Cisco Nexus Dashboard Orchestrator 展開ガイド、リリース 3.4(x)

初版：2021 年 7 月 30 日

最終更新：2021 年 7 月 30 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。

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

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: http://www.cisco.com/go/softwareterms.Cisco product warranty information is available at http://www.cisco.com/go/warranty. US Federal Communications Commission Notices are found here http://www.cisco.com/c/en/us/products/us-fcc-notice.html.

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

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

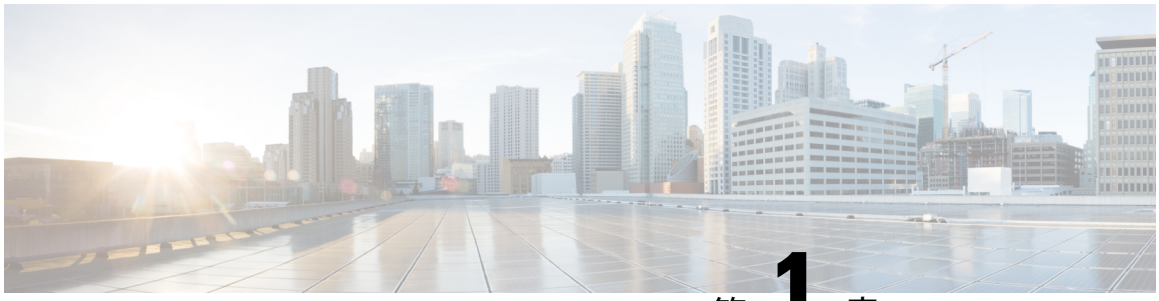
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual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

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

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

© 2021 Cisco Systems, Inc. All rights reserved.

目 次



第 1 章

新規および変更情報

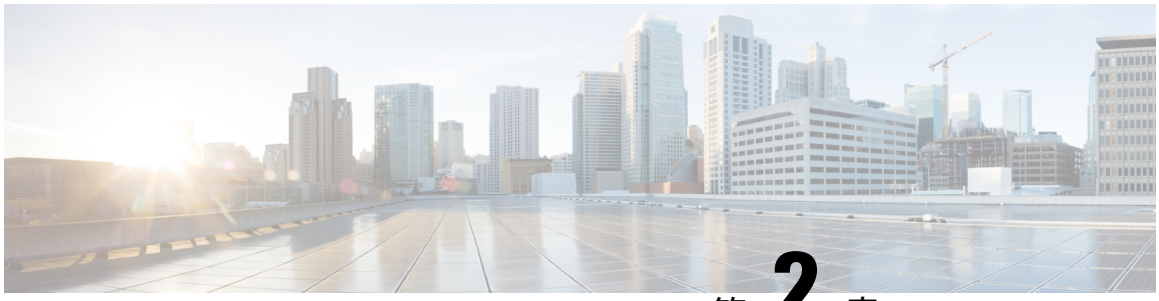
新規および変更情報

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
3.4(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

リリース 3.2(1) 以降では、Cisco Nexus Dashboard Orchestrator（NDO）を Cisco Nexus Dashboard のアプリケーションとして展開する必要があります。

（注）

リリース 3.2(1) は Nexus Dashboard の物理フォーム ファクタのみをサポートしていましたが、リリース 3.3(1) 以降は物理、仮想、またはクラウドの Nexus Dashboard クラスタに導入できます。

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、この項で説明する導入の概要をよく理解し、Nexus Dashboard への既存のクラスタの移行 （79 ページ） の手順に従ってください。

Cisco Nexus Dashboard は、複数のデータ センター サイト向けの中央管理コンソールであり、Nexus Dashboard Orchestrator や Nexus Insights などのシスコ データ センター アプリケーション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アプリケーション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、さまざまな最新アプリケーションのライフ サイクル管理を簡素化し、これらのアプリケーション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 Dashboard クラスタは、3 つのマスターノードで構成されます。また、最大 4 つのワーカー ノードを追加して水平方向のスケーリングを有効にし、最大 2 つのスタンバイ ノードを使用して、マスター ノードに障害が発生した場合にクラスタを簡単に回復できます。

Nexus Dashboard 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 Dashboard 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、マニュアルでは、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、管理するファブリックのタイプに応じて、『*Cisco Multi-Site Configuration Guide for Cisco ACI*』または『*Cisco Multi-Site Configuration Guide for Cisco DCNM*』を参照してください。

前提条件とガイドライン

Nexus Dashboard

ここで説明する追加要件と Nexus Dashboard Orchestrator サービスのインストールを進める前に、『*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 3.4(1) 以降	Cisco Nexus Dashboard リリース 2.0.2h またはそれ以降 （注） Nexus Dashboard リリース 2.1.1 以降を必要とする機能は、プラットフォームをアップグレードするまで無効になります。詳細については、『*Release Notes*』を参照してください。

Nexus Dashboard のネットワーク

最初に Nexus Dashboard を設定するときは、2 つの Nexus Dashboard 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 Cisco 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 Dashboard 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 のラウンド トリップ時間（RTT）が 150 ミリ秒を超えないノード間の接続が必要です。同じ Nexus Dashboard クラスタで実行されている他のアプリケーションの RTT 要件は低くなる可能性があり、同じ Nexus Dashboard クラスタに複数のアプリケーションを展開する場合は、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 アプリを Nexus Dashboard に導入すると、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 Dashboard のネットワーク
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
クラスタ内通信	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 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ています。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』 ツールを参照してください。

Nexus Dashboard Orchestrator に加えて他のアプリケーションをホストする場合は、クラスタ サイジング ツールの推奨事項に基づいて追加の Nexus Dashboard ノードを展開し、設定してください。詳細は『Cisco Nexus Dashboard User Guide』で説明されています。また、Nexus Dashboard GUI から直接入手もできます。

（注） Nexus Dashboard Orchestrator のこのリリースは、物理 Nexus Dashboard クラスタでのみ他のサービスとホストできます。仮想またはクラウド Nexus Dashboard クラスタに Nexus Dashboard Orchestrator サービスを展開する場合は、同じクラスタに他のアプリケーション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、使用環境で 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

マルチサイトでは、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 Cloud Scale 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、マルチサイト 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。

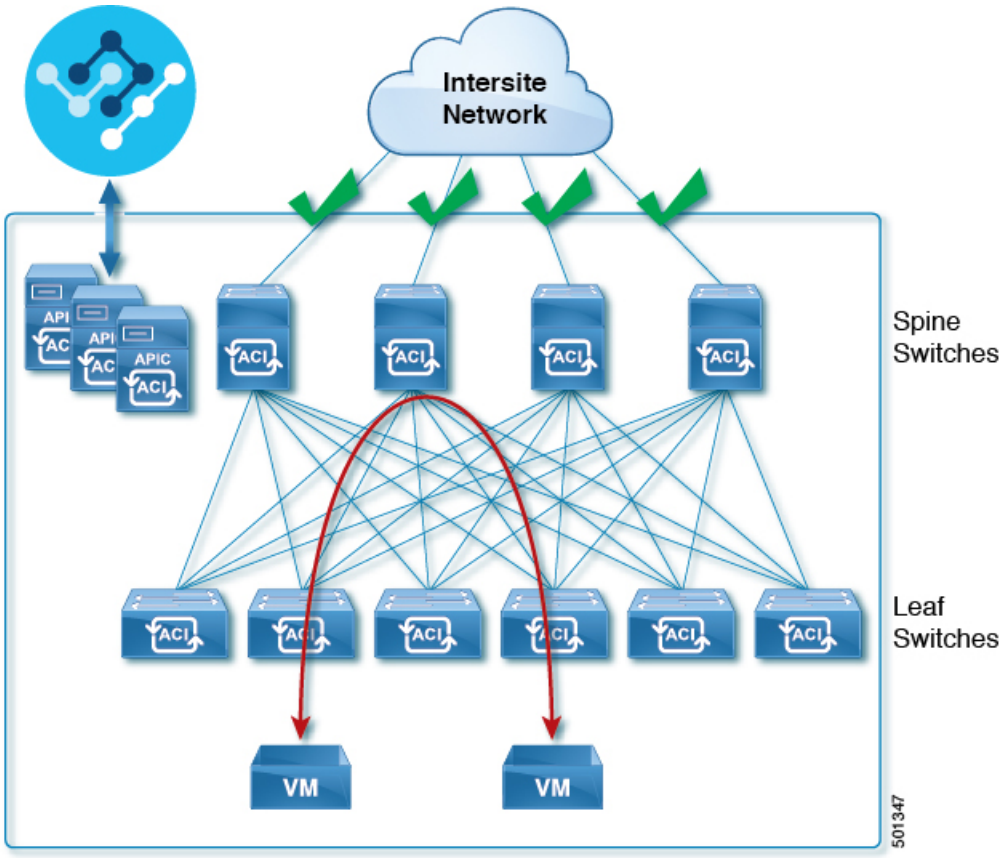
各リリースでサポートされるスパインの完全なリストについては、『ACI-mode Switches Hardware Support Matrix』 を参照してください。

リーフ スイッチの要件

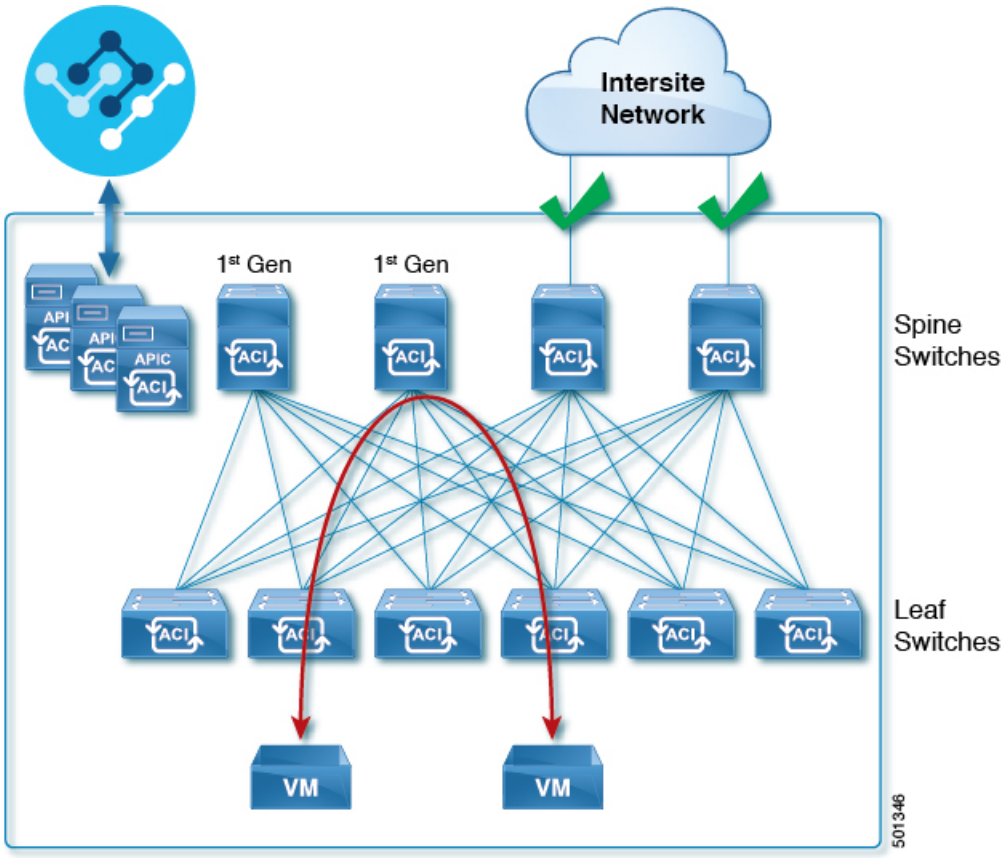
Multi-Site はファブリックのリーフ スイッチに依存しないため、Cisco APIC と同じリーフ スイッチ モデルをサポートします。サポートされているハードウェアの完全なリストは、ACI モードスイッチ ハードウェア サポート マトリックスに記載されています。

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 マルチサイト 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 Dashboard 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

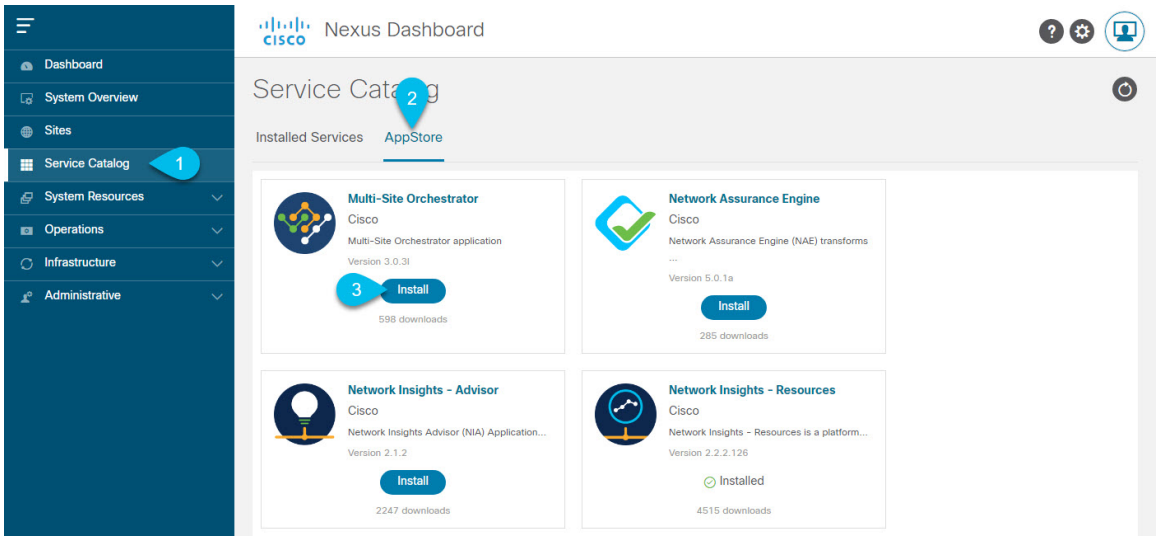
- 前提条件とガイドライン （4 ページ） に記載されている要件とガイドラインを満たしていることを確認します。
- Cisco DC App Center は、直接管理ネットワークを介して、またはプロキシ設定を使用して Nexus Dashboard から到達可能である必要があります。Nexus Dashboard のプロキシ設定については、 『*Nexus Dashboard User Guide*』を参照してください。

  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 （11 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 GUI にログインします

ステップ 2 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) **[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 3 開いた [License Agreement] ウィンドウで、**[同意してダウンロードする（Agree and Download）]** をクリックします。

ステップ 4 アプリケーションが Nexus Dashboard にダウンロードされ、展開されるまで待ちます。

アプリケーションがすべてのノードおよびすべてのサービスに完全に展開されるまでには、最大30分かかります。

ステップ 5 アプリケーションを有効にします。

インストールが完了すると、アプリケーションはデフォルトで `[無効（Disabled）]` 状態のままになるため、有効にする必要があります。

アプリケーションを有効にするには、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 6 アプリケーションを起動します。

アプリケーションを起動するには、Nexus Dashboard 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 Dashboard 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。

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

ここでは、Cisco Nexus Dashboard Orchestrator サービスを既存の Cisco Nexus Dashboard クラスタに手動でアップロードして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 サービスをダウンロードします。

a) DC App Center で Nexus Dashboard Orchestrator アプリ 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ます。

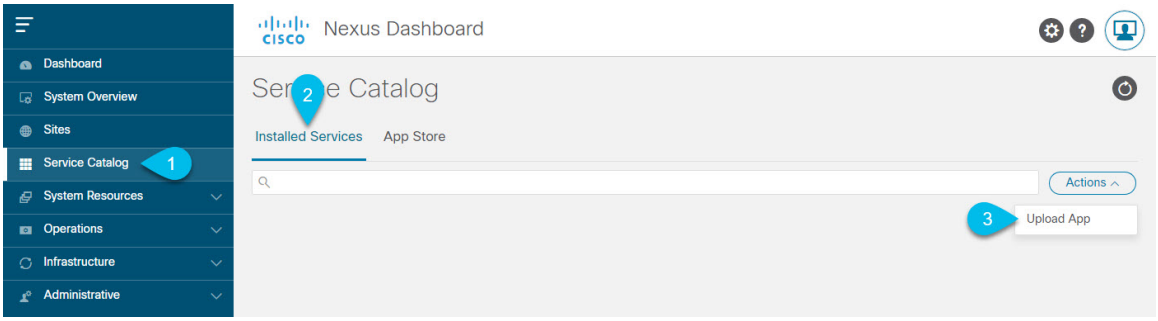
c) **[ダウンロード（Download）]** ボタンをクリックします。

d) **[同意してダウンロードする（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 ダッシュボードにログインします。

