Cisco Nexus ダッシュボード展開ガイド、リリース 3.7(x)

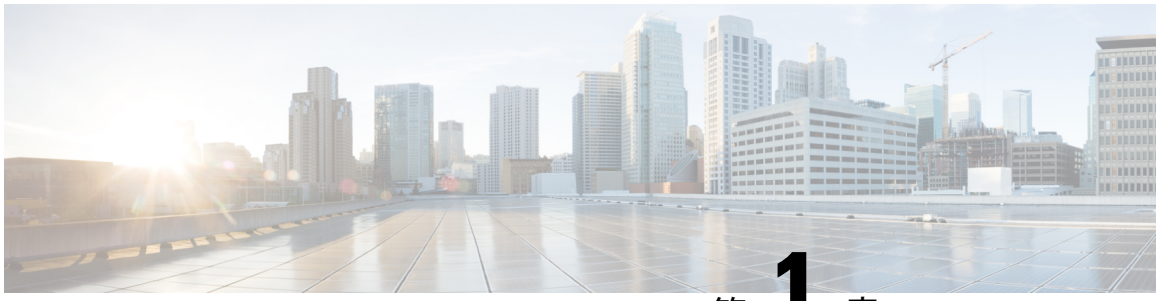
初版：2022 年 3 月 14 日

最終更新：2022 年 4 月 21 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

新規および変更情報

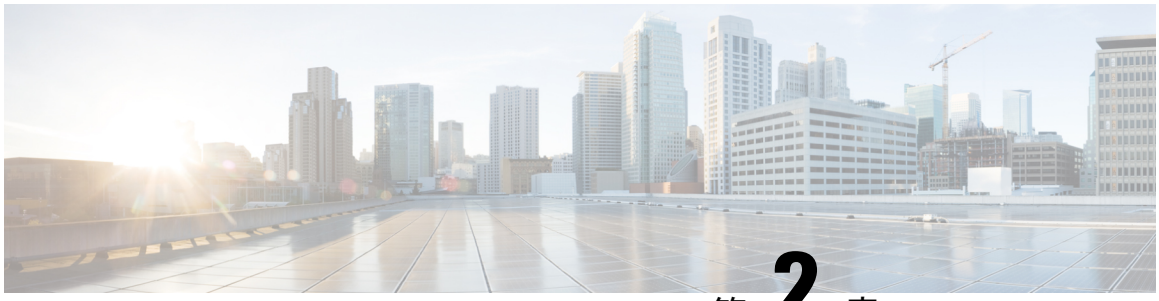
新規および変更情報

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。	--

新規および変更情報



第 2 章

Nexus Dashboard Orchestrator の展開

デプロイ概要

Cisco Nexus Dashboard Orchestrator（NDO）を Cisco Nexus Dashboard のサービスとして展開する必要があります。

（注） リリース 3.2(1) よりも前のリリースからアップグレードする場合は、この項で説明されている導入の概要をよく理解してから、Nexus ダッシュボードへの既存のクラスタの移行 （87 ページ）の手順に従ってください。

Cisco Nexus ダッシュボードは、複数のデータセンターサイト用の中央管理コンソールであり、Nexus Dashboard Orchestrator や Nexus ダッシュボード Insights などのシスコのデータセンターサービスをホストするための共通プラットフォームです。Nexus Dashboard は、これらのマイクロサービスベースのサービスに共通のプラットフォームと最新のテクノロジースタックを提供し、さまざまな最新のサービスのライフサイクル管理を簡素化し、これらのサービスを実行および維持するための運用オーバーヘッドを削減します。

各 Nexus ダッシュボードクラスタは、3 つのマスターノードで構成されます。また、水平スケーリングを有効にするために追加のワーカーノードを展開したり、マスターノードで障害が発生した場合にクラスタを簡単に回復できるようスタンバイ ノードを展開したりすることもできます。

Nexusダッシュボードクラスタの初期導入と設定の詳細については、*Cisco Nexus Dashboard Deployment Guide* を参照してください。

Nexusダッシュボードの使用方法の詳細については、*Cisco Nexus Dashboard User Guide*を参照してください。

このドキュメントでは、Nexus Dashboard Orchestrator サービスの初期インストール要件と手順について説明します。設定および使用例の詳細については、ご使用のリリースの *Cisco Nexus Dashboard Orchestrator Configuration Guide for Cisco ACI* または *Cisco Nexus Dashboard Orchestrator Configuration Guide for Cisco DCNM* および管理するファブリックのタイプに応じた Cisco クラウド APIC の使用例ドキュメントを参照してください。

前提条件とガイドライン

Nexusダッシュボード

ここで説明する追加の要件を満たし、Nexus Dashboard Orchestrator サービスのインストールに進む前に、『*Cisco Nexus Dashboard Deployment Guide*』の説明に従って、Cisco Nexus Dashboard クラスタを展開し、そのファブリック接続を設定する必要があります。

Orchestrator リリース	Nexus Dashboard の最小リリース
リリース 3.7(1) 以降	Cisco Nexus Dashboard、リリース 2.1.1 以降

Nexus Dashboard Orchestrator のイメージ フォーマット

Nexus Dashboard Orchestrator、リリース 3.6(1) 以降で、Orchestrator サービスは新しい `.nap` イメージ形式を使用して配布されます。これにより、サービスは追加機能を提供でき、初期の展開時間を大幅に短縮できます。すべての新しい Nexus Dashboard Orchestrator の展開とリリース 3.6(1) 以降へのアップグレードでは、新しいフォーマットを使用して Nexus Dashboard リリース 2.1.1 以降で展開することを推奨します。

Nexus ダッシュボードのネットワーク

最初に Nexus ダッシュボードを設定するときは、2 つの Nexus ダッシュボード インターフェイスに 2 つの IP アドレスを指定する必要があります。1 つはデータ ネットワークに接続し、もう 1 つは管理ネットワークに接続します。データ ネットワークは、ノードのクラスタリングおよびシスコ ファブリック トラフィックに使用されます。管理ネットワークは、Cisco Nexus ダッシュボードの GUI、CLI、または API への接続に使用されます。

2 つのメジャー インターフェイスは同じサブネットまたは異なるサブネット内に設定できます。また、クラスタ内の異なるノードにまたがる各ネットワークのインターフェイスは、異なるサブネットに属することもできます。

両方のネットワークで、Nexus Dashboard Orchestrator に対して 150ms を超えないラウンドトリップ時間（RTT）でのノード間の接続が必要です。同じ Nexus ダッシュボードクラスタで実行されている他のサービスの RTT 要件は低くなる可能性があります。同じ Nexus ダッシュボードクラスタに複数のサービスを展開する場合は、常に最も低い RTT 要件を使用する必要があります。詳細については、『*Cisco Nexus Dashboard Deployment Guide*』を参照することを推奨します。

Nexus Dashboard Orchestrator アプリ が Nexus ダッシュボードに展開されると、次の表に示すように 2 つのネットワークのそれぞれが異なる目的で使用されます。

NDO トラフィック タイプ	Nexus ダッシュボードのネットワーク
任意の送受信トラフィック： • Cisco APIC • Cisco DCNM • その他のリモート デバイスまたはコントローラ	データ ネットワーク
クラスタ間通信	データ ネットワーク
監査ログ ストリーミング（Splunk/syslog）	管理ネットワーク
リモート バックアップ	管理ネットワーク

Nexus Dashboard クラスタのサイジング

Nexus Dashboard は、サービスの共同ホスティングをサポートします。実行するサービスの種類と数によっては、クラスタに追加のワーカーノードを展開する必要があります。クラスタのサイジング情報と、特定の使用例に基づく推奨ノード数については、『Cisco Nexus Dashboard Capacity Planning』を参照してください。

Nexus Dashboard Orchestrator に加えて他のサービスもホストする予定の場合は、『*Cisco Nexus ダッシュボード ユーザーガイド*』（Nexus Dashboard GUI から直接アクセスも可能）に記載されているように、確実に、クラスタのサイジングツールの推奨事項に基づいて、追加の Nexus ダッシュボードノードを展開して設定するようにしてください。

（注） Nexus Dashboard Orchestrator のこのリリースは、物理または仮想（ESX）Nexus Dashboard クラスタでのみ、他のサービスと共にホストできます。Nexus Dashboard Orchestrator サービスを仮想（KVM）またはクラウド Nexus ダッシュボード クラスタに展開する場合は、同じクラスタに他のサービスをインストールしないでください。

Network Time Protocol（NTP）

Nexus Dashboard Orchestrator はクロックの同期に NTP を使用するため、環境内で NTP サーバを設定する必要があります。

ACI ファブリックのハードウェア要件

スパイン スイッチの要件

Multi-Site では、サイト間接続のために第 2 世代（クラウド スケール）スパイン スイッチが必要です。特定の ACI リリースでサポートされるすべてのクラウド スケール スパイン スイッチは、Multi-Site Orchestrator でサポートされます。

Nexus 9000 第 1 世代スイッチは、Multi-Site サイト間接続ではサポートされていませんが、ファブリックが 5.0(1) より前の APIC リリースを実行している限り、そのファブリック内で引き続き使用できます。

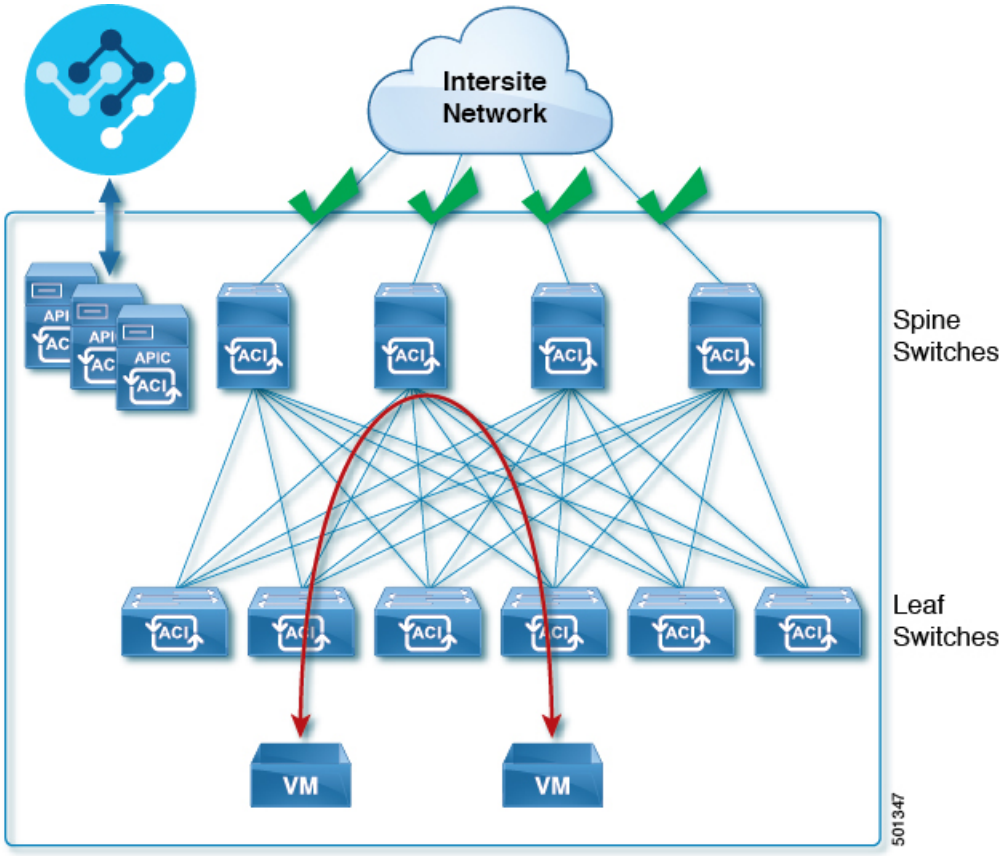
各リリースでサポートされるスパインの完全なリストについては、ACI-mode Switches Hardware Support Matrix を参照してください。

リーフ スイッチの要件

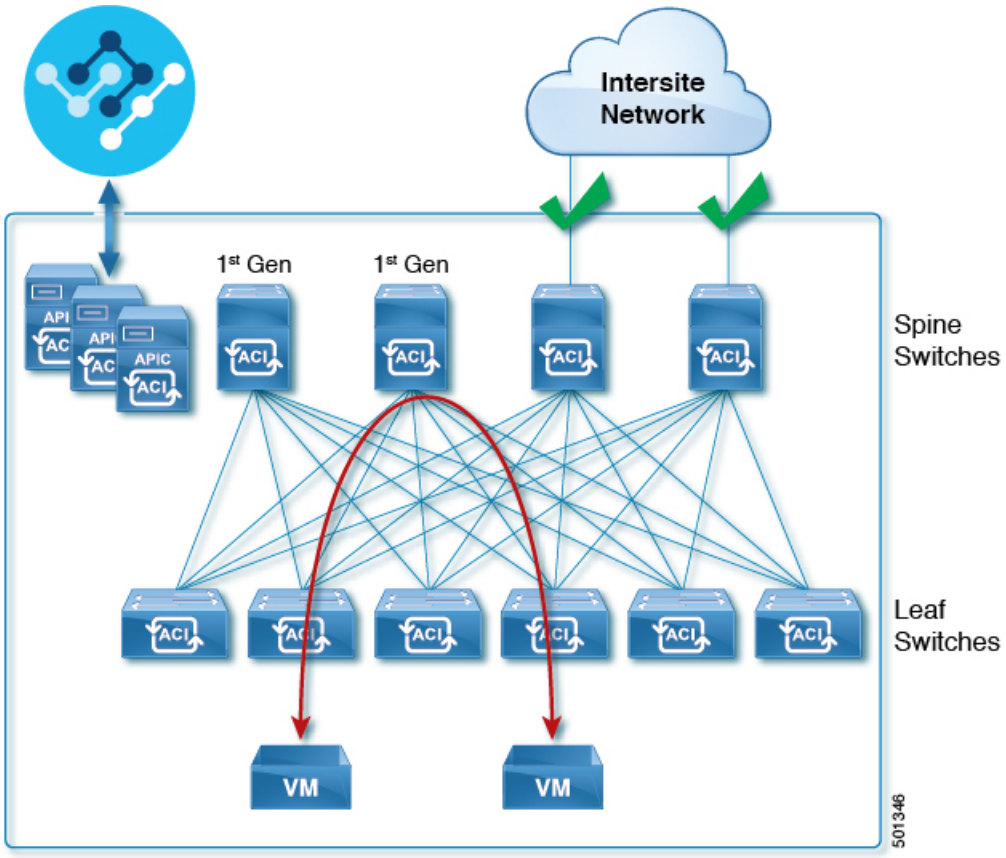
Multi-Site はファブリックのリーフ スイッチに依存しないため、Cisco APIC と同じリーフ スイッチ モデルをサポートします。サポートされているハードウェアの完全なリストは、ACI モード スイッチ ハードウェア サポート マトリックス に記載されています。

サイト間の IPN 接続

次の図は、ACI Multi-Site でサポートされるスパイン スイッチをサイト間ネットワークに接続する方法を示しています。



Multi-Site でサポートされるスパイン スイッチと、同じ Cisco APIC ファブリック内でサポートされないスイッチを混在させることもできますが、次の図に示すように、サポートされるスイッチのみがサイト間ネットワークに接続できます。



DCNM ファブリックのハードウェア要件

ボーダー ゲートウェイの要件

次の表に、EVPN Multi-Site アーキテクチャのハードウェア要件の概要を示します。

- Cisco Nexus 9300 EX プラットフォーム
- Cisco Nexus 9300 FX プラットフォーム
- Cisco Nexus 9300 FX2 プラットフォーム
- Cisco Nexus 9300-GX プラットフォーム
- Cisco Nexus 9332C プラットフォーム
- Cisco Nexus 9364C プラットフォーム
- Cisco Nexus 9500 プラットフォーム（X9700-EX ラインカード装備）
- Cisco Nexus 9500 プラットフォーム（X9700-FX ラインカード装備）

VXLAN BGP EVPN サイトのサイト内部 BGP ルートリフレクタ（RR）および VTEP のハードウェア要件は、EVPN マルチサイト ボーダー ゲートウェイ（BGW）がない場合と同じです。

このドキュメントでは、VXLAN EVPN サイト内部ネットワークのハードウェア要件とソフトウェア要件については説明しません。

App Storeを使用した Nexus Dashboard Orchestrator サービスのインストール

ここでは、Cisco Nexus Dashboard Orchestrator サービスを既存の Cisco Nexus ダッシュボード クラスタにインストールする方法について説明します。

始める前に

- 前提条件とガイドライン （4 ページ） に記載されている要件とガイドラインを満たしていることを確認します。
- Cisco DC App Center は、管理ネットワークを介して直接、またはプロキシ設定を使用して Nexus Dashboard から到達可能である必要があります。Nexus Dashboard のプロキシ設定については、『*Nexus Dashboard User Guide*』を参照してください。

  DC App Center への接続を確立できない場合は、このセクションをスキップして、Nexus Dashboard Orchestrator サービスの手動インストール （9 ページ） の手順に従ってください。
- App Store では、サービスの最新バージョンのみをインストールできます。

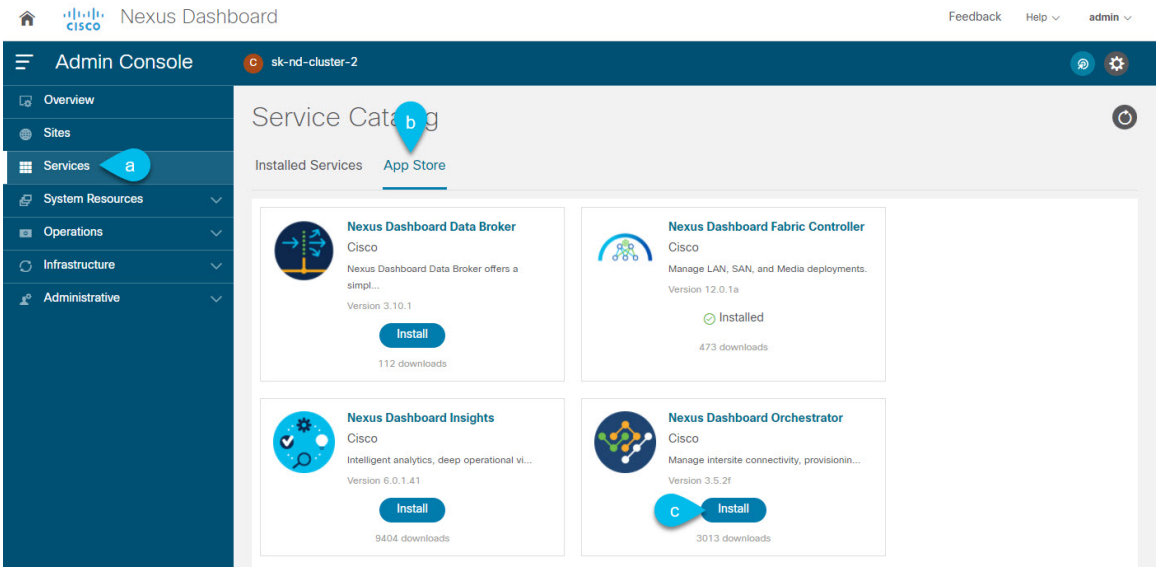
  リリース 3.3(1) より前のバージョンをインストールする場合は、使用可能な展開オプションと手順について、そのリリースに固有の『*Nexus Dashboard Orchestrator Installation Guide*』を参照してください。

ステップ 1 Nexus Dashboard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、**[管理コンソール（Admin Console）]** を選択します。

サービスを展開するには、`admin` 権限が必要です。

ステップ 3 App Store に移動し、Nexus Dashboard Orchestrator アプリを選択します。



a) 左のナビゲーションメニューから **[サービス カタログ (Service Catalog)]** を選択します。

b) **[アプリ ストア (App Store)]** タブを選択します。

c) [Nexus Dashboard Orchestrator] タイルで、**[インストール (Install)]** をクリックします。

ステップ 4 開いた [ライセンス契約 (License Agreement)] ウィンドウで、**[同意してダウンロード (Agree and Download)]** をクリックします。

ステップ 5 サービスが Nexus Dashboard にダウンロードされ、展開されるまで待ちます。

ステップ 6 アプリケーションを有効にします。

インストールが完了した後、デフォルトではサービスは [無効 (Disabled)] 状態のままであるため、有効にする必要があります。

アプリを有効にするには、アプリの **[...]**メニューをクリックし、**[有効 (Enable)]** を選択します。

ステップ 7 アプリを起動します。

アプリを起動するには、Nexus ダッシュボードの **[サービスカタログ (Service Catalog)]** ページのサービスタイルで **[開く (Open)]** をクリックします。

シングルサインオン（SSO）機能を使用すると、Nexus Dashboard で使用したものと同じクレデンシャルを使用してサービスにログインできます。

Nexus Dashboard Orchestrator サービスの手動インストール

ここでは、Cisco Nexus Dashboard Orchestrator サービスを手動で既存の Cisco Nexus ダッシュボード クラスタにアップロードし、インストールする方法について説明します。

始める前に

- 前提条件とガイドライン （4 ページ） に記載されている要件とガイドラインを満たしていることを確認します。

ステップ 1 Cisco Nexus Dashboard Orchestrator イメージをダウンロードします。

a) DC App Center で Nexus Dashboard Orchestrator ページを参照します。
https://dcappcenter.cisco.com/nexus-dashboard-orchestrator.html

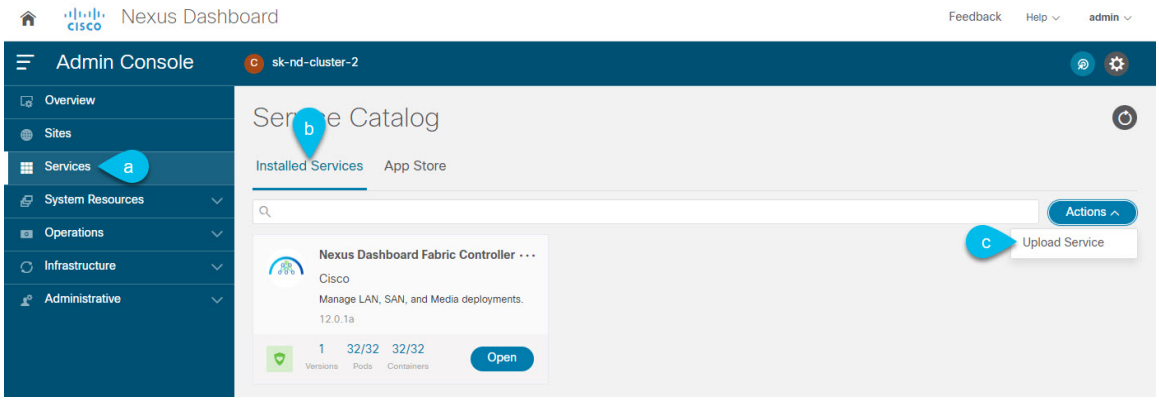
b) **[バージョン (Version)]** ドロップダウンから、インストールするバージョンを選択し、**[ダウンロード (Download)]** をクリックします。

c) **[同意してダウンロード (Agree and download)]** をクリックしてライセンス契約に同意し、イメージをダウンロードします。

ステップ 2 Cisco Nexus Dashboard にログインします。

サービスを展開する場合、Nexus ダッシュボードノードの 1 つだけにインストールしてください。サービスはクラスタ内の他のノードに自動的に複製されます。その際、管理 IP アドレスを使用して、Nexus ダッシュボード ノードのどれにでもログインできます。

