Cisco Nexus Dashboard Orchestrator Configuration Guide for NDFC Fabrics、リリース 4.0(x)

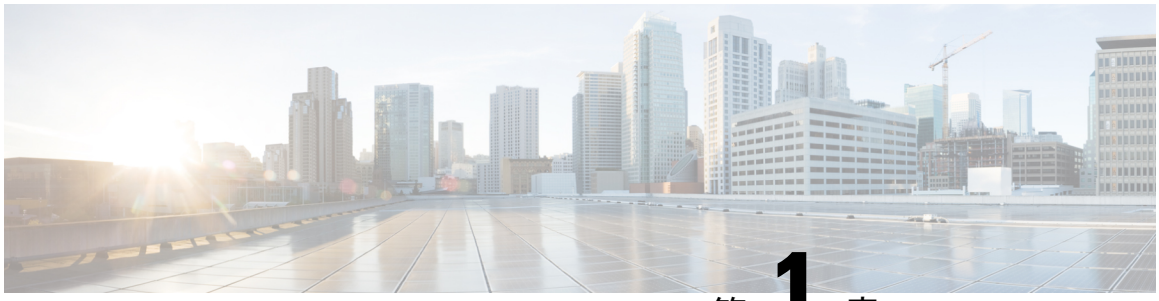
初版：2022 年 6 月 27 日

最終更新：2022 年 6 月 27 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/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次



第 1 章

新機能と変更情報

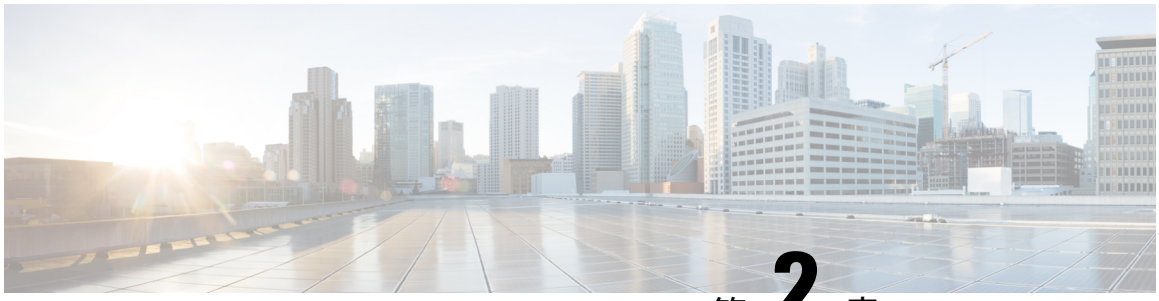
新機能と変更情報

次の表に、このガイドの最初に発行されたリリースから現在のリリースまでに、このガイドの編成と機能に加えられた大幅な変更の概要を示します。テーブルは、ガイドに加えられたすべての変更のすべてを網羅したリストを提供しているわけではありません。

表 *1*: 最新のアップデート

リリース	新機能またはアップデート	参照先
3.7(1)	このドキュメントの最初のリリース。	--

新機能と変更情報



第 2 章

サイトの追加と削除

Cisco NDFC サイトの追加

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

始める前に

- 追加するサイトが Cisco NDFC リリース 11.5(1) 以降を実行していることを確認する必要があります。

ステップ 1 Nexus Dashboard にログインして **[管理コンソール（Admin Console）]**を開きます。

ステップ 2 左のナビゲーションメニューから **[サイト（Sites）]** を選択し、**[サイトを追加（Add Site）]**をクリックします。

ステップ 3 サイト情報を入力します。

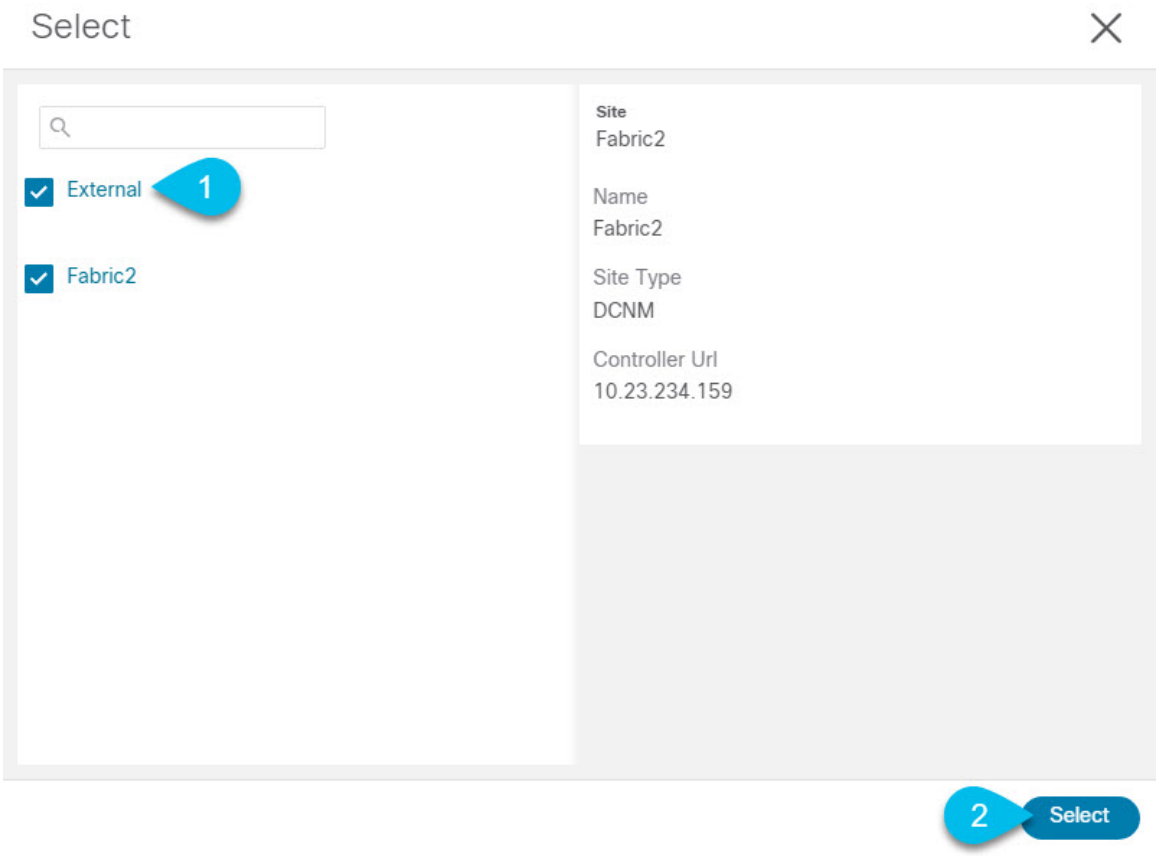
a) **[サイトのタイプ（Site Type）]** で、**NDFCまたは NDFC** を選択します。

b) NDFC コントローラの情報を入力します。

現在 NDFC ファブリックを管理している NDFC コントローラ用に、インバンド（`eth2`）インターフェイスの **[ホスト名/IP アドレス（Host Name/IP Address）]**、**[ユーザー名（User Name）]**、および **[パスワード（Password）]**を入力する必要があります。

c) **[サイトの選択 (Select Sites)]** をクリックして、コントローラによって管理される特定のファブリックを選択します。

開いたファブリック選択ウィンドウで、Nexus Dashboard に追加するファブリックを選択し、**[選択（Select）]** をクリックします。



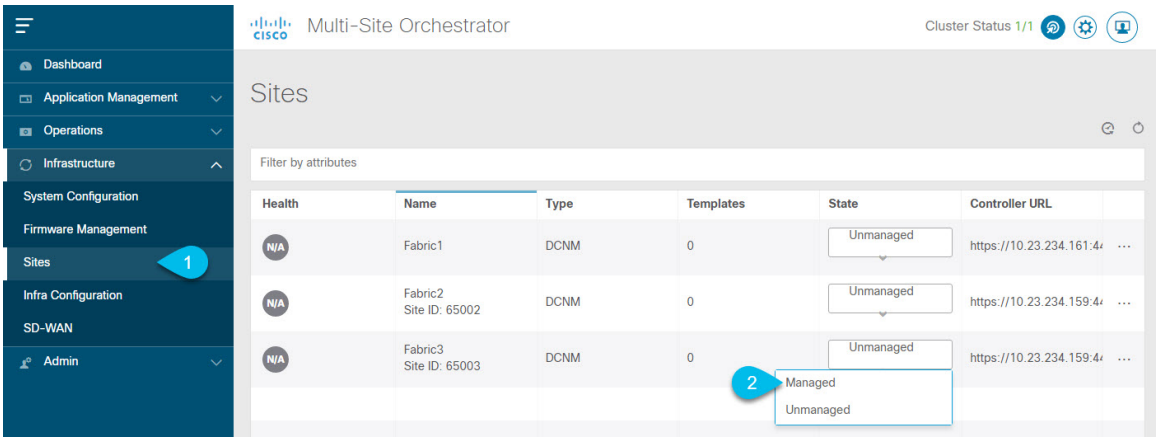
d) **[セキュリティ ドメインの追加（Add Security Domains）]**をクリックして、このサイトにアクセスできる 1 つ以上のセキュリティ ドメインを選択します。

ステップ 4 追加する任意の NDFC サイトに対して前の手順を繰り返します。

ステップ 5 Nexus Dashboard の**[サービスカタログ（Service Catalog）]**から、Nexus Dashboard Orchestrator サービスを開きます。

Nexus ダッシュボード ユーザーのクレデンシャルを使用して自動的にログインします。

ステップ 6 Nexus Dashboard Orchestrator GUIで、サイトを管理します。



a) 左のナビゲーションメニューから、**[インフラストラクチャ (Infrastructure)]** > **[サイト (Sites)]**を選択します。

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

管理しているファブリックがマルチサイトドメイン（MSD）の一部である場合、すでに関連付けられている **[サイト ID（Site ID）]** があります。この場合、**[状態 (State)]** を［管理対象 (Managed)］に変更するだけでファブリックが管理されます。

ただし、ファブリックが MSD の一部ではない場合、その状態を［管理対象（Managed）］に変更すると、サイトの **[ファブリック ID（Fabric ID）]** も指定するように求められます。

（注） 既存の MSD の一部であるファブリックとそうでないファブリックの両方を管理する場合は、最初に MSD ファブリックをオンボードし、次にスタンドアロン ファブリックをオンボードする必要があります。

サイトの削除

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

始める前に

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

ステップ 1 Nexus Dashboard Orchestrator GUI を開きます。

Nexus ダッシュボードの**サービス カタログ**から NDO サービスを開きます。Nexus ダッシュボードユーザーのクレデンシャルを使用して自動的にログインします。

ステップ 2 サイトのアンダーレイ設定を削除します。

a) 左側のナビゲーションメニューで、**[インフラストラクチャ（Infrastructure）]**>**[インフラの設定（Infra Configuration）]**を選択します。
b) メイン ペインにある **[インフラの設定（Configure Infra）]** をクリックします。
c) 左側のサイドバーで、管理対象から外すサイトを選択します。
d) 右側のバーの **[オーバレイの設定 (Overlay Configuration)]** タブで、**[Multi-Site]** ノブを無効にします。
e) 右側のサイドバーで、**[アンダーレイ設定 (Underlay Configuration)]** タブを選択します。
f) サイトからすべてのアンダーレイ設定を削除します。
g) **[展開 (Deploy)]** をクリックして、アンダーレイとオーバーレイの設定変更をサイトに展開します。

ステップ 3 Nexus Dashboard Orchestrator GUI で、サイトを無効にします。

a) 左のナビゲーションメニューから 、**[インフラストラクチャ (Infrastructure)]** > **[サイト (Sites)]**を選択します。
b) メインペインで、NDOで管理する各ファブリックの **[状態 (State)]** を `[管理対象 (Managed)]` から `[非管理対象 (Unmanaged)]` に変更します。

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

ステップ 4 Nexus ダッシュボードからサイトを削除します。

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

（注） この時点で、このサイトは、Nexus Dashboard クラスタにインストールされているどのアプリケーションでも使用されていてはならないことに注意してください。

a) Nexusダッシュボード GUIの左側のナビゲーションメニューから、**[サイト (Sites)]** を選択します。
b) 削除するサイトを1つ以上選択します。
c) メインペインの右上にある**[アクション (Actions)]** > **[サイトの削除 (Delete Site)]**をクリックします。
d) サイトのログイン情報を入力し、**[OK]** をクリックします。

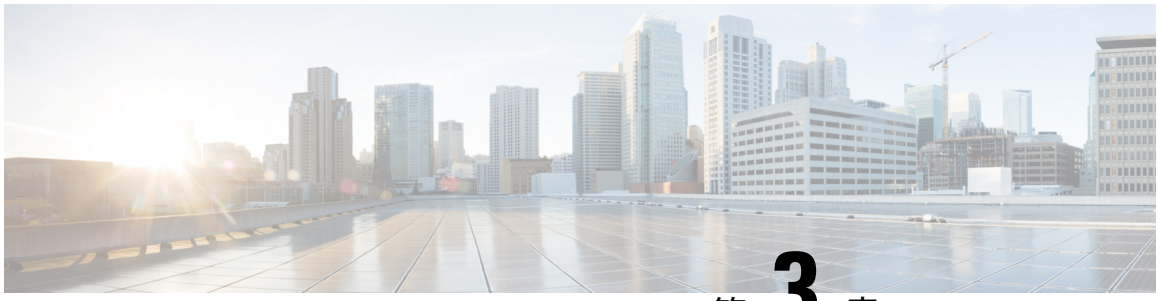
Nexus ダッシュボードからサイトが削除されます。

ファブリック コントローラへの相互起動

Nexus Dashboard Orchestrator は現在、ファブリックのタイプごとに多数の設定オプションをサポートしています。追加の多くの設定オプションでは、ファブリックのコントローラに直接ログインする必要があります。

NDO の**[インフラストラクチャ (Infrastucture)]** > **[サイト (Sites)]**画面から特定のサイト コントローラのGUIにクロス起動するには、サイトの横にあるアクション（...）メニューを選択し、ユーザー インターフェイスで **[開く (Open)]** をクリックします。クロス起動は、ファブリックのアウトオブバンド（OOB）管理IPで動作することに注意してください。

Nexus Dashboardとファブリックで同じユーザが設定されている場合、Nexus Dashboardユーザと同じログイン情報を使用して、ファブリックのコントローラに自動的にログインします。一貫性を保つために、Nexusダッシュボードとファブリック全体で共通のユーザによるリモート認証を設定することを推奨します。



第 3 章

Cisco NDFC サイトのインフラの構成

前提条件とガイドライン

次のセクションでは、全般とサイト固有のファブリック インフラ設定を行うために必要な手順について説明します。

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

さらに、次の点に注意してください。

- 境界ゲートウェイ スイッチの追加や削除には、一般的なインフラの設定手順の一部として、サイト接続性情報の更新 （13 ページ）に記載されている、Nexus Dashboard Orchestrator のファブリック接続情報の更新が必要です。

インフラの設定: 一般設定

このセクションでは、Nexus Dashboard Orchestrator によって搭載および管理される NDFC サイトの一般的なインフラ設定を構成する方法について説明します。

ステップ 1 Nexus Dashboard にログインし、Nexus Dashboard Orchestrator サービスを開きます。

ステップ 2 左のナビゲーションメニューから 、**[インフラストラクチャ（Infrastructure）] > [サイト接続（Site Connectivity）]**を選択します。

ステップ 3 メイン ペインにある **[構成（Configure）]** をクリックします。

ステップ 4 左側のサイドバーで、**[全般設定（General Settings）]**を選択します。

ステップ 5 **[コントロール プレーン設定（Control Plane Configuration）]** を指定します。

a) **[コントロール プレーン設定（Control Plane Configuration）]** タブを選択します。

b) **[BGP ピアリング タイプ（Bgp Peering Type）]** を選択します。

- `full-mesh`：各サイトのすべてのボーダー ゲートウェイ スイッチは、リモート サイトのボーダー ゲートウェイ スイッチとのピア接続を確立します。
- `route-server`：route-server オプションを使用すると、各サイトが MP-BGP EVPN セッションを確立する 1 つ以上のコントロールプレーン ノードを指定できます。ルートサーバー ノードは、従来の BGP ルート リフレクタと同様の機能を実行しますが、EBGP（iBGP）セッションでは使用しません。ルートサーバー ノードを使用すると、NDO によって管理されるすべての VXLAN EVPN サイト間で MP-BGP EVPN フルメッシュ隣接関係が作成されなくなります。

c) **[BGP ピアリングタイプ（BGP Peering Type）]** を `route-server` に設定する場合は、**[+ルート サーバーを追加（+ Add Route Server）]** をクリックして、1 台以上のルート サーバーを追加します。

[ルート サーバーの追加（Add Route Server）] ウィンドウが開きます。

- **[サイト（Site）]** ドロップダウンから、ルート サーバーに接続するサイトを選択します。
- **[ASN]** フィールドには、サイトのASNが自動的に入力されます。
- **[コア ルータ デバイス（Core Router Device）]** ドロップダウンから、接続するルート サーバーを選択します。
- **[インターフェイス（Interface）]** ドロップダウンから、コア ルータ デバイスのインターフェイスを選択します。

ルート サーバーは最大 4 台まで追加できます。複数のルート サーバーを追加すると、すべてのサイトがすべてのルート サーバーに対して MP-BGP EVPAN 隣接関係を確立します。

d) **[キープアライブ間隔（秒）（Keepalive Interval（Seconds））]**、**[ホールド間隔（秒）Hold Interval（Seconds）]**、**[ステール間隔（秒）（Stale Interval（Seconds））]**、**[グレースフル ヘルパー（Graceful Helper）]**、**[最大 AS 限界（Maximum AS Limit）]**、および **[ピア間の BGP TTL（BGP TTL Between Peers）]** フィールドは、Cisco ACI ファブリックにのみ関連するため、デフォルト値のままにします。

e) Cloud Network Controller ファブリックのみに関連するため、**[OSPF エリア ID（OSPF Area ID）]** および **[外部サブネット プール（External Subnet Pool）]** フィールドは、デフォルト値でスキップします。

ステップ 6 **[オンプレミス IPSec デバイス情報（On Premises IPSec Device）]** を提供します。

オンプレミスとクラウドサイト間接続でプライベート接続を使用し、IPSec をエネーブル化しない場合は、この手順をスキップできます。パブリック インターネット経由の接続では、IPSec が常に有効になっており、この手順で情報を提供する必要があります。

後のセクションで説明するように、オンプレミスとクラウドサイト間のサイトアンダーレイ接続を設定する場合は、クラウド CSR への接続を確立するオンプレミス IPN デバイスを選択する必要があります。これらの IPN デバイスは、オンプレミスのサイト設定画面で使用可能になる前に、ここで定義する必要があります。

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

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

c) デバイスが**[管理対象外（Unmanaged）]**か**[管理対象（Managed）]**かを選択し、デバイス情報を提供します。

これは、デバイスが NDFC によって直接管理されるかどうかを定義します。

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

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

- **[管理対象（Managed）]** IPN デバイスには、デバイスが入っているNDFC **[サイト（Site）]** を選択し、そのサイトの **[デバイス（Device）]** を選択します。

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

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

ステップ 7 **[IPSecトンネル サブネット プール（IPSec Tunnel Subnet Pools）]** 情報を入力します。

ここで指定できるサブネットプールには、次の 2 つのタイプがあります。

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

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

  1 つ以上のクラウド サイトから外部接続を有効にする場合は、少なくとも 1 つの外部サブネット プールを提供する必要があります。

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

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

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

（注） 両方のサブネット プールの最小マスク長は /24 です。

1 つ以上の**外部サブネット プール**を追加するには：

a) **[IPSec トンネル サブネット プール（IPSec Tunnel Subnet Pools）]** タブを選択します。
b) **[外部サブネット プール（External Subnet Pool）]** エリアで、**[+ IP アドレスの追加（+Add IP Address）]** をクリックして、1 つ以上の外部サブネット プールを追加します。

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

サブネットは、他のオンプレミス TEP プールと重複してはならず、`0.xxx` または `0.0.xx`で 始まってはならず、`/16` と `/24` の間のネットワーク マスク（`30.29.0.0/16` など）が必要です。

c) チェックマーク アイコンをクリックして、サブネット情報を保存します。
d) 追加するサブネット プールについて、これらのサブステップを繰り返します。

1 つ以上の **[サイト固有のサブネット プール（Site-Specific Subnet Pools）]** を追加するには：

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

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

c) サブネットの **[名前（Name）]** を入力します。

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

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

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

e) チェックマーク アイコンをクリックして、サブネット情報を保存します。

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

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

ステップ 8 **[NDFC 設定（NDFC Settings）]**を構成します。

a) **[NDFC 設定（NDFC Settings）]** タブを選択します。
b) **[L2 VXLAN VNI範囲（L2 VXLAN VNI Range）]** を指定します。
c) L3 VXLAN VNI範囲を指定します。
d) **[マルチサイト ルーティング ループバック IP 範囲（Multi-Site Routing Loopback IP Range）]**.を指定します。

このフィールドは、各ファブリックの **[マルチサイト TEP（Multi-Site TEP）]**フィールドに自動入力するために使用されます。インフラの構成: NDFC インフラ サイト固有の設定 （13 ページ）で説明します。

以前に NDFC のマルチサイト ドメイン（MSD）の一部であったサイトの場合、このフィールドには以前に定義された値が事前に入力されます。

e) **[エニーキャスト ゲートウェイ MAC（Anycast Gateway MAC）]** を入力します。

サイト接続性情報の更新

ボーダーゲートウェイスイッチの追加や削除などのインフラストラクチャの変更には、Nexus Dashboard Orchestrator ファブリックの接続の更新が必要です。このセクションでは、各サイトのコントローラから直接最新の接続性情報を取得する方法を説明します。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左のナビゲーションメニューから 、**[インフラストラクチャ（Infrastructure）]** > **[サイト接続（Site Connectivity）]**を選択します。

ステップ 3 メイン ペインの右上にある **[構成（Configure）]** をクリックします。

ステップ 4 左側のペインの **[サイト (Sites)]** の下で、特定のサイトを選択します。

ステップ 5 メイン ウィンドウで、APIC からファブリック情報を取得するために **[更新 (Refresh)]** ボタンをクリックします。

ステップ 6 （任意）使用停止されたボーダーゲートウェイスイッチの設定を削除する場合は、**[確認（Confirmation）]** ダイアログでチェックボックスをオンにします。

このチェックボックスを有効にすると、現在使用されていないボーダーゲートウェイスイッチのすべての設定情報がデータベースから削除されます。

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

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

インフラの構成: NDFC インフラ サイト固有の設定

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

ステップ 1 Nexus Dashboard にログインし、Nexus Dashboard Orchestrator サービスを開きます。

ステップ 2 左のナビゲーションメニューから 、**[インフラストラクチャ（Infrastructure）]** > **[サイト接続（Site Connectivity）]**を選択します。

ステップ 3 メイン ペインにある **[構成（Configure）]** をクリックします。

ステップ 4 左側のペインの **[サイト (Sites)]** の下で、特定のNDFCを選択します。

ステップ 5 右側の ***<Site>*[設定 (Settings)]**サイドバーで、**[オーバレイ マルチキャスト TEP (Overlay Multicast TEP)]** を指定します。

このアドレスは、サイト間の L2 BUM および L3 マルチキャスト トラフィックのために使用されます。この IP アドレスは、同じファブリックの一部であるすべてのボーダーゲートウェイスイッチに導入されます。

（注） 設定するサイトが NDFC マルチサイトドメイン（MDS）の一部である場合、このフィールドには NDFC からインポートされた情報が事前に入力されます。この場合、値を変更してインフラ設定を再展開すると、MDS の一部であるサイト間のトラフィックに影響します。

[自動割り当て (Auto Allocate)] フィールドを選択すると、前のセクションで定義した**マルチサイト ルーティング ループバック IP 範囲**から次に使用可能なアドレスが割り当てられます。

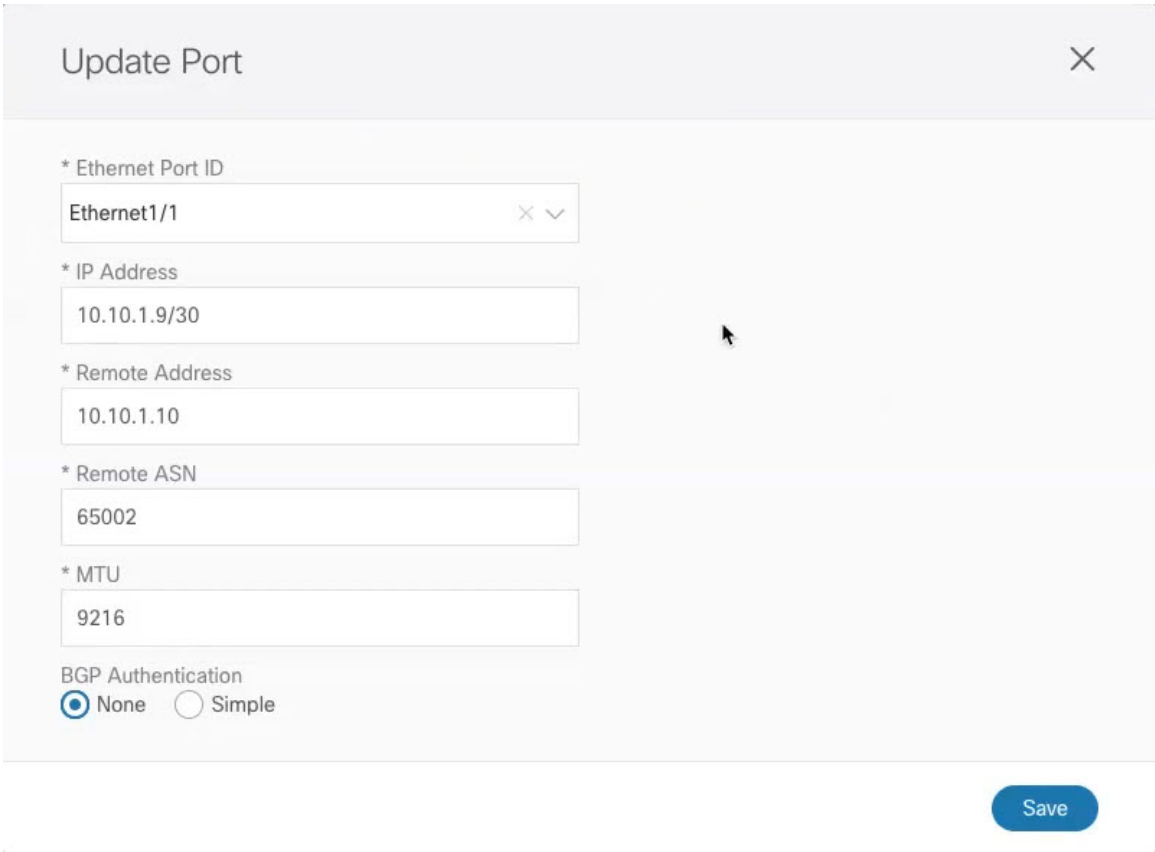
ステップ 6 **<fabric-name>** タイル内で、ボーダーゲートウェイを選択します。

ステップ 7 右側**<*border-gateway*>**サイドバーを設定し、**BGP-EVPN ROUTER-ID** と **BGW PIP** を指定します。

vPC ドメインの一部であるボーダーゲートウェイの場合は、**VPC VIP** も指定する必要があります。

ステップ 8 **[ポートの追加 (Add Port)]** をクリックして、IPN に接続するポートを設定します。

（注） このリリースでは、NDFC からのポート設定のインポートはサポートされていません。設定するサイトがすでに NDFC マルチサイトドメイン（MDS）の一部である場合は、NDFC ですでに設定されている値と同じ値を使用する必要があります。



このボーダーゲートウェイをコアスイッチまたは別のボーダーゲートウェイに接続するポートの展開に固有の次の情報を入力します。

- **[イーサネット ポート ID (Ethernet Port ID)]** ドロップダウンから、IPNに接続するポートを選択します。
- [**IP アドレス (IP Address)**] フィールドに、IP アドレスとネットマスクを入力します。
- **[リモート アドレス (Remote Address)]** フィールドに、ポートが接続されているリモート デバイスの IP アドレスを入力します。
- **[リモート ASN (Remote ASN)]** フィールドに、リモート サイトのIDを入力します。
- **[MTU]** フィールドに、サーバーの MTU を入力します。

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

  [継承 (inherit)] を指定することも、576 ～ 9000 の値を指定することもできます。
- **BGP認証**の場合は、[なし (None)] または [シンプル (Simple (MD5))] を選択できます。

  [シンプル (Simple)]を選択した場合は、**認証キー**も指定する必要があります。

インフラ設定の展開

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

始める前に

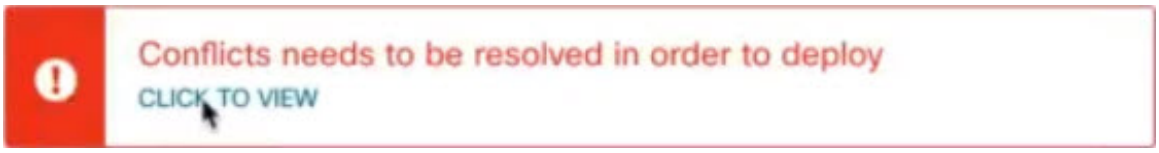
この章の前のセクションで説明したように、全般的な、およびサイト固有のインフラ設定を完了している必要があります。

ステップ 1 設定の競合がないことを確認するか、必要に応じて解決します。

各サイトですでに設定されている設定との設定の競合がある場合、**[展開 (Deploy)]** ボタンが無効になり、警告が表示されます。たとえば、同じ名前のVRFまたはネットワークが複数のサイトに存在し、各サイトで異なる VNI を使用している場合です。

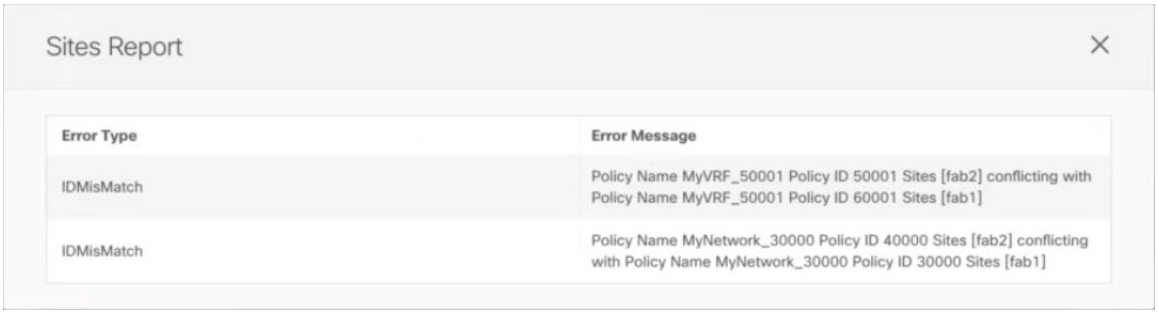
設定が競合する場合：

a) 競合通知ポップアップの **[クリックして表示 (Click to View)]** リンクをクリックします。



b) 競合の原因となっている特定の設定を書き留めます。

たとえば、次のレポートでは、fab1 サイトと fab2 サイトの VRF とネットワーク間に ID の不一致があります。



c) [X] ボタンをクリックしてレポートを閉じ、インフラ設定画面を終了します。

d) サイトの削除 （5 ページ）の説明に従って、NDO でサイトの管理を解除します。

Nexus ダッシュボードからサイトを削除する必要はありません。NDO GUI でサイトの管理を解除するだけです。

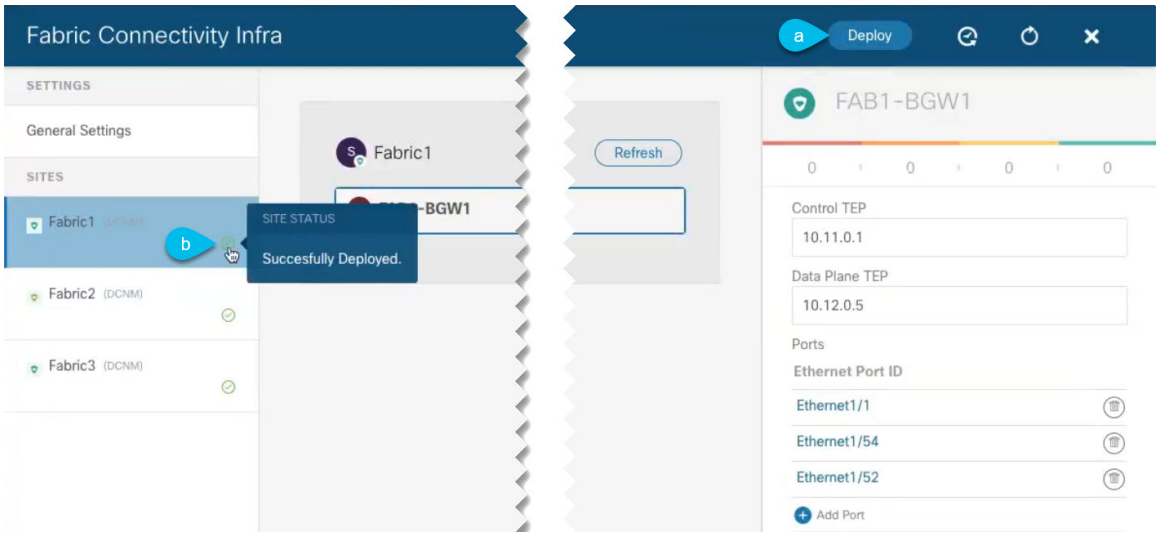
e) 既存の設定の競合を解決します。

f) Cisco NDFC サイトの追加 （3 ページ）の説明に従って、サイトを再度管理状態にします。

サイトはすでに Nexus ダッシュボードに追加されているため、NDO で管理できるようにします。

g) すべての競合が解決され、**[展開 (Deploy)]** ボタンが使用可能であることを確認します。

ステップ 2 設定を展開します。



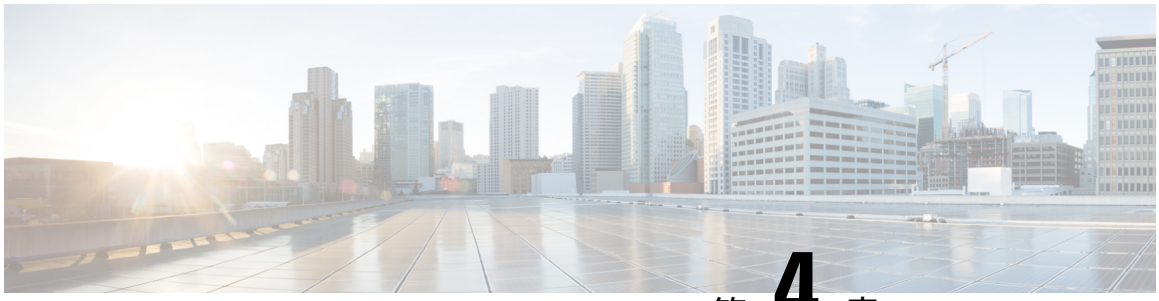
a) **[ファブリック接続インフラ (Fabric Connectivity Infra)]** 画面の右上で、適切な **[展開 (Deploy)]** オプションを選択して設定を展開します。

