Cisco マルチサイト オーケストレータ導入ガイド、リリース 3.2（x）

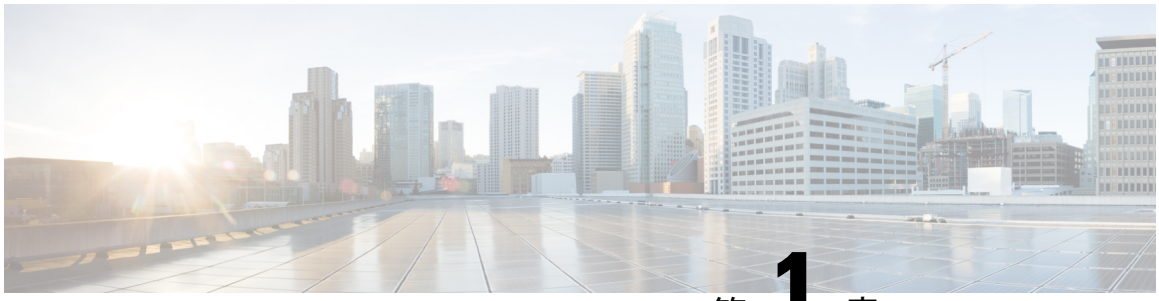
初版：2020 年 11 月 25 日

最終更新：2020 年 12 月 22 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次



第 1 章

新機能および変更された機能に関する情報

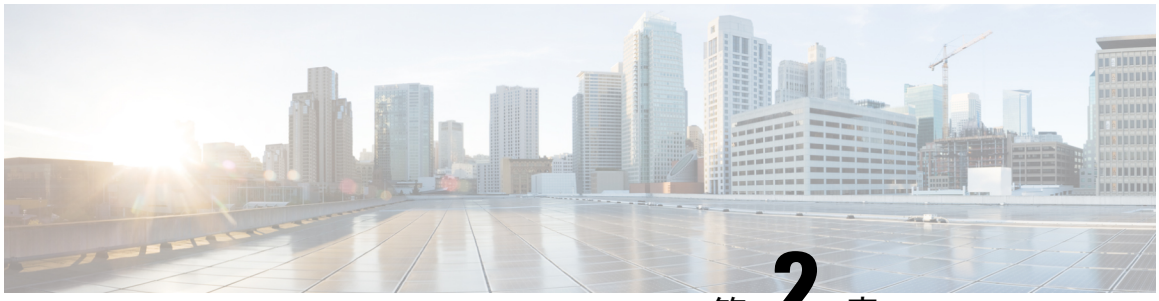
新機能および変更された機能に関する情報

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

表 *1* : 最新のアップデート

リリース	新機能またはアップデート	参照先
3.2(1)	このドキュメントの最初のリリース。	--

新機能および変更された機能に関する情報



第 2 章

マルチサイト オーケストレータを展開

デプロイ概要

リリース 3.2（1）以降では、マルチサイト オーケストレータ（MSO）を Cisco Nexus ダッシュボードのアプリケーションとして展開する必要があります。

Cisco Nexus Dashboard は、複数のデータセンターサイト用の中央管理コンソールであり、Nexus Dashboard オーケストレータ や Nexus Dashboard インサイト などのシスコのデータセンター アプリケーションをホストするための共通プラットフォームです。Nexus Dashboard は、これらのマイクロサービスベースのアプリケーションに共通のプラットフォームと最新のテクノロジースタックを提供し、さまざまな最新アプリケーションのライフサイクル管理を簡素化し、これらのアプリケーションを実行および維持するための運用オーバーヘッドを削減します。Cisco Nexus ダッシュボードは、ポリシーとインフラストラクチャのリアルタイム分析、可視性、保証を提供する Cisco Day-2 オペレーション アプリと、複数の Cisco ACI および Cisco DCNM ファブリック。

各 Nexus Dashboard クラスタは、3 つのマスターノードで構成されます。また、最大 4 つのワーカー ノードを追加して水平方向のスケーリングを有効にし、最大 2 つのスタンバイ ノードを使用して、マスター ノードに障害が発生した場合にクラスタを簡単に回復できます。

Nexus Dashboard クラスタの初期導入と設定の詳細については、『*Cisco Nexus Dashboard Deployment Guide*』を参照してください。

サイトとユーザーの追加などの 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、マルチサイト オーケストレータ アプリケーションの初期インストール要件と手順について説明します。設定および使用例の詳細については、管理するファブリッ

クのタイプに応じて、『*Cisco Multi-Site Configuration Guide for Cisco ACI*』または『*Cisco Multi-Site Configuration Guide for Cisco DCNM*』を参照してください。

前提条件とガイドライン

Nexusダッシュボード

*Cisco Nexus ダッシュボード導入ガイド*の説明に従って、Cisco Nexus ダッシュボードを導入し、ファブリック接続を構成する必要があります。

Cisco マルチサイト オーケストレータのこのリリースは、Nexus ダッシュボードの物理アプライアンス クラスタのみでサポートされています。次の表は、Cisco マルチサイト オーケストレータの Nexus ダッシュボードの要件をまとめたものです。

オーケストレータ バージョン	要件
リリース 3.2(1) 以降	Cisco Nexus Dashboard リリース 2.0.1 Nexus ダッシュボード クラスタは、物理アプライアンスとして展開する必要があります。

Nexus ダッシュボードのネットワーク

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

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

マルチサイト オーケストレータに対して 150ms を超えないラウンドトリップ時間（RTT）で、両方のネットワークでノード間の接続が必要です。同じ Nexus ダッシュボード クラスタで実行されている他のアプリケーションでは、RTT 要件が低い場合があるため、*Nexus ダッシュボード ユーザー ガイド*または特定のアプリケーションのドキュメントを参照することをお勧めします。

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

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

Nexus Dashboard クラスタのサイジング

Nexusダッシュボードは、アプリケーションの共同ホスティングをサポートします。実行するアプリケーション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 マルチサイト オーケストレータ に加えて他のアプリケーション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 ダッシュボード ユーザー ガイド（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。

Network Time Protocol（NTP）

Nexusマルチサイト オーケストレータはクロックの同期にNTPを使用するため、環境内でNTPサーバーを設定する必要があります。

マルチサイト オーケストレータ アプリケーションの App Store を使用してインストール

ここでは、Cisco マルチサイト オーケストレータ アプリケーションを既存の 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、マルチサイト オーケストレータ アプリケーションの手動インストール （8 ページ） の手順に従ってください。

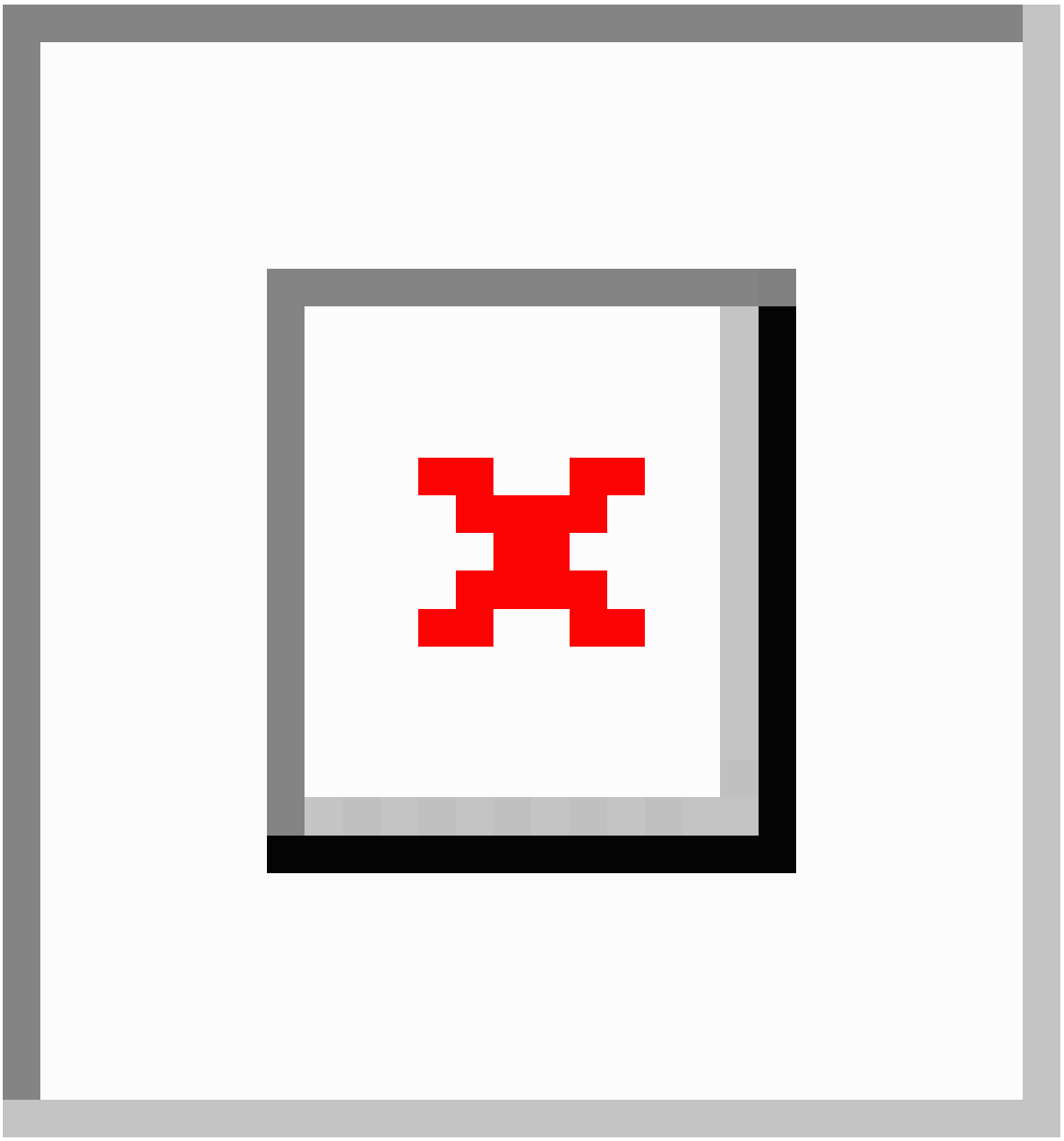
- App Store では、アプリケーションの最新バージョンのみをインストールできます。

  以前のバージョンをインストールする場合は、マルチサイト オーケストレータ アプリケーションの手動インストール （8 ページ） で説明されているようにアプリケーション イメージをダウンロードして、手動でNexusダッシュボードにアップロードする必要があります。

（注） Nexus ダッシュボードは、MSO リリース 3.2（1）以降のみをサポートします。リリース 3.2（1）より前のバージョンをインストールする場合は、使用可能な展開オプションと手順について、そのリリースに固有の『*Nexus* ダッシュボード オーケストレータ インストール ガイド（*Nexus Dashboard Orchestrator Installation Guide*）』を参照してください。

ステップ 1 Nexus ダッシュボード GUI にログインします。

ステップ 2 App Store に移動し、マルチサイト オーケストレータ アプリを選択します。



a) 左のナビゲーションメニューから **[サービス カタログ (Service Catalog)]** を選択します。
b) **[アプリ ストア (App Store)]** タブを選択します。
c) マルチサイト オーケストレータ タイルで、**[インストール（Install）]** をクリックします。

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

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

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

ステップ 5 アプリケーションを有効にします。

インストールが完了した後、デフォルトではアプリケーションは [無効 (Disabled)] 状態のままであるため、有効にする必要があります。

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

ステップ 6 アプリを起動します。

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

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

マルチサイトオーケストレータ アプリケーションの手動インストール

ここでは、Cisco マルチサイト オーケストレータ アプリケーションを手動で既存の 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 マルチサイト オーケストレータ アプリケーションをダウンロードします。

必要な MSO イメージは、次の 2 つの方法のいずれかでダウンロードできます。

a) ソフトウェア ダウンロード ページ リンクを参照します：
https://software.cisco.com/download/home/285968390/type

b) **[マルチサイト ソフトウェア（Multi-Site Software）]** をクリックします。

c) 左側のサイドバーから、Cisco マルチサイト オーケストレータ リリース バージョンを選択します。

d) マルチサイト アプリのイメージ ファイル（`Cisco-MSO-<version> .aci`）をリリースします。

または、Cisco DC App Center からイメージをダウンロードすることもできます：

a) マルチサイト オーケストレータ アプリケーション ページ DC App Center を参照します：
https://dcappcenter.cisco.com/multi-site-orchestrator.html