ステップ 3 画像を手動でアップロードすることを選択します。



a) 左のナビゲーションバーで、**[サービス カタログ (Service Catalog)]** をクリックします。

b) **[インストール済みサービス (Installed Services)]** タブをクリックします。

c) メインペインの右上にある**[アクション (Actions)]**>**[サービスのアップロード (Upload Service)]**をクリックします。

ステップ 4 アップロードする画像ファイルを選択してください。

a) イメージの場所を選択します。

サービス画像をシステムにダウンロードした場合は、**[ローカル (Local)]** を選択します。

サーバでイメージをホストしている場合は、**[リモート (Remote)]** を選択します。

b) ファイルを選択します。

前のサブステップで **[ローカル (Local)]** を選択した場合は、**[ファイルの選択 (Select File)]** をクリックし、ダウンロードした画像を選択します。

[リモート（Remote）] を選択した場合は、イメージ ファイルのフル URL を指定します。たとえば、`http://<ip-address>:<port>/<full-path>/cisco-mso-<version>.nap` のようになります。

c) **[アップロード (Upload)]** をクリックして、サービスをクラスタに追加します。

ステップ 5 サービスが Nexus Dashboard にダウンロードされ、展開されるまで待ちます。

ステップ 6 サービスを有効化します。

インストールが完了した後、デフォルトではサービスは `[無効 (Disabled)]` 状態のままであるため、有効にする必要があります。

サービスを有効にするには、**[...]** メニューをクリックし、**[有効 (Enable)]** を選択します。

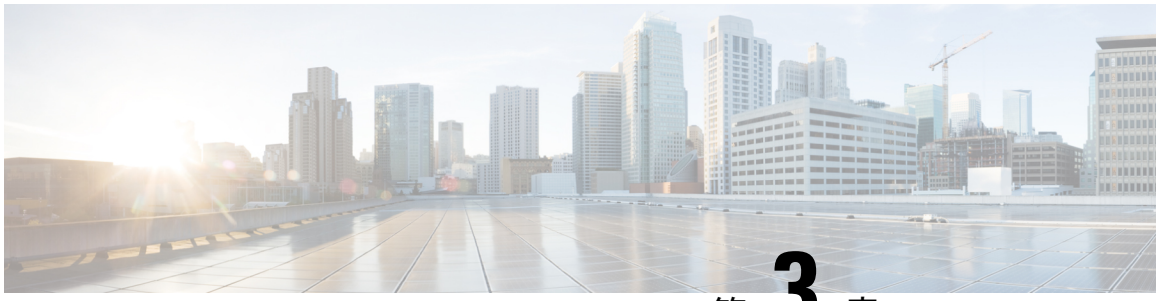
ステップ 7 サービスを開始します。

アプリを起動するには、Nexus ダッシュボードの **[サービスカタログ (Service Catalog)]** ページのサービス タイルで **[開く (Open)]** をクリックします。サービス

シングル サインオン（SSO）機能を使用すると、Nexus Dashboard で使用したものと同じクレデンシャルを使用してサービスにログインできます。

第 I 部

ACI ファブリックの Day-0 オペレーション



第 3 章

Cisco ACI サイトの設定

ポッド プロファイルとポリシー グループ

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

ステップ 1 サイトの APIC GUI にログインします。

ステップ 2 ポッド プロファイルにポッド ポリシー グループが含まれているかどうかを確認します。

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

ステップ 3 必要であれば、ポッド ポリシー グループを作成します。

a) **[ファブリック (Fabric)]** > **[ファブリック ポリシー (Fabric Policies)]** > **[ポッド (Pods)]** > **[ポリシー グループ (Policy Groups)]**に移動します。

b) **[ポリシー グループ (Policy Groups)]** を右クリックし、**[ポッド ポリシー グループの作成 (Create Pod Policy Groups)]** を選択します。

c) 適切な情報を入力して、[Submit] をクリックします。

ステップ 4 新しいポッド ポリシー グループをデフォルトのポッド プロファイルに割り当てます。

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

b) デフォルトのプロファイルを選択します。

c) 新しいポッド ポリシー グループを選択し、**[更新 (Update)]** をクリックします。

すべての APIC サイトのファブリック アクセス ポリシーの設定

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

ファブリック アクセス グローバル ポリシーの設定

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

ステップ 1 サイトの APIC GUI に直接ログインします。

ステップ 2 メイン ナビゲーション メニューから、**[ファブリック (Fabric)]** > **[アクセス ポリシー (Access Policies)]** を選択します。

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

ステップ 3 VLAN プールを指定します。

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

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

b) **[VLAN]** カテゴリを右クリックし、**[VLAN プールの作成 (Create VLAN Pool)]** を選択します。

[**VLAN プールの作成 (CREATE VLAN Pool)**] ウィンドウで、次の項目を指定します。

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

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

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

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

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

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

インターフェイスなどの追加の変更は必要ありません。

ステップ 5 ドメインを設定します。

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

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

b) [**外部ルーテッド ドメイン(External Routed Domains)**] カテゴリを右クリックし、[**レイヤ 3 ドメインの作成 (Create Layer 3 Domain)**] を選択します。

[**レイヤ 3 ドメインの作成 (Create Layer 3 Domain)**] ウィンドウで、次の項目を指定します。

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

c) [**送信 (Submit)**] をクリックします。

セキュリティ ドメインなどの追加の変更は必要ありません。

次のタスク

グローバル アクセス ポリシーを設定した後も、ファブリック アクセス インターフェイス ポリシーの設定 （17 ページ） の説明に従って、インターフェイス ポリシーを追加する必要があります。

ファブリック アクセス インターフェイス ポリシーの設定

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

始める前に

サイトの APIC では、ファブリック アクセス グローバル ポリシーの設定 （16 ページ） の説明に従って、VLAN プール、AEP、および ドメインなどのグローバル ファブリック アクセス ポリシーを設定しておく必要があります。

ステップ 1 サイトの APIC GUI に直接ログインします。

ステップ 2 メイン ナビゲーション メニューから、**[ファブリック (Fabric)]** > **[アクセス ポリシー (Access Policies)]** を選択します。

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

ステップ 3 スパイン ポリシー グループを設定します。

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

これは、ベアメタル サーバを追加する方法と類似していますが、リーフ ポリシー グループの代わりにスパイン ポリシー グループを作成する点が異なります。

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

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

- **[名前 (Name)]** フィールドの場合、ポリシー グループの名前を指定します。たとえば `Spine1-PolGrp` です。
- [**リンク レベル ポリシー (Link Level Policy)**] フィールドには、スパイン スイッチと ISN の間のリンク ポリシーを指定します。
- **[CDP ポリシー (CDP Policy)]** の場合、CDP を有効にするかどうかを選択します。
- **[添付したエンティティ プロファイル (Attached Entity Profiel)]**の場合、前のセクションで設定した AEP を選択します。たとえば `msite-aep` です。

c) [**送信 (Submit)**] をクリックします。

セキュリティ ドメインなどの追加の変更は必要ありません。

ステップ 4 スパイン プロファイルを設定します。

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

b) **[プロファイル (Profiles)]** カテゴリを右クリックし、**[スパイン インターフェイス プロファイルの作成 (Create Spine Interface Profile]** を選択します。

[スパイン インターフェイス プロファイルの作成 (Create Spine Interface Profile)] ウィンドウで、次のとおり指定します。

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

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

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

ステップ 5 スパイン スイッチ セレクター ポリシーを設定します。

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

b) **[スパイン プロファイル (Spine Profiles)[** カテゴリを右クリックし、**[スパイン プロファイルの作成 (Create Spine Profile)]** を選択します。

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

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

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

d) **[次へ (Next)]** をクリックして、次の画面に進みます。

e) 前の手順で作成したインターフェイス プロファイルを選択します。

たとえば、`Spine1-ISN`などです。

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

リモート リーフ スイッチを含むサイトの設定

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

リモート リーフの注意事項と制限事項

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

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

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

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

  各 APIC ノードのルーティング可能な IP アドレスは、**[ルーティング可能 IP (Routable IP)]** フィールド (APIC GUI の **[システム (System)]** > **[コントローラ (Controllers)]** > **<コントローラ名>**画面) に表示されます。

リモート リーフ スイッチのルーティング可能なサブネットの設定

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

ステップ 1 サイトの APIC GUI に直接ログインします。

ステップ 2 メニュー バーから、**[ファブリック (Fabric)]** > **[インベントリ (Inventory)]** を選択します。

ステップ 3 [ナビゲーション (Navigation)] ウィンドウで、**[ポッド ファブリック セットアップ ポリシー (Pod Fabric Setup Policy)]** をクリックします。

ステップ 4 メイン ペインで、サブネットを設定するポッドをダブルクリックします。

ステップ 5 **ルーティング可能なサブネット**エリアで、 **+** 記号をクリックしてサブネットを追加します。

ステップ 6 **IP**アドレスと**予約アドレスの数**を入力し、状態をアクティブまたは非アクティブに設定してから、**[更新 (Update)]** をクリックしてサブネットを保存します。

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

ステップ 7 [送信（Submit）] をクリックして設定を保存します。

リモート リーフ スイッチの直接通信の有効化

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

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

ステップ 1 サイトの APIC に直接ログインします。

ステップ 2 リモート リーフ スイッチの直接トラフィック転送を有効にします。

a) メニュー バーから、**[システム (System)]** > **[システムの設定 (System Settings)]** に移動します。

b) 左側のサイドバーのメニューから **[ファブリック全体の設定 (Fabric Wide Setting)]** を選択します。

c) **[リモート リーフ 直接トラフィック転送 (Enable Remote Leaf Direct Traffice Forwarding)]** チェックボックスをオンにします。

（注） 有効にした後は、このオプションを無効にすることはできません。

d) **[送信 (Submit)]** をクリックして変更を保存します。

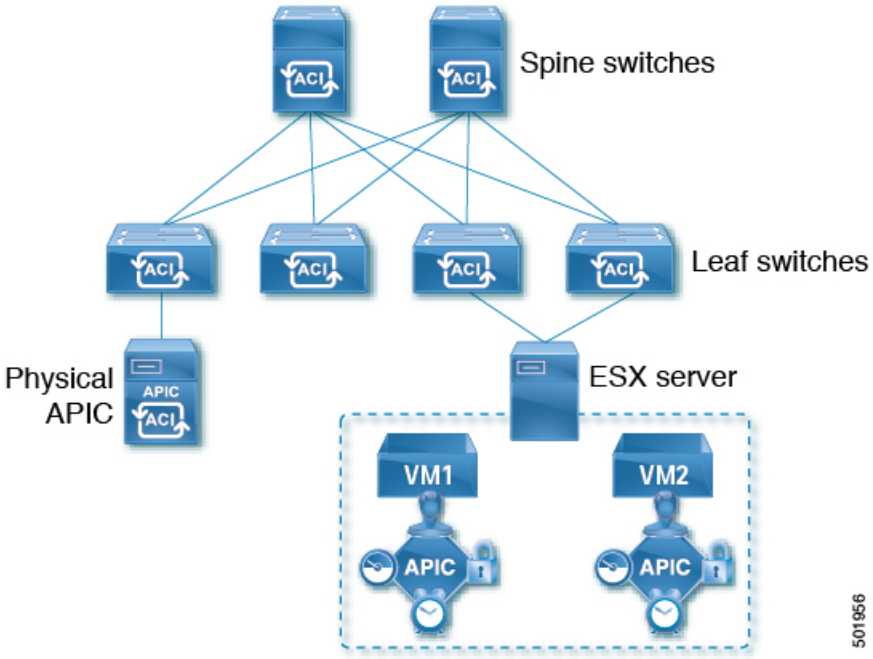
Cisco Mini ACI ファブリック

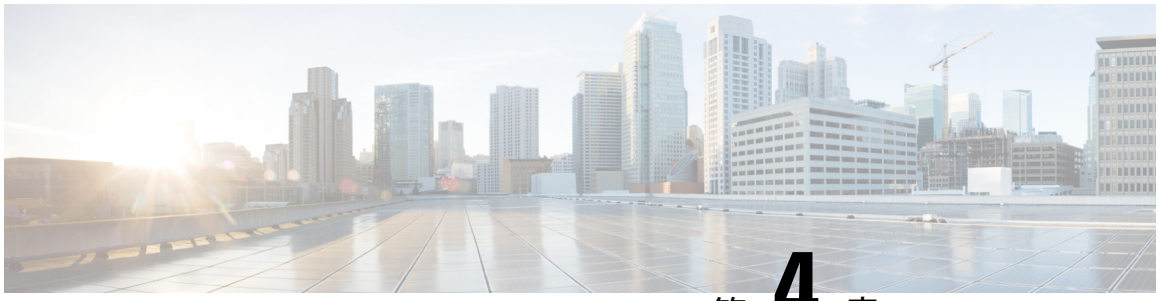
Cisco Multi-Site は、追加の設定を必要とせずに、一般的なオンプレミス サイトとして Cisco Mini ACI ファブリックをサポートします。ここでは、Mini ACI ファブリックの概要について説明します。このタイプのファブリックの導入と設定に関する詳細情報は、『*Cisco Mini ACI ファブリックおよび仮想 APIC*』に記述されています。

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

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

図 *1 : Cisco Mini ACI* ファブリック





第 4 章

サイトの追加と削除

Cisco NDO と APIC の相互運用性のサポート

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

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

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

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

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

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

機能	最小バージョン
ACI マルチポッドのサポート	リリース 4.2(4)
サービス グラフ (L4 ~ L7 サービス)	リリース 4.2(4)
外部 EPG	リリース 4.2(4)
ACI 仮想エッジ VMM のサポート	リリース 4.2(4)
DHCP Support	リリース 4.2(4)
整合性チェッカー	リリース 4.2(4)
vzAny	リリース 4.2(4)
ホストベースのルーティング	リリース 4.2(4)
CloudSec 暗号化	リリース 4.2(4)
レイヤ 3 マルチキャスト	リリース 4.2(4)
OSPF の MD5 認証	リリース 4.2(4)
EPG 優先グループ	リリース 4.2(4)
サイト内 L3Out	リリース 4.2(4)
QoS の優先順位	リリース 4.2(4)
コントラクト QoS 優先順位	リリース 4.2(4)
シングル サインオン（SSO）	リリース 5.0(1)
マルチキャスト ランデブー ポイント（RP）のサポート	リリース 5.0(1)
AWS および Azure サイトのトランジット ゲートウェイ（TGW）サポート	リリース 5.0(1)
SR-MPLS サポート	リリース 5.0(1)
クラウド ロードバランサ 高可用性ポート	リリース 5.0(1)

機能	最小バージョン
UDR を使用したサービスグラフ（L4-L7 サービス）	Release 5.0(2)
クラウドでのサードパーティデバイスのサポート	Release 5.0(2)
クラウドロードバランサのターゲット接続モード機能	Release 5.1(1)
Express Route 経由で到達可能な非 ACI ネットワークの Azure でのセキュリティおよびサービス挿入サポート	Release 5.1(1)
CSR プライベート IP サポート	Release 5.1(1)
Azure のクラウド ネイティブ サービスの ACI ポリシー モデルと自動化の拡張	Release 5.1(1)
Azure の単一 VNET 内での複数の VRF サポートによる柔軟なセグメンテーション	Release 5.1(1)
Azure PaaS および サードパーティ サービスのプライベート リンク自動化	Release 5.1(1)
ACI-CNI を使用した Azure での OpenShift 4.3 IPI	Release 5.1(1)
クラウド サイト アンダーレイの設定	リリース 5.2(1)

Cisco ACI サイトの追加

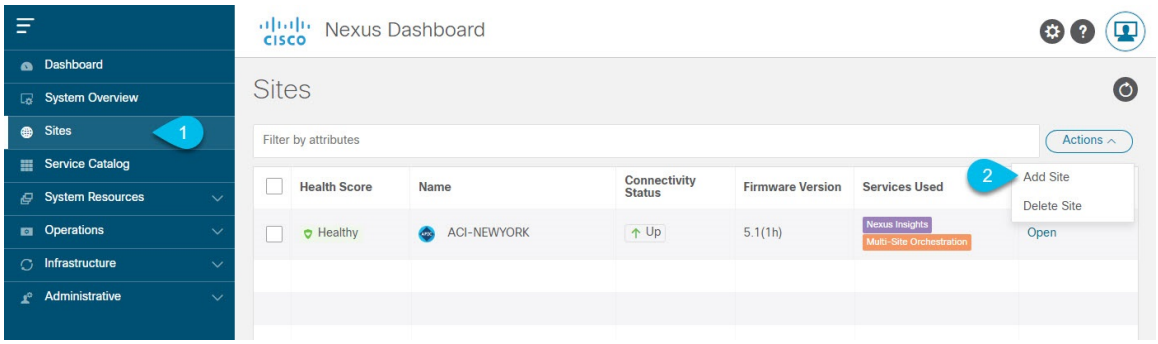
ここでは、Nexus Dashboard GUI を使用して Cisco APIC または Cloud APIC サイトを追加し、そのサイトを Nexus Dashboard Orchestrator で管理できるようにする方法について説明します。

始める前に

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

ステップ 1 Nexus ダッシュボード GUI にログインします。

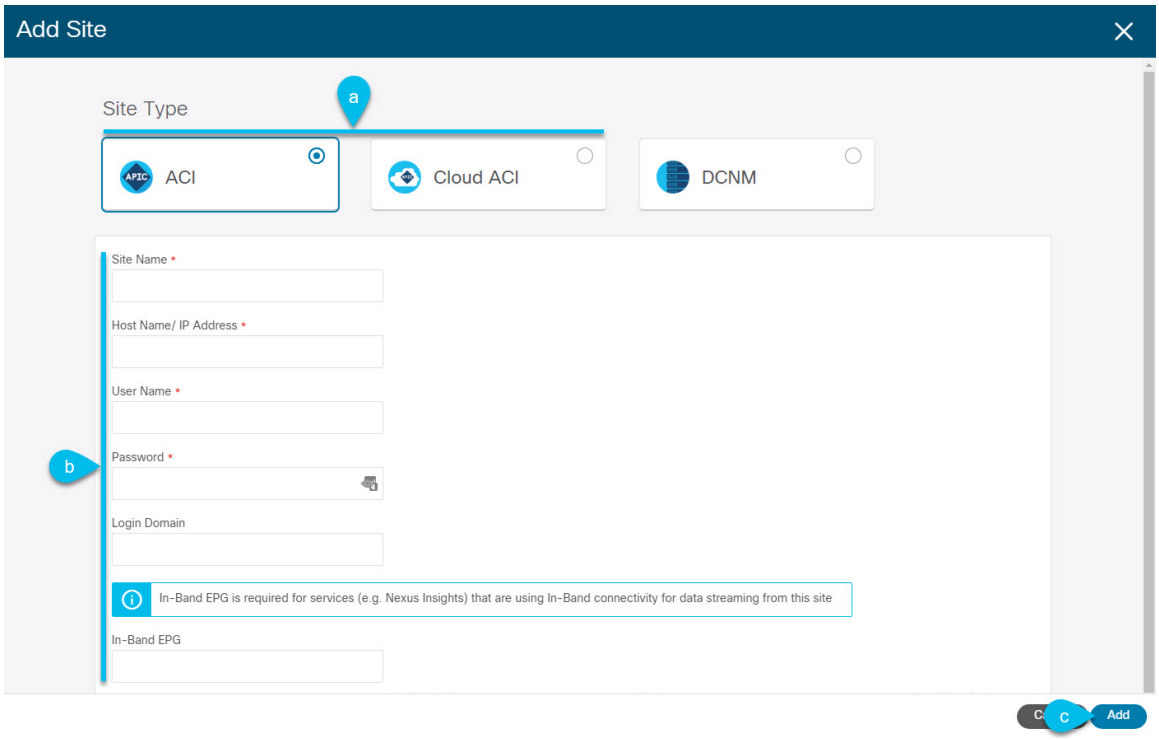
ステップ 2 新サイトを追加します。



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

b) メインペインの右上にある**[アクション (Actions)]** > **[サイトの追加 (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、追加する ACI ファブリックのタイプに応じて **[ACI]** または **[クラウド ACI (Cloud ACI)]** を選択します。

b) コントローラ情報を入力します。

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

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

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

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

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

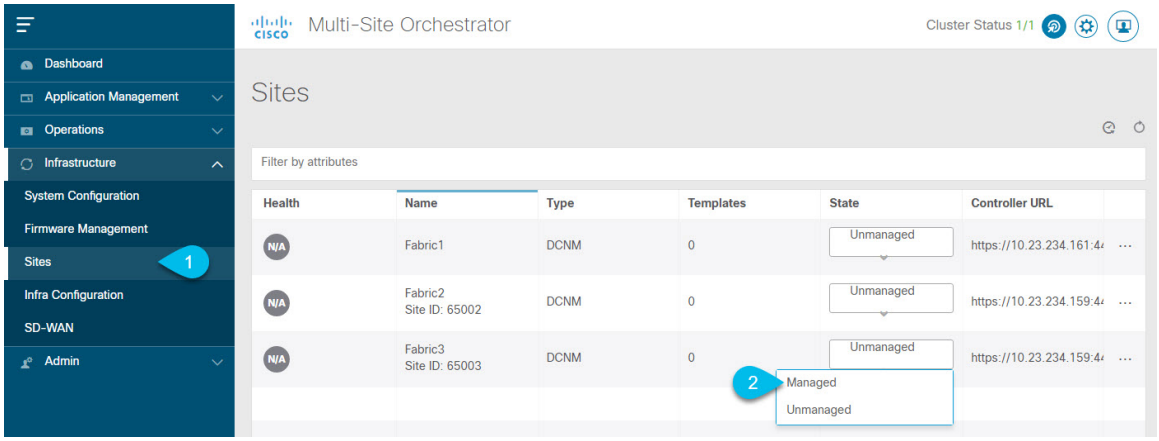
この時点で、サイトは Nexus ダッシュボードで使用できるようになりますが、次の手順で説明するように、Nexus Dashboard Orchestrator の管理用にそれらのサイトを有効にする必要があります。