アプリケーションを展開する場合、Nexus Dashboard ノードの 1 つだけにインストールする必要があります。アプリケーションはクラスタ内の他のノードに自動的に複製されます。そのため、管理 IP アドレスを使用して Nexus Dashboard ノードのいずれかにログインできます。

ステップ 3 アプリケーション イメージをアップロードします。

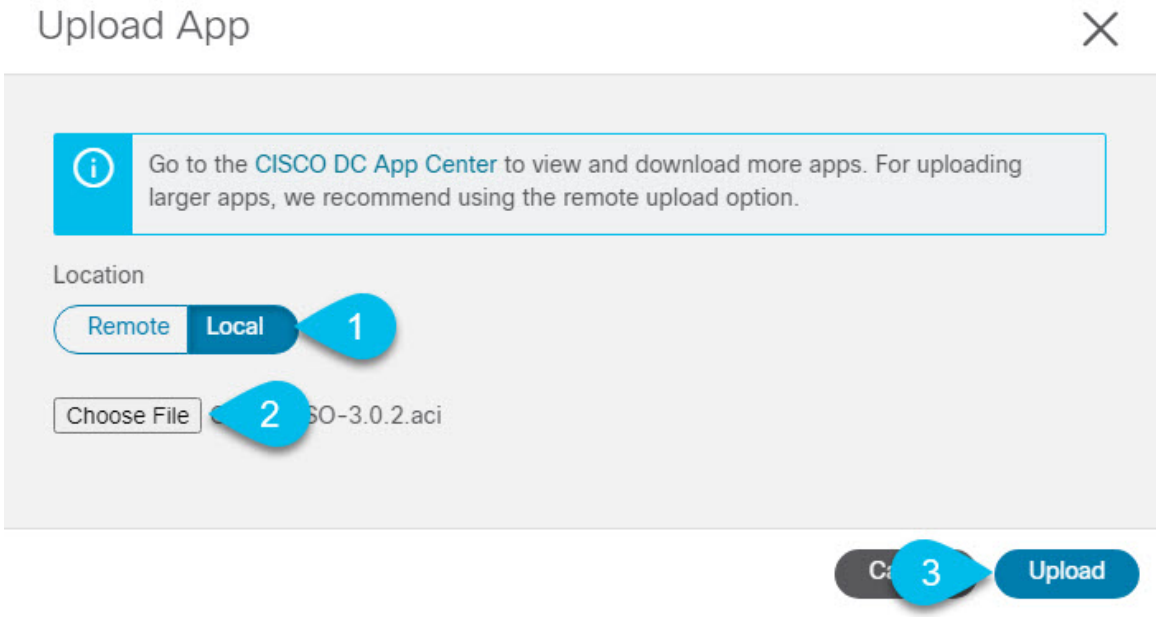


a) 左のナビゲーションバーで、**[サービス カタログ（Service Catagol）]** をクリックします。

b) **[インストール済みのサービス（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)]**>**[アプリケーションのアップロード（Upload App）]** をクリックします。

ステップ 4 イメージ ファイルを Nexus Dashboard クラスタにアップロードします。



a) 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。

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、以下のように、イメージ ファイルへの完全な URL を入力します。（http：//<ip-address>：<port>/<full-path>/cisco-mso-<version>.aci

c) **[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。

ステップ 5 アプリケーションが Nexus Dashboard にダウンロードされ、展開されるまで待ちます。

アプリケーションがすべてのノードおよびすべてのサービスに完全に展開されるまでには、最大30分かかります。

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すると、アプリケーションはデフォルトで `[無効（Disabled）]` 状態のままになるため、有効にする必要があります。

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

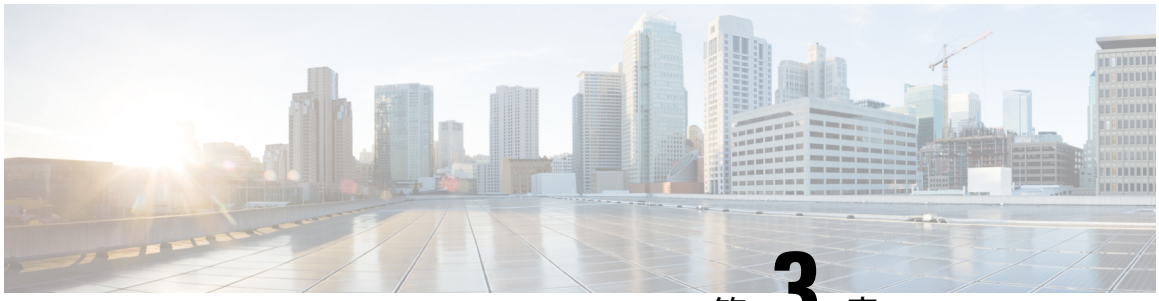
ステップ 7 アプリケーションを起動します。

アプリケーションを起動するには、Nexus Dashboard 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 Dashboard 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。

第 I 部

ACI ファブリックの 0 日目の運用



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、ファブリックを最初に展開したときに設定したとおりです。

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 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 ポッド ポリシー グループを必要に応じて、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）]**の順に移動します。

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 Group）]** を選択します。

c) 適切な情報を入力して、**[送信（Submit）]** をクリックします。

ステップ 4 ポ新しいポッド 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）]** の順に移動します。

b) デフォルト 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、**[アップデート（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 ファブリックを追加するか、Nexus Dashboard Orchestrator により管理されるに前に、各サイトで設定される必要がある多くのファブリック指定のアクセス 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 に追加および管理する前に、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 （19 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 （18 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

リリース 2.1(2) 以降、 マルチサイト アーキテクチャはリモート リーフ スイッチをもつ 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ガイドライン、制限事項、および設定手順を説明します。

リモート リーフのガイドラインと制限事項

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

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

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

- 次の項で説明するように、リモートリーフの直接通信をイネーブルにし、APIC 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

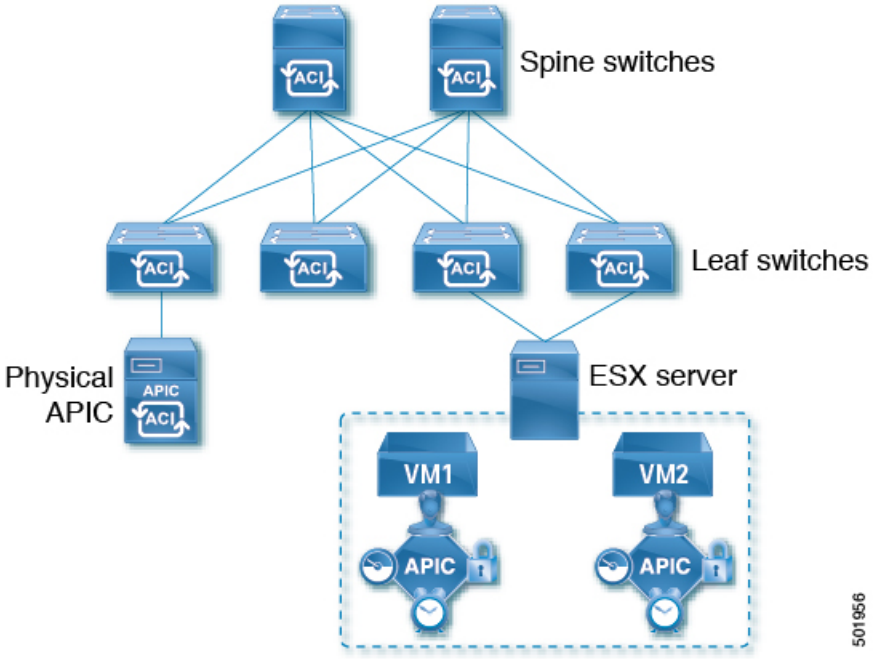
Cisco Multi-Site は、追加の設定を必要とせずに、一般的なオンプレミス サイトとして Cisco Mini ACI ファブリックをサポートします。ここでは、Mini ACI ファブリックの概要について

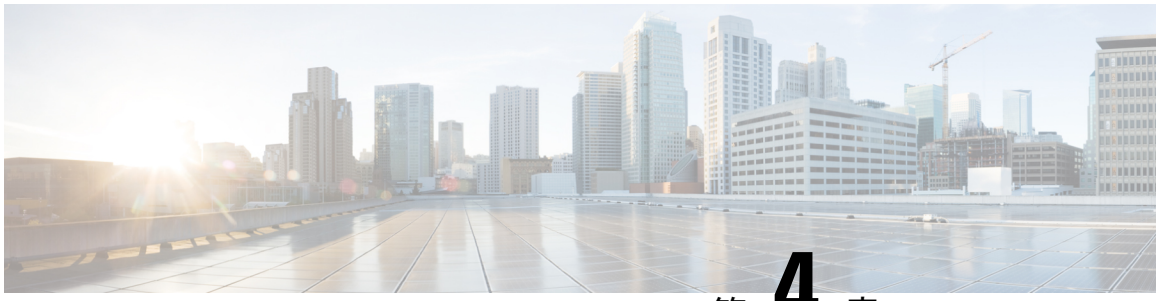
説明します。このタイプのファブリックの導入と設定に関する詳細情報は、*Cisco Mini ACI ファブリックおよび仮想 APIC* で入手できます。

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）で構成されるクラスタで動作します。Cisco APICこれにより、APIC クラスタの物理的な設置面積とコストが削減され、ACI ファブリックをラック スペースまたは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。フルスケールの ACI インストールは物理的な設置面積や初期コストにより実用的でないことがあります。

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

図 *1 : Cisco Mini ACI* ファブリック





第 4 章

サイトの追加と削除

シスコ NDO と APIC 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 Dashboard 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できます。そのため、Nexus Dashboard Orchestrator の最新リリースに常にアップグレードする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 機能が以前の APIC リリースでまだサポートされていない可能性があ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た場合、以下のようなエラー メッセージが表示されます。`この APIC サイト バージョン <site-version> は NDOで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、リリース 4.2(4) は、Nexus Dashboard 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 サポート	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)
EPG QoS の優先順位	リリース 4.2(4)
コントラクト QoS 優先度	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)
Cloud LoadBalancer 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製デバイスのサポート	Release 5.0(2)
クラウドロードバランサ 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をサポート	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	Release 5.2(1)

Cisco ACI サイトの追加

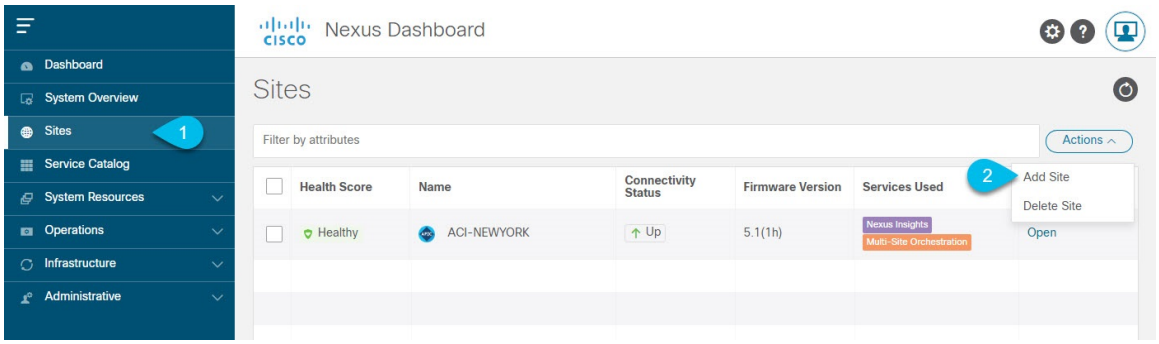
ここでは、Nexus Dashboard GUI を使用して Cisco APIC または Cloud APIC サイトを追加し、そのサイトを Nexus Dashboard Orchestrator で管理できるようにする方法について説明します。

始める前に

- オンプレミス ACI サイトを追加した場合、この章の前のセクションで説明したように、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 Dashboard GUI にログインします

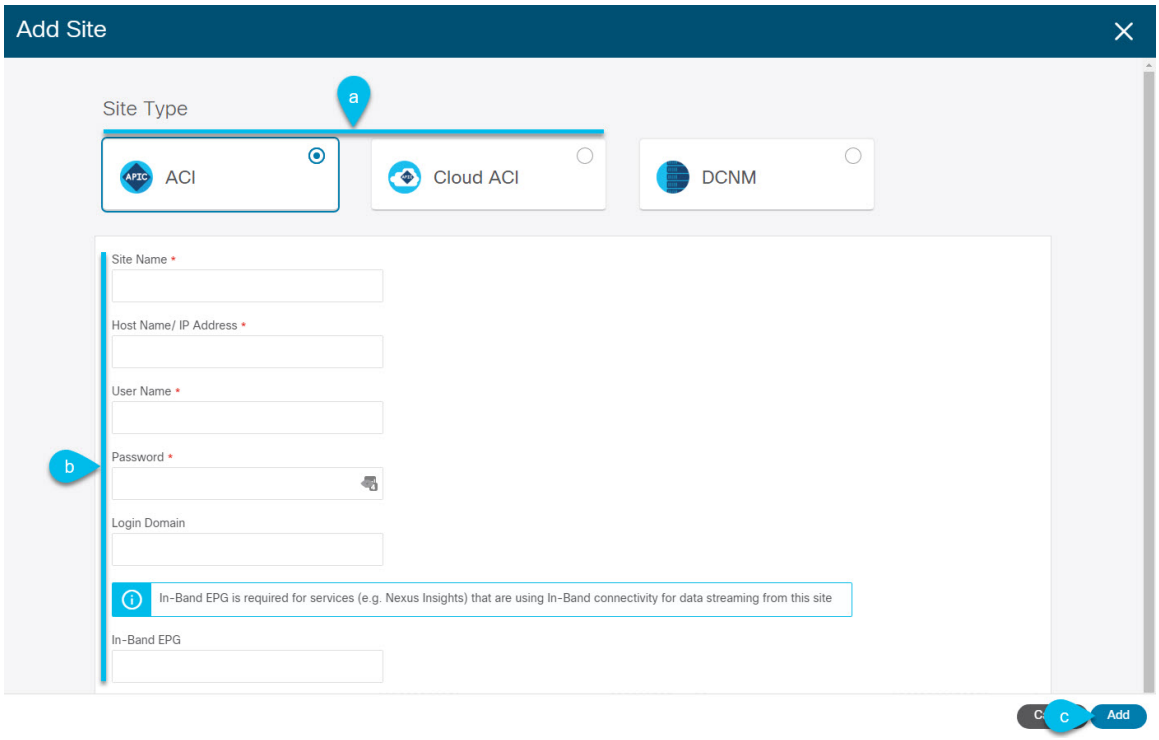
ステップ 2 新サイトを追加します。



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

b) コントローラの情報を入力します。

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

（注） APIC ファブリックの場合、Nexus Dashboard Orchestrator サービスのみでサイトを使用する場合は、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 Day-2 Operations アプリケーションで使用する場合は、Nexus Dashboard を追加している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。

