



展開の概要と要件

- [デプロイ概要 \(1 ページ\)](#)
- [前提条件とガイドライン \(4 ページ\)](#)
- [通信ポート \(18 ページ\)](#)
- [ファブリック接続 \(36 ページ\)](#)
- [サイト間のノード分散 \(42 ページ\)](#)
- [サービスのコロケーションの使用例 \(46 ページ\)](#)
- [インストール前のチェックリスト \(48 ページ\)](#)

デプロイ概要

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。



- (注) このドキュメントでは、ベースクラスタの初期設定について説明します。クラスタが稼働したら、『[Cisco Nexus Dashboard User Guide](#)』の説明に従って追加ノードを設定して展開できます。このガイドは、Nexus Dashboard GUI から直接入手することもできます。

ハードウェアとソフトウェアのスタック

Nexus Dashboardは、ソフトウェアフレームワーク (Nexus Dashboard) がプリインストールされた、特殊なCisco UCSサーバ (Nexus Dashboardプラットフォーム) のクラスタとして提供されます。Cisco Nexus ダッシュボードソフトウェアスタックは、ハードウェアから分離して、多数の仮想フォームファクタで展開できます。このドキュメントでは、「Nexus Dashboard platform」はハードウェアを指し、「Nexus Dashboard」はソフトウェアスタックとGUIコンソールを指します。

このガイドでは、Nexus ダッシュボードソフトウェアの初期導入について説明します。ハードウェアのセットアップについては『[Nexus Dashboard Hardware Setup Guide](#)』で説明しています。その他の Nexus ダッシュボードの操作手順については、『[Cisco Nexus Dashboard User Guide](#)』を参照してください。

[サービス (Services)]

Nexus ダッシュボードは、一貫した統一された方法ですべての Nexus ダッシュボード製品を使用できるようにするサービスを構築および展開するための標準のアプライアンスプラットフォームです。Insights、Orchestrator、Fabric Controller、Data Broker などのサービスをサブスクリブして使用するには、Nexus ダッシュボードプラットフォームを使用して、これらのサービスに必要な容量とライフサイクル管理操作を提供します。

通常、Nexus ダッシュボードプラットフォームには、これらのサービスのライフサイクルを管理するために必要なソフトウェアのみが同梱されていますが、実際のサービスはアプライアンスにパッケージ化されていません。データセンターからのパブリック ネットワーク接続を許可している場合は、数回クリックするだけでサービスをダウンロードしてインストールできます。ただし、パブリック ネットワークに接続していない場合は、これらのサービスを手動でダウンロードしてプラットフォームにアップロードし、インストール操作を実行してから使用する必要があります。

物理的な Nexus ダッシュボードサーバを購入する場合、Nexus ダッシュボード Insights および Nexus Dashboard Orchestrator サービスを、出荷前にハードウェアに事前インストールすることを選択できます。詳細については、『[Nexus ダッシュボードの注文ガイド](#)』を参照してください。Nexus ダッシュボードの仮想またはクラウドフォームファクターを展開している場合、サービスのインストールに変更はなく、クラスタの準備が整った後にサービスを個別に展開する必要があることに注意してください。

利用可能なフォームファクタ

Cisco Nexus Dashboardのこのリリースは、さまざまなフォームファクタを使用して展開できます。ただし、すべてのノードに同じフォームファクタを使用する必要があります。同じクラスタ内で異なるフォームファクタを混在させることはサポートされていません。

- Cisco Nexus ダッシュボード物理アプライアンス (.iso)

このフォームファクタは、Cisco Nexus Dashboardソフトウェアスタックがプレインストールされた状態で購入した元の物理アプライアンスハードウェアを指します。

このドキュメントの後半のセクションでは、既存の物理アプライアンスハードウェアでソフトウェアスタックを設定してクラスタを展開する方法について説明します。元の Cisco Nexus ダッシュボードプラットフォームハードウェアのセットアップについては、『[Cisco Nexus Dashboard Hardware Setup Guide](#)』を参照してください。

- VMware ESX (.ova)

3つのVMware ESX仮想マシンを使用してNexusダッシュボードクラスタを展開できる仮想フォームファクタ。

- Linux KVM (.qcow2)

3つのLinux KVM仮想マシンを使用してNexusダッシュボードクラスタを展開できる仮想フォームファクタ。

- Amazon Web Services (.ami)

3つのAWSインスタンスを使用してNexusダッシュボードクラスタを展開できるクラウドフォームファクタ。

- Microsoft Azure (.arm)

3つの Azure インスタンスを使用して Nexus ダッシュボードクラスタを展開できるクラウドフォームファクタ。

- 既存のRed Hat Enterprise Linux(RHEL)システムの場合

リリース2.2(1)以降、既存のRed Hat Enterprise LinuxサーバーでNexus Dashboardノードを実行できます。

以前のバージョンの Nexus ダッシュボードからのアップグレード

すでに Nexus ダッシュボード リリース 2.0.1 以降を実行している場合は、[Nexus ダッシュボードのアップグレード](#)の説明に従って、クラスタ設定とアプリケーションを保持したまま、最新リリースに直接アップグレードできます。

Application Services Engineからのアップグレード

Cisco Application Services Engine を実行している場合は、Nexus ダッシュボード リリース 2.1(x) 以降にアップグレードする前に、[Cisco Nexus ダッシュボード展開ガイド](#)、[リリース 2.0\(x\)](#)の説明に従って、Nexus ダッシュボード リリース 2.0(2g) にアップグレードする必要があります。

クラスタのサイジングと可用性の注意事項

前述のように、各 Nexus ダッシュボード クラスタは、最初に 1 つまたは 3 つのマスター ノードを使用してデプロイされます。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ことが必要な場合があります。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 Cluster Sizing](#)』を参照してください。



- (注)
- 単一ノードクラスターは、限られた数のサービスでサポートされており、最初の展開後に3ノードクラスターに拡張することはできません。
 - 追加のワーカーノードをサポートするのは3ノードクラスターのみです。
 - 単一ノードクラスターをデプロイし、それを3ノードクラスターに拡張するか、ワーカーノードを追加する場合は、基本の3ノードクラスターとして再デプロイする必要があります。
 - 3ノードクラスターの場合、クラスターが動作し続けるには、少なくとも2つのマスターノードが必要です。2つのマスターノードに障害が発生した場合、クラスターはオフラインの読み取り専用モードになり、回復するまで使用できません。その点は[Cisco Nexus ダッシュボード ユーザー ガイド](#)で説明されています。

最初のクラスターが稼働したら、[Cisco Nexus ダッシュボード ユーザー ガイド](#)の説明に従って追加ノードを設定して展開できます。このガイドは、Nexus ダッシュボード GUI から直接利用することもできます。

サポートされるサービス

サポートされるアプリケーションと関連する互換性および相互運用性情報の完全なリストについては、『[Nexus ダッシュボードおよびサービスの互換性マトリクス](#)』を参照してください。

前提条件とガイドライン

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（到達不能またはプレースホルダ 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。

Nexus ダッシュボード外部ネットワーク

Cisco Nexus ダッシュボードは、各サービス ノードを2つのネットワークに接続するクラスタとして展開されます。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。

Nexus ダッシュボードにインストールされた個々のサービスは、追加の目的で2つのネットワークを使用する場合があるため、展開計画については、このドキュメントに加えて特定のサービスのドキュメントを参照することを推奨します。

表 1:外部ネットワークの目的

Data Network	管理ネットワーク
<ul style="list-style-type: none"> • Nexus Dashboard ノードのクラスタリング • サービス間通信 • Cisco APIC、クラウド ネットワーク コントローラ、および NDFC/DCNM 通信への Nexus Dashboard ノード <p>たとえば、Nexus ダッシュボード Insights などのサービスのネットワーク トラフィックです。</p>	<ul style="list-style-type: none"> • Nexus ダッシュボード GUI へのアクセス • SSH を介した Nexus ダッシュボード CLI へのアクセス • DNS および NTP 通信 • Nexus Dashboard ファームウェアのアップロード • Cisco DC App Center (AppStore) へのアクセス <p>Nexus ダッシュボード App Store を使用してアプリケーションをインストールする場合は、https://dcappcenter.cisco.com は管理ネットワーク経由で到達可能である必要があります</p> <ul style="list-style-type: none"> • Intersight デバイス コネクタ

2つのネットワークには次の要件があります。

- すべての新しい Nexus Dashboard 展開では、管理ネットワークとデータネットワークが異なるサブネットに存在する必要があります。
- 物理クラスタの場合、管理ネットワークは各ノードの CIMI に対して、TCP ポート 22/443 を介して IP 到達可能性を提供する必要があります。

Nexus Dashboardのクラスタ設定では、各ノードのCIMC IPアドレスを使用してノードを設定します。

- Nexus ダッシュボード Insights サービスの場合、データ ネットワークは、各ファブリック および APIC のインバンド ネットワークに IP 到達可能性を提供する必要があります。
- Nexus Dashboard Insights と AppDynamics の統合では、データ ネットワークが AppDynamics コントローラに IP 到達可能性を提供する必要があります。

- Nexus Dashboard Orchestrator サービスの場合、データネットワークは、Cisco APIC サイトに対してインバンドおよび/またはアウトオブバンド IP 到達可能性を持ちますが、Cisco DCNM サイトに対してはインバンド到達可能性が必要です。
- データ ネットワーク インターフェイスで、Nexus Dashboard トラフィックに使用できる最小 MTU が 1500 である必要があります。
必要に応じて、高いMTUを設定できます。
- 次の表は、管理ネットワークとデータネットワークのサービス固有の要件をまとめたものです。



- (注) データサブネットを変更するにはクラスタを再展開する必要があります。そのため、今後の追加サービスを考慮して、ノードとサービスの必要最低限よりも大きなサブネットを使用することをお勧めします。このセクションに記載されている要件に加えて、展開を計画している特定のサービスのリリースノートを参照してください。

永続的な IP アドレスの割り当ては、『[Cisco Nexus ダッシュボードユーザガイド](#)』で説明されているように、UI の外部サービス プール設定を使用してクラスタが展開された後に行われます。

永続的な IP 構成に関連する追加の要件と警告については、特定のサービスのドキュメントを参照することをお勧めします。

表 2: サービス固有のネットワーク要件

Nexus Dashboard サービス	管理インターフェイス	データ インターフェイス	永続的 IP の総数
Nexus Dashboard Orchestrator	レイヤ 3 隣接	レイヤ 3 隣接	なし
SFLOW/NetFlow のない Nexus Dashboard Insights (ACI ファブリック)	レイヤ 3 隣接	レイヤ 3 隣接	なし
SFLOW/NetFlow (NDFC/DCNM ファブリック) のない Nexus Dashboard Insights	レイヤ 3 隣接	レイヤ 2 隣接	IPv4 を使用している場合、データ インターフェイス ネットワーク内の 6 つの IP IPv6 を使用している場合、データ インターフェイス ネットワーク内の 7 つの IP