ステップ 4 他のサイトに対して上記の手順を繰り返します。

ステップ 5 Nexus ダッシュボードの **[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。

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。

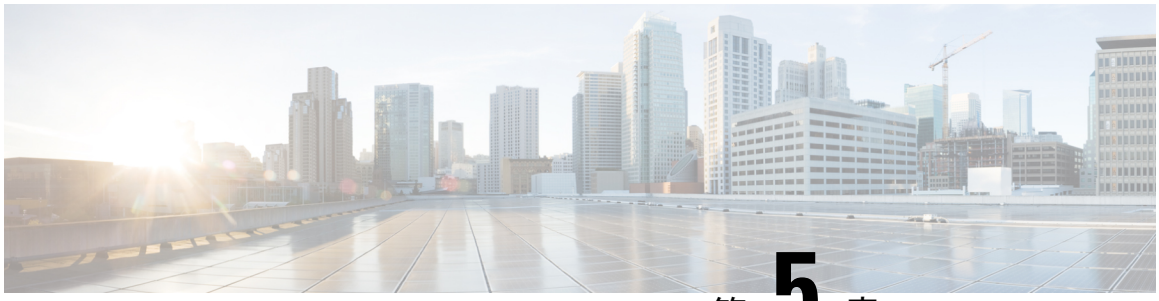
Nexus ダッシュボードからサイトが削除されます。

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。



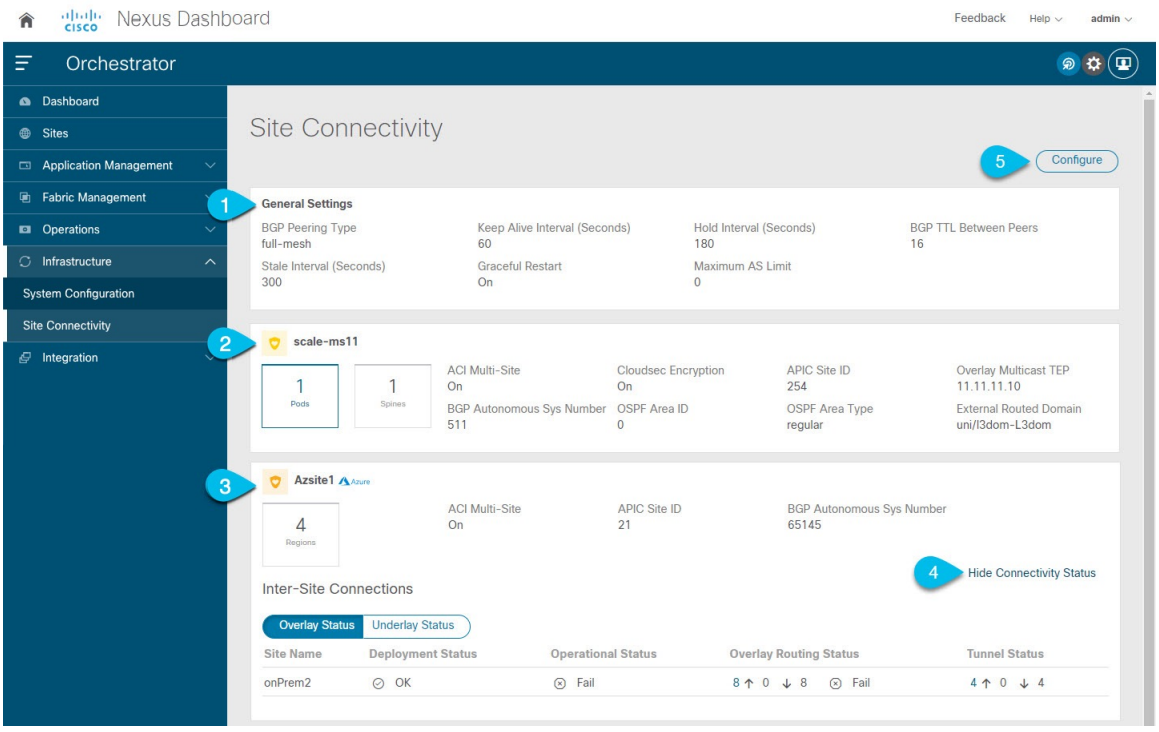
第 5 章

インフラ一般設定

インフラ設定ダッシュボード

[インフラ設定 (Infra Configuration)] ページには、Nexus Dashboard Orchestrator 展開環境のすべてのサイトとサイト間接続の概要が表示されます。

図 *2:* インフラ設定の概要



1. **[全般設定 (General Settings)]** タイルには、BGP ピアリング タイプとその設定に関する情報が表示されます。

   詳細については、次のセクションで説明します。

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

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

   詳細については、Cisco APIC サイトのインフラの設定 （39 ページ）を参照してください。

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

   詳細については、Cisco Cloud APIC サイトのインフラの設定 （47 ページ）を参照してください。

4. **[接続ステータスの表示]** をクリックして、特定のサイトのサイト間接続の詳細を表示できます。

5. **[構成]** ボタンを使用して、サイト間接続構成に移動できます。これについては、次のセクションで詳しく説明します。

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

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

加えて、スパイン スイッチの追加や削除、またはスパイン ノード ID の変更などのインフラストラクチャの変更には、一般的なインフラの設定手順の一部として、サイト接続性情報の更新 （39 ページ） に記載されているような、 Nexus Dashboard Orchestrator のファブリック接続情報の更新が必要です。

パーシャル メッシュ サイト間接続

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

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

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

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

パーシャル メッシュ接続のガイドライン

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

- パーシャル メッシュ接続は、2 つのクラウドサイト間、またはクラウドとオンプレミスのサイト間でサポートされています。

  すべてのオンプレミス サイト間で完全なメッシュ接続が自動的に確立されます。

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

  ただし、テンプレートのストレッチは、BGP-EVPN プロトコルを使用して接続されているサイトに対してのみ許可されることに注意してください。BGP-IPv4 を使用して 2 つ以上のサイトを接続している場合、それらのサイトのいずれかに割り当てられたテンプレートは、1 つのサイトにのみ展開できます。

インフラの設定: 一般設定

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

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

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。

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

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

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

c) **[キープアライブ間隔 (秒) (Keepalive Interval (Seconds))]** フィールドに、キープアライブ間隔を秒単位で入力します。

デフォルト値を維持することを推奨します。

d) **[保留間隔 (秒) (Hold Interval (Seconds))]** フィールドに、保留間隔を秒単位で入力します。

デフォルト値を維持することを推奨します。

e) **[失効間隔 (秒) (Stale Interval (Seconds))]** フィールドに、失効間隔を秒単位で入力します。

デフォルト値を維持することを推奨します。

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

g) **[AS 上限（Maximum AS Limit）]**を入力します。

デフォルト値を維持することを推奨します。

h) **[ピア間のBGP TTL（BGP TTL Between Peers）]** を入力します。

デフォルト値を維持することを推奨します。

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

クラウド APIC サイトがない場合、このフィールドは UI に表示されません。

これは、以前の Nexus Dashboard Orchestrator リリースでサイト間接続用にクラウド APIC で以前に設定した、オンプレミス IPN ピアリング用のクラウドサイトで使用される OSPF エリア ID です。

ステップ 6 **[IPN デバイス情報]** を入力します。

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

後のセクションで説明するように、オンプレミスとクラウドサイト間のサイトアンダーレイ接続を設定する場合は、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、オンプレミスサイトの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。詳細はインフラの設定: オンプレミス サイトの設定 （40 ページ）を参照してください。

a) **[デバイス (Devices)]** タブを選択します。

b) **[IPN デバイスの追加 (Add IPN Device)]** をクリックします。
c) IPN デバイスの **[名前（Name）]** と **[IPアドレス（IP Address）]** を入力します。

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 APIC の CSR からのトンネル ピア アドレスとして使用されます。

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

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

クラウド APIC サイトがない場合、このタブは UI に表示されません。

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

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

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

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

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

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

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

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

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

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

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

クラウド APIC サイトがない場合、このタブは UI に表示されません。

ここで指定できるサブネットプールには、次の 2 つのタイプがあります。

- **外部サブネット プール**：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クラウド APIC 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。

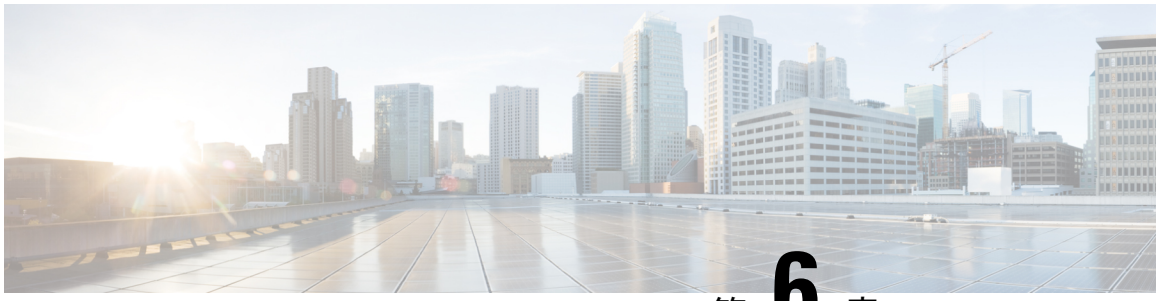
e) チェックマーク アイコンをクリックして、サブネット情報を保存します。

   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。

次のタスク

全般的なインフラ設定を構成した後も、管理するサイトのタイプ（オンプレミスACI、クラウドACI、またはオンプレミスファブリック）に基づいて、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。



第 6 章

Cisco APIC サイトのインフラの設定

サイト接続性情報の更新

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

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 （オプション）オンプレミス サイトの場合、廃止されたスパイン スイッチノードの設定を削除する場合は、**[確認 (Confirmation)]** ダイアログでチェックボックスをオンにします。

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

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。

インフラの設定: オンプレミス サイトの設定

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

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、特定のオンプレミス サイトを選択します。

ステップ 5 **[サイト間接続（Inter-Site Connectivity）]** 情報を入力します。

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

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

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

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

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

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

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

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

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

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

サイトと IPN 間のアンダーレイ接続に OSPF プロトコルを使用する場合は、次の設定が必要です。代わりに BGP を使用する場合は、この手順を省略できます。BGP アンダーレイの設定は、インフラの設定: スパイン スイッチ （43 ページ）で説明されているように、ポート レベルで行われます。

g) ドロップダウン メニューから **[OSPF エリア タイプ (OSPF Area Type)]**を選択します。

サイトと IPN 間のアンダーレイ接続に OSPF プロトコルを使用する場合は、次の設定が必要です。代わりに BGP を使用する場合は、この手順を省略できます。BGP アンダーレイの設定は、インフラの設定: スパイン スイッチ （43 ページ）で説明されているように、ポート レベルで行われます。

OSPF エリアタイプは、次のいずれかになります。

- `nssa`
- `regular`

h) サイトの OSPF ポリシーを設定します。

サイトと IPN 間のアンダーレイ接続に OSPF プロトコルを使用する場合は、次の設定が必要です。代わりに BGP を使用する場合は、この手順を省略できます。BGP アンダーレイの設定は、インフラの設定: スパイン スイッチ （43 ページ）で説明されているように、ポート レベルで行われます。

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

- **[ポリシー名（Policy Name）]** フィールドにポリシー名を入力します。
- **[(ネットワーク タイプ (Network Type)]** フィールドで、`[ブロードキャスト (broadcast)]`、`[ポイントツーポイント (point-to-point)]`、または `[未指定 (unspecified)]` のいずれかを選択します。

  デフォルトは `[ブロードキャスト (broadcast)]` です。
- **[優先順位 (Priority)]** フィールドに、優先順位番号を入力します。

  デフォルトは `1` です。
- **[インターフェイスのコスト (Cost of Interface)]** フィールドに、インターフェイスのコストを入力します。

  デフォルト値は `0` です。
- **[インターフェイス コントロール(Interface Controls)]** ドロップダウン メニューで、以下のいずれかを選択します。
  - **アドバタイズサブネット (advertise-subnet)**
  - **BFD (bfd)**
  - **MTU 無視 (mtu-ignore)**
  - **受動的参加 (passive-participation)**
- **[Hello 間隔 (秒) (Hello Interval (Seconds))]** フィールドに、hello 間隔を秒単位で入力します。

  デフォルト値は `10` です。
- **[Dead 間隔 (秒) (Dead Interval (Seconds))]** フィールドに、dead 間隔を秒単位で入力します。

  デフォルト値は `40` です。
- **[再送信間隔 (秒) (Retransmit Interval (Seconds))]** フィールドに、再送信間隔を秒単位で入力します。

  デフォルト値は `5` です。
- **[転送遅延 (秒) (Transmit Delay (Seconds))]** フィールドに、遅延を秒単位で入力します。

  デフォルトは `1` です。

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

Cisco APIC GUI で作成した外部ルータ ドメインを選択します。使用している APIC リリースに固有の詳細については、『*Cisco APIC Layer 3 Networking Configuration Guide*』を参照してください。

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

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

サイトの SDA 接続を有効にする場合は、『*Cisco Multi-Site Configuration Guide for ACI Fabrics*』の「SDA 使用例」の章で説明されている追加構成を行う必要があります。

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

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

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

デフォルトの範囲は `16000 ～ 23999` です。

サイトのMPLS接続を有効にする場合は、『*Cisco Multi-Site Configuration Guide for ACI Fabrics*』の「Sites Connected via SR-MPLS」の章で説明されている追加設定を行う必要があります。

ステップ 6 オンプレミスとクラウド サイト間のサイト間接続を設定します。

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

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

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

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

IPNデバイスは、**[一般設定 (General Settings)]** > **[IPN デバイス (IPN Devices)]**リストですでに定義されている必要があります。インフラの設定: 一般設定 （33 ページ）を参照してください。

c) クラウド サイトのサイト間接続を設定します。

クラウドサイトからこのオンプレミス サイトへの以前に設定された接続はすべてここに表示されますが、追加の設定は、Cisco Cloud APIC サイトのインフラの設定 （47 ページ）の説明に従ってクラウド サイト側から行う必要があります。

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 （51 ページ）の説明に従って、設定を展開する必要があります。

インフラの設定: ポッドの設定

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

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、ポッドを選択します。

ステップ 6 右の **[ポッドのプロパティ (Pod Properties)]** ペインで、ポッドについてオーバーレイ ユニキャスト TEP を追加できます。

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

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

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

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

ステップ 8 サイトの各ポッドに対してこの手順を繰り返します。

インフラの設定: スパイン スイッチ

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

リリース 3.5(1) より前は、OSPF プロトコルを使用してアンダーレイ接続が確立されていました。一方、このリリースでは、OSPF、BGP（IPv4 のみ）、または混合プロトコルを使用できます。混合とは、一部のサイトではサイト間アンダーレイ接続に OSPF を使用し、一部のサイトでは BGP を使用することです。両方ではなく OSPF または BGP のいずれかを設定すること

を推奨します。両方のプロトコルを設定した場合には、BGP が優先され、OSPF はルートテーブルにインストールされません。

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、特定のオンプレミス サイトを選択します。

ステップ 5 メイン ペインで、ポッド内のスパイン スイッチを選択します。

ステップ 6 右側の **[<スパイン> 設定 (Settings)]** ペインで、**[+ ポート追加(Add Port)]** をクリックします。

ステップ 7 **[ポートの追加 (Add Port)]** ウィンドウで、アンダーレイの接続情報を入力します。

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

a) 次の一般情報を指定します。

- **[イーサネット ポート ID (Ethernet Port ID)]** フィールドに、ポート ID、たとえば `1/29` を入力します。

  これは、IPN への接続に使用されるインターフェイスです。

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

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

- **[MTU]** フィールドに、サーバの MTU を入力します。MTUを9150Bに設定する継承を指定するか、`576` ー `9000` の値を選択します。

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

ステップ 8 アンダーレイ プロトコルを選択します。

a) アンダーレイ接続に OSPF プロトコルを使用する場合は、**[OSPF]** を設定します。

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

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

  OSPF 設定が使用可能になります。

- **[OSPF ポリシー (OSPF Policy)]** ドロップダウンで、インフラの設定: オンプレミス サイトの設定（40 ページ） で設定したスイッチの OSPF ポリシーを選択します。

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

- **[OSPF 認証 (OSPF Authentication)]** では、`[なし (none)]` または以下のいずれかを選択します。

  - `MD5`

- Simple

- **[BGP]** を [無効 (Disabled)] に設定します。

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

アンダーレイ接続に OSPF プロトコルを使用しており、前のサブステップですでに設定している場合は、この部分をスキップします。

（注） 次の場合、BGP IPv4 アンダーレイはサポートされません。

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

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

- **[OSPF]** を [無効 (Disabled)] に設定します。

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

- **[BGP]** を [有効 (Enabled)] に設定します。

BGP 設定が使用可能になります。

- **[ピア IP (Peer IP)]** フィールドに、このポートの BGP ネイバーの IP アドレスを入力します。

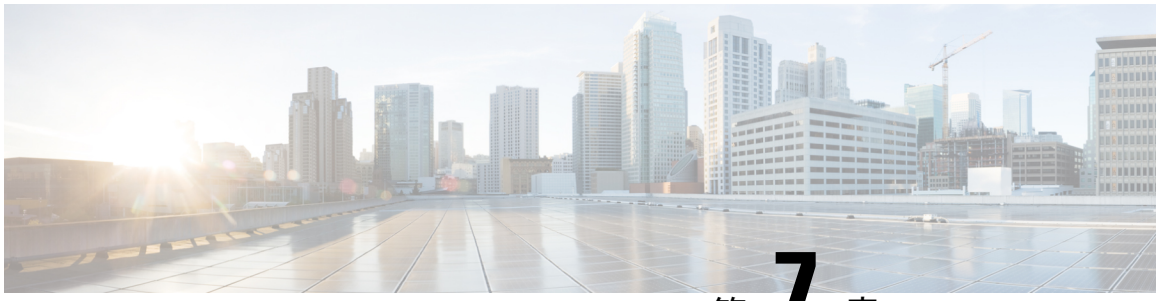
BGP アンダーレイ接続では、IPv4 IP アドレスのみがサポートされます。

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

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

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

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



第 7 章

Cisco Cloud APIC サイトのインフラの設定

クラウド サイト接続性情報の更新

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

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 **[更新 (Refresh)]** ボタンをクリックして、新規または変更されたCSRおよびリージョンを検出します。

ステップ 6 最後に、**[はい (Yes)]** をクリックして確認し、接続情報をロードします。

これにより、新規または削除された CSR およびリージョンが検出されます。

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

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

インフラの設定: クラウド サイトの設定

ここでは、クラウド APIC 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 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、特定のクラウド サイトを選択します。

ステップ 5 **[サイト間接続（Inter-Site Connectivity）]** 情報を入力します。

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

b) **マルチサイト** ノブを有効にします。

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

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

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

ステップ 6 サイト固有の **[サイト間接続 (Inter-Site Connectivity)]** 情報を入力します。

a) クラウド サイトの右側のプロパティ サイドバーで、**[サイトの追加]** 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]** で、**[サイトの選択]** をクリックし、構成しているサイト (たとえば、 `Site1`) からの接続を確立するサイト (たとえば、 `Site2`) を選択します。

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

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

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

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

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

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

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

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

Site1 > Site2 の接続情報が提供された後、**Site2 > Site1** 領域は、反対方向の接続情報を反映します。

e) **[保存 (Save)]** をクリックして、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) 他のサイトのサイト間接続を追加するには、この手順を繰り返します。

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

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

ステップ 7 **[外部接続 (External Connectivity)]** 情報を入力します。

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

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

a) 右側の ***[<Site> 設定 (Settings)]*** ペインで、**[外部接続 (External Connectivity)]** タブを選択します。
b) **[外部接続の追加 (Add External Connectivity)]** をクリックします。

[外部接続の追加 (Add External Connectivity)] ダイアログが開きます。

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

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

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

これは、一般的なインフラストラクチャ設定時に**[一般設定 (General Settings)]** > **[外部デバイス (External Devices)]** リストに追加した外部デバイスであり、インフラの設定: 一般設定 （33 ページ）の説明に従ってすでに定義されている必要があります。

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

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

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

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

この接続に特定のサブネット プールを提供する場合は、インフラの設定: 一般設定 （33 ページ）の説明に従って作成済みである必要があります。

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

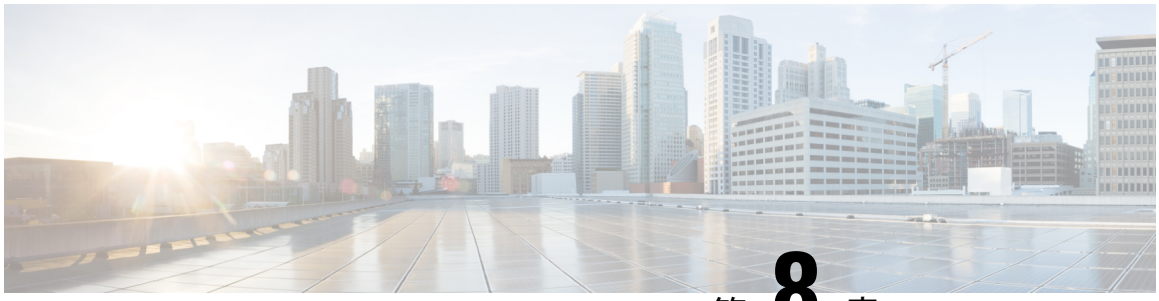
h) 必要に応じて、同じ外部接続（同じ VRF ）に対して追加する外部デバイスについて、前のサブステップを繰り返します。

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

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

次のタスク

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 （51 ページ）の説明に従って、設定を展開する必要があります。



第 8 章

ACI サイト向けのインフラ設定の展開

インフラ設定の展開

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

ステップ 1 メインペインの右上にある **[展開 (deploy)]** をクリックして、設定を展開します。

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

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

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

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

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

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

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

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

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。

次のタスク

インフラ オーバーレイとアンダーレイの構成設定が、すべてのサイトのコントローラとクラウド CSR に展開されます。残った最後の手順では、サイト接続性情報の更新 （39 ページ）で説明するように、IPN デバイスをクラウド CSR のトンネルを使用して設定します。

オンプレミスとクラウド サイト間の接続の有効化

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

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

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

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

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

インフラ設定の展開 （51 ページ）の手順の一部として、Nexus Dashboard Orchestrator の **[IPN デバイス設定ファイルの展開とダウンロード (Deploy & Download IPN Device config files)]** オプションまたは **[IPN デバイス設定ファイルのダウンロード (IPN Device config files only)]** オプションを使用して、必要な設定の詳細を取得できます。