NDFC サイトのみを設定する場合は、**[展開 (Deploy)]** をクリックしてインフラ設定を展開します。

b) 設定が展開されるのを待ちます。

インフラ設定を展開すると、NDOはNDFCに信号を送り、ボーダーゲートウェイ間のアンダーレイとEVPN オーバーレイを設定します。

設定が正常に展開されると、**[ファブリック接続インフラ (Fabric Connectivity Infra)]** 画面のサイトの横に緑色のチェックマークが表示されます。



第 4 章

ファブリック管理

テナントの概要

テナントは、アプリケーションポリシーの論理コンテナで、管理者はドメインベースのアクセスコントロールを実行できます。テナントはポリシーの観点から分離の単位を表しますが、プライベート ネットワークは表しません。テナントは、サービス プロバイダーの環境ではお客様を、企業の環境では組織またはドメインを、または単にポリシーの便利なグループ化を表すことができます。

（注） テナントを管理するには、パワー ユーザまたはサイトとテナント マネージャの読み取り/書き込みロールのいずれかが必要です。

3 つのデフォルト テナントが事前に設定されています。

- common：ACI ファブリックの他のテナントに「共通」のサービスを提供するための特別なテナント。共通テナントの基本原則はグローバルな再利用です。一般的なサービスには、共有 L3Out、DNS、DHCP、Active Directory、共有プライベート ネットワークまたはブリッジドメインなどがあります。

- `dcnm-default-tn`：Cisco NDFC ファブリックの設定を提供する特別なテナント。

  Nexus Dashboard Orchestrator を使用して Cisco DCNM ファブリックを管理する場合は、事前に設定されているデフォルトの `dcnm-default-tn` を使用し、次のオブジェクトを作成および管理できます。

  - VRF
  - ネットワーク

- `infra`：トンネルやポリシー展開など、ファブリック内部の通信に使用されるインフラストラクチャ テナント。これには、スイッチ間の切り替えと APIC 通信への切り替えが含まれます。`infra`テナントは、ユーザー空間（テナント）には公開されず、独自のプライベート ネットワーク空間とブリッジ ドメインを備えています。ファブリックの検出、イメージ管理、ファブリック機能用の DHCP は、すべてこのテナント内で処理されます。

  Nexus Dashboard Orchestrator を使用して Cisco NDFC ファブリックを管理する場合は、常にデフォルトの `dcnm-default-tn` テナントを使用します。

テナント ポリシー テンプレート

このセクションでは、Cisco APIC によって管理されるオンプレミスの ACI ファブリックでサポートされる多数のテナント テンプレートを提供します。詳細については、*Cisco Nexus Dashboard Orchestrator Configuration Guide for ACI Fabrics* を参照してください。

スキーマとテンプレート

スキーマは、ネットワーク設定の定義に使用されるテンプレートの集合であり、各テンプレートは特定のテナントに割り当てられます。テンプレートは、1 つ以上のサイトに一度に展開する設定オブジェクトとそのプロパティのセットです。展開の使用例に固有のスキーマとテンプレートの設定を作成する際に、複数のアプローチを実行できます。ここでは、マルチサイト環境でスキーマ、テンプレート、およびポリシーを定義する方法を決定する際に実行できる、いくつかの簡単な設計方針について説明します。

スキーマを設計する際には、スキーマ、テンプレート、およびスキーマあたりのオブジェクトの数に対してサポートされているスケーラビリティ制限を考慮する必要があることに注意してください。検証済みスケーラビリティ制限の詳細については、お使いのリリースの『*Cisco Multi-Site Verified Scalability Guides*』を参照してください。

単一スキーマの展開

最も簡単なスキーマ設計アプローチは、単一のスキーマ展開です。そのスキーマのすべての VRF およびネットワークで単一のスキーマを作成できます。その後、1 つのアプリケーション プロファイルまたは複数のアプリケーション プロファイルをテンプレート内に作成し、それを 1 つ以上のサイトに展開することができます。

Multi-Site スキーマを作成する最も簡単な方法は、同じスキーマとテンプレート内にすべてのオブジェクトを作成することです。ただし、スキーマごとにサポートされているスキーマまた

はテンプレートの数に制限があるため、このアプローチは大規模な展開に適していない場合があります。これは、これらの制限を超える可能性があります。

オブジェクトの関係性に基づく複数スキーマ

共有オブジェクト参照を使用して複数のスキーマを設定する場合、それらのオブジェクトを変更する際に注意を払うことが大切です。たとえば、共有ネットワークオブジェクトを変更または削除すると、1 つ以上のサイトのアプリケーションに影響を与える可能性があります。そのため、サイトとそのアプリケーションで使用されているオブジェクトのみを含む、個々のサイトのためのテンプレートを作成するのがよいでしょう。それから、共有オブジェクトを含む別のテンプレートを作成します。

たとえば、3つの異なるサイトに展開する予定の設定には、次のテンプレートを使用できます。

- サイト 1 テンプレート
- サイト 2 テンプレート
- サイト 3 テンプレート
- サイト 1 と 2 の共有テンプレート
- サイト 1 と 3 の共有テンプレート
- サイト 2 と 3 の共有テンプレート
- すべての共有テンプレート

同様に、展開されているサイトに基づいてオブジェクトを分離するのではなく、個々のアプリケーションに基づいてスキーマとテンプレートを作成することもできます。これにより、各アプリケーションプロファイルを簡単に特定し、それらをスキーマとサイトにマッピングし、さらには各アプリケーションをローカルまたは拡張されたサイト全体のものとして設定することができます。

ただし、これはスキーマごとのテンプレート数の制限（使用しているリリースの Verified Scalability Guide に記載）をすぐに越えてしまう可能性があるため、複数の組み合わせに対応するために追加のスキーマを作成することが必要になります。これにより、複数のスキーマとテンプレートが追加され、さらに複雑になりますが、サイトまたはアプリケーションに基づいてオブジェクトを正確に分離できます。

テンプレート設計

このリリースでは、各スキーマ内で VRF とネットワーク用に個別のテンプレートを作成してから、最初に VRF テンプレートを展開し、次にネットワークを含むテンプレートを展開することをお勧めします。このようにして、ネットワーク構成をサイトにプッシュするときに、ネットワークに必要な VRF がすでに作成されています。

同様に、複数のネットワークと VRF を展開解除する場合は、最初にネットワーク テンプレートを展開解除してから、VRF テンプレートを展開解除することをお勧めします。これにより、VRF が展開解除されたときに、VRF をまだ使用している既存のネットワークとの競合が発生しなくなります。

テンプレート タイプ

Nexus Dashboard Orchestrator では、それぞれ特定の目的のために設計された 3 種類のテンプレートを使用できます。

- [ACI マルチクラウド（ACI Multi-Cloud）]：Cisco ACI オンプレミスおよびクラウド サイトに使用されるテンプレート。これにより、複数のサイト間でテンプレートとオブジェクトを拡張できます。このテンプレートは、次の 2 つの展開タイプをサポートしています。
  - [マルチサイト（Multi-Site）]：テンプレートは、単一のサイト（サイトローカル ポリシー）または複数のサイト（拡張ポリシー）に関連付けることができます。マルチサイト ネットワーク（ISN）または VXLAN サイト間通信用にオプションを選択する必要があります。
  - [自律（Autonomous）]：テンプレートは、独立して運用され、サイト間ネットワークを介して接続されていない（サイト間 VXLAN 通信なしの）1 つ以上のサイトに関連付けることができます。

  このガイドでは、オンプレミスの Cisco NDFC ファブリック向けの Nexus Dashboard Orchestrator 構成について説明しています。Cisco ACI サイトの操作については、代わりに *Cisco Nexus Dashboard Orchestrator Configuration Guide for ACI Fabrics* を参照してください。
- **[NDFC]**：Cisco Nexus Dashboard ファブリック コントローラ（以前のデータセンター ネットワーク マネージャ）サイト用に設計されたテンプレート。

  次のセクションでは、主にこのタイプのテンプレートに焦点を当てます。
- **[クラウド ローカル（Cloud Local）]**：Google Cloud サイト接続など、特定のクラウド ネットワーク コントローラのユース ケース向けに設計されたテンプレートであり、複数のサイト間で拡張することはできません。

  このガイドでは、オンプレミスの Cisco NDFC ファブリック向けの Nexus Dashboard Orchestrator 構成について説明しています。クラウド ネットワーク コントローラ ファブリックの操作については、代わりに Nexus Dashboard Orchestrator のユース ケース ライブラリを参照してください。

設定の同時更新

Nexus ダッシュボード オーケストレータ GUI は、同じサイトまたはスキーマオブジェクトでの同時更新が意図せずに相互に上書きされることがないようにします。自分が開いた後に別のユーザによって更新されたサイトまたはテンプレートに変更を加えようと、GUI はそれ以降の変更を拒否し、追加の変更を行う前にオブジェクトを更新するように求める警告を表示します。テンプレートを更新すると、その時点までに行った編集内容は失われるため、再度変更する必要があります。

ただし、既存のアプリケーションとの下位互換性を維持するために、デフォルトの REST API 機能は変更されていません。つまり、UI はこの保護を常に有効にしていますが、設定変更を追跡するためには、NDO の API コールに対しても明示的に有効にする必要があります。

（注） この機能を有効にする場合は、次の点に注意してください。

- このリリースでは、サイト オブジェクトとスキーマ オブジェクトの競合する設定変更の検出のみがサポートされています。
- PUT および PATCH API コールのみがバージョンチェック機能をサポートします。
- API コールでバージョン チェック パラメータを明示的に有効にしていない場合、NDO は内部的に更新を追跡しません。その結果、設定の更新は、後続の API コールまたは GUI ユーザの両方によって上書きされる可能性があります。

設定のバージョン チェックを有効にするには、使用している API エンドポイントの末尾に enableVersionCheck = true パラメータを追加して、API コールにこのパラメータを渡します。次の例をご覧ください。

https://*<mso-ip-address>*/mso/api/v1/schemas/*<schema-id>*?**enableVersionCheck=true**

例

スキーマ内のテンプレートの表示名を更新する簡単な例を使用して、 PUT または PATCH コールでバージョンチェック属性を使用する方法を示します。

最初に、変更するスキーマを GET します。これにより、コールの応答で現在の最新バージョンのスキーマが返されます。

```
{
    "id": "601acfed38000070a4ee9ec0",
    "displayName": "Schema1",
    "description": "",
    "templates": [
        {
            "name": "Template1",
            "displayName": "current name",
            [...]
        }
    ],
    "_updateVersion": 12,
    "sites": [...]
}
```

次に、リクエスト URL に、2 つの方法のいずれかで、enableVersionCheck = true を追加して、スキーマを変更します。

（注） ペイロードの _updateVersion フィールドの値が、元のスキーマで取得した値と同じであることを確認する必要があります。

- PUT API を使用して、更新されるスキーマ全体ペイロードとします。

```
PUT /v1/schemas/601acfed38000070a4ee9ec0?enableVersionCheck=true
```

```
{
    "id": "601acfed38000070a4ee9ec0",
    "displayName": "Schema1",
    "description": "",
    "templates": [
        {
            "name": "Template1",
            "displayName": "new name",
            [...]
        }
    ],
    "_updateVersion": 12,
    "sites": [...]
}
```

- PATCH API 操作のいずれかを使用して、スキーマ内のオブジェクトの 1 つに特定の変更を加えます。

```
PATCH /v1/schemas/601acfed38000070a4ee9ec0?enableVersionCheck=true
```

```
[
    {
        "op": "replace",
        "path": "/templates/Template1/displayName",
        "value": "new name",
        "_updateVersion": 12
    }
]
```

リクエストが行われると、APIは現在のスキーマバージョンを 1 ずつ増やし（12 から 13 など）、新しいバージョンのスキーマの作成を試みます。（enableVersionCheck が有効で）新しいバージョンがまだ存在しない場合、操作は成功し、スキーマは更新されます。別の API コールまたは UI がその間にスキーマを変更していた場合、操作は失敗し、API コールは次の応答を返します。

```
{
    "code": 400,
    "message": "Update failed, object version in the DB has changed, refresh your client
 and retry"
}
```

スキーマとテンプレートの作成

始める前に

- NDFCテナントへのユーザーの追加で説明されているように、スキーマを作成するため、およびスキーマが使用するテナントにすでに関連付けられているスキーマを変更するために使用する、ユーザー アカウントが必要です。

ステップ 1 Nexus Dashboard にログインし、Nexus Dashboard Orchestrator サービスを開きます。

ステップ 2 スキーマを新規作成します。

a) 左側のナビゲーション メニューで、**[アプリケーション管理 (Application Management)]** > **[スキーマ (Schemas)]** を選択します。

b) [スキーマ (Schema)] ページで、**[スキーマの追加 (Add Schema)]** をクリックします。

c) スキーマ作成ダイアログで、スキーマの **[名前 (Name)]** と説明（オプション）を入力し、**[追加（Add）]** をクリックします。

デフォルトでは、新しいスキーマは空であるため、1 つ以上のテンプレートを追加する必要があります。

ステップ 3 テンプレートを作成します。

a) スキーマ ページで、**[表示（View）]** > **[概要（Overview）]** をクリックし、**[新しいテンプレートの追加（Add New Template）]** をクリックします。

b) **[テンプレート タイプの選択（Select a Template type）]** ウィンドウで、`[NDFC]` を選択し、**[追加（Add）]** をクリックします。

- [ACI マルチクラウド（ACI Multi-Cloud）]：Cisco ACI オンプレミスおよびクラウド サイトに使用されるテンプレート。これにより、複数のサイト間でテンプレートとオブジェクトを拡張できます。このテンプレートは、次の 2 つの展開タイプをサポートしています。
  - `[マルチサイト（Multi-Site）]`：テンプレートは、単一のサイト（サイトローカル ポリシー）または複数のサイト（拡張ポリシー）に関連付けることができます。マルチサイト ネットワーク（ISN）または VXLAN サイト間通信用にオプションを選択する必要があります。
  - `[自律（Autonomous）]`：テンプレートは、独立して運用され、サイト間ネットワークを介して接続されていない（サイト間 VXLAN 通信なしの）1 つ以上のサイトに関連付けることができます。

このガイドでは、オンプレミスの Cisco NDFC ファブリック向けの Nexus Dashboard Orchestrator 構成について説明しています。Cisco ACI サイトの操作については、代わりに *Cisco Nexus Dashboard Orchestrator Configuration Guide for ACI Fabrics* を参照してください。

- **[NDFC]**：Cisco Nexus Dashboard ファブリック コントローラ（以前のデータセンター ネットワーク マネージャ）サイト用に設計されたテンプレート。

次のセクションでは、主にこのタイプのテンプレートに焦点を当てます。

- **[クラウド ローカル（Cloud Local）]**：Google Cloud サイト接続など、特定のクラウド ネットワーク コントローラのユース ケース向けに設計されたテンプレートであり、複数のサイト間で拡張することはできません。

  このガイドでは、オンプレミスの Cisco NDFC ファブリック向けの Nexus Dashboard Orchestrator 構成について説明しています。クラウド ネットワーク コントローラ ファブリックの操作については、代わりに Nexus Dashboard Orchestrator のユース ケース ライブラリを参照してください。

c) 右側のサイドバーで、テンプレートの **[表示名（Display Name）]** を入力します。
d) （任意）**[説明 (Description)]** を入力します。
e) **[テナントの選択 (Select a Tenant)]** ドロップダウンから、`dcnm-default-tn` テナントを選択します。
f) テンプレート ビュー ページで、**[保存（Save）]** をクリックします。

   追加のオプション（サイトの関連付けなど）を使用できるようにするには、この初期構成の後にテンプレートを保存する必要があります。

g) この手順を繰り返して、追加のテンプレートを作成します。

   スキーマとテンプレートの設計の詳細については、スキーマとテンプレート （20 ページ） を参照してください。

ステップ 4 テンプレートをサイトに割り当てます。

ファブリック構成を展開するには、一度に 1 つのテンプレートを 1 つ以上のサイトに展開します。それで、設定を展開する少なくとも 1 つのサイトにテンプレートを関連付ける必要があります。

a) テンプレート ビュー ページで、**[アクション（Actions）]** をクリックし、**[サイトの関連付け（Site Association）]** を選択します。
b) **[サイトを <テンプレート> に追加（Add Sites to <template>）]** ダイアログで、テンプレートを展開する 1 つ以上のサイトを選択し、**[OK]** をクリックします。

次のタスク

スキーマと 1 つ以上のテンプレートを作成したら、特定のユース ケースに基づいて、このドキュメントの次のセクションで説明するように、テンプレートの編集に進むことができます。構成の定義が完了したら、テンプレートの展開 （41 ページ） で説明されているようにテンプレートを展開できます。

NDFC サイトからのスキーマ要素のインポート

新しいオブジェクトを作成し、1 つまたは複数のサイトに公開できます。または、サイトローカルの既存のオブジェクトをインポートし、Nexus Dashboard Orchestrator を使用して管理できます。ここでは、1 つ以上の既存のオブジェクトをインポートする方法について説明します。このドキュメントでは、新しいオブジェクトを作成する方法について説明します。

ステップ 1 [スキーマ (Schema)] ページで、オブジェクトをインポートするスキーマを選択します。

ステップ 2 左側のサイドバーで、オブジェクトをインポートする**テンプレート**を選択します。

ステップ 3 メインペインで**[インポート (Import)]**ボタンをクリックし、インポート元の**[サイト (Site)]**を選択します。

ステップ 4 **[インポート元 (Import from)] <*site-name*>** ウィンドウが開いたら、インポートするオブジェクトを 1 つまたは複数選択します。

（注） Nexus Dashboard Orchestrator にインポートするオブジェクトの名前は、すべてのサイトにわたって一意にする必要があります。重複する名前を持つ別のオブジェクトをインポートすると、スキーマ検証エラーとなり、インポートに失敗します。同じ名前のオブジェクトをインポートする必要がある場合は、先に名前を変更してください。

VRF の作成

このセクションでは、VRF の作成方法を説明します。

始める前に

スキーマとテンプレートの作成 （25 ページ）の説明に従って、スキーマとテンプレートを作成し、テンプレートにテナントを割り当てる必要があります。

ステップ 1 VRF を作成するためのスキーマとコントラクトを選択します。

ステップ 2 VRF を作成します。

a) スキーマ編集ビューで、**[オブジェクトの作成 (Create Object)]** > **[VRF]**を選択します。

b) 右側ペインで、VRF の **[表示名 (Display Name)]** を入力します。

c) （任意）**[VRF ID]** を指定します。

VRF の VNI を指定することも、フィールドを空のままにしておくこともできます。VNI は、インフラの設定: 一般設定 （9 ページ）で指定した範囲から NDO によって自動的に割り当てられます。

d) **[VRF プロファイル (VRF Profile)]** ドロップダウンから、VRF プロファイルを選択します。

`Default_VRF_Universal` プロファイルを割り当てるか、NDFC で以前に作成した使用可能な VRF プロファイルを選択できます。NDFC で作成されたプロファイルは自動的に NDO にインポートされ、ここで選択できます。

e) **[VRF 拡張プロファイル (VRF Extension Profile)]**ドロップダウンから、拡張プロファイルを選択します。

`Default_VRF_Extension_Universal` プロファイルを割り当てるか、NDFC で以前に作成した使用可能な VRF 拡張プロファイルを選択できます。NDFC で作成されたプロファイルは自動的に NDO にインポートされ、ここで選択できます。

f) **[ループバックルーティングタグ (Loopback Routing Tag)]** を指定します。

VLAN が複数のサブネットに関連付けられている場合、このタグは各サブネットの IP プレフィックスに関連付けられます。このルーティング タグは、オーバーレイ ネットワークの作成にも関連付けられています。

g) **[直接ルート マップの再配布 (Redistribute Direct Route Map)]** を指定します。

VRF でルートを再配布するためのルート マップ名を指定します。

h) (オプション) **[RT 自動生成の無効化（Disable RT Auto-Generate）]** をオンにして、ルート ターゲットの自動生成を無効にします。

（注） この機能は、Nexus Dashboard Orchestrator リリース 3.5(2) 以降でサポートされています。

デフォルトで、このオプションがオフになっているときは、ルート ターゲット（RT）がスイッチにより生成され、既存の自動生成されたものに加えて、カスタム RT を生成するように選択できます。このオプションを有効にすると、RT の自動生成が無効になり、カスタム RT のみを使用できます。

i) （オプション）カスタム ルート ターゲットを指定します。

（注） この機能は、Nexus Dashboard、リリース 3.5(2) 以降でサポートされます。

カスタム RT を指定するために、次のフィールドに 1 つ以上の値を入力します。

- **インポート（Import）**：VPN ルート インポート
- **エクスポート（Export）**：VPN ルートのエクスポート用
- **EVPN のインポート（Import EVPN）**：EVPN ルートのインポート用
- **EVPN のエクスポート（Export EVPN）**：EVPN ルートのエクスポート用

有効な値を入力する必要があります（例: `12.2.3.4:2200`）。値を入力すると、UI がその値を検証し、フォーマットが正しくなると、`Create "<value>"` ドロップダウンのオプションが表示されます。

合計で最大 10 個のカスタム ルート ターゲット値を指定できます。

ステップ 3 VRF のサイトローカル プロパティを設定します。

VRF が展開されているすべてのサイトに適用されるネットワークの一般プロパティに加えて、この VRF のサイト固有のプロパティをサイトごとに個別に設定できます。

a) **[テンプレート プロパティ（Template Properties）]** ドロップダウンから、このテンプレートが関連付けられているサイトを選択します。
b) メイン ペインで、ネットワークを選択します。
c) 右側の **[プロパティ (Properties)]** サイドバーで、サイト固有の設定を指定します。

次のサイトローカル プロパティを設定できます。

- **[テナント ルーテッド マルチキャスト (Tenant Routed Multicast)]** をオンにする： テナント ルーテッドマルチキャスト（TRM）は、BGP ベースの EVPN コントロールプレーンを使用する VXLAN ファブリック内でのマルチキャスト転送を有効にします。TRM は、ローカルまたは VTEP 間で同じサブネット内または異なるサブネット内の送信元と受信側の間にマルチテナント対応のマルチキャスト転送を実装します。

  TRMを有効にする場合は、**[RPアドレス (RP Address)]** と **[オーバーレイ マルチキャスト グループ (Overlay Multicast Group)]** も指定する必要があります。

- ランデブーポイント（RP）がファブリックの外部にある場合は、**[RP 外部 (RP External)]** を有効にします。
- **[スタティック リーフの追加 (Add Static Leaf)]** をクリックして、VRF を設定する 1 つ以上のリーフ スイッチを選択します。

  開いた **[スタティック リーフの追加 (Add Static Leaf)]** ウィンドウで、リーフノードを選択し、VRF の VLAN ID を入力します。

ネットワークの作成

ここでは、Nexus Dashboard Orchestrator から NDFC ネットワークを設定する方法について説明します。

始める前に

- スキーマとテンプレートの作成 （25 ページ）の説明に従って、スキーマとテンプレートを作成し、テンプレートにテナントを割り当てる必要があります。
- VRF の作成 （27 ページ）の説明に従って VRF を作成する必要があります。

ステップ 1 スキーマを選択し、アプリケーション プロファイルを作成するテンプレートを選択します。

ステップ 2 ネットワークを作成します。

a) テンプレート編集ビューで、**[オブジェクトの作成 (Create Object)]** > **[ネットワーク (Network)]**を選択します。

b) 右側の **[表示名 (Display Name)]** ペインで、ネットワークの名前を入力します。

c) （オプション）**[ネットワーク ID (Network ID)]** を入力します。

ネットワーク ID を指定するか、フィールドを空のままにしておくと、スキーマを保存するときに ID が NDO によって自動的に割り当てられます。

d) これが**[レイヤ 2 専用 (Layer2 Only)]** ネットワークであるかどうかを選択します。

e) **[仮想ルーティングと転送 (Virtual Routing & Forwarding)]** ドロップダウンから、先ほど作成した、ネットワーク用の VRF を選択します。

このオプションは、**[レイヤ 2 専用 (Layer2 Only)]** を有効にした場合は使用できません。

f) **[ネットワーク プロファイル (Network Profile)]** ドロップダウンから、ネットワーク プロファイルを選択します。

`Default_Network_Universal` プロファイルを割り当てるか、NDFC で以前に作成した使用可能なネットワークプロファイルを選択できます。NDFC で作成されたプロファイルは自動的に NDO にインポートされ、ここで選択できます。

g) **[ネットワーク拡張プロファイル (Network Extension Profile)]** ドロップダウンから、ネットワーク プロファイルを選択します。

`Default_Network_Extension_Universal` プロファイルを割り当てるか、NDFC で以前に作成した使用可能なネットワーク拡張プロファイルを選択します。NDFC で作成されたプロファイルは自動的に NDO にインポートされ、ここで選択できます。

h) ネットワークの **[VLAN ID]** を指定します

i) **[VLAN 名 (VLAN Name)]** を指定します。

j) 1 つ以上の**[サブネット (Subnets)]** を追加します。

このオプションは、**[レイヤ 2 専用 (Layer2 Only)]** を有効にした場合は使用できません。

1. **[+ 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 (Add Subnet)**] ウィンドウが開きます。

2. **[+ ゲートウェイ IP の追加 (+ Add Gateway IP)]** をクリックし、サブネットの **[ゲートウェイ IP (Gateway IP)]** アドレスを入力します。

   最大 4 つのゲートウェイ IP を設定できます。

3. 追加する最初のゲートウェイに対して `[プライマリ (Primary)]` を選択します。

4. ゲートウェイ情報を保存するには、チェックマークをクリックします。

5. 追加のゲートウェイを提供するには、前のサブステップを繰り返します。

6. **[追加 (Add)]** をクリックして、サブネットの追加を終了します。

k) **[ARP の抑制 (Suppress ARP)]** を行うかどうかを選択します。

l) このネットワークの **[MTU]** を指定します。

m) **[ルーティング タグ (Rounting Tag)]** を指定します。

ステップ 3 ネットワークのサイトローカル プロパティを設定します。

ネットワークが展開されているすべてのサイトに適用されるネットワークの一般的なプロパティに加えて、このネットワークのサイト固有のプロパティをサイトごとに個別に設定できます。

a) **[サイト (SITES)]** の下の左側のサイドバーで、VRFが定義されているテンプレートを選択します。

b) メインペインで、[VRF] を選択します。

c) 右側の **[プロパティ (Properties)]** サイドバーで、サイト固有の設定を指定します。

次のサイトローカル プロパティを設定できます。

- **[テナント ルーテッド マルチキャスト (Tenant Routed Multicast)]** をオンにする： テナント ルーテッドマルチキャスト（TRM）は、BGPベースのEVPNコントロールプレーンを使用するVXLANファブリック内でのマルチキャスト転送を有効にします。TRM は、ローカルまたは VTEP 間で同じサブネット内または異なるサブネット内の送信元と受信側の間にマルチテナント対応のマルチキャスト転送を実装します。
- **[L3ゲートウェイボーダーの有効化 (Enable L3 Gateway Border)]** をオンにして、ボーダー ゲートウェイでレイヤ 3 SVIを有効にし、デュアルアタッチド ホストを接続できるようにします。

- **[DHCP ループバック ID (DHCP Loopback ID)]** を入力します。

  値は 0 ～ 1023 の範囲にする必要があります。

- **[+ DHCP サーバーの追加 (+ Add DHCP Server)]** をクリックして、1 つ以上の DHCP リレー サーバーを追加します。

  開いた **[DHCP サーバーの追加 (Add DHCP Server)]** ウィンドウで、DHCP リレーの IP アドレスと所属する VRF を入力します。

- **[+ スタティック ポートの追加 (+ Add Static Port)]** をクリックして、ネットワークの VLAN を接続する 1 つ以上のポートを追加します。

  開いた **[スタティック ポートの追加 (Add Static Port)]** ウィンドウで、ポートを含むリーフスイッチを選択し、VLAN IDを入力し、最後に **[ポートの追加 (Add Port)]** をクリックしてネットワークのポートを 1 つ以上指定します。

  異なるリーフ スイッチから複数のスタティック ポートを追加する場合は、リーフ スイッチごとにこのプロセスを繰り返す必要があります。

テンプレート オブジェクトの一括更新

一括更新機能を使用すると、テンプレート内の同じタイプの複数の異なるオブジェクトの複数のプロパティを一度に更新できます。このワークフローを使用する場合、選択したすべてのオブジェクトは同じタイプである必要があります。そうでない場合、更新機能は機能しません。たとえば、Cisco NDFC の場合、VRF とネットワークを同時に更新することは選択できません。

オブジェクトのタイプで「選択」を使用して、それらのオブジェクトのプロパティを更新できます。選択したオブジェクトにすでに別のプロパティ値が構成されている場合、更新により、それらのプロパティが指定した値で上書きされます。

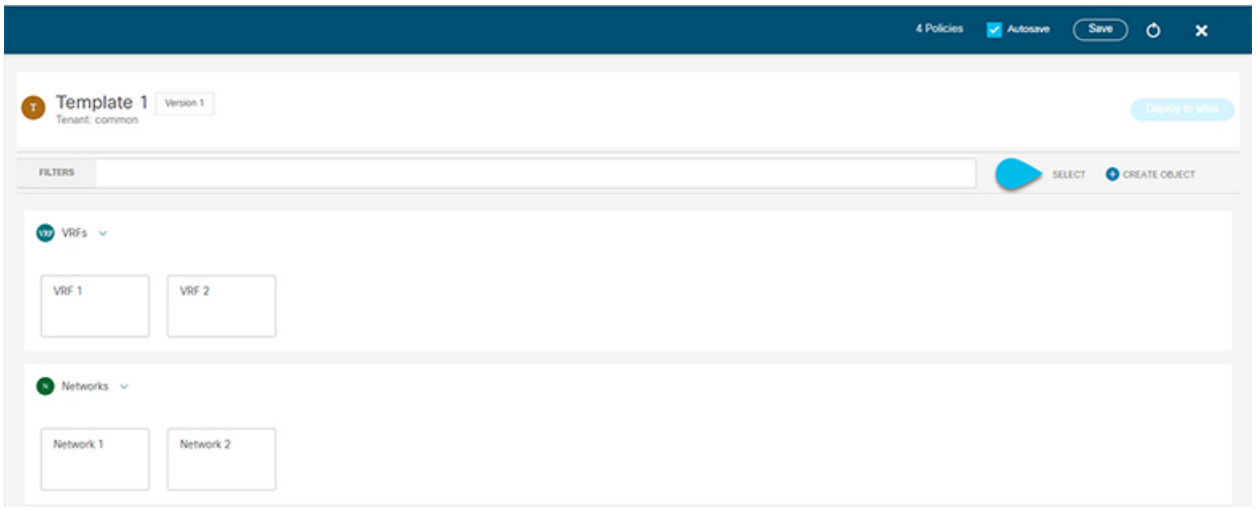
（注） この機能は、Cisco APIC および Cisco NDFC ファブリックでのみサポートされています。 Cisco Cloud Network Controller サイトではサポートされていません。