Nexus Dashboard サービス	管理インターフェイス	データ インターフェイス	永続的 IP の総数
SFLOW/NetFlow (ACI または NDFC/DCNMファブリック) を使用した Nexus ダッシュボード Insights	レイヤ 3 隣接	レイヤ 2 隣接	データ インターフェイス ネットワーク内の 6 つの IP

Nexus Dashboard サービス	管理インターフェイス	データ インターフェイス	永続的 IP の総数
Nexus ダッシュボードファブリックコントローラ、リリース 12.0.x	レイヤ 2 隣接	レイヤ 2 隣接	

Nexus Dashboard サービス	管理インターフェイス	データ インターフェイス	永続的 IP の総数
			<ul style="list-style-type: none"> • [LAN デバイス管理の接続性 (LAN Device Management Connectivity)] が [管理 (Management)] (デフォルト) に設定されている場合 : • SNMP/Syslog および SCP サービス用の管理ネットワーク内の 2 つの IP • [EPL] が有効になっている場合、各ファブリックのデータネットワークに 1 つの追加 IP • [メディア用の IP ファブリック (IP Fabric for Media)] が有効になっている場合、テレメトリ用の管理ネットワークに 1 つの追加の IP • [LAN デバイス管理の接続性 (LAN Device

Nexus Dashboard サービス	管理インターフェイス	データ インターフェイス	永続的 IP の総数
			<p>Management Connectivity)] が [データ (Data)] に設定されている場合 :</p> <ul style="list-style-type: none"> • SNMP/Syslog および SCP サービス用のデータ ネットワーク内の 2 つの IP • [EPL] が有効になっている場合、各ファブリックのデータ ネットワークに 1 つの追加 IP • [メディア用の IP ファブリック (IP Fabric for Media)] が有効になっている場合、テレメトリ用のデータ ネットワークに 1 つの追加の IP

Nexus Dashboard サービス	管理インターフェイス	データ インターフェイス	永続的 IP の総数
Nexus ダッシュボードファブリックコントローラ、リリース 12.1.1 以降	レイヤ 2 またはレイヤ 3 隣接	レイヤ 2 またはレイヤ 3 隣接	

Nexus Dashboard サービス	管理インターフェイス	データ インターフェイス	永続的 IP の総数
			<ul style="list-style-type: none"> • LAN 展開タイプで [LAN デバイス管理の接続性 (LAN Device Management Connectivity)] が [管理 (Management)] (デフォルト) に設定されたレイヤー 2 モードで動作している場合 <ul style="list-style-type: none"> • SNMP/Syslog および SCP サービス用の管理ネットワーク内の 2 つの IP • [EPL] が有効になっている場合、各ファブリックのデータネットワークに 1 つの追加 IP • [メディア用の IP ファブリック (IP Fabric for Media)] が有効になっている場合、テレメトリ用の管理ネットワークに 1 つの追加の IP

Nexus Dashboard サービス	管理インターフェイス	データ インターフェイス	永続的 IP の総数
			<ul style="list-style-type: none"> • LAN 展開タイプで [LAN デバイス管理の接続性 (LAN Device Management Connectivity)] が [データ (Data)] (デフォルト) に設定されたレイヤー 2 モードで動作している場合 <ul style="list-style-type: none"> • SNMP/Syslog および SCP サービス用のデータ ネットワーク内の 2 つの IP • [EPL] が有効になっている場合、各ファブリックのデータ ネットワークに 1 つの追加 IP • [メディア用の IP ファブリック (IP Fabric for Media)] が有効になっている場合、テレメトリ用のデータ ネットワークに 1 つの追加の IP

Nexus Dashboard サービス	管理インターフェイス	データ インターフェイス	永続的 IP の総数
			<ul style="list-style-type: none"> • LAN 展開タイプのレイヤ 3 モードで動作している場合： <ul style="list-style-type: none"> • [LAN デバイス管理の接続性 (LAN Device Management Connectivity)] が [データ (Data)] に設定されている必要があります • SNMP/Syslog および SCP サービス用の 2 つの IP • [EPL] が有効になっている場合、各ファブリックのデータネットワークに 1 つの追加 IP • すべての永続的 IP は、管理サブネットまたはデータサブネットと重複していない別のプールの一部である必要があります。

Nexus Dashboard サービス	管理インターフェイス	データ インターフェイス	永続的 IP の総数
			<p>永続的 IP のレイヤ 3 モードの詳細については、ユーザーガイドの「永続的 IP」のセクションを参照してください。</p> <ul style="list-style-type: none"> • SAN コントローラ展開タイプのレイヤ 3 モードで動作している場合： <ul style="list-style-type: none"> • SSH 用の 1 つの IP • SNMP/Syslog 用の 1 つの IP • SAN Insights 機能用の 1 つの IP • メディア モードの IP ファブリックは、レイヤ 3 モードではサポートされていません。
Cisco Nexus Dashboard Data Broker	レイヤ 3 隣接	なし	なし

- 両方のネットワークでノード間の接続が必要であり、次の追加のラウンドトリップ時間 (RTT) 要件があります。



- (注) Nexus ダッシュボードクラスタと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。例えば、Insightsとオーケストレータサービスを共同ホストする場合、サイト接続性RTTは50msを超えないようにします。

表 3: RTT 要件

サービス	接続	最大 RTT
Nexus Dashboard クラスタ	ノード間	150 ミリ秒
Nexus Dashboard Orchestrator	ノード間	150 ミリ秒
	サイトへ	APIC サイトの場合 : 500 ミリ秒 NDFC サイトの場合 : 150 ミリ秒
Nexus Dashboard Insights	ノード間	50 ミリ秒
	サイトへ	50 ミリ秒
Nexus ダッシュボードファブリックコントローラ	ノード間	50 ミリ秒
	サイトへ	50 ミリ秒
Cisco Nexus Dashboard Data Broker	ノード間	150 ミリ秒
	サイトへ	500 ミリ秒

Nexus ダッシュボードの内部ネットワーク

Nexus ダッシュボードで使用されるコンテナ間の通信には、さらに2つの内部ネットワークが必要です。

- **アプリケーションオーバーレイ**は、Nexus ダッシュボード内のアプリケーションで内部的に使用されます。

アプリケーションオーバーレイは /16 ネットワークである必要があります、導入時にデフォルト値が事前入力されます。

- **サービスオーバーレイ**は、Nexus ダッシュボードによって内部的に使用されます。

サービスオーバーレイは /16 ネットワークである必要があります、導入時にデフォルト値が事前入力されます。

複数のNexusダッシュボードクラスタの展開を計画している場合、同じアプリケーションサブネットとサービスサブネットをそれらに使用できます。



- (注) 異なる Nexus ダッシュボード ノードに展開されたコンテナ間の通信は VXLAN でカプセル化され、送信元と宛先としてデータ インターフェイスの IP アドレスを使用します。これは、アプリケーション オーバーレイとサービス オーバーレイのアドレスがデータ ネットワークの外部に公開されることはなく、これらのサブネット上のトラフィックは内部でルーティングされ、クラスタノードから出ないことを意味します。

たとえば、オーバーレイ ネットワークの1つと同じサブネット上に別のサービス (DNS など) がある場合、そのサブネット上のトラフィックはクラスタの外部にルーティングされないため、Nexus ダッシュボードからそのサービスにアクセスできません。そのため、これらのネットワークは一意であり、クラスタの外部にある既存のネットワークまたはサービスと重複しないようにしてください。これらは Nexus ダッシュボード クラスタ ノードからアクセスする必要があります。

同じ理由で、アプリまたはサービスのサブネットには 169.254.0.0/16 (Kubernetes br1 サブネット) を使用しないことをお勧めします。

BGP 構成と永続的な IP

Nexus ダッシュボードの以前のリリースでは、サービスが異なる Nexus ダッシュボードノードに再配置された場合でも、同じ IP アドレスを保持する必要があるサービス (Nexus ダッシュボード Insights など) に対して 1 つ以上の永続的な IP アドレスを構成できました。ただし、これらのリリースでは、永続的な IP は管理サブネットとデータサブネットの一部である必要があります。クラスタ内のすべてのノードが同じレイヤー 3 ネットワークの一部である場合にのみ機能を有効にできました。ここで、サービスは、Gratuitous ARP やネイバー探索などのレイヤ 2 メカニズムを使用して、レイヤ 3 ネットワーク内で永続的な IP をアドバタイズします。

リリース 2.2(1) 以降、異なるレイヤ 3 ネットワークにクラスタノードを展開する場合でも、永続的な IP 機能がサポートされます。この場合、永続的な IP は、「レイヤー 3 モード」と呼ばれる BGP を介して各ノードのデータリンクからアドバタイズされます。また、IP は、ノードの管理サブネットまたはデータサブネットと重複していないサブネットの一部である必要があります。永続IPがデータネットワークおよび管理ネットワークの外部にある場合、この機能はデフォルトでレイヤ 3 モードで動作します。IP がそれらのネットワークの一部である場合、機能はレイヤ 2 モードで動作します。

BGP は、クラスタの展開中、またはクラスタの稼働後に Nexus ダッシュボード GUI から有効にすることができます。

BGP を有効にして永続的な IP 機能を使用することを計画している場合は、次のことを行う必要があります。

- ピアルータが、ノードのレイヤ 3 ネットワーク間でアドバタイズされた永続的な IP を交換することを確認します。

- 以降のセクションで説明されているようにクラスタの展開時に BGP を有効にするか、『ユーザーガイド』の「永続的な IP アドレス」セクションで説明されているように Nexus ダッシュボード GUI で後で有効にするかを選択します。
- 割り当てる永続的な IP アドレスが、ノードの管理サブネットまたはデータサブネットと重複しないようにしてください。

通信ポート

次のセクションでは、Nexus Dashboard クラスタとサービスに必要なポートのリファレンスを示します。



- (注) すべてのサービスは、暗号化を備えた TLS または mTLS を使用して、ネットワーク上のデータのプライバシーと完全性を保護します。

Nexus Dashboard ポート

Nexus Dashboard クラスタには、次のポートが必要です。

表 4: Nexus Dashboard ポート (管理ネットワーク)

サービス	ポート	プロトコル	方向 イン: クラスタに対して アウト: クラスタから ファブリックまたは 世界外に対して	接続
ICMP	ICMP	ICMP	入力 / 出力	他のクラスタ ノード、CIMC、デフォルト ゲートウェイ
SSH	22	TCP	入力 / 出力	クラスタ ノードの CLI および CIMC
TACACS	49	TCP	発信	TACACS サーバー
DNS	53	TCP/UDP	アウト	DNS サーバ
HTTP	80	TCP	発信	インターネット/プロキシ
NTP	123	UDP	発信	NTP サーバー