ステップ 2 オンプレミスの IPsec デバイスにログインします。

ステップ 3 最初の CSR のトンネルを設定します。

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

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

  トンネルの宛先は、アンダーレイ接続のタイプによって異なります。

  - アンダーレイがパブリック インターネット経由の場合、トンネルの宛先はクラウド ルータ インターフェイスのパブリック IP です。
  - アンダーレイがプライベート接続（AWS の DX や Azure の ER など）を介している場合、トンネルの宛先はクラウド ルータ インターフェイスのプライベート IP です。

- <*first-csr-preshared-key*>：最初の CSR の事前共有キーです。
- <*onprem-device-interface*>：Amazon Web Services に展開された Cisco Cloud サービス ルータ 1000V への接続に使用されるインターフェイスです。
- <*onprem-device-ip-address*>：Amazon Web Services に展開された Cisco Cloud サービス ルータ 1000V への接続に使用される、<*interface*> インターフェイスの IP アドレスです。
- <*peer-tunnel-for-onprem-IPsec-to-first-CSR*>：最初のクラウド CSR に対してオンプレミスの IPsec デバイスのピア トンネル IP アドレスとして使用されます。
- <*process-id*> ：OSPF プロセス ID です。
- <*area-id*>：OSPF エリア ID です。

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

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

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

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

crypto ikev2 profile ikev2-infra:overlay-1-<first-csr-tunnel-id>
    match address local interface <onprem-device-interface>
    match identity remote address <first-csr-ip-address> 255.255.255.255
    identity local address <onprem-device-ip-address>
    authentication remote pre-share
```

```
    authentication local pre-share
    keyring local key-ikev2-infra:overlay-1-<first-csr-tunnel-id>
    lifetime 3600
    dpd 10 5 on-demand
exit

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

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

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

例：

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

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

crypto ikev2 keyring key-ikev2-infra:overlay-1-2001
    peer peer-ikev2-keyring
        address 52.12.232.0
        pre-shared-key 144904725321902286651389219409672714611O
    exit
exit

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

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

crypto ipsec profile infra:overlay-1-2001
```

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

! These tunnel interfaces establish point-to-point connectivity between the on-prem device and the
 cloud Routers
! The destination of the tunnel depends on the type of underlay connectivity:
! 1) The destination of the tunnel is the public IP of the cloud Router interface if the underlay
is via internet
! 2) The destination of the tunnel is the private IP of the cloud Router interface if the underlay
 is via private
     connectivity like DX on AWS or ER on Azure

interface tunnel 2001
    ip address 5.5.1.26 255.255.255.252
    ip virtual-reassembly
    ! Please change GigabitEthernet1 to the appropriate interface
    tunnel source GigabitEthernet1
    tunnel destination 52.12.232.0
    tunnel mode ipsec ipv4
    tunnel protection ipsec profile infra:overlay-1-2001
    ip mtu 1400
    ip tcp adjust-mss 1400
    ! Please update process ID according with your configuration
    ip ospf 1 area 0.0.0.1
    no shut
exit
```

ステップ 4 2 番目、および設定する必要があるその他の CSR について、これらの手順を繰り返します。

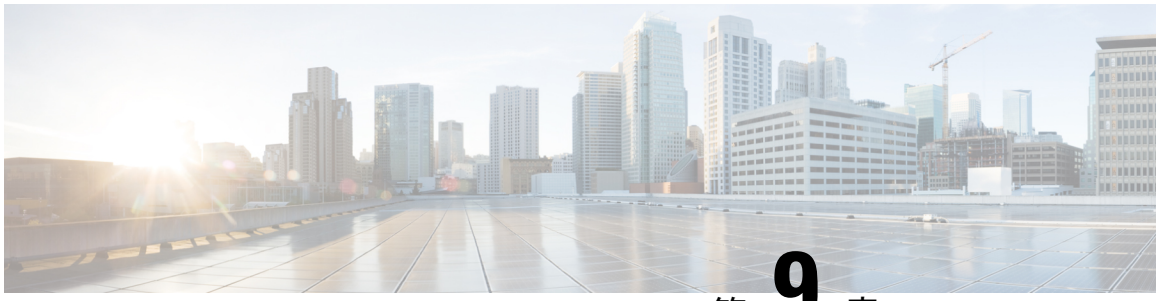
ステップ 5 オンプレミスの IPsec デバイスでトンネルがアップしていることを確認します。

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

```
ISN_CSR# show ip interface brief | include Tunnel
Interface              IP-Address      OK? Method Status                Protocol
Tunnel1000             30.29.1.2         YES manual up                    up
Tunnel1001             30.29.1.4         YES manual up                    up
```

第 II 部

DCNM ファブリックの Day-0 運用



第 9 章

サイトの追加と削除

Cisco DCNM サイトの追加

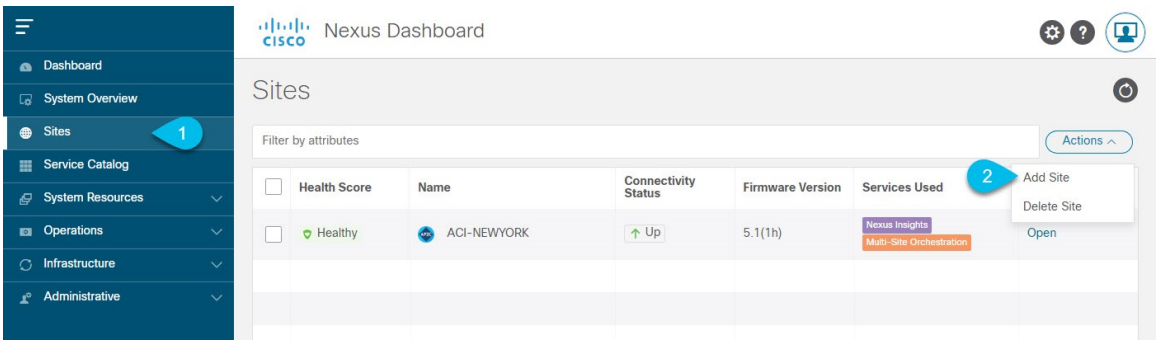
ここでは、Nexus Dashboard GUI を使用して DCNM サイトを追加し、そのサイトを Nexus Dashboard Orchestrator で管理できるようにする方法について説明します。

始める前に

- 追加するサイトが Cisco DCNM 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 ダッシュボード GUI にログインします。

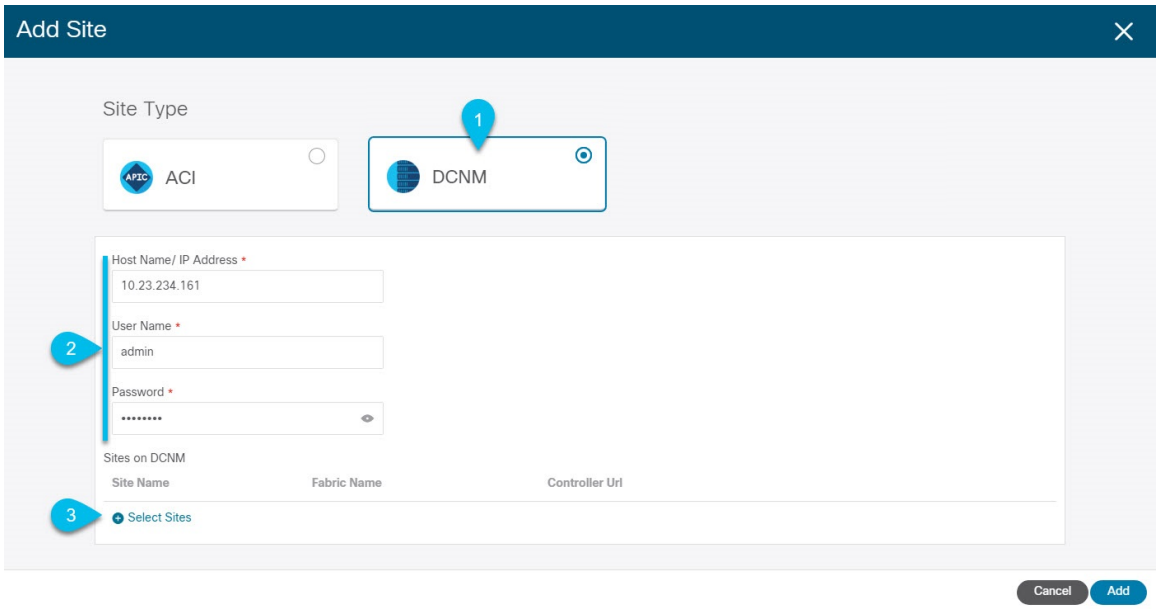
ステップ 2 新サイトを追加します。



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

b) メインペインの右上にある**[アクション (Actions)]** > **[サイトの追加 (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、**[DCNM]** を選択します。

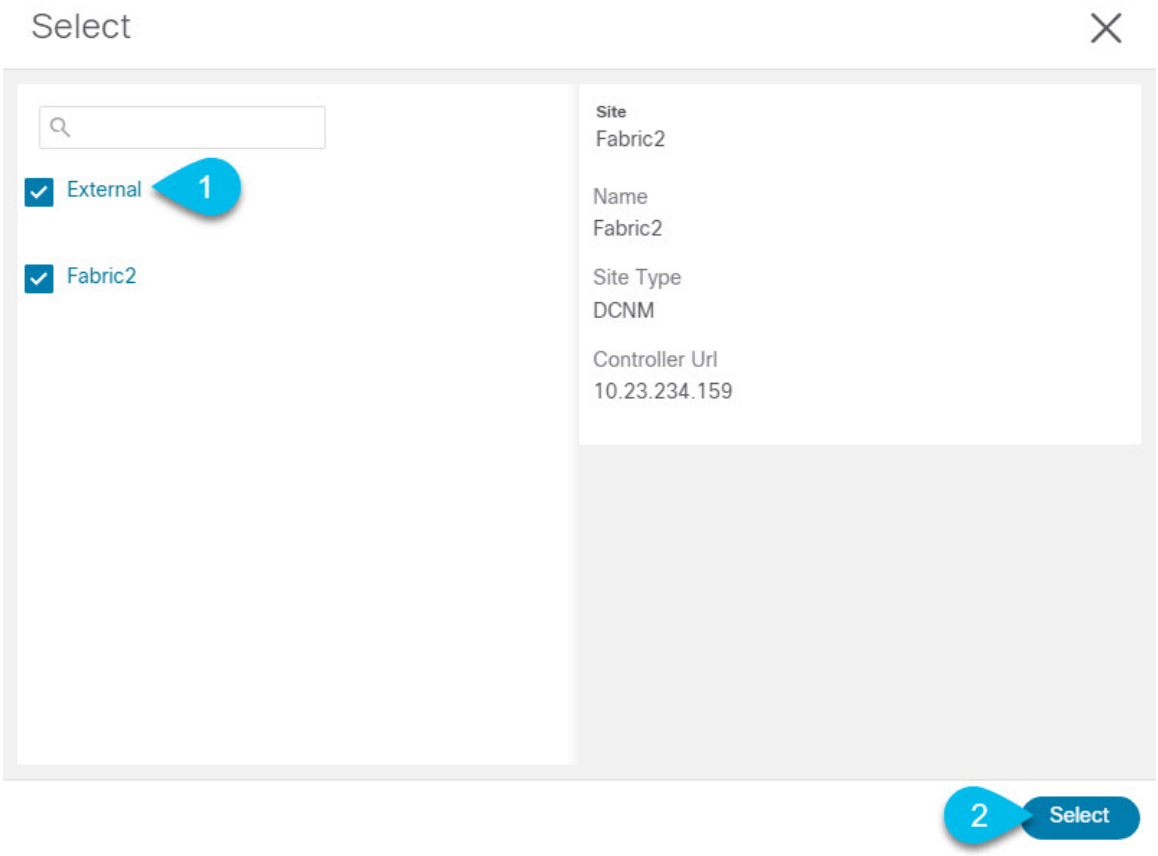
b) DCNM コントローラ情報を入力します。

現在 DCNM ファブリックを管理している DCNM コントローラ用に、**[ホスト名/IP アドレス (Host Name/IP Address)]**（インバンド（`eth2`）インターフェイスのもの）、**[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、DCNM 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。

ファブリック選択ウィンドウが開きます。

ステップ 4 Nexus ダッシュボードに追加するファブリックを選択します。



a) Nexusダッシュボードで実行しているアプリケーションで使用できる1つ以上のファブリックをオンにします。
b) [選択（Select）] をクリックします。

ステップ 5 **[サイトの追加 (Add Site)]** ウィンドウで、**[追加 (Add)]** をクリックしてサイトの追加を終了します。

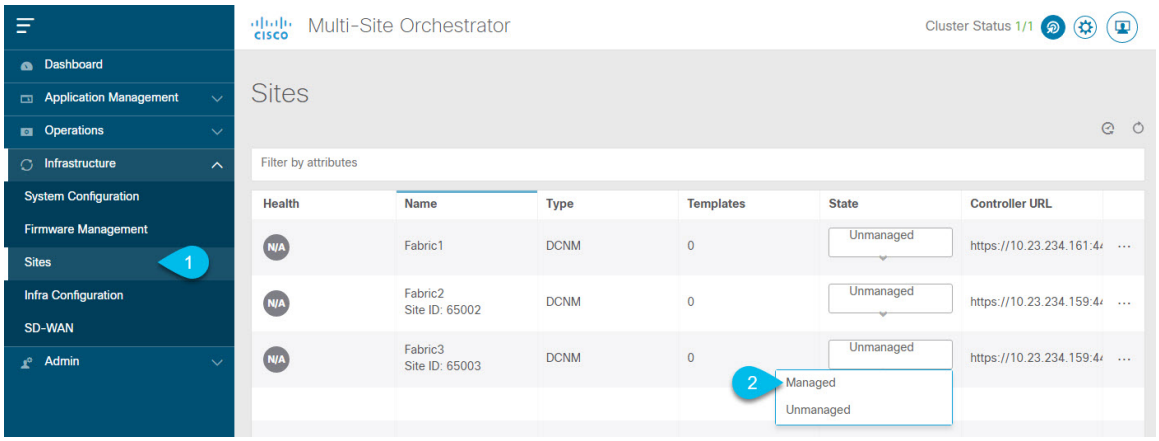
この時点で、サイトはNexusダッシュボードで使用できるようになりますが、次の手順で説明するように、Nexus Dashboard Orchestratorの管理用にそれらのサイトを有効にする必要があります。

ステップ 6 追加の DCNM コントローラについて、前の手順を繰り返します。

ステップ 7 Nexus ダッシュボードの **[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 8 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DCNM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 DCNM MSD の一部ではない場合、サイトの **[ファブリック ID (Fabric ID)]** を指定しない限り、その状態を［管理対象 (Managed)］に変更することはできません。

（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。

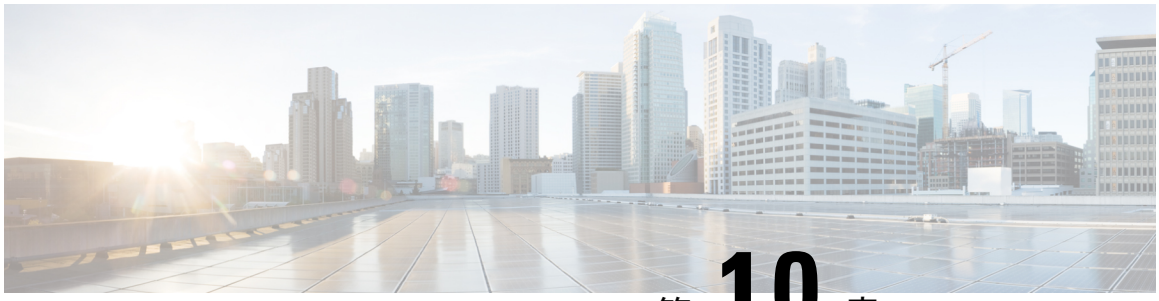
Nexus ダッシュボードからサイトが削除されます。

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 10 章

Cisco DCNM サイトのインフラの設定

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 （67 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

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

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）] > [インフラの設定（Infra Configuration）]**を選択します。

ステップ 3 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。

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 プレーン構成 (Control Plane Configuration)]** を設定します。

a) **[コントロール プレーン BGP（Control Plane BGP）]** 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) Cisco Cloud ACI 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 **[IPNデバイス（IPN Devices）]** タブの設定をスキップします。

[IPNデバイス（IPN Devices）] タブの設定は、オンプレミス APIC サイトとクラウド APIC サイト間の Cisco ACI サイト間接続用です。Cisco DCNM サイトのみを管理する場合は、これらの設定をスキップできます。

ステップ 7 **[DCNM 設定（DCNM Settings）]** を構成します。

a) **[DCNM 設定（DCNM 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。インフラの設定: DCNN サイトの設定 （67 ページ）で説明します。

以前に DCNM 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。

インフラの設定: DCNN サイトの設定

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

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）]** > **[インフラの設定（Infra Configuration）]**を選択します。

ステップ 3 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。

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

ステップ 5 右側の **<*Site*>[設定 (Settings)]**サイドバーで、**マルチサイト 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 DCNM 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DCNM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。

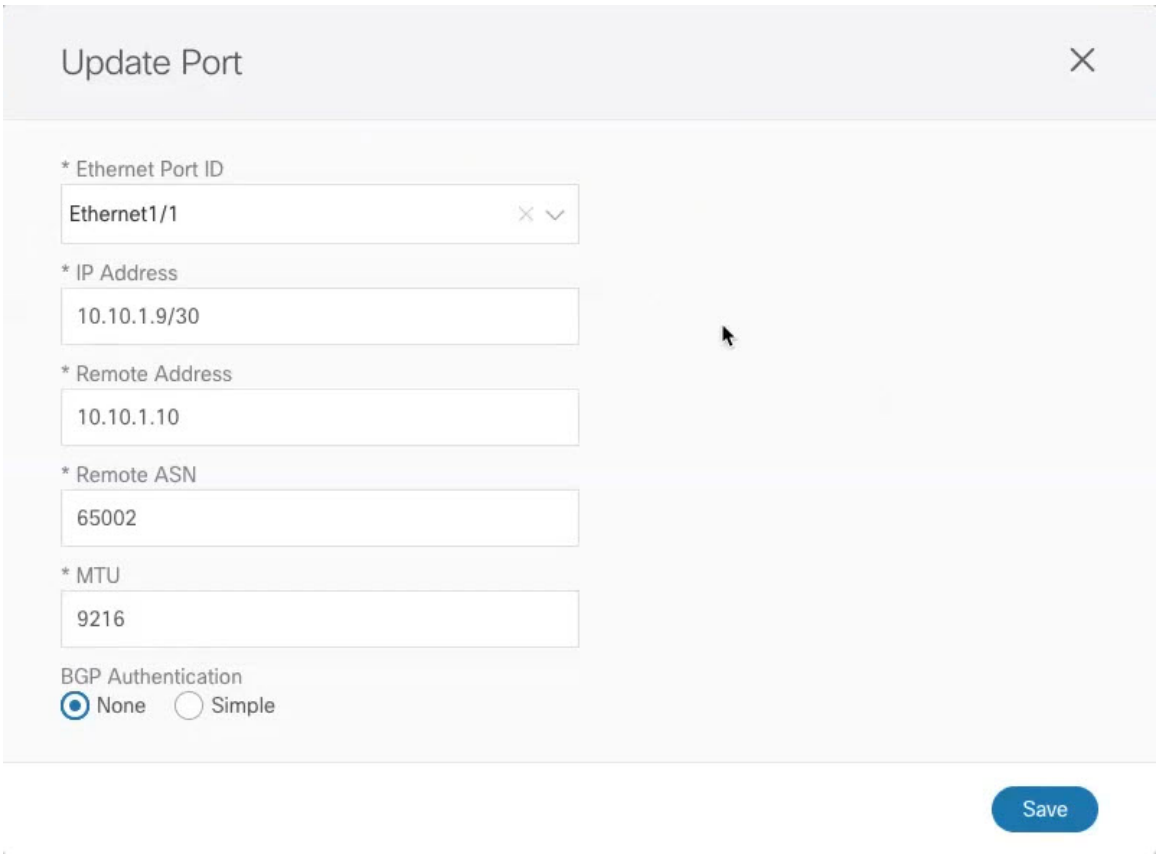
ステップ 6 **<fabric-name>** タイル内で、ボーダーゲートウェイを選択します。

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、DCNM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 DCNM マルチサイトドメイン（MDS）の一部である場合は、DCNM 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 DCNM 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

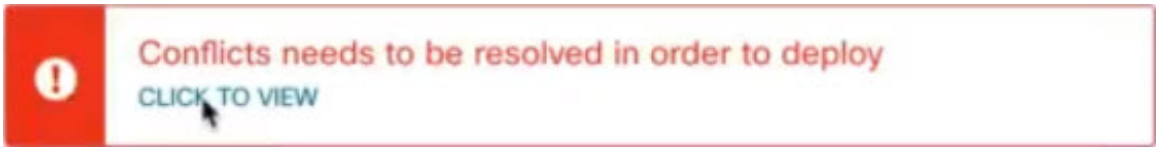
この章の前のセクションで説明したように、全般的な、およびサイト固有のインフラ設定を完了している必要があります。

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。

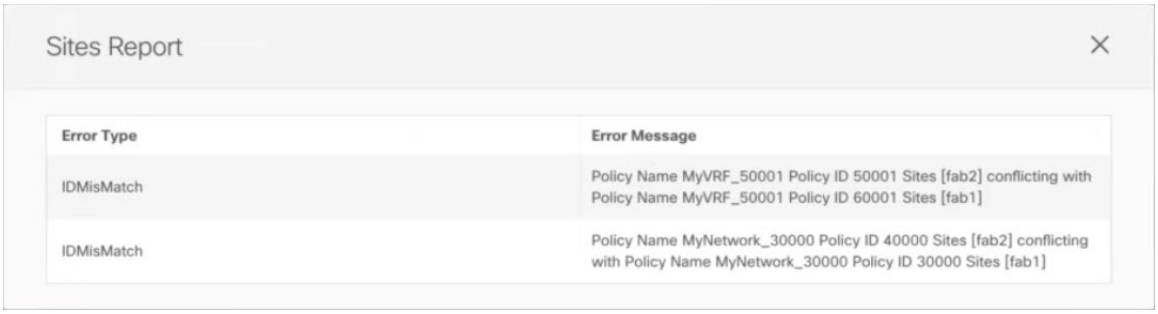
設定が競合する場合：

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 （28 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。

