトンネルを確立し、ハブサイトのBGWデバイスとのみBGP EVPN隣接を確立します。
- クラウドルータは、ハブサイトのBGWとBGP EVPNをピアリングします。

- サイト 2 (Cisco Catalyst 8000V が EVPN に現れる) 内で展開された BGW は、後ろにファブリックを持つことはできません。オンプレミスのとクラウドサイトとの間のプレフィックスの交換のみに使用されています。

図 13:

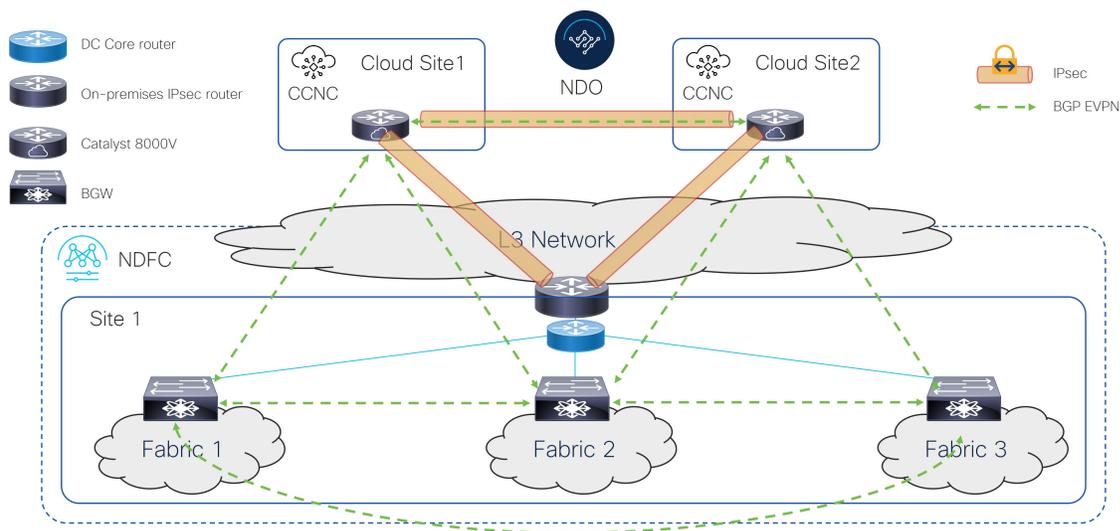


## オプション 5

次の図は、IPsec を使用したマルチクラウド接続の例を示しています。

- 全てのオンプレミスサイトにある BGW ノードは、フルメッシュ EVPN 隣接関係 (アジャセンシー) を間に確立させます。
- クラウドサイトの Cisco Catalyst 8000V は、オンプレミスサイトのすべての BGW デバイスとのフルメッシュ BGP EVPN 隣接関係を確立します。
- クラウドサイトの Cisco Catalyst 8000V は、特定のオンプレミスハブサイトに展開されたコア ルータとのみ IPsec トンネルを確立します。
- 異なるクラウドサイトの Cisco Catalyst 8000V は、フルメッシュ IPsec トンネルとそれらの間の EVPN 隣接を確立します。

図 14:



## IPSec なしてサポートされているトポロジ (シングルクラウド)

次の表は、オンプレミス サイト間またはオンプレミスとクラウドサイト間で BGP EVPN コントロールプレーンの隣接関係 (アジャセンシー) を確立する方法を示しています。

| オンプレミス サイト間の BGP EVPN | クラウドサイトへの BGP EVPN               |                                  |
|-----------------------|----------------------------------|----------------------------------|
|                       | フルメッシュ                           | ハブ サイト経由                         |
| フルメッシュ                | <a href="#">オプション 1 (25 ページ)</a> | <a href="#">オプション 3 (27 ページ)</a> |
| ルーティング サーバ付き          | <a href="#">オプション 2 (26 ページ)</a> | <a href="#">オプション 4 (28 ページ)</a> |



(注) 次の各図は、簡単な例を表示します。実際のシナリオでは、各ロールにデバイスが重複で展開されている可能性があります。

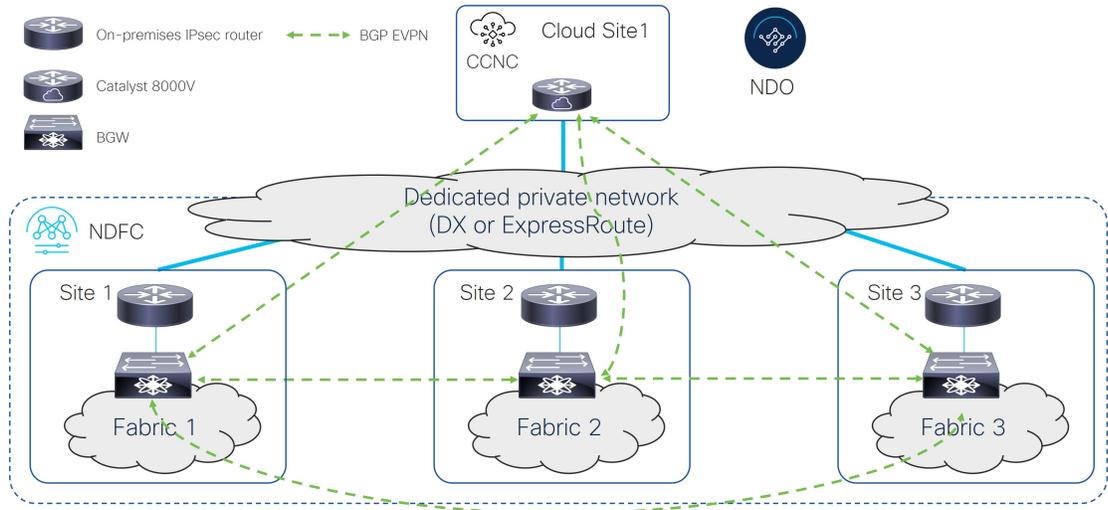
### オプション 1

次の図は、IPsec を使用しないシングルクラウド接続の例を示しています。

- 全てのオンプレミスサイトにある BGW ノードは、フルメッシュ BGP EVPN 隣接関係 (アジャセンシー) を間に確立させます。

- クラウドサイトの Cisco Catalyst 8000V は、オンプレミス サイトのすべての BGW デバイスとのフルメッシュ BGP EVPN 隣接関係を確立します。

図 15:

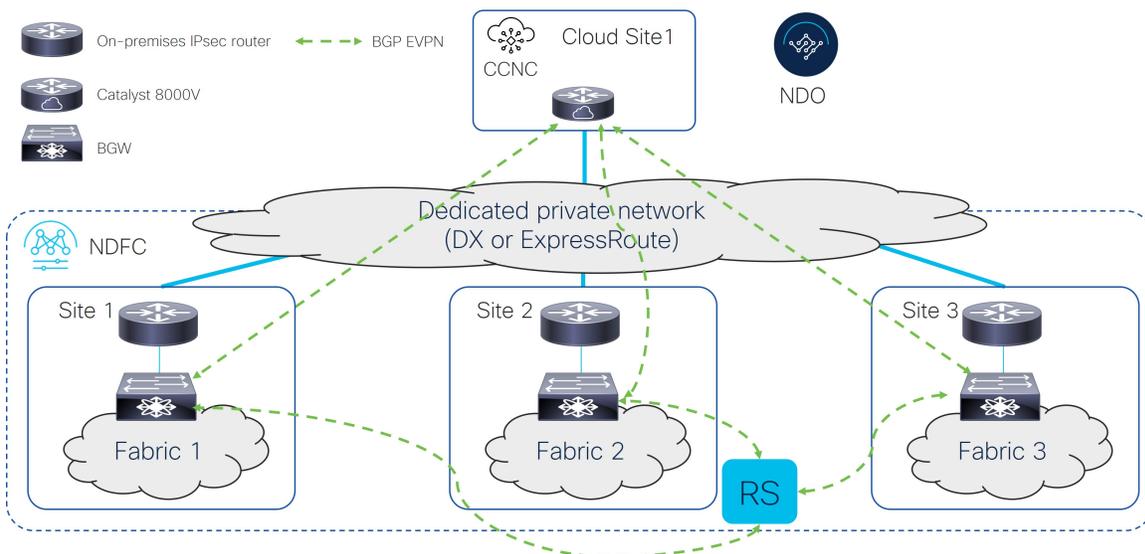


## オプション2

次の図は、IPsec を使用しないシングルクラウド接続の例を示しています。

- BGW ノードは、全てのオンプレミス サイトに EVPN 隣接関係 (アジャセンシー) と一緒にルートサーバー (RS) コントロールプレーン ノードを確立します。
- クラウドサイトの Cisco Catalyst 8000V は、オンプレミス サイトのすべての BGW デバイスとのフルメッシュ BGP EVPN 隣接関係を確立します。

図 16:

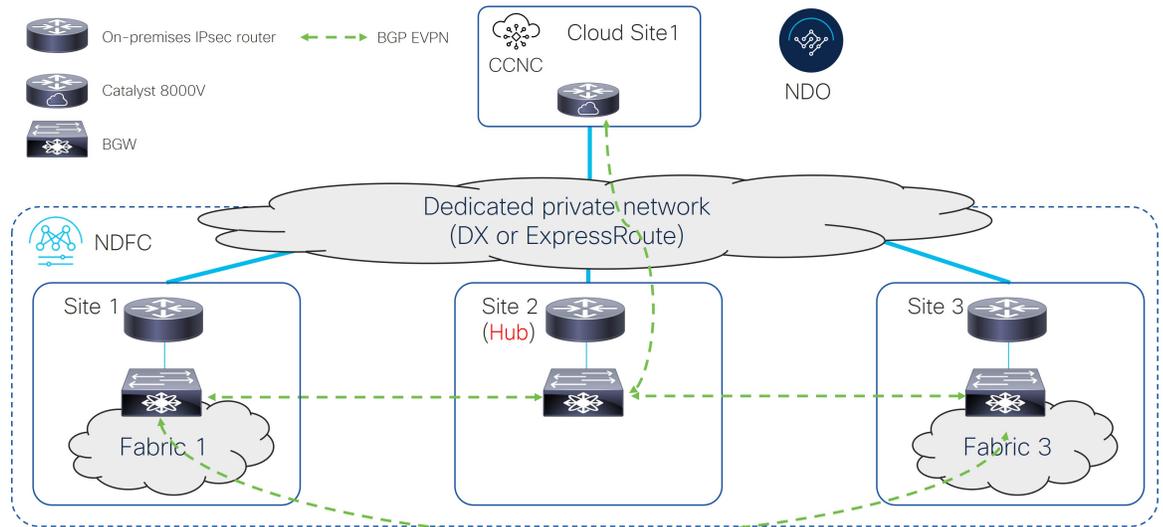


### オプション 3

次の図は、IPsec を使用しないシングルクラウド接続の例を示しています。

- 全てのオンプレミスサイトにある BGW ノードは、フルメッシュ BGP EVPN 隣接関係 (アジャセンシー) を間に確立させます。
- クラウドサイトの Cisco Catalyst 8000V は、ハブサイトの BGW デバイスとだけ BGP EVPN 隣接関係を確立します。
- サイト 2 (Cisco Catalyst 8000V が EVPN に現れる) 内で展開された BGW は、後ろにファブリックを持つことはできません。オンプレミスとクラウドサイトの間でプレフィックスを交換するためにのみ使用されます。

図 17:

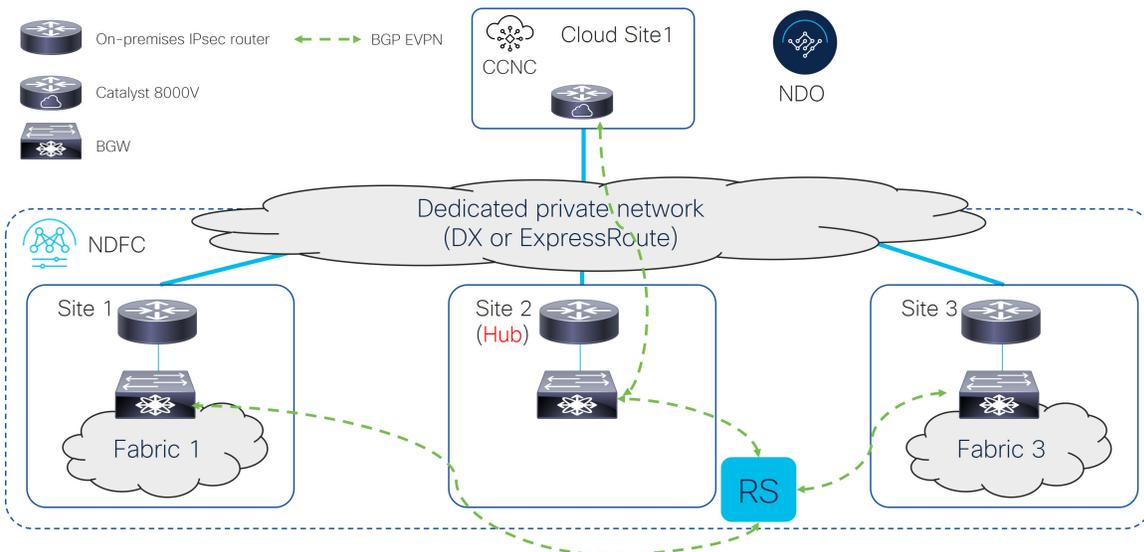


#### オプション4

次の図は、IPsec を使用しないシングルクラウド接続の例を示しています。

- BGW ノードは、全てのオンプレミスサイトに EVPN 隣接関係 (アジャセンシー) と一緒にルートサーバーコントロールプレーンノードを確立します。
- クラウドサイトの Cisco Catalyst 8000V は、ハブサイトの BGW デバイスとだけ BGP EVPN 隣接関係を確立します。
- サイト 2 (Cisco Catalyst 8000V が EVPN に現れる) 内で展開された BGW は、後ろにファブリックを持つことはできません。オンプレミスとクラウドサイトの間でプレフィックスを交換するためのみ使用されます。

図 18:



## IPsec なしでサポートされるトポロジ (マルチクラウド)

次の表は、オンプレミス サイト間またはオンプレミスとクラウドサイト間で BGP EVPN コントロールプレーンの隣接関係 (アジャセンシー) を確立する方法を示しています。

| オンプレミスの間の BGP EVPN | クラウドサイトへの BGP EVPN |                  | クラウドサイト間の BGP EVPN |
|--------------------|--------------------|------------------|--------------------|
|                    | フルメッシュ             | ハブ サイト経由         |                    |
| フルメッシュ             | オプション 1 (29 ページ)   | オプション 3 (31 ページ) | フルメッシュ             |
| ルーティング サーバ         | オプション 2 (30 ページ)   | オプション 4 (32 ページ) |                    |



(注) 次の各図は、簡単な例を表示します。実際のシナリオでは、各ロールにデバイスが重複で展開されている可能性があります。

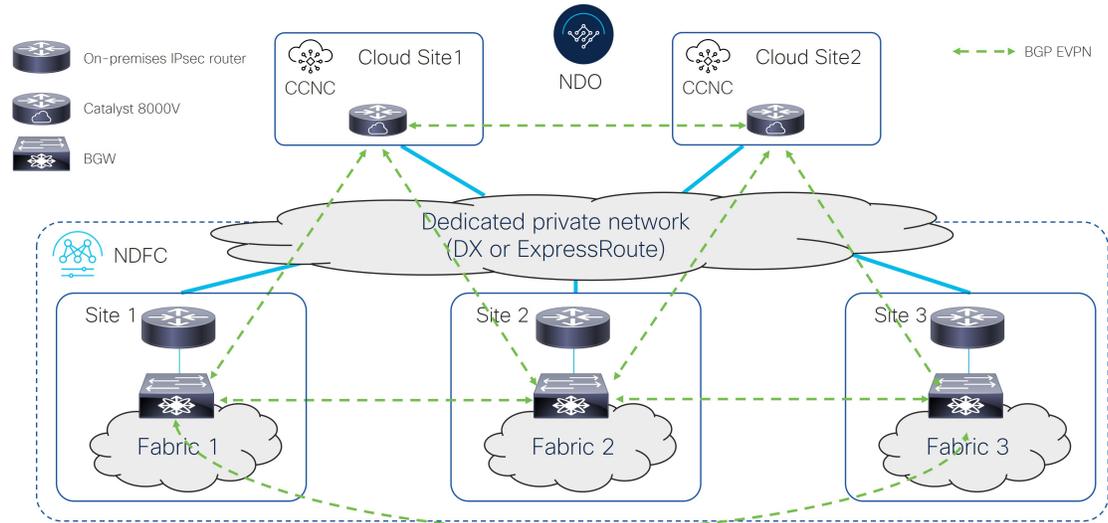
### オプション 1

次の図は、IPsec を使用しないマルチクラウド接続の例を示しています。

- 全てのオンプレミスサイトにある BGW ノードは、フルメッシュ BGP EVPN 隣接関係 (アジャセンシー) を間に確立させます。

- クラウドサイトの Cisco Catalyst 8000V は、オンプレミス サイトのすべての BGW デバイスとのフルメッシュ BGP EVPN 隣接関係 (アジャセンシー) を確立します。
- 異なるクラウドサイトの Cisco Catalyst 8000V は、フルメッシュ BGP とそれらの間の EVPN 隣接を確立します。

図 19:

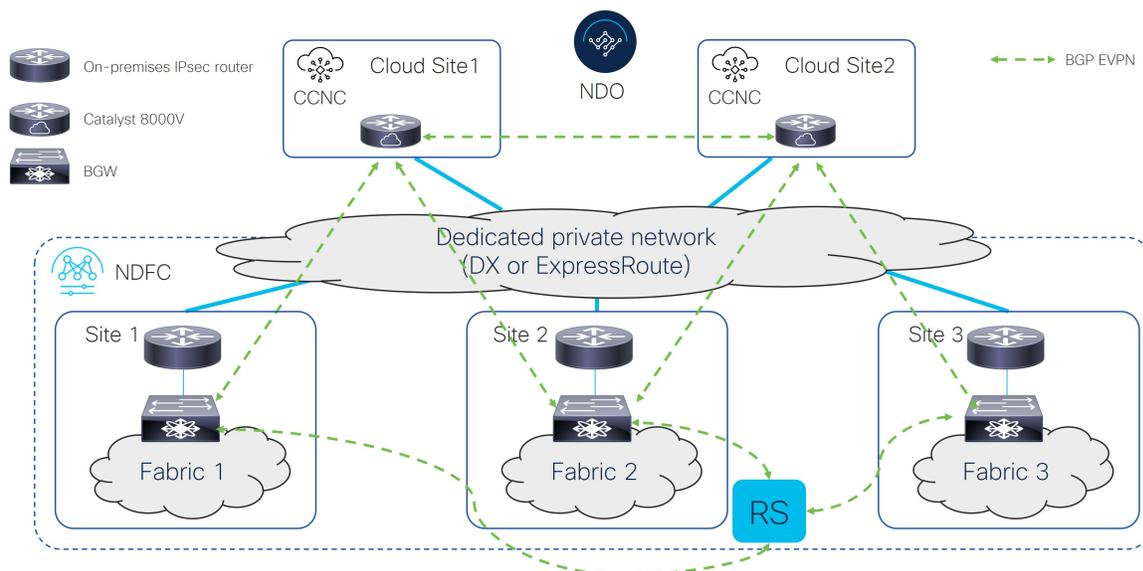


## オプション 2

次の図は、IPsec を使用しないマルチクラウド接続の例を示しています。

- BGW ノードは、全てのオンプレミス サイトに EVPN 隣接関係 (アジャセンシー) と一緒にルートサーバーコントロールプレーン ノードを確立します。
- クラウドサイトの Cisco Catalyst 8000V は、オンプレミス サイトのすべての BGW デバイスとのフルメッシュ BGP EVPN 隣接関係 (アジャセンシー) を確立します。
- 異なるクラウドサイトの Cisco Catalyst 8000V は、フルメッシュ BGP とそれらの間の EVPN 隣接を確立します。

図 20:

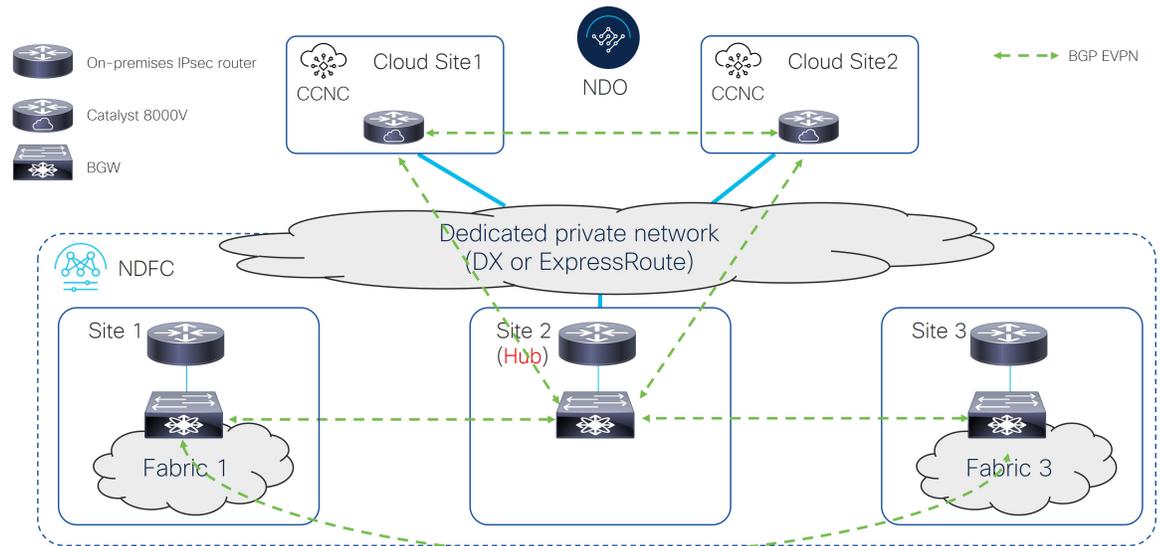


### オプション3

次の図は、IPsec を使用しないマルチクラウド接続の例を示しています。

- 全てのオンプレミスサイトにあるBGWノードは、フルメッシュBGP/EVPN隣接関係（アジャセンシー）を間に確立させます。
- クラウドサイトのCisco Catalyst 8000Vは、ハブサイトのBGWデバイスとだけBGP/EVPN隣接関係（アジャセンシー）を確立します。
- 異なるクラウドサイトのCisco Catalyst 8000Vは、フルメッシュBGPとそれらとの間のEVPN隣接を確立します。
- サイト2（Cisco Catalyst 8000VがEVPNに現れる）内で展開されたBGWは、後ろにファブリックを持つことはできません。オンプレミスのとクラウドサイトとの間のプレフィックスの交換のみに使用されています。

図 21:

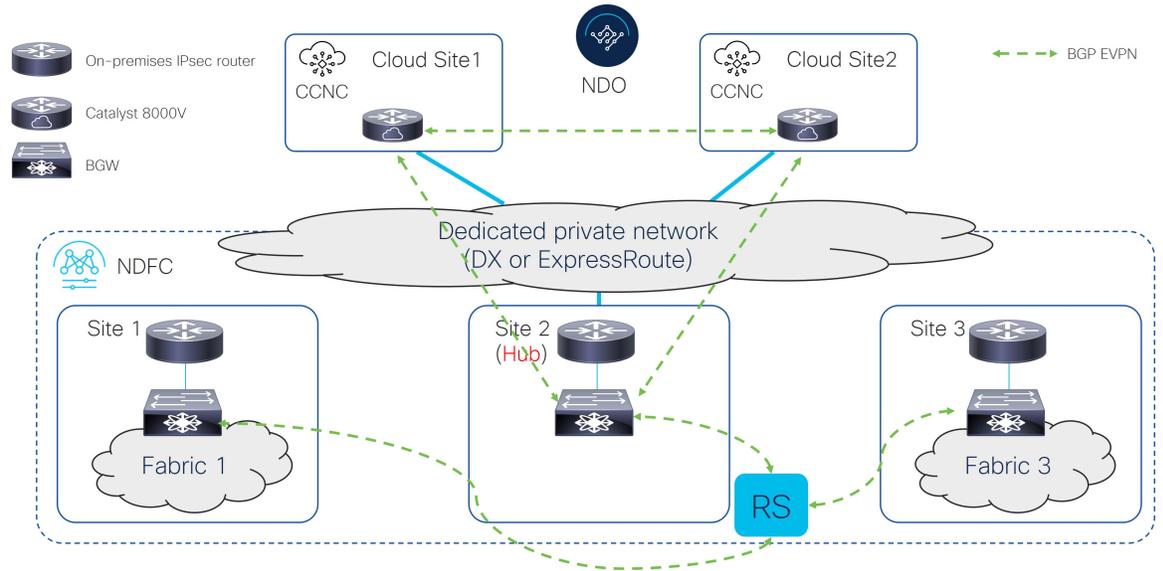


#### オプション4

次の図は、IPsec を使用しないマルチクラウド接続の例を示しています。

- BGW ノードは、全てのオンプレミスサイトに EVPN 隣接関係（アジャセンシー）と一緒にルートサーバーコントロールプレーンノードを確立します。
- クラウドサイトの Cisco Catalyst 8000V は、ハブサイトの BGW デバイスとだけ BGP EVPN 隣接関係（アジャセンシー）を確立します。
- 異なるクラウドサイトの Cisco Catalyst 8000V は、フルメッシュ BGP とそれらとの間の EVPN 隣接を確立します。
- サイト 2（Cisco Catalyst 8000V が EVPN に現れる）内で展開された BGW は、後ろにファブリックを持つことはできません。オンプレミスのとクラウドサイトの間のプレフィックスの交換のみに使用されています。

図 22:







## 第 4 章

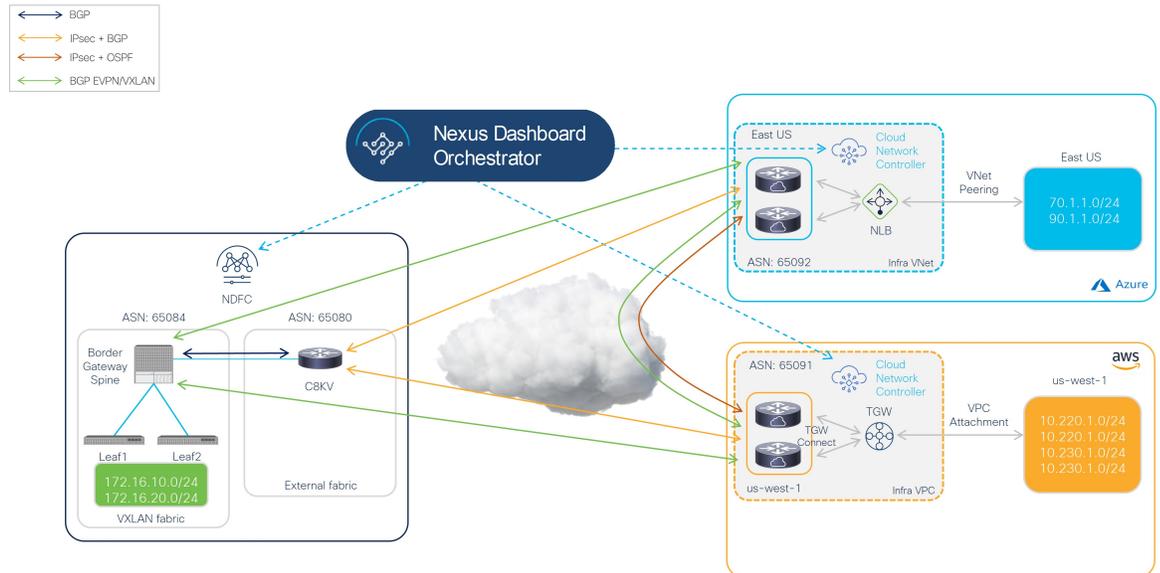
# ハイブリッドクラウドとマルチクラウド 接続展開のインフラ構成を設定する

- 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 (35 ページ)
- オンプレミス NDFC ファブリックを設定 (37 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 (55 ページ)
- NDFC とクラウドサイトを ND と NDO に導入準備する (70 ページ)
- Complete サイト間の接続 NDFC とクラウドサイトの間 (78 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 23:



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（21 ページ）のオプション1（21 ページ）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トール
- 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 :

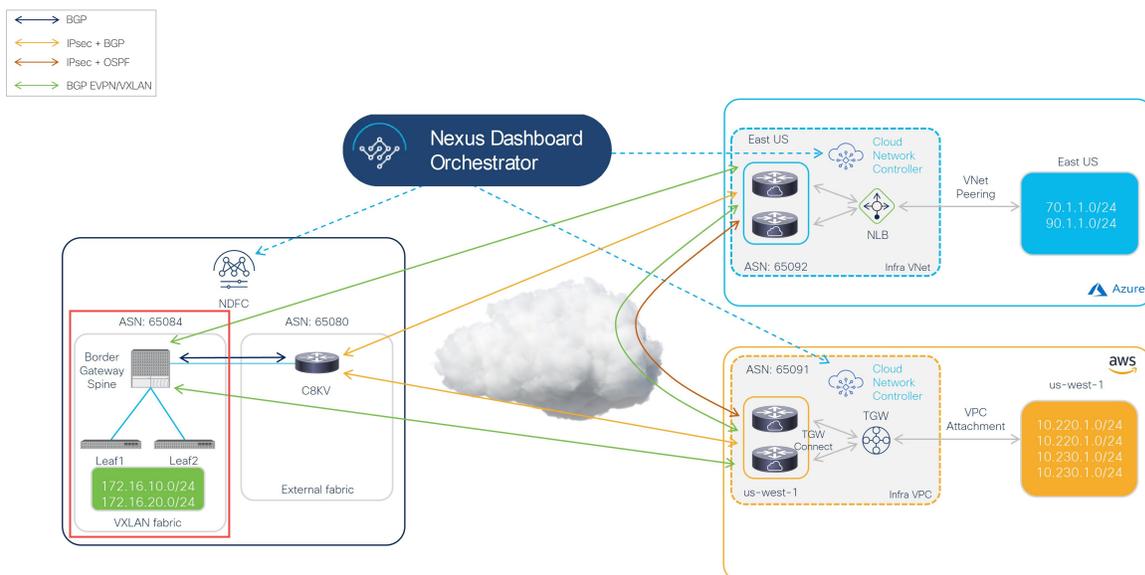
- NDFC VXLAN ファブリック
- NDFC 外部ファブリック

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 24 :



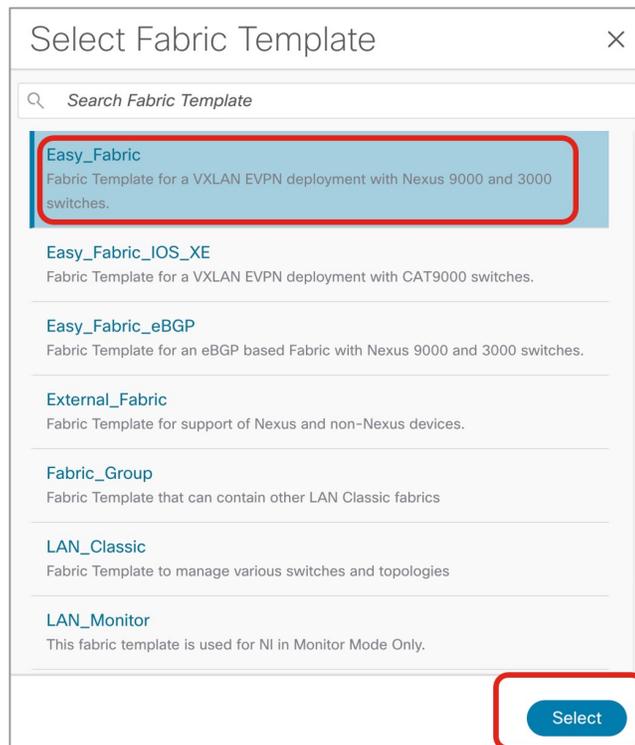
VXLAN ファブリックには、オンプレミスファブリックとクラウドサイト間の VXLAN マルチサイト接続を構築するために使用される 1 つ以上のボーダー ゲートウェイ (BGW) デバイスが含まれている必要があります。

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。
- [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。
  - [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。
  - Easy\_Fabric テンプレートを見つけてクリックします。
  - [選択 (Select)] をクリックします。

図 25:



- 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 26:

The screenshot shows the configuration interface for a VXLAN fabric. The 'Fabric Name' is 'sydney'. The 'Pick Template' dropdown is set to 'Easy\_Fabric'. The 'General Parameters' tab is active, showing the following settings:

- BGP ASN\***: 65084 (Note: 1-4294967295 | 1-65535[0-65535] it is a good practice to have a unique ASN for each Fabric.)
- Enable IPv6 Underlay**:  (Note: If not enabled, IPv4 underlay is used)
- Enable IPv6 Link-Local Address**:  (Note: If not enabled, Spine-Leaf interfaces will use global IPv6 addresses)
- Fabric Interface Numbering\***: p2p (Note: Numbered(Point-to-Point) or Unnumbered)
- Underlay Subnet IP Mask\***: 30 (Note: Mask for Underlay Subnet IP Range)
- Underlay Subnet IPv6 Mask**: Select an Option (Note: Mask for Underlay Subnet IPv6 Range)
- Underlay Routing Protocol\***: ospf (Note: Used for Spine-Leaf Connectivity)
- Route-Reflectors\***: 2 (Note: Number of spines acting as Route-Reflectors)

**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。

## NDFC VXLAN ファブリックを作成

- 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 27:

The screenshot shows the configuration page for a fabric. The 'Advanced' tab is active. On the right side, the 'Anycast Border Gateway advertise-pip' checkbox is checked and highlighted with a red box. Other visible settings include VTEP HoldDown Time (180), Brownfield Overlay Network Name Format (Auto\_Net\_VNI\$VNI\$\$VLAN\$\$VLAN\_ID\$\$), and various other options like 'Enable CDP for Bootstrapped Switch', 'Enable VXLAN OAM', 'Enable Tenant DHCP', 'Enable NX-API', 'Enable NX-API on HTTP port', 'Enable Policy-Based Routing (PBR)', 'Enable Strict Config Compliance', 'Enable AAA IP Authorization', and 'Enable NDFC as Trap Host'.

**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、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 28:

The screenshot shows the configuration page for a VXLAN fabric named 'sydney'. The 'Resources' tab is selected, displaying various IP address ranges for underlay and overlay networks. Red boxes highlight the following fields:

- Underlay Routing Loopback IP Range\*:** 20.2.0.0/22 (Typically Loopback0 IP Address Range)
- Underlay VTEP Loopback IP Range\*:** 20.3.0.0/22 (Typically Loopback1 IP Address Range)
- Underlay RP Loopback IP Range\*:** 20.254.254.0/24 (Anycast or Phantom RP IP Address Range)
- Underlay Subnet IP Range\*:** 20.4.0.0/16 (Address range to assign Numbered and Peer Link SVI IPs)
- VRF Lite Subnet IP Range\*:** 20.33.0.0/16 (Address range to assign P2P Interfabric Connections)

Other visible fields include:

- Layer 2 VXLAN VNI Range\*: 30000-49000 (Overlay Network Identifier Range)
- Layer 3 VXLAN VNI Range\*: 50000-59000 (Overlay VRF Identifier Range)
- Network VLAN Range\*: 2300-2999 (Per Switch Overlay Network VLAN Range)
- VRF VLAN Range\*: 2000-2299 (Per Switch Overlay VRF VLAN Range)
- Subinterface Dot1q Range\*: 2-511 (Per Border Dot1q Range For VRF Lite Connectivity)
- VRF Lite Deployment\*: Manual (VRF Lite Inter-Fabric Connection Deployment Options)
- Auto Deploy Both:  (Whether to auto generate VRF Lite sub-interface and BGP peering configuration)
- VRF Lite Subnet Mask\*: 30 (Min:0, Max:31)
- Service Network VLAN Range\*: 3000-3199 (Per Switch Overlay Service Network VLAN Range)
- Route Map Sequence Number Range\*: 1-65534 (Min:1, Max:65534)

**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 \(41 ページ\)](#) 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 \(38 ページ\)](#) 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ある場合に便利な 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ザー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。

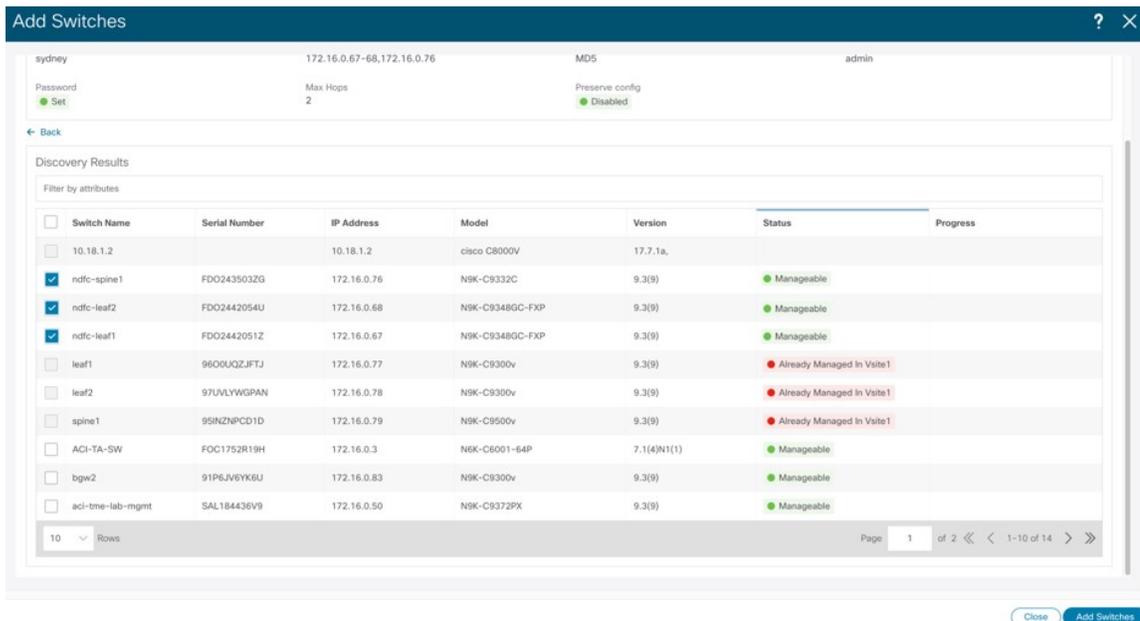
表示される確認ポップアップ ウィンドウで [確認 (Confirm)] をクリックします。

**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 29:



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

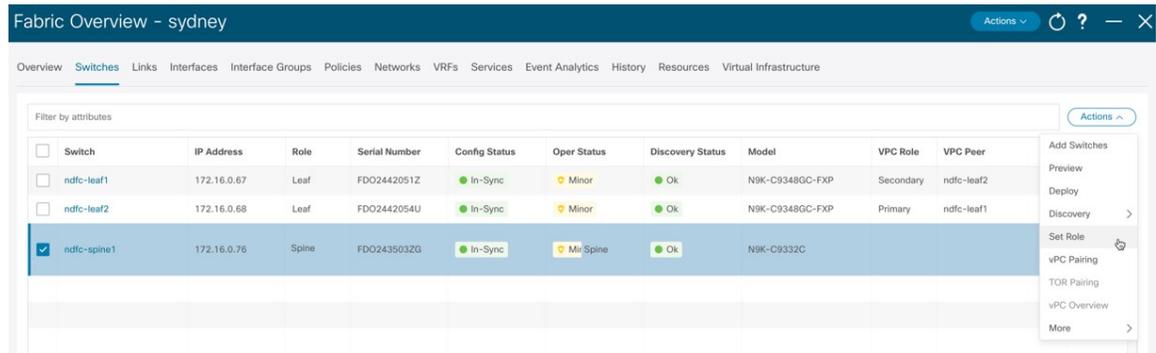
(注) [構成を保持 (Preserve Config)] オプションがオンになっている場合、スイッチは NDFC VXLAN ファブリックに追加された後に再起動します。

**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。

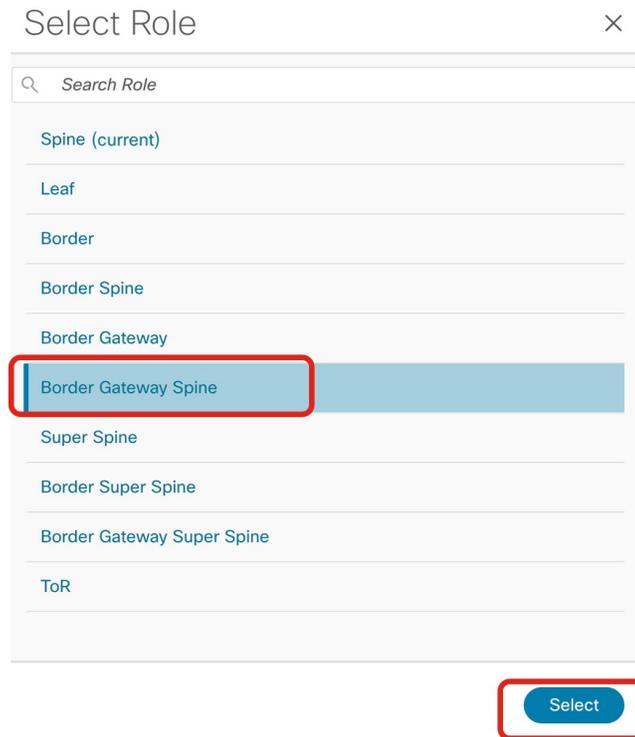
- NDFC VXLAN ファブリック概要ウィンドウの[スイッチ (Switches)] タブをクリックします。このファブリックに追加されたスイッチが表示されます。
- スパインスイッチの横にあるボックスをクリックしてそのスイッチを選択し、[アクション (Actions)] > [役割を設定 (Set Role)] をクリックします。

図 30:



- 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 31:



**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 32:

| Switch      | IP Address  | Role                 | Serial Number | Config Status | Oper Status | Discovery Status | Model           | VPC Role  | VPC Peer   | Mode   |
|-------------|-------------|----------------------|---------------|---------------|-------------|------------------|-----------------|-----------|------------|--------|
| ndfc-leaf1  | 172.16.0.67 | Leaf                 | FDO2442051Z   | In-Sync       | Minor       | Ok               | N9K-C9348GC-FXP | Secondary | ndfc-leaf2 | Normal |
| ndfc-leaf2  | 172.16.0.68 | Leaf                 | FDO2442054U   | In-Sync       | Minor       | Ok               | N9K-C9348GC-FXP | Primary   | ndfc-leaf1 | Normal |
| ndfc-spine1 | 172.16.0.76 | Border Gateway Spine | FDO2435032G   | In-Sync       | Minor       | Ok               | N9K-C9332C      |           |            | Normal |

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 33:

| Switch      | IP Address  | Role                 | Serial Number | Config Status | Oper Status | Discovery Status | Model           | VPC Role  | VPC Peer   | Mode   |
|-------------|-------------|----------------------|---------------|---------------|-------------|------------------|-----------------|-----------|------------|--------|
| ndfc-leaf1  | 172.16.0.67 | Leaf                 | FDO2442051Z   | In-Sync       | Minor       | Ok               | N9K-C9348GC-FXP | Secondary | ndfc-leaf2 | Normal |
| ndfc-leaf2  | 172.16.0.68 | Leaf                 | FDO2442054U   | In-Sync       | Minor       | Ok               | N9K-C9348GC-FXP | Primary   | ndfc-leaf1 | Normal |
| ndfc-spine1 | 172.16.0.76 | Border Gateway Spine | FDO2435032G   | In-Sync       | Minor       | Ok               | N9K-C9332C      |           |            | Normal |

### 次のタスク

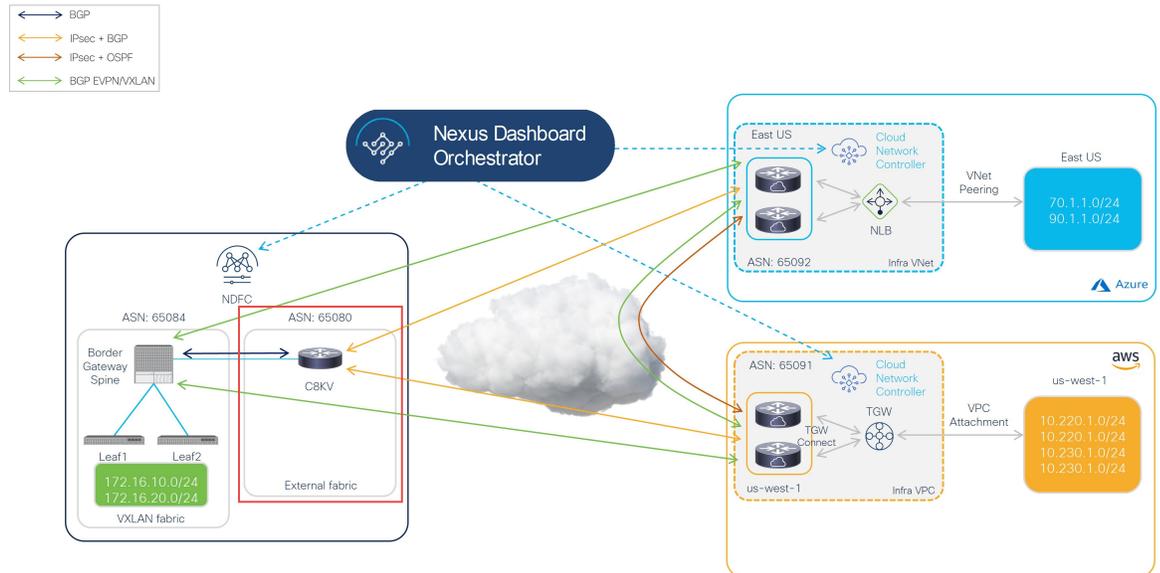
[NDFC 外部ファブリックを構成 \(45 ページ\)](#) で提供されている手順を使用して、NDFC 外部ファブリックを設定します。

## 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。

## NDFC 外部ファブリックを作成

図 34:



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 \(38 ページ\)](#) 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。

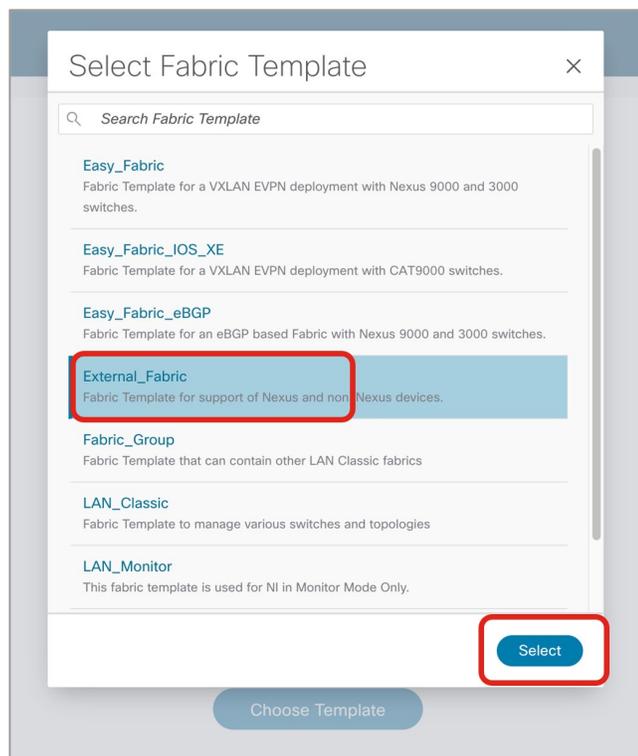
External\_Fabric テンプレートは、Nexus および Catalyst 8000V などの非 Nexus デバイスを使用して従来の LAN ファブリックを構築するために使用されます。

- 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 35:



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 36:

**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)] パラメーター 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 \(49 ページ\)](#) 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 \(46 ページ\)](#) 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。

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

図 37:

The screenshot shows the 'Add Switches' configuration window. The 'Switch Addition Mechanism\*' is set to 'Discover'. The 'Seed Switch Details' section includes the following fields:

- Seed IP\*: 172.16.0.234
- Authentication Protocol\*: MDS
- Device Type\*: IOS-XE
- Device Type radio buttons: CSR/C8000V (selected), ASR, CAT9K
- Username\*: admin
- Password\*: [Redacted]

At the bottom right, there are 'Close' and 'Discover Switches' buttons.

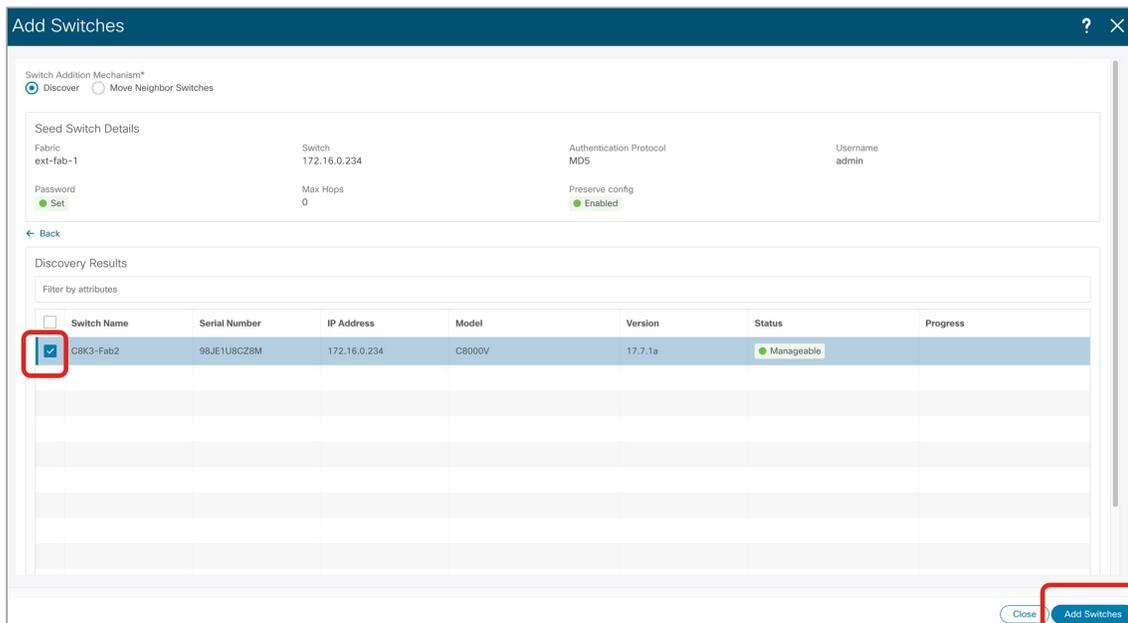
ステップ 4 [スイッチの検出 (Discover Switches)] をクリックします。

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。

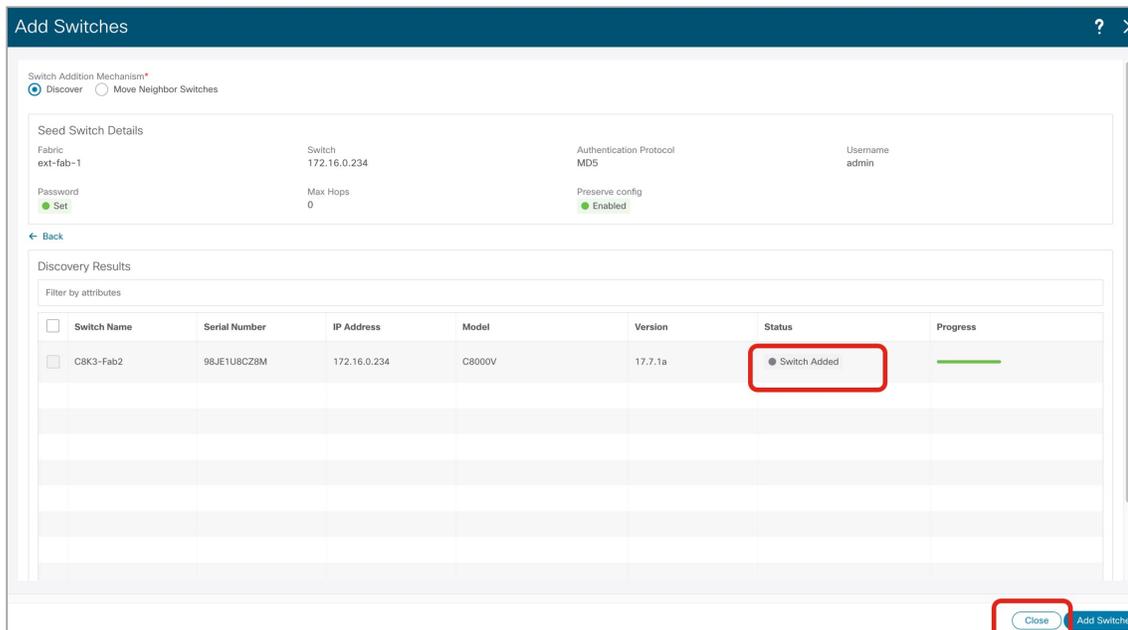
[発見結果 (Discovery Results)] エリアで、Cisco Catalyst 8000V を選択し (Cisco Catalyst 8000V の隣のボックスをクリック)、[スイッチを追加 (Add Switches)] をクリックします。

図 38:



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。

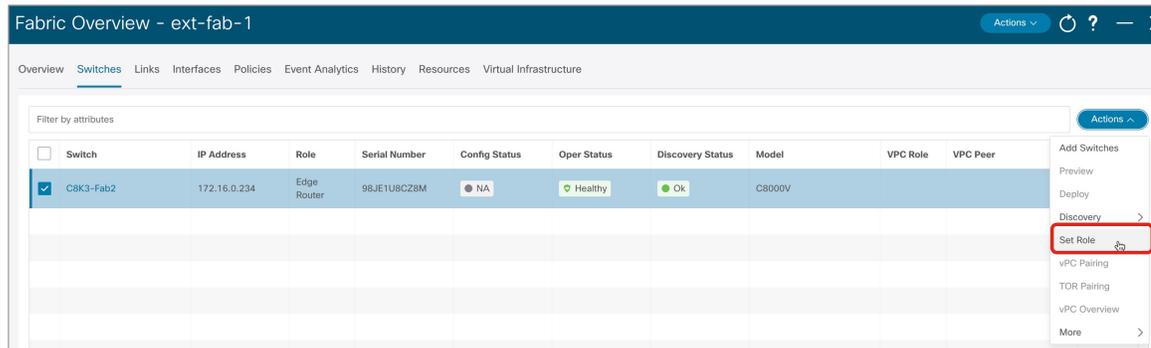
図 39:



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。

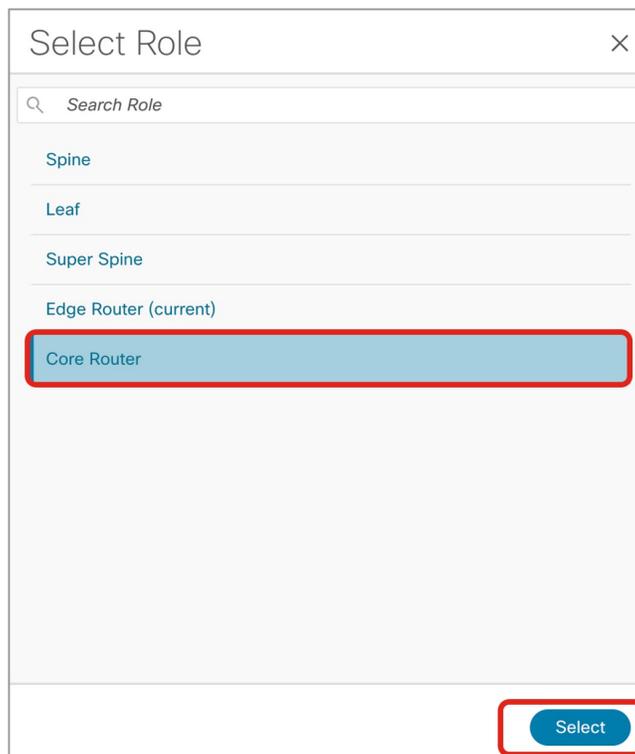
図 40:



- 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 41:



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 42:

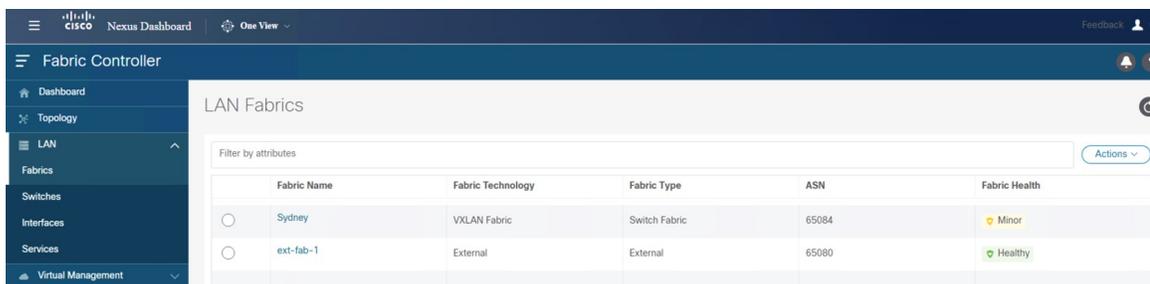


| Switch                             | IP Address   | Role        | Serial Number | Config Status | Oper Status | Discovery Status | Model  | VPC Role | VPC Peer | Mode   |
|------------------------------------|--------------|-------------|---------------|---------------|-------------|------------------|--------|----------|----------|--------|
| <input type="checkbox"/> CBK3-Fab2 | 172.16.0.234 | Core Router | 98JE1UBCZ8M   | NA            | Healthy     | OK               | C8000V |          |          | Normal |

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 43:

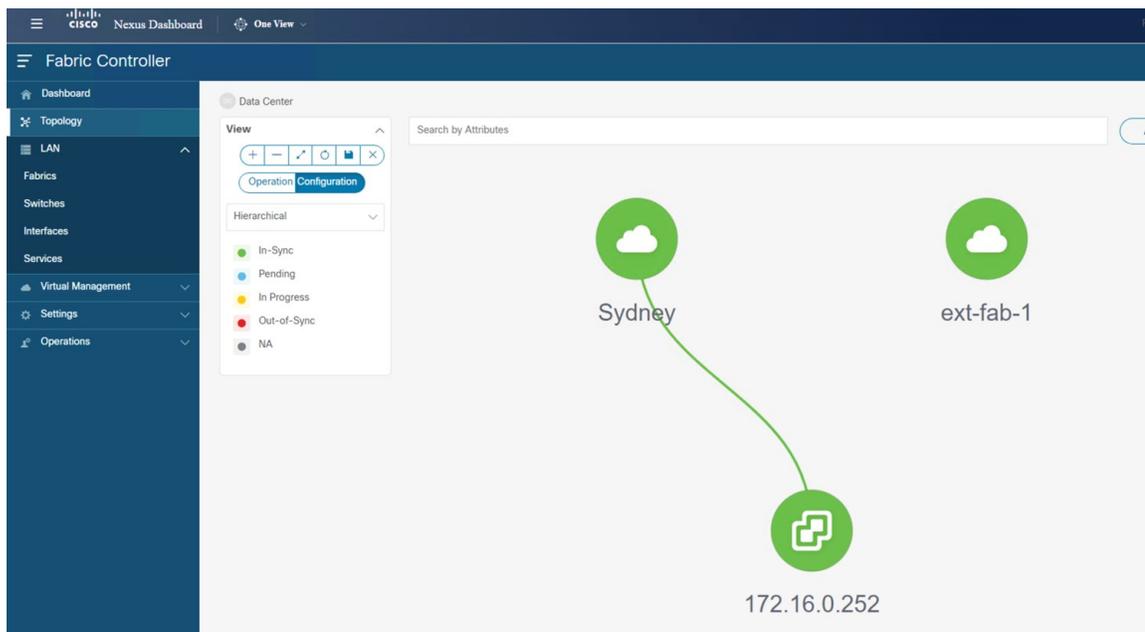


| Fabric Name                     | Fabric Technology | Fabric Type   | ASN   | Fabric Health |
|---------------------------------|-------------------|---------------|-------|---------------|
| <input type="radio"/> Sydney    | VXLAN Fabric      | Switch Fabric | 65084 | Minor         |
| <input type="radio"/> ext-fab-1 | External          | External      | 65080 | Healthy       |

[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：

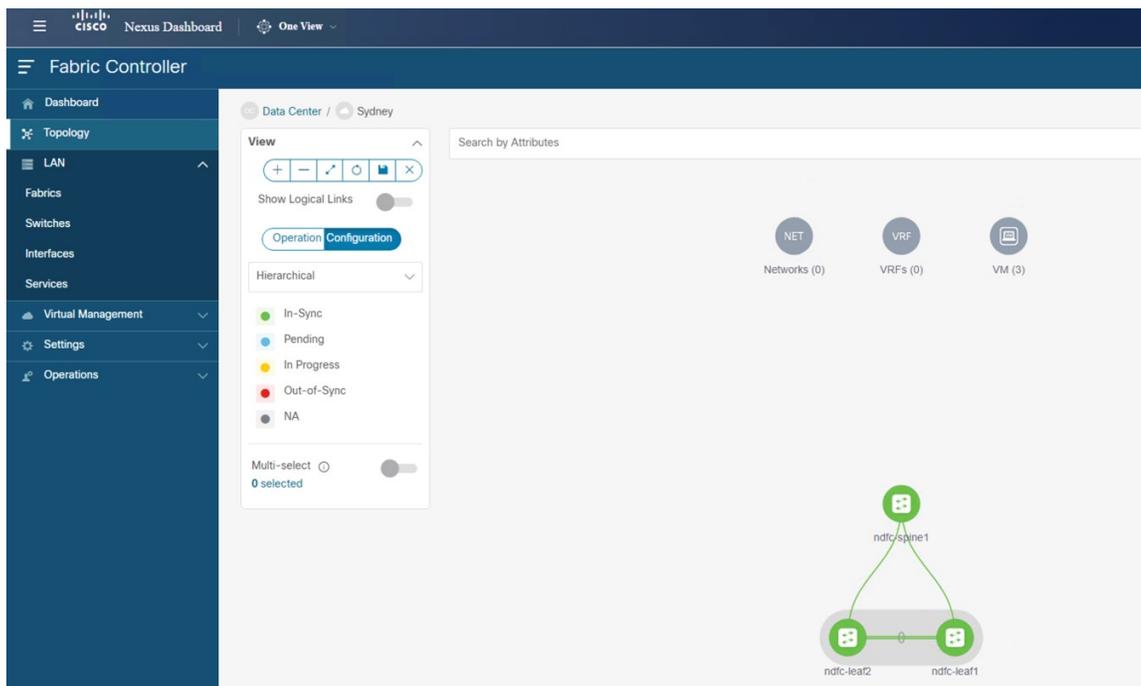
図 44:



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 45:



### 次のタスク

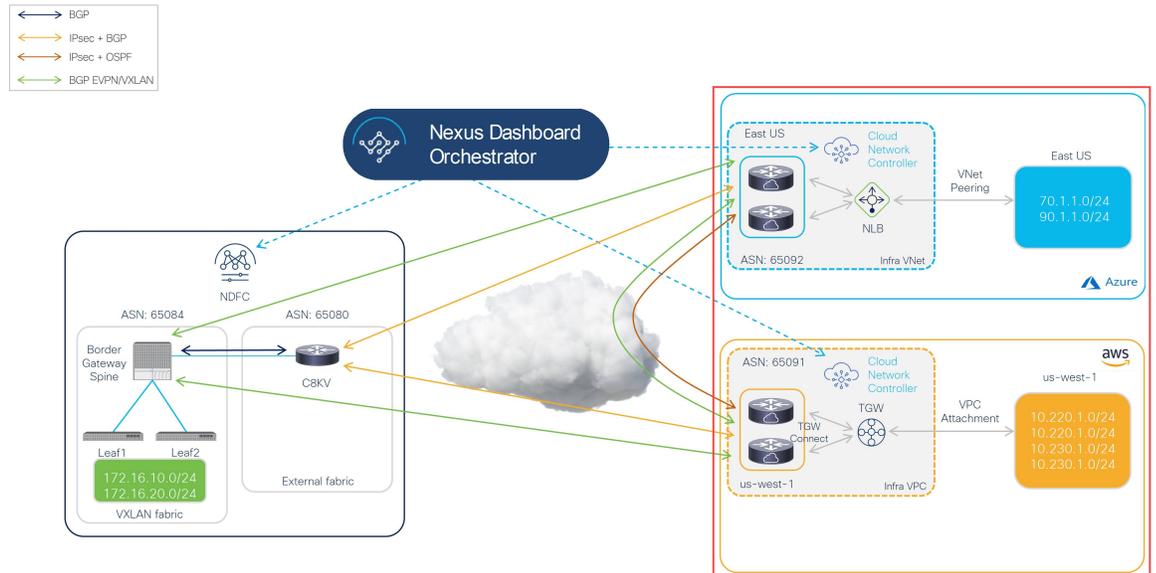
クラウドサイト上のクラウドネットワークコントローラを展開します (55 ページ) で提供されている手順を使用して、クラウドサイトにクラウドネットワークコントローラを展開します。

## 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。

## 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

図 46:



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、[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

## AWS のリージョン管理の必要なパラメータを構成します

- 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 \(58 ページ\)](#) 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、**[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 \(57 ページ\)](#) 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 **[構成の編集 (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ているはずですが、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があります。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。

## AWS のリージョン管理の必要なパラメータを構成します

図 47:

Select the regions to be managed by Cloud Network Controller and which regions should host Cloud Routers. Cloud Routers need to be deployed in at least one region to enable connectivity between VPCs in all managed regions.