サービス	ポート	プロトコル	方向 イン：クラスタに対して アウト：クラスタから ファブリックまたは世界外に対して	接続
HTTPS	443	TCP	入力 / 出力	UI、他のクラスタ(マルチクラスタ接続用)、ファブリック、インターネット/プロキシ
LDAP	389 636	TCP	発信	LDAP サーバ
RADIUS	1812	TCP	発信	Radius サーバー
KMS	9880	TCP	入力 / 出力	その他クラスタ ノードおよび ACI ファブリック
インフラサービス	30012 30021 30500 ~ 30600	TCP および UDP	入力 / 出力	その他のクラスタ ノード

表 5: Nexus Dashboard ポート (データ ネットワーク)

サービス	ポート	プロトコル	方向 イン：クラスタに対して アウト：クラスタから ファブリックまたは世界外に対して	接続
ICMP	ICMP	ICMP	入力 / 出力	他のクラスタ ノード、CIMC、デフォルト ゲートウェイ
SSH	22	TCP	発信	スイッチと APIC の帯域内

サービス	ポート	プロトコル	方向 イン：クラスタに対して アウト：クラスタから ファブリックまたは世界外に対して	接続
DNS	53	TCP および UDP	入力 / 出力	DNS サーバー
HTTPS	443	TCP	発信	スイッチのインバンドおよび APIC / NDFC / DCNM。
VXLAN	4789	UDP	入力 / 出力	その他のクラスタ ノード
KMS	9880	TCP	入力 / 出力	その他クラスタ ノードおよび ACI ファブリック
インフラサービス	3379 3380 8989 9090 9969 9979 9989 15223 30002 ~ 30006 30009 ~ 30010 30012 30014-30015 30018-30019 30025 30027	TCP	入力 / 出力	その他のクラスタ ノード
Kafka	30001	TCP	入力 / 出力	スイッチのインバンドおよび APIC/NDFC/DCNM

サービス	ポート	プロトコル	方向	接続
			イン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	
インフラサービス	30016 30017	TCP および UDP	入力 / 出力	その他のクラスタ ノード
インフラサービス	30500 ~ 30600	TCP および UDP	入力 / 出力	その他のクラスタ ノード

Nexus Dashboard Insights ポート

上記の Nexus Dashboard クラスタ ノードに必要なポートに加えて、Nexus Dashboard Insights サービスには次のポートが必要です。

表 6: Nexus Dashboard Insights ポート (データ ネットワーク)

サービス	ポート	プロトコル	方向	接続
			イン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	
テックコレクションを表示	2022	TCP	入力 / 出力	スイッチのインバンドおよび APIC/NDFC/DCNM
フローテレメトリ	5640 ~ 5671	UDP	入力	スイッチの帯域内
TAC アシスト	8884	TCP	入力 / 出力	外部
KMS	9989	TCP	入力 / 出力	その他クラスタ ノードおよび ACI ファブリック

サービス	ポート	プロトコル	方向	接続
			イン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	
SW テレメトリ	5695 30000 57500 30570	TCP	入力 / 出力	その他のクラスタ ノード

Nexus Dashboard Fabric Controller ポート

Nexus Dashboard (ND) クラスタ ノードに必要なポートに加えて、Nexus Dashboard Fabric Controller (NDFC) サービスには次のポートが必要です。



- (注) 次のポートは、NDFC サービスからスイッチへの IP 到達可能性を提供するインターフェイスに応じて、Nexus Dashboard 管理ネットワークおよび/またはデータ ネットワーク インターフェイスに適用されます。

表 7: Nexus Dashboard Fabric Controller ポート

サービス	ポート	プロトコル	方向	接続
			イン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	(特に明記されていない限り、LAN と SAN の両方の展開に適用されます)
SSH	22	TCP	発信	SSH は、デバイスにアクセスするための基本的なメカニズムです。
SCP	22	TCP	発信	NDFC バックアップ ファイルをリモート サーバーにアーカイブする SCP クライアント。

サービス	ポート	プロトコル	方向	接続
			イン：クラス タに対して アウト：クラ スタから ファブリッ クまたは世 界外に対し て	(特に明記されていない限り、 LAN と SAN の両方の展開に適用されます)
SMTP	25	TCP	発信	SMTP ポートは、NDFC の [サーバー設 定 (Server Settings)] メニューから構成 できます。 これはオプションの機能です。
DHCP	67	UDP	入力	NDFC ローカル DHCP サーバーがブー トストラップ/POAP 用に構成されてい る場合。 これは、LAN 展開にのみ適用されま す。 (注) POAP の目的でローカル DHCP サーバーとして NDFC を使用する場合、す べての ND マスターノード の IP を DHCP リレーとし て構成する必要があります。 ND ノードの管理 IP ま たはデータ IP が DHCP サー バーにバインドされるかど うかは、NDFC サーバー設 定の LAN デバイス管理接 続によって決定されます。
DHCP	68	UDP	発信	
SNMP	161	TCP/UDP	アウト	NDFC からデバイスへの SNMP トラ フィック。

サービス	ポート	プロトコル	方向	接続
			イン：クラス タに対して アウト：クラ スタから ファブリッ クまたは世 界外に対し て	（特に明記されていない限り、 LAN と SAN の両方の展開に適用されます）
HTTPS/HTTP (NX-API)	443/80	TCP	発信	NX-API HTTPS/HTTP クライアントは、 構成可能でもあるポート 443/80 でデバ イスの NX-API サーバーに接続します。 NX-API はオプション機能であり、 NDFC 機能の限られたセットで使用さ れます。 これは、LAN 展開にのみ適用されま す。
HTTPS (vCenter、 Kubernetes、 OpenStack、 Discovery)	443	TCP	発信	NDFC は、VMware vCenter や OpenStack などの登録済み VMM ドメインと、 Kubernetes などのコンテナ オーケスト レーターから取得した情報を関連付け ることにより、統合されたホストおよ び物理ネットワーク トポロジビューを 提供します。 これはオプションの機能です。



(注) 次のポートは、一部の NDFC サービスで使用される永続的 IP と呼ばれる外部サービス IP に適用されます。これらの外部サービス IP は、構成された設定に応じて、Nexus Dashboard の管理サブネットプールまたはデータサブネットプールから取得される場合があります。

表 8 : Nexus Dashboard Fabric Controller 永続的 IP ポート

サービス	ポート	プロトコル	方向	接続
			イン：クラス タに対して アウト：クラ スタから ファブリッ クまたは世 界外に対し て	(特に明記されていない限り、 LAN と SAN の両方の展開に適用されます)
SCP	22	TCP	入力	<p>SCP は、デバイスと NDFC サービス間でファイルを転送するさまざまな機能によって使用されます。NDFC SCP サービスは、ダウンロードとアップロードの両方の SCP サーバーとして機能します。SCP は、POAP 関連ファイルをダウンロードするために、デバイス上の POAP クライアントによっても使用されます。</p> <p>NDFC の SCP-POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続的な IP があります。これは、NDFC サーバー設定の [LAN デバイス管理接続 (LAN Device Management Connectivity)] 設定によって制御されます。</p>

サービス	ポート	プロトコル	方向	接続
TFTP (POAP)	69	TCP	<p>イン：クラス タに対して</p> <p>アウト：クラ スタから ファブリッ クまたは世 界外に対し て</p> <p>入力</p>	<p>(特に明記されていない限り、LAN と SAN の両方の展開に適用されます)</p> <p>POAP 経由のデバイス ゼロタッチ プロ ビジョニングにのみ使用されます。デ バイスは、基本的なインベントリ情報 を NDFC に送信して (NDFC への制限付 きの書き込み専用アクセス)、セキュア な POAP 通信を開始できます。NDFC ブートストラップまたは POAP は、 TFTP または HTTP/HTTPS 用に構成で きます。</p> <p>NDFC の SCP-POAP サービスには、管 理サブネットまたはデータ サブネット のいずれかに関連付けられた永続的な IP があります。これは、NDFC サーバー 設定の [LAN デバイス管理接続 (LAN Device Management Connectivity)] 設定 によって制御されます。</p> <p>これは、LAN 展開にのみ適用されま す。</p>

サービス	ポート	プロトコル	方向	接続
HTTP (POAP)	80	TCP	<p>イン：クラス タに対して</p> <p>アウト：クラ スタから ファブリッ クまたは世 界外に対 して</p> <p>入力</p>	<p>(特に明記されていない限り、LAN と SAN の両方の展開に適用されます)</p> <p>POAP 経由のデバイスゼロタッチプロ ビジョニングにのみ使用されます。デ バイスは、基本的なインベントリ情報 を NDFC に送信して (NDFC への制限付 きの書き込み専用アクセス)、セキュア な POAP 通信を開始できます。NDFC ブートストラップまたは POAP は、 TFTP または HTTP/HTTPS 用に構成で きます。</p> <p>NDFC の SCP-POAP サービスには、管 理サブネットまたはデータサブネット のいずれかに関連付けられた永続的な IP があります。これは、NDFC サーバー 設定の [LAN デバイス管理接続 (LAN Device Management Connectivity)] 設定 によって制御されます。</p> <p>これは、LAN 展開にのみ適用されま す。</p>

サービス	ポート	プロトコル	方向	接続
			イン：クラス タに対して アウト：クラ スタから ファブリッ クまたは世 界外に対し て	（特に明記されていない限り、 LAN と SAN の両方の展開に適用されます）
BGP	179	TCP	入力 / 出力	<p>エンドポイント ロケータの場合、有効になっているファブリックごとに、独自の永続的な IP を使用して EPL サービスが生成されます。このサービスは、常に Nexus Dashboard データ インターフェイスに関連付けられています。エンドポイント情報を追跡するために必要な BGP アップデートを取得するために、ファブリック上の適切な BGP エンティティ（通常は BGP ルートリフレクタ）と NDFC EPL サービスはピアを行います。</p> <p>この機能は、VXLAN BGP EVPN ファブリックの展開にのみ適用されます。</p> <p>これは、LAN 展開にのみ適用されます。</p>
HTTPS (POAP)	443	TCP	入力	<p>セキュア POAP は、ポート 443 の NDFC HTTPS サーバーを介して実現されます。HTTPS サーバーは SCP-POAP サービスにバインドされ、そのポッドに割り当てられたのと同じ永続的 IP を使用します。</p> <p>NDFC の SCP-POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続的な IP があります。これは、NDFC サーバー設定の [LAN デバイス管理接続 (LAN Device Management Connectivity)] 設定によって制御されます。</p> <p>これは、LAN 展開にのみ適用されます。</p>