b) **[バージョン（Version）]** ドロップダウンから、Cisco マルチサイト オーケストレータ リリース バージョンを選択します。

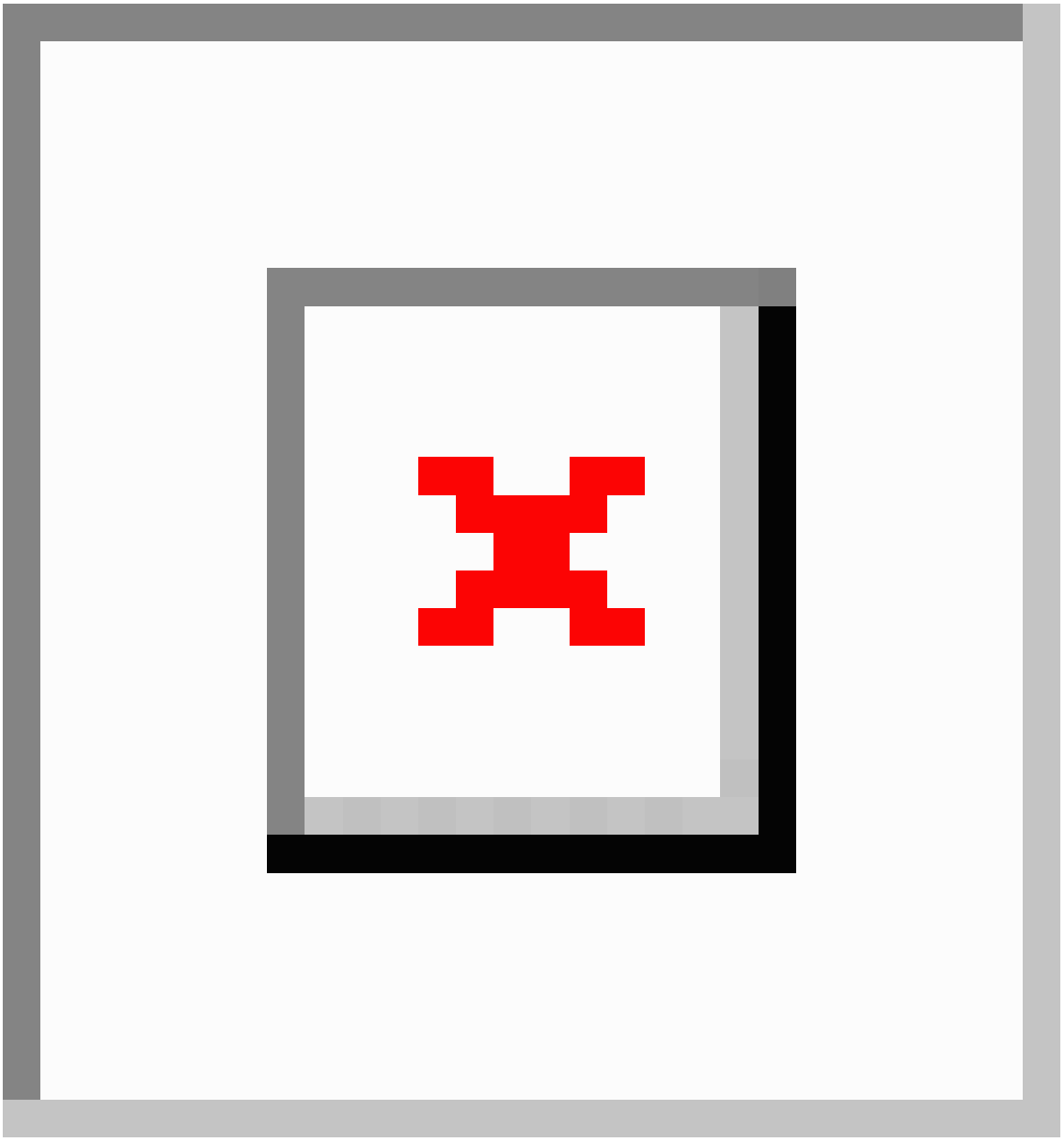
c) [ダウンロード（Download）] ボタンをクリックします。

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

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

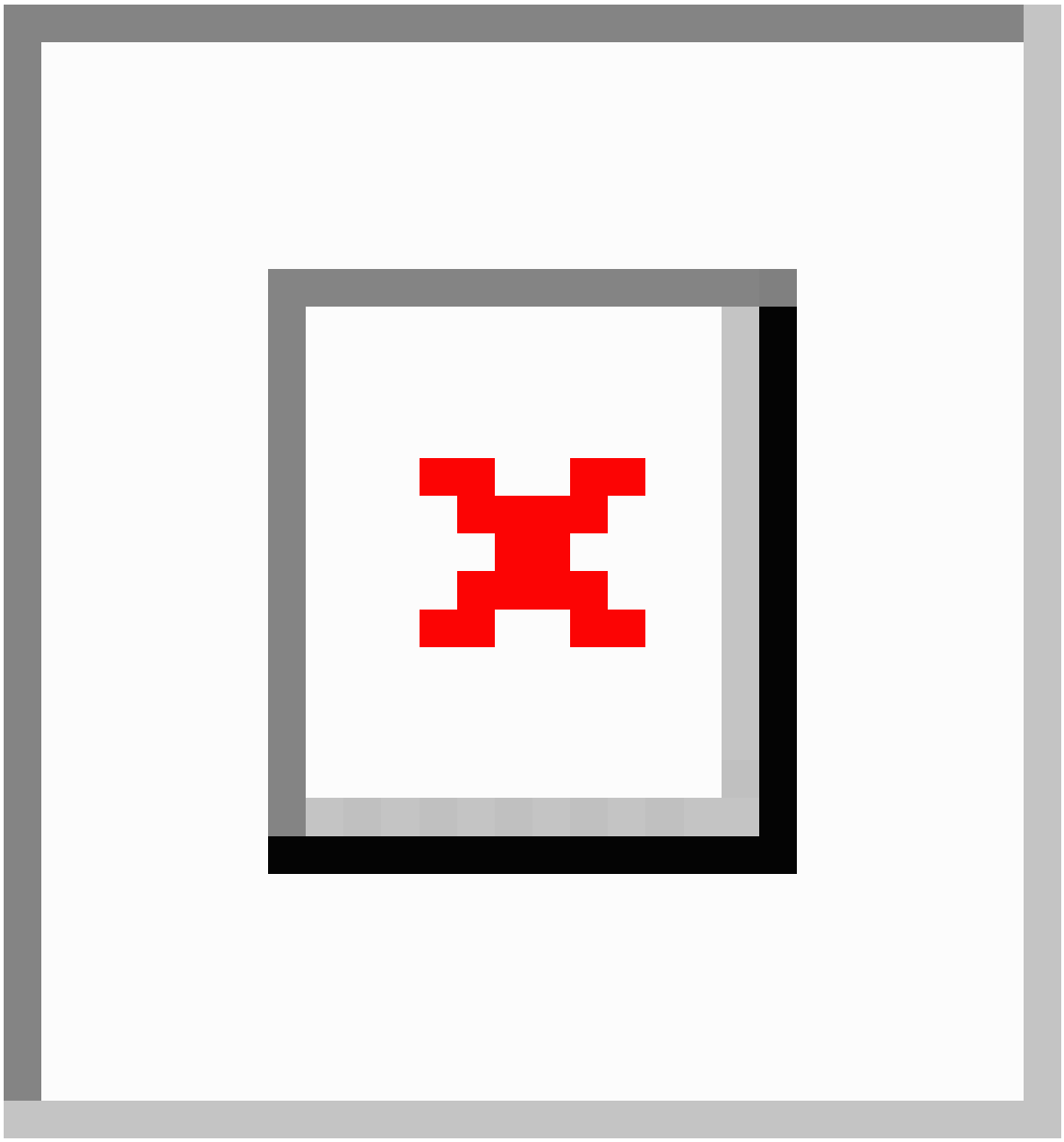
アプリケーションを展開する場合、Nexus ダッシュボードノードの 1 つだけにインストールしてください。アプリケーションはクラスタ内の他のノードに自動的に複製されます。その際、管理 IP アドレスを使用して、Nexus ダッシュボード ノードのどれにでもログインできます。

ステップ 3 アプリケーション イメージをアップロードします。



a) 左のナビゲーションバーで、**[サービス カタログ (Service Catalog)]** をクリックします。
b) **[インストール済みサービス (Installed Services)]** タブをクリックします。
c) メインペインの右上にある**[アクション (Actions)]** > **[アプリケーションのアップロード (Upload App)]**をクリックします。

ステップ 4 Nexus ダッシュボード クラスタにイメージ ファイルをアップロードします。



a) イメージの場所を選択します。

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

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

b) ファイルを選択します。

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

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

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

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

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

ステップ 6 アプリケーションを有効にします。

インストールが完了した後、デフォルトではアプリケーションは `[無効 (Disabled)]` 状態のままであるため、有効にする必要があります。

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

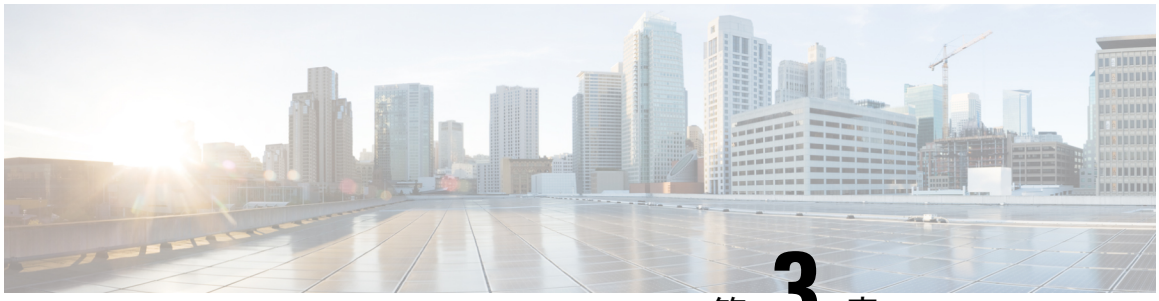
ステップ 7 アプリを起動します。

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

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

第 I 部

ACI ファブリックの Day-0 オペレーション



第 3 章

Cisco ACI サイトの設定

ポッド プロファイルとポリシー グループ

各サイトの APIC には、ポッド ポリシー グループを持つポッド プロファイルが 1 つ必要です。サイトにポッド ポリシー グループがない場合は、作成する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	サイトCisco APICの 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。	
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。	

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 マルチサイト オーケストレータに追加し、Nexus ダッシュボード オーケストレータ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、Multi-Site Orchestrator に追加および管理する前に、APIC サイトごとに作成する必要があるグローバル ファブリック アクセス ポリシーの設定について説明します。

ステップ 1 サイトの APIC GUI に直接ログインします。

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

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

ステップ 3 VLAN プールを指定します。

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

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

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

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

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

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

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

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

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

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

インターフェイスなどの追加の変更は必要ありません。

ステップ 5 ドメインを設定します。

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

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

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

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

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

c) [**送信 (Submit)**] をクリックします。

セキュリティ ドメインなどの追加の変更は必要ありません。

次のタスク

グローバル アクセス ポリシーを設定した後も、#unique_14 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 Multi-Site 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、#unique_16 の説明に従って、VLAN プール、AEP、および ドメインなどのグローバル ファブリック アクセス ポリシーを設定しておく必要があります。

ステップ 1 サイトの APIC GUI に直接ログインします。

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

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

ステップ 3 スパイン ポリシー グループを設定します。

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

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

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

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

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

c) [**送信 (Submit)**] をクリックします。

セキュリティ ドメインなどの追加の変更は必要ありません。

ステップ 4 スパイン プロファイルを設定します。

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

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

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

- **[名前 (name)]** フィールドに、プロファイルの名前 (`Spine1`など) を指定します。
- **[インターフェイス セレクタ (Interface Selectors)]**では、+ 記号をクリックして、ISN に接続されるスパイン スイッチ上のポートを追加します。次に、**[スパイン アクセス ポート セレクターの作成 (Create Spine Access Port Selector)]** ウィンドウで、次のように指定します。

- **[名前 (name)]** フィールドに、ポート セレクタの名前を指定します (例: `Spine1`)。
- **[インターフェイス ID (Interface IDs)]** に、ISN に接続するスイッチ ポートを指定します (例 `5/32`)。
- **[インターフェイス ポリシー グループ (Interface Policy Group)]** に、前の手順で作成したポリシー グループを選択します (例: `Spine1-PolGrp`)。

それから、**[OK]** をクリックして、ポート セレクタを保存します。

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

ステップ 5 スパイン スイッチ セレクター ポリシーを設定します。

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

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

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

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

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

d) **[次へ (Next)]** をクリックして、次の画面に進みます。

e) 前の手順で作成したインターフェイス プロファイルを選択します。

たとえば、`Spine1-ISN`などです。

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

リモート リーフ スイッチを含むサイトの設定

リリース 2.1(2) 以降、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、マルチサイト オーケストレータがこれらのサイトを管理できるようにするために必要なガイドライン、制限事項、および設定手順を説明します。

リモート リーフの注意事項と制限事項

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

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

ステップ 1 サイトの APIC に直接ログインします。

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

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

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

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

（注） 有効にした後は、このオプションを無効にすることはできません。

d) **[送信 (Submit)]** をクリックして変更を保存します。

Cisco Mini ACI ファブリック

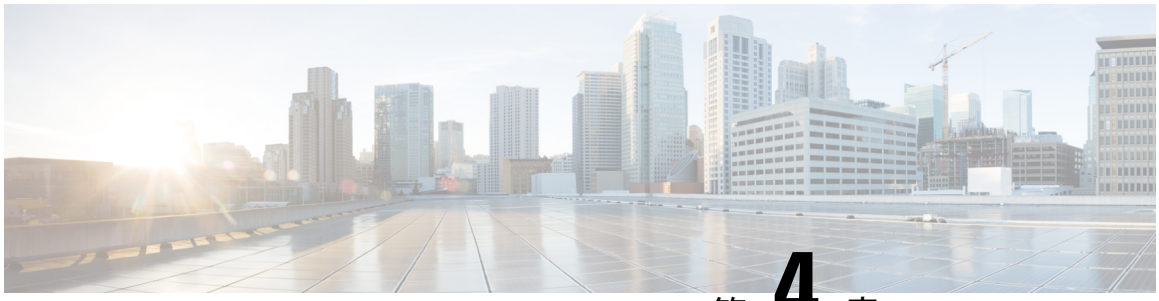
Cisco Multi-Site は、追加の設定を必要とせずに、一般的なオンプレミス サイトとして Cisco Mini ACI ファブリックをサポートします。ここでは、Mini ACI ファブリックの概要について説明します。このタイプのファブリックの導入と設定に関する詳細情報は、『*Cisco Mini ACI ファブリックおよび仮想 APIC*』に記述されています。

Cisco ACI リリース 4.0(1) では、小規模導入向けに Mini ACI ファブリックが導入されました。Mini ACI ファブリックは、仮想マシンで実行される1つの物理 APIC と 2 つの仮想 APIC（vAPIC）

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

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

図 *1 : Cisco Mini ACI* ファブリック



第 4 章

サイトの追加と削除

Cisco MSO と APIC 相互運用性サポート

Cisco マルチサイト Orchestrator（MSO）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。それぞれのファブリックで APIC のリリース 3.2（6）以降が実行されていれば、各サイトの APIC クラスタと MSO それ自体は相互に独立してアップグレードすることができ、それらは混合動作モードで実行できます。そのため、常にマルチサイト 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 MSO をアップグレードすると、新しい MSO 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、MSO 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、このリリースのマルチサイト 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)

Cisco APIC サイトを追加

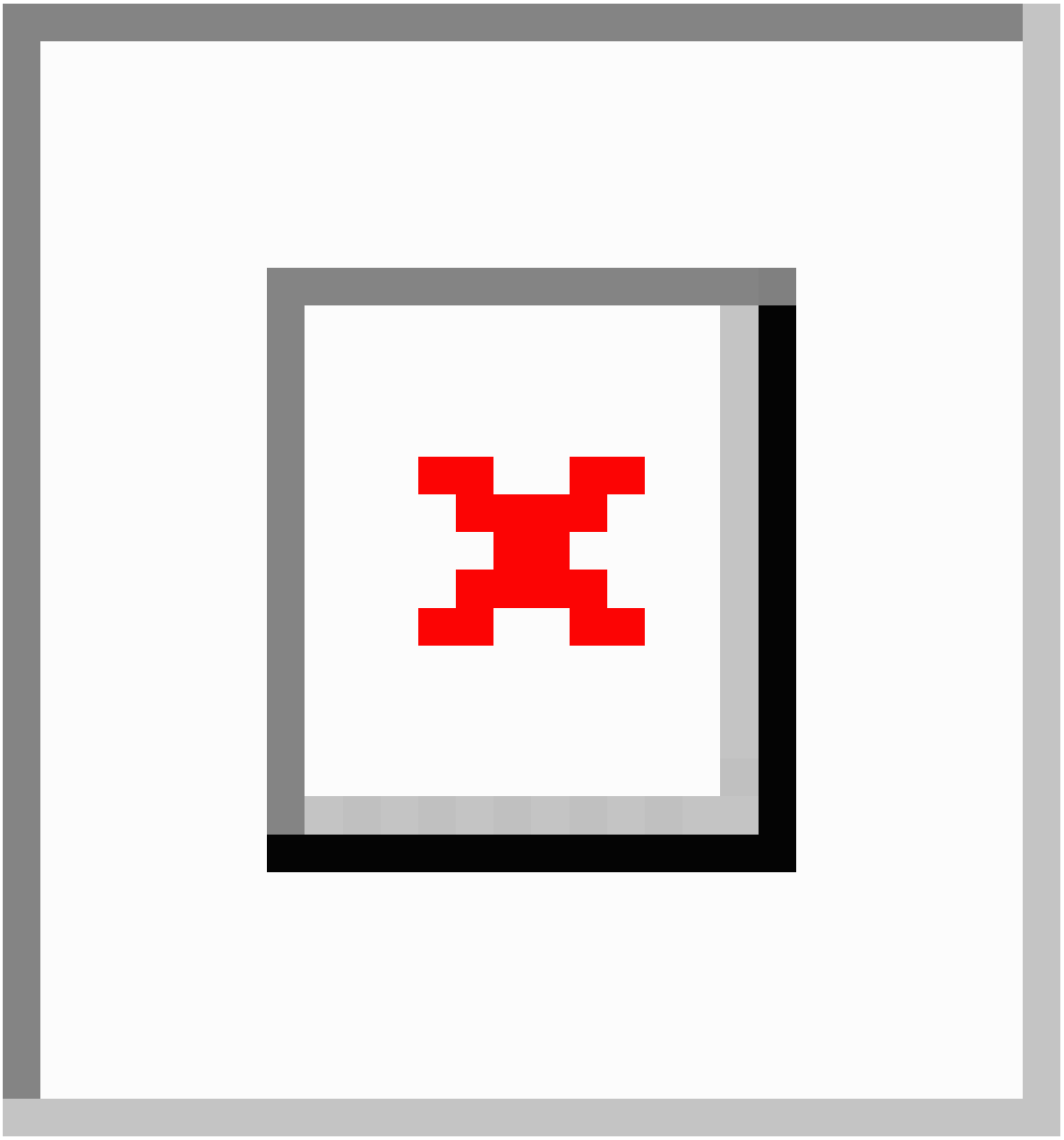
ここでは、Nexus Dashboard GUI を使用して Cisco APIC サイトを追加し、そのサイトをマルチサイト オーケストレータ で管理できるようにする方法について説明します。