Please note that CSR is now changed to Catalyst 8000V.

| Region Name  | Region   | Catalyst 8000Vs          | TGW Stats                           |
|--|--|--------------------------|-------------------------------------|
| <input type="checkbox"/> Africa (Cape Town)          | af-south-1   | <input type="checkbox"/> | <input type="checkbox"/>            |
| <input type="checkbox"/> Asia Pacific (Hong Kong)    | ap-east-1  | <input type="checkbox"/> | <input type="checkbox"/>            |
| <input type="checkbox"/> Asia Pacific (Tokyo)        | ap-northeast-1   | <input type="checkbox"/> | <input type="checkbox"/>            |
| <input type="checkbox"/> Asia Pacific (Seoul)        | ap-northeast-2   | <input type="checkbox"/> | <input type="checkbox"/>            |
| <input type="checkbox"/> Asia Pacific (Osaka-Local)  | ap-northeast-3   | <input type="checkbox"/> | <input type="checkbox"/>            |
| <input type="checkbox"/> Asia Pacific (Mumbai)       | ap-south-1   | <input type="checkbox"/> | <input type="checkbox"/>            |
| <input type="checkbox"/> Asia Pacific (Singapore)    | ap-southeast-1   | <input type="checkbox"/> | <input type="checkbox"/>            |
| <input type="checkbox"/> Asia Pacific (Sydney)       | ap-southeast-2   | <input type="checkbox"/> | <input type="checkbox"/>            |
| <input type="checkbox"/> Asia Pacific (Jakarta)      | ap-southeast-3   | <input type="checkbox"/> | <input type="checkbox"/>            |
| <input type="checkbox"/> Canada (Central)            | ca-central-1   | <input type="checkbox"/> | <input type="checkbox"/>            |
| <input type="checkbox"/> EU (Frankfurt)              | eu-central-1   | <input type="checkbox"/> | <input type="checkbox"/>            |
| <input type="checkbox"/> EU (Stockholm)              | eu-north-1   | <input type="checkbox"/> | <input type="checkbox"/>            |
| <input type="checkbox"/> Europe (Milan)              | eu-south-1   | <input type="checkbox"/> | <input type="checkbox"/>            |
| <input type="checkbox"/> EU (Ireland)                | eu-west-1  | <input type="checkbox"/> | <input type="checkbox"/>            |
| <input type="checkbox"/> EU (London)                 | eu-west-2  | <input type="checkbox"/> | <input type="checkbox"/>            |
| <input type="checkbox"/> EU (Paris)                  | eu-west-3  | <input type="checkbox"/> | <input type="checkbox"/>            |
| <input type="checkbox"/> Middle East (Bahrain)       | me-south-1   | <input type="checkbox"/> | <input type="checkbox"/>            |
| <input type="checkbox"/> South America (Sao Paulo)   | sa-east-1  | <input type="checkbox"/> | <input type="checkbox"/>            |
| <input type="checkbox"/> US East (N. Virginia)       | us-east-1  | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| <input type="checkbox"/> US East (Ohio)              | us-east-2  | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| <input type="checkbox"/> US West (N. California)     | us-west-1  | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> US West (Oregon) | us-west-2 <small>Cloud Network Controller Deployed</small> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

Back to Overview Previous Next Save and Continue

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 ~ 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 ネットを使用した 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。

- [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。
- 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 48:



The image shows a configuration window titled "CIDR". It contains two main input areas: "Region" and "CIDR". The "Region" field has a dropdown menu with a "Select Region >" button. The "CIDR" field is an empty text box with a checkmark icon and an "X" icon to its right.

- 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。
- 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 49:

The screenshot shows the 'Add Hub Network' configuration interface. Key elements include:

- Name:** hub1
- BGP Autonomous System Number:** 65091
- TGW Connect:**  Enable
- Warning:** Changing the use of TGW Connect will cause temporary traffic loss.
- CIDR Table:**

| Region           | CIDR           |
|------------------|----------------|
| US West (Oregon) | 176.16.11.0/24 |
- TGW Route Table Association Labels:** Section with an 'Add TGW Route Table Association Label' button.
- Buttons:** '+ Add CIDR', '+ Add TGW Route Table Association Label', and 'Add'.

**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 \(63 ページ\)](#) 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、[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 \(56 ページ\)](#) 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 \(65 ページ\)](#) 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、[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 \(63 ページ\)](#) の手順を実行します。

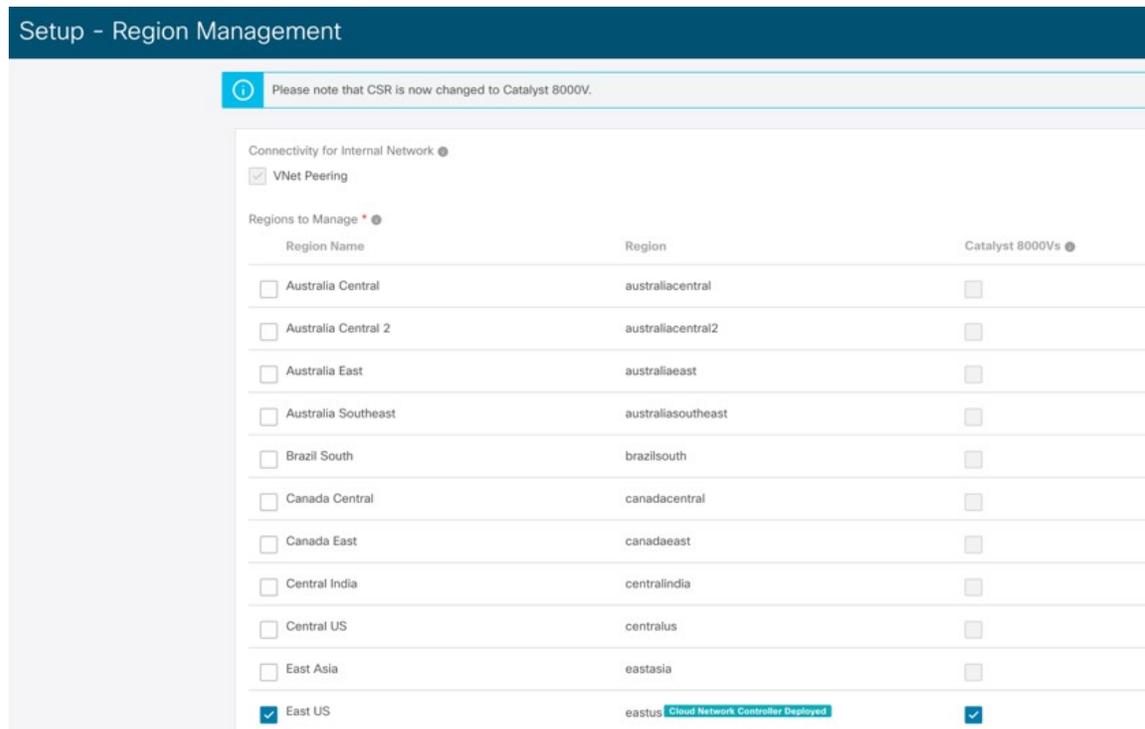
- 
- ステップ 1** [リージョン管理 (Region Management)] エリアを探して適切なボタンをクリックします。
- クラウド ネットワーク コントローラを初めてセットアップする場合は [開始 (Begin)] をクリックし、以前にこのクラウド ネットワーク コントローラでリージョン管理を既に構成している場合は [構成の編集 (Edit Configuration)] をクリックします。
- ステップ 2** [内部ネットワークの接続 (Connectivity for Internal Network)] エリア内の [仮想ネットワーク ピアリング (Virtual Network 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 50:



**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 Azure 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 2~4 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 5~8 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 51:

Setup - Region Management

External Cloud Network Controller, External Router, On-Premises ACI Site, Inter-Site Connectivity, Catalyst 8000V

Configure the fabric infra connectivity for the Cloud Site. The Fabric Autonomous System Number is used for BGP peering inside the configuration template used for the Cloud Routers in the Cloud Site.

Please note that CSR is now changed to Catalyst 8000V.

General

| Subnet *     | Regions | Created By      |
|--------------|---------|-----------------|
| 10.90.0.0/24 |         | System Internal |
| 10.90.1.0/24 |         | User            |

+ Add Subnet Pool for Cloud Routers

**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 1-65534 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 52:

Setup - Region Management

Catalyst 8000Vs

BGP Autonomous System Number for CBKVs \* ●  
65092

Assign Public IP to CBKV Interface ●  
 Enable

Changing CBKV connectivity from private to public (or vice versa) may cause disruption in your network.

Number of Routers Per Region  
2

Username \*  
cisco

Password  
[Redacted]

Confirm Password  
[Redacted]

Please ensure that the license account has licenses corresponding to the Router's throughput entered below.

Pricing Type \*  
BYOL

Throughput of the routers ●  
Tier1 (up to 100M throughput)

TCP MSS \* ●  
1300

License Token ●

Back to Overview Previous **Next**

ステップ 10 [次へ (Next)] 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 Azure 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 (70 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

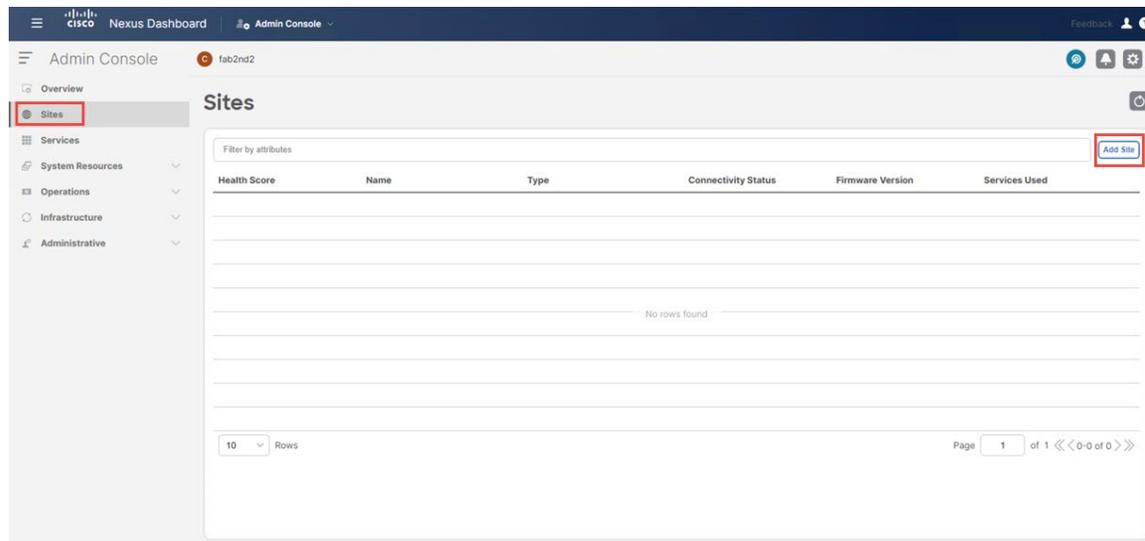
## 始める前に

- [NDFC VXLAN ファブリックを作成 \(38 ページ\)](#) 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 \(46 ページ\)](#) 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 \(56 ページ\)](#) 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 \(63 ページ\)](#) 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 53:



[サイトの追加 (Add Site)] ページが表示されます。

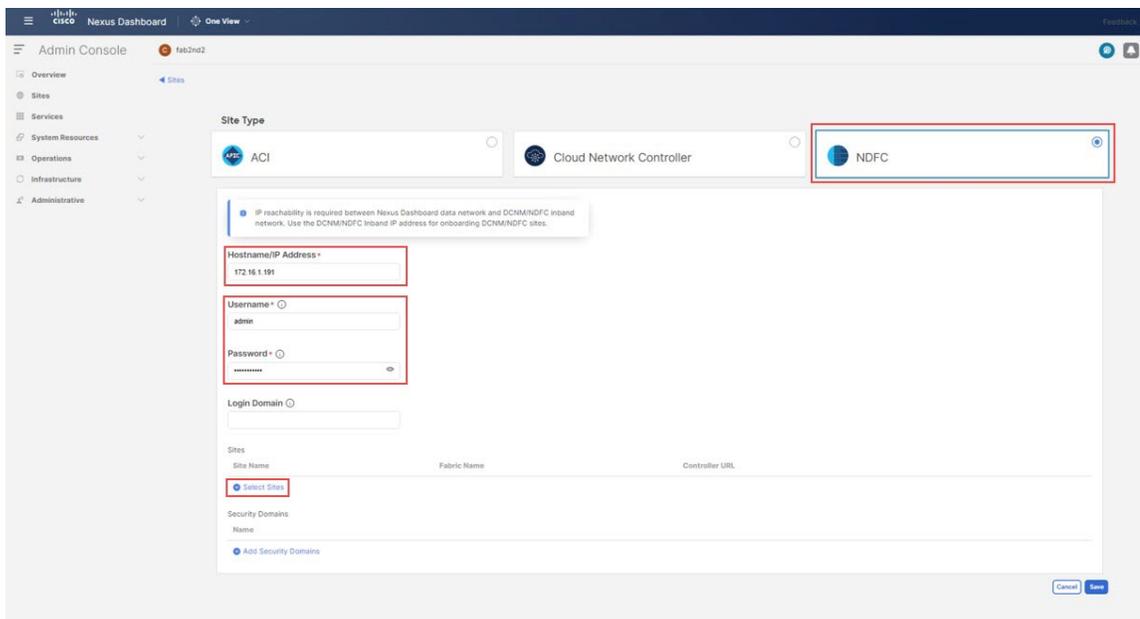
**ステップ 3** [サイトの追加 (Add Site)] ページの [NDFC] ボックスをクリックします。

**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。

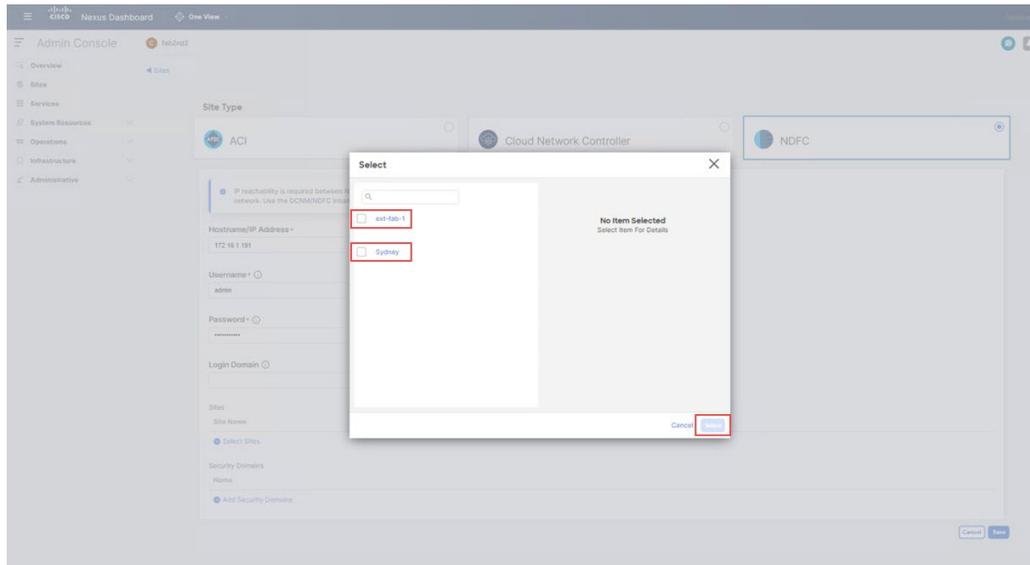
図 54:



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。

## NDFC とクラウドサイトを ND と NDO に導入準備する

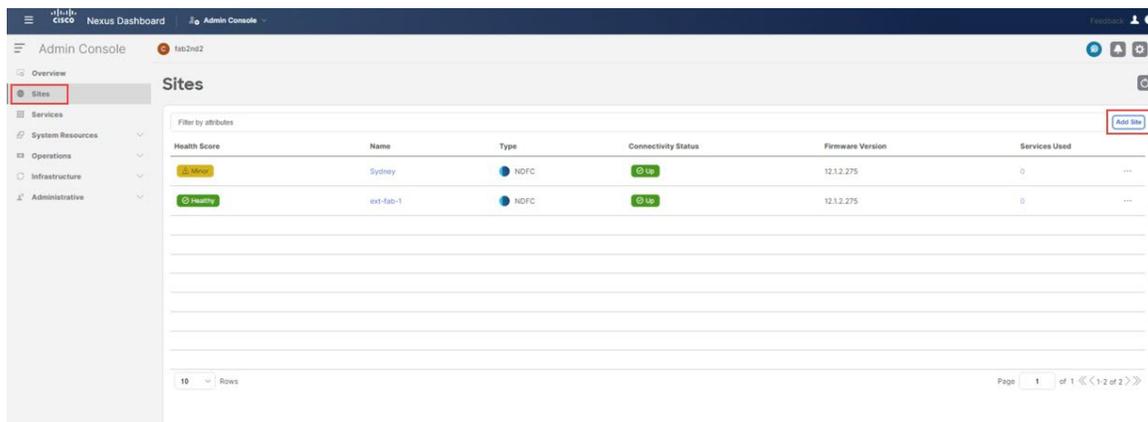
図 55:



[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 56:

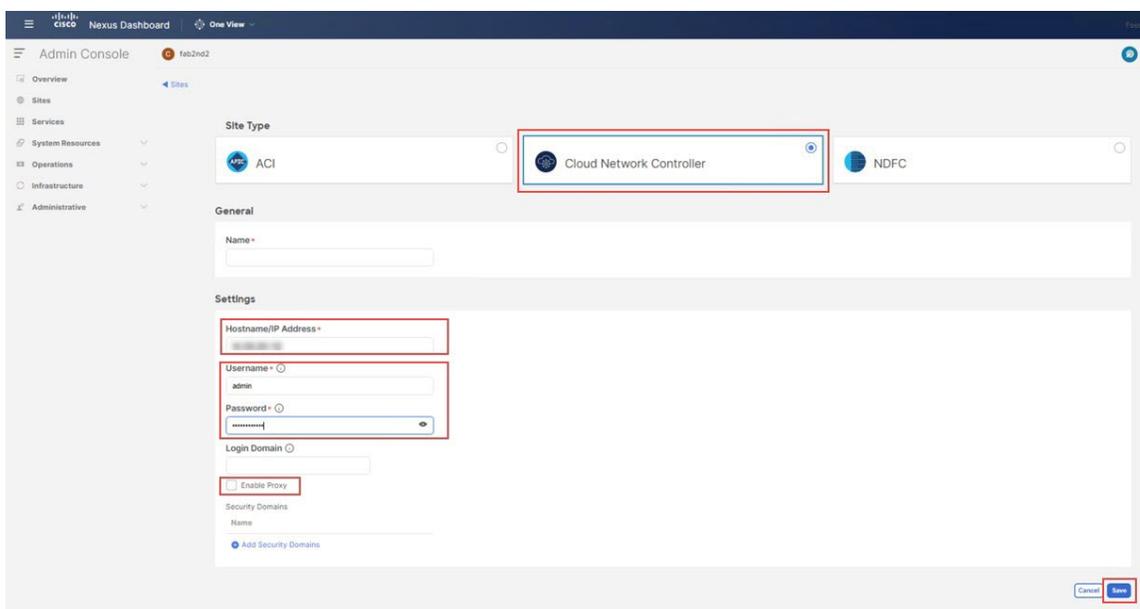


[サイトの追加 (Add Site)] ページが表示されます。

- 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。

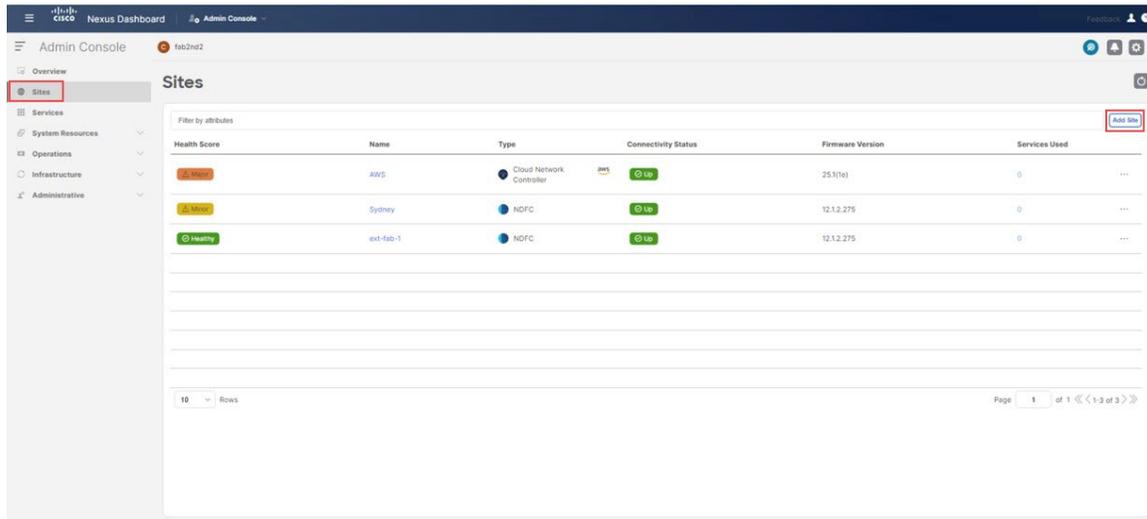
図 57:



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 58:

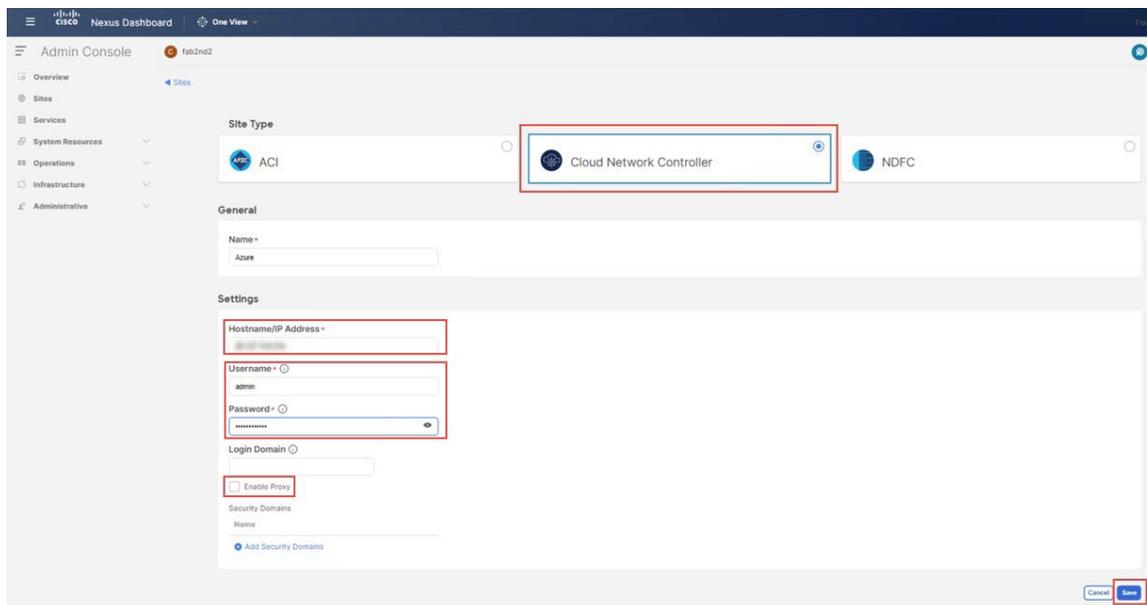


[サイトの追加 (Add Site)] ページが表示されます。

**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。

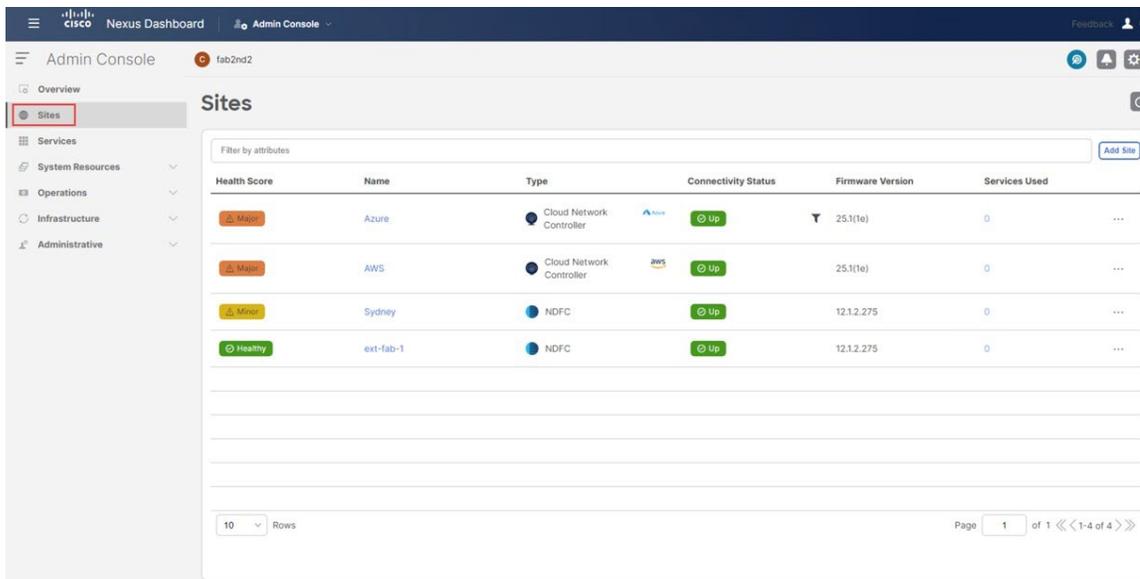
図 59:



**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)

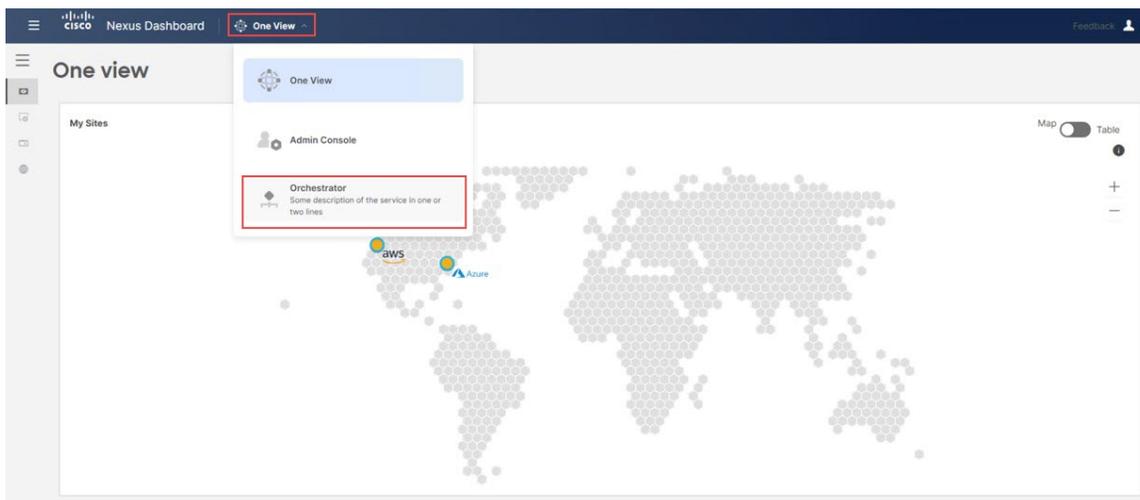
図 60:



**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 61:

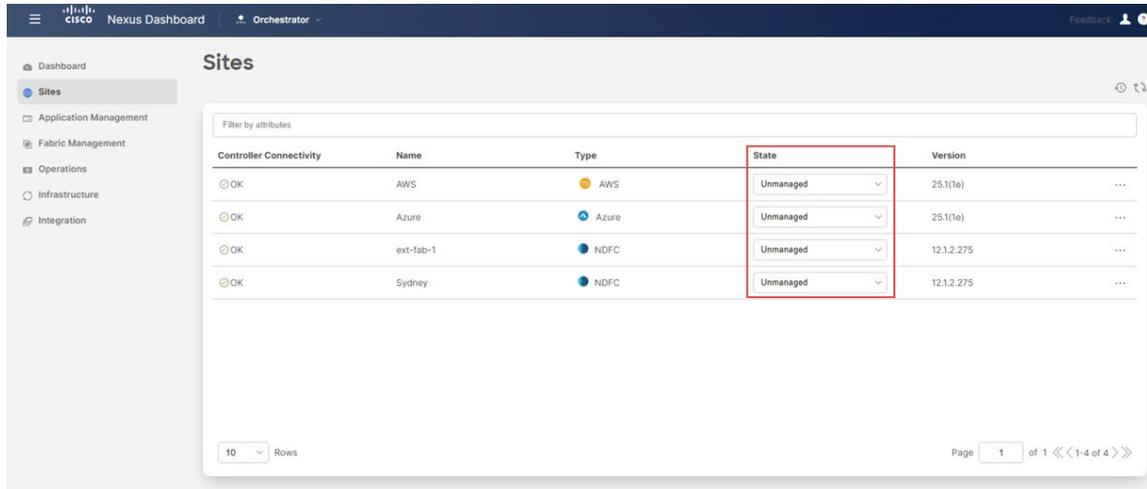


## NDFC とクラウドサイトを ND と NDO に導入準備する

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 62:

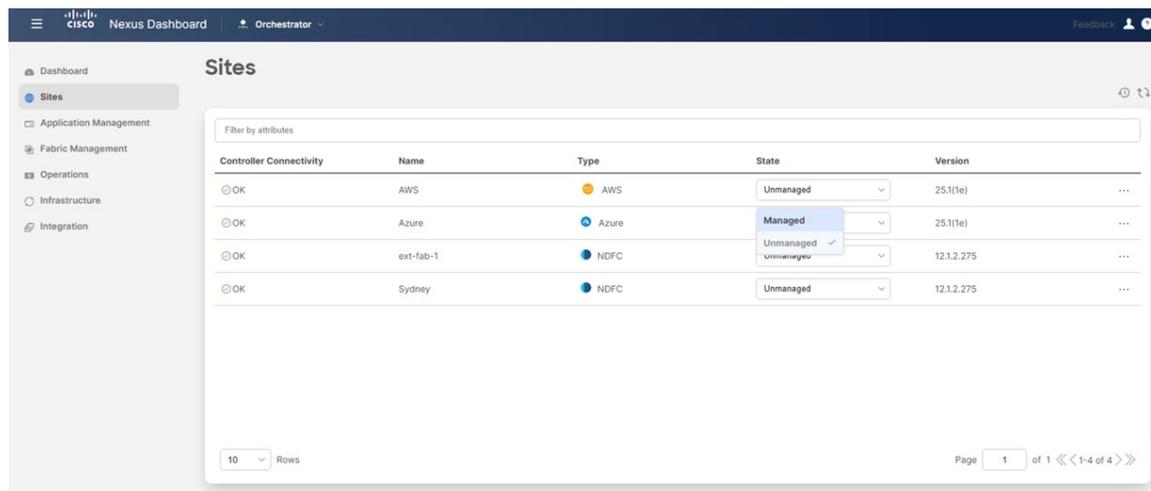


ステップ 16 NDO から、4 つのサイトを管理します。

NDO の各サイトに対して次の手順を実行します。

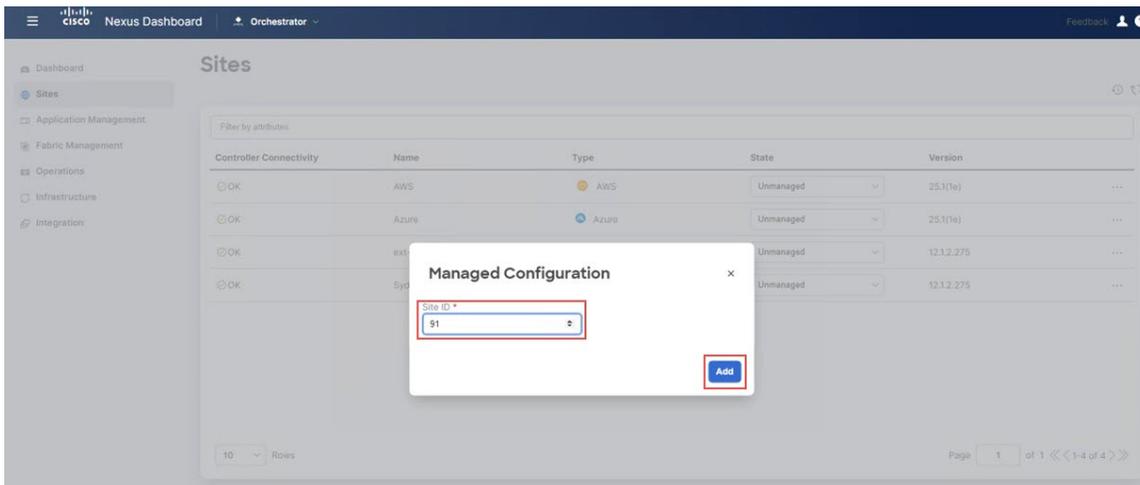
- NDO にリストされている最初のサイトの [状態 (State)] 列で、状態を [管理対象外 (Unmanaged)] から [管理対象 (Managed)] に変更します。

図 63:



- 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。

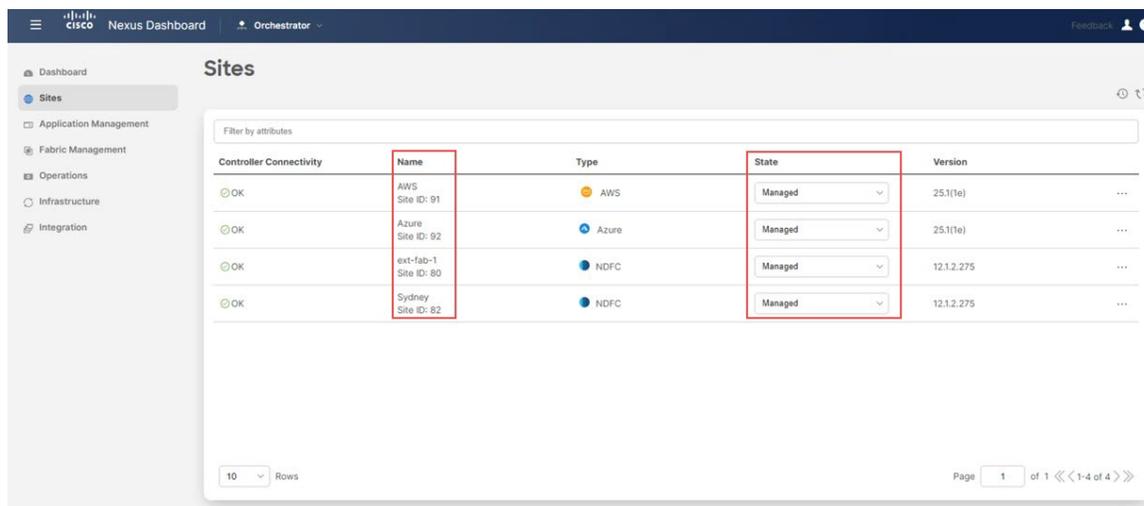
図 64:



- 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 65:



### 次のタスク

[Complete](#) サイト間の接続 NDFC とクラウドサイトの間 (78 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。

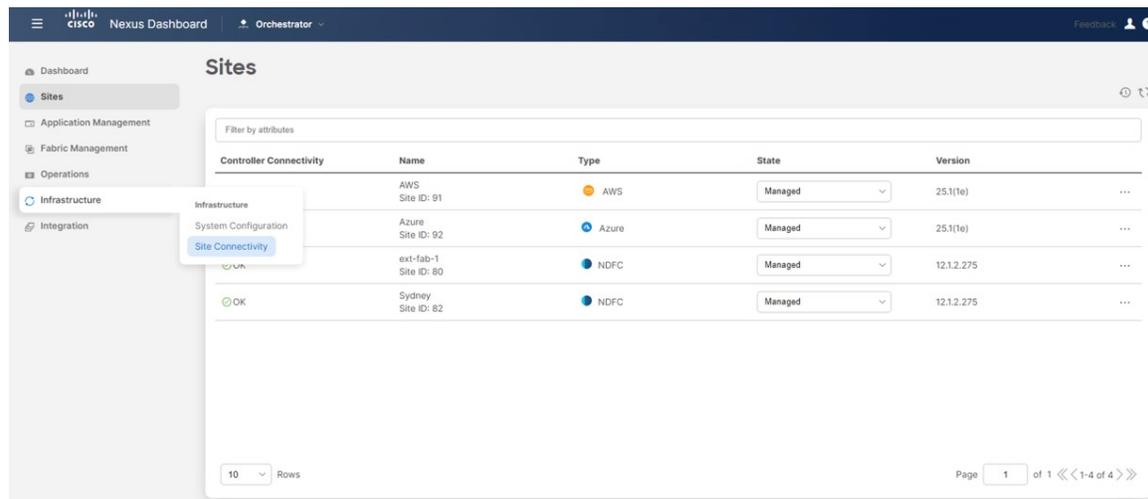
## 必要なコントロールプレーン構成を完了する

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 (70 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。

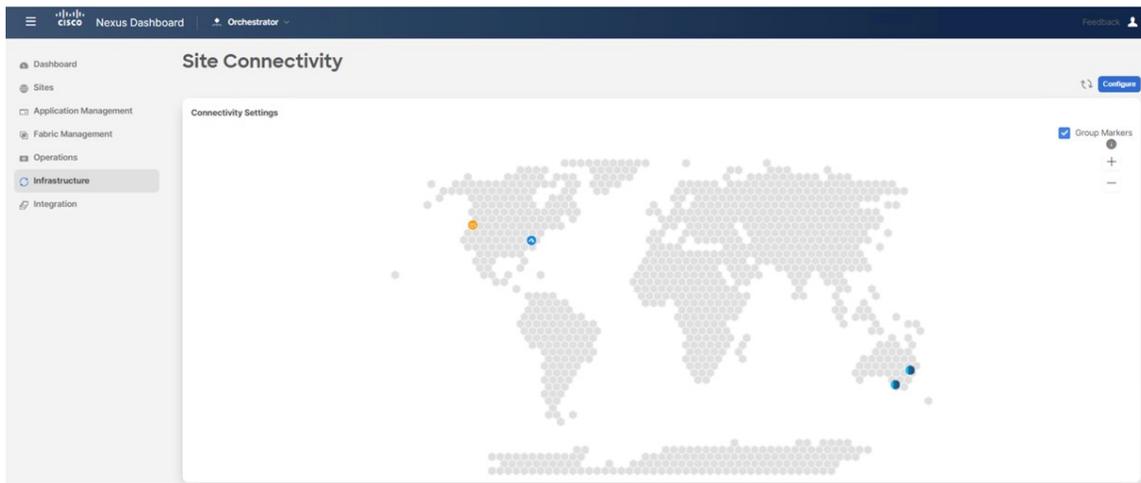
**ステップ 1** NDO 内で、[インフラストラクチャ (Infrastructure)] > [サイト接続 (Site Connectivity)] に移動します。

図 66:



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。

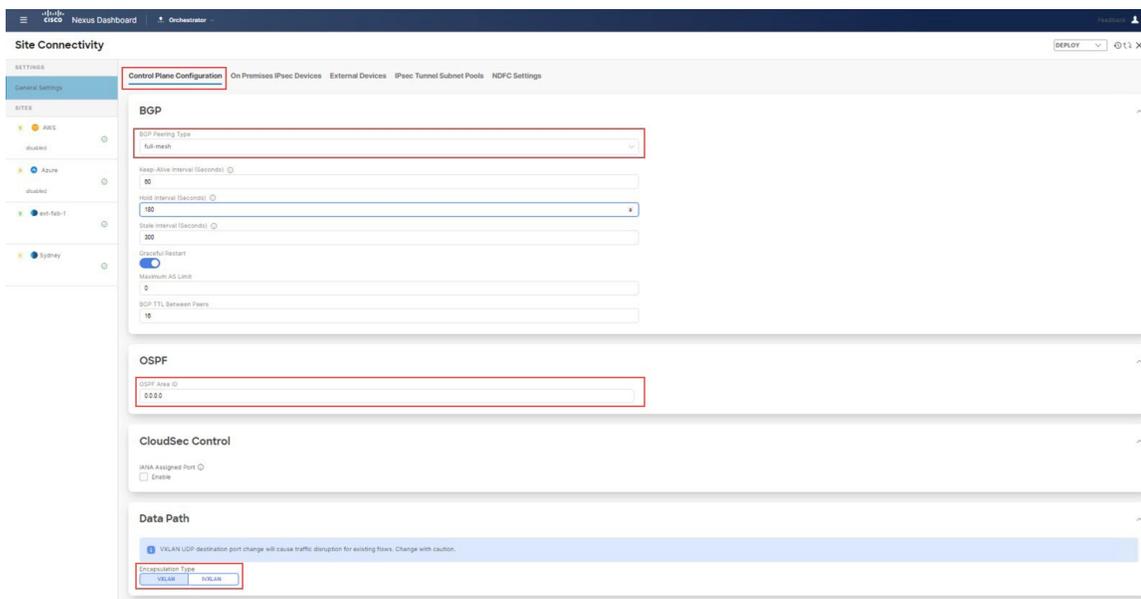
図 67:



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 68:



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 \(15 ページ\)](#) 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 \(21 ページ\)](#) の [オプション 1 \(21 ページ\)](#) 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 **OSPF** 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 \(80 ページ\)](#) 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。

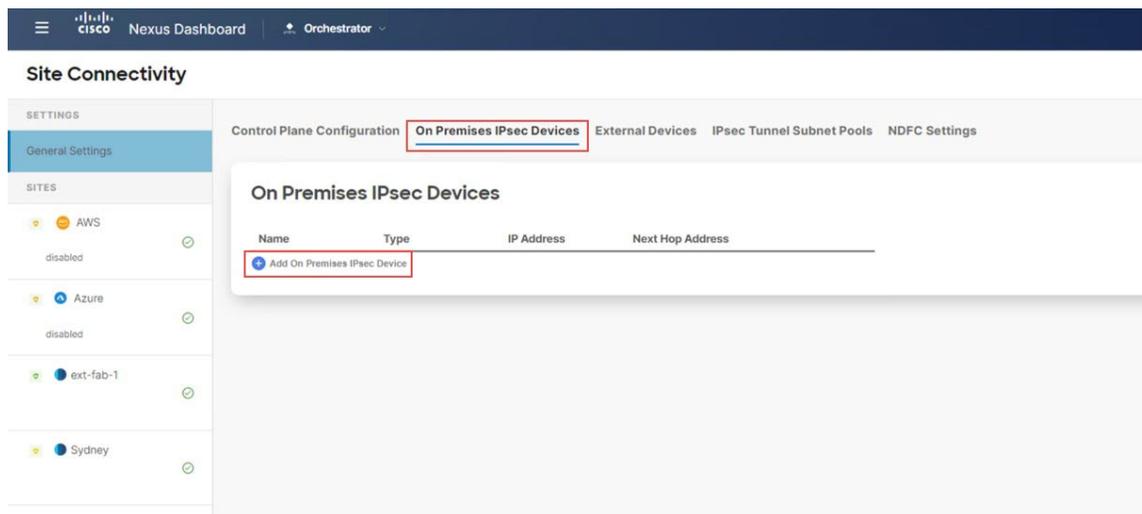
#### 始める前に

[必要なコントロールプレーン構成を完了する \(78 ページ\)](#) 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 69:



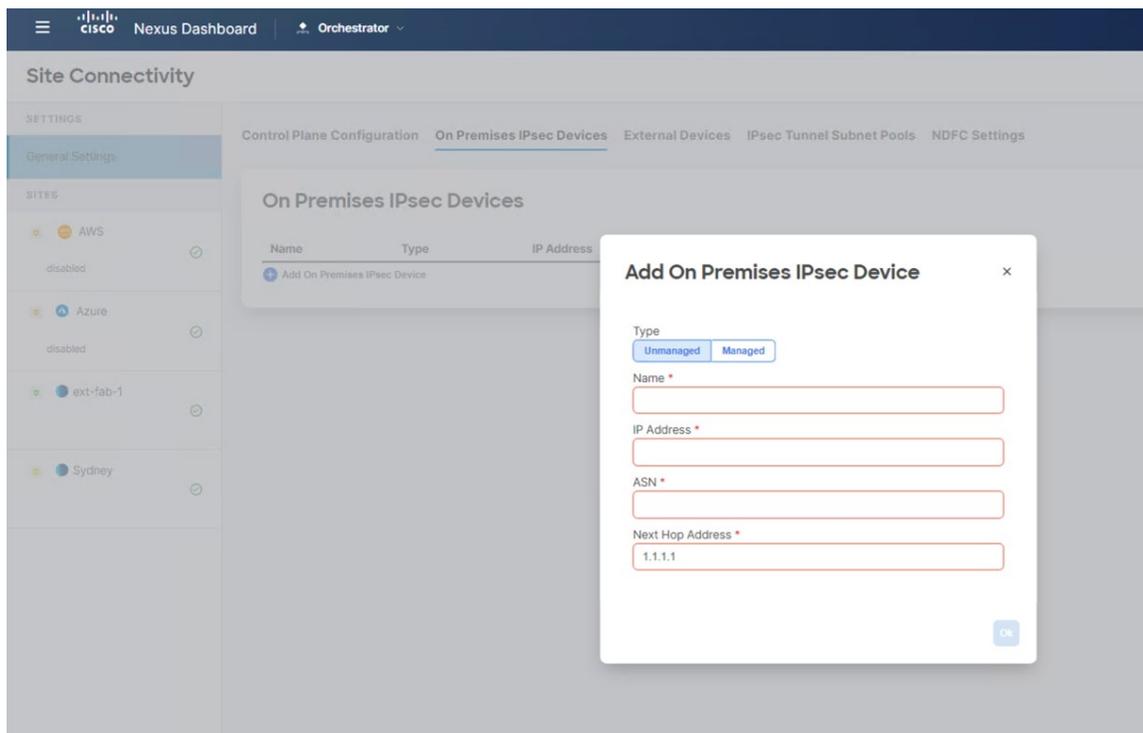
[オンプレミス IPsec デバイスを追加 (Add On Premises IPsec Device)] ページが表示されます。

**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。

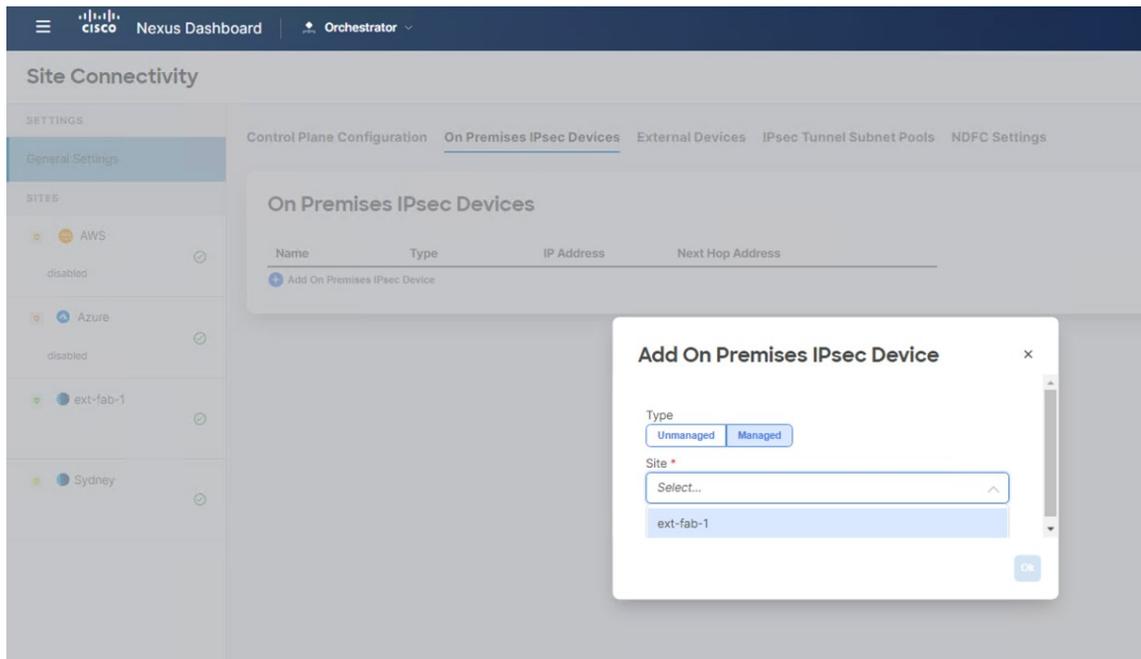
- オンプレミスの IPsec デバイスに対して [管理対象外 (Unmanaged)] オプションを選択した場合は、[名前 (Name)]、[IP アドレス (IP Address)]、[ネクストホップアドレス (Next Hop Address)] など、この管理対象外のオンプレミス IPsec デバイスに必要な情報を入力する必要があります。オンプレミスの IPsec デバイスが NDFC で管理されていない場合 (そのデバイスが NDFC でサポートされていないか、サードパーティのデバイスである場合)、[管理対象外 (Unmanaged)] を使用します。次に、NDO は、管理対象外の IPsec 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 70:



- 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 71:



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。

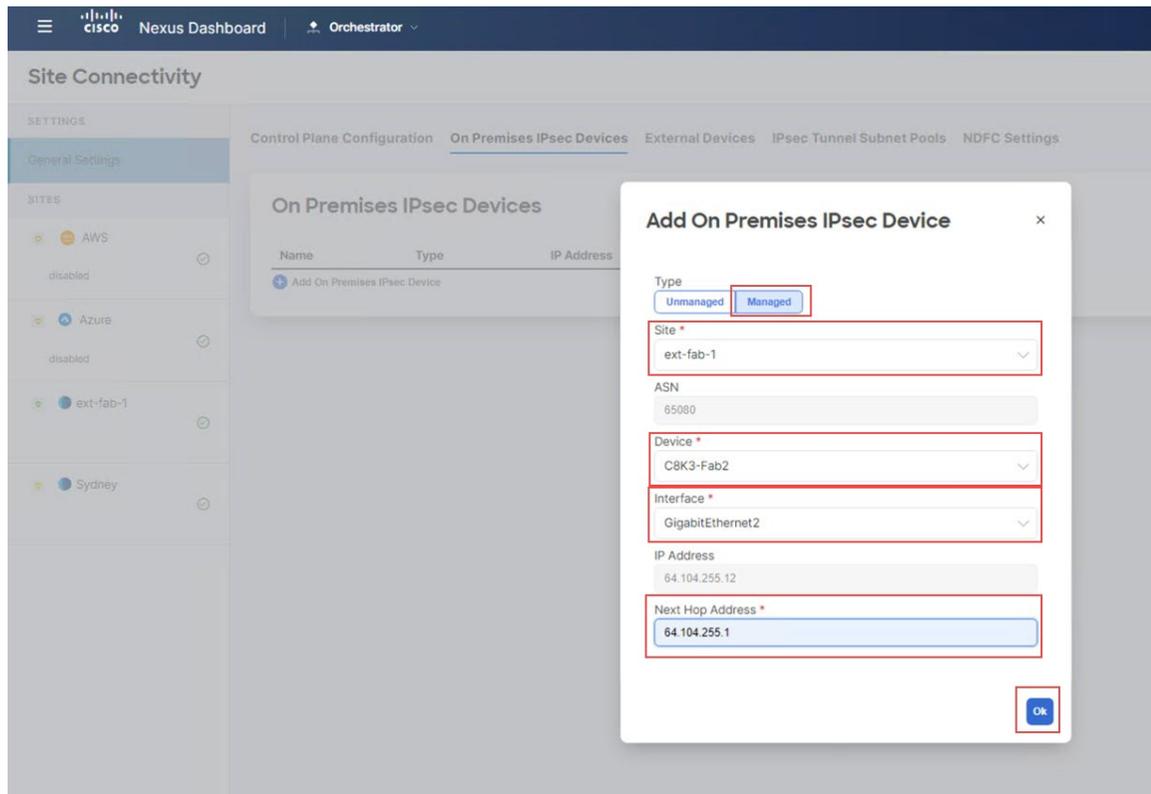
**[デバイス (Device)]** フィールドで使用できるデバイスは、上で選択した NDFC サイトで構成されたオンプレミスの IPsec デバイスについて、NDO が NDFC からプルする情報に基づいています。**[デバイス (Device)]** フィールドで選択したオンプレミスの IPsec デバイスに基づいて、**ASN** フィールドが自動的に入力されます。

- 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。

このインターフェイスの **[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イ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 72:



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。

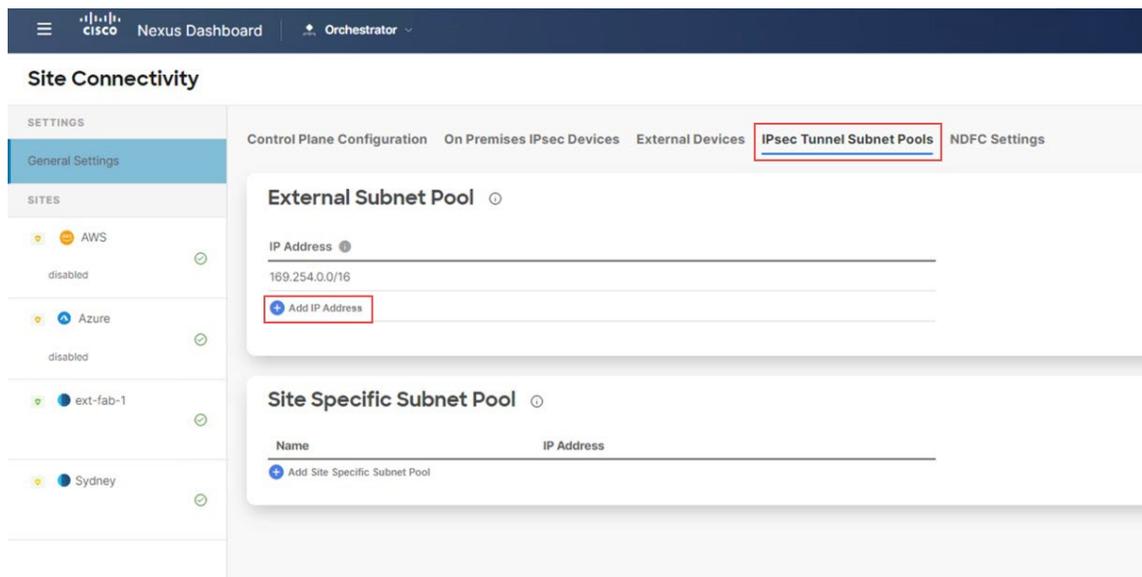
[オンプレミス IPsec デバイス (On Premises IPsec Device)] ページに戻ります。このページには、構成されたオンプレミスの IPsec デバイスが表示されています。

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 73:

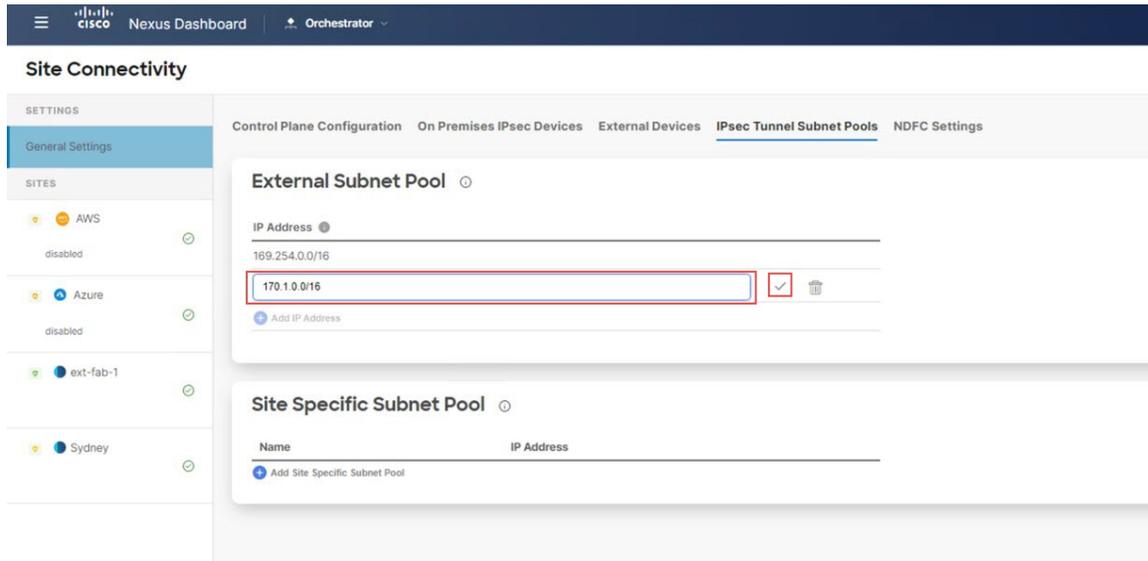


**ステップ 7** IPsec トンネルに使用する IP サブネットプールを入力します。

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。

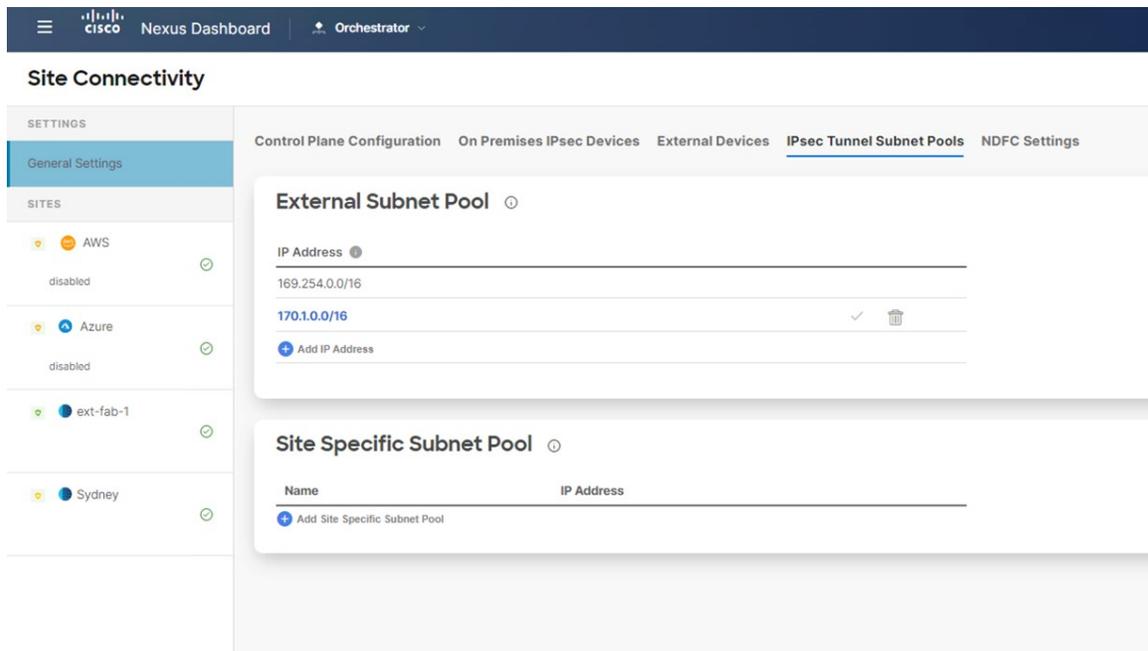
図 74:



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。

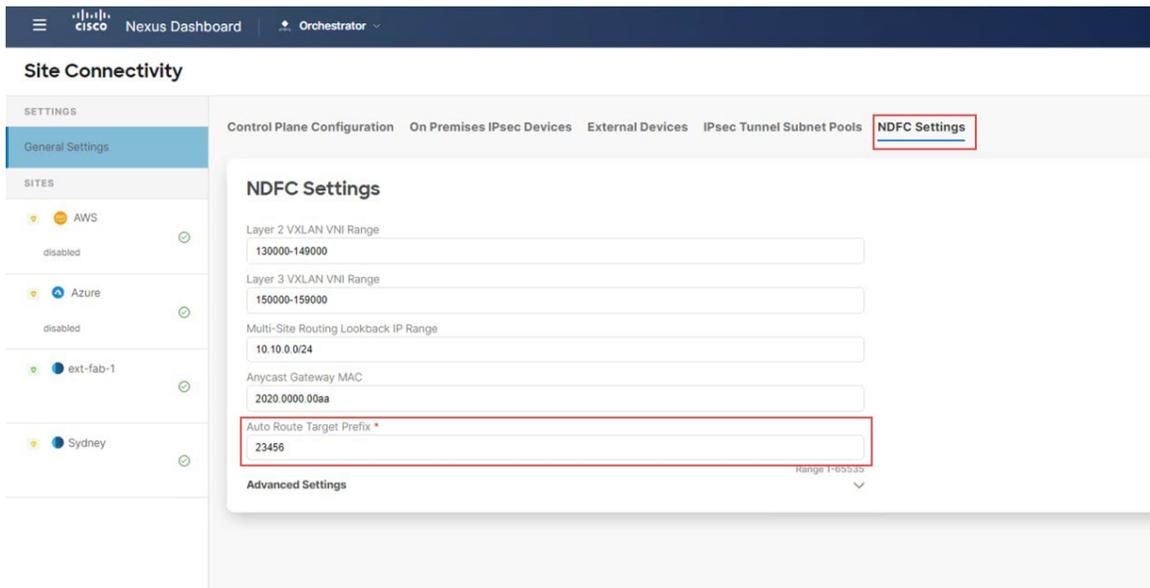
[外部サブネットプール (External Subnet Pool)] エリアの下に IP サブネットプールが表示されます。

図 75:



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 76:



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 \(87 ページ\)](#) 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 \(80 ページ\)](#) の手順を実行します。

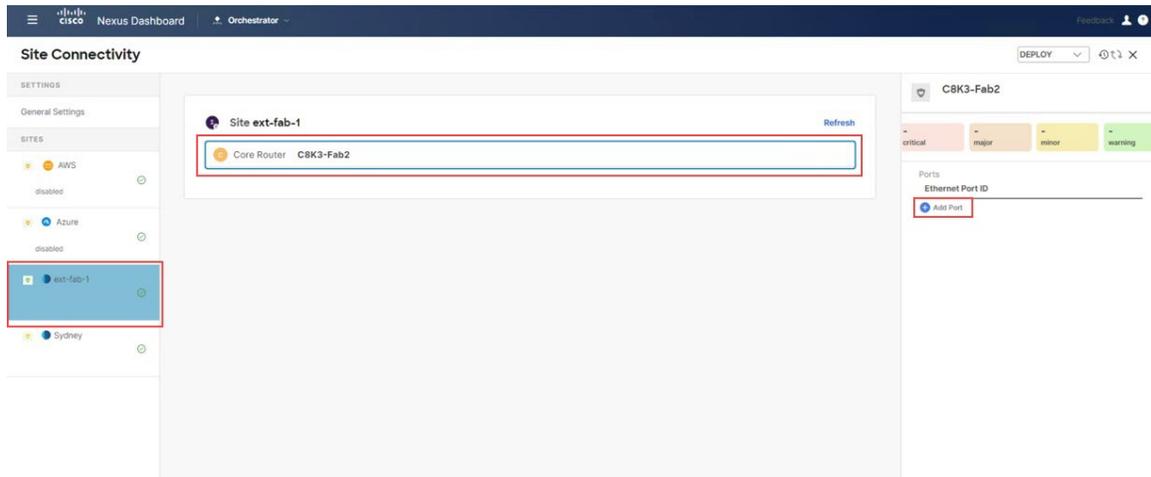
**ステップ 1** **[一般設定 : サイト (General Settings: Sites)]** の下の左側のウィンドウで、NDFC 外部ファブリック (この例では ext-fab-1 サイト) をクリックします。

**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。

## 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

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 77:

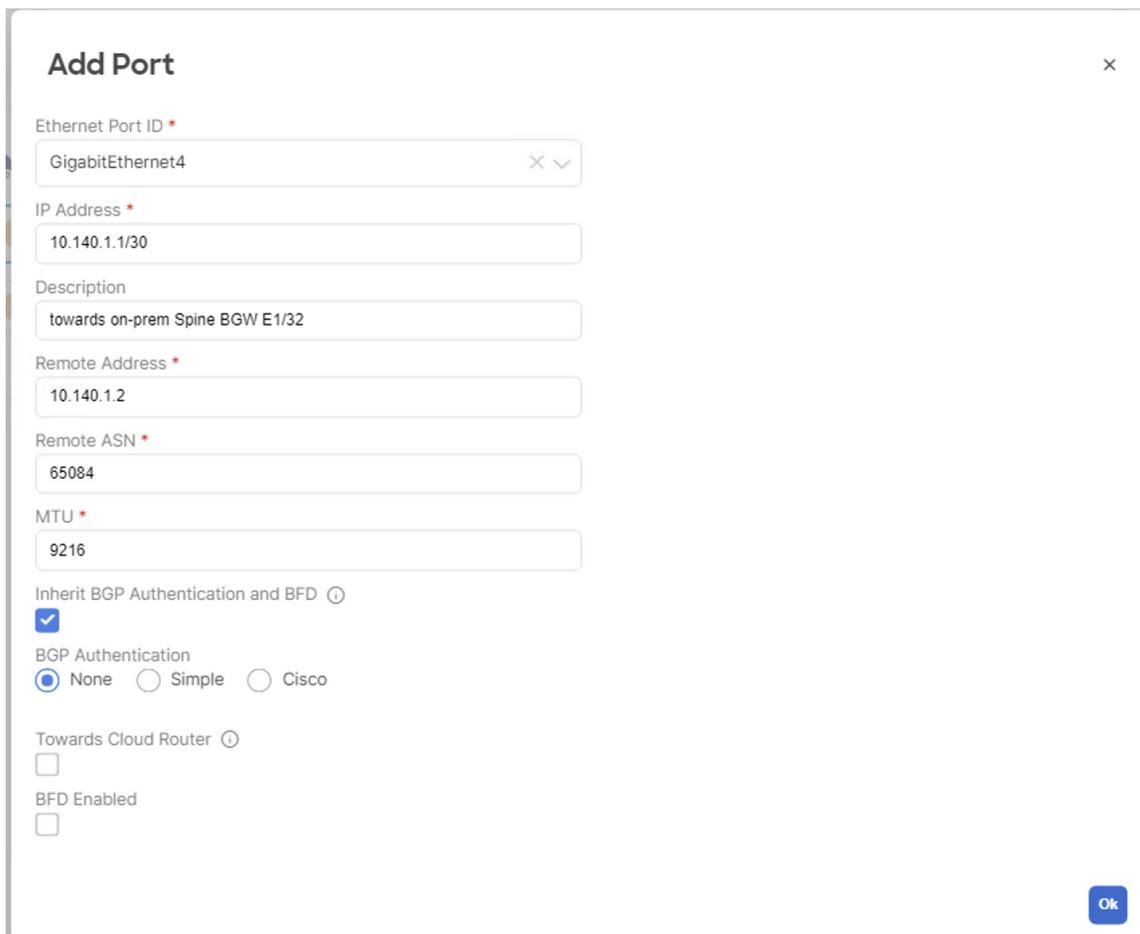


ステップ4 IP アドレス、リモート IP アドレス、リモート ASN など、ポート構成に必要な情報を入力します。

(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この導入例に[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 (21 ページ) のオプション 3 (23 ページ) 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 (92 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 78:



**Add Port** [Close]

Ethernet Port ID \*  
GigabitEthernet4 [X] [v]

IP Address \*  
10.140.1.1/30

Description  
towards on-prem Spine BGW E1/32

Remote Address \*  
10.140.1.2

Remote ASN \*  
65084

MTU \*  
9216

Inherit BGP Authentication and BFD ⓘ

BGP Authentication  
 None  Simple  Cisco

Towards Cloud Router ⓘ

BFD Enabled

[Ok]

**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。 (89 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 (87 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

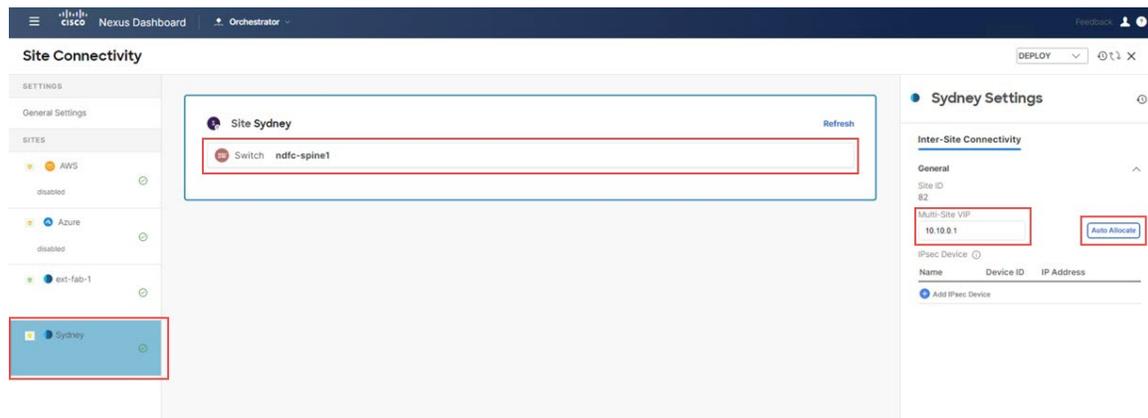
**ステップ 1** [一般設定：サイト（General Settings: Sites）] の下の左側のペインで、NDFC VXLAN ファブリック サイトをクリックします。

**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 79:



## 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 (90 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

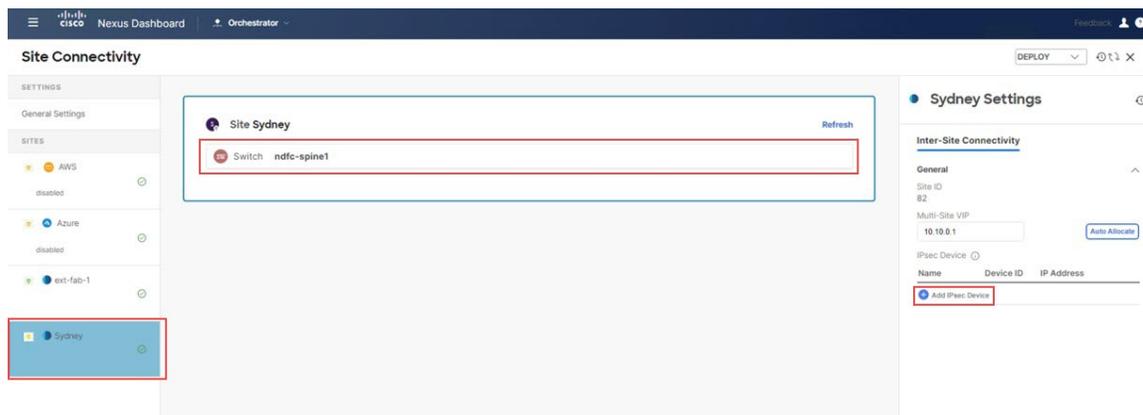
VXLAN ファブリック サイトのマルチサイト VIP を定義します。(89 ページ) の手順を実行します。

**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。

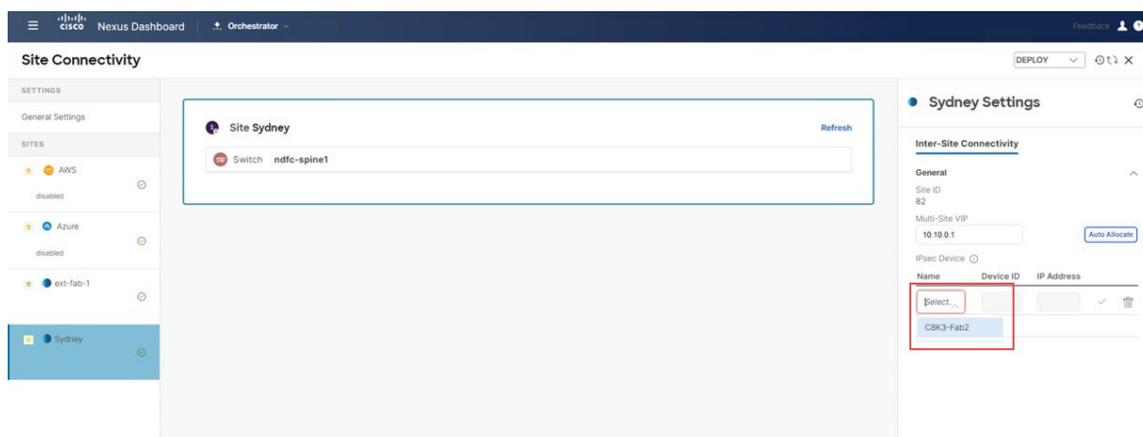
**ステップ 3** 右側のペインの [サイト間接続（Inter-Site Connectivity）] で、[IPsec デバイスの追加（Add IPsec Device）] をクリックします。

図 80:



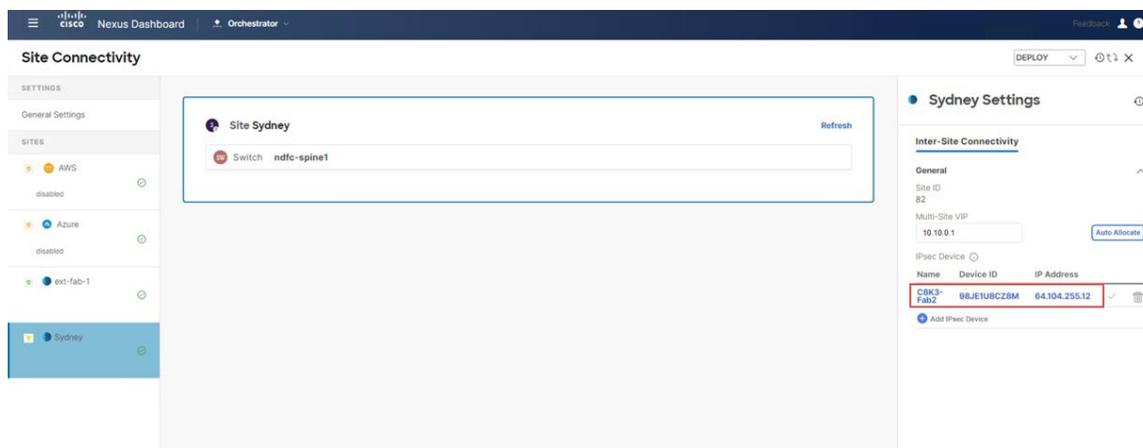
ステップ 4 [選択 (Select)] をクリックして、適切な IPsec デバイスを選択します。

図 81:



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 82:



## 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

**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（92 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

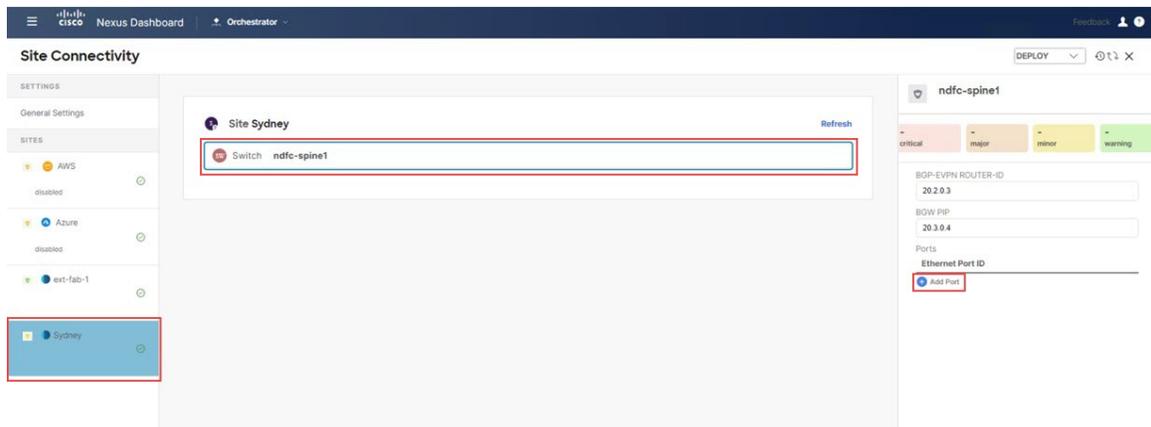
[IPsec デバイスを VXLAN ファブリック サイトにマップする（90 ページ）](#) の手順を実行します。

**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。

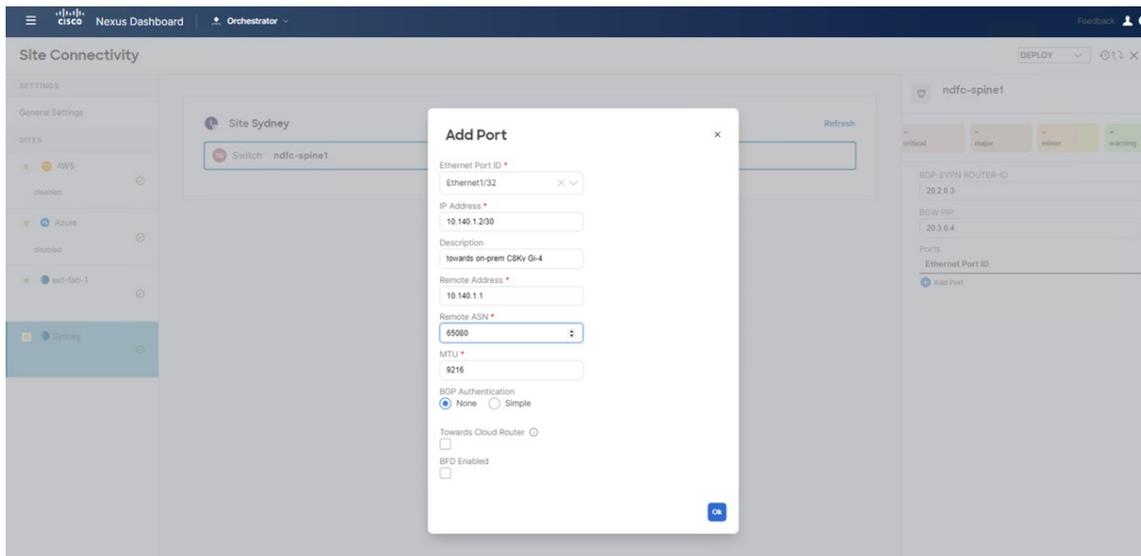
図 83:



**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 84:



- **[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 (21 ページ) のオプション 3 (23 ページ) 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。

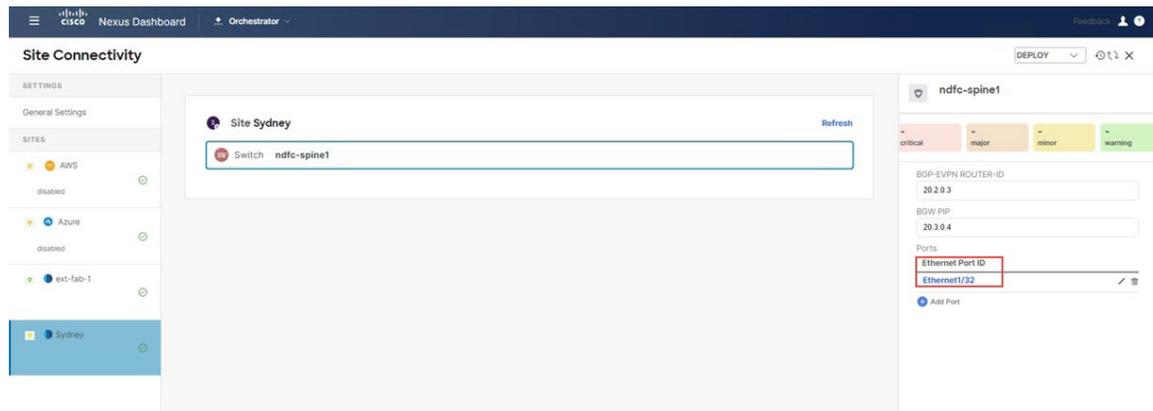
この導入例に使用しているトポロジは、ハブサイトを使用していないのでこの導入例に**[クラウドルータに向かう (Towards Cloud Router)]**をイネーブル化しません。

**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

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

図 85:



## 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 (94 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 (92 ページ) の手順を実行します。

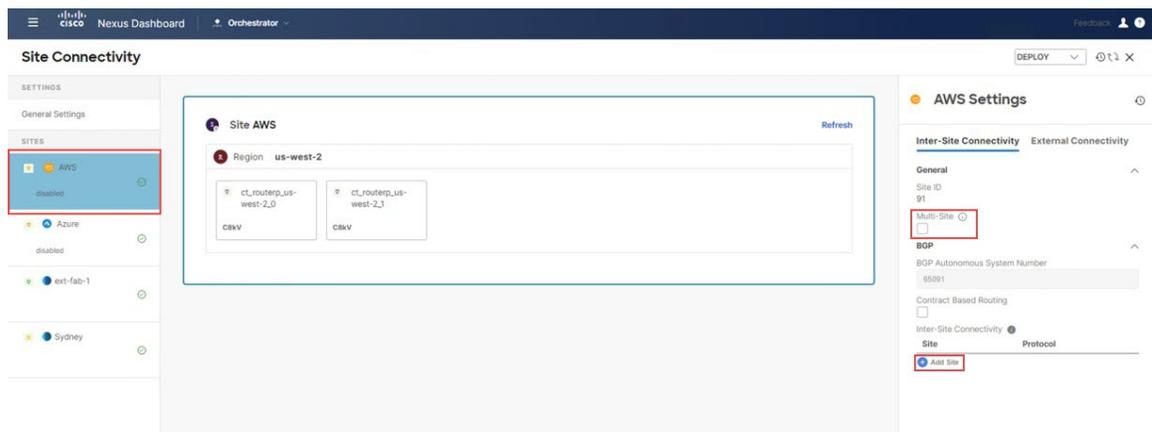
**ステップ 1** [一般設定 : サイト (General Settings: Sites)] の下の左側のペインで、最初のクラウドサイト (AWS サイトなど) をクリックします。

**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。

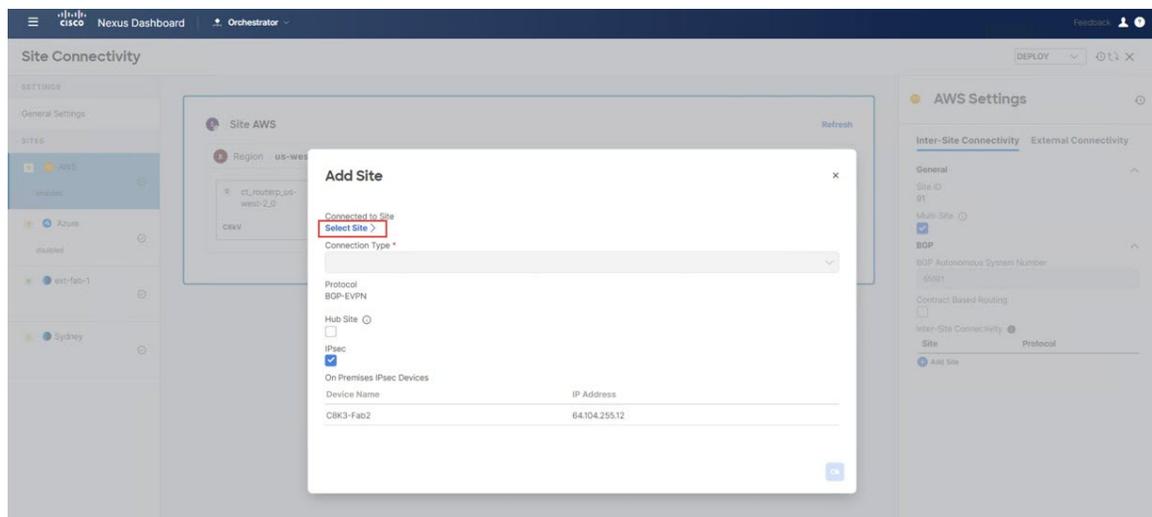
図 86:



[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 87:

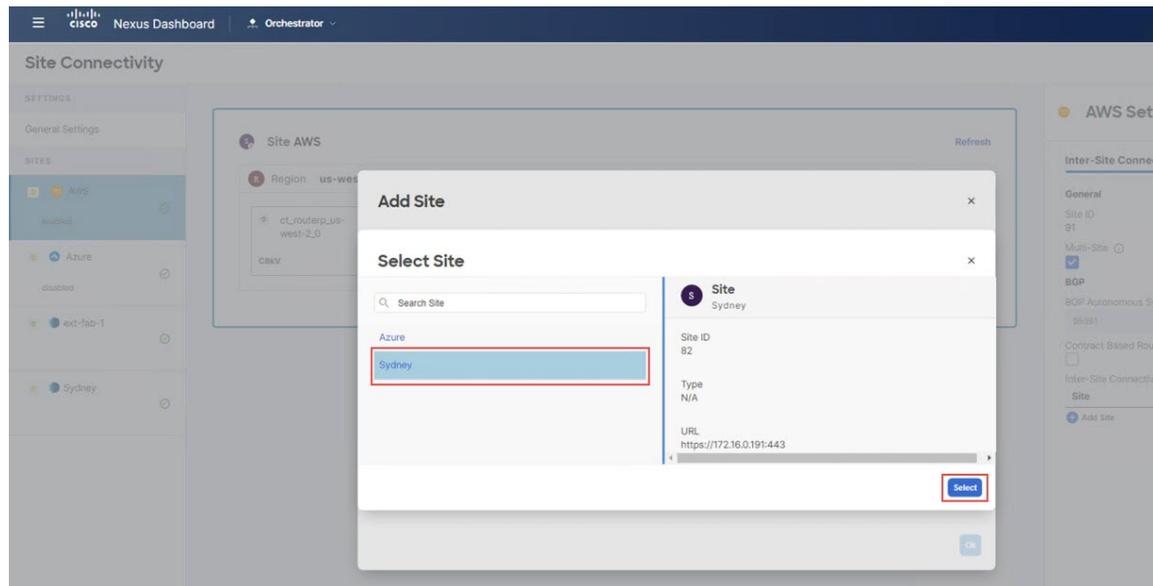


[サイトを選択 (Select a Site)] ページが表示されます。

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。

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

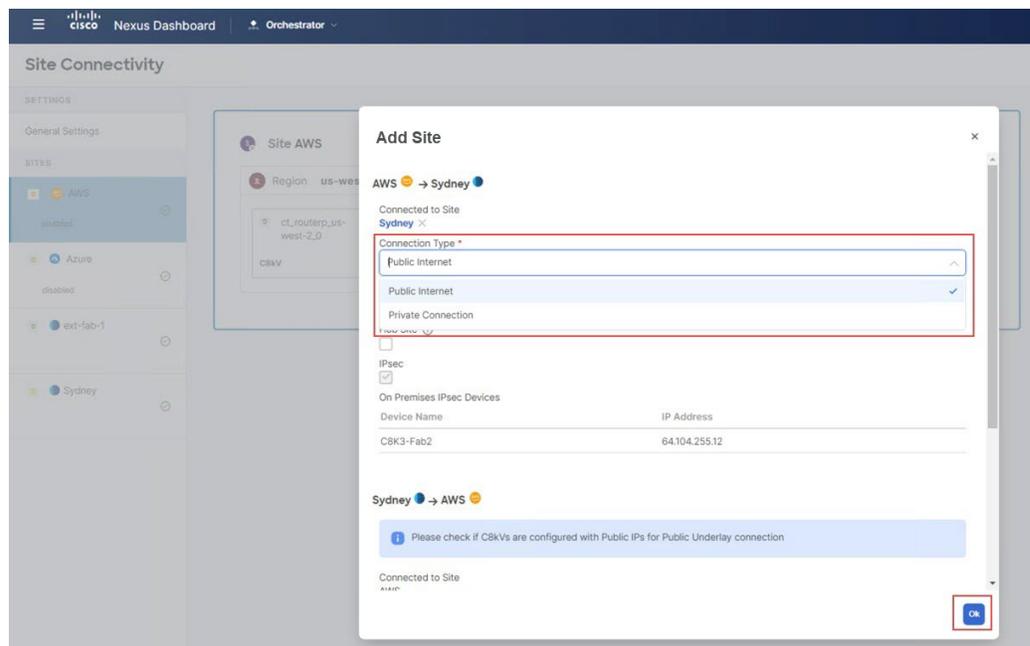
図 88:



[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 89:



[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 \(21 ページ\)](#) のオプション3 ([23 ページ](#)) 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この導入例に[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 \(97 ページ\)](#) 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 \(94 ページ\)](#) の手順を実行します。

---

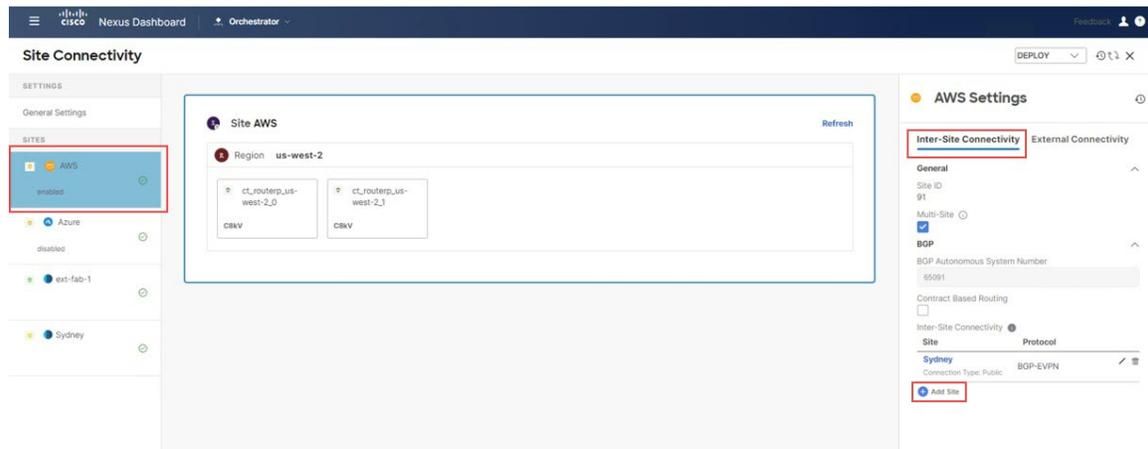
**ステップ1** [一般設定: サイト (General Settings: Sites)] の下の左側のペインで、最初のクラウドサイト (AWS サイトなど) をクリックします。

**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。

## 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

図 90:



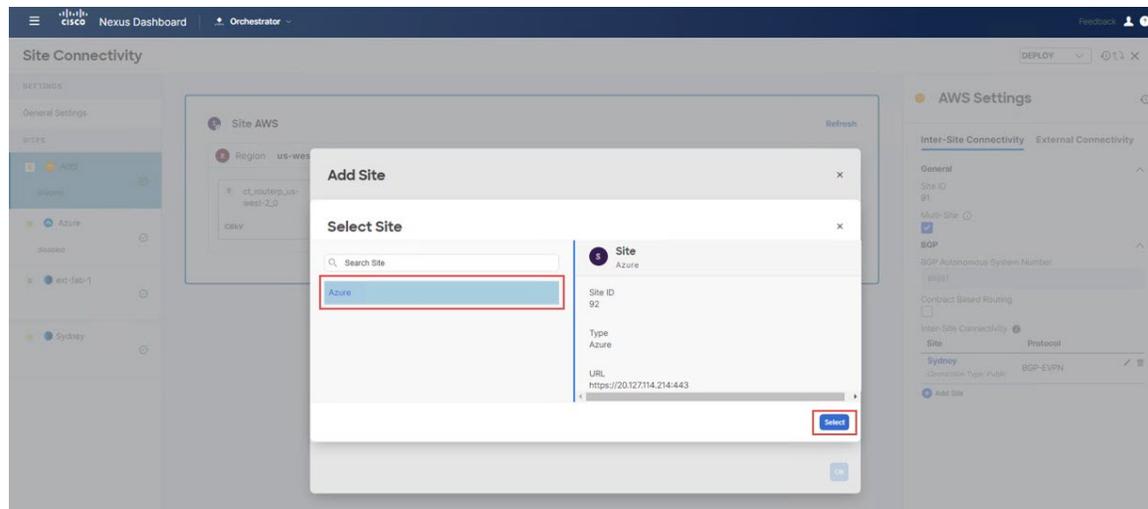
[サイトの追加 (Add Site)] ページが表示されます。

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 91:



[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、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。

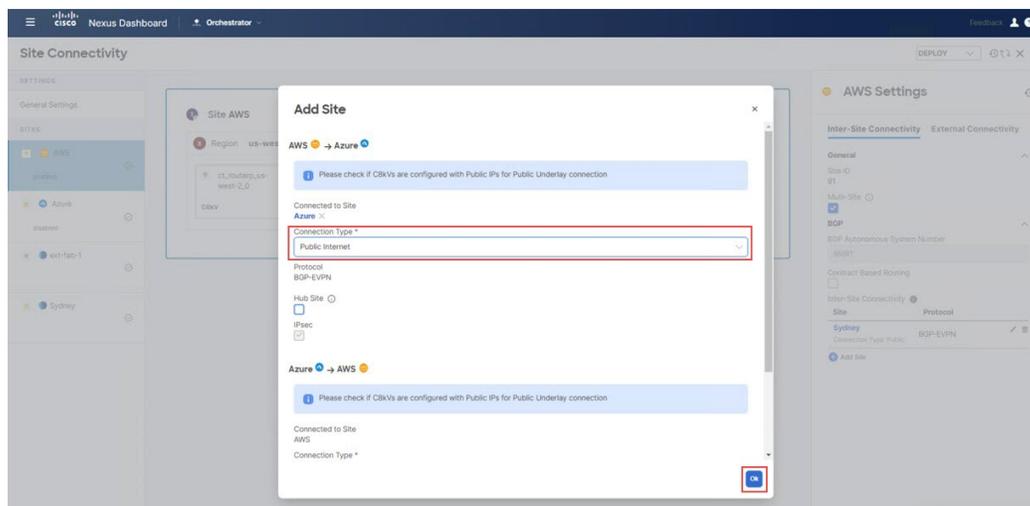
一部のタイプのクラウド間接続では、次のオプションを使用できます。

- 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 92:



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 (99 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。

## 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 \(94 ページ\)](#) 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 \(97 ページ\)](#) 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 \(97 ページ\)](#) 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

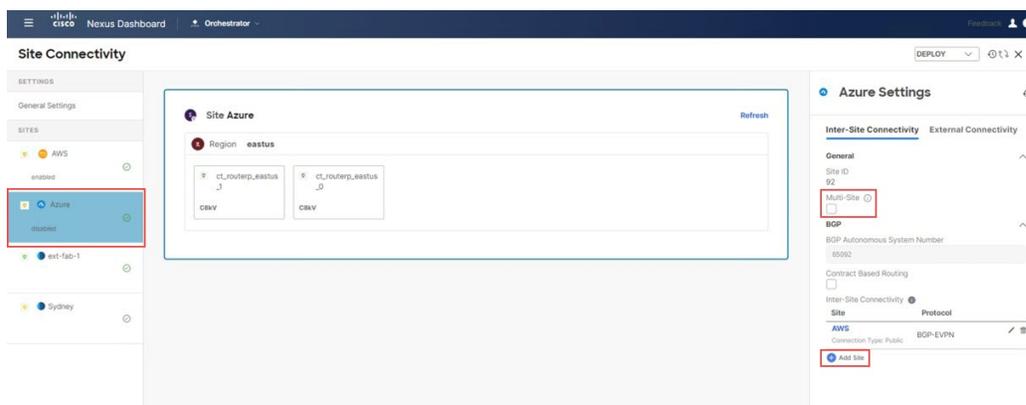
[1つ目のクラウドサイトを2つ目のクラウドサイトに接続する \(97 ページ\)](#) の手順を実行します。

**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 93:



[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。

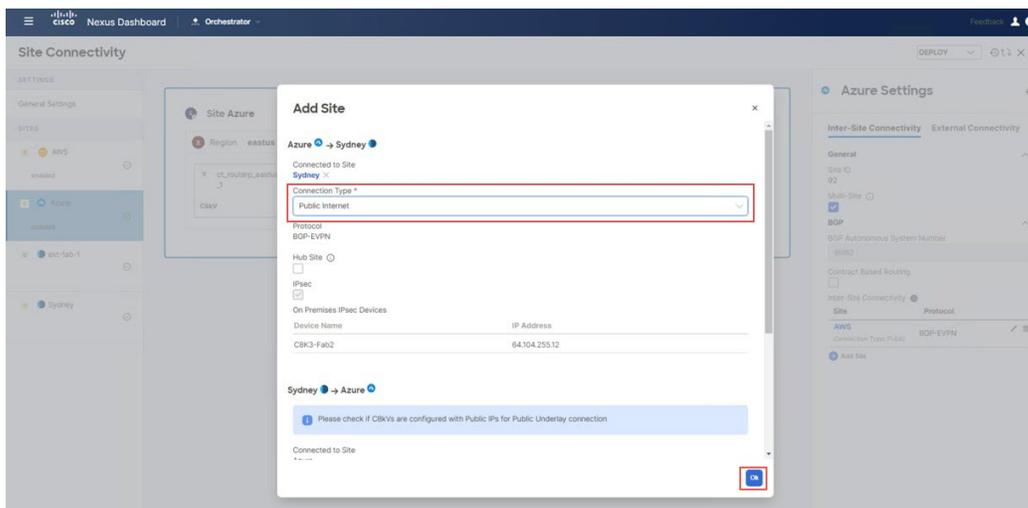
[サイトを選択 (Select a Site)] ページが表示されます。

**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。

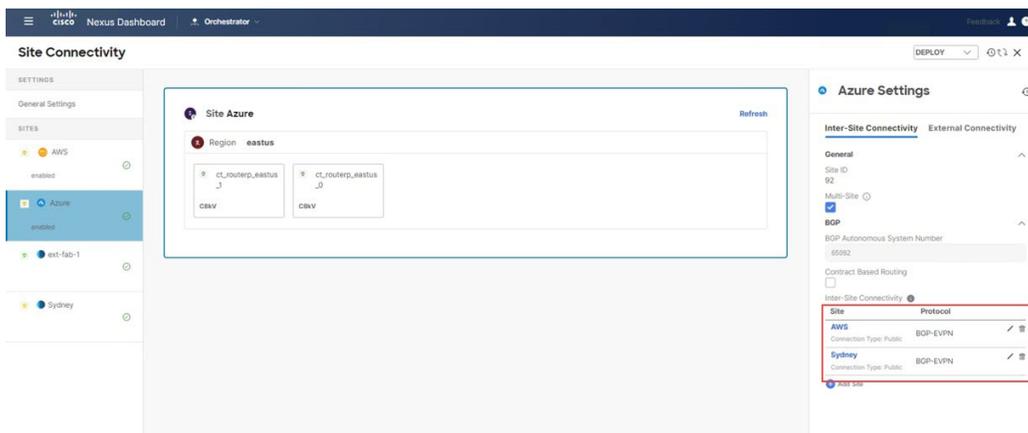
図 94:



**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 95:



## 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 (102 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（99 ページ）の手順を実行します。

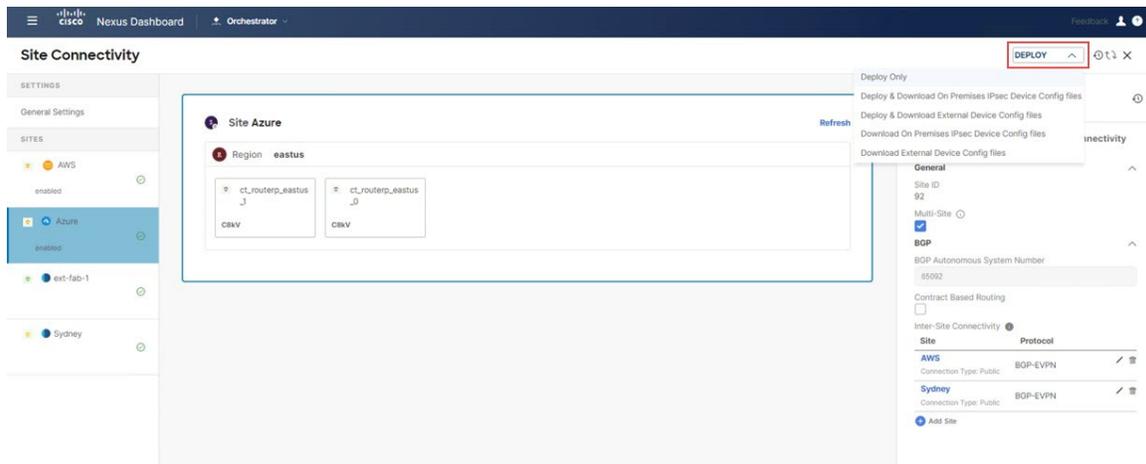
ステップ1 NDO で構成を展開します。

- [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（80 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か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（80 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 96:



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。

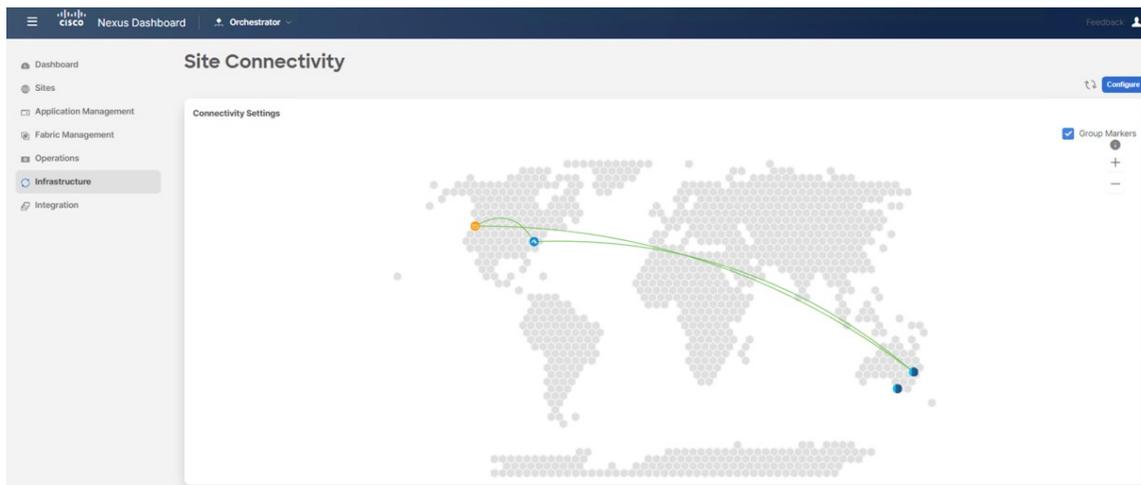
- クラウドネットワーク コントローラを介して NDFC およびクラウド サイト（AWS および Azure）との通信を開始して、IPsec トンネルを自動化します。
- Azure Catalyst 8000V と AWS Catalyst 8000V の間で OSPF を構成します。

- 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 97:



- 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。

## Nexus ダッシュボード オーケストレータの構成を展開

図 98:

| Device                 | Device Status | Interface Status | Peering Status | BGP Peer    | Destination   |
|------------------------|---------------|------------------|----------------|-------------|---------------|
| ct_routerp_us-west-2_3 | ↑ Up          | tunn-7 ↑ Up      | OSPF ↑ Up      | -           | -             |
| ct_routerp_us-west-2_3 | ↑ Up          | tunn-6 ↑ Up      | BGP ↑ Up       | 170.1.254.6 | 64.104.255.12 |
| ct_routerp_us-west-2_3 | ↑ Up          | tunn-8 ↑ Up      | OSPF ↑ Up      | -           | -             |
| ct_routerp_us-west-2_0 | ↑ Up          | tunn-7 ↑ Up      | OSPF ↑ Up      | -           | -             |
| ct_routerp_us-west-2_0 | ↑ Up          | tunn-8 ↑ Up      | OSPF ↑ Up      | -           | -             |
| ct_routerp_us-west-2_0 | ↑ Up          | tunn-6 ↑ Up      | BGP ↑ Up       | 170.1.254.2 | 64.104.255.12 |

- 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 99:

| Device              | Device Status | Interface Status | Peering Status | BGP Peer    | Destination   |
|---------------------|---------------|------------------|----------------|-------------|---------------|
| ct_routerp_eastus_0 | ↑ Up          | tunn-3 ↑ Up      | OSPF ↑ Up      | -           | -             |
| ct_routerp_eastus_0 | ↑ Up          | tunn-2 ↑ Up      | OSPF ↑ Up      | -           | -             |
| ct_routerp_eastus_0 | ↑ Up          | tunn-1 ↑ Up      | BGP ↑ Up       | 170.1.255.2 | 64.104.255.12 |
| ct_routerp_eastus_3 | ↑ Up          | tunn-2 ↑ Up      | OSPF ↑ Up      | -           | -             |
| ct_routerp_eastus_3 | ↑ Up          | tunn-3 ↑ Up      | OSPF ↑ Up      | -           | -             |
| ct_routerp_eastus_3 | ↑ Up          | tunn-1 ↑ Up      | BGP ↑ Up       | 170.1.255.6 | 64.104.255.12 |

- 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。

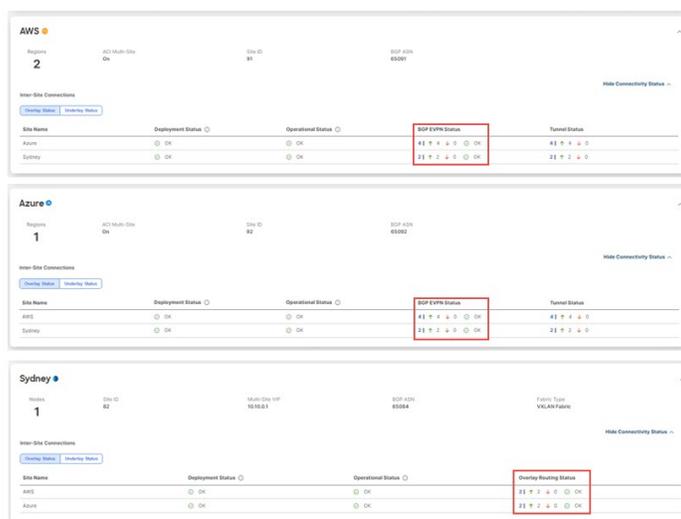
アンダーレイ ステータスは、BGW スパイン スイッチとオンプレミス IPsec デバイス間の eBGP セッション ステータスを示します。

図 100:



- 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。

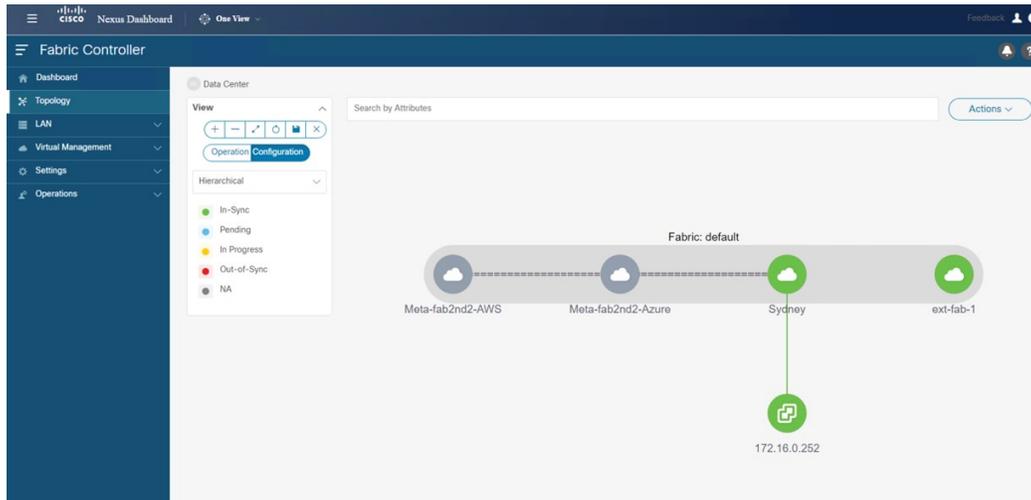
図 101:



- 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。

## Nexus ダッシュボード オーケストレータの構成を展開

図 102:





## 第 **II** 部

### 使用例

- [テナントを展開 \(109 ページ\)](#)
- [ストレッチされた VRF ユース ケース \(117 ページ\)](#)
- [ルート リークの使用例 \(155 ページ\)](#)





## 第 5 章

# テナントを展開

- [テナントを展開 \(109 ページ\)](#)

## テナントを展開

サイト間にアンダーレイとオーバーレイの接続が確立されたら、エンドポイント ネットワーク/VPC/VNet を展開して、オンプレミスとクラウドサイトに展開されたテナント エンドポイント間の通信を確立する必要があります。

NDOは、VRFとネットワークを定義するためにスキーマとテンプレートの概念を使用します。NDFCのコンテキストでは、VRFは、あるテナントを別のテナントから分離するために使用されます。1つのテナントのすべてのエンドポイントネットワーク（サブネット）は、それぞれのVRFにマッピングされます。VRFの同じ概念をクラウドに拡張することもできます。VRFはAWSのVPCおよびAzureのVNetに対応します。

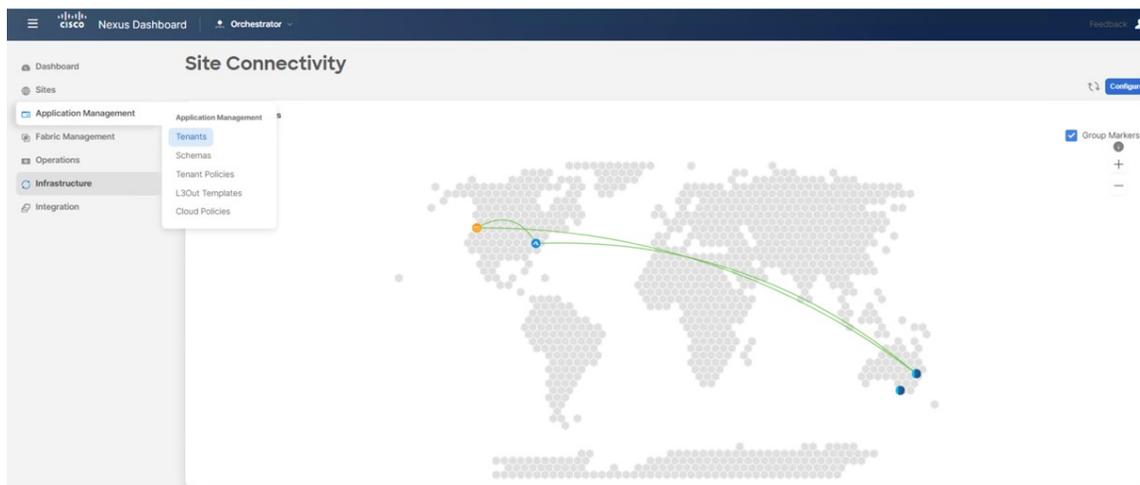
テナントを展開するための次の手順は、前述のすべてのトポロジに適用され、展開された特定のインフラ構成を活用します。また、次のユースケースのいずれにも適用されます。



- (注) NDOには、事前に構築された `dcnm-default-tn` テナントがあり、オンプレミスサイトとクラウドサイトに関連付けることができます。ハイブリッドクラウド接続を展開するときに、この事前構築済みの `dcnm-default-tn` テナントをNDFCおよびクラウドサイトに関連付けることをお勧めしますが、必要に応じて、独自のテナントを最初から作成することもできます。

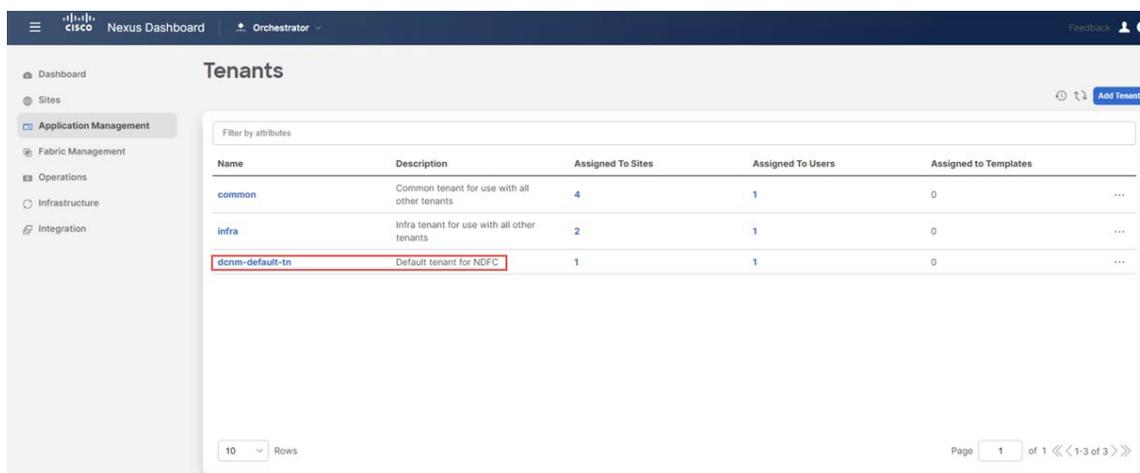
ステップ1 NDOで[アプリケーション管理 (Application Management)] > [テナント (Tenants)]に移動します。

図 103 :



テナント ウィンドウが表示されます。

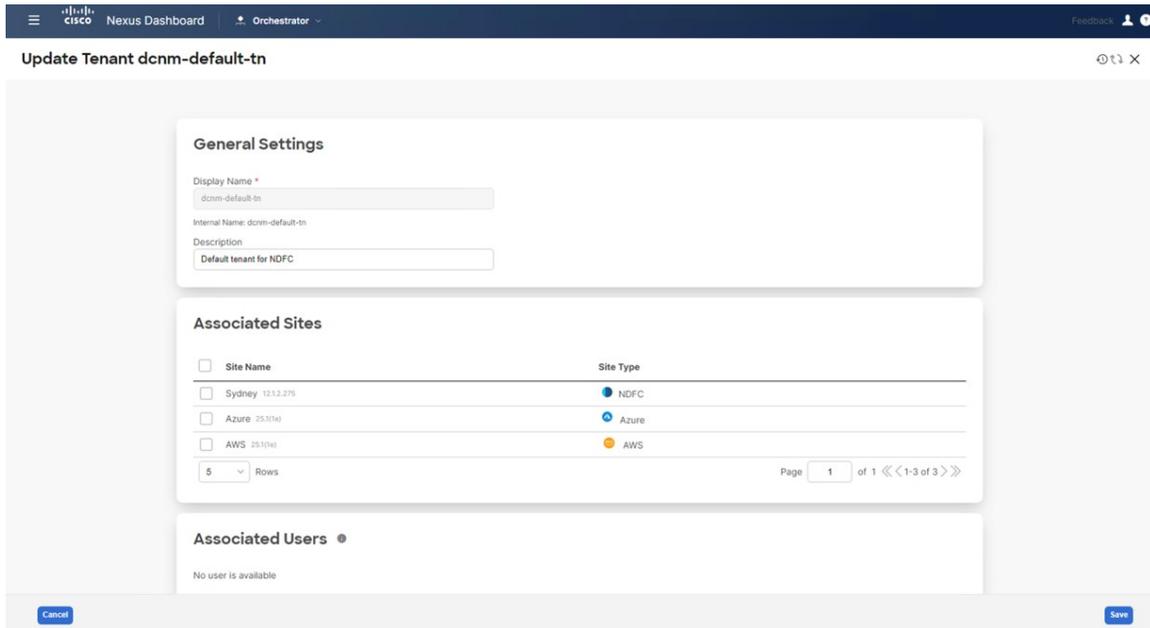
図 104 :



ステップ 2 dcnm-default-tn テナントをクリックします。

dcnm-default-tn テナントの [テナントの更新 (Update Tenant)] ページが表示されます。

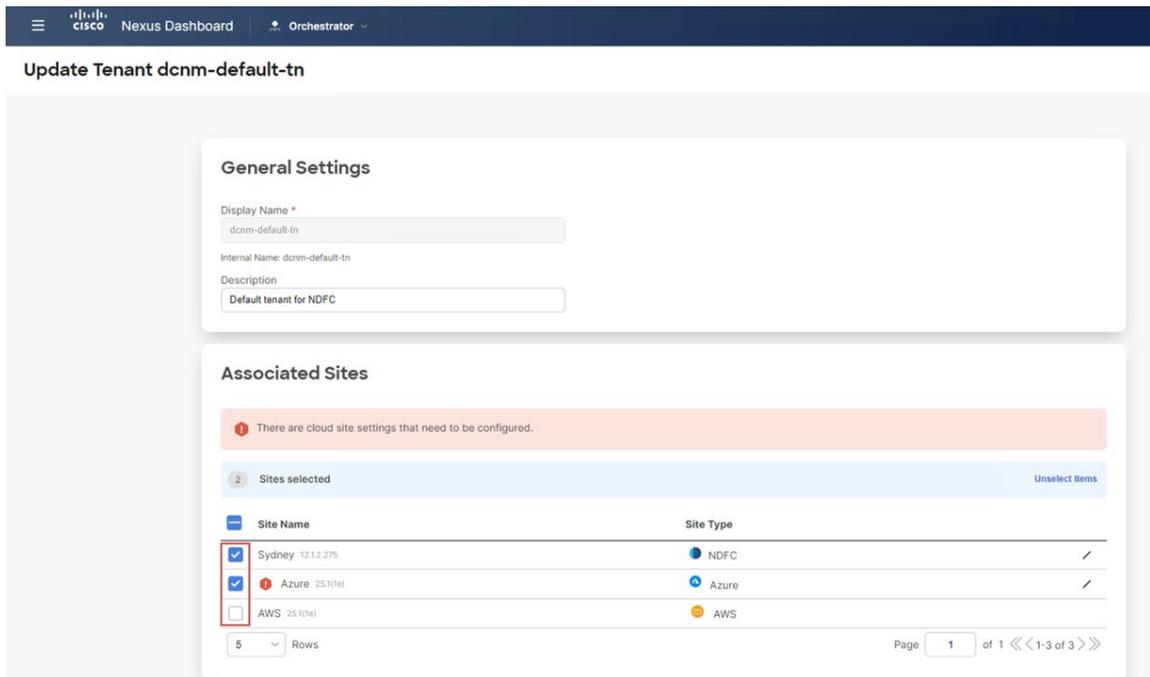
図 105:



**ステップ 3** 画面に表示されているサイトを選択します。

外部ファブリック サイトはリストに表示されないことに注意してください。外部サイトは、オンプレミスサイトとクラウドサイト間の接続を提供するためにのみ使用され、外部ファブリックにはエンドホストがないため、外部ファブリックにテナントを展開する必要はありません。

図 106:

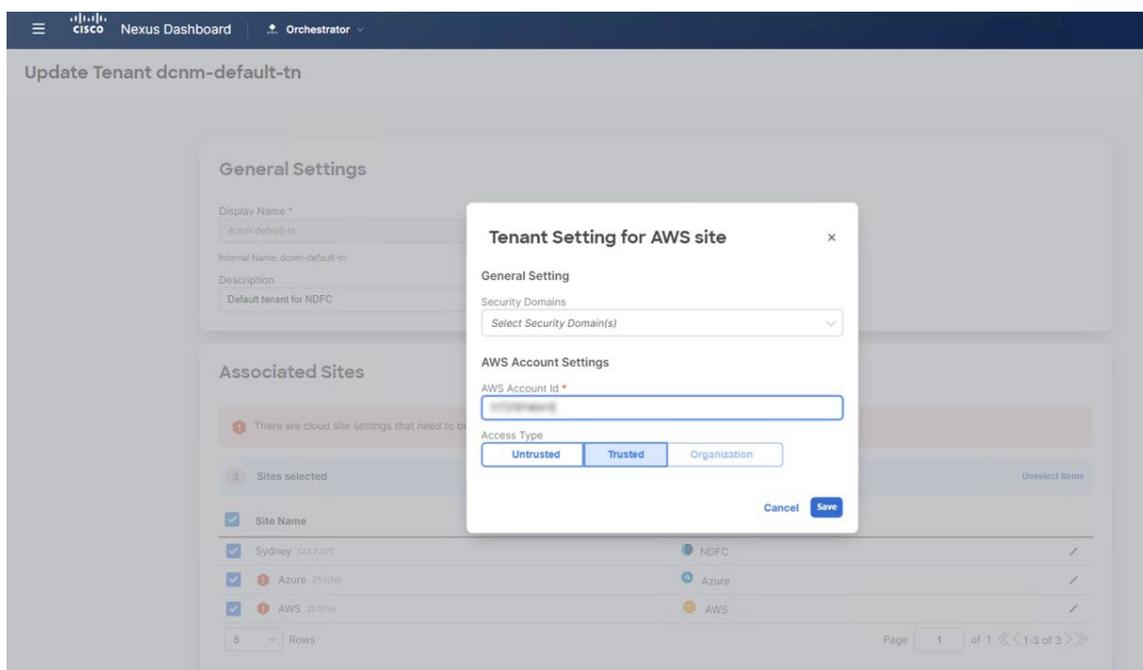


**ステップ 4** クラウドサイトの場合は、編集ボタン (鉛筆アイコン) をクリックして、各クラウドアカウントに必要な情報を入力します。

ユーザーテナントにはAWSの追加アカウントが必要ですが、Azureの場合は、Azureインフラテナントと同じサブスクリプションを使用できます。

- たとえば、AWSクラウドサイトの編集ボタンをクリックした後、**[AWSアカウント設定 (AWS Account Setting)]** エリアで、**[アクセスタイプ (Access Type)]** で**[信頼 (Trusted)]** をクリックし、関連するAWSアカウント識別子をそのフィールドに入力します。

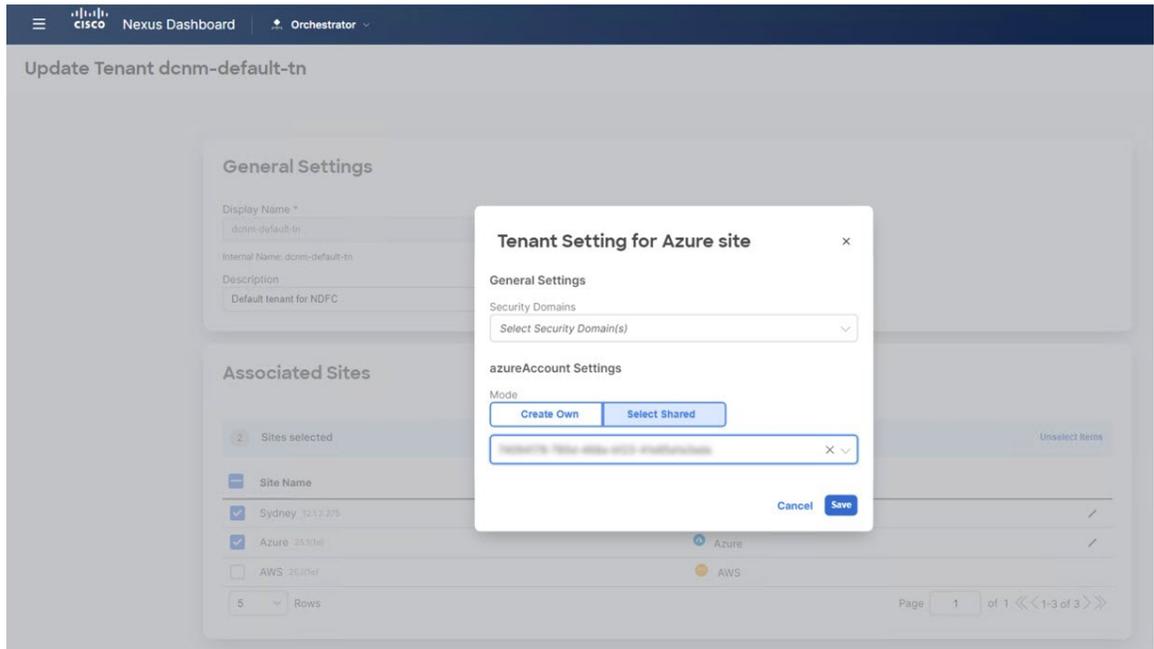
図 107:



AWSのテナントのさまざまなアクセスタイプの詳細については、[\[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 \(Cisco Cloud Network Controller for AWS Installation Guide\)\]](#)、リリース25.1(1)以降の「Setting Up the AWS Account for the User Tenant」セクションを参照してください。

- 同様に、Azureクラウドサイトの編集ボタンをクリックした後、テナントが管理されているかどうかに応じて、必要な情報を入力します。

図 108:

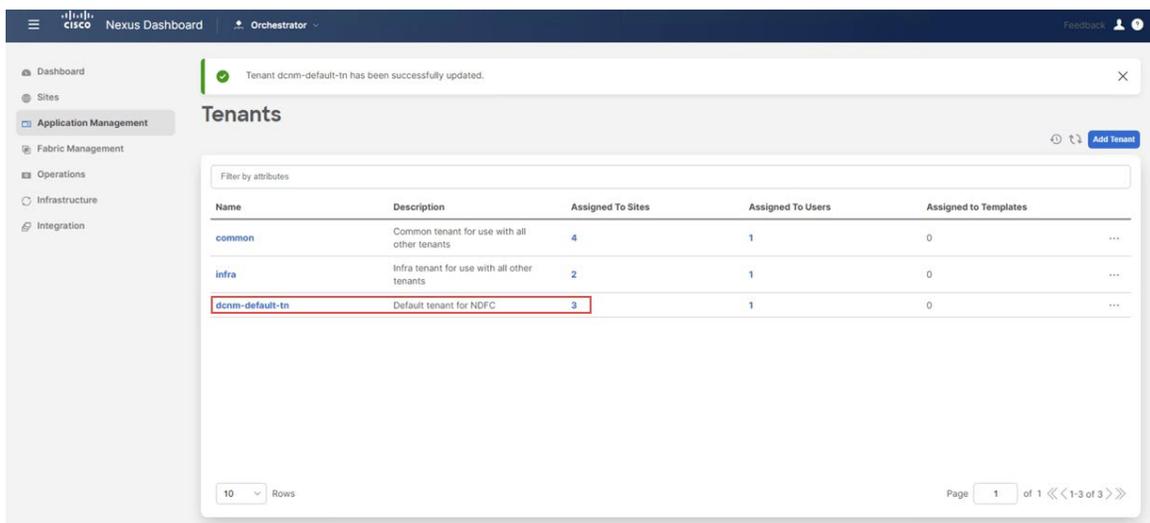


Azure のテナントのさまざまなアクセスタイプの詳細については、[\[Azure インストールガイドの Cisco クラウドネットワーク コントローラ \(Cisco Cloud Network Controller for Azure Installation Guide\)\]](#)、リリース 25.1 (1) 以降の「Adding a Role Assignment」セクションを参照してください。

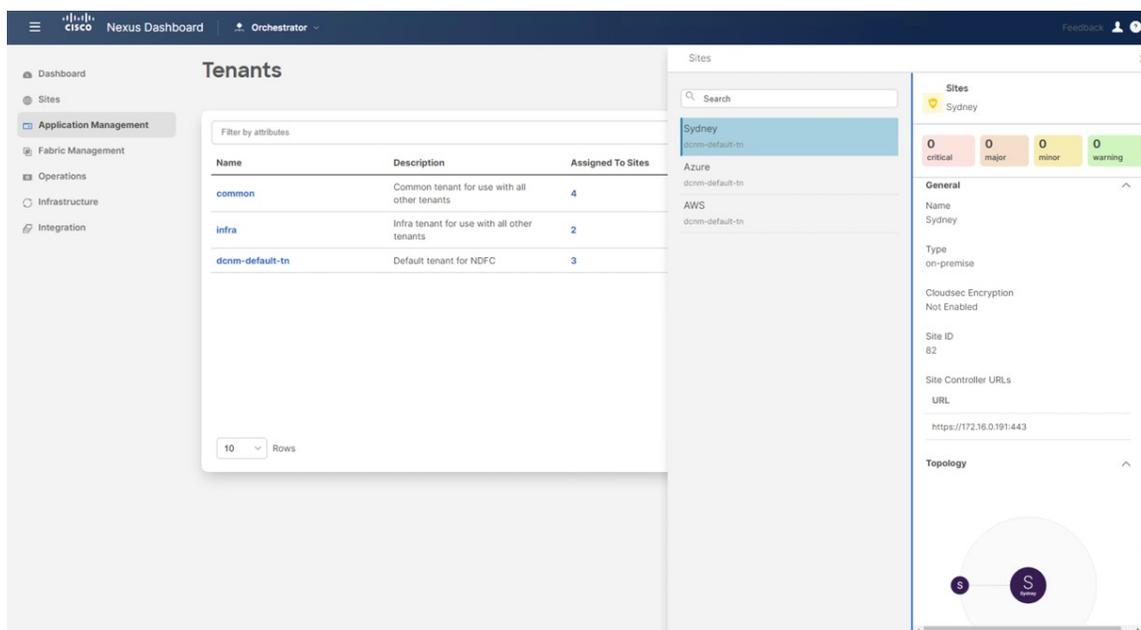
**ステップ 5** テナントが正しく展開されたことを確認します。

たとえば、次の図では、`dcnm-default-tn` テナントには 3 つのサイトがマップされています (1 つのオンプレミス NDFC サイトと 2 つのクラウドサイト)。

図 109:

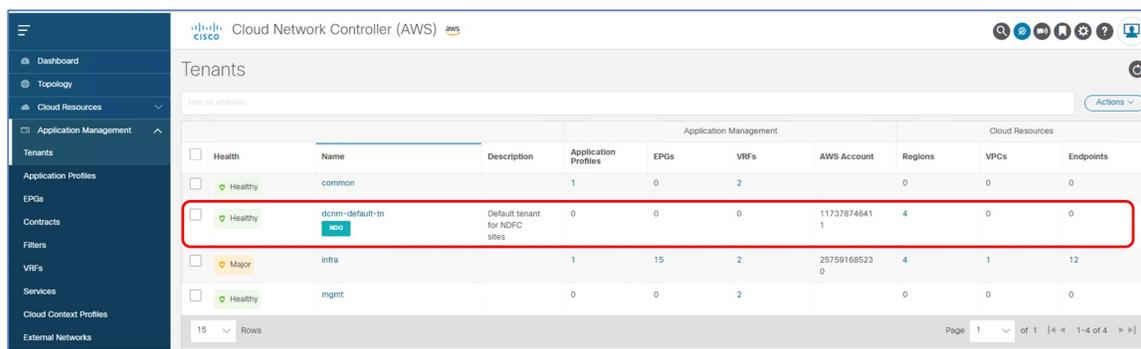


テナントを展開



クラウドサイトの Cisco Cloud Network Controller に展開された dcnm-default-tn テナントを確認することもできます。

図 110:



| Cisco Cloud Network Controller (AZURE) |                |                               |                      |                        |      |                                       |                 |                  |           |
|--|----------------|-------------------------------|----------------------|------------------------|------|---------------------------------------|-----------------|------------------|-----------|
| Tenants                                |                |                               |                      |                        |      |                                       |                 |                  |           |
| Filter by attributes                   |                |                               |                      |                        |      |                                       |                 |                  |           |
| Actions                                |                |                               |                      |                        |      |                                       |                 |                  |           |
|  |                |                               |                      | Application Management |      |                                       | Cloud Resources |                  |           |
| Health                                 | Name           | Description                   | Application Profiles | EPGs                   | VRFs | Azure Subscription                    | Regions         | Virtual Networks | Endpoints |
| <input type="checkbox"/>               | common         |                               | 1                    | 0                      | 2    |                                       | 0               | 0                | 0         |
| <input type="checkbox"/>               | dcm-default-tn | Default tenant for NDFC sites | 0                    | 0                      | 0    | Shared from infra                     | 0               | 0                | 0         |
| <input type="checkbox"/>               | infra          |                               | 1                    | 12                     | 2    | 74094178-785d-468a-bf23-41e85a1a3a da | 1               | 1                | 7         |
| <input type="checkbox"/>               | mgmt           |                               | 0                    | 0                      | 2    |                                       | 0               | 0                | 0         |

## 次のタスク

次の使用例のいずれかまたは両方を構成します。

- [ストレッチされた VRF ユース ケース \(117 ページ\)](#)
- [ルート リークの使用例 \(155 ページ\)](#)





## 第 6 章

# ストレッチされた VRF ユース ケース

- [ストレッチされた VRF ユース ケースについて \(117 ページ\)](#)
- [ストレッチされた VRF ユース ケースの構成 \(118 ページ\)](#)

## ストレッチされた VRF ユース ケースについて

ストレッチ VRF (VRF 内) は、すべてのサイト (オンプレミスおよびクラウド サイト) に関連付けられたテンプレートで単一の (共通) VRF が定義される一般的な使用例です。オンプレミス サイトとクラウド サイト間でネットワークを拡張することはできないため、オンプレミス サイトのネットワークの展開には別のテンプレートが使用されます。

同じ VRF をすべてのサイトに拡張すると、追加のルーティング構成を必要とせずに、サイト間でプレフィックスを交換できます。CIDR ブロック (クラウド VPC/VNet でサブネットをプロビジョニングするために使用) は、この拡張 VRF にマッピングされます。

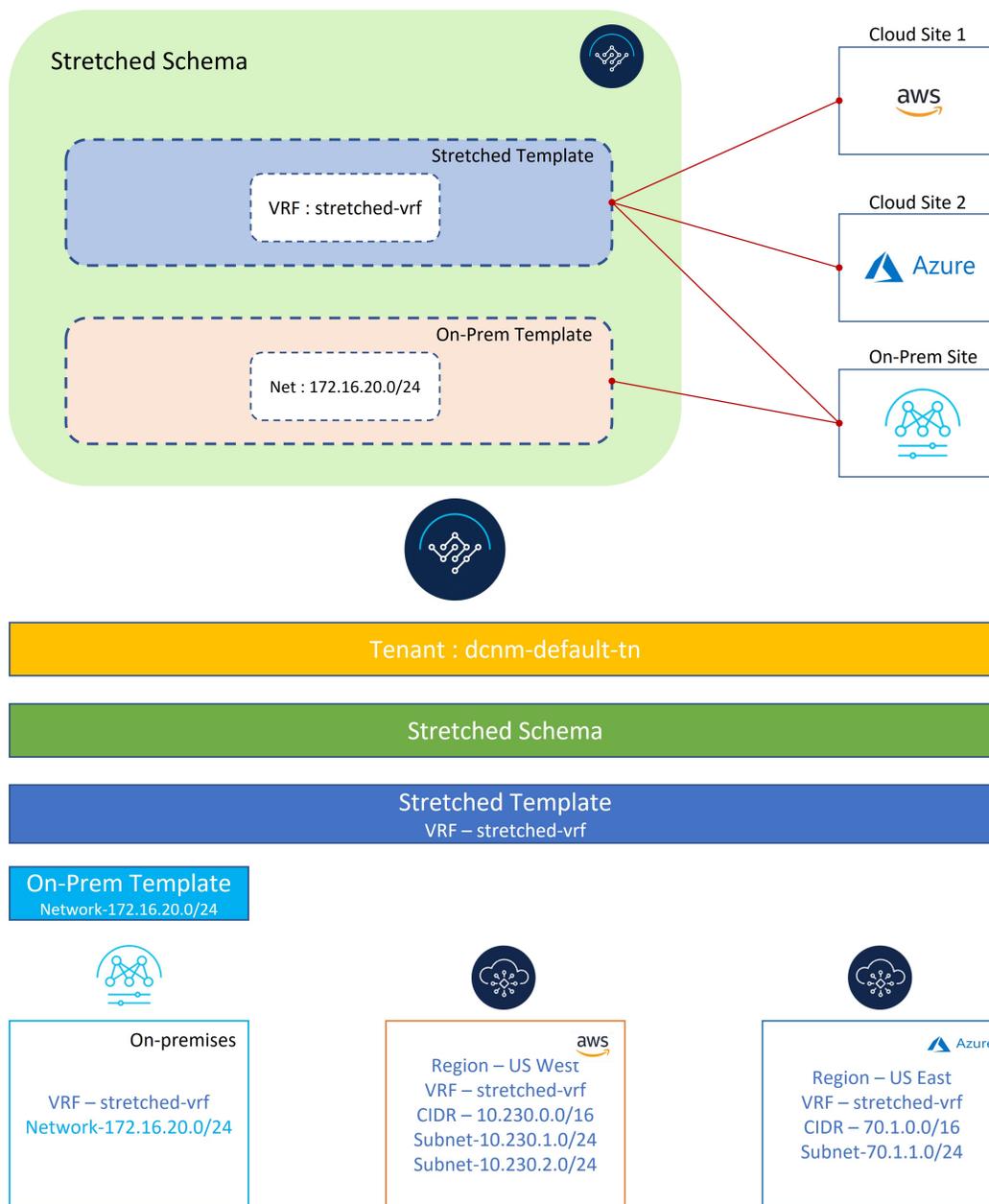


- (注) オンプレミスとクラウド サイト間、またはクラウド サイト間でのレイヤー 2 サブネットの拡張はサポートされていません。

次の図は、デモ スキーマの下で作成される 2 つのテンプレートを示しています：

- 3 つのサイトすべてに展開される VRF を定義する [ストレッチ テンプレート (Stretched Template)]。クラウド サイトの場合、VRF の下でリージョンと CIDR ブロックを定義します。
- オンプレミスの VXLAN ファブリックに展開されるネットワークを含む On\_Prem テンプレート。

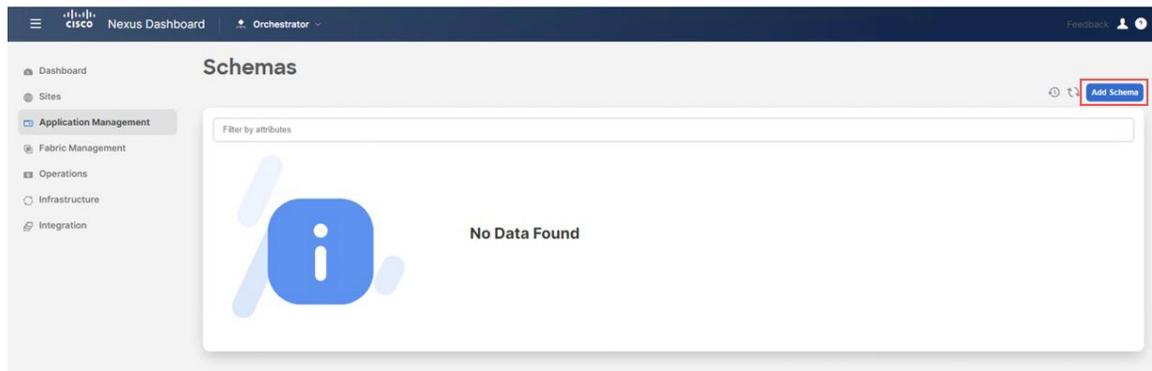
図 111:



## ストレッチされた VRF ユース ケースの構成

ステップ 1 NDO で、[アプリケーション管理 (Application Management)] > [スキーマ (Schema)] に移動し、[スキーマの追加 (Add Schema)] をクリックします。

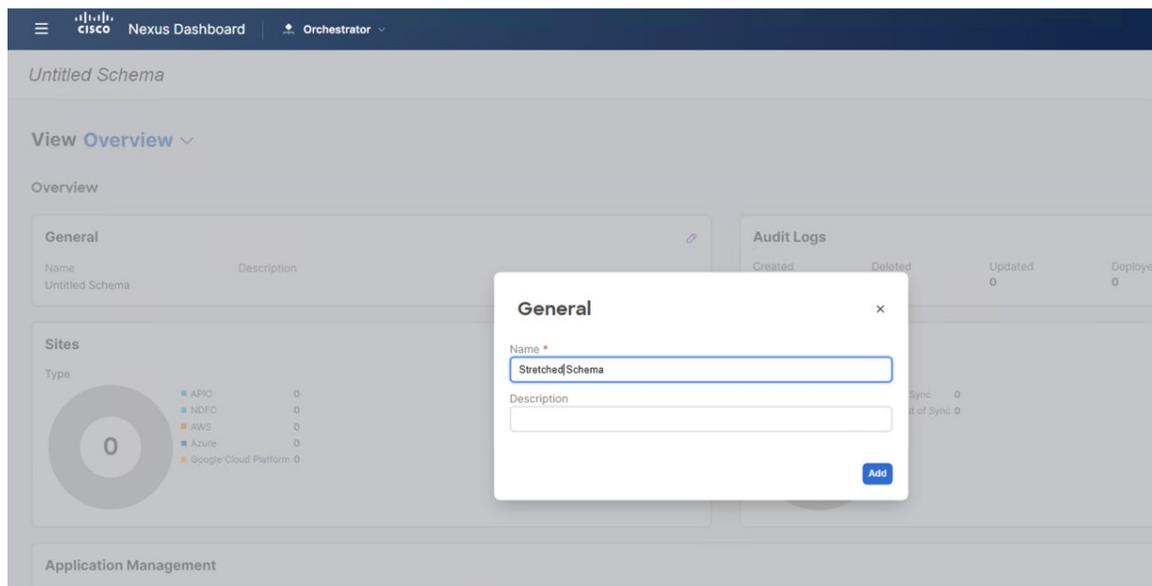
図 112:



**ステップ 2** スキーマ名を指定し、[追加 (Add)] をクリックします。

このユースケースでは、新しいスキーマに [ストレッチ スキーマ (Stretched Schema)] という名前を付けます。

図 113:

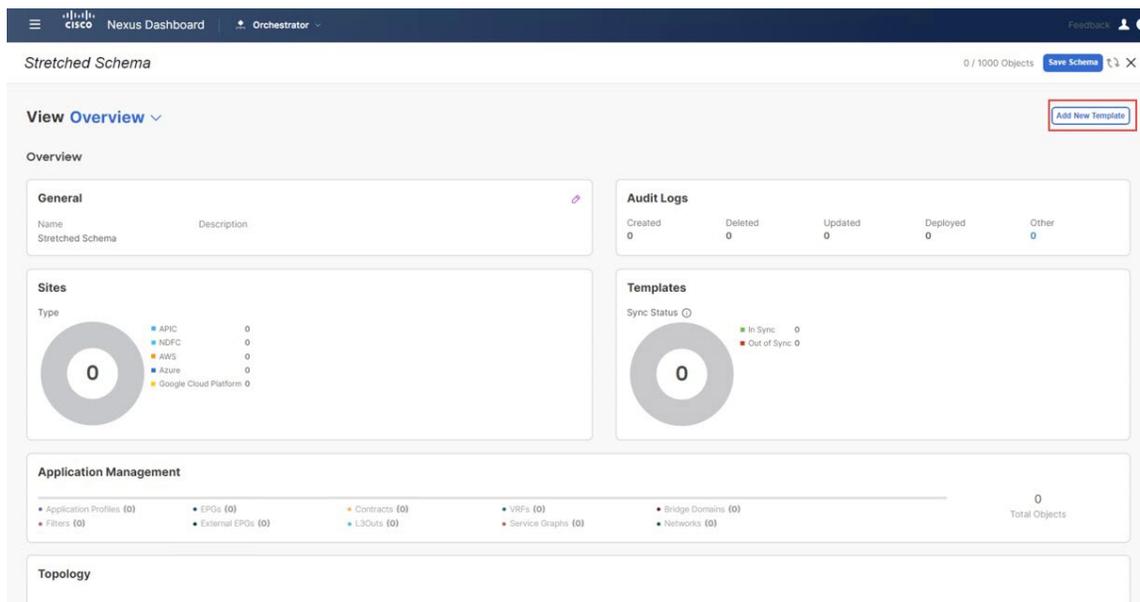


新しい [ストレッチ スキーマ (Stretched Schema)] スキーマの [概要 (Overview)] ページに戻ります。

**ステップ 3** [新しいテンプレートを追加 (Add New Template)] をクリックします。

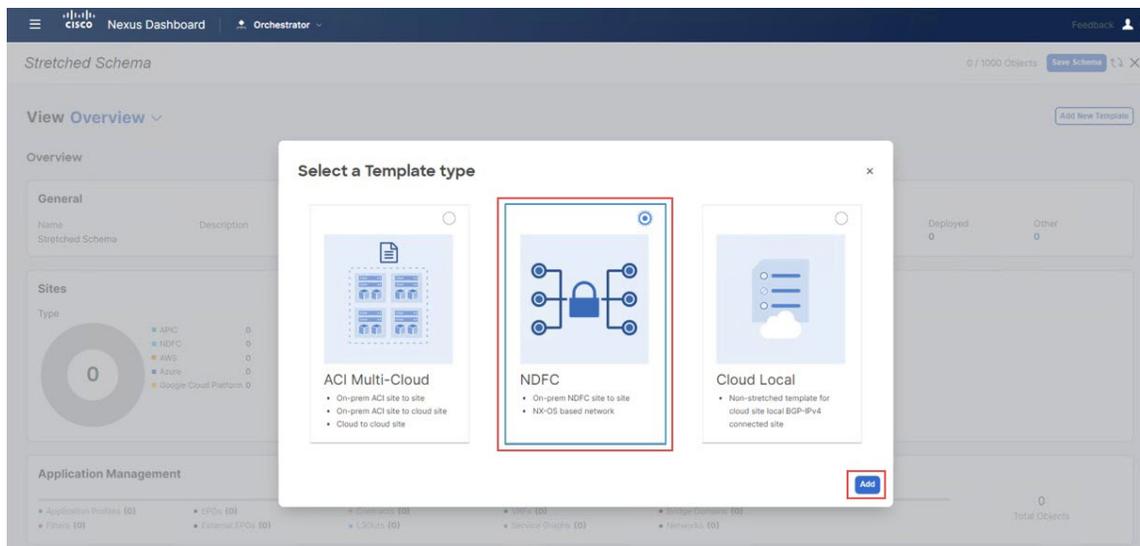
## ストレッチされた VRF ユース ケースの構成

図 114:



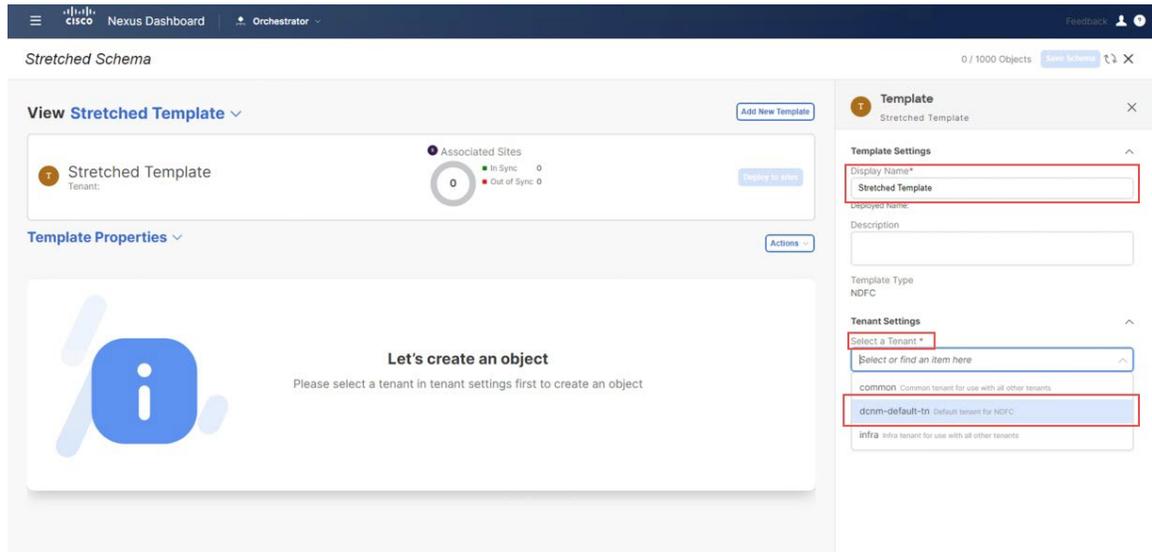
- ステップ 4** NDFC テンプレートを選択し、[追加 (Add)] をクリックします。  
 オンプレミスおよびクラウドサイトには、NDFC テンプレート タイプを使用する必要があります。

図 115:



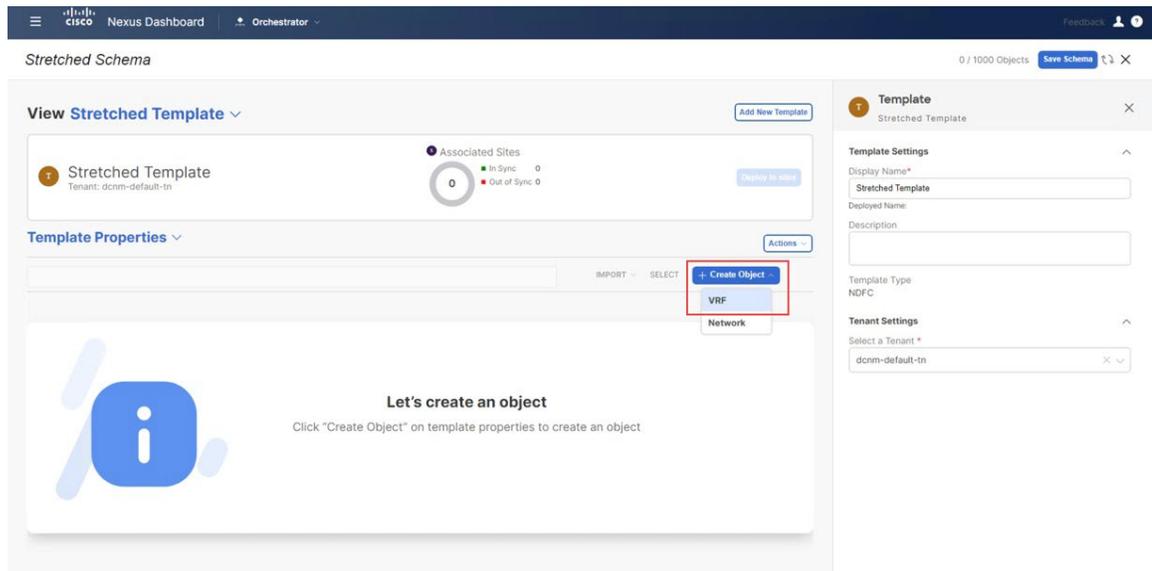
- ステップ 5** [表示名 (Display Name)] フィールドに名前を入力して NDFC タイプのテンプレート (たとえば、ストレッチされたテンプレート) を作成し、[テナントの選択 (Select a Tenant)] フィールドで dcnm-default-tn テナントを選択して、テンプレートをそのテナントにマップします。

図 116:



ステップ 6 [テンプレート プロパティ (Template Properties)] で [オブジェクトの作成 (Create Object)] をクリックし、[VRF] を選択して、全てのサイトにストレッチされた VRF を作成します。

図 117:



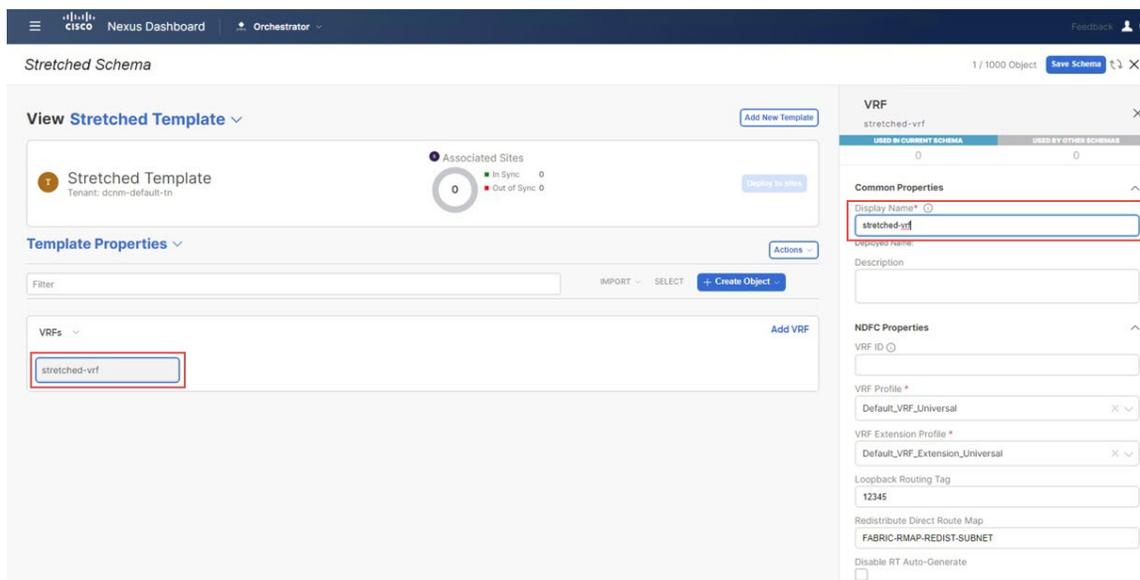
(注) 新しい VRF を作るより、既に使用したいオンプレミス VRF を作成した場合、[テンプレート プロパティ (Template Properties)] の下、[インポート (Import)] をクリックします。そして既に作成された VRF をインポートします。

現在、オンプレミスサイトからの VRF とネットワークのインポートのみがサポートされています。

## ストレッチされた VRF ユース ケースの構成

ステップ 7 ストレッチされた VRF の [表示名 (Display Name)] フィールドに名前を入力します (例: stretched-vrf)。

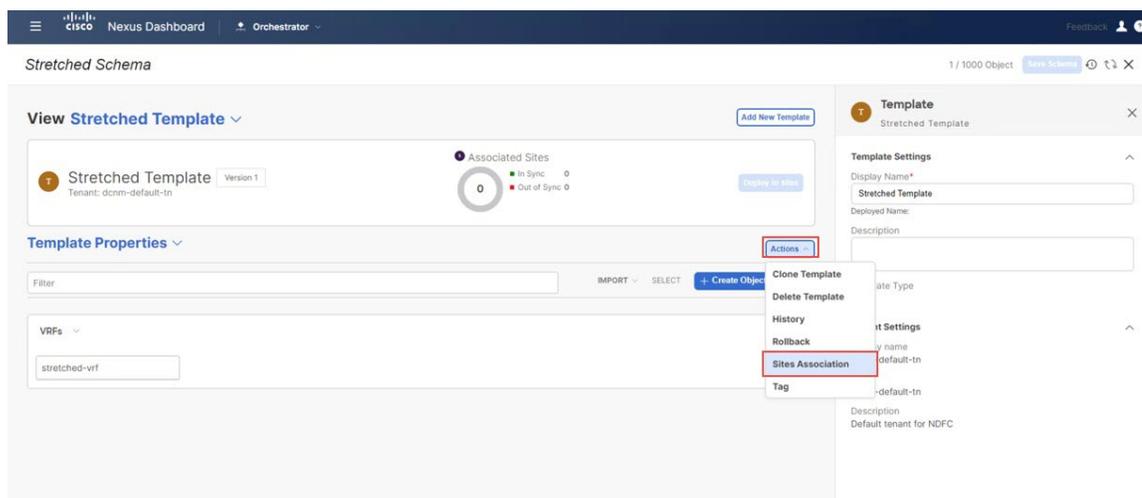
図 118:



ステップ 8 拡張 VRF ユース ケースの [ストレッチされたテンプレート (Stretched Template)] にすべてのサイト (オンプレミスおよびクラウドサイト) を関連付けます。

- a) [テンプレート プロパティ (Template Properties)] エリア内で [アクション (Actions)] > [サイトの関連付け (Sites Association)] をクリックします。

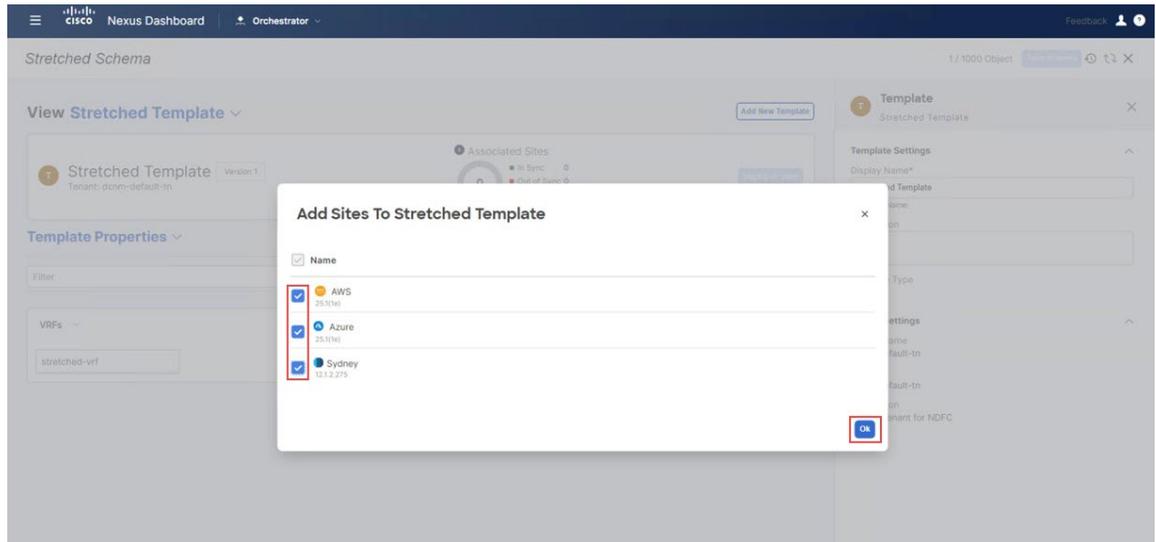
図 119:



- b) すべてのサイトを選択し、[OK] をクリックします。

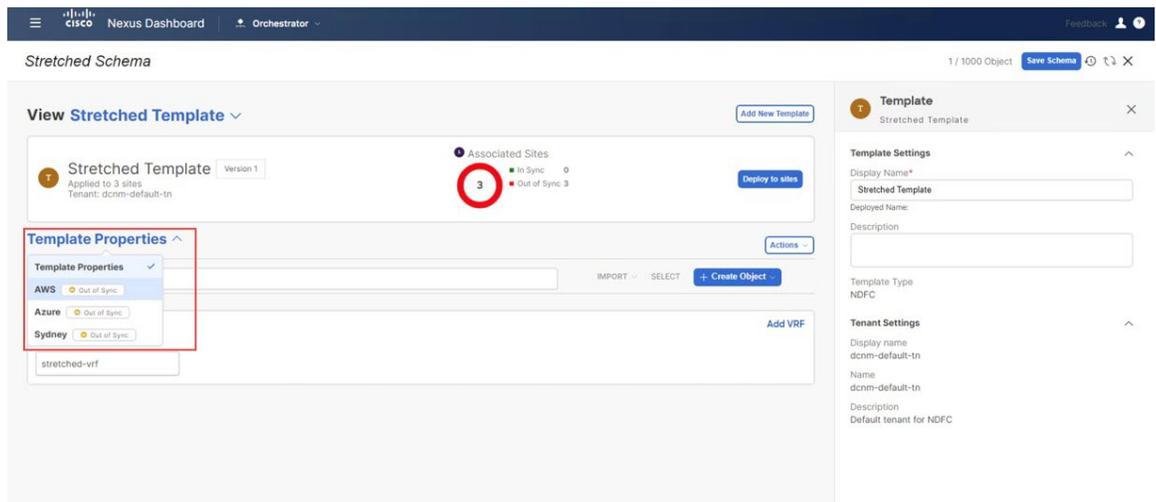
これにより、各サイトを個別に選択して、このテンプレートで定義されたオブジェクト (この特定のケースでは、拡張された VRF) のサイト レベルの構成をプロビジョニングすることもできます。

図 120:



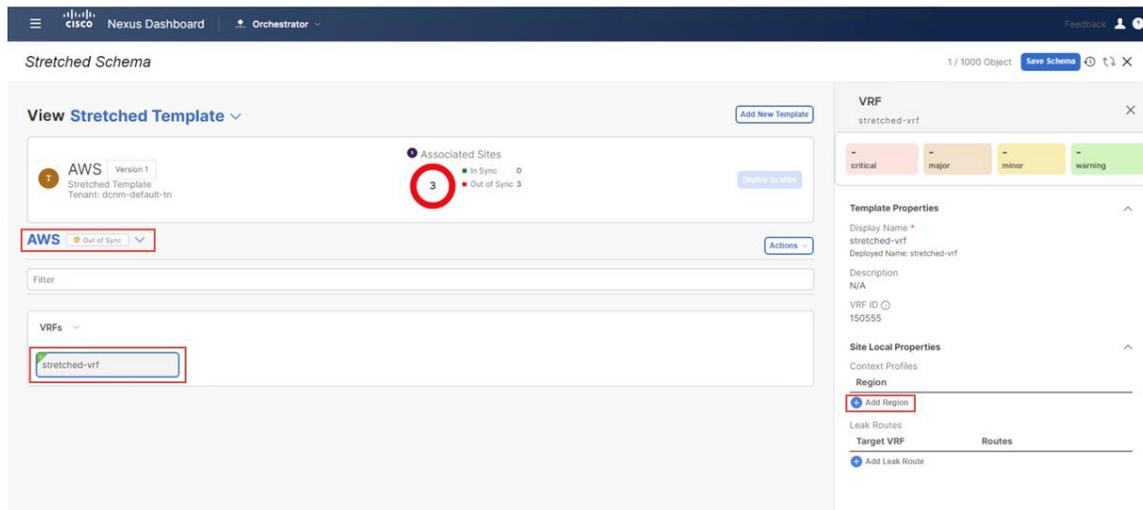
サイトがテンプレートに関連付けられると、それらは [テンプレートのプロパティ (Template Properties)] の下に表示されます。

図 121:



- ステップ 9** [テンプレートのプロパティ (Template Properties)] をクリックして最初のクラウドサイト（このユースケースの例では AWS サイト）を選択し、VRF を適切なリージョンに関連付けて VPC を作成します。
- VRF をクリックし、[リージョンの追加 (Add Region)] をクリックして、選択したリージョンに VPC を作成します。

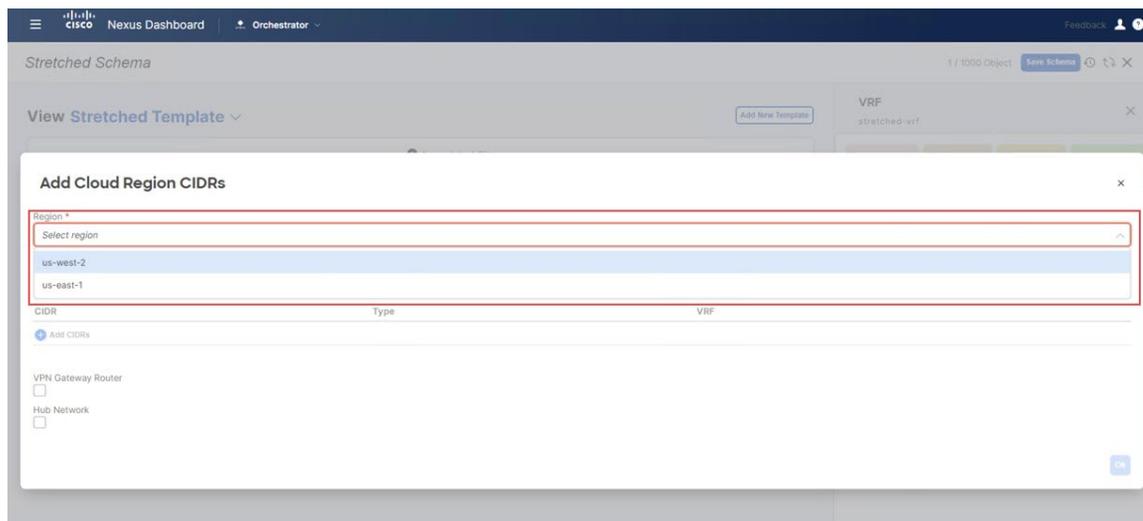
図 122:



[クラウドリージョン CIDRs を追加 (Add Cloud Region CIDRs) ウィンドウ が表示されます。

- b) [リージョン (Region) ]フィールド内で VPC を作成したいリージョンを選択します。

図 123:



- c) **CIDR**フィールド内で**[CIDR を追加 (Add CIDRs) ]**をクリックし、VPCの CIDR ブロックを定義します。
- d) サブネットを作成するためと可用性ゾーンにマップするために**[サブネットを追加 (Add Subnet) ]**をクリックし、**[保存 (Save) ]**をクリックします。

図 124:

The screenshot shows the 'Add Cloud Region CIDRs' dialog in the Cisco Nexus Dashboard Orchestrator. The 'Region' is set to 'us-west-2'. The 'Container Overlay' checkbox is unchecked. The 'CIDRs' section contains a table with the following data:

| CIDR          | Type | VRF |
|---------------|------|-----|
| 10.230.0.0/16 |      |     |

Below the table, the 'CIDR Type' is set to 'Primary'. The 'Add Subnets' table lists the following subnets:

| Subnet        | Name | Private Link Labels | Availability Zone |
|---------------|------|---------------------|-------------------|
| 10.230.1.0/24 |      |                     | us-west-2a        |
| 10.230.2.0/24 |      |                     | us-west-2b        |

The 'Add Subnet' button is highlighted. The 'Cancel' and 'Save' buttons are at the bottom.

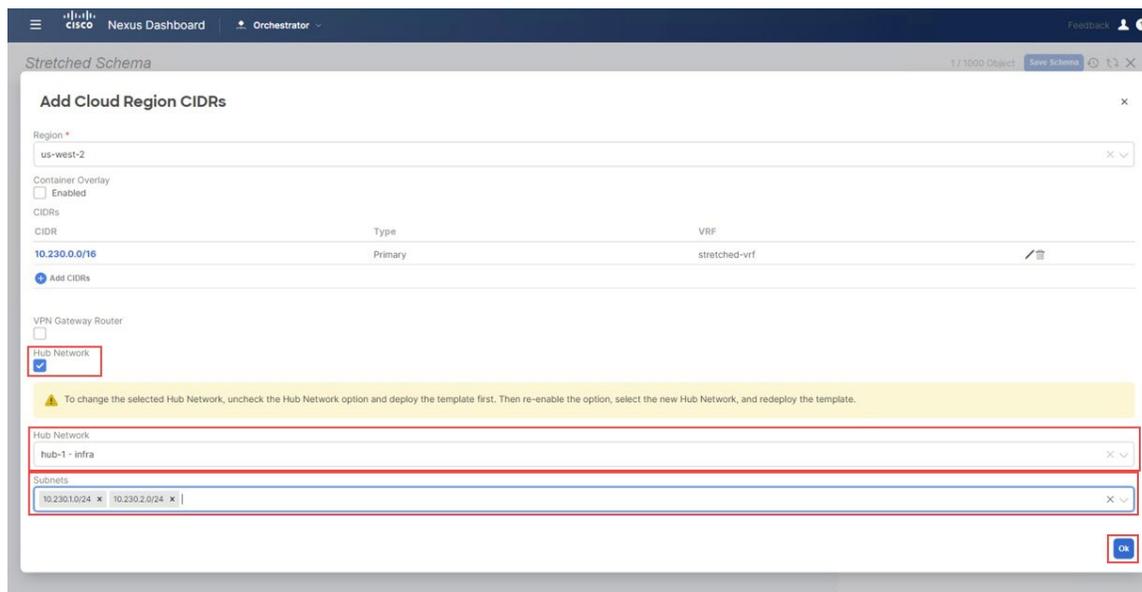
- e) **[ハブ ネットワーク (Hub Network)]** フィールドの下にあるチェックボックスをオンにして、AWS 用の Cisco クラウド ネットワーク コントローラで作成されたハブ ネットワークを選択します。

Cisco クラウド ネットワーク コントローラがサブネットをトランジット ゲートウェイに付加することを許可します。これは、トランジット ゲートウェイが既に接続のあるサブネットからクラウド上の Cisco Catalyst 8000Vs にトランジット ゲートウェイに接続を積み上げます。

- f) **[サブネット (Subnet)]** フィールド内でトランジット ゲートウェイに使われるサブネットをマップします。

トランジット ゲートウェイに専用のサブネットを使用するのがベストプラクティスです。

図 125:



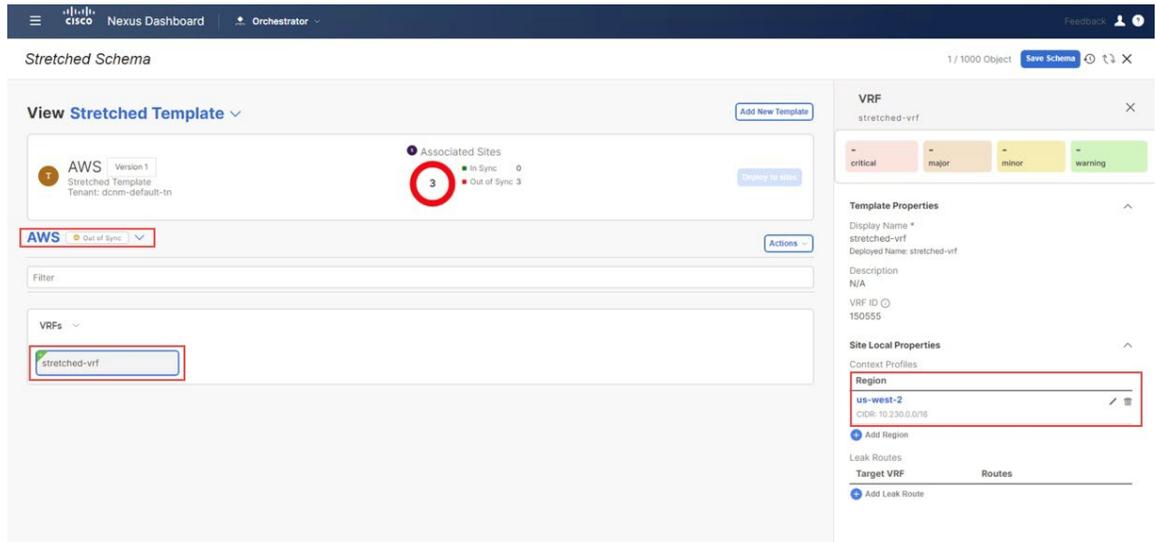
(注) または、ハブネットワーク（TGW）への接続に、アベイラビリティゾーンごとに専用の /25 サブネットを使用できます。これにより、エンドポイントサブネット全体をエンドホストに使用できるようになります。

g) [OK] をクリックします。

AWS テンプレート ウィンドウに戻ります。

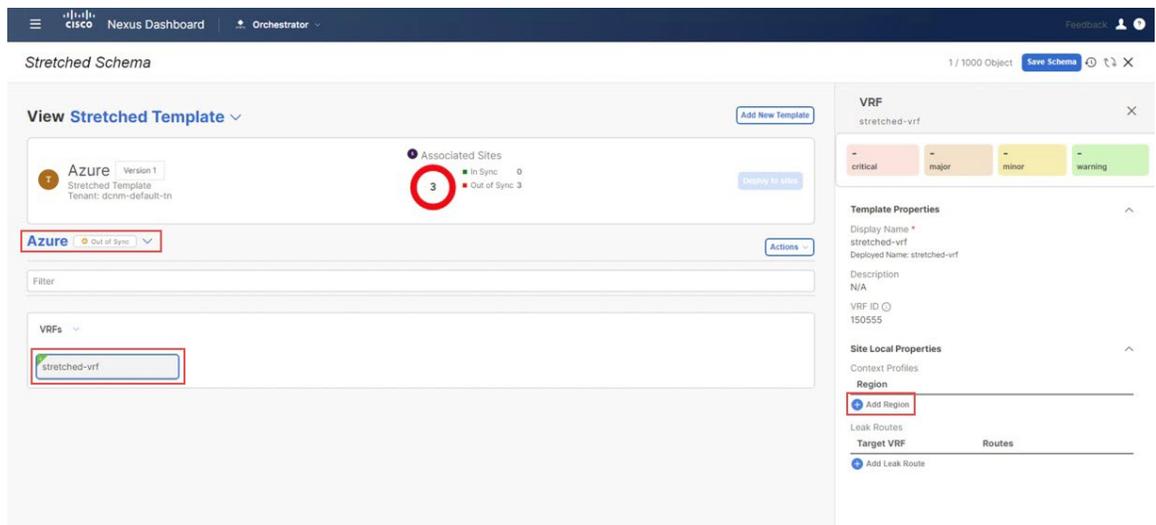
この構成が展開されると、CIDR 10.230.0.0/16 の VPC が AWS クラウドに作成され、us-west-2a と us-west-2b の可用性ゾーンにまたがり、10.230.1.0/24 と 10.230.2.0/24 サブネットがそれぞれ作成されます。

図 126:



- ステップ 10 [テンプレートのプロパティ (Template Properties)] をクリックして 2 番目のクラウドサイト (このユースケースの例では Azure サイト) を選択し、VRF を適切なリージョンに関連付けて VNet を作成します。
- VRF をクリックし、[リージョンの追加 (Add Region)] をクリックして、選択したリージョンに VNet を作成します。

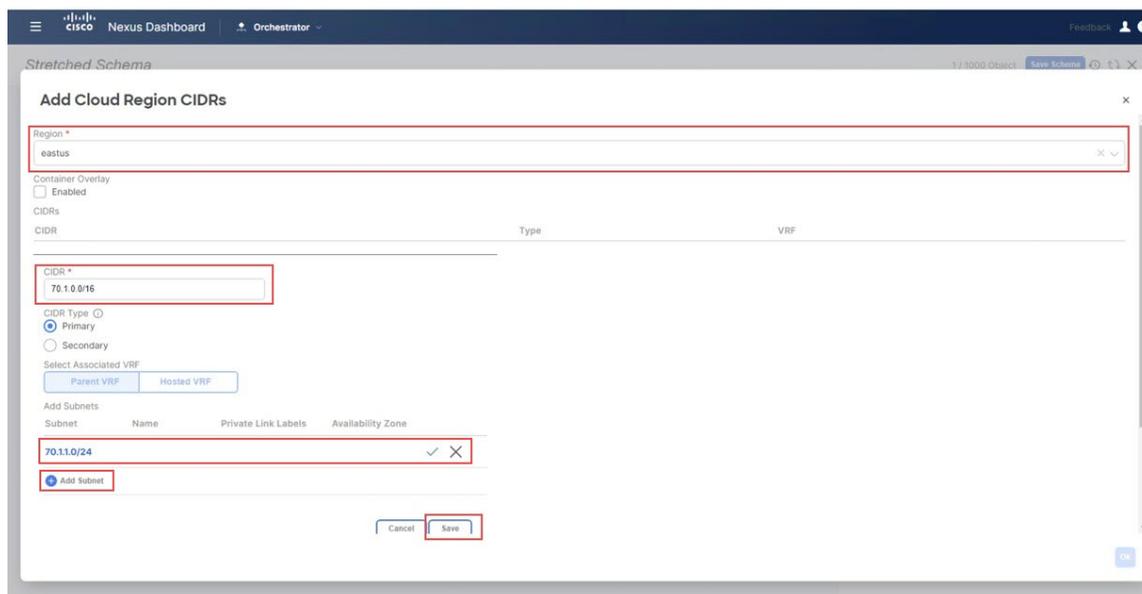
図 127:



- [クラウドリージョン CIDRs を追加 (Add Cloud Region CIDRs)] ウィンドウが表示されます。
- [リージョン (Region)] フィールド内で VNet を作成したいリージョンを選択します。
  - CIDR フィールド内で [CIDR を追加 (Add CIDRs)] をクリックし、VNet の CIDR ブロックを定義します。
  - サブネットを作成するために [サブネットを追加 (Add Subnet)] をクリックし、[保存 (Save)] をクリックします。

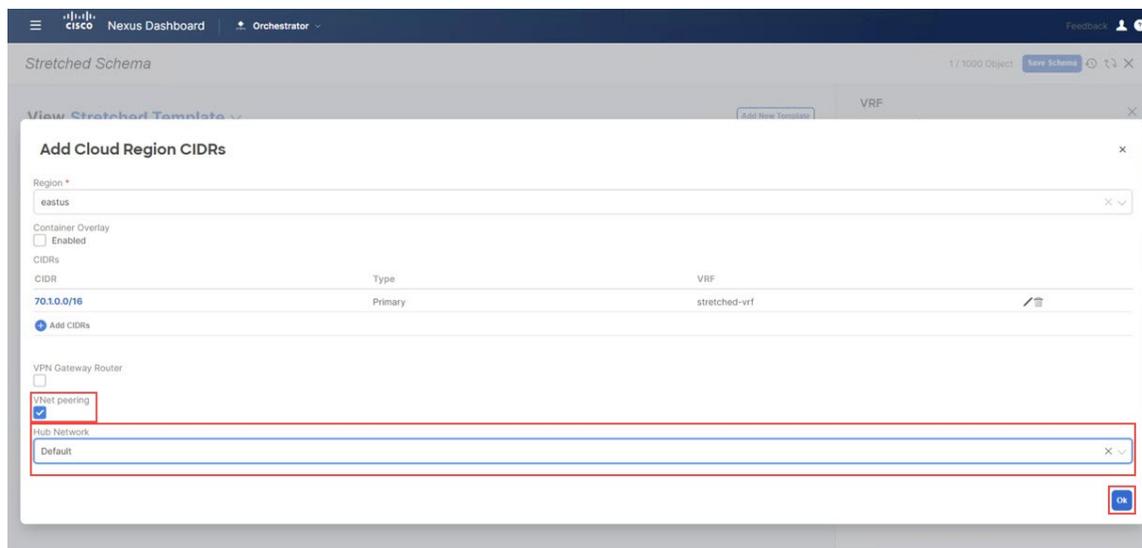
## ストレッチされた VRF ユース ケースの構成

図 128:



- e) [VNet ピアリング (VNet Peering)] フィールドの下にあるチェックボックスをオンにして、Azure 用の Cisco クラウドネットワーク コントローラで作成された [デフォルト (Default)] ハブ ネットワークを選択します。

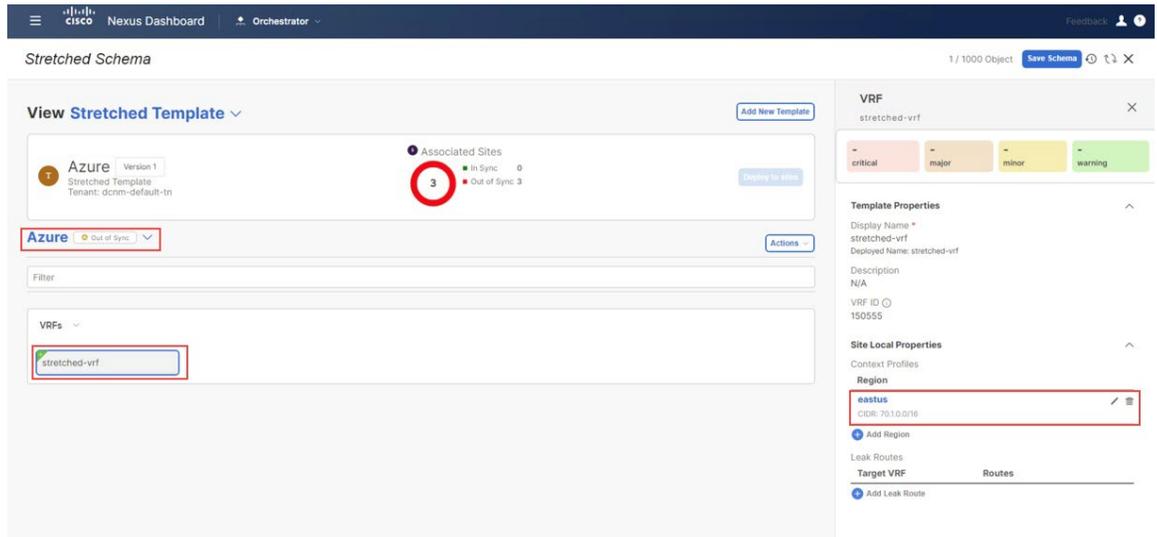
図 129:



- f) [OK] をクリックします。

この構成が展開されると、構成した VNet (この例では 70.1.0.0/16) が Azure の適切なリージョン (この例では eastus Azure リージョン) に作成され、VNet ピアリングが Azure のインフラ テナント内のインフラ VNet に構成されます。

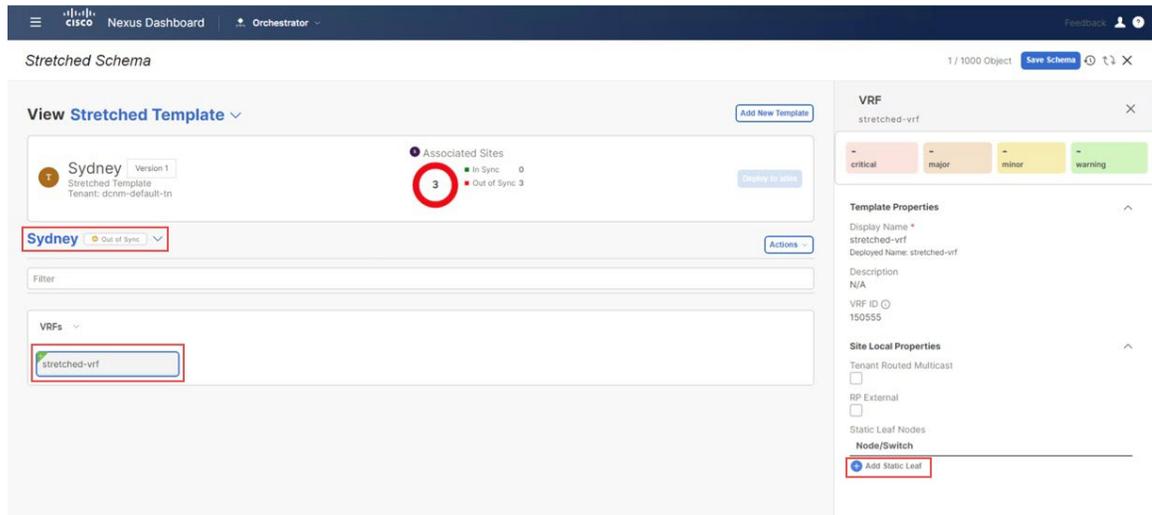
図 130:



ステップ 11 [テンプレート プロパティ (Template Properties)] をクリックし、オンプレミス サイト (このユース ケースの例では シドニー サイト) を選択してから、stretched-vrf VRF を選択します。

ステップ 12 右側のペインで [静的リーフの追加 (Add Static Leaf)] をクリックします。

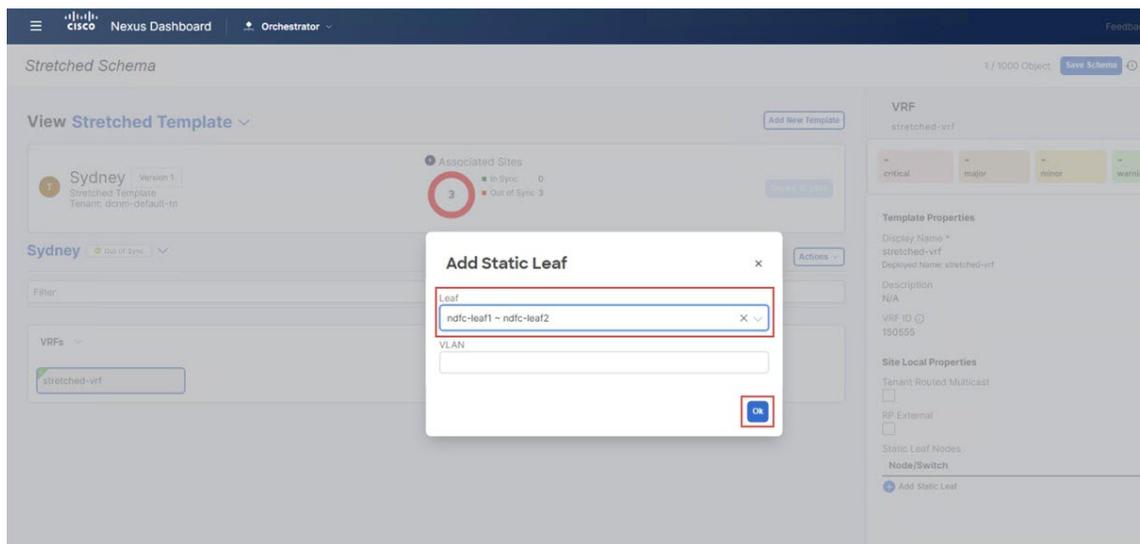
図 131:



[静的リーフの追加 (Add Static Leaf)] ウィンドウが表示されます。

ステップ 13 [リーフ (Leaf)] フィールド内で、VRF が展開されるべき場所のリーフ/ボーダー/ボーダーゲートウェイ デバイスを選択し、Ok をクリックします。

図 132:

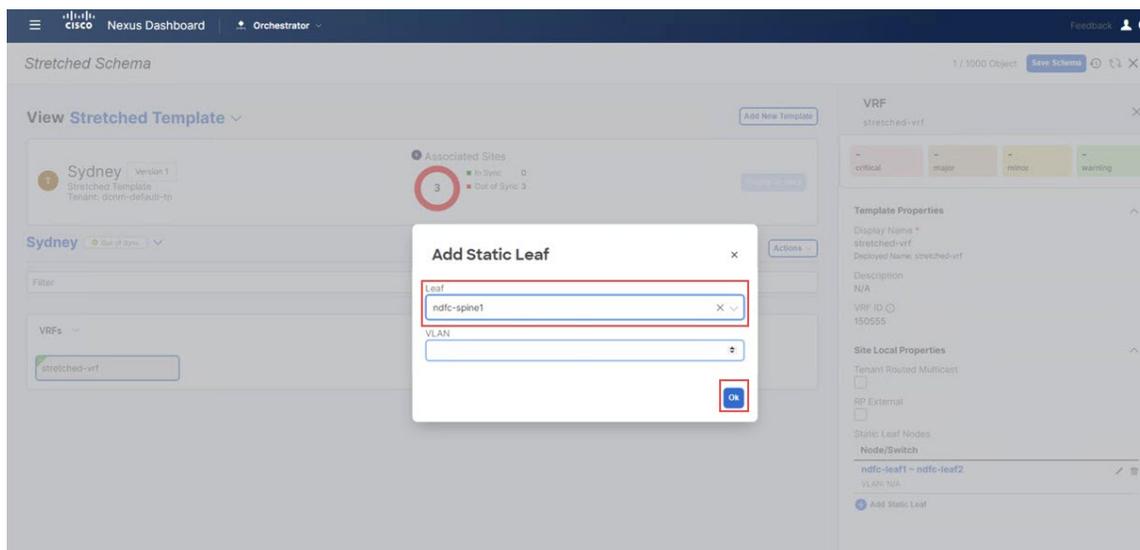


[ストレッチされたテンプレート (Stretched Template) ] ページに戻ります。

**ステップ 14** [静的リーフの追加 (Add Static Leaf) ] を再度クリックして、この VRF が展開される追加のリーフ/境界/境界ゲートウェイ デバイスを追加します。

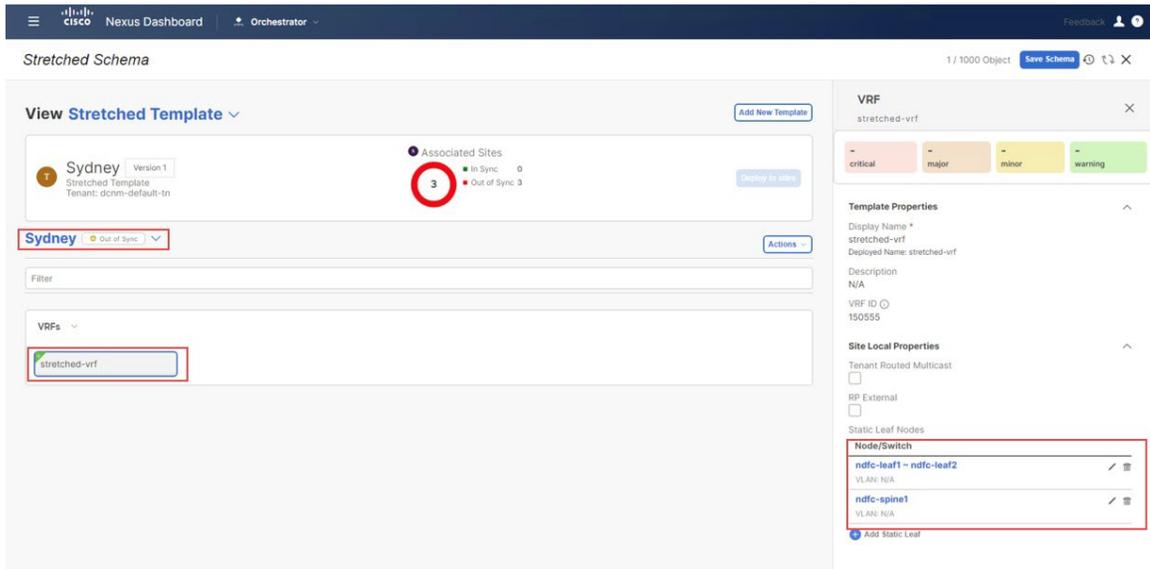
この例では、リーフ ノードに VRF を展開する必要があります (VRF にマップされたネットワークのエンドポイントに接続される)。そして、VRF からクラウドサイトへのレイヤー 3 接続に拡張するために BGW スパイン ノードを展開する必要があります。

図 133:



この VRF が展開されるすべてのリーフ/ボーダー/ボーダー ゲートウェイ デバイスを追加すると、[ストレッチされたテンプレート (Stretched Template) ] ページに表示されます。

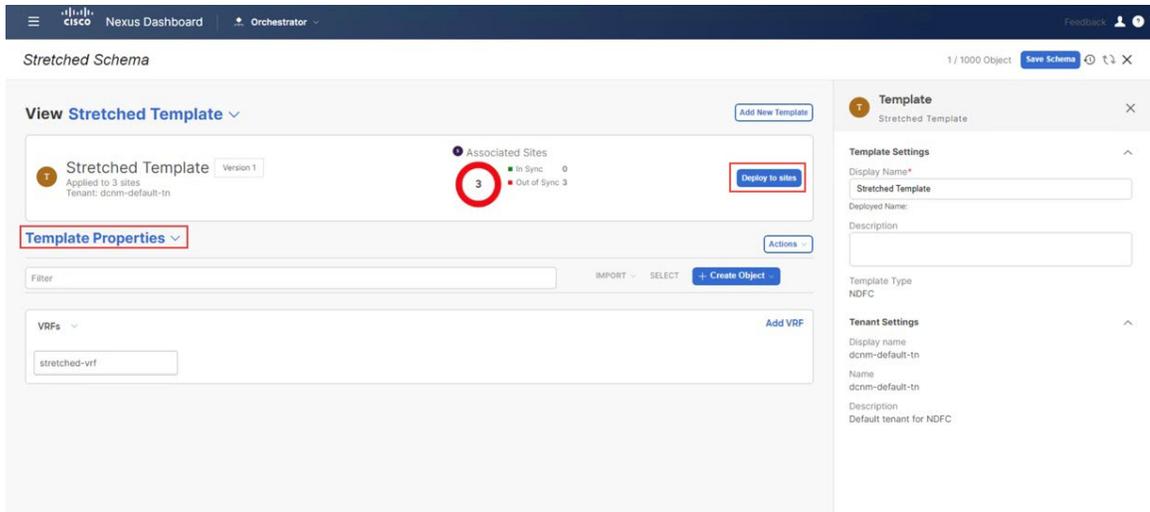
図 134:



ステップ 15 シドニーサイトの横にある矢印をクリックし、ドロップダウンメニューから[テンプレートのプロパティ (Template Properties)]を選択します。

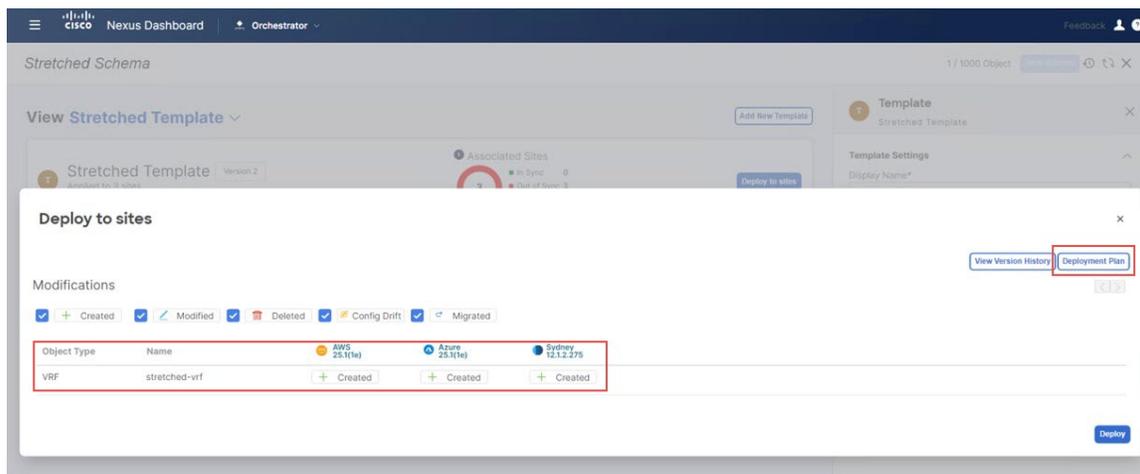
ステップ 16 [サイトに展開 (Deploy to sites)]をクリックします。

図 135:



[サイトに展開 (Deploy to Sites)] ウィンドウが表示され、拡張されたテンプレートが展開される 3 つのサイトが表示されます。

図 136:



ステップ 17 [展開プラン (Deployment Plan)] を追加認証のためにクリックします。そして、その特定のサイトの展開プランを表示するために各サイトをクリックします。

図 137:

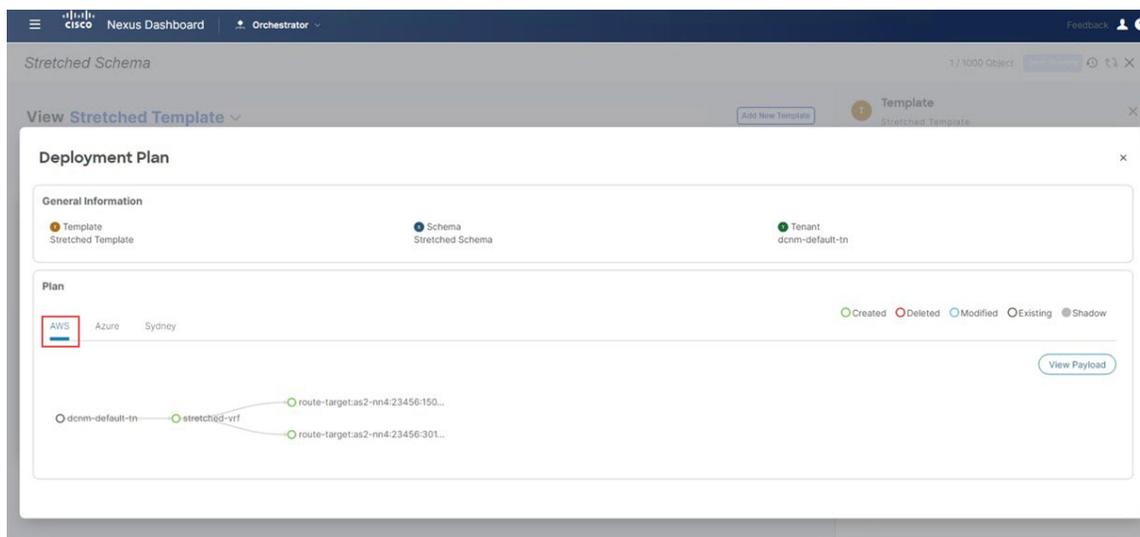


図 138:

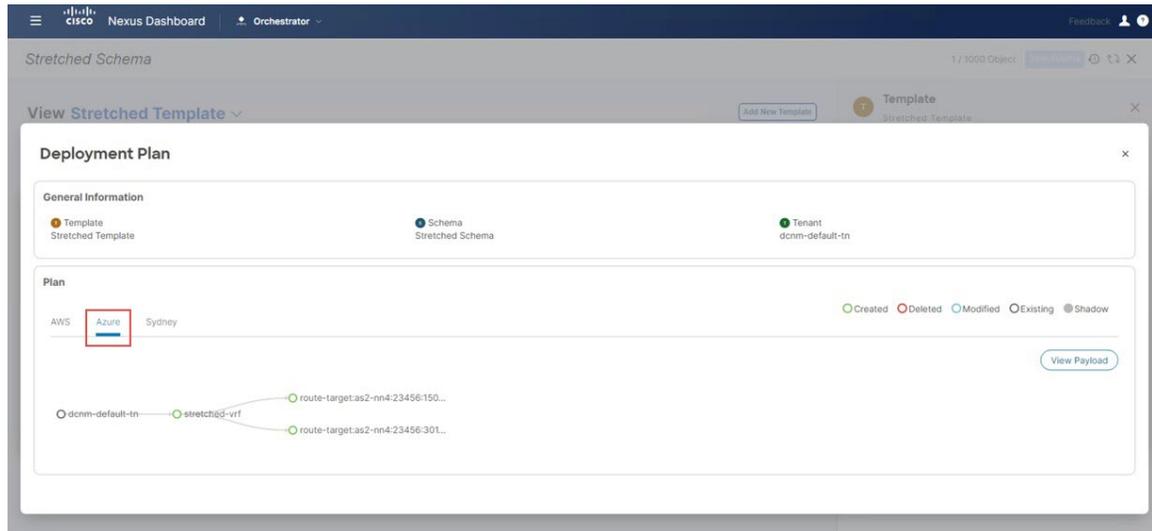
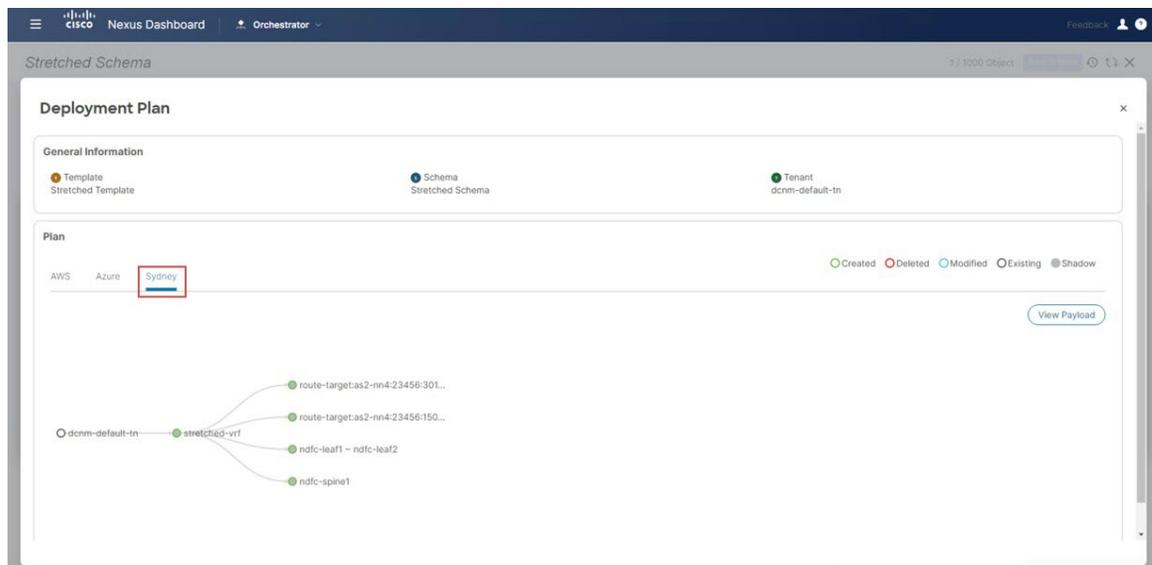
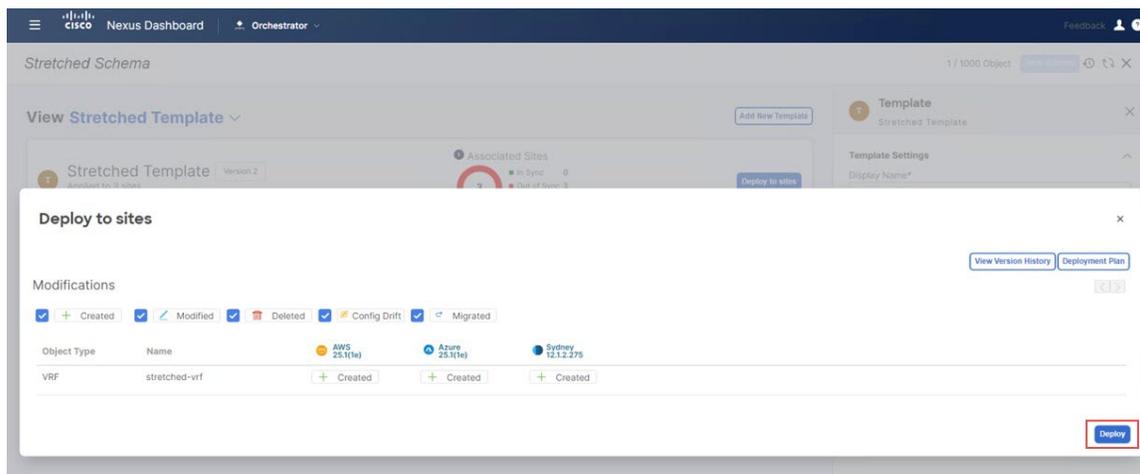


図 139:



ステップ 18 [展開 (Deploy)] を NDO が構成をサイト固有のコントローラ (NDFC とクラウド ネットワーク コントローラ) にプッシュするためにクリックします。

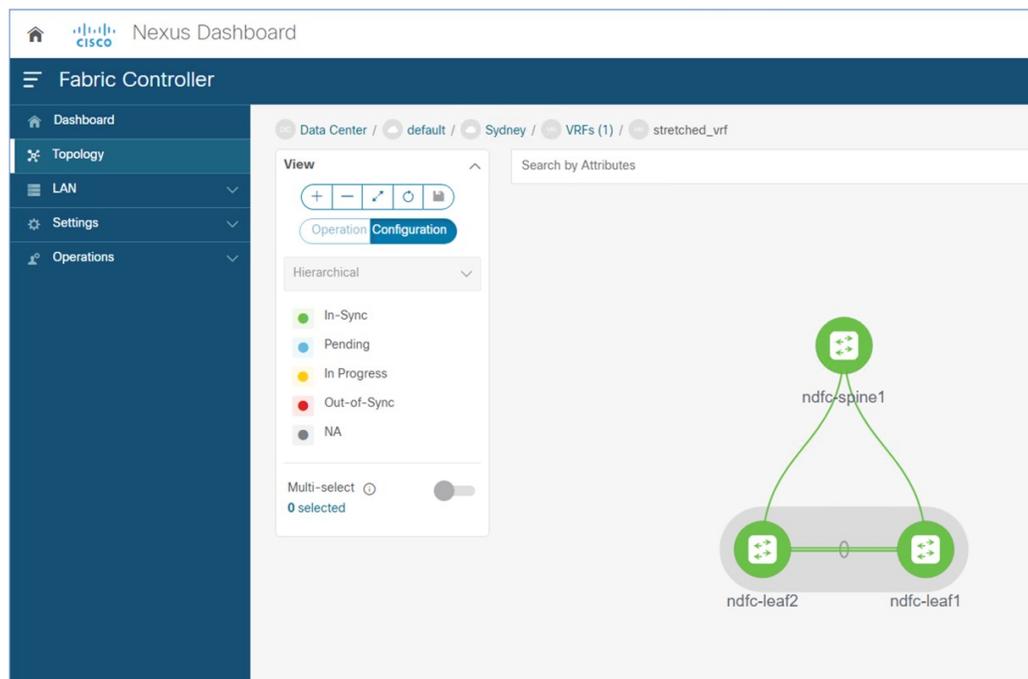
図 140:



ステップ 19 構成が正常に展開されたことを確認します。

- NDFC での VRF 展開を表示するには、[トポロジ (Topology)] ビューに移動し、オンプレミス ファブリックの[シドニー (Sydney)] > VRF を選択してから、stretched-vrf を選択します。

図 141:



- AWS に展開されたクラウドネットワークコントローラに接続して、最初のクラウドサイト (AWS) の構成が正常に展開されたことを確認します。

[アプリケーション管理 (Application Management)] > VRF に移動し、stretched-vrf を見つけて、列 VPC をクリックしてから、[概要 (Overview)] ページに移動して、[サブネット (Subnets)] をクリックします。

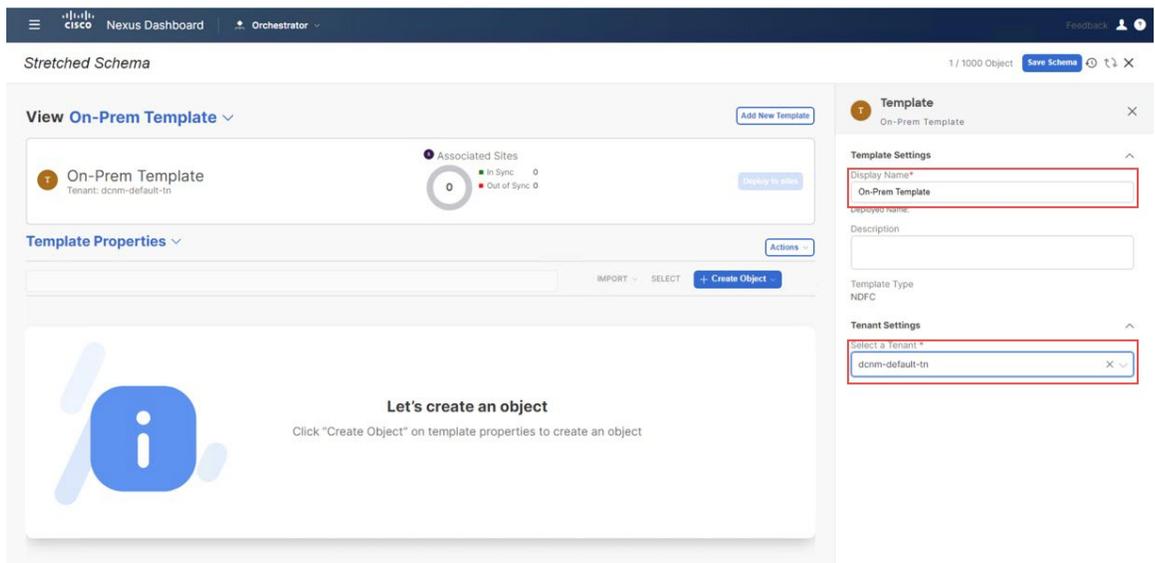
- Azure に展開されたクラウド ネットワーク コントローラに接続して、2 番目のクラウド サイト (Azure) の構成が正常に展開されたことを確認します。

[アプリケーション管理 (Application Management)] > VRF に移動し、stretched-vrf を見つけて、列 [仮想ネットワーク (Virtual Networks)] をクリックしてから、[概要 (Overview)] ページに移動して、[サブネット (Subnets)] をクリックします。

**ステップ 20** オンプレミス サイトにネットワークを展開するために、[デモ スキーマ (Demo Schema)] の下に別のテンプレートを作成します。

- [デモ スキーマ (Demo Schema)] テンプレートで、[新しいテンプレートの追加 (Add New Template)] をクリックします。
- NDFC テンプレートを選択します。
- [表示名 (Display Name)] フィールドに名前を入力して NDFC タイプのテンプレート (たとえば、On-Prem テンプレート) を作成し、[テナントの選択 (Select a Tenant)] フィールドで dcnm-default-tn テナントを選択して、テンプレートをそのテナントにマップします。

図 142:

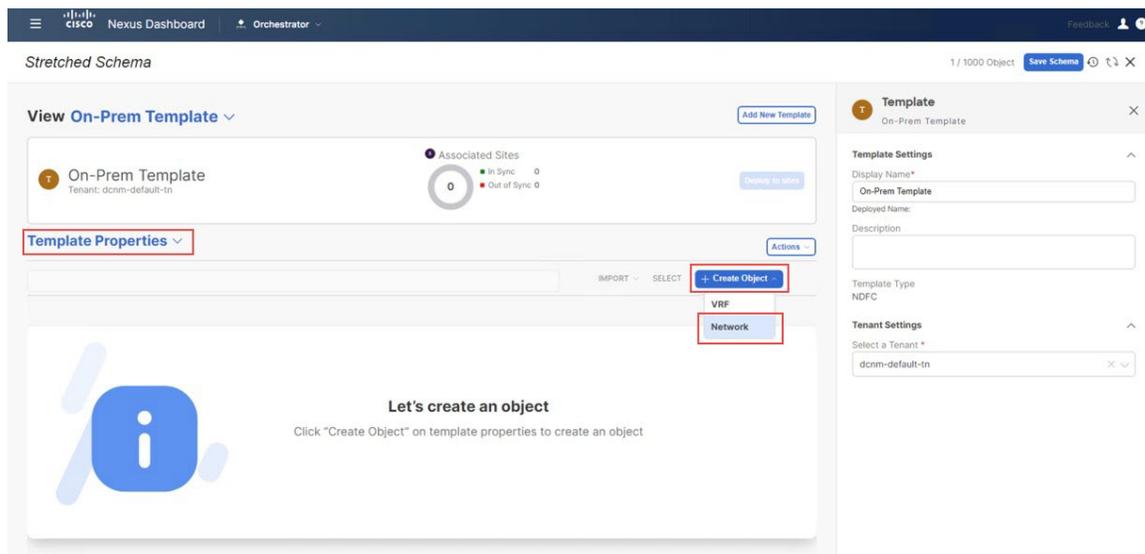


**ステップ 21** On-Prem テンプレートの VRF の下に net20 ネットワークを作成します。

(注) 新しい VRF を作るより、既に使用したい VRF を作成した場合、[テンプレート プロパティ (Template Properties)] の下、[インポート (Import)] をクリックします。そして既に作成された ネットワーク をインポートします。

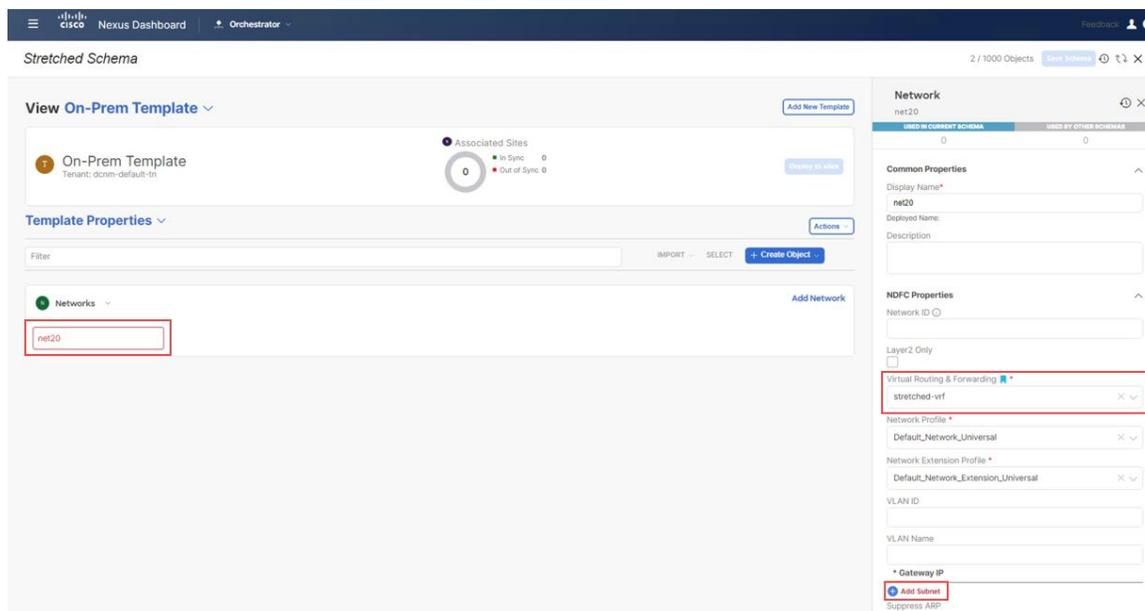
- [テンプレート プロパティ (Template Properties)] の下、[オブジェクトを作成 (Create Object)] をクリックしてネットワークを作成するために [ネットワーク (Network)] を選択します。

図 143:



- b) ネットワークの [表示名 (Display Name)] フィールドに名前を入力します (例: net20)。
- c) [バーチャル ルートと転送 (Virtual Routing & Forwarding)] フィールドで、stretched-vrf VRF を選択して、net20 をその VRF にマッピングします。

図 144:

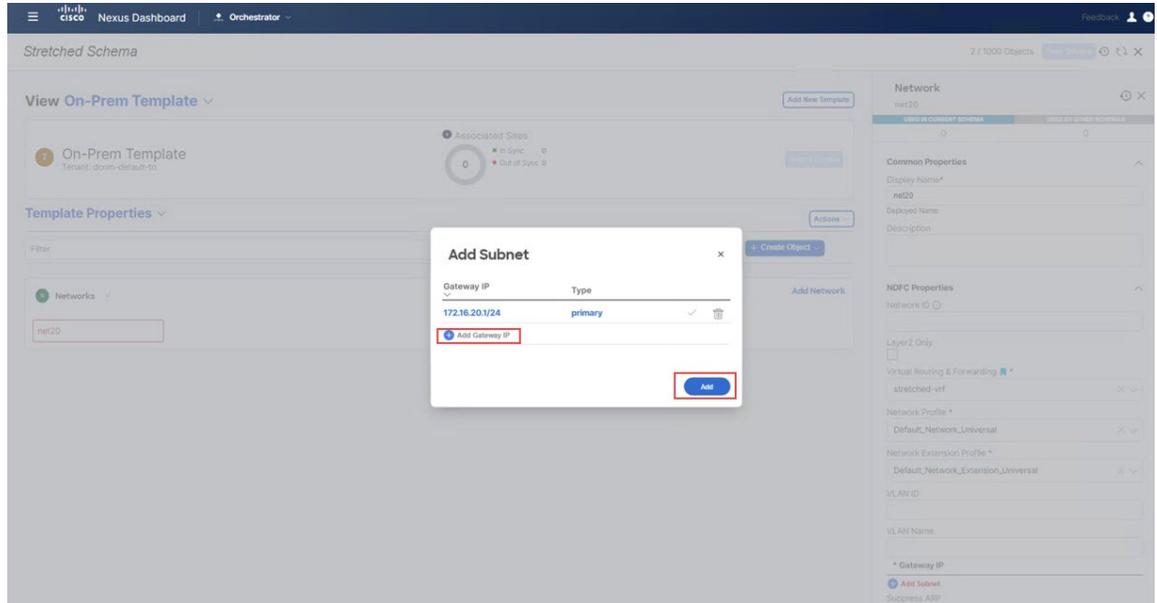


- d) [ゲートウェイ IP (Gateway IP)] フィールドで、[サブネットの追加 (Add Subnet)] をクリックします。

サブネットの追加ウィンドウが表示されます。

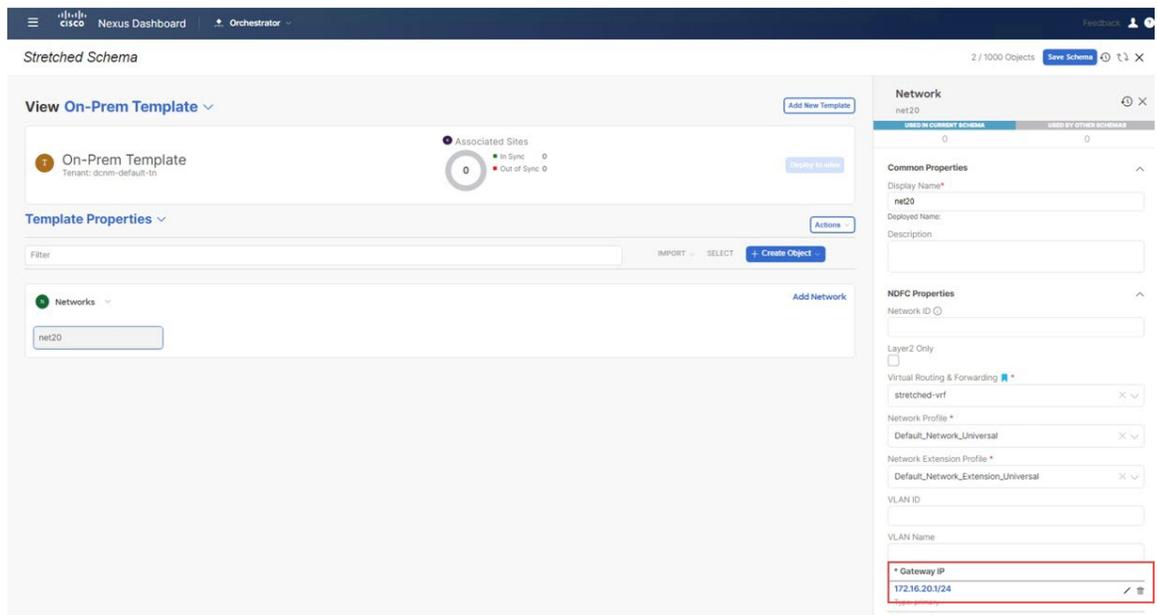
- e) [ゲートウェイ IP の追加 (Gateway IP)] をクリックしてゲートウェイ IP アドレスを入力し、チェックマークをクリックして値を受け入れ、[追加 (Add)] をクリックします。

図 145:



ゲートウェイ IP アドレスは[ゲートウェイ IP (Gateway IP)] フィールドに表示されます。

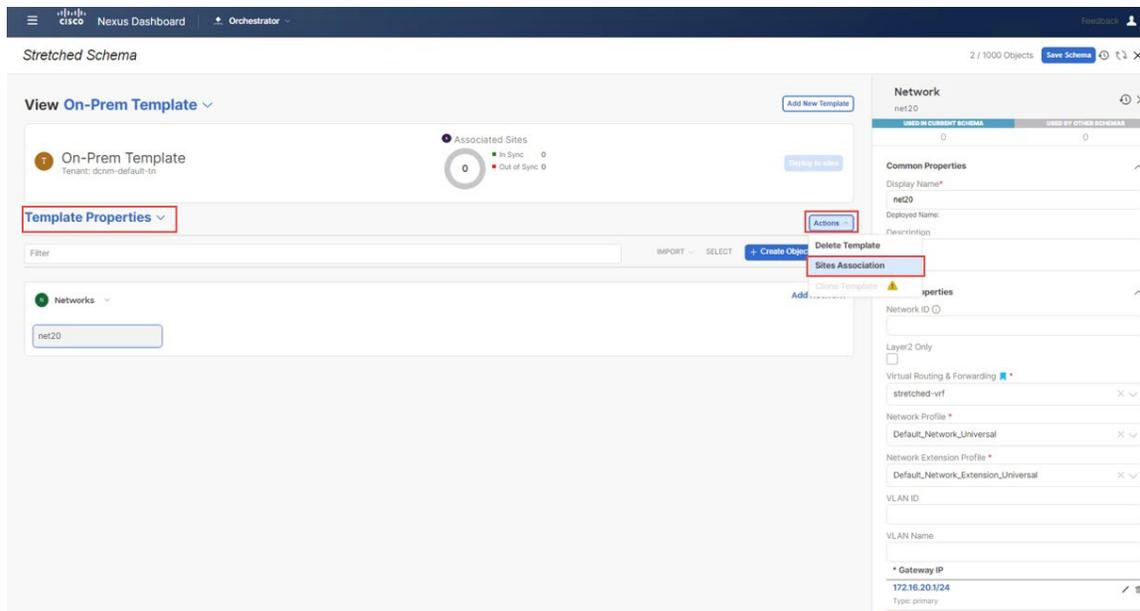
図 146:



- f) 必要な場合、ネットワークのオプション パラメータを定義します。

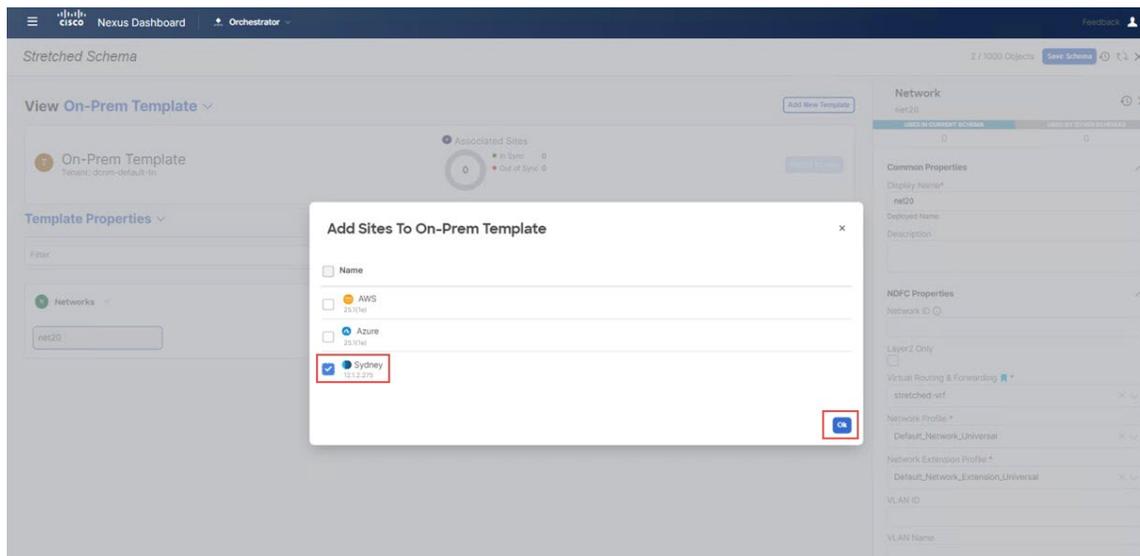
ステップ 22 [テンプレート プロパティ (Template Properties)] エリア内で [アクション (Actions)] > [サイトの関連付け (Sites Association)] をクリックします。

図 147:



ステップ 23 このテンプレートをオンプレミス サイト (このユース ケースの例ではシドニー サイト) にのみ関連付け、[OK] をクリックします。

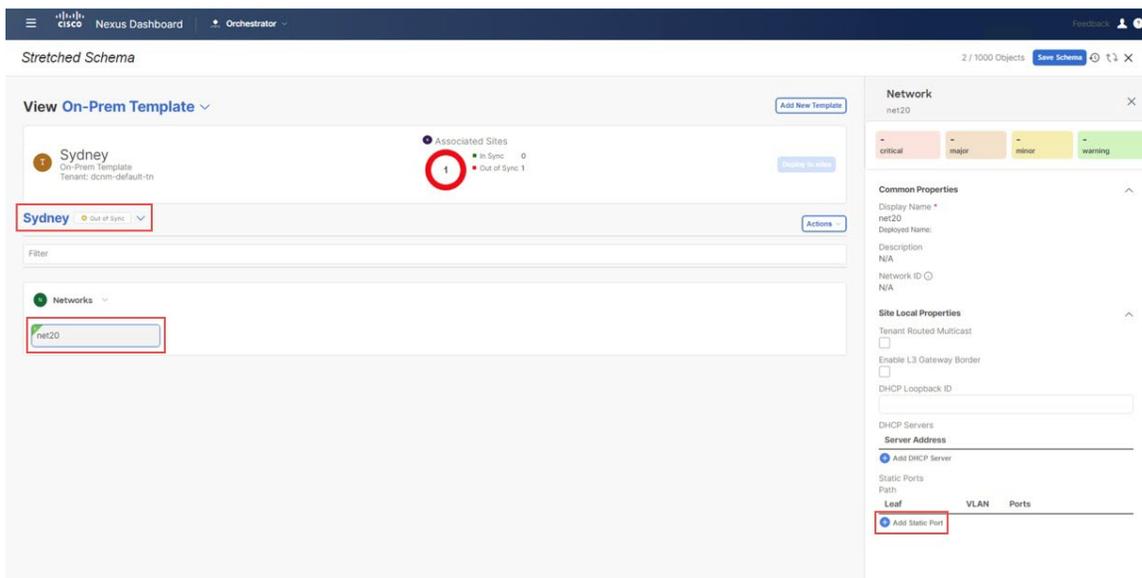
図 148:



[On-Prem テンプレート (On-Prem Template) ウィンドウに戻ります。

ステップ 24 [テンプレート プロパティ (Template Properties)] ドロップダウンから、オンプレミス サイト (このユースケースの例ではシドニー サイト) を選択し、net20 ネットワークをクリックしてから、[静的ポートの追加 (Add Static Port)] をクリックして、このネットワークを展開するポートを追加します。[静的ポートの追加 (Add Static Port)] ウィンドウが表示されます。

図 149:



ステップ 25 [静的ポートの追加 (Add Static Port)] ウィンドウで[パスを追加 (Add Path)] をクリックします。[静的ポートの追加 (Add Static Port)] ウィンドウが表示されます。

ステップ 26 [リーフ (Leaf)] フィールドで展開したいネットワークのデバイスを選択します。

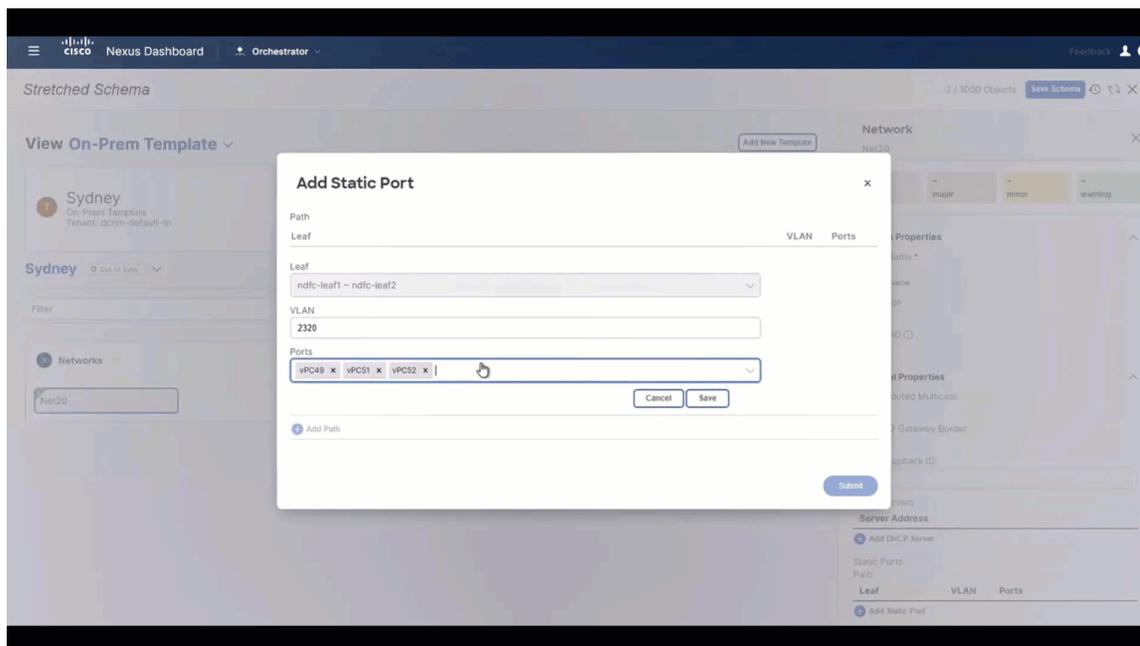
ステップ 27 (任意) VLAN フィールドに必要な情報を入力します。

ステップ 28 [ポート (Port)] フィールドで展開したいネットワークのポートを選択します。

ステップ 29 [保存 (Save)] をクリックします。

## ストレッチされた VRF ユース ケースの構成

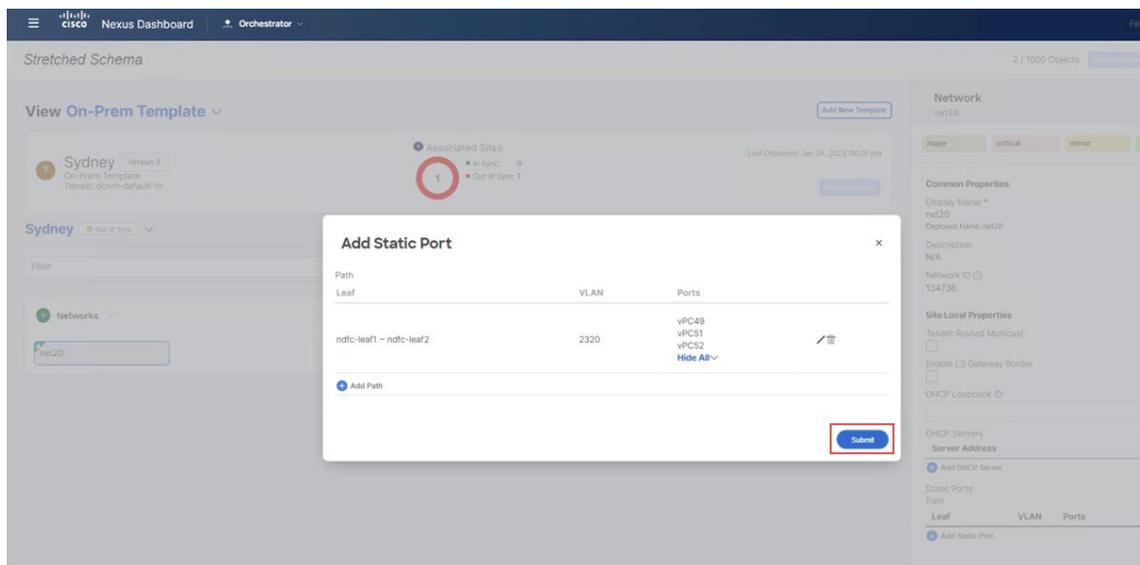
図 150:



[静的ポートの追加 (Add Static Port)] ウィンドウに戻ります。

ステップ 30 [静的ポートの追加 (Add Static Port)] ウィンドウで[送信 (Submit)] をクリックします。

図 151:

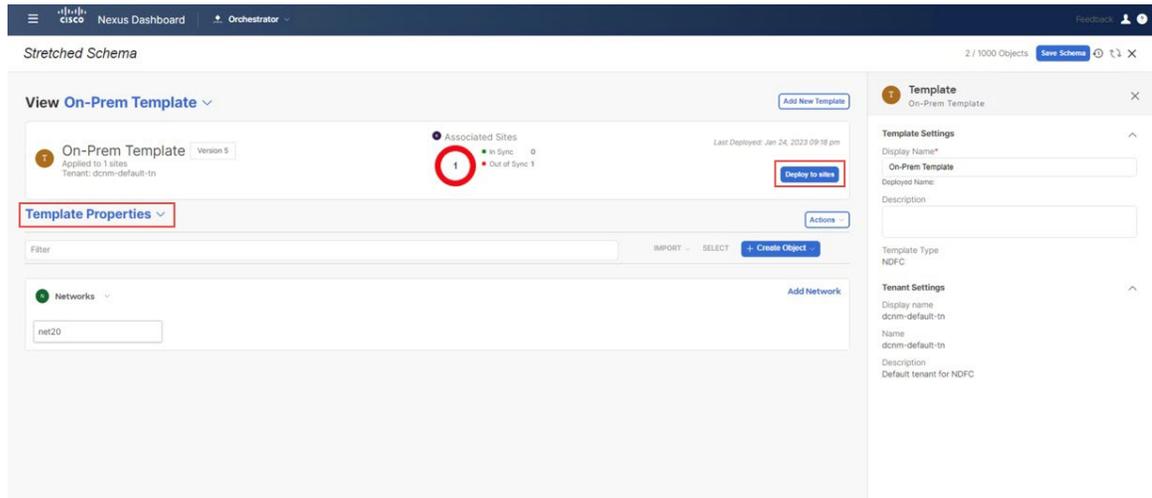


[On-Prem テンプレート (On-Prem Template)] ウィンドウに戻ります。

ステップ 31 オンプレミス サイト (このユース ケースの例ではシドニー サイト) の横にある矢印をクリックし、ドロップダウンメニューから [テンプレート プロパティ (Template Properties)] を選択します。

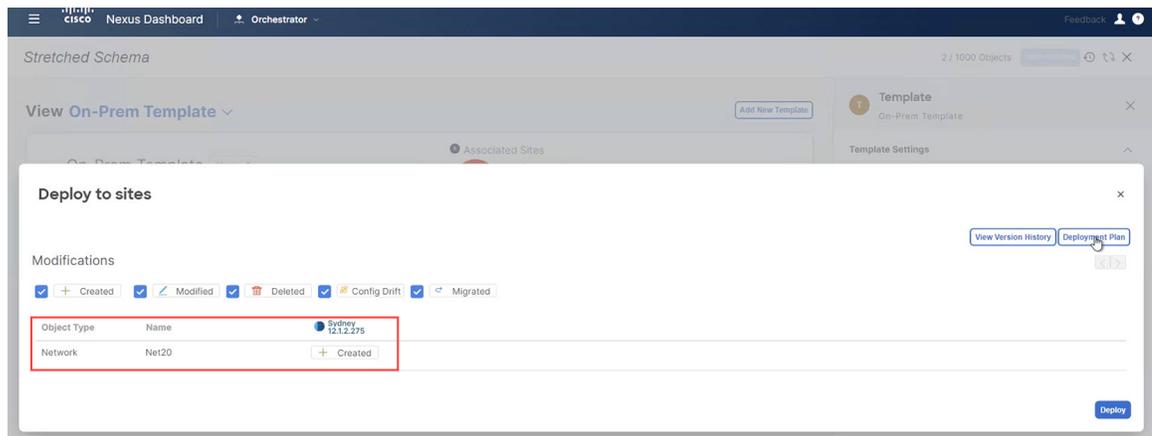
ステップ 32 [サイトに展開 (Deploy to Sites)] をクリックします。

図 152:



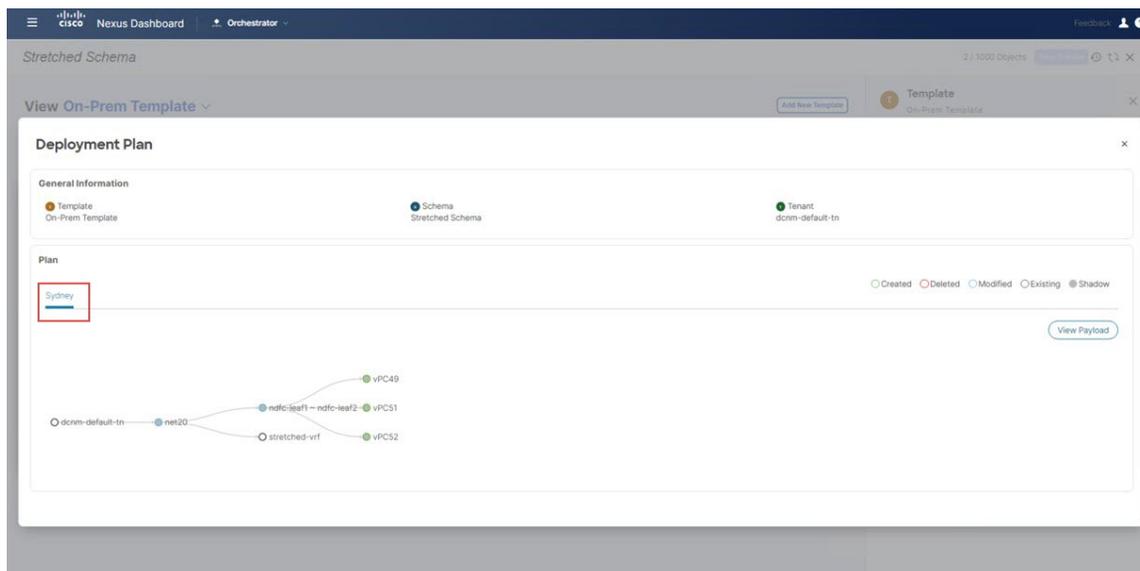
[サイトに展開 (Deploy to Sites) ] ウィンドウが表示され、テンプレートが展開されるサイトが表示されます。

図 153:



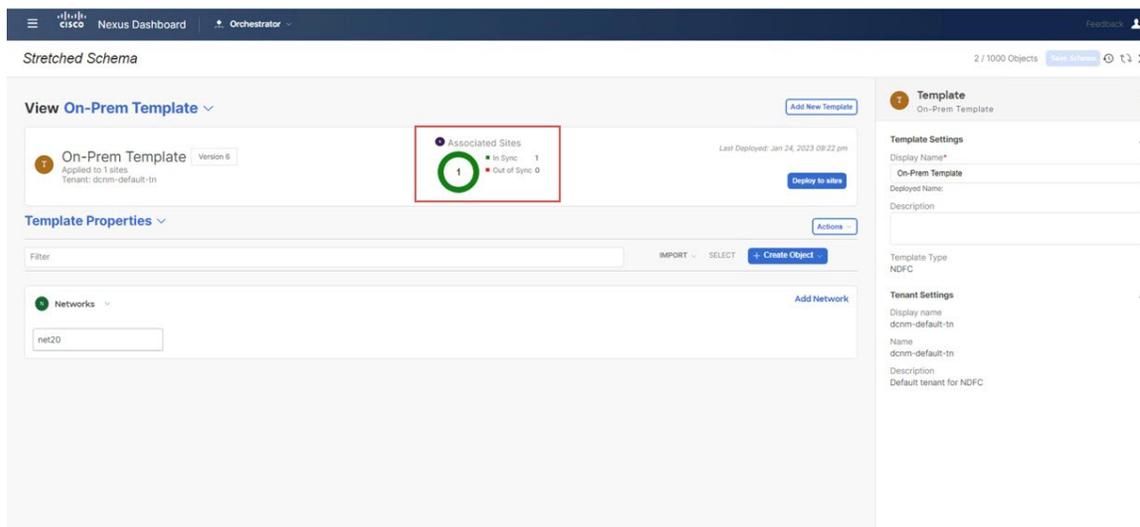
ステップ 33 [展開プラン (Deployment Plan) ]を追加認証のためにクリックします。そして、その特定のサイトの展開プランを表示するためにそのオンプレミスサイトをクリックします。

図 154:



ステップ 34 [展開 (Deploy)] をクリックして、NDO が NDFC に構成をプッシュします。

図 155:



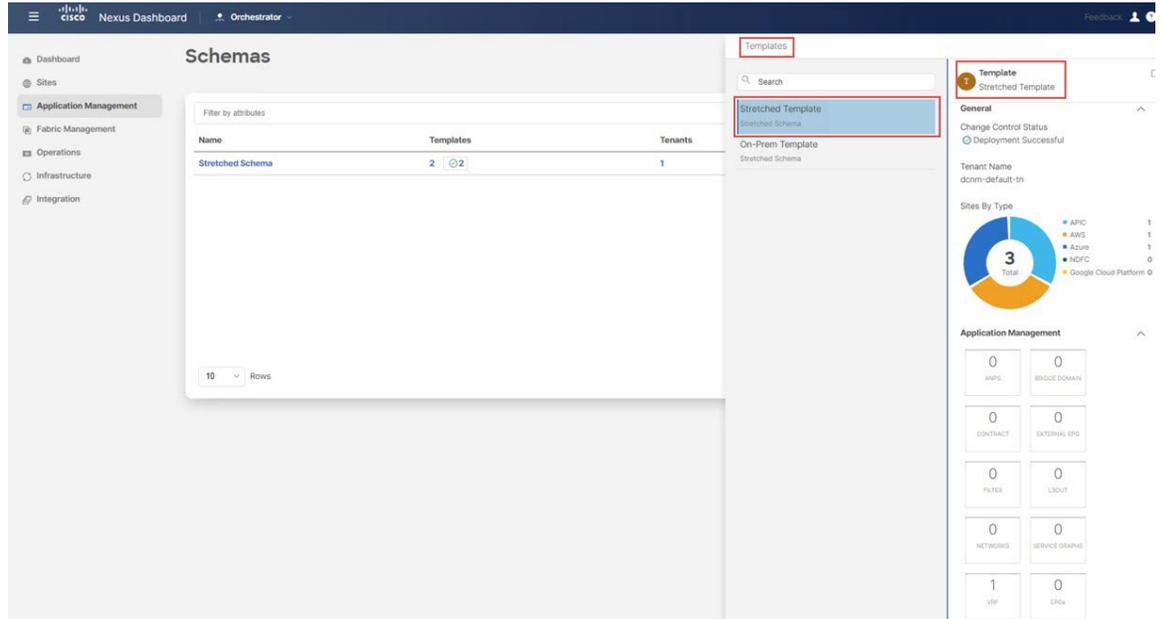
ステップ 35 構成が正常に展開されたことを確認します。

これらの各検証ステップでは、表示されているこのユース ケースの構成のために特定のコマンドが使用されることにご注意ください。構成に基づいて各コマンドの適切な変数を入れ替えます。

a) NDO 内で構成が正常に展開されたことを確認します。

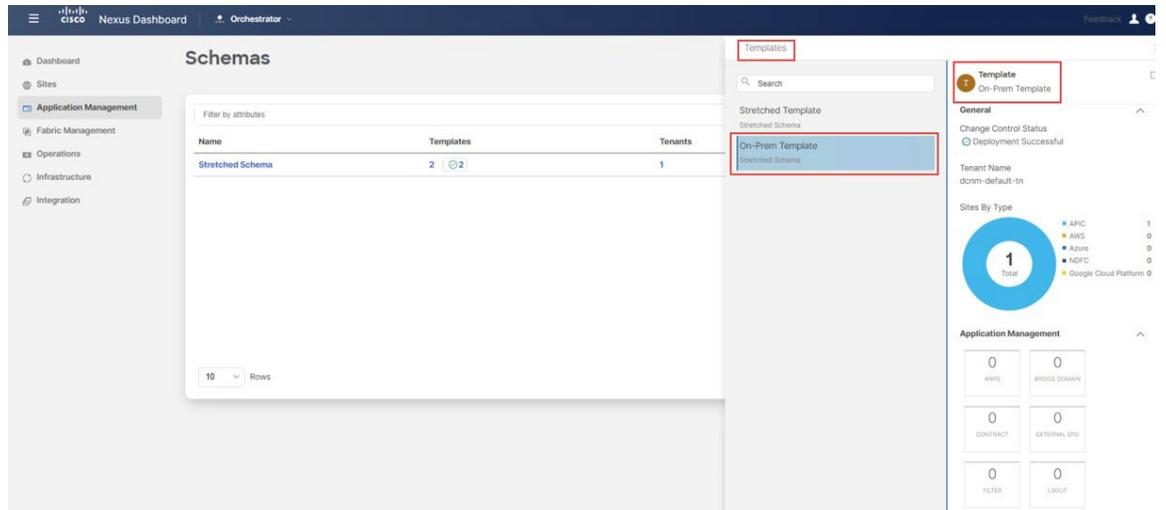
- [ストレッチされた テンプレート (Stretched Template)] が正常に展開されたことを確認します。

