



Cisco Nexus ダッシュボード展開ガイド、リリース 4.2(x)

初版：2023年8月23日

最終更新：2023年8月23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](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023–2023 Cisco Systems, Inc. All rights reserved.



目次

第 1 章	新機能と更新情報 1
	新機能と更新情報 1

第 2 章	Nexus Dashboard Orchestrator の展開 3
	デプロイ概要 3
	前提条件とガイドライン 4
	ACI ファブリックのハードウェア要件 6
	NDFC ファブリックのハードウェア要件 8
	App Storeを使用した Nexus Dashboard Orchestrator サービスのインストール 9
	Nexus Dashboard Orchestrator サービスの手動インストール 10

第 1 部 :	APIC と Cloud Network Controller サイトの Day-0 オペレーション 13
---------	--

第 3 章	Cisco APIC サイトの準備 15
	ポッドプロファイルとポリシー グループ 15
	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 16
	ファブリック アクセス グローバル ポリシーの設定 16
	ファブリック アクセス インターフェイス ポリシーの設定 17
	リモート リーフ スイッチを含むサイトの設定 20
	リモート リーフの注意事項と制限事項 20
	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 20
	リモート リーフ スイッチの直接通信の有効化 21
	Cisco Mini ACI ファブリック 22

第 4 章	サイトの追加と削除	23
	Cisco NDO と APIC の相互運用性のサポート	23
	Cisco ACI サイトの追加	25
	サイトの削除	27
	ファブリック コントローラへの相互起動	28

第 5 章	インフラ一般設定	31
	インフラ設定ダッシュボード	31
	パーシャル メッシュ サイト間接続	33
	インフラの設定: 一般設定	34

第 6 章	Cisco APIC サイトのインフラの設定	39
	サイト接続性情報の更新	39
	インフラの設定: オンプレミス サイトの設定	40
	インフラの設定: ポッドの設定	43
	インフラの設定: スパイン スイッチ	43

第 7 章	Cisco Cloud Network Controller サイトのインフラの構成	47
	クラウド サイト接続性情報の更新	47
	インフラの設定: クラウド サイトの設定	48
	クラウド ネットワーク コントローラ サイトのダウンタイムからの回復	50

第 8 章	ACI サイト向けのインフラ設定の展開	53
	インフラ設定の展開	53
	オンプレミスとクラウド サイト間の接続の有効化	54

第 11 部 :	NDFC ファブリックの Day-0 オペレーション	59
----------	-----------------------------------	-----------

第 9 章	サイトの追加と削除	61
	Cisco NDFC サイトの追加	61

サイトの削除	63
ファブリック コントローラへの相互起動	65

第 10 章	Cisco NDFC サイトのインフラの構成	67
	前提条件とガイドライン	67
	インフラの設定: 一般設定	67
	サイト接続性情報の更新	71
	インフラの構成: NDFC インフラ サイト固有の設定	71
	インフラ設定の展開	74

第 III 部 :	Nexus Dashboard Orchestrator の更新	77
-----------	---	----

第 11 章	サービス カタログを介した自動アップグレード	79
	概要	79
	前提条件とガイドライン	82
	Nexus Dashboard Cluster のアップグレード	85
	Cisco App Store を使用した Orchestrator Service のアップグレード	90
	Orchestrator サービスの手動アップグレード	93
	データベースのアップグレードのファイナライズ	95
	設定のばらつきの解決	97

第 12 章	構成の復元を使用した手動アップグレード	101
	概要	101
	前提条件とガイドライン	103
	Nexus Dashboard の展開と Nexus Dashboard Orchestrator のインストール	106
	構成の復元	108
	設定のばらつきの解決	113



第 1 章

新機能と更新情報

- [新機能と更新情報 \(1 ページ\)](#)

新機能と更新情報

次の表に、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
4.1(2)	アップグレードワークフローを更新しました。	<ul style="list-style-type: none">• サービス カタログを介した自動アップグレード (79 ページ)• 構成の復元を使用した手動アップグレード (101 ページ)
4.1(1)	このドキュメントの最初のリリース。	--



第 2 章

Nexus Dashboard Orchestrator の展開

- [デプロイ概要 \(3 ページ\)](#)
- [前提条件とガイドライン \(4 ページ\)](#)
- [App Storeを使用した Nexus Dashboard Orchestrator サービスのインストール \(9 ページ\)](#)
- [Nexus Dashboard Orchestrator サービスの手動インストール \(10 ページ\)](#)

デプロイ概要

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

Cisco Nexus ダッシュボードは、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 ダッシュボード Insights や Nexus Dashboard Orchestrator などのシスコデータセンター運用サービスをホストするための共通プラットフォームです。これらのサービスはすべてのデータセンターサイトで利用でき、ネットワークポリシーと運用のためのリアルタイム分析、可視性、保証、また Cisco ACI や Cisco NDFC などのデータセンターファブリックのポリシーオーケストレーションを提供しています。

Nexus ダッシュボードは、上述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ックスタックを提供し、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ながら、これらのアプリケーションを実行し維持するための運用オーバーヘッドを削減します。また、ローカルにホストされているアプリケーションと外部のサードパーティ製アプリケーションの中央統合ポイントも提供します。

各 Nexus ダッシュボードクラスタは通常、1つまたは3つのマスターノードで構成されます。また、3ノードクラスタの場合、マスターノードで障害が発生した際に簡単にクラスタを回復させられるよう、いくつかのワーカーノードをプロビジョニングして、水平スケーリングやスタンバイノードを有効化できます。このリリースでサポートされるワーカーノードとスタンバイノードの最大数については、Cisco Nexus ダッシュボードリリース ノートの「[検証済みのスケーラビリティ制限](#)」セクションを参照してください。

Nexus ダッシュボードクラスタの初期導入と設定の詳細については、[Cisco Nexus Dashboard Deployment Guide](#) を参照してください。Nexus ダッシュボードの使用方法の詳細については、[Cisco Nexus Dashboard User Guide](#) を参照してください。

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

前提条件とガイドライン

Nexus ダッシュボード

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

Orchestrator リリース	Nexus Dashboard の最小リリース
リリース 4.1(2) 以降 (注) 4.1(2) より前のリリースの展開はお勧めしません。	Cisco Nexus Dashboard、リリース 2.2(2) 以降

Nexus ダッシュボードのネットワーク

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



(注) 二つのインターフェースは別々のサブネットに入っていないといけません。

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

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

NDO トラフィック タイプ	Nexus ダッシュボードのネットワーク
任意の送受信トラフィック： <ul style="list-style-type: none"> • Cisco APIC • Cisco NDFC • その他のリモート デバイスまたはコントローラ 	データ ネットワーク
クラスタ間通信	データ ネットワーク
監査ログ ストリーミング (Splunk/syslog)	管理ネットワーク
リモート バックアップ	管理ネットワーク

Nexus Dashboard クラスタのサイジングとサービスの共同ホスティング

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

Nexus Dashboard Orchestrator に加えて他のサービスもホストする予定の場合は、クラスタのサイジングツールの推奨事項に基づいて追加のNexusダッシュボードノードを展開して設定します。これについては、『[Cisco Nexus Dashboard User Guide](#)』（Nexus Dashboard GUI から直接入手可能）にも記載されています。



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

Network Time Protocol (NTP) とドメイン ネーム システム (DNS)

Nexus ダッシュボード ノードでの展開とアップグレードには、常に、有効な DNS サーバーと NTP サーバーが必要です。

有効な DNS 接続がない場合（到達不能またはブレースホルダ IP アドレスを使用している場合など）、システムを正常に展開またはアップグレードできない可能性があります。



(注) Nexus Dashboard は、DNS クライアントとリゾルバーの両方として機能します。内部サービス向けには、DNS リゾルバーとして機能する内部の Core DNS サーバーを使用します。また、DNS クライアントとしても動作して、イントラネット内またはインターネットの外部ホストに到達できるようにするためには、外部 DNS サーバーを構成する必要があります。

加えて、Nexus Dashboard は、ワイルドカードレコードを持つ DNS サーバーをサポートしていません。

ACI ファブリックのハードウェア要件

スパインスイッチの要件

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

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

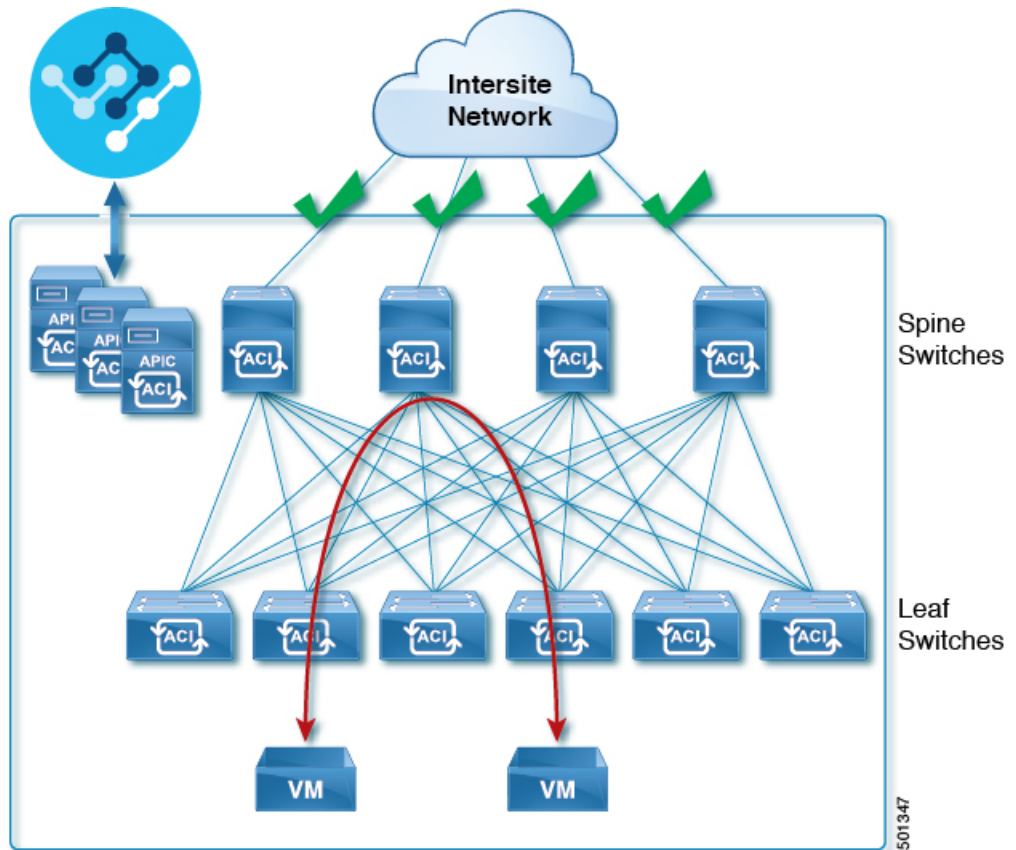
各リリースでサポートされるスパインの完全なリストについては、[ACI-mode Switches Hardware Support Matrix](#) を参照してください。

リーフスイッチの要件

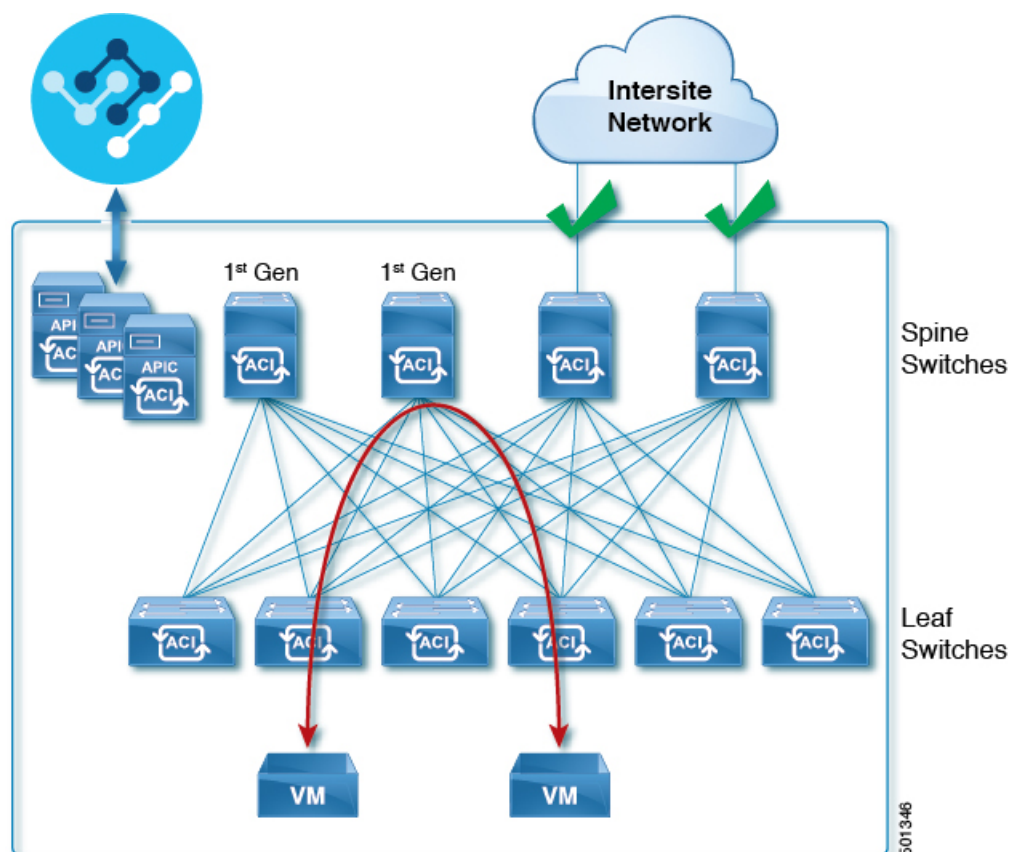
Multi-Site はファブリックのリーフスイッチに依存しないため、Cisco APIC と同じリーフスイッチモデルをサポートします。サポートされているハードウェアの完全なリストは、[ACI モードスイッチハードウェアサポートマトリックス](#) に記載されています。

サイト間の IPN 接続

次の図は、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。



NDFC ファブリックのハードウェア要件

ボーダー ゲートウェイの要件

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

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

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

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

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

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

始める前に

- [前提条件とガイドライン \(4 ページ\)](#) に記載されている要件とガイドラインを満たしていることを確認します。
- Cisco DC App Center は、管理ネットワークを介して直接、またはプロキシ設定を使用して Nexus Dashboard から到達可能である必要があります。Nexus Dashboard のプロキシ設定については、『[Nexus Dashboard User Guide](#)』を参照してください。
DC App Center への接続を確立できない場合は、このセクションをスキップして、[Nexus Dashboard Orchestrator サービスの手動インストール \(10 ページ\)](#) 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。
App Store のバージョンとは異なるバージョンをインストールする場合は、代わりに [Nexus Dashboard Orchestrator サービスの手動インストール \(10 ページ\)](#) の手順に従う必要があります。

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

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

ステップ 2 上部のナビゲーションメニューから、[管理コンソール (Admin Console)] を選択します。

サービスを展開するには、admin 権限が必要です。

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

- a) 左のナビゲーションメニューから [操作 (Operate)] > [サービス (Services)] を選択します。
- b) [アプリストア (App Store)] タブを選択します。
- c) [Nexus Dashboard Orchestrator] タイルで、[インストール (Install)] をクリックします。

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

ステップ 5 サービスが Nexus Dashboard にダウンロードされ、インストールされるまで待ちます。

ステップ 6 アプリを有効にして起動します。

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

- a) [サービス (Services)] ページで、[インストール済みサービス (Installed Services)] タブを選択します。
- b) **Nexus Dashboard Orchestrator** タイルで、[有効 (Enable)] をクリックします。
サービスが有効になると、[有効 (Enable)] ボタンが [開く (Open)] に変わります。
- c) **Nexus Dashboard Orchestrator** 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一のクレデンシャルを使用してサービスにログインできます。

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

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

始める前に

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

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

- a) DC App Center で Nexus Dashboard Orchestrator ページを参照します。
<https://dcappcenter.cisco.com/nexus-dashboard-orchestrator.html>
- b) [バージョン (Version)] ドロップダウンから、インストールするバージョンを選択し、[ダウンロード (Download)] をクリックします。
- c) [同意してダウンロードする (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 Nexus Dashboard の GUI にログインします。

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

ステップ 3 上部のナビゲーションメニューから、[管理コンソール (Admin Console)] を選択します。

サービスを展開するには、admin 権限が必要です。

ステップ 4 画像を手動で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 [操作 (Operate)] > [サービス (Services)] を選択します。
- b) [インストール済みサービス (Installed Services)] タブをクリックします。
- c) メインペインの右上にある [アクション (Actions)] > [サービスのアップロード (Upload Service)] をクリックします。
- d) イメージの場所を選択します。
サービス画像をシステムにダウンロードした場合は、[ローカル (Local)] を選択します。
サーバでイメージをホストしている場合は、[リモート (Remote)] を選択します。
- e) イメージファイルを選択します
前のサブステップで [ローカル (Local)] を選択した場合は、[ファイルの選択 (Select File)] をクリックし、ダウンロードした画像を選択します。
[リモート (Remote)] を選択した場合は、イメージファイルのフル URL を指定します。たとえば、`http://<ip-address>:<port>/<full-path>/cisco-mso-<version>.nap` のようになります。
- f) [アップロード (Upload)] をクリックして、サービスをクラスタに追加します。

ステップ 5 サービスが Nexus Dashboard にダウンロードされ、インストールされるまで待ちます。**ステップ 6** アプリを有効にして起動します。

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

- a) [サービス (Services)] ページで、[インストール済みサービス (Installed Services)] タブを選択します。
- b) **Nexus Dashboard Orchestrator** タイルで、[有効 (Enable)] をクリックします。
サービスが有効になると、[有効 (Enable)] ボタンが [開く (Open)] に変わります。
- c) **Nexus Dashboard Orchestrator** 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一クレデンシャルを使用してサービスにログインできます。



第 1 部

APIC と Cloud Network Controller サイトの Day-0 オペレーション

- [Cisco APIC サイトの準備 \(15 ページ\)](#)
- [サイトの追加と削除 \(23 ページ\)](#)
- [インフラ一般設定 \(31 ページ\)](#)
- [Cisco APIC サイトのインフラの設定 \(39 ページ\)](#)
- [Cisco Cloud Network Controller サイトのインフラの構成 \(47 ページ\)](#)
- [ACI サイト向けのインフラ設定の展開 \(53 ページ\)](#)



第 3 章

Cisco APIC サイトの準備

- [ポッドプロファイルとポリシーグループ \(15 ページ\)](#)
- [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 \(16 ページ\)](#)
- [リモートリーフスイッチを含むサイトの設定 \(20 ページ\)](#)
- [Cisco Mini ACI ファブリック \(22 ページ\)](#)

ポッドプロファイルとポリシーグループ

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

ステップ 1 サイトの APIC GUI にログインします。

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

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

ステップ 3 必要であれば、ポッドポリシーグループを作成します。

- [**ファブリック (Fabric)**] > [**ファブリック ポリシー (Fabric Policies)**] > [**ポッド (Pods)**] > [**ポリシーグループ (Policy Groups)**] に移動します。
- [**ポリシーグループ (Policy Groups)**] を右クリックし、[**ポッドポリシーグループの作成 (Create Pod Policy Groups)**] を選択します。
- 適切な情報を入力して、[**Submit**] をクリックします。

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

- [**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。
- デフォルトのプロファイルを選択します。
- 新しいポッドポリシーグループを選択し、[**更新 (Update)**] をクリックします。

すべての APIC サイトのファブリック アクセス ポリシーの設定

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

ファブリック アクセス グローバル ポリシーの設定

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

ステップ 1 サイトの APIC GUI に直接ログインします。

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

サイトを Nexus Dashboard Orchestrator に追加するには、いくつかのファブリックポリシーを設定する必要があります。APIC の観点からは、ベアメタルホストを接続していた場合と同様に、ドメイン、AEP、ポリシーグループ、およびインターフェイスセレクトア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VLAN4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。