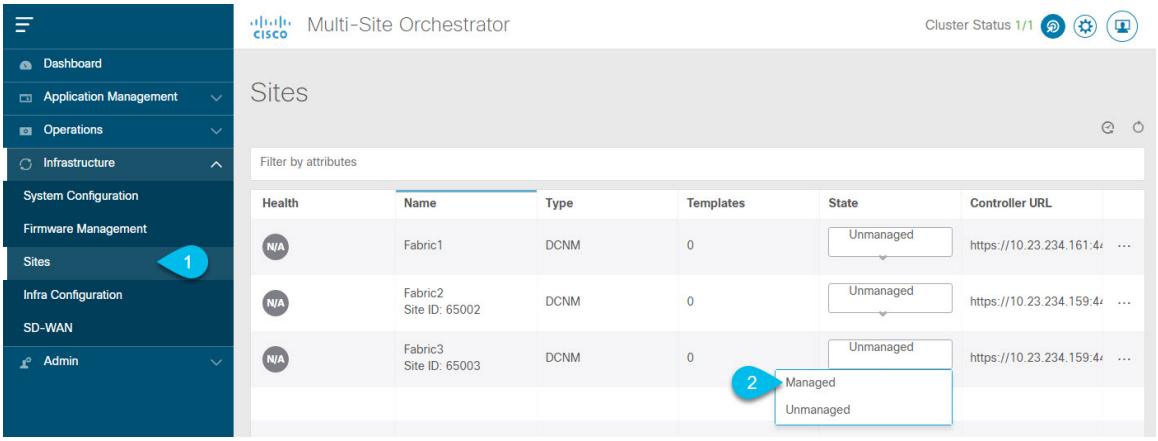
この時点で、サイトは Nexus Dashboard で使用できるようになりますが、次の手順で説明するように、Nexus Dashboard Orchestrator の管理用にそれらのサイトを有効にする必要があります。

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

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

Nexus Dashboard のユーザ 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) 左側のナビゲーション 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 の管理を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 Dashboard 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 Dashboard の**サービス カタログ**から NDO サービスを開くことができます。Nexus Dashboard のユーザ 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 メニューから、**[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、管理対象外のサイトを選択します。
d) 右側のバーの **[オーバーレイ設定（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) 左側のナビゲーション 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 の管理を停止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［管理対象外（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 Dashboard からサイトを削除することもできます。

（注） このサイトは、Nexus Dashboard クラスタにインストールされているアプリケーションで現在使用されていないことに注意してください。

a) Nexus Dashboard 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（Delite 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。

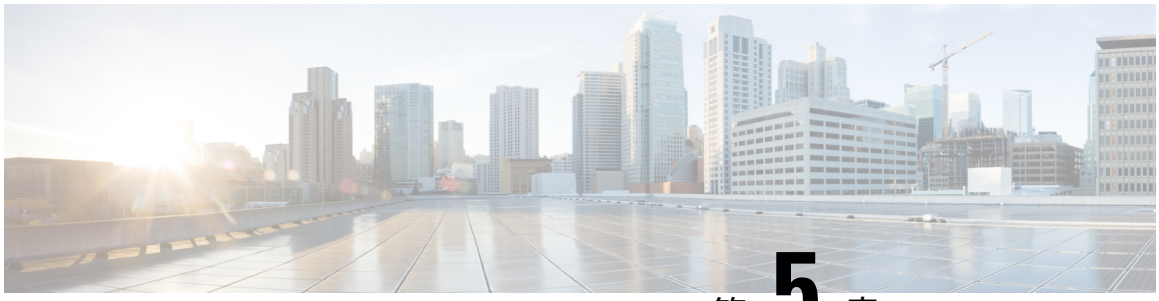
Nexus Dashboard からサイトが削除されます。

ファブリックコントローラへの相互起動

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。その他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 > サイト**（Infrastucture 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 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。



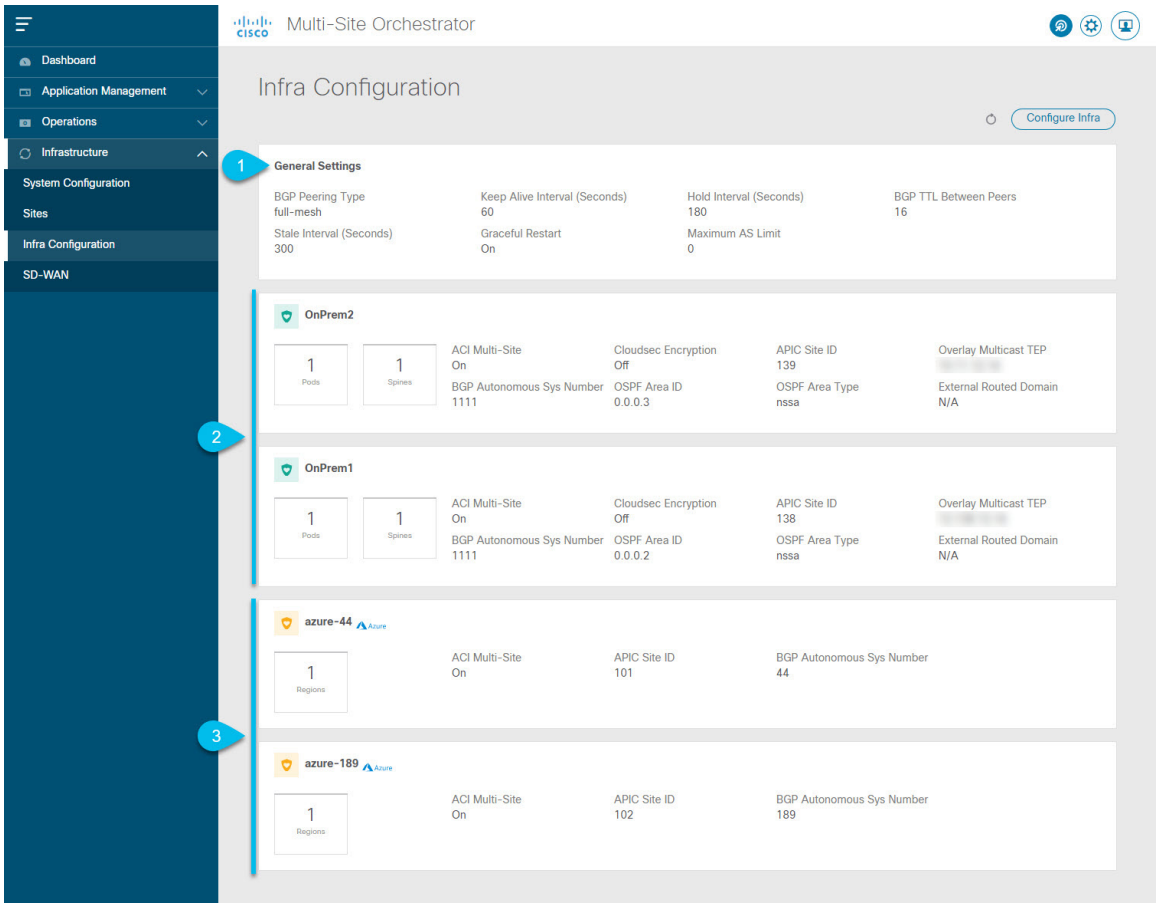
第 5 章

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 導入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、以下の情報が含まれます。

図 *2:* インフラ設定の概要



1. **[一般設定（General Settings）]** タイルには、BGP ピアリング タイプとその設定に関する情報が表示されます。

   この詳細は、後のセクションで説明します。

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

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

   詳細については、を参照してください。Cisco APIC サイトのインフラの設定 （37 ページ）

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

   詳細については、Cisco Cloud APIC サイトのインフラの設定 （43 ページ） を参照してください。

次のセクションでは、一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 スイッチまたはスパイン ノード ID の変更の追加や削除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（37 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 BGP（Control Plane BGP）]** 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。

  `[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。

次の設定は、クラウド サイトのサイト間接続用です。

a) **[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。

b) **[+ 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。

ステップ 6 **[IPN デバイス情報]** を入力します。

後のセクションで説明するように、オンプレミスとクラウドサイト間のサイトアンダーレイ接続を設定する場合は、クラウド CSR への接続を確立するオンプレミス IPN デバイスを選択する必要があります。これらの IPN デバイスは、オンプレミスのサイト設定画面で使用可能になる前に、ここで定義する必要があります。インフラの設定: オンプレミス サイトの設定 （38 ページ） で詳細を説明しています。

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

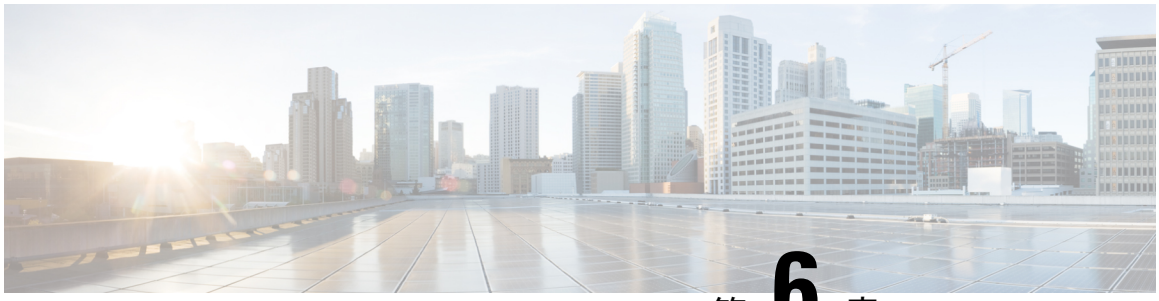
b) **[IPN デバイスの追加 (Add IPN Device)]** をクリックします。

c) IPN デバイスの **[名前（Name）]** と **[IP アドレス（IP Adress）]** 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) 追加するその他の IPN デバイスについて、この手順を繰り返します。



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 **メイン 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 メインの **[インフラ コンフィギュレーション（Infra Configuration）]** ビューの右上の、**[インフラの設定（Configure Infra）]** ボタンをクリックします。

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、サイトして、オンプレミス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)]** で、特定のオンプレミス サイトを選択します。

ステップ 5 **[オーバーレイ設定（Overlay Configuration）]** を指定します。

a) 右側の **<*Site*> [設定（Settings）]** ペインで、**[オーバーレイ設定（Overlay Configuration）]** タブを選択します。

b) 右側の **<*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。

c) (任意) **[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。

d) **[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。

e) （任意）**[External Routed Domain]** ドロップダウンから、使用するドメインを選択します。

Cisco APIC GUI で作成した外部ルータ ドメインを選択します。詳細については、『*Cisco APIC* レイヤ *3* ネットワーキング設定ガイド』 を参照してください：

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

g) (任意) **[BGP パスワード（BGP Password）]** を指定します。

h) （任意）サイトの **SR-MPLS 接続**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 **アンダーレイ設定** を指定します。

a) 右側 **<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。

b) 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。

OSPF エリアタイプは、次のいずれかになります。

- nssa
- regular

c) サイトの OSPF 設定を行います。

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。

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) **+Add IPN デバイス（+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、以前に定義した IPN デバイスのいずれかを選択します。

IPN デバイスは、 で説明したように、[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 （35 ページ）

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 （43 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 （47 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 **メイン メニュー**で **[サイト]** をクリックします。

ステップ 3 **[サイト]** ビューで、**[インフラの構築]** 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 右ポ **[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り、サイト間の既知のユニキャスト トラフィックに使用されるすべてのスパイン スイッチに導入されます。

ステップ 7 **[+ TEP プールの追加]** 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TEPプールは、ISC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、サイト間 L3Out 機能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 マルチサイト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。

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

ステップ 2 **メイン メニュー**で **[サイト]** をクリックします。

ステップ 3 **[サイト]** ビューで、**[インフラの構築]** 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、次の情報を入力します。

- **[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。
- **[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。

  NDO によって、指定されたポートで指定された IP アドレスを持つ VLAN 4 で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。
- **[OSPF ポリシー (OSPF Policy)]** フィールドで、インフラの設定: オンプレミス サイトの設定 （38 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

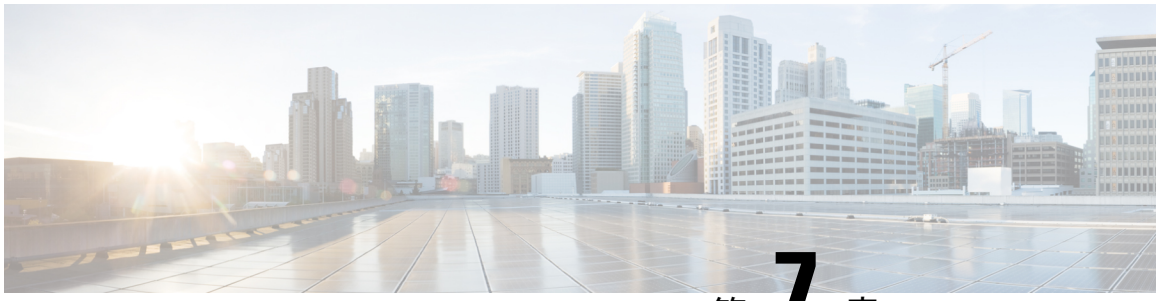
ステップ 8 **[BGP ピアリング (BGP Peering)]** ノブを有効にします。

2つより多くのスパイン スイッチのある単一のポッドファブリックでは、BGP ピアリングは**BGP スピーカ (BGP Speakers)** と呼ばれるスパイン スイッチのペア (冗長性のためのもの) 上でのみ有効にします。他のすべてのスパイン スイッチでは、BGP ピアリングを無効にします。これらは**BGP フォワーダ (BGP Forwarders)** としてのみ機能します。

マルチポッド ファブリック BGP ピアリングは、それぞれが異なるポッドに展開された、2 台の BPG スピーカ スパイン スイッチ上でのみ有効にします。他のすべてのスパイン スイッチでは、BGP ピアリングを無効にします。これらは BGP フォワーダ (BGP Forwarders) としてのみ機能します。

ステップ 9 **[BGP-EVPN Router-ID (BGP-EVPN ルータ ID)]** フィールドでは、サイト間の BGP-eVPN セッションで使用する IP アドレスを指定します。

ステップ 10 すべてのスパイン スイッチで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 **メイン 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 メインの **[インフラ コンフィギュレーション（Infra Configuration）]** ビューの右上の、**[インフラの設定（Configure Infra）]** ボタンをクリックします。

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、Cloud APIC 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 **メイン 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 メインペインの右上にある **[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、特定のクラウド サイトを選択します。

ステップ 5 **[オーバーレイ設定（Overlay Configuration）]** を指定します。

a) 右側の **<*Site*> [設定（Settings）]** ペインで、**[オーバーレイ設定（Overlay Configuration）]** タブを選択します。

b) 右側の **<*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。

c) (任意) **[BGP パスワード（BGP Password）]** を指定します。

ステップ 6 **アンダーレイ設定** を指定します。

a) 右側 **<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。

b) **[接続の追加 (Add Connectivity)]** をクリックします。

c) **[サイト（Site）]**ドロップダウンから、接続を確立するサイトを選択します。

d) **[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：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：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：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が異なる接続タイプを使用できます。

e) (任意) **IPsec** を有効にします。

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 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 を有効または無効にすることができます。

f) IPsec が有効になっている場合は、**IKE バージョン** を選択します。

インターネットキーエクスチェンジ（IKE）はIPsec向けのセキュリティ接続を確立するために使用するプロトコルです。使用するプロトコルのバージョン（設定に応じてIKEv1（バージョン 1）またはIKEv2（バージョン 1））を選択できます。

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

Site1 から Site2 への接続情報を保存すると、Site2 から Site1 へのリバース接続が自動的に作成されます。これは、他のサイトを選択し、**[アンダーレイ 設定（Underlay Configuration）]** タブをチェックすることで確認できます。

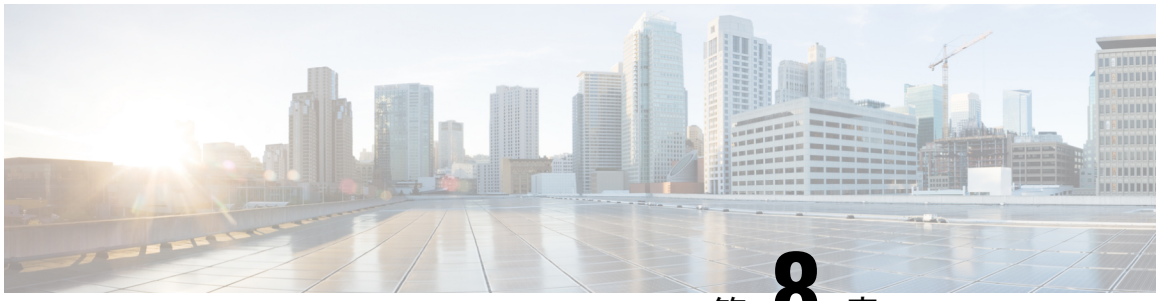
h) 他のサイトのサイト間接続を追加するには、この手順を繰り返します。

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。

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。次の説明に従って、設定を展開する必要があります。 インフラ設定の展開 （47 ページ）