サービス	ポート	プロトコル	方向	接続
			イン：クラスターに対して アウト：クラスターからファブリックまたは世界外に対して	接続 （特に明記されていない限り、 LAN と SAN の両方の展開に適用されます）
Syslog	514	UDP	入力	<p>NDFC が Syslog サーバーとして構成されている場合、デバイスからの Syslog は、SNMP-Trap/Syslog サービス ポッドに関連付けられた永続的な IP に向けて送信されます。</p> <p>NDFC の SNMP-Trap-Syslog サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続的な IP があります。これは、NDFC サーバー設定の [LAN デバイス管理接続 (LAN Device Management Connectivity)] 設定によって制御されます。</p>
SCP	2022	TCP	発信	<p>NDFC POAP-SCP ポッドの永続的な IP から、Nexus Dashboard Insights を実行している別の ND クラスターにテクニカルサポートファイルを転送します。</p> <p>NDFC の SCP-POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続的な IP があります。これは、NDFC サーバー設定の LAN デバイス管理接続設定によって制御されます。</p>

サービス	ポート	プロトコル	方向	接続
			イン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	(特に明記されていない限り、LAN と SAN の両方の展開に適用されます)
SNMP トラップ	2162	UDP	入力	デバイスから NDFC への SNMP トラップは、SNMP-Trap/Syslog サービス ポッドに関連付けられた永続的な IP に向けて送信されます。 NDFC の SNMP-Trap-Syslog サービスには、管理サブネットまたはデータサブネットのいずれかに関連付けられた永続的な IP があります。これは、NDFC サーバー設定の [LAN デバイス管理接続 (LAN Device Management Connectivity)] 設定によって制御されます。
GRPC (テレメトリ)	33000	TCP	入力	NDFC 永続的 IP に関連付けられた GRPC トランスポートを介して SAN データ(ストレージ、ホスト、フローなど)を受信する SAN Insights Telemetry サーバー。 これは、SAN 展開でのみ有効です。
GRPC (テレメトリ)	50051	TCP	入力	メディア展開用の IP ファブリックおよび一般的な LAN 展開用の PTP のマルチキャストフローに関連する情報は、ソフトウェアテレメトリを介して、NDFC GRPC レシーバー サービス ポッドに関連付けられた永続的 IP にストリーミングされます。 これは、LAN およびメディア展開でのみ有効です。

SAN 展開向けの Nexus Dashboard Fabric Controller ポート

Nexus Dashboard Fabric Controller は、単一ノードまたは 3 ノードの Nexus Dashboard クラスタに導入できます。単一ノードクラスタでの NDFC SAN 展開には、次のポートが必要です。

表 9: 単一ノードクラスタでの SAN 展開向けの *Nexus Dashboard Fabric Controller* ポート

サービス	ポート	プロトコル	方向 イン: クラスタに 対して アウト: クラスタ からファブリック または世界外に対 して	接続 (特に明記されて いない限り、 LAN と SAN の両方の 展開に適用されま す)
SSH	22	TCP	発信	SSH は、デバイス にアクセスするた めの基本的なメカ ニズムです。
SCP	22	TCP	発信	NDFC バックアッ プ ファイルをリ モート サーバー にアーカイブする SCP クライアン ト。
SMTP	25	TCP	発信	SMTP ポートは、 NDFC の [サー バー設定 (Server Settings)] メ ニューから構成で きます。 これはオプション の機能です。
SNMP	161	TCP/UDP	アウト	NDFC からデバイ スへの SNMP ト ラフィック。

サービス	ポート	プロトコル	方向	接続
			イン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	（特に明記されていない限り、 LAN と SAN の両方の展開に適用されます）
HTTPS (vCenter、Kubernetes、OpenStack、Discovery)	443	TCP	発信	NDFC は、VMware vCenter や OpenStack などの登録済み VMM ドメインと、Kubernetes などのコンテナオーケストレーターから取得した情報を関連付けることにより、統合されたホストおよび物理ネットワーク ポロジビューを提供します。 これはオプションの機能です。



(注) 次のポートは、一部の NDFC サービスで使用される、永続的 IP とも呼ばれる外部サービス IP に適用されます。これらの外部サービス IP は、構成された設定に応じて、Nexus Dashboard の管理サブネットプールまたはデータサブネットプールから取得される場合があります。

表 10: 単一ノードクラスタでの SAN 展開向けの *Nexus Dashboard Fabric Controller* 永続的 IP ポート

サービス	ポート	プロトコル	方向 イン: クラスタに 対して アウト: クラスタ からファブリック または世界外に対 して	接続
SCP	22	TCP	入力	SCP は、デバイス と NDFC サービス 間でファイルを 転送するさまざま な機能によって使 用されます。 NDFC SCP サービス は、ダウンロード とアップロード の両方で機能しま す。

サービス	ポート	プロトコル	方向 イン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	接続
Syslog	514	UDP	入力	<p>NDFC が Syslog サーバーとして構成されている場合、デバイスからの syslog は、SNMP-Trap/Syslog サービス ポッドに関連付けられた永続的 IP に向けて送信されます。</p> <p>NDFC の SNMP-Trap-Syslog サービスには、管理サブネットまたはデータサブネットのいずれかに関連付けられた永続的な IP があります。これは、NDFC サーバー設定の [LAN デバイス管理接続 (LAN Device Management Connectivity)] 設定によって制御されます。</p>

サービス	ポート	プロトコル	方向 イン：クラスタに 対して アウト：クラスタ からファブリック または世界外に対 して	接続
SNMP トラップ	2162	UDP	入力	<p>デバイスから NDFC への SNMP トラップは、SNMP-Trap/Syslog サービス ポッドに関連付けられた永続的な IP に向けて送信されます。</p> <p>NDFC の SNMP-Trap-Syslog サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続的な IP があります。</p>
GRPC (テレメトリ)	33000	TCP	入力	<p>NDFC 永続的な IP に関連付けられた GRPC トランスポートを介して SAN データ (ストレージ、ホスト、フローなど) を受信する SAN Insights Telemetry サーバー。</p> <p>これは、SAN 展開でのみ有効です。</p>

ファブリック接続

ここでは、Nexus ダッシュボード クラスタをファブリックに接続する方法について説明します。

オンプレミス APIC または NDFC ファブリックの場合、Nexus ダッシュボード クラスタは次の2つの方法のいずれかで接続できます。

- レイヤ 3 ネットワーク経由でファブリックに接続された Nexus Dashboard クラスタ。
- リーフ スイッチに接続された Nexus Dashboard ノードは、一般的なホストです。

Cisco Cloud Network Controller ファブリックの場合は、レイヤ 3 ネットワーク経由で接続する必要があります。

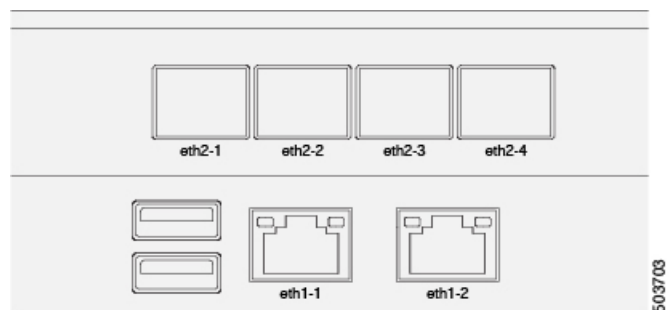
物理ノードのケーブル接続

仮想またはクラウドフォーム ファクタ クラスタを展開する場合は、このセクションをスキップできます。

次の図に、Nexus Dashboard の物理ノード インターフェイスを示します。

- eth1-1 および eth1-2 は管理ネットワークに接続する必要があります。
- eth2-1 および eth2-2 はデータ ネットワークに接続する必要があります。

図 1: ノード接続



インターフェイスは、アクティブ/スタンバイ モードで実行されている、データインターフェイス用と管理インターフェイス用の Linux ボンドとして設定されます。すべてのインターフェイスは個々のホストポートに接続する必要があります。PortChannelおよびvPCはサポートされていません。

Nexus ダッシュボード ノードが Cisco Catalyst スイッチに接続されている場合、VLAN が指定されていない場合、パケットはvlan0でタグ付けされます。この場合、データネットワーク上での到達可能性を確保するために、ノードが接続されているスイッチ インターフェイスに `switchport voice vlan dot1p` コマンドを追加する必要があります。

外部レイヤ3 ネットワークを介した接続

Nexus ダッシュボード クラスタは、外部のレイヤ3 ネットワーク経由でファブリックに接続することを推奨します。これは、クラスタをどのファブリックにも結び付けず、すべてのサイトに同じ通信パスを確立できるためです。特定の接続は、Nexus ダッシュボードに展開されたアプリケーションのタイプによって異なります。

- Cisco ACI ファブリックのみを管理するために Nexus ダッシュボード オーケストレータを展開する場合は、データ インターフェイスから各サイトの APIC のインバンドまたはアウトオブバンド (OOB) インターフェイスまたは両方への接続を確立できます。
- Cisco NDFC ファブリックを管理するために Nexus Dashboard Orchestrator を展開する場合は、データ インターフェイスから各サイトの NDFC のインバンド インターフェイスへの接続を確立する必要があります。
- Nexus ダッシュボード Insights などの Day-2 Operations アプリケーションを展開する場合は、データ インターフェイスから各ファブリックおよび APIC のインバンド ネットワークへの接続を確立する必要があります。

レイヤ3 ネットワークを介してクラスタを接続する場合は、次の点に注意してください。

- ACI ファブリックの場合、管理テナントで Cisco Nexus Dashboard データ ネットワーク接続用の L3Out および外部 EPG を設定する必要があります。

ACI ファブリックでの外部接続の設定については、『[Cisco APIC Layer 3 Networking Configuration Guide](#)』を参照してください。

- NDFC ファブリックの場合、データ インターフェイスと NDFC のインバンド インターフェイスが異なるサブネットにある場合は、Nexus ダッシュボードのデータ ネットワーク アドレスに到達するためのルートを NDFC で追加する必要があります。

NDFC UI からルートを追加するには、[管理者 (Administration)] > [カスタマイズ (Customization)] > [ネットワーク設定 (Network Preference)] > [インバンド (In-Band) (eth2)] に移動し、ルートを追加して保存します。

- クラスタのセットアップ中にデータ インターフェイスの VLAN ID を指定する場合、その VLAN を許可するトランクとしてホスト ポートを設定する必要があります。

ただし、ほとんどの一般的な導入では、VLAN ID を空のままにして、ホスト ポートをアクセス モードに設定できます。

次の2つの図は、Nexus Dashboard クラスタをレイヤ3 ネットワーク経由でファブリックに接続する場合の2つの異なるネットワーク接続シナリオを示しています。それぞれの主な目的は、Nexus ダッシュボードで実行しているアプリケーションのタイプによって異なります。