次の例では、プロセスを順を追って説明します。

ステップ 1 更新するオブジェクトが含まれているスキーマとテンプレートに移行します。

ステップ 2 次の図は、1 つのテンプレートに属するすべてのオブジェクトを示しています。

[選択] を選びます。複数のオブジェクトを一度に選択できるようになります。



ステップ 3 更新するすべてのオブジェクトを選択した後。

a) キャンセル オプションの横にある [...] を選択します。

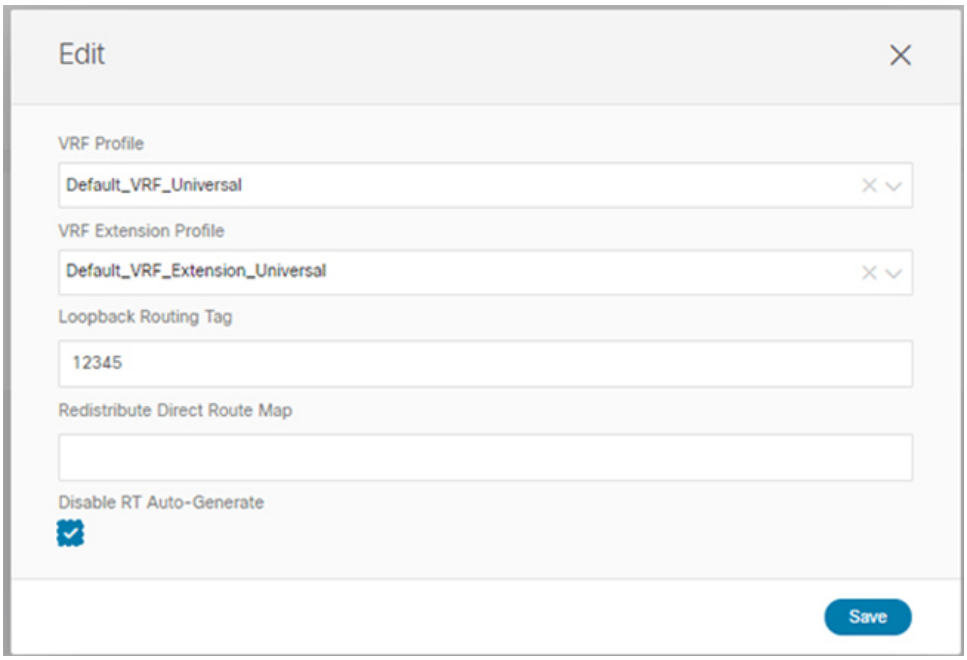
b) ドロップダウンから [編集（Edit）] を選択します。

異なるタイプのオブジェクトを選択した場合、ドロップダウンに [編集（Edit）] オプションは表示されません。

ステップ 4 [編集（Edit）] を選択すると、ポップアップが表示されます。

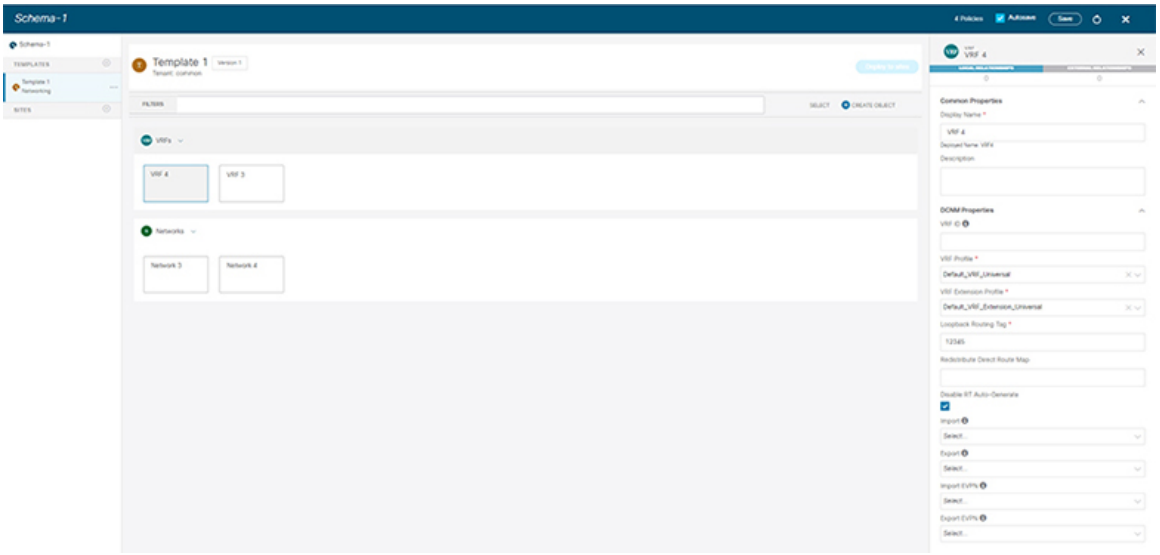
選択したオブジェクトのタイプに基づいて、次のプロパティを更新できます。

1. **VRF**：VRF プロファイル、VRF 拡張プロファイル、ループバック ルーティング タグ、ダイレクト ルート マップの再配布、RT 自動生成の無効化。
2. **ネットワーク**：レイヤ 2 のみ、ネットワーク プロファイル、ネットワーク拡張プロファイル。



ステップ 5 [保存] を選択すると、行った更新が実装されます。

ステップ 6 更新を保存すると、行った変更を確認できます。



テンプレートのバージョニング

テンプレートが保存されるたびに、新しいバージョンのテンプレートが作成されます。NDO UI 内から、テンプレートのすべての設定変更の履歴を、変更者と変更日時に関する情報とともに表示できます。以前のバージョンを現在のバージョンと比較することもできます。

新しいバージョンはスキーマ レベルではなくテンプレート レベルで作成されるため、各テンプレートを個別に設定、比較、ロールバックできます。

テンプレート バージョンは、次のルールに従って作成および管理されます。

- すべてのテンプレート バージョンは、Deployed または Intermediate のいずれかです。

  Deployed — サイトに展開されたテンプレートのバージョン。

  Intermediate — 変更および保存されたが、サイトに展開されていないテンプレートのバージョン。

- テンプレートごとに最大 20 の Deployed バージョンと 20 の Intermediate バージョンをいつでも保存できます。
- 20 バージョンの制限を超える新しい Intermediate バージョンが作成されると、最も古い既存の Intermediate バージョンが削除されます。
- テンプレートが展開され、新しいDeployedバージョンが作成されると、すべてのIntermediateバージョンが削除されます。新しい Deployed バージョンが 20 バージョン制限を超えると、最も古い既存の Deployed バージョンが削除されます。
- バージョンに Golden のタグを付けても、保存されているテンプレート バージョンの数には影響しません。
- `Golden` のタグが付いたテンプレートは削除できません。

  テンプレートを削除する前に、まずタグを解除する必要があります。

- テンプレートが変更されて保存または展開されると、20 のDeployed および 20 の Intermediate スケールを超えるバージョンは、上記のルールに従って削除されます。
- 4.0(1) より前のリリースからリリース 4.0(1) 以降にアップグレードする場合、テンプレートの最新バージョンのみが保持されます。

タギング テンプレート

任意の時点で、テンプレートの現在のバージョンに「ゴールデン」のタグを付けることができます。たとえば、完全に検証された設定で確認、承認、および展開されたバージョンを示すために、今後の参照用に選択できます。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左型のナビゲーション メニューで、**[アプリケーション管理 (Application Management)]** > **[スキーマ (Schemas)]** を選択します。

ステップ 3 表示するテンプレートを含むスキーマをクリックします。

ステップ 4 [スキーマ (Schema)]ビューで、確認するテンプレートを選択します。

ステップ 5 テンプレートのアクション（**...**）メニューから、**[ゴールデンとして設定 (Set as Golden)]** を選択します。

テンプレートがすでにタグ付けされている場合、オプションは **[ゴールデンの削除 (Remove Golden)]** に変更され、現在のバージョンからタグを削除できます。

タグ付けされたバージョンは、テンプレートのバージョン履歴画面でスターアイコンで示されます。

履歴の表示と以前のバージョンの比較

ここでは、テンプレートの以前のバージョンを表示し、現在のバージョンと比較する方法について説明します。

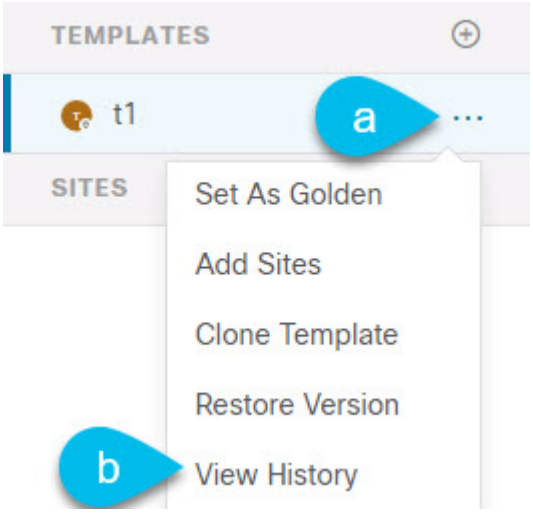
ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左型のナビゲーション メニューで、**[アプリケーション管理 (Application Management)]** > **[スキーマ (Schemas)]** を選択します。

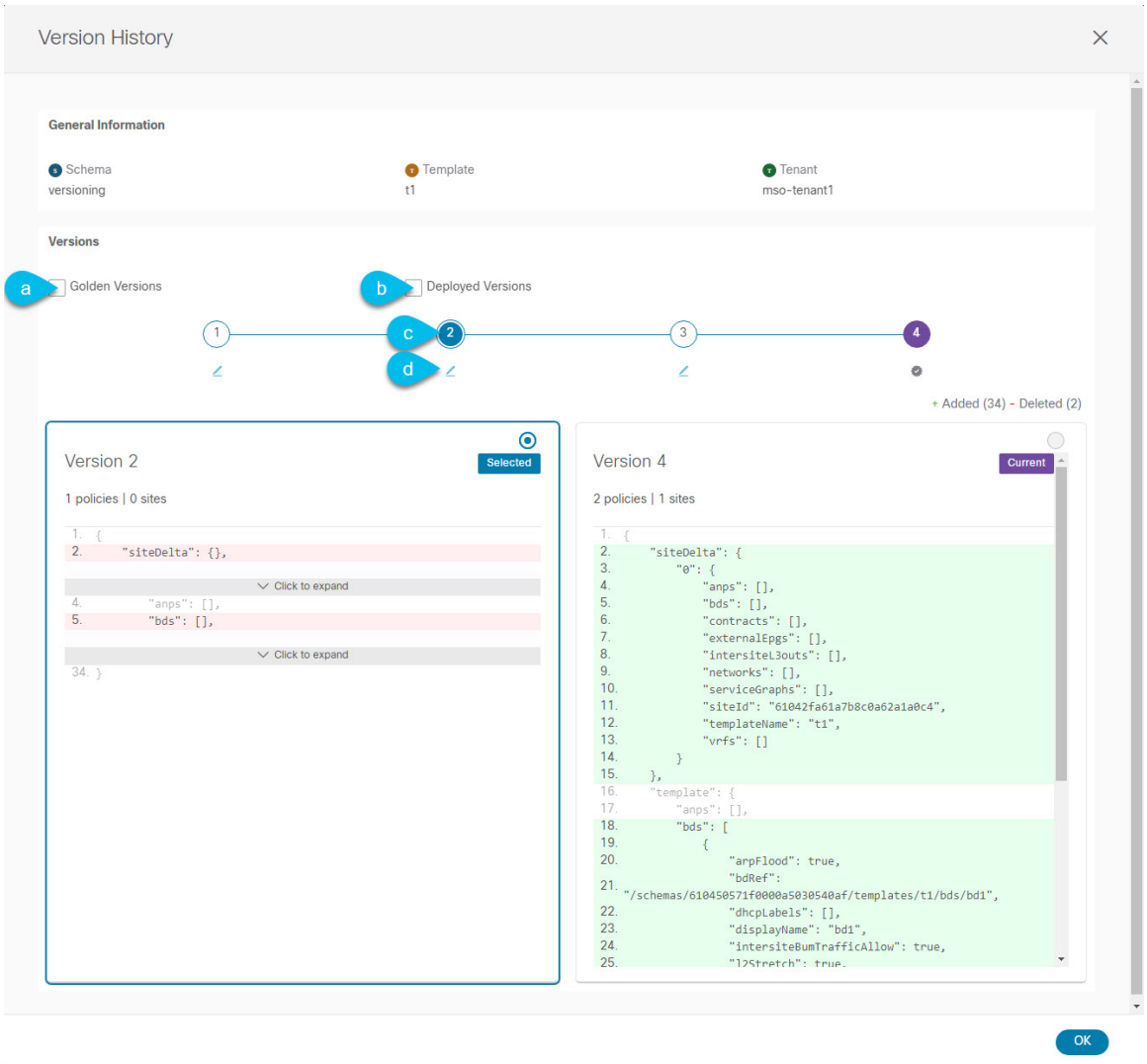
ステップ 3 表示するテンプレートを含むスキーマをクリックします。

ステップ 4 [スキーマ (Schema)]ビューで、確認するテンプレートを選択します。

ステップ 5 テンプレートのアクション（**...**）メニューから、**[履歴の表示 (View History)]** を選択します。



ステップ 6 **[バージョン履歴 (Version History)]** ウィンドウで、適切な選択を行います。



a) **[ゴールデン バージョン (Golden Versions)]** チェックボックスをオンにして、以前のバージョンのリストをフィルタリングし、`Golden` としてマークされていたこのテンプレートのバージョンのみを表示します。

「Golden」としてのテンプレートのタグ付けについては、タギング テンプレート （34 ページ）を参照してください。

b) 以前のバージョンのリストをフィルタリングして、サイトに展開されていたこのテンプレートのバージョンのみを表示するには、**[展開済みバージョン (Deployed Versions)]**チェックボックスをオンにします。

新しいテンプレート バージョンは、テンプレートが変更され、スキーマが保存されるたびに作成されます。ある時点でサイトに実際に展開されたテンプレートのバージョンのみを表示するように選択できます。

c) 特定のバージョンをクリックして、現在のバージョンと比較します。

選択したバージョンは、常にテンプレートの現在のバージョンと比較されます。**[ゴールデンバージョン (Golden Versions)]** または **[導入済みバージョン (Deployed Versions)]** フィルタを使用してリストをフィルタリングした場合でも、導入済みまたはゴールデンとしてタグ付けされていない場合でも、現在のバージョンが常に表示されます。

d) **[編集 (Edit)]** アイコンの上にマウスを置くと、バージョンの作成者と作成日時に関する情報が表示されます。

ステップ 7 **[OK]** をクリックして、バージョン履歴ウィンドウを閉じます。

以前の製品バージョンへの復元

ここでは、以前のバージョンのテンプレートを復元する方法について説明します。テンプレートを元に戻す場合、次のルールが適用されます。

- ターゲットバージョンが存在しないオブジェクトを参照している場合、復元操作は許可されません。
- ターゲットバージョンが NDO で管理されなくなったサイトを参照している場合、復元操作は許可されません。
- 現在のバージョンが、ターゲットバージョンが展開されていない1つ以上のサイトに展開されている場合、復元操作は許可されません。

  テンプレートを元に戻す前に、まずそれらのサイトから現在のバージョンを展開解除する必要があります。
- ターゲットバージョンが、現在のバージョンが展開されていない1つ以上のサイトに展開されている場合、復元操作は許可されます。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左型のナビゲーションメニューで、**[アプリケーション管理 (Application Management)]**>**[スキーマ (Schemas)]** を選択します。

ステップ 3 表示するテンプレートを含むスキーマをクリックします。

ステップ 4 [スキーマ (Schema)]ビューで、確認するテンプレートを選択します。

ステップ 5 **[アクション（Actions）]**（**[...]**）メニューから、**[ロールバック（Rollback）]** を選択します。

ステップ 6 **[ロールバック（Rollback）]** ウィンドウで、復元する以前のバージョンのいずれかを選択します。

[ゴールデン バージョン (Golden Versions)] チェックボックスと**[展開済みバージョン (Deployed Versions)]** チェックボックスを使用して、バージョンのリストをフィルタリングできます。

バージョンを選択すると、そのバージョンのテンプレート設定をテンプレートの現在のバージョンと比較できます。

ステップ 7 **[復元 (Restore)]** をクリックして、選択したバージョンを復元します。

以前のバージョンを復元すると、前の手順で選択したバージョンと同じ設定の新しいバージョンのテンプレートが作成されます。

たとえば、最新のテンプレートバージョンが 3 で、バージョン 2 を復元すると、バージョン 4 が作成されます。バージョン 2 の設定と同じだからです。復元を確認するには、テンプレートのバージョン履歴を参照し、現在の最新バージョンと復元時に選択したバージョンを比較します。

テンプレートのレビューと承認（変更管理）が無効になっており、アカウントにテンプレートを展開するための適切な権限がある場合は、復元したバージョンを展開できます。

ただし、変更制御が有効になっている場合は、次のようになります。

- 以前に展開したバージョンに戻し、アカウントにテンプレートを展開するための正しい権限がある場合は、すぐにテンプレートを展開できます。
- 以前に展開されていなかったバージョンに戻す場合、またはアカウントにテンプレートを展開するための適切な権限がない場合は、復元されたバージョンを展開する前にテンプレートの承認を要求する必要があります。

  レビューと承認プロセスに関する追加情報については、テンプレートのレビューと承認（38ページ）セクションを参照してください。

テンプレートのレビューと承認

テンプレートのレビューと承認（変更管理）ワークフローは、テンプレートの設計者、レビュー担当者、承認者、およびテンプレートの導入者に指定されたロールを設定し、また、導入した設定が検証プロセスを確実にパスできるようにします。

テンプレート設計者は、NDO UI 内から、作成したテンプレートのレビューを要求できます。その後、レビュー担当者は、テンプレートのすべての設定変更の履歴と、誰がいつ変更したかに関する情報を表示できます。この時点で、テンプレートの現在のバージョンを承認または拒否できます。テンプレート設定が拒否された場合、テンプレート設計者は必要な変更を行い、レビューを再要求できます。テンプレートが承認されると、展開担当者のロールを持つユーザがサイトに展開できます。最後の点として、導入者自身が承認済みテンプレートの導入を拒否し、レビュー プロセスを最初からやり直すことができます。

ワークフローはスキーマ レベルではなくテンプレート レベルで実行されるため、各テンプレートを個別に設定、確認、承認できます。

テンプレート承認要件の有効化

テンプレートの設定と展開に確認と承認のワークフローを使用するには、Nexus Dashboard Orchestrator のシステム設定でこの機能を有効にする必要があります。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左側のナビゲーション メニューで、**[インフラストラクチャ (Infrastructure)]** > **[システムの設定 (System Configuration)]**を選択します。

ステップ 3 **[変更制御 (Change Control)]** タイルで、**[編集 (Edit)]** アイコンをクリックします。

ステップ 4 **[変更制御 (Change Control)]** ウィンドウで、**[変更制御ワークフロー (Change Control Workflow)]** チェックボックスをオンにして機能を有効にします。

ステップ 5 **[承認者 (Approvers)]** フィールドに、テンプレートを展開する前に必要な一意の承認の数を入力します。

ステップ 6 [保存（Save）] をクリックして、変更内容を保存します。

必要なロールを持つユーザの作成

テンプレートの設定と展開のため、レビューと承認のワークフローを実施する前に、NDO サービスが展開されているNexusダッシュボードで必要な権限を持つユーザーを作成する必要があります。

ステップ 1 Nexus Dashboard の GUI にログインします。

NDO GUI でユーザーを作成または編集することはできません。サービスが展開されている Nexus ダッシュボード クラスタに直接ログインする必要があります。

ステップ 2 左のナビゲーション メニューから、**[管理 (Administrative)]** > **[ユーザー (Users)]**を選択します。

ステップ 3 必要なユーザーを作成します。

ワークフローは、テンプレート設計者、承認者、および展開者という 3 つの異なるユーザー ロールに依存します。各ロールを異なるユーザーに割り当てることも、同じユーザーにロールの組み合わせを割り当てることもできます。管理者権限を持つユーザは、3 つのアクションすべてを実行できます。

ローカルまたはリモートの Nexus ダッシュボード ユーザーのユーザーとその権限の設定の詳細については、『Nexus Dashboard User Guide』を参照してください。

承認者ロールを持つ別個のユーザーが、テンプレート承認要件の有効化 （38 ページ）で設定した承認の最小数と同数以上必要です。

（注） **変更制御ワークフロー**機能を無効にすると、承認者と展開者のユーザーは Nexus Dashboard Orchestrator に読み取り専用でアクセスできます。

テンプレートのレビューと承認の要求

ここでは、テンプレートのレビューと承認を要求する方法について説明します。

始める前に

次のものが必要です。

- 承認要件のグローバル設定を有効にした（テンプレート承認要件の有効化 （38 ページ）を参照）。
- 承認者ロールと展開者ロールを使用してNexusダッシュボードでユーザを作成または更新した（必要なロールを持つユーザの作成 （39 ページ）を参照）。
- 1 つ以上のポリシー設定を含むテンプレートを作成し、1 つ以上のサイトに割り当てた。

ステップ 1 テナントマネージャ、サイトマネージャ、または管理者ロールを持つユーザとして Nexus Dashboard Orchestrator GUI にログインします。

ステップ 2 左型のナビゲーション メニューで、**[アプリケーション管理 (Application Management)]** > **[スキーマ (Schemas)]** を選択します。

ステップ 3 承認を要求するテンプレートを含むスキーマをクリックします。

ステップ 4 スキーマビューで、テンプレートを選択します。

ステップ 5 メイン ペインで、**[承認のために送信 (Send for Approval)]** をクリックします。

[承認のために送信 (Send for Approval)] ボタンは、次の場合には使用できません。

- グローバル変更制御オプションが有効になっていない
- テンプレートにポリシー設定がないか、どのサイトにも割り当てられていない
- ユーザにテンプレートを編集する権限がない
- テンプレートは承認のためにすでに送信されている
- テンプレートが承認者ユーザによって拒否された

テンプレートのレビューと承認

ここでは、テンプレートのレビューと承認を要求する方法について説明します。

始める前に

次のものが必要です。

- 承認要件のグローバル設定を有効にした（テンプレート承認要件の有効化 （38 ページ）を参照）。
- 承認者ロールと展開者ロールを使用してNexusダッシュボードでユーザを作成または更新した（必要なロールを持つユーザの作成 （39 ページ）を参照）。
- 1 つ以上のポリシー設定を含むテンプレートを作成し、1 つ以上のサイトに割り当てた。
- テンプレートのレビューと承認の要求 （39 ページ）に記載されているように、スキーマエディタによってテンプレートの承認が要求されました。

ステップ 1 承認者 (Approver) または管理者 (admin) ロールを持つユーザとして Nexus Dashboard Orchestrator GUIにログインします。

ステップ 2 左型のナビゲーション メニューで、**[アプリケーション管理 (Application Management)]**>**[スキーマ (Schemas)]** を選択します。

ステップ 3 確認して承認するテンプレートを含むスキーマをクリックします。

ステップ 4 スキーマビューで、テンプレートを選択します。

ステップ 5 メインペインで、**[承認 (Approve)]** をクリックします。

すでにテンプレートを承認または拒否している場合は、テンプレート デザイナが変更を行い、再確認のためにテンプレートを再送信するまで、このオプションは表示されません。

ステップ 6 **[テンプレートの承認 (Approving template)]** ウィンドウでテンプレートを確認し、**[承認 (Approve)]** をクリックします。

承認画面には、テンプレートがサイトに展開するすべての変更が表示されます。

[バージョン履歴の表示 (View Version History)] をクリックすると、完全なバージョン履歴と、バージョン間で行われた増分変更を表示できます。バージョン履歴の詳細については、履歴の表示と以前のバージョンの比較 （35 ページ）を参照してください。

[展開計画 (Deployment Plan)] をクリックして、このテンプレートから展開される設定の可視化と JSON を表示することもできます。[展開計画 (Deployment Plan)] ビューの機能は、現在展開されている設定の表示 （47 ページ）で説明した、すでに導入されているテンプレートの [展開ビュー (Deployed View)] に似ています。

次のタスク

必要な数の承認者がテンプレートを確認して承認したら、テンプレートの展開 （41 ページ）の説明に従ってテンプレートを展開できます。

テンプレートの展開

ここでは、NDFC ファブリックに新しい設定または更新された設定を展開する方法について説明します。

始める前に

- このドキュメントの前のセクションで説明したように、作成されたサイトには、展開するスキーマ、テンプレート、およびオブジェクトと、1 つまたは複数のサイトに割り当てられるテンプレートが必要です。
- テンプレートのレビューと承認 （38 ページ）で説明しているように、テンプレートの確認と承認が有効になっている場合は、必要な数の承認者によってテンプレートがすでに承認されている必要があります。

ステップ 1 展開するテンプレートを含むスキーマに移動します。

ステップ 2 **[表示（View）]** ドロップダウン メニューから、展開するテンプレートを選択します。

ステップ 3 テンプレート ビューで、**[サイトに展開（Deploy to site）]** をクリックします。

[サイトに展開 (Deploy to Sites)] ウィンドウが開き、展開するオブジェクトの概要が表示されます。

ステップ 4 テンプレートに変更を加えた場合は、**[展開の計画（Deployment Plan）]** を確認して新しい構成を確認します。

以前にこのテンプレートを展開したが、それ以降に変更を加えていない場合は、**[展開]** の概要に変更がないことが示され、テンプレート全体を再展開することを選択できます。この場合は、この手順をスキップできます。

[サイトに展開 (Deploy to Sites)] ウィンドウには、サイトに展開される構成の違いの概要が表示されます。

情報目的で `[作成日 (Created)]`、`[変更日 (Modified)]`、および `[削除済み (Deleted)]` チェックボックスを使用してビューをフィルタリングすることもできますが、**[展開 (Deploy)]**をクリックするとすべての変更が展開されることに注意してください。

ここでは、次のことも選択できます。

- **[バージョン履歴の表示 (View Version History)]** を選択すると、完全なバージョン履歴とバージョンアップグレードで行われた更新内容を表示します。バージョン履歴の詳細については、履歴の表示と以前のバージョンの比較 （35 ページ）を参照してください。
- **[展開プラン (Deployment Plan)]**を確認して、このテンプレートから展開される構成の可視化と XML ペイロードを表示します。

  この機能により、テンプレートに変更を加えて 1 つ以上のサイトに展開した後に、Orchestrator がマルチサイトドメインの一部であるさまざまなファブリックにプロビジョニングする構成の変更を、より適切に可視化できます。

  テンプレートとサイト構成に加えられた特定の変更のリストを引き続き提供していた Nexus Dashboard Orchestrator の以前のリリースとは異なり、展開プランでは、テンプレートの展開によってさまざまなファブリック全体にプロビジョニングされる、すべてのオブジェクトに対する完全な可視性が提供されます。たとえば、変更内容によっては、特定の変更が 1 つのサイトのみに適用された場合でも、シャドウオブジェクトが複数のサイトに作成される場合があります。

  （注） テンプレートを展開する前に、この手順で説明されているように、展開プランを使用して変更を確認することをお勧めします。構成変更の視覚的に示すことは、意図しない構成変更の展開による潜在的なエラーを低減するのに役立ちます。

a) **[展開プラン（Deployment Plan）]** ボタンをクリックします。
b) 最初にリストされたサイトで変更を確認します。
c) 前のサブステップを繰り返して、他のサイトの変更を確認します。
d) （オプション）**[ペイロードの表示（View Payload）]** をクリックすると、各サイトの XML ペイロードを表示できます。

新規および変更されたオブジェクトの視覚的表現に加えて、各サイトの変更について [**ペイロードの表示（View Payload**）] を選択することもできます。

e) 変更の確認が完了したら、[x] アイコンをクリックして [**展開プラン（Deployment Plan**）] 画面を閉じます。

ステップ 5 [**サイトに展開（Deploy to sites**）] ウィンドウで、[**展開（Deploy**）] をクリックしてテンプレートを展開します。

サイトからのテンプレートの関連付け解除

展開を解除せずに、サイトからテンプレートの関連付けを解除することもできます。これにより、NDO からサイトに展開された設定を保持しながら、スキーマのテンプレートとサイトの関連付けを削除できます。管理対象オブジェクトとポリシーの所有権が NDO からサイトのコントローラに移されます。

始める前に

- テンプレートとその設定がサイトにすでに展開されている必要があります。
- テンプレートは、単一のサイトにのみ展開し、サイト間で展開しないようにする必要があります。
- テンプレートで定義されたオブジェクトは、他のサイトのシャドウオブジェクトとして展開しないでください。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左型のナビゲーション メニューで、**[アプリケーション管理 (Application Management)]**>**[スキーマ (Schemas)]** を選択します。

ステップ 3 関連付けを解除するテンプレートを含むスキーマをクリックします。

ステップ 4 スキーマ ビューで、関連付けを解除する特定のサイトの下のテンプレートを選択します。

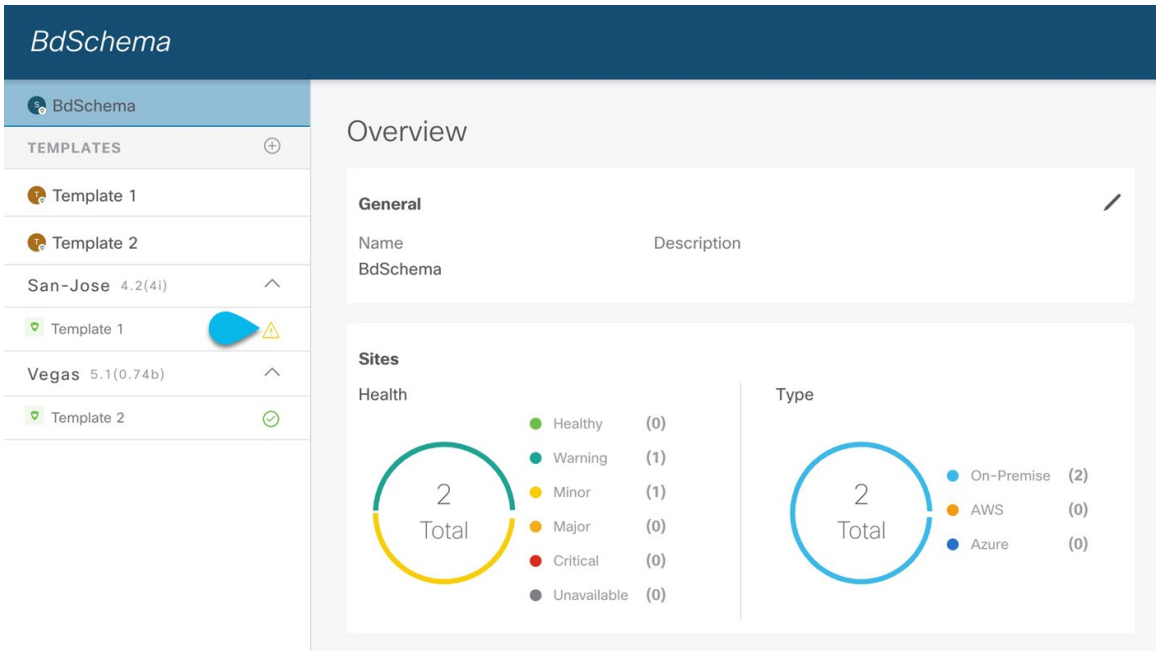
ステップ 5 **[アクション (Actions)]** メニューから **[テンプレートの関連付け解除 (Disassociate Template)]** を選択します。

ステップ 6 確認ウィンドウで、**[アクションの確認 (Confirm Action)]** をクリックします。

設定のばらつき

時折、NDFC ドメインに実際に展開された構成が、Nexus Dashboard Orchestrator でそのドメインに対して定義された構成と異なる場合があります。これらの構成の不一致は、**[構成のばらつき（Configuration Drifts**）] と呼ばれ、次の図に示すように、スキーマ ビューのテンプレート名の横に黄色の注意サインで示されます。

図 *1:*



設定のばらつきは、さまざまな理由で発生する可能性があります。構成のばらつきを解決するために必要な実際の手順は、その原因によって異なります。最も一般的なシナリオとその解決策を次に示します。

- **NDO で設定が変更された**：NDO GUIでテンプレートを変更すると、変更をサイトに展開するまでは、設定のばらつきとして表示されます。

  このタイプの設定のずれを解決するには、テンプレートを展開して変更をサイトに適用するか、スキーマの変更を元に戻します。

- **設定がサイトのコントローラで直接変更された**：NDO から展開されたオブジェクトは、サイトの NDFC で警告アイコンとテキストで示されるので、管理ユーザーは、設定のばらつきの原因に対し、引き続き変更を加えられます。

- **NDO 設定がバックアップから復元された**：NDO のバックアップから設定を復元すると、バックアップが作成されたときのオブジェクトとその状態のみが復元され、復元された設定は自動的に再展開されません。そのため、バックアップが作成されてから構成に変更が加えられ、NDFC に展開された場合、バックアップを復元すると構成のばらつきが生じる可能性があります。

- **NDO 設定は、古いリリースで作成されたバックアップから復元された**：新しいリリースで、以前のリリースではサポートされていなかったオブジェクトプロパティのサポートが追加された場合、これらのプロパティによって設定がずれる可能性があります。通常、これは、サイトの NDFC GUI で新しいプロパティが直接変更され、それらの値が Nexus Dashboard Orchestrator が想定しているデフォルトと食い違った場合に発生します。

- **NDO が以前のリリースからアップグレードされた**：このシナリオは、新しいオブジェクトプロパティが新しいリリースに追加された場合に、既存の設定がずれている可能性がある、前のシナリオと似ています。

  テンプレートに対して「ばらつきの調整」ワークフローを実行して、ばらつきの原因をより詳細に把握し、ばらつきを調整できるようにすることをお勧めします。この推奨事項は、このセクションで前述したすべてのばらつきのシナリオに適用されます。ばらつきの調整ワークフローの詳細については、以下の「構成のばらつきの調整」セクションを参照してください。

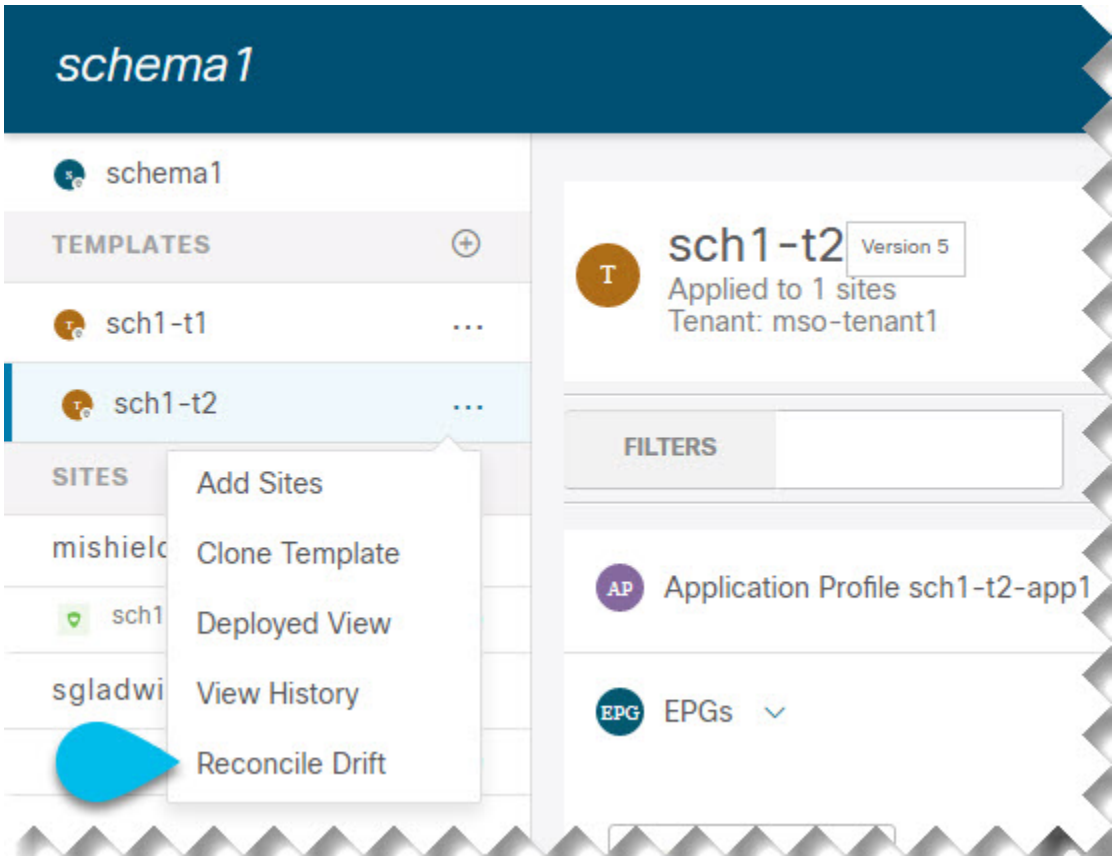
設定のばらつきの調整

NDO リリース 3.6(1) では、Nexus Dashboard Orchestrator で定義されたテンプレート構成と、マルチサイト ドメインのサイト部分の NDFC コントローラでレンダリングされた構成を比較するために実行できる、ばらつき調整ワークフローのサポートが導入されています。これにより、構成のばらつき（つまり、Nexus Dashbaord Orchestrator または NDFC で直接行われた変更）の原因をより明確に把握でき、以下の手順で説明するように、ばらつきを調整する方法をユーザーに選択させることができます。