第 8 章

ACI サイトのインフラ コンフィギュレーションの展開

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 ペインの右上の **[展開 (deploy)]** をクリックして、適切なオプションを選択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 2 つ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 IPN 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、クラウド サイトに導入された Cisco クラウド サービス ルータ（CSR）とオンプレミスの IPsec 終端デバイスとの間の接続を有効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ダウンロード:** 設定を展開することなく Cisco クラウド サービス ルータ（CSR）間との接続を有効にするために使用する設定情報を含む zip ファイルをダウンロードします。

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

[展開が開始されました。個々のサイトの展開ステータスについては左側のメニューを参照します。] メッセージが表示され、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 に展開されました。残りの手順では、サイト接続性情報の更新 （37 ページ） の説明のように 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 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情報を収集します。

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のみ（Download 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。インフラ設定の展開 （47 ページ）

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*> は、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*> は、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*> は、最初の CSR の事前共有キーです。
- <*onprem-device-interface*> は、Amazon Web Services に展開された Cisco Cloud サービス ルータ 1000V への接続に使用されるインターフェイスです。
- <*onprem-device-ip-address*> は、Amazon Web Services に展開された Cisco Cloud サービス ルータ 1000V への接続に使用される <*interface*> インターフェイスです。
- <*peer-tunnel-for-onprem-IPsec-to-first-CSR*> は、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*> は OSPF プロセス ID です。
- <*area-id*> は、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 設定する必要があるその他の CSR について、前の手順を繰り返します。

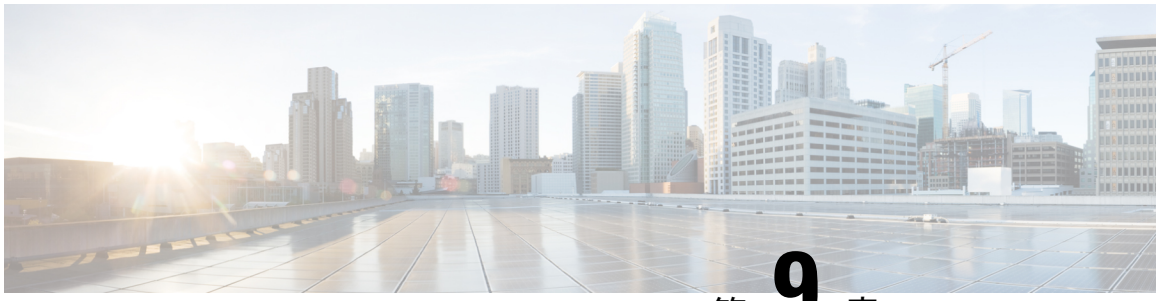
ステップ 5 オンプレミスの IPsec デバイスでトンネルがアップしていることを確認します。

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 0 日目の運用



第 9 章

サイトの追加と削除

Cisco DCNM サイトの追加

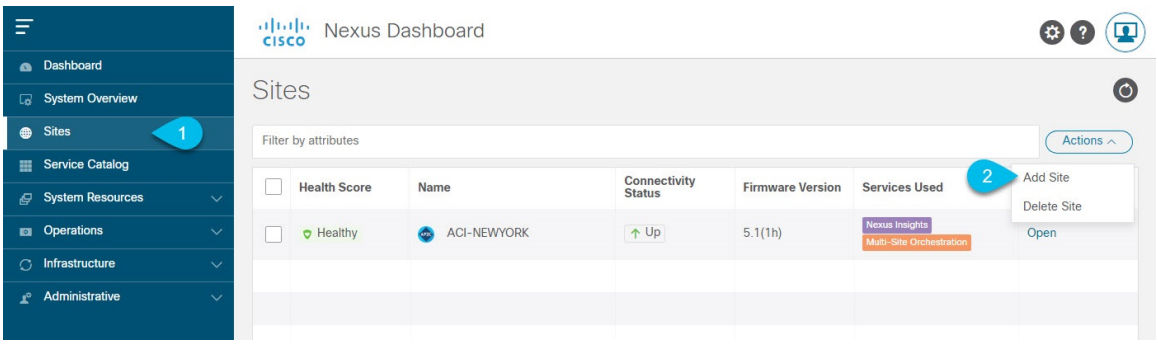
ここでは、Nexus Dashboard GUI を使用して DCNM サイトを追加し、そのサイトを Nexus Dashboard Orchestrator で管理できるようにする方法について説明します。

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 Dashboard GUI にログインします

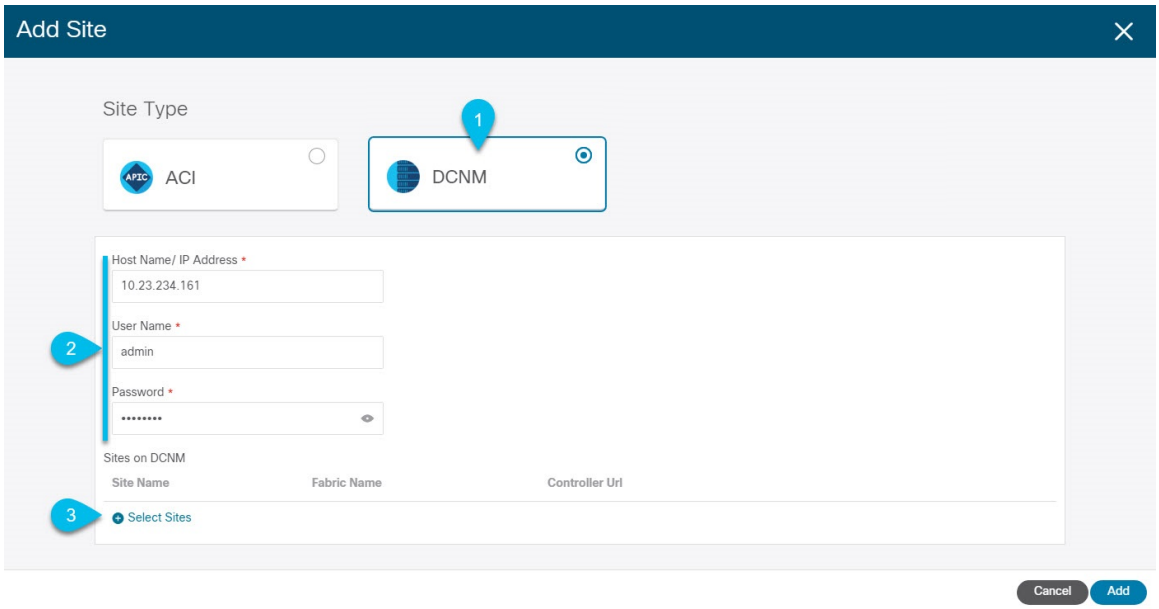
ステップ 2 新サイトを追加します。



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 タイプ（Site Type）]**で、**[DCNM]** を選択します。

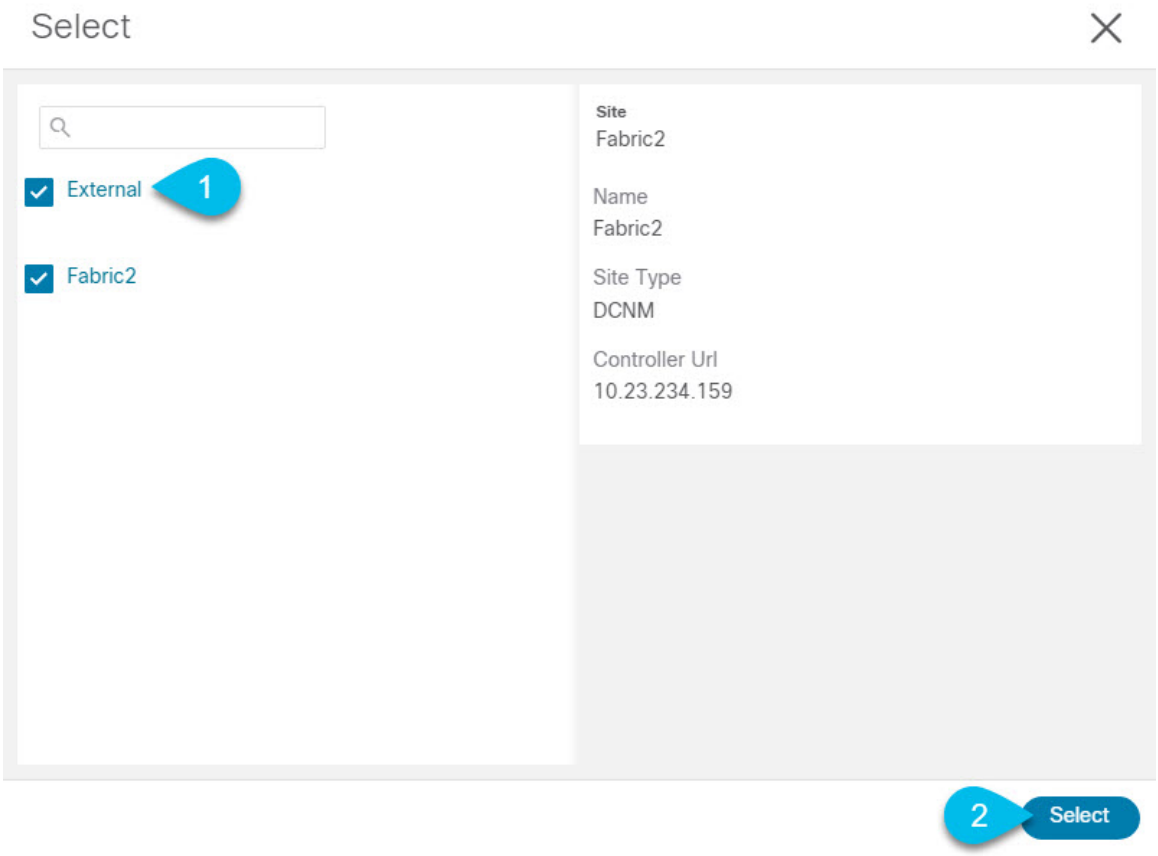
b) DCNM コントローラ情報を入力します。

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

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 Dashboard に追加するファブリックを選択します。



a) Nexus Dashboard 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。

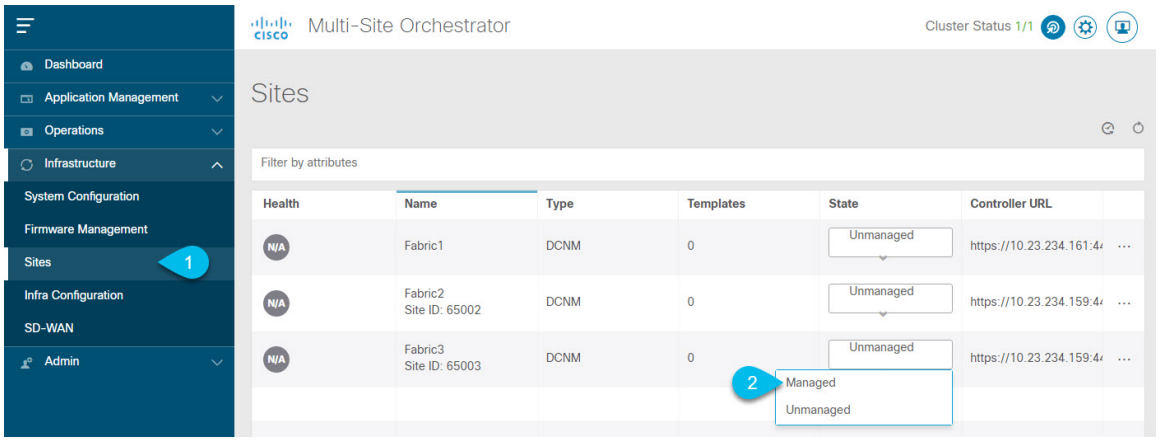
この時点で、サイトはNexusダッシュボードで使用できるようになりますが、次の手順で説明するように、Nexus Dashboard Orchestrator の管理用にそれらのサイトを有効にする必要があります。

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 Dashboard の**サービスカタログ**から、Nexus Dashboard Orchestrator サービスを開きます。

Nexus Dashboard のユーザ 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) 左側のナビゲーション 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 の管理を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** があります。この場合、**[サイト（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、その状態を [管理対象（Managed）] に変更すると、サイトの **[ファブリック ID（Fabric ID）]** を指定するように求められます。

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

サイトの削除

ここでは、Nexus Dashboard Orchestrator GUI を使用して 1 つ以上のサイトのサイト管理を無効にする方法について説明します。サイトは Nexus Dashboard 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 Dashboard の**サービス カタログ**から NDO サービスを開くことができます。Nexus Dashboard のユーザ 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 メニューから、**[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、管理対象外のサイトを選択します。
d) 右側のバーの **[オーバーレイ設定（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) 左側のナビゲーション 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 の管理を停止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 [管理対象外（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 Dashboard からサイトを削除することもできます。

（注） このサイトは、Nexus Dashboard クラスタにインストールされているアプリケーションで現在使用されていないことに注意してください。

a) Nexus Dashboard 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（Delite 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。

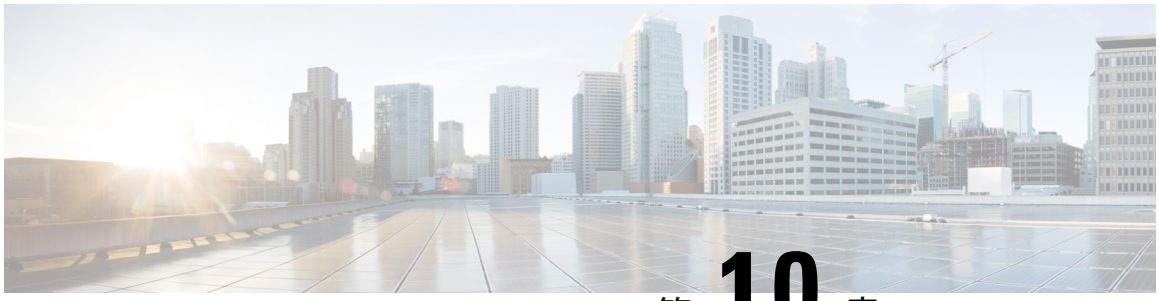
Nexus Dashboard からサイトが削除されます。

ファブリックコントローラへの相互起動

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。その他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** > **サイト**（Infrastucture 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 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設定して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 スイッチの追加または削除には、Nexus Dashboard Orchestrator ファブリックの接続情報の更新が必要です。これは、一般インフラ設定の手順の一部として、サイト接続性情報の更新 （63 ページ） で説明されています。

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。

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 BGP（Control Plane BGP）]** 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 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 ではない）セッション用です。ルートサーバ 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 サーバの追加（+Add Route Server）]** をクリックして 1 つ以上のルート サーバを追加します。

[ルートサーバの追加（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 サーバは最大 4 つまで追加できます。複数のルート サーバを追加すると、すべてのサイトがすべてのルート サーバに対して 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)）]**、**[ステート間隔(秒)（State Interval （Seconds））]**、**[グレースフル ヘルパー（Graceful Helper）]**、**[最大 AS 制限（Maximum AS Limit）]**、および **[ピアの 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）]** フィールドをスキップします。

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** 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**を指定します。

このフィールドは、各ファブリックの **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: DCNM サイトの設定 （63 ページ）

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** 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、コントローラ 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 サイトのコントローラからインポートし直します。