図 2: レイヤ 3 ネットワークを介した接続、2 日目の運用アプリケーション

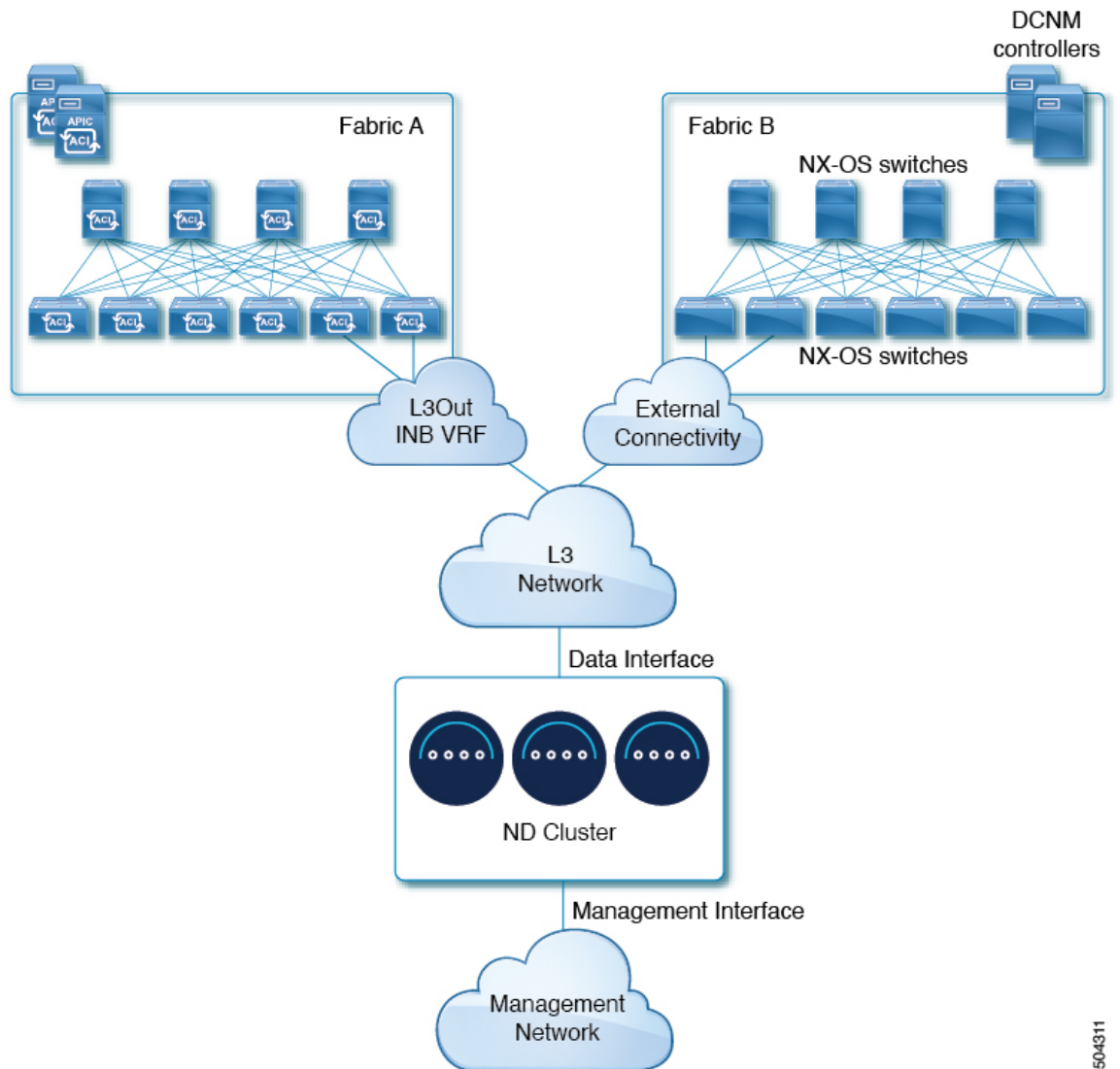
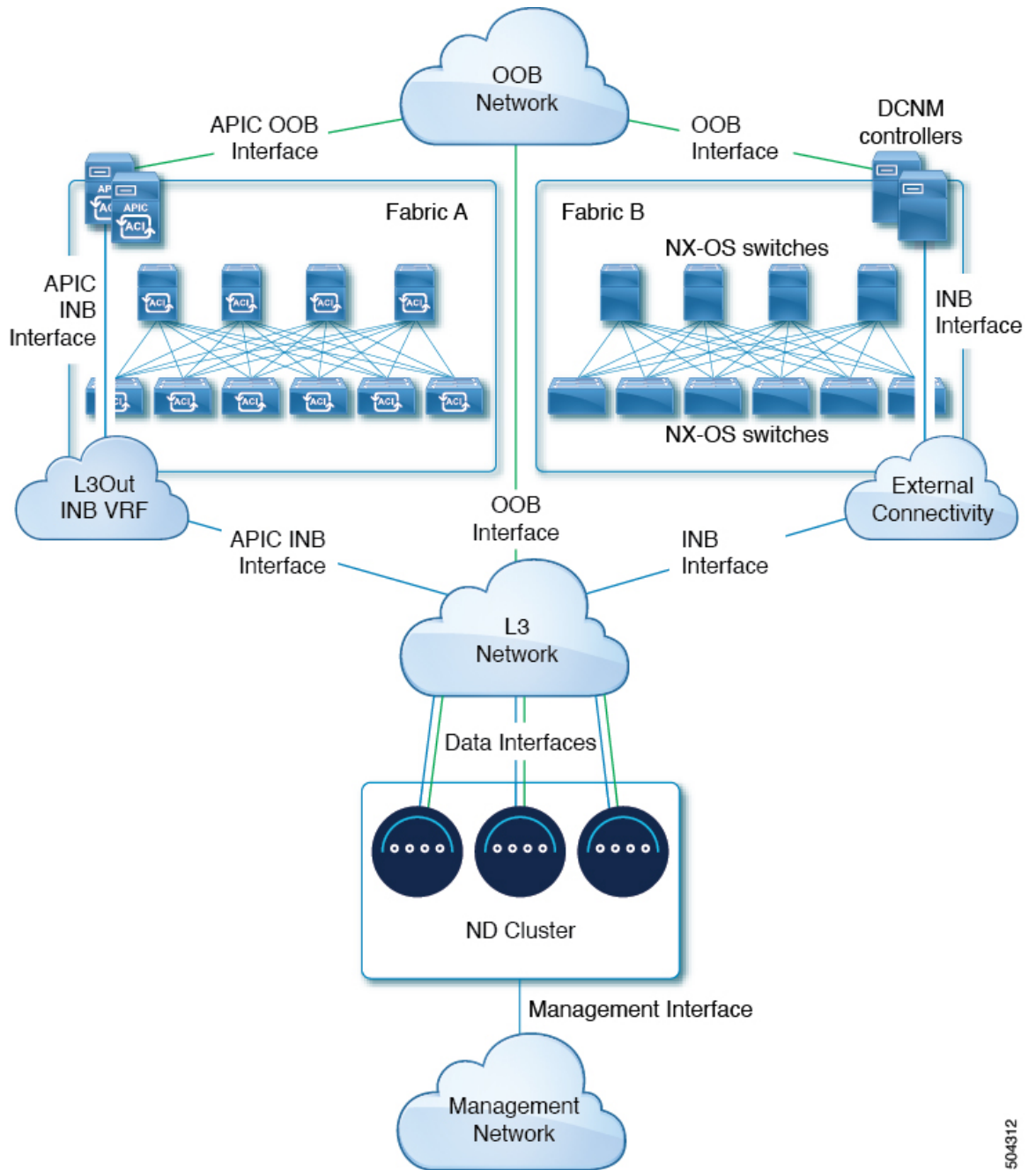


図 3: レイヤ3ネットワーク、*Nexus Dashboard Orchestrator*を介した接続

リーフスイッチへのノードの直接接続

Nexus Dashboard クラスタをファブリックの1つに直接接続することもできます。これにより、クラスタとファブリックのインバンド管理が容易になりますが、クラスタを特定のファブリックに結び付け、外部接続を介して他のファブリックに到達できるようにする必要があります。これにより、クラスタが特定のファブリックに依存するようになるため、ファブリック内の問

題が Nexus Dashboard の接続に影響を与える可能性があります。前の例と同様に、接続は Nexus ダッシュボードに展開されたアプリケーションのタイプによって異なります。

- Cisco ACI ファブリックのみを管理するために Nexus Dashboard Orchestrator を展開する場合は、データインターフェイスから各サイトの APIC のインバンドまたはアウトオブバンド (OOB) インターフェイスへの接続を確立できます。
- Nexus ダッシュボード Insights を展開する場合は、データインターフェイスから各ファブリックのインバンドインターフェイスへの接続を確立する必要があります。

ACI ファブリックの場合、データインターフェイス IP サブネットはファブリック内の EPG / BD に接続し、管理テナントのローカルインバンド EPG に対して確立されたコントラクトが必要です。Nexus ダッシュボードは、管理テナントおよびインバンド VRF に導入することを推奨します。他のファブリックへの接続は、L3Out 経由で確立されます。

- ACI ファブリックを使用して Nexus Dashboard Insights を展開する場合は、データインターフェイスの IP アドレスと ACI ファブリックのインバンド IP アドレスは、異なるサブネット内にある必要があります。

クラスタをリーフスイッチに直接接続する場合は、次の点に注意してください。

- VMware ESX または Linux KVM で展開する場合、ホストはトランク ポート経由でファブリックに接続する必要があります。
- クラスタのセットアップ中にデータ ネットワークの VLAN ID を指定する場合は、Nexus ダッシュボード インターフェイスと接続されたネットワークデバイスのポートをトランクとして設定する必要があります。