図 156 :



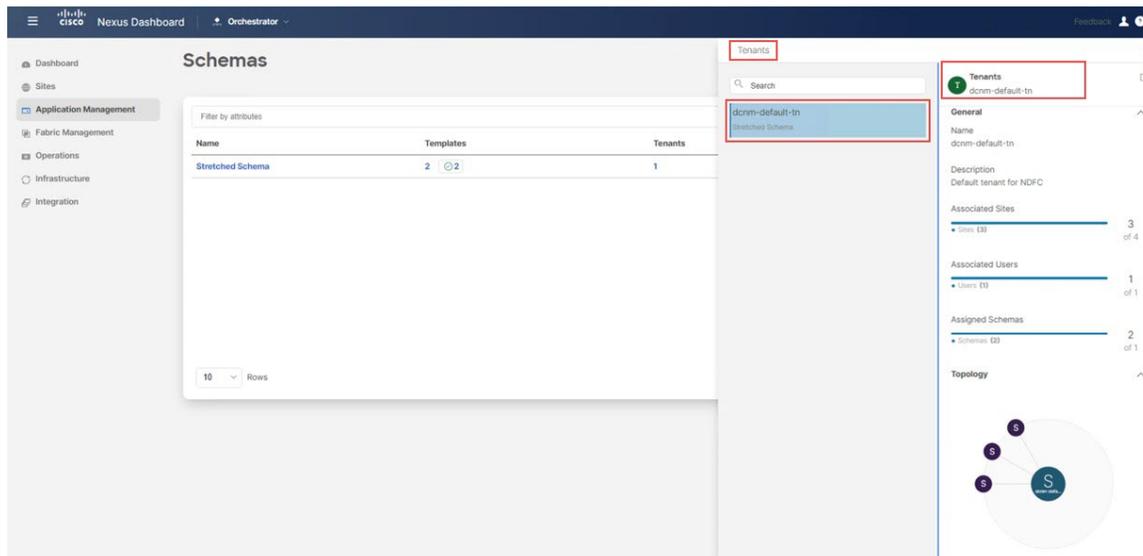
- [On-Premテンプレート (On-Prem Template) ] が正常に展開されたことを確認します。

図 157 :



- dcn-default-tn テナントが正常に展開されたことを確認します。

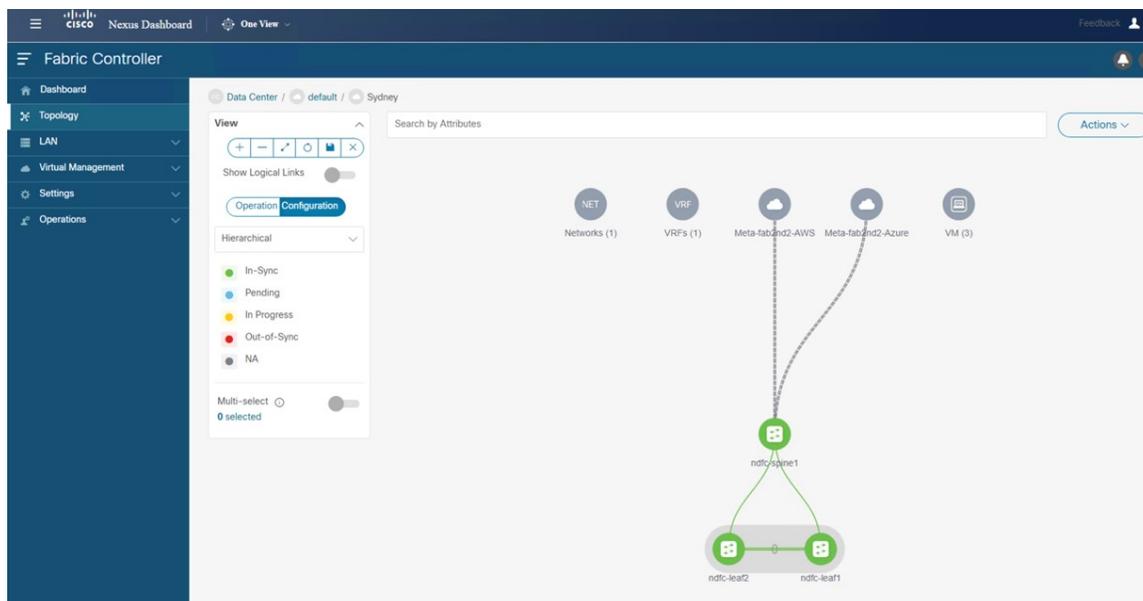
図 158 :



b) NDFC で、以下が正常に実行されたことを確認します。

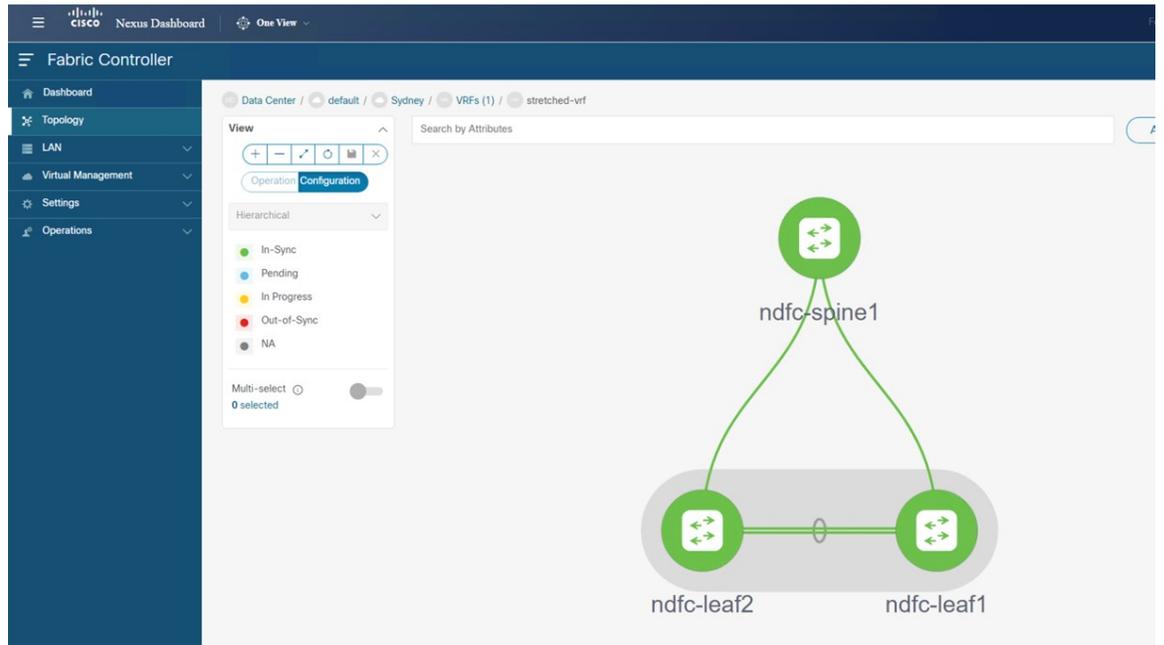
- 1つの vrf と 1つのネットワークが作成されていることを確認します。

図 159 :



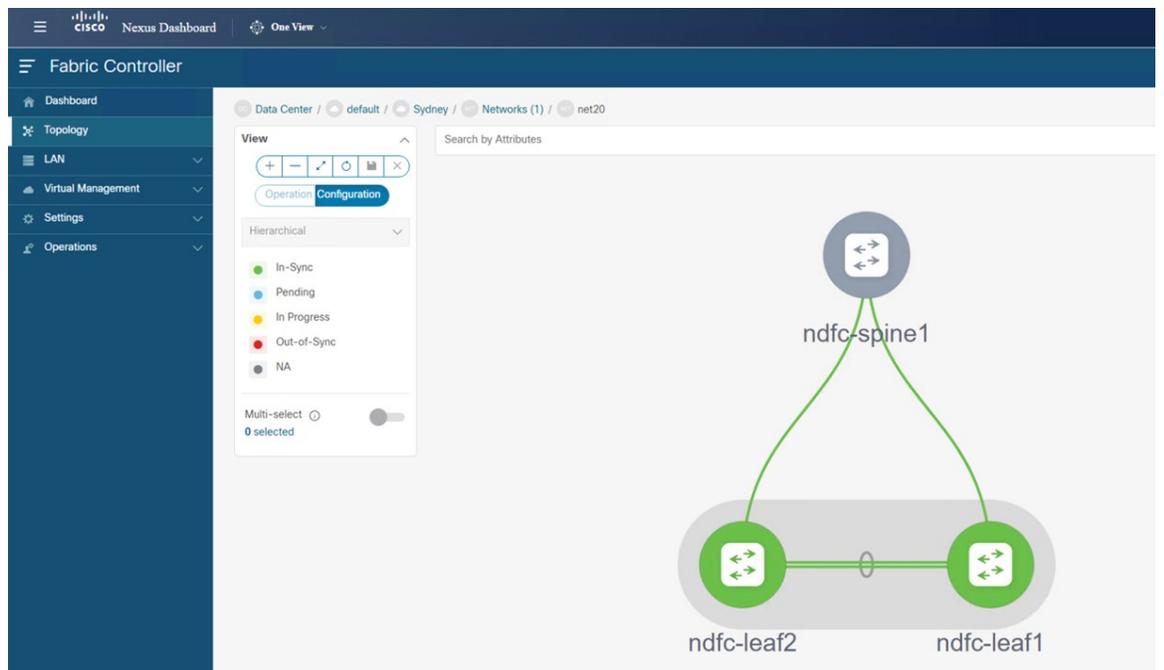
- VRF が正常に展開されたことを確認します。

図 160 :



- ネットワーク が正常に展開されたことを確認します。

図 161 :



- c) オンプレミスのボーダー ゲートウェイ スパイン デバイスで `sh ip route vrf stretched-vrf` を入力します。

## ストレッチされた VRF ユース ケースの構成

```

ndfc-leaf1#
ndfc-leaf1#
ndfc-leaf1#
ndfc-leaf1#
ndfc-leaf1#
ndfc-leaf1# sh ip rou vrf stretched-vrf
IP Route Table for VRF "stretched-vrf"
'*' denotes best ucast next-hop
'*:*' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>
10.230.0.0/16, ubest/mbest: 1/0
   *via 10.10.0.1%default, [200/0], 00:16:32, bgp-65084, internal, tag 65091, segid: 150555 tunnelid: 0xa0a0001 encap: VXLAN
70.1.0.0/16, ubest/mbest: 1/0
   *via 10.10.0.1%default, [200/0], 00:17:37, bgp-65084, internal, tag 65092, segid: 150555 tunnelid: 0xa0a0001 encap: VXLAN
172.16.20.0/24, ubest/mbest: 1/0, attached
   *via 172.16.20.1, vlan2320, [0/0], 00:04:48, direct, tag 12345
172.16.20.1/32, ubest/mbest: 1/0, attached
   *via 172.16.20.1, vlan2320, [0/0], 00:04:48, local, tag 12345
ndfc-leaf1#

```

このユースケースでは、ルーティングテーブルを使用して、NDFC リーフスイッチが次のサブネットに到達できることを確認できます。

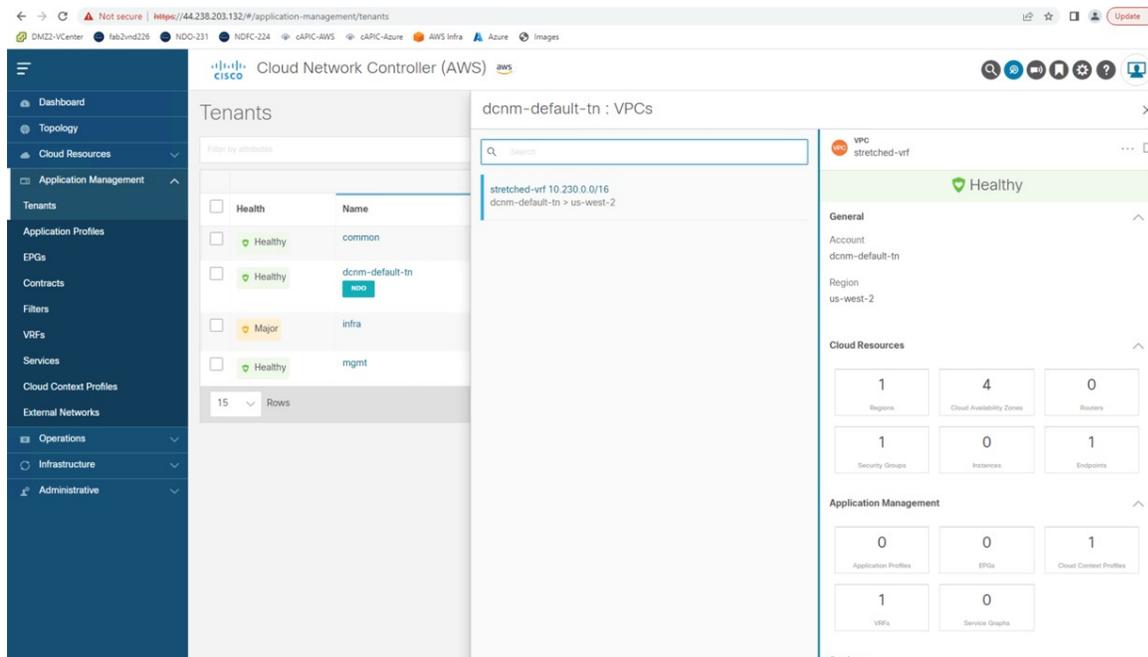
- **AWS** : 10.230.0.0/1
- **Azure** : 70.1.0.0/16

d) AWS に展開されたクラウドネットワークコントローラに接続し、次の検証を行います。

- `dcnm-default-tn` テナントが作成され、1つのVPCが展開されていることを確認します。

| Application Management |                 |                         |                      |      |      |              |         |      |           | Cloud Resources |  |
|------------------------|-----------------|-------------------------|----------------------|------|------|--------------|---------|------|-----------|-----------------|--|
| Health                 | Name            | Description             | Application Profiles | EPGs | VRFs | AWS Account  | Regions | VPCs | Endpoints |                 |  |
| Healthy                | common          |                         | 1                    | 0    | 2    |              | 0       | 0    | 0         |                 |  |
| Healthy                | dcnm-default-tn | Default tenant for NDFC | 0                    | 0    | 1    | 117378746411 | 2       | 1    | 1         |                 |  |
| Major                  | infra           |                         | 1                    | 15   | 2    | 257591685230 | 2       | 1    | 12        |                 |  |
| Healthy                | mgmt            |                         | 0                    | 0    | 2    |              | 0       | 0    | 0         |                 |  |

- VPC が展開されていることを確認します。



- AWS に展開されたクラウド ネットワーク コントローラのルーティング テーブル ビューを使用して、到達可能なサブネットが次のようになっていることを確認します。

- **NDFC** : 172.16.20.0/24
- **Azure** : 70.1.0.0/16

## ストレッチされた VRF ユース ケースの構成

The image displays two screenshots of the AWS Management Console for a VPC named 'VPC stretched-vrf' in the 'us-west-2' region. The left pane shows the 'Overview' tab with summary statistics for Cloud Resources and Application Management. The right pane shows the 'Subnets for CIDR Block 10.230.0.0/16' page, which lists two subnets: 10.230.1.0/24 and 10.230.2.0/24. The bottom screenshot shows the 'Route Table Settings' for the 'stretched-vrf.egress' route table, which is configured with three entries: 172.16.20.1/24 (Hub Network), 70.1.0.0/16 (Hub Network), and 10.230.0.0/16 (local).

e) AWS コンソールで、次のことを確認します。

- 1つの VPC と 2つのサブネットが表示されていることを確認します。

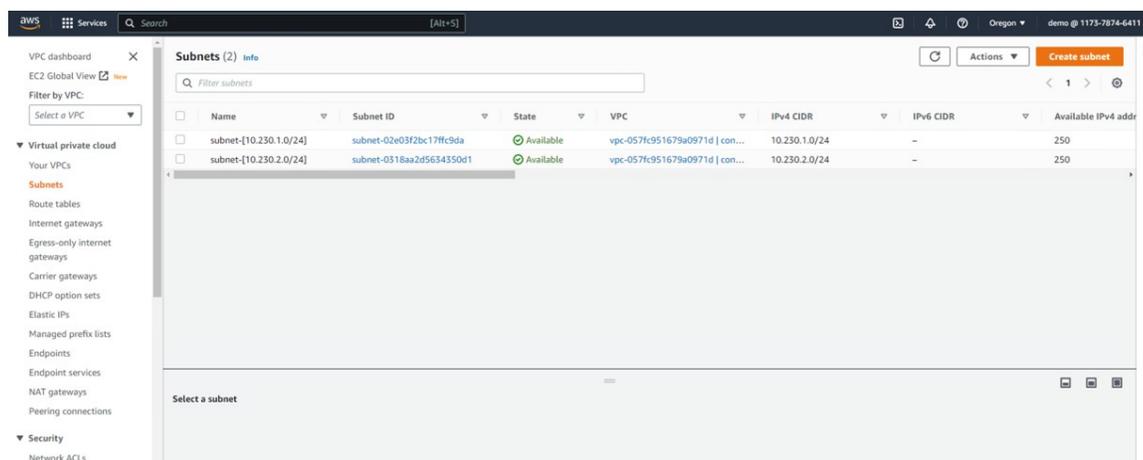
The screenshot shows the AWS VPC dashboard with the following resources listed by region (US West):

| Resource                      | Count |
|-------------------------------|-------|
| VPCs                          | 1     |
| NAT Gateways                  | 0     |
| Subnets                       | 2     |
| VPC Peering Connections       | 0     |
| Route Tables                  | 3     |
| Network ACLs                  | 1     |
| Internet Gateways             | 1     |
| Security Groups               | 2     |
| Egress-only Internet Gateways | 0     |
| Customer Gateways             | 0     |
| DHCP option sets              | 1     |
| Virtual Private Gateways      | 0     |
| Elastic IPs                   | 2     |
| Site-to-Site VPN Connections  | 0     |
| Endpoints                     | 0     |
| Running Instances             | 0     |
| Endpoint Services             | 0     |

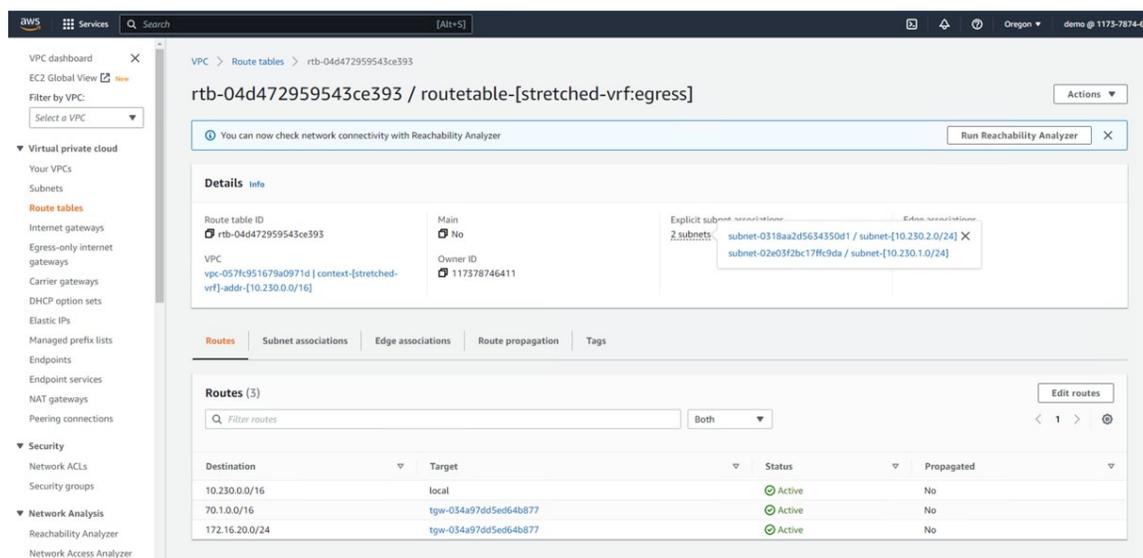
The screenshot shows the details for a VPC named 'context-[stretched-vrf]-addr-[10.230.0.0/16]'. The table below summarizes the VPC details:

| Name   | VPC ID                | State     | IPv4 CIDR     | IPv6 CIDR | DHCP option set |
|--|-----------------------|-----------|---------------|-----------|-----------------|
| context-[stretched-vrf]-addr-[10.230.0.0/16] | vpc-057fc951679a0971d | Available | 10.230.0.0/16 | -         | dopt-2278255a   |

## ストレッチされた VRF ユース ケースの構成



- ルーティング テーブルが表示されていることを検証する。



- f) Azure に展開されたクラウド ネットワーク コントローラに接続し、次の検証を行います。

- dcnm-default-tn テナントが作成されていることを確認します。

| Health                   |         | Name            | Description             | Application Profiles | EPGs | VRFs | Azure Subscription                   | Regions | Virtual Networks | Endpoints |
|--------------------------|---------|-----------------|-------------------------|----------------------|------|------|--------------------------------------|---------|------------------|-----------|
| <input type="checkbox"/> | Healthy | common          |                         | 1                    | 0    | 2    |                                      | 0       | 0                | 0         |
| <input type="checkbox"/> | Healthy | dcnm-default-tn | Default tenant for NDFC | 0                    | 0    | 1    | Shared from infra                    | 1       | 1                | 0         |
| <input type="checkbox"/> | Major   | infra           |                         | 1                    | 12   | 2    | 7408417b-785d-468a-bf23-41e85a1a3ada | 1       | 1                | 10        |
| <input type="checkbox"/> | Healthy | mgmt            |                         | 0                    | 0    | 2    |                                      | 0       | 0                | 0         |

dcnm-default-tn : Virtual Networks

Virtual Network stretched-vrf

Healthy

General

Account dcnm-default-tn

Region eastus

Cloud Resources

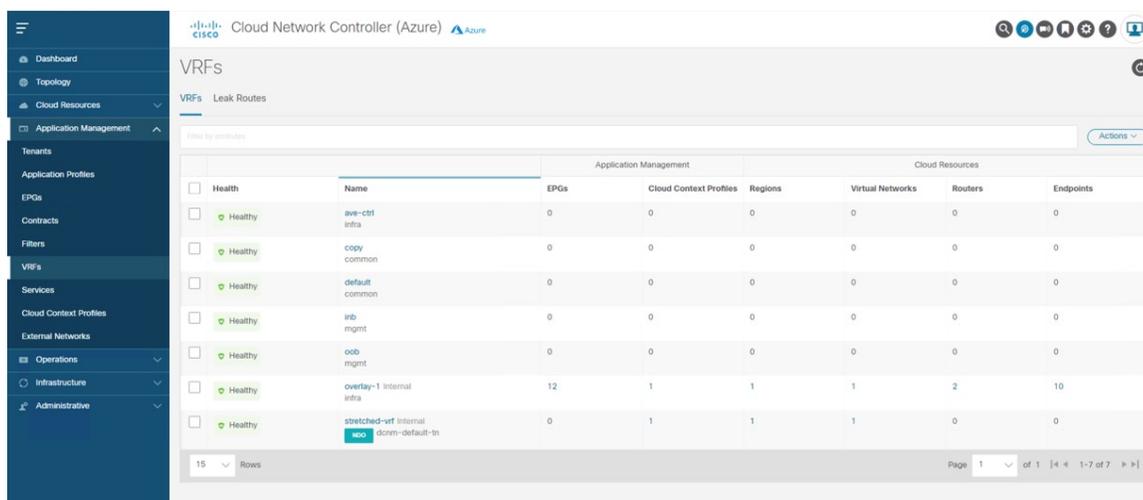
|                             |                  |                         |
|-----------------------------|------------------|-------------------------|
| 1                           | 0                | 1                       |
| Regions                     | Routers          | Network Security Groups |
| 1                           | 0                | 0                       |
| Application Security Groups | Virtual Machines | Endpoints               |

Application Management

|                      |                |                        |
|----------------------|----------------|------------------------|
| 0                    | 0              | 1                      |
| Application Profiles | EPGs           | Cloud Context Profiles |
| 1                    | 0              |                        |
| VRFs                 | Service Graphs |                        |

- VRF が展開されていることを確認します：

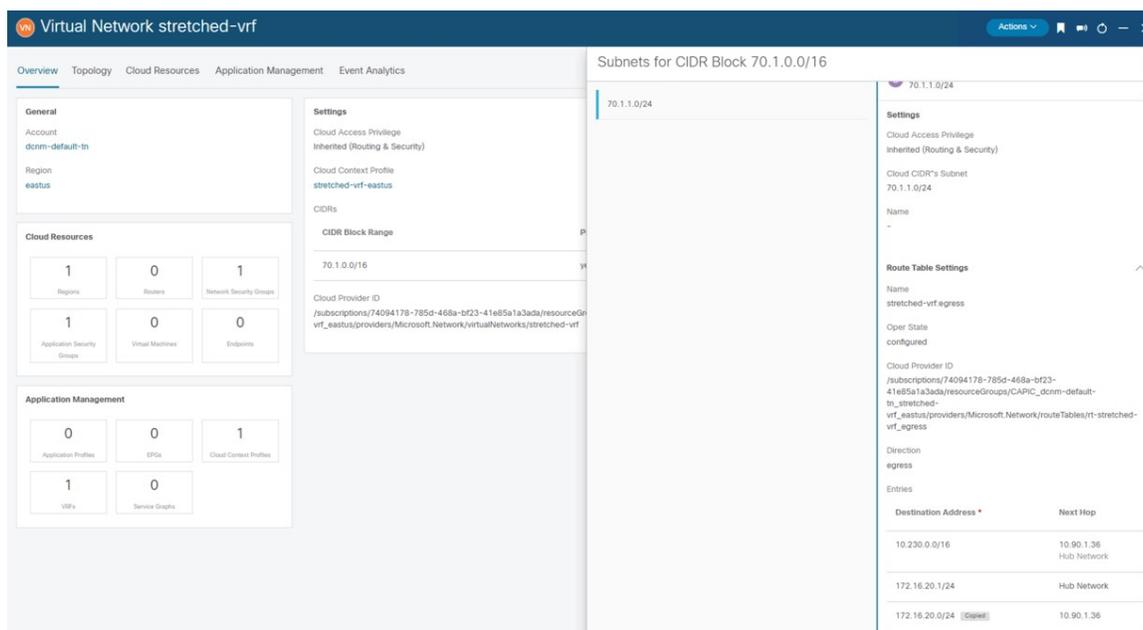
ストレッチされた VRF ユース ケースの構成



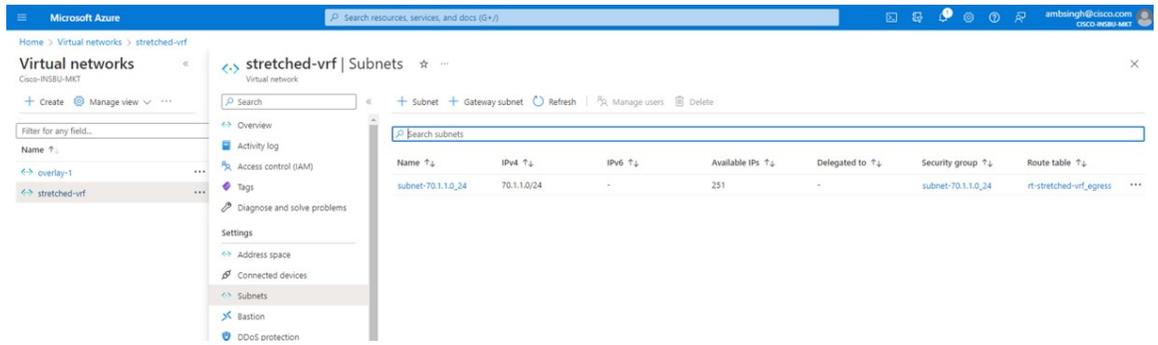
• AWS に展開されたクラウド ネットワーク コントローラのルーティング テーブル ビューを使用して、到達可能なサブネットが次のようになっていることを確認します。

• **NDFC** : 172.16.20.0/24

• **AWS** : 10.230.0.0/1



g) Azure コンソールで、サブネットが表示されることを確認します。







## 第 7 章

# ルート リークの使用例

---

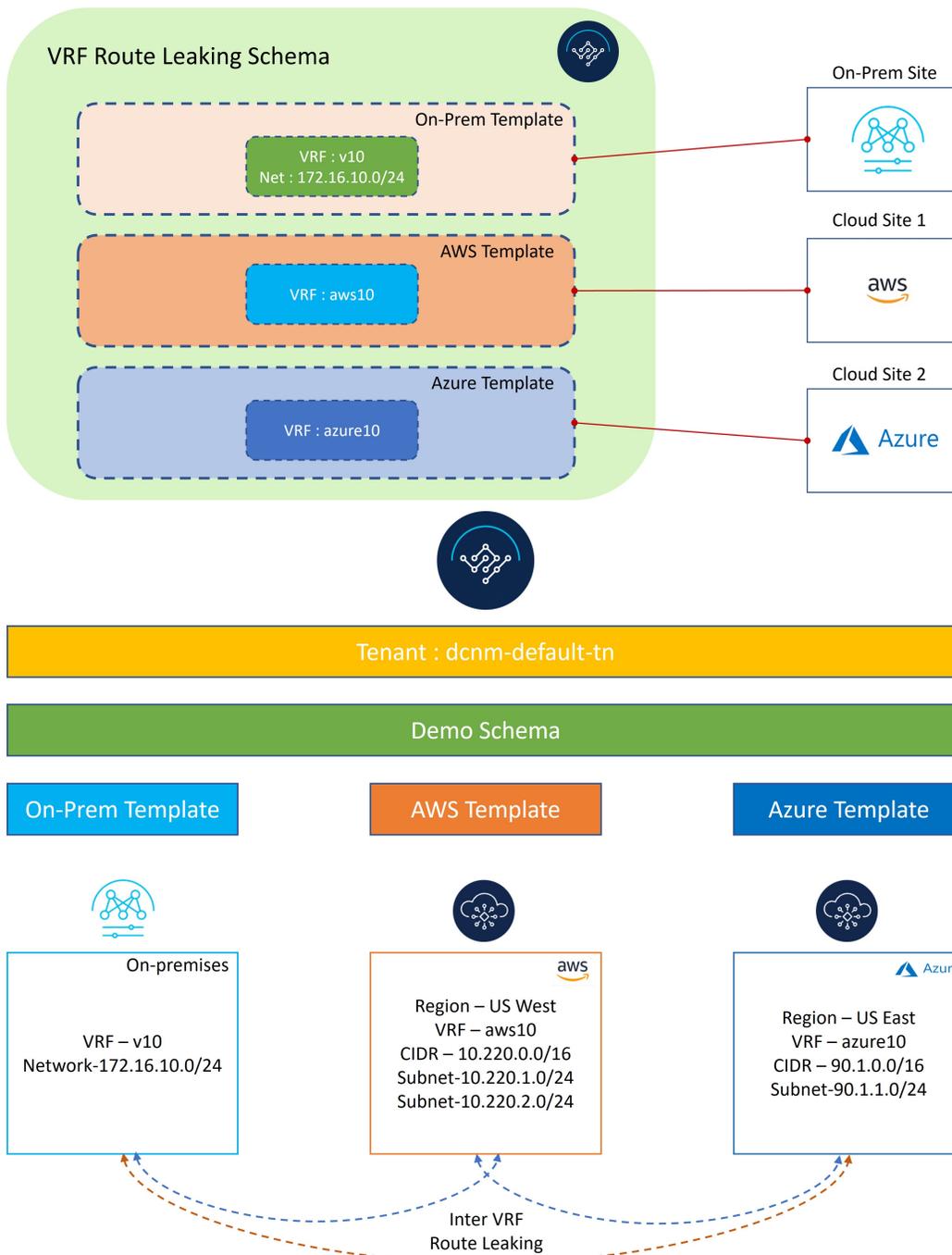
- [ルート リークの使用例について \(155 ページ\)](#)
- [必要なテンプレートの構成 \(157 ページ\)](#)
- [ルート リークの設定 \(177 ページ\)](#)

## ルート リークの使用例について

このルート リークのユース ケースでは、オンプレミスサイトの VRF およびネットワーク定義を含むサイトごとに個別のテンプレートを使用しますが、クラウドサイトの場合、これらのテンプレートには VRF 定義のみが含まれます。同じ VRF が全てのサイトに渡っているためサイト間でプレフィックスの交換のために構成を必要としない [ストレッチされた VRF ユース ケース \(117 ページ\)](#) で説明されている拡張 VRF (内部 VRF) の使用例とは異なり、各サイトは違う VRF を使うのでこのユース ケースでは VRF リーク構成する必要があります。

サイト (オンプレミスとクラウドサイト) 間でプレフィックスを伝達するには、サイトに関連付けられているそれぞれのテンプレートでルート リークを明示的に構成する必要があります。

図 162:



上の図に示すように、各サイトには個別に関連付けられたテンプレートがあり、そのサイトのみに固有の VRF/ネットワーク定義が含まれています。オンプレミス テンプレートは NDFC 管理のオンプレミス サイトに関連付けられていますが、AWS テンプレートと Azure テンプレートはそれぞれ AWS と Azure クラウド サイトに関連付けられています。Inter-VRF ルートリークは、サイト間の通信を可能にするために、異なる VRF 間で明示的に構成されます。

## 必要なテンプレートの構成

次のセクションの手順を使用して、ルート リークのユース ケースに必要なテンプレートを構成します。

### オンプレミス サイト テンプレートの構成

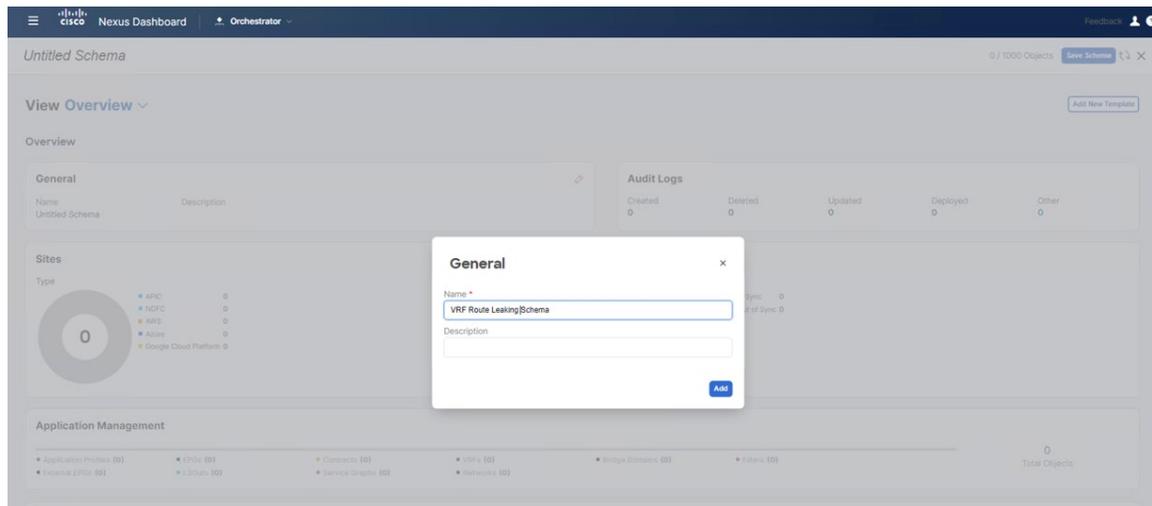
このセクションでは、NDFC 管理のオンプレミス サイトに関連付けられる [オンプレミス テンプレート (On-Prem Template)] を構成します。

**ステップ 1** NDO で、[アプリケーション管理 (Application Management)] > [スキーマ (Schema)] に移動し、[スキーマの追加 (Add Schema)] をクリックします。

**ステップ 2** スキーマ名を指定し、[追加 (Add)] をクリックします。

このユース ケースでは、新しいスキーマに [VRF ルート リーク スキーマ (VRF Route Leaking Schema)] という名前を付けます。

図 163:



新しい [VRF ルート リーク スキーマ (VRF Route Leaking Schema)] スキーマの [概要 (Overview)] ページに戻ります。

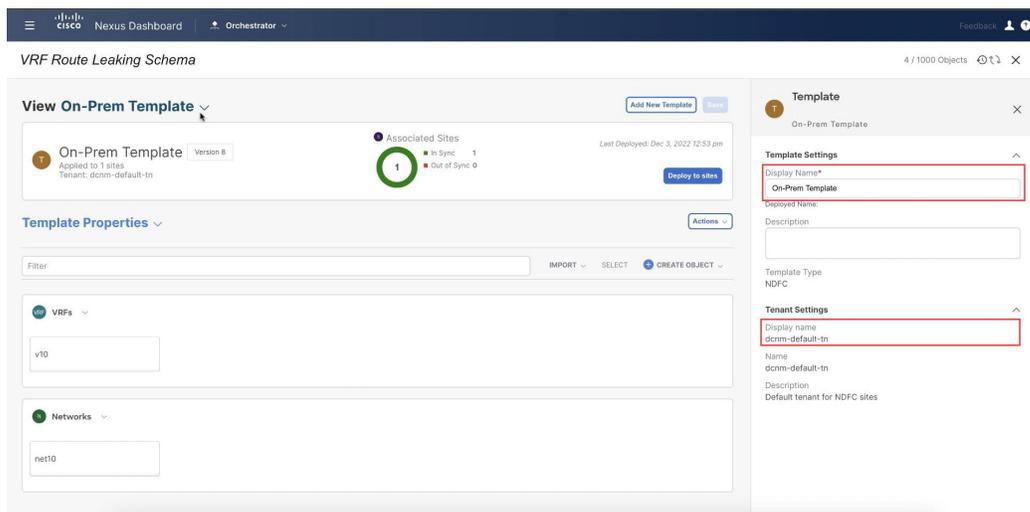
**ステップ 3** [VRF ルート リーク スキーマ (VRF Route Leaking Schema)] スキーマの下で [新しいテンプレートを追加します (Add New Template)] をクリックします。

**ステップ 4** NDFC テンプレートを選択します。

**ステップ 5** [表示名 (Display Name)] フィールドに名前を入力して、NDFC タイプのテンプレートを作成します (例: [On-Prem テンプレート (On-Prem Template)] )。

**ステップ 6** テナントにテンプレートをマップするために [テナントを選択 (Select a Tenant)] フィールド内の dcnm-default-tn テナントを選択します。

図 164:



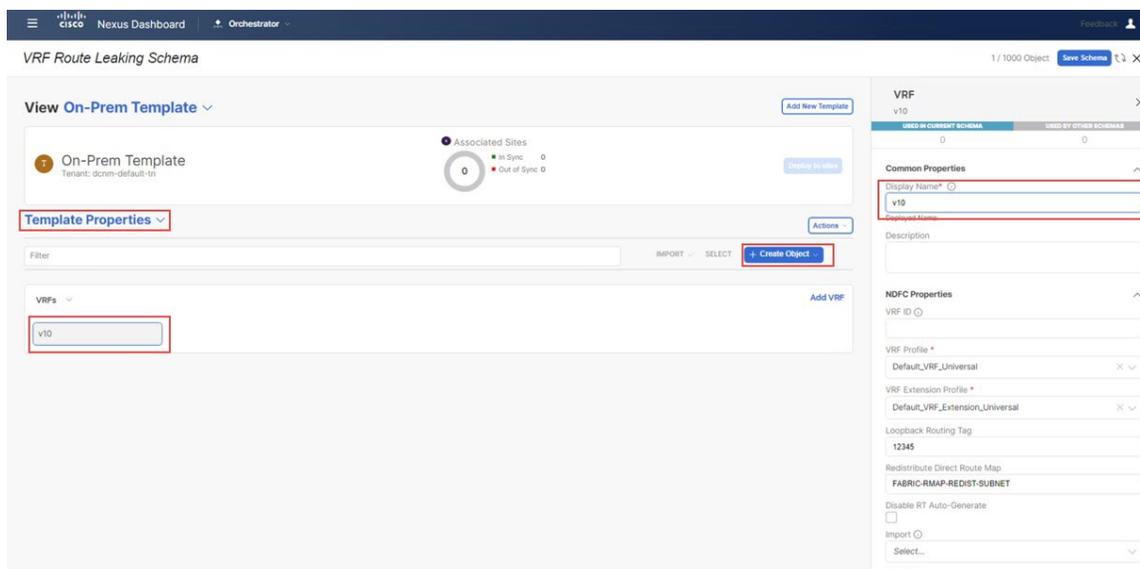
ステップ7 [テンプレートプロパティ (Template Properties)] で [オブジェクトの作成 (Create Object)] をクリックし、[VRF] を選択して、NDFC に管理されたオンプレミス サイトで使用される VRF を作成します。

(注) 新しい VRF を作るより、既に使用したいオンプレミス VRF を作成した場合、[テンプレートプロパティ (Template Properties)] の下、[インポート (Import)] をクリックします。そして既に作成された VRF をインポートします。

現在、サポートはオンプレミスサイトからの VRF とネットワークのインポートに対してのみ利用できます。

ステップ8 この VRF の [表示名 (Display Name)] フィールドに名前を入力します (例 : v10) 。

図 165:



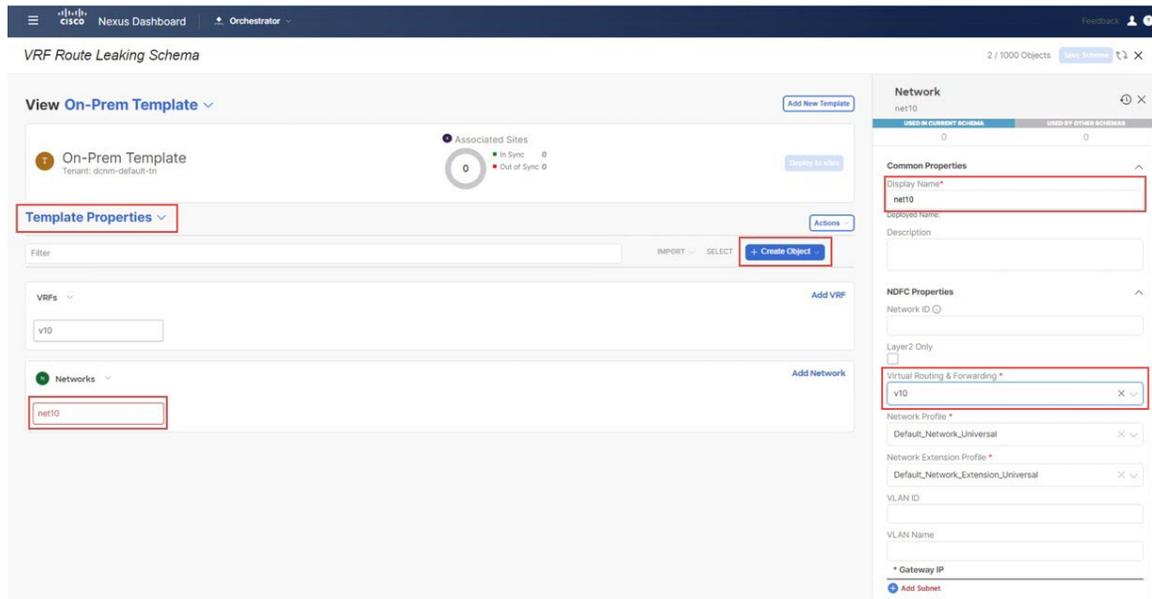
ステップ 9 [テンプレート プロパティ (Template Properties)] の下、[オブジェクトを作成 (Create Object)] をクリックしてネットワークを作成するために[ネットワーク (Network)] を選択します。

(注) 新しい VRF を作るより、既に使用したい VRF を作成した場合、[テンプレート プロパティ (Template Properties)] の下、[インポート (Import)] をクリックします。そして既に作成された ネットワーク をインポートします。

ステップ 10 ネットワークの [表示名 (Display Name)] フィールドに名前を入力します (例: net10)。

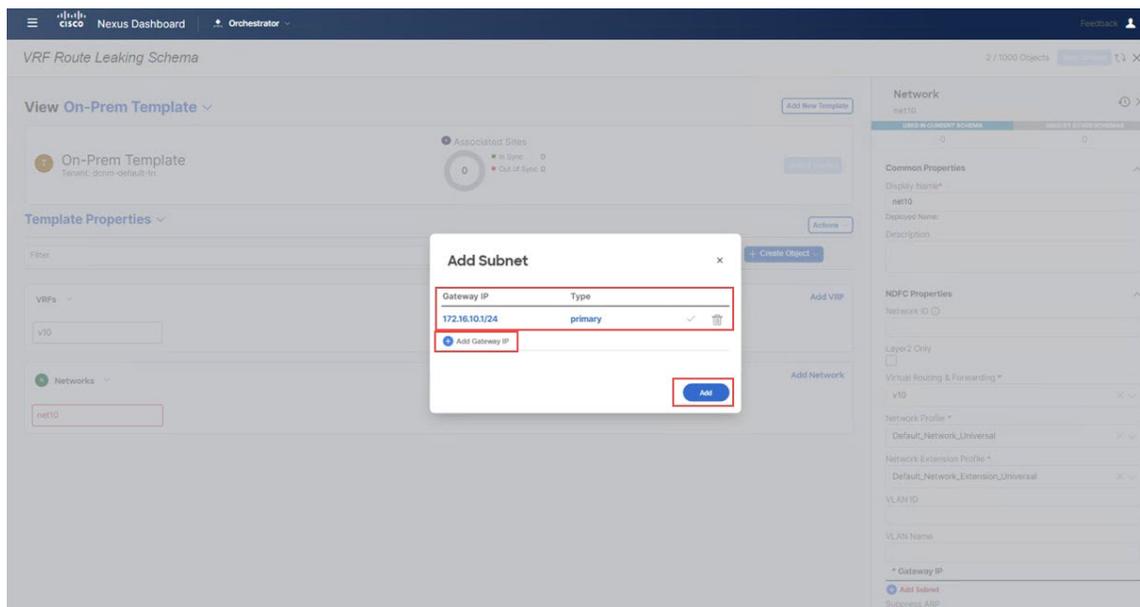
ステップ 11 [バーチャルルートと転送 (Virtual Routing & Forwarding)] フィールドで、v10 VRF を選択して、net10 ネットワークをその VRF にマッピングします。

図 166:



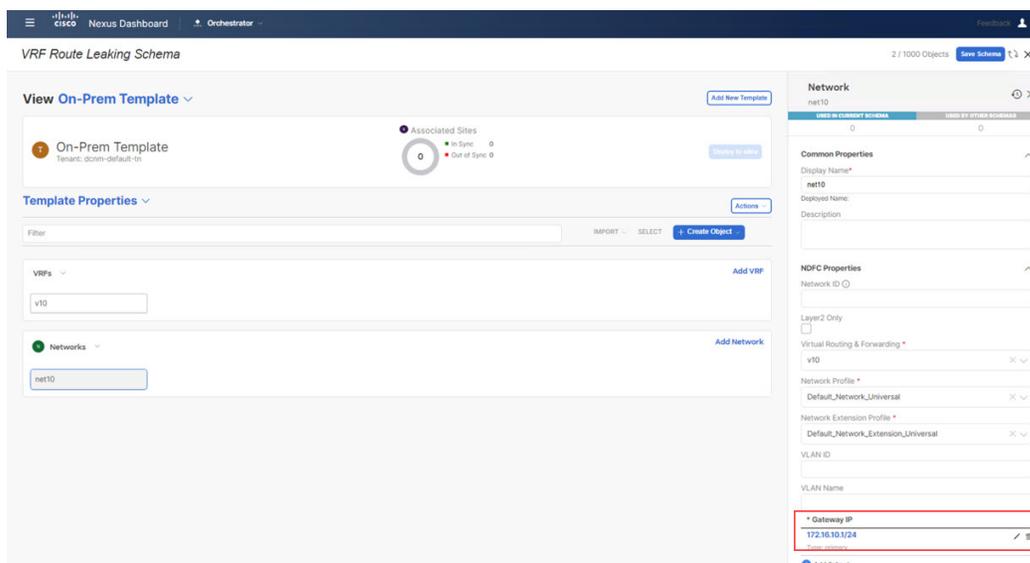
ステップ 12 [ゲートウェイ IP (Gateway IP)] フィールドで、[サブネットの追加 (Add Subnet)] をクリックしてゲートウェイの IP アドレスを入力し、[追加 (Add)] をクリックします。

図 167:



ゲートウェイ IP アドレスは[ゲートウェイ IP (Gateway IP)]フィールドに表示されます。

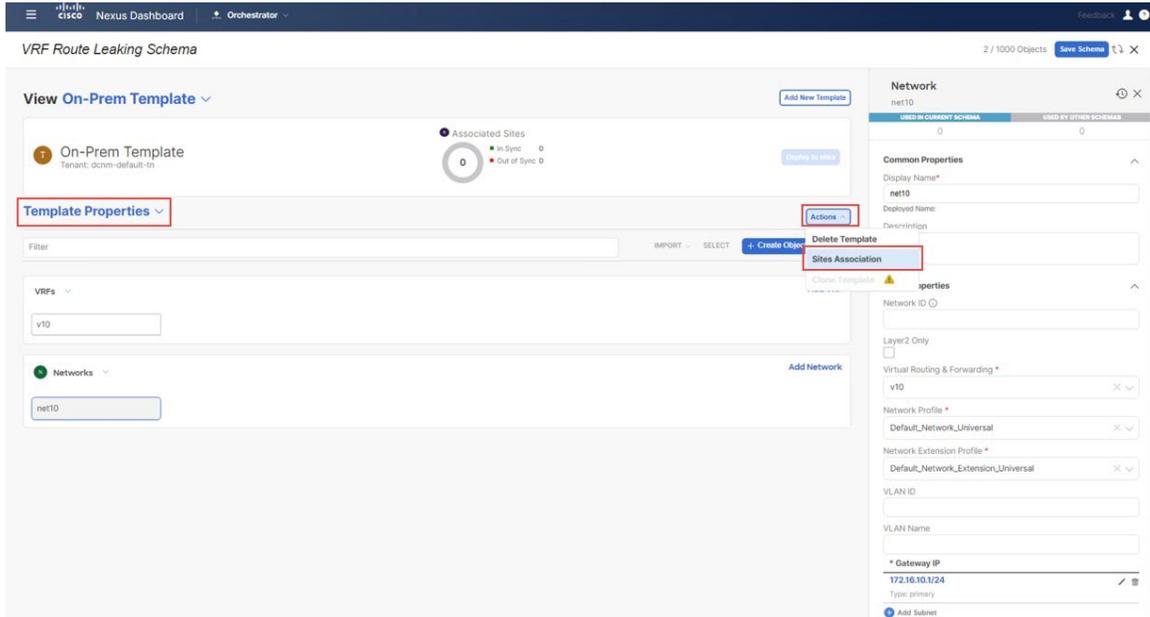
図 168:



ステップ 13 必要な場合、ネットワークのオプションパラメータを定義します。

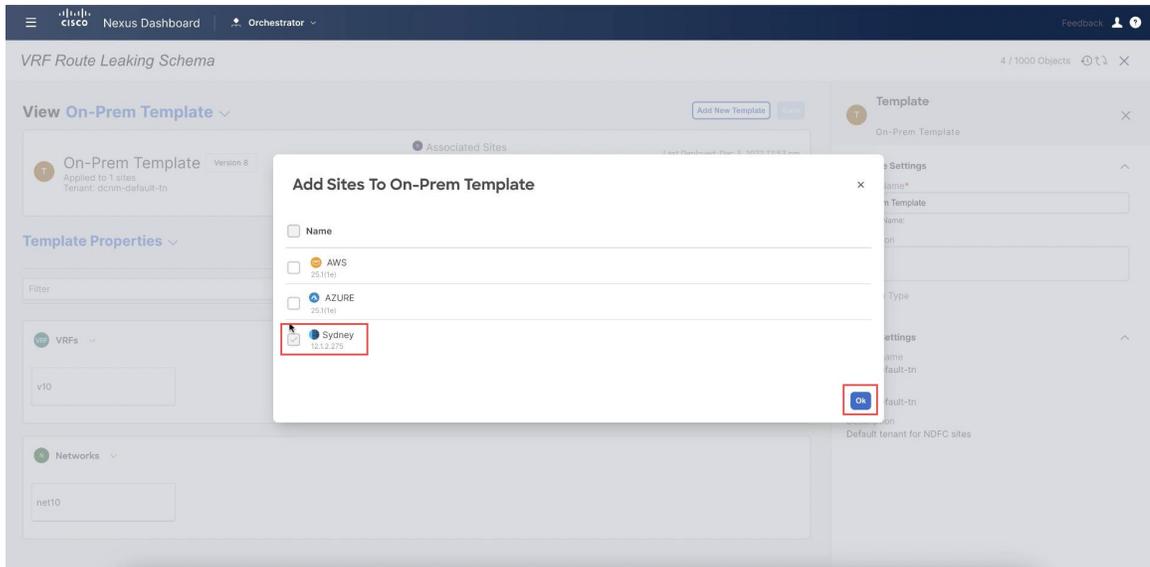
ステップ 14 [テンプレート プロパティ (Template Properties)] エリア内で [アクション (Actions)] > [サイトの関連付け (Sites Association)] をクリックします。

図 169:



ステップ 15 このテンプレートをオンプレミスサイト(このユースケースの例ではシドニーサイト)にのみ関連付け、[OK] をクリックします。

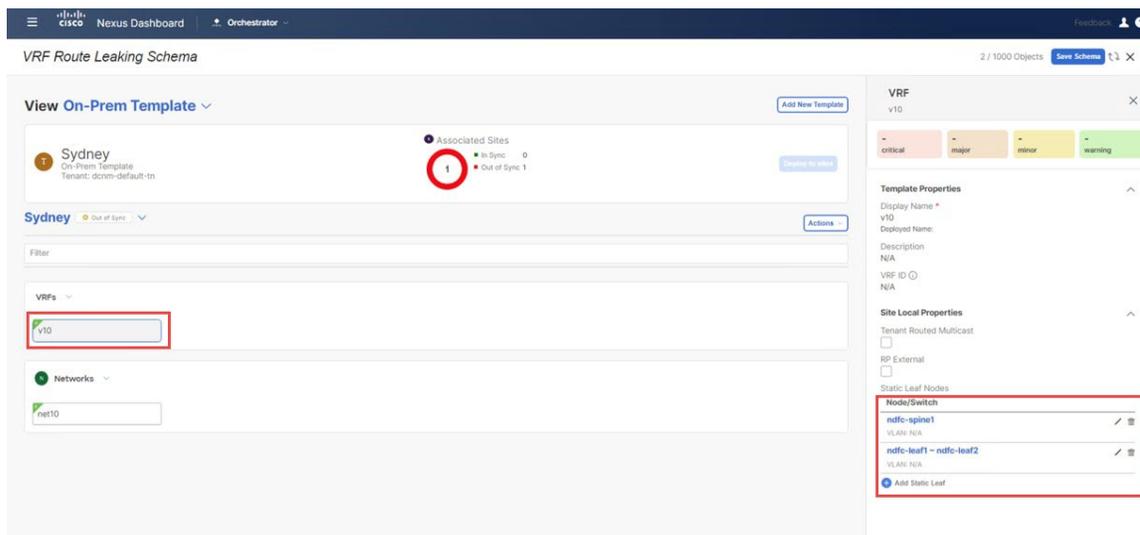
図 170:



ステップ 16 [テンプレート プロパティ (Template Properties)] をクリックし、オンプレミスサイト(このユースケースの例ではシドニーサイト)を選択してから、v10 VRF を選択します。

ステップ 17 右側のペインで [静的リーフの追加 (Add Static Leaf)] をクリックします。

図 171:



[静的リーフの追加 (Add Static Leaf)] ウィンドウが表示されます。

**ステップ 18** [リーフ (Leaf)] フィールド内で、VRF が展開されるべき場所のリーフ/ボーダー/ボーダーゲートウェイ デバイスを選択し、**Ok** をクリックします。

この例では、リーフ ノードに VRF を展開する必要があります (VRF にマップされたネットワークの エンドポイントに接続される)。そして、VRF からクラウドサイトへのレイヤー 3 接続に拡張するために BGW スパイン ノードを展開する必要があります。

**ステップ 19** ネットワークをリーフスイッチに接続するには、net10 ネットワークをクリックし、[静的ポートの追加] をクリックして、このネットワークを展開するポートを追加します。

[静的ポートの追加 (Add Static Port)] ウィンドウが表示されます。

**ステップ 20** [静的ポートの追加 (Add Static Port)] ウィンドウで[パスを追加 (Add Path)] をクリックします。

[静的ポートの追加 (Add Static Port)] ウィンドウが表示されます。

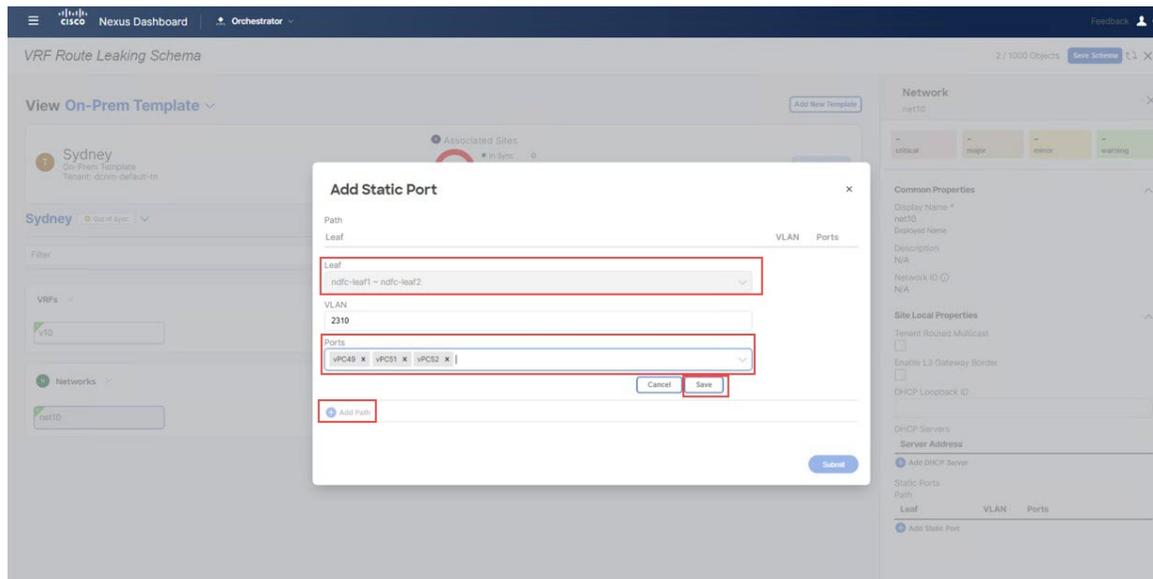
**ステップ 21** [リーフ (Leaf)] フィールドで展開したいネットワークのデバイスを選択します。