- 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。
- [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。

- 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 エンティティ 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-13です。
 - 関連付けられている接続可能エンティティ プロファイルの場合は、ステップ 4で作成した AEP を選択します。
 - VLAN プールの場合は、ステップ 3で作成した VLAN プールを選択します。
- c) [送信 (Submit)] をクリックします。

セキュリティ ドメインなどの追加の変更は必要ありません。

次のタスク

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

ファブリック アクセス インターフェイス ポリシーの設定

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

始める前に

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

ステップ 1 サイトの APIC GUI に直接ログインします。

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

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

ステップ 3 スパイン ポリシー グループを設定します。

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

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

b) **[スパイン ポリシー グループ (Spine Policy Groups)]** カテゴリを右クリックして、**[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 Profil)]** 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 Selector)]** で、**[+]** をクリックしてスパインを追加し、次の情報を入力します。
 - **[名前 (name)]** フィールドで、セレクタの名前を指定します (例: Spine1)。
 - **[ブロック (Blocks)]** フィールドで、スパイン ノードを指定します (例: 201)。
- c) **[更新 (Update)]** をクリックして、セレクタを保存します。
- d) **[次へ (Next)]** をクリックして、次の画面に進みます。
- e) 前の手順で作成したインターフェイス プロファイルを選択します。
たとえば、Spine1-ISN などです。
- f) **[完了 (Finish)]** をクリックしてスパイン プロファイルを保存します。

リモート リーフ スイッチを含むサイトの設定

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

リモート リーフの注意事項と制限事項

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

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

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

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

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

リモート リーフ スイッチのルーティング可能なサブネットの設定

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

-
- ステップ 1** サイトの APIC GUI に直接ログインします。
- ステップ 2** メニューバーから、[ファブリック (Fabric)] > [インベントリ (Inventory)] を選択します。
- ステップ 3** [ナビゲーション (Navigation)] ウィンドウで、[ポッドファブリックセットアップポリシー (Pod Fabric Setup Policy)] をクリックします。
- ステップ 4** メインペインで、サブネットを設定するポッドをダブルクリックします。
- ステップ 5** ルーティング可能なサブネットエリアで、+ 記号をクリックしてサブネットを追加します。
- ステップ 6** IP アドレスと予約アドレスの数を入力し、状態をアクティブまたは非アクティブに設定してから、[更新 (Update)] をクリックしてサブネットを保存します。
- ルーティング可能なサブネットを設定する場合は、/22~/29 の範囲のネットマスクを指定する必要があります。
- ステップ 7** [送信 (Submit)] をクリックして設定を保存します。
-

リモートリーフスイッチの直接通信の有効化

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



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

-
- ステップ 1** サイトの APIC に直接ログインします。
- ステップ 2** リモートリーフスイッチの直接トラフィック転送を有効にします。
- 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。
 - 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。
 - [リモートリーフ直接トラフィック転送 (Enable Remote Leaf Direct Traffic 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。
- [送信 (Submit)] をクリックして変更を保存します。
-

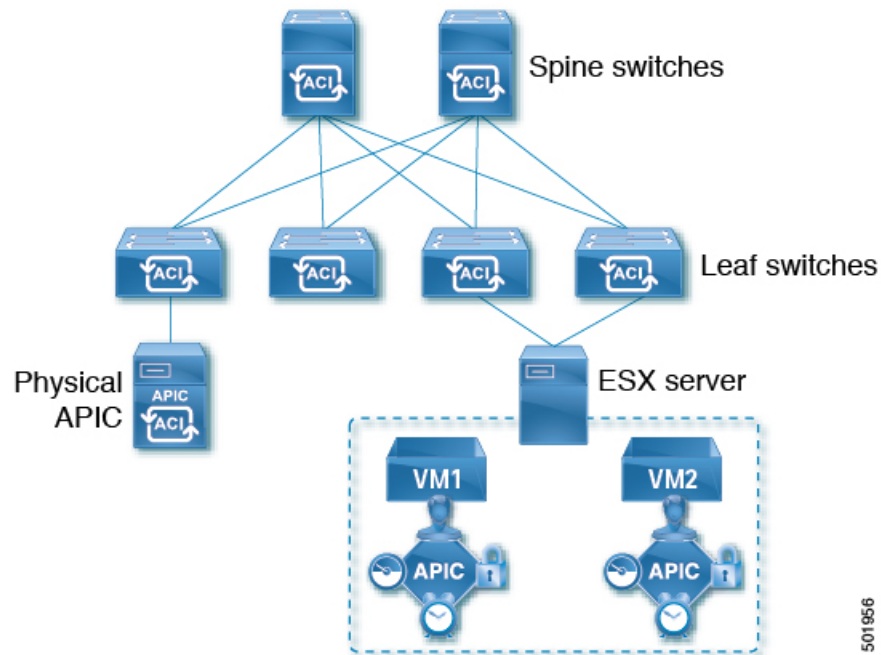
Cisco Mini ACI ファブリック

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 of ファブリックの導入と設定に関する詳細情報は、『[Cisco Mini ACI ファブリックおよび仮想 APIC](#)』に記述されています。

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

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

図 1: Cisco Mini ACI ファブリック



501956



第 4 章

サイトの追加と削除

- [Cisco NDO と APIC の相互運用性のサポート \(23 ページ\)](#)
- [Cisco ACI サイトの追加 \(25 ページ\)](#)
- [サイトの削除 \(27 ページ\)](#)
- [ファブリック コントローラへの相互起動 \(28 ページ\)](#)

Cisco NDO と APIC の相互運用性のサポート

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

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

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

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

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



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

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

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

Cisco ACI サイトの追加

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

始める前に

- この章の前のセクションで説明したように、オンプレミスの ACI サイトを追加する際には、各サイトの APIC でサイト固有の構成を完了している必要があります。
- 追加するサイトの 1 つ以上がリリース 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 Cisco Nexus Dashboard にログインして [管理コンソール (Admin Console)] を開きます。

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

ステップ 3 **[サイトの追加 (Add Site)]** を選択し、情報を提供します。

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

(注) APIC ファブリックでは、Cisco Nexus Dashboard Orchestrator サービスのみでサイトを使用する場合、APIC のインバンドまたはアウトオブバンド IP アドレスを指定できます。Cisco 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 Cisco Nexus Insights などのデイ 2 オペレーションアプリケーションで使用する場合は、追加する Cisco Nexus Dashboard をファブリックに接続するために使用する **インバンド EPG** 名も指定する必要があります。それ以外の場合、このサイトを Cisco 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。
- Cloud Network Controller サイトの場合、プロキシ経由でクラウドサイトに到達できる場合は、**[プロキシを有効 (Enable Proxy)]** にします。

プロキシは、Cisco Nexus Dashboard のクラスタ設定ですでに構成されている必要があります。管理ネットワーク経由でプロキシに到達できる場合は、プロキシ IP アドレス用のスタティック管理ネットワークルートも追加する必要があります。プロキシとルートの構成の詳細については、お使いのリリースの Nexus Dashboard ユーザーガイドを参照してください。 <https://www.cisco.com/c/en/us/support/data-center-analytics/nexus-dashboard/products-installation-and-configuration-guides-list.html>

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

現在、サイトは Cisco Nexus ダッシュボードで使用できますが、次の手順で説明するように、Cisco Nexus Dashboard Orchestrator 管理のため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 または、Cloud Network Controller サイトに対して前の手順を繰り返します。

ステップ 5 Cisco Nexus Dashboard の **[サービス (Services)]** から、Cisco Nexus Dashboard Orchestrator サービスを開きます。

Cisco Nexus Dashboard ユーザーのクレデンシャルを使用して自動的にサインインします。

ステップ 6 Cisco Nexus Dashboard Orchestrator GU でサイトを管理します。

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

サイトを管理するときは、サイトごとに一意のサイト ID を指定する必要があります。

サイトの削除

ここでは、Cisco 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 Cisco 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 Cisco Nexus Dashboard Orchestrator GUI を開きます。

Cisco Nexus Dashboard の **サービス カタログ** から NDO サービスを開きます。Cisco Nexus Dashboard ユーザーのクレデンシャルを使用して自動的にサインインします。

ステップ 2 すべてのテンプレートからサイトを削除します。

サイトを管理解除して Cisco Nexus Dashboard から削除する前に、関連付けられているすべてのテンプレートからサイトを削除する必要があります。

- a) **[構成 (Configure)] > [テナント テンプレート (Tenant Template)] > [アプリケーション (Applications)]** に移動します。
- b) サイトに関連付けられた 1 つ以上のテンプレートを含む **[スキーマ (Schema)]** をクリックします。
- c) **[概要 (Overview)]** ドロップダウンから、削除するサイトに関連付けられているテンプレートを選択します。
- d) **[アクション (Actions)]** ドロップダウンから、**[サイトの追加/削除 (Add/Remove Sites)]** を選択し、削除するサイトのチェックを外します。

これにより、このテンプレートを使用してこのサイトに展開された構成が削除されます。

(注) ストレッチされていないテンプレートの場合、代わりに **[アクション (Actions)] > [サイトの関連付けを解除 (Dissociate Sites)]** を選択して、テンプレートによってサイトに展開された構成を保持することを選択できます。このオプションを使用すると、NDO によって展開された構成を保持できますが、それらのオブジェクトを NDO から管理することはできなくなります。

- e) このスキーマおよび他のすべてのスキーマで管理解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について、この手順を繰り返します。

ステップ 3 サイトのアンダーレイ設定を削除します。

- a) 左のナビゲーションメニューから、**[構成 (Configure)] > [サイト間接続 (Site To Site Connectivity)]** を選択します。
- b) メイン ペインにある **[構成 (Configure)]** をクリックします。

- c) 左のサイドバーで、管理対象から外すサイトを選択します。
- d) 右側のサイドバーの [サイト間接続 (Inter-Site Connectivity)] タブで、[マルチサイト (Multi-Site)] チェックボックスを無効にします。

これにより、このサイトと他のサイト間の EVPN ピアリングが無効になります。

- e) [展開する (Deploy)] をクリックして、変更をサイトに展開します。

ステップ 4 Cisco Nexus Dashboard Orchestrator GUI で、サイトを無効にします。

- a) 左のナビゲーションメニューから [サイト (Sites)] を選択します。
- b) メインペインで、非管理対象に設定したいサイトに対して [状態 (State)] を [非管理対象 (Unmanaged)] から [管理対象 (Managed)] に変更します。

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

ステップ 5 Cisco Nexus Dashboard 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、Cisco Nexus ダッシュボードからもサイトを削除できます。

(注) このサイトは、Cisco Nexus Dashboard クラスタにインストールされているどのサービスでも使用されないようにしてください。

- a) 上部のナビゲーションバーで [ホーム (Home)] アイコンをクリックして、Cisco Nexus Dashboard GUI に戻ります。
- b) Cisco Nexus Dashboard GUI の左側のナビゲーションメニューから、[操作 (Operate)] > [サイト (Sites)] を選択します。
- c) 削除するサイトを1つ以上選択します。
- d) メインペインの右上にある [アクション (Actions)] > [サイトの削除 (Delete Site)] をクリックします。
- e) サイトのサインイン情報を入力し、[OK] をクリックします。

Cisco 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

Cisco Nexus Dashboard Orchestrator は現在、ファブリックのタイプごとにいくつかの構成オプションをサポートしています。追加の多くの構成オプションでは、ファブリックのコントローラに直接サインインする必要があります。

NDO の [操作 (Operate)] > [サイト (Sites)] 画面から特定のサイトコントローラの GUI にクロス起動するには、サイトの横にあるアクション (...) メニューを選択し、ユーザーインターフェイスで [開く (Open)] をクリックします。クロス起動は、ファブリックのアウトオブバンド (OOB) 管理IPで動作します。

Cisco Nexus Dashboardとファブリックで同じユーザーが構成されている場合、Cisco Nexus Dashboard ユーザーと同じサイン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、Cisco Nexus Dashboard とファブリック全体で共通のユーザーによるリモート認証を構成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](#) (31 ページ)
- [パーシャルメッシュサイト間接続](#) (33 ページ)
- [インフラの設定: 一般設定](#) (34 ページ)

インフラ設定ダッシュボード

[構成 (Config)] > [サイト間の接続 (Site To Site Connectivity)] ページでは、Cisco Nexus Dashboard Orchestrator 展開のすべてのサイトと、サイト間接続の概要が表示され、次の情報が含まれています

図 2: インフラ設定の概要

The screenshot shows the 'Site To Site Connectivity' configuration page in the Cisco Nexus Dashboard. The page is divided into several sections, each marked with a numbered blue circle:

- 1. General Settings:** Displays BGP Peering Type (full-mesh), Keep Alive Interval (60), Hold Interval (180), BGP TTL (16), State Interval (300), Graceful Start (True), Maximum AS Limit (N/A), and IANA Assigned Port (False).
- 2. Site1:** Displays Pods (2), Spines (4), ACI Multi-Site (On), BGP ASN (655), Cloudsec Encryption (Off), OSPF Area ID (backbone), APIC Site ID (1), OSPF Area Type (regular), and Overlay Multicast TEP (12.10.100.200).
- 3. Site2:** Displays Pods (1), Spines (2), ACI Multi-Site (On), BGP ASN (100), Cloudsec Encryption (Off), OSPF Area ID (backbone), APIC Site ID (2), OSPF Area Type (regular), and Overlay Multicast TEP (16.16.200.100).
- 4. Inter-Site Connections:** Shows a table for Site2 connections with columns for Site Name, Deployment Status, Operational Status, BGP EVPN Status, and Tunnel Status.

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

詳細については、次のセクションで説明します。

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

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

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

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

詳細については、[Cisco Cloud Network Controller サイトのインフラの構成 \(47 ページ\)](#) を参照してください。

4. [接続ステータスの表示 (Show Connectivity Status)] をクリックして、特定のサイトのサイト間接続の詳細を表示できます。
5. [構成 (Configure)] ボタンを使用して、サイト間接続構成に移動できます。これについては、次のセクションで詳しく説明します。

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

パーシャルメッシュ サイト間接続

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

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

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

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

パーシャルメッシュ接続のガイドライン

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

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

すべてのオンプレミスサイト間で完全なメッシュ接続が自動的に確立されます。

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

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

インフラの設定: 一般設定

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



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

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

ステップ 2 左のナビゲーションメニューから、[構成 (Configure)] > [サイト間接続 (Site To Site Connectivity)] を選択します。

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

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

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

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

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

- **full-mesh** : 各サイトのすべてのボーダーゲートウェイスイッチは、リモートサイトのボーダーゲートウェイスイッチとのピア接続を確立します。

full-mesh 構成では、Cisco Nexus Dashboard Orchestrator は ACI 管理ファブリックのスパインスイッチと NDFC 管理ファブリックのボーダーゲートウェイを使用します。

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

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

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

デフォルト値を維持することを推奨します。

- d) **[保留間隔 (秒) (Hold Interval (Seconds))]** フィールドに、保留間隔を秒単位で入力します。
デフォルト値を維持することを推奨します。
- e) **[失効間隔 (秒) (Stale Interval (Seconds))]** フィールドに、失効間隔を秒単位で入力します。
デフォルト値を維持することを推奨します。
- f) **[グレースフル ヘルパー (Graceful Helper)]** オプションをオンにするかどうかを選択します。
- g) **[AS 上限 (Maximum AS Limit)]**を入力します。
デフォルト値を維持することを推奨します。
- h) **[ピア間のBGP TTL (BGP TTL Between Peers)]**を入力します。
デフォルト値を維持することを推奨します。
- i) **[OSPF エリア ID (OSPF Area ID)]** を入力します。
Cloud Network Controller サイトがない場合、このフィールドは UI に表示されません。
これは、オンプレミス IPN ピアリングのためにクラウドサイトで使用される OSPF エリア ID です。
- j) (オプション) CloudSec 暗号化の **[IANA 割り当てポート (IANA Assigned Port)]**を有効にします。
デフォルトでは、CloudSec は独自の UDP ポートを使用します。このオプションを使用すると、サイト間の CloudSec 暗号化に公式の IANA 予約ポート 8017 を使用するように CloudSec を構成できます。

(注) IANA 予約ポートは、リリース 5.2(4) 以降を実行している Cisco APIC サイトでサポートされています。

この設定を変更するには、すべてのサイトで CloudSec を無効にする必要があります。IANA 予約ポートを有効にしたいが、すでに 1 つ以上のサイトで CloudSec 暗号化を有効にしている場合は、すべてのサイトで CloudSec を無効にし、**[IANA 予約 UDP ポート (IANA Reserve UDP Port)]** オプションを有効にしてから、必要なサイトで CloudSec を再度有効にします。

CloudSec を構成するための詳細情報と手順については、『[ACI ファブリック用の Nexus Dashboard Orchestrator 構成ガイド \(Nexus Dashboard Orchestrator Configuration Guide for ACI Fabrics\)](#)』の「CloudSec 暗号化」の章を参照してください。

ステップ 6 [IPN デバイス情報] を入力します。

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

後のセクションで説明するように、オンプレミスとクラウドサイト間のサイトアンダーレイ接続を構成する場合は、クラウド CSR への接続を確立するオンプレミス IPN デバイスを選択する必要があります。これらの IPN デバイスは、オンプレミスサイトの設定画面で使用可能になる前に、ここで定義する必要があります。詳細は [インフラの設定: オンプレミス サイトの設定 \(40 ページ\)](#) を参照してください。

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

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

これは、デバイスが NDFC によって直接管理されるかどうかを定義します。

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

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

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

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

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

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

Cloud Network Controller サイトがない場合、このタブは UI に表示されません。

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

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

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

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

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

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

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

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

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

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

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

Cloud Network Controller サイトがない場合、このタブは UI に表示されません。

ここで指定できるサブネットプールには、次の 2 つのタイプがあります。

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

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

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

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

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

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

(注) 両方のサブネットプールの最小マスク長は /24 です。

1 つ以上の外部サブネットプールを追加するには :

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

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

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

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

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

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

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

- c) サブネットの **[名前 (Name)]** を入力します。

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

- d) **[+IPアドレスの追加(+Add IP Address)]**をクリックして、1つ以上のサブネットプールを追加します。
サブネットには /16 と /24 の間のネットワークが必要で、0.x.x.x または 0.0.x.x で始めることはできません。たとえば、30.29.0.0/16 のようにします。
 - e) チェックマーク アイコンをクリックして、サブネット情報を保存します。
同じ名前付きサブネット プールに複数のサブネットを追加する場合は、この手順を繰り返します。
 - f) **[保存 (Save)]**をクリックして、名前付きサブネット プールを保存します。
 - g) 追加する名前付きサブネット プールについて、これらのサブステップを繰り返します。
-

次のタスク

全般的なインフラ設定を構成した後も、管理するサイトのタイプ (ACI、Cloud Network Controller、またはNDFC) に基づいて、サイト固有の設定に関する追加情報を指定する必要があります。次の項で説明する手順に従って、サイト固有のインフラストラクチャ設定を行います。



第 6 章

Cisco APIC サイトのインフラの設定

- [サイト接続性情報の更新 \(39 ページ\)](#)
- [インフラの設定: オンプレミス サイトの設定 \(40 ページ\)](#)
- [インフラの設定: ポッドの設定 \(43 ページ\)](#)
- [インフラの設定: スパインスイッチ \(43 ページ\)](#)

サイト接続性情報の更新

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

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

ステップ 2 左のナビゲーションメニューから、**[構成 (Config)]** > **[サイト間接続 (Site To Site Connectivity)]** を選択します。

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

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

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

ステップ 6 (オプション) オンプレミス サイトの場合、廃止されたスパインスイッチノードの設定を削除する場合は、**[確認 (Confirmation)]** ダイアログでチェックボックスをオンにします。

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

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

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

インフラの設定: オンプレミス サイトの設定

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

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

ステップ 2 左のナビゲーションメニューから、**[構成 (Configure)] > [サイト間接続 (Site To Site Connectivity)]** を選択します。

