前提条件：Nexus Dashboard

前提条件とガイドライン

（注） このセクションでは、Nexus Dashboard クラスタで有効にできるすべてのサービスに共通の要件とガイドラインについて説明します。サービス固有のその他の要件は、このドキュメントの次のセクションに記載されています。

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（到達不能な IP アドレス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し、通常のサービスの機能にも影響が及びます。

（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。

Nexus Dashboard は、ワイルドカード レコードを持つ DNS サーバーは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、クラスタの構成時に次の情報を入力する必要があります。

- **NTP キー**：Nexus ダッシュボードと 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 の両方で同じ構成にする必要があります。

  ID、認証タイプ、およびキー/パスフレーズ自体は、NTP サーバーと Nexus ダッシュボードの両方で一致し、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。

Nexus ダッシュボード外部ネットワーク

Nexus Dashboardはクラスタとして展開され、各サービスノードは2つのネットワークに接続されます。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 Dashboard にインストールされる個々のサービスは、次のセクションで説明するように、追加の目的で 2 つのネットワークを使用する場合があります。

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。 • スイッチおよびオンボード ファブリックのテレメトリ トラフィック	• 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 • 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 サービスだけを実行するNexus Dashboard クラスタは例外です。これは、データ ネットワークと管理ネットワークで同じサブネットを使用して展開できます。

- 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。
- 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。
- 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。

（注） データ ネットワーク トラフィックに使用されるスイッチ ポートに外部 VLAN タグが設定されている場合は、ジャンボ フレームをイネーブルにするか、1504 バイト以上のカスタム MTU を設定する必要があります。

- 両方のネットワークでノード間の接続が必要です。そして、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 Dashboard クラスタからサイト コントローラまたはスイッチへの接続に関するRTT要件は、有効にする予定のサービスに応じて異なります。以下のサービス固有の章の「ネットワーク要件」セクションを参照してください。

表 *2:* クラスタの *RTT* 要件

接続	最大 RTT
同じ Nexus Dashboard クラスタ内のノード間	50 ミリ秒

接続	最大 RTT
あるクラスタ内のノードと別のクラスタ内のノード間（クラスタがマルチクラスタ接続を介して接続されている場合） 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

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混合構成はサポートされていません。
  - 物理的なサーバーの CIMC にも IPv6 アドレスが必要です。
  - 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。
  - Kubernetes 内部コア サービスは IPv4 モードで開始されます。
  - DNS は IPv4 要求と IPv6 要求の両方を処理し、転送します。
  - 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 および Azure 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。

BGP 構成と永続的な IP

Nexus Dashboard の以前の一部のリリースでは、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（Insights やファブリック コントローラなど）に対しては、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。

この機能は引き続きサポートされていますが、このリリースでは、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 機能を構成することができます。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、インフラストラクチャ管理ドキュメントの「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。

- 以下のサービス固有のセクションに記載されている、サービス固有の永続 IP 要件を満たしていることを確認します。

各サービスに必要な永続 IP の総数は、以下のサービス固有の要件のセクションに記載されています。

通信ポート

Nexus Dashboard クラスタには、次のポートが必要です。

（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。

表 *3 : 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

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
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 *4 : 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、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

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
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
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

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	30019	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

ファブリック接続

ここでは、Nexus Dashboard クラスタ ノードを管理ネットワークとデータ 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。
- 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。

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 Dashboard オーケストレータを展開する場合は、データ インターフェイスまたは管理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）インターフェイスあるいは両方への接続を確立できます。

  ファブリック接続が Nexus ダッシュボードの管理インターフェイスからのものである場合は、特定のスタティック ルートを設定するか、管理インターフェイスが APIC インターフェイスの同じ IP サブネットの一部であることを確認する必要があります。

- 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 *1* : 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

