

前提条件とガイドライン

- 全般的な前提条件とガイドライン （1 ページ）
- Nexus Dashboard データ ネットワークと管理ネットワークの前提条件 （6 ページ）
- Nexus Dashboard 内部アプリおよびサービス ネットワークの前提条件 （8 ページ）
- LAN 展開の前提条件 （9 ページ）
- SAN 展開の前提条件 （27 ページ）
- Nexus Dashboardの 永続 IP アドレス （40 ページ）
- ラウンド トリップ時間の要件 （48 ページ）
- Nexus Dashboard ストレージの前提条件（仮想フォーム ファクタ） （49 ページ）
- ファブリック接続 （51 ページ）

全般的な前提条件とガイドライン

ここでは、デプロイメントタイプに関係ない Nexus Dashboard クラスターの要件とガイドラインについて説明します。

全般的な展開のガイドラインと制限

- リモートストレージでの仮想 Nexus Dashboard VM の展開はサポートされていないため、予期しない動作が発生する可能性があります。

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

Nexus Dashboard 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。

DNS については次のガイドラインが適用されます。

- Nexus Dashboard リリース 4.3.1 より前のリリースでは、DNS ドメイン名はクラスタ名を使用して作成されていました。Nexus Dashboard リリース 4.3.1 以降、DNS 名は `cluster.case.local` に固定されています。
- 外部 DNS サーバーの場合、 TCPと UDP トラフィックの両方を許可する必要があります。詳細については、LAN 展開用の通信ポート （13 ページ）と SAN 展開用の通信ポート （28 ページ）を参照してください。
- 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。

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（NTP Key）]**：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（Key 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（Auth Type）]**：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。

- Windows サーバを NTP サーバとして使用しないことをお勧めします。
- 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。

- Nexus Dashboard ノードは、NTP サーバーと同期している必要があります。ただし、Nexus Dashboard ノード間で最大 1 秒の遅延が発生する可能性があります。Nexus Dashboard ノード間の遅延が 1 秒以上の場合、Nexus Dashboard クラスタでの動作が不安定になる可能性があります。

- NTP 遅延、オフセット、およびジッターの要件は次のとおりです。
  - 遅延：100 ミリ秒未満
  - オフセット：±25 ms
  - ジッター：10 ミリ秒以下

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。

IPv4 および IPv6 のサポート

Nexus Dashboard は、クラスタ ノードおよびサービスの IPv4 専用、IPv6 専用、またはデュアル スタック構成をサポートします。

IP アドレス構成を定義するとき、以下の注意事項が適用されます。

- クラスタ内のすべてのノードとネットワークは、IPv4 専用、IPv6 専用、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 IPv4 専用モードで展開し、デュアル スタック IPv4/IPv6 または IPv6 専用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：
  - データ、管理、アプリ、およびサービス ネットワークはデュアル 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。
  - IPv6 ベースの Nexus Dashboard の展開では、すべての物理サーバーの 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 アドレスを指定する必要があります。

    管理 IP アドレスは、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。
  - GUI は、構成されている限り、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。
- IPv6 専用構成の場合：
  - IPv6 専用モードは、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 パブリック クラウドでの vND 展開プロセスを介して展開されたクラスタは、IPv6 専用またはデュアル スタック モードをサポートしません。
  - 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 アドレスを使用して GUI 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。
- 物理サーバーの CIMC にも IPv6 アドレスが必要です。

特定の接続に必要な URL

これらの接続に必要な、Nexus Dashboard が到達する必要がある特定の URL があります。

- Cisco Intersight： Nexus DashboardクラスターをCisco Intersightに接続すると、次の利点があります。
  - メタデータの自動更新（特定の機能で、更新されたデータを提供するために使用できる）
  - TAC ログの収集とアップロード
- スマート ライセンスへの接続
- 電力マップからのエネルギー管理統計の取得