始める前に

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

ステップ 1 Nexus ダッシュボード GUI にログインします。

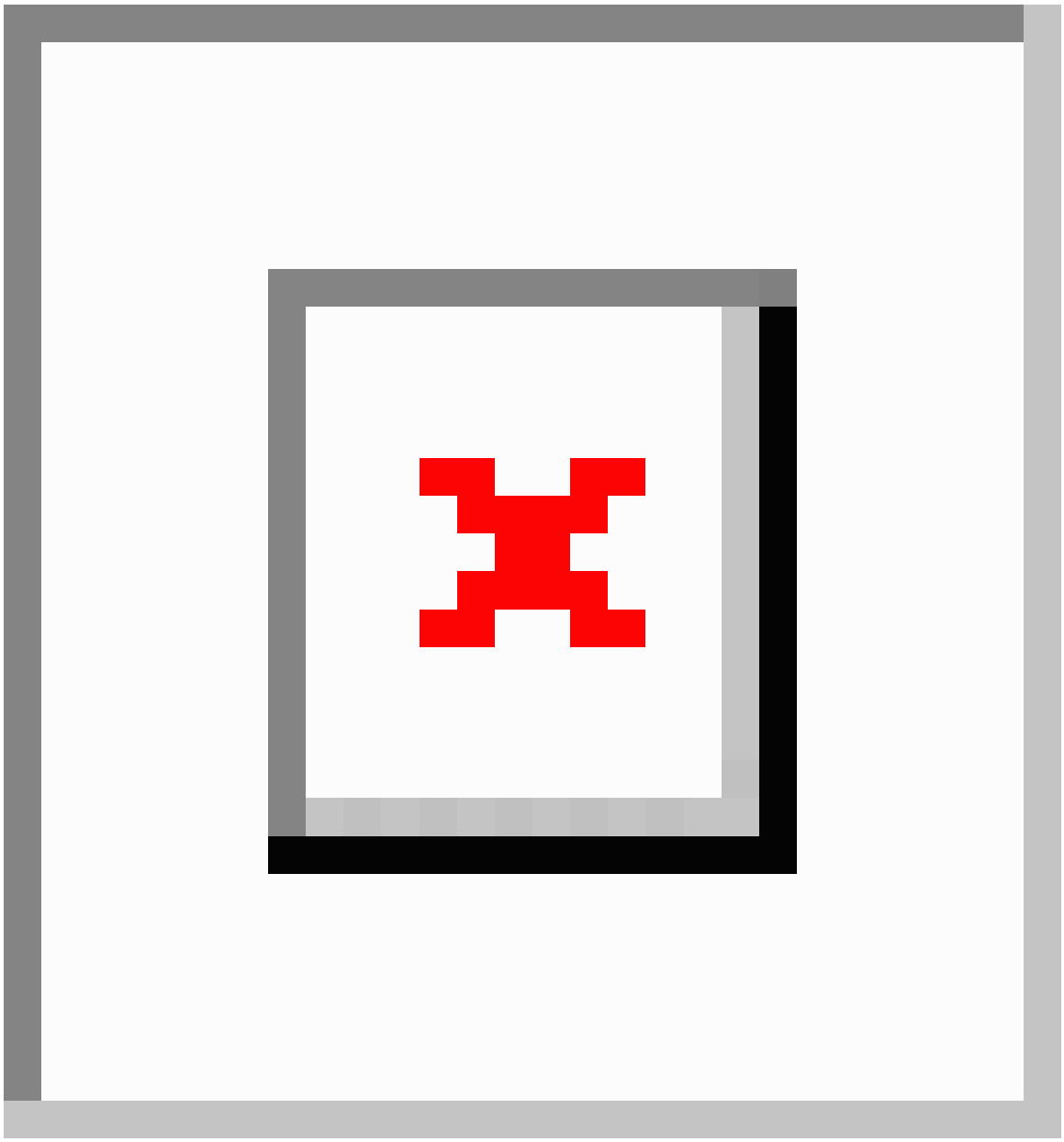
ステップ 2 新サイトを追加します。



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

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

ステップ 3 サイト情報を入力します。



a) **[サイトのタイプ (Site Type)]** で、**ACI** を選択します。
b) APIC 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。

このサイトを Nexus インサイトなどのデイ 2 オペレーション アプリケーションで使用する場合は、追加する Nexus ダッシュボードをファブリックに接続するために使用する**インバンド EPG** 名も指定する必要があります。それ以外の場合、このサイトをマルチサイト オーケストレータでのみ使用する場合は、このフィールドを空白のままにすることができます。

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

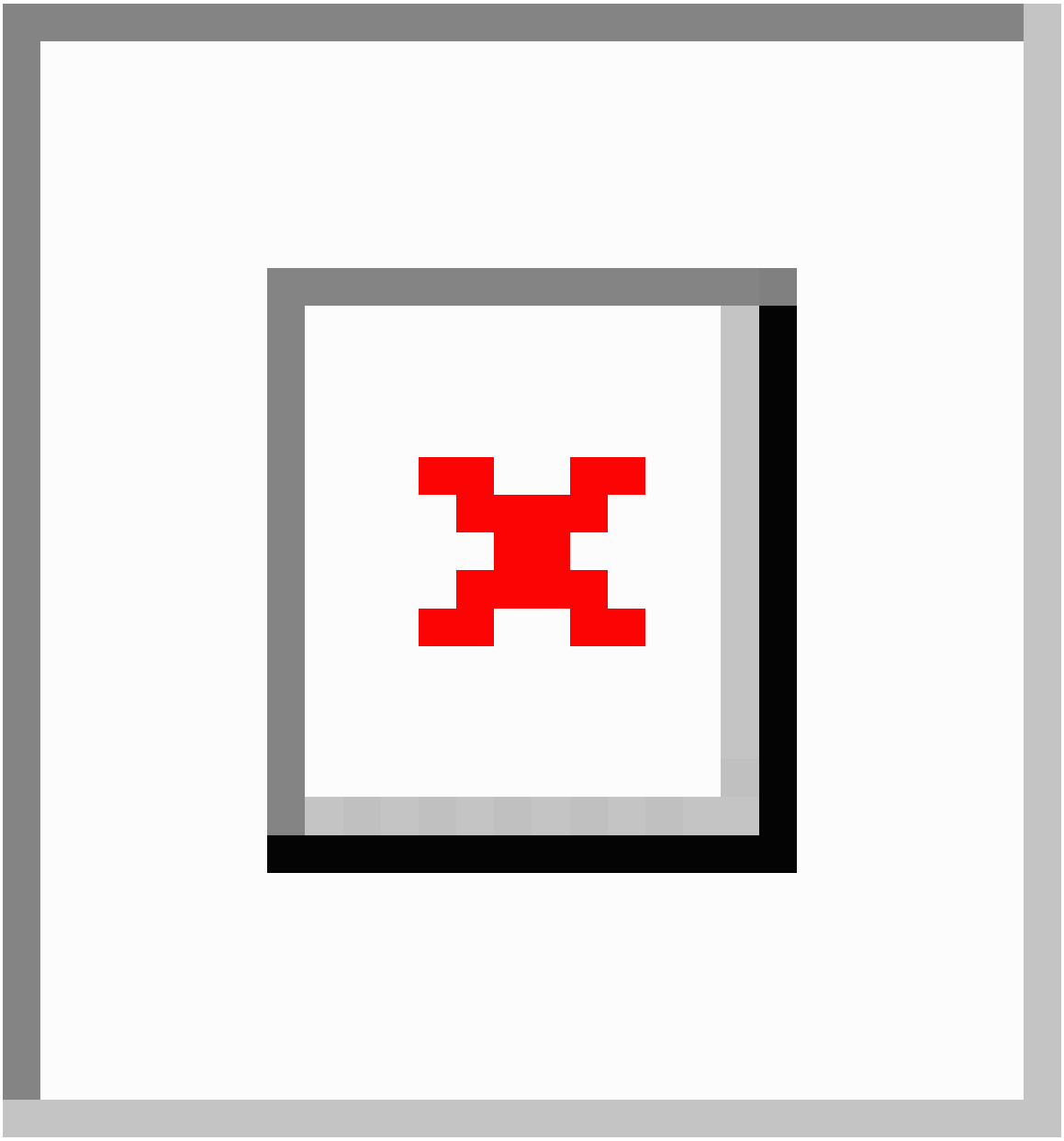
この時点で、サイトは Nexus ダッシュボードで使用できるようになりますが、次の手順で説明するように、マルチサイト オーケストレータの管理用にそれらのサイトを有効にする必要があります。

ステップ 4 他の APIC サイトに対して上記の手順を繰り返します。

ステップ 5 Nexus ダッシュボードの **[サービス カタログ（Service Catalog）]** から、マルチサイト オーケストレータ アプリケーションを開きます。

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 マルチサイト オーケストレータ GUI で、サイトを有効にします。



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

サイトの削除

ここでは、マルチサイト オーケストレータ 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。

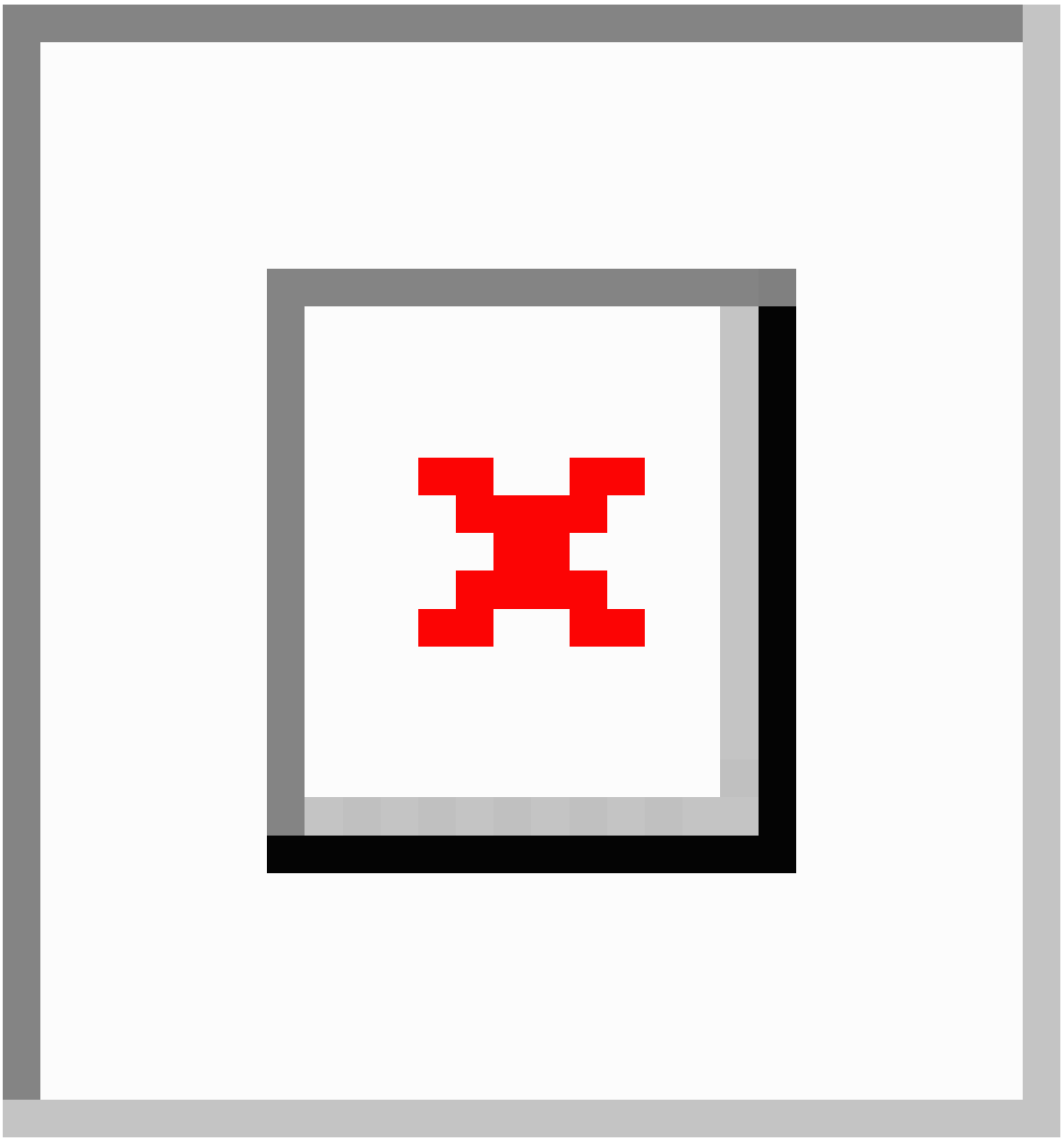
始める前に

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 マルチサイト オーケストレータ 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 MSO アプリケーションを開きます。Nexus ダッシュボードユーザーのクレデンシャルを使用して自動的にログインします。

ステップ 2 マルチサイト オーケストレータ GUI 内でサイトを無効化。



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

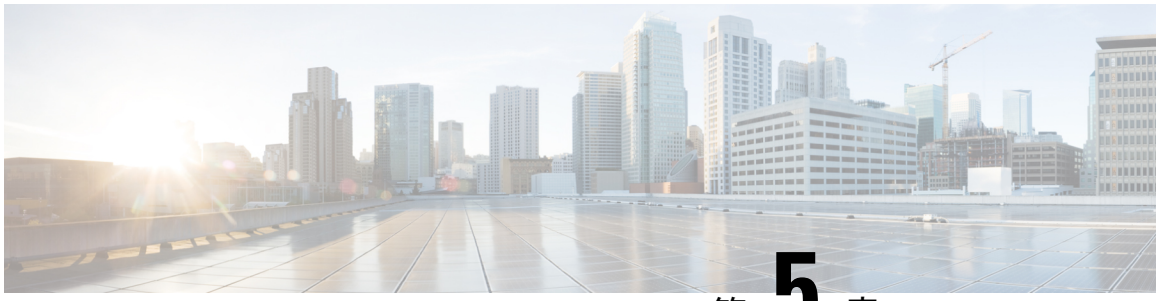
（注） サイトが 1 つ以上の展開済みテンプレートに関連付けられている場合、それらのテンプレートを展開解除するまで、その状態を［非管理対象（Unmanaged）］に変更することはできません。

ファブリック コントローラへの相互起動

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

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

Nexus Dashboardとファブリックがリモート ユーザー認証のために構成されている場合、Nexus Dashboard ユーザーと同じログイン情報を使用して、ファブリックのコントローラに自動的にログインします。



第 5 章

Cisco ACI サイトのインフラの設定

前提条件とガイドライン

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

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

- 各サイトのファブリック アクセス ポリシーの設定。
- リモート リーフ スイッチを使用したサイトの直接通信およびルーティング可能なサブネットの設定。

さらに、次の点に注意してください。

- スパイン スイッチまたはスパイン ノード識別子の変更の追加や削除などのインフラストラクチャの変更には、一般的なインフラの設定手順の一部として、サイト接続性情報の更新 （32 ページ） に記載されているマルチサイト オーケストレータ ファブリック接続情報の更新が必要です。
- Orchestrator に割り当てられているオーバーレイ ユニキャスト TEP、オーバーレイ マルチキャスト TEP、および BGP EVPN ルータ ID IP 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。

インフラの設定: 一般設定

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

ステップ 1 Cisco マルチサイト Orchestrator GUI にログインします。

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

ステップ 3 メイン ペインにある **[インフラの設定（Configure Infra）]** をクリックします。

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

ステップ 5 コントロール プレーン BGP を構成します。

a) **[BGP ピアリング タイプ (BGP Peering Type)]** ドロップダウンから、`[フルメッシュ (full-mesh)]` または `[ルートリフレクタ (route-reflector)]` のいずれかを選択します。

`[ルートリフレクタ (route-reflector)]`オプションは、すべてのサイトが同じ BGP 自律システム (AS) に属している場合にのみ有効です。

b) **[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。

c) **[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。

d) **[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。

e) **[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。

f) **[最大AS 制限値 (Maximum AS Limit)]** フィールドで、最大 AS 制限値を入力します。

g) **[ピア間 BGP TTL (BGP TTL Between Peer)]** フィールドで、ピア間の BGP TTL を入力します。

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 マルチサイト オーケストレータ GUI にログインします。

ステップ 2 **[メイン メニュー (Main menu)]** で、**[インフラストラクチャ (Infrastructure)]** > **[インフラの設定 (Infra Configuration)]**を選択します。

ステップ 3 右上にある **[インフラの構成 (Infra Configuration)]** ビューで、**[インフラの設定 (Configure Infra)]** ボタンをクリックします。

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

ステップ 5 メイン ウィンドウで、**[サイト データのリロード（Reload Site Data）]** ボタンをクリックし、APIC からファブリック情報をプルします。

ステップ 6 （オプション）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 マルチサイト オーケストレータ GUI にログインします。

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

ステップ 3 メイン ペインにある **[インフラの設定（Configure Infra）]** をクリックします。

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

ステップ 5 右側の **[<サイト> 設定（Settings）]** ペインで、**[マルチサイト （Multi-Site）]** ノブを有効にしてオーケストレータでサイトを管理できるようにします。

ステップ 6 (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。

ステップ 7 **[オーバレイ マルチキャスト TEP (Overlay Multicast TEP)]** を指定します。

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

ステップ 8 **[BGP 自律システム番号 (BGP Autonomous System Number)]** を指定します。

ステップ 9 **[BGP パスワード (BGP Password)]** を指定します。

ステップ 10 **[OSPF Area ID (OSPF エリア ID)]** を指定します。

マルチサイト インフラ OSPF の詳細を設定する際には、OSPF エリア `0` を使用することを推奨します。`0` 以外のエリア ID を使用する場合、次の手順ではそれを`regular` OSPF エリア タイプとして設定することになります。 `stub` エリア タイプにはなりません。

ステップ 11 ドロップダウン メニューから **[OSPF エリア タイプ (OSPF Area Type)]**を選択します。

OSPF エリアタイプは、次のいずれかになります。

- `nssa`
- `regular`
- `stub`

ステップ 12 ドロップダウン メニューから外部ルート 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。

ステップ 13 サイトの OSPF 設定を行います。

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

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

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

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

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

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

デフォルト値は 40 です。

- **[再送信間隔 (秒) (Retransmit Interval (Seconds))]** フィールドに、再送信間隔を秒単位で入力します。

  デフォルト値は 5 です。

- **[転送遅延 (秒) (Transmit Delay (Seconds))]** フィールドに、遅延を秒単位で入力します。

  デフォルトは 1 です。

ステップ 14 (オプション) サイトの SR-MPLS 設定を構成します。

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

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

デフォルトの範囲は 16000 ～ 23999 です。

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

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 マルチサイト オーケストレータ GUI にログインします。