ただし、ほとんどの場合、VLAN をデータ ネットワークに割り当てないことを推奨します。この場合、ポートをアクセス モードで設定する必要があります。

- ACI ファブリックの場合：

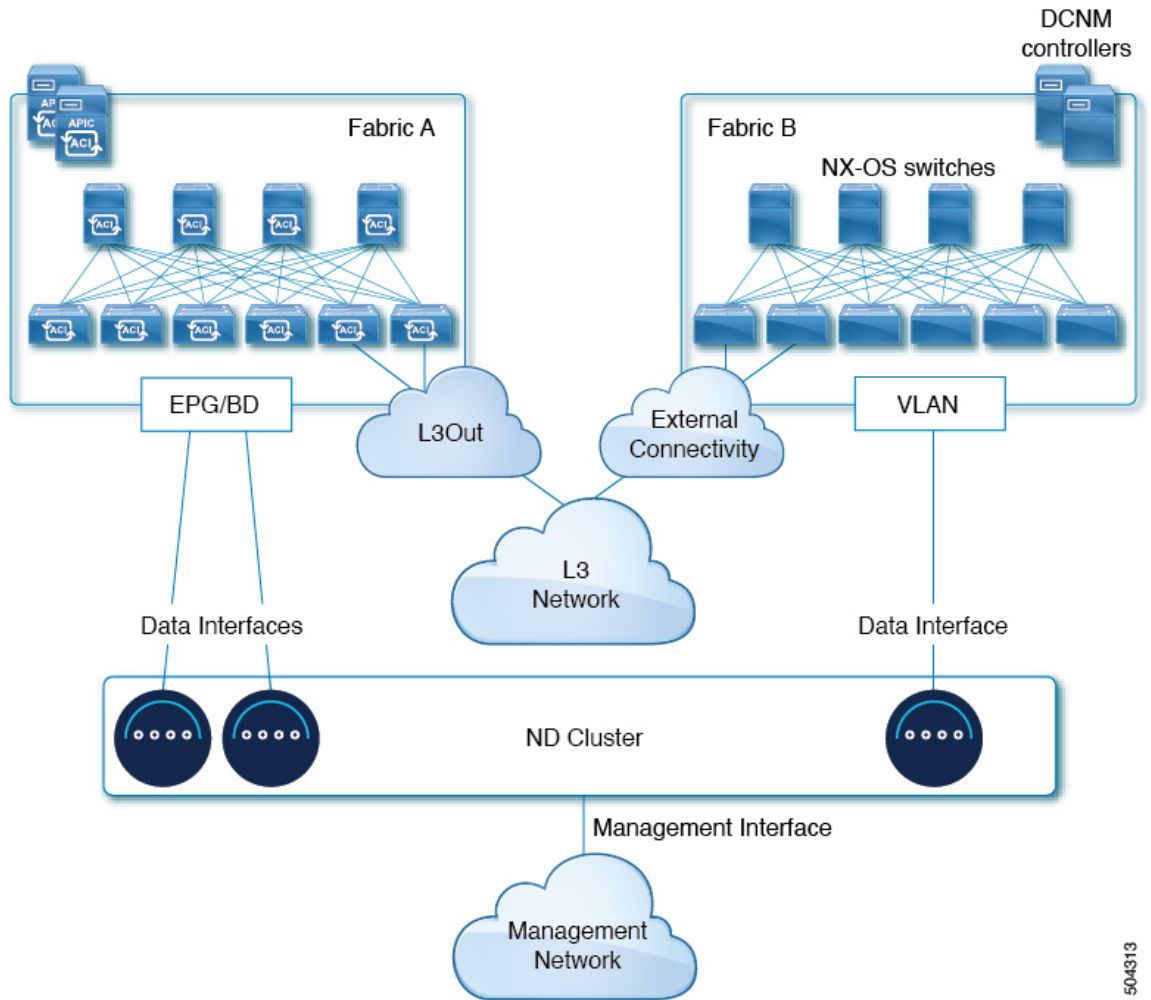
- 管理テナントの Cisco Nexus Dashboard 接続用にブリッジドメイン (BD)、サブネット、およびエンドポイントグループ (EPG) を設定することを推奨します。

Nexus Dashboard はインバンド VRF のインバンド EPG への接続を必要とするため、管理テナントで EPG を作成すると、ルートリークが不要になります。

- ファブリックのインバンド管理 EPG と Cisco Nexus ダッシュボード EPG 間のコントラクトを作成する必要があります。
- 複数のファブリックが Nexus ダッシュボード クラスタのアプリケーションでモニターされている場合、デフォルトルートまたは他の ACI ファブリックインバンド EPG への特定のルートを持つ L3Out をプロビジョニングし、クラスタ EPG と L3Out の外部 EPG の間でコントラクトを確立する必要があります。

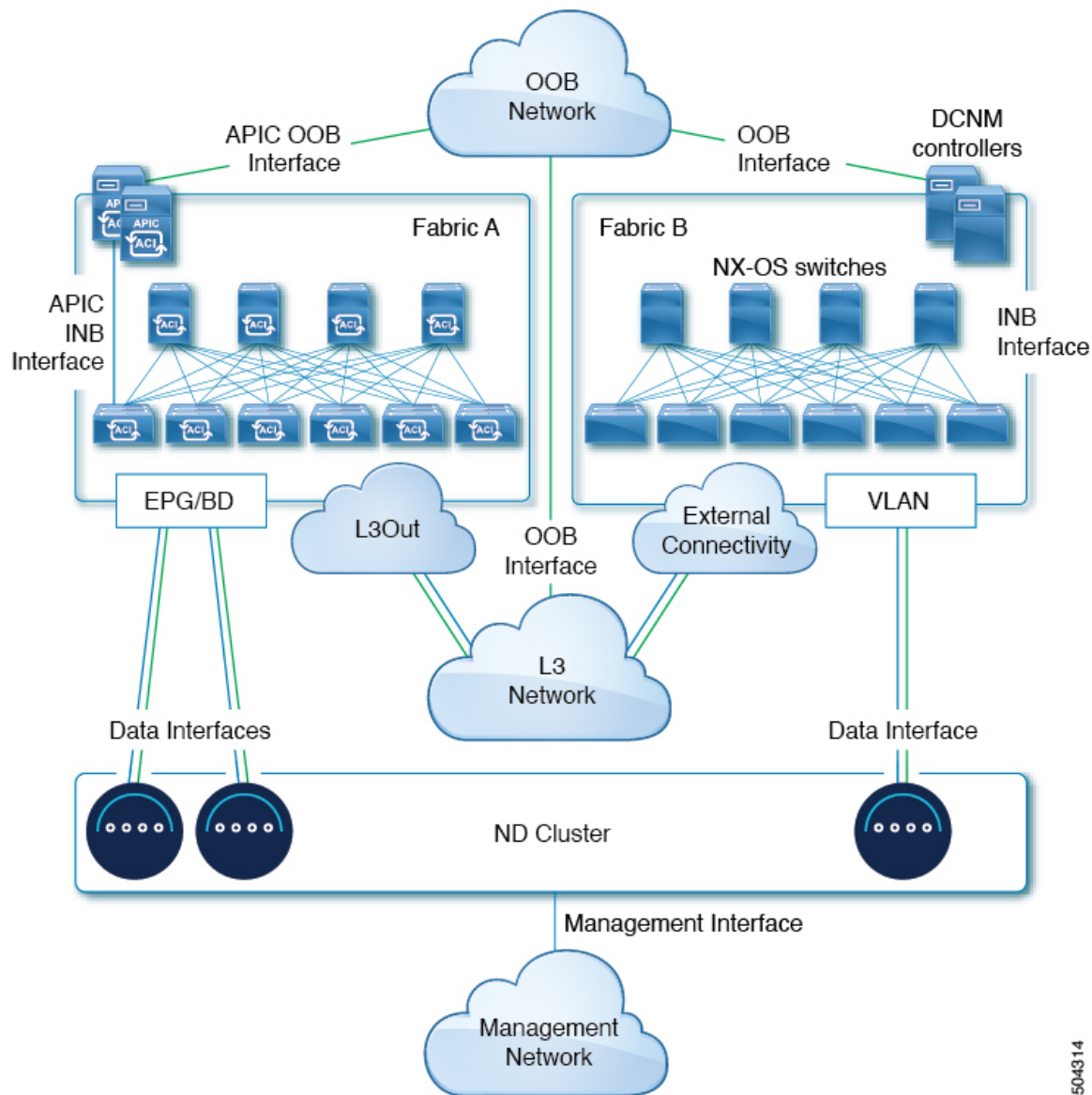
次の2つの図は、Nexus ダッシュボード クラスタをファブリックのリーフスイッチに直接接続する場合の2つの異なるネットワーク接続シナリオを示しています。それぞれの主な目的は、Nexus ダッシュボードで実行しているアプリケーションのタイプによって異なります。

図 4: リーフスイッチへの直接接続、2日目の運用アプリケーション



504813

図 5: リーフスイッチ、Nexus ダッシュボードオーケストレータへの直接接続



504314

サイト間のノード分散

Nexus ダッシュボードは、複数のサイトへのクラスタ ノードの分散をサポートします。次のノード分散の推奨事項は、物理クラスタと仮想クラスタの両方に適用されます。

Nexus Dashboard インサイトのノード配布

Nexus ダッシュボード Insights サービスには、一元化された単一サイトの展開をお勧めします。このサービスは、ノードが異なるサイトにある場合に、クラスタを相互接続障害にさらす可能性がある分散クラスタの冗長性の利点を得ることができません。

Nexus Dashboard オークストレータ およびファブリック コントローラのノード配布

Nexus Dashboard Orchestrator と Nexus ダッシュボードファブリック コントローラについては、分散クラスタをお勧めします。クラスタが動作し続けるには、少なくとも2つの Nexus ダッシュボードマスター ノードが必要であるため、物理的な Nexus ダッシュボードクラスタを2つのサイトに展開する場合は、次の図に示すように、1つのマスターノードを持つサイトにスタンバイ ノードを展開することを推奨します。



- (注) 次の図は、NDO または NDFC サービスを使用した物理または仮想 Nexus ダッシュボードクラスタの可能な展開シナリオのいくつかの例を示しています。特定のユースケースに必要なノード数の詳細については、[Nexus ダッシュボード キャパシティ プランニング ツール](#)を参照してください。