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

ステップ 4 左側のペインの **[サイト (Sites)]** の下で、特定のオンプレミスサイトを選択します。

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

a) 右側の **<サイト (Site)> [設定 (Settings)]** ペインで、**[マルチサイト (Multi-Site)]** ノブを有効にします。これは、オーバーレイ接続がこのサイトと他のサイト間で確立されるかどうかを定義します。

b) (オプション n) **[CloudSec 暗号化 (CloudSec Encryption)]** ノブを有効にして、サイトを暗号化します。CloudSec 暗号化は、サイト間トラフィックの暗号化機能を提供します。この機能の詳細については、[Cisco Multi-Site Configuration Guide](#) の「Infrastructure Management」の章を参照してください。

c) **[オーバーレイ 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係なく、同じファブリックの一部であるすべてのスパインスイッチに展開されます。

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

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

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

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

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

g) ドロップダウンリストから、該当する **[OSPF エリアタイプ (OSPF Area Type)]** を選択します。

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

OSPF エリアタイプは、次のいずれかになります。

- nssa
- regular

- h) サイトの OSPF ポリシーを設定します。

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

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

- **[ポリシー名 (Policy Name)]** フィールドにポリシー名を入力します。
- **[(ネットワーク タイプ (Network Type))]** フィールドで、**[ブロードキャスト (broadcast)]**、**[ポイントツーポイント (point-to-point)]**、または **[未指定 (unspecified)]** のいずれかを選択します。
デフォルトは **[ブロードキャスト (broadcast)]** です。
- **[優先順位 (Priority)]** フィールドに、優先順位番号を入力します。
デフォルトは **1** です。
- **[インターフェイスのコスト (Cost of Interface)]** フィールドに、インターフェイスのコストを入力します。
デフォルト値は **0** です。
- **[インターフェイス制御 (Interface Controls)]** ドロップダウンリストから、以下のいずれかを選択します。
 - **アドバタイズサブネット (advertise-subnet)**
 - **BFD (bfd)**
 - **MTU 無視 (mtu-ignore)**
 - **受動的参加 (passive-participation)**
- **[Hello 間隔 (秒) (Hello Interval (Seconds))]** フィールドに、hello 間隔を秒単位で入力します。
デフォルト値は **10** です。
- **[Dead 間隔 (秒) (Dead Interval (Seconds))]** フィールドに、dead 間隔を秒単位で入力します。
デフォルト値は **40** です。
- **[再送信間隔 (秒) (Retransmit Interval (Seconds))]** フィールドに、再送信間隔を秒単位で入力します。
デフォルト値は **5** です。
- **[転送遅延 (秒) (Transmit Delay (Seconds))]** フィールドに、遅延を秒単位で入力します。
デフォルトは **1** です。

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

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

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

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

サイトの SDA 接続を有効にする場合は、『*ACI ファブリックの Cisco マルチサイト構成ガイド*』の「SDA 使用例」の章で説明されている追加構成を行う必要があります。

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

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

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

デフォルトの範囲は 16000 ~ 23999 です。

サイトの MPLS 接続を有効にする場合は、『*ACI ファブリックの Cisco マルチサイト構成ガイド*』の「SR-MPLS 経路で接続されたサイト」の章で説明されている追加構成を行う必要があります。

ステップ 6 オンプレミスとクラウドサイト間のサイト間接続を構成します。

オンプレミスサイトとクラウドサイトの間サイトに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構成する場合は、Cloud Network Controller の CSR がトンネルを確立する IPN デバイスの IP アドレスを指定し、クラウドサイトのインフラ設定を行う必要があります。

- a) **[+ IPN デバイスの追加 (+ Add IPN Device)]** をクリックして、IPN デバイスを指定します。
b) ドロップダウンから、前に定義した IPN デバイスのいずれかを選択します。

IPN デバイスは、**[一般設定 (General Settings)] > [IPN デバイス (IPN Devices)]** リストですでに定義されている必要があります。 [インフラの設定: 一般設定 \(34 ページ\)](#) を参照してください。

- c) クラウドサイトのサイト間接続を構成します。

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 Network Controller サイトのインフラの構成 \(47 ページ\)](#) の説明に従ってクラウドサイト側から行う必要があります。

次のタスク

必要なサイト間接続情報をすべて設定しましたが、まだサイトにプッシュされていません。[インフラ設定の展開 \(53 ページ\)](#) の説明に従って、構成を展開する必要があります。

インフラの設定: ポッドの設定

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

- ステップ 1** Cisco Nexus Dashboard Orchestrator の GUI にログインします。
- ステップ 2** 左のナビゲーションメニューから、**[構成 (Configure)] > [サイト間接続 (Site To Site Connectivity)]** を選択します。
- ステップ 3** メインペインの右上にある **[構成 (Configure)]** をクリックします。
- ステップ 4** 左側のペインの **[サイト (Sites)]** の下で、特定のサイトを選択します。
- ステップ 5** メイン ウィンドウで、ポッドを選択します。
- ステップ 6** 右の **[ポッドのプロパティ (Pod Properties)]** ペインで、ポッドについてオーバーレイ ユニキャスト TEP を追加できます。

この IP アドレスは、同じポッドの一部であるすべてのスパインスイッチに展開され、レイヤ 2 およびレイヤ 3 ユニキャスト通信の VXLAN カプセル化トラフィックの送信と受信に使用されます。
- ステップ 7** **[+ TEP プールの追加 (+Add TEP Pool)]** をクリックして、ルーティング可能な TEP プールを追加します。

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

以前に APIC でファブリックに割り当てられた外部 TEP プールは、ファブリックが Multi-Site ドメインに追加されると、NDO によって自動的に継承され、GUI に表示されます。
- ステップ 8** サイトの各ポッドに対してこの手順を繰り返します。

インフラの設定: スパインスイッチ

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

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

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

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

ステップ 2 左のナビゲーションメニューから、**[構成 (Config)] > [サイト間接続 (Site To Site Connectivity)]** を選択します。

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

ステップ 4 左側のペインの **[サイト (Sites)]** の下で、特定のオンプレミスサイトを選択します。

ステップ 5 メインペインで、ポッド内のスパインスイッチを選択します。

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

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

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

a) 次の一般情報を指定します。

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

これは、IPN への接続に使用されるインターフェイスです。

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

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

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

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

ステップ 8 アンダーレイ プロトコルを選択します。

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

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

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

OSPF 設定が使用可能になります。

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

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

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

- MD5

- Simple

- **[BGP]** を [無効 (Disabled)] に設定します。

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

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

(注) 次の場合、BGP IPv4 アンダーレイはサポートされません。

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

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

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

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

- **[BGP]** を [有効 (Enabled)] に設定します。

BGP 設定が使用可能になります。

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

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

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

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

- **[BGP パスワード (BGP Password)]** フィールドに、BGP ピア パスワードを入力します。

- 必要に応じて追加のオプションを指定します。

- 双方向フォワーディング検出: 双方向フォワーディング検出 (BFD) プロトコルを有効にして、このポートと IPN デバイスの物理リンクの障害を検出します。
- 管理状態: ポートの管理状態を有効に設定します。

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



第 7 章

Cisco Cloud Network Controller サイトのインフラの構成

- [クラウドサイト接続性情報の更新](#) (47 ページ)
- [インフラの設定: クラウドサイトの設定](#) (48 ページ)
- [クラウドネットワークコントローラサイトのダウンタイムからの回復](#) (50 ページ)

クラウドサイト接続性情報の更新

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

- ステップ 1** Cisco Nexus Dashboard Orchestrator の GUI にログインします。
- ステップ 2** 左のナビゲーションメニューから、**[構成 (Config)]** > **[サイト間接続 (Site To Site Connectivity)]** を選択します。
- ステップ 3** メインペインの右上にある **[構成 (Configure)]** をクリックします。
- ステップ 4** 左側のペインの **[サイト (Sites)]** の下で、特定のサイトを選択します。
- ステップ 5** メインウィンドウで **[更新 (Refresh)]** ボタンをクリックして、新規または変更された CSR およびリージョンを検出します。
- ステップ 6** 最後に、**[はい (Yes)]** をクリックして確認し、接続情報をロードします。
これにより、新規または削除された CSR およびリージョンが検出されます。
- ステップ 7** **[導入 (Deploy)]** をクリックして、クラウドサイトの変更を、接続している他のサイトに伝達します。
クラウドサイトの接続を更新し、CSR またはリージョンが追加または削除された後、インフラ構成を展開して、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 Network Controller サイト固有のインフラ設定を構成する方法について説明します。

- ステップ 1** Cisco Nexus Dashboard Orchestrator の GUI にログインします。
- ステップ 2** 左のナビゲーションメニューから、**[構成 (Config)]** > **[サイト間接続 (Site To Site Connectivity)]** を選択します。
- ステップ 3** メイン ペインの右上にある **[構成 (Configure)]** をクリックします。
- ステップ 4** 左側のペインの **[サイト (Sites)]** の下で、特定のクラウドサイトを選択します。
- ステップ 5** **[サイト間接続 (Inter-Site Connectivity)]** 情報を入力します。
- 右側の **[<Site> 設定 (Settings)]** ペインで、**[サイト間接続 (Inter-Site Connectivity)]** タブを選択します。
 - [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。
オーバーレイ構成は、次の手順で説明するようにアンダーレイ サイト間接続が確立されていないサイトにはプッシュされません。
 - (オプション) **[BGP パスワード (BGP Password)]** を指定します。
- ステップ 6** サイト固有の **[サイト間接続 (Inter-Site Connectivity)]** 情報を入力します。
- クラウドサイトの右側のプロパティ サイドバーで、**[サイトの追加 (Add Site)]** をクリックします。
[サイトの追加 (Add Site)] ウィンドウが表示されます。
 - [サイトへの接続 (Connected to Site)]** で、**[サイトの選択 (Select a Site)]** をクリックし、構成しているサイト (たとえば、Site1) からの接続を確立するサイト (たとえば、Site2) を選択します。
リモートサイトを選択するとき、**[サイトの追加 (Add Site)]** ウィンドウが更新され、両方向の接続が反映されます。**[サイト 1 (Site1)]** > **[サイト 2 (Site2)]** および **[サイト 1 (Site1)]** > **[サイト 2 (Site2)]**。
 - [サイト 1 (Site1)]** > **[サイト 2 (Site2)]** エリアで、**[接続タイプ (Connection Type)]** ドロップダウンから、サイト間の接続のタイプを選択します。
次のオプションを使用できます。
 - パブリック インターネット** : 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は異なる接続タイプを使用できます。

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

[BGP-EVPN] 接続を使用している場合、オプションで [IPsec] を有効にして、使用するインターネットキー エクスチェンジ (IKE) プロトコルのバージョン（構成に応じて IKEv1（バージョン 1）または IKEv2（バージョン 1））を選択できます。

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

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

[サイト1 (Site1)] > [サイト2 (Site2)] の接続情報が提供された後、[サイト2 (Site2)] > [サイト1 (Site1)] 領域は、反対方向の接続情報を反映します。

- e) [保存 (Save)] をクリックして、サイト間の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、右側のサイドバーにある [サイト間接続 (Inter-site Connectivity)] 情報を選択することで確認できます。

- f) 他のサイトのサイト間接続を追加するには、この手順を繰り返します。

site1 から site2 へのアンダーレイ接続を確立すると、リバース接続が自動的に行われます。

ただし、site1 から site3 へのサイト間接続も確立する場合は、そのサイトに対してもこの手順を繰り返す必要があります。

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

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

外部接続の使用例の詳細な説明は、『Nexus Dashboard Orchestrator を使用したクラウド CSR からの外部接続の構成』ドキュメントで入手できます。

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

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

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

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

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

これは、一般的なインフラストラクチャ構成時に**[一般設定 (General Settings)]** > **[外部デバイス (External Devices)]** リストに追加した外部デバイスであり、[インフラの設定: 一般設定 \(34 ページ\)](#)の説明に従ってすでに定義されている必要があります。

- e) **[トンネル IKE バージョン (Tunnel IKE Version)]** ドロップダウンから、クラウドサイトの CSR と外部デバイス間の IPSec トンネルの確立に使用する IKE バージョンを選択します。
- f) (オプション) **[トンネル サブネット プール (Tunnel Subnet Pool)]** ドロップダウンから、名前付きサブネット プールのいずれかを選択します。

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

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

この接続に特定のサブネット プールを提供する場合は、[インフラの設定: 一般設定 \(34 ページ\)](#)の説明に従って作成済みである必要があります。

- g) (オプション) **[事前共有キー (Pre-Shared Key)]** フィールドに、トンネルの確立に使用するカスタムキーを入力します。
- h) 必要に応じて、同じ外部接続 (同じ VRF) に対して追加する外部デバイスについて、前のサブステップを繰り返します。
- i) 必要に応じて、追加の外部接続 (異なる VRF) に対してこの手順を繰り返します。

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

次のタスク

必要なサイト間接続情報をすべて構成しましたが、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 \(53 ページ\)](#)の説明に従って、構成を展開する必要があります。

クラウド ネットワーク コントローラ サイトのダウンタイムからの回復

クラウド ネットワーク コントローラ (以前の Cloud APIC) インスタンス/VM が NDO によって管理されているときに何らかの理由でダウンすると、そのクラウドサイトに関連付けられている既存のテンプレートを展開解除または削除できない場合があります。この場合、NDO でサイトを強制的に管理解除しようとする、サイトが回復した場合でも、古い構成および展開エラーが発生する可能性があります。

この状態から回復するには：

ステップ 1 新しいクラウドネットワーク コントローラ サイトを起動し、クラウドサイトを再登録します。

- a) NDOにログインします。
- b) 管理コンソールを開きます。
- c) **[操作 (Operate)]** > **[サイト (Sites)]** ページに移動します。
- d) 再展開したサイトの隣にあるアクション (...) メニューから、**[サイトの編集 (Edit Site)]** を選択します。
- e) **[サイトを再登録する (Reregister site)]** チェックボックスをチェックします。
- f) 新しいサイトの詳細を提供します。

サイトの新しいパブリック IP アドレスとサインイン資格情報を提供する必要があります。

- g) **[保存 (Save)]** をクリックして、サイトを再登録します。

サイトの接続ステータスが UP と表示されると、NDO のサイト IP も更新され、新しいサイトは「管理」状態になります。

ステップ 2 スキーマごとに以前に展開されたテンプレートを展開解除します。

- a) NDOにログインします。
- b) **[構成 (Configure)]** に移動し、**[テナント テンプレート (Tenant Template)]** > **[アプリケーション (Applications)]** を選択します。
- c) テンプレートが展開されているスキーマをクリックします。
- d) **[テンプレート プロパティ]** の横にある **[アクション]** メニューから、**[テンプレートの展開解除]** を選択し、テンプレートが正常に展開解除されるまで待ちます。

ステップ 3 サイトのインフラ構成を更新して、新しい Cisco Catalyst 8000V スイッチが NDO に追加されるようにします。

- a) **[構成 (Configure)]** に移動して **[サイト接続 (Site To Site Connectivity)]** を選択します。
- b) 画面右上の **[構成 (Configure)]** をクリックします。
- c) **[サイト (Sites)]** パネルでクラウドサイトを選択し、**[更新 (Refresh)]** をクリックします。
- d) 画面の右上にある **[展開]** をクリックし、すべてのサイトが正常に展開されるまで待ちます。

ステップ 4 このクラウドネットワーク コントローラ サイトに関連付けられているすべてのテンプレートを再展開します。

- a) **[アプリケーション (Applications)]** タブで **[構成 (Configure)]** > **[テナント テンプレート (Tenant Templates)]** に移動します。
- b) 以前に展開されていないテンプレートを使用してスキーマをクリックします。
- c) **[サイトに展開 (Deploy to Sites)]** をクリックし、テンプレートが展開されるまで待ちます。



第 8 章

ACI サイト向けのインフラ設定の展開

- [インフラ設定の展開 \(53 ページ\)](#)
- [オンプレミスとクラウド サイト間の接続の有効化 \(54 ページ\)](#)

インフラ設定の展開

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

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

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

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

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

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

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

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

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

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

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

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

次のタスク

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

オンプレミスとクラウドサイト間の接続の有効化

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

ここでは、オンプレミス APIC サイトと Cloud Network Controller 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 Network Controller 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 に対する IPsec トンネルです。複数のオンプレミス IPsec デバイスがある場合は、各オンプレミスデバイスの CSR に同じトンネルを設定する必要があります。

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

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

[インフラ設定の展開 \(53 ページ\)](#) の手順の一部として、Nexus Dashboard Orchestrator の **[IPN デバイス設定ファイルの展開とダウンロード (Deploy & Download IPN Device config files)]** オプションまたは **[IPN デバイス設定ファイルのダウンロード (IPN Device config files only)]** オプションを使用して、必要な設定の詳細を取得できます。

ステップ 2 オンプレミスの IPsec デバイスにログインします。

ステップ 3 最初の CSR のトンネルを設定します。

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

- `<first-csr-tunnel-id>` : このトンネルに割り当てる一意のトンネル ID です。
- `<first-csr-ip-address>` : 最初の CSR の 3 番目のネットワーク インターフェイスのパブリック IP アドレスです。
トンネルの宛先は、アンダーレイ接続のタイプによって異なります。
 - アンダーレイがパブリック インターネット経由の場合、トンネルの宛先はクラウド ルータ インターフェイスのパブリック IP です。
 - アンダーレイがプライベート接続 (AWS の DX や Azure の ER など) を介している場合、トンネルの宛先はクラウド ルータ インターフェイスのプライベート IP です。
- `<first-csr-preshared-key>` : 最初の CSR の事前共有キーです。
- `<onprem-device-interface>` 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>` : 最初のクラウド CSR に対してオンプレミスの IPsec デバイスのピア トンネル IP アドレスとして使用されます。
- `<process-id>` : OSPF プロセス ID です。
- `<area-id>` : OSPF エリア ID です。

次の例は、Nexus Dashboard Orchestrator リリース 3.3(1) および Cloud Network Controller 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 1449047253219022866513892194096727146110
    exit
exit

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

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

```

```

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

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

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

```

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

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

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