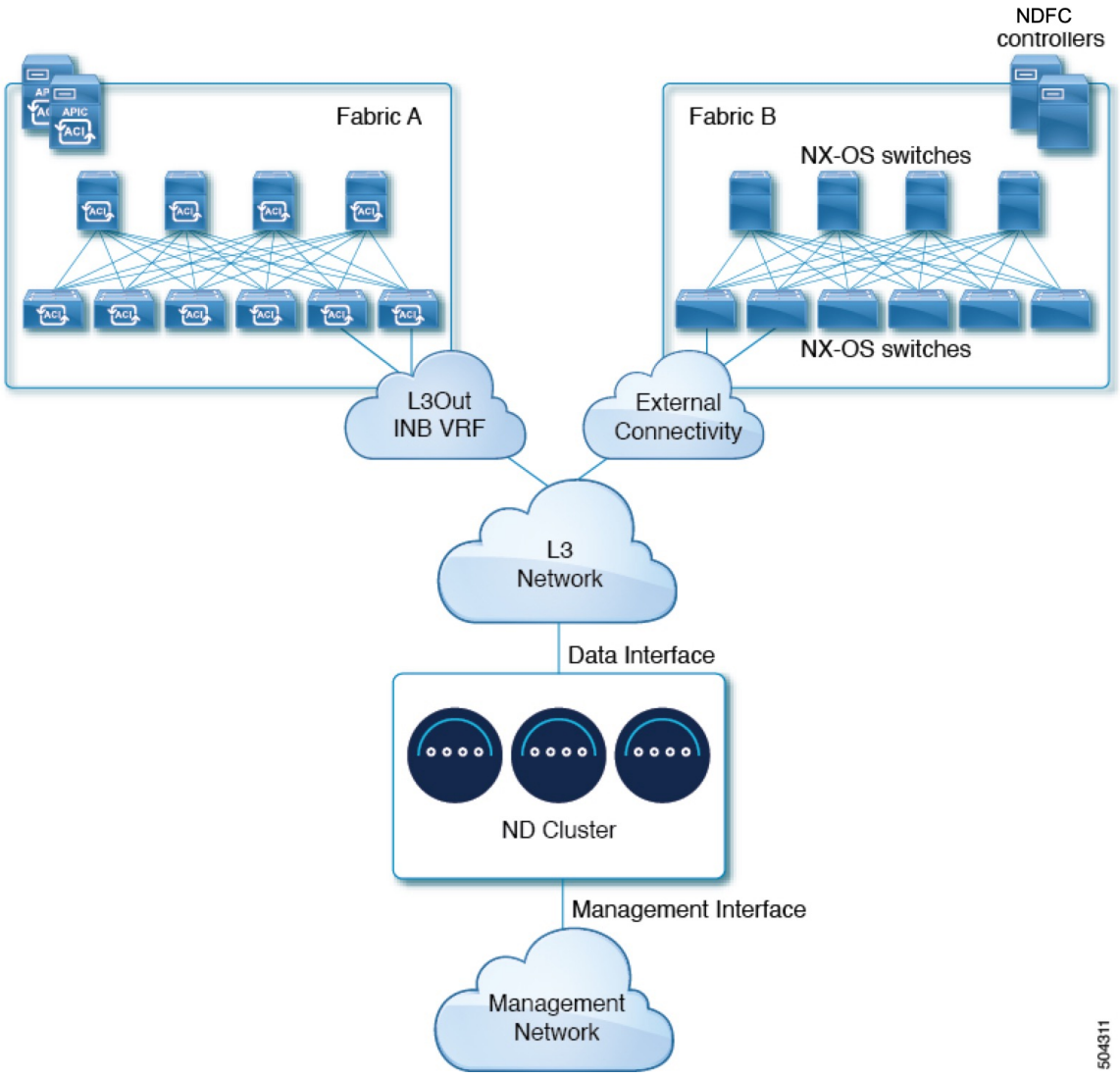
