展開の概要と要件

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。

Nexus Dashboard クラスタは通常、1つまたは3つのプライマリ ノードで構成されます。また、3 ノード クラスタの場合、プライマリ 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 worker ノードをプロビジョニングして、水平スケーリングや standby 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 worker」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。

（注） Nexus Dashboard ソフトウェアへのルートアクセスは、Cisco TAC のみに制限されています。一連の操作とトラブルシューティング コマンドを有効にするために、すべての Nexus Dashboard 展開用に特別なユーザー `rescue-user` が作成されます。使用可能な `rescue-user` コマンドの詳細については、『*Nexus Dashboard ユーザー ガイド*』の「トラブルシューティング」の章を参照してください。

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 ハードウェア セットアップ ガイド*』で説明しています。その他のNexus Dashboardの構成と操作手順については、『*Cisco Nexus Dashboard ユーザー ガイド*』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 などのサービスを展開するには、Nexus Dashboard 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、これらのサービスのイメージ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 Dashboard サーバーを購入する場合、一部のサービスを、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、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。物理フォームファクタは現在、クラスタノード用に 2 つの異なる UCS サーバ（UCS-C220-M5 および UCS-C225-M6）をサポートしており、同じクラスタ内で混在させることができます。

（注） すべてのサービスがすべてのフォームファクタでサポートされているわけではありません。展開を計画するときは、フォームファクタとクラスタサイズの要件についてCisco Nexus Dashboardクラスタのサイズ設定を確認してください。

- 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。

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、Nexus Dashboard クラスタは、最初に 1 つまたは 3 つのプライマリ 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 ツールを参照してください。

（注）

- 単一ノードクラスタは、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 クラスタに拡張することはできません。
- 追加の `worker` または `standby` ノードをサポートするのは 3 ノード クラスタのみです。
- 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 クラスタの場合、クラスタが動作し続けるには、少なくとも 2 つのプライマリ ノードが必要です。2 つのプライマリ ノードに障害が発生した場合、『*Cisco Nexus Dashboard ユーザー ガイド*』の説明に従って回復するまで使用できません。

最初のクラスタが稼働したら、*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。

リリース 3.0(1) 以降、Nexus Dashboard は対称キーを使用した NTP 認証もサポートしています。NTP 認証を有効にする場合は、次の情報を入力する必要があります。

- **NTP キー**：Nexus Dashboard と NTP サーバ間の NTP トラフィックを認証するために使用される暗号キー。次の手順で NTP サーバーを定義します。複数の NTP サーバで同じ NTP キーを使用できます。
- **キー ID**：各 NTP キーに一意のキー ID を割り当てる必要があります。この ID は、NTP パケットの検証時に使用する適切なキーを識別するために使用されます。
- **認証タイプ**：このリリースでは、`MD5`、`SHA`、および`AES128CMAC` 認証タイプがサポートされています。

NTP 認証を有効にする場合は、次の注意事項が適用されます。

- 対称認証の場合、使用するキーは、NTP サーバーと Nexus Dashboard の両方で同じに構成をする必要があります。

  ID、認証タイプ、およびキー/パスフレーズ自体が一致し、NTP サーバーと Nexus Dashboard の両方で信頼されている必要があります。

- 複数のサーバーが同じキーを使用できます。

  この場合、キーは Nexus Dashboard で 1 回だけ構成してから、複数のサーバーに割り当てる必要があります。

- キー ID が一意である限り、Nexus Dashboard と NTP サーバの両方に複数のキーを設定できます。
- このリリースでは、NTP キーの SHA1、MD5、および AES128CMAC 認証/エンコーディング タイプがサポートされています。

（注） セキュリティが高い AES128CMAC を使用することを推奨します。

- Nexus Dashboard で NTP キーを追加する場合は、`信頼できる` としてタグ付けする必要があります。信頼できないキーは認証に失敗します。

  このオプションを使用すると、キーが侵害された場合に Nexus Dashboard で特定のキーを簡単に無効にすることができます。

- Nexus Dashboard で一部の NTP サーバーを優先としてタグ付けすることを選択できます。

  NTP クライアントは、RTT、応答時間の差異、およびその他の変数を考慮することで、時間の経過に伴う NTP サーバーの「品質」を推定できます。プライマリ サーバーを選択する場合、優先サーバーの優先順位が高くなります。

- `ntpd` を実行している NTP サーバーを使用している場合は、少なくともバージョン 4.2.8p12 を推奨します。

- 以下の制限事項がすべての NTP キーに適用されます。

  - SHA1 および MD5 キーの最大長は 40 文字ですが、AES128 キーの最大長は 32 文字です。
  - 20 文字未満のキーには、「#」とスペースを除く任意の ASCII 文字を含めることができます。長さが 20 文字を超えるキーは、16 進形式である必要があります。
  - キー ID は 1 ～ 65535 の範囲で指定する必要があります。
  - 1 つの NTP サーバーのキーを構成する場合は、他のすべてのサーバーのキーも構成する必要があります。

NTP 認証の有効化と構成については、後のセクションで展開手順の一部として説明します。

BGP 構成と永続的な IP

Nexus Dashboard の以前のリリースでは、サービスが異なる Nexus Dashboard 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 Dashboard 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、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 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。

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
• 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 通信へのNexus Dashboard ノード 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。	• 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 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 • 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。

（注） Nexus Dashboard ファブリック コントローラ（SAN コントローラ）を除き、データ ネットワークと管理ネットワークに同じサブネットを使用して Nexus Nexus Dashboard に展開できます。