```

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

```




第 II 部

NDFC ファブリックの Day-0 オペレーション

- [サイトの追加と削除 \(61 ページ\)](#)
- [Cisco NDFC サイトのインフラの構成 \(67 ページ\)](#)



第 9 章

サイトの追加と削除

- [Cisco NDFC サイトの追加 \(61 ページ\)](#)
- [サイトの削除 \(63 ページ\)](#)
- [ファブリック コントローラへの相互起動 \(65 ページ\)](#)

Cisco NDFC サイトの追加

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

始める前に

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

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

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

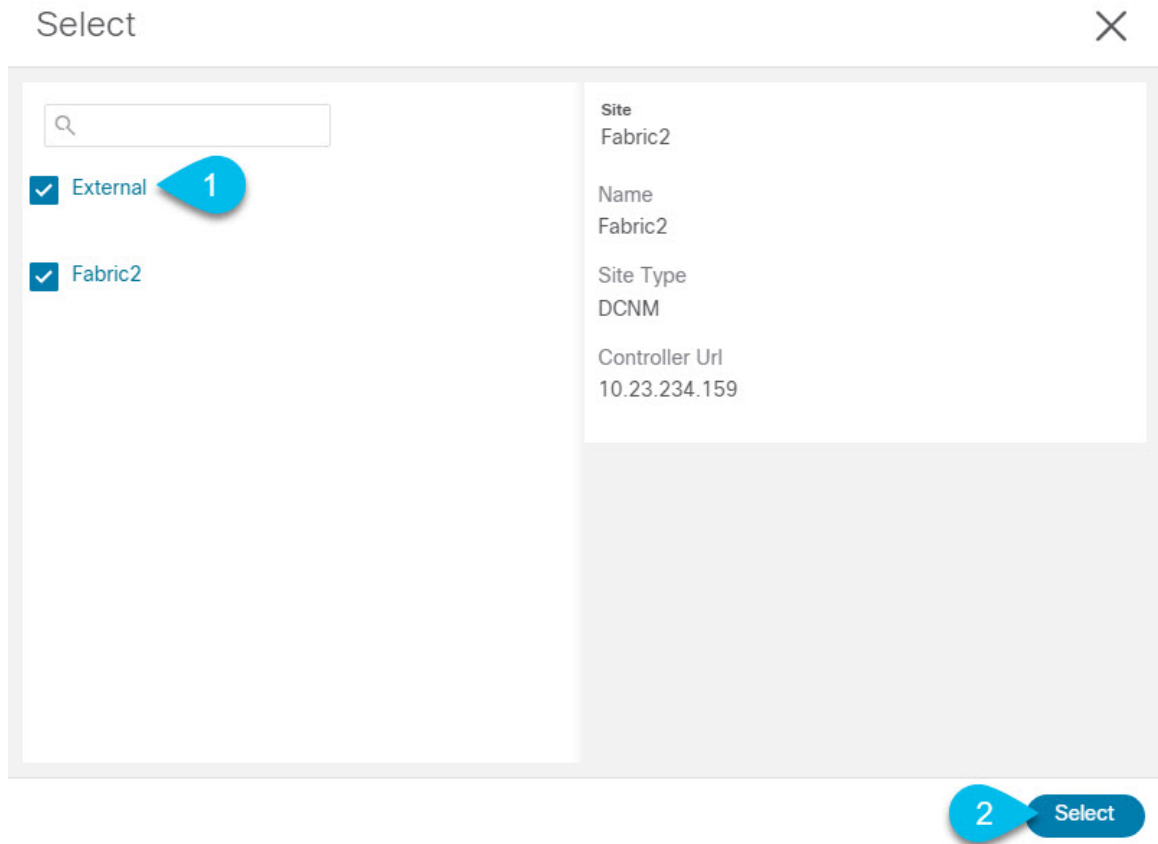
ステップ 3 サイト情報を入力します。

- a) [サイトのタイプ (Site Type)] で、NDFC または NDFC を選択します。
- b) NDFC コントローラの情報を入力します。

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

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

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



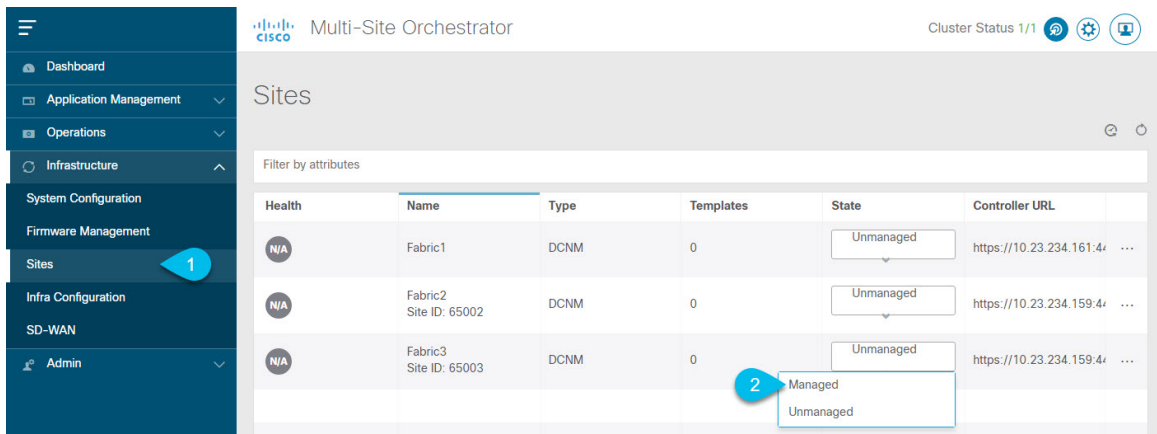
- d) **[セキュリティドメインの追加 (Add Security Domains)]** をクリックして、このサイトにアクセスできる 1 つ以上のセキュリティドメインを選択します。

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

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

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

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



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

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

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

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

サイトの削除

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

始める前に

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

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

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

ステップ 2 すべてのテンプレートからサイトを削除します。

サイトを管理解除して Nexus Dashboard から削除する前に、関連付けられているすべてのテンプレートからサイトを削除する必要があります。

- a) [アプリケーション管理 (Application Management)] > [スキーマ (Schemas)] の順に移動します。
- b) サイトに関連付けられた 1 つ以上のテンプレートを含むスキーマをクリックします。
- c) [表示] ドロップダウンから、削除するサイトに関連付けられているテンプレートを選択します。
- d) [アクション] ドロップダウンから、[サイトの関連付け] を選択し、削除するサイトのチェックを外します。

これにより、このテンプレートを使用してこのサイトに展開された構成が削除されます。

(注) ストレッチされていないテンプレートの場合、代わりに [アクション] > [サイトの関連付けを解除] を選択して、テンプレートによってサイトに展開された構成を保持することを選択できます。このオプションを使用すると、NDO によってデプロイされた構成を保持できますが、それらのオブジェクトを NDO から管理することはできなくなります。

- e) このスキーマおよび他のすべてのスキーマで管理解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について、この手順を繰り返します。

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

- a) 左のナビゲーションメニューから [サイト (Sites)] を選択します。
- b) メインペインで、非管理対象に設定したいサイトに対して [状態 (State)] を [非管理対象 (Unmanaged)] から [管理対象 (Managed)] に変更します。

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

ステップ 4 Nexus ダッシュボードからサイトを削除します。

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

(注) この時点で、このサイトは、Nexus Dashboard クラスタにインストールされているどのサービスでも使用されていないことに注意してください。

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

Nexus ダッシュボードからサイトが削除されます。

ファブリック コントローラへの相互起動

Cisco Nexus Dashboard Orchestrator は現在、ファブリックのタイプごとにいくつかの構成オプションをサポートしています。追加の多くの構成オプションでは、ファブリックのコントローラに直接サインインする必要があります。

NDO の[操作 (Operate)] > [サイト (Sites)]画面から特定のサイト コントローラの GUI にクロス起動するには、サイトの横にあるアクション (...) メニューを選択し、ユーザー インターフェイスで [開く (Open)] をクリックします。クロス起動は、ファブリックのアウトオブバンド (OOB) 管理IPで動作します。

Cisco Nexus Dashboard とファブリックで同じユーザーが構成されている場合、Cisco Nexus Dashboard ユーザーと同じサイン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、Cisco Nexus Dashboard とファブリック全体で共通のユーザーによるリモート認証を構成することを推奨します。



第 10 章

Cisco NDFC サイトのインフラの構成

- [前提条件とガイドライン \(67 ページ\)](#)
- [インフラの設定: 一般設定 \(67 ページ\)](#)
- [サイト接続性情報の更新 \(71 ページ\)](#)
- [インフラの構成: NDFC インフラ サイト固有の設定 \(71 ページ\)](#)
- [インフラ設定の展開 \(74 ページ\)](#)

前提条件とガイドライン

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

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

さらに、次の点に注意してください。

- 境界ゲートウェイスイッチの追加や削除には、一般的なインフラの設定手順の一部として、[サイト接続性情報の更新 \(71 ページ\)](#)に記載されている、Nexus Dashboard Orchestrator のファブリック接続情報の更新が必要です。

インフラの設定: 一般設定

このセクションでは、Cisco Nexus Dashboard Orchestrator によって搭載および管理される NDFC サイトの一般的な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 にログインし、Cisco Nexus Dashboard Orchestrator サービスを開きます。

ステップ 2 左のナビゲーションメニューから、**[構成 (Configure)] > [サイト間接続 (Site To Site Connectivity)]** を選択します。

ステップ 3 メインペインで、**[構成 (Configure)]** ボタンを選択します。

ステップ 4 左側の **[全般設定 (General Settings)]** タブを選択します。

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

- a) [コントロールプレーン設定 (Control Plane Configuration)] タブを選択します。
- b) [BGP ピアリングタイプ (Bgp Peering Type)] を選択します。
 - `full-mesh` : 各サイトのすべてのボーダー ゲートウェイ スイッチは、リモートサイトのボーダー ゲートウェイ スイッチとのピア接続を確立します。
 - `route-server` : `route-server` オプションを使用すると、各サイトが MP-BGP EVPN セッションを確立する 1 つ以上のコントロールプレーン ノードを指定できます。ルートサーバノードは、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、外部ボーダーゲートウェイプロトコル (および内部ボーダーゲートウェイプロトコル) セッションでは使用しません。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 サーバーを追加 (+Add Route Server)] をクリックして、1 台以上のルート サーバーを追加します。

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

- [サイト (Site)] ドロップダウンから、ルート サーバ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 サーバーは最大 4 台まで追加できます。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 EVPN 隣接関係を確立します。

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

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

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

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

- a) [オンプレミス IPsec デバイス (On Premises IPsec Devices)] タブを選択します。
- b) [+オンプレミス IPsec デバイスを追加 (+Add On-Premises IPsec Device)] をクリックします。

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

これは、デバイスが NDFC によって直接管理されるかどうかを定義します。

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

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

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

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

- d) チェックマークアイコンをクリックして、デバイス情報を保存します。

- e) 追加する IPN デバイスについて、この手順を繰り返します。

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

ここで指定できるサブネットプールには、次の 2 つのタイプがあります。

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

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

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

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

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

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

(注) 両方のサブネットプールの最小マスク長は /24 です。

1 つ以上の外部サブネットプールを追加するには :

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

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

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

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

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

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

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

- c) サブネットの [名前 (Name)] を入力します。
後ほど、サブネットプールの名前を使用して、IP アドレスを割り当てるプールを選択できます。
- d) [+IP アドレスの追加 (+Add IP Address)] をクリックして、1 つ以上のサブネットプールを追加します。
サブネットには /16 と /24 の間のネットワークが必要で、0.x.x.x または 0.0.x.x で始めることはできません。たとえば、30.29.0.0/16 のようにします。
- e) チェックマーク アイコンをクリックして、サブネット情報を保存します。
同じ名前付きサブネット プールに複数のサブネットを追加する場合は、この手順を繰り返します。
- f) [保存 (Save)] をクリックして、名前付きサブネットプールを保存します。
- g) 追加する名前付きサブネット プールについて、これらのサブステップを繰り返します。

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

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

このフィールドは、各ファブリックの [マルチサイト TEP (Multi-Site TEP)] フィールドに自動入力するために使用されます。 [インフラの構成: NDFC インフラ サイト固有の設定 \(71 ページ\)](#) で説明します。

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

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

サイト接続性情報の更新

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

- ステップ 1** Cisco Nexus Dashboard Orchestrator の GUI にログインします。
- ステップ 2** 左のナビゲーションメニューから、**[構成 (Configure)]** > **[サイト間接続 (Site To Site Connectivity)]** を選択します。
- ステップ 3** メインペインの右上にある **[構成 (Configure)]** をクリックします。
- ステップ 4** 左側のペインの **[サイト (Sites)]** の下で、特定のサイトを選択します。
- ステップ 5** メイン ウィンドウで、APIC からファブリック情報を取得するために **[更新 (Refresh)]** ボタンをクリックします。
- ステップ 6** (任意) 使用停止されたボーダーゲートウェイスイッチの構成を削除する場合は、**[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構成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、新しいまたは削除されたボーダーゲートウェイを検出し、すべてのサイトに関連するファブリック接続がサイトのコントローラから再インポートされます。

インフラの構成: NDFC インフラ サイト固有の設定

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

- ステップ 1** Cisco Nexus Dashboard にログインし、Cisco Nexus Dashboard Orchestrator サービスを開きます。
- ステップ 2** 左のナビゲーションメニューから、**[構成 (Configure)]** > **[サイト間接続 (Site To Site Connectivity)]** を選択します。
- ステップ 3** メインペインにある **[構成 (Configure)]** をクリックします。
- ステップ 4** 左側のペインの **[サイト (Sites)]** の下で、特定の NDFC を選択します。
- ステップ 5** 右側の **<Site>[設定 (Settings)]** サイドバーで、**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展開されません。

(注) 設定するサイトが NDFC マルチサイトドメイン (MSD) の一部である場合、このフィールドには NDFC からインポートされた情報が事前に入力されます。この場合、値を変更して構成を再展開すると、MSD 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。

また、共有ボーダー構成を展開することもできます。この構成により、これらのデバイスを介してこれらのサービスを共有できると同時に、内部サイトからインターネットに「ボーダー」を越える手段も提供されます。詳細については、『[Cisco Nexus Dashboard Fabric Controller における共有ボーダーの構成](#)』を参照してください。

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

(注) このリリースでは、NDFC からのポート設定のインポートはサポートされていません。すでに NDFC マルチサイトドメイン (MSD) の一部であるサイトを構成する場合、NDFC で構成されているのと同じ値を使用する必要があります。

[**BGP 認証と BFD の継承 (Inherit BGP Authentication and BFD)**] オプション ボタンを使用して、サイトとファブリック間で設定を継承できます。

Add Port

Description

Remote Address *

Remote ASN *

MTU *

Inherit BGP Authentication and BFD ⓘ

BGP Authentication
 None Simple Cisco

Towards Cloud Router ⓘ

BFD Enabled

Log Neighbor

BGP Send Community

Route Tag

Enable Redistribute Direct

RS Route Tag

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

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

- **[リモートアドレス (Remote Address)]** フィールドに、ポートが接続されているリモートデバイスの IP アドレスを入力します。
- **[リモート ASN (Remote ASN)]** フィールドに、リモートサイトの **[自律システム番号 (Autonomous System Number)]** を提供します。
- **[MTU]** フィールドに、ポートの最大伝送単位を入力します。
スパイン ポートの最大伝送単位は、IPN 側の MTU と一致する必要があります。
[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 (MD5) (Simple (MD5))] または Cisco を選択できます。
[シンプル (Simple)] または [Cisco] 認証方式を選択した場合は、**認証キー**を入力します。
- **[BFD 対応 (BFD Enabled)]**、**[ログネイバー (Log Neighbor)]**、および **[BGP 送信コミュニティ (BGP Send Community)]** オプションボタンをオンにして、これらすべての機能をすべてのマルチサイトアンダーレイ インターフェイスに継承します。
- **ルートタグ**は、すべてのスイッチ間のデータパスを構成するために使用され、ファブリック内のすべてのノードに伝播されます。ループバック 0、1、および 100。ルートタグが指定されている場合は、**[直接再配布の有効化 (Enable Redistribute Direct)]** を選択します。

インフラ設定の展開

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

始める前に