（注） 選択した構成が必要ない場合は、スキーマを閉じて再度開くことができます。これにより、元の構成が表示されます。必要に応じて、「Reconcile Drift」フローを再度トリガーできます。[保存（Save）] または [展開（Deploy）] ボタンを選択した後にのみ、スキーマが保存されます。

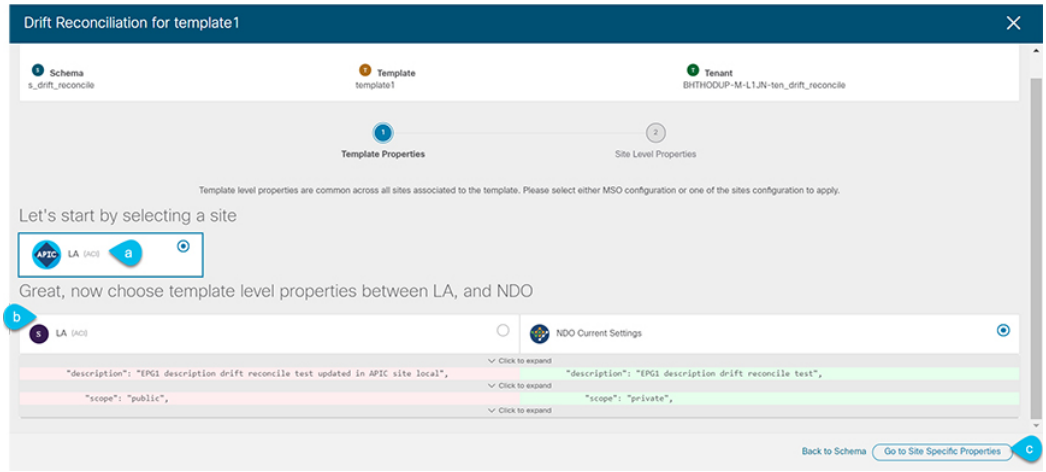
ステップ 1 設定のばらつきを確認するテンプレートを含むスキーマに移動します。

ステップ 2 テンプレートの **[アクション (Actions)]** メニューから、**[ばらつきの調整 (Reconcile Drift)]** を選択します。



[ばらつきの調整 (Reconcile Drift)] ウィザードが開きます。

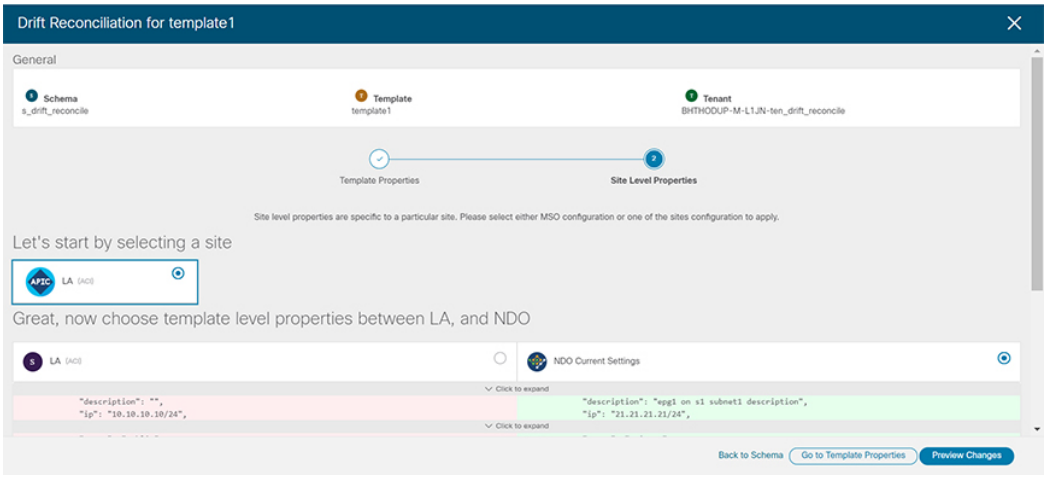
ステップ 3 **[ばらつきの調整 (Reconcile Drift)]** 画面で、各サイトのテンプレートレベルの構成を比較し、希望のものを選択します。



テンプレートレベルのプロパティは、テンプレートに関連付けられているすべてのサイトに共通です。Nexus Dashboard Orchestrator で定義されたテンプレート レベルのプロパティを各サイトでレンダリングされた構成と比較し、Nexus Dashboard Orchestrator テンプレートの新しい構成を決定できます。サイト構成の

選択は、既存の Nexus Dashboard Orchestrator テンプレートのこれらのプロパティを変更し、その場合、Nexus Dashboard Orchestrator の構成を選択すると、既存の Nexus Dashboard Orchestrator テンプレートの設定はそのまま残されます

ステップ 4 **[サイト特有のプロパティに移動（Go to Site Specific Properties）]** をクリックして、サイトレベルの構成に切り替えます。



特定のサイトの構成を比較するために、サイトを選択できます。テンプレートレベルの設定とは異なり、各サイトの Nexus Dashboard Orchestrator 定義または実際の既存の設定を個別に選択して、そのサイトのテンプレートのサイトローカル プロパティとして保持できます。

ほとんどのシナリオでは、テンプレートレベルとサイトレベルの両方の構成で同じ選択を行いたとしても、ばらつきの調整ウィザードでは、サイトのコントローラで「テンプレートのプロパティ」レベルで定義された構成と Nexus Dashboard Orchestratorで定義された構成またはその逆を選択できます。

ステップ 5 **[変更のプレビュー（Preview Changes）]** をクリックして、選択内容を確認します。

プレビューは **[ばらつきの調整 (Reconcile Drift)]** ウィザードの選択肢に基づいて調整された完全なテンプレート構成を表示します。その後、**[サイトに展開（Deploy to site）]** をクリックして構成を展開し、そのテンプレートのばらつきを調整できます。

現在展開されている設定の表示

特定のテンプレートからサイトに現在展開されているすべてのオブジェクトを表示できます。任意のテンプレートを何度でも展開、展開解除、更新、および再展開できますが、この機能では、これらすべてのアクションの結果としての最終的な状態のみが表示されます。たとえば、`Template1` に `VRF1` オブジェクトのみが含まれ、`Site1` に展開されている場合、API はテンプレートの `VRF1` のみを返します。その後、`VRF2` を追加して再展開すると、API はこの時点から `VRF1` と `VRF2` の両方のオブジェクトを返します。

この情報は Orchestrator データベースから取得されるため、サイトのコントローラで直接行われた変更によって発生する可能性のある設定の変動は考慮されません。

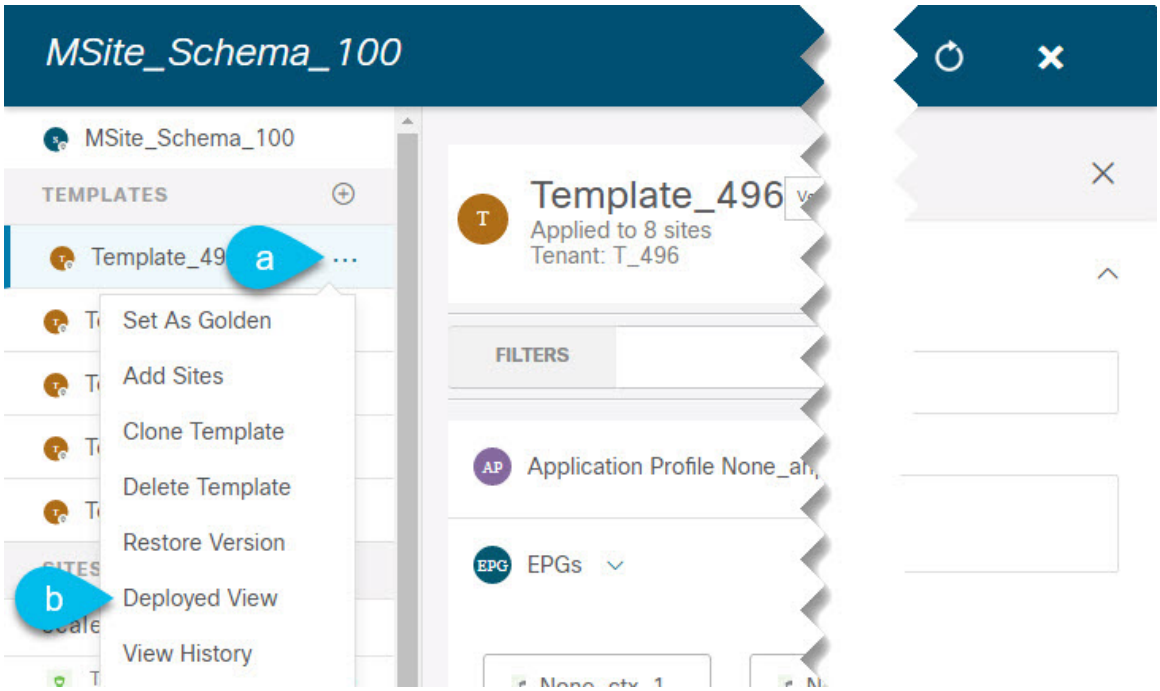
ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左型のナビゲーション メニューで、**[アプリケーション管理 (Application Management)]** > **[スキーマ (Schemas)]** を選択します。

ステップ 3 表示するテンプレートを含むスキーマをクリックします。

ステップ 4 左側のサイドバーで、テンプレートを選択します。

ステップ 5 そのテンプレートの **[展開ビュー (Deployed View)]** を開きます。



a) テンプレートの名前の横にある **[アクション (Actions)]** メニューをクリックします。

b) **[展開ビュー (Deployed View)]** をクリックします。

ステップ 6 **[展開ビュー (Deployed View)]** 画面で、情報を表示するサイトを選択します。

サイトにすでに展開されているものと、テンプレートで定義されているものとのテンプレート設定の比較がグラフィカルに表示されます。

a) 色分けされた凡例は、この時点でテンプレートを展開する場合に作成、削除、または変更されるオブジェクトを示します。

テンプレートの最新バージョンがすでに展開されている場合、ビューには色分けされたオブジェクトは含まれず、現在展開されている設定が表示されます。

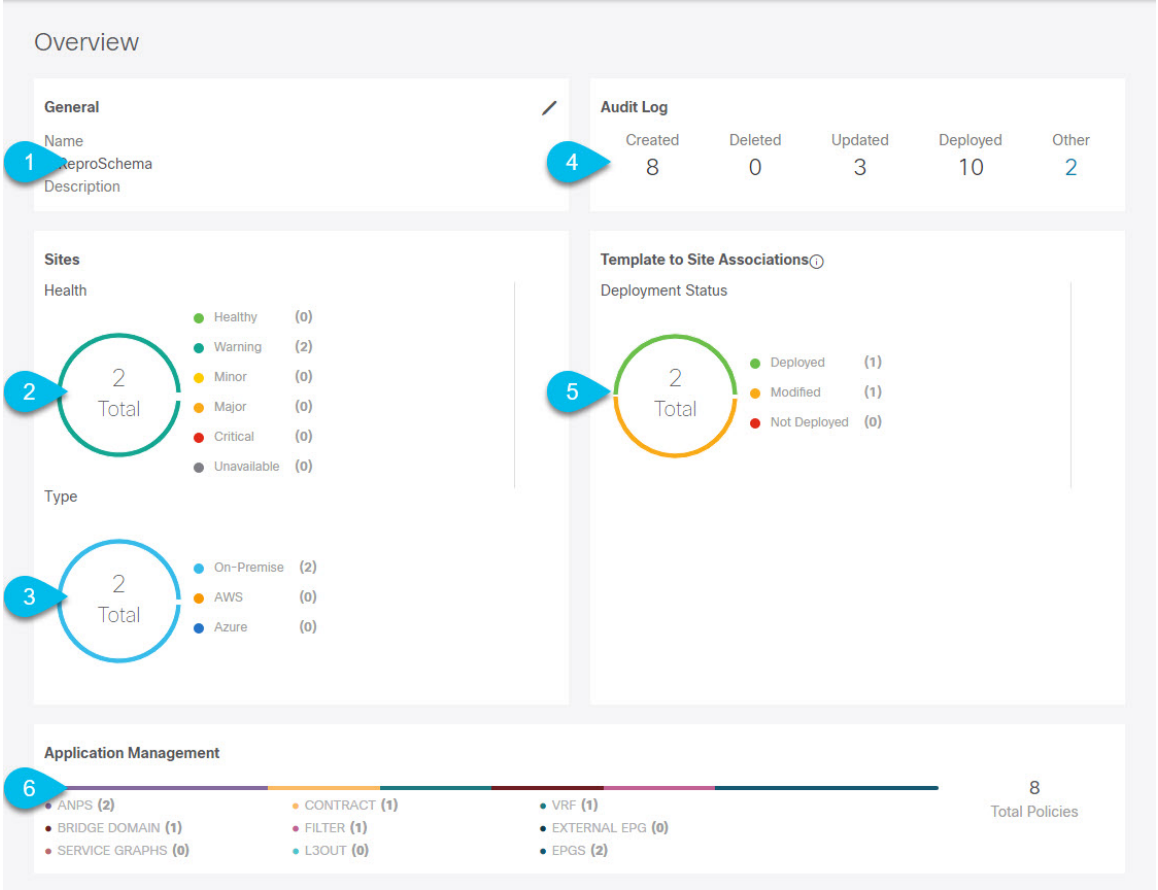
b) サイト名をクリックすると、その特定のサイトの設定を表示できます。

c) **[JSON 表示 (View JSON)]** をクリックすると、選択したサイトに展開されているすべてのオブジェクトの構成が表示されます。

スキーマの概要と展開ビジュアライザ

1 つ以上のオブジェクトが定義され、1 つ以上のファブリックに展開されているスキーマを開くと、スキーマの **[概要 (Overview)]** ページに展開の概要が表示されます。

図 *2 :* スキーマの概要



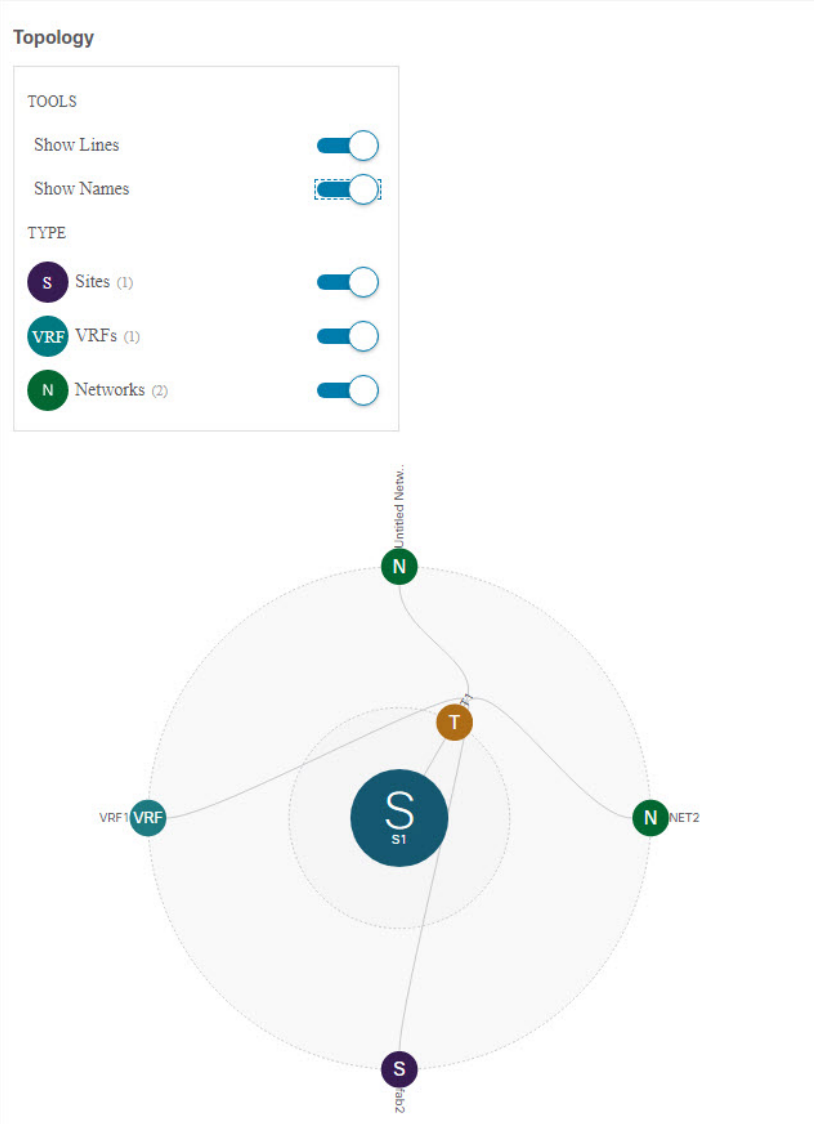
このページには、次の詳細が表示されます。

1. **[一般 (General)]**：名前や説明など、スキーマの一般情報を提供します。
2. **[監査ログ (Audit Log)]**：スキーマで実行されたアクションの監査ログの概要を提供します。
3. **[サイト (Sites)]** > **[正常性 (Health)]**：サイトの正常性ステータスでソートされた、このスキーマのテンプレートに関連付けられているサイトの数を提供します。
4. **[サイト (Sites)]** > **[タイプ (Type)]**：サイトのタイプでソートされた、このスキーマのテンプレートに関連付けられているサイトの数を提供します。
5. **[テンプレートとサイトの関連付け (Template to Site Associations)]** > **[展開ステータス (Deployment Status)]**：1 つ以上のサイトに関連付けられているこのスキーマ内のテンプレートの数とその展開ステータスを提供します。

6. **[アプリケーション管理 (Application Management)]**：このスキーマのテンプレートに含まれる個々のオブジェクトの概要を提供します。

[トポロジ (Topology)] タイルでは、次の図に示すように、1 つ以上のオブジェクトを選択してダイアグラムに表示することで、トポロジ ビジュアライザを作成できます。

図 *3*: 展開ビジュアライザ



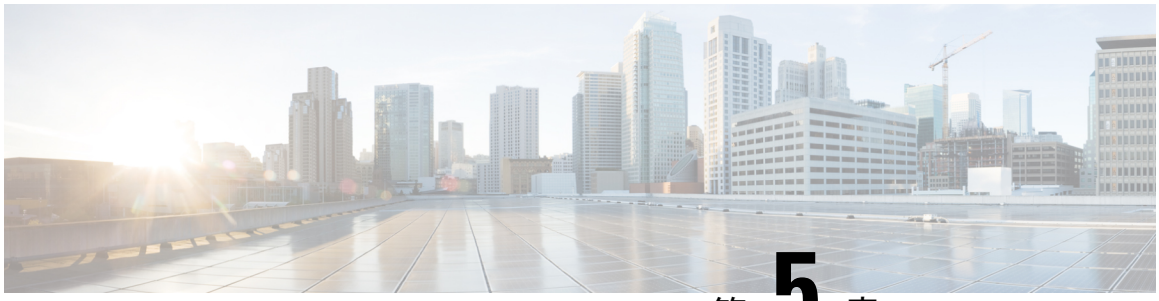
1. **[設定オプション (Configuration Options)]**：次のトポロジ図に表示するポリシー オブジェクトを選択できます。
2. **[トポロジ図 (Topology Diagram)]**：サイトに割り当てられているすべてのスキーマ テンプレートで設定されたポリシーを視覚的に表示します。

上記の **[設定オプション (Configuration Options)]** を使用して、表示するオブジェクトを選択できます。

また、オブジェクトの上にマウスを置くと、すべての依存関係を強調表示できます。

第 I 部

運用とインフラストラクチャ



第 5 章

監査ログ

監査ログ

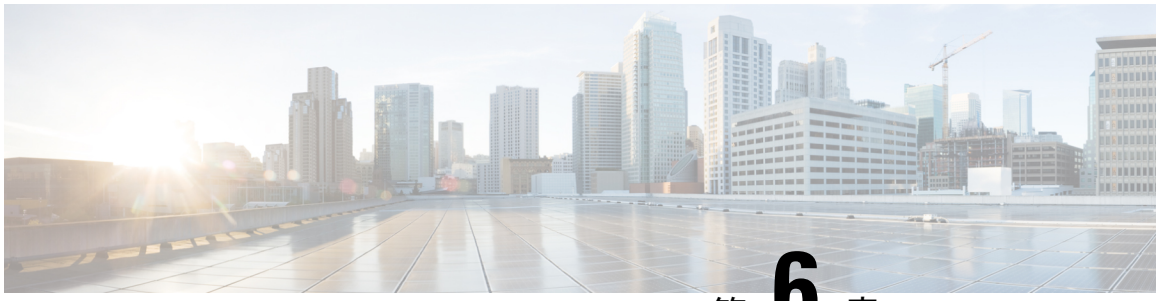
Nexus Dashboard Orchestrator のシステム ロギングは、最初に Orchestrator クラスタをデプロイしたときに自動的に有効になり、環境内で発生したイベントと障害をキャプチャします。

GUI 内で直接 Nexus Dashboard Orchestrator のログを表示するには、メインのナビゲーション メニューから **[操作 (Operations)]** > **[監査ログ (Audit logs)]** を選択します。

[**監査ログ (Audit Logs)**] ページで、**最新のフィールド**をクリックして、ログを表示する特定の期間を選択できます。たとえば、2017 年 11 月 14日から 2017 年 11 月 17日までの範囲を選択し、[**適用 (Apply)**] をクリックすると、この期間の監査ログの詳細が [**監査ログ (Audit Logs)**] ページに表示されます。

次の基準に従ってログの詳細のフィルタ処理を行うには、[**フィルタ (Filter)**] アイコンをクリックします。

- **ユーザ(User)**: ユーザ タイプに基づいて監査ログのフィルタ処理を行うには、このオプションを選択し、[**適用 (Apply)**] をクリックします。
- **タイプ (Type)** : 監査ログをポリシータイプ（サイト、ユーザ、テンプレートなど）でフィルタリングするには、このオプションを選択して、**[適用 (Apply)]** をクリックします。
- **アクション(Action)**: アクションに基づいて監査ログをフィルタ処理するには、このオプションを選択します。使用可能なアクションとしては作成、更新、削除、追加、関連付け、関連付けの解除解除、展開、展開の解除、ダウンロード、アップロード、復元、ログイン、ログの失敗があります。アクションに従ってログの詳細をフィルタ処理するには、アクションを選択して **Apply** をクリックします。



第 6 章

バックアップと復元

設定のバックアップと復元

Nexus Dashboard Orchestrator の障害またはクラスタの再起動からのリカバリを容易にする、Orchestrator 設定のバックアップを作成できます。Orchestrator の各アップグレードまたはダウングレードの前で、各設定の変更または展開後に、設定のバックアップを作成することを推奨します。バックアップは常に、Nexus Dashboard Orchestratorで定義されているリモート サーバ（Nexus Dashboard クラスタ以外）に作成されます。定義については、続くセクションで説明します。

構成のバックアップと復元に関するガイドライン

Nexus Dashboard Orchestrator の障害またはクラスタの再起動からのリカバリを容易にする、Orchestrator 設定のバックアップを作成できます。Orchestrator の各アップグレードまたはダウングレードの前で、各設定の変更または展開後に、設定のバックアップを作成することを推奨します。バックアップは常に、Nexus Dashboard Orchestratorで定義されているリモート サーバ（Nexus Dashboard クラスタ以外）に作成されます。定義については、続くセクションで説明します。

構成のバックアップを作成する際には、次のガイドラインが適用されます。

- より新しいリリースから作成されたバックアップのインポートおよび復元はサポートされていません。

たとえば、Nexus Dashboard Orchestrator を以前のリリースにダウングレードした場合、それ以降のリリースで作成された設定のバックアップを復元することはできません。

- リリース 4.0(1) より前のリリースで作成された構成バックアップの復元は、このリリースへの最初のアップグレード時にのみサポートされます。

  リリース 4.0(1) より前のリリースからこのリリースにアップグレードする場合は、*Cisco Nexus Dashboard Orchestrator* 導入ガイドの「Nexus ダッシュボードでの NDO サービスのアップグレード」の章を参照してください。

- バックアップを保存すると、設定は展開されたのと同じ状態で保存されます。バックアップを復元すると、展開されたすべてのポリシーが展開済みとして表示されますが、展開されていなかったポリシーは未展開の状態のままになります。

- バックアップ アクションの復元では、Nexus Dashboard Orchestrator のデータベースを復元しますが、各サイトのコントローラ（APIC、クラウド ネットワーク、NDFC など）データベースは変更されません。

  Orchestrator データベースを復元した後、このガイドの「構成のばらつき」セクションで説明されているように、テンプレートに表示される可能性のある構成のばらつきを解決してから、既存のテンプレートを再展開して、Nexus Dashboard と各サイトのコントローラの間でポリシーが一致しない可能性を回避することをお勧めします。

- 構成のバックアップを作成するとき、ファイルは最初に Orchestrators のローカル ドライブに作成され、リモートの場所にアップロードされた後、ローカル ストレージから削除されます。十分なローカル ディスク領域がない場合、バックアップは失敗します。

- リリース 4.0(1) 以降にアップグレードする前に、ローカル バックアップを作成できるようバックアップ スケジューラを有効にしていた場合、アップグレード後に無効になります。

  アップグレード後、セットアップしたリモート ロケーションを再度追加してから、バックアップ スケジューラを再度有効にする必要があります。

- UI を使用してバックアップを削除すると、バックアップ ファイルもリモート ロケーションから削除されます。

構成のバックアップを復元する際には、次のガイドラインが適用されます。

- バックアップが作成されてから復元されるまでの間にポリシーの変更がない場合は、追加の考慮事項は必要ありません。また、バックアップの復元 （63 ページ） の説明に従って設定を復元するだけです。

- 設定のバックアップが作成されてから復元された時間までの間に設定変更が行われた場合は、次の点を考慮してください。

  - バックアップを復元しても、サイトのオブジェクト、ポリシー設定は変更されません。バックアップ以降に作成および展開された新しいオブジェクトまたはポリシーは、展開されたままになります。

    Orchestrator データベースを復元した後、このガイドの「構成のbaratukiドリフト」セクションで説明されているように、テンプレートに表示される可能性のある構成のドリフトを解決してから、既存のテンプレートを再デプロイして、Nexusダッシュボー

ド間でポリシーが一致しない可能性を回避することをお勧めします。オーケストレーターと各サイトのコントローラー。We recommend that after you restore the Orchestrator database you resolve any configuration drifts that may appear in the templates, as described in "Configuration Drifts" section of this guide, and then re-deploy the existing templates to avoid potentially mismatching policies between the Nexus Dashboard Orchestrator and each site's controller.

または、すべてのポリシーを最初に展開解除することもできます。これにより、バックアップから設定が復元された後に、古いオブジェクトの潜在的な問題が回避されます。ただし、これにより、これらのポリシーによって定義されたトラフィックまたはサービスの中断が発生します。

- 設定のバックアップを復元するために必要な手順については、バックアップの復元（63 ページ） で説明しています。
- 復元した設定バックアップが、サイトに展開される前に保存されたものであった場合、未展開状態で復元されるので、必要に応じてサイトに展開できます。
- 復元した設定バックアップが、設定がすでに展開されているときに保存されたものであった場合、サイトにどの設定もまだ存在していなかったとしても、展開済み状態で復元されます。

  この場合、このガイドの「構成のばらつき」セクションで説明されているように、テンプレートに表示される可能性のある構成のばらつきを解決し、テンプレートを再展開して、Nexus Dashboard Orchestrator の構成をサイトと同期します。
- バックアップの作成時に管理されていたサイトがNexusダッシュボードに存在しない場合、復元は失敗します。
- バックアップ後にサイトのステータス（管理対象と非管理対象）を変更していて、サイトがNexusダッシュボードにまだ存在している場合、ステータスはバックアップ時の状態に復元されます。

古いローカル バックアップのダウンロードとインポート

3.4(1) より前のリリースでは、オーケストレータのローカルディスクでの設定バックアップの作成がサポートされていました。リリース 3.4(1) 以降にアップグレードする前に、ローカル バックアップをダウンロードしておくことを推奨します。ただし、ローカル バックアップはアップグレード後も引き続きダウンロードできます。

アップグレード後に古いバックアップをダウンロードすることはできますが、UI で直接バックアップを復元することはできません。このセクションでは、このようなバックアップを Orchestrator GUI からローカルマシンにダウンロードし、今度はリモートロケーションを使用して Nexus Dashboard Orchestrator GUI に再インポートする方法について説明します。

始める前に

次の設定が済んでいる必要があります。

- リリース 3.3(1) 以前からリリース 3.4(1) 以降にアップグレードされていること。新しいリリースでは、ローカルバックアップはサポートされなくなりました。
- バックアップのリモート ロケーションの設定 （60 ページ） の説明に従って、バックアップのためのリモート ロケーションが追加されていること。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左側のナビゲーション メニューで、**[操作 (Operations)]** > **[バックアップと復元 (Backups & Restore)]**を選択します。

ステップ 3 メイン ウィンドウで、ダウンロードするバックアップの隣のアクション (**...**) アイコンをクリックし、**[ダウンロード (Download)]**を選択します。

これにより、バックアップファイルがシステムにダウンロードされます。

ステップ 4 Nexus Dashboard Orchestrator GUIでダウンロードしたバックアップを削除します。

以前のバージョンから既存のローカルバックアップを削除せずにバックアップを再インポートしようとすると、同じ名前のバックアップファイルがすでに存在するため、アップロードが失敗します。

ダウンロードしたバックアップを削除するには、バックアップの横にあるアクション（**...**）メニューをクリックし、**[削除 (Delete)]** を選択します。

ステップ 5 バックアップをリモートの場所にインポートします。

バックアップをリモート ロケーションへインポートする （61 ページ）に記載されているように、リモート ロケーションを使用してダウンロードしたバックアップ ファイルを Nexus Dashboard Orchestrator に再アップロードします。

バックアップのリモート ロケーションの設定

このセクションでは、設定バックアップをエクスポートできる Nexus Dashboard Orchestrator のリモート ロケーションの設定方法を説明します。

ステップ 1 Nexus Dashboard にログインし、Nexus Dashboard Orchestrator サービスを開きます。

ステップ 2 左側のナビゲーション ペインで、**[操作 (Operations)]** > **[リモート ロケーション (Remote Loacation)]**を選択します。

ステップ 3 メイン ウィンドウの右上隅で、[**リモート ロケーションの追加 (Add Remote Location)**] をクリックします。

[**新規リモート ロケーションの追加 (Add New Remote Location)**] 画面が表示されます。

ステップ 4 リモート ロケーションの名前と説明 (任意) を入力します。

現在、2 つのプロトコルが設定バックアップのリモート エクスポートに対してサポートされています。

- SCP

- SFTP

（注） SCPはWindows以外のサーバーでのみサポートされます。リモートロケーションがWindowsサーバーの場合は、SFTPプロトコルを使用する必要があります。

ステップ 5 リモート サーバのホスト名または IP アドレスを指定します。

[**プロトコル (Protocol)**] セクションに基づいて、指定するサーバーでは SCP または SFTP 接続を許可する必要があります。

ステップ 6 バックアップを保証するリモート サーバーのディレクトリにフル パスを指定します。

パスの先頭にはスラッシュ (/) 文字を使用し、ピリオド (.) とバックスラッシュ (\) を含むことはできません。例: */backups/multisite*

（注） ディレクトリは、リモート サーバにすでに存在しなければなりません。

ステップ 7 リモート サーバに接続するために使用するポートを指定します。

デフォルトで、ポートは 22 に設定されます。

ステップ 8 リモート サーバに接続するときに使用される認証タイプを指定します。

次の 2 つの認証方式のうちの 1 つを使用して設定できます。

- パスワード—リモート サーバにログインするために使用されるユーザ名とパスワードを指定します。
- SSH プライベート ファイル—ユーザ名とリモート サーバにログインするために使用される SSH キー/パスフレーズのペアを指定します。

ステップ 9 [**保存 (Save)**] を使用して、リモート サーバを追加します。

バックアップをリモートロケーションへインポートする

ここでは、以前にダウンロードした既存の設定バックアップをアップロードし、Nexus Dashboard Orchestratorで設定されたリモートロケーションのいずれかにインポートする方法について説明します

始める前に

次の設定が済んでいる必要があります。

- バックアップの作成 （62 ページ） および バックアップのエクスポート（ダウンロード）（68 ページ） の説明に従って、設定のバックアップを作成されていること。

  リリース3.4(1)以降で作成したバックアップなど、バックアップがすでにリモートロケーションにある場合は、ローカル マシンにダウンロードして、別のリモート ロケーションにアップロードできます。

- バックアップのリモート ロケーションの設定 （60 ページ） の説明に従って、バックアップのためのリモート ロケーションが追加されていること。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左側のナビゲーション ペインで、**[操作 (Operations)]** > **[バックアップと復元 (Backups & Restore)]**を選択します。