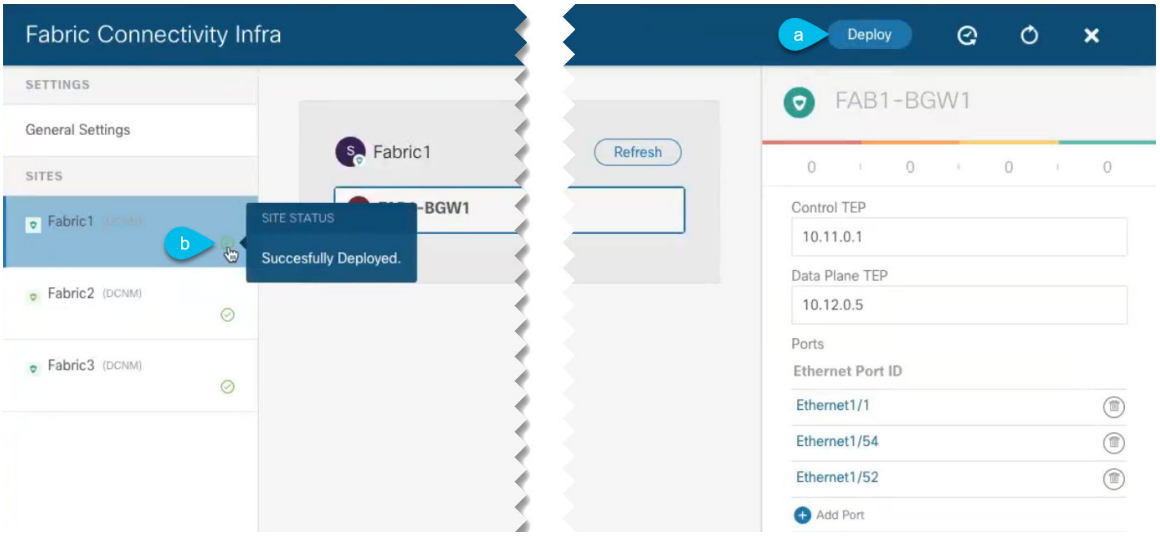
e) 既存の設定の競合を解決します。

f) Cisco DCNM サイトの追加 （59 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。

DCNM 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。

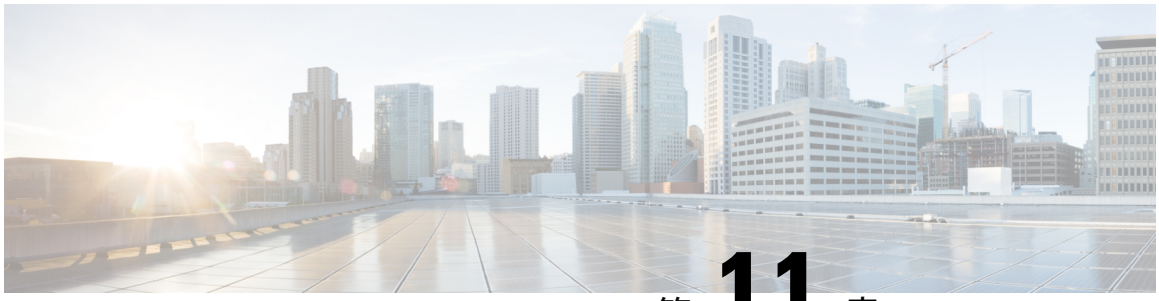
b) 設定が展開されるのを待ちます。

インフラ設定を展開すると、NDO は DCNM 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 III 部

Nexus Dashboard Orchestrator の更新



第 11 章

Nexus Dashboard での NDO サービスのアップグレード

概要

以下のセクションでは、Cisco Nexus ダッシュボードに展開されている Cisco Nexus Dashboard Orchestrator をアップグレードまたはダウングレードする方法について説明します。

VMware ESX VM または Cisco Application Services Engine に導入されている以前のリリースを実行している場合は、代わりに、*Cisco Nexus Dashboard Orchestrator* 展開ガイドの「Nexus ダッシュボードへの既存のクラスタの移行」の章の説明に従って、まったく新しいクラスタを展開し、既存のクラスタから設定を転送する必要があります。

前提条件とガイドライン

Cisco Nexus Dashboard Orchestrator クラスタをアップグレードまたはダウングレードする前に、次の手順を実行します。

- リリース 3.2(1) より前のリリースからのステートフルアップグレードはサポートされていません。

  それより前のリリースからアップグレードする場合は、この章の残りの部分をスキップし、『*12.0.1a12.0.2fNexus Dashboard Orchestrator Deployment Guide*』の「Migrating Existing Cluster to Nexus Dashboard」の章に記載されている手順に従ってください。

- 現在の Nexus ダッシュボードクラスタが正常であることを確認します。

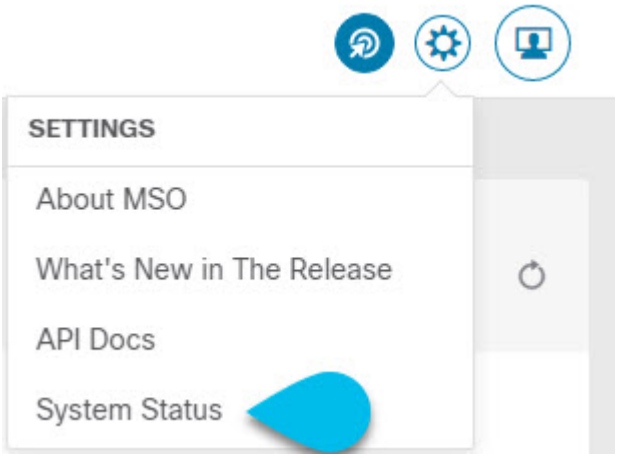
  Nexus ダッシュボード クラスタの状態は、次の 2 つの方法のいずれかで確認できます。

- Nexus ダッシュボード GUI にログインし、**[システム概要（System Overview）]** ページでシステムステータスを確認します。
- いずれかのノードに直接 `rescue-user` としてログインし、次のコマンドを実行します。

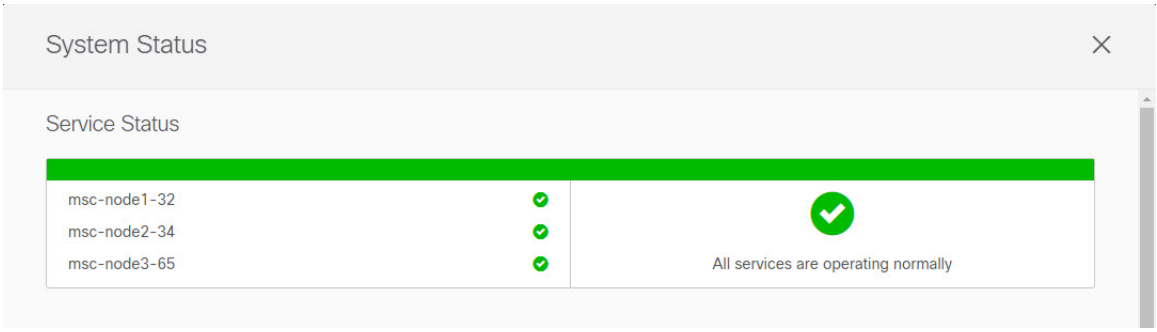
```
# acs health
All components are healthy
```

- 現在の Cisco Nexus Dashboard Orchestrator が正常に動作していることを確認します。

  Nexus Dashboard Orchestratorサービスのステータスは、**[設定（Settings）]** > **[システムステータス（System Status）]**に移動して確認できます。



次に、すべてのノードとサービスのステータスが正常であることを確認します。



- NDO サービスのアップグレードは次のいずれかの方法で実行できます。
  - Cisco App Store を使用した NDO サービスのアップグレード （77 ページ）の説明に従って、Nexus ダッシュボードの App Store を使用します。

    この場合、Cisco DC App Center は、管理ネットワークを介して直接、またはプロキシ設定を使用してNexus ダッシュボードから到達可能である必要があります。Nexusダッシュボードのプロキシ設定については、『*Nexus Dashboard User Guide*』を参照してください。

（注） App Storeでは、サービスの最新バージョンにのみアップグレードできます。たとえば、リリース 3.7(1) が利用可能な場合は、App Storeを使用してそれより前のリリースにアップグレードすることはできません。別のリリースにアップグレードするには、以下で説明する手動アップグレードプロセスを使用する必要があります。

- NDO サービスの手動アップグレード （79 ページ）の説明に従って、新しいアプリケーション イメージを手動でアップロードします。

  この方法は、DC App Center への接続を確立できない場合、または使用可能な最新リリースではないアプリケーションのバージョンにアップグレードする場合に使用できます。

- Nexus Dashboard Orchestrator をこのリリースにアップグレードした後に新しい Cloud APIC サイトを追加および管理する場合は、それらのサイトが Cloud APIC リリース 5.2(1) 以降を実行していることを確認してください。

  以前のリリースを実行しているクラウド APIC サイトのオンボーディングと管理はサポートされていません。

- リリース 3.3(1) より前のリリースへのダウングレードはサポートされていません。
- アップグレードを開始する前に、既存の構成をバックアップすることをお勧めします。

Cisco App Store を使用した NDO サービスのアップグレード

ここでは、Cisco Nexus Dashboard Orchestrator をアップグレードする方法について説明します。

始める前に

- 前提条件とガイドライン （75 ページ）で説明している前提条件をすべて満たしていることを確認します。
- Cisco DC App Center が Nexus ダッシュボードから管理ネットワーク経由で直接、またはプロキシ設定を使用して到達可能であることを確認します。

  Nexusダッシュボードのプロキシ設定については、『*Nexus Dashboard User Guide*』を参照してください。

ステップ 1 Nexus Dashboard 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 **[サービス カタログ (Service Catalog)]** を選択します。

ステップ 3 App Store を使用してアプリケーションをアップグレードします。

a) **[サービス カタログ (Service Catalog)]** 画面で **[アプリ ストア (App Store)]** タブを選択します。

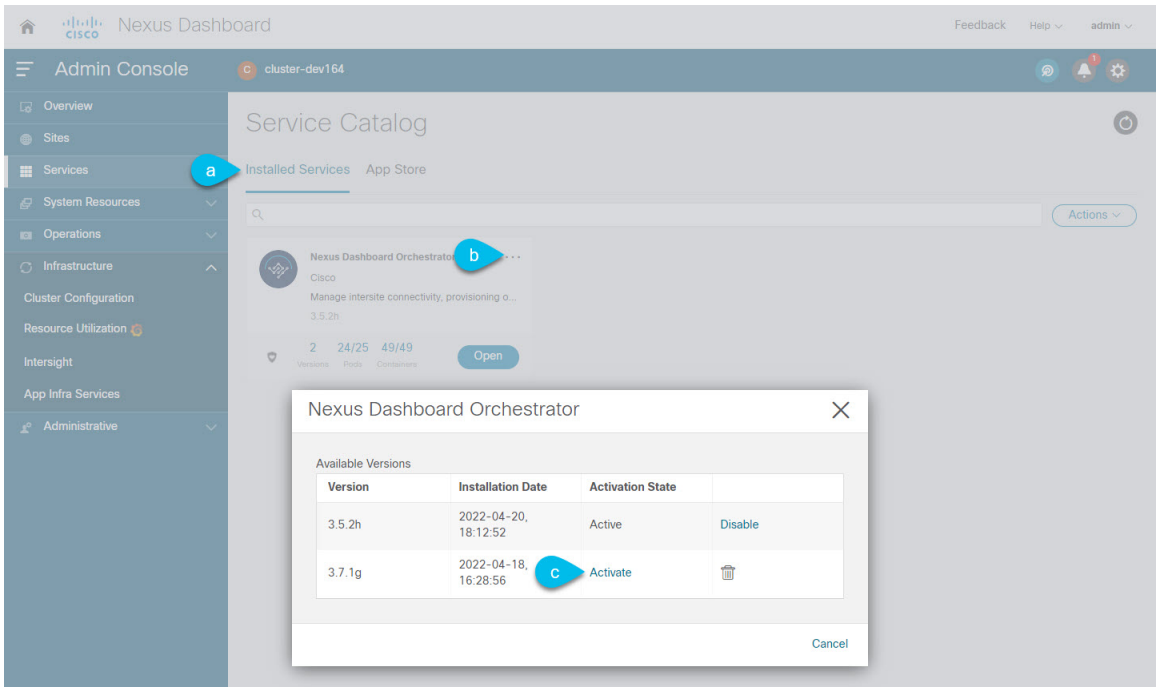
b) **[Nexus ダッシュボード オーケストレータ (Nexus Dashboard Orchestrator)]**タイルで、**[アップグレード (Upgrade)]**をクリックします。

c) 開いた[ライセンス契約(License Agreement)]ウィンドウで、**[同意してダウンロード(Agree and Download)]**をクリックします。

ステップ 4 新しいイメージが初期化されるまで待ちます。

新しいアプリケーションイメージが使用可能になるまでに最大 20 分かかることがあります。

ステップ 5 新しい画像をアクティブにします。



a) **[サービス カタログ (Service Catalog)]** 画面で、**[インストール済みサービス (Installed Services)]** タブを選択します。

b) [Nexus Dashboard Orchestrator]タイルの右上にあるメニュー（...）をクリックし、**[利用可能なバージョン (Available Versions)]** を選択します。

c) [Available Versions]ウィンドウで、新しいイメージの横にある **[アクティベート (Activate)]** をクリックします。

（注） 新しいイメージをアクティブにする前に、現在実行中のイメージを**無効にしないでください**。イメージ アクティベーション プロセスは、現在実行中のイメージを認識し、現在実行中のバージョンに必要なアップグレードワークフローを実行します。

すべてのアプリケーションサービスが起動し、GUIが使用可能になるまでに、さらに最大20分かかる場合があります。このページは、プロセスが完了した時点で自動的に再ロードされます。

ステップ 6 （任意）古いアプリケーション イメージを削除します。

ダウングレードする場合に備えて、古いアプリケーション バージョンを保持しておくこともできます。または、この手順の説明に従って削除することもできます。

a) **[サービス カタログ (Service Catalog)]** 画面で、**[インストール済みサービス (Installed Services)]** タブを選択します。

b) [Nexus Dashboard Orchestrator]タイルの右上にあるメニュー（...）をクリックし、**[利用可能なバージョン (Available Versions)]** を選択します。

c) 使用可能なバージョンのウィンドウで、削除するイメージの横にある削除アイコンをクリックします。

ステップ 7 アプリを起動します。

アプリケーションを起動するには、Nexus ダッシュボードの **[サービスカタログ (Service Catalog)]** ページのアプリケーションタイルで **[開く (Open)]** をクリックします。

シングルサインオン（SSO）機能を使用すると、Nexus ダッシュボードで使用したものと同じクレデンシャルを使用してアプリケーションにログインできます。

次のタスク

NDO サービスをアップグレードした後、構成のばらつきを解決し、「設定のばらつきの解決とテンプレートの再展開 （81 ページ）」で説明されているようにテンプレートを再展開する必要があります。

NDO サービスの手動アップグレード

ここでは、Cisco Nexus Dashboard Orchestrator をアップグレードする方法について説明します。

始める前に

- 前提条件とガイドライン （75 ページ）で説明している前提条件をすべて満たしていることを確認します。

ステップ 1 ターゲットのリリース イメージをダウンロードします。

a) DC App Center で Nexus Dashboard Orchestrator ページを参照します。
https://dcappcenter.cisco.com/nexus-dashboard-orchestrator.html

b) **[バージョン (Version)]** ドロップダウンから、インストールするバージョンを選択し、**[ダウンロード (Download)]** をクリックします。

c) **[同意してダウンロード (Agree and download)]** をクリックしてライセンス契約に同意し、イメージをダウンロードします。

ステップ 2 Nexus Dashboard にログインします。

ステップ 3 Nexus ダッシュボードにイメージをアップロードします。

a) 左のナビゲーションメニューから **[サービス カタログ (Service Catalog)]** を選択します。
b) Nexus ダッシュボードの **[サービス カタログ (Service Catalog)]** 画面で、**[インストール済みサービス (Installed Services)]** タブを選択します。
c) メインペインの右上にある **[アクション (Actions)]** メニューから、**[アプリケーションのアップロード (Upload App)]** を選択します。
d) **[アプリケーションのアップロード (Upload App)]** ウィンドウで、イメージの場所を選択します。

アプリケーション イメージをシステムにダウンロードした場合は、**[ローカル (Local)]** を選択します。

サーバでイメージをホストしている場合は、**[リモート (Remote)]** を選択します。

e) ファイルを選択します。

前のサブステップで **[ローカル (Local)]** を選択した場合は、**[ファイルの選択 (Select File)]** をクリックし、ダウンロードしたアプリケーションイメージを選択します。

[リモート（Remote）] を選択した場合は、イメージ ファイルのフル URL を指定します。たとえば、`http://<ip-address>:<port>/<full-path>/cisco-mso-<version>.nap` のようになります。

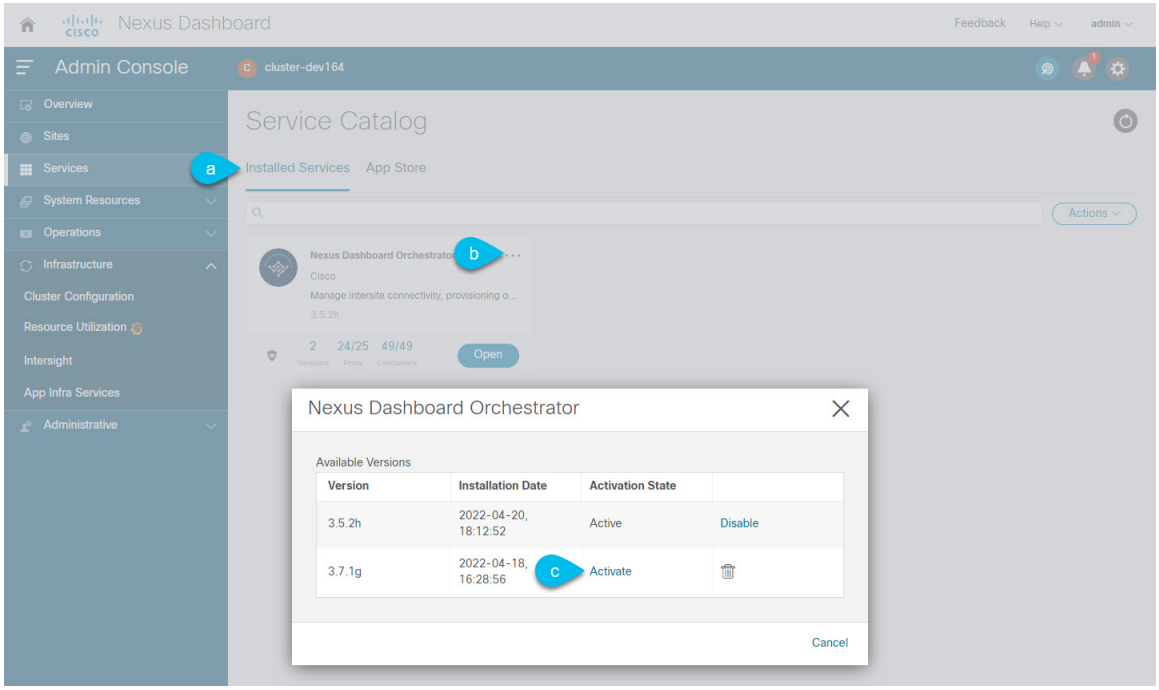
f) **[アップロード (Upload)]** をクリックして、アプリケーションをクラスタに追加します。

アップロードの進行状況バーとともに新しいタイルが表示されます。イメージのアップロードが完了すると、Nexus ダッシュボードは新しいイメージを既存のアプリケーションとして認識し、新しいバージョンとして追加します。

ステップ 4 新しいイメージが初期化されるまで待ちます。

新しいアプリケーションイメージが使用可能になるまでに最大 20 分かかることがあります。

ステップ 5 新しい画像をアクティブにします。



a) **[サービス カタログ (Service Catalog)]** 画面で、**[インストール済みサービス (Installed Services)]** タブを選択します。
b) [Nexus Dashboard Orchestrator]タイルの右上にあるメニュー（...）をクリックし、**[利用可能なバージョン (Available Versions)]** を選択します。
c) [Available Versions]ウィンドウで、新しいイメージの横にある **[アクティベート (Activate)]** をクリックします。

（注） 新しいイメージをアクティブにする前に、現在実行中のイメージを**無効にしないでください**。イメージ アクティベーション プロセスは、現在実行中のイメージを認識し、現在実行中のバージョンに必要なアップグレードワークフローを実行します。

すべてのアプリケーション サービスが起動し、GUI が使用可能になるまでに、さらに最大 20 分かかる場合があります。このページは、プロセスが完了した時点で自動的に再ロードされます。

ステップ 6 （任意）古いアプリケーション イメージを削除します。

ダウングレードする場合に備えて、古いアプリケーション バージョンを保持しておくこともできます。または、この手順の説明に従って削除することもできます。

a) **[サービス カタログ (Service Catalog)]** 画面で、**[インストール済みサービス (Installed Services)]** タブを選択します。
b) [Nexus Dashboard Orchestrator]タイルの右上にあるメニュー（...）をクリックし、**[利用可能なバージョン (Available Versions)]** を選択します。
c) 使用可能なバージョンのウィンドウで、削除するイメージの横にある削除アイコンをクリックします。

ステップ 7 アプリを起動します。

アプリケーションを起動するには、Nexus ダッシュボードの **[サービスカタログ (Service Catalog)]** ページのアプリケーションタイルで **[開く (Open)]** をクリックします。

シングルサインオン（SSO）機能を使用すると、Nexus ダッシュボードで使用したものと同じクレデンシャルを使用してアプリケーションにログインできます。

次のタスク

NDO サービスをアップグレードした後、構成のばらつきを解決し、「設定のばらつきの解決とテンプレートの再展開 （81 ページ）」で説明されているようにテンプレートを再展開する必要があります。

設定のばらつきの解決とテンプレートの再展開

いくつかの事例では、構成がサイト コントローラで実際に展開される状況が、Nexus Dashboard Orchestrator で定義された設定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。

Nexus Dashboard Orchestrator のこのリリースにアップグレードした後、アップグレード時のデータベース変換により生じる構成のばらつきがないことを確認してから、すべてのテンプレートを再展開してアップグレードを完了する必要があります。

（注） 構成のばらつきを解決する前にテンプレートを展開すると、Orchestrator で定義された構成がプッシュされ、ファブリックのコントローラで定義された値が上書きされます。

始める前に

Cisco App Store を使用した NDO サービスのアップグレード （77 ページ） または NDO サービスの手動アップグレード （79 ページ） の説明に従って、Nexus Dashboard Orchestrator をアップグレードしておく必要があります。