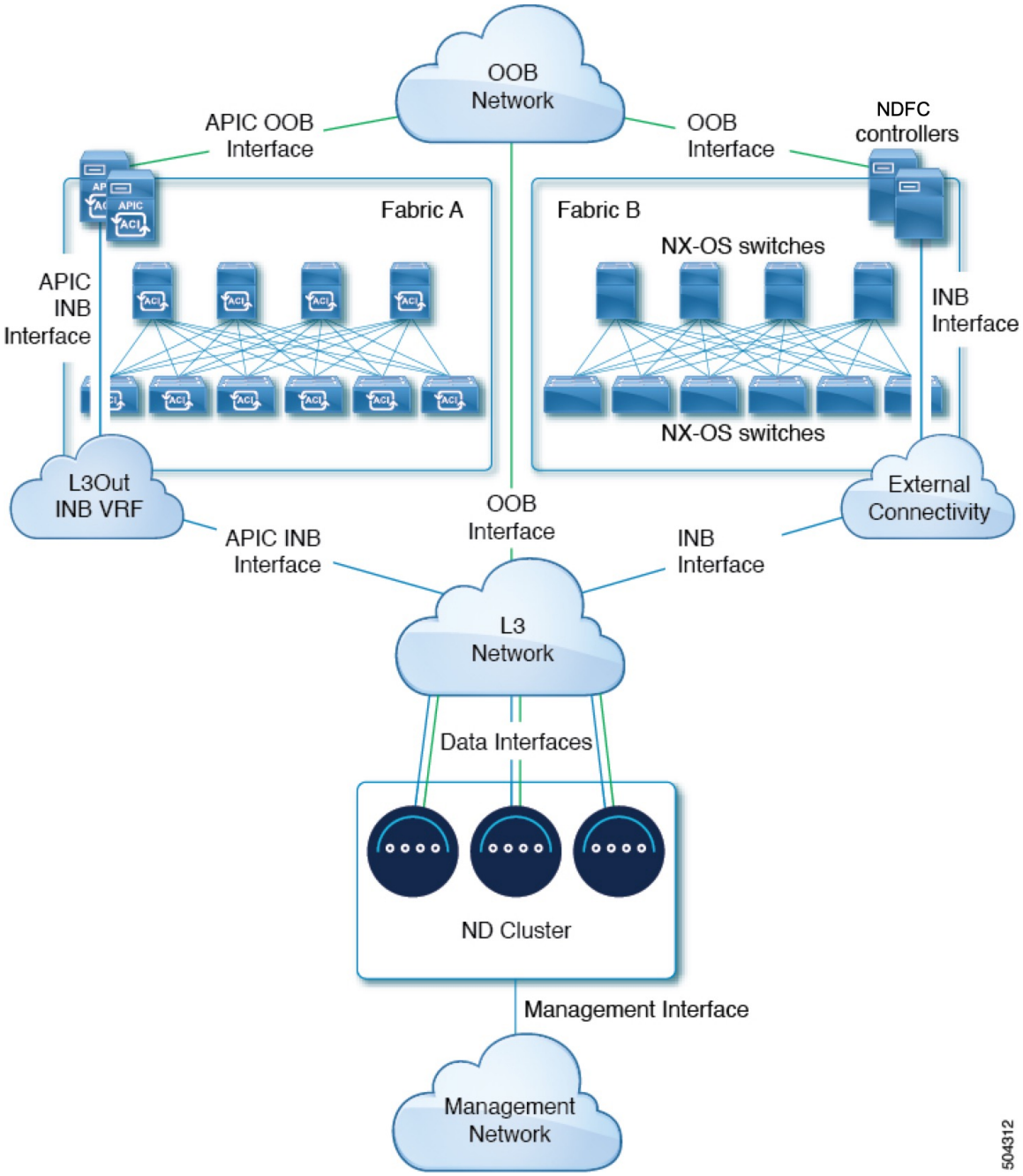