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

ステップ 1 設定の競合がないことを確認するか、必要に応じて解決します。

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

以下に構成の競合があります。

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



- b) 競合の原因となっている特定の設定を書き留めます。

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

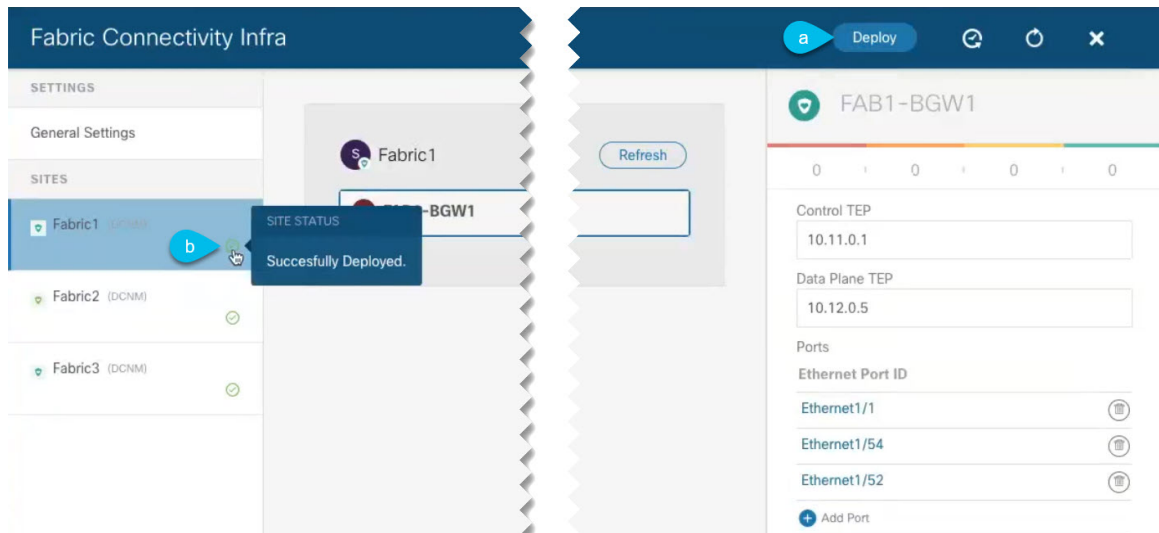
Error Type	Error Message
IDMismatch	Policy Name MyVRF_50001 Policy ID 50001 Sites [fab2] conflicting with Policy Name MyVRF_50001 Policy ID 60001 Sites [fab1]
IDMismatch	Policy Name MyNetwork_30000 Policy ID 40000 Sites [fab2] conflicting with Policy Name MyNetwork_30000 Policy ID 30000 Sites [fab1]

- 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 \(63 ページ\)](#) の説明に従って、NDO でサイトの管理を解除します。

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

- e) 既存の設定の競合を解決します。
 f) [Cisco NDFC サイトの追加 \(61 ページ\)](#) の説明に従って、サイトを再度管理状態にします。
 サイトはすでに CiscoNexus ダッシュボードに追加されているため、NDO で管理できるようにします。
 g) すべての競合が解決され、**[展開 (Deploy)]** ボタンが使用可能であることを確認します。

ステップ 2 設定を展開します。



- a) **[ファブリック接続インフラ (Fabric Connectivity Infra)]** 画面の右上で、適切な **[展開 (Deploy)]** オプションを選択して設定を展開します。
 NDFC サイトのみを設定する場合は、**[展開 (Deploy)]** をクリックしてインフラ設定を展開します。
 b) 設定が展開されるのを待ちます。

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

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



第 III 部

Nexus Dashboard Orchestrator の更新

- [サービス カタログを介した自動アップグレード \(79 ページ\)](#)
- [構成の復元を使用した手動アップグレード \(101 ページ\)](#)



第 11 章

サービス カタログを介した自動アップグレード

- [概要 \(79 ページ\)](#)
- [前提条件とガイドライン \(82 ページ\)](#)
- [Nexus Dashboard Clusterのアップグレード \(85 ページ\)](#)
- [Cisco App Store を使用した Orchestrator Service のアップグレード \(90 ページ\)](#)
- [Orchestrator サービスの手動アップグレード \(93 ページ\)](#)
- [データベースのアップグレードのファイナライズ \(95 ページ\)](#)
- [設定のばらつきの解決 \(97 ページ\)](#)

概要

Nexus Dashboard Orchestrator のアップグレードに関しては、2つのアプローチがあります。

- 各コンポーネント (Nexus Dashboard プラットフォームや Orchestrator サービスなど) を順番にアップグレードすることによるインプレース アップグレード。

このアプローチは、この章で説明されており、次の場合に推奨されます。

- 物理的な Nexus Dashboard クラスタを使用している場合。
- Nexus Dashboard (2.2.2以降) および Nexus Dashboard Orchestrator (3.7.1以降) の最近のリリースを実行している場合。

このアプローチを使用して Orchestrator リリース 3.3(1) 以降をアップグレードできませんが、Orchestrator サービスをアップグレードする前に、基礎となる Nexus Dashboard プラットフォームをアップグレードする必要がある場合があります。このような場合、以下で説明する構成の復元によるアップグレードの方が、より高速で簡単な場合があります。

- 新しい Nexus Dashboard クラスタを展開し、新しい NDO サービス インスタンスをインストールして、構成復元ワークフローで既存の Orchestrator 構成を転送します。

このアプローチは、[構成の復元を使用した手動アップグレード \(101 ページ\)](#) で説明されており、次の場合に推奨されます。

- リリース 3.3(1) より前の Nexus Dashboard Orchestrator またはマルチサイト Orchestrator のいずれかのリリースを実行している場合。

この場合、インプレースアップグレードはサポートされていないため、構成の復元を使用してアップグレードする必要があります。

- 仮想 Nexus Dashboard クラスタを使用していて、Nexus Dashboard Orchestrator の古いリリースを実行している場合。

古い Nexus Dashboard Orchestrator リリースからアップグレードするには、基盤となる Nexus Dashboard プラットフォームもアップグレードする必要があります。その場合、新しいクラスタを展開して構成を復元すると、必要なメンテナンスウィンドウが短縮される可能性があります。

これにより、以前のバージョンに戻したい場合やアップグレードが失敗した場合に備えて、既存のクラスタを切断して、アップグレードが完了するまで既存の VM を保持することもできます。

リリース 4.0(1) 以降における変更

リリース 4.0(1) 以降、Nexus Dashboard Orchestrator は、テンプレートの設計と展開に関して、いくつかのベスト プラクティスを検証して適用します。

- すべてのポリシー オブジェクトは、依存関係に応じた順序で**[展開 (deployed)]**する必要があります。

たとえば、ブリッジドメイン (BD) を作成するときは、それを VRF に関連付ける必要があります。この場合、BD には VRF 依存関係があるため、VRF は BD の前または一緒にファブリックに展開する必要があります。これらの2つのオブジェクトが同じテンプレートで定義されている場合、Orchestrator は展開時に VRF が最初に作成され、ブリッジドメインに関連付けられるようにします。

ただし、これら2つのオブジェクトを別々のテンプレートで定義し、最初に BD を使用してテンプレートを展開しようとする、関連付けられている VRF がまだ展開されていないため、Orchestrator は検証エラーを返します。この場合、最初に VRF テンプレートを展開してから、BD テンプレートを展開する必要があります。

- すべてのポリシー オブジェクトは、依存関係に応じた順序で**[展開解除 (undeployed)]**する必要があります。つまり、展開された順序と逆の順序で展開する必要があります。

上記の結果から、テンプレートを展開解除するときは、他のオブジェクトが依存しているオブジェクトを展開解除してはなりません。たとえば、VRF が関連付けられている BD を展開解除する前に、VRF を展開解除することはできません。

- 複数のテンプレートにまたがる循環的な依存関係は許可されません。

ブリッジドメイン (bd1) に関連付けられた VRF (vrf1) の場合を考えてみます。これは、次に EPG (ep1) に関連付けられます。[テンプレート 1 (template1)] に vrf1 を作成してそ

のテンプレートをデプロイし、次に [テンプレート 2 (template2)] に bd1 を作成してそのテンプレートをデプロイすると、オブジェクトが正しい順序でデプロイされるため、検証エラーは発生しません。ただし、その後 [テンプレート1 (template1)] に epg1 を作成しようとすると、2つのテンプレート間に循環依存関係が作成されるため、Orchestrator は、EPG の [テンプレート1 (template1)] 追加を保存することを許可しません。

これらの追加のルールと要件により、以前のリリースからリリース 4.0(1) 以降にアップグレードするには、既存のすべてのテンプレートを分析し、新しい要件を満たさないテンプレートを変換する必要があります。これは、次のセクションで説明するアップグレードプロセス中に自動的に実行され、既存のテンプレートを新しいベストプラクティスに準拠させるために適用する必要があったすべての変更の詳細なレポートを受け取ります。



- (注) リリース 4.0(1) に移行する既存の構成をバックアップする前に、次の「前提事項と注意事項」セクションで説明されているすべての要件を満たしていることを確認する必要があります。そうしないと、1つ以上のテンプレートでテンプレートの変換が失敗し、手動で問題を解決するか、移行プロセスを再開する必要があります。

アップグレードのワークフロー

次のリストに、アップグレードプロセスの概要と実行する必要があるタスクの順序を示します。

1. アップグレードガイドラインの確認と充します。
2. 必要に応じて、既存の Nexus Dashboard Orchestrator サービスを無効にして、Nexus Dashboard クラスタをアップグレードします。

Nexus Dashboard リリースが 2.2(1) 以前の場合は、Nexus Dashboard プラットフォーム ソフトウェアもアップグレードする必要があるため、これは必須です。これには、アップグレード中にすべてのサービスを無効にする必要があります。

ただし、Nexus Dashboard クラスタが仮想の場合は、新しいクラスタを展開して、そこに Nexus Dashboard リリース 2.3(2b) 以降を Orchestrator リリース 4.1(2) をインストールすることを選択できます。新しいクラスタが稼働したら、古いクラスタの VM を切断し、新しいクラスタで移行プロセスを完了することができます。これにより、既存のクラスタを保持し、移行手順で問題が発生した場合に簡単にサービスを再開できます。これにより、アップグレードがバックアップリストアプローチを使用した手動アップグレードに効果的に変わります。この場合、代わりに [構成の復元を使用した手動アップグレード \(101 ページ\)](#) で説明されている手順に従うことをお勧めします。

3. 既存の Orchestrator サービスを再度有効にしてから、Nexus Dashboard Orchestrator リリース 4.1(2) 以降をアップロードしてアクティブ化します。

アップグレードする目的で、新しい ND で古いバージョンの Orchestrator を再度有効にすることがサポートされていることを明確にするために、ここにメモを追加することができます。



- (注) より新しい Nexus Dashboard で古いバージョンの NDO を実行することは、NDO のアップグレード目的でのみ限定的にサポートされています。このマニュアルの説明に従って、NDO リリース 4.1(2) 以降にアップグレードする必要があります。

4. アップグレードを完了し、構成のばらつきを解決します。

前提条件とガイドライン

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

- Nexus Dashboard Orchestrator リリース 3.3(1) 以降を実行していることを確認します。



- (注) リリース 3.3(1), より前のリリースを実行している場合は、この章をスキップして、代わりに [構成の復元を使用した手動アップグレード \(101 ページ\)](#) で説明されている手順に従ってください。

- このリリースからのダウングレードはサポートされていないのでご注意ください。

ダウングレードする場合は、以前のバージョンを使用して新しいクラスタを展開し、以前のリリースから構成を復元できます。新しいバージョンで作成されたバックアップを古いバージョンで復元することはできないことに注意してください。つまり、リリース 3.7(1) でのリリース 4.1(2) からのバックアップの復元はサポートされていません。

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

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

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

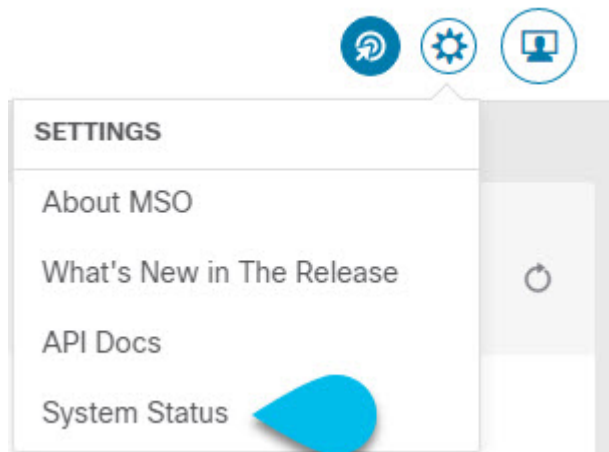
```
# acs health
All components are healthy
```

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

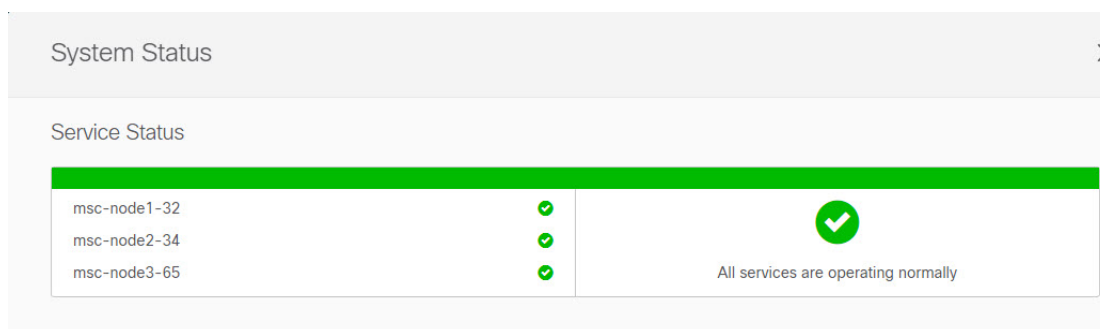
既存の Orchestrator のバージョンに応じて、次の2つの方法のいずれかでサービスのステータスを確認できます。

- 最近の NDO リリースについては、プラットフォームとサービスの正常性を示す Nexus ダッシュボードの [概要 (Overview)] ページを確認してください。

- 旧版の Orchestrator リリースの場合、Nexus Dashboard Orchestrator サービスのステータスは、[設定 (Settings)] > [システム ステータス (System Status)] に移動して確認できます。



次に、すべてのノードとサービスのステータスが正常であることを確認します。



- 既存の構成をバックアップする前に、構成のばらつきがないことを確認してください。
これは、アプリケーション、テナント ポリシー、ファブリック ポリシー、ファブリック リソース ポリシー テンプレートなど、既存のリリースで使用可能なすべてのテンプレート タイプに適用されます。
既存の Nexus Dashboard Orchestrator がリリース 3.7(1) 以降である場合、『[Nexus Dashboard Orchestrator 構成ガイド](#)』の「構成のばらつき」セクションに記載されているアプリケーション テンプレートのばらつきの調整ワークフローを使用できます。
- バックアップして、既存の Orchestrator 構成をダウンロードします。
構成のバックアップについては、お使いのリリースの [Nexus Dashboard Orchestrator 構成ガイド](#) の「バックアップと復元」の章で説明されています。
- バックアップして、既存のファブリックの構成をダウンロードします。
Nexus Dashboard Orchestrator をアップグレードした後、構成のばらつきの調整を実行することをお勧めします。これには、構成をファブリックに再展開する必要がある場合があります。

ます。そのため、Nexus Dashboard Orchestrator によって管理されるすべてのファブリックの構成バックアップを作成することをお勧めします。

Cisco APIC 構成バックアップの作成の詳細については、使用しているリリースの [Cisco APIC Basic Configuration Guide](#) の「Management」の章を参照してください。

Cisco Cloud Network Controller 構成バックアップの作成の詳細については、ご使用のリリースの [Cisco Cloud Network Controller User Guide](#) の「Configuring Cisco Cloud Network Controller Components」の章を参照してください。

Cisco Nexus ダッシュボードファブリックコントローラコンフィギュレーションバックアップの作成の詳細については、使用しているリリースの `format="html" href="https://www.cisco.com/en/US/products_systems_management/products_data_centers_network_products/installation_and_configuration_guides/html/scope="external">`[Cisco NDFC](#) ファブリックコントローラ構成ガイドの「バックアップと復元」の章を参照してください。

- テンプレートのバージョン管理を有効にしている場合（リリース 3.4(1)以降サポートされている）、アップグレード中にテンプレートの最新バージョンのみが保持されることに注意してください。

[ゴールデン (Golden)] のタグが付けられた古いバージョンを含む、テンプレートの他のすべての既存バージョンは転送されません。

- 既存のクラスターの構成バックアップを作成する前に、すべてのテンプレートがサポートされている状態であることを確認します。
 - **[展開解除 (Undeployed)]** されたテンプレート、または作成後に **[未展開 (Never Deployed)]** テンプレートは、特に注意する必要はなく、アップグレード中に移行されます。
 - **[展開された (Deployed)]** すべてのテンプレートには、保留中の構成変更が含まれていてはなりません。

前回の展開以降に変更されたテンプレートが1つ以上ある場合は、テンプレートの最新バージョンを展開するか、最後に展開されたバージョンに戻して再展開することにより、展開以降のテンプレートへの変更を元に戻す必要があります。

- Orchestrator サービスをアップグレードするときは、次の2つの方法のいずれかで実行できます。
 - [Cisco App Store](#) を使用した [Orchestrator Service](#) のアップグレード (90 ページ) の説明に従って、Nexus ダッシュボードの App Store を使用します。

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



(注) App Storeでは、サービスの最新バージョンにのみアップグレードできます。別のリリースにアップグレードしたい場合は、以下に説明したとおり、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。

- **Orchestrator サービスの手動アップグレード (93 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。

このアプローチは、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サービスのバージョンにアップグレードする場合に使用できません。

- SR-MPLS および SDA 統合構成は、アップグレード中に転送されません。

展開にこれらの統合のいずれかが含まれている場合、移行には影響しませんが、通知を受け取り、アップグレードの完了後にそれらを再構成する必要があります。

- Nexus Dashboard Orchestrator をこのリリースにアップグレードした後に新しい Cloud Network Controller 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 Network Controller 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 Network Controller サイトのオンボーディングと管理はサポートされていません。

Nexus Dashboard Clusterのアップグレード

Nexus Dashboard Orchestrator のリリース 4.1(2) にアップグレードする前に、このセクションの説明に従って、Nexus Dashboard クラスタをリリース 2.2.2 以降にアップグレードする必要があります。



(注) Nexus ダッシュボードクラスタがすでにリリース 2.2.2 以降である場合は、このセクションをスキップすることを選択できます。ただし、Nexus Dashboard リリース 2.3.2 にアップグレードすることをお勧めします。

始める前に

次の前提条件があります。

- 既存の Nexus Dashboard Orchestrator 構成をバックアップおよびダウンロードしました。

Nexus Dashboard Clusterをアップグレードする前。

- 既存の Nexus Dashboard リリースを確認します。

少なくとも、Nexus Dashboard リリース 2.2.2 にアップグレードする必要があります。Nexus Dashboard リリース 2.2.2 以降をすでに実行している場合は、このセクションをスキップできます。

以前のリリースからアップグレードする必要がある場合は、リリース 2.3.2 にアップグレードすることをお勧めします。



(注) Nexus Dashboard は、特定のリリースセット間の直接アップグレードのみをサポートします。

- リリース 2.1.2 以降の場合は、リリース 2.3.2 に直接アップグレードできます。
- リリース 2.1.2 以前のリリースを使用している場合は、最初にリリース 2.2.2 にアップグレードしてから、リリース 2.3.2 にアップグレードする必要があります。

- アップグレードに影響を与える可能性のある動作、ガイドライン、および問題の変更点については、すべてのアップグレードホップのターゲットリリースの [リリースノート](#) を必ずお読みください。

アップグレードプロセスは、すべての Nexus ダッシュボードフォームファクタで同じです。物理サーバ、VMware ESX Linux KVM、または Azure または AWS を使用してクラスタを展開したかどうかに関係なく、ターゲットリリースの ISO イメージを使用してアップグレードします。

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