- 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 NDFC 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るため、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 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
SFLOW/NetFlow（ACI または NDFC 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 Dashboard ファブリック コントローラ、リリース 12.1.3	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
			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 • 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 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

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
			• 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 LAN 展開タイプのレイヤ 3 モードで動作している場合：

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
			• [**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。 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。 SAN コントローラ展開タイプのレイヤ 2 またはレイヤ 3 モードで動作している場合：

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
			• SSH 用の 1 つの IP • SNMP/Syslog 用の 1 つの IP • SAN Insights 機能用の Nexus Dashboard クラスタ ノードごとに 1 つの IP メディア用の 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

- 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	クラスタ内のノード間	150 ミリ秒
Nexus Dashboard マルチクラスタ接続	マルチクラスタ接続を介して接続されたクラスタ間のノード間 マルチクラスタ接続の詳細については、『*Cisco Nexus Dashboard* インフラストラクチャ管理』を参照してください。	500 ミリ秒

サービス	接続	最大 RTT
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
	スイッチ	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
	スイッチ	200 ms*

* POAP（PowerOn Auto Provisioning）は、Nexus Dashboard ファブリック コントローラとスイッチ間の最大 RTT 50 ミリ秒でサポートされます。

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、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、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。

IPv4 および IPv6 のサポート

Nexus Dashboard の以前のリリースでは、クラスタ ノードの純粋な IPv4 構成またはデュアル スタック IPv4/IPv6（管理ネットワークのみ）構成がサポートされていました。リリース 3.0(1) 以降、Nexus Dashboard は、クラスタ ノードおよびサービスの純粋な IPv4、純粋な IPv6、またはデュアル スタック IPv4/IPv6 構成をサポートします。

IP 構成を定義するとき、以下のガイドラインが適用されます。

- クラスタ内のすべてのノードとネットワークは、純粋な IPv4、純粋な IPv6、またはデュアル スタック IPv4/IPv6 のいずれかの均一な IP 構成を持つ必要があります。
- クラスタを純粋な IPv4 モードで展開し、デュアル スタック IPv4/IPv6 または純粋な IPv6 に切り替える場合は、クラスタを再展開する必要があります。
- デュアル スタック構成の場合：
  - 外部（データと管理）ネットワークと内部（アプリケーションとサービス）ネットワークの両方がデュアル スタック モードである必要があります。

    IPv4 データ ネットワークやデュアル スタック管理ネットワークなどの部分的な構成はサポートされていません。
  - IPv6 アドレスは、物理サーバの CIMC にも必要です。
  - ノードの初期起動時にノードの管理ネットワークに IPv4 または IPv6 アドレスを構成できますが、クラスタのブートストラップ ワークフロー中に両方のタイプの IP を指定する必要があります。

    管理 IP は、初めてノードにログインしてクラスタのブートストラップ プロセスを開始するために使用されます。

- すべての内部証明書は、IPv4 と IPv6 の両方のサブジェクト代替名（SAN）を含むように生成されます。
- Kubernetes 内部コア サービスは IPv4 モードで開始されます。
- DNS は、IPv4 と IPv6 の両方にサービスを提供して転送し、両方のタイプのレコードをサーバに提供します。
- ピア接続用のVxLANオーバーレイは、データネットワークのIPv4アドレスを使用します。

  IPv4 パケットと IPv6 パケットは両方とも、VxLAN の IPv4 パケット内にカプセル化されます。
- UI は、IPv4 と IPv6 の両方の管理ネットワーク アドレスでアクセスできます。

- 純粋な IPv6 構成の場合：
  - 純粋な IPv6 モードは、物理および仮想フォーム ファクタのみでサポートされます。

    AWS、Azure、または既存の Red Hat Enterprise Linux（RHEL）システムに展開されたクラスタは、純粋な IPv6 モードをサポートしていません。
  - ノードを最初に構成するときに、IPv6 管理ネットワーク アドレスを指定する必要があります。

    ノード（物理、仮想、またはクラウド）が起動した後、これらの IP を使用して UI にログインし、クラスタのブートストラップ プロセスを続行します。
  - 前述の内部アプリケーションおよびサービス ネットワークに IPv6 CIDR を提供する必要があります。
  - 前述のデータ ネットワークと管理ネットワークに IPv6 アドレスとゲートウェイを提供する必要があります。
  - すべての内部証明書は、IPv6 サブジェクト代替名（SAN）を含むように生成されます。
  - すべての内部サービスは IPv6 モードで開始されます。
  - ピア接続用のVxLANオーバーレイは、データネットワークのIPv6アドレスを使用します。

    IPv6 パケットは、VxLAN の IPv6 パケット内にカプセル化されます。
  - すべての内部サービスは IPv6 アドレスを使用します。

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、移行中に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
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

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
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
DNS	53	TCP および UDP	入力 / 出力	他のクラスタノードと DNS サーバー
NFSv3	111	TCP および UDP	入力 / 出力	リモート NFS サーバー
HTTPS	443	TCP	発信	スイッチと APIC の帯域内
NFSv3	608	UDP	入力 / 出力	リモート NFS サーバー
SSH	1022	TCP および UDP	入力 / 出力	その他のクラスタ ノード
NFSv3	2049	TCP	入力 / 出力	リモート NFS 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
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
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 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
テックコレクションを表示	2022	TCP	入力 / 出力	スイッチと APIC/NDFC の帯域内
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	その他のクラスタ ノード
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
Kafka	30001	TCP	入力 / 出力	スイッチと APIC/NDFC の帯域内 IP
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 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。
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 ィン：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）
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 *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 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）
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。 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。