図 *2*：レイヤ*3*ネットワーク、*Nexus Dashboard Orchestrator*を介した接続



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 オーケストレータを展開する場合は、データ インターフェイスまたは管理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）インターフェイスあるいは両方への接続を確立できます。

  ファブリック接続がNexusダッシュボードの管理インターフェイスからのものである場合は、特定のスタティック ルートを設定するか、管理インターフェイスが APIC インターフェイスの同じ IP サブネットの一部であることを確認する必要があります。

- 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 *3*: 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

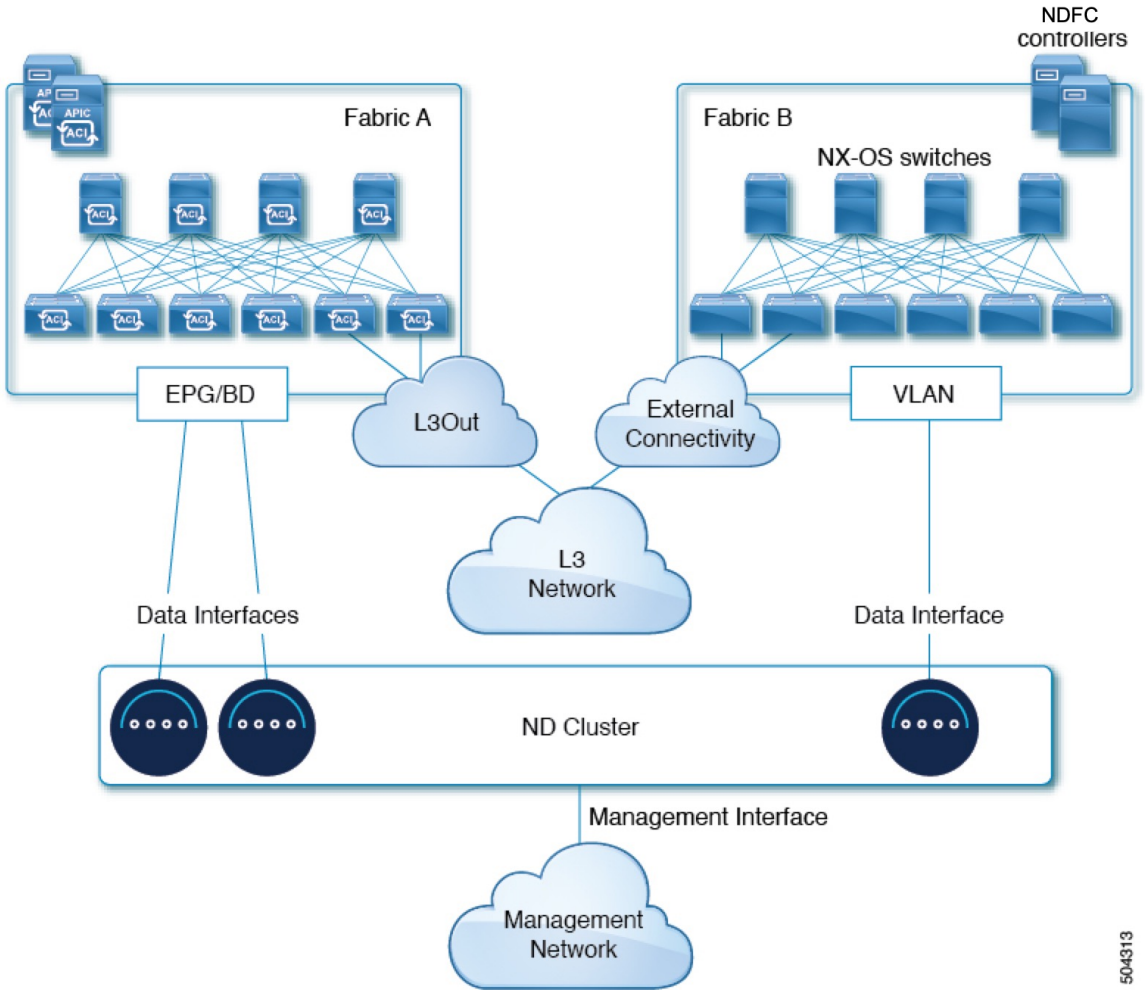
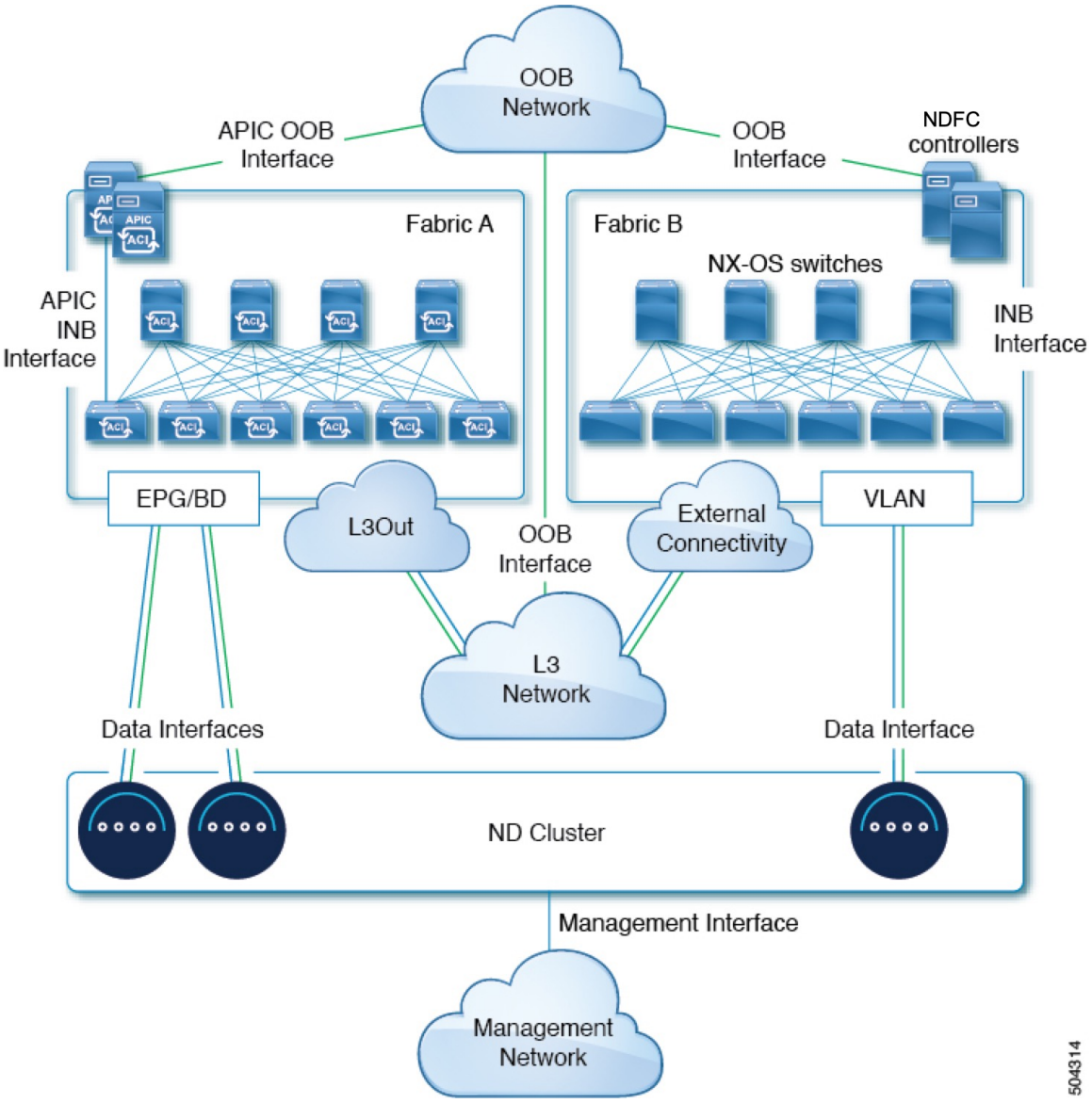