Nexus ダッシュボード GUI の **[システム概要 (System Overview)]** ページでシステムの状態を確認するか、`rescue-user` としてノードの1つにログインし、`acs health` コマンドを実行して `All components are healthy` が返ってくることを確認します。

- アップグレードの前に、既存の Nexus Dashboard クラスタ構成のバックアップを作成することをお勧めします。
- アップグレードが進行中にワーカーまたはスタンバイノードを追加するなど、設定変更がクラスタに対して行われていないことを確認します。
- Nexus Dashboard をリリース 2.1(1) 以前からアップグレードする場合は、UI を適切に表示するには、アップグレードの完了後にブラウザのキャッシュをクリアする必要がある場合があります。

ステップ 1 Nexus ダッシュボードイメージをダウンロードします。

上記の「始める前に」セクションで説明したように、複数のホップにまたがってアップグレードする必要がある場合は、すべてのターゲットホップのイメージをダウンロードします。

- a) [ソフトウェア ダウンロード (Software Download)] ページを参照します。

<https://software.cisco.com/download/home/286327743/type/286328258>

- b) ダウンロードするNexusダッシュボードのバージョンを選択します。
c) Cisco Nexus ダッシュボード イメージ (nd-dk9.<version>.iso) 。

(注) 最初のクラスタ展開にVMware ESX.ova イメージまたはクラウドプロバイダーのマーケットプレイスを使用した場合でも、すべてのアップグレードで .iso イメージをダウンロードする必要があります。

- d) (オプション) 環境内のWebサーバでイメージをホストします。

イメージをNexusダッシュボードクラスタにアップロードする場合、イメージに直接URLを指定するオプションがあります。

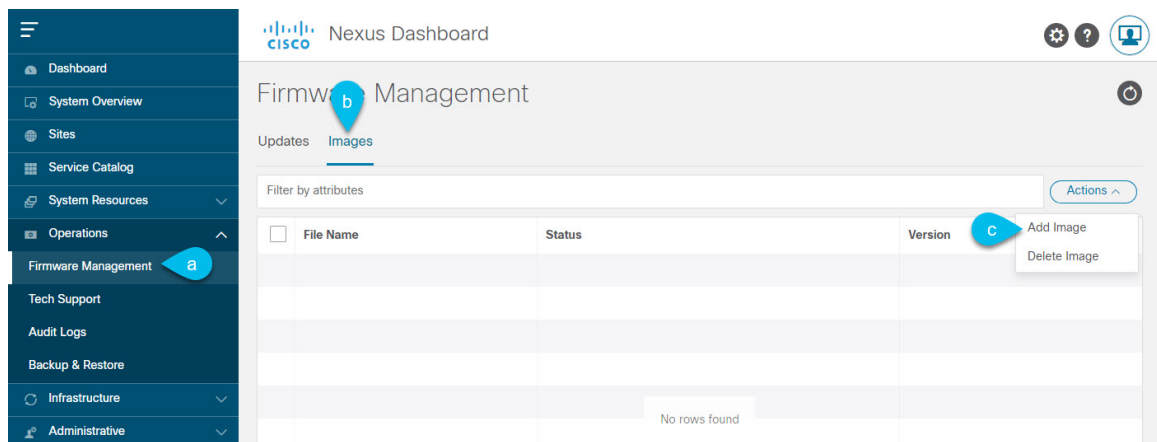
ステップ 2 現在の Nexus ダッシュボード GUI に管理者ユーザとしてログインします。

ステップ 3 クラスタ内のインストールしたすべてのサービスを無効にします。

Nexus Dashboard をアップグレードするときは、現在インストールされているすべてのサービス (Nexus Dashboard Orchestrator または Nexus Dashboard Insights など) を無効にする必要があります。

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

(注) Nexus Dashboard のリリースによって UI が若干異なる場合がありますが、ナビゲーションは同じです。



- a) [Operations (オペレーション)] > [ファームウェア管理 (Firmware Management)] に移動します。
b) [イメージ] タブを選択します。
c) [アクション (Actions)] メニューから、[イメージの追加 (Add Image)] をクリックします。

ステップ 5 新しいイメージを選択します。

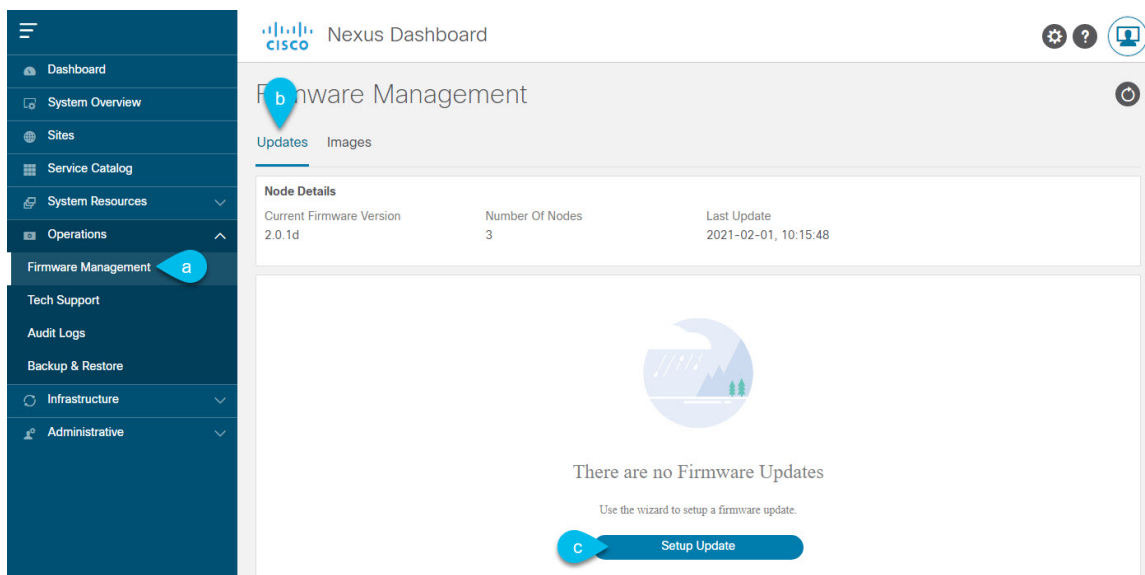
(注) 複数のホップでアップグレードする必要がある場合は、アップグレード先の即時リリース用に一度に1つのイメージのみをアップロードする必要があります。次に、そのホップへのアップグレードが完了したら、次のホップのイメージを使用してプロセスを繰り返すことができます。

- a) **[ファームウェア イメージの追加 (Add Firmware Image)]** ウィンドウで、**[ローカル (Local)]** を選択します。
 または、ウェブサーバでイメージをホストした場合は、代わりに**[リモート (Remote)]** を選択します。
- b) **[ファイルの選択 (Select file)]** をクリックし、最初の手順でダウンロードした ISO イメージを選択します。
 リモートイメージのアップロードを選択した場合は、リモートサーバ上のイメージのファイルパスを指定します。
- c) **[アップロード (Upload)]** をクリックして、イメージを追加します。
 イメージがNexusダッシュボードクラスタにアップロードされ、解凍されて処理され、アップグレードに使用できるようになります。プロセス全体に数分かかる場合があります、**[イメージ (Images)]** タブでプロセスのステータスを確認できます。

ステップ 6 イメージステータスが「ダウンロード済み」に変わるのを待ちます。

イメージでイメージのダウンロードの進行状況を確認できます。

ステップ 7 更新を設定します。



- a) **[Operations (オペレーション)]** > **[ファームウェア管理 (Firmware Management)]** に移動します。
- b) **[更新]** タブを選択します。
- c) **[更新のセットアップ (Setup Update)]** をクリックします。
[ファームウェアの更新 (Update Firmware)] ダイアログボックスが開きます。

ステップ 8 アップグレードイメージを選択します。

- a) **[ファームウェアの更新 (Firmware Update)]** > **[バージョン選択 (Version selection)]** 画面で、アップロードしたファームウェアバージョンを選択し、**[次へ (Next)]** をクリックします。

- b) [ファームウェアの更新 (Firmware Update)] > [確認 (Confirmation)] 画面で、詳細を確認し、[インストールの開始 (Begin Install)] をクリックします。

インストールの進行状況ウィンドウが表示されます。更新中は、この画面から移動できます。後で更新ステータスを確認するには、[ファームウェア管理 (Firmware Management)] 画面に移動し、[最終更新ステータス (Last Update Status)] タイルで [詳細の表示 (View Details)] をクリックします。

これにより、必要な Kubernetes イメージとサービスが設定されますが、クラスタは新しいバージョンに切り替わりません。次の手順で新しいイメージをアクティブ化するまで、クラスタは既存のバージョンを実行し続けます。このプロセスは、全体で最大 20 分かかる場合があります。

ステップ 9 新しい画像をアクティブにします。

- a) [オペレーション (Operations)] > [ファームウェア管理 (Firmware Management)] 画面に戻ります。
b) [最終更新ステータス (Last Update Status)] タイルで、[詳細の表示 (View Details)] をクリックします。
c) [Activate] をクリックします。
d) [アクティブ化確認] ウィンドウで、[続行] をクリックします。

すべてのクラスタサービスが起動し、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 10 VMware ESX に展開された仮想クラスタをアップグレードした場合は、ノードを新しいプロファイルに変換します。

(注) クラスタが VMware ESX に展開されていない場合、または既にリリース 2.1.1 以降にある場合は、この手順をスキップしてください。

リリース 2.1.1 以降、Nexus ダッシュボードは、VMware ESX に展開された仮想ノードに対して 2 つの異なるノードプロファイルをサポートします。アップグレード後、既存のクラスタのすべてのノードを新しいプロファイルの 1 つに変換する必要があります。

- **データ ノード** : Nexus ダッシュボード Insights などのデータ集約型アプリケーション向けに設計されたノードプロファイル
- **アプリ ノード** : Nexus ダッシュボード Insights などのデータ集約型アプリケーション向けに設計されたノードプロファイル

選択するプロファイルは、使用例のシナリオによって異なります。

- Nexus ダッシュボード オーケストレータ サービスのみを実行する予定の場合は、すべてのノードをアプリ ノードプロファイルに変換します。
- Nexus ダッシュボード Insights または共同ホストアプリケーションを実行する予定の場合は、ノードをデータ プロファイルに変換する必要があります。

ノードを新しいプロファイルに変換するには、そのプロファイルを使用して新しいノードを展開し、既存のノードを一度に 1 つずつ置き換えます。

- a) ノードの 1 つを停止します。

一度に 1 つのノードを置き換える必要があります。

- b) アプリまたはデータ プロファイル OVA を使用して、VMware ESX に新しいノードを展開します。
新しいノードを展開するときは、置き換えるノードとまったく同じネットワーク設定パラメータを使用する必要があります。
- c) 既存の Nexus ダッシュボード GUI にログインします。
残りの正常なマスター ノードのいずれかの管理 IP アドレスを使用できます。
- d) 左側のナビゲーション ペインから、[システム リソース (System Resources)] > [ノード (Nodes)] を選択します。
交換するノードが [非アクティブ (Inactive)] としてリスト化されます。
- e) 置換する非アクティブ マスター ノードの隣にある(...) メニューをクリックして、[置換 (Replace)] を選択します。
[置換 (Replace)] ウィンドウが開きます。
- f) ノードの管理 IP アドレスとパスワードを入力し、[確認 (Verify)] をクリックします。
クラスタは新しいノードの管理 IP アドレスに接続し、接続性を確認します。
- g) [置換 (Replace)] をクリックします。
ノードが設定されてクラスタに参加するまでに、最大で 20 分かかる場合があります。
- h) クラスタが正常になるのを待ってから、他の 2 つのノードに対してこの手順を繰り返します。

ステップ 11 アップグレードが成功したら、アップロードしたアップグレードイメージを削除します。

次のアップグレードのために新しいイメージをアップロードする前に、古いアップグレードイメージを削除する必要があります。

ステップ 12 複数のホップにわたってアップグレードする場合は、アップグレードごとにこれらの手順を一度に 1 つずつ繰り返します。

Cisco App Store を使用した Orchestrator Service のアップグレード

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

始める前に

- [前提条件とガイドライン \(82 ページ\)](#) 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 (Services)]** を選択します。

ステップ 3 Nexus Dashboard Orchestrator の既存のバージョンを再度有効にします。

前のセクションで説明したように、Nexus Dashboard プラットフォームをアップグレードするために NDO サービスを無効にする必要があった場合は、NDO リリース 4.1(2) 以降にアップグレードする前に再度有効にする必要があります。

(注) より新しい Nexus Dashboard で古いバージョンの NDO を実行することは、NDO のアップグレード目的でのみ限定的にサポートされています。このセクションの説明に従って、NDO リリース 4.1(2) 以降にアップグレードする必要があります。

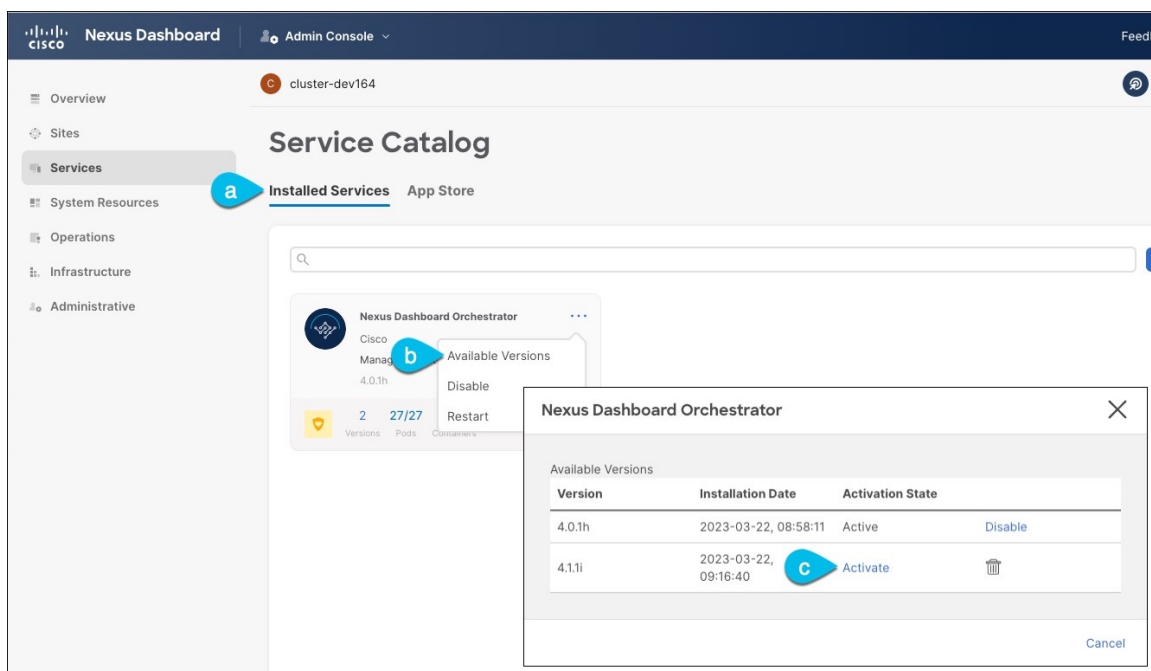
ステップ 4 App Store を使用してアプリケーションをアップグレードします。

- a) **[サービス (Services)]** 画面で、**[App Store]** タブを選択します。
- b) **[Nexus ダッシュボード オーケストレータ (Nexus Dashboard Orchestrator)]** タイルで、**[アップグレード (Upgrade)]** をクリックします。
- c) 開いた **[ライセンス契約 (License Agreement)]** ウィンドウで、**[同意してダウンロード (Agree and Download)]** をクリックします。

ステップ 5 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 6 新しい画像をアクティブにします。



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

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

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

ステップ7 古いサービス イメージを削除します。

サービスのダウングレードはサポートされていないため、アップグレード後に Nexus Dashboard から古いイメージを削除することをお勧めします。

- [サービス (Services)] ページで、[インストール済みサービス (Installed Services)] タブを選択します。
- [Nexus Dashboard Orchestrator] タイルの右上にあるメニュー (...) をクリックし、[利用可能なバージョン (Available Versions)] を選択します。
- 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。

次のタスク

NDO サービスをアップグレードした後、[データベースのアップグレードのファイナライズ \(95 ページ\)](#) で説明されているように、NDO UI からアップグレードを完了する必要があります。

Orchestrator サービスの手動アップグレード

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

始める前に

- [前提条件とガイドライン \(82 ページ\)](#) で説明している前提条件をすべて満たしていることを確認します。

ステップ 1 ターゲットの NDO リリース イメージをダウンロードします。

- a) DC App Center で Nexus Dashboard Orchestrator ページを参照します。
<https://dcappcenter.cisco.com/nexus-dashboard-orchestrator.html>
- b) [バージョン (Version)] ドロップダウンから、インストールするバージョンを選択し、[ダウンロード (Download)] をクリックします。
- c) [同意してダウンロードする (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 Nexus Dashboard にログインします。

ステップ 3 Nexus Dashboard Orchestrator の既存のバージョンを再度有効にします。

前のセクションで説明したように、Nexus Dashboard プラットフォームをアップグレードするために NDO サービスを無効にする必要があった場合は、NDO リリース 4.1(2) 以降にアップグレードする前に再度有効にする必要があります。

- (注) より新しい Nexus Dashboard で古いバージョンの NDO を実行することは、NDO のアップグレード目的でのみ限定的にサポートされています。このセクションの説明に従って、NDO リリース 4.1(2) 以降にアップグレードする必要があります。

ステップ 4 Nexus Dashboard に NDO 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 (Services)] を選択します。
- b) Nexus Dashboard の [サービス (Services)] 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、イメージファイルのフル URL を指定します。たとえば、`http://<ip-address>:<port>/<full-path>/cisco-mso-<version>.nap` のようになります。

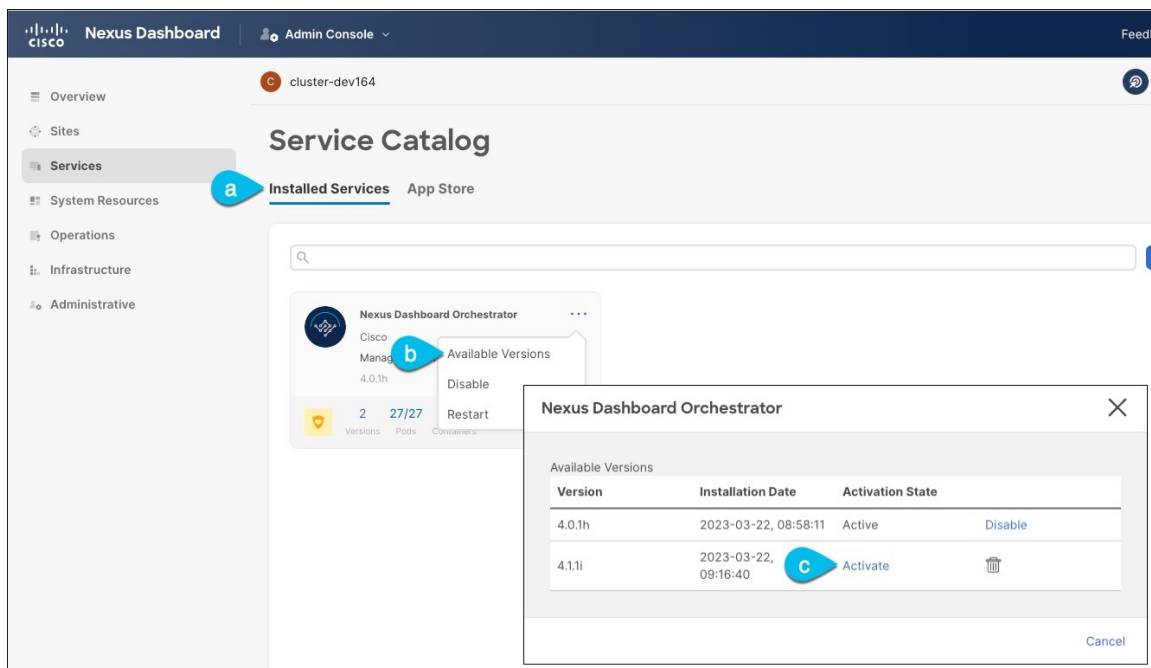
- f) [アップロード (Upload)] をクリックして、アプリケーションをクラスタに追加します。

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

ステップ 5 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 6 新しい画像をアクティブにします。



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

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

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

ステップ7 古いサービス イメージを削除します。

サービスのダウングレードはサポートされていないため、アップグレード後に Nexus Dashboard から古いイメージを削除することをお勧めします。

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

次のタスク

NDO サービスをアップグレードした後、[データベースのアップグレードのファイナライズ \(95 ページ\)](#) で説明されているように、NDO UI からアップグレードを完了する必要があります。

データベースのアップグレードのファイナライズ

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

始める前に

次の前提条件があります。

- 既存の Nexus Dashboard Orchestrator 構成をバックアップおよびダウンロードしました。
- [Nexus Dashboard の展開と Nexus Dashboard Orchestrator のインストール \(106 ページ\)](#) の説明に従って、対象の Orchestrator リリースをインストールしました。

ステップ1 Orchestrator サービスの UI を開きます。

アプリを起動するには、Nexus Dashboard の [サービス] ページのサービススタイルで [開く] をクリックするだけです。

NDO 4.1(2) 以降を初めて開くと、**アップグレード後の検証** プロセスが自動的に開始されます。

ステップ2 データベースのアップグレードをファイナライズします。

- a) レポートに障害がリストされていないことを確認し、[復元して続行] をクリックして続行します。

このリリース用に構成データベースを更新する前に、アップグレードプロセスでいくつかの検証が実行されます。検証は、次のステップの最終アップグレード段階で実行されるテンプレートとポリシーの変更の概要が表示され、次の内容が含まれます。

- 暗黙的なテンプレート ストレッチ – 1 つ以上のオブジェクトが暗黙的にストレッチされている場合、アップグレードプロセスにより、明示的にストレッチされた新しいテンプレートが作成され、オブジェクトがそれらのテンプレートに移動されます。
たとえば、vrf1 を含み、site1 に関連付けられているテンプレート (t1) と、vrf1 を参照する BD を含む (t2) が 2 つのサイトがあるが、2 つのサイト (site1 と site2) に関連している場合、vrf1 は 2 つのサイトの間で暗黙的に拡張されます。
これは、リリース 4.0(1) から許可されなくなり、VRF を両方のサイトに明示的に拡張する必要があります。このような場合、アップグレード中に、VRF は、両方のサイト間で明示的に拡張される別のテンプレートに移動されるか、そのテンプレートの他のポリシーにも拡張が必要かどうかに応じて、元のテンプレートが両方のサイトに関連付けられます。
この場合に作成されるテンプレートはすべて、[テンプレート %d のアップグレード (UpgradeTemplate %)] という名前になります。%d は、新しく追加されたすべてのテンプレートが一意であることを保証するために、1 から始まる増分番号です。
- グローバル ポリシーの移行 – すべてのグローバル テナント ポリシー (DHCP リレーまたはルート マップなど) およびファブリック ポリシー (QoS など) は、リリース 4.0(1) で追加された新しいテナントおよびファブリック ポリシー テンプレートに移動されます。

これは、4.0(1) のベスト プラクティスに従って、既存のスキーマとテンプレートが NDO 構成データベースに再作成されるアップグレードの段階です。これらのスキーマとテンプレートは、グリーンフィールドのスキーマ/テンプレートの作成であるかのように、ローカルの NDO データベースにポストされます。次に、新しく保存されたテンプレートは、現在の展開要件とベスト プラクティスに準拠する正しい順序で展開されます。このステップのテンプレート展開では、「ローカル展開」オプションを使用して展開 プランを計算し、データベースを更新しますが、サイトのコントローラに構成ペイロードを送信しません。

アップグレードプロセスでは、ローカル NDO データベース (NDO の観点からは正しい構成) とファブリックに実際にデプロイされているものとの間の構成のずれもチェックされます。NDO のこのリリースが、アップグレード元のリリースと比較して追加のオブジェクトまたはプロパティをサポートしている場合、アップグレードはサイトのコントローラから既存の構成をインポートすることにより、それらのばらつきを自動的に調整します。

- b) 前のサブステップのレポートを確認し、**[OK]** をクリックして終了します。

データベース アップグレードの最終段階では、実行したアクションの完全なレポートが表示され、確認できます。レポートを閉じた後でもう一度確認したい場合は、**[バックアップ]** ページの **[復元レポートの表示]** をクリックするだけです。

ステップ 3 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。

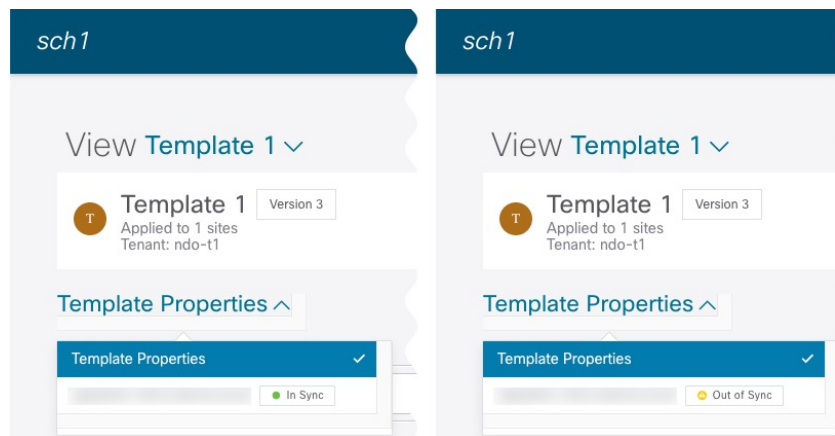