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

ステップ 3 **[サイト]** ビューで、**[インフラの構築]** をクリックします。

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

ステップ 5 メイン ウィンドウで、ポッドを選択します。

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

このIPアドレスは、同じポッドの一部であり、サイト間の既知のユニキャスト トラフィックに使用されるすべてのスパイン スイッチに導入されます。

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

ルーティング可能な TEP プールは、サイト間接続のパブリック IP アドレスに使用されます。

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。

ステップ 1 Cisco マルチサイト オーケストレータ GUI にログインします。

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

ステップ 3 **[サイト]** ビューで、**[インフラの構築]** をクリックします。

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

ステップ 5 メイン ウィンドウで、ポッド内のスパイン スイッチを選択します。

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

ステップ 7 **[ポートの追加（Add Port）]** ウィンドウで、次の情報を入力します。

- **[イーサネット ポート ID (Ethernet Port ID)]** フィールドに、ポート ID、たとえば `1/29` を入力します。
- **[IP アドレス (IP Address)]** フィールドに、IP アドレス/ネットマスクを入力します。

  MSO によって、指定されたポートで指定された IP アドレスを持つ VLAN 4 でサブインターフェイスが作成されます。
- **[MTU]** フィールドに、サーバの MTU を入力します。`[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。

  スパイン ポートの MTU は、IPN 側の MTU と一致させる必要があります。
- **[OSPF ポリシー (OSPF Policy)]** フィールドで、インフラの設定: オンプレミス サイトの設定 （33 ページ） で設定したスイッチの OSPF ポリシーを選択します。

  OSPF ポリシーの OSPF 設定は、IPN 側と一致させる必要があります。
- **[OSPF 認証 (OSPF Authentication)]** では、`[なし (none)]` または以下のいずれかを選択します。
  - `MD5`
  - `Simple`

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

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

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

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

ステップ 10 すべてのスパイン スイッチで手順を繰り返します。

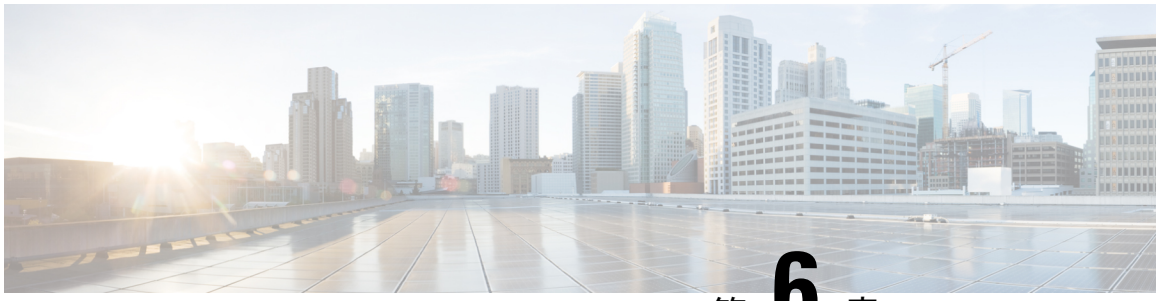
インフラ設定の展開

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。

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。

第 II 部

DCNM ファブリックの Day-0 運用



第 6 章

サイトの追加と削除

Cisco DCNM サイトの追加

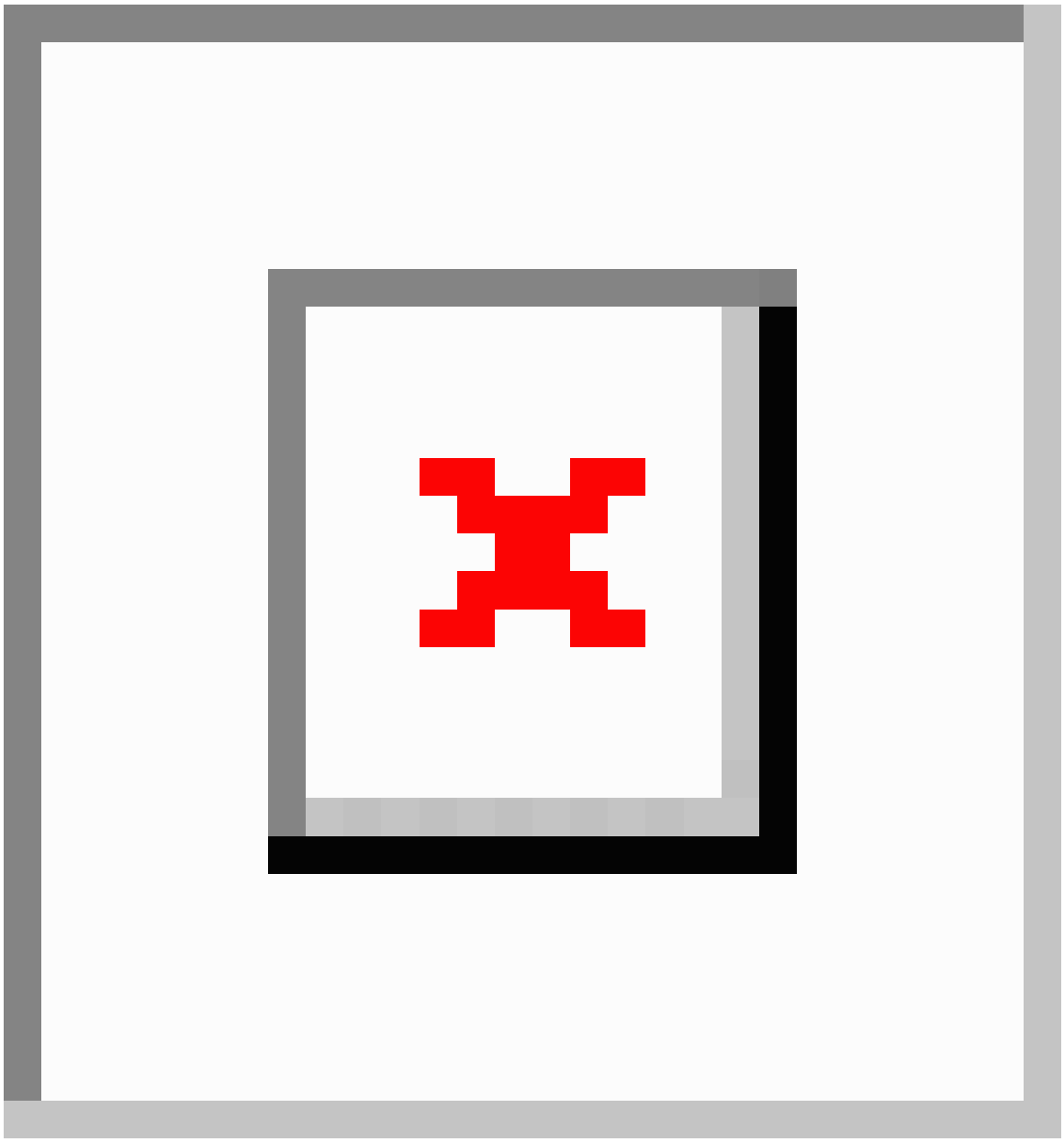
ここでは、Nexus Dashboard GUI を使用して DCNM サイトを追加し、そのサイトを マルチサイト オーケストレータ で管理できるようにする方法について説明します。

始める前に

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

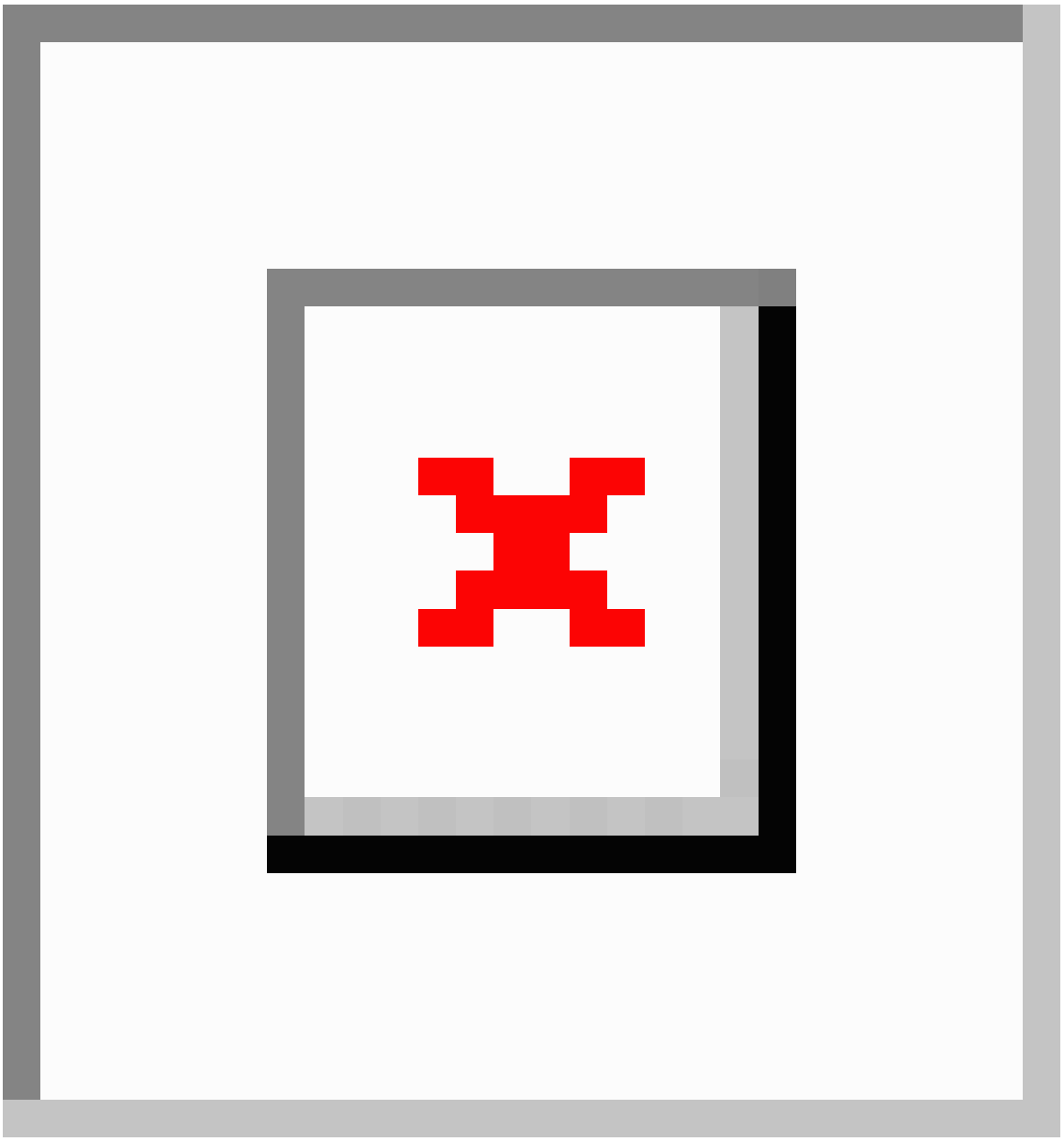
ステップ 1 Nexus ダッシュボード GUI にログインします。

ステップ 2 新サイトを追加します。



a) 左のナビゲーションメニューから **[サイト (Sites)]** を選択します。
b) メインペインの右上にある**[アクション (Actions)]** > **[サイトの追加 (Add Site)]**をクリックします。

ステップ 3 サイト情報を入力します。



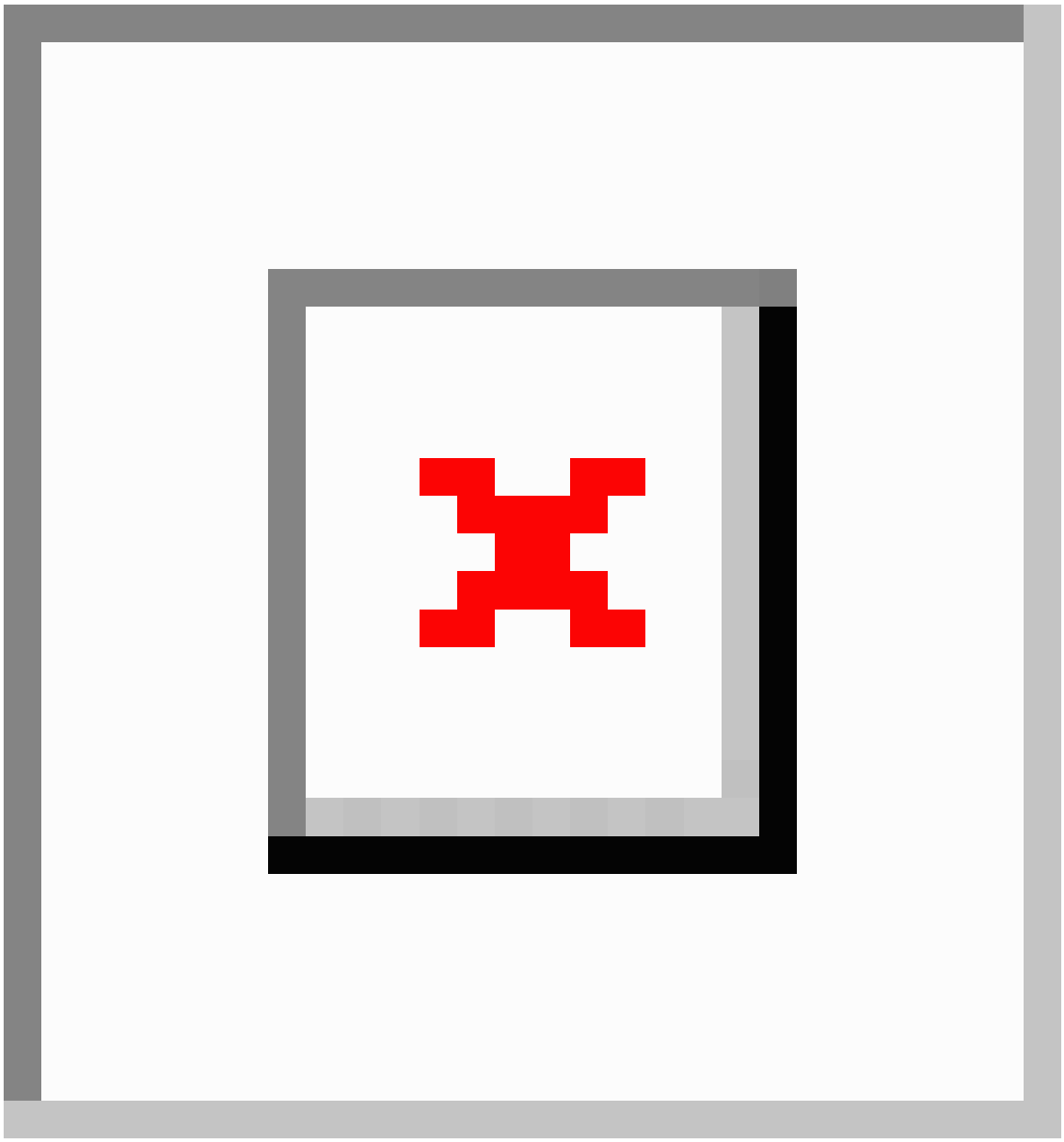
a) **[サイトのタイプ (Site Type)]** で、**[DCNM]** を選択します。
b) DCNM コントローラ情報を入力します。

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

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

   ファブリック選択ウィンドウが開きます。

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



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

b) [選択（Select）] をクリックします。

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

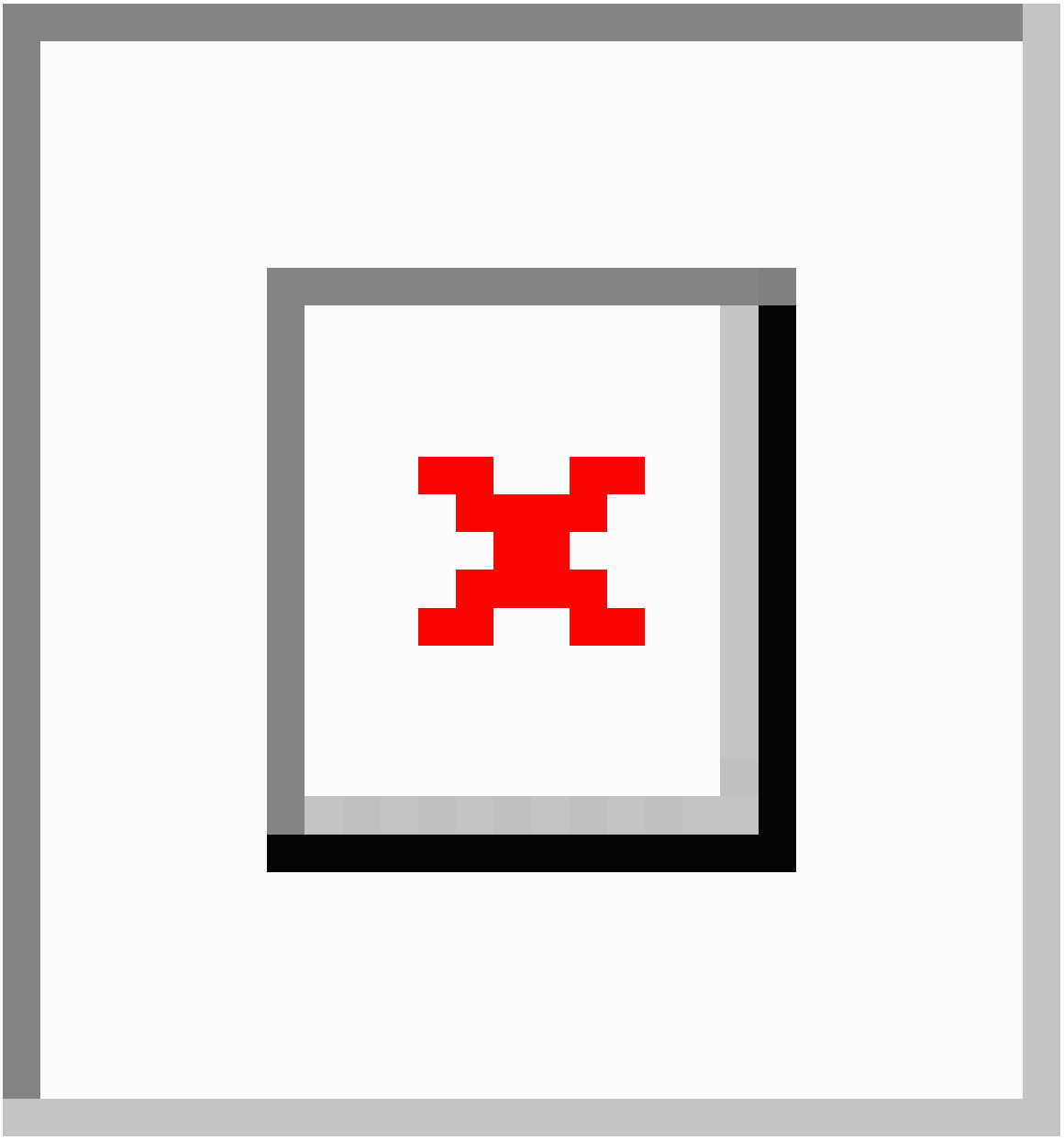
この時点で、サイトは Nexus ダッシュボードで使用できるようになりますが、次の手順で説明するように、マルチサイト オーケストレータの管理用にそれらのサイトを有効にする必要があります。