図 *4 :* リーフ スイッチ、*Nexus* ダッシュボード オーケストレータへの直接接続



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。

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には回復をサポートしていないため、

分散クラスタからの冗長性の利点は得られません。むしろ、ノードが異なるサイトにある場合、クラスタで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

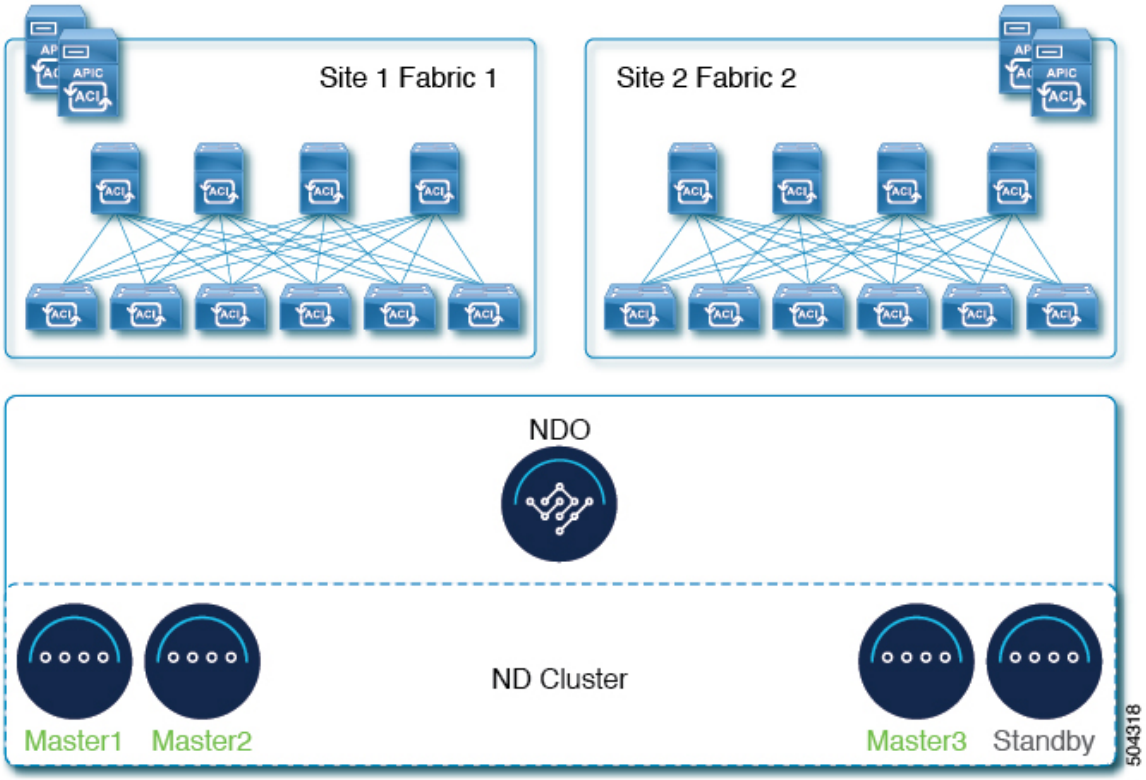
Nexus Dashboard Fabric Controller には、一元化された単一サイトの展開をお勧めします。このサービスは、2つのプライマリ ノードが使用できない場合には回復をサポートしていないため、分散クラスタからの冗長性の利点は得られません。むしろ、ノードが異なるサイトにある場合、クラスタで相互接続障害が発生する可能性があります。

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。

（注） スタンバイ ノードは、物理クラスタでのみサポートされます。仮想クラスタの場合は、障害が発生したノードと同じ設定で新しい VM を起動できます。

図 *5 : 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

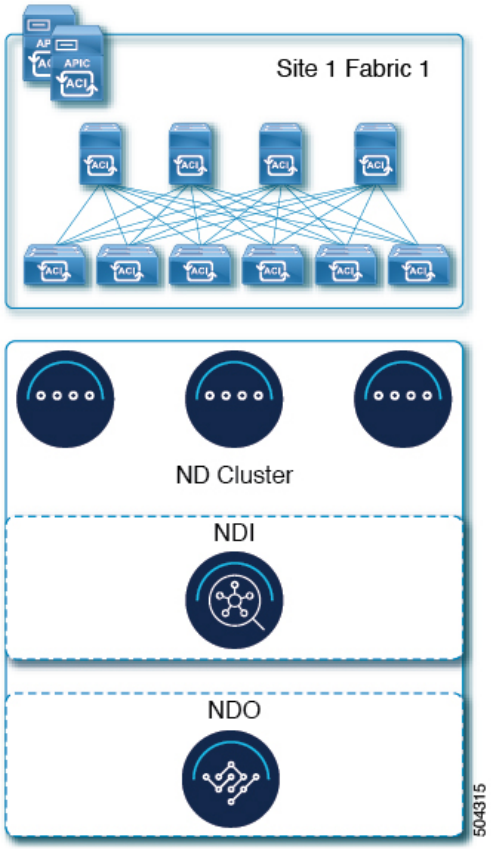
このセクションでは、特定の単一サービスまたは複数サービスの共同ホストの使用例について、いくつかの推奨される展開シナリオについて説明します。