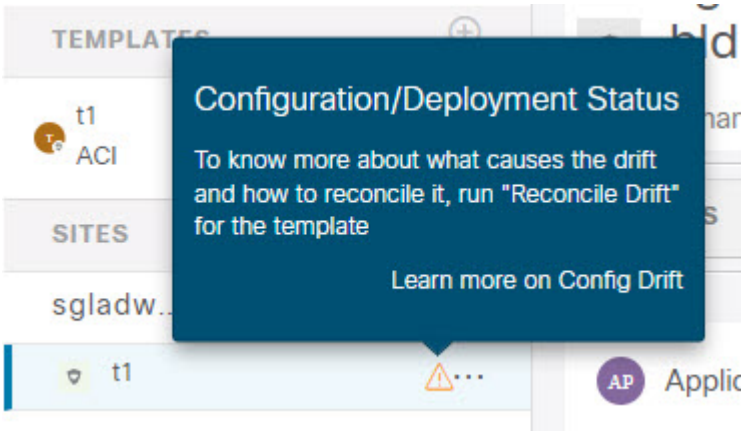
ステップ 1 Nexus Dashboard Orchestrator で、**[アプリケーション管理 (Application Management)]** > **[スキーマ (Schemas)]** に移動します。

ステップ 2 最初のスキーマを選択し、そのテンプレートで構成ドリフトを確認します。

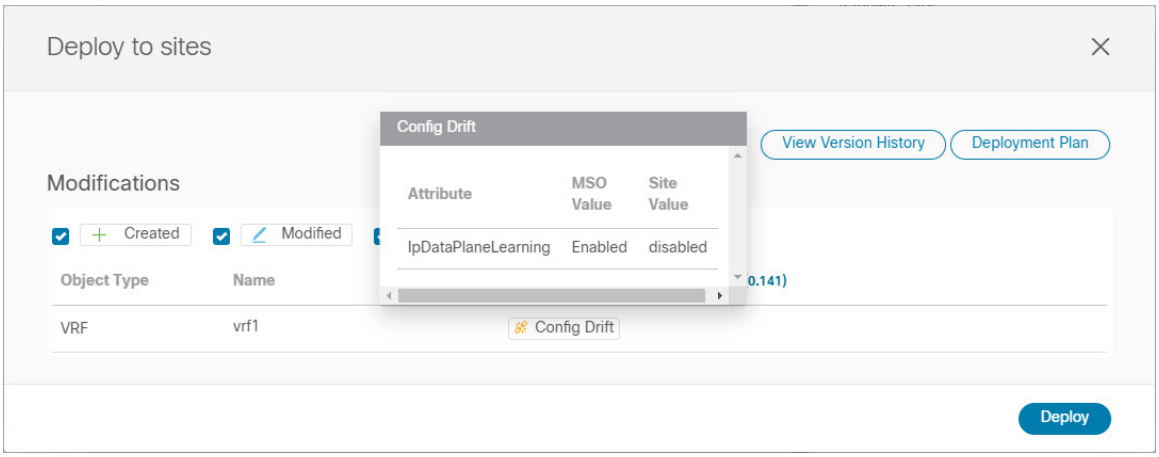
展開内のすべてのスキーマとテンプレートについて、次の手順を繰り返します。

次の 2 つの方法のいずれかで、構成のばらつきを確認できます。

- 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、**[サイトへの展開 (Deploy to sites)]** をクリックして構成比較画面を呼び出し、構成のばらつきが含まれているオブジェクトを確認します。



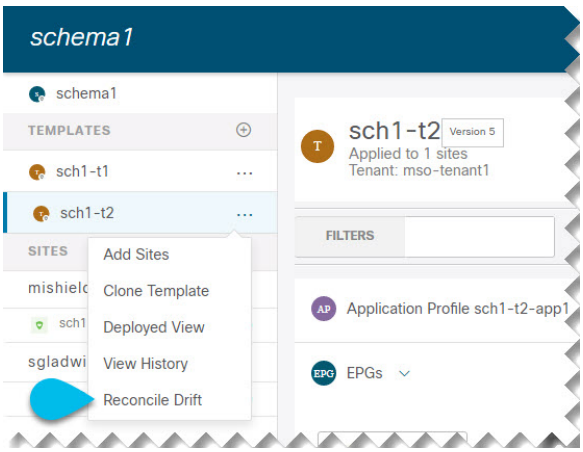
ステップ 3 テンプレートに構成のばらつきが含まれている場合は、競合を解決します。

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。

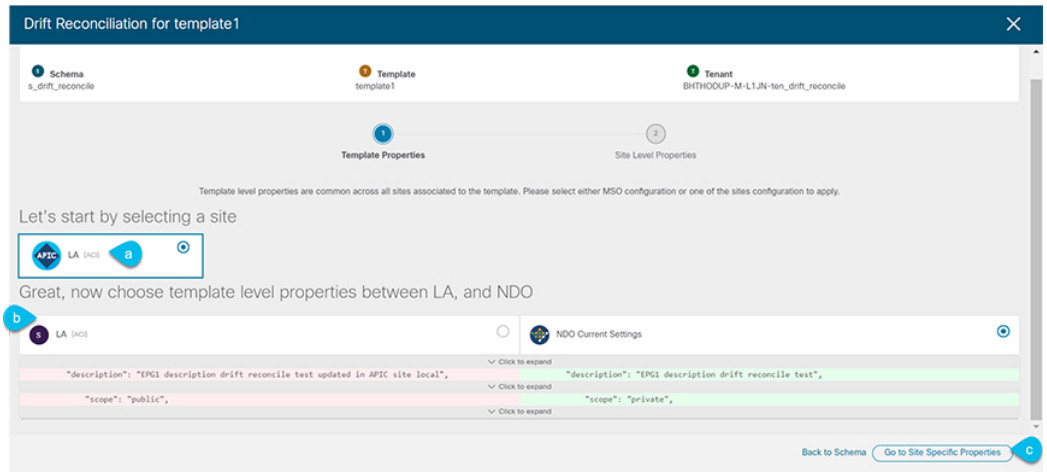
この時点でテンプレートを展開すると、Orchestrator データベースの値をプッシュして、ファブリックの既存の設定を上書きします。

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。



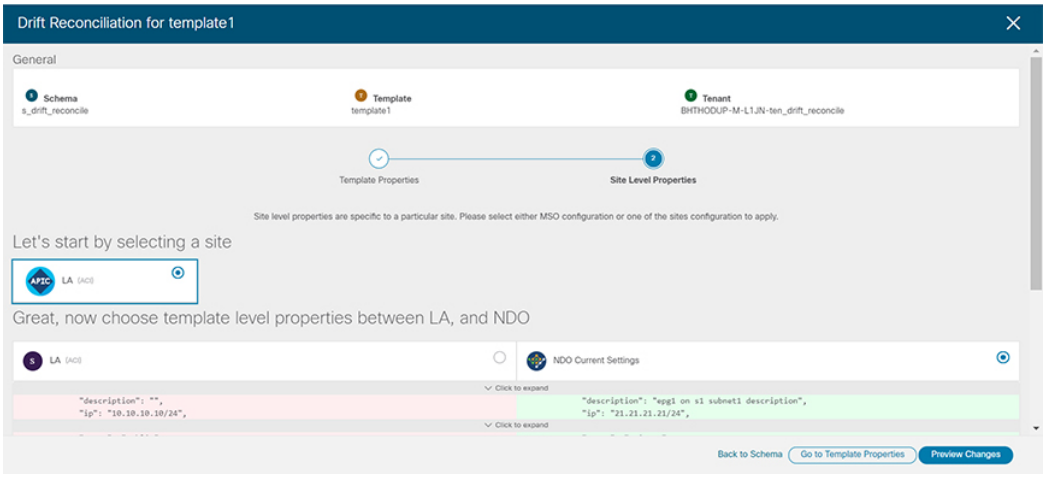
[ばらつきの調整 (Reconcile Drift)] ウィザードが開きます。

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。サイト構成を選択すると、既存の Nexus Dashboard Orchestrator テンプレート内のこれらのプロパティが変更されますが、Nexus Dashboard Orchestrator 構成を選択した場合は、既存の Nexus Dashbaord Orchestrator テンプレートの設定はそのまま保持されます。

d) **[サイト固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 レベルの構成とサイト レベルの構成のどちらでも同じ選択を行いますが、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定義されている構成を「テンプレートのプロパティ」レベルで選択し、Nexus Dashboard Orchestrator で定義された構成を 「サイトのローカルプロパティ」レベルで選択したり、またその逆で選択したりすることもできます。

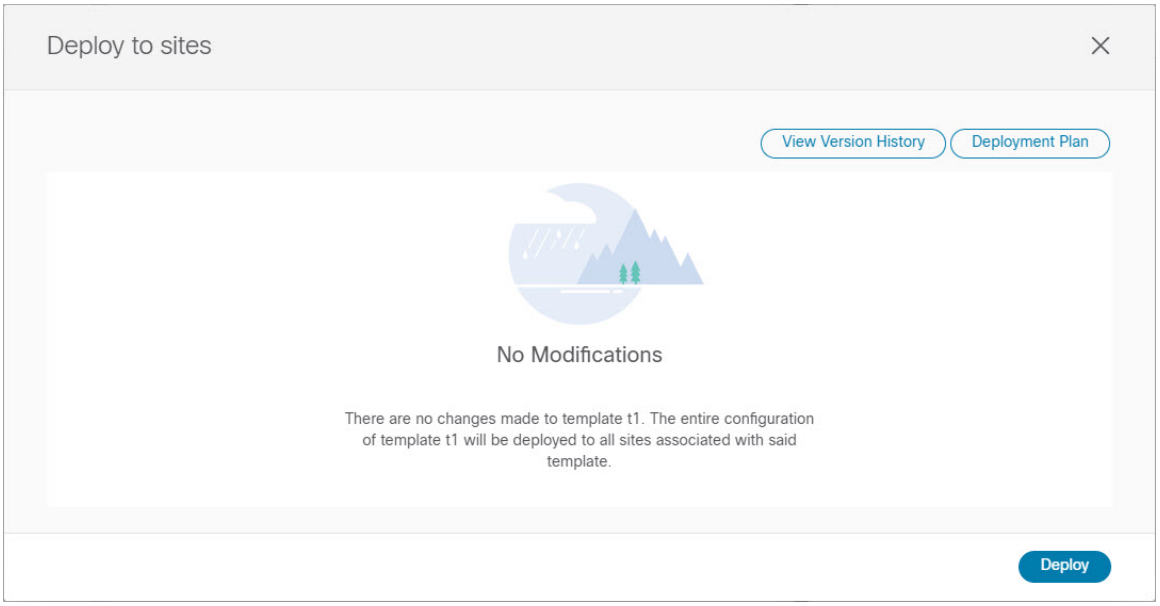
e) **[変更のプレビュー（Preview Changes）]** をクリックして、選択内容を確認します。

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)]** をクリックして設定を展開し、そのテンプレートのばらつきを調整できます。

ステップ 4 すべての構成のばらつきが解決され、**[サイトへの展開（Deploy to sites）]** ダイアログに変更が表示されなくなったら、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。

次の図に示すように、**[サイトへの展開（Deploy to sites）]** ダイアログに変更が含まれていないことを確認し、**[展開（Deploy）]** をクリックして、完全な構成を再展開します。

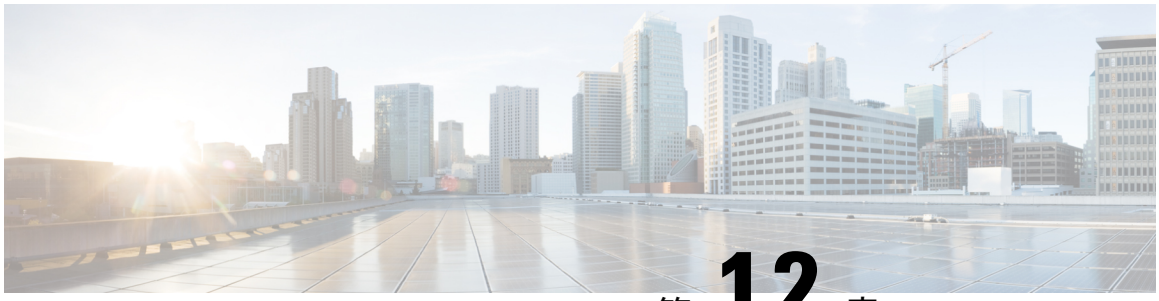


ステップ 5 Nexus Dashboard Orchestrator で各スキーマとテンプレートに対して上記の手順を繰り返します。

ステップ 6 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。



第 12 章

Nexusダッシュボードへの既存のクラスタの移行

概要

Nexus Dashboard Orchestrator のこのリリース（旧称 Multi-Site Orchestrator）は、Cisco Nexus ダッシュボードのサービスとして導入する必要があります。以前サポートされていた VMware ESX 仮想アプライアンスおよび Cisco Application Services Engine フォームファクタのサポートは廃止されました。

ここでは、Cisco Multi-Site Orchestrator の以前のリリースをNexus ダッシュボードプラットフォームの Nexus Dashboard Orchestrator に移行する方法について説明します。

すでに Cisco Nexus ダッシュボードで NDO クラスタを展開している場合は、代わりに Nexus Dashboard での NDO サービスのアップグレード （75 ページ） に記載されている手順に従ってください。

移行ワークフロー

次のリストに、移行プロセスの概要と実行する必要があるタスクの順序を示します。

1. 既存の Multi-Site Orchestrator 設定をバックアップし、既存の Multi-Site Orchestrator クラスタを接続解除します。

既存のクラスタをアップグレードするのではなく、新しいNexusダッシュボードクラスタを展開する場合は、新しい Nexus Dashboard Orchestrator サービスが展開され、設定が復元されるまで、既存のMulti-Site Orchestrator クラスタを保持することをお勧めします。

2. 物理、仮想、またはクラウドのフォーム ファクタを使用して Nexus ダッシュボード クラスタを展開します。

   新しいクラスタの展開中に、次のことも完了します。

   1. （オプション）サービスの共同ホスティングに必要な場合は、追加のノードで Nexus ダッシュボード クラスタを設定します。
   2. （オプション）既存の Multi-Site Orchestrator の導入で必要な場合は、Nexusダッシュボードでリモート認証サーバーを設定します。
   3. Multi-Site Orchestrator から Nexus Dashboard に現在管理している APIC、クラウド APIC、または DCNM サイトをオンボードします。

   （注） 新しいクラスタでファブリックをオンボードするときは、元のクラスタとまったく同じ名前を各ファブリックに使用する必要があります。

   4. Nexus ダッシュボードに Nexus Dashboard Orchestrator サービスをインストールします。

3. Nexus ダッシュボードにインストールされた新しい NDO サービスで、設定のバックアップを復元します。
4. クラウド サイトをクラウド APIC リリース 5.2(x) に一度に 1 サイトずつアップグレードします。

   サイトのクラウド APIC をアップグレードしてから、そのサイトの CSR をアップグレードし、追加のサイトごとに手順を繰り返します。
5. Nexus Dashboard Orchestrator のインフラ設定を更新します。
6. 構成のばらつきの解決とテンプレートの再展開

   すべてのばらつきが解決された後に、データベース変換のために完全な再展開を行う必要があります。

   構成のドリフトを解決するには、オンボードのファブリックからオブジェクトをインポートするか、Orchestratorから構成をデプロイする必要があります。構成を再展開してばらつきを解決する場合は、データベース変換のために 2 回目の完全な再展開を実行する必要があります。

前提条件とガイドライン

新しいプラットフォームは、クラスタリングとインフラストラクチャ、サイト管理、およびユーザー管理の実装方法が大きく異なるため、移行プロセスでは、新しいNexusダッシュボードプラットフォームを並行展開することと、既存の Multi-Site Orchestrator（MSO）クラスタから現在の設定データベースを手動で転送することが必要になります。

既存のクラスタを Nexus ダッシュボードに移行する前には、次の作業を実行します。

- 最初に、*Cisco Nexus Dashboard Deployment Guide* およびこのドキュメントのNexus Dashboard Orchestrator の展開 （3 ページ）章で説明されている、Nexus Dashboard プラットフォームおよび全体的な導入の概要とガイドラインを理解しておいてください。
- 現在の Multi-Site Orchestrator クラスタが正常であることを確認します。

  既存の設定のバックアップを作成し、Nexusダッシュボードで新しく導入されたNDOサービスにインポートします。

  クラスタが正常であり、クラウドとオンプレミス サイト間の既存の IPsec サイト間接続が稼働していることを確認します。
- オンプレミスサイトが Cisco APIC リリース 4.2(4) 以降を実行していることを確認します。

  サイト管理は、Multi-Site Orchestrator UI から、リリース 4.2(4) 以降をサポートする Nexus ダッシュボード共通サイト管理に移動しました。ファブリックのアップグレードの詳細については、*Cisco APIC Installation, Upgrade, and Downgrade Guide* を参照してください。
- クラウドサイトが Cisco Cloud APIC リリース 5.1(1) を実行していることを確認します。

  サイト管理は、Multi-Site Orchestrator UI から、クラウド サイト リリース 5.1(1) 以降のオンボーディングをサポートする Nexus ダッシュボード共通サイト管理に移動しました。ファブリックのアップグレードの詳細については、*Cisco APIC Installation, Upgrade, and Downgrade Guide* を参照してください。

（注） ただし、Nexus Dashboard Orchestrator をこのリリースに移行する前に、Cloud APIC 5.2(1) リリース以降にアップグレードしないでください。クラウドサイトで Cloud APIC 4.x または 5.0(x) リリースを実行している場合は、この章の手順に従う前に Cloud APIC 5.1(x) リリースにアップグレードする必要があります。

- Cisco Cloud APIC サイトを管理する場合は、クラウドサイトを Cloud APIC リリース 5.2(1) 以降にアップグレードする前に、Nexus Dashboard Orchestrator を展開し、既存の設定をインポートしてください。

  NDO の移行が完了したら、すべてのクラウドサイトを Cloud APIC リリース 5.2(1) にアップグレードする必要があります。

- Nexus Dashboard Orchestrator のこのリリースに移行した後、リリース 3.3(1) より前のリリースへのダウングレードはサポートされません。

既存のクラスタ設定のバックアップ

移行プロセスには、既存の Multi-Site Orchestrator クラスタから現在の設定のバックアップを作成し、Nexus Dashboard で実行されている新しい Nexus Dashboard Orchestrator サービスに復元することが含まれます。

この項では、既存のクラスタの設定をバックアップする方法について説明します。

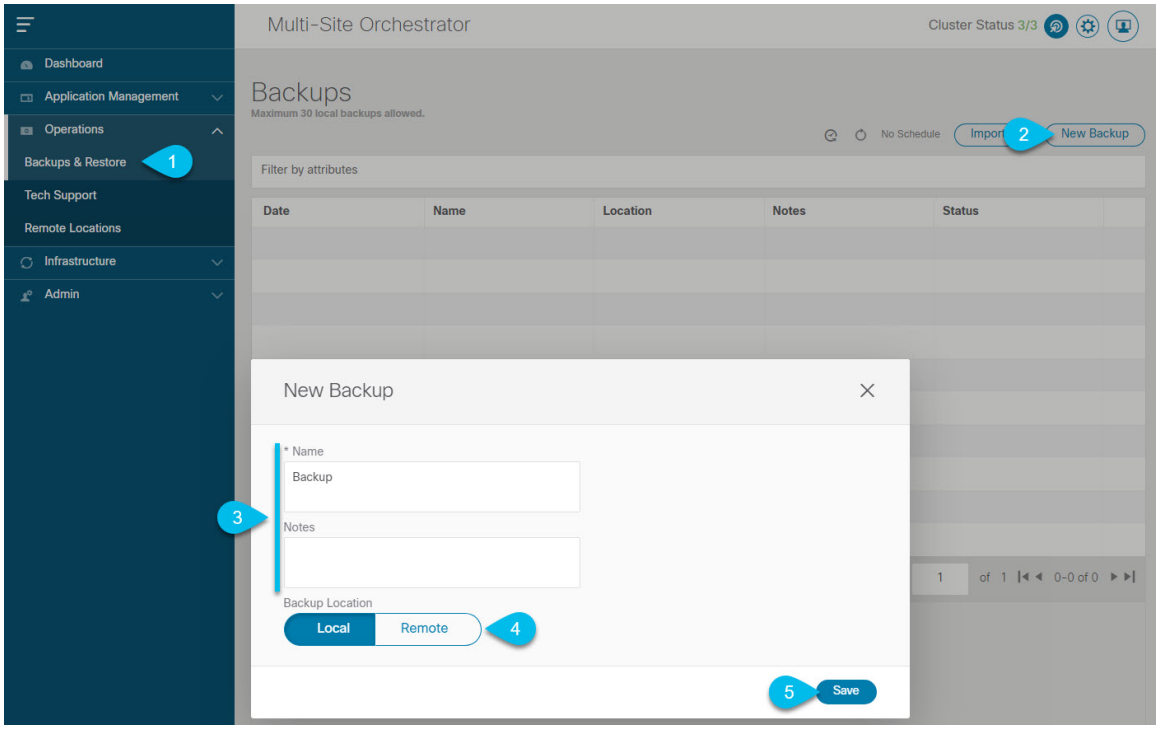
始める前に

次の前提条件があります。

- 概要 （87 ページ）で説明されている移行ワークフローの順序を理解していること。
- 前提条件とガイドライン （89 ページ）に記載されている一般的な前提条件を確認して完了していること。

ステップ 1 既存の Multi-Site Orchestrator 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) **[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。

d) `[ローカル (Lcal)]` を選択します (**[バックアップの場所 (Backup Location)]**)。

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

ステップ 3 既存の Orchestrator からバックアップファイルをダウンロードします。

リモート ロケーションを使用してバックアップを作成した場合は、この手順をスキップできます。

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。

新規クラスタの準備

ここでは、Nexus Dashboard Orchestrator サービスをインストールするための Nexus Dashboard クラスタの準備方法について説明します。

これには、Nexus Dashboard クラスタの適切なフォーム ファクタの選択と展開、およびクラスタから Nexus Dashboard Orchestrator で管理する予定の各サイトへのネットワーク接続の確立が含まれます。

始める前に

次の前提条件があります。

- 概要 （87 ページ）で説明されている移行ワークフローの順序を理解していること。
- 前提条件とガイドライン （89 ページ）に記載されている一般的な前提条件を確認して完了していること。
- 既存のクラスタ設定のバックアップ （90 ページ）の説明に従って、既存の設定をバックアップしていること。