- b) [テナント (Tenants)] および [スキーマ (Schemas)] ページで、以前の Nexus Dashboard Orchestrator クラスタのすべてのテナントとスキーマが存在することを確認します。
- c) [インフラストラクチャ (Infrastructure)] > [サイトの接続 (Site Connectivity)] に移動し、サイト間接続が変更されていないことを確認します。
- メインペインで、各サイトの隣の [接続ステータスの表示 (Show Connectivity Status)] をクリックし、既存のトンネルが稼働しており、接続が中断されていないことを確認します。
- d) メインペインで [構成] をクリックして [ファブリック接続インフラ] 画面を開き、外部サブネットプールのアドレスを確認します。

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

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

設定のばらつき の解決

いくつかの事例では、構成がサイトコントローラで実際に展開される状況が、Nexus Dashboard Orchestrator で定義された設定と異なる場合があります。これらの構成の不一致は、[構成のばらつき (Configuration Drifts)] と呼ばれ、次の図に示すように、テンプレートビューページのサイト名の横に [同期されていません (Out of Sync)] の注意で示されます。



Nexus Dashboard Orchestrator をアップグレードし、以前の構成バックアップを復元した後、このセクションの説明に従って、アップグレードプロセスによって自動的に解決されなかった構成のばらつきを確認して解決することをお勧めします。



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

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

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

展開内のすべてのスキーマとテンプレートについて、次の手順を繰り返します。

次の 2 つの方法のいずれかで、構成のばらつきをチェックできます。

- テンプレートが割り当てられている各サイトのテンプレート展開ステータスアイコンを確認します。
- テンプレートを選択し、[サイトへの展開 (Deploy to sites)] をクリックして構成比較画面を呼び出し、構成のばらつきが含まれているオブジェクトを確認します。

ステップ 3 テンプレートに構成のばらつきが含まれる場合、競合を解決してください。

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

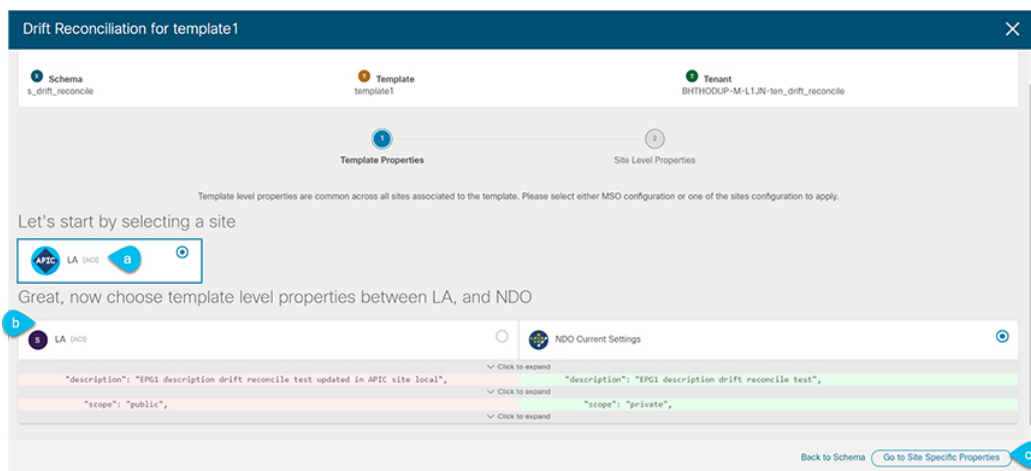
a) テンプレート展開ダイアログを閉じて、スキーマ表示に戻ります。

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

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

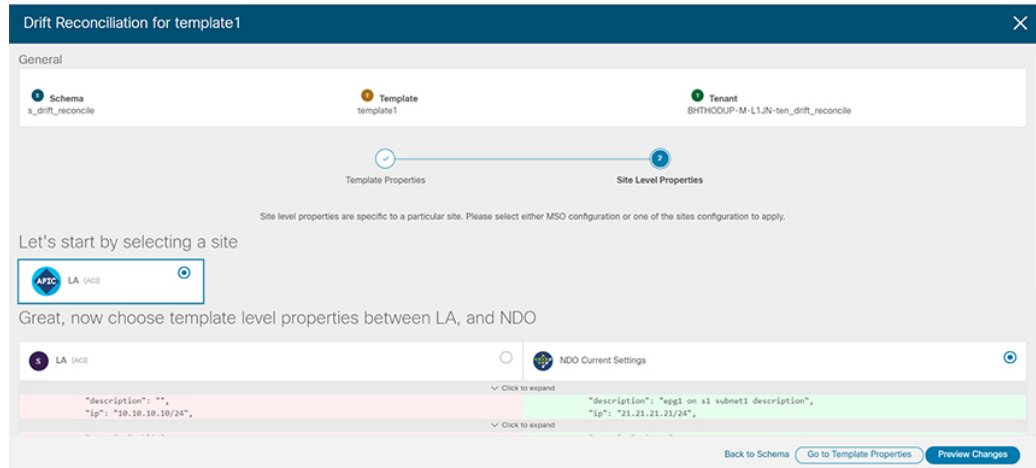
[ばらつきの調整 (Reconcile Drift)] ウィザードが開きます。

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



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

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



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

ほとんどのシナリオでは、テンプレート レベルの構成とサイト レベルの構成のどちらでも同じ選択を行います。ばらつきの調整ウィザードでは、サイトのコントローラで定義されている構成を「テンプレートのプロパティ」レベルで選択し、Nexus Dashboard Orchestrator で定義された構成を「サイトのローカルプロパティ」レベルで選択したり、またその逆で選択したりすることもできます。

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

プレビューは [ばらつきの調整 (Reconcile Drift)] ウィザードの選択肢に基づいて調整された完全なテンプレート構成を表示します。

- f) スキーマを保存します。
g) その後、[サイトに展開 (Deploy to site)] をクリックして構成を展開し、そのテンプレートのばらつきの調整を完了できます。

ステップ 4 Nexus Dashboard Orchestrator で各スキーマとテンプレートに対して上記の手順を繰り返します。

ステップ 5 監査ログをチェックして、すべてのテンプレートが再展開されていることを確認します。

[オペレーション (Operations)] タブの監査ログを表示できます。

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



第 12 章

構成の復元を使用した手動アップグレード

- [概要 \(101 ページ\)](#)
- [前提条件とガイドライン \(103 ページ\)](#)
- [Nexus Dashboard の展開と Nexus Dashboard Orchestrator のインストール \(106 ページ\)](#)
- [構成の復元 \(108 ページ\)](#)
- [設定のばらつきの解決 \(113 ページ\)](#)

概要

Nexus Dashboard Orchestrator のアップグレードに関しては、2つのアプローチがあります。

- 各コンポーネント (Nexus Dashboard プラットフォームや Orchestrator サービスなど) を順番にアップグレードすることによるインプレースアップグレード。

このアプローチは、[サービスカタログを介した自動アップグレード \(79 ページ\)](#) で説明されており、次の場合に推奨されます。

- 物理的な Nexus Dashboard クラスタを使用している場合。
- Nexus Dashboard (2.2.2 以降) および Nexus Dashboard Orchestrator (3.7.1 以降) の最近のリリースを実行している場合。

このアプローチを使用して Orchestrator リリース 3.3(1) 以降をアップグレードできませんが、Orchestrator サービスをアップグレードする前に、基礎となる Nexus Dashboard プラットフォームをアップグレードする必要がある場合があります。このような場合、以下で説明する構成の復元によるアップグレードの方が、より高速で簡単な場合があります。

- 新しい Nexus Dashboard クラスタを展開し、新しい NDO サービス インスタンスをインストールして、構成復元ワークフローで既存の Orchestrator 構成を転送します。

このアプローチは、この章で説明されており、次の場合に推奨されます。

- リリース 3.3(1) より前の Nexus Dashboard Orchestrator またはマルチサイト Orchestrator のいずれかのリリースを実行している場合。

この場合、インプレースアップグレードはサポートされていないため、構成の復元を使用してアップグレードする必要があります。

- 仮想 Nexus Dashboard クラスタを使用していて、Nexus Dashboard Orchestrator の古いリリースを実行している場合。

古い Nexus Dashboard Orchestrator リリースからアップグレードするには、基盤となる Nexus Dashboard プラットフォームもアップグレードする必要があります。その場合、新しいクラスタを展開して構成を復元すると、必要なメンテナンスウィンドウが短縮される可能性があります。

これにより、以前のバージョンに戻りたい場合やアップグレードが失敗した場合に備えて、既存のクラスタを切断して、アップグレードが完了するまで既存の VM を保持することもできます。

リリース 4.0(1) 以降における変更

リリース 4.0(1) 以降、Nexus Dashboard Orchestrator は、テンプレートの設計と展開に関して、いくつかのベスト プラクティスを検証して適用します。

- すべてのポリシー オブジェクトは、依存関係に応じた順序で**[展開 (deployed)]**する必要があります。

たとえば、ブリッジドメイン (BD) を作成するときは、それを VRF に関連付ける必要があります。この場合、BD には VRF 依存関係があるため、VRF は BD の前または一緒にファブリックに展開する必要があります。これらの2つのオブジェクトが同じテンプレートで定義されている場合、Orchestrator は展開時に VRF が最初に作成され、ブリッジドメインに関連付けられるようにします。

ただし、これら2つのオブジェクトを別々のテンプレートで定義し、最初に BD を使用してテンプレートを展開しようとする、関連付けられている VRF がまだ展開されていないため、Orchestrator は検証エラーを返します。この場合、最初に VRF テンプレートを展開してから、BD テンプレートを展開する必要があります。

- すべてのポリシー オブジェクトは、依存関係に応じた順序で**[展開解除 (undeployed)]**する必要があります。つまり、展開された順序と逆の順序で展開する必要があります。

上記の結果から、テンプレートを展開解除するときは、他のオブジェクトが依存しているオブジェクトを展開解除してはなりません。たとえば、VRF が関連付けられている BD を展開解除する前に、VRF を展開解除することはできません。

- 複数のテンプレートにまたがる循環的な依存関係は許可されません。

ブリッジドメイン (bd1) に関連付けられた VRF (vrf1) の場合を考えてみます。これは、次に EPG (epg1) に関連付けられます。[テンプレート 1 (template1)] に vrf1 を作成してそのテンプレートをデプロイし、次に [テンプレート 2 (template2)] に bd1 を作成してそのテンプレートをデプロイすると、オブジェクトが正しい順序でデプロイされるため、検証エラーは発生しません。ただし、その後 [テンプレート1 (template1)] に epg1 を作成しようとする、2つのテンプレート間に循環依存関係が作成されるため、Orchestrator は、EPG の [テンプレート1 (template1)] 追加を保存することを許可しません。

これらの追加のルールと要件により、以前のリリースからリリース 4.0(1)以降にアップグレードするには、既存のすべてのテンプレートを分析し、新しい要件を満たさないテンプレートを変換する必要があります。これは、次のセクションで説明するアップグレードプロセス中に自動的に実行され、既存のテンプレートを新しいベストプラクティスに準拠させるために適用する必要があります。すべての変更の詳細なレポートを受け取ります。



- (注) リリース 4.0(1)に移行する既存の構成をバックアップする前に、次の「前提事項と注意事項」セクションで説明されているすべての要件を満たしていることを確認する必要があります。そうしないと、1つ以上のテンプレートでテンプレートの変換が失敗し、手動で問題を解決するか、移行プロセスを再開する必要があります。

アップグレードのワークフロー

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

1. アップグレードガイドラインの確認と充します。
2. 既存の Nexus Dashboard Orchestrator 構成をバックアップし、バックアップをローカルマシンにダウンロードします。
3. 既存のクラスタを切断または停止します。
既存のクラスターが仮想の場合は、新しいクラスタを展開して構成のバックアップを復元するまで、ネットワークから切断するだけです。これにより、既存のクラスタを保持し、移行手順で問題が発生した場合に簡単にサービスを再開できます。
4. 新しい Nexus ダッシュボードクラスタ リリース 2.3(b) 以降を展開し、Nexus Dashboard Orchestrator リリース 4.1(2) 以降をインストールします。
5. バックアップ用のリモートロケーションを新しい Nexus Dashboard Orchestrator インスタンスに追加し、以前のリリースで作成したバックアップをアップロードして、新しい NDO のインストールで構成バックアップを復元します。
6. 設定のばらつきを解決します。

前提条件とガイドライン

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

- このリリースからのダウングレードはサポートされていないのでご注意ください。

ダウングレードする場合は、以前のバージョンを使用して新しいクラスタを展開し、以前のリリースから構成を復元できます。以前のバージョンで新しいバージョンで作成したバックアップを復元することはできないので注意してください。言い換えると、リリース 3.7(1)でリリース 4.2(1)からのバックアップを復元することはできません。

- バックアップ/復元アップグレードワークフローは、Multi-Site Orchestrator (MSO) リリース 2.x および 3.x、および Nexus Dashboard Orchestrator (NDO) リリース 3.x および 4.x からこのリリースの NDO へのアップグレードをサポートします。

- 既存の構成をバックアップする前に、構成のばらつきがないことを確認してください。

これは、アプリケーション、テナント ポリシー、ファブリック ポリシー、ファブリック リソース ポリシー テンプレートなど、既存のリリースで使用可能なすべてのテンプレート タイプに適用されます。

既存の Nexus Dashboard Orchestrator がリリース 3.7(1) 以降である場合、『[Nexus Dashboard Orchestrator 構成ガイド](#)』の「構成のばらつき」セクションに記載されているアプリケーションテンプレートのばらつきの調整ワークフローを使用できます。

- バックアップして、既存の Orchestrator 構成をダウンロードします。

構成のバックアップについては、お使いのリリースの [Nexus Dashboard Orchestrator 構成ガイド](#) の「バックアップと復元」の章で説明されています。

- バックアップして、既存のファブリックの構成をダウンロードします。

Nexus Dashboard Orchestrator をアップグレードした後、構成のばらつきの調整を実行することをお勧めします。これには、構成をファブリックに再展開する必要がある場合があります。そのため、Nexus Dashboard Orchestrator によって管理されるすべてのファブリックの構成バックアップを作成することをお勧めします。

Cisco APIC 構成バックアップの作成の詳細については、使用しているリリースの [Cisco APIC Basic Configuration Guide](#) の「Management」の章を参照してください。

Cisco Cloud Network Controller 構成バックアップの作成の詳細については、ご使用のリリースの [Cisco Cloud Network Controller User Guide](#) の「Configuring Cisco Cloud Network Controller Components」の章を参照してください。

Cisco Nexus ダッシュボードファブリックコントローラ コンフィギュレーションバックアップの作成の詳細については、使用しているリリースの `format="html" href="https://www.cisco.com/en/US/support/tutorials/systemsmanagement/industrialnetworkmanagement/products/installationandconfiguration/guides/html/scope="external">Cisco NDFC` ファブリックコントローラ構成ガイドの「バックアップと復元」の章を参照してください。

- バージョン管理が有効になっている場合（リリース 3.4(1) 以降サポート）、アップグレード中にテンプレートの最新バージョンのみが保持されることに注意してください。

[ゴールデン (Golden)] のタグが付けられた古いバージョンを含む、テンプレートの他のすべての既存バージョンは転送されません。

- 既存のクラスターの構成バックアップを作成する前に、すべてのテンプレートがサポートされている状態であることを確認します。

- [展開解除 (Undeployed)] されたテンプレート、または作成後に [未展開 (Never Deployed)] テンプレートは、特に注意する必要はなく、アップグレード中に移行されます。

- [展開された (Deployed)] すべてのテンプレートには、保留中の構成変更が含まれていてはなりません。

前回の展開以降に変更されたテンプレートが1つ以上ある場合は、テンプレートの最新バージョンを展開するか、最後に展開されたバージョンに戻して再展開することにより、展開以降のテンプレートへの変更を元に戻す必要があります。



- (注) 無効なテンプレートを含むバックアップを復元しようとするすると失敗し、既存のリリースに戻し、バックアップを復元し、既存の問題を解決してから、移行プロセスを再開する必要があります。そのため、以下の**既存の構成の検証とバックアップの作成**セクションで説明するように、アップグレードを続行する前に、提供されている Python スクリプトを使用してローカルでバックアップを検証することを強くおすすめします。何らかの理由でスクリプトを実行できない場合は、アップグレードを続行する前に、シスコサポートに連絡して設定のバックアップを検証してもらうことをおすすめします。

- Orchestrator サービスをインストールするときは、次の2つの方法のいずれかで実行できます。
 - Nexus Dashboard アプリストアを使用して、この場合、Cisco DC App Center は、管理ネットワークを介して直接、またはプロキシ設定を使用して Nexus Dashboard から到達可能である必要があります。Nexusダッシュボードのプロキシ設定については、『*Nexus Dashboard User Guide*』を参照してください。



- (注) App Storeでは、サービスの最新バージョンにのみアップグレードできます。別のリリースにアップグレードしたい場合は、以下に説明したとおり、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。

- 手動で新しいアプリ イメージをアップロードすることにより、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サービス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。
- SR-MPLS および SDA 統合構成は、アップグレード中に転送されません。

展開にこれらの統合のいずれかが含まれている場合、移行には影響しませんが、通知を受け取り、アップグレードの完了後にそれらを再構成する必要があります。
- Nexus Dashboard Orchestrator をこのリリースにアップグレードした後に新しい Cloud Network Controller 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 Network Controller 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 Network Controller サイトのオンボーディングと管理はサポートされていません。

- アップグレード後に Nexus Dashboard Orchestrator に追加できるバックアップ用のリモートロケーションがあることを確認してください。

リリース 4.1(2) 以降で設定をバックアップおよび復元するには、バックアップをリモートの場所に保存する必要があります。これは、NDO UI で設定する必要があります。バックアップとリモートロケーションの詳細については、『[Cisco Nexus Dashboard Orchestrator Configuration Guide](#)』の「**Operations > Backup and Restore**」の章を参照してください。

既存のインストールですでにリモートの場所が構成されている場合、その場所は構成の復元中に保持されないことに注意してください。したがって、このリリースを展開した後、構成を復元するには、同じリモートの場所を追加する必要があります。

Nexus Dashboard の展開と Nexus Dashboard Orchestrator のインストール

新しいクラスターをデプロイするため、手順はこのガイドの [Nexus Dashboard Orchestrator の展開 \(3 ページ\)](#) 章で説明されている手順と同じです。このセクションでは、手順を要約し、それぞれの特定のリンクを提供します。

始める前に

次の前提条件があります。

- 既存の Nexus Dashboard Orchestrator 構成をバックアップおよびダウンロードしました。

ステップ 1 新しい Nexus Dashboard クラスターを展開します。

展開要件、利用可能なフォームファクタ、およびインストール手順に関する詳細情報は、『[Cisco Nexus Dashboard Deployment Guide, Release 2.3.x](#)』から入手できます。

(注) Nexus ダッシュボードリリース 2.3.2以降を導入することを推奨します。

ステップ 2 Nexus Dashboard と Nexus Dashboard Orchestrator が正常に展開されたら、Nexus Dashboard の**管理コンソール**に移動します。

Nexus Dashboard にログインするには、ブラウザを開き、Nexus Dashboard クラスターのいずれかのノードの管理 IP アドレスに移動し、上部のナビゲーションバーのドロップダウンメニューから **[管理コンソール]** を選択します。