図 6: Nexus ダッシュボード オークストレータの2つのサイトにまたがるノードの分散

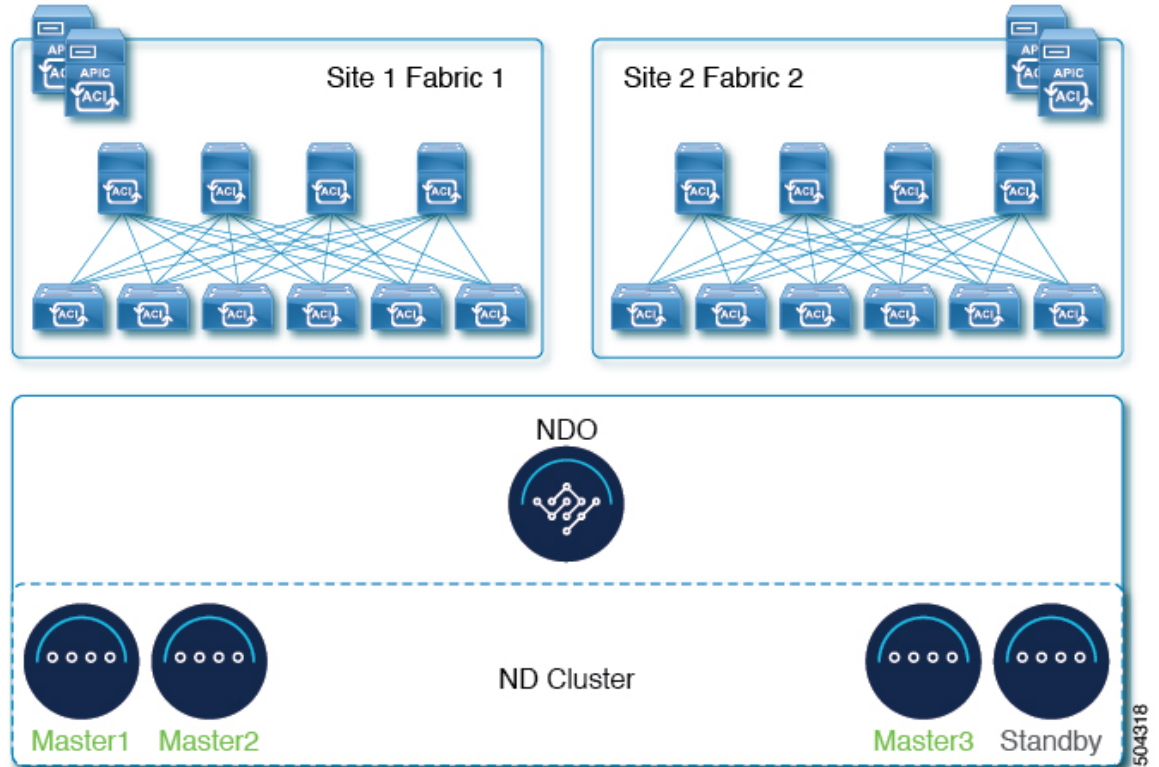
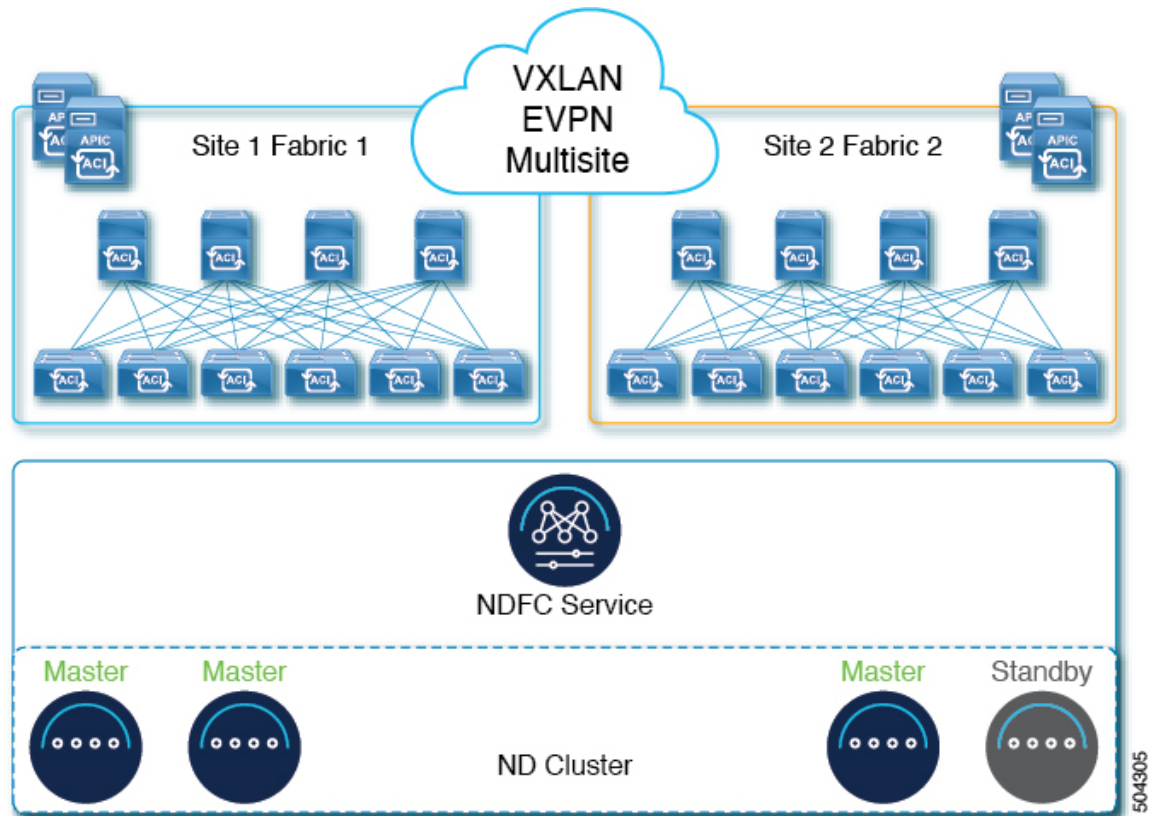
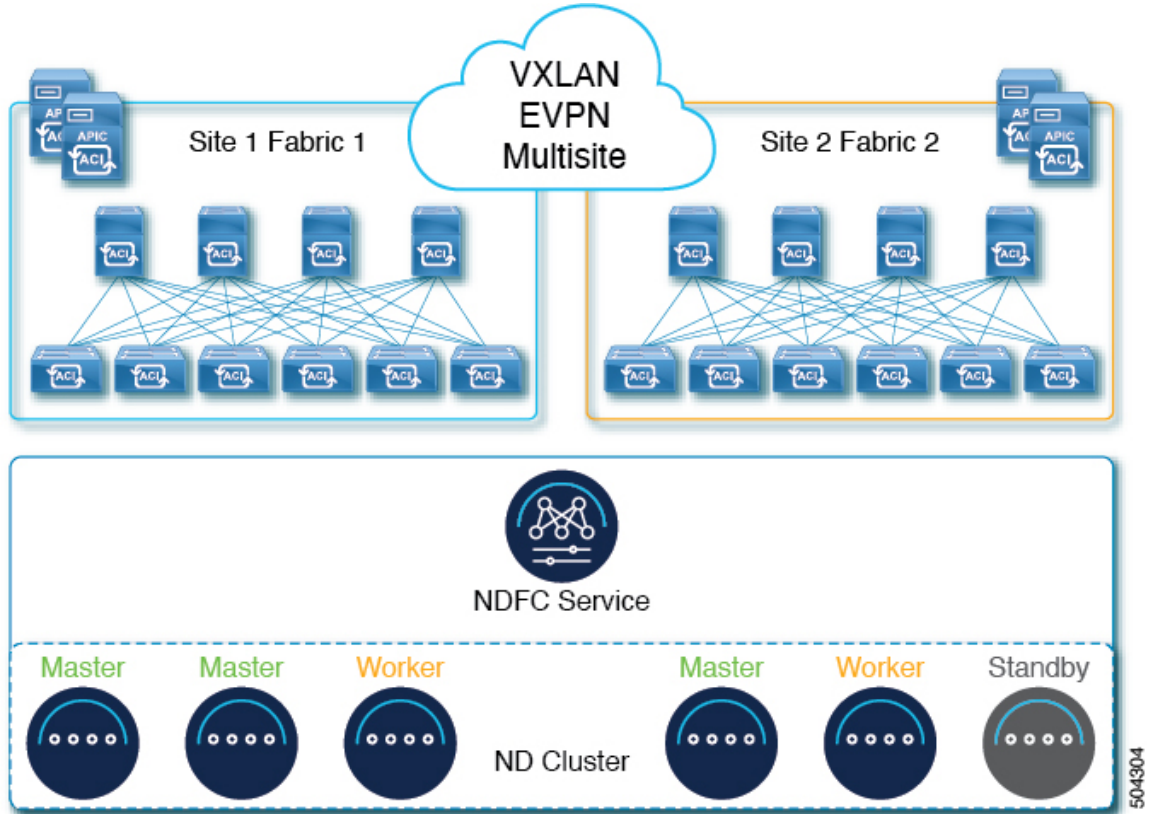


図 7: Nexus Dashboard Fabric Controller の 2つのサイトにまたがるノードの分散 (4ノード)



504305

図 8 : Nexus Dashboard Fabric Controller の 2つのサイトにまたがるノードの分散 (6 ノード)



次の表に、複数のサイトにまたがる物理的な Nexus ダッシュボード マスター (M1、M2、M3) およびスタンバイ (S1) ノードの分散でサポートされる追加のシナリオをまとめます。

表 11: サイト間の Nexus ダッシュボード ノードの分散

サイト数	サイト1のノード	サイト2のノード	サイト3のノード	サイト4のノード
1	M1、M2、M3、S1	--	--	--
2	M1、M2	M3、S1	--	--
3	M1、S1* *スタンバイノードは 3つのサイトのい ずれか1つに追加 可能	M2	M3	--
4	M1	M2	M3	S1

サービスのコロケーションの使用例

このセクションでは、特定の単一サービスまたは複数サービスの共同ホストの使用例について、いくつかの推奨される展開シナリオについて説明します。

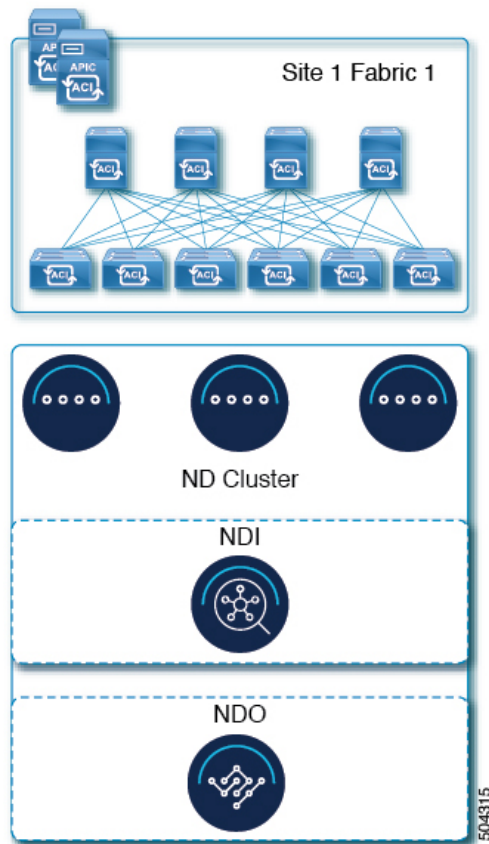


- (注) このリリースは、Linux KVM、AWS、Azure、または RHEL に展開されている Nexus ダッシュボードクラスタでの共同ホスティングサービスをサポートしていません。以下のすべてのサービス共同ホスティングのシナリオは、物理フォームファクタまたは VMware ESX クラスタフォームファクタに適用されます。