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）
TFTP（POAP）	69	TCP	入力	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。 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。 これは、LAN 展開にのみ適用されます。

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 （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）
HTTP（POAP）	80	TCP	入力	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。 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。 これは、LAN 展開にのみ適用されます。

サービス	ポート	プロトコル	方向 ィン：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）
BGP	179	TCP	入力 / 出力	エンドポイント ロケーターの場合、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。 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。 これは、LAN 展開にのみ適用されます。
HTTPS（POAP）	443	TCP	入力	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。 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。 これは、LAN 展開にのみ適用されます。

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 （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	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。 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。
SCP	2022	TCP	発信	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。 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。

サービス	ポート	プロトコル	方向 ィン：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）
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 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）
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	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。 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。

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	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。
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。

ファブリック接続

ここでは、Nexus Dashboard クラスタ ノードを管理とデータ ネットワークに接続し、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。

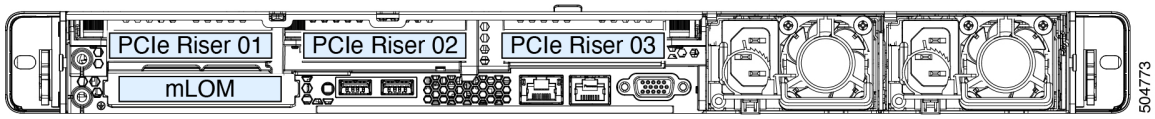
Cisco Cloud Network Controller ファブリックの場合は、レイヤ 3 ネットワーク経由で接続する必要があります。

物理ノードのケーブル接続

（注） 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。

物理ノードは、次のネットワーク カードを使用して、UCS-C220-M5 および UCS-C225-M6 物理サーバーに展開できます。

図 *1 : ノード接続に使用される mLOM および PCIe ライザー 01 カード*



- 両方のサーバーに、Nexus Dashboard 管理ネットワークへの接続に使用する Modular LAN on Motherboard (mLOM) カードが付属しています。
- UCS-C220-M5 サーバーには、「`PCIe-Riser-01`」スロットに 4 ポートの VIC1455 カードが含まれており (上の図を参照)、Nexus Dashboard のデータ ネットワーク接続に使用します。
- UCS-C225-M6 サーバーには、「`PCIe-Riser-01`」スロット（上の図に表示）に 2x10GbE NIC (`APIC-P-ID10GC`) または 2x25/10GbE SFP28 NIC（`APIC-P-I8D25GF`）が含まれており、Nexus Dashboard のデータ ネットワーク接続に使用します。

ノードを管理ネットワークおよびデータ ネットワークに接続する場合：

- 管理ネットワークの場合、mLOM カードで `mgmt0` および `mgmt1` を使用する必要があります。
- UCS-C220-M5 サーバーのデータ ネットワークでは、VIC1455 カードを使用する必要があります。
  - すべてのポートは、10G または 25G のいずれかの同じ速度である必要があります。

- ポート 1 は Nexus Dashboard の `fabric0` に対応し、ポート 2 は `fabric1` に対応します。

  データ ネットワーク接続には、`fabric0` と `fabric1` の両方を使用できます。

- UCS-C225-M6 サーバーでのデータ ネットワークの場合、2x10GbE NIC (`APIC-P-ID10GC`)、または 2x25/10GbE SFP28 NIC (`APIC-P-I8D25GF`)、または VIC1455 カードを使用できます。
  - すべてのポートは、10G または 25G のいずれかの同じ速度である必要があります。
  - ポート 1 は Nexus Dashboard の `fabric0` に対応し、ポート 2 は `fabric1` に対応します。

    データ ネットワーク接続には、`fabric0` と `fabric1` の両方を使用できます。

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 (PC) および Virtual PortChannel (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