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

ステップ 7 Nexus ダッシュボードの **[サービス カタログ (Service Catalog)]** から、マルチサイト オーケストレータ アプリケーションを開きます。

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

ステップ 8 マルチサイト オーケストレータ GUI 内でサイトを有効化。



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

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

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

ただし、ファブリックが DCNM MSD の一部ではない場合、サイトの **[ファブリック ID (Fabric ID)]** を指定しない限り、その状態を［管理対象 (Managed)］に変更することはできません。

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

サイトの削除

ここでは、マルチサイト オーケストレータ 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。

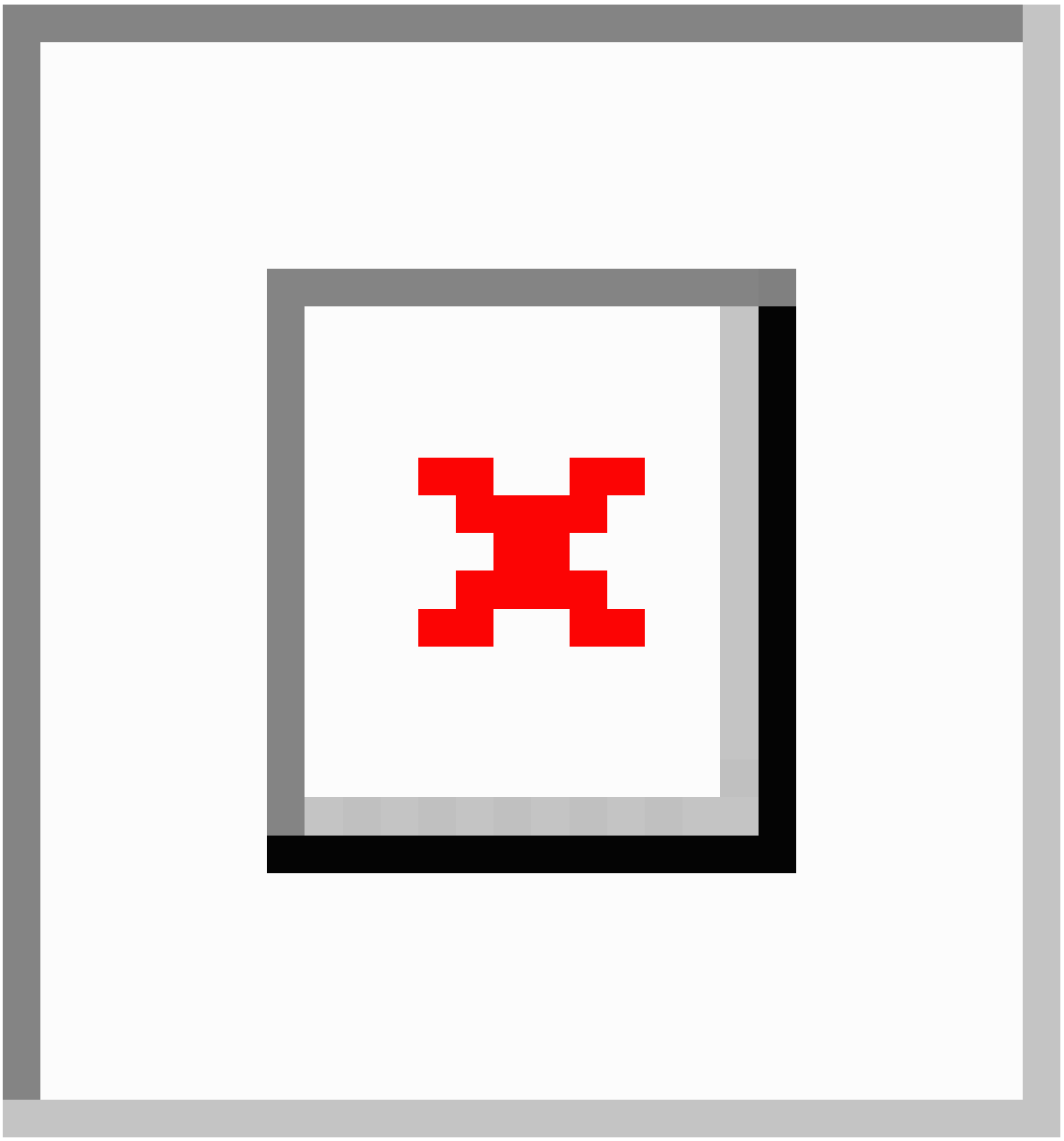
始める前に

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 マルチサイト オーケストレータ 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 MSO アプリケーションを開きます。Nexus ダッシュボード ユーザーのクレデンシャルを使用して自動的にログインします。

ステップ 2 マルチサイト オーケストレータ GUI 内でサイトを無効化。



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

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

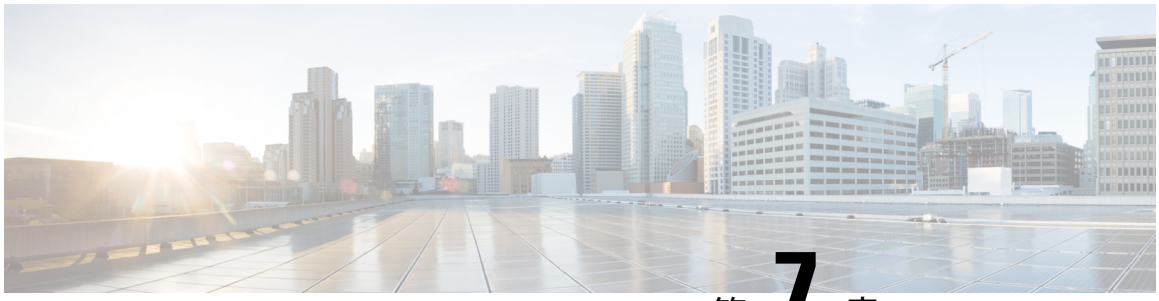
（注） サイトが 1 つ以上の展開済みテンプレートに関連付けられている場合、それらのテンプレートを展開解除するまで、その状態を［非管理対象（Unmanaged）］に変更することはできません。

ファブリック コントローラへの相互起動

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

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

Nexus Dashboardとファブリックがリモート ユーザー認証のために構成されている場合、Nexus Dashboard ユーザーと同じログイン情報を使用して、ファブリックのコントローラに自動的にログインします。



第 7 章

Cisco DCNM サイトのインフラの設定

前提条件とガイドライン

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

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

さらに、次の点に注意してください。

- 境界ゲートウェイ スイッチの追加や削除には、一般的なインフラの設定手順の一部として、サイト接続性情報の更新 （51 ページ）に記載されている、マルチサイト オーケストレータのファブリック接続情報の更新が必要です。

インフラの設定: 一般設定

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

ステップ 1 Cisco マルチサイト Orchestrator GUI にログインします。

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

ステップ 3 メイン ペインにある **[インフラの設定（Configure Infra）]** をクリックします。

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

ステップ 5 コントロール プレーン BGP を構成します。

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

- `full-mesh`：各サイトのすべてのボーダー ゲートウェイ スイッチは、リモート サイトのボーダー ゲートウェイ スイッチとのピア接続を確立します。
- `route-server`：route-server オプションを使用すると、各サイトが MP-BGP EVPN セッションを確立する 1 つ以上のコントロールプレーン ノードを指定できます。ルートサーバー ノードは、従来の BGP ルート リフレクタと同様の機能を実行しますが、EBGP（iBGP）セッションでは使用しません。ルート サーバー ノードを使用すると、MSO 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。

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

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

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

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

a) **[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。

b) **[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。

c) **[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。

d) **[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。
e) **[最大AS 制限値 (Maximum AS Limit)]** フィールドで、最大 AS 制限値を入力します。
f) **[ピア間 BGP TTL (BGP TTL Between Peer)]** フィールドで、ピア間の BGP TTL を入力します。

ステップ 6 DCNM 設定を構成します。

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

このフィールドは、各ファブリックの**[マルチサイト TEP（Multi-Site TEP）]**フィールドに自動入力するために使用されます。インフラの設定: DCNN サイトの設定 （51 ページ）で説明します。

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

d) **[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、マルチサイト オーケストレータ 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 マルチサイト Orchestrator GUI にログインします。

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

ステップ 3 メイン ペインにある **[インフラの設定（Configure Infra）]** をクリックします。

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

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

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

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

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

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

インフラの設定: DCNN サイトの設定

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

ステップ 1 Cisco マルチサイト Orchestrator GUI にログインします。

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

ステップ 3 メイン ペインにある **[インフラの設定（Configure Infra）]** をクリックします。

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

ステップ 5 右側の **<*Site*>[設定 (Settings)]**サイドバーで、**マルチサイト TEP** を指定します。

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

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

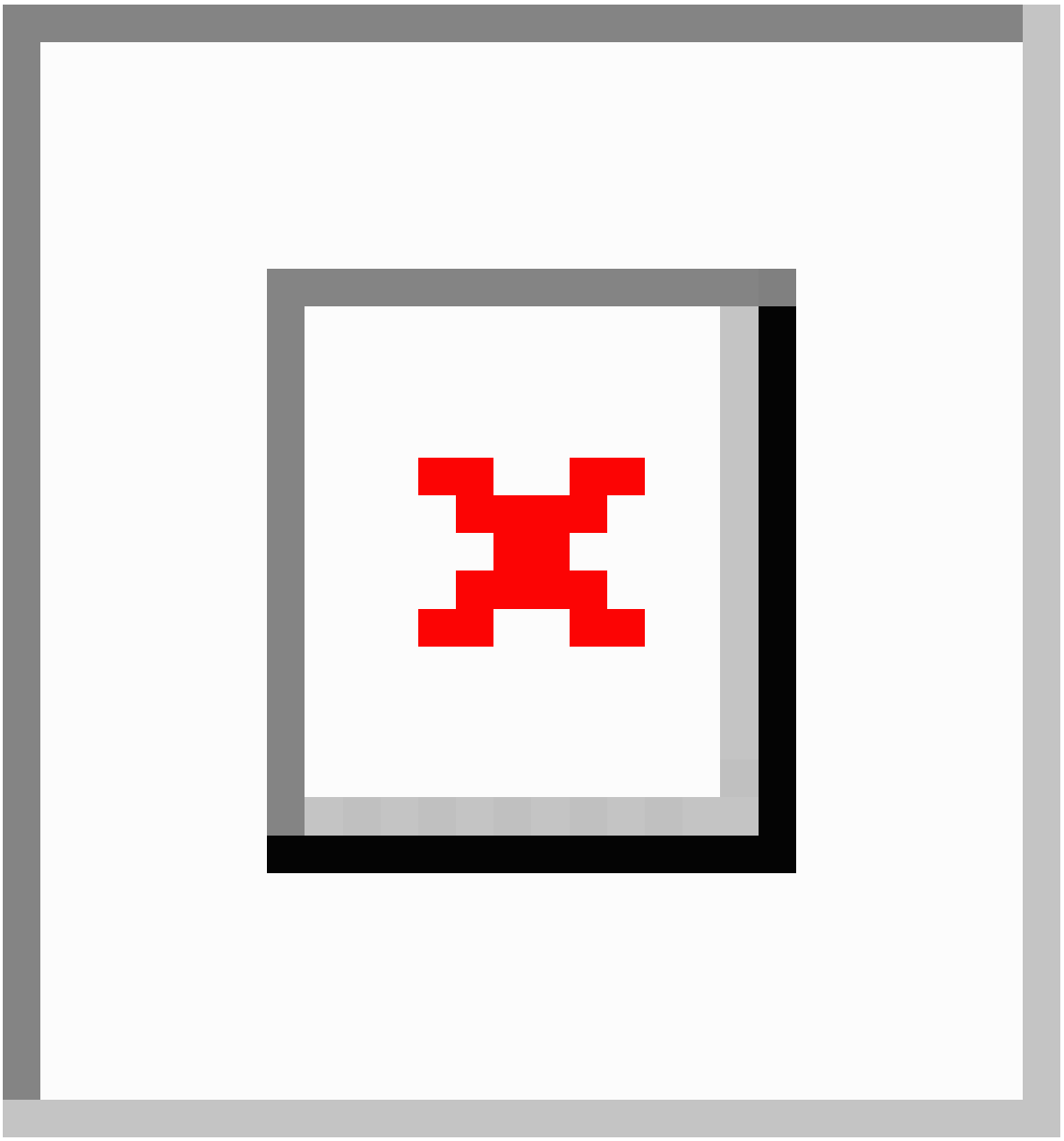
[自動割り当て (Auto Allocate)] フィールドを選択すると、前のセクションで定義した**マルチサイト ルーティング ループバック IP 範囲**から次に使用可能なアドレスが割り当てられます。

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

ステップ 7 右に **<*border-gateway*>** サイドバーの設定で、**コントロール プレーン TEP** と**データ プレーン TEP**を指定します。

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

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



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

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

- **[MTU]** フィールドに、サーバーの MTU を入力します。

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

  [継承 (inherit)] を指定することも、576 ～ 9000 の値を指定することもできます。

- **BGP認証**の場合は、[なし (None)] または [シンプル (Simple (MD5))] を選択できます。

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

インフラ設定の展開

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

始める前に

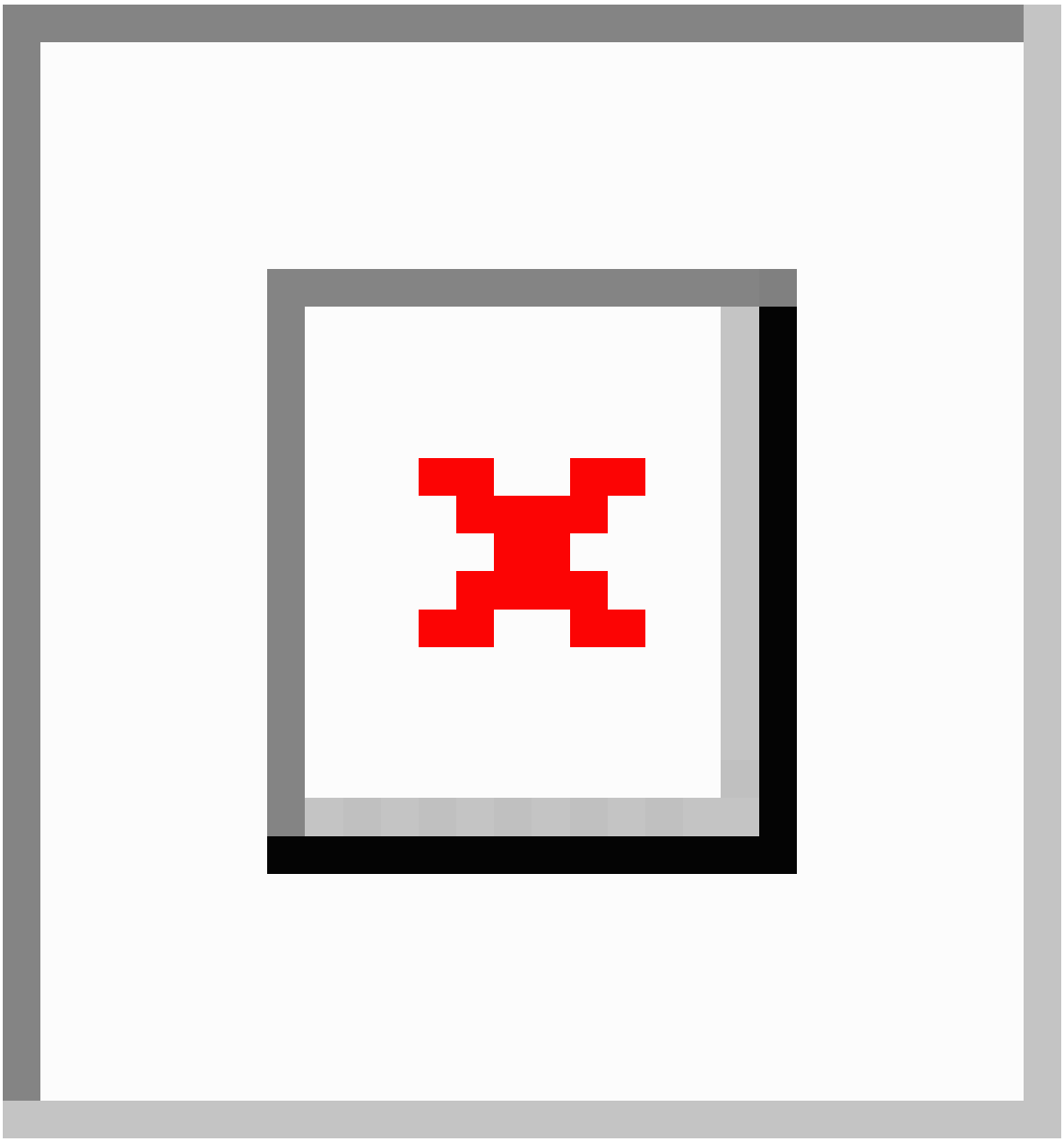
この章の前のセクションで説明したように、全般的な、およびサイト固有のインフラ設定を完了している必要があります。