次に、 Nexus Dashboard がこれらの接続で到達する必要がある URL と、その理由を示します。

[URL（URL）]	プロトコル/ポート/サービス	説明
amazontrust.com	TCP/80（HTTP） TCP/443（HTTPS）	Cisco Intersight にセキュアに接続するために使用
connectdna.cisco.com	TCP/443（HTTPS）	Cisco Intersight およびスマートライセンスにセキュアに接続するために使用
swapi.cisco.com	TCP/443（HTTPS）	Cisco Smart Licensing にセキュアに接続するために使用
svc.ucs-connect.com	TCP/443（HTTPS）	Cisco Intersight にセキュアに接続するために使用
svc-static1.ucs-connect.com	TCP/443（HTTPS）	Cisco Intersight にセキュアに接続するために使用

[URL（URL）]	プロトコル/ポート/サービス	説明
svc.eu-central-1.intersight.com	TCP/443（HTTPS）	Cisco Intersight にセキュアに接続するために使用（EMEA リージョン）
svc-static1.eu-central-1.intersight.com	TCP/443（HTTPS）	Cisco Intersight にセキュアに接続するために使用（EMEA リージョン）

Nexus Dashboard データ ネットワークと管理ネットワークの前提条件

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。Nexus Dashboard を最初に設定するときは、クラスター ノードごとに、2 つの Nexus Dashboard 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され、最適なパフォーマンスのためのバックエンド、クラスター、およびインフラ接続に使用されます
- もう 1 つは、管理ネットワークに接続されます。これは、シームレスな GUI とフロントエンド オペレーションのために使用されます。

表 *1:* 外部ネットワークの目的

データ ネットワーク	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 • Nexus Dashboard ノードから Cisco APIC ノードへの通信 • 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 Dashboard 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 • AAA トラフィック • マルチクラスタ接続

2つのネットワークには次の要件があります。

- 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 管理インターフェイス（bond1）には、 ICMP パケットを毎秒平均 6 パケットとバースト制限 5 にレート制限する内部 iptables ルールがあります。このICMPレートおよびバースト制限は、データ ネットワーク ポート(bond0)にも適用されます。ICMP ベースのモニタリング ツールを使用して管理ネットワークの状態を追跡している場合、ポーリング周波数がこれらの制限を超えると、断続的なパケット ドロップが発生することがあります。これは、管理プレーンを保護するために設計された予期される動作です。

- 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。
- リモート認証を設定する場合、AAA サーバをデータ インターフェイスと同じサブネットに配置することはできません。
- 物理クラスタの場合、管理ネットワークは各ノードの CIMC に TCP ポート 22 および 443 を使用して IP 到達可能性を提供する必要があります。これは、Nexus Dashboard クラスター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するためです。
- 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、ノードが接続されているスイッチでより高い MTU を構成できます。

（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 タグが構されている場合は、ジャンボ フレームを有効にするか、ノードが接続されているスイッチ ポートで 1504 バイト以上のカスタム MTU を構成する必要があります。

- テレメトリを使用している場合、デフォルトでは、データ ネットワークは、各ファブリックのインバンド ネットワークに、および ACI ファブリック用の Cisco APIC（オーケストレーション機能を使用している場合）のインバンド ネットワークに IP 到達可能性可能性を提供する必要があります（オーケストレーション機能を使用している場合）。 。

（注） Nexus Dashboard のルートテーブルでルートを定義し、代わりに管理ネットワークを使用して、次のいずれかのサービスに到達することもできます。

  - DNS 統合の場合、DNS サーバーへ。

- Panduit PDU 統合の場合は、Panduit PDU サーバーへの接続。
- 外部 Kafka 統合の場合は、外部 Kafka サーバー（コンシューマ）への接続。
- SysLog 統合の場合は、SysLog サーバーへの接続。
- ネットワーク接続ストレージ統合の場合は、ネットワーク接続ストレージサーバーへの接続。
- VMware vCenter 統合の場合は、 VMware vCenter に移動します。
- AppDynamics 統合の場合は、AppDynamics コントローラへの接続。