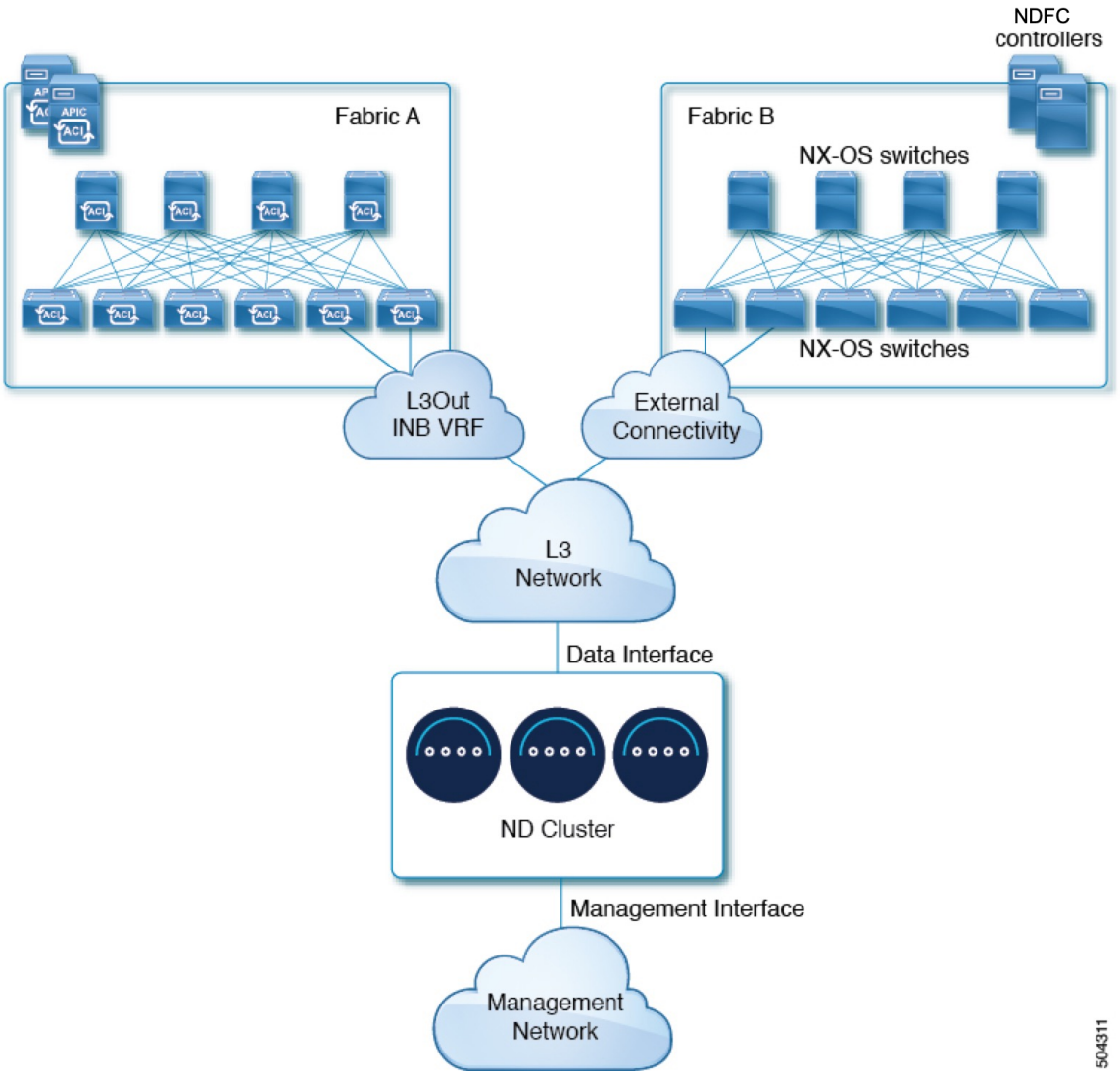
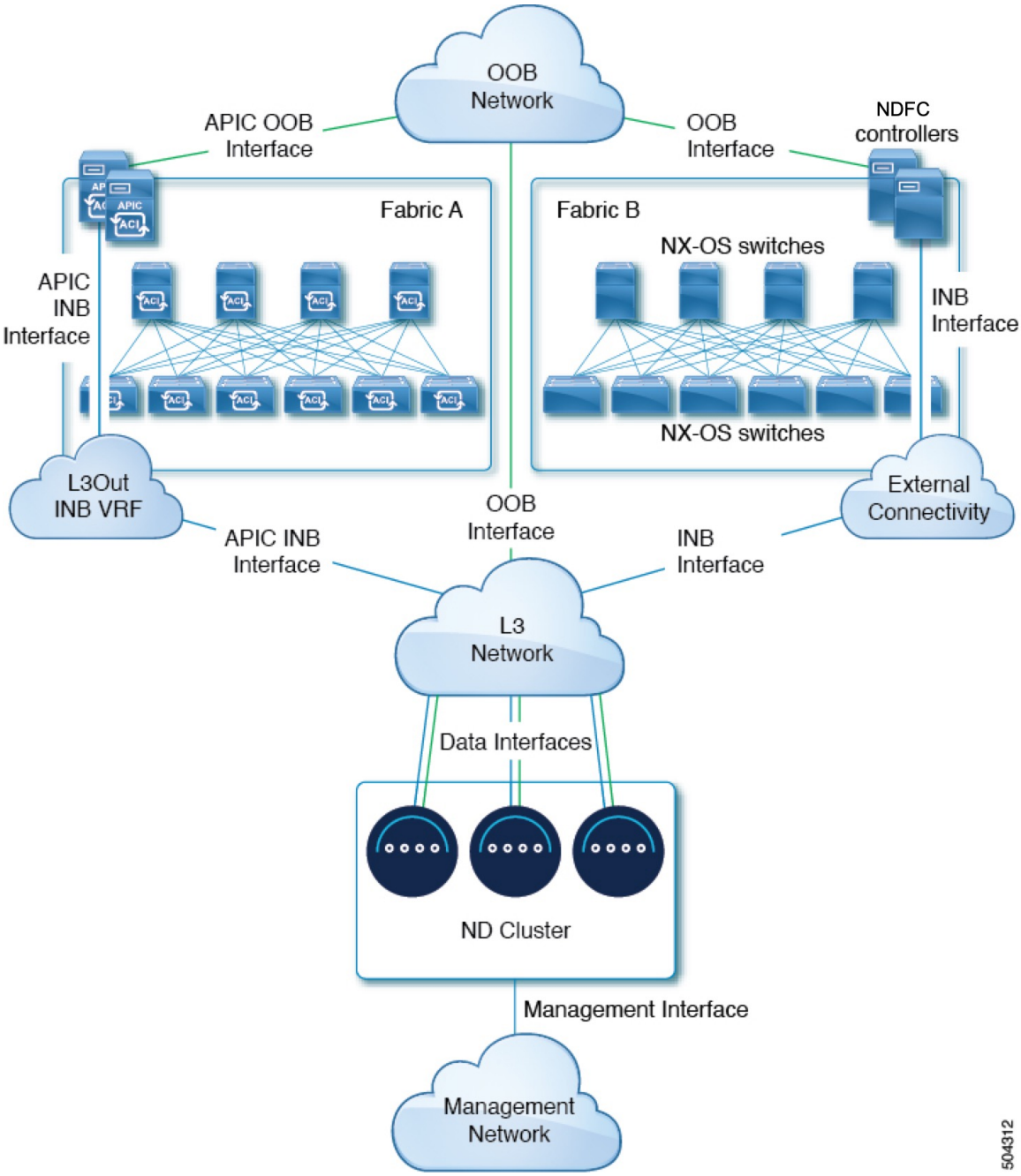