ステップ 3 メインペインで、**[アップロード (Upload)]** をクリックします。

ステップ 4 開いた **[ファイルからのアップロード (Upload from file)]** ウィンドウで、**[ファイルを選択 (Select File)]** を選択して、インポートするバックアップ ファイルを選択します。

バックアップをアップロードすると、**[バックアップ (Backups)]** ページに表示されるバックアップのリストに追加されます。

ステップ 5 **[リモート ロケーション (Remote location)]** ドロップダウンメニューから、リモート ロケーションを選択します。

ステップ 6 (オプション) リモート ロケーションのパスを更新します。

リモート バックアップのロケーションを作成するときに設定したリモート サーバ上のターゲット ディレクトリが、**[リモート パス (Remote Path)]** フィールドに表示されます。

パスにはサブディレクトリを追加することができます。ただし、ディレクトリはデフォルトの設定済みパスの下にある必要があり、すでにリモート サーバで作成されている必要があります。

ステップ 7 **[アップロード (Upload)]** をクリックしてファイルをインポートします。

バックアップのインポートは、[**バックアップ (Backups)**]ページに表示されたバックアップのリストにそれを追加します。

バックアップは NDO UI に表示されますが、リモート サーバーにのみ存在することに注意してください。

バックアップの作成

ここでは、Nexus Dashboard Orchestrator 設定の新しいバックアップを作成する方法について説明します。

始める前に

バックアップのリモート ロケーションの設定 （60 ページ） の説明に従って、最初にリモート ロケーションを追加する必要があります。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 既存の展開設定をバックアップします。

a) 左側のナビゲーション ペインで、**[操作 (Operations)]** > **[バックアップと復元 (Backups & Restore)]**を選択します。
b) メイン ウィンドウ ペインで、**[新規バックアップ (New Backup)]** をクリックします。

[新規バックアップ (New Backup)] ウィンドウが開きます。

c) バックアップ情報を提供します。

- **[名前 (Name)]** フィールドに、バックアップ ファイルの名前を入力します。

  名前には、最大 10 文字の英数字を使用できますが、スペースまたはアンダースコア (_) は使用できません。

- **[リモート ロケーション (Remote location)]** ドロップダウンから、バックアップを保存するために構成したリモート ロケーションを選択します。
- （オプション）**[リモート パス（Remote Path）]** では、バックアップを保存する先のリモート サーバーの特定のディレクトリを提供します。

  指定したディレクトリはすでに存在しているはずです。

d) **[保存（Save）]** をクリックして、バックアップを作成します。

バックアップの復元

このセクションでは、Orchestrator 設定を前の状態に復元する方法について説明します。

始める前に

- バックアップのリモート ロケーションの設定 （60 ページ） で説明されているように、NDO バックアップを保存するためのリモート ロケーションを構成しておく必要があります。
- バックアップをリモート ロケーションへインポートする （61 ページ） の説明に従って、復元するバックアップがリモート ロケーション サーバーにあることを確認するか、バックアップをリモート ロケーションにインポートします。

（注） バックアップ アクションの復元では、Nexus Dashboard Orchestrator のデータベースを復元しますが、各サイトのコントローラ（APIC、クラウド ネットワーク、NDFC など）データベースは変更されません。

Orchestrator データベースを復元した後、このガイドの「構成のばらつき」セクションで説明されているように、テンプレートに表示される可能性のある構成のばらつきを解決してから、既存のテンプレートを再展開して、Nexus Dashboard と各サイトのコントローラの間でポリシーが一致しない可能性を回避することをお勧めします。

特定の構成の不一致とそれぞれに関連する望ましい復元手順の詳細は、構成のバックアップと復元に関するガイドライン （57 ページ）を参照してください。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 必要に応じて、既存のポリシーの展開を解除します。

バックアップが作成されたときから現在の設定までに、設定に新しいオブジェクトまたはポリシーが追加されている場合は、この手順を実行することをお勧めします。追加情報については、構成のバックアップと復元に関するガイドライン （57 ページ） を参照してください。

ステップ 3 左側のナビゲーション メニューで、**[操作 (Operations)]** > **[バックアップと復元 (Backups & Restore)]**を選択します。

ステップ 4 メイン ウィンドウで、復元するバックアップの隣のアクション (**...**) アイコンをクリックし、**[このバックアップにロールバック (Rollback to this backup)]** を選択します。

選択したバックアップのバージョンが、実行中の Nexus Dashboard Orchestrator のバージョンと異なる場合、ロールバックが原因で、バックアップされたバージョンには存在しない機能が削除される可能性があります。

ステップ 5 **[はい (Yes)]** をクリックして、選択したバックアップを復元することを確認します。

[はい (Yes)] をクリックすると、システムは現在のセッションを終了して、ユーザはログアウトされます。

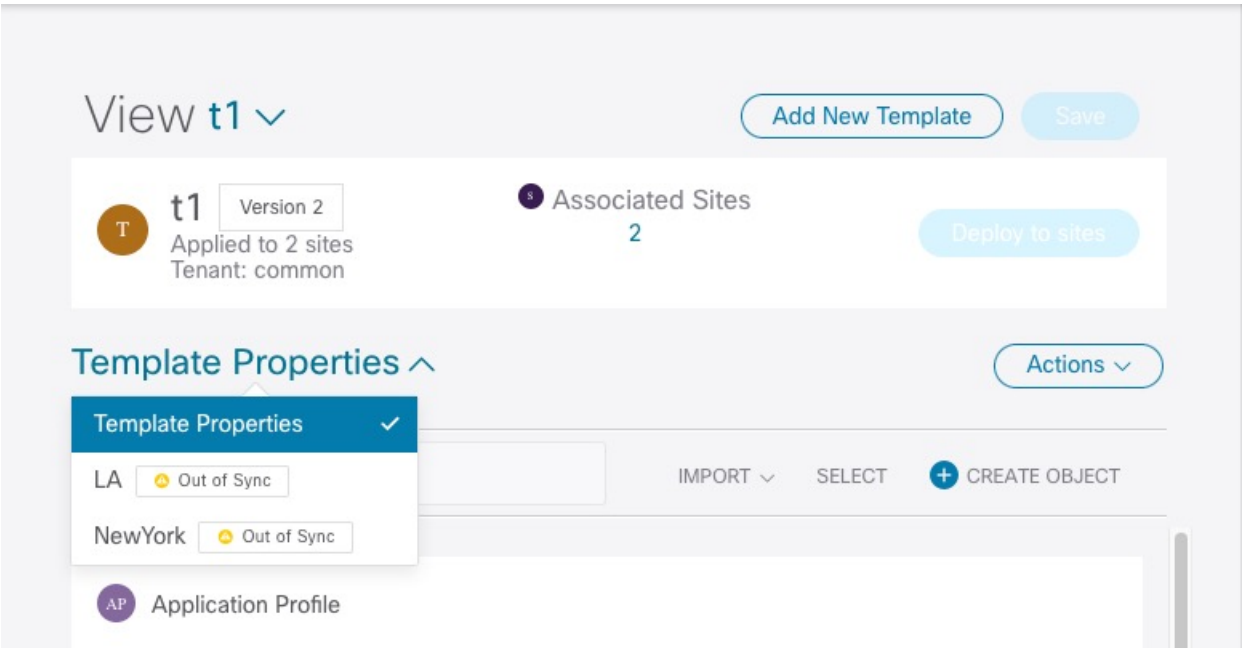
（注） 設定の復元プロセス中に複数のサービスが再起動されます。その結果、復元された設定が NDO GUI に正しく反映されるまでに最大 10 分の遅延が発生することがあります。

ステップ 6 テンプレートに構成のばらつきがあるかどうかを確認してください。

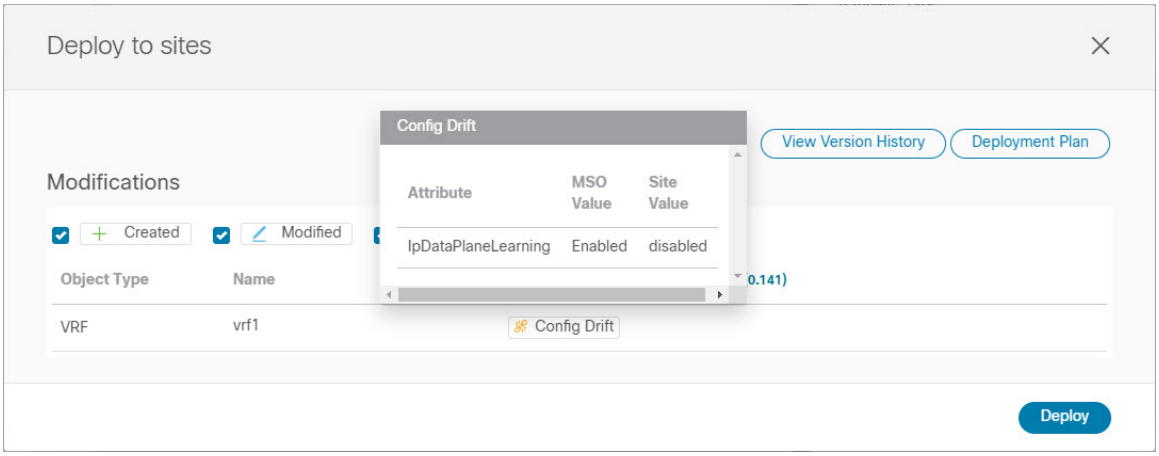
展開のスキーマとテンプレートごとに次の手順を繰り返します

次の 2 つの方法のいずれかで、構成のばらつきをチェックできます。

- テンプレートが割り当てられている各サイトのテンプレート展開ステータス アイコンを確認します。



- テンプレートを選択して **[サイトへの展開 (Deploy to sites)]** をクリックして、構成のばらつきが含まれているオブジェクトをチェックするために、構成比較画面を呼び出します。



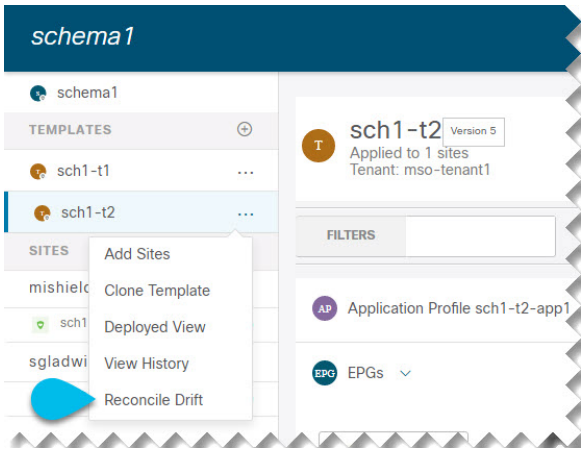
ステップ 7 テンプレートのどれかに構成のばらつきが含まれている場合は、競合を解決します。

構成のばらつきの詳細については、『*Cisco Nexus Dashboard Orchestrator Configuration Guide for ACI Fabrics*』の「構成のばらつき」の詳細を確認してください。

a) テンプレート展開ダイアログを閉じて、スキーマ表示に戻ります。

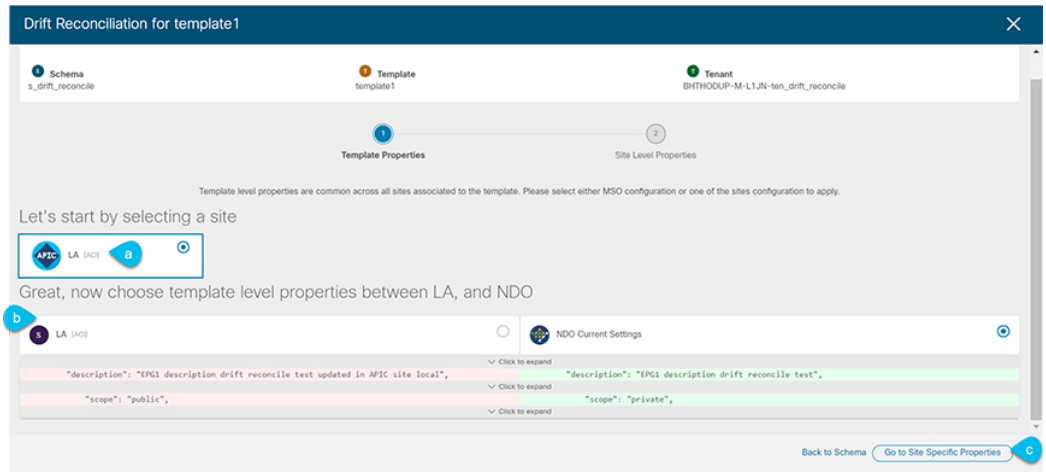
この時点でテンプレートを展開すると、Orchestrator データベースの値をプッシュして、ファブリックの既存の設定を上書きします。

b) テンプレートの **[アクション (Actions)]** メニューから、**[ばらつきの調整 (Reconcile Drift)]** を選択します。



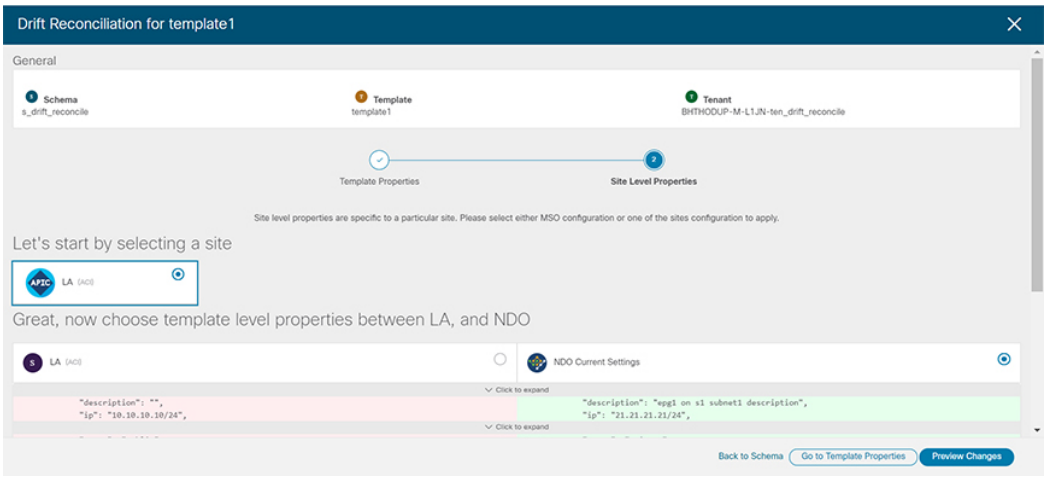
[ばらつきの調整 (Reconcile Drift)] ウィザードが開きます。

c) **[ばらつきの調整 (Reconcile Drift)]** 画面で、各サイトのテンプレートレベルの構成を比較し、希望のものを選択します。



テンプレートレベルのプロパティは、テンプレートに関連付けられているすべてのサイトに共通です。Nexus Dashboard Orchestrator で定義されたテンプレート レベルのプロパティを各サイトでレンダリングされた構成と比較し、Nexus Dashboard Orchestrator テンプレートの新しい構成を決定できます。サイト構成の選択は、既存の Nexus Dashboard Orchestrator テンプレートのこれらのプロパティを変更し、その場合、Nexus Dashboard Orchestrator の構成を選択すると、既存の Nexus Dashboard Orchestrator テンプレートの設定はそのまま残されます

d) **[サイト特有のプロパティに移動（Go to Site Specific Properties）]** をクリックして、サイトレベルの構成に切り替えます。



特定のサイトの構成を比較するために、サイトを選択できます。テンプレートレベルの設定とは異なり、各サイトの Nexus Dashboard Orchestrator 定義または実際の既存の設定を個別に選択して、そのサイトのテンプレートのサイトローカル プロパティとして保持できます。

ほとんどのシナリオでは、テンプレートレベルとサイトレベルの両方の構成で同じ選択を行いたとしても、ばらつきの調整ウィザードでは、サイトのコントローラで「テンプレートのプロパティ」レベルで定義された構成と Nexus Dashboard Orchestratorで定義された構成またはその逆を選択できます。

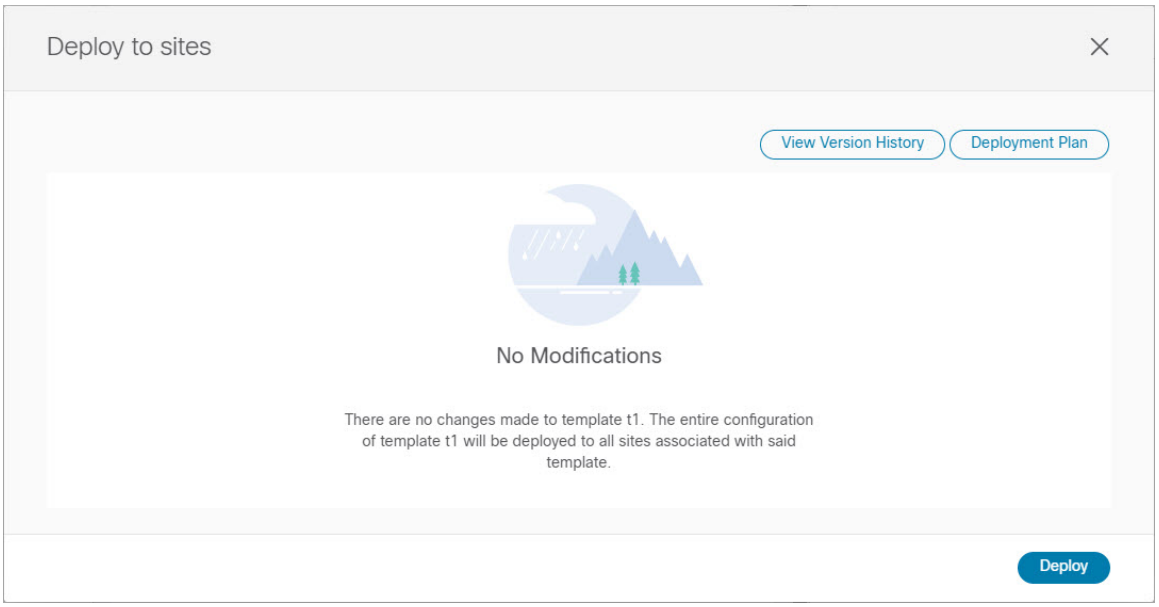
e) **[変更のプレビュー（Preview Changes）]** をクリックして、選択内容を確認します。

プレビューは **[ばらつきの調整 (Reconcile Drift)]** ウィザードの選択肢に基づいて調整された完全なテンプレート構成を表示します。その後、**[サイトに展開（Deploy to site）]** をクリックして構成を展開し、そのテンプレートのばらつきを調整できます。

ステップ 8 すべての構成のばらつきを解決した後で、**[サイトへの展開（Deploy to sites）]** ダイアログに変更が表示されていない場合、テンプレートの完全な再展開を実行します。

（注） リリース 3.7(1) のデータベース変換のため、各テンプレートの完全な再展開を実行する必要があります。

[サイトへの展開（Deploy to sites）] ダイアログに、次の図で表示される変更が含まれない場合、**[展開（Deploy）]** をクリックして、完全な構成を再展開します。



ステップ 9 Nexus Dashboard Orchestrator で各スキーマとテンプレートに対して上記の手順を繰り返します。

ステップ 10 監査ログをチェックして、すべてのテンプレートが再展開されていることを確認します。

[オペレーション（Operations）]タブの監査ログを表示できます。

[監査ログ（Audit Logs）]ページで、すべてのテンプレートが `[再展開済み（Redeployed）]` と表示され、完全な再展開が正常に完了したことを確認します。

バックアップのエクスポート（ダウンロード）

ここでは、Nexus Dashboard Orchestrator からバックアップをダウンロードする方法について説明します。

始める前に

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左側のナビゲーション メニューで、**[操作 (Operations)]** > **[バックアップと復元 (Backups & Restore)]**を選択します。

ステップ 3 メイン ウィンドウで、ダウンロードするバックアップの隣のアクション **(...)** アイコンをクリックし、**[ダウンロード (Download)]**を選択します。

これにより `msc-backups-<タイムスタンプ>.tar.gz` 形式でシステムにバックアップ ファイルがをダウンロードされます。その後、ファイルを抽出してその内容を表示することができます。

バックアップ スケジューラ

ここでは、定期的に完全な設定バックアップを実行するバックアップスケジューラを有効または無効にする方法について説明します。

始める前に

バックアップのリモート ロケーションの設定 （60 ページ） の説明に従って、バックアップのためのリモート ロケーションを追加してある必要があります。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左側のナビゲーション メニューで、**[操作 (Operations)]** > **[バックアップと復元 (Backups & Restore)]**を選択します。

ステップ 3 メイン ペインの右上にある **[スケジューラ (Scheduler)]** をクリックします。

[バックアップ スケジューラ設定 (Backup Scheduler Settings)] ウィンドウが開きます。

ステップ 4 バックアップ スケジューラをセットアップします。

a) **[スケジューラの有効化 (Enable Scheduler)]** チェックボックスをオンにします。

b) **[開始日の選択 (Select Start Date)]** フィールドに、スケジューラを開始する日を指定します。

c) **[時間の選択 (Select Time)]** フィールドに、スケジューラを開始する時刻を入力します。

d) **[頻度の選択 (Select Frequency)]** ドロップダウンから、バックアップを実行する頻度を選択します。

e) **[リモート ロケーション (Remote Location)]** ドロップダウンから、バックアップを保存する場所を選択します。

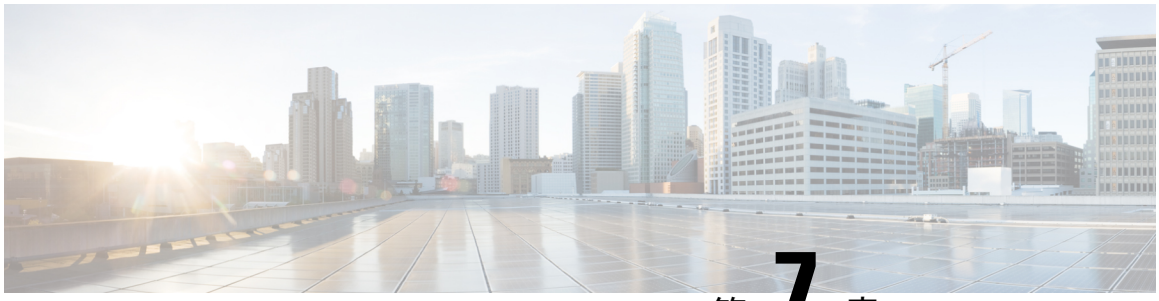
f) （オプション）**[リモート パス (Remote Path)]** フィールドで、バックアップが保存されるリモート ロケーションのパスを更新します。

リモートバックアップのロケーションを作成するときに設定したリモートサーバ上のターゲットディレクトリが、**[リモート パス (Remote Path)]** フィールドに表示されます。

パスにはサブディレクトリを追加することができます。ただし、ディレクトリはデフォルトの設定済みパスの下にある必要があり、すでにリモート サーバで作成されている必要があります。

g) [OK] をクリックして終了します。

ステップ 5 バックアップ スケジューラを無効にする場合は、上記の手順で**[スケジューラの有効化 (Enable Scheduler)]** チェックボックスをオフにします。



第 7 章

[Tech Support]

テクニカル サポートおよびシステム ログ

Nexus Dashboard Orchestrator のシステム ロギングは、最初に Orchestrator クラスタをデプロイしたときに自動的に有効になり、環境内で発生したイベントと障害をキャプチャします。

追加のツールを使用して重要なイベントを遅延なく迅速に解析、表示、応答する必要がある場合は、いつでも、ログをダウンロードするか、Splunk などの外部ログ アナライザにストリーミングするかを選択できます。

リリース 3.3(1) 以降、テクニカル サポートログは 2 つの部分に分割されています。

- 以前のリリースと同じ情報を含む、オリジナルのデータベース バックアップ ファイル
- 可読性を高めた、JSON ベースのデータベース バックアップ

各バックアップ アーカイブには、次の内容が含まれています。

- *xxxx*：バックアップ時に使用可能なコンテナ ログ用の *xxxx* 形式の 1 つ以上のファイル。
- `msc-backup-<date>_temp`：以前のリリースと同じ情報を含む、オリジナルのデータベース バックアップ。
- `msc-db-json-<date>_temp`：JSON 形式のバックアップコンテンツ。

  例：

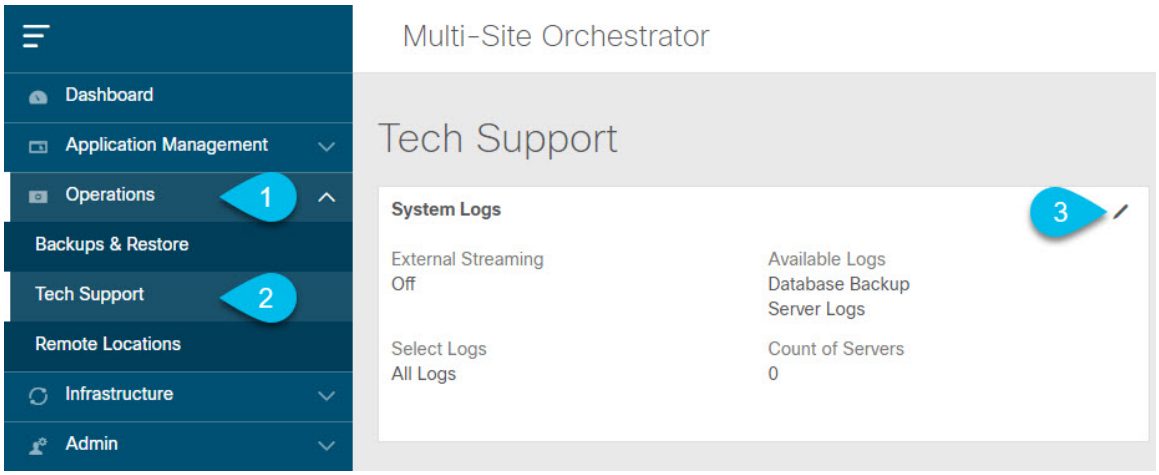
```
msc_anpEpgRels.json
msc_anpExtEpgRels.json
msc_asyncExecutionStatus.json
msc_audit.json
msc_backup-versions.json
msc_backupRecords.json
msc_ca-cert.json
msc_cloudSecStatus.json
msc_consistency.json
...
```

システム ログのダウンロード

このセクションでは、Nexus Dashboard Orchestrator により管理されているすべてのスキーマ、サイト、テナント、およびユーザのトラブルシューティング レポートとインフラストラクチャ ログ ファイルを生成します。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 **[システムログ (System Logs)]** 画面を開きます。



a) メインメニューで、**[操作 (Operations)]** > **[テクニカル サポート (Tech Support)]**を選択します。

b) **[システム ログ (System Logs)]** フレームの右上隅にある編集ボタンをクリックします。

ステップ 3 **[ログのダウンロード (Download Log)]** ボタンをクリックしてログをダウンロードします。

アーカイブがシステムにダウンロードされます。この章の最初のセクションで説明されているすべての情報を含んでいます。

外部アナライザへのストリーミング システム ログ

Nexus Dashboard Orchestrator を使用すると、Orchestrator ログを外部のログアナライザー ツールにリアルタイムで送信できます。生成されたイベントをストリーミングすることにより、追加のツールを使用して、遅延なしで重要なイベントをすばやく解析、表示、および対応できます。

ここでは、Nexus Dashboard Orchestrator が外部アナライザツール (Splunk や syslog など) にログをストリーミングできるようにする方法について説明します。

始める前に

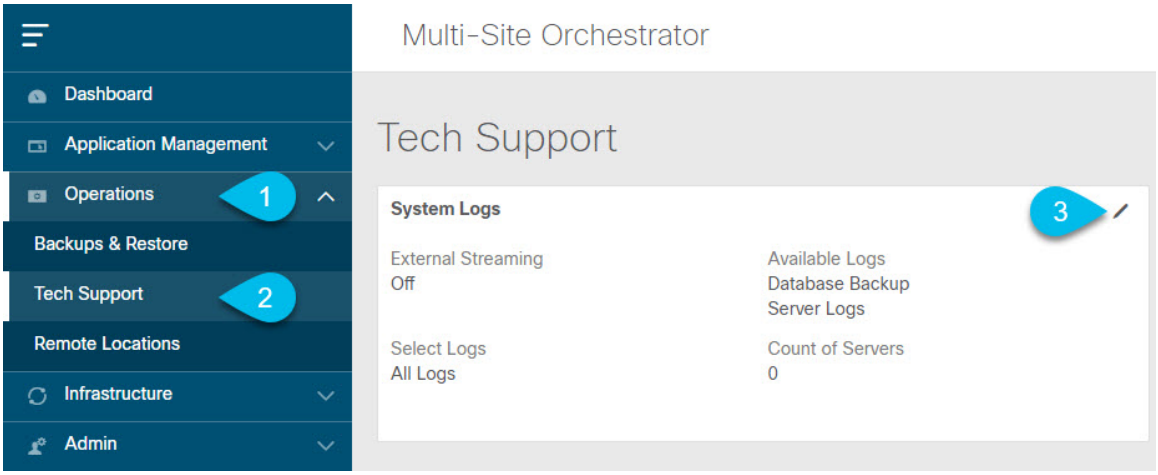
- このリリースでは、外部ログ アナライザーとして Splunk と `syslog` のみがサポートされています。
- このリリースでは、Application Services Engine 展開で Nexus Dashboard Orchestrator の `syslog` のみがサポートされます。
- このリリースは、最大 5 台の外部サーバをサポートします。
- Splunk を使用する場合は、ログ アナライザー サービス プロバイダをセットアップして構成します。

  外部ログ アナライザーの設定方法の詳細については、マニュアルを参照してください。
- Splunk を使用する場合は、サービス プロバイダの認証トークンを取得します。

  分裂サービスの認証トークンの取得については、「分裂」のマニュアルで詳しく説明していますが、要するに、**[設定 (Settings)]** > **[データ入力 (Data Inputs)]** > **[HTTP イベントコレクタ (Data input HTTP Event Collector)]**を選択し、[**新規トークン (New token**)] をクリックして、認証トークンを取得できます。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 **[システムログ (System Logs)]** 画面を開きます。



a) メインメニューで、**[操作 (Operations)]** > **[テクニカル サポート (Tech Support)]**を選択します。

b) **[システム ログ (System Logs)]** フレームの右上隅にある編集ボタンをクリックします。

ステップ 3 **[システムログ (System Logs)]** ウィンドウで、外部ストリーミングを有効にし、サーバを追加します。

a) **[外部ストリーミング (External Streaming)]** ノブを有効にします。
b) **[すべてのログ (All Logs)]** をストリーミングするか、**[監査ログ (Audit Logs)]** のみをストリーミングするかを選択します。
c) **[サーバーの追加 (Add Server)]** をクリックして、外部ログ アナライザ サーバーを追加します。

ステップ 4 Splunk サーバーを追加します。

Splunk サービスを使用する予定がない場合は、この手順をスキップします。

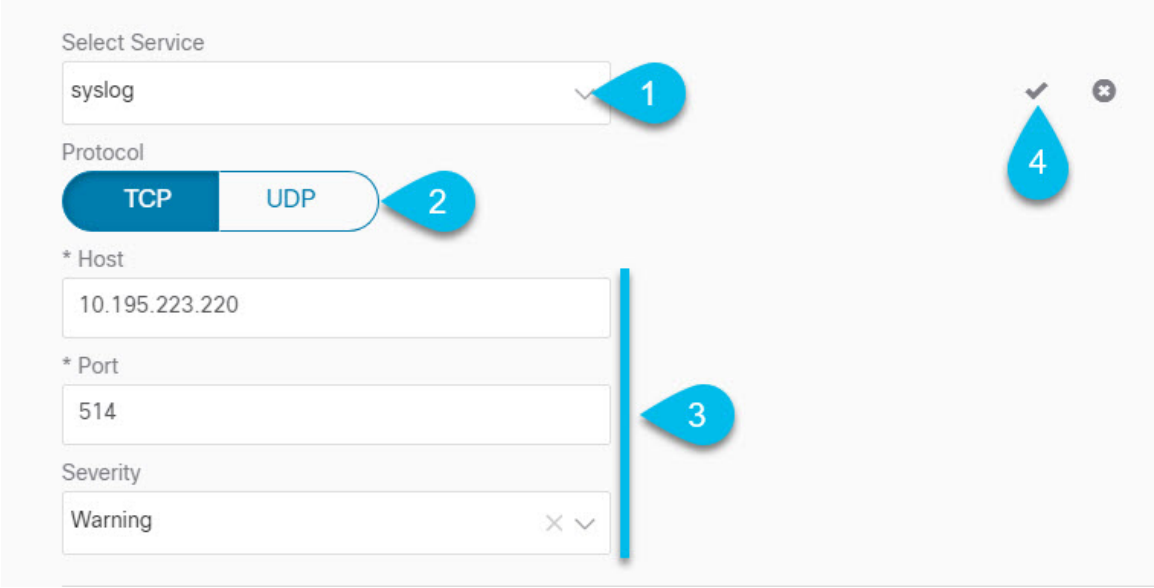
a) サーバーのタイプとして `[Splunk]` を選択します。
b) プロトコルを選択します。
c) Splunk サービスから取得したサーバ名または IP アドレス、ポート、および認証トークンを入力します。