詳細については、*Nexus Dashboard* の統合の操作を参照してください。

（注） すべての統合が管理ネットワークと同じサブネット内にある場合は、管理ネットワークを使用します。

Nexus Dashboard 内部アプリおよびサービス ネットワークの前提条件

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 ネットワーク：Nexus Dashboard 内のアプリケーションで内部的に使用されますアプリ ネットワークは、IPv4 の場合は `/16` ネットワーク、IPv6 の場合は `/108` ネットワークである必要があり、展開時にデフォルト値が事前に入力されます。
- サービス ネットワーク：Nexus Dashboardによって内部的に使用されます。サービス ネットワークは、IPv4 の場合は `/16` ネットワーク、IPv6 の場合は `/108` ネットワークである必要があり、展開中にデフォルト値が事前に入力されます。

複数の Nexus Dashboard 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 ネットワークとサービス ネットワーク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 ノードを離れないことを意味します。

たとえば、アプリまたはサービス ネットワークのいずれか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 Dashboard 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。

LAN 展開の前提条件

LAN 展開のためのネットワークの前提条件

次のネットワークの前提条件が LAN の導入に適用されます：

- 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。
- データ ネットワークと管理ネットワークの両方のインターフェイスは、レイヤ 2 またはレイヤ 3 隣接のいずれかにすることができます。データ ネットワークのレイヤ 3 隣接関係については、ブートストラップ プロセス中に BGP を構成する必要があります。管理ネットワーク インターフェイスは、BGPプロトコルをサポートしていません。異なるサブネット内の管理アドレスを使用して異なるNexus Dashboard ノードを展開する場合、それらは単に相互にルーティングされます。
- 永続的なデータIPアドレスを使用してクラスターを起動する必要があるため、設定に応じて特定の数の永続 IP アドレスを割り当てる必要があります。
  - クラスターに 1 つのノードがある場合は、3 つの永続 IP アドレスを割り当てます。
  - クラスターに 3 つ以上のノードがある場合は、永続 IP アドレスを 5 つ割り当てます。
  - デュアルスタック IPv4 および IPv6 を設定する場合は、IPv6 に同じ数の永続 IP アドレスを追加します（つまり、デュアル スタックを設定する場合は、5 つの IPv4 と 5 つの IPv6 の永続的IPアドレス）。

永続 IP アドレスの詳細については、Nexus Dashboardの 永続 IP アドレス （40 ページ）を参照してください。ブートストラップ プロセス中に、必要最小限の永続 IP アドレスを割り当てる必要があります。追加の永続IPアドレスの割り当ては、クラスタの展開後にGUIの外部サービス プール設定を使用して行うことができます。

LAN 展開で ACI ファブリックをオンボーディングするための前提条件

これらのネットワークの前提条件は、LAN 展開での ACI ファブリックのオンボーディングに適用されます。

- Cisco ACI ファブリックを管理するためにオーケストレーションを使用する場合は、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ファブリックの APIC クラスター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。

  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。

ACI ファブリックの追加の前提条件

ACIファブリックでオーケストレーションを使用する場合は、次の前提条件も適用されます。

- ACIファブリックとリモートリーフスイッチでオーケストレーションを使用する場合は、次の制限が適用されます。
  - 1 つのファブリックのリモート リーフ スイッチで別のファブリックの L3Out を使用することはできません。
  - あるファブリック（ローカル リーフまたはリモート リーフ）と別のファブリックのリモート 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。

- オーケストレーションは、非実稼働（ラボ）展開の単一ノード Nexus Dashboard クラスタ（仮想データプロファイルまたは物理アプライアンス）でのみサポートされています。これらのフォームファクタのいずれかでオーケストレーションを有効にする場合は、組み込みの Swagger API を使用して有効にする必要があります。