単一サイト、Nexus ダッシュボード Insights およびオーケストレータ

Nexus ダッシュボード Insights およびオーケストレータ サービスを使用する単一サイトのシナリオでは、両方のサービスを共存させて単一の Nexus ダッシュボードクラスタを展開できます。

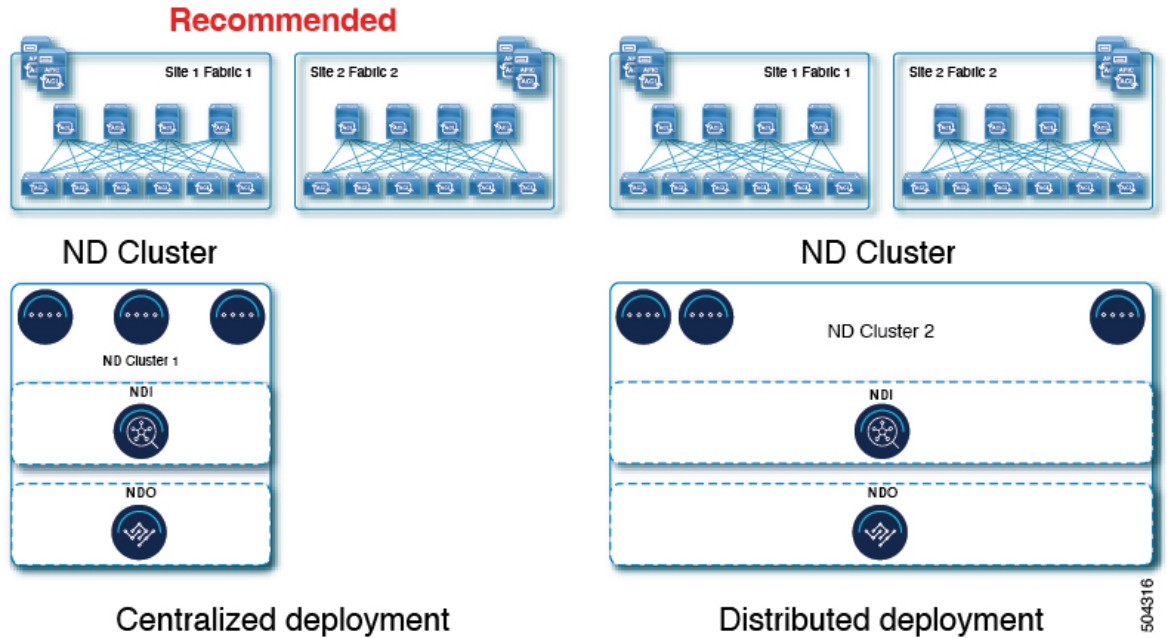
図 9: 単一サイト、Nexus ダッシュボード Insights およびオーケストレータ



Nexus ダッシュボード Insights およびオーケストレータの複数サイト、単一クラスタ

Nexus ダッシュボード Insights およびオーケストレータ サービスを使用する複数サイトのシナリオでは、両方のサービスを共存させて単一の Nexus ダッシュボード クラスタを展開できます。この場合、ノードはサイト間で分散できますが、Insights サービスは分散クラスタから冗長性の利点を得ることができず、ノードが異なるサイトにあるときに相互接続障害にさらされる可能性があるため、左側の展開オプションを推奨します。

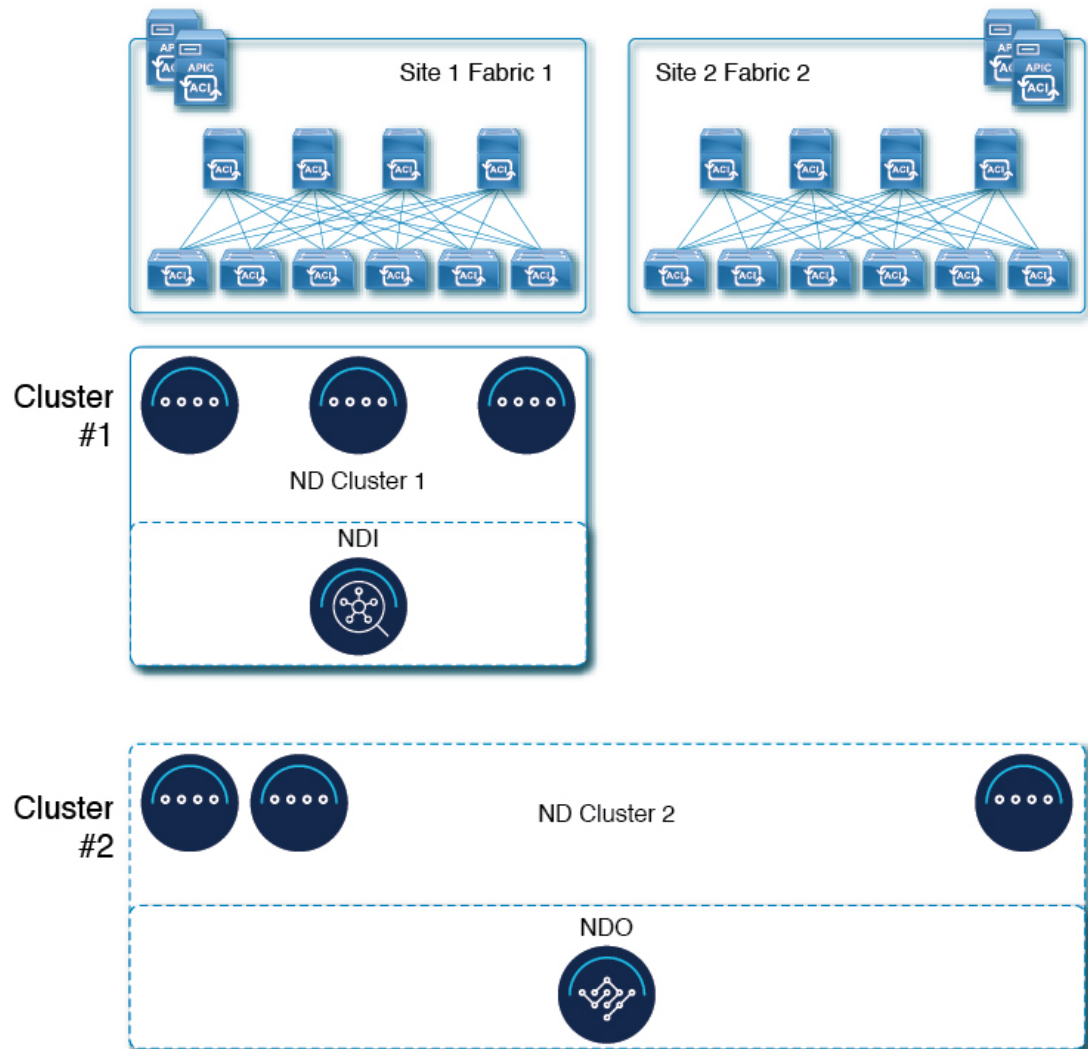
図 10: Nexus ダッシュボード Insights およびオーケストレータの複数サイト、単一クラスタ



Nexus ダッシュボード Insights およびオーケストレータの複数のサイト、複数のクラスタ

この場合、2つの Nexus ダッシュボード クラスタを導入することを推奨します。そのうちの1つは、仮想またはクラウドフォーム ファクタを使用する Nexus ダッシュボード オーケストレータ サービス専用で、サイト全体に分散されたノードです。

図 11: Nexus ダッシュボード Insights およびオーケストレータの複数のサイト、複数のクラスタ



インストール前のチェックリスト

Nexus ダッシュボードクラスタの展開に進む前に、プロセス中に参照しやすいように次の情報を準備します。

表 12: クラスタの詳細

パラメータ (Parameters)	例	入力する値
クラスタ名	nd-cluster	
NTP サーバー	171.68.38.65	

パラメータ (Parameters)	例	入力する値
DNS プロバイダー	64.102.6.247 171.70.168.183	
DNS 検索ドメイン	cisco.com	
アプリ ネットワーク	172.17.0.1/16	
サービスネットワーク	100.80.0.0/16	

表 13: ノードの詳細

パラメータ (Parameters)	例	入力する値
物理ノードの場合、最初のノードの CIMC アドレスとログイン情報	10.195.219.84/24 ユーザ名: admin パスワード: Cisco1234	
物理ノードの場合、2 番目のノードの CIMC アドレスとログイン情報	10.195.219.85/24 ユーザ名: admin パスワード: Cisco1234	
物理ノードの場合、3 番目のノードの CIMC アドレスとログイン情報	10.195.219.86/24 ユーザ名: admin パスワード: Cisco1234	
各ノードのレスキュー ユーザに使用されるパスワードと初期 GUI パスワード。 クラスタ内のすべてのノードに同じパスワードを設定することを推奨します。	Welcome2Cisco!	
最初のノードの 管理 IP	192.168.9.172/24	
最初のノードの管理ゲートウェイ	192.168.9.1	
最初のノードのデータ ネットワーク IP	192.168.6.172/24	
最初のノードのデータ ネットワーク ゲートウェイ	192.168.6.1	
(オプション) 最初のノードのデータ ネットワーク VLAN	101	

パラメータ (Parameters)	例	入力する値
(オプション) 最初のノードの ASN	63331	
(オプション) 最初のノードの BGP ピア の IP アドレス	200.11.11.2 または 200:11:11::2	
(オプション) 最初のノードの BGP ピア の ASN	55555	
2 番目のノードの 管理 IP	192.168.9.173/24	
2 番目のノードの 管理ゲートウェイ 。	192.168.9.1	
2 番目のノードの データ ネットワーク IP	192.168.6.173/24	
2 番目のノードの データ ネットワーク ゲートウェイ	192.168.6.1	
(オプション) 2番目のノードの データ ネットワーク VLAN	101	
(オプション) 2番目のノードの ASN	63331	
(オプション) 2番目のノードの BGP ピア の IP アドレス	200.12.12.2 または 200:12:12::2	
(オプション) 2番目のノードの BGP ピア の ASN	55555	
3 番目のノードの 管理 IP	192.168.9.174/24	
3 番目のノードの 管理ゲートウェイ 。	192.168.9.1	
3 番目のノードの データ ネットワーク IP	192.168.6.174/24	
3 番目のノードの データ ネットワーク ゲートウェイ	192.168.6.1	
(オプション) 3番目のノードの データ ネットワーク VLAN	101	

パラメータ (Parameters)	例	入力する値
(オプション) 3番目のノードの ASN	63331	
(オプション) 3番目のノードの BGP ピア の IP アドレス	200.13.13.2 または 200:13:13::2	
(オプション) 3番目のノードの BGP ピア の ASN	55555	

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。