図 *3 :* レイヤ*3*ネットワーク、*Nexus Dashboard Orchestrator*を介した接続



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

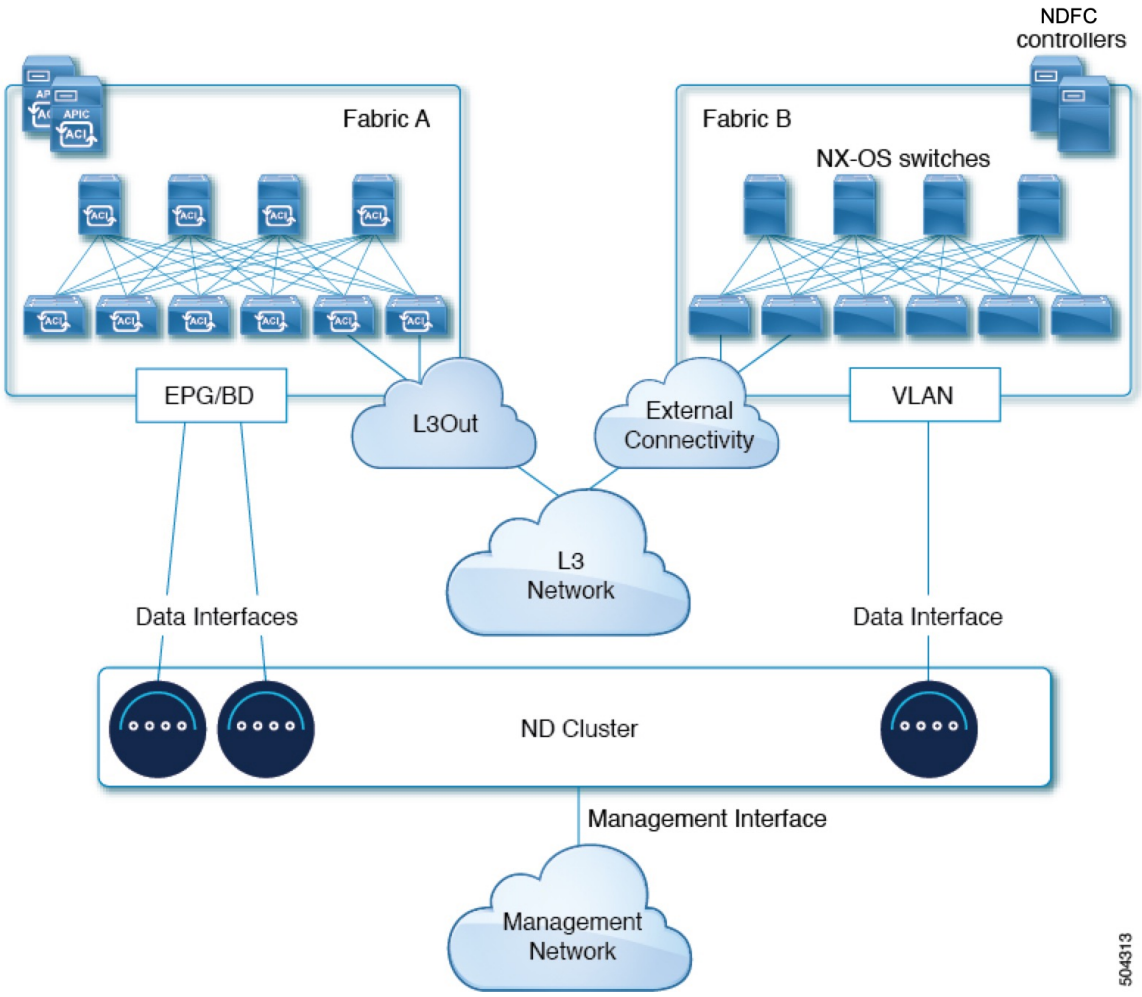
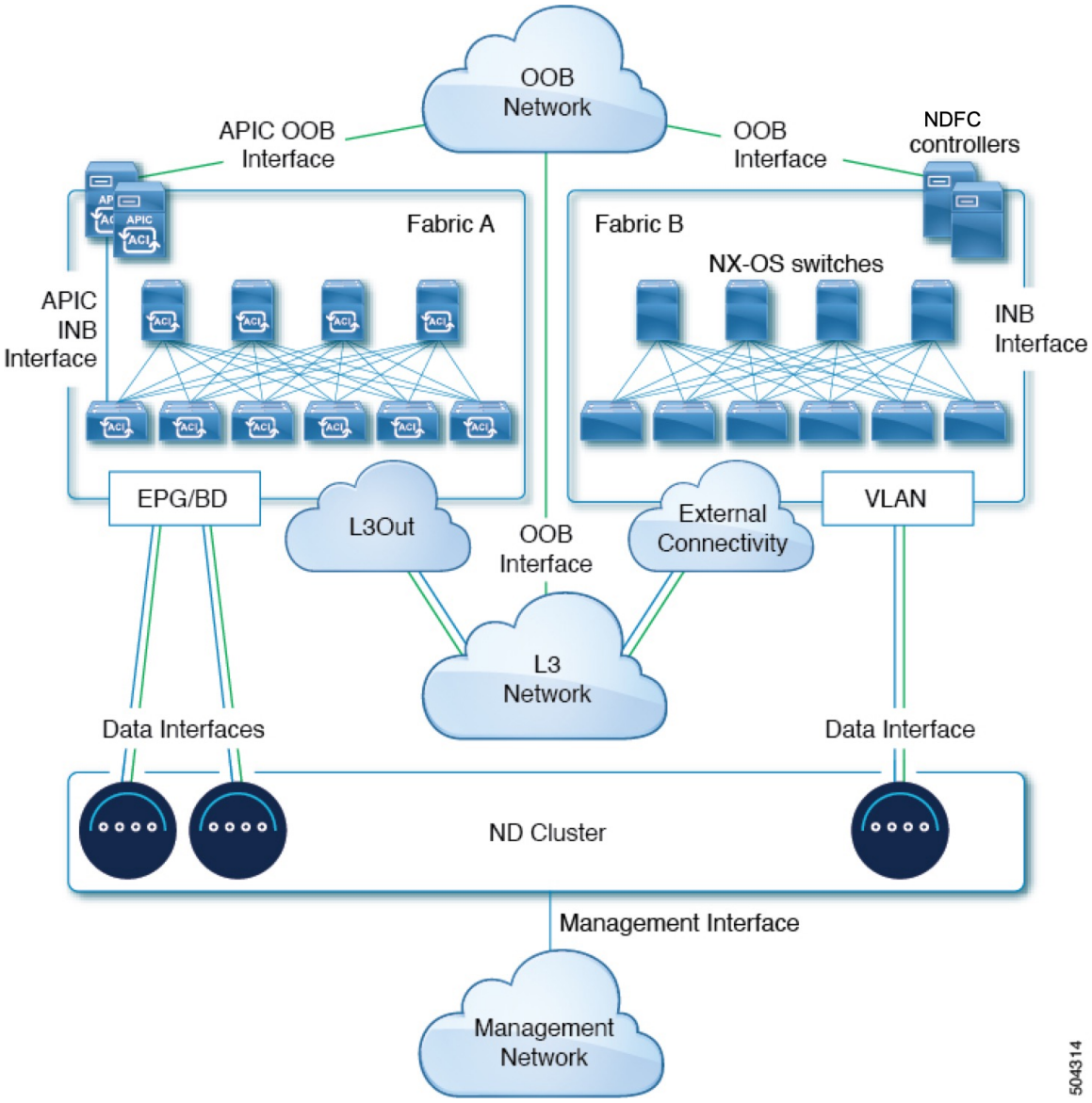