  1. Nexus Dashboard UIから、[?]アイコンをクリックし、**[ヘルプ センター（Help Center）]** を選択します。
  2. **[ヘルプ センター（Help Center）]** で、 **[API reference: Swagger (In-product)]** をクリックします。
  3. API リスト内で、左側のナビゲーションから **[インフラ（Infra）]** グループをクリックします。
  4. **[システム設定** （System Settings）] サブメニューを見つけて矢印をクリックして展開し、必要に応じて `/settings/general/actions/enableOrchestration`を検索します。

5. [API] を展開し、次をクリックします。

これで、クラスター上でオーケストレーション サービスが有効になります。

ACI ファブリックでテレメトリを使用する場合の追加の前提条件

ACIファブリックでテレメトリを使用する場合は、次の前提条件も適用されます。

- テレメトリ収集は、 ACI バージョン 6.1(2f) 以降を実行している限り、 APIC およびスイッチの OOB ネットワークでサポートされます。
- Cisco APICでNTP設定を構成しておきます。

  詳細については、ACI ファブリック ソリューションでのNTPの設定を参照してください。
- フローテレメトリを使用する場合は、 ACI の **ノード制御** ポリシーを **テレメトリの優先順位** に設定する必要があります。トラフィック分析を使用している場合は、Netflow またはテレメトリの優先順位を使用できます。
  - NetFlow 優先順位モードを使用すると、 ACI は、 ACI から Stealthwatch などの外部送信元にも標準規格の NetFlow レコードをエクスポートできます。
  - テレメトリの優先順位は、トラフィック分析の NetFlow レコードの Nexus Dashboard へのエクスポートのみをサポートします。
- フロー テレメトリまたはトラフィック分析機能を使用するには、Cisco APIC で高精度時間プロトコル（PTP）を有効にして、テレメトリが複数のスイッチからのフローを適宜関連付けできるようにする必要があります。

  Cisco APIC で、**[システム（System）] > [システム設定（System Settings）] > [PTP および遅延測定（PTP and Latency Measurement）] > [管理状態（Admin State）]**の順に選択し、PTP を有効にします。

  PTP による時刻同期の品質は、クロックのソースである PTP グランドマスター（GM）クロックの精度、およびその間の ACI スイッチや IPN デバイスなどの PTP デバイスの精度と数に依存します。

  PTP GM デバイスには通常、PTP の標準要件であるナノ秒単位の精度を実現する GNSS/GPS ソースが装備されていますが、フローテレメトリではマイクロ秒単位の精度で十分であるため、通常は GNSS/GPS ソースは必要ありません。

  シングルポッド ACI ファブリックの場合、リーフスイッチを介して PTP GM を接続できます。それ以外の場合、スパインスイッチの1つがGMとして選出されます。マルチポッド ACI ファブリックの場合、リーフ スイッチまたは IPN デバイスを介して PTP GM を接続できます。ACI スイッチノードがポッド間でクロックを同期できるように、IPN デバイスは PTP 境界クロックまたは PTP Transparent Clock にする必要があります。ポッド全体で同じ精度を維持するため、IPN デバイスを介して PTP GM を接続することをお勧めします。

  PTP 接続オプションの詳細については、『*Cisco APIC System Management Configuration Guide*』の「Precision Time Protocol」の項を参照してください。

- インバンド テレメトリでは、Cisco APIC および静的管理アクセスの説明に従って、インバンド管理を構成しておきます。ACI リリース 6.1（2）以降では、アウトオブバンドテレメトリも使用できます。フローテレメトリはインバンド管理でのみサポートされますが、トラフィック分析はどちらでもサポートされます。
- DNSプロファイルの下に1つ以上のDNSドメインが設定されている場合、1つのDNSドメインをデフォルトとして設定することが必須です。

  Cisco APIC で、**[ファブリック（Fabric）] > [ファブリックポリシー（Fabric Policies）] > [ポリシー（Policies）] > [グローバル（Global）] > [DNSプロファイル（DNS Profile）] > [デフォルト（Default）] > [DNS ドメイン（DNS Domains）]**の順に選択し、デフォルトとして 1 つを設定します。