Splunk サービスの認証トークンの取得については、Splunk のマニュアルで詳しく説明していますが、要するに、**[設定 (Settings)]** > **[データ入力 (Data Inputs)]** > **[HTTP イベントコレクタ (HTTP Event Collector)]** を選択し、**[新規トークン (New token)]** をクリックして、認証トークンを取得できます。

d) チェックマーク アイコンをクリックして、サーバーの追加を終了します。

ステップ 5 `syslog` サーバーを追加します。

`syslog` を使用しない場合は、この手順をスキップします。



a) サーバーのタイプとして `[syslog]` を選択します。

b) プロトコルを選択します。

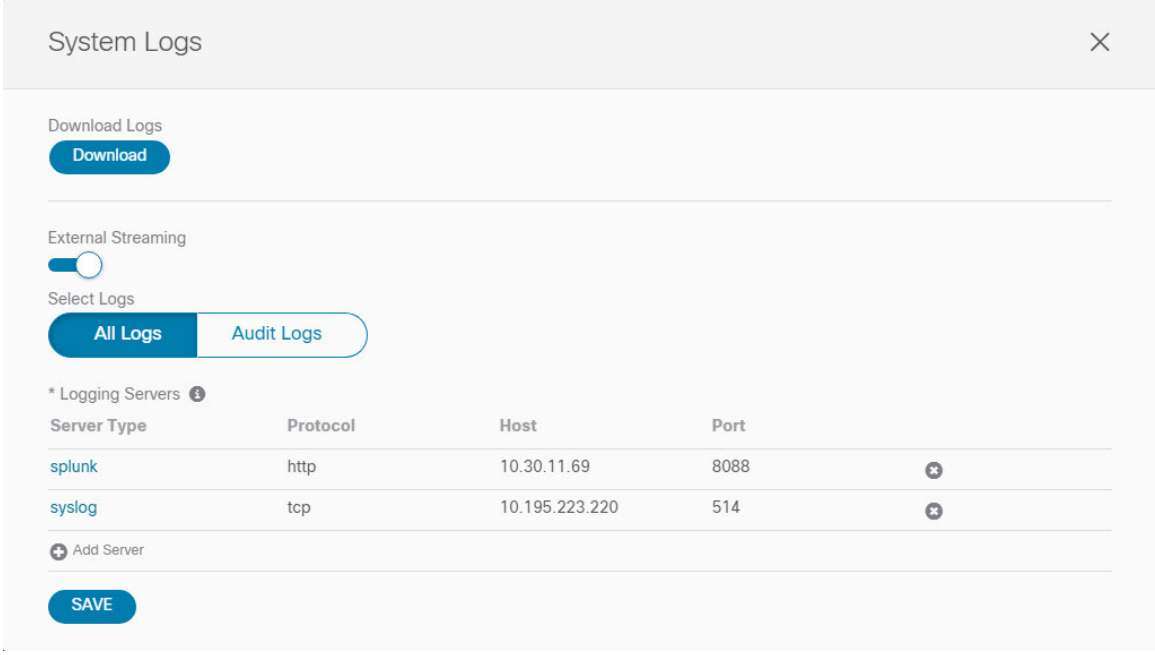
c) サーバー名またはIPアドレス、ポート番号、およびストリーミングするログ メッセージの重大度を指定します。

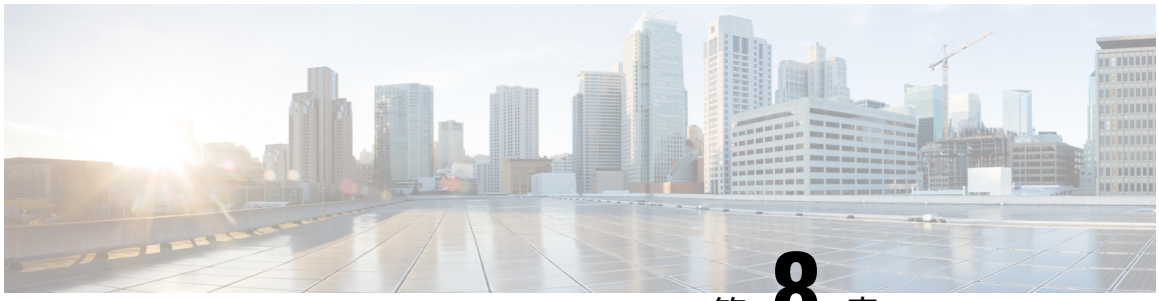
d) チェックマーク アイコンをクリックして、サーバーの追加を終了します。

ステップ 6 複数のサーバーを追加する場合は、この手順を繰り返します。

このリリースは、最大 5 台の外部サーバ0をサポートします。

ステップ 7 [保存（Save）] をクリックして、変更内容を保存します。


System Logs
Download Logs
Download
External Streaming
Select Logs
All Logs
Audit Logs
* Logging Servers
Server Type
Protocol
Host
Port
splunk
http
10.30.11.69
8088
syslog
tcp
10.195.223.220
514
Add Server
SAVE



第 8 章

システム設定

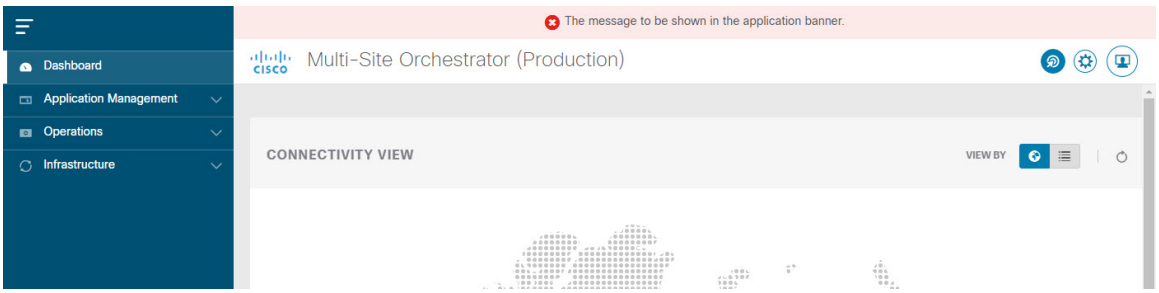
システム設定

次のセクションで説明するように、Multi-Site Orchestrator に対して設定できる、 **管理** > **システム設定**で使用可能なグローバルシステム設定が多数あります。

システム エイリアスとバナー

このセクションでは、Nexus Dashboard Orchestrator のエイリアスを設定する方法と、次の図に示すように、GUI 全体で画面の上部に表示されるカスタムのバナーを有効にする方法について説明します。

図 *4:* システム バナーの表示



ステップ 1 Orchestrator にログインします。

ステップ 2 左側のナビゲーション ペインから**[管理 (Admin)]** > **[システム設定 (System Configuration)]** を選択します。.

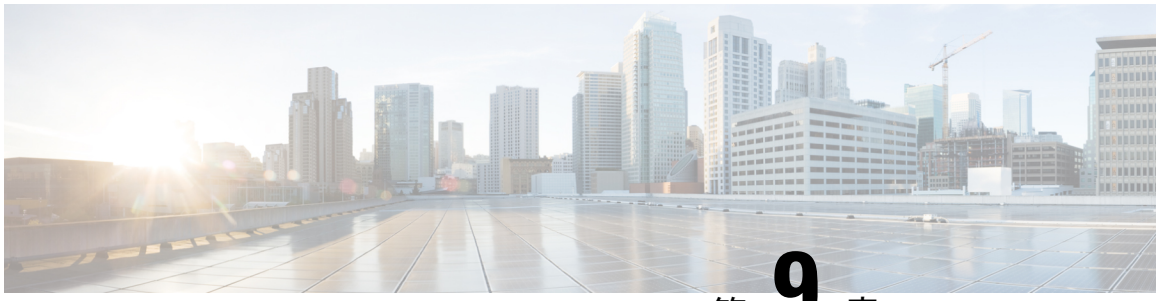
ステップ 3 **[編集 (Edit)]** のアイコンをクリックします。これは**[システム エイリアスとバナー System Alias & Banners)]** 領域の右にあります。

[システム エイリアスとバナー System & Banners)] の設定ウィンドウが表示されます。

ステップ 4 **[エイリアス (Alias)]** フィールドで、システムのエイリアスを指定します。
ステップ 5 GUI バナーを有効にするかどうかを選択します。
ステップ 6 バナーを有効にする場合には、バナーに表示されるメッセージを指定する必要があります。
ステップ 7 バナーを有効にする場合には、バナーの重大度を意味する色を選択する必要があります。
ステップ 8 [保存（Save）] をクリックして、変更内容を保存します。

第 II 部

機能と使用例



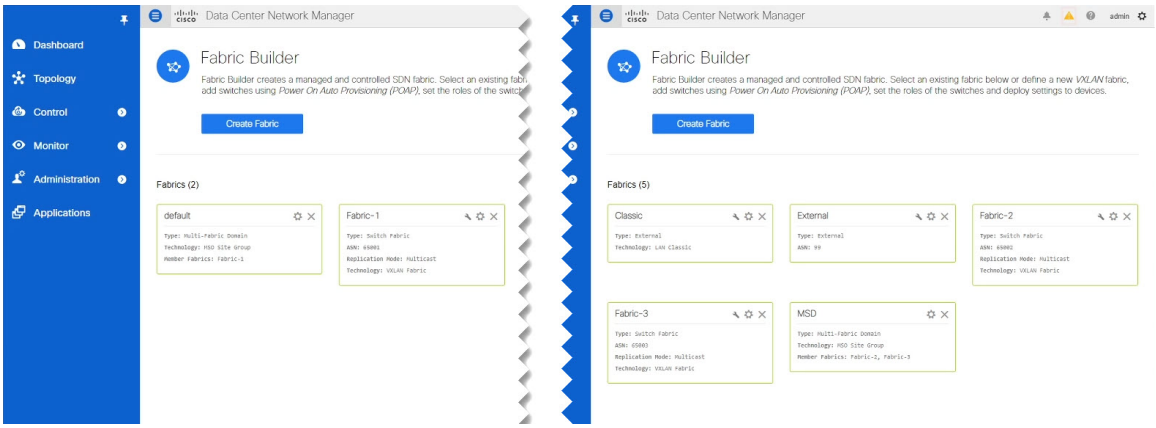
第 9 章

VRFおよびネットワークのブラウンフィールドインポート

概要

次の項では、ブラウンフィールドインポート使用例のシナリオについて説明します。これにより、マルチサイト ドメイン（MSD）の一部であるファブリックを含む、既存の NDFC ファブリック設定をインポートできます。また、これらの設定を、Nexus Dashboard Orchestrator を使用して、単一の場所から、複数のグリーンフィールドまたはブラウンフィールドファブリックにわたって拡張できます。同じ使用例が、*Cisco NDFC VRF および Nexus Dashboard Orchestrator* を使用したネットワーク設定のビデオデモで示されています。

この章の例では 2 つの異なる NDFC コントローラを使用します。最初の NDFC の `Fabric-1` は単一のファブリックです。`Fabric-2` と `Fabric-3` は MSD の一部であり、2 番目の NDFC によって管理されます。



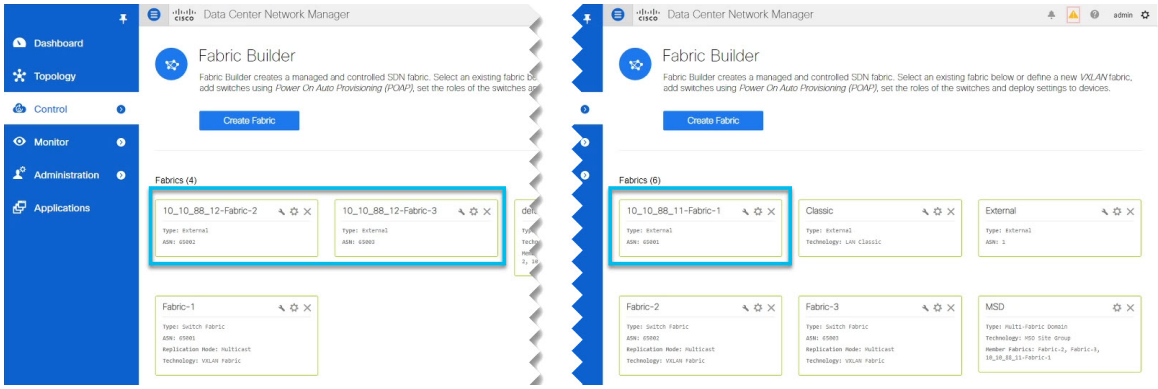
次の項では、既存の設定をインポートし、別のNDFCで管理されるファブリック間で拡張する方法と、新しいVRFおよびネットワークを展開する方法について説明します。

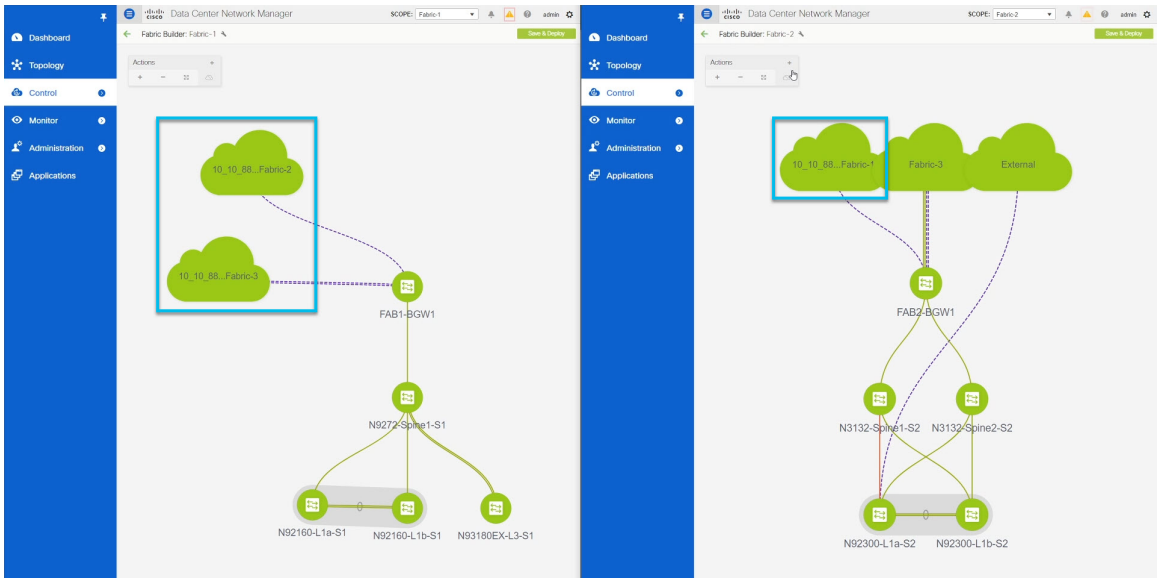
前提条件

環境内の既存のNDFCファブリックからVRFとネットワークをインポートして管理する前に、次のものが必要です。

- *Cisco Nexus Dashboard Deployment Guide*および*Cisco Nexus Dashboard Orchestrator Deployment Guide*の説明に従って展開され、インストールされたNexus DashboardクラスタとNexus Dashboard Orchestratorサービス。
- Nexus Dashboardにオンボードされ、Nexus Dashboard Orchestrator GUIで管理できる既存のNDFCファブリック（サイトの追加と削除 （3 ページ）を参照）。
- Cisco NDFC サイトのインフラの構成 （9 ページ）の説明に従って、サイト間インフラストラクチャを設定して展開します。

  上記の「概要」セクションに示されている例のファブリックを展開すると、すべてのファブリックのインフラ設定を構成した後、各DCNMに展開されたサイト間接続が表示されます。





構成のインポートのためのスキーマとテンプレートの作成

このセクションでは、スキーマとテンプレートを作成する方法について説明します。その後、既存の設定をそれらにインポートし、新しい設定を作成します。

始める前に

- 前提条件 （82 ページ）で説明されている前提条件を確認し、完了している必要があります。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 スキーマを新規作成します。

a) 左側のナビゲーション メニューで、**[アプリケーション管理 (Application Management)]** > **[スキーマ (Schemas)]** を選択します。

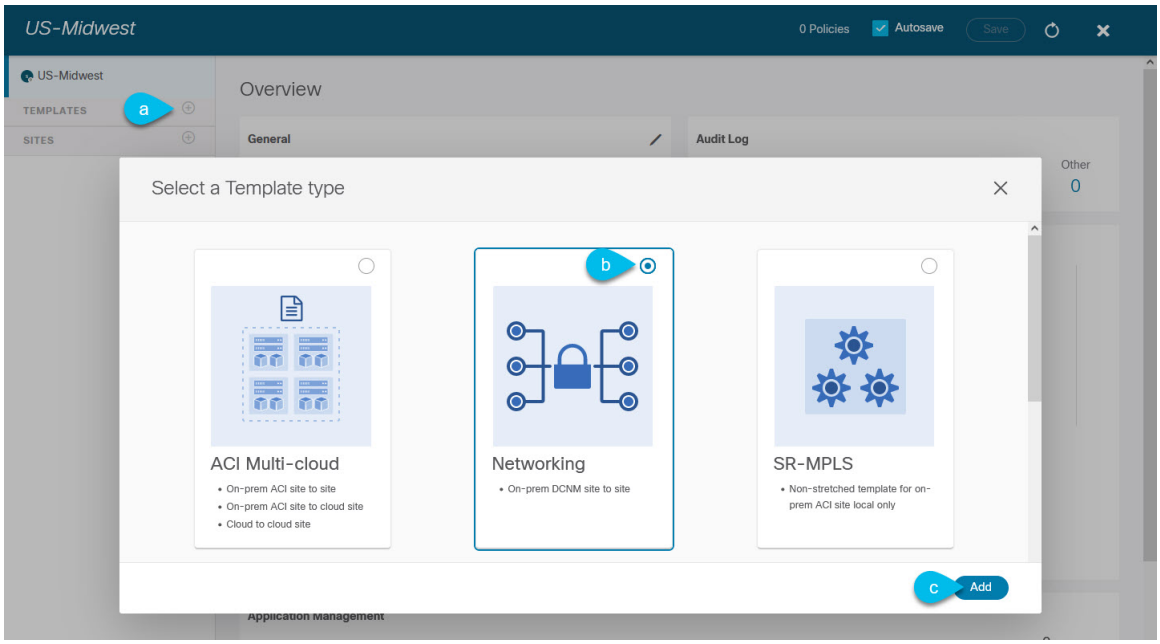
b) [スキーマ (Schema)] ページで、**[スキーマの追加 (Add Schema)]** をクリックします。

c) スキーマ作成ダイアログで、スキーマの **[名前 (Name)]** と説明（オプション）を入力します。

デフォルトでは、新しいスキーマは空であるため、1 つ以上のテンプレートを追加する必要があります。

ステップ 3 テンプレートを作成します。

VRF 用に 1 つとネットワーク用に 1 つの 2 つの個別のテンプレートを作成することをお勧めします。次の 2 つの手順では、テンプレートを作成する方法について説明します。

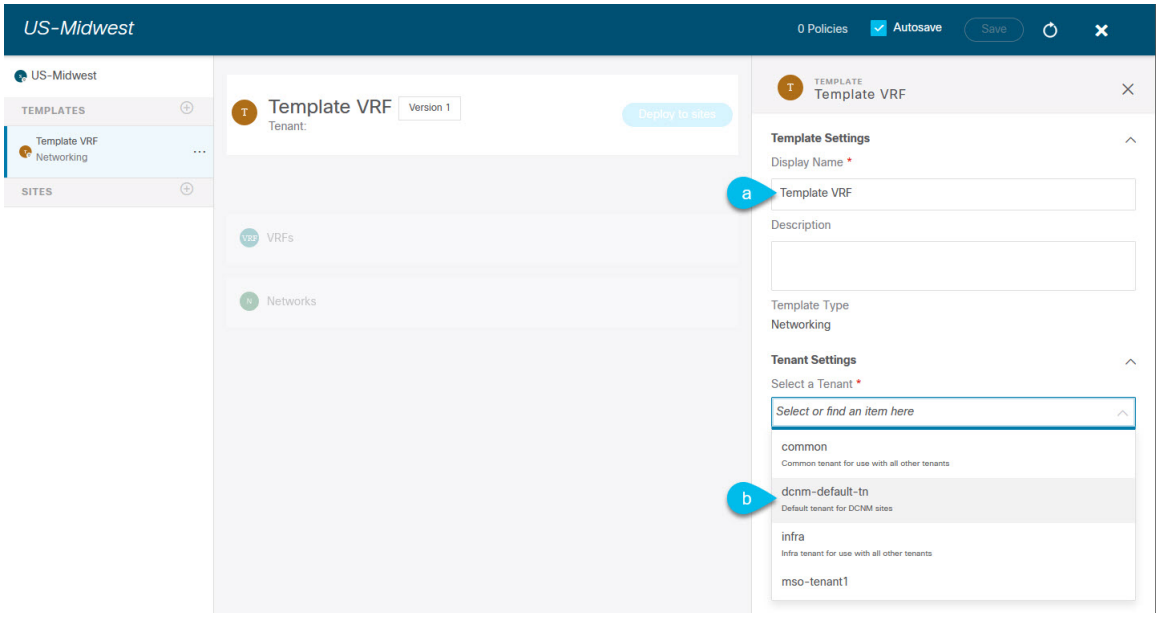


a) 左側のサイドバーの **[テンプレート (Templates)]** で、**[+]** 記号をクリックして新しいテンプレートを追加します。

b) **[テンプレート タイプの選択 (Select a Template type)]** ウィンドウで、テンプレート タイプとして **[ネットワーキング (Networking)]** を選択します。

c) **[追加 (Add)]** をクリックしてテンプレートを追加します。

ステップ 4 テンプレートの名前とテナントを指定します。



a) 右側のサイドバーで、テンプレートの **[表示名 (Display Name)]** を指定します。

b) **[テナントの選択 (Select a Tenant)]** ドロップダウンから、`dcnm-default-tn` テナントを選択します。

このテナントは、NDFC サイトのオブジェクトと設定を定義するために、デフォルトで NDO で作成されます。

ステップ 5 以前の 2 つの手順を繰り返して、2 つ目のテンプレートを作成します。

このリリースでは、各スキーマ内でVRF とネットワーク用に個別のテンプレートを作成してから、最初に VRF テンプレートを展開し、次にネットワークを含むテンプレートを展開することをお勧めします。このようにして、ネットワーク構成をサイトにプッシュするときに、ネットワークに必要なVRF がすでに作成されています。

同様に、複数のネットワークと VRF を展開解除する場合は、最初にネットワーク テンプレートを展開解除してから、VRF テンプレートを展開解除することをお勧めします。これにより、VRF が展開解除されたときに、VRF をまだ使用している既存のネットワークとの競合が発生しなくなります。

ステップ 6 スキーマビューの右上隅で、**[保存 (Save)]** をクリックしてスキーマとテンプレートを保存します。

設定をインポートする前に、作成したスキーマとテンプレートを保存する必要があります

NDFC サイトからのスキーマ要素のインポート

ここでは、既存のファブリックから設定をインポートする方法について説明します。

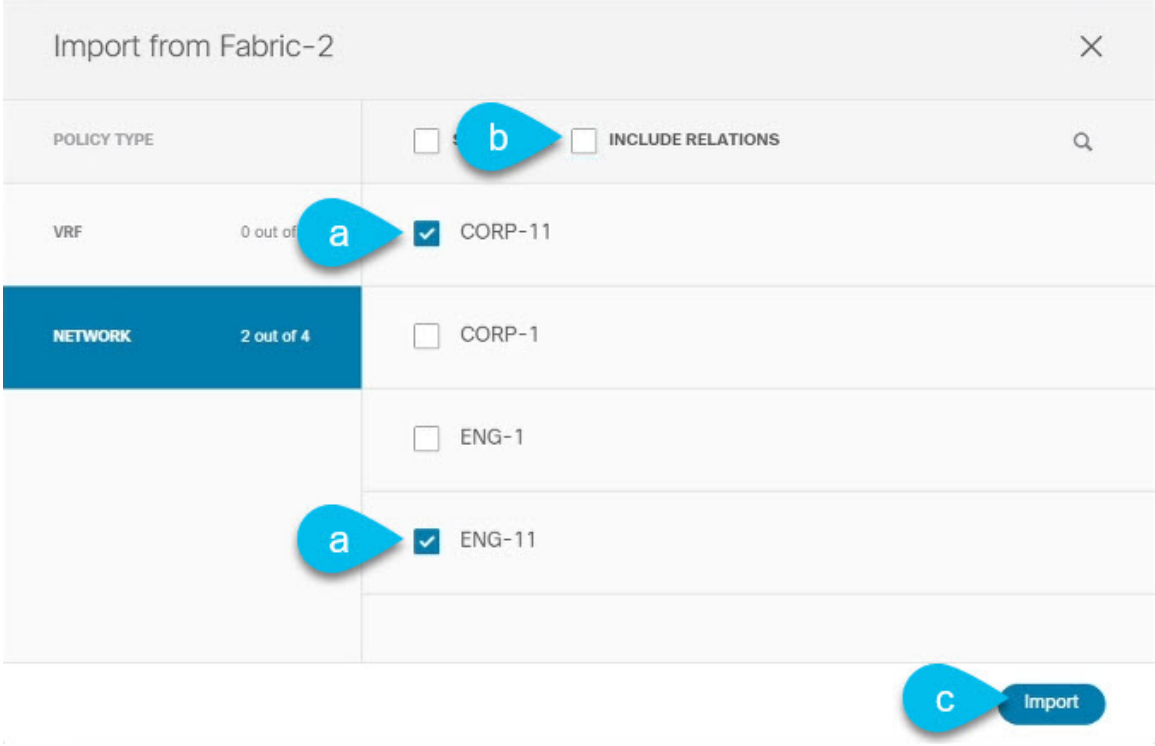
始める前に

- 前のセクションで説明したように、テンプレートを既存のファブリックに関連付ける必要があります。

ステップ 1 メインペインで**[インポート (Import)]** ボタンをクリックし、インポート元の**[サイト (Site)]** を選択します。

インポートできるのは一度に 1 つのファブリックからなので、各ファブリックに対してこれらの手順を繰り返します。

ステップ 2 開いた **[<*site-name*>からのインポート]** ウィンドウから 1 つまたは複数の VRF を選択します。



a) インポート画面で、既存のオブジェクトのすべてまたは一部を選択できます。

上記の例では、ENG-11 および CORP-11 ネットワークを、MSDの一部である Fabric-2 からインポートします。

（注） Nexus Dashboard Orchestrator にインポートするオブジェクトの名前は、すべてのサイトにわたって一意にする必要があります。重複する名前を持つ別のオブジェクトをインポートすると、スキーマ検証エラーとなり、インポートに失敗します。同じ名前のオブジェクトをインポートする必要がある場合は、先に名前を変更してください。

b) **[リレーションを含む（Include Relations）]** ボックスがオフになっていることを確認します。

VRF を個別に 2 番目のテンプレートにインポートします。

c) **[インポート (Import)]** をクリックしてオブジェクトをインポートします。

ステップ 3 このステップを繰り返して、ほかのファブリックからネットワークをインポートします。

インポートしたサイト（この例のFabric-2）の下でテンプレートを選択する場合、ネットワークはそのサイトからインポートされたかのように、スイッチとポート構成がすでに作成されています。ただし、同じネットワークが存在する別のファブリック（Fabric-3）でテンプレートを選択した場合、スイッチ設定は空になります。

インポートしたネットワークのインターフェイス設定を取得するには、他のファブリックから同じネットワークを再度インポートします。

ステップ 4 2 番目のテンプレートを選択し、前の 2 つの手順を繰り返して、必要なすべての VRF をインポートします。

ベスト プラクティスとして、テンプレートの 1 つを使用して、サイトから VRF 構成をインポートし、もう 1 つのテンプレートを使用してネットワーク構成をインポートします。

テンプレートの展開と変更

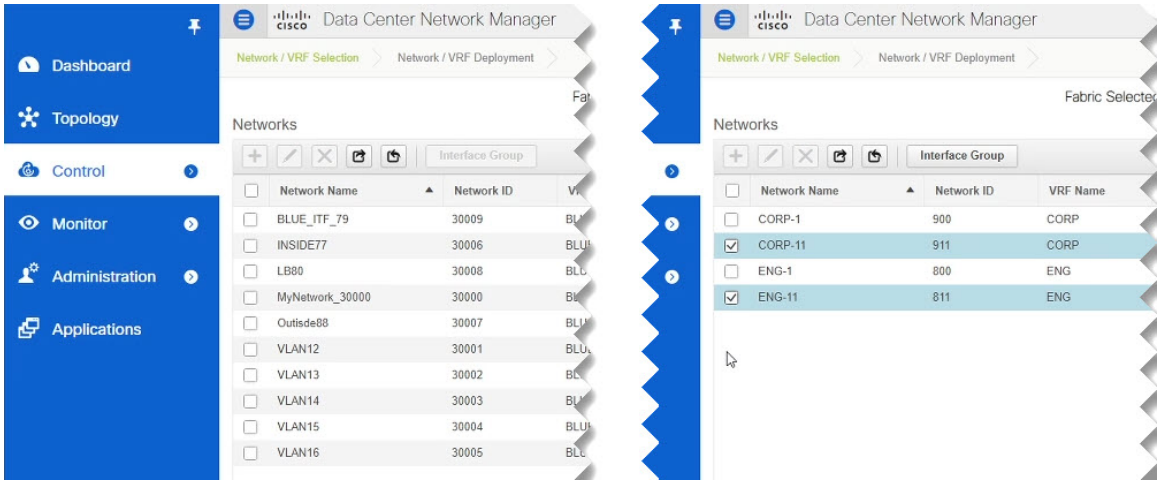
このセクションでは、インポートされた設定を、設定がまだ存在しないサイトに展開する方法について説明します。

始める前に

前のセクションの説明に従って、設定をインポートする必要があります。

ステップ 1 左側のサイドバーで、展開するテンプレートを選択します。

同じ例に従い、NDFC UIを使用して、`Fabric-2` と `Fabric-3` からインポートしたネットワークとVRFが `Fabric-1` に存在しないことを確認します。



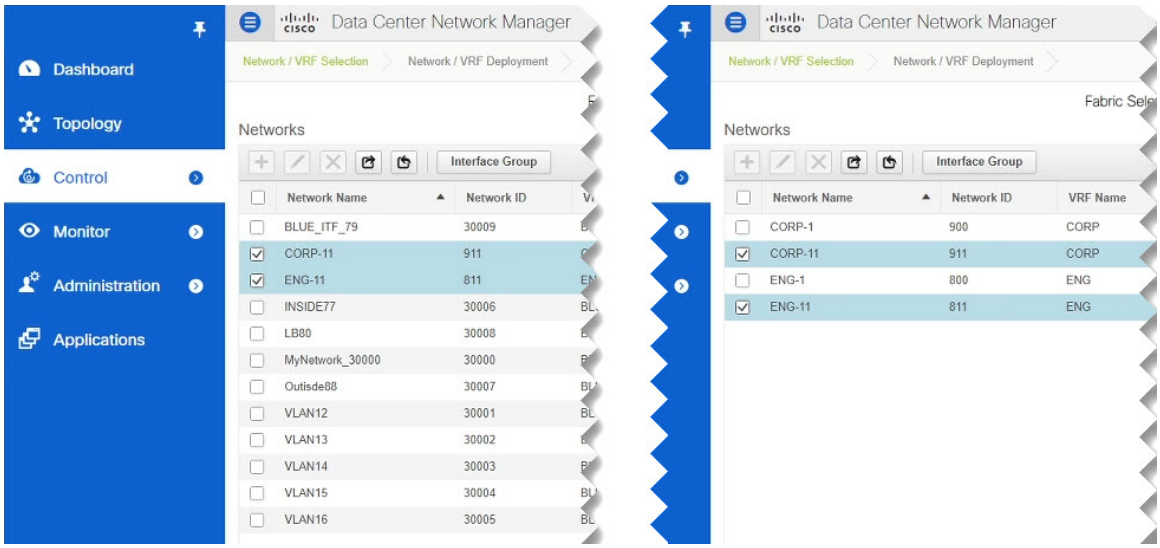
ステップ 2 テンプレート編集ビューの右上で、**[サイトに展開 (Deploy to site)]** をクリックします。

[サイトに展開 (Deploy to Sites)] ウィンドウが開き、展開するオブジェクトの概要が表示されます。

ステップ 3 **[展開 (Deploy)]** をクリックして、新しいテンプレートを展開します。

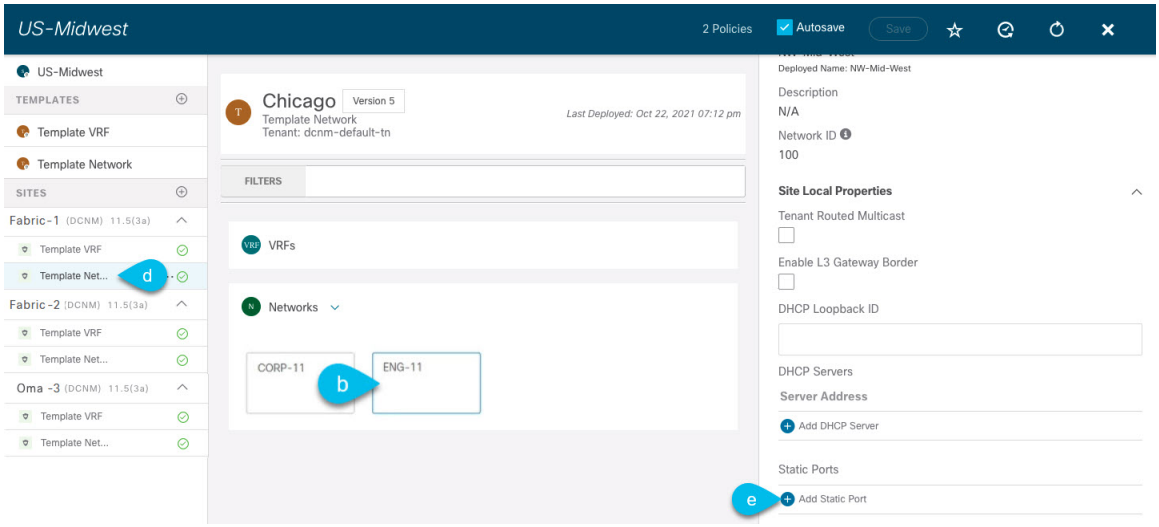
このテンプレートを初めて展開するので、**[サイトに展開 (Deploy to Sites)]** のサマリーに、サイトに展開される設定の違いが表示されます。

設定が展開されるまで数分かかる場合があります。NDO GUI に確認メッセージが表示されたら、NDFC UI を使用して設定が展開されたことを確認できます。



ステップ 4 新しいネットワークにスイッチ ポートを割り当てます。

これで、`Fabric-2` および `Fabric-3` からインポートしたネットワークが `Fabric-1` に展開されていることを確認しました。`Fabric-1` には 1 つ以上のスイッチ ポートを割り当てる必要があります。



a) `Fabric-1` でテンプレートを選択します。

b) 展開したネットワークを選択します。

c) 右側のサイドバーで、**[スタティック ポートの追加 (Add Static Port)]** をクリックします。

表示される **[スタティック ポートの追加 (Add Static Port)]** ウィンドウで、ネットワークの VLAN を割り当てるスイッチとポートを選択します。次に [保存（Save）] をクリックします。