図 *5:* リーフ スイッチ、*Nexus* ダッシュボード オーケストレータへの直接接続



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。

（注） 次のセクションのこのダイアグラムは、物理または仮想の Nexus Dashboard クラスター ノードで考えられる展開シナリオのいくつか例を示しています。特定のユース ケースに必要な正確なノード数の詳細については、Nexus Dashboard キャパシティ プランニング ツールを参照してください。

Nexus Dashboard Insights のノード配布

Nexus Dashboard 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、2 つのプライマリ ノードが使用できない場合、回復をサポートしていないため、分散クラスタから冗長性の利点が得られず、ノードが異なるサイトにある場合クラスタが相互接続障害が発生する可能性があります。

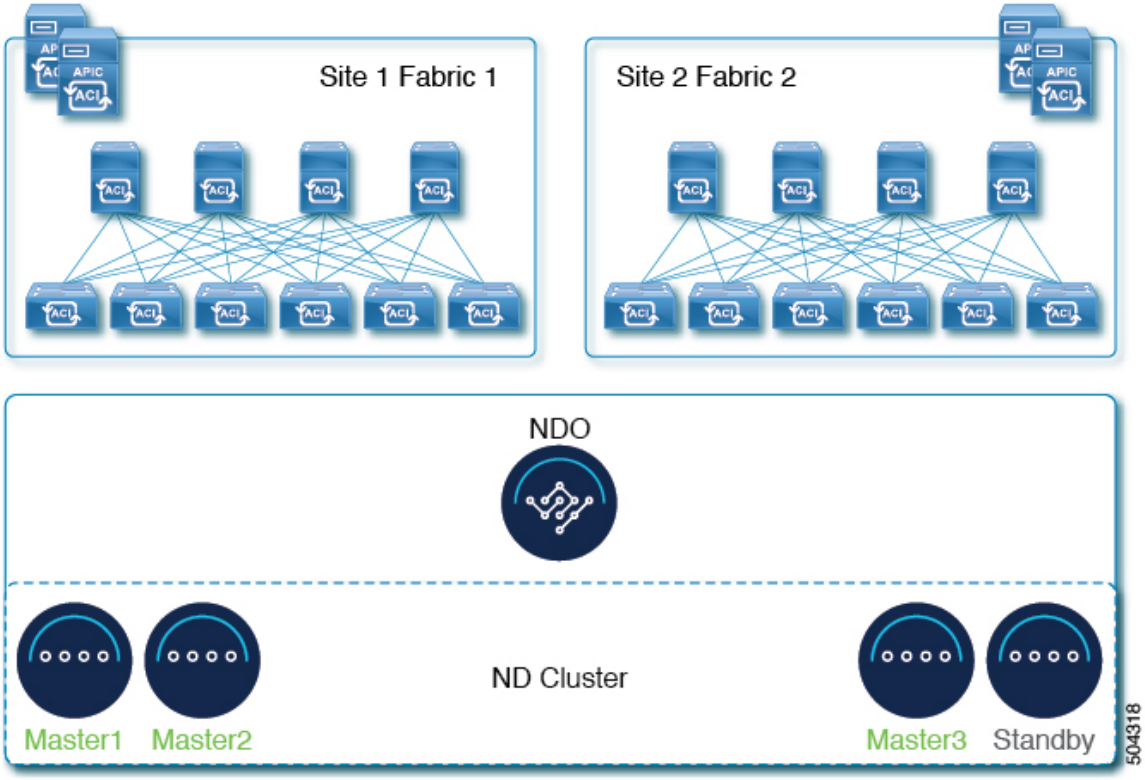
ファブリック コントローラのノード分散

Nexus Dashboard Fabric Controller 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、2 つのプライマリ ノードが使用できない場合、回復をサポートしていないため、分散クラスタから冗長性の利点が得られず、ノードが異なるサイトにある場合クラスタが相互接続障害が発生する可能性があります。

Nexus Dashboard Orchestrator のノードの分散