インフラの設定: DCNM サイトの設定

ここでは、サイトして、オンプレミス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。

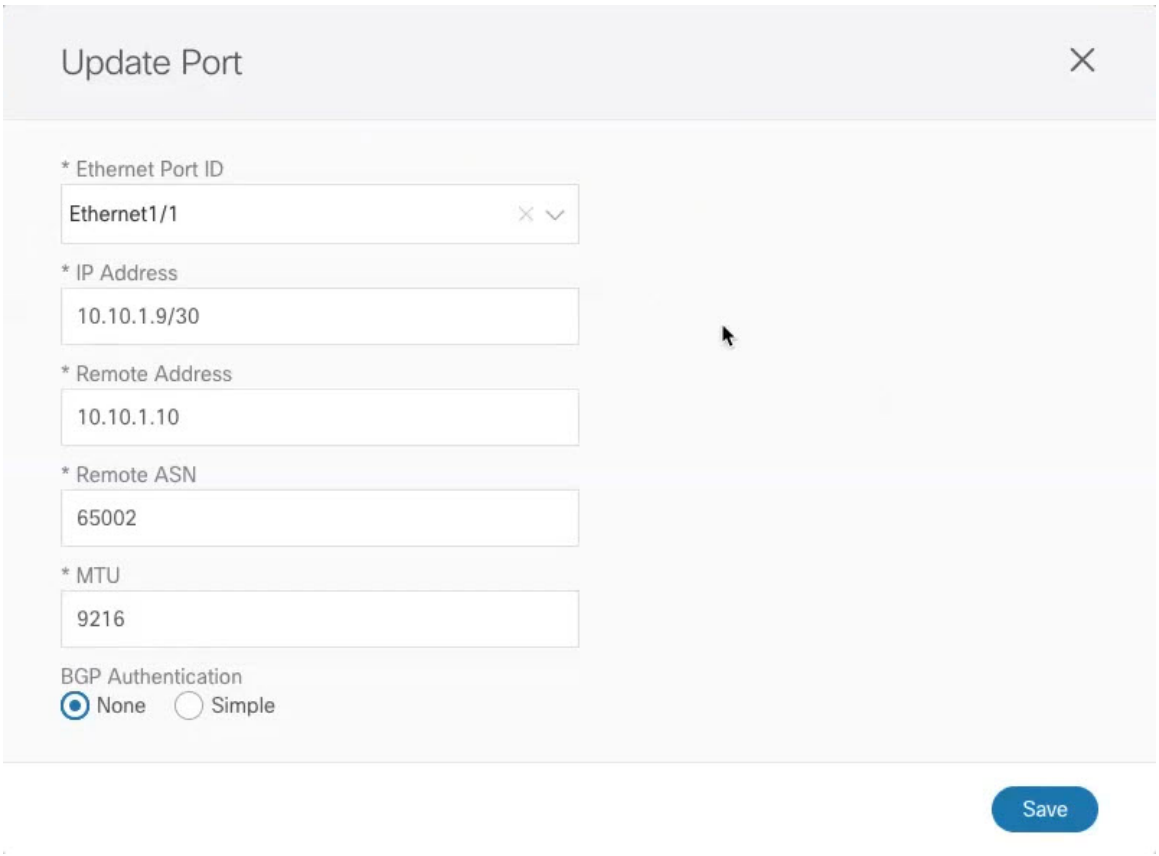
ステップ 6 **<fabric-name>** タイル内で、ボーダー ゲートウェイを選択します。

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/ネットマスクを入力します。
- **[リモート アクセス（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、ポートの 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（Authentication Key）]** 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

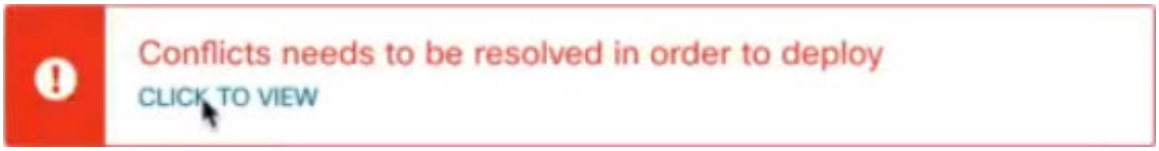
一般およびサイト指定のインフラ設定を完了しておく必要があります。このチャプターの前のセクションで説明されています。

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。

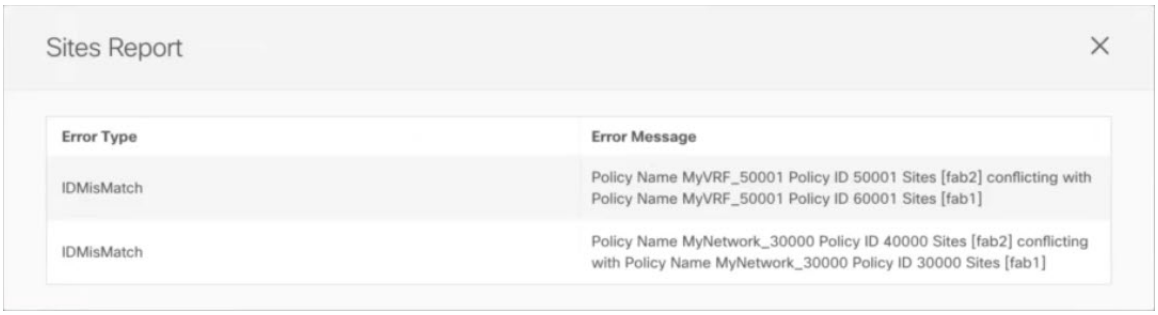
設定が競合する場合：

a) 競合通知ポップアップの **[クリックして確認（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 （29 ページ） の説明に従って、NDO でサイトを管理解除します。

Nexus Dashboard からサイトを削除する必要はありません。NDO GUI でサイトを管理解除するだけです。

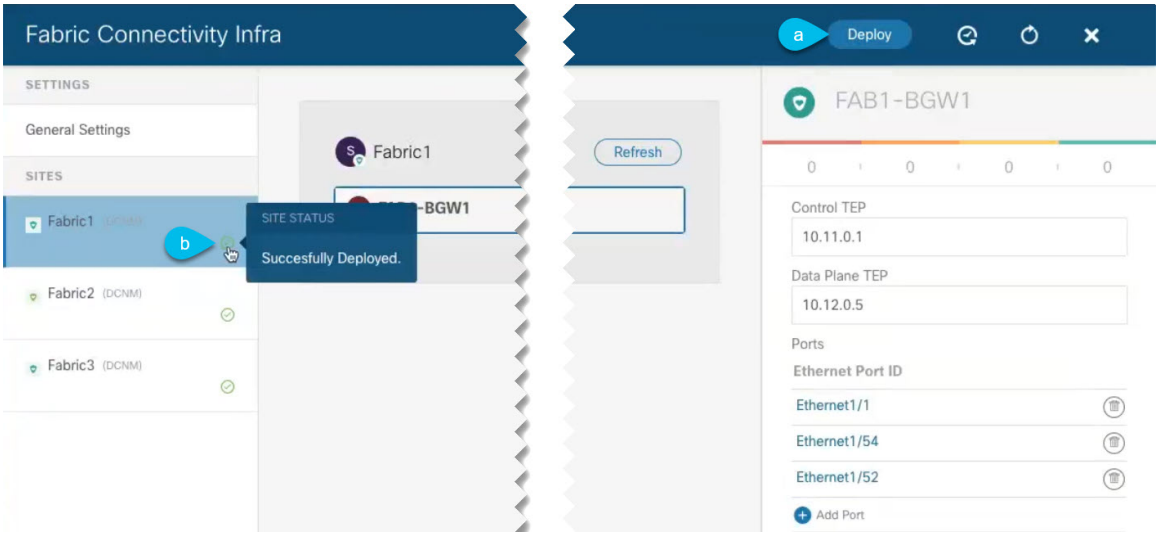
e) 既存の設定の競合を解決します。

f) の説明に従って、サイトを再度管理します。Cisco DCNM サイトの追加 （55 ページ）

サイトはすでに Nexus Dashboard 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 設定の導入



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。

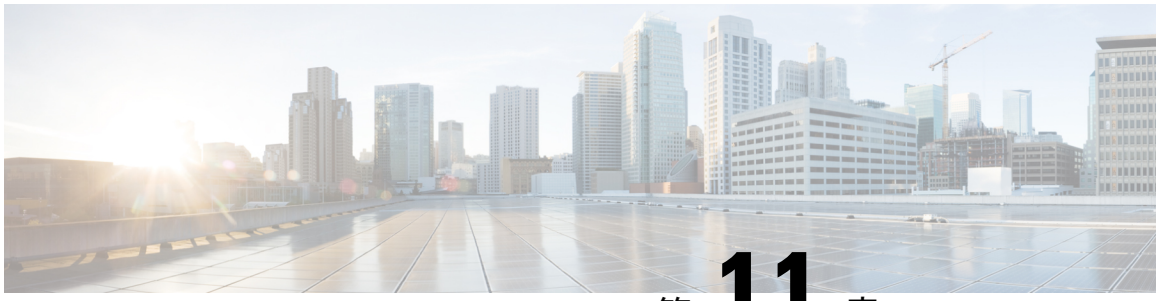
b) 設定が展開されるのを待ちます。

インフラ設定を展開すると、NDO は DCNM にシグナリングして、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 のアップグレード



第 11 章

NDO サービスのアップグレードまたはダウングレード

概要

ここでは、Cisco Nexus Dashboard に導入されている Cisco Nexus Dashboard Orchestrator リリース 3.2（1）以降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、「*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、新しいクラスタを導入し、既存のクラスタから設定を転送する必要があります。 Nexus Dashboard Orchestrator 導入ガイド。

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。

  以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、『*Nexus Dashboard Orchestrator Deployment Guide*』の「Migrating Existing Cluster to Nexus Dashboard」の項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。

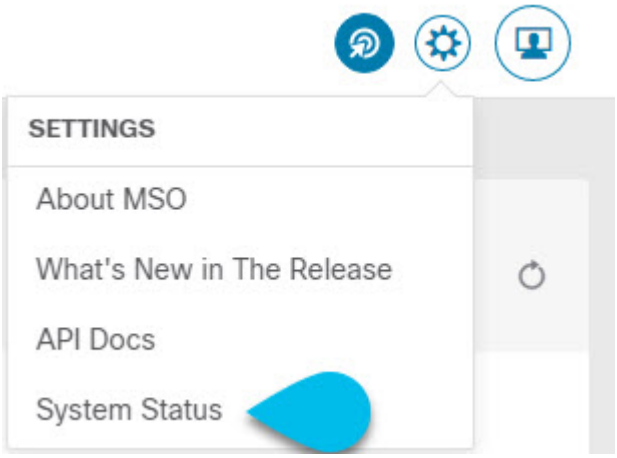
  Nexus Dashboard クラスタの状態は、次の 2 つの方法のいずれかで確認できます。

- Nexus Dashboard 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。
- 任意のノードに直接レスキューユーザとしてログインし、次のコマンドを実行します。

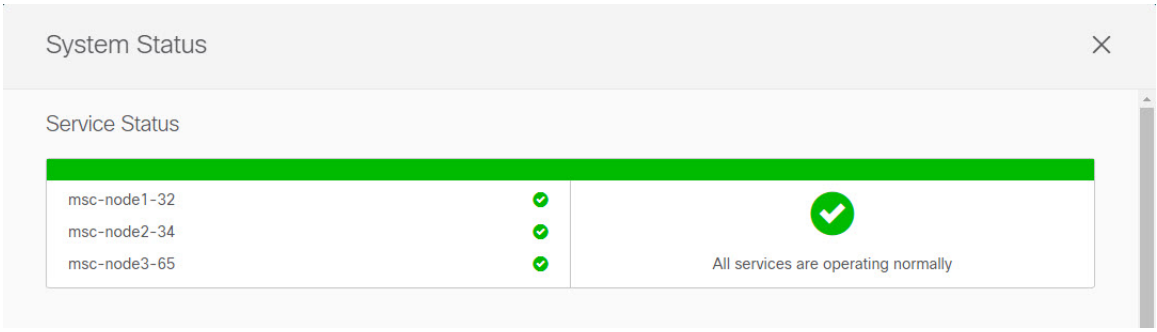
```
# acs health
All components are healthy
```

- 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。

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



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。



- アップグレードは次のいずれかの方法の NDO サービスで実行できます。
  - Cisco App Store を使用した NDO サービスのアップグレード （73 ページ） の説明に従って、Nexus Dashboard の App Store を使用します。

    この場合、Cisco DC App Center は、管理ネットワーク経由で直接、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。

注 App Store では、入手可能な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。つまり、リリース 3.4(1) が使用可能な場合、App Store を使用してリリース 3.3(1) にアップグレードすることはできず、以下に説明する手動のアップグレード 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 （75 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 をリリース 3.3(1) 以降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、Nexus Dashboard Orchestrator 3.3(1) で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。

  以前のリリースにダウングレードする場合は、以前のリリースでサポートされているプラットフォームに新しい Nexus Dashboard Orchestrator クラスタを展開してから、古い設定のバックアップを復元する必要があります。リリース 3.3(1) 以降で作成されたバックアップを古い NDO クラスタに復元することはサポートされていません。

  Nexus Dashboard Orchestrator の以前のリリースにダウングレードする場合は、すべてのクラウド APIC サイトをリリース 5.2(1) より前のリリースにダウングレードする必要もあります。

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 リリース 3.2(1) 以降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 （71 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、**[App Store]** タブを選択します。

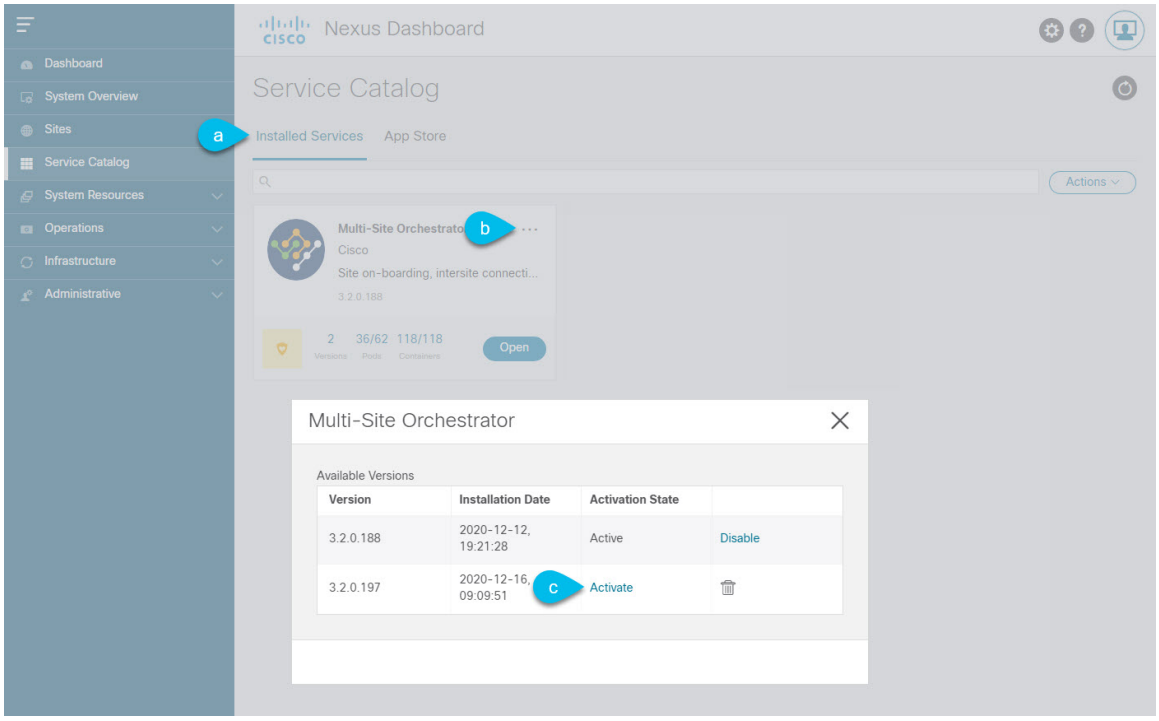
b) **[Nexus Dashboard Orchestrator]** タイルで、**[アップグレード（Upgrade）]** をクリックします。

c) 開いた [License Agreement] ウィンドウで、**[同意してダウンロードする（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、**[インストール済みのサービス（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、**[使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] ウィンドウで、新しいイメージの横にある **[起動（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、現在実行中のアプリケーション 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、プロセスが完了すると、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 バージョンを保持することもできます。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、**[インストール済みのサービス（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、**[使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 アプリケーションを起動します。

アプリケーションを起動するには、Nexus Dashboard 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 Dashboard 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。

NDO サービスの手動アップグレード

ここでは、Cisco Nexus Dashboard Orchestrator リリース 3.2(1) 以降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 （71 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 リリース イメージをダウンロードします。

a) [Nexus Dashboard Orchestrator service DC App Center]ページを参照しますhttps://dcappcenter.cisco.com/multi-site-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) 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 Dashboard 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 Dashboard の **[サービス カタログ（Service Catalog）]** 画面で、**[インストール済みのサービス（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、以下のように、イメージ ファイルへの完全な URL を入力します。（http：//<ip-address>：<port>/<full-path>/cisco-mso-<version>.aci