ステップ 5 テンプレートを保存し、新しい設定の変更で再展開します。

NDFC GUI に戻り、[ネットワーク（Networks）]ページを更新することで、変更を再度確認できます。ネットワークのステータスは、NA から In Progress、そして Deployed に変わります。

第 10 章

Cloud Network Controller との統合

概要

ご存じのとおり、Nexus Dashboard Orchestrator は、異なる Nexus ダッシュボード ファブリック コントローラ（NDFC）インスタンスによって管理される複数のオンプレミス VXLAN EVPN ファブリック間の EVPN マルチサイト拡張をサポートしています。これには、ボーダー ゲートウェイ（BGW）での EVPN ピアリングのプロビジョニングと、さまざまなオンプレミス NX-OS ベースのネットワーク スイッチにわたるテンプレートを介したオーバーレイ ネットワーク/VRF のプロビジョニングが含まれます。Nexus Dashboard Orchestrator は、オンプレミスとクラウドの統合と、オンプレミスの ACI ファブリックと Cisco Cloud Network Controller（以前の Cisco Cloud APIC）によって管理されるパブリック クラウド ネットワーク間のワークロード接続もサポートしています。

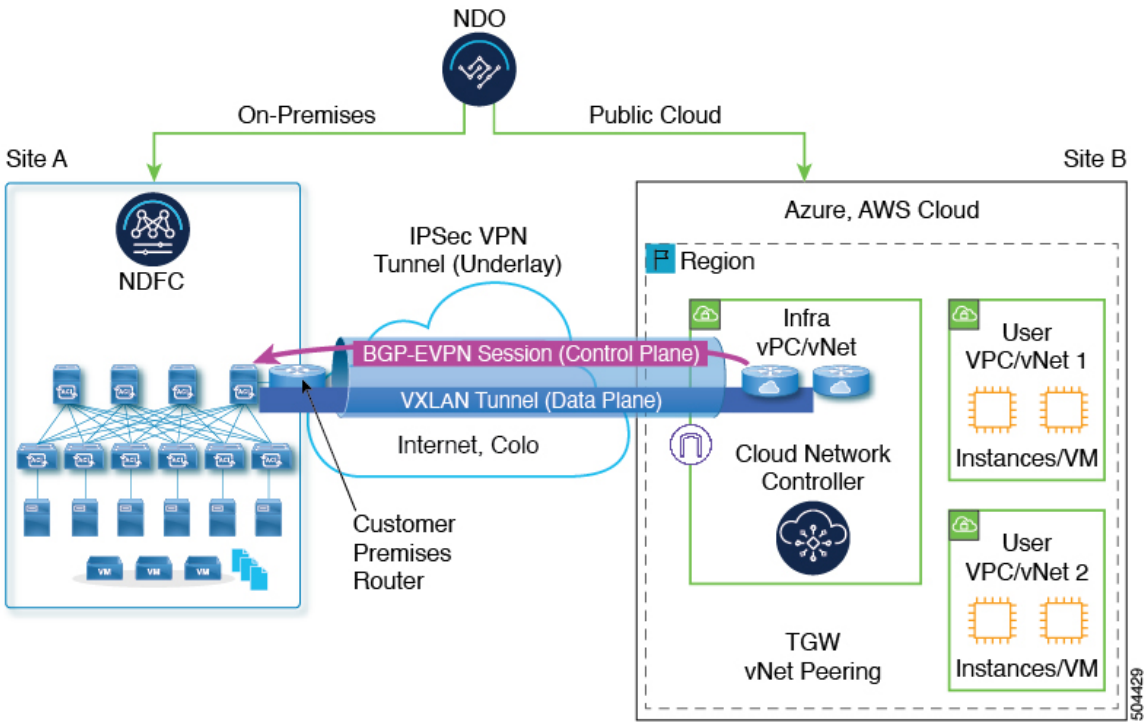
Nexus Dashboard Orchestrator のリリース 4.0(2) は、NDFC によって管理されるオンプレミスの NX-OS ベースのファブリックにパブリック クラウドを統合します。次のセクションでは、NDFC によって管理されるオンプレミスの VXLAN EVPN ベースのデータ センターからのワークロードを構成して、パブリック クラウドで実行され、クラウド ネットワーク コントローラによって管理されるワークロードと通信する方法について詳しく説明します。

（注） Nexus Dashboard Orchestrator のこのリリースは、Amazon Web Services（AWS）および Microsoft Azure のみの NDFC ファブリックとパブリック クラウド間の統合をサポートします。

次の図は、このドキュメント全体で使用されるサンプル トポロジを示しています。これには、NDFC によって管理されるオンプレミス サイト（SiteA）、AWS または Azure パブリック クラウド サイト（SiteB）、およびインフラストラクチャの Catalyst 8000V が接続されている 2 つのサイト間の安全な接続が含まれます。 VPC/VNET は、オンプレミス サイトとの間で送受信されるすべてのトラフィックのクラウド ゲートウェイとして機能します。

（注） 次の図は、ボーダー ゲートウェイ（BGW）として機能するスパイン スイッチを示しています。ただし、BGW はリーフ スイッチとしても展開できます。

図 *5: NDO*、*NDFC*、およびクラウド ネットワーク コントローラの統合例のトポロジ



サイト間のアンダーレイとオーバーレイの接続を確立するときは、次のアプローチを取ります。

- オンプレミス側では、異なるオンプレミス VXLAN EVPN サイト間のシームレスなレイヤ 2/レイヤ 3 DCI 拡張をすでにサポートしている BGW により、VRF をパブリック クラウドに拡張できます。

  BGW 機能は、一連のリーフ スイッチで有効にすることも、スパイン スイッチ上で同じ場所に配置することもできます。

- Orchestrator は、オンプレミスの BGW とクラウド内の Catalyst 8000V 間のコントロール プレーンに BGP EVPN を使用します。

  VXLAN カプセル化は、オンプレミス サイトとパブリック クラウド間の L3 拡張のデータ プレーンで使用されます。

- 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 トンネルが作成されます。

  この目的のため、BGW は、ASR 1000 または CSR 1000v または Catalyst 8000V などのオンプレミスの IPsec 対応デバイスに接続されます。このデバイスは基本的に、オンプレミスの BGW からクラウドの Catalyst 8000V へのエンドツーエンド トラフィックが VXLAN over IPsec を使用するように IPsec トンネルを追加します。

  BGW が Direct Connect または Express Route オプションを介してパブリック クラウドに接続されている場合、IPsec の有効化はオプションであることに注意してください。

- アンダーレイの観点から、BGW はオンプレミスの IPsec デバイスと eBGP をピアリングします。オンプレミスの IPsec デバイスは、確立された IPsec トンネルを介して、クラウド内の Catalyst 8000V と eBGP をピアリングします。

  NDFC は NX-OS ベースのデバイスと IOS-XE ベースのデバイスの両方を管理できるため、NDO は BGP EVPN オーバーレイ、eBGP アンダーレイ、および NDFC 経由でオンプレミス側の IPsec トンネル構成をプロビジョニングします。同様に、NDO は、クラウド ネットワーク コントローラを介して、対応するピア関連の構成を Catalyst 8000V にプロビジョニングします。

  IPsec が有効になっている場合、アンダーレイは IPsec デバイスで終了します。それ以外の場合は、オンプレミス サイトの BGW で終了します。

- これは標準ベースのオンプレミス ファブリックであるため、ACI ファブリックで使用される iVXLAN（UDP 宛先ポート `0xBEEF`）の代わりに、オンプレミス VXLAN EVPN データセンターとクラウド Catalyst 8000V ルータの間で標準 VXLAN（UDP 宛先ポート `4789`）を使用することに注意してください。

必要なコンポーネント

ハイブリッド クラウドは、オンプレミス ネットワークとパブリック クラウド ネットワークを相互接続するためのソリューションです。ハイブリッド クラウド ソリューションの主なコンポーネントは次のとおりです。

- **Easy Fabric**：ボーダー ゲートウェイ（BGW）を含む NDFC 管理のオンプレミス VXLAN ベースのファブリック。

  このファブリックはスタンドアロンにすることも、他のオンプレミス サイトからパブリック クラウドへの接続を提供する POP サイトとして機能させることもできます。

- **外部ファブリック**：オンプレミスの Easy Fabric をパブリック クラウドに相互接続するための IPN デバイス（ASR 1000、CSR 1000v、または Catalyst 8000V など）を含む NDFC 管理ファブリック。

この場合、オンプレミスの Easy Fabric サイトの BGW は、外部ファブリックの IPN デバイスに接続されます。

- **パブリック クラウド**：クラウドネットワーク コントローラによって管理され、CSR 1000v または Catalyst 8000V を含むパブリック クラウド サイト。

  オンプレミスとパブリック クラウド間のレイヤ 3 到達可能性は、パブリック クラウドと外部ファブリックの CSR 1000v または Catalyst 8000V を介してプロビジョニングされます。

ワークフロー

このドキュメントの他のセクションでは、必要な構成について詳しく説明しています。簡単に言えば、次のワークフローを実行します。

- Nexus Dashboard Orchestrator のホストに使用される Nexus ダッシュボード クラスターを展開します。

（注） NDO サービスと NDFC サービスには、個別の Nexus ダッシュボード クラスタを使用する必要があります。

- Cisco Nexus Dashboard Orchestrator をインストール。
- NDFC サイトとクラウド ネットワーク コントローラ サイトをオンボードします。
- NDO を使用してサイトのインフラ接続を構成し、オンプレミス サイトとクラウド サイト間の接続を確立します。
- 既存の NDFC 構成をインポートします。

サポートされる使用例

VRF ストレッチング

このユース ケースでは、NDFC サイトから AWS または Azure のパブリック サイトへの VRF のレイヤ 3 拡張を構成できます。これは、NDFC サイトのボーダー ゲートウェイ（BGW）のルート ターゲット （RT）と、クラウド ネットワーク コントローラ側の CSR 1000v または Catalyst 8000V をプログラミングすることによって行われます。これにより、これらのサイトのワークロード間でトラフィックが流れるようになります。

このユースケースを展開するには、次の手順を実行します。

1. 単一のテンプレートで VRF を定義し、そのテンプレートを両方のサイトに関連付けます。
2. NDFC のサイトローカル VRF プロパティを設定します。
3. クラウドのサイトローカル VRF プロパティを設定します。

4. 設定を展開します。

VRF リーク（共有サービス）

これは、オンプレミスのACIファブリックで以前サポートされていた機能です。これにより、オンプレミス サイトに VRF（vrf1）、クラウド サイトに別の VRF（vrf2）を設定し、それらの VRF のワークロードが相互に通信できるようにします。この場合、オンプレミスの VRF は、ストレッチまたはサイトローカルのいずれかにすることができます。

このユースケースを展開するには、次のことができます。

1. dcnm-default-tn テナントに関連付けられた template1 に vrf1 を定義します。
2. template1 をオンプレミスおよびクラウド サイト、またはオンプレミス サイトのみに関連付けます。
3. dcnm-default-tn テナントに関連付けられた template2 に vrf2 を定義します。

   このテンプレートをクラウド サイトにも関連付けますが、dcnm-default-tn と別のクラウド テナントとの間のルート リークはサポートされないことに注意してください。
4. template2 をクラウド サイトのみに関連付けます。
5. 2 つの VRF 間のルート リークを構成します。
6. 設定を展開します。

サポートされるトポロジ

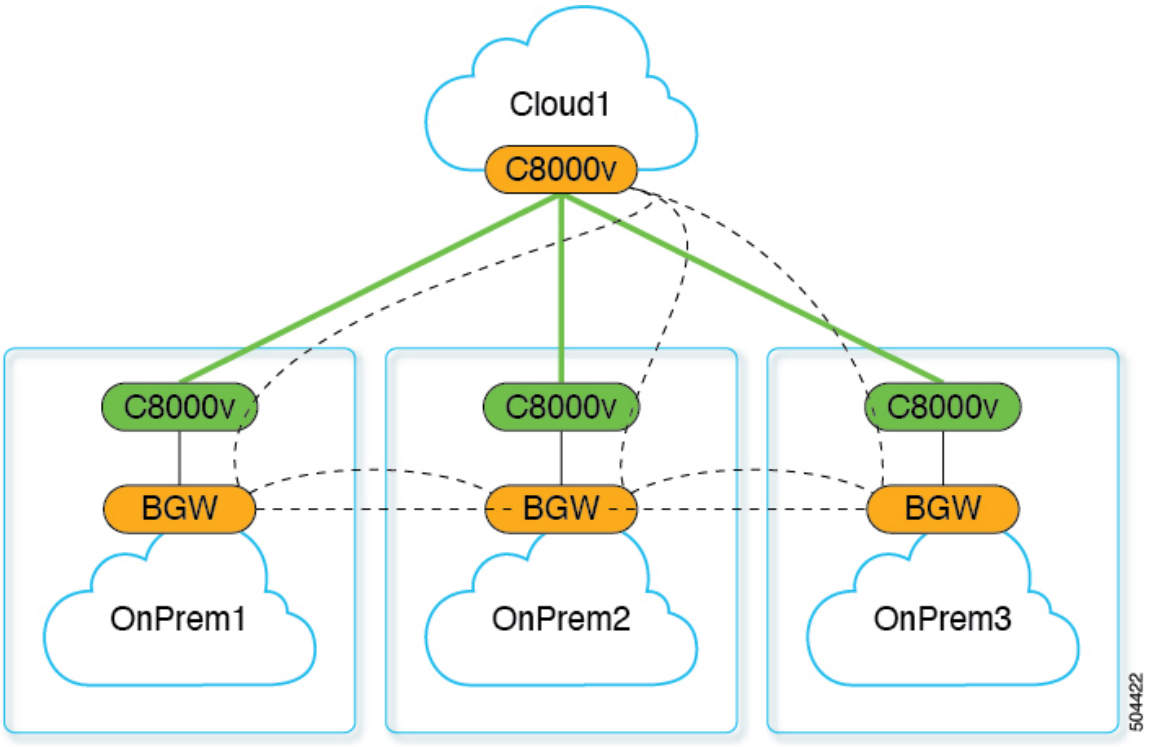
NDFCファブリックとクラウドサイト間のサイト間接続を展開する場合、次の全体的なトポロジがサポートされます。

（注） 次のすべての図で：

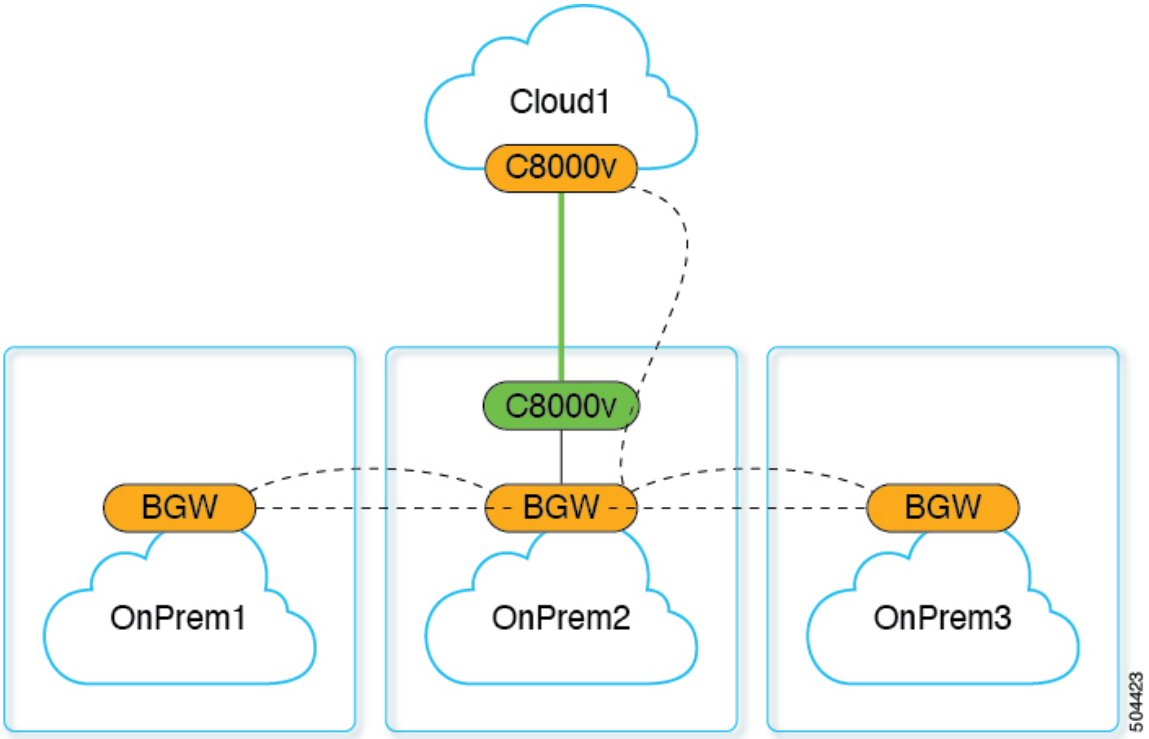
- 緑の実線は IPsec トンネルを表します。
- 点線は、BGP-EVPN オーバーレイ ピアリングを表します。
- クラウド サイトの C8KV は CSR を表しています。CSR 1000v または Catalyst 8000V の可能性があります。
- オンプレミス サイトの C8KV は IPN デバイスで、ASR 1000、CSR 1000v、または Catalyst 8000V の可能性があります。

  NDFC の観点からは、これらはすべて管理対象の IOS-XE デバイスです。

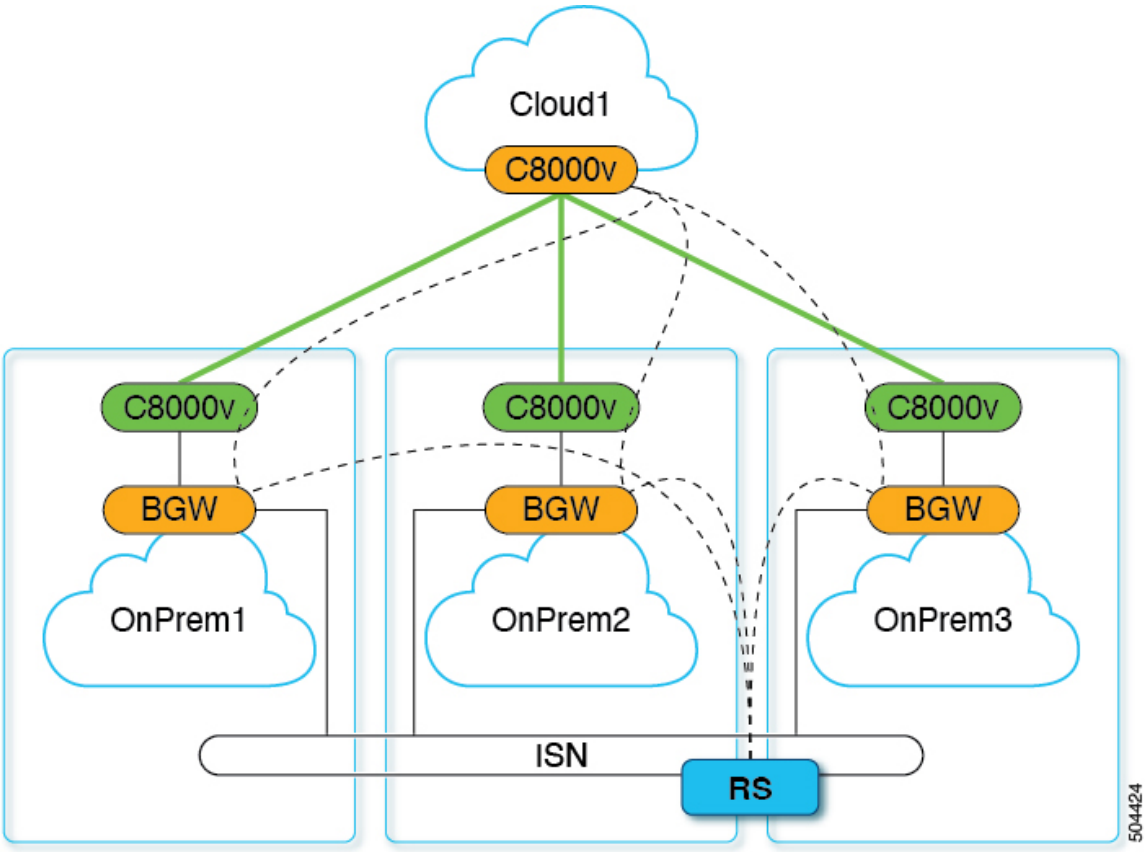
- オンプレミス サイトと、クラウド サイト両方の分散型フルメッシュ接続：



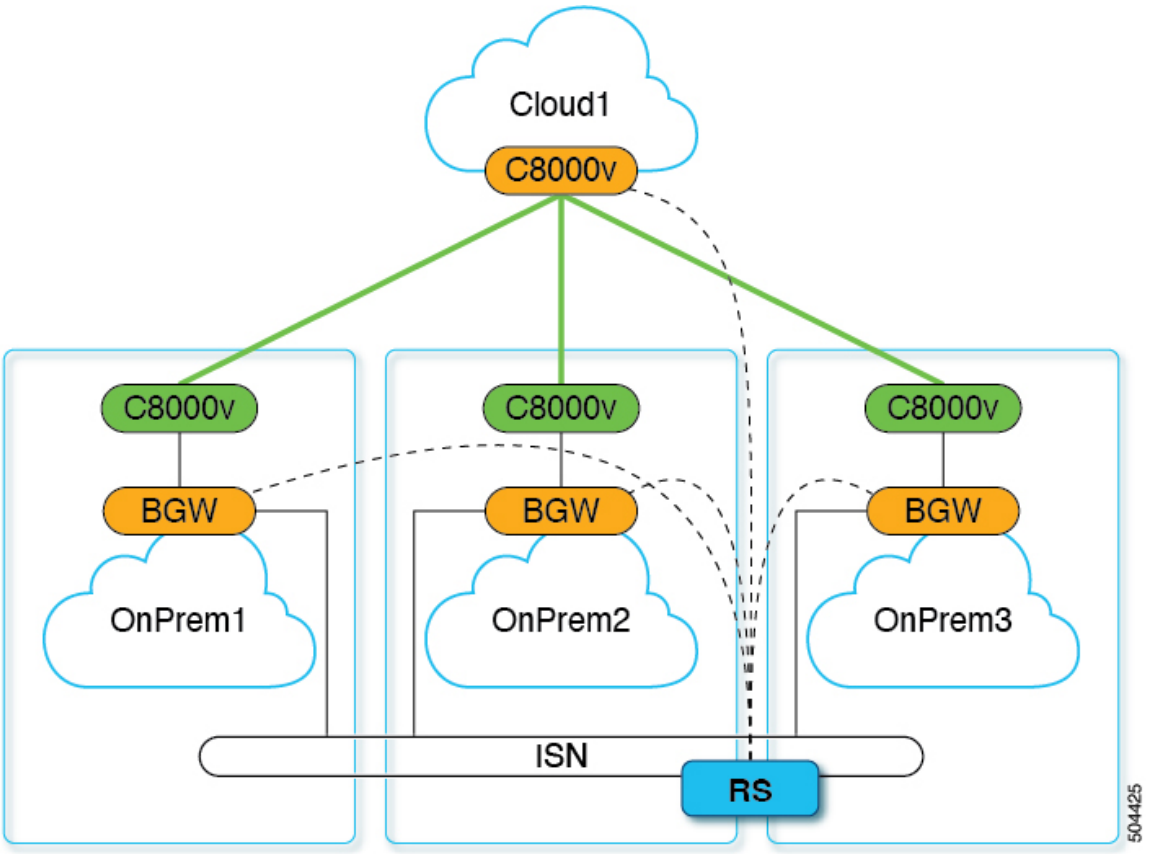
- オンプレミス サイトと、クラウド サイトに接続されている単一のオンプレミス サイトとの分散型フルメッシュ接続：



- ルート サーバー（RS）を備えたオンプレミス サイトと、クラウド サイトに接続されているすべてのオンプレミス サイトとのフルメッシュ接続：



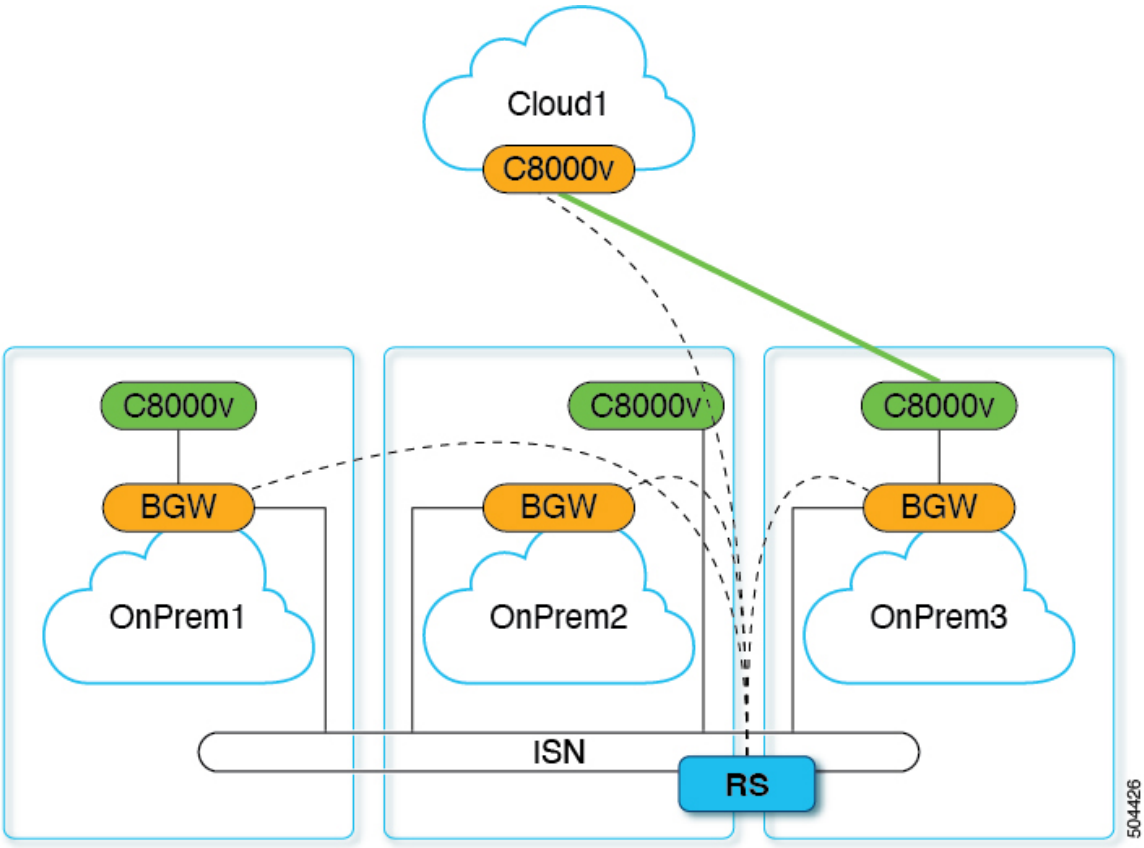
- RS を備えたオンプレミス サイトと、RS を介してクラウド サイトに接続されているすべてのオンプレミス サイトとのフルメッシュ接続：



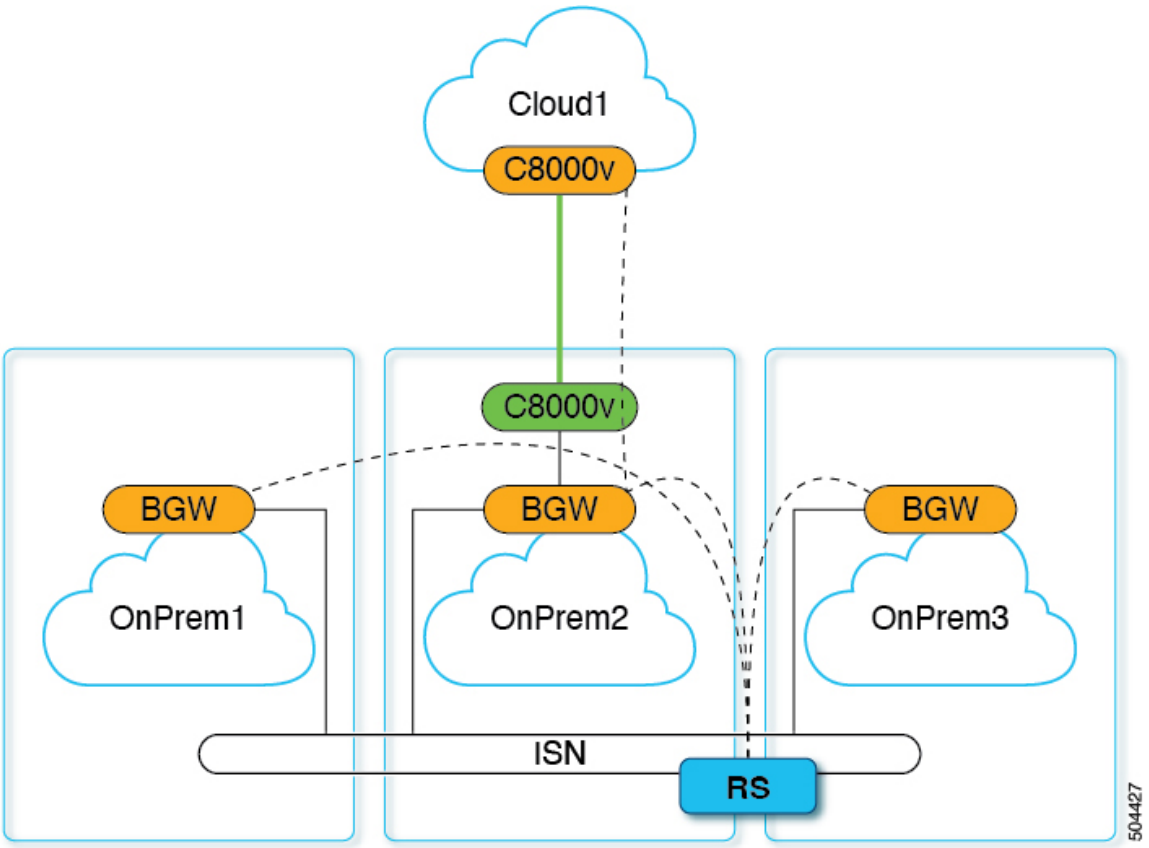
サポートされていないトポロジ

以下のトポロジは**サポートされていません**。

- RS を備えたオンプレミス サイトと、すべてのクラウド サイトの共有 CSR とのフル メッシュ接続：



- RS を備えたオンプレミス サイトと、クラウド サイトに接続された単一のオンプレミス サイトとのフル メッシュ接続：



前提条件とガイドライン

このユースケースを構成する前に、以下を完了しておく必要があります。

- このユースケースに必要なすべてのソフトウェアのサポートされているバージョンがデプロイまたはアップグレードされている：
  - Nexus Dashboard リリース 2.2(2) 以降と、Nexus Dashboard ファブリック コントローラ リリース 12.1(1p)

（注） 既存の NDFC インストールをこのリリースにアップグレードすることはサポートされていないため、新しい NDFC インスタンスをデプロイする必要があります。

NDFC 12.1(1p) リリースの提供対象は限られています。詳細については、シスコの担当者にお問い合わせください。

  - Nexus Dashboard リリース 2.1(2d) 以降と、Nexus Dashboard Orchestrator リリース 4.0(2)

（注） ファブリック コントローラとオーケストレータ サービスは、別々の Nexus ダッシュボード クラスタにデプロイする必要があります。

詳細については、*Cisco Nexus Dashboard Deployment Guide* および *Cisco Nexus Dashboard Orchestrator Deployment Guide* を参照してください。

- AWS または Azure パブリック クラウドのクラウド ネットワーク コントローラー リリース 25.0(5) 以降。

（注） このユース ケースは、AWS または Azure クラウド サイトでのみサポートされています。

詳細については、*Cisco Cloud Network Controller for AWS Installation Guide* または *Cisco Cloud Network Controller for Azure Installation Guide* を参照してください。

- Nexus Dashboard Orchestrator サービスをホストしている Nexus Dashboardクラスタで、NDFC とクラウド ファブリックをオンボーディングします。

  これには、Nexus Dashboard にサイトを追加し、Nexus Dashboard Orchestrator で管理できるようにすることが含まれます（*Cisco Nexus Dashboard Orchestrator 導入ガイド*を参照）。

上記の要件に加えて、このユース ケースには次の制限があります。

- このリリースでは、オンプレミス サイトとクラウド サイト間の VRF のストレッチがサポートされています。
- VRF 間のルート リークを設定する場合、「Leak All」オプションはサポートされません。
- クラウド サイトへのインターネット ルートのエクスポートはサポートされていません。

  その結果、インターネット接続が NDFC サイトで構成されていて、NDFC とクラウド サイトの間でサイト間接続が確立されている場合、クラウド EPG はインターネットに到達できません。

インフラの設定：Orchestrator 一般設定

このセクションでは、Nexus Dashboard Orchestrator によって搭載および管理される NDFC サイトの一般的なインフラ設定を構成する方法について説明します。

このセクションでは、複数の UI タブにわたっていくつかの設定を構成します。

- **[コントロール プレーンの構成（Control Plane Configuration）]** タブには、オンプレミス サイト間のマルチサイト VXLAN 構成の設定情報が含まれています。

- **[IPN デバイス（IPN Devices）]** タブには、オンプレミスの IPN デバイス（ASR 1000、CSR 1000v、Catalyst 8000V など）に関する設定情報が含まれています。これらは、オンプレミス サイトの BGW とクラウド CSR 1000v または Catalyst 8000V 間の安全な接続を提供します。
- **[外部デバイス（External Devices）]** タブは、このハイブリッド クラウドのユース ケースでは使用されません。
- **[IPsec トンネル サブネット プール（IPsec Tunnel Subnet Pools）]** タブでは、IPsec トンネルに使用されるサブネット プールを定義できます。
- **[NDFC 設定（NDFC Settings）]** タブには、VNI、マルチサイト ループバック IP、エニーキャスト ゲートウェイ、およびオンプレミス VXLAN 接続のその他の設定が含まれています。