ステップ 1 設定の競合がないことを確認するか、必要に応じて解決します。

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

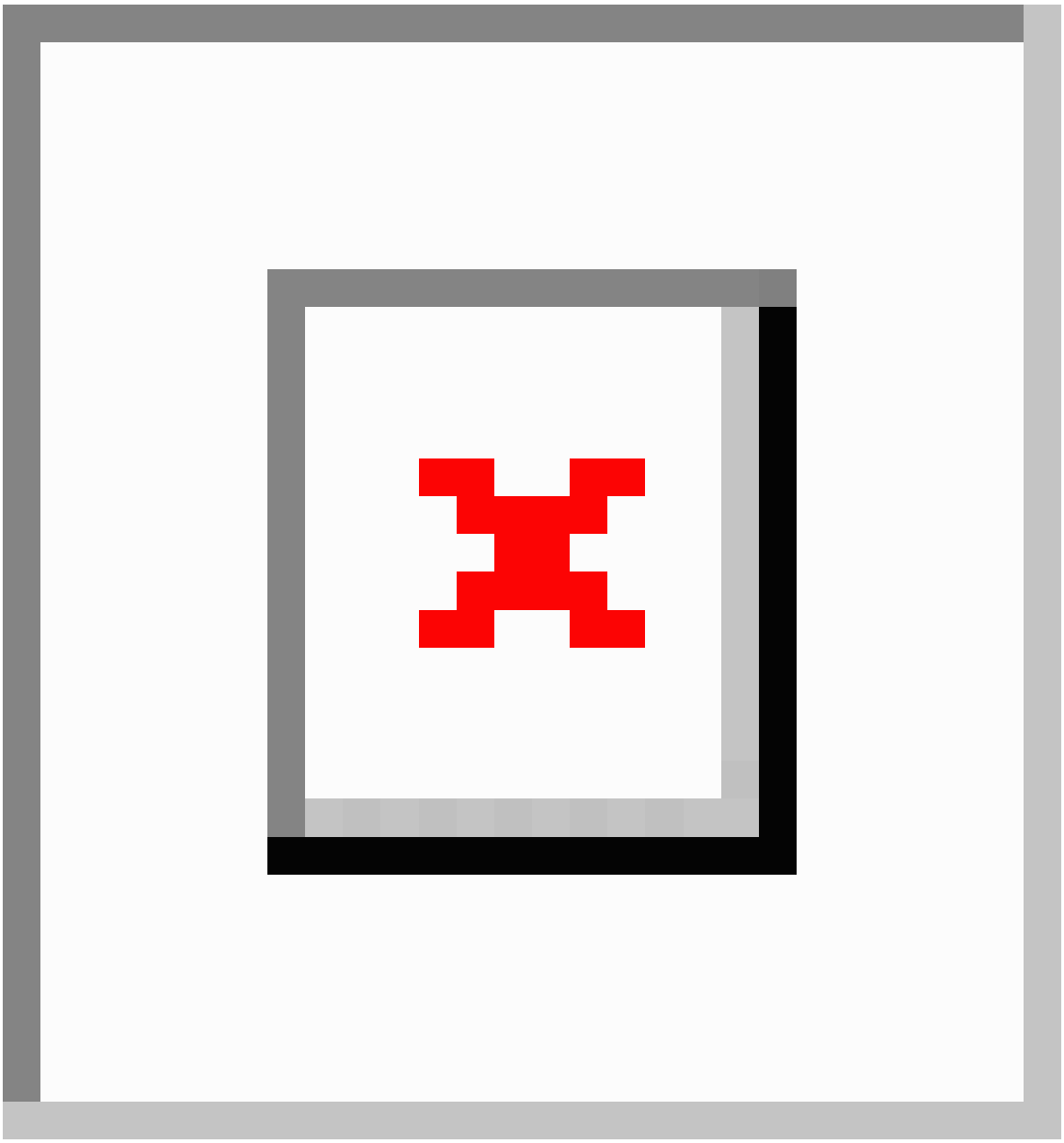
設定が競合する場合：

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



b) 競合の原因となっている特定の設定を書き留めます。

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



c) [X] ボタンをクリックしてレポートを閉じ、インフラ設定画面を終了します。
d) サイトの削除 （28 ページ）の説明に従って、MSO でサイトの管理を解除します。

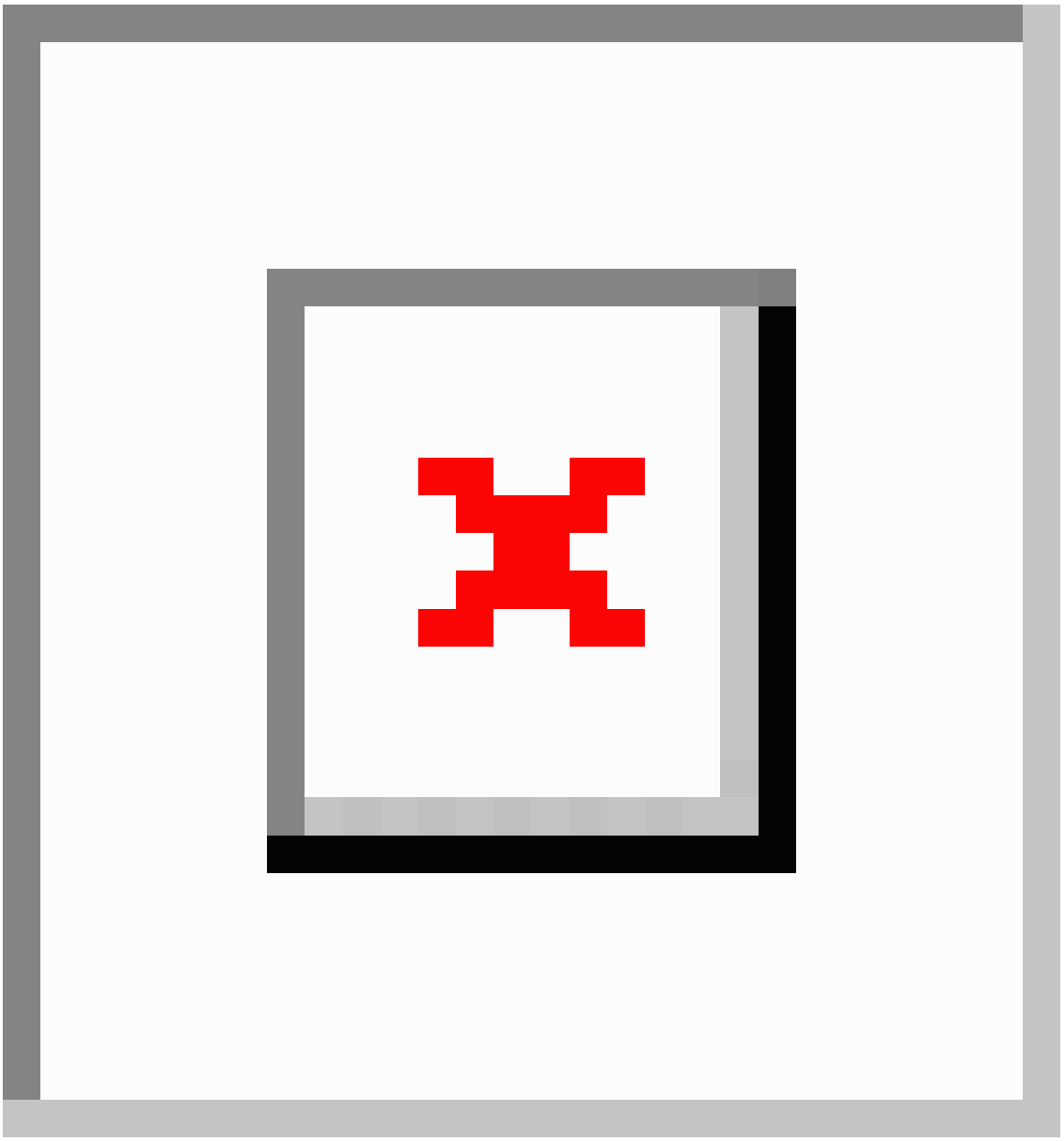
Nexus ダッシュボードからサイトを削除する必要はありません。MSO GUI でサイトの管理を解除するだけです。

e) 既存の設定の競合を解決します。
f) Cisco DCNM サイトの追加 （41 ページ）の説明に従って、サイトを再度管理状態にします。

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

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

ステップ 2 設定を展開します。



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

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

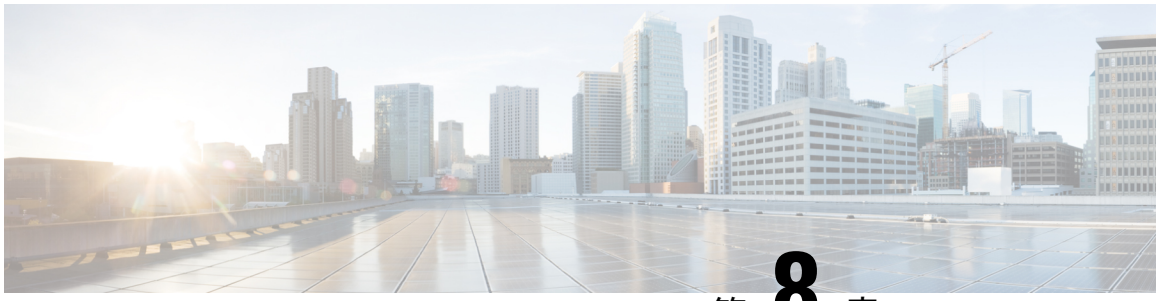
b) 設定が展開されるのを待ちます。

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

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

第 III 部

マルチサイトオーケストレータアプリケーションのアップグレードまたはダウングレード



第 8 章

MSO アプリケーションのアップグレードまたはダウングレード

概要

ここでは、Cisco Nexus Dashboard に導入されている Cisco マルチサイト オーケストレータ リリース 3.2（1）以降をアップグレードまたはダウングレードする方法について説明します。

VMware ESX VM または Cisco アプリケーション サービス エンジンに導入されている以前のリリースを実行している場合は、マルチサイト オーケストレータ 導入ガイドの「*Nexus* ダッシュボードへの既存のクラスタの移行」の章の説明に従って、新しいクラスタを導入し、既存のクラスタから設定を転送する必要があります。

前提条件とガイドライン

Cisco Nexus マルチサイト オーケストレータ クラスタをアップグレードまたはダウングレードする前に、次の手順を実行します。

- リリース 3.2（1）より前のリリースからのステートフルアップグレードはサポートされていないため、クラスタを再展開し、既存の構成バックアップを復元する必要があります。
- 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 クラスタの状態は、次の 2 つの方法のいずれかで確認できます。

  - Nexus ダッシュボード GUI にログインし、**[システム概要（System Overview）]** ページでシステムステータスを確認します。

- いずれかのノードに直接 rescue-user としてログインし、次のコマンドを実行します。

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

- 現在の マルチサイト オーケストラが正常に動作していることを確認します。
- MSO アプリケーションのアップグレードは次のいずれかの方法で実行できます。
  - Cisco App Store を使用した MSO アプリケーションのアップグレード （62 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。

    App Storeでは、アプリケーションの最新バージョンにのみアップグレードできることに注意してください。

  - MSO アプリケーションを手動でアップグレード （65 ページ）で説明されているようにこのセクションの説明に従って、新しいアプリケーションイメージを手動でアップロードします。

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

- ダウングレード ワークフローは手動アップグレード プロセスに似ており、MSO アプリケーションのダウングレード （68 ページ）で説明されています。
- リリース 3.2（1）より前のリリースへのダウングレードはサポートされていません。

  以前のリリースにダウングレードする場合は、そのリリースでサポートされているプラットフォームに新しい マルチサイト オーケストレータ クラスタを展開し、古い設定のバックアップを復元する必要があります。リリース 3.2（1）以降で作成されたバックアップを古い MSO クラスタに復元することはサポートされていません。

Cisco App Store を使用した MSO アプリケーションのアップグレード

ここでは、Cisco マルチサイト オーケストレータ リリース 3.2（1）以降をアップグレードする方法について説明します。

始める前に

- 前提条件とガイドライン （61 ページ）で説明している前提条件をすべて満たしていることを確認します。

- Cisco DC App Center が Nexus ダッシュボードから管理ネットワーク経由で直接、またはプロキシ設定を使用して到達可能であることを確認します。

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

ステップ 1 Nexus Dashboard にログインします。

ステップ 2 左のナビゲーションメニューから **[サービス カタログ (Service Catalog)]** を選択します。

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

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

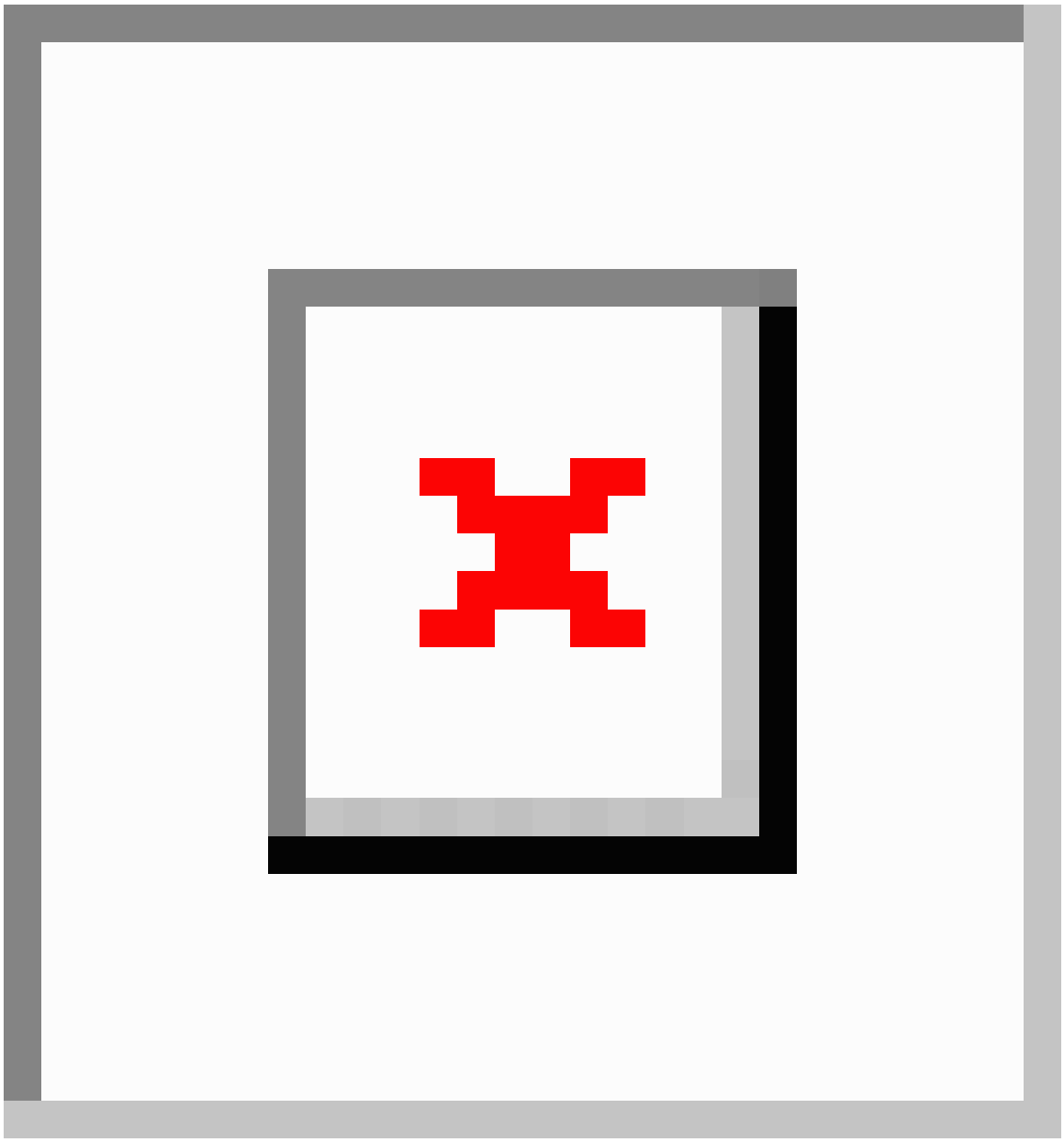
b) **[マルチサイト オーケストレータ（Multi-Site Orchestrator）]**タイルで、**[アップグレード（Upgrade）]** をクリックします。