Nexus Dashboard Orchestrator の場合は、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 Dashboard プライマリ ノードが必要であるため、Nexus Dashboard 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 つのプライマリ 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。

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



サービスのコロケーションの使用例

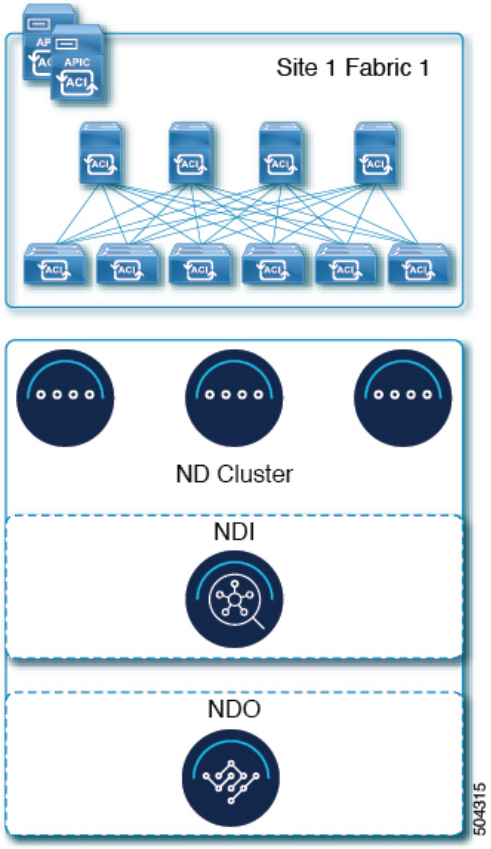
このセクションでは、特定の単一サービスまたは複数サービスの共同ホストの使用例について、いくつかの推奨される展開シナリオについて説明します。

（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。クラスタのサイジングと展開計画の参考情報については、『Cisco Nexus ダッシュボード クラスタ サイジング ツール』を参照してください。

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。

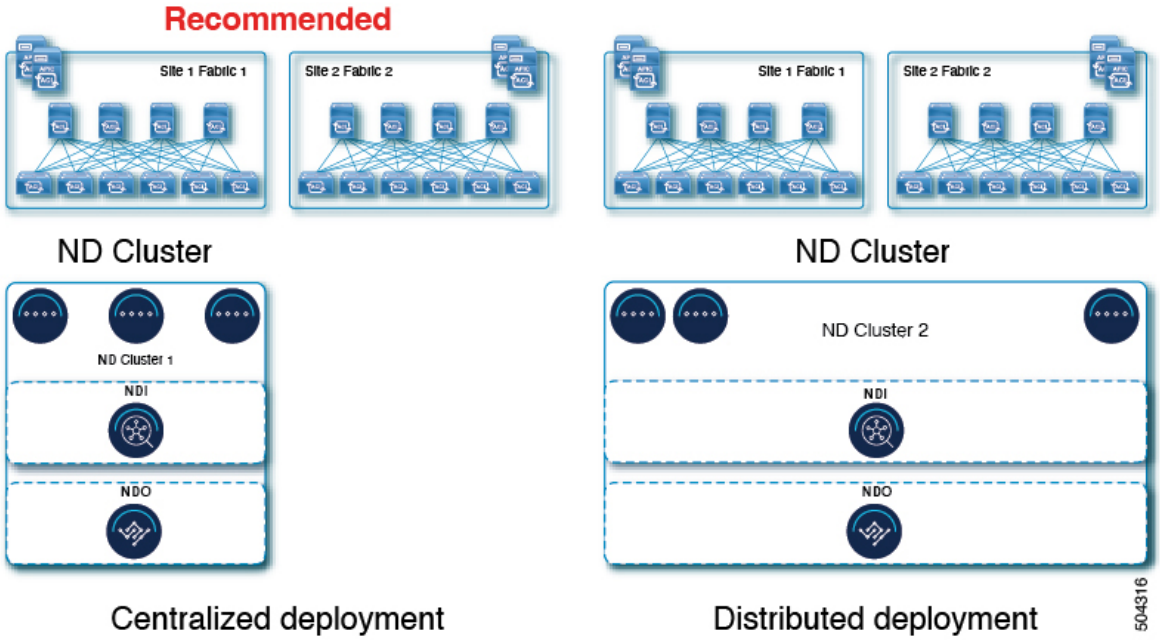
図 *7:* 単一サイト、*Nexus* ダッシュボード *Insights* およびオーケストレータ