ステップ 1 Orchestrator の左のナビゲーションメニューから 、**[インフラストラクチャ（Infrastructure）]** > **[サイト接続（Site Connectivity）]**を選択します。

ステップ 2 メイン ペインにある **[構成（Configure）]** をクリックします。

ステップ 3 左側のサイドバーで、**[全般設定（General Settings）]**を選択します。

ステップ 4 **[コントロール プレーン設定（Control Plane Configuration）]** を指定します。

a) **[コントロール プレーン設定（Control Plane Configuration）]** タブを選択します。

b) **[BGP ピアリング タイプ（Bgp Peering Type）]** を選択します。

- `full-mesh`：各サイトのすべてのボーダー ゲートウェイ スイッチは、リモート サイトのボーダー ゲートウェイ スイッチとのピア接続を確立します。
- `route-server`：route-server オプションを使用すると、各サイトが MP-BGP EVPN セッションを確立する 1 つ以上のコントロールプレーン ノードを指定できます。ルートサーバー ノードは、従来の BGP ルート リフレクタと同様の機能を実行しますが、EBGP（iBGP）セッションでは使用しません。ルートサーバー ノードを使用すると、NDO によって管理されるすべての VXLAN EVPN サイト間で MP-BGP EVPN フルメッシュ隣接関係が作成されなくなります。

c) **[BGP ピアリングタイプ（BGP Peering Type）]** を `route-server` に設定する場合は、**[+ルート サーバーを追加（+ Add Route Server）]** をクリックして、1 台以上のルート サーバーを追加します。

[ルート サーバーの追加（Add Route Server）] ウィンドウが開きます。

- **[サイト（Site）]** ドロップダウンから、ルート サーバーに接続するサイトを選択します。
- **[ASN]** フィールドには、サイトのASNが自動的に入力されます。
- **[コア ルータ デバイス（Core Router Device）]** ドロップダウンから、接続するルート サーバーを選択します。
- **[インターフェイス（Interface）]** ドロップダウンから、コア ルータ デバイスのインターフェイスを選択します。

ルート サーバーは最大 4 台まで追加できます。複数のルート サーバーを追加すると、すべてのサイトがすべてのルート サーバーに対して MP-BGP EVPN 隣接関係を確立します。

d) **[キープアライブ間隔（秒）（Keepalive Interval（Seconds））]**、**[ホールド間隔（秒）Hold Interval（Seconds）]**、**[ステール間隔（秒）（Stale Interval（Seconds））]**、**[グレースフル ヘルパー（Graceful Helper）]**、**[最大 AS 限界（Maximum AS Limit）]**、および **[ピア間の BGP TTL（BGP TTL Between Peers）]** フィールドは、Cisco ACI ファブリックにのみ関連するため、デフォルト値のままにします。

e) 設定は eBGP ピアリングには適用されないため、**[OSPF エリア ID（OSPF Area ID）]** をスキップします。

f) 設定は Cisco ACI ファブリックのみに適用されるため、**[IANA 割り当てポート（IANA Assigned Port）]** をスキップします。

ステップ 5 **[IPN デバイス情報]** を入力します。

IPN（IP ネットワーク）デバイスは、オンプレミスまたはクラウドサイト（あるいはその両方）の間のネットワーク インフラストラクチャを提供します。これにより、VXLAN EVPN コントロールおよびデータ プレーン接続を確立できます。

オンプレミスとクラウド サイト間接続でプライベート接続を使用し、IPsec を有効化しない場合は、この手順をスキップできます。パブリック インターネット経由の接続では、IPsec が常に有効になっており、この手順で情報を提供する必要があります。

後のセクションで説明するように、オンプレミスとクラウドサイト間のサイト アンダーレイ接続を設定する場合は、クラウド CSR への接続を確立するオンプレミス IPN デバイスを選択する必要があります。これらの IPN デバイスは、オンプレミスのサイト設定画面で使用可能になる前に、ここで定義する必要があります。

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

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

c) デバイスが**[管理対象外（Unmanaged）]**か**[管理対象（Managed）]**かを選択し、デバイス情報を提供します。

これは、デバイスが NDFC によって直接管理されるかどうかを定義します。

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

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

- **[管理対象（Managed）]** IPN デバイスには、デバイスが入っているNDFC **[サイト（Site）]** を選択し、そのサイトの **[デバイス（Device）]** を選択します。

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

d) チェック マーク アイコンをクリックして、デバイス情報を保存します。

e) 追加する IPN デバイスについて、この手順を繰り返します。

ステップ 6 **[IPsec トンネル サブネット プール（IPsec Tunnel Subnet Pools）]** 情報を入力します。

ここで指定できるサブネットプールには、次の 2 つのタイプがあります。

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

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

  1 つ以上のクラウド サイトから外部接続を有効にする場合は、少なくとも 1 つの外部サブネット プールを提供する必要があります。

- **サイト固有のサブネット プール**：クラウド サイトの CSR と外部またはオンプレミス デバイス間の接続に使用されます。

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

  サイト固有のサブネット プールを指定しない場合でも、クラウド サイトの CSR と外部デバイス間の接続を設定すると、外部またはオンプレミスのサブネット プールが IP 割り当てに使用されます。.

（注） 両方のサブネット プールの最小マスク長は /24 です。

1 つ以上の**外部サブネット プール**を追加するには：

a) **[IPsec トンネル サブネット プール（IPsec Tunnel Subnet Pools）]** タブを選択します。
b) **[外部サブネット プール（External Subnet Pool）]** エリアで、**[+ IP アドレスの追加（+Add IP Address）]** をクリックして、1 つ以上の外部サブネット プールを追加します。

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

   サブネットは、他のオンプレミス TEP プールと重複してはならず、`0.xxx` または `0.0.xx`で 始まってはならず、`/16` と `/24` の間のネットワーク マスク（`30.29.0.0/16` など）が必要です。

c) チェックマーク アイコンをクリックして、サブネット情報を保存します。
d) 追加するサブネット プールについて、これらのサブステップを繰り返します。

1 つ以上の **[サイト固有のサブネット プール（Site-Specific Subnet Pools）]** を追加するには：

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

   [サイト固有サブネットプールの追加（Add Site-Specific Subnet Pool）] ダイアログが開きます。

c) サブネットの **[名前（Name）]** を入力します。

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

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

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

e) チェックマーク アイコンをクリックして、サブネット情報を保存します。

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

f) **[保存（Save）]** をクリックして、名前付きサブネット プールを保存します。

g) 追加する名前付きサブネット プールについて、これらのサブステップを繰り返します。

次のタスク

全般的なインフラ設定を構成した後も、サイト固有の設定に関する追加情報を指定する必要があります。次の項で説明する手順に従って、サイト固有のインフラストラクチャ設定を行います。

インフラの構成: NDFC インフラ サイト固有の設定

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

ステップ 1 **[サイト接続（Site Connectivity）]** ページの左サイドバーの、**[サイト（Sites）]** の下で、特定の NDFC サイトを選択します。

ステップ 2 右側の ***<Site>*** **[設定 (Settings)]**サイドバーで、**[マルチサイト（Multi-Site）]** を有効にします。

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

オーバーレイ構成は、以下の手順で説明するようにアンダーレイ サイト間接続が確立されていないサイトにはプッシュされないことに注意してください。

ステップ 3 **[マルチサイト VIP（Multi-Site VIP）]** を指定します。

このアドレスは、サイト間の L2 BUM および L3 マルチキャスト トラフィックのために使用されます。この IP アドレスは、同じファブリックの一部であるすべてのボーダーゲートウェイスイッチに導入されます。

（注） 設定するサイトが NDFC マルチサイトドメイン（MDS）の一部である場合、このフィールドには NDFC からインポートされた情報が事前に入力されます。この場合、値を変更してインフラ設定を再展開すると、MDS の一部であるサイト間のトラフィックに影響します。

ステップ 4 **[IPN デバイス IPsec IP（IPN Devices IPsec IP）]** 情報を追加します。

複数のサイトがあり、それらの各サイトが異なる IPsec デバイス セットに接続している場合は、ここでその情報を定義できます。前のセクションで説明したように、最初にすべての IPN デバイスを **[一般設定（General Settings）]** タブで指定する必要があることに注意してください。

a) 右側のプロパティ サイドバーの **[サイト間接続（Inter-Site Connectivity）]** タブで、**[+ IPN デバイスの追加（+Add IPN Divice）]** をクリックします。
b) **[名前（Name）]** ドロップダウンから、前に追加した IPN デバイスのいずれかを選択します。
c) チェックマーク アイコンをクリックして保存します。

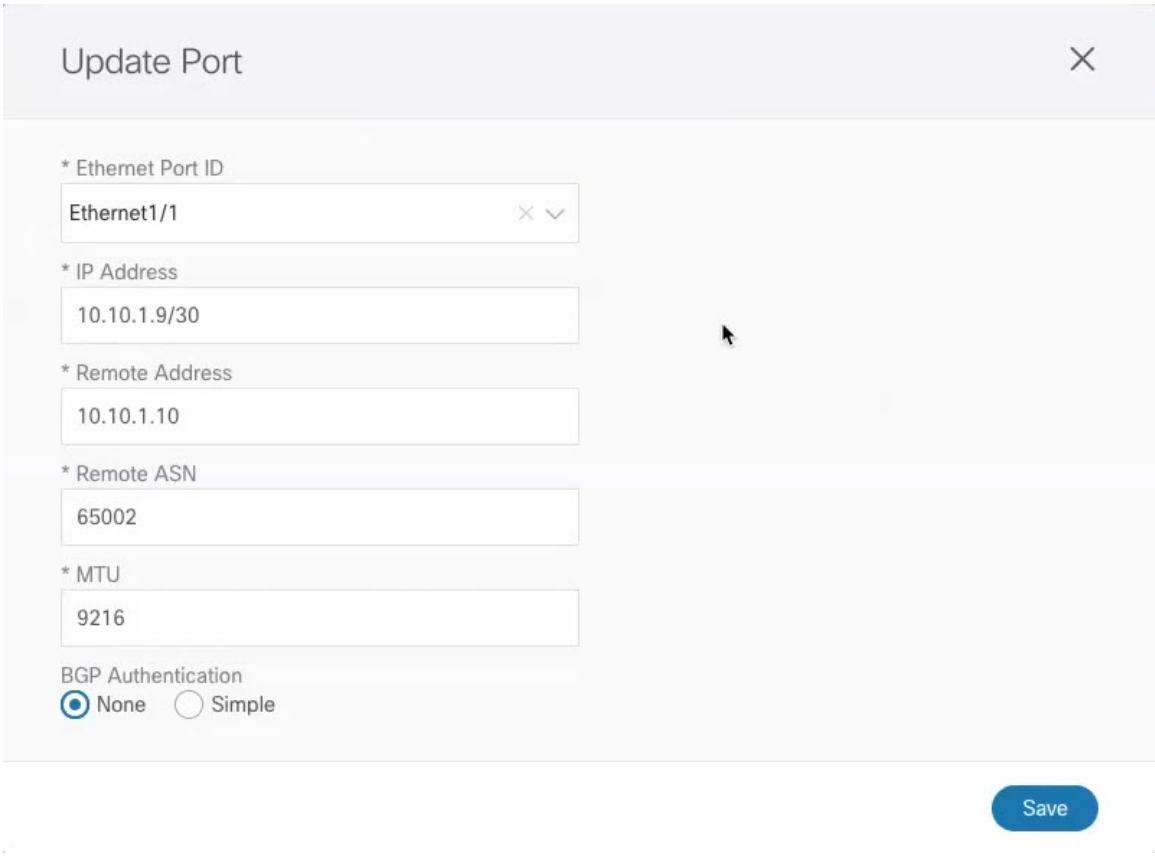
ステップ 5 **<fabric-name>** タイル内で、ボーダーゲートウェイを選択します。

ステップ 6 右側**<*border-gateway*>**サイドバーを設定し、**BGP-EVPN ROUTER-ID** と **BGW PIP** を指定します。

vPCドメインの一部であるボーダーゲートウェイの場合は、**VPC VIP** も指定する必要があります。

ステップ 7 **[ポートの追加 (Add Port)]** をクリックして、IPN に接続するポートを設定します。

（注） このリリースでは、NDFC からのポート設定のインポートはサポートされていません。設定するサイトがすでに NDFC マルチサイトドメイン（MDS）の一部である場合は、NDFC ですでに設定されている値と同じ値を使用する必要があります。



このボーダーゲートウェイをコアスイッチまたは別のボーダーゲートウェイに接続するポートの展開に固有の次の情報を入力します。

- **[イーサネット ポート ID (Ethernet Port ID)]** ドロップダウンから、IPNに接続するポートを選択します。
- **[IP アドレス (IP Address)]** フィールドに、IP アドレスとネットマスクを入力します。

- **[リモート アドレス (Remote Address)]** フィールドに、ポートが接続されているリモート デバイスの IP アドレスを入力します。
- **[リモート ASN (Remote ASN)]** フィールドに、リモート サイトのIDを入力します。
- **[MTU]** フィールドに、サーバーの MTU を入力します。

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

  [継承 (inherit)] を指定することも、576 ～ 9000 の値を指定することもできます。
- **BGP認証**の場合は、[なし (None)] または [シンプル (Simple (MD5))] を選択できます。

  [シンプル (Simple)]を選択した場合は、**認証キー**も指定する必要があります。

インフラの構成：パブリック クラウドサイトの設定とサイト間接続

このセクションでは、クラウド サイトのサイト固有のインフラ設定を構成し、クラウド サイトとオンプレミスの NDFC ファブリック間の接続を確立する方法について説明します。

ステップ 1 **[サイト接続（Site Connectivity）]** ページの左サイドバーの、**[サイト（Sites）]** の下で、特定のクラウド サイトを選択します。

ステップ 2 右側の ***[<Site>* 設定 (Settings)]*** ペインで、**[サイト間接続 (Inter-Site Connectivity)]** タブを選択し、**[マルチサイト（Multi-Site）]** を有効にします。

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

オーバーレイ構成は、以下の手順で説明するようにアンダーレイ サイト間接続が確立されていないサイトにはプッシュされないことに注意してください。

ステップ 3 このサイトから他のサイトへの **[サイト間接続（Inter-Site Connectivity）]** を構成します

a) クラウドサイトの右側のプロパティ サイドバーで、**[サイトの追加（+Add Site）]** をクリックします。

[サイトの追加（Add Site）] ウィンドウが表示されます。

b) **[サイトへの接続（Connected to Site）]** で、**[サイトの選択 >（Select a Site >）]** をクリックし、確立する接続の接続先サイトを選択します。

リモート サイトを選択すると、[サイトの追加（Add Site）] ウィンドウが更新され、両方向の接続が反映されます：[サイト1（Site1）] > [サイト2（Site2）] および [サイト2（Site2）] > [サイト1（Site1）]。

c) [サイト1（Site1）] > [サイト2（Site2）] エリアで、[接続タイプ（Connection Type）] ドロップダウンから、サイト間の接続のタイプを選択します。

次のオプションを使用できます。

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

  このタイプは、任意の 2 つのクラウド サイト間、またはクラウド サイトとオンプレミス サイト間でサポートされます。

- [プライベート接続 (Private Connection)]：2 つのサイト間のプライベート接続を使用して接続が確立されます。

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

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

d) **[プロトコル（Protocol）]** で、[BGP-EVPN] を選択し、追加の詳細を指定します。

このユース ケースでは、オンプレミスの NDFC ファブリックとクラウド サイトの間で BGP-EVPN 接続を確立する方法について説明します。

オプションで **[IPsec]** を有効にして、使用するインターネット キー エクスチェンジ（IKE）プロトコルのバージョンを選択します。構成に応じて IKEv1（バージョン 1）または IKEv2（バージョン 2）を選択できます。

- パブリック インターネット接続の場合、IPsec は常に有効です。
- プライベート接続の場合、IPsec は有効または無効にすることができます。

また、**[ハブ サイト（Hub Site）]** オプションを有効にすることもできます。これは、2 つのクラウド サイト間の EVPN ピアリングが、ルート サーバー モデルなどの中間のオンプレミス VXLAN EVPN サイトを経由することを示します。

e) **[保存 (Save)]** をクリックして、設定を保存します。

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

f) 他のクラウド サイトへのサイト間接続を追加するには、この手順を繰り返します。

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

次のタスク

必要なサイト間接続情報をすべて設定しましたが、まだサイトにプッシュされていません。インフラ設定の展開 （109 ページ）の説明に従って、設定を展開する必要があります。

インフラ設定の展開

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

インフラ構成を展開すると、IPsec デバイスの構成、オンプレミス サイトに対してローカルのオーバーレイ ピアリング、およびサイト間接続を構成したクラウド サイトとオンプレミス サイト間のオーバーレイ ピアリングがプッシュされます。

ステップ 1 メインペインの右上で、**[展開（Deploy）]**そして**[IPN デバイス構成ファイルの展開とダウンロード（Deploy & Download External Device Config files）]** クリックします。

[IPN デバイス構成ファイルの展開とダウンロード（Deploy & Download IPN Device Config files）] は、オンプレミスの NDFC 管理対象サイトと Cloud Network Controller サイトの両方に構成をプッシュし、サイト間のエンドツーエンド インターコネクトを有効にします。

さらに、IPN デバイスを非管理対象として構成していた場合、このオプションは、IPN デバイスからクラウド サイトの C8000V への接続を可能にするための構成情報を含む zip ファイルをダウンロードします。すべてまたは一部の設定ファイルのどちらをダウンロードするかを選択できるようにするための、フォローアップ画面が表示されます。

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

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

クラウド テナント情報の提供

ここでは、クラウド テナント情報を追加する方法について説明します。

始める前に

- Nexus Dashboard Orchestrator でクラウド サイトをオンボーディングし、管理する必要があります。

ステップ 1 Orchestrator' の左型のナビゲーションメニューから、**[アプリケーション管理（Application Management）]>>[テナント（Tenants）]** を選択します。

ステップ 2 情報を提供するテナントをクリックするか、**[テナントの追加（Add Tenant）]** をクリックして新しいテナントを追加します。

ステップ 3 クラウド サイトのテナント情報を提供します。

a) **[関連サイト（Associated Sites）]** 領域で、このテナントを関連付けるクラウド サイトを選択します。
b) サイト名の横にある **[編集（Edit）]** アイコンをクリックして、情報を編集します。
c) （任意）**[セキュリティ ドメイン（Security Domains）]** ドロップダウン リストから、セキュリティ ドメインを選択します。

セキュリティドメイン（例では `SecDom1`）を使用すると、両方のグループのユーザーに同じ特権が割り当てられている場合であっても、別のセキュリティドメイン（例では `SecDom2`）のユーザーグループによって作成されたオブジェクトを表示または変更できないようにすることができます。たとえば、`SecDom1` のセキュリティ ドメインのテナント管理者は、`SecDom2` で構成されたポリシー、プロファイル、またはユーザーを表示できません。

d) テナントのクラウド アカウント情報を提供します。

クラウド テナントとそれらに必要なクラウド アカウント情報の詳細については、クラウド プロバイダーおよびリリースに対応したクラウド ネットワーク コントローラ 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 コンポーネントの構成」の章を参照してください。

e) マルチサイト ドメインに統合する追加のクラウド サイトについて、この手順を繰り返します。

スキーマとテンプレートの作成

このセクションでは、オンプレミス サイトとクラウド サイトのワークロード間ネットワーク接続を可能にする構成を定義するための、スキーマとテンプレートを作成する方法について説明します。

始める前に

- オンプレミスの NDFC ファブリックとクラウド サイト間のサイト インフラおよびサイト間接続を構成しておく必要があります。

ステップ 1 スキーマを新規作成します。

a) 左側のナビゲーション メニューで、**[アプリケーション管理 (Application Management)]** > **[スキーマ (Schemas)]** を選択します。
b) [スキーマ (Schema)] ページで、**[スキーマの追加 (Add Schema)]** をクリックします。
c) スキーマ作成ダイアログで、スキーマの **[名前 (Name)]** と説明（オプション）を入力します。
d) **[追加（Add）]** をクリックして、スキーマの概要ページに移動します。

デフォルトでは、新しいスキーマは空であるため、次の手順に従って 1 つ以上のテンプレートを追加する必要があります。

ステップ 2 テンプレートを作成します。

a) スキーマの概要ページで、**[新しいテンプレートの追加（Add New Template）]** をクリックします。

b) **[テンプレート タイプの選択 (Select a Template type)]** ウィンドウで、テンプレート タイプとして **[NDFC]** を選択します。
c) **[追加 (Add)]** をクリックしてテンプレートを追加します。

ステップ 3 テンプレートの名前とテナントを指定します。

a) 右側のサイドバーで、テンプレートの **[表示名（ Display Name）]** を入力します。
b) **[テナントの選択（Select a Tenant）]** ドロップダウンから、このテンプレートに関連付けるテナントを選択します。

ステップ 4 スキーマビューの右上隅で、**[保存 (Save)]** をクリックしてスキーマとテンプレートを保存します。

ステップ 5 テンプレートをサイトと関連付けます。

a) メイン ペインの **[表示（View）]** ドロップダウンから、テンプレートを選択します。
b) **[アクション（Actions）]** メニューから、**[サイトの関連付け（Site Association）]** を選択します。
c) テンプレートを関連付けるオンプレミスおよびクラウド サイトを選択します。

テンプレートをオンプレミス サイトとクラウド サイトの両方に関連付けると、テンプレートで定義されているすべてのオブジェクトがそれらのサイト間に「ストレッチ」されます。オンプレミス サイトとクラウド サイトにまたがるネットワークのストレッチはサポートされていないため、ネットワークを含むテンプレートをオンプレミス サイトとクラウド サイトに同時に割り当てないでください。

ステップ 6 スキーマビューの右上隅で、**[保存 (Save)]** をクリックしてスキーマとテンプレートを保存します。

NDFC サイトから VRF とネットワークをインポートする

このセクションでは、既存の NDFC ファブリックから VRF とネットワークをインポートする方法について説明します。

（注） グリーンフィールド構成を定義する場合は、このセクションをスキップして、VRF とネットワークの作成 （112 ページ） の説明に従って新しい VRF とネットワークを作成します。

始める前に

- 前のセクションで説明したように、テンプレートを既存のファブリックに関連付ける必要があります。

ステップ 1 メインペインで **[インポート (Import)]** ボタンをクリックし、インポート元の **[サイト (Site)]** を選択します。

インポートできるのは一度に 1 つのファブリックからなので、ファブリックごとにこれらの手順を繰り返します。

ステップ 2 開いた **[<*site-name*>からのインポート（Import from <site-name>）]** ウィンドウから 1 つまたは複数の VRF またはネットワーク（あるいはその両方）を選択します。

a) インポート画面で、既存のオブジェクトのすべてまたは一部を選択できます。

（注） Nexus Dashboard Orchestrator にインポートするオブジェクトの名前は、すべてのサイトにわたって一意にする必要があります。重複する名前を持つ別のオブジェクトをインポートすると、スキーマ検証エラーとなり、インポートに失敗します。同じ名前のオブジェクトをインポートする必要がある場合は、先に名前を変更してください。

b) 選択したオブジェクトに関連するすべてのオブジェクトもインポートする場合は、**[関係を含める（Include Relations）]** オプションをオンにします。

たとえば、インポートするネットワークを選択した場合、このオプションはそのネットワークに関連付けられた VRF を自動的にインポートします。

c) **[インポート (Import)]** をクリックしてオブジェクトをインポートします。

ステップ 3 このステップを繰り返して、ほかのファブリックから追加の構成をインポートします。

インポートしたサイトの下でテンプレートを選択した場合、そのサイトからインポートされたかのように、スイッチとポート構成がネットワークにすでに作成されています。ただし、同じネットワークが存在する別のファブリックでテンプレートを選択した場合、スイッチ構成は空になります。

インポートしたネットワークのインターフェイス構成を取得するには、他のファブリックから同じネットワークを再度インポートする必要があります。

VRF とネットワークの作成

このセクションでは、既存の NDFC ファブリックから VRF とネットワークを作成する方法について説明します。

（注） NDFC ファブリックから既存の VRF とネットワークをインポートする場合は、このセクションをスキップして、代わりに NDFC サイトから VRF とネットワークをインポートする （111 ページ） で説明されている手順に従ってください。

始める前に

- 前のセクションで説明したように、テンプレートを既存のファブリックに関連付ける必要があります。

ステップ 1 VRF を作成するためのスキーマとコントラクトを選択します。

ステップ 2 VRF を作成します。

a) スキーマ編集ビューで、**[オブジェクトの作成 (Create Object)]** > **[VRF]**を選択します。

b) 右側ペインで、VRF の **[表示名 (Display Name)]** を入力します。

c) （任意）**[VRF ID]** を指定します。

VRF の VNI を指定することも、フィールドを空のままにしておくこともできます。VNI は、インフラの設定：Orchestrator 一般設定（101 ページ）で指定した範囲から NDO によって自動的に割り当てられます。

d) **[VRF プロファイル (VRF Profile)]** ドロップダウンから、VRF プロファイルを選択します。

`Default_VRF_Universal` プロファイルを割り当てるか、NDFC で以前に作成した使用可能な VRF プロファイルを選択できます。NDFC で作成されたプロファイルは自動的に NDO にインポートされ、ここで選択できます。

e) **[VRF 拡張プロファイル (VRF Extension Profile)]** ドロップダウンから、拡張プロファイルを選択します。

`Default_VRF_Extension_Universal` プロファイルを割り当てるか、NDFC で以前に作成した使用可能な VRF 拡張プロファイルを選択できます。NDFC で作成されたプロファイルは自動的に NDO にインポートされ、ここで選択できます。

f) **[ループバックルーティングタグ (Loopback Routing Tag)]** を指定します。

VLAN が複数のサブネットに関連付けられている場合、このタグは各サブネットの IP プレフィックスに関連付けられます。

g) **[直接ルート マップの再配布 (Redistribute Direct Route Map)]** を指定します。

VRF でルートを再配布するためのルート マップ名を指定します。

h) (オプション) **[RT 自動生成の無効化（Disable RT Auto-Generate）]** をオンにして、ルート ターゲットの自動生成を無効にします。

デフォルトで、このオプションがオフになっているときは、ルート ターゲット（RT）がスイッチにより生成され、既存の自動生成されたものに加えて、カスタム RT を生成するように選択できます。このオプションを有効にすると、RT の自動生成が無効になり、カスタム RT のみを使用できます。

i) （オプション）カスタム ルート ターゲットを指定します。

カスタム RT を指定するために、次のフィールドに 1 つ以上の値を入力します。

- **インポート（Import）**：VPN ルート インポート
- **エクスポート（Export）**：VPN ルートのエクスポート用
- **EVPN のインポート（Import EVPN）**：EVPN ルートのインポート用
- **EVPN のエクスポート（Export EVPN）**：EVPN ルートのエクスポート用

有効な値を入力する必要があります（例: `12.2.3.4:2200`）。値を入力すると、UI がその値を検証し、フォーマットが正しくなると、`Create "<value>"` ドロップダウンのオプションが表示されます。

合計で最大 10 個のカスタム ルート ターゲット値を指定できます。

ステップ 3 VRF のサイトローカル プロパティを設定します。

VRF が展開されているすべてのサイトに適用されるネットワークの一般プロパティに加えて、この VRF のサイト固有のプロパティをサイトごとに個別に設定できます。

a) **[テンプレート プロパティ（Template Properties）]** ドロップダウンから、このテンプレートが関連付けられているサイトを選択します。
b) メイン ペインで、ネットワークを選択します。
c) 右側の **[プロパティ (Properties)]** サイドバーで、サイト固有の設定を指定します。

次のサイトローカル プロパティを設定できます。

- **[テナント ルーテッド マルチキャスト (Tenant Routed Multicast)]** をオンにする： テナント ルーテッドマルチキャスト（TRM）は、BGP ベースの EVPN コントロールプレーンを使用する VXLAN ファブリック内でのマルチキャスト転送を有効にします。TRM は、ローカルまたは VTEP 間で同じサブネット内または異なるサブネット内の送信元と受信側の間にマルチテナント対応のマルチキャスト転送を実装します。

  TRMを有効にする場合は、**[RPアドレス (RP Address)]** と **[オーバーレイ マルチキャスト グループ (Overlay Multicast Group)]** も指定する必要があります。

- ランデブーポイント（RP）がファブリックの外部にある場合は、**[RP 外部 (RP External)]** を有効にします。

- **[スタティック リーフの追加 (Add Static Leaf)]** をクリックして、VRF を設定する 1 つ以上のリーフ スイッチを選択します。

  開いた **[スタティック リーフの追加 (Add Static Leaf)]** ウィンドウで、リーフノードを選択します。必要に応じて、VRF の VLAN ID を指定することもできます。

ステップ 4 ネットワークを作成します。

（注） VRF は、NDFC サイトとクラウド ネットワーク コントローラ サイトの両方に関連付けられて拡張されたテンプレートで作成できますが、ネットワークは NDFC サイトにのみ展開できるため、NDFC サイトのみに関連付けられた別のテンプレートで作成する必要があります。

a) テンプレート ビューに戻り、**[オブジェクトの作成（Create Object）]** > **[ネットワーク（Network）]** を選択します。
b) 右側の **[表示名 (Display Name)]** ペインで、ネットワークの名前を入力します。
c) （オプション）**[ネットワーク ID (Network ID)]** を入力します。

ネットワーク ID を指定するか、フィールドを空のままにしておくと、スキーマを保存するときに ID が NDO によって自動的に割り当てられます。

d) これが**[レイヤ 2 専用 (Layer2 Only)]** ネットワークであるかどうかを選択します。
e) **[仮想ルーティングと転送 (Virtual Routing & Forwarding)]** ドロップダウンから、先ほど作成した、ネットワーク用の VRF を選択します。

このオプションは、**[レイヤ 2 専用 (Layer2 Only)]** を有効にした場合は使用できません。

f) **[ネットワーク プロファイル (Network Profile)]** ドロップダウンから、ネットワーク プロファイルを選択します。

Default_Network_Universal プロファイルを割り当てるか、NDFC で以前に作成した使用可能なネットワークプロファイルを選択できます。NDFC で作成されたプロファイルは自動的に NDO にインポートされ、ここで選択できます。

g) **[ネットワーク拡張プロファイル (Network Extension Profile)]** ドロップダウンから、ネットワーク プロファイルを選択します。

Default_Network_Extension_Universal プロファイルを割り当てるか、NDFC で以前に作成した使用可能なネットワーク拡張プロファイルを選択します。NDFC で作成されたプロファイルは自動的に NDO にインポートされ、ここで選択できます。

h) （オプション）ネットワークの **[VLAN ID]** を指定します

i) （オプション）**[VLAN 名 (VLAN Name)]** を指定します。

j) 1 つ以上の**[サブネット (Subnets)]** を追加します。

このオプションは、**[レイヤ 2 専用 (Layer2 Only)]** を有効にした場合は使用できません。

1. **[+ 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 (Add Subnet)**] ウィンドウが開きます。

2. **[+ ゲートウェイ IP の追加 (+ Add Gateway IP)]** をクリックし、サブネットの **[ゲートウェイ IP (Gateway IP)]** アドレスを入力します。

   最大 4 つのゲートウェイ IP を設定できます。

3. 追加する最初のゲートウェイに対して [プライマリ (Primary)] を選択します。

4. ゲートウェイ情報を保存するには、チェックマークをクリックします。

5. 追加のゲートウェイを提供するには、前のサブステップを繰り返します。

6. **[追加 (Add)]** をクリックして、サブネットの追加を終了します。

k) **[ARP の抑制 (Suppress ARP)]** を行うかどうかを選択します。

l) このネットワークの **[MTU]** を指定します。

m) **[ルーティング タグ (Rounting Tag)]** を指定します。

ステップ 5 ネットワークのサイトローカル プロパティを設定します。

ネットワークが展開されているすべてのサイトに適用されるネットワークの一般的なプロパティに加えて、このネットワークのサイト固有のプロパティをサイトごとに個別に設定できます。

a) **[サイト (SITES)]** の下の左側のサイドバーで、VRFが定義されているテンプレートを選択します。

b) メインペインで、[VRF] を選択します。

c) 右側の **[プロパティ (Properties)]** サイドバーで、サイト固有の設定を指定します。

次のサイトローカル プロパティを設定できます。

- **[テナント ルーテッド マルチキャスト (Tenant Routed Multicast)]** をオンにする： テナント ルーテッドマルチキャスト（TRM）は、BGPベースのEVPNコントロールプレーンを使用するVXLANファブリック内でのマルチキャスト転送を有効にします。TRM は、ローカルまたは VTEP 間で同

じサブネット内または異なるサブネット内の送信元と受信側の間にマルチテナント対応のマルチキャスト転送を実装します。

- **[L3ゲートウェイボーダーの有効化 (Enable L3 Gateway Border)]** をオンにして、ボーダー ゲートウェイでレイヤ 3 SVIを有効にし、デュアルアタッチド ホストを接続できるようにします。
- **[DHCP ループバック ID (DHCP Loopback ID)]** を入力します。

  値は `0` ー `1023` の範囲にする必要があります。
- **[+ DHCP サーバーの追加 (+ Add DHCP Server)]** をクリックして、1 つ以上の DHCP リレー サーバーを追加します。

  開いた **[DHCP サーバーの追加 (Add DHCP Server)]** ウィンドウで、DHCP リレーの IP アドレスと所属する VRF を入力します。
- **[+ スタティック ポートの追加 (+ Add Static Port)]** をクリックして、ネットワークの VLAN を接続する 1 つ以上のポートを追加します。

  開いている **[静的ポートの追加（Add Static Port）]** ウィンドウで、ポートを含むリーフ スイッチを選択します。必要に応じて、VLAN ID も指定できます。最後に、**[ポートの追加（Add Port）]** をクリックして、ネットワークの 1 つ以上のポートを指定します。

  異なるリーフ スイッチから複数のスタティック ポートを追加する場合は、リーフ スイッチごとにこのプロセスを繰り返す必要があります。

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。