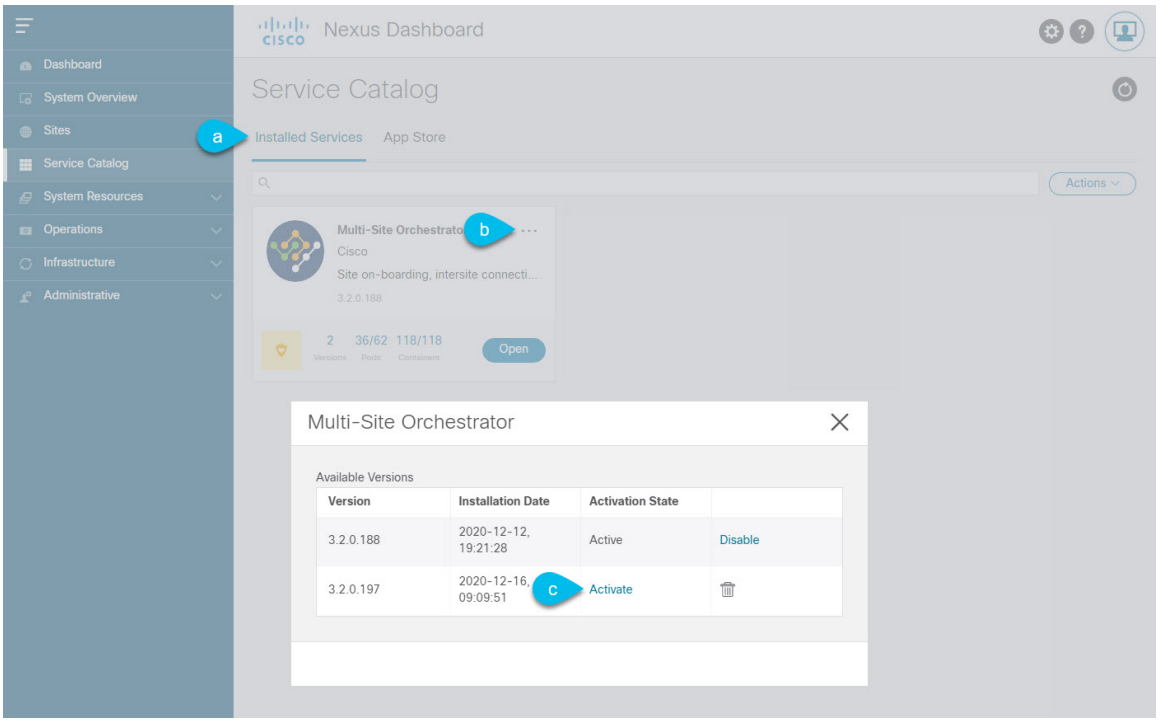
f) **[アップロード（Upload）]** をクリックして、アプリケーションをクラスタに追加します。

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 Dashboard 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、**[インストール済みのサービス（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、**[使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] ウィンドウで、新しいイメージの横にある **[起動（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、現在実行中のアプリケーション 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、プロセスが完了すると、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 バージョンを保持することもできます。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、**[インストール済みのサービス（Installed Services）]** タブを選択します。

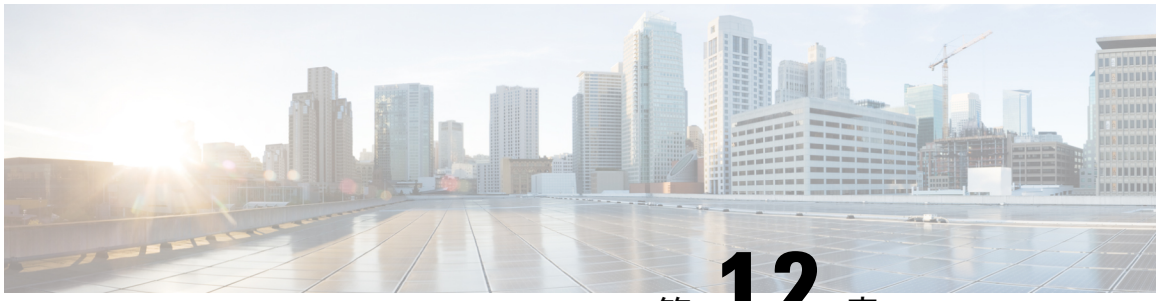
b) [Nexus Dashboard Orchestrator]タイルの右上にあるメニュー（...）をクリックし、**[使用可能なバージョン（Available Versions）]** を選択します。

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 アプリケーションを起動します。

アプリケーションを起動するには、Nexus Dashboard 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 Dashboard 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。



第 12 章

Nexus Dashboard 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 Dashboard 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 Dashboard 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 Nexus Dashboard を導入している場合は、代わりに NDO サービスのアップグレードまたはダウングレード （71 ページ） に記載されている手順に従います。

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。

NDO 固有の手順を示すビデオは、Nexus Dashboard の「MSO 3.1 から MSO 3.3 への移行」で参照できます。このビデオは、Nexus Dashboard の導入やクラウド APIC サイトのアップグレードなど、この章に記載されている要件と手順の完全なリストを置き換えるものではありません。

- 既存の Multi-Site Orchestrator 設定をバックアップし、既存の Multi-Site Orchestrator クラスタを切断または停止します。

  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 Dashboard 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。

- 物理的、仮想的、またはクラウドのフォーム ファクタを使用して Nexus Dashboard クラスタを展開します。
- （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 Dashboard クラスタを設定します。
- （オプション）既存の Multi-Site Orchestrator の導入で必要な場合は、Nexus Dashboard でリモート認証サーバを設定します。
- 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。
- Nexus Dashboard に Nexus Dashboard Orchestrator サービスをインストールします。
- Nexus Dashboard にインストールされた新しい NDO サービスの設定バックアップを復元します。
- 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。

- Nexus Dashboard Orchestrator のインフラ設定を更新します。

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 Dashboard プラットフォームの並行展開と、既存の Multi-Site Orchestrator（MSO）クラスタから現在の設定データベースへの手動による転送を含みます。

既存のクラスタを Nexus Dashboard に移行する前に:

- Nexus Dashboard Orchestrator サービスリリース 3.2(x) で既存の**物理** Nexus Dashboard クラスタがある場合は、この章をスキップし、『*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てから、Nexus Dashboard Orchestrator のアップグレード （69 ページ） で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。

注 リリース 3.2(1) は、オンボーディング クラウド サイトをサポートしていませんでした。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ます。

- 最初に、『*Cisco Nexus Dashboard Deployment Guide*』およびこのマニュアルの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することをお勧めします。Nexus Dashboard Orchestrator の展開 （3 ページ）
- 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した 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 Dashboard 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 Nexus Dashboard 共通サイト管理に移行しました。これは、オンボーディング クラウド サイト リリース 5.1(1) 以降をサポートします。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 3.3(1) リリースに移行する前に、最新の Cloud APIC 5.2(1) リリース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 リリース 3.3(1) を展開し、既存の設定をインポートしてください。

  リリース 3.3 への 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。
- 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。

以前のリリースにダウングレードする場合は、以前のリリースでサポートされているプラットフォームに新しい Nexus Dashboard Orchestrator クラスタを展開してから、古い設定のバックアップを復元する必要があります。リリース 3.3(1) 以降で作成されたバックアップを古い NDO クラスタに復元することはサポートされていません。

Nexus Dashboard Orchestrator の以前のリリースにダウングレードする場合は、すべてのクラウド APIC サイトをリリース 5.2(1) より前のリリースにダウングレードする必要もあります。

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。

ここでは、既存のクラスタ設定をバックアップする方法について説明します。

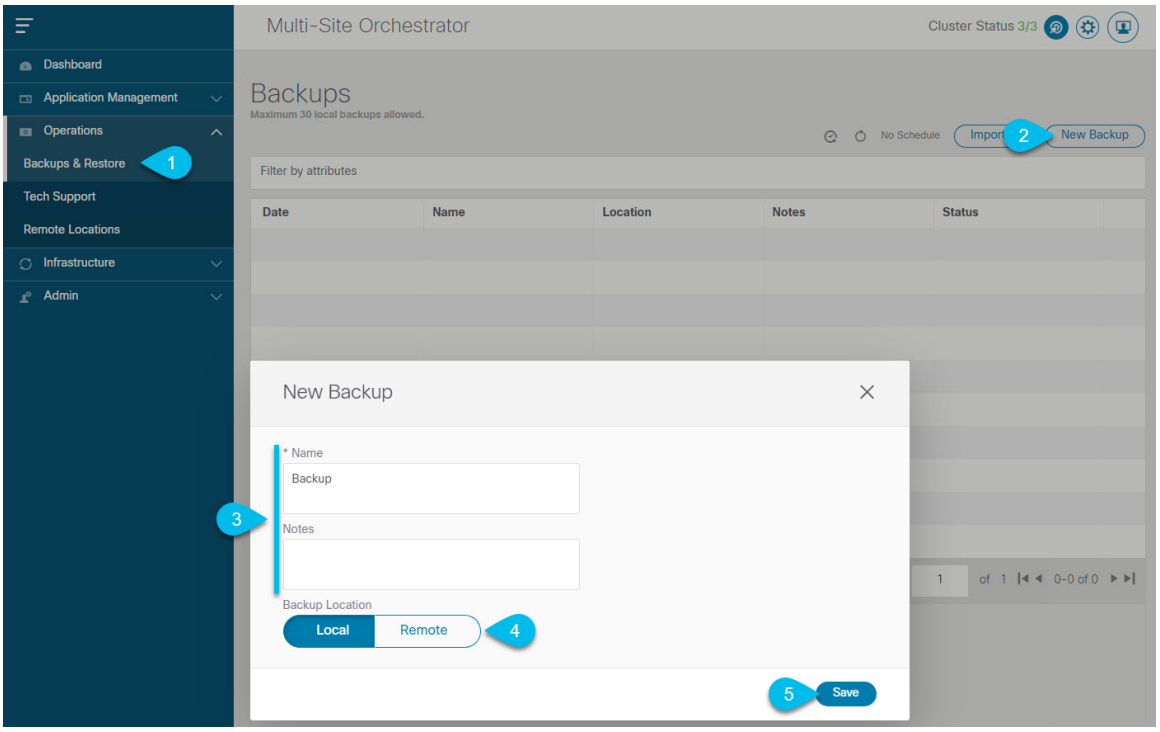
始める前に

完了するには次が必要です。

- 概要 （79 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 （80 ページ） で説明されている一般的な前提条件をレビューし、完了します。

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 ウィンドウで、**[管理 ([Operation])]** > **[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) [場所のバックアップ（Backup Location)] 用に [ローカル（Local）] を選択します。

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、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

完了するには次が必要です。

- 以下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。 概要 （79 ページ）
- 前提条件とガイドライン （80 ページ） で説明されている一般的な前提条件をレビューし、完了すること。
- 既存のクラスタ設定のバックアップ （82 ページ） の説明に従い既存の設定をバックアップすること。

ステップ 1 Nexus Dashboard リリース 2.0.2h 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 Dashboard 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。

- Multi-Site Orchestrator サービスを備えた既存の**仮想** Cisco Application Services Engine クラスタがある場合は、『*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 Dashboard 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 Dashboard リリース 2.0.2h 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 Dashboard 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 のアップグレード （69 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） リリース 3.2(1) は、オンボーディング クラウド サイトをサポートしていませんでした。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ます。

ステップ 2 Nexus Dashboard 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 Dashboard 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。

物理的な Nexus Dashboard クラスタを導入し、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であるため、この手順は省略できます。

ただし、物理的な Nexus Dashboard クラスタを展開し、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 Dashboard に NDO サービスをインストールします。

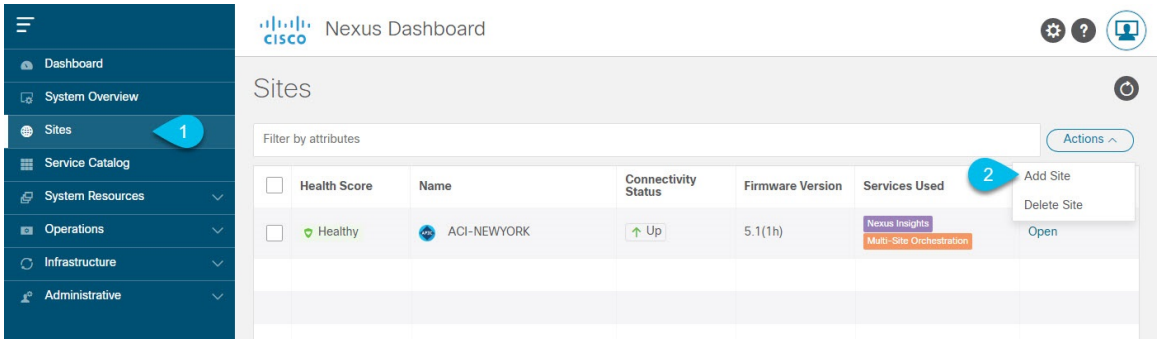
この手順の詳細は、Nexus Dashboard Orchestrator の展開 （3 ページ） の章で説明します。

ステップ 4 すべてのサイトを Nexus Dashboard にオンボードします。

サイト管理は、Multi-Site Orchestrator UI から Nexus Dashboard の共通サイト管理に移動しました。したがって、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 Dashboard GUI にオンボードする必要があります。サイトの追加と削除 （25 ページ） で説明されています。現在の展開に存在するサイトが Nexus Dashboard 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、`Pre-restore check failed` というエラー メッセージで失敗します。

（注） Nexus Dashboard 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。

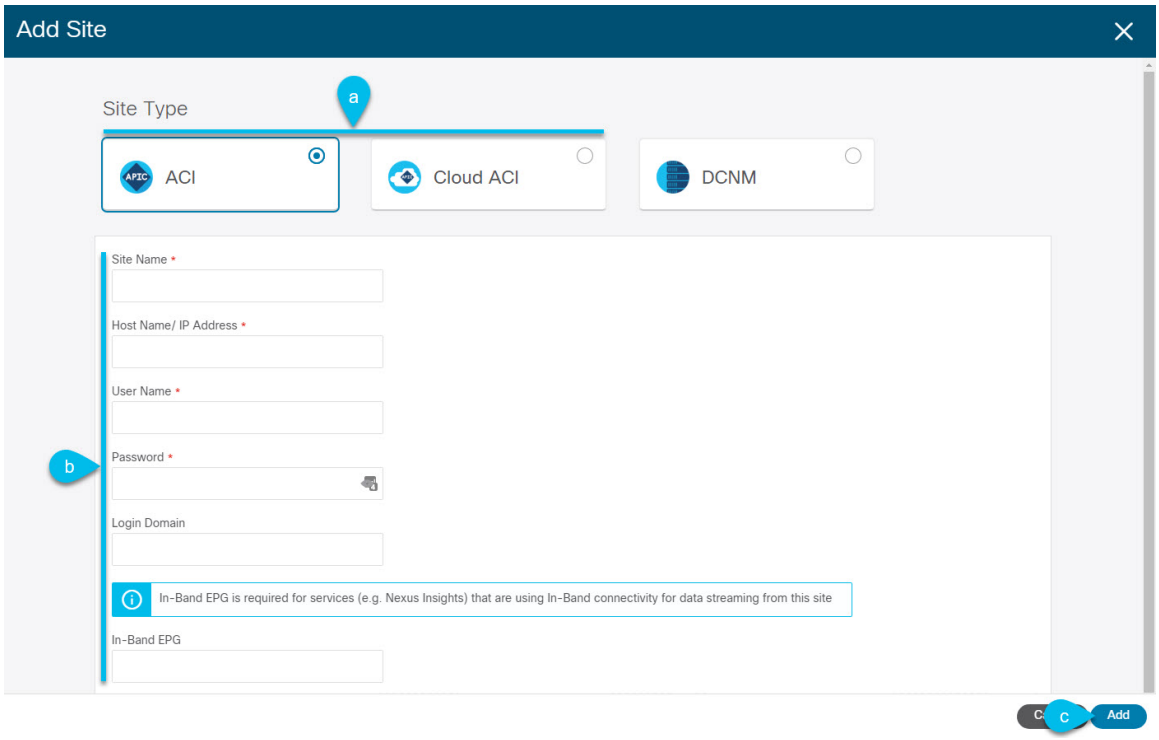
サイトの追加:



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

b) コントローラの情報を入力します。

ACI ファブリックを現在管理している APIC コントローラ用の **[ホスト名/IP アドレス（Host Name/IP Address）]**、**[ユーザ名（User Name）]**、および **[パスワード（Password）]** を入力する必要があります。NDO 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、オンプレミス APIC のインバンドアドレスまたは out-of-band アドレスを指定できます。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。

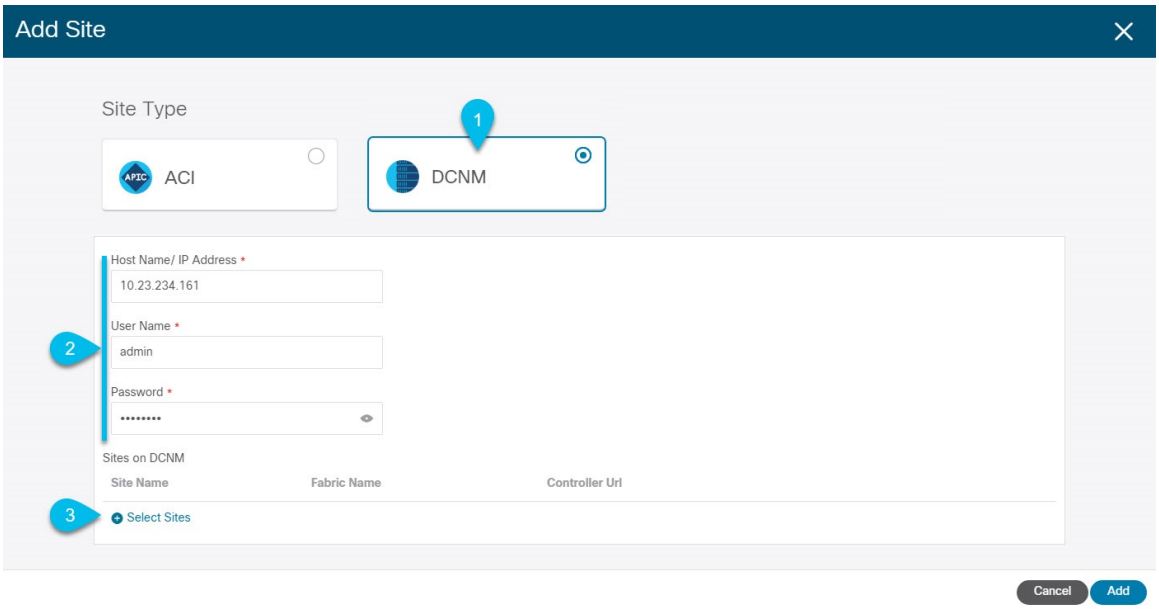
（注） このアドレスは、Nexus Dashboard のデータ インターフェイスから到達可能である必要があります。

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 Day-2 Operations アプリケーションで使用する場合は、Nexus Dashboard を追加している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 Dashboard 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。

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 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。

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

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。

開いたファブリック選択ウィンドウで、既存のマルチサイト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。

既存のマルチサイト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 Dashboard に追加します。

ユーザ管理は、Multi-Site Orchestrator UI から Nexus Dashboard の共通ユーザ管理に移行しました。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と認証サーバを Nexus Dashboard に追加する必要があります。

以前に Multi-Site Orchestrator で直接設定したローカルユーザは、既存の設定バックアップをインポートすると、Nexus Dashboard に自動的に追加されます。

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 Dashboard 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

完了するには次が必要です。

- 既存のクラスタ設定のバックアップ （82 ページ） の説明に従って既存の設定をバックアップすること。
- 新規クラスタの準備 （84 ページ） の説明に従って、Nexus Dashboard クラスタを展開し、Nexus Dashboard Orchestrator サービスをインストールすること。

ステップ 1 既存の Multi-Site Orchestrator クラスタを切断します。

移行中にクラウド APIC サイトと通信しないように、既存の Multi-Site Orchestrator クラスタを切断または停止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 Dashboard クラスタを展開した場合は、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お勧めします。

ステップ 2 新しい Nexus Dashboard 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、サイトまたはポリシーの設定が変更されていない新規インストールである必要があります。

ステップ 3 Nexus Dashboard GUI にログインします。

ステップ 4 すべてのサイトが Nexus Dashboard 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 Dashboard 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 Dashboard 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、再試行する前にサイトをオンボードする必要があります。オンボーディングサイトについては、Cisco ACI サイトの追加 （27 ページ） および Cisco DCNM サイトの追加 （55 ページ） を参照してください。

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。

リリース 3.4(1) 以降、Nexus Dashboard Orchestrator 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のサポート対象外になりました。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、**[管理 ([Operation])]** > **[リモート ロケーション (Remote Locations)]** 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
- SFTP

（注） SCP は Windows 以外のサーバ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 ウィンドウで、**[管理 ([Operation])]** > **[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 [**ファイルからのインポート (Import from file)**] ウィンドウで、[**ファイルを選択 (Select File)**] を選択して、インポートするバックアップ ファイルを選択します。

バックアップのロードポートは、[**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。

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、リモート サーバにのみ存在すること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 Dashboard にオンボードされていたサイトは、GUI で NDO管理が有効になります。設定のバックアップに Nexus Dashboard 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 [復元の事前チェックが失敗しました（Pre-restore check failed）] エラーで失敗し、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。

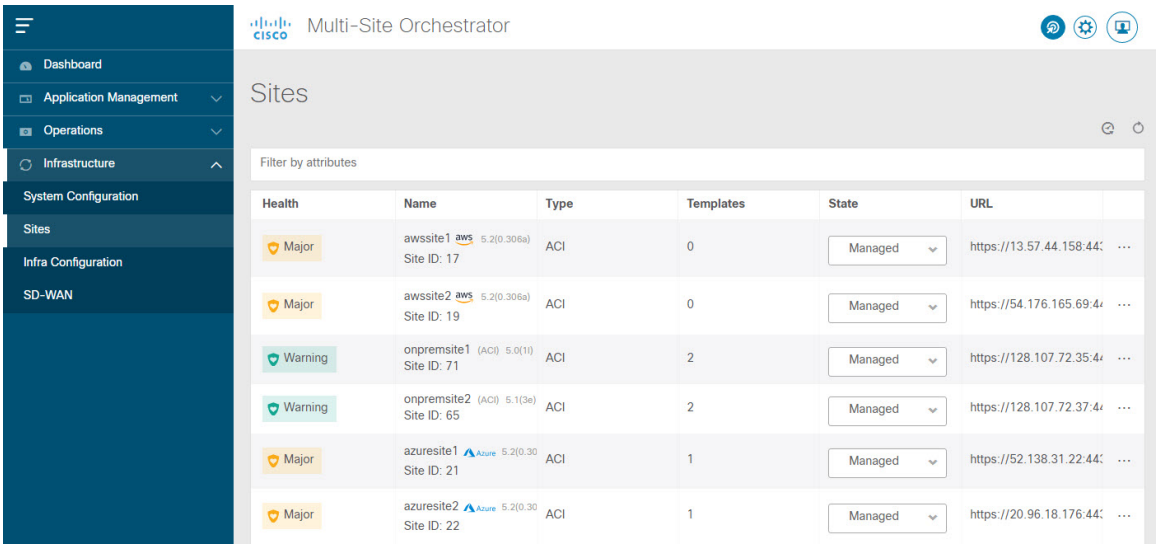
設定をインポートして復元すると、いくつかのサービスが再起動されます。

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 [管理者（admin）] ユーザ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。

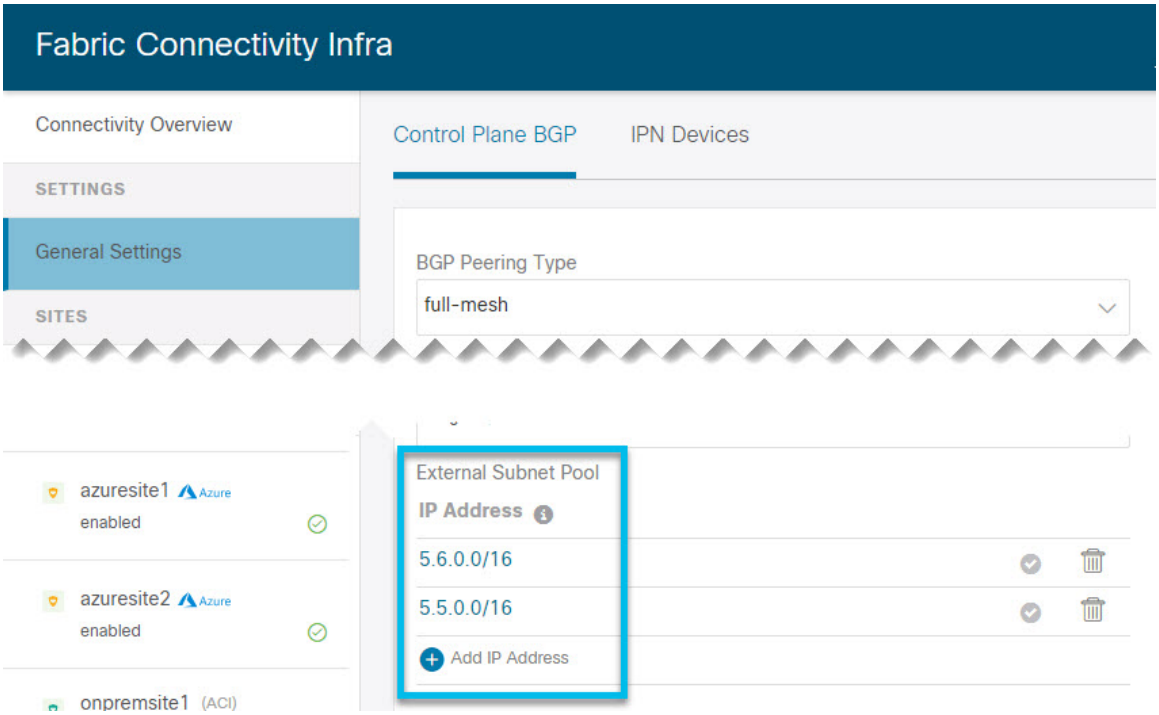


b) **[テナント（Tenants）]** および **[スキーマ（Schemas）]** ページで、以前の Multi-Site Orchestrator クラスタのすべてのテナントとスキーマが存在することを確認します。

c) **[インフラストラクチャ（Infrastructure）]** > **[インフラ設定（Infra Configuration）]** > **[インフラの構成（Configure Infra）]** の順に移動し、サイト間接続が変更されていないことを確認します。

[接続の概要（Connectivity Overview）] 画面で、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。

[全般設定（General Settings）] 画面で、クラウド APIC で以前に設定した外部サブネット 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します。



これらのサブネットは、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。

（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 3.3(1) 以降のリリースに移行した後、NDO によって管理されるクラウド APIC サイトをリリース 5.2(1) 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て、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

完了するには次が必要です。

- 新規クラスタの準備 （84 ページ） の説明に従って、Nexus Dashboard クラスタを展開し、Nexus Dashboard Orchestrator サービスをインストールしました。
- 新しいクラスタでの設定の復元 （87 ページ） の説明に従って、既存の設定のバックアップを新しいクラスタに復元します。

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。サイトが正常にアップグレードされたら、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。

通常、クラウド APIC をアップグレードするには、『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」の章を参照してください。https://www.cisco.com/c/en/us/td/docs/dcn/aci/cloud-apic/5x/installation/azure/cisco-cloud-apic-for-azure-installation-guide-52x.htmlhttps://www.cisco.com/c/en/us/td/docs/dcn/aci/cloud-apic/5x/installation/aws/cisco-cloud-apic-for-aws-installation-guide-52x.html

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、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」の章を参照してください。

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、トラフィックは流れ続けます。
- 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 から発信された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アドレス `/31` 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 `/30` トンネルが CSR に作成され、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すべての新しいトンネルは `/31` トンネルになります。

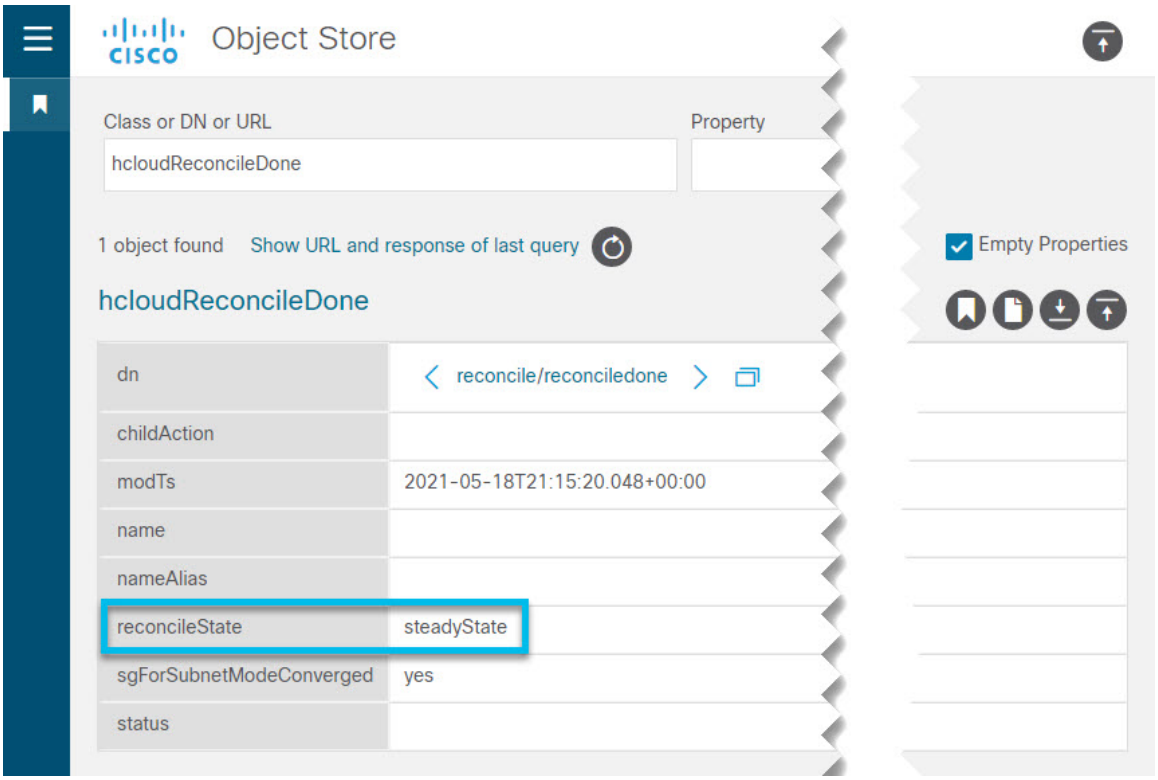
（注） CSR のアップグレードが完了して CSR が起動してから 5 分以内に BGP セッションが表示されない場合は、Nexus Dashboard Orchestrator の **[インフラ設定（Infra Configuration）]** 画面でサイトのインフラ接続を更新します。