（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 Dashboard Cluster Sizing tool 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。

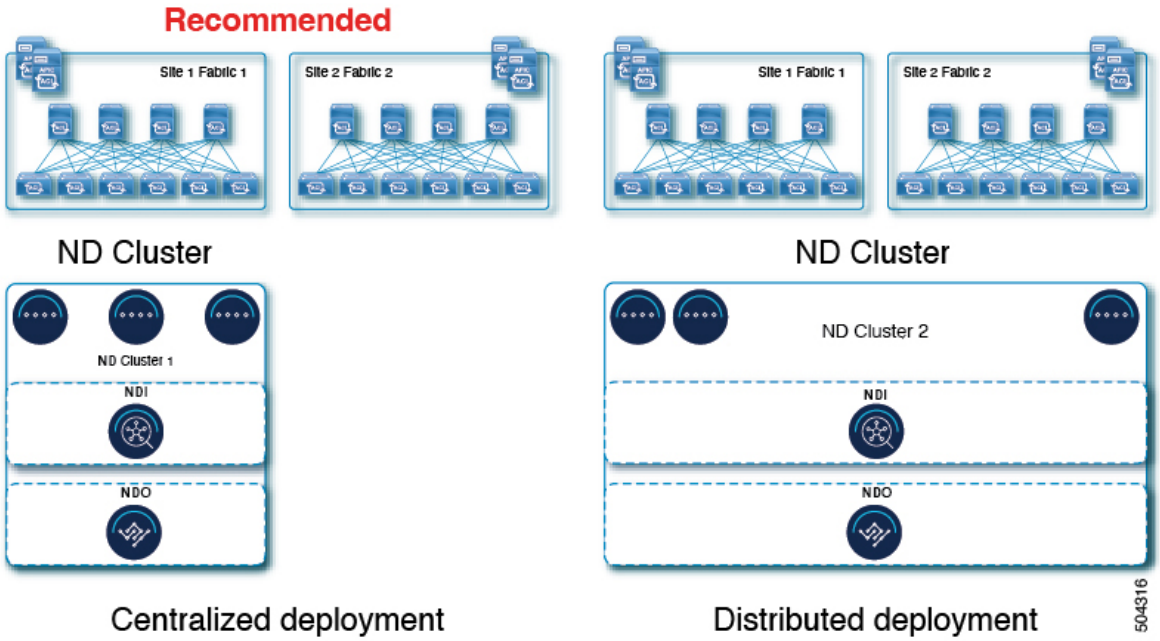
図 *6 :* 単一サイト、*Nexus* ダッシュボード *Insights* およびオーケストレータ