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

ステップ 4 新しいイメージが初期化されるまで待ちます。

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

ステップ 5 新しい画像をアクティブにします。



a) **[サービス カタログ (Service Catalog)]** 画面で、**[インストール済みサービス (Installed Services)]** タブを選択します。
b) マルチサイト オーケストレータ 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、現在実行中のアプリケーション バージョンに必要なアップグレード ワークフローを実行します。

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

ステップ 6 （任意）古いアプリケーション イメージを削除します。

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

a) **[サービス カタログ (Service Catalog)]** 画面で、**[インストール済みサービス (Installed Services)]** タブを選択します。
b) マルチサイト オーケストレータ 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。

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

ステップ 7 アプリを起動します。

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

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

MSO アプリケーションを手動でアップグレード

ここでは、Cisco マルチサイト オーケストレータ リリース 3.2（1）以降をアップグレードする方法について説明します。

始める前に

- 前提条件とガイドライン （61 ページ）で説明している前提条件をすべて満たしていることを確認します。

ステップ 1 ターゲットのリリース イメージをダウンロードします。

a) マルチサイト オーケストレータ アプリケーション DC App Center ページを参照します：https://dcappcenter.cisco.com/multi-site-orchestrator.html
b) **[バージョン (Version)]** ドロップダウンから、インストールするバージョンを選択し、**[ダウンロード (Download)]** をクリックします。
c) ライセンス契約に同意し、イメージをダウンロードします。

ステップ 2 Nexus Dashboard にログインします。

ステップ 3 Nexus ダッシュボードにイメージをアップロードします。

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

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

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

e) ファイルを選択します。

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

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

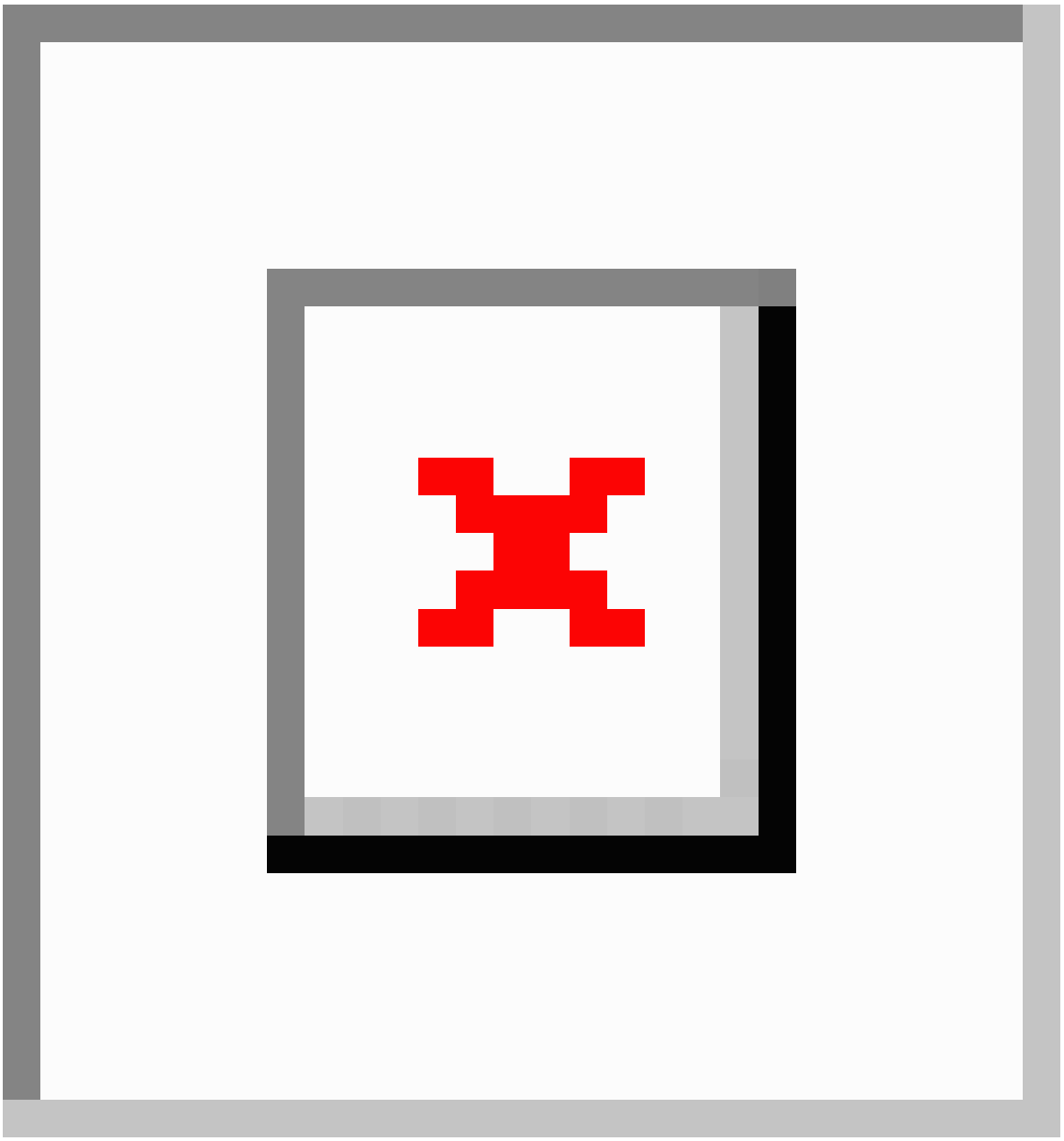
f) **[アップロード (Upload)]** をクリックして、アプリケーションをクラスタに追加します。

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

ステップ 4 新しいイメージが初期化されるまで待ちます。

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

ステップ 5 新しい画像をアクティブにします。



a) **[サービス カタログ (Service Catalog)]** 画面で、**[インストール済みサービス (Installed Services)]** タブを選択します。
b) マルチサイト オーケストレータ 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、現在実行中のアプリケーション バージョンに必要なアップグレード ワークフローを実行します。

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

ステップ 6 （任意）古いアプリケーション イメージを削除します。

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

a) **[サービス カタログ (Service Catalog)]** 画面で、**[インストール済みサービス (Installed Services)]** タブを選択します。
b) マルチサイト オーケストレータ 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。

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

ステップ 7 アプリを起動します。

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

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

MSO アプリケーションのダウングレード

ここでは、Cisco マルチサイト オーケストレータ リリース 3.2（1）以降をダウングレードする方法について説明します。

ダウングレードワークフローはアップグレードワークフローに似ており、ターゲットのリリース イメージをアップロードし、以下で説明するように、現在実行中のアプリケーション バージョンを新しいイメージに切り替えます。

始める前に

- リリース 3.2（1）より前のリリースへのダウングレードはサポートされていません。

  以前のリリースにダウングレードする場合は、そのリリースでサポートされているプラットフォームに新しい マルチサイト オーケストレータ クラスタを展開し、古い設定のバックアップを復元する必要があります。リリース 3.2（1）以降で作成されたバックアップを古い MSO クラスタに復元することはサポートされていません。

- 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。前提条件とガイドライン （61 ページ）

ステップ 1 ターゲットのリリース イメージをダウンロードします。

a) マルチサイト オーケストレータ アプリケーション DC App Center ページを参照します：https://dcappcenter.cisco.com/multi-site-orchestrator.html

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

c) ライセンス契約に同意し、イメージをダウンロードします。

ステップ 2 Nexus Dashboard にログインします。

ステップ 3 Nexus ダッシュボードにイメージをアップロードします。

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

b) Nexus ダッシュボードの **[サービス カタログ (Service Catalog)]** 画面で、**[インストール済みサービス (Installed Services)]** タブを選択します。

c) メインペインの右上にある **[アクション (Actions)]** メニューから、**[アプリケーションのアップロード (Upload App)]** を選択します。

d) **[アプリケーションのアップロード (Upload App)]** ウィンドウで、イメージの場所を選択します。

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

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

e) ファイルを選択します。

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

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

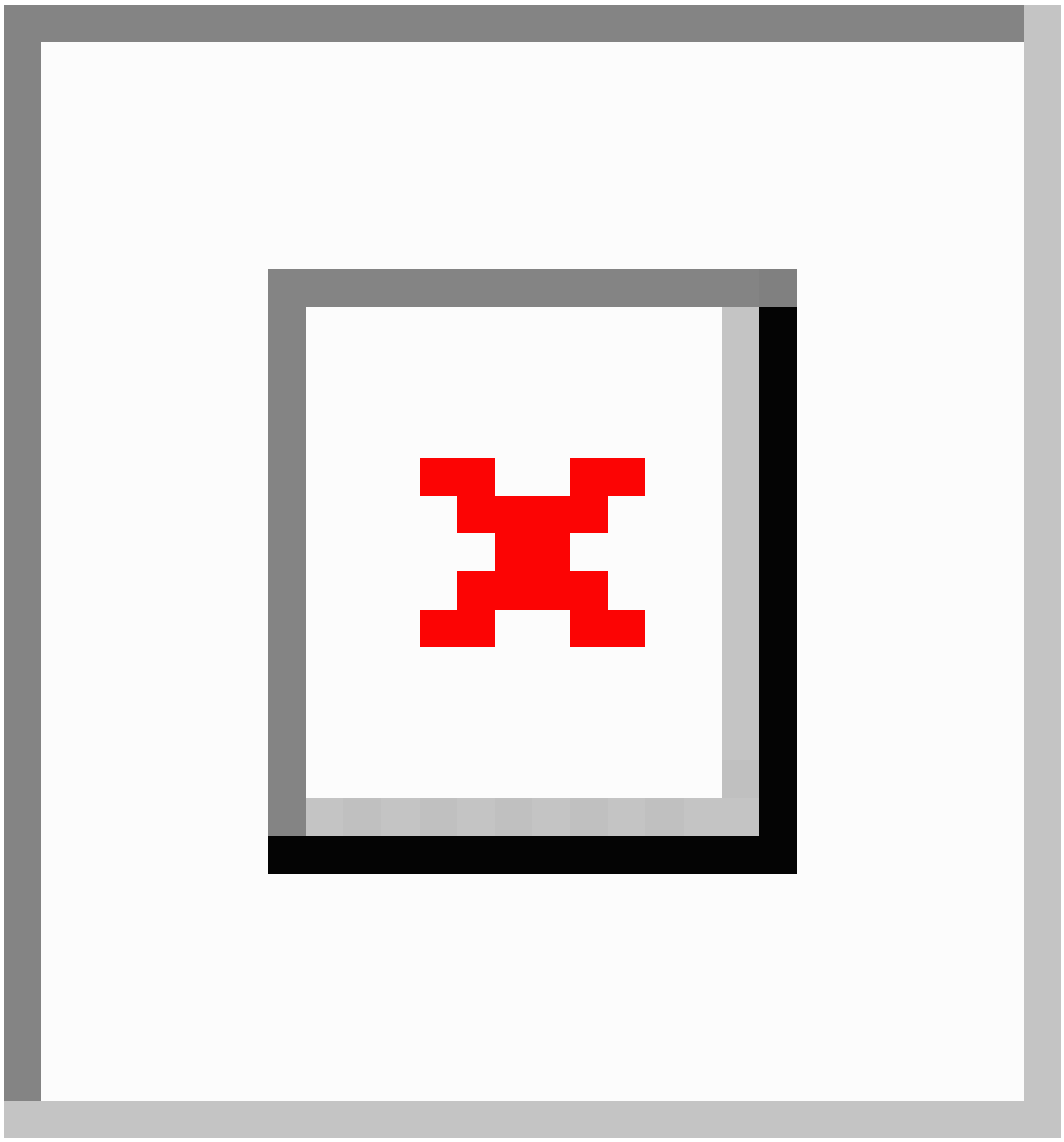
f) **[アップロード (Upload)]** をクリックして、アプリケーションをクラスタに追加します。

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

ステップ 4 新しいイメージが初期化されるまで待ちます。

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

ステップ 5 新しい画像をアクティブにします。



a) **[サービス カタログ (Service Catalog)]** 画面で、**[インストール済みサービス (Installed Services)]** タブを選択します。
b) マルチサイト オーケストレータ 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、現在実行中のアプリケーション バージョンに必要なダウングレード ワークフローを実行します。

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

ステップ 6 （任意）古いアプリケーション イメージを削除します。

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

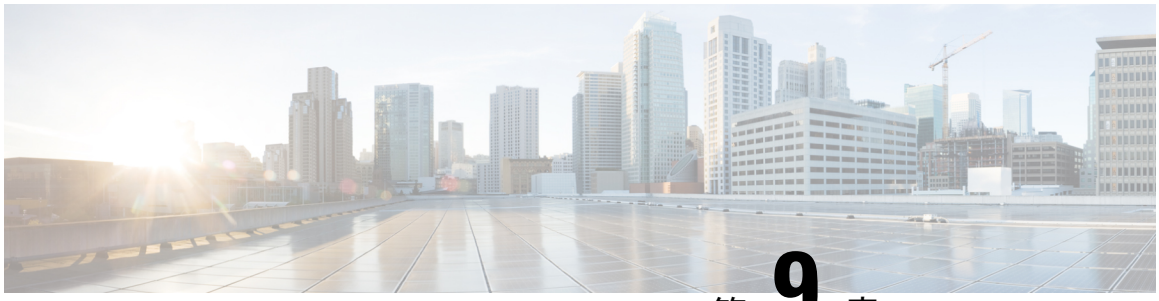
a) **[サービス カタログ (Service Catalog)]** 画面で、**[インストール済みサービス (Installed Services)]** タブを選択します。
b) マルチサイト オーケストレータ タイルの右上にあるメニュー（...）をクリックし、**[利用可能なバージョン（Available Versions）]** を選択します。
c) 使用可能なバージョンのウィンドウで、削除するイメージの横にある削除アイコンをクリックします。

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

ステップ 7 アプリを起動します。

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

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



第 9 章

Nexus ダッシュボードへの既存のクラスタの移行

Nexus ダッシュボードへの既存のクラスタの移行

リリース 3.2（1）以降、マルチサイト オーケストレータ は Cisco Nexus ダッシュボードのアプリケーションとして展開する必要があります。以前サポートされていた VMware ESX 仮想アプライアンスおよび Cisco Application Services Engine フォームファクタのサポートは廃止されました。

次のサブセクションでは、VMware ESX VM または Cisco アプリケーション サービス エンジンに導入されている既存の Cisco マルチサイト オーケストレータを Cisco Nexus ダッシュボードに移行する方法について説明します。

すでに Cisco Nexus ダッシュボードで MSO クラスタを展開している場合は、代わりに 概要 （61 ページ） に記載されている手順に従ってください。

前提条件とガイドライン

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

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

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

  構成のバックアップを作成する時に使用します。そして、Nexus Dashboard 内の新しく展開した MSO アプリケーション内にインポートします。
- ファブリックが Cisco APIC リリース 4.2（4）以降にアップグレードされていることを確認してください。

  サイト管理は、MSO UI から、リリース 4.2（6）以降をサポートする Nexus ダッシュボード共通サイト管理に移動しました。ファブリックのアップグレードの詳細については、*Cisco APIC Installation, Upgrade, and Downgrade Guide* を参照してください。
- *Cisco Nexus* ダッシュボード導入ガイドの説明に従って、新しい Nexus ダッシュボード クラスタを導入し、ファブリック接続を設定します。

  Nexus Dashboard へのアップグレードを計画している MSO アプリケーションを含む既存のアプリケーション サービス エンジン クラスタがある場合は、最初に、そこで実行されている MSO アプリケーションを無効にしてアンインストールする必要があります。次に、*Cisco Nexus* ダッシュボード導入ガイドの説明に従って、クラスタを Nexus ダッシュボードにアップグレードできます。
- マルチサイト オーケストレータを展開 （3 ページ）の説明に従って、Nexus ダッシュボードに MSO アプリケーションをインストールします。