ステップ 1 Nexus ダッシュボード リリース 2.1.1e 以降のクラスタを展開し、ファブリック接続を設定します。

Nexus ダッシュボードを展開またはアップグレードする方法は、既存のクラスタの展開タイプによって異なります。

- 既存の Multi-Site Orchestrator が直接、VMware ESX または**仮想** Cisco Application Services Engine クラスタで展開される場合、*Cisco Nexus Dashboard Deployment Guide* の説明に従って、新しい仮想またはクラウド Nexus ダッシュボード クラスタを展開する必要があります。

  また、既存のクラスタを削除する前に、移行プロセス全体を完了することをお勧めします。

- Multi-Site Orchestrator サービス リリース 3.1(x) で既存の**物理** Cisco Application Services Engine クラスタがある場合は、既存のサービスをアンインストールしてから、「アップグレード」の章の説明に従ってクラスタを Nexus ダッシュボード リリース 2.1.1e にアップグレードする必要があります。*Cisco Nexus Dashboard Deployment Guide*を参照してください。

- Nexus Dashboard Orchestrator サービス リリース 3.2(x) で既存の**物理** Nexus ダッシュボード クラスタがある場合は、*Cisco Nexus Dashboard Deployment Guide* の「Upgrading」の章の説明に従ってクラスタをアップグレードし、Nexus Dashboard Orchestrator の更新 （73 ページ） に説明されているように Nexus Dashboard Orchestrator サービスをアップグレードできます。この章の残りの部分は省略してください。

  （注） アップグレード後に Cloud APIC サイトを追加する場合は、それらのサイトで Cloud APIC リリース 5.2(1) 以降を実行していることを確認してください。

ステップ 2 Nexus ダッシュボード クラスタが、ファブリックのサイズとアプリケーションの数に基づいて適切にスケーリングされていることを確認します。

Nexus ダッシュボードの仮想またはクラウド フォーム ファクタを展開した場合、サポートされるアプリケーションは Nexus Dashboard Orchestrator のみであり、基本 3 ノードクラスタで十分なので、この手順は省略できます。

物理 Nexus ダッシュボード クラスタを展開し、Nexus Dashboard Orchestrator がホストする予定の唯一のアプリケーションである場合は、基本 3 ノードクラスタで十分なので、この手順は省略できます。

ただし、物理 Nexus ダッシュボード クラスタを導入し、複数のアプリケーションを共同ホストする場合は、Cisco Nexus Dashboard キャパシティ プランニング ツールを使用して、特定の使用例に必要なクラスタ サイズを決定します。必要なすべてのサービスをサポートするためにクラスタを拡張する必要がある場合は、追加のワーカー ノードの展開について、*Cisco Nexus Dashboard User Guide*を参照してください。

ステップ 3 Nexus ダッシュボードに NDO サービスをインストールします。

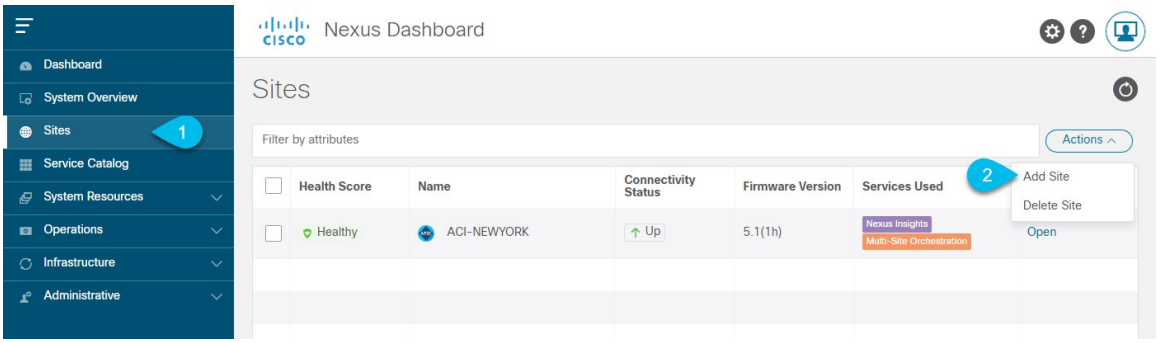
このプロセスの詳細は、Nexus Dashboard Orchestrator の展開 （3 ページ） 章に記載されています。

ステップ 4 すべてのサイトを Nexus ダッシュボードにオンボードします。

サイト管理は、Multi-Site Orchestrator UI から Nexus ダッシュボードの共通サイト管理に移動されました。したがって、サイトの追加と削除 （23 ページ） に説明されているように、既存の設定を新しいクラスタに移行する前に、元の Multi-Site Orchestrator クラスタでオンボードされたときにサイトに割り当てられていた同じ名前を使用して、同じサイトを Nexus ダッシュボード GUI にオンボードする必要があります。現在の展開に存在するサイトが Nexus ダッシュボードに存在しない場合（または別の名前で存在する場合）、移行中の設定の復元は、`復元前チェックに失敗 (Pre-restore check failed)` というエラーメッセージで失敗します。

（注） Nexus ダッシュボードにサイトを追加した後は、NDO サービスでそれらを`管理対象`に設定しないでください。バックアップから設定を復元すると、サイトの管理が自動的に有効になります。

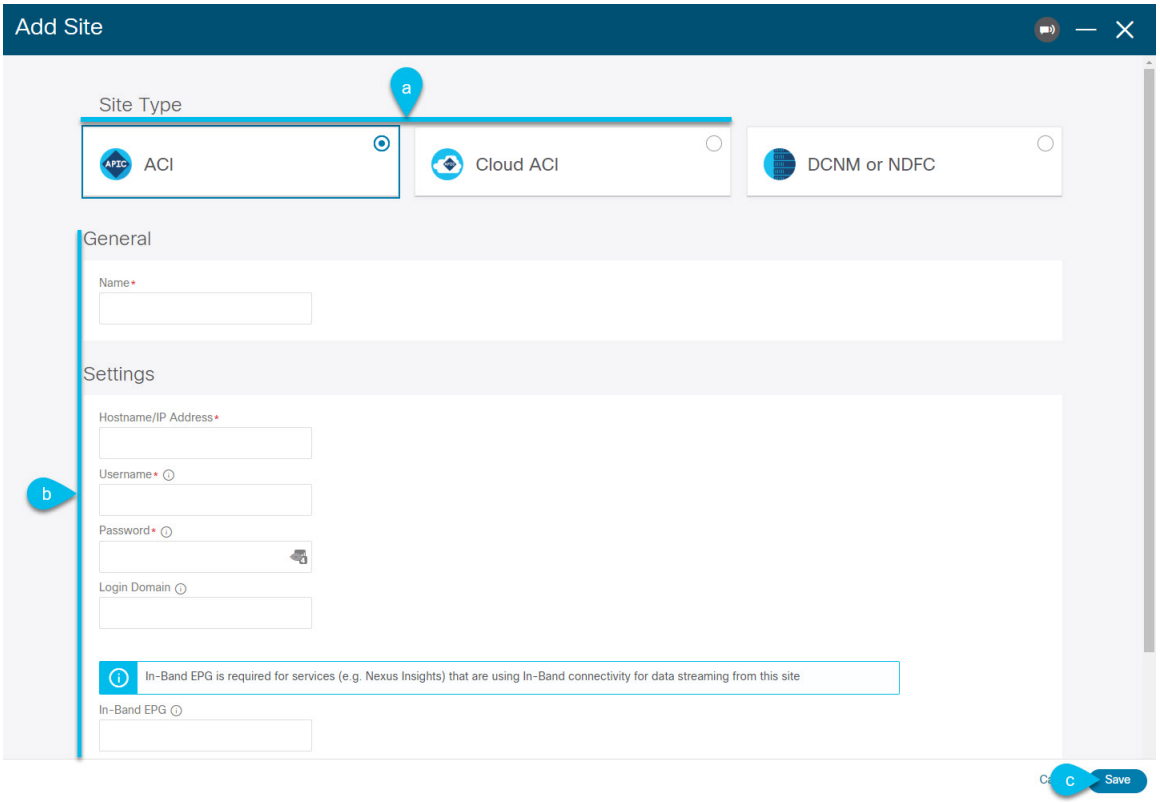
サイトを追加するには：



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

b) メインペインの右上にある**[アクション (Actions)]** > **[サイトの追加 (Add Site)]**をクリックします。

ACI サイトを追加する場合は、次の情報を入力します。



a) **[サイトのタイプ (Site Type)]** で、追加する ACI ファブリックのタイプに応じて **[ACI]** または **[クラウド ACI (Cloud ACI)]** を選択します。

b) コントローラ情報を入力します。

ACI ファブリックを現在管理している APIC コントローラについて、**[ホスト名/IP アドレス (Host Name/IP Address)]**、**[ユーザー名 (User Name)]**、および **[パスワード (Password)]** を入力する必要があります。用です。ホストする予定のアプリケーションが NDO だけである場合は、オンプレミス APIC のインバン

ドアドレスまたはアウトオブバンドアドレスのどちらでも指定できます。ただし、Nexus Insights などの他のアプリケーションをホストする場合は、インバンドアドレスを指定する必要があります。

（注） デフォルトでは、ファブリックのオンボードに使用するオンプレミス APIC の帯域内または帯域外アドレスは、Nexus ダッシュボードのデータインターフェイスから到達可能である必要があります。

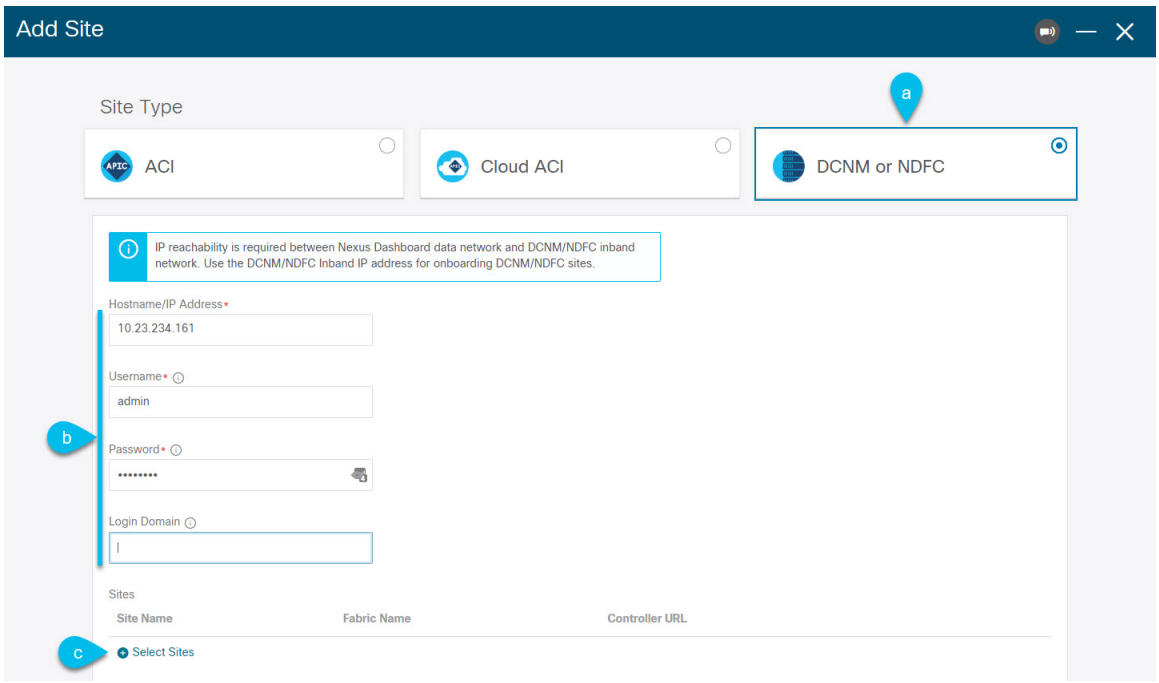
NDO トラフィックに Nexus ダッシュボードの管理インターフェイスを使用する場合は、管理インターフェイスから、Nexus ダッシュボードクラスタからファブリック IP へのスタティックルートを設定する必要があります。詳細については、『*Nexus ダッシュボード ユーザーガイド*』の「**インフラストラクチャの管理**」>「**クラスタ構成**」の章を参照してください。

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

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

この時点で、サイトは Nexus ダッシュボードで使用できるようになりますが、次の手順で説明するように、Nexus Dashboard Orchestrator の管理用にそれらのサイトを有効にする必要があります。

NDFC または DCNM サイトを追加する場合は、次の情報を入力します。



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

b) コントローラ情報を入力します。

以下の情報を指定する必要があります。

- **ホスト名/IP アドレス**：
  - DCNM の場合、これは帯域内（`eth2`）インターフェイスの IP アドレスです。
  - NDFC の場合、これは、NDFC サービスがホストされている Nexus ダッシュボードクラスタのデータインターフェイスの IP アドレスです。
- コントローラの管理者権限を持つユーザーの**ユーザー名**と**パスワード**

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、既存の Multi-Site 展開で管理している 1 つ以上のファブリックをオンにし、**[選択 (Select)]** をクリックします。

既存の Multi-Site 展開からすべてのサイトを追加するには、この手順を繰り返します。

ステップ 5 Multi-Site Orchestrator で設定したリモート認証サーバを Nexusダッシュボードに追加します。

ユーザー管理は、Multi-Site Orchestrator UI から Nexus ダッシュボードの共通ユーザー管理に移行されました。そのため、*Cisco Nexus Dashboard User Guide* の説明に従って、同じリモート ユーザーと認証サーバーを Nexus ダッシュボードに追加する必要があります。

管理者が以前に Multi-Site Orchestratorで直接設定したローカル ユーザーは、既存の設定バックアップをインポートすると、Nexus ダッシュボードに自動的に追加されます。

ステップ 6 Multi-Site Orchestrator で構成した任意のプロキシ構成を Nexus ダッシュボードに追加します。

プロキシ構成は、Multi-Site Orchestrator UI から Nexus ダッシュボードの共通クラスタ構成に移動しました。そのため、*Cisco Nexus Dashboard User Guide* の説明に従って、プロキシサーバーを Nexus Dashboard に追加する必要があります。

既存のプロキシ構成は自動的に移行されないため、移行後に Nexus ダッシュボードに手動で再追加する必要があります。

新しいクラスタでの設定の復元

ここでは、以前の設定を復元するために使用する、新しい Nexus ダッシュボード クラスタと NDO サービスを展開して設定する方法について説明します。

始める前に

次の前提条件があります。

- 既存のクラスタ設定のバックアップ （90 ページ）の説明に従って、既存の設定をバックアップしていること。

- 新規クラスタの準備 （91 ページ）の説明に従って、Nexus ダッシュボード クラスタを展開し、Nexus Dashboard Orchestrator サービスをインストールしていること。

ステップ 1 既存の Multi-Site Orchestrator クラスタを接続解除します。

移行中にサイトと通信しないように、既存の Multi-Site Orchestrator クラスタは接続解除する必要があります。

既存のクラスタをアップグレードするのではなく、新しい Nexus ダッシュボード クラスタを展開する場合は、新しいクラスタが展開されて設定が復元されるまで、既存の Multi-Site Orchestrator クラスタを保持することを推奨します。

ステップ 2 新しいNexusダッシュボードクラスタが稼働中であり、NDOサービスがインストールされていることを確認します。

NDOサービスは、新規インストールで、サイトまたはポリシーの設定を変更していないものであることが必要です。

ステップ 3 Nexus Dashboard の GUI にログインします。

ステップ 4 すべてのサイトが Nexus ダッシュボードにオンボードされていることを確認します。

バックアップを復元すると、NDOは、バックアップ内のすべてのサイトが、一致するサイト名とタイプでNexusダッシュボードに存在することを検証します。検証が失敗した場合、たとえば、Nexusダッシュボードでサイトがオンボードされていない場合、設定の復元は失敗します。再試行する前に、前のセクションで説明しているように、サイトをオンボードする必要があります。

ステップ 5 新しい Nexus Dashboard Orchestrator サービスを開きます。

ステップ 6 設定バックアップ用のリモート ロケーションを追加します。

このリリースの Nexus Dashboard Orchestrator では、クラスタのローカルディスクに保存されている設定のバックアップをサポートしていません。したがって、移行前に保存したバックアップをインポートする前に、Nexus Dashboard Orchestrator でリモート ロケーションを設定し、そこに設定のバックアップをインポートする必要があります。

a) 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。

b) 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。

c) 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
- ステップ

（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。

d) 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。

e) 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。たとえば、*/backups/ndo* です。

（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。

f) 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。

g) 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。

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

ステップ 7 新しい Nexus Dashboard Orchestrator クラスタにバックアップ ファイルをインポートします。

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

f) **[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、ファイルは、クラスタノードに直接保存されるのではなく、リモートサーバーにのみ保存する点に注意してください。

ステップ 8 設定を復元します。

a) 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。

b) **[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。

設定が復元されると、以前 Multi-Site Orchestrator で管理され、Nexus ダッシュボードにオンボードされていたサイトの、GUI での NDO 管理が有効になります。設定のバックアップに Nexus ダッシュボードにオンボードされていないサイトが含まれている場合、バックアップの復元は `Pre-restore check failed` エラーで失敗します。欠落しているサイトをオンボードした後に手順を繰り返す必要があります。

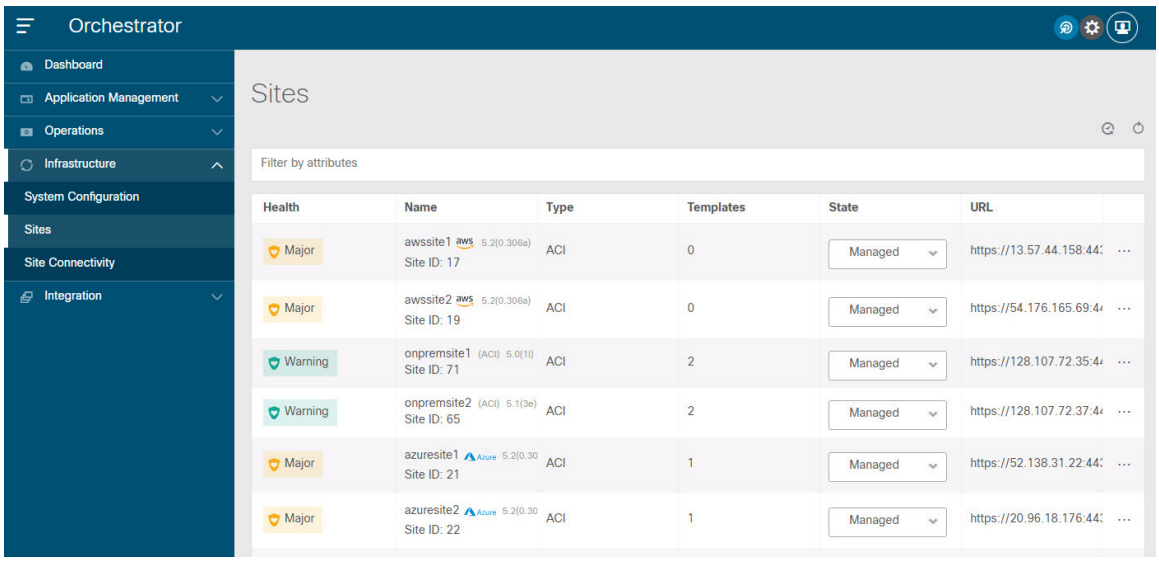
設定をインポートして復元すると、いくつかのサービスが再起動されます。

ステップ 9 パスワードを更新します。

CSDL（Cisco Secure Development Lifecycle）の要件により、設定の復元が完了した後に `admin` ユーザーのパスワードを更新する必要があります。

ステップ 10 バックアップが正常に復元され、すべてのオブジェクトと設定が存在することを確認します。

a) **[サイト (Sites)]** ページで、すべてのサイトが `[管理対象 (Managed)]` としてリストされていることを確認します。



b) **[テナント (Tenants)]** および **[スキーマ (Schemas)]** ページで、以前の Multi-Site Orchestrator クラスタのすべてのテナントとスキーマが存在することを確認します。

c) **[インフラストラクチャ（Infrastructure）]** > **[サイトの接続（Site Connectivity）]** に移動し、サイト間接続が変更されていないことを確認します。

メインペインで、各サイトの隣の **[接続ステータスの表示（Show Connectivity Status）]** をクリックし、既存の `[/30]` トンネルが稼働しており、接続が中断されていないことを確認します。

d) メインペインで **[構成（Configure）]** をクリックして **[ファブリック接続インフラ（Fabric Connectivity Infra）]** 画面を開き、**外部サブネットプール**のアドレスを確認します。

[ファブリック接続インフラ（Fabric Connectivity Infra）] 画面の **[全般設定（General Settings）]** > **[IPSec トンネルサブネットプール（IPSec Tunnel Subnet Pools）]** タブを選択して外部サブネットプールを表示し、Cloud APIC で以前に構成された外部サブネットプールがクラウドサイトからインポートされていることを確認できます。

これらのサブネットは、オンプレミス接続のためのクラウド ルータの IPsec トンネル インターフェイスとループバックのアドレス指定のために使用されるもので、以前の Nexus Dashboard Orchestrator リリースのクラウド APIC では、直接設定する必要がありました。

（注） 次の項で説明するように、クラウド サイトがクラウド APIC リリース 5.2(1) にアップグレードされるまで、この段階で変更を加えたり、設定を展開したりしないでください。

クラウド サイトのアップグレード

Nexus Dashboard Orchestrator をこのリリースに移行した後には、NDO で管理されていたクラウド APIC サイトをすべてリリース 5.2(1) 以降にアップグレードする必要があります。既存のサイト間接続はそのまま残りますが、リリース 5.2(1) より前のリリースのクラウド APIC を実行しているサイトに対し、クラウドサイトのインフラ設定を変更または展開することはできません。

始める前に

次の前提条件があります。

- 新規クラスタの準備 （91 ページ）の説明に従って、Nexus ダッシュボード クラスタを展開し、Nexus Dashboard Orchestrator サービスをインストールしていること。
- 新しいクラスタでの設定の復元 （95 ページ）の説明に従って、既存の設定のバックアップが新しいクラスタに復元されていること。

ステップ 1 クラウド サイトをアップグレードします。

各クラウド サイトでは、次のサイトのアップグレードに進む前に、クラウド APIC をアップグレードしてから CSR をアップグレードする必要があります。サイトがアップグレードされて正常になったら、同じ手順を繰り返して追加のサイトをアップグレードできます。

a) サイトのクラウド APIC をアップグレードします。

クラウド APIC を通常の方法でアップグレードする場合には、Cisco Cloud APIC for Azure Installation Guide または Cisco Cloud APIC for AWS Installation Guide の「Performing a System Upgrade、Downgrade or Recovery」の章に詳述されている手順に従ってください。