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。

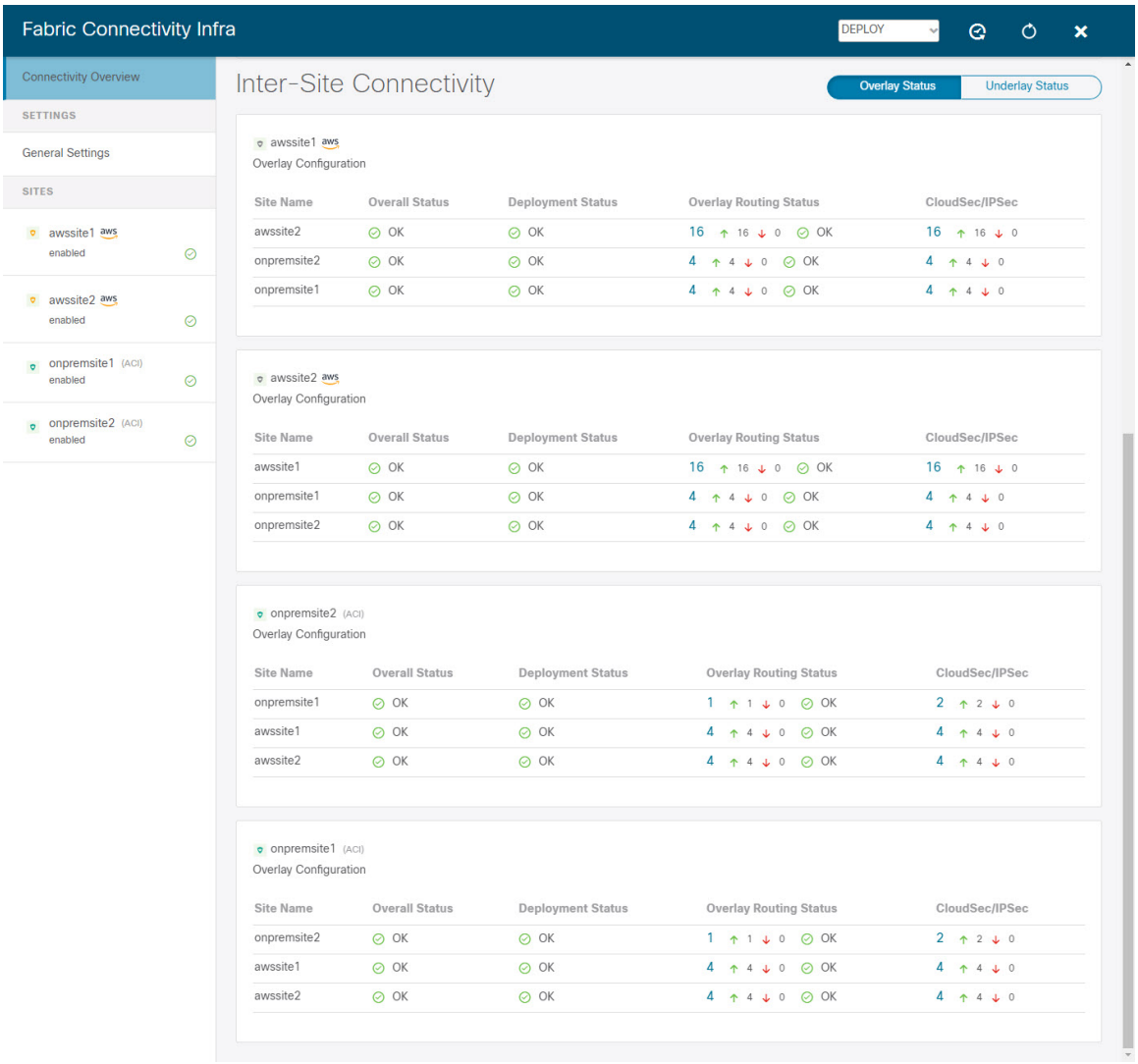
a) 各サイトのクラウド APIC で、`hcloudReconcileDone` MO に `reconcileState=steadyState` が表示されていることを確認します。

https://<cloud-apic-ip>/visore.html に移動して MO を確認できます。[クラス（Class）] または [DN] または [URL] フィールドで hcloudReconcileDone を検索します。



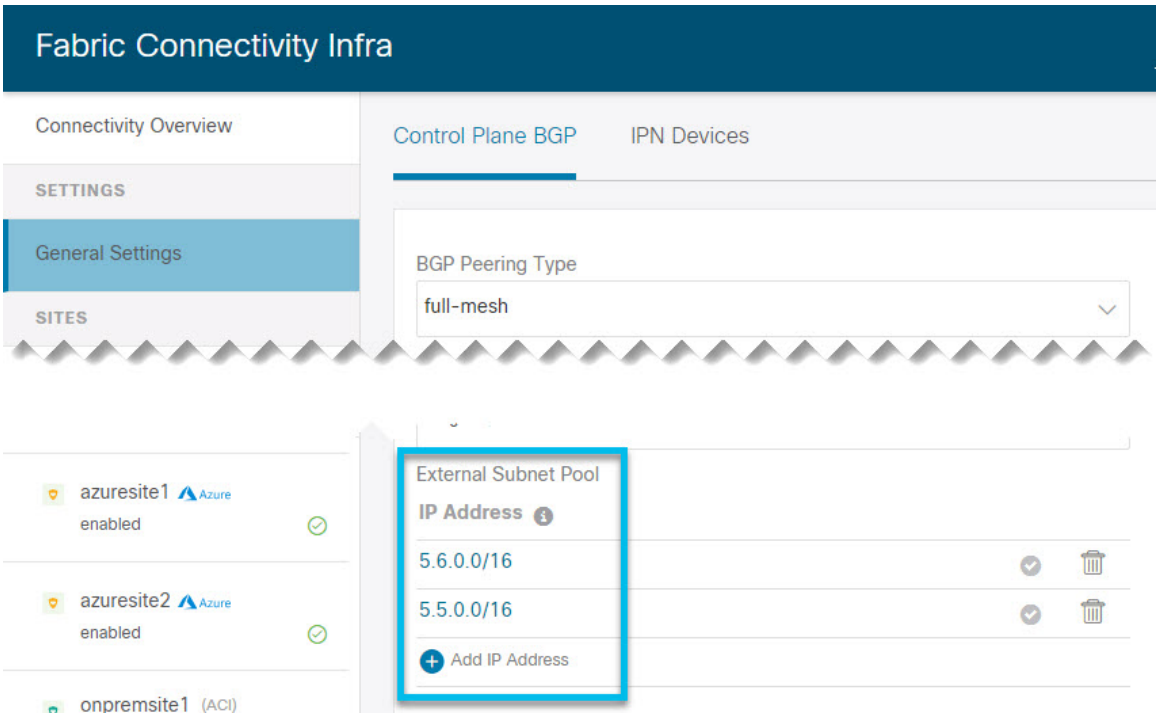
b) Nexus Dashboard Orchestrator で、サイト間の接続が損なわれていないことを確認します。

[インフラストラクチャ（Infrastructure）] > **[インフラの構成（Infra Configuration）]** > **[インフラの設定（Configure Infra）]** > **[接続の概要（Connectivity Overview）]**の順に移動し、[上書きステータス（Overlay Status）] タブと [アンダーレイ ステータス（Underlay Status）] タブを確認することで、ステータスを表示できます。



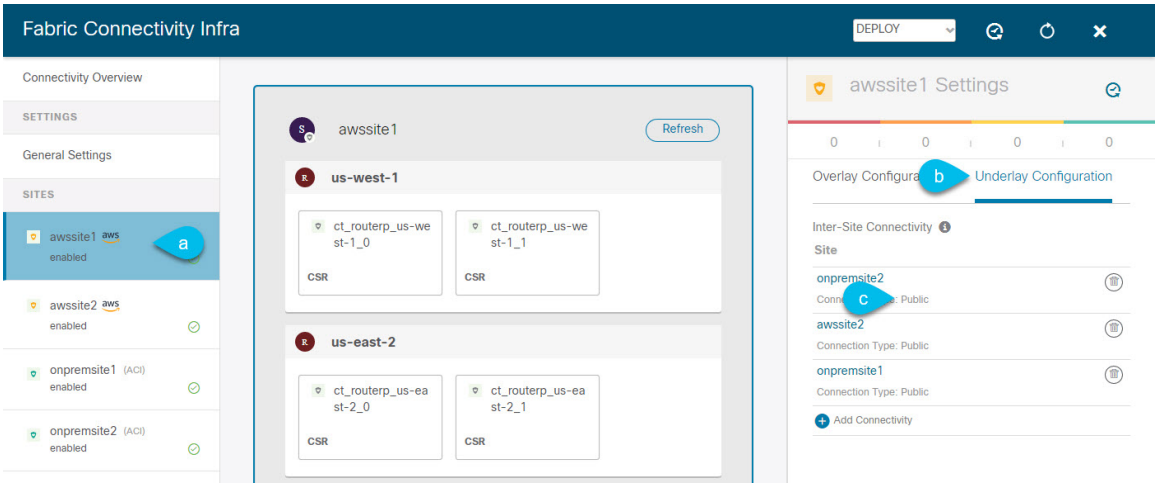
c) Nexus Dashboard Orchestrator で、以前にクラウド APIC で設定された外部サブネット プールがインポートされ、存在することを確認します。

[インフラストラクチャ（Infrastructure）] > [インフラの構成（Infra Configuration）] > [インフラの設定（Configure Infra）] > [一般設定（General Settings）]に移動して、外部プールを表示できます。



d) Nexus Dashboard Orchestrator で、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対して保持されていることを確認します。

既存のサイト間接続を確認するには、**[インフラストラクチャ（Infrastructure）]** > **[インフラの設定（Infra Configuration）]** > **[インフラの構成（Configure Infra）]**、の順に移動し、左側のサイドバーと **[アンダーレイ接続（Underlay Connectivity）]**タブから特定のクラウド サイトを選択します。



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

始める前に

完了するには次が必要です。

- 新規クラスタの準備 （84 ページ） の説明に従って、Nexus Dashboard クラスタを展開し、Nexus Dashboard Orchestrator サービスをインストールしました。
- 新しいクラスタでの設定の復元 （87 ページ） の説明に従って、既存の設定のバックアップを新しいクラスタに復元します。
- クラウドサイトのアップグレード （92 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ました。

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 **[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** 情報を追加します。

a) **[IPNデバイス（IPN 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) オンプレミスの 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) 追加するその他の 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)]** で、オンプレミス サイトを選択します。
b) 右側 **<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) **+Add IPN デバイス（+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、以前に定義した IPN デバイスのいずれかを選択します。

IPN デバイスは、前の手順で説明したように、 **[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。

設定の変更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 リリースからリリース 3.3(1) 以降に移行する場合は、このセクションで説明するように、設定のずれを解決し、テンプレートを再展開する必要があります。

（注） この時点でテンプレートを展開すると、デフォルト値がプッシュされ、ファブリック内のこれらのプロパティの既存の値が上書きされます。

また、リリース 3.3(1) 以降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を強制的に再展開するために、すべてのテンプレートが明示的に設定の変更を示します。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

完了するには次が必要です。

- 新規クラスタの準備 （84 ページ） の説明に従って、Nexus Dashboard クラスタを展開し、Nexus Dashboard Orchestrator サービスをインストールしました。
- 新しいクラスタでの設定の復元 （87 ページ） の説明に従って、既存の設定のバックアップを新しいクラスタに復元します。
- クラウドサイトのアップグレード （92 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ました。

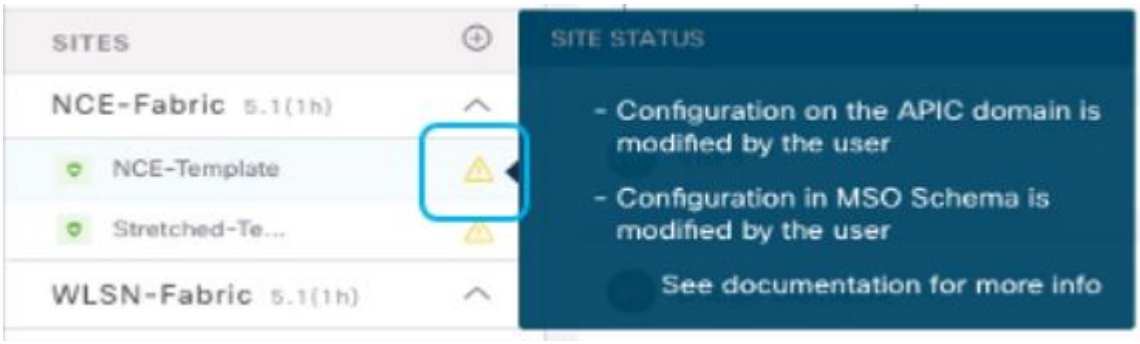
- NDO インフラ設定の更新 （97 ページ） の説明に従って、クラウド サイトの Nexus Dashboard Orchestrator Infra 設定を更新しました。

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 コントローラ レベルで変更された可能性があるオブジェクトをインポートします。

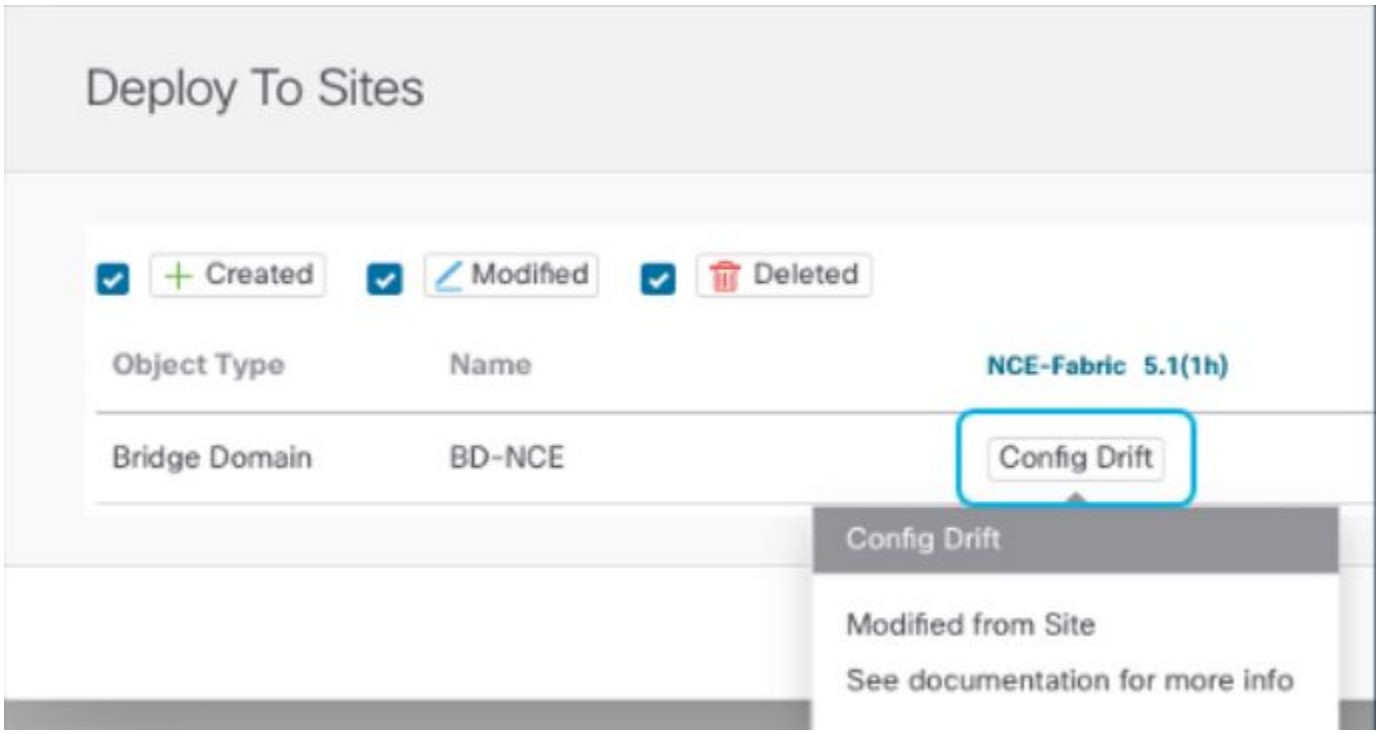
a) スキーマを選択します。
b) テンプレートを選択します。
c) **[インポート（Import）]** をクリックしてオブジェクトをインポートするサイトから選択します。
d) インポート元<site>ウィンドウで、オブジェクトを選択し、[インポート（Import）]をクリックします。
e) スキーマ内のすべてのテンプレートに対してこの手順を繰り返します。

ステップ 3 [スキーマ（Schema）]ビューで、展開ステータスが設定の変動を示しているかどうかを確認します。



ステップ 4 **[展開（Deploy）]** をクリックして設定比較画面を表示し、どのオブジェクトに設定の変動が含まれているかを確認します。

設定の差分画面には、最後の展開以降に変更されたオブジェクトが表示されます。`Config Drift` を示すオブジェクトをメモします。



ステップ 5 設定の変動が実際の場合は、競合を解決します。

a) 展開プロセスをキャンセルして、スキーマ ビューに戻ります。

b) サイトローカルのプロパティをNDOに同期するために、設定の変更を含むすべてのオブジェクトを再インポートします。

c) テンプレートを再展開します。

新しく管理されたオブジェクトのプロパティに起因するすべての設定のずれを解決したら、スキーマを再展開して、NDO とファブリック間で展開ステータスを同期します。

ステップ 6 比較に変更が表示されない場合は、テンプレートを再展開します。

ステップ 7 Nexus Dashboard Orchestrator のすべてのスキーマに対して上記の手順を繰り返します。