**ステップ 22** (任意) VLAN フィールドに必要な情報を入力します。

**ステップ 23** [ポート (Port)] フィールドで展開したいネットワークのポートを選択します。

**ステップ 24** [保存 (Save)] をクリックします。

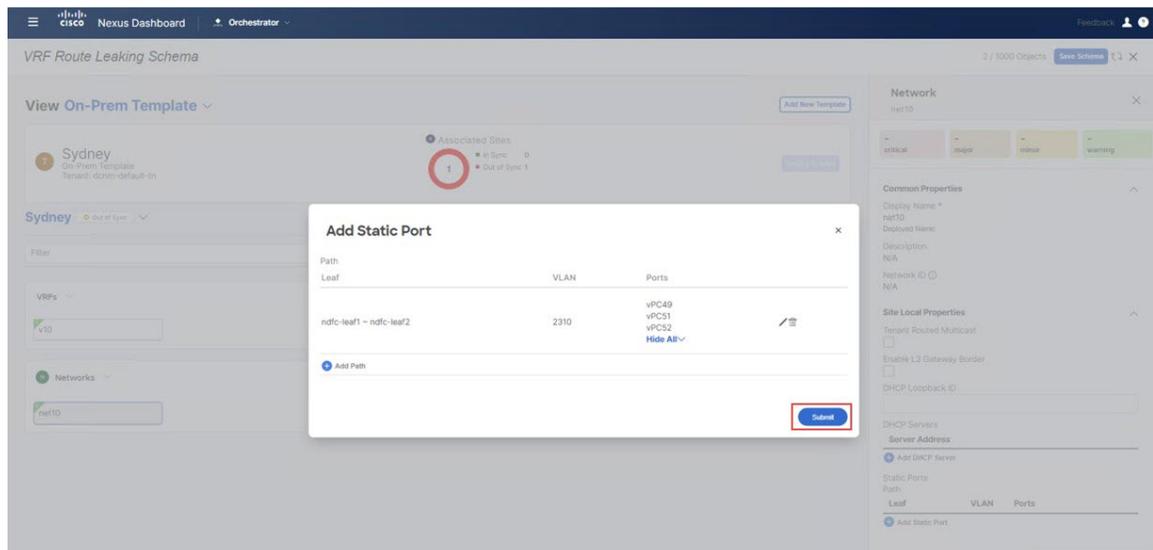
図 172:



[静的ポートの追加 (Add Static Port)] ウィンドウに戻ります。

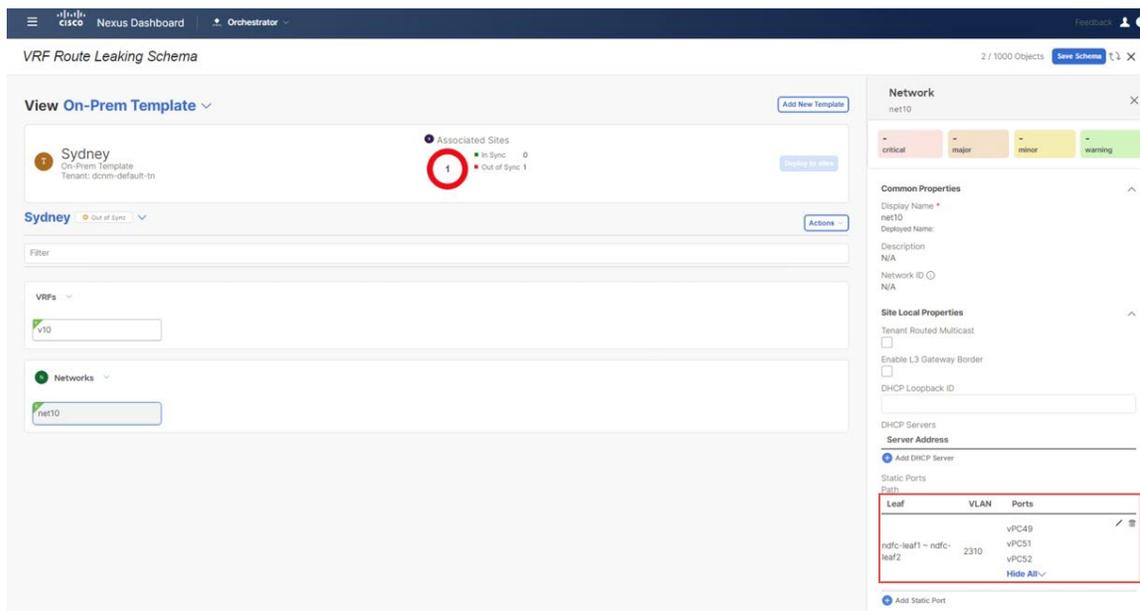
ステップ 25 [静的ポートの追加 (Add Static Port)] ウィンドウで[送信 (Submit)] をクリックします。

図 173:



オンプレミス テンプレート ウィンドウに戻ります。

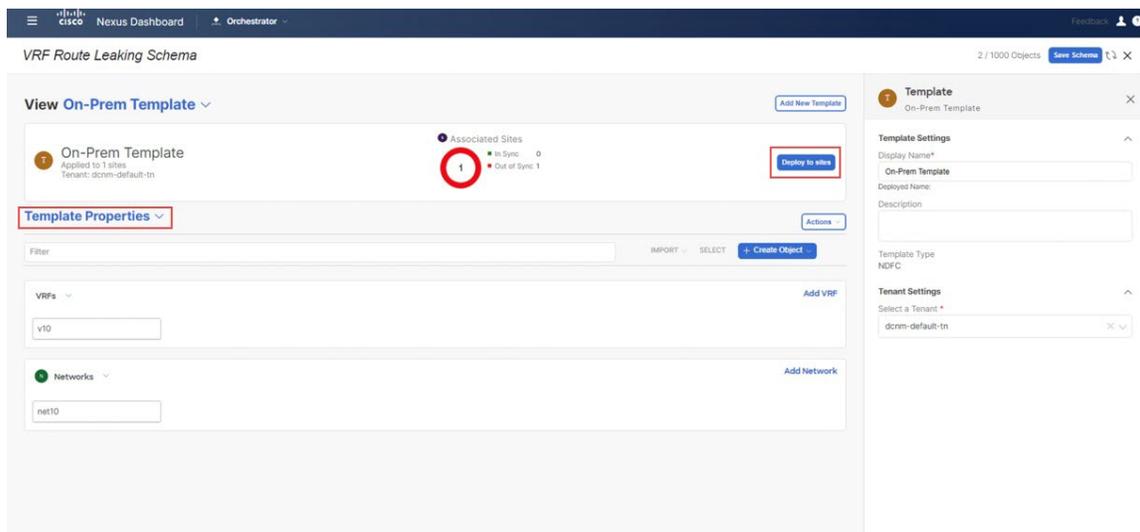
図 174:



ステップ 26 オンプレミス サイトの横にある矢印をクリックし、ドロップダウンメニューから [テンプレートのプロパティ (Template Properties)] を選択します。

ステップ 27 [サイトに展開 (Deploy to Sites)] をクリックします。

図 175:

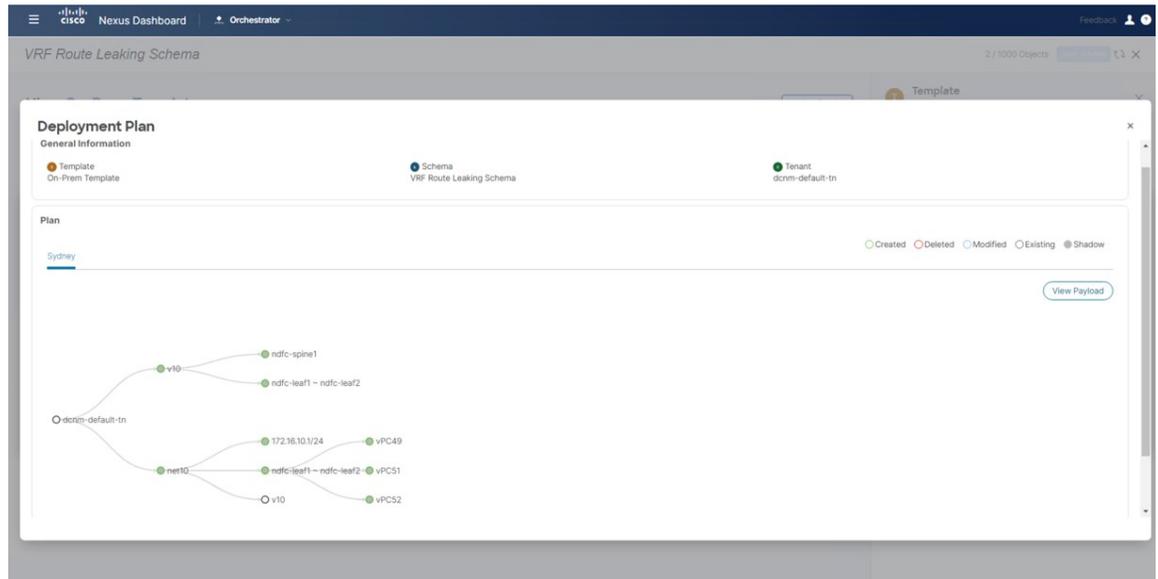


ステップ 28 [On-Prem テンプレート (AWS Template)] をサイトに展開します。

- 追加認証のために [展開プラン (Deployment Plan)] をクリックします。

オンプレミス サイトをクリックして、その特定のサイトの展開プランを表示します。

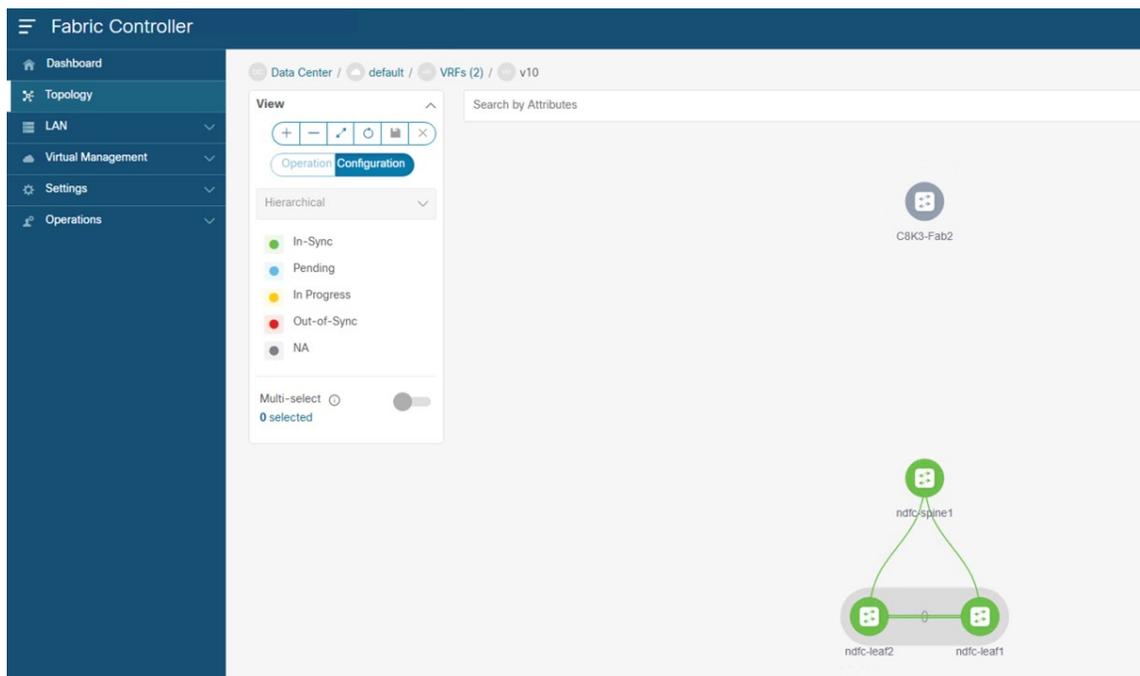
図 176:



- [展開 (Deploy)] をクリックして、NDO が NDFC に構成をプッシュします。  
これにより、NDO 構成が NDFC にプッシュされます。

**ステップ 29** NDFC で、VRF が正常に展開されたことを確認します。

図 177:



### 次のタスク

[Azure サイト テンプレートの構成 \(166 ページ\)](#) の手順を実行します。

## Azure サイト テンプレートの構成

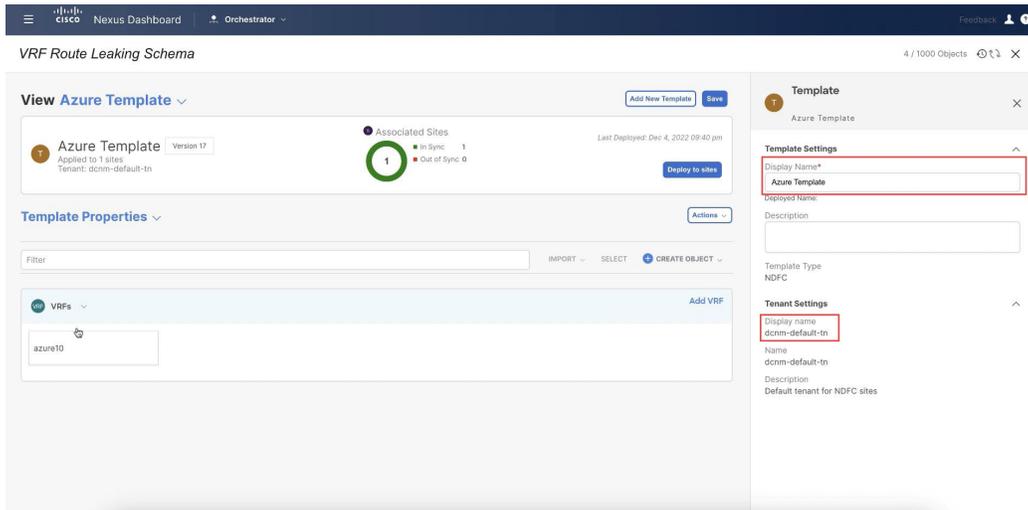
このセクションでは、Azure サイトに関連付けられる Azure テンプレートを構成します。

### 始める前に

[オンプレミス サイト テンプレートの構成 \(157 ページ\)](#) の手順を実行します。

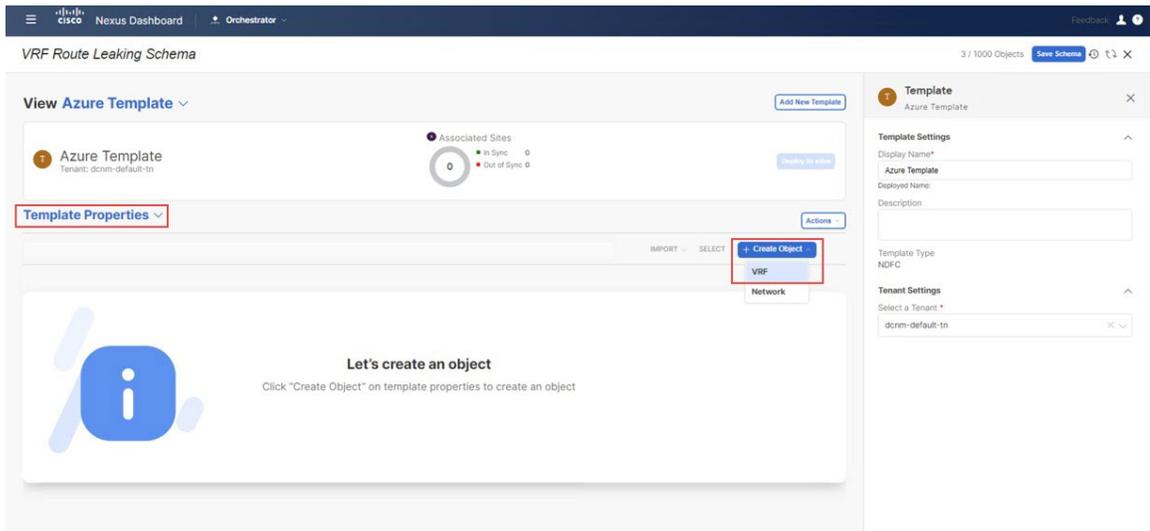
- ステップ 1 [VRF ルート リーク スキーマ (VRF Route Leaking Schema) ] スキーマの下で[新しいテンプレートを追加します (Add New Template) ]をクリックします。
- ステップ 2 NDFC テンプレートを選択します。
- ステップ 3 [表示名 (Display Name) ]フィールドに名前を入力して、Azure サイトのNDFCタイプのテンプレートを作成します (例: [Azure テンプレート (Azure Template) ] )。
- ステップ 4 テナントにテンプレートをマップするために[テナントを選択 (Select a Tenant) ]フィールド内の dcnm-default-tn テナントを選択します。

図 178:



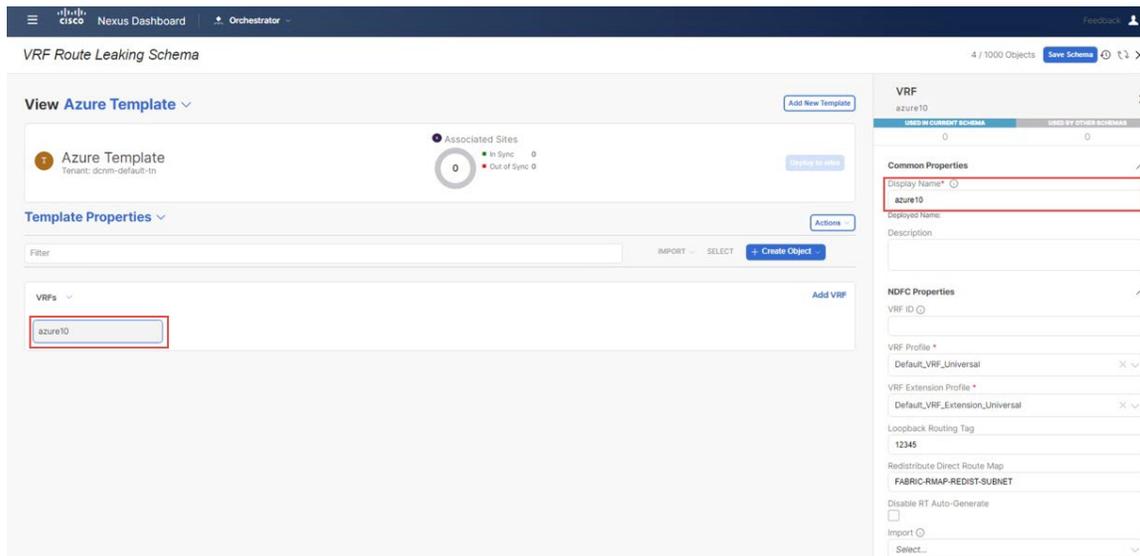
ステップ 5 [テンプレート プロパティ (Template Properties)] で [オブジェクトの作成 (Create Object)] をクリックし、[VRF] を選択して、Azure サイトで使用される VRF を作成します。

図 179:



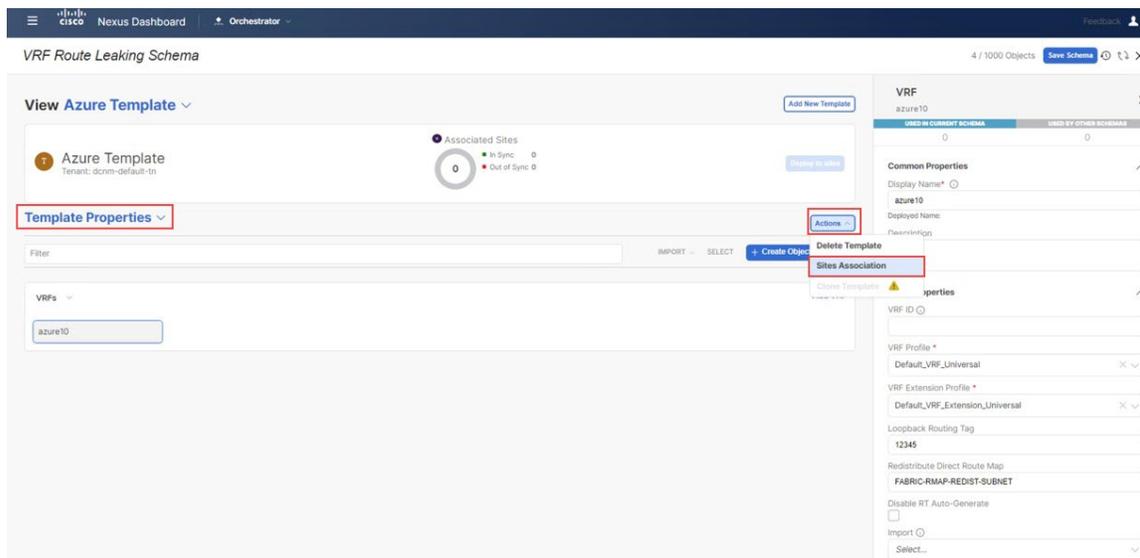
ステップ 6 この VRF の [表示名 (Display Name)] フィールドに名前を入力します (例: azure10)。

図 180:



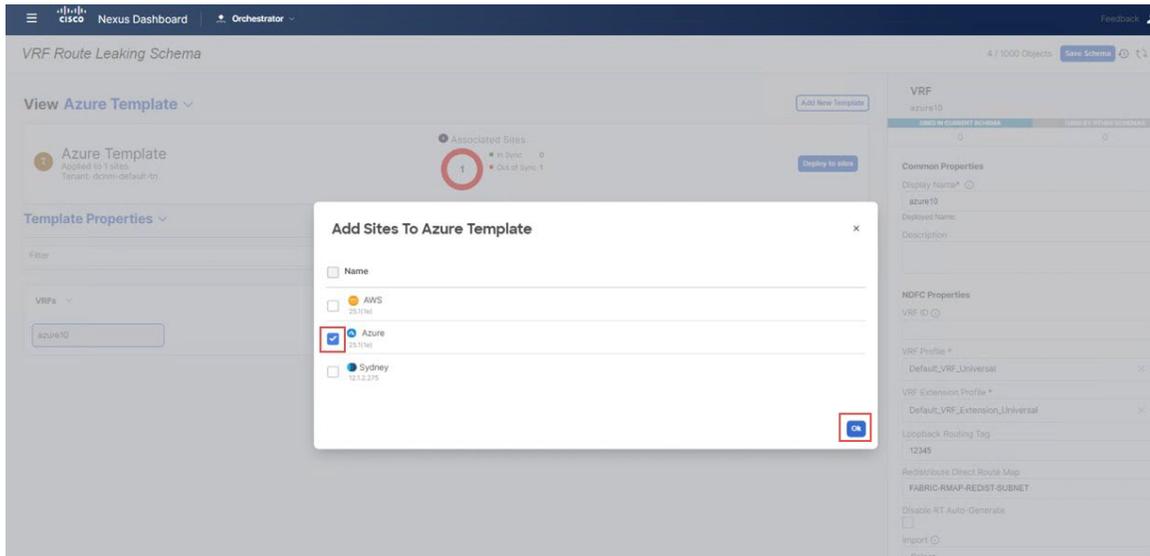
ステップ 7 [テンプレートプロパティ (Template Properties)] エリア内で [アクション (Actions)] > [サイトの関連付け (Sites Association)] をクリックします。

図 181:



ステップ 8 このテンプレートを Azure サイトのみに関連付け、[OK] をクリックします。

図 182:



**ステップ 9** azure10 VRF をクリックし、[リージョンの追加 (Add Region)] をクリックして、選択したリージョンに VNet を作成します。

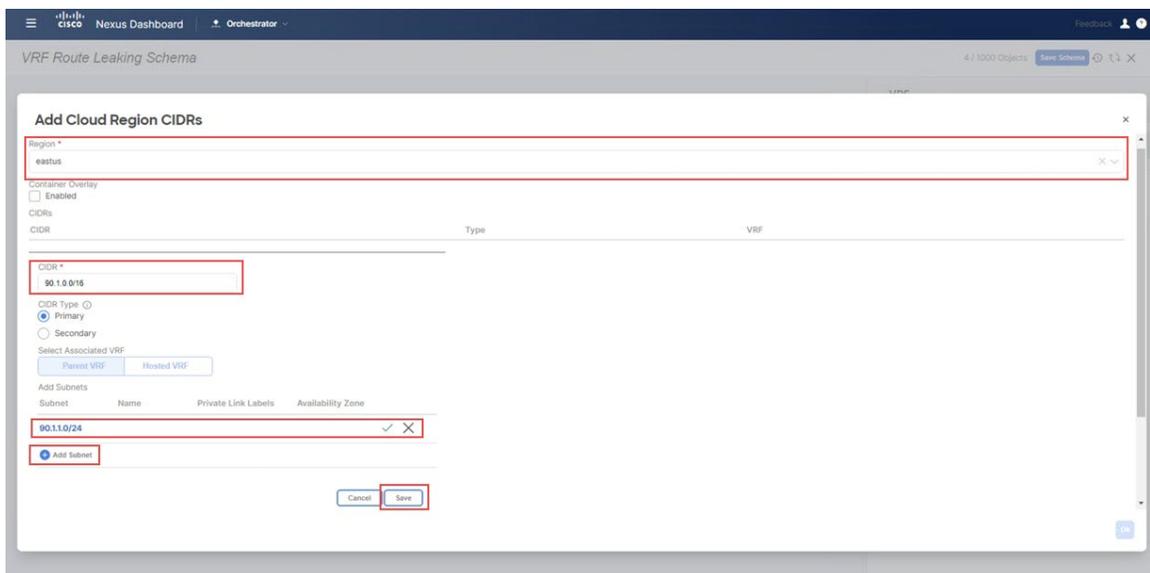
[クラウドリージョン CIDRs を追加 (Add Cloud Region CIDRs)] ウィンドウが表示されます。

**ステップ 10** [リージョン (Region)] フィールド内で VNet を作成したいリージョンを選択します。

**ステップ 11** CIDR フィールド内で [CIDR を追加 (Add CIDRs)] をクリックし、VNet の CIDR ブロックを定義します。

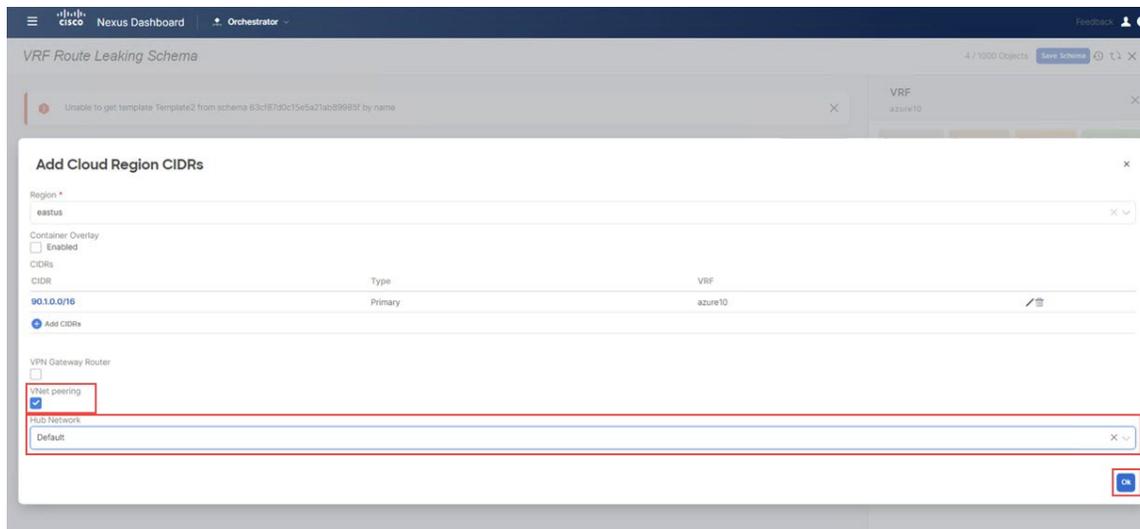
**ステップ 12** サブネットを作成するために [サブネットを追加 (Add Subnet)] をクリックし、[保存 (Save)] をクリックします。

図 183:



**ステップ 13** [VNet ピアリング (VNet Peering)] フィールドの下にあるチェックボックスをオンにして、Azure 用の Cisco クラウド ネットワーク コントローラで作成されたハブ ネットワークを選択します。

図 184:



**ステップ 14** [OK] をクリックします。  
Azure テンプレート ウィンドウに戻ります。

**ステップ 15** Azure サイトの横にある矢印をクリックし、ドロップダウン メニューから [テンプレートのプロパティ (Template Properties)] を選択します。

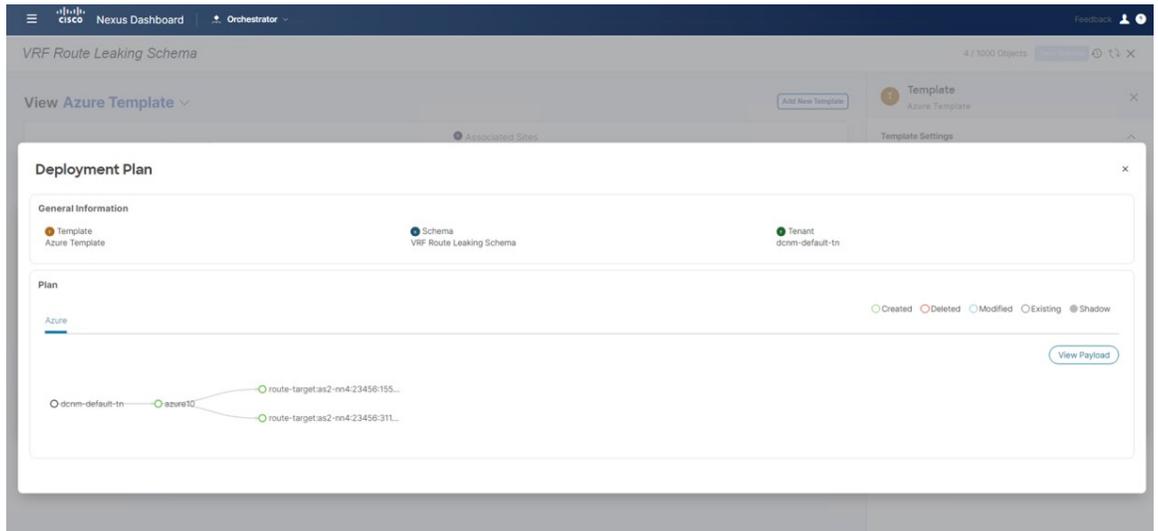
**ステップ 16** [サイトに展開 (Deploy to Sites)] をクリックします。

**ステップ 17** [Azure テンプレート (Azure Template)] をサイトに展開します。

- 追加認証のために[展開プラン (Deployment Plan)]をクリックします。

Azure サイトをクリックして、その特定のサイトの展開計画を表示します。

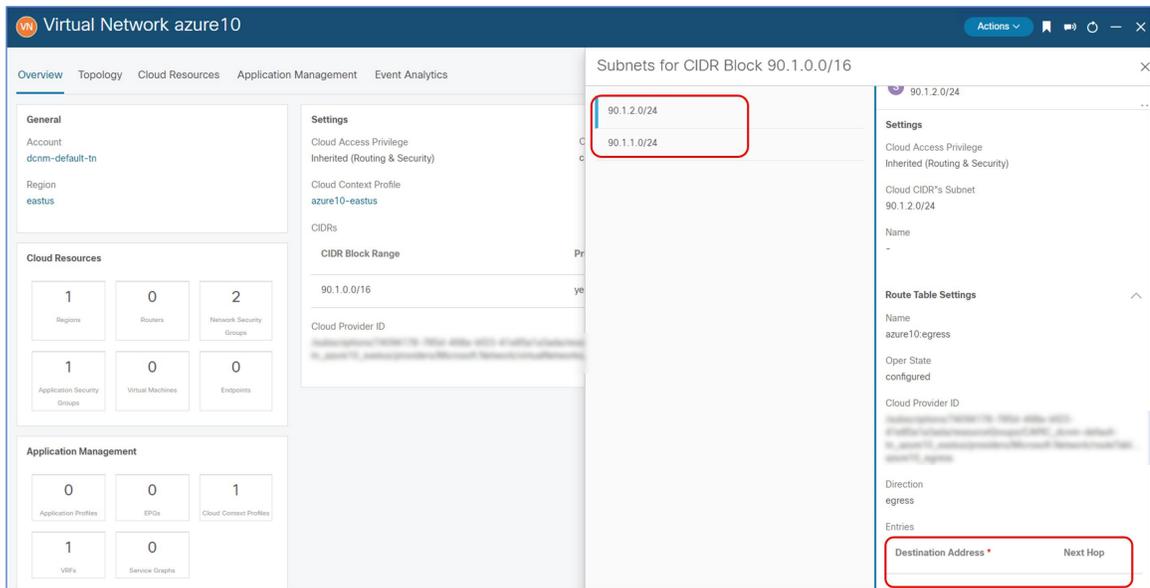
図 185 :



- [展開 (Deploy) ] をクリックして、NDO が NDFC に構成をプッシュします。

構成が正しくプッシュされたことを確認するには、Azureに展開されたクラウドネットワークコントローラに接続し、クラウド技術情報の > 仮想ネットワークに移動してから、azure10 VNet をクリックし、概要ページの情報を使用して追加の確認を行います。

図 186 :



プロセスのこの時点では宛先アドレスが構成されていないため、Azure サイトはプロセスのこの時点ではまだ他のサイトと通信できないことに注意してください。この宛先アドレス構成は、ルートリーク手順が完了した後にプッシュされます。

### 次のタスク

[AWS サイトテンプレートの構成 \(172 ページ\)](#) の手順を実行します。

## AWS サイトテンプレートの構成

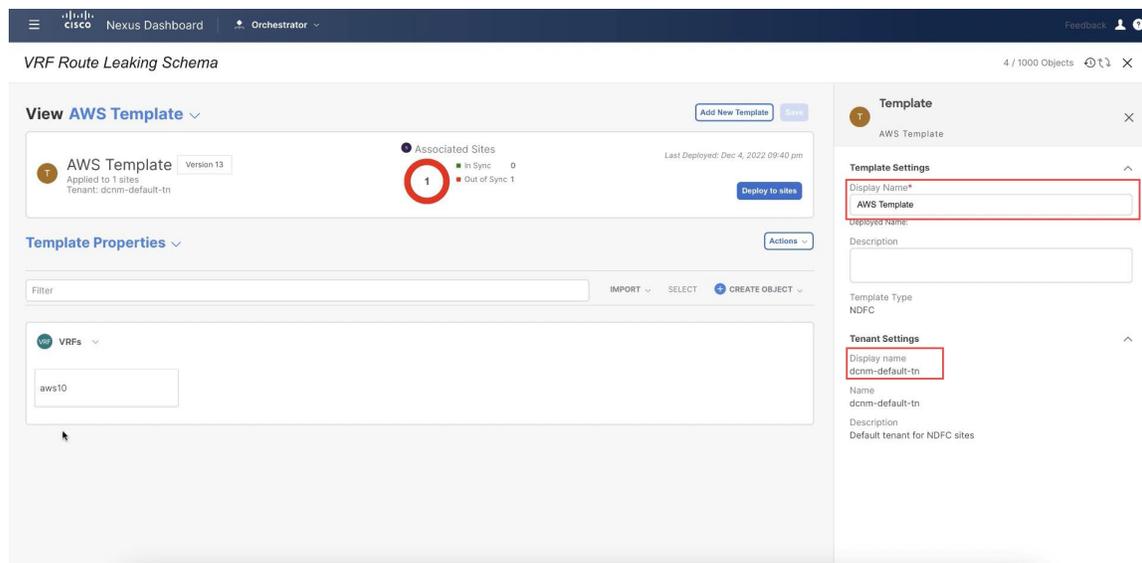
このセクションでは、AWS サイトに関連付けられる [AWS テンプレート (AWS Template)] を構成します。

### 始める前に

[Azure サイトテンプレートの構成 \(166 ページ\)](#) の手順を実行します。

- ステップ 1** [VRF ルートリークスキーマ (VRF Route Leaking Schema)] スキーマの下で**[新しいテンプレートを追加します (Add New Template)]** をクリックします。
- ステップ 2** NDFC テンプレートを選択します。
- ステップ 3** **[表示名 (Display Name)]** フィールドに名前を入力して、AWS サイトの NDFC タイプのテンプレートを作成します (例: [AWS テンプレート (AWS Template)])。
- ステップ 4** テナントにテンプレートをマップするために**[テナントを選択 (Select a Tenant)]** フィールド内の dcnm-default-tn テナントを選択します。

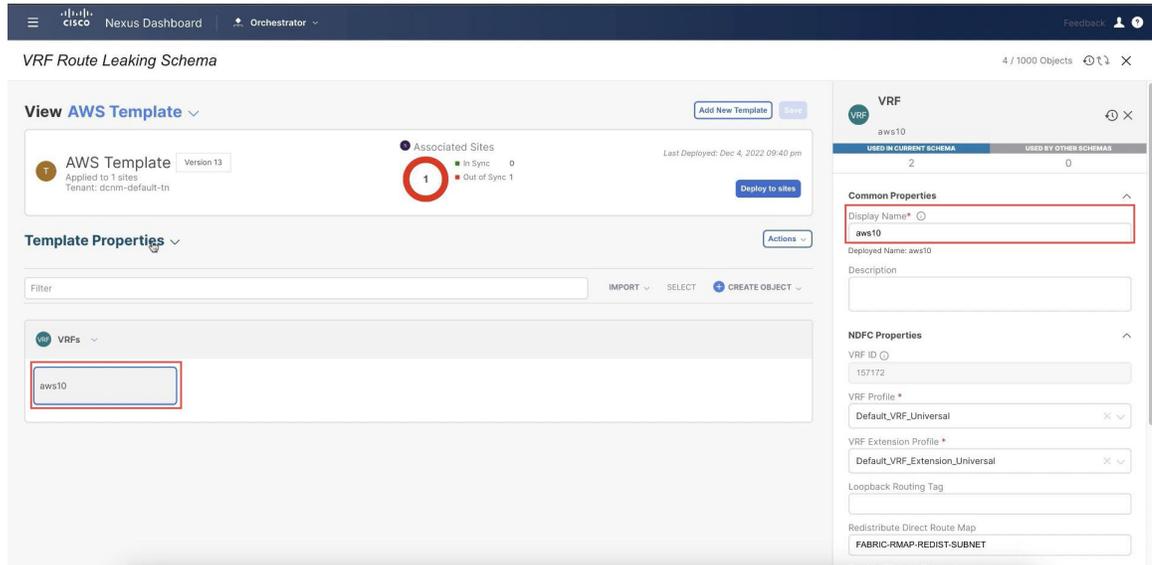
図 187:



ステップ5 [テンプレート プロパティ (Template Properties)] で [オブジェクトの作成 (Create Object)] をクリックし、[VRF] を選択して、AWS サイトで使用する VRF を作成します。

ステップ6 この VRF の [表示名 (Display Name)] フィールドに名前を入力します (例: aws10)。

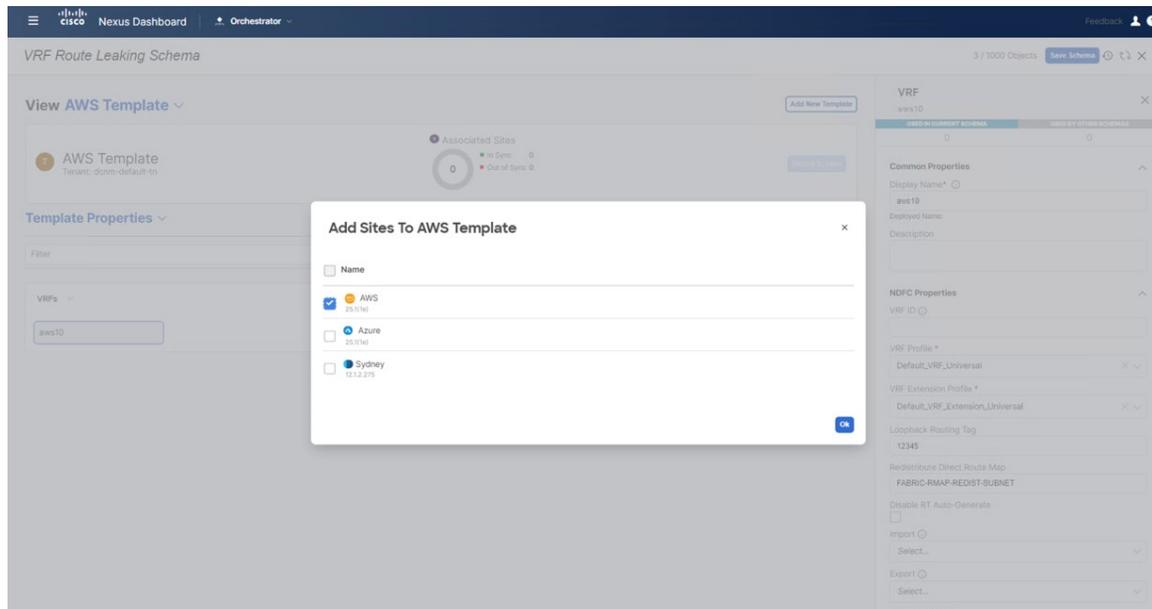
図 188:



ステップ7 [テンプレート プロパティ (Template Properties)] エリア内で [アクション (Actions)] > [サイトの関連付け (Sites Association)] をクリックします。

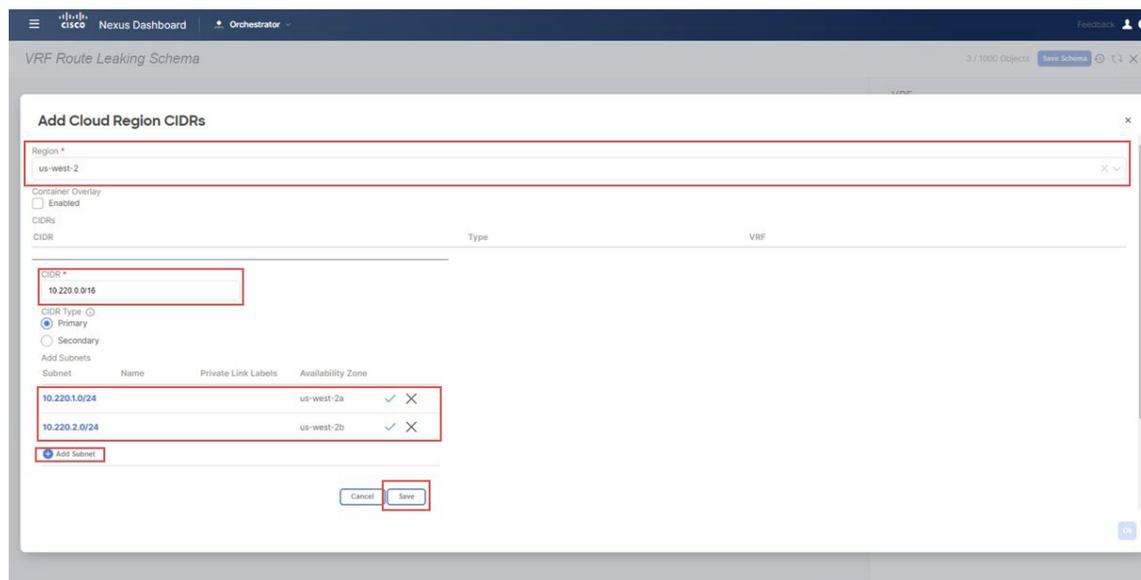
ステップ8 このテンプレートを AWS サイトのみに関連付け、[OK] をクリックします。

図 189:



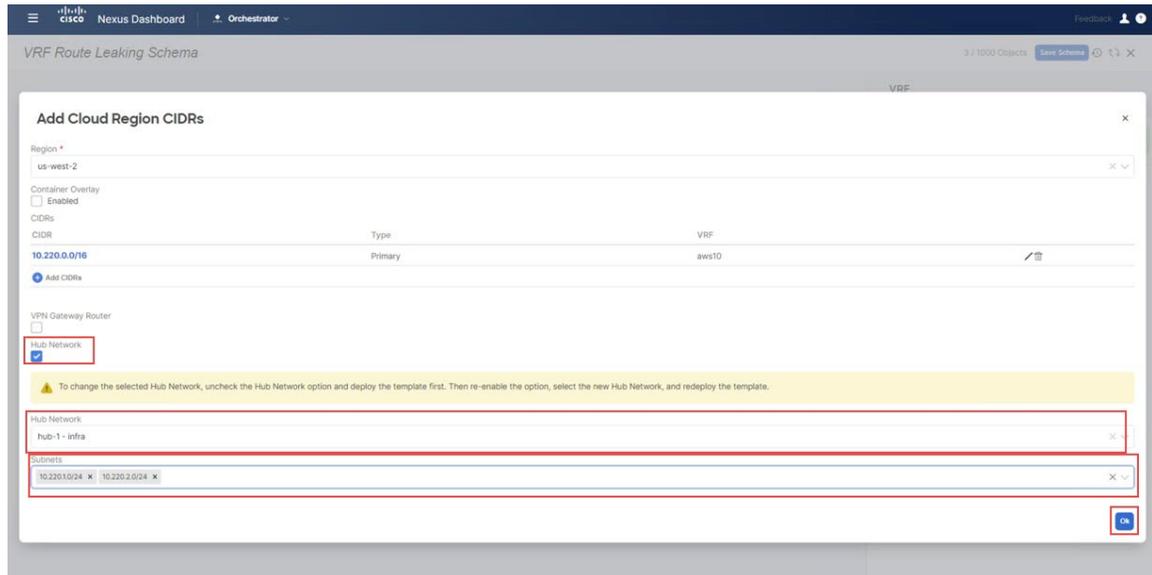
- ステップ 9** [テンプレートのプロパティ (**Template Properties**)] の横にある矢印をクリックし、ドロップダウンメニューから AWS クラウド サイト を選択します。
- ステップ 10** aws10 VRF をクリックし、[リージョンの追加 (**Add Region**)] をクリックして、選択したリージョンに VPC を作成します。  
[クラウドリージョン CIDRs を追加 (**Add Cloud Region CIDRs**)] ウィンドウ が表示されます。
- ステップ 11** [リージョン (**Region**)] フィールド内で VPC を作成したいリージョンを選択します。
- ステップ 12** CIDR フィールド内で [CIDR を追加 (**Add CIDRs**)] をクリックし、VPC の CIDR ブロックを定義します。
- ステップ 13** サブネットを作成するためと可用性ゾーンにマップするために [サブネットを追加 (**Add Subnet**)] をクリックし、[保存 (**Save**)] をクリックします。

図 190:



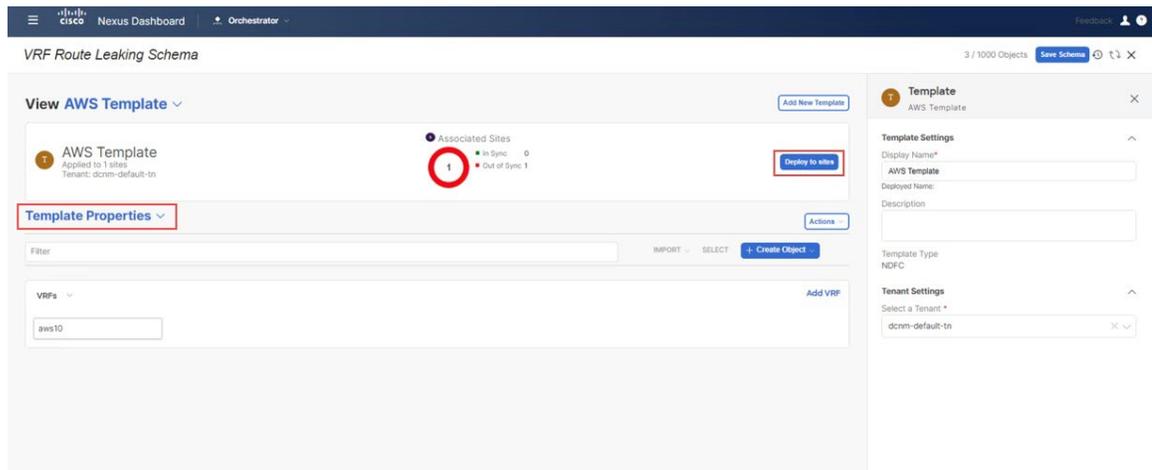
- ステップ 14** [ハブ ネットワーク (**Hub Network**)] フィールドの下にあるチェックボックスをオンにして、AWS 用の Cisco クラウド ネットワーク コントローラで作成されたハブ ネットワークを選択します。  
Cisco クラウド ネットワーク コントローラがサブネットをトランジットゲートウェイに付加することを許可します。これは、トランジットゲートウェイが既に接続のあるサブネットからクラウド上の Cisco Catalyst 8000Vs にトランジットゲートウェイに接続を積み上げます。
- ステップ 15** [サブネット (**Subnet**)] フィールド内でトランジットゲートウェイに使われるサブネットをマップします。  
トランジットゲートウェイに専用のサブネットを使用するのがベストプラクティスです。

図 191:



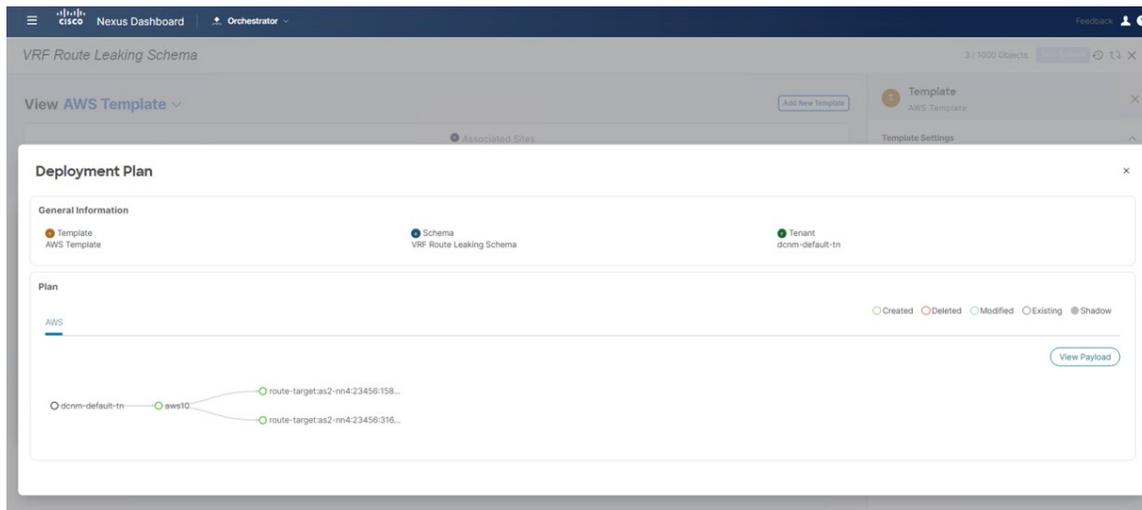
- ステップ 16 [OK] をクリックします。  
AWS テンプレート ウィンドウに戻ります。
- ステップ 17 AWS サイトの横にある矢印をクリックし、ドロップダウンメニューから [テンプレートのプロパティ (Template Properties)] を選択します。
- ステップ 18 [サイトに展開 (Deploy to Sites)] をクリックします。

図 192:



- ステップ 19 [AWS テンプレート (AWS Template)] をサイトに展開します。
- 追加認証のために [展開プラン (Deployment Plan)] をクリックします。  
AWS サイトをクリックして、その特定のサイトの展開プランを表示します。

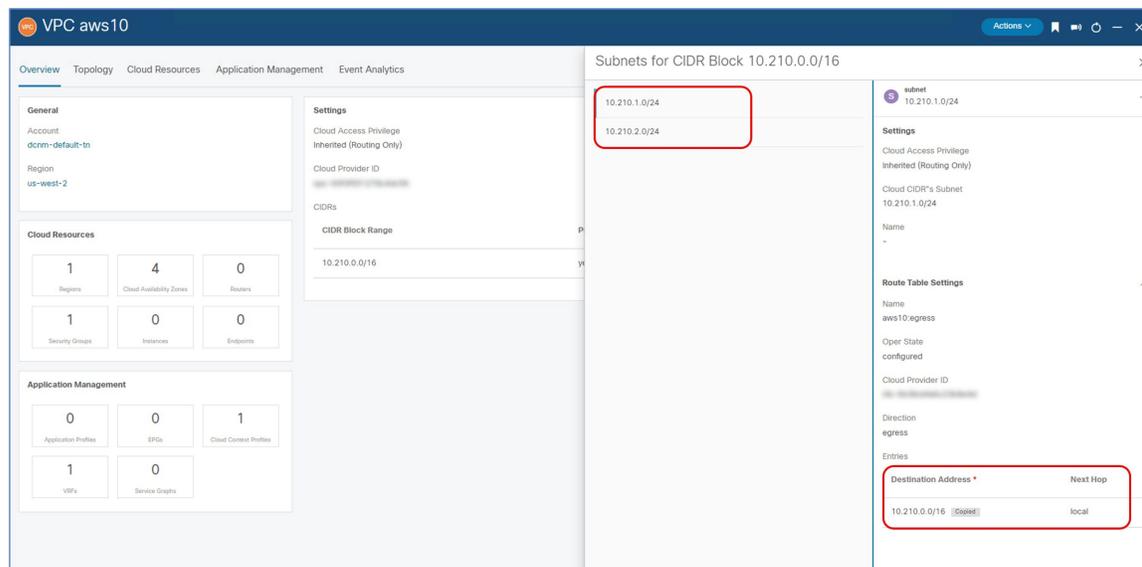
図 193:



- [展開 (Deploy)] をクリックして、NDO が NDFC に構成をプッシュします。

構成が正しくプッシュされたことを確認するには、AWSに展開されたクラウドネットワークコントローラに接続し、クラウド技術情報の > VPC に移動してから、aws10 VPC をクリックし、概要ページの情報を使用して追加の確認を行います。

図 194:



AWS のプロセスのこの時点で宛先アドレスが構成されていることに注意してください。ただし、これは、この AWS サイトがそれ自体と通信できることを示しています。AWS サイトは、プロセスのこの時点ではまだ他のサイトと通信できません。AWS サイトが別のサイトと通信できるようにするために必要な宛先アドレス構成は、ルートリーク手順が完了した後にプッシュされます。

## 次のタスク

[ルートルークの設定（177ページ）](#) で提供されている手順を使用して、ルートルークを設定します。

## ルートルークの設定

ルートルーク ユース ケース の構成するために次のセクションの手順を使用します。

### Azure VRF から NDFC VRF へのルートルークの構成

このセクションでは、Azure VRF (azure10) から NDFC VRF (v10) へのルートルークを構成します。

## 始める前に

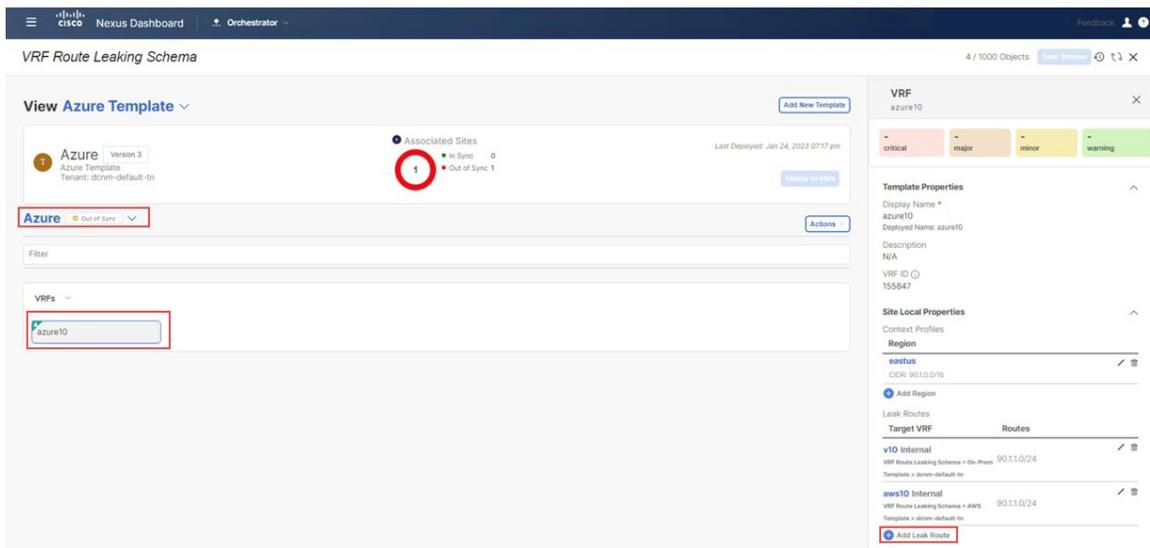
[必要なテンプレートの構成（157ページ）](#) で提供される手順を使用して、必要なテンプレートを構成します。

**ステップ 1** これらの手順で前に構成した Azure テンプレートと、dcnm-default-tn テナントをクリックします。

**ステップ 2** これらの手順で前に構成した azure10 VRF をクリックします。

**ステップ 3** 右のペインで、[リーク ルートを追加 (Add Leak Route)] をクリックします。

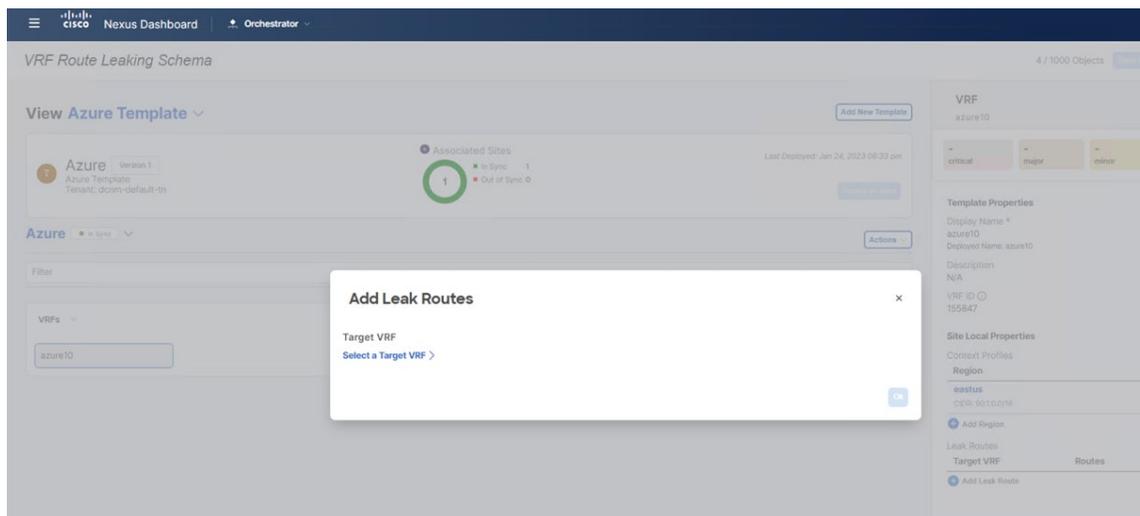
図 195:



[リーク ルートを追加 (Add Leak Routes)] ウィンドウが表示されます。

**ステップ 4** [リーク ルートを追加 (Add Leak Routes)] ウィンドウ内で [ターゲット VRF を選択 (Select a Target VRF)] をクリックします。

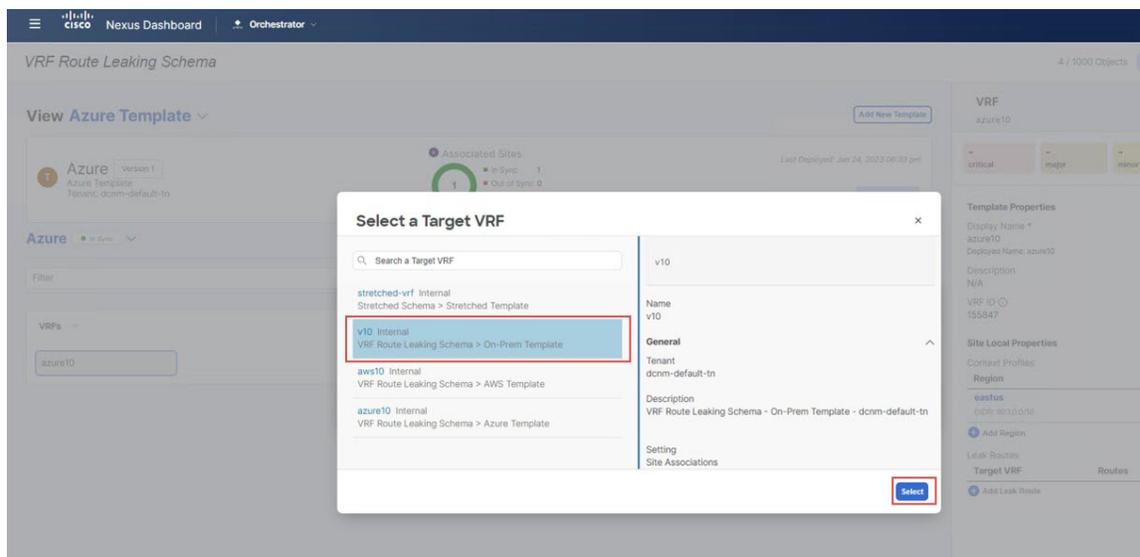
図 196:



[ターゲット VRF を選択 (Select a Target VRF)] ウィンドウが表示されます。

ステップ 5 [ターゲット VRF を選択 (Select a Target VRF)] ページで、ルートをリークしたい NDFC VRF (v10) を選択し、[選択 (Select)] をクリックします。

図 197:

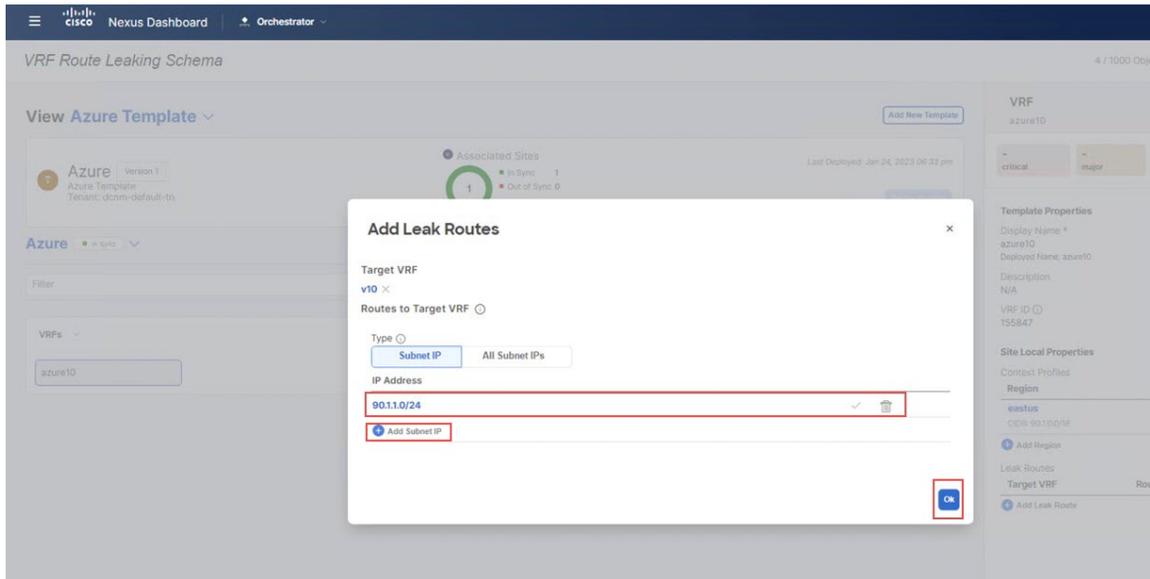


[リーク ルートの追加 (Add Leak Routes)] ウィンドウに戻ります。

ステップ 6 [リーク ルートを追加 (Add Leak Routes)] ウィンドウで [サブネット IP の追加 (Add Subnet IP)] をクリックし、オンプレミスサイトに伝達する Azure クラウドサブネットを追加します。

(注) [サブネット IP を追加 (Add Subnet IP)] オプションは、選択的サブネットのみのリークを許可します。または、全てのプレフィックスが接続先 VRF にリークされる必要のある場合、全てのサブネット IPs オプションを代わりに使用できます。

図 198:



このユースケースの場合、90.1.1.0/24 サブネットを使用します。

**ステップ 7** [OK] をクリックします。

Azure テンプレート ページに戻り、Azure VRF から NDFC VRF へのこのルート リークの構成を確認できます。

### 次のタスク

[Azure VRF から AWS VRF へのルート リークの構成 \(179 ページ\)](#) の手順を実行します。

## Azure VRF から AWS VRF へのルート リークの構成

このセクションでは、Azure VRF (azure10) から AWS VRF (aws10) へのルート リークを構成します。

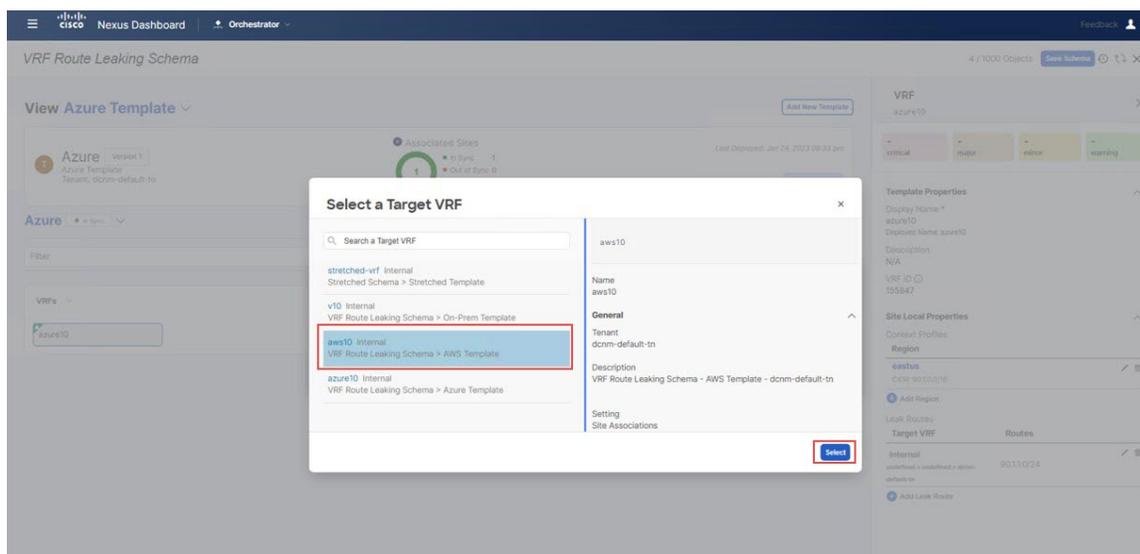
この手順は、[Azure VRF から NDFC VRF へのルート リークの構成 \(177 ページ\)](#) と全く同じ手順を行います、しかしこれらの手順では、違うターゲット VRF (この手順の AWS ターゲット VRF) を選択します。

### 始める前に

[Azure VRF から NDFC VRF へのルート リークの構成 \(177 ページ\)](#) の手順を実行します。

**ステップ 1** [ターゲット VRF の選択 (Select a Target VRF)] ページで、ルートをリークする AWS VRF (aws10) を選択し、[選択 (Select)] をクリックします。

図 199:

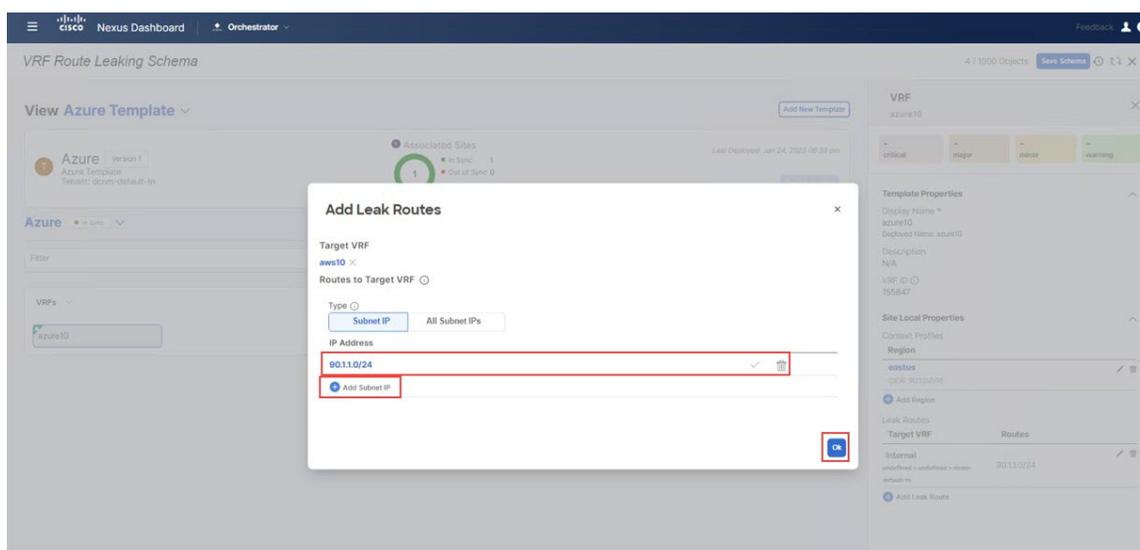


[リークルート追加 (Add Leak Routes)] ウィンドウに戻ります。

**ステップ 2** [リークルート追加 (Add Leak Routes)] ウィンドウ内で AWS クラウドへ伝達したいサブネットを追加します。

このユースケースの場合、90.1.1.0/24 サブネットを使用します。したがって、ドロップダウンメニューをクリックして、90.1.1.0/24 サブネットを選択します。

図 200:



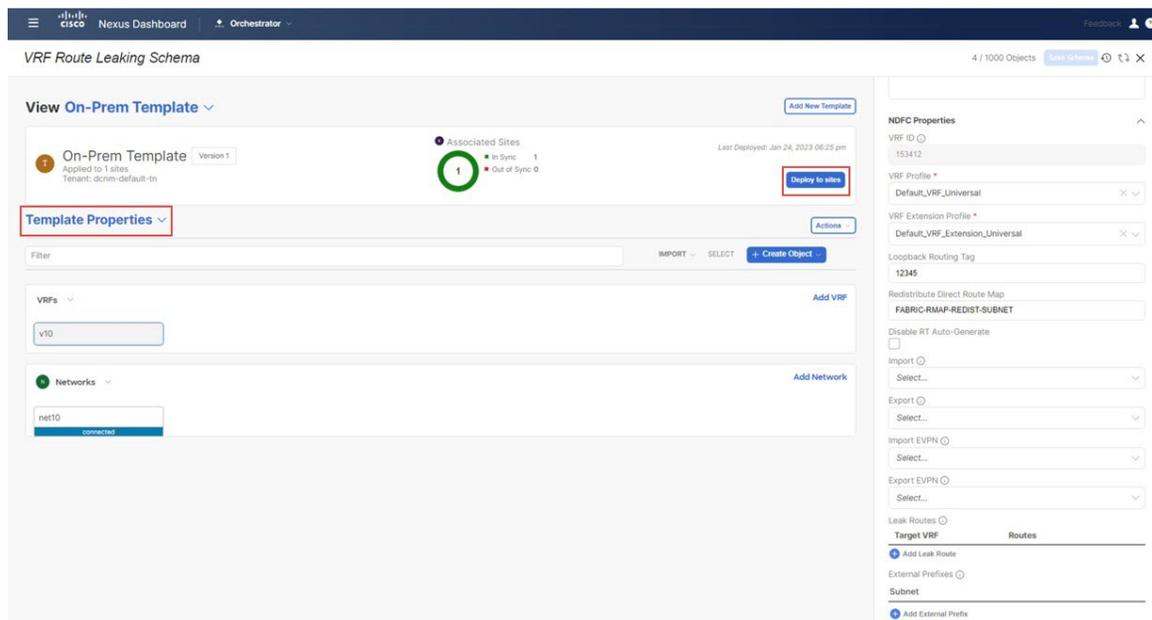
**ステップ 3** [OK] をクリックします。

[Azure テンプレート (Azure Template)] ページに戻ります。ここでは、Azure VRF から AWS VRF へのこのルート リークの構成と前のステップのセットで構成した Azure VRF から NDFC VRF へのルート リークを確認できます。

**ステップ 4** Azure サイトの横にある矢印をクリックし、ドロップダウンメニューから [テンプレートのプロパティ (Template Properties)] を選択します。

**ステップ 5** [サイトへ展開 (Deploy to sites)] をクリックします。

図 201:

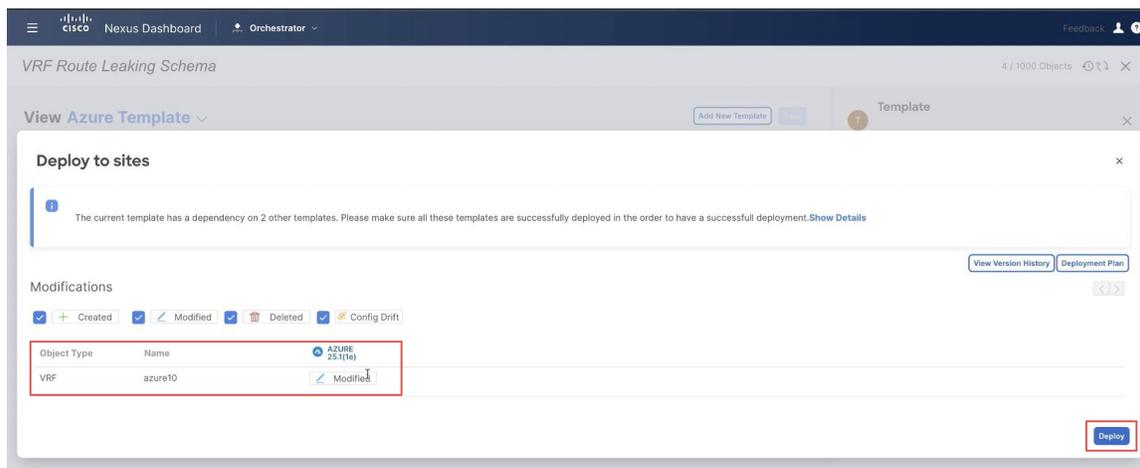


[サイトへ展開 (Deploy to sites)] ウィンドウが表示され、テンプレートが展開される場所を表示します。

**ステップ 6** [展開プラン (Deployment Plan)] を追加認証のためにクリックします。そして、その特定のサイトの展開プランを表示するためにそのサイトをクリックします。

**ステップ 7** [展開 (Deploy)] を NDO が構成をサイト固有のコントローラにプッシュするためにクリックします。

図 202:



### 次のタスク

[AWS VRF から NDFC VRF へのルート リークの構成 \(182 ページ\)](#) の手順を実行します。

## AWS VRF から NDFC VRF へのルート リークの構成

このセクションでは、AWS VRF (aws10) から NDFC VRF (v10) へのルート リークを構成します。

### 始める前に

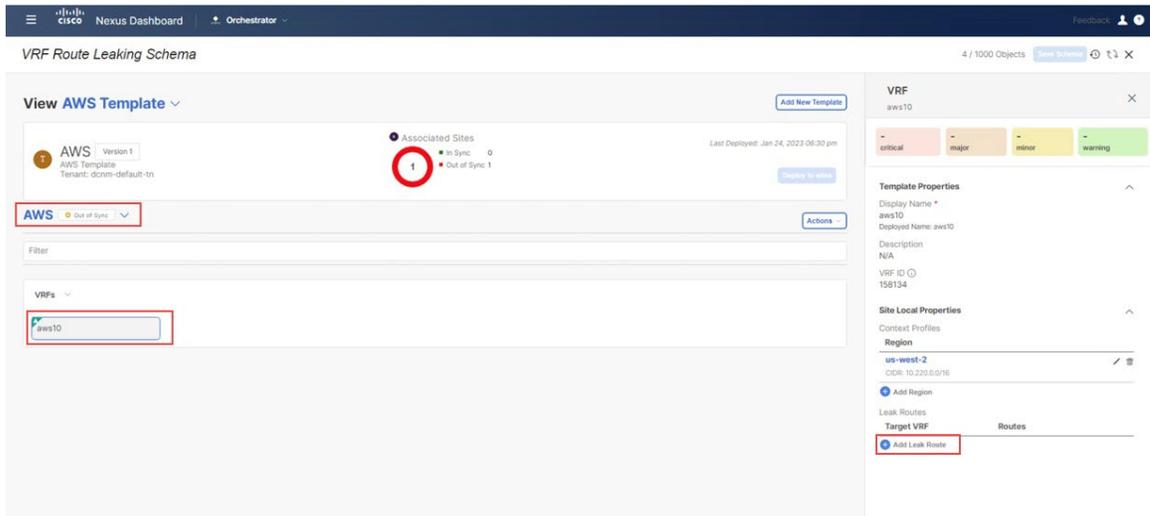
[Azure VRF から AWS VRF へのルート リークの構成 \(179 ページ\)](#) の手順を実行します。

**ステップ 1** これらの手順で前に構成した AWS テンプレートと、`dcnm-default-tn` テナントをクリックします。

**ステップ 2** これらの手順で前に構成した `aws10 VRF` をクリックします。

**ステップ 3** 右のペインで、[リーク ルートを追加 (Add Leak Route)] をクリックします。

図 203:



[リーク ルートを追加 (Add Leak Routes)] ウィンドウが表示されます。

ステップ 4 [リーク ルートを追加 (Add Leak Routes)] ウィンドウ内で [ターゲット VRF を選択 (Select a Target VRF)] をクリックします。

[ターゲット VRF を選択 (Select a Target VRF)] ウィンドウが表示されます。

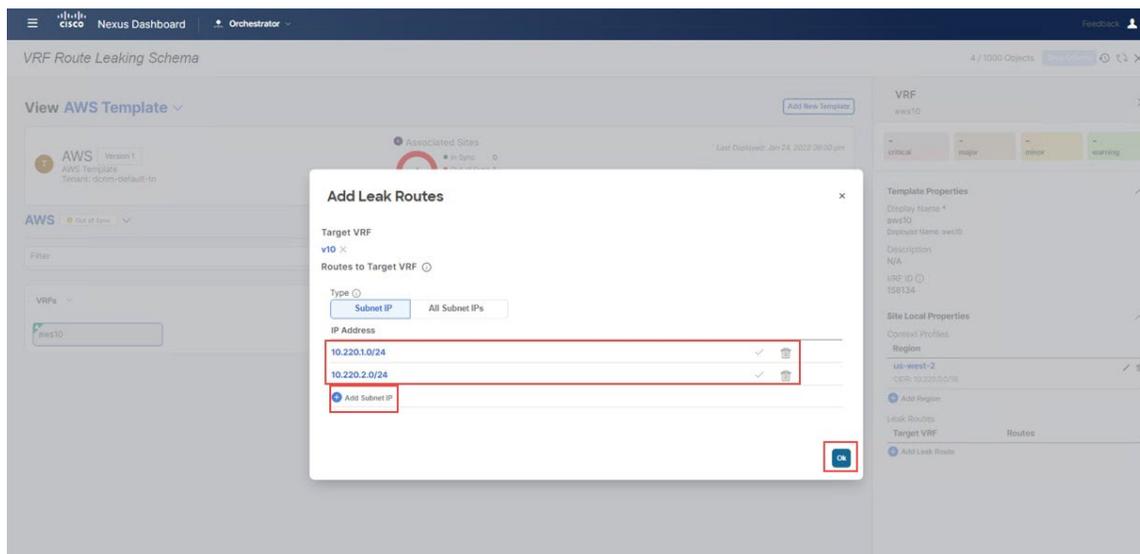
ステップ 5 [ターゲット VRF を選択 (Select a Target VRF)] ウィンドウで、ルートをリークしたい NDFC VRF (v10) を選択し、[選択 (Select)] をクリックします。

[リーク ルートの追加 (Add Leak Routes)] ウィンドウに戻ります。

ステップ 6 [リーク ルートを追加 (Add Leak Routes)] ウィンドウで [サブネット IP の追加 (Add Subnet IP)] をクリックし、オンプレミス サイトに伝達する AWS クラウド サブネットを追加します。

(注) [サブネット IP を追加 (Add Subnet IP)] オプションは、選択的サブネットのみのリークを許可します。または、全てのプレフィックスが接続先 VRF にリークされる必要のある場合、全てのサブネット IPs オプションを代わりに使用できます。

図 204 :



このユースケースには、次のサブネットを使用します：

- 10.220.1.0/24
- 10.220.2.0/24

**ステップ 7** [OK] をクリックします。

AWS テンプレート ページに戻り、AWS VRF から NDFC VRF へのこのルートリークの構成を確認できます。

### 次のタスク

[AWS VRF から Azure VRF へのルートリークの構成 \(184 ページ\)](#) の手順を実行します。

## AWS VRF から Azure VRF へのルートリークの構成

このセクションでは、AWS VRF (aws10) から Azure VRF (azure10) へのルートリークを構成します。

この手順は、[AWS VRF から NDFC VRF へのルートリークの構成 \(182 ページ\)](#) と全く同じ手順を行います、しかしこれらの手順では、違うターゲット VRF (この手順の Azure ターゲット VRF) を選択します。

### 始める前に

[AWS VRF から NDFC VRF へのルートリークの構成 \(182 ページ\)](#) の手順を実行します。

**ステップ 1** [ターゲット VRF の選択 (Select a Target VRF)] ページで、ルートをリークする Azure VRF (azure10) を選択し、[選択 (Select)] をクリックします。

[リーク ルートの追加 (Add Leak Routes)] ウィンドウに戻ります。

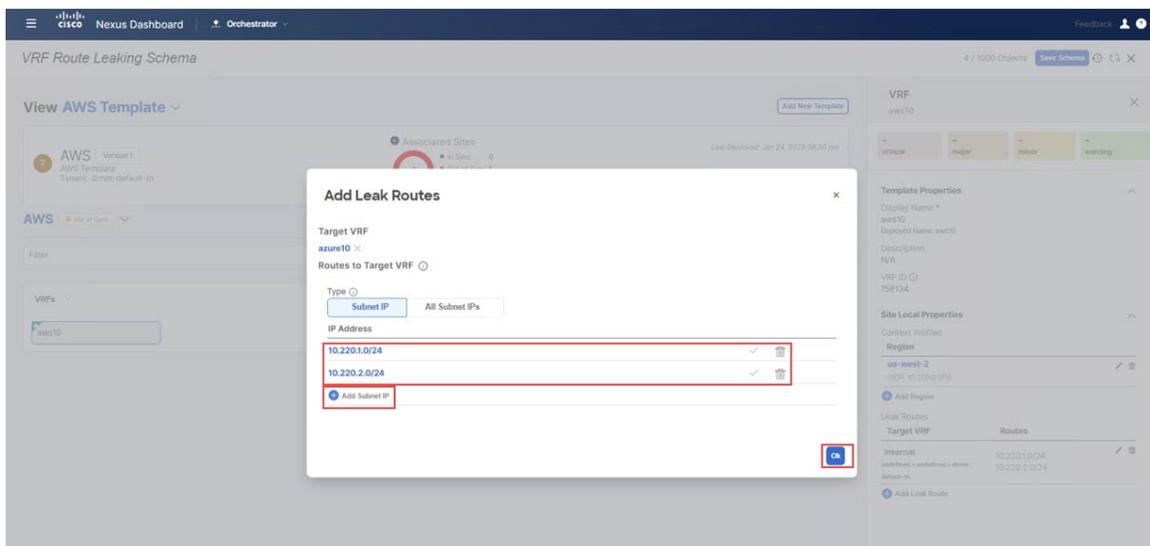
**ステップ 2** [リーク ルートの追加 (Add Leak Routes)] ウィンドウ内で Azure クラウドへ伝達したいサブネットを追加します。

このユース ケースには、次のサブネットを使用します：

- 10.220.1.0/24
- 10.220.2.0/24

したがって、ドロップダウン メニューをクリックして、それらのサブネットを選択します。

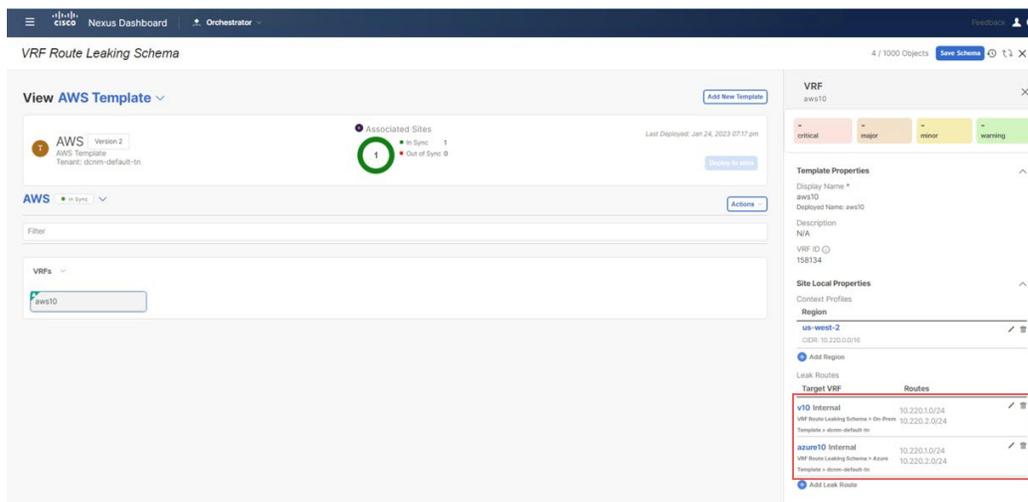
図 205:



**ステップ 3** [OK] をクリックします。

[AWS テンプレート (AWS Template)] ページに戻ります。ここでは、AWS VRF から Azure VRF へのこのルート リークの構成と前のステップのセットで構成した AWS VRF から NDFC VRF へのルート リークを確認できます。

図 206 :



ステップ 4 AWS サイトの横にある矢印をクリックし、ドロップダウンメニューから [テンプレートのプロパティ (Template Properties)] を選択します。

ステップ 5 [サイトへ展開 (Deploy to sites)] をクリックします。

[サイトへ展開 (Deploy to sites)] ウィンドウが表示され、テンプレートが展開される場所を表示します。

ステップ 6 [展開プラン (Deployment Plan)] を追加認証のためにクリックします。そして、その特定のサイトの展開プランを表示するためにそのサイトをクリックします。

ステップ 7 [展開 (Deploy)] を NDO が構成をサイト固有のコントローラ (NDFC とクラウドネットワークコントローラ) にプッシュするためにクリックします。

### 次のタスク

[NDFC VRF から AWS VRF へのルート リークの構成 \(186 ページ\)](#) の手順を実行します。

## NDFC VRF から AWS VRF へのルート リークの構成

このセクションでは、NDFC VRF (v10) から AWS VRF (aws10) へのルート リークを構成します。

### 始める前に

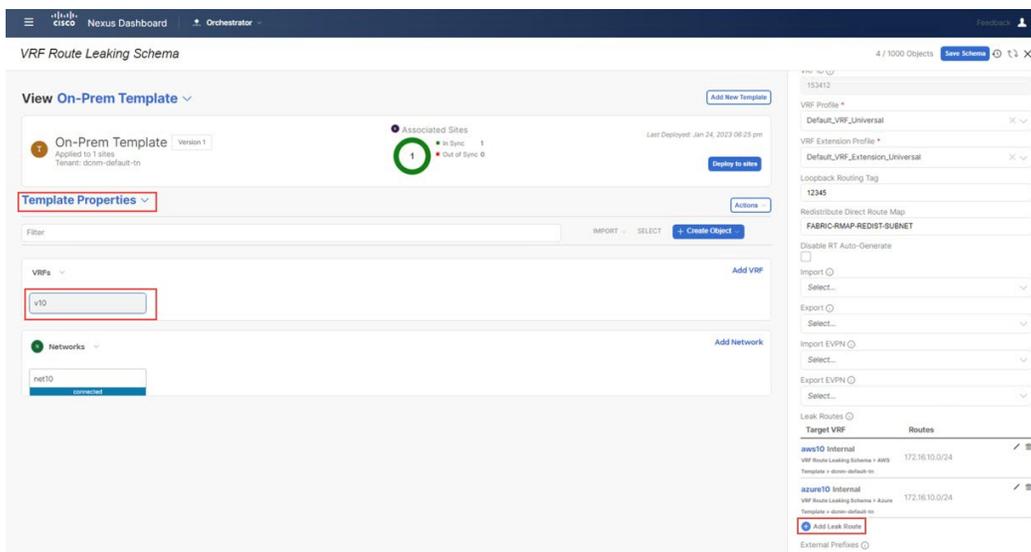
[AWS VRF から Azure VRF へのルート リークの構成 \(184 ページ\)](#) の手順を実行します。

ステップ 1 これらの手順で前に構成した [オンプレミス テンプレート (On-Prem Template)] と dcnm-default-tn テナントをクリックします。

ステップ 2 これらの手順で前に構成した v10 VRF をクリックします。

ステップ3 右のペインで、[リーク ルートを追加 (Add Leak Route)] をクリックします。

図 207:



[リーク ルートを追加 (Add Leak Routes)] ウィンドウが表示されます。

ステップ4 [リーク ルートを追加 (Add Leak Routes)] ウィンドウ内で [ターゲット VRF を選択 (Select a Target VRF)] をクリックします。

[ターゲット VRF を選択 (Select a Target VRF)] ウィンドウが表示されます。

ステップ5 [ターゲット VRF を選択 (Select a Target VRF)] ウィンドウで、ルートをリークする AWS クラウド サイト VRF (aws10) を選択し、[選択 (Select)] をクリックします。

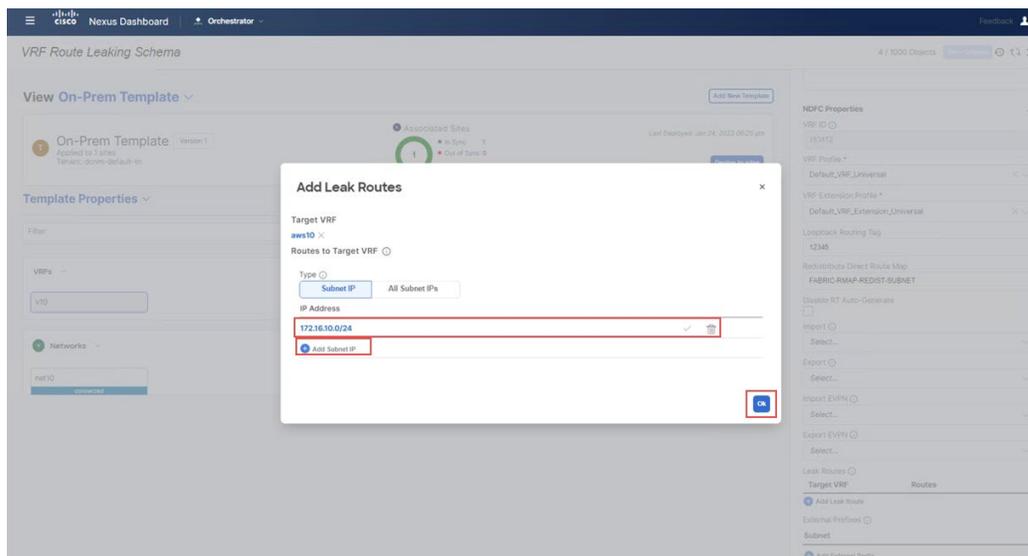
[リーク ルートの追加 (Add Leak Routes)] ウィンドウに戻ります。

ステップ6 [リーク ルートを追加 (Add Leak Routes)] ウィンドウで [サブネット IP の追加 (Add Subnet IP)] をクリックし、オンプレミス サイトに伝達する AWS クラウド サブネットを追加します。

(注) [サブネット IP を追加 (Add Subnet IP)] オプションは、選択的サブネットのみのリークを許可します。または、全てのプレフィックスが接続先 VRF にリークされる必要がある場合、全てのサブネット IPs オプションを代わりに使用できます。

このユースケースでは、172.16.10.0/24 サブネットを使用します。

図 208 :



ステップ 7 [OK] をクリックします。

[オンプレミス テンプレート (On-Prem Template)] ページに戻り、NDFC VRF から AWS VRF へのこのルートリークの構成を確認できます。

### 次のタスク

[NDFC VRF から Azure VRF へのルートリークの構成 \(188 ページ\)](#) の手順を実行します。

## NDFC VRF から Azure VRF へのルートリークの構成

このセクションでは、NDFC VRF (v10) から Azure VRF (azure10) へのルートリークを構成します。

この手順は、[NDFC VRF から AWS VRF へのルートリークの構成 \(186 ページ\)](#) と全く同じ手順を行います、しかしこれらの手順では、違うターゲット VRF (この手順の Azure ターゲット VRF) を選択します。

### 始める前に

[NDFC VRF から AWS VRF へのルートリークの構成 \(186 ページ\)](#) の手順を実行します。

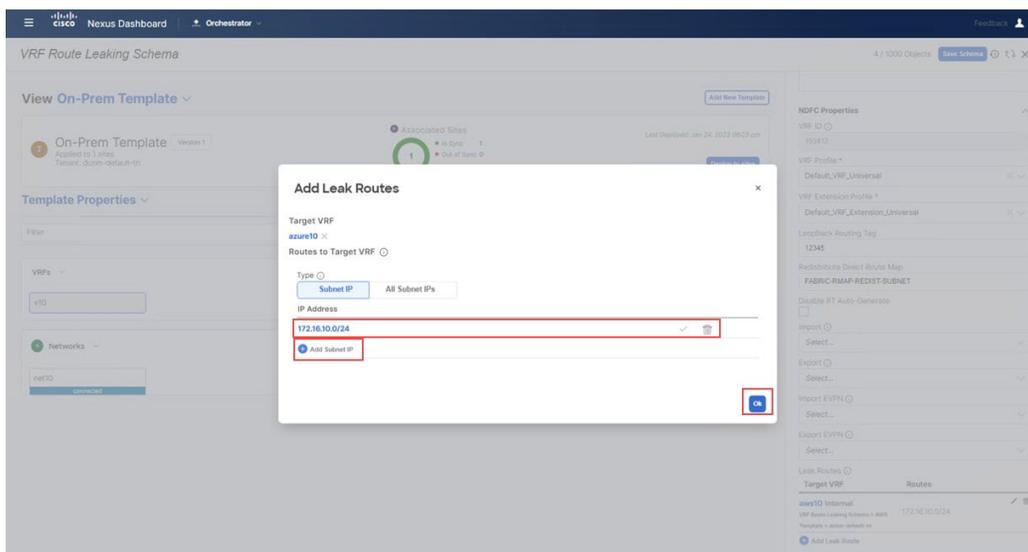
ステップ 1 [ターゲット VRF の選択 (Select a Target VRF)] ウィンドウで、ルートをリークする Azure VRF (azure10) を選択し、[選択 (Select)] をクリックします。

[リーク ルートの追加 (Add Leak Routes)] ウィンドウに戻ります。

**ステップ 2** [リークルート追加 (Add Leak Routes)] ウィンドウ内で Azure クラウドへ伝達したいサブネットを追加します。

このユースケースでは、172.16.10.0/24 サブネットを使用します。したがって、ドロップダウンメニューをクリックして、172.16.10.0/24 サブネットを選択します。

図 209:



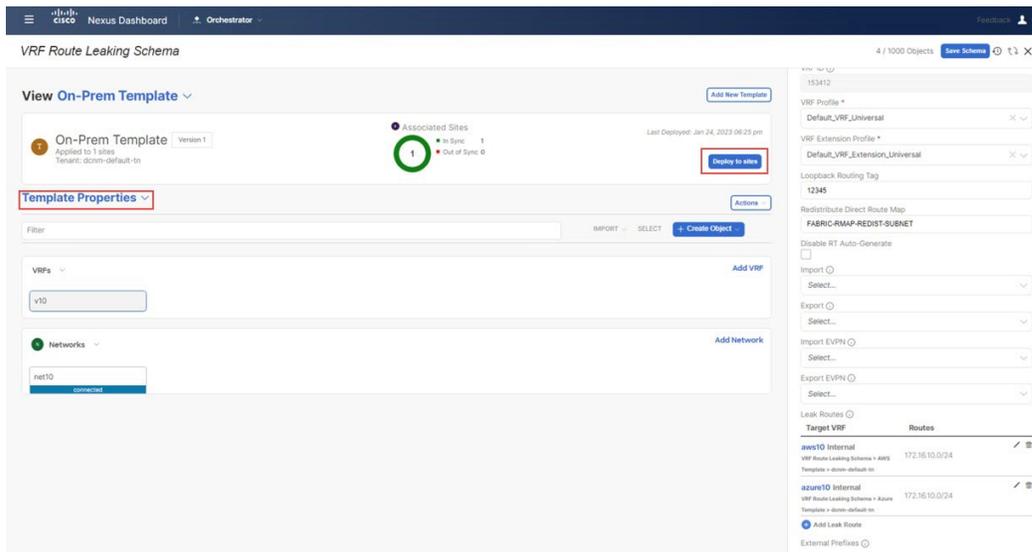
**ステップ 3** [OK] をクリックします。

[オンプレミス テンプレート (On-Prem Template)] ページに戻ります。ここでは、NDFC VRF から Azure VRF へのこのルート リークの構成と前のステップのセットで構成した NDFC VRF から AWS VRF へのルート リークを確認できます。

**ステップ 4** オンプレミス サイトの横にある矢印をクリックし、ドロップダウンメニューから [テンプレートのプロパティ (Template Properties)] を選択します。

**ステップ 5** [サイトへ展開 (Deploy to sites)] をクリックします。

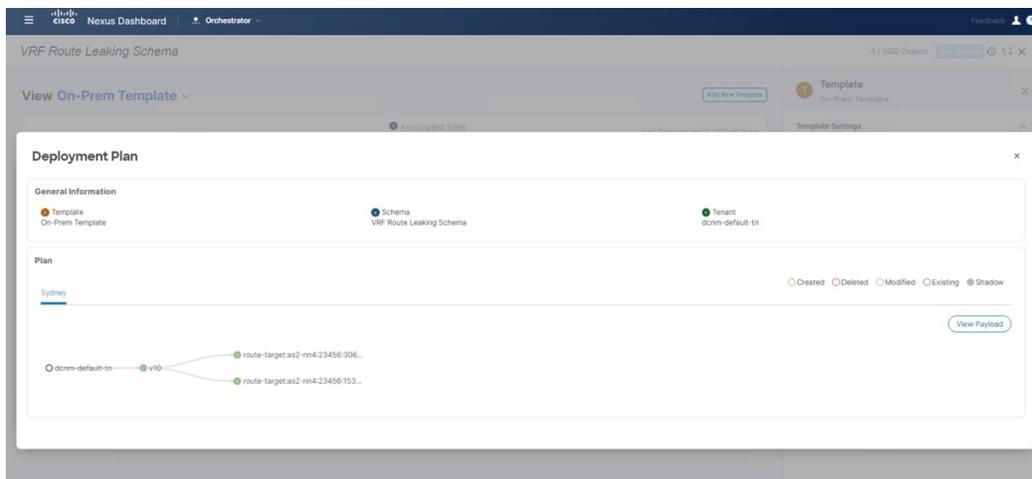
図 210:



[サイトへ展開 (Deploy to sites)] ウィンドウが表示され、テンプレートが展開される場所を表示します。

ステップ 6 [展開プラン (Deployment Plan)] を追加認証のためにクリックします。そして、その特定のサイトの展開プランを表示するためにそのサイトをクリックします。

図 211:



ステップ 7 [展開 (Deploy)] を NDO が構成をサイト固有のコントローラ (NDFC とクラウドネットワークコントローラ) にプッシュするためにクリックします。

次のタスク

構成の確認 (191 ページ) で提供された手順を使用して構成の展開が成功したことを検証します。

## 構成の確認

このセクションでは、構成が正常に展開されたことを確認します。これらの各検証ステップでは、表示されているこのユースケースの構成のために特定のコマンドが使用されることにご注意ください。構成に基づいて各コマンドの適切な変数を入れ替えます。

始める前に

[NDFC VRF から Azure VRF へのルートリークの構成 \(188 ページ\)](#) の手順を実行します。

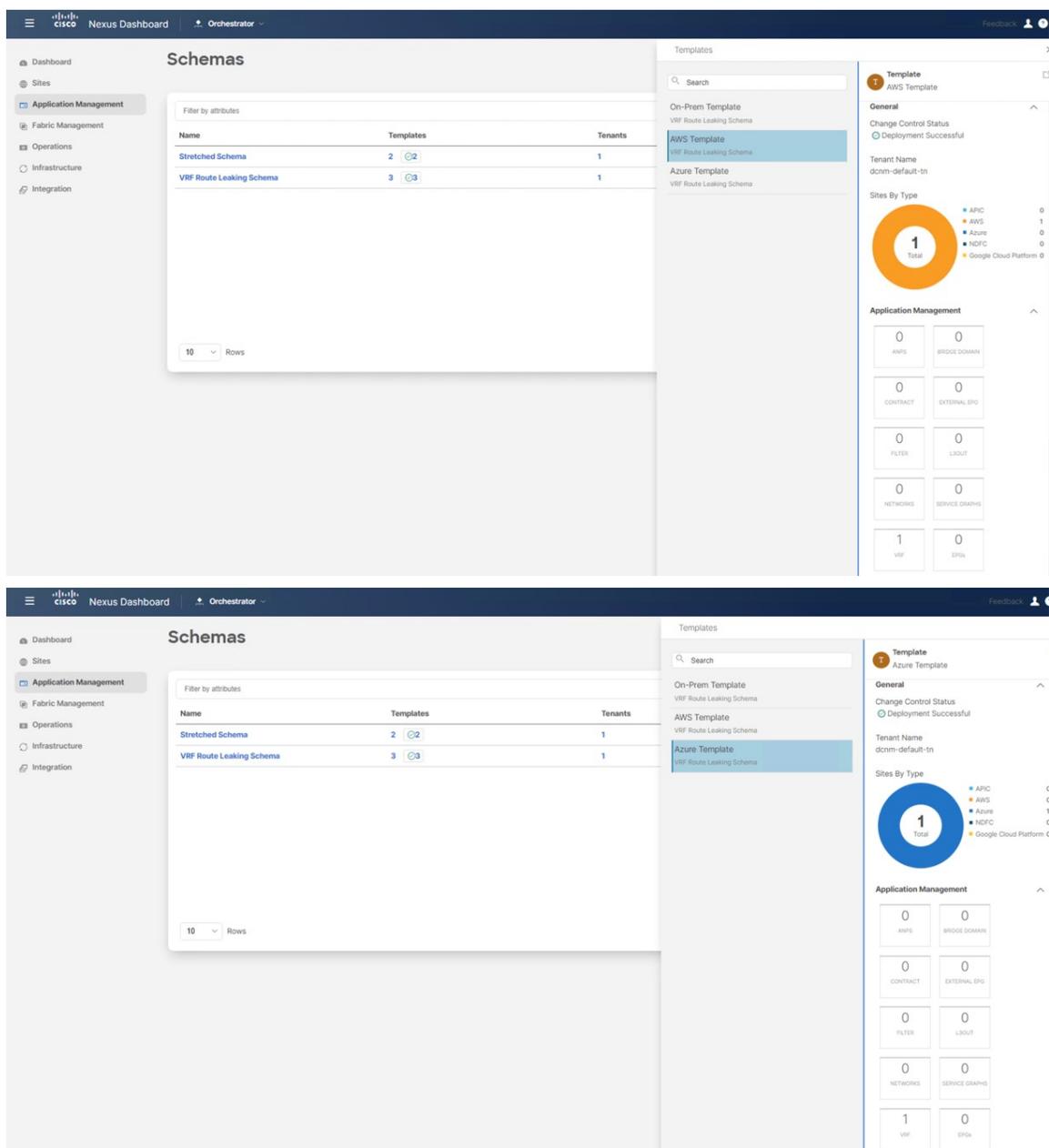
ステップ 1 NDO の構成を確認します。

The top screenshot shows the 'Schemas' page in the Cisco Nexus Dashboard Orchestrator. The main content area displays a table with the following data:

| Name                     | Templates | Tenants |
|--------------------------|-----------|---------|
| Stretched Schema         | 2         | 1       |
| VRF Route Leaking Schema | 3         | 1       |

The right sidebar shows the 'Tenants' section for 'dcrn-default-tn', including details like Name, Description, Associated Sites (3 of 4), Associated Users (1 of 1), and Assigned Schemas (5 of 2). A topology diagram is also visible.

The bottom screenshot shows the same 'Schemas' page, but the right sidebar is now displaying 'Templates'. The table in the main content area is identical to the top screenshot. The 'Templates' sidebar lists several templates, including 'On-Prem Template', 'AWS Template', and 'Azure Template'. Below the list, there is a 'Sites By Type' chart showing a total of 1 site, and an 'Application Management' section with various status indicators.



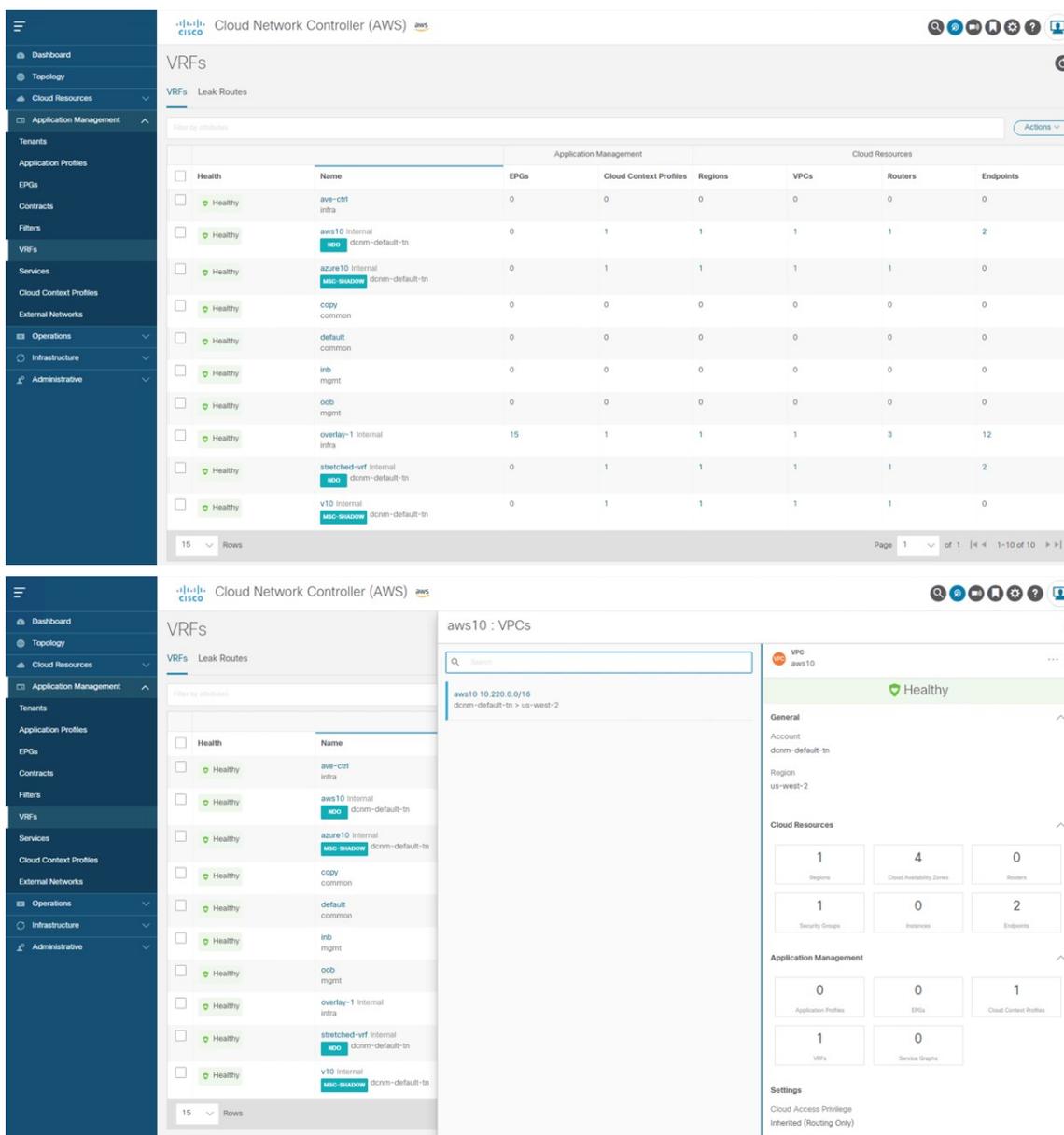
ステップ2 オンプレミスのボーダー ゲートウェイ スパイン デバイスで **sh ip route vrf v10** を入力します。

```
ndfc-leaf1 - SecureCRT
File Edit View Options Transfer Script Tools Window Help
ndfc-est-cbk CatBK-AWS CatBK-AZURE ndfc-leaf1 x ndfc-spine CatBK-AWS (1) CatBK-AWS-2
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
ndfc-leaf1#
ndfc-leaf1#
ndfc-leaf1#
ndfc-leaf1#
ndfc-leaf1#
ndfc-leaf1# sh ip route vrf v10
IP Route Table for VRF "v10"
  ** denotes best ucast next-hop
  *** denotes best mcast next-hop
  '[x/y]' denotes [preference/metric]
  '%<string>' in via output denotes VRF <string>
10.220.1.0/24, ubest/mbest: 1/0
   *via 10.10.0.1%default, [200/0], 03:01:42, bgp-65084, internal, tag 65091, segid: 153412 tunnelid: 0xa0a0001 encap: VXLAN
10.220.2.0/24, ubest/mbest: 1/0
   *via 10.10.0.1%default, [200/0], 03:01:42, bgp-65084, internal, tag 65091, segid: 153412 tunnelid: 0xa0a0001 encap: VXLAN
90.1.1.0/24, ubest/mbest: 1/0
   *via 10.10.0.1%default, [200/0], 03:06:33, bgp-65084, internal, tag 65092, segid: 153412 tunnelid: 0xa0a0001 encap: VXLAN
172.16.10.0/24, ubest/mbest: 1/0, attached
   *via 172.16.10.1, v1an2310, [0/0], 03:23:02, direct, tag 12345
172.16.10.1/32, ubest/mbest: 1/0, attached
   *via 172.16.10.1, v1an2310, [0/0], 03:23:02, local, tag 12345
172.16.10.11/32, ubest/mbest: 1/0, attached
   *via 172.16.10.11, v1an2310, [190/0], 03:20:45, hnm
ndfc-leaf1#
```

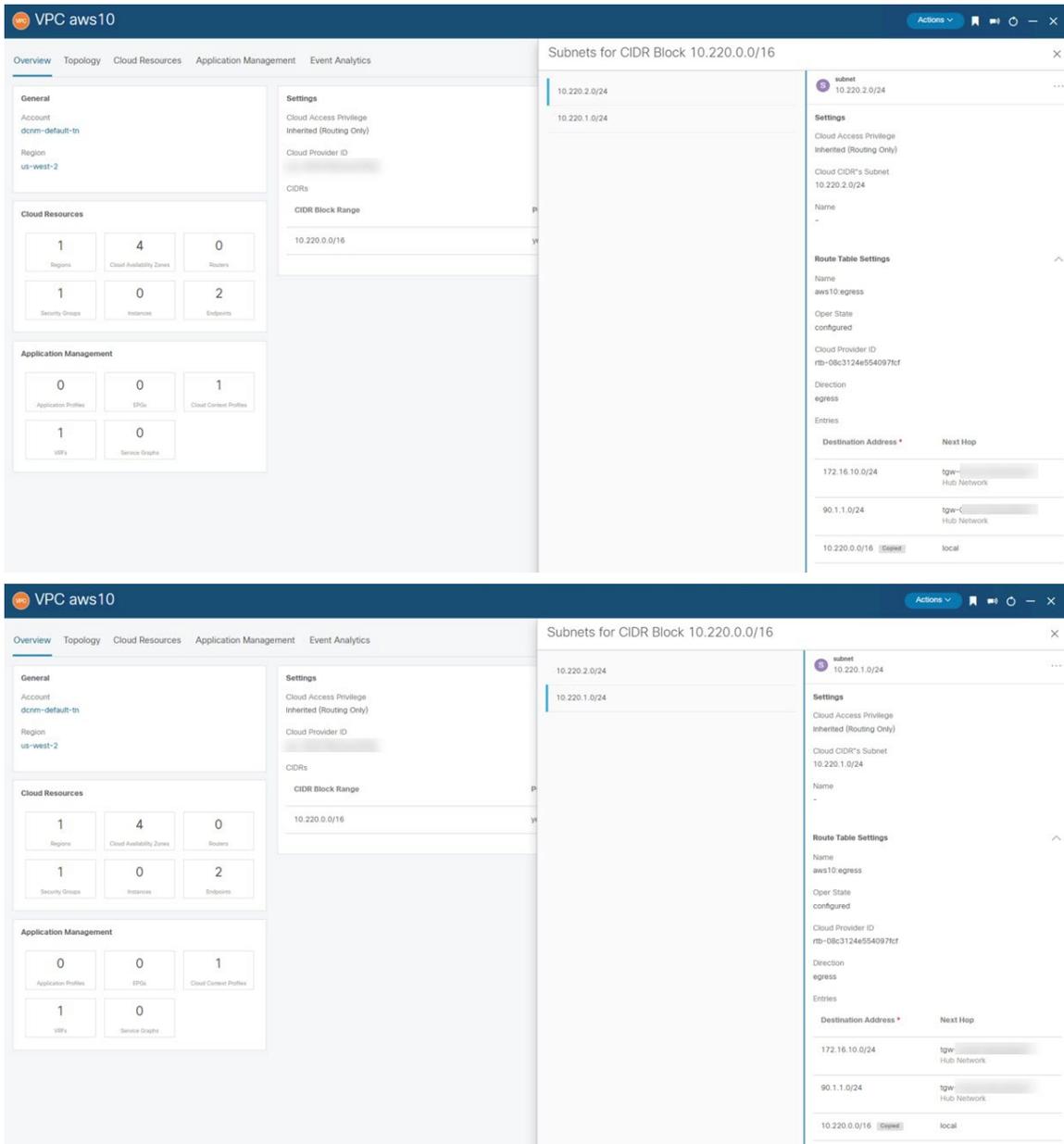
オンプレミスのリーフスイッチのルーティングテーブルは、到達可能なサブネットが次のことを示しています。

- **AWS** : 10.220.0.0/16
- **Azure** : 10.220.0.0/16

**ステップ 3** AWS に展開されたクラウドネットワークコントローラに接続し、**アプリケーション管理 > VRF** に移動して、Azure および NDFC VRF が表示されることを確認します。



ステップ 4 AWS に展開された Cloud Network Controller に残ったまま、ルート テーブル表示で検証を実行します。



ステップ5 AWS コンソールで、ルートテーブル表示で検証を実行します。

The screenshot shows the AWS Management Console interface for a Route Table. The breadcrumb navigation is VPC > Route tables > rtb-... / routetable-[aws10:egress]. A notification banner at the top says "You can now check network connectivity with Reachability Analyzer" with a "Run Reachability Analyzer" button. The "Details" section shows:

- Route table ID: rtb-...
- Main: No
- VPC: vpc-... | context-[aws10]-addr-[10.220.0.0/16]
- Owner ID: [redacted]
- Explicit subnet associations: 2 subnets (subnet-[redacted] / subnet-[10.220.1.0/24] and subnet-[redacted] / subnet-[10.220.2.0/24])

The "Routes" section shows a table with 3 routes:

| Destination    | Target  | Status | Propagated |
|----------------|---------|--------|------------|
| 10.220.0.0/16  | local   | Active | No         |
| 90.1.1.0/24    | tgw-... | Active | No         |
| 172.16.10.0/24 | tgw-... | Active | No         |

**ステップ 6** Azure に展開されたクラウド ネットワーク コントローラに接続し、**アプリケーション管理 > VRF**に移動して、AWS および NDFC VRF が表示されることを確認します。

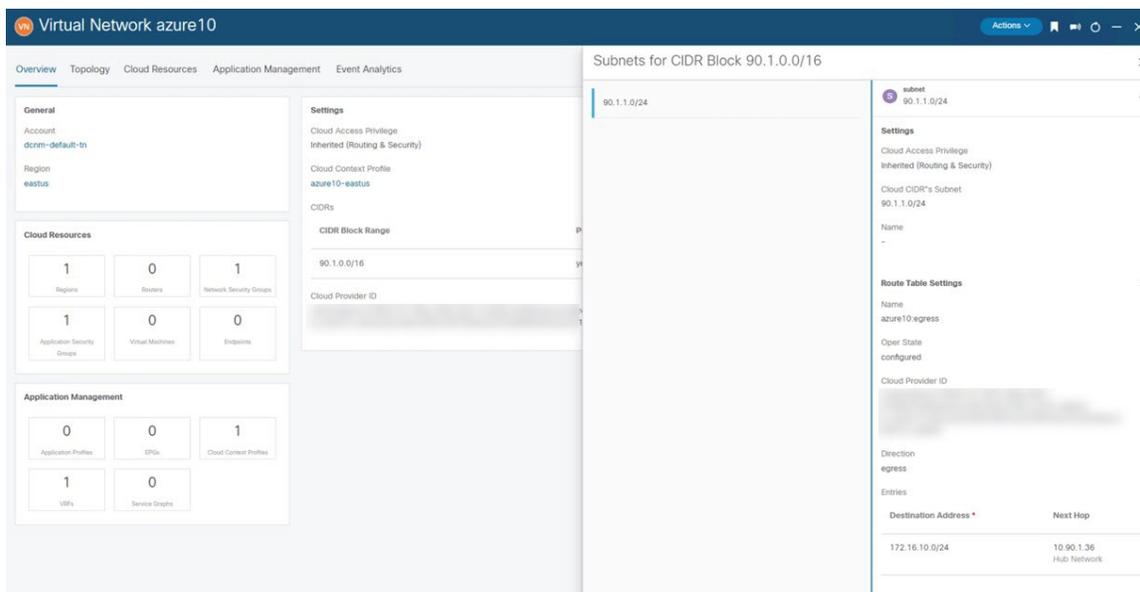
The image shows two screenshots of the Cisco Cloud Network Controller (Azure) interface. The top screenshot displays the 'VRFs' page with a table of VRF configurations. The bottom screenshot shows the 'Virtual Networks' page for 'azure10', displaying a detailed overview of the VNet's health and associated resources.

| Health  | Name  | EPGs | Cloud Context Profiles | Regions | Virtual Networks | Routers | Endpoints |
|---------|---|------|------------------------|---------|------------------|---------|-----------|
| Healthy | ave-clt infra   | 0    | 0                      | 0       | 0                | 0       | 0         |
| Healthy | aws10 Internal<br>msc-aws10 dcrn-default-tn           | 0    | 1                      | 1       | 1                | 0       | 0         |
| Healthy | azure10 Internal<br>msc-azure10 dcrn-default-tn       | 0    | 1                      | 1       | 1                | 0       | 0         |
| Healthy | copy common   | 0    | 0                      | 0       | 0                | 0       | 0         |
| Healthy | default common  | 0    | 0                      | 0       | 0                | 0       | 0         |
| Healthy | inf mgmt  | 0    | 0                      | 0       | 0                | 0       | 0         |
| Healthy | oob mgmt  | 0    | 0                      | 0       | 0                | 0       | 0         |
| Healthy | overlay-1 Internal<br>infra                           | 12   | 1                      | 1       | 1                | 2       | 10        |
| Healthy | stretched-vrf Internal<br>msc-azure10 dcrn-default-tn | 0    | 1                      | 1       | 1                | 0       | 0         |
| Healthy | v10 Internal<br>msc-aws10 dcrn-default-tn             | 0    | 1                      | 1       | 1                | 0       | 0         |

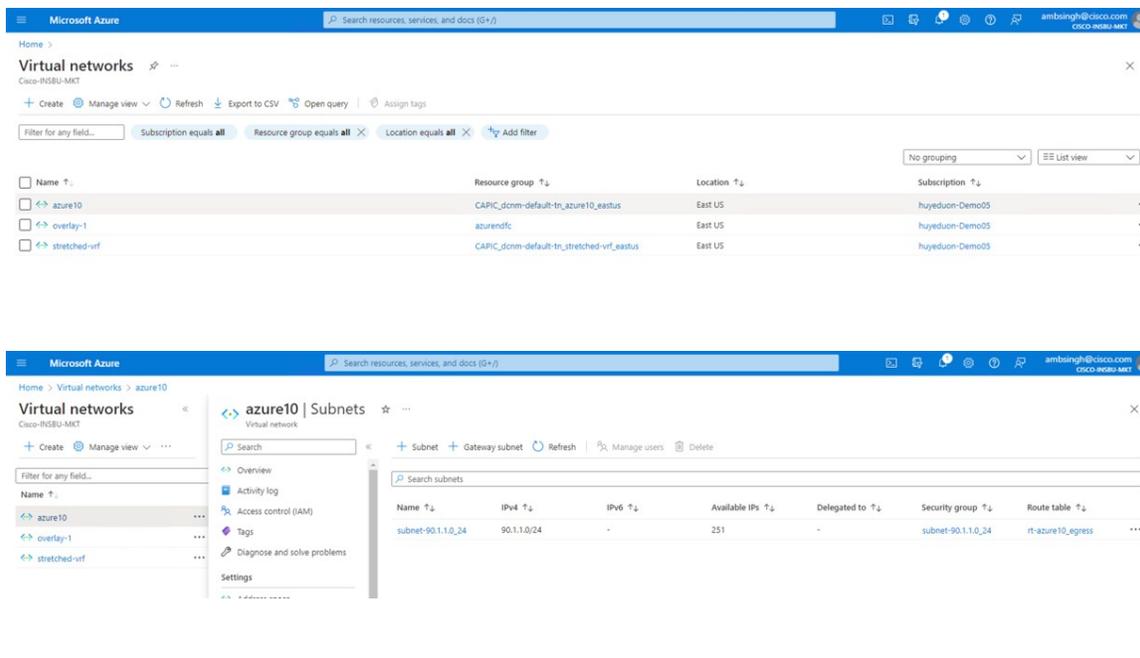
  

| Resource                    | Count |
|-----------------------------|-------|
| Regions                     | 1     |
| Routers                     | 0     |
| Network Security Groups     | 1     |
| Application Security Groups | 1     |
| Virtual Machines            | 0     |
| Endpoints                   | 0     |
| Application Profiles        | 0     |
| EPGs                        | 0     |
| Cloud Context Profiles      | 1     |
| VRFs                        | 1     |
| Service Graphs              | 0     |

ステップ7 Azureに展開されたクラウドネットワークコントローラーに残ったまま、[クラウド情報技術 (Cloud Resources)] > [仮想ネットワーク (Virtual Networks)]に移動し、azure10 VNetをクリックし、概要ページの情報を使用して追加の検証を行います。



ステップ 8 Azure コンソールで、追加の検証を実行します。



## 翻訳について

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