クラウド APIC のアップグレード後、既存のパブリック IP トンネルはそのまま残り、パブリック IPsec 経由のサイト間接続は中断されません。

b) そのサイトの CSR をアップグレードします。

クラウド APIC リリース 5.2(1) 以降では、以前のリリースのように CSR のアップグレードは自動的に行われないため、クラウド APIC のアップグレード後に手動で CSR アップグレードをトリガーする必要があります。次のサイトのアップグレードに進む前に、サイトの CSR をアップグレードする必要があります。

クラウド APIC CSR をアップグレードする場合には、Cisco Cloud APIC for Azure Installation Guide または Cisco Cloud APIC for AWS Installation Guide の「Performing a System Upgrade、Downgrade or Recovery」の章に詳述されている手順に従ってください。

各サイトで CSR をアップグレードすると、次のようになります。

- 各 CSR がアップグレードされると、既存の `/30` トンネルが再作成され、トラフィックは継続します。
- いずれかのクラウド サイトで 5.2(1) より前のリリースのクラウド APIC または CSR が実行されている限り、Nexus Dashboard Orchestrator からのトンネル管理およびすべてのインフラ設定変更は無効になります。
- 最後にアップグレードしたサイトが AWS クラウドサイトである場合、そのサイトの CSR についてのみ以下が発生します。
  - 最後のクラウド サイトのトンネル エンドポイントはクラウド APICによって削除され、NDO はエンドポイントを使用する対応するトンネルを削除します。
  - NDOは、最後のクラウド サイトの CSR から発するトンネルを削除します。
  - 新しい `hcloudInterCloudSiteTunnel` MOが作成され、Nexus Dashboard Orchestrator のトンネル管理が新しいトンネルに `/31` のアドレスを割り当てます。
  - このサイトの CSR と、このサイトとピアリングしている別のクラウド サイトの CSR は、`/31` トンネルを確立します。

  最後にアップグレードしたサイトが Azure サイトの場合、同じように `/30` トンネルが CSR に作成されます。上記の 4 つの箇条書きは関係ありません。

移行プロセスの完了後に既存のCSRに追加したCSRまたはアンダーレイ設定の変更については、NDO によって作成された新しいトンネルはすべて `/31` トンネルになります。

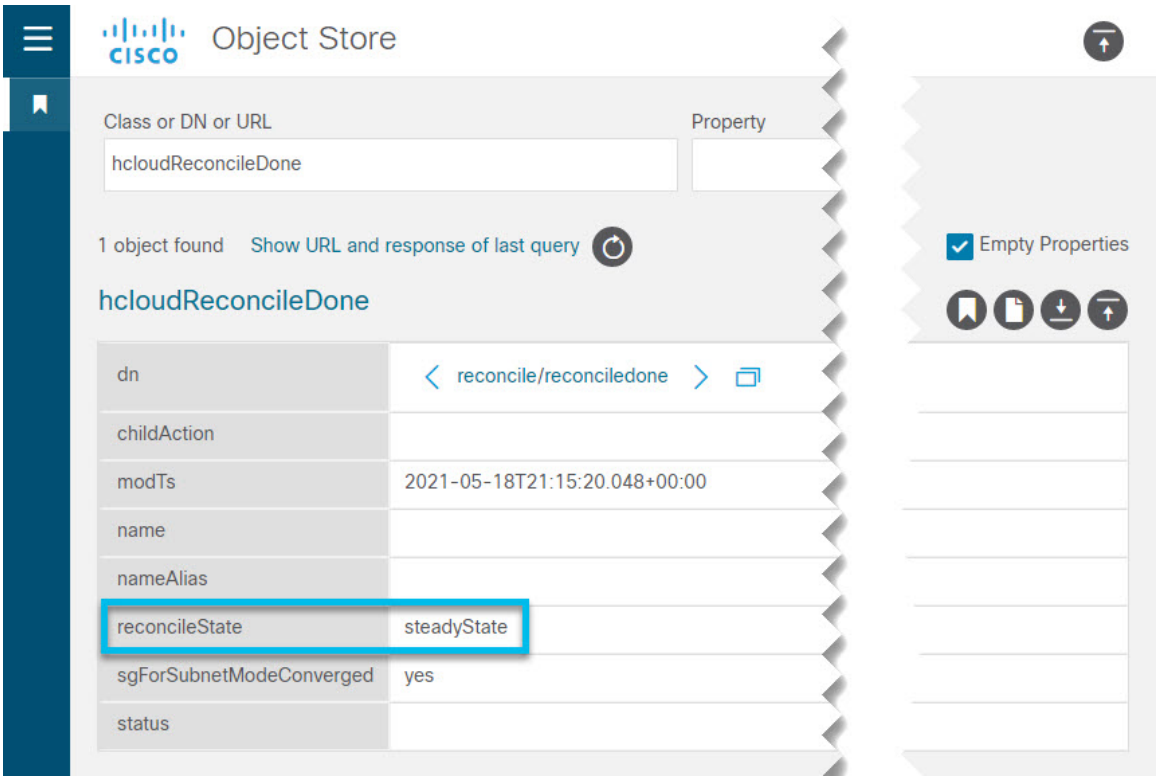
（注） CSR のアップグレードが完了して CSR が起動してから 5 分以内に BGP セッションが表示されない場合は、**[Nexus Dashboard Orchestrator Infra Configuration]** 画面でサイトのインフラ接続を更新します。

c) クラウド サイトごとにこの手順を 1 つずつ繰り返します。

ステップ 2 クラウド APIC と CSR のアップグレードが完了していることを確認します。

a) 各サイトのクラウドAPICで、`hcloudReconcileDone` MO に `reconcileState=steadyState` が表示されていることを確認します。

MO は、`https://<cloud-apic-ip>/visore.html` に移動し、`hcloudReconcileDone` を **[クラスまたは DN または URL (Class or DN or URL)]** フィールドで検索すれば、確認できます。



b) Nexus Dashboard Orchestrator で、**[インフラストラクチャ（Infrastructure）]** > **[サイトの接続（Site Connectivity）]** に移動し、サイト間の接続が損なわれていないことを確認します。

メインペインで、各サイトの横にある **[接続ステータスを表示（Show Connectivity Status）]** をクリックし、[オーバーレイ ステータス（Overlay Status）] タブと [アンダーレイ ステータス（Underlay Status）] タブで接続が正常であることを確認します。

c) Nexus Dashboard Orchestrator の **[サイトの接続（Site Connectivity）]** ページで **[構成（Configure）]** をクリックして、以前にクラウド APIC で設定された外部サブネット プールがインポートされ、存在することを確認します。

[ファブリック接続インフラ（Fabric Connectivity Infra）] 画面の **[全般設定（General Settings）]** > **[IPSec トンネル サブネット プール（IPSec Tunnel Subnet Pools）]** タブを選択すると、外部サブネットプールを表示できます。

d) Nexus Dashboard Orchestrator の **[ファブリック接続インフラ（Fabric Connectivity Infra）]** 画面で、クラウドサイトを選択し、右側のサイドバーの **[サイト間接続（Inter-Site Connectivity）]** タブをクリックして、パブリック IP を使用したアンダーレイ接続が既存のサイトに保持されていることを確認します。

クラウド サイト用の NDO インフラ設定の更新

インフラストラクチャ設定を変更するには、クラウド サイトをクラウド APIC リリース 5.2(1) にアップグレードした直後に、次の情報を提供する必要があります。

- OSPF エリア ID。
- IPN 設定

（注） 該当するクラウドサイトがない場合は、このセクションをスキップできます。

始める前に

次の前提条件があります。

- 新規クラスタの準備 （91 ページ）の説明に従って、Nexus ダッシュボード クラスタを展開し、Nexus Dashboard Orchestrator サービスをインストールしていること。
- 新しいクラスタでの設定の復元 （95 ページ）の説明に従って、既存の設定のバックアップが新しいクラスタに復元されていること。
- クラウド サイトのアップグレード （99 ページ）の説明に従って、クラウドサイトをアップグレードしていること。

ステップ 1 新しい Nexus Dashboard Orchestrator 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 **[OSPF エリア ID（OSPF Area ID）]** を入力します。

これは、以前の Nexus Dashboard Orchestrator リリースでサイト間接続用にクラウド APIC で以前に設定した、オンプレミス ISN ピアリング用のクラウド サイトで使用される OSPF エリア ID です。

ステップ 6 **[IPN デバイス (IPN Devices)]** 情報を追加します。

a) **[デバイス (Devices)]** タブを選択します。

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

c) オンプレミス IPN デバイスの **[名前 (Name)]** と **[IP アドレス (IP Address)]** を入力します。

IPN デバイスの管理 IP アドレスではなく、クラウド APIC の CSR からトンネル ピア アドレスとして使用されるオンプレミス サイトのデバイスの IP アドレスを指定する必要があります。

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 オンプレミスとクラウドサイト間のサイト間接続の**[アンダーレイ設定 (Underlay Configuration)]** を更新します。

クラウドサイトに接続するオンプレミス サイトごとに、前の手順で追加した IPN デバイスの IP アドレスのうち少なくとも 1 つを指定する必要があります。このアドレスに、クラウド APIC の CSR がトンネルを確立します。

a) 左側のペインの **[サイト (Sites)]** の下で、オンプレミス サイトを選択します。
b) 右側の **<サイト *(Site)*> [設定 (Settings)]** ペインで、**[アンダーレイ設定 (Underlay Configuration)]** タブを選択します。
c) **[+ IPN デバイスの追加 (+ Add IPN Device)]** をクリックして、IPNデバイスを指定します。
d) ドロップダウンから、前に定義した IPN デバイスのいずれかを選択します。

IPNデバイスは、**[一般設定 (General Settings)]** > **[IPN デバイス (IPN Devices)]**リストですでに定義されている必要があります。

ステップ 8 画面上部のドロップダウンから **[展開 (Deploy)]** を選択して、インフラ設定を再展開します。

設定のばらつきの解決とテンプレートの再展開

Nexus Dashboard Orchestrator は、以前は APIC で直接管理する必要があったオブジェクトプロパティの管理のサポートを追加するたびに、それらのプロパティを NDO スキーマ内の既存のオブジェクトのデフォルト値に設定しますが、サイトにはプッシュしません。リリース 3.3(1) より前の Multi-Site Orchestrator リリースからこのリリースに移行する場合は、このセクションで説明するように、構成のばらつきを解決し、テンプレートを再展開する必要があります。

（注） 構成のばらつきを解決する前にテンプレートを展開すると、Orchestrator で定義された構成をプッシュし、ファブリックのコントローラで定義された値を上書きします。

また、リリース 3.2(1) 以前に最初に移行する場合は、データベース内の情報を再構築するために必要なすべてのテンプレートが強制的に再展開されるため、すべてのテンプレートで明示的に構成のばらつきが発生します。この場合、コントローラレベルでプロパティが変更された可能性があるすべてのオブジェクトをインポートしてから、テンプレートを再展開することをお勧めします。

始める前に

次の前提条件があります。

- 新規クラスタの準備 （91 ページ）の説明に従って、Nexus ダッシュボード クラスタを展開し、Nexus Dashboard Orchestrator サービスをインストールしていること。

- 新しいクラスタでの設定の復元 （95 ページ）の説明に従って、既存の設定のバックアップが新しいクラスタに復元されていること。
- クラウド サイトのアップグレード （99 ページ）の説明に従って、クラウドサイトをアップグレードしていること。
- クラウド サイト用の NDO インフラ設定の更新 （102 ページ）の説明に従って、クラウドサイトのNexus Dashboard Orchestrator のインフラ設定を更新していること。

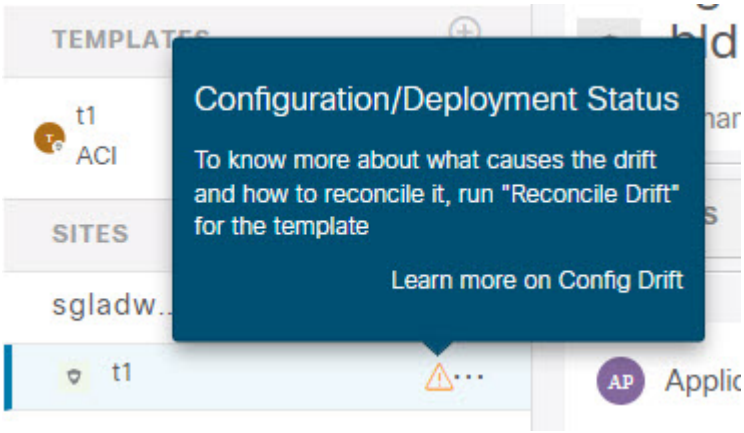
ステップ 1 Nexus Dashboard Orchestrator で、**[アプリケーション管理 (Application Management)]** > **[スキーマ (Schemas)]** に移動します。

ステップ 2 最初のスキーマを選択し、そのテンプレートで構成ドリフトを確認します。

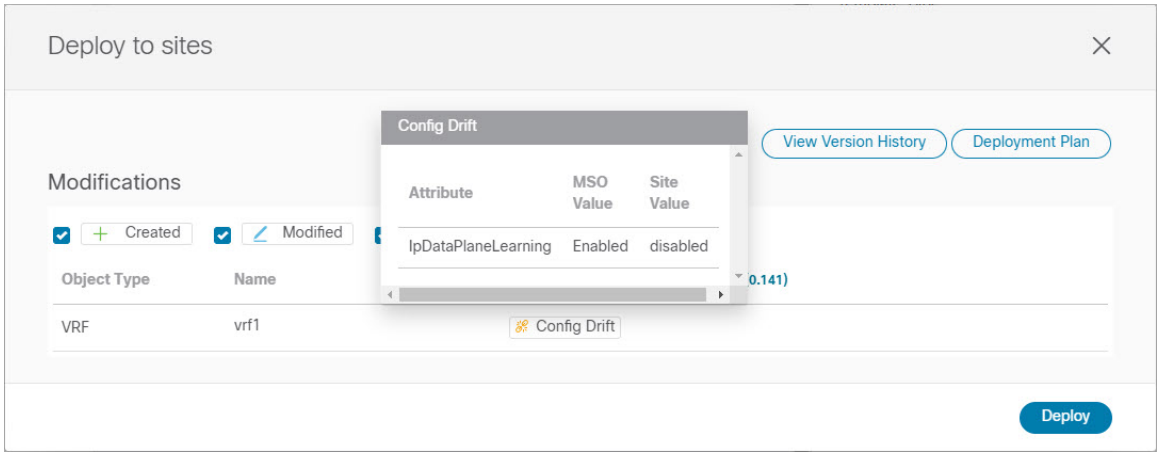
展開内のすべてのスキーマとテンプレートについて、次の手順を繰り返します。

次の 2 つの方法のいずれかで、構成のばらつきを確認できます。

- 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、**[サイトへの展開 (Deploy to sites)]** をクリックして構成比較画面を呼び出し、構成のばらつきが含まれているオブジェクトを確認します。



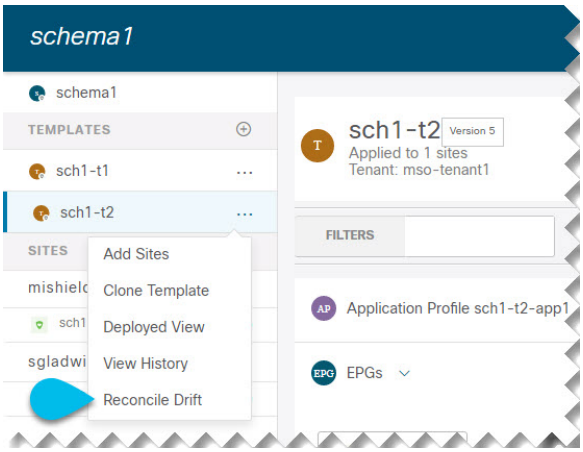
ステップ 3 テンプレートに構成のばらつきが含まれている場合は、競合を解決します。

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。

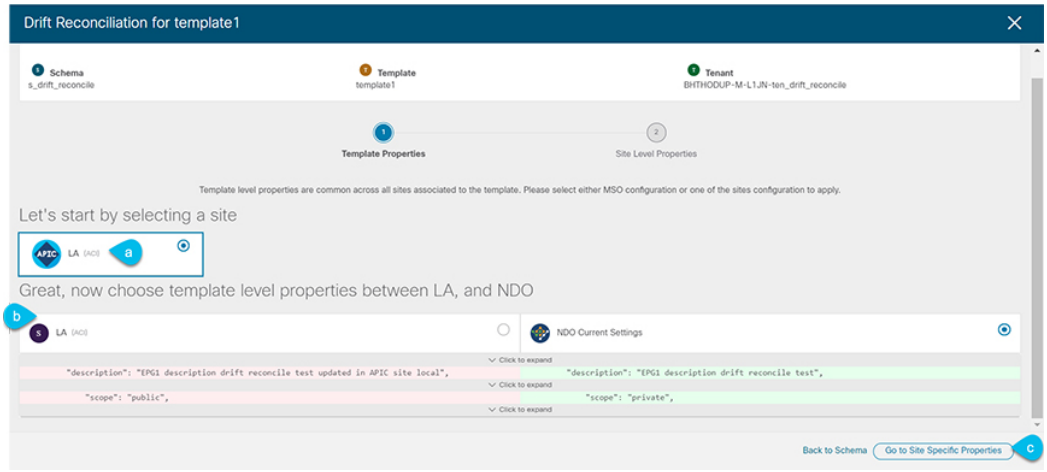
この時点でテンプレートを展開すると、Orchestrator データベースの値をプッシュして、ファブリックの既存の設定を上書きします。

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。

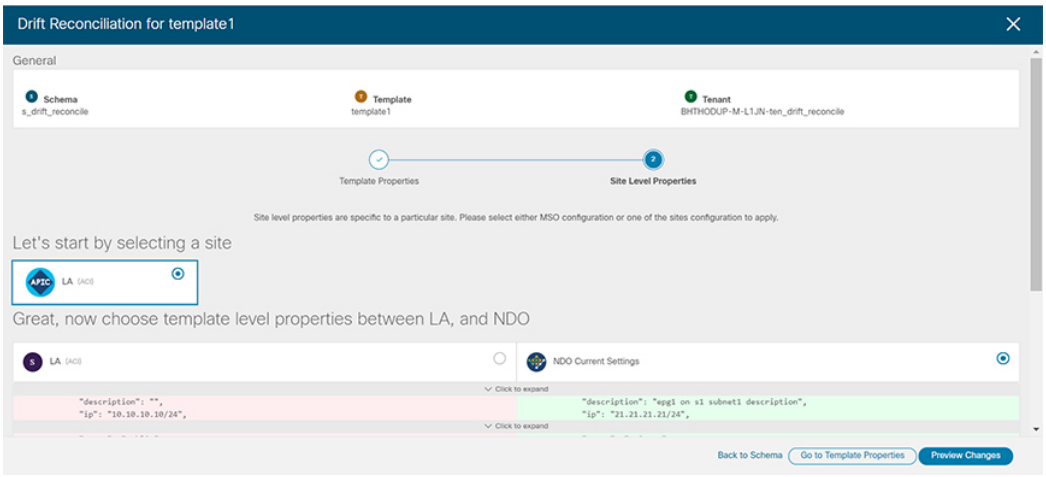
c) **[ばらつきの調整 (Reconcile Drift)]** 画面で、各サイトのテンプレートレベルの構成を比較し、希望のものを選択します。



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。サイト構成を選択すると、既存の Nexus Dashboard Orchestrator テンプレート内のこれらのプロパティが変

更されますが、Nexus Dashboard Orchestrator 構成を選択した場合は、既存の Nexus Dashbaord Orchestrator テンプレートの設定はそのまま保持されます。

d) **[サイト固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 レベルの構成とサイト レベルの構成のどちらでも同じ選択を行いますが、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定義されている構成を「テンプレートのプロパティ」レベルで選択し、Nexus Dashboard Orchestrator で定義された構成を 「サイトのローカルプロパティ」レベルで選択したり、またその逆で選択したりすることもできます。

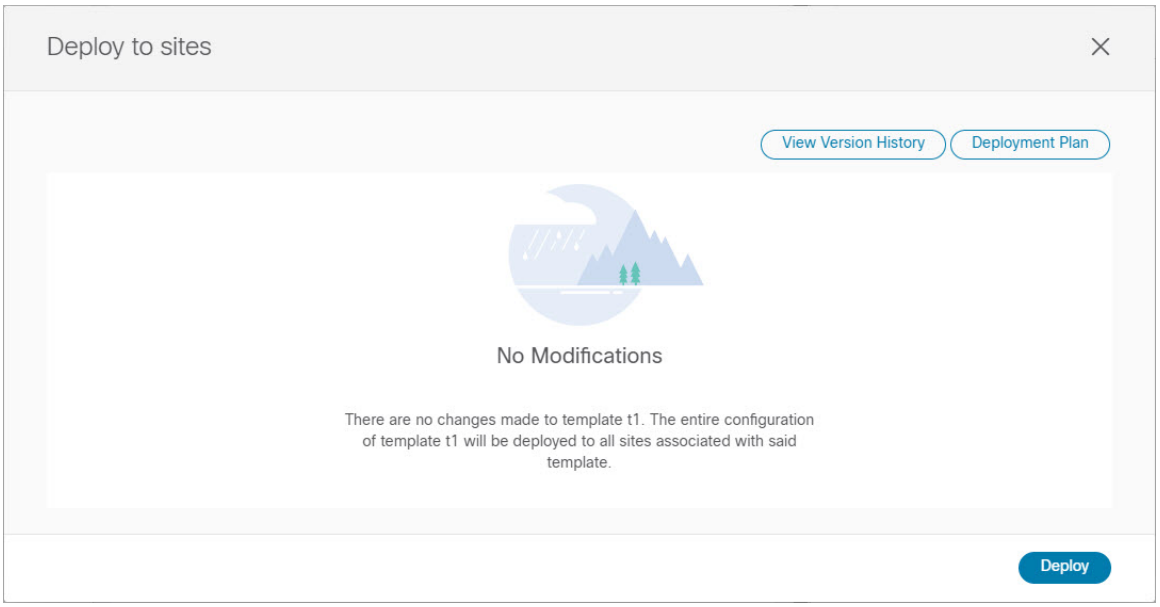
e) **[変更のプレビュー（Preview Changes）]** をクリックして、選択内容を確認します。

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)]** をクリックして設定を展開し、そのテンプレートのばらつきを調整できます。

ステップ 4 すべての構成のばらつきが解決され、**[サイトへの展開（Deploy to sites）]** ダイアログに変更が表示されなくなったら、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。

次の図に示すように、**[サイトへの展開（Deploy to sites）]** ダイアログに変更が含まれていないことを確認し、**[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 5 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 6 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。