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。

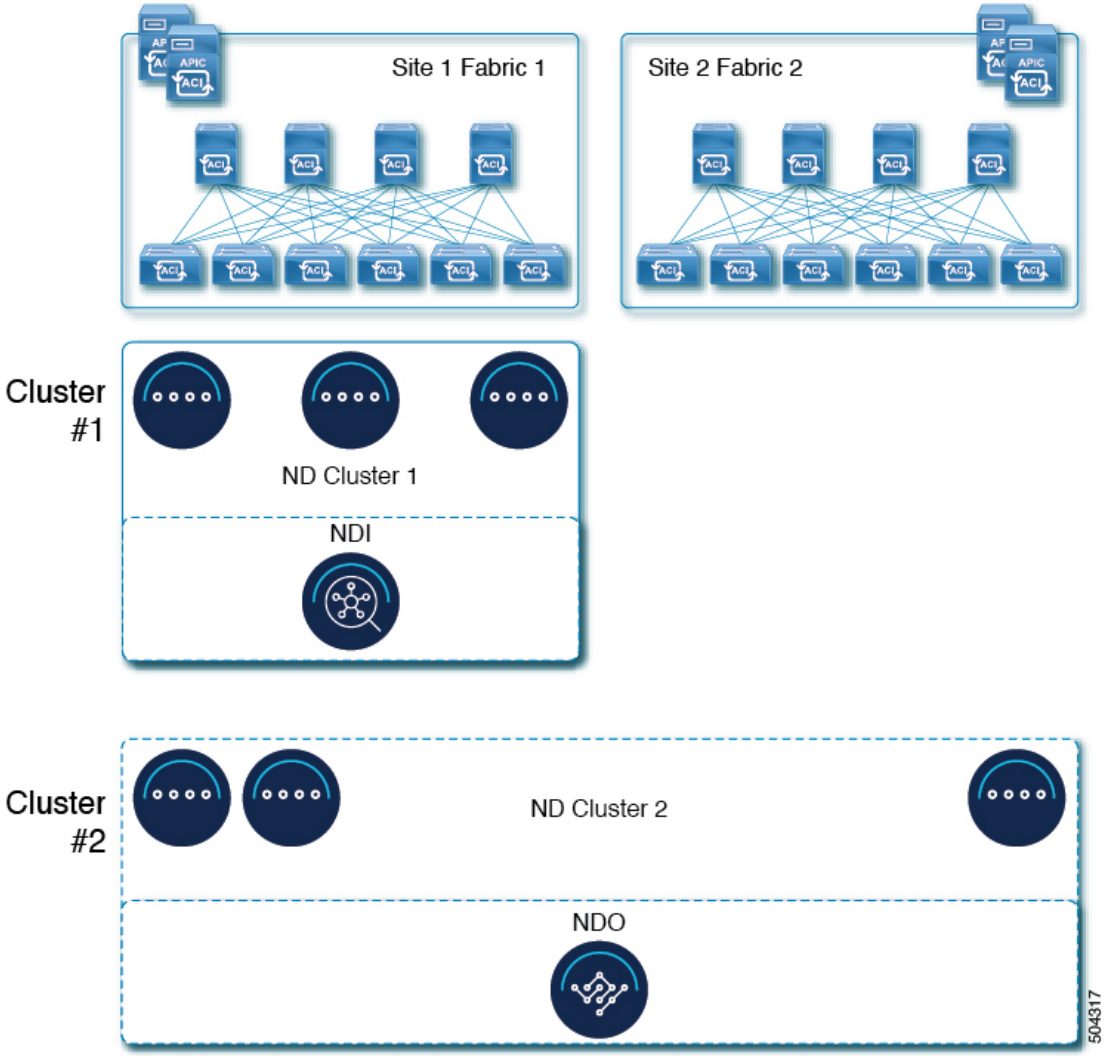
図 *7: Nexus* ダッシュボード *Insights* およびオーケストレータの複数サイト、単一クラスタ



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 *8 : 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 *5 :* 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	170.78.48.55	

パラメータ（Parameters）	例	入力する値
DNS プロバイダー	170.71.68.83	
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	

（注） リリース 3.1(1) 以降では、クラスタの初期展開時に、セカンダリ ノードとスタンバイ ノードを含むすべてのノードを定義できます。わかりやすくするために、次の表では3 ノードの基本クラスタを想定していますが、より大きなクラスタを展開する場合は、すべての追加ノードのノードの詳細も必要です。

表 *6:* 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	10.196.220.84/24 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	10.196.220.85/24 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	10.196.220.86/24 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**	192.168.11.172/24	
最初のノードの**管理ゲートウェイ**	192.168.11.1	

パラメータ（Parameters）	例	入力する値
最初のノードの**データ ネットワーク IP**	192.168.8.172/24	
最初のノードの**データ ネットワーク ゲートウェイ**	192.168.8.1	
（オプション）最初のノードの**データ ネットワーク VLAN**	101	
BGP を有効にする場合、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	

パラメータ（Parameters）	例	入力する値
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	
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。