ステップ 3 Orchestrator サービスによって管理されるファブリックを Nexus Dashboard にオンボードします。

- (注) 構成の復元を続行してアップグレードプロセスを完了する前に、Nexus Dashboard Orchestrator (または Multi-Site Orchestrator) によって以前に管理されていたすべてのファブリックを Nexus Dashboard にオンボードする必要があります。

このリリースでは、ファブリックのオンボーディングは、共通の Nexus Dashboard 画面で実行されます。このプロセスについては、『Cisco Nexus Dashboard User Guide』の「[Site Management](#)」の章で詳しく説明されていますが、簡単に言えば次のとおりです。

- a) メインナビゲーションメニューから **[サイト (Sites)]** を選択します。
- b) メインペインで、**[サイトの追加 (Add Site)]** をクリックします。
- c) オンボードするサイトのタイプを選択し、コントローラの IP アドレス、ユーザー名、パスワードなどのサイトの情報を提供します。

- Cisco APICによって管理されるオンプレミスサイトの場合、**[ACI]** を選択します。
 - クラウド ネットワーク コントローラ (以前のクラウド APIC) により管理されるクラウドサイトの場合、**[クラウド ネットワーク コントローラ (Cloud Network Controller)]** を選択します。
- Orchestrator によって管理されていたすべての Cloud APIC サイトにこのオプションを使用します。
- NDFC (以前の DCNM) によって管理されるオンプレミスサイトの場合は、**NDFC** を選択します。
- Orchestrator によって管理されていたすべての DCNM サイトにこのオプションを使用します。

- (注) 過去にサイトを Orchestrator にオンボードしたときと同じサイトの名前を使用する必要があります。別の名前でサイトを追加すると、構成の復元が失敗します。

- d) **[保存 (Save)]** をクリックして、サイトを追加します。
- e) サイトが起動し、Nexus Dashboard UI に **up** と表示されるまで待ちます。
- f) Orchestrator によって以前に管理されていたすべてのサイトについて、この手順を繰り返します。

ステップ 4 Cisco Nexus Dashboard Orchestrator サービスをインストールします。

これについては、このガイドの [Nexus Dashboard Orchestrator の展開 \(3 ページ\)](#) 章で詳しく説明されていますが、Orchestrator のインストールにすでに精通している場合は、次の手順でプロセスを要約します。

App Store を使用してサービスをインストールする場合:

- a) **[サービス (Services)]** 画面で、**[App Store]** タブを選択します。
- b) **[Nexus ダッシュボード オーケストレータ (Nexus Dashboard Orchestrator)]** タイルで、**[アップグレード (Upgrade)]** をクリックします。
- c) 開いた **[ライセンス契約 (License Agreement)]** ウィンドウで、**[同意してダウンロード (Agree and Download)]** をクリックします。

サービスの手動インストールする場合。

- a) DC App Center で Nexus Dashboard Orchestrator ページを参照します。
<https://dcappcenter.cisco.com/nexus-dashboard-orchestrator.html>
- b) **[バージョン (Version)]** ドロップダウンから、インストールするバージョンを選択し、**[ダウンロード (Download)]** をクリックします。

- c) [同意してダウンロードする (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。
- d) Nexus Dashboardの左のナビゲーションメニューから [サービス (Services)] を選択します。
- e) Nexus Dashboard の [サービス (Services)] 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。
- f) メインペインの右上にある [アクション (Actions)] メニューから、[アップロード (Upload)] を選択します。
- g) [サービスをアップロード (Upload Service)] 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。
- h) ファイルを選択します。
前のサブステップで [ローカル (Local)] を選択した場合は、[ファイルの選択 (Select File)] をクリックし、ダウンロードしたアプリケーションイメージを選択します。
[リモート (Remote)] を選択した場合は、イメージファイルのフル URL を指定します。たとえば、`http://<ip-address>:<port>/<full-path>/cisco-mso-<version>.nap` のようになります。
- i) [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。
イメージがクラスタにアップロードされ、初期化されるまでに数分かかる場合があります。

ステップ 5 新しいイメージが初期化されるまで待ちます。

ステップ 6 Nexus Dashboard Orchestrator タイルで、[有効 (Enable)] をクリックします。

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、数分かかる場合があります。

ステップ 7 オーケストレータサービスを起動します。

サービス タイルで [開く (Open)] をクリックするだけです。

シングルサインオン (SSO) 機能を使用すると、Nexus ダッシュボードで使用したものと同一のクレデンシャルを使用してアプリケーションにログインできます。

次のタスク

Nexus ダッシュボードと Nexus ダッシュボードオーケストレータがインストールされ、すべてのサイトがオンボードされたら、[構成の復元 \(108 ページ\)](#) の説明に従って構成の復元に進みます。

構成の復元

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

始める前に

次の前提条件があります。

- 既存の Nexus Dashboard Orchestrator 構成をバックアップおよびダウンロードしました。
- [Nexus Dashboard の展開と Nexus Dashboard Orchestrator のインストール \(106 ページ\)](#) の説明に従って、対象の Orchestrator リリースをインストールしました。

ステップ 1 新しい Nexus ダッシュボード クラスタが稼働中であり、NDO サービスがインストールされていることを確認します。

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

ステップ 2 新しい Nexus Dashboard Orchestrator サービスを開きます。

ステップ 3 設定バックアップ用のリモート ロケーションを追加します。

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

- a) 左側のナビゲーション ペインで、**[操作 (Operations)] > [リモート ロケーション (Remote Location)]** を選択します。
- b) メイン ウィンドウの右上隅で、**[リモート ロケーションの追加 (Add Remote Location)]** をクリックします。

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

- c) リモート ロケーションの名前と説明 (任意) を入力します。

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

- SCP
- ステップ

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

- d) リモート サーバのホスト名または IP アドレスを指定します。

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

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

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

(注) ディレクトリは、リモート サーバにすでに存在しなければなりません。

- f) リモート サーバに接続するために使用するポートを指定します。
デフォルトで、ポートは 22 に設定されます。
- g) リモート サーバに接続するときを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/パズ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 4 新しい Nexus Dashboard Orchestrator クラスタにバックアップ ファイルをインポートします。

- a) 左側のナビゲーション ペインで、**[操作 (Operations)] > [バックアップと復元 (Backups & Restore)]** を選択します。
- b) メイン ペインで、**[アップロード (Upload)]** をクリックします。
- c) 開いた **[リモートへのアップロード]** ウィンドウで、**[ファイルの選択]** をクリックし、アップグレード前に作成した構成バックアップファイルを選択します。
- d) **[リモート ロケーション (Remote location)]** ドロップダウンメニューから、リモート ロケーションを選択します。
- e) (オプション) リモート ロケーションのパスを更新します。

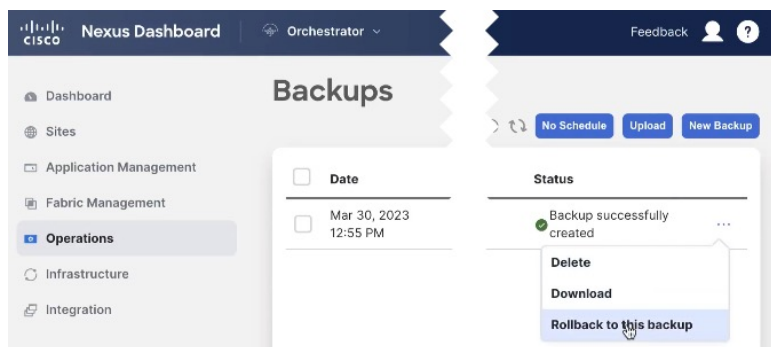
リモートバックアップのロケーションを作成するときに設定したリモートサーバ上のターゲットディレクトリが、**[リモートパス (Remote Path)]** フィールドに表示されます。

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

- f) **インポート** をクリックしてファイルをアップロードします。
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 5 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) [このバックアップから復元 (Restore from this backup)] ウィンドウで、警告を読み、[復元 (Restore)] 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。

復元プロセスはバックアップをインポートし、問題がないかチェックします。完了までに数分かかる場合があります。次のステップで、最初のバックアップのインポート後、データベースをリリース 4.0(1) にアップグレードするために必要な追加の検証を求めるプロンプトが表示されます。

- c) バックアップのインポートが完了したら、レポートにエラーがリストされていないことを確認し、[検証の復元が必要] をクリックして続行します。

このリリース用に構成データベースを更新する前に、アップグレードプロセスでいくつかの検証が実行されます。検証は、次のステップの最終アップグレード段階で実行されるテンプレートとポリシーの変更の概要が表示され、次の内容が含まれます。

- 暗黙的なテンプレート ストレッチ – 1 つ以上のオブジェクトが暗黙的にストレッチされている場合、アップグレードプロセスにより、明示的にストレッチされた新しいテンプレートが作成され、オブジェクトがそれらのテンプレートに移動されます。

たとえば、vrf1 を含み、site1 に関連付けられているテンプレート (t1) と、vrf1 を参照する BD を含む (t2) が 2 つのサイトがあるが、2 つのサイト (site1 と site2) に関連している場合、vrf1 は 2 つのサイトの間で暗黙的に拡張されます。

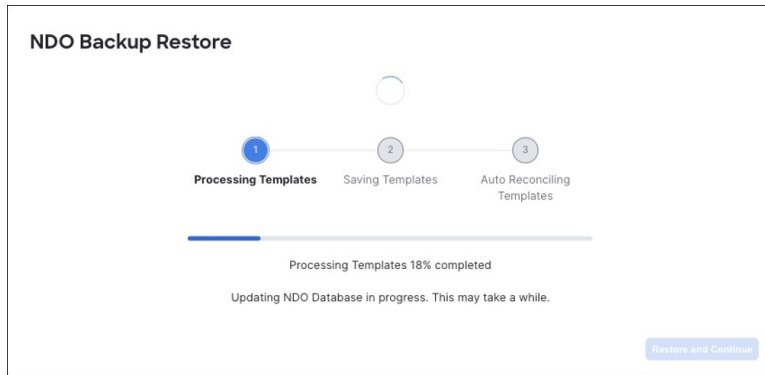
これは、リリース 4.0(1) から許可されなくなり、VRF を両方のサイトに明示的に拡張する必要があります。このような場合、アップグレード中に、VRF は、両方のサイト間で明示的に拡張される別のテンプレートに移動されるか、そのテンプレートの他のポリシーにも拡張が必要かどうかに応じて、元のテンプレートが両方のサイトに関連付けられます。

この場合に作成されるテンプレートはすべて、[テンプレート %d のアップグレード (UpgradeTemplate %)] という名前になります。%d は、新しく追加されたすべてのテンプレートが一意であることを保証するために、1 から始まる増分番号です。

- グローバル ポリシーの移行 – すべてのグローバル テナント ポリシー (DHCP リレーまたはルート マップなど) およびファブリック ポリシー (QoS など) は、リリース 4.0(1) で追加された新しい テナントおよびファブリック ポリシー テンプレートに移動されます。

(注) この段階では、すべてのテナントがバックアップからインポートされ、NDO で作成されていますが、スキーマとテンプレートは次の手順で作成されます。

- d) [検証レポートの復元 (Restore Validation Report)] ウィンドウで、[復元して続行 (Restore and Continue)] をクリックして続行します。



これは、現在のベストプラクティスに従って、バックアップに存在するスキーマとテンプレートがインポートされ、NDO 構成データベースに再作成されるアップグレードの段階です。これらのスキーマとテンプレートは、グリーンフィールドのスキーマ/テンプレートの作成であるかのように、ローカルのNDOデータベースにポストされます。次に、新しく保存されたテンプレートは、現在の展開要件とベストプラクティスに準拠する正しい順序で展開されます。このステップのテンプレート展開では、「ローカル展開」オプションを使用して展開プランを計算し、データベースを更新しますが、サイトのコントローラに構成ペイロードを送信しません。

アップグレードプロセスでは、ローカル NDO データベース（NDO の観点からは正しい構成）とファブリックに実際にデプロイされているものとの間の構成のずれもチェックされます。NDO のこのリリースが、アップグレード元のリリースと比較して追加のオブジェクトまたはプロパティをサポートしている場合、アップグレードはサイトのコントローラから既存の構成をインポートすることにより、それらのばらつきを自動的に調整します。

テンプレートが自動的に調整される場合、2つのテンプレートバージョンが作成されることに注意してください。1つは自動調整の前、もう1つは自動調整の後です。

Version History

General Information
Schema: DriftSchema | Template: Template 1 | Tenant: Anagha

Versions
Golden Versions: | Deployed Versions:

Timeline: 189, 190, 191, 192, 193, 194, 195 (Pre-reconciled), 196 (Post-reconciled)

Version 195	Version 196
"l2UnknownUnicast": "proxy",	"l2UnknownUnicast": "flood",
"multiDstPktAct": "bd-flood",	"multiDstPktAct": "drop",
"unkMcastAct": "flood",	"unkMcastAct": "opt-flood",
"v6unkMcastAct": "flood",	"v6unkMcastAct": "opt-flood",

Version 195: 13 policies | 3 sites (Selected)
Version 196: 13 policies | 3 sites (Current)

+ Added (4) - Deleted (4)

OK

- e) 前のサブステップのレポートを確認し、[OK] をクリックして終了します。

データベース アップグレードの最終段階では、実行したアクションの完全なレポートが表示され、確認できます。レポートを閉じた後でもう一度確認したい場合は、[バックアップ] ページの [復元レポートの表示] をクリックするだけです。

ステップ 6 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 Nexus Dashboard Orchestrator クラスターのすべてのテナントとスキーマが存在することを確認します。
- c) [インフラストラクチャ (Infrastructure)] > [サイトの接続 (Site Connectivity)] に移動し、サイト間接続が変更されていないことを確認します。

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

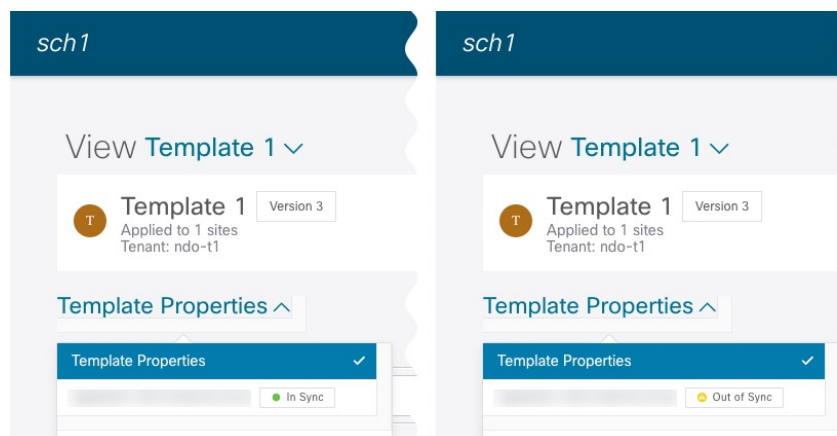
- d) メインペインで [構成] をクリックして [ファブリック接続インフラ] 画面を開き、外部サブネット プールのアドレスを確認します。

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

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

設定のばらつき の解決

いくつかの事例では、構成がサイトコントローラで実際に展開される状況が、Nexus Dashboard Orchestrator で定義された設定と異なる場合があります。これらの構成の不一致は、[構成のばらつき (Configuration Drifts)] と呼ばれ、次の図に示すように、テンプレート ビュー ページのサイト名の横に [同期されていません (Out of Sync)] の注意で示されます。



Nexus Dashboard Orchestrator をアップグレードし、以前の構成バックアップを復元した後、このセクションの説明に従って、アップグレードプロセスによって自動的に解決されなかった構成のばらつきを確認して解決することをお勧めします。



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

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

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

展開内のすべてのスキーマとテンプレートについて、次の手順を繰り返します。

次の 2 つの方法のいずれかで、構成のばらつきをチェックできます。

- テンプレートが割り当てられている各サイトのテンプレート展開ステータスアイコンを確認します。
- テンプレートを選択し、[サイトへの展開 (Deploy to sites)] をクリックして構成比較画面を呼び出し、構成のばらつきが含まれているオブジェクトを確認します。

ステップ 3 テンプレートに構成のばらつきが含まれる場合、競合を解決してください。

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

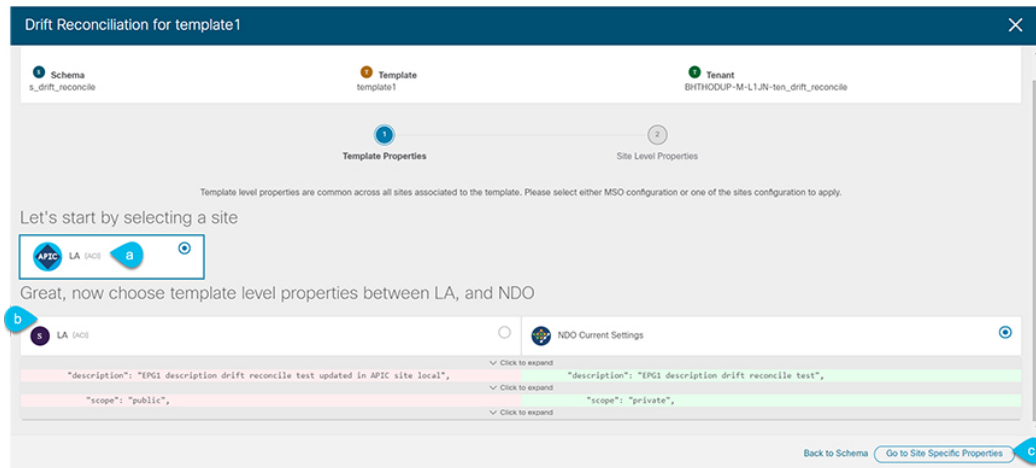
a) テンプレート展開ダイアログを閉じて、スキーマ表示に戻ります。

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

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

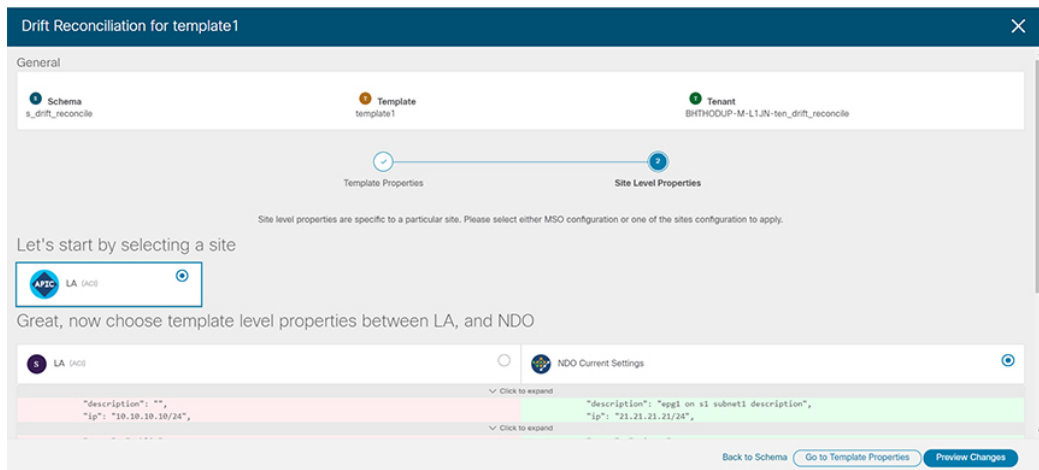
[ばらつきの調整 (Reconcile Drift)] ウィザードが開きます。

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



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

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



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

ほとんどのシナリオでは、テンプレートレベルの構成とサイトレベルの構成のどちらでも同じ選択を行います。ばらつきの調整ウィザードでは、サイトのコントローラで定義されている構成を「テン

プレートのプロパティ」レベルで選択し、Nexus Dashboard Orchestrator で定義された構成を「サイトのローカルプロパティ」レベルで選択したり、またその逆で選択したりすることもできます。

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

プレビューは**[ばらつきの調整 (Reconcile Drift)]** ウィザードの選択肢に基づいて調整された完全なテンプレート構成を表示します。

- f) スキーマを保存します。
g) その後、**[サイトに展開 (Deploy to site)]** をクリックして構成を展開し、そのテンプレートのばらつきの調整を完了できます。

ステップ 4 Nexus Dashboard Orchestrator で各スキーマとテンプレートに対して上記の手順を繰り返します。

ステップ 5 監査ログをチェックして、すべてのテンプレートが再展開されていることを確認します。

[オペレーション (Operations)] タブの監査ログを表示できます。

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

翻訳について

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