  これを行わないと、テレメトリ フローマップに同じスイッチが複数回表示されます。
- 次を使用して EPG を設定することにより、ACI インバンド ネットワークを展開します。
  - テナント = `mgmt`
  - VRF = `inb`
  - BD = `inb`
  - ノード管理 EPG = `デフォルト/<any_epg_name>`
- Nexus Dashboard のデータ ネットワーク 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、異なるサブネットにある必要があります。

LAN 展開での NX-OS、 IOS XR、およびIOS XE デバイスのオンボーディングに関する前提条件

詳細については、*Cisco Nexus Dashboard* でのテレメトリによる *Nexus* ファブリックの展開 を参照します。

これらのネットワークの前提条件は、LAN 展開での NX OS、 IOS XR、およびIOS XE デバイスのオンボーディングに適用されます。

- オーケストレーションを使用して NX- OSファブリックを管理する場合、データ ネットワークには NX- OS ファブリックのインバンド到達可能性が必要です。

NX-OS ファブリックまたはスタンドアロン NX-OS スイッチの追加の前提条件

NX-OS ファブリックまたはスタンドアロンNX-OS スイッチでテレメトリを使用する場合は、次の前提条件も適用されます。

- データ ネットワークが、ファブリックのインバンドまたはアウトオブバンド IP アドレスへの IP 到達可能性を備えている必要があります。

（注） フロー テレメトリ機能を使用している場合、データ ネットワークがファブリックの帯域内 IP アドレスへの IP 到達可能性を備えている必要があります。

- フローテレメトリまたはトラフィック分析を有効にするには、テレメトリでサポート対象にするすべてのノードで Precision Time Protocol（PTP）を構成する必要があります。

  管理ファブリック モードとモニタ ファブリック モードの両方で、ファブリック内のすべてのノードでPTPが正しく構成されていることを確認する必要があります。ファブリック セットアップの **[詳細設定]** タブで **[精密時間プロトコル（PTP）を有効にする（Enable Precision Time Protocol）]** オプションをオンにすると、PTP を有効にできます。

  PTP グランドマスター クロックは、ネットワーク ファブリックの外部にあるデバイスによって提供される必要があります。

  PTP による時刻同期の品質は、クロックのソースである PTP グランドマスター（GM）クロックの精度、およびネットワークパスに沿ったPTPデバイスの精度と数によって異なります。PTP GM デバイスには通常、PTP の標準要件であるナノ秒単位の精度を実現する GNSS/GPS ソースが装備されていますが、フローテレメトリではマイクロ秒単位の精度で十分であるため、通常は GNSS/GPS ソースは必要ありません。

  Nexus スイッチでの Precision Time Protocol の手動構成の詳細については、*Cisco Nexus 9000 シリーズ NX-OS システム管理設定ガイド*を参照してください。

LAN 展開用の通信ポート

Nexus Dashboard 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。

このセクションで説明されている全てのポートを開きます。

この表に、LAN 展開用の管理ネットワーク通信ポートを示します。**[方向（Direction）]** 列は次のようになっています。

- **In**は、クラスタに向うことを意味します
- **Out**は、クラスタからファブリックまたは外に向かうことを意味します

表 *2: LAN* 展開用の管理ネットワーク通信ポート

サービス	ポート	プロトコル	方向 （In /Out）	接続
Nexus Dashboard エージェント ポート	30022	TCP	入力 / 出力	Nexus Dashboard でサポートされている SONiC デバイスを管理する場合、このポートを Nexus Dashboard の管理ネットワークとデータ ネットワークの両方に対して開いている必要があります。Nexus Dashboard は、30022 ポートへの Web ソケットを開く SONiC デバイスにエージェントをインストールします。
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、スイッチ検出。 クラスターが動作するには ICMP が必要であるため、 ICMP サービスを許可する必要があります。 （注） DCNM で LAN デバイスを追加または検出すると、検出プロセスの一部として ICMP エコー パケットが使用されます。したがって、 Nexus Dashboard クラスタとスイッチの間にファイア ウォールがある場