  同じ Nexus ダッシュボード クラスタで複数のアプリケーションを共同ホストすることを計画している場合は、クラスタ サイズがファブリック サイズとアプリケーション数に基づいて適切にスケーリングされていることを確認する必要があります。Cisco Nexus ダッシュボード キャパシティ プランニング ツールは、特定のユース ケースに必要なクラスタ サイズを提供できます。MSO アプリケーションの付属をサポートするためにクラスタを拡張する必要がある場合は、追加のワーカー ノードの展開について、*Cisco Nexus* ダッシュボード ユーザー ガイドを参照してください。
- MSO アプリケーションから管理したいすべてのサイトが Nexus ダッシュボードに組み込まれていることを確認してください。

  サイト管理は、MSO UI から Nexus ダッシュボードの共通サイト管理に移動されました。したがって、サイトの追加と削除 （23 ページ） に説明されているように、既存の設定を新しいクラスタに移行する前に、同じサイトと Nexusダッシュボードと同じ名前を使用して GUI にオンボードする必要があります。バックアップに存在するサイトが Nexus ダッシュボードに存在しない場合、復元は失敗し、`[復元前チェックに失敗しました（Pre-restore check failed）]`というエラー メッセージが表示されます。

（注） Nexus ダッシュボードにサイトを追加した後は、MSO アプリケーションでそれらを[管理対象（Managed）]に設定しないでください。バックアップから設定を復元すると、サイトの管理が自動的に有効になります。

- MSO で構成したすべてのリモート ユーザーが Nexus ダッシュボードに追加されていることを確認します。

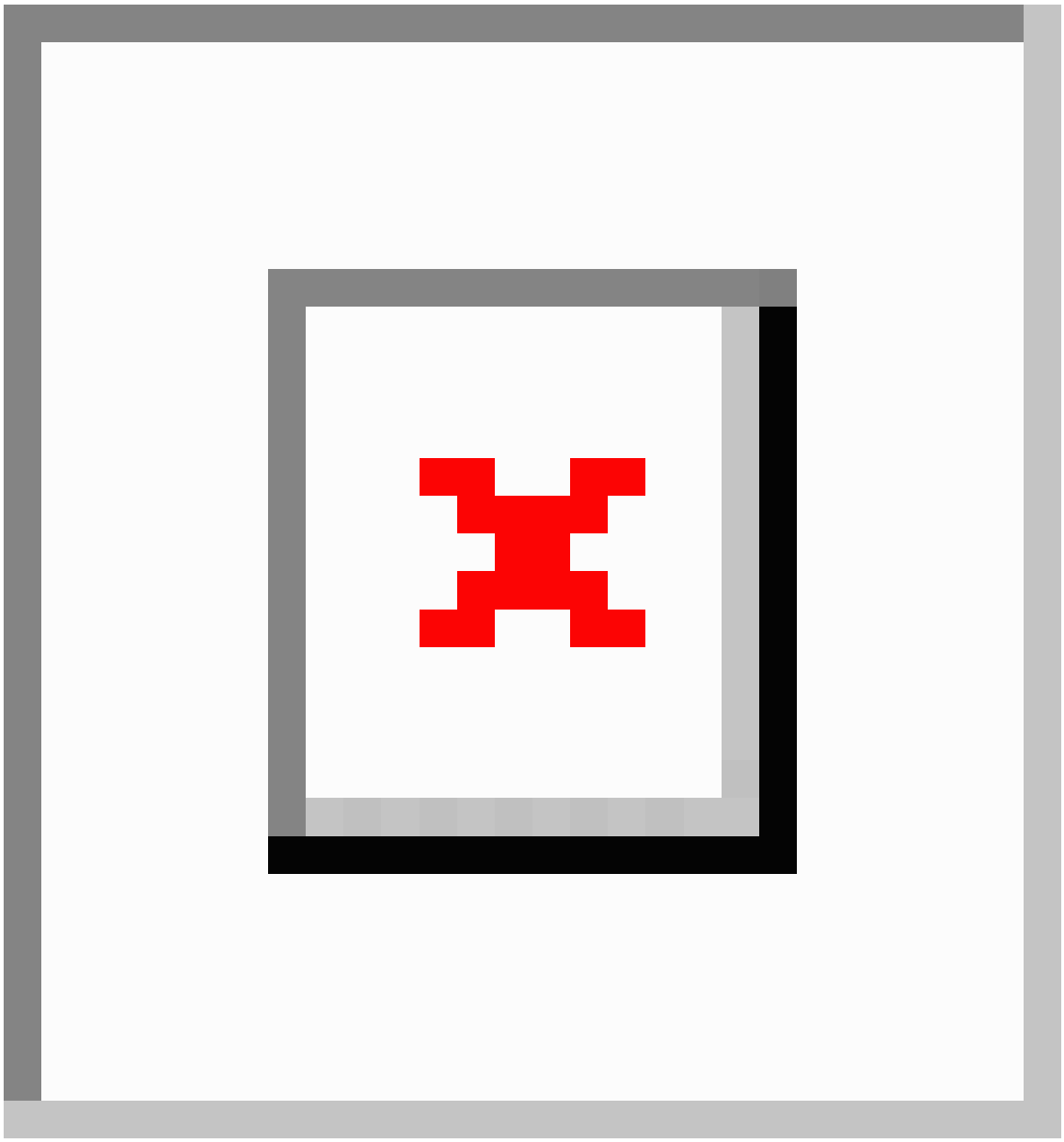
  ユーザー管理は、MSO UI から Nexus ダッシュボードの共通ユーザー管理に移動されました。そのため、*Cisco Nexus Dashboard User Guide* の説明に従って、同じリモート ユーザーと認証サーバーを Nexus ダッシュボードに追加する必要があります。

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

既存のクラスタ設定のバックアップ

この項では、既存のクラスタの設定をバックアップする方法について説明します。

ステップ 1 既存の展開設定をバックアップします。



a) 既存の Multi-Site Orchestrator にログインします。
b) 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。
c) メイン ウィンドウ ペインで、**[新規バックアップ (New Backup)]** をクリックします。

[新規バックアップ (New Backup)] ウィンドウが開きます。

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

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

e) **[バックアップの場所 (Bacjup Location)]**を選択します。

バックアップファイルは、Orchestrator ノードにローカルに保存するか、またはリモート ロケーションにエクスポートすることができます。リモート ロケーションへのバックアップを選択した場合は、リモート ロケーションがすでに MSO で構成されている必要があることに注意してください。

バックアップ ファイルをローカルに保存する場合は、**[ローカル (Local)]** を選択します。

それ以外で、バックアップ ファイルをリモートの場所に保存するには、**[リモート (Remote)]** を選択して次の情報を入力します。

- **[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。
- **[リモートパス (Remote Path)]** では、デフォルトのターゲット ディレクトリのままにするか、またはパスに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) **[保存（Save）]** をクリックして、バックアップを作成します。

ステップ 2 既存のオーケストレータからバックアップファイルをコピーします。

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

メイン ウィンドウで、ダウンロードするバックアップの隣のアクション()アイコンをクリックし、**[ダウンロード (Download)]** を選択します。これにより、バックアップ ファイルがシステムにダウンロードされます。

新しいクラスタを展開して構成を復元する

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 MSO アプリケーションを展開して設定する方法について説明します。

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

新しいクラスタが展開され、構成が復元されるまで、既存の MSO クラスタを保持することをお勧めします。

ステップ 2 新しい Nexus ダッシュボード クラスタが稼働中であり、MSO アプリケーションがインストールされていることを確認します。

MSOアプリケーションは、新規インストールで、サイトまたはポリシーの設定を変更していないものであることが必要です。

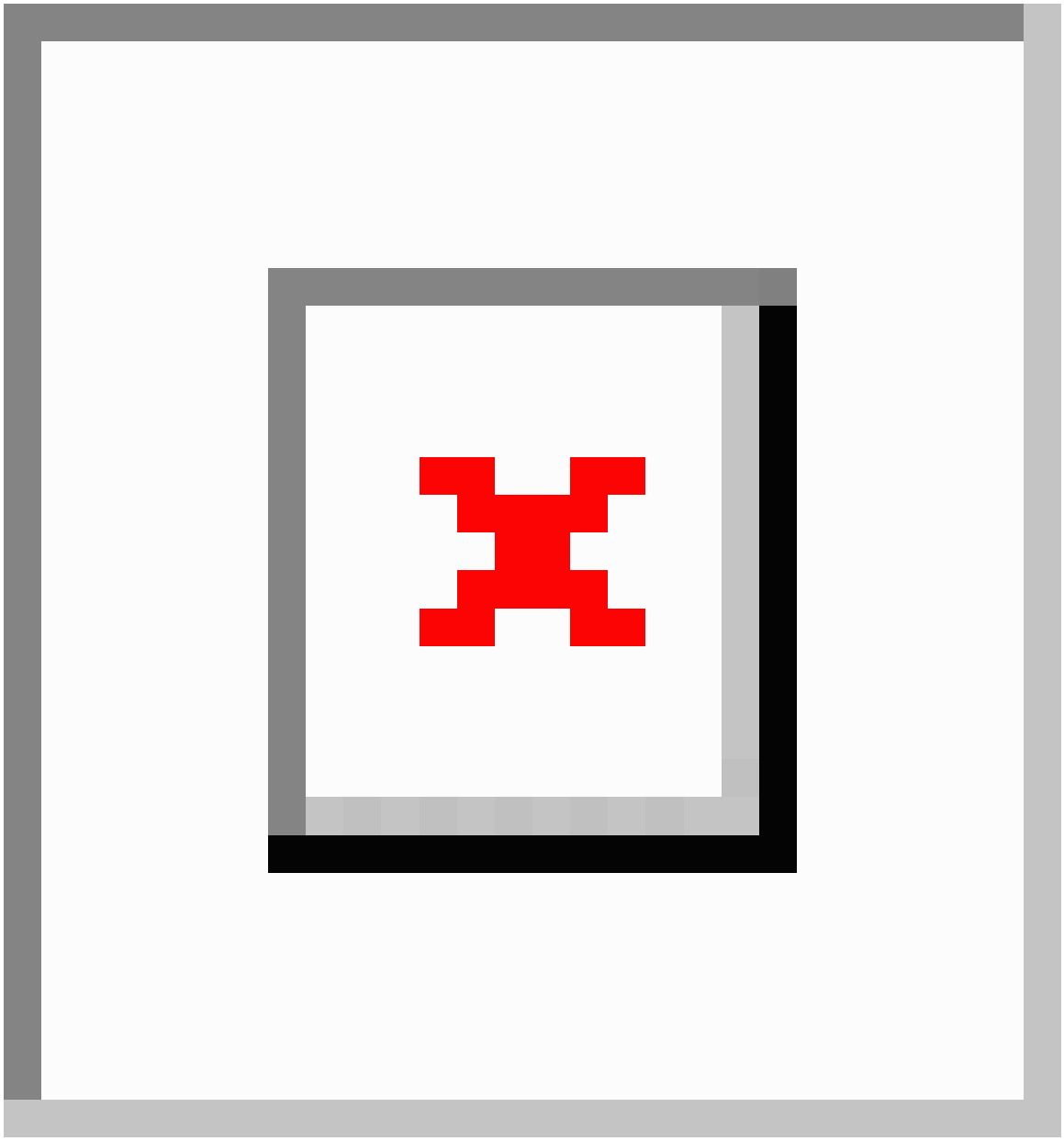
ステップ 3 Nexus Dashboard の GUI にログインします。

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

バックアップを復元すると、MSOは、バックアップ内のすべてのサイトが、一致するサイト名とタイプでNexus ダッシュボードに存在することを検証します。検証が失敗した場合、たとえば、Nexus Dashboardでサイトがオンボードされていない場合、設定の復元は失敗します。再試行の前にサイトをオンボードする必要があります。オンボーディングサイトについては、サイトの追加と削除 （23 ページ） を参照してください。

ステップ 5 新しい Nexus Dashboardに展開されたオーケストレータ クラスタにバックアップ ファイルをインポートします。

バックアップをローカルに保存した場合は、ファイルをインポートするだけです：



a) 新しいマルチサイト オーケストレータ アプリケーションを開きます。

b) 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。
c) メイン ウィンドウで、[**インポート (Import)**] をクリックします。
d) 開いた [**ファイルからのインポート (Import from file)**] ウィンドウで、[**ファイルを選択 (Select File)**] を選択して、インポートするバックアップ ファイルを選択します。

バックアップのインポートは、[**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。

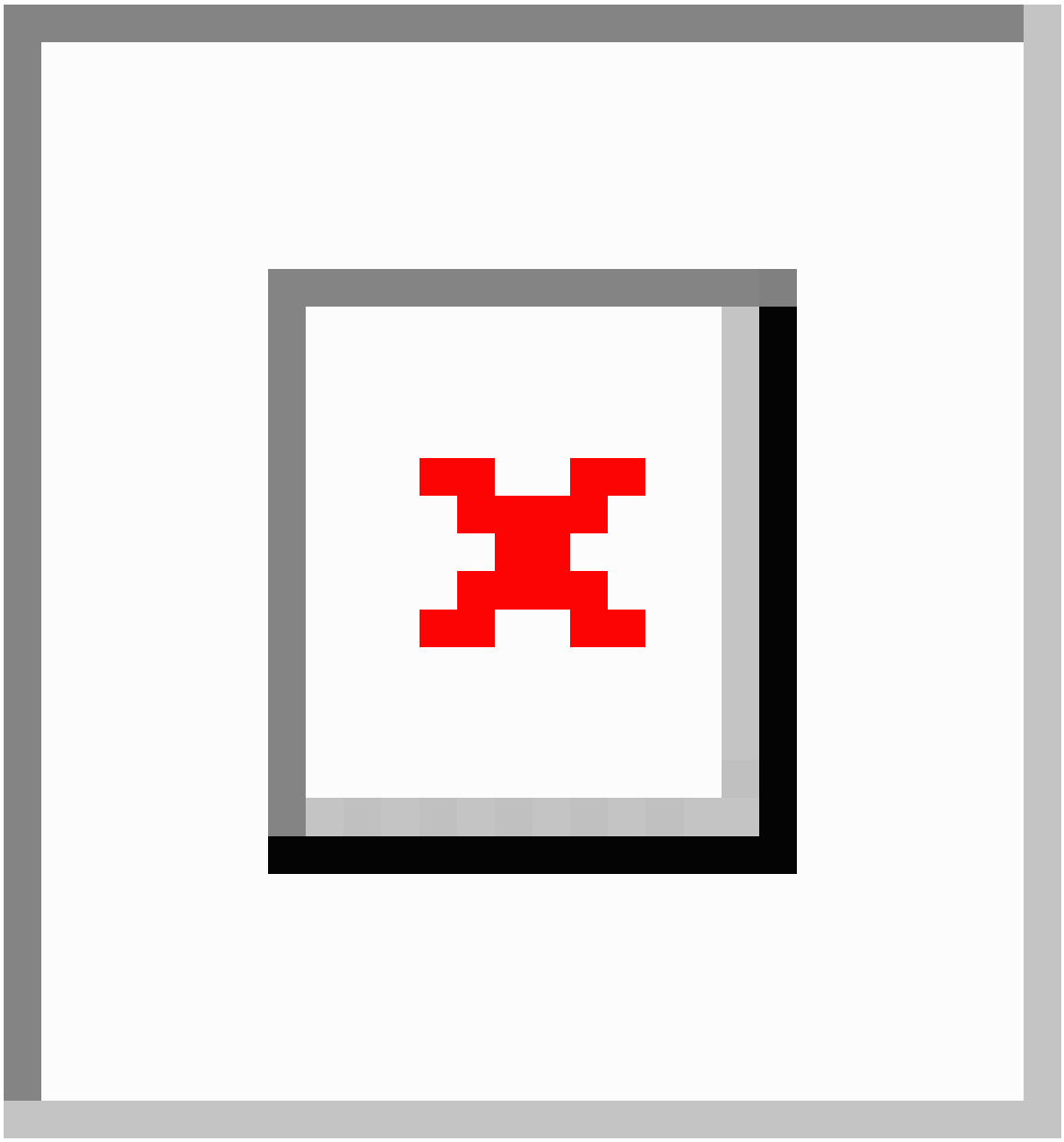
バックアップをリモートの場所に保存した場合は、そのリモートの場所を新しいマルチサイト オーケストレータに追加します。

a) 新しい マルチサイト オーケストレータ アプリケーションを開きます。
b) 左側のナビゲーション ペインで、**[管理（Admin）]** > **[リモート ロケーション（Remote Locations）]** を選択します。
c) 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。

d) 古いオーケストレータで使用したのと同じ情報をリモート ロケーションに提供します。
e) [**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 6 設定を復元します。



a) 左のナビゲーション メニューから**[管理者（Admin）]** > **[バックアップ（Backups）]**を選択します。

b) 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。

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

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

設定をインポートして復元すると、いくつかのサービスが再起動されます。

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。