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。

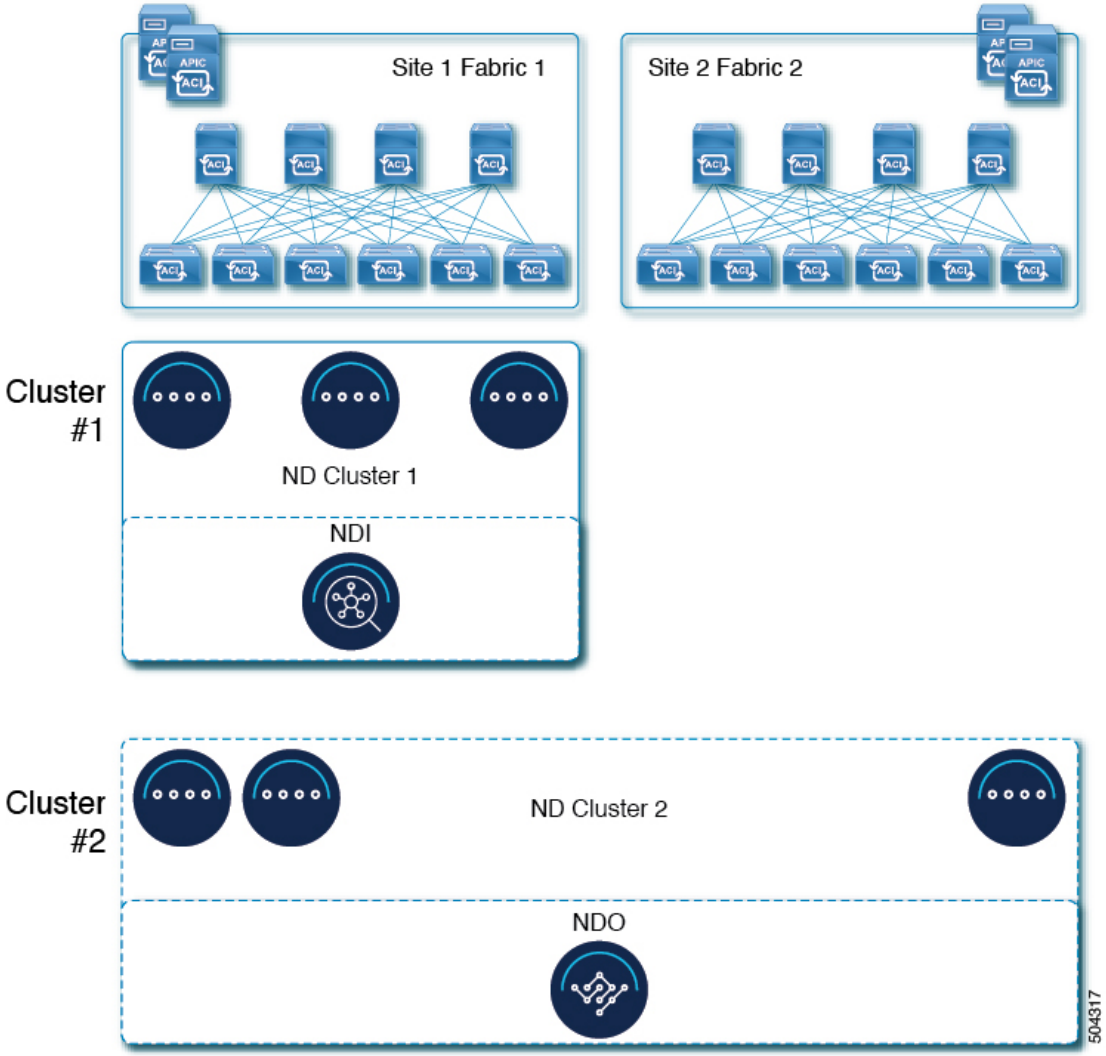
図 *8 : Nexus* ダッシュボード *Insights* およびオーケストレータの複数サイト、単一クラスタ



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 *9* : *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 *11* : 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	172.17.0.0/16	
サービスネットワーク	100.80.0.0/16	

表 *12 :* 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
BGP を有効にする場合、最初のノードの **ASN**	63331	
BGP を有効にし、純粋な IPv6 展開を使用する場合、最初のノードの**ルータ ID**（IPv4 アドレスの形式）	1.1.1.1	
BGP を有効にする場合、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	
BGP を有効にする場合、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	
BGP を有効にする場合、2 番目のノードの **ASN**	63331	
BGP を有効にし、純粋な IPv6 展開を使用する場合、2番目のノードの**ルータ ID**（IPv4 アドレスの形式）	2.2.2.2	
BGP を有効にする場合、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	
BGP を有効にする場合、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	

パラメータ（**Parameters**）	例	入力する値
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`	
BGP を有効にする場合、3 番目のノードの **ASN**	`63331`	
BGP を有効にし、純粋な IPv6 展開を使用する場合、3番目のノードの**ルータ ID**（IPv4アドレスの形式）	`3.3.3.3`	

BGP を有効にする場合、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`	

BGP を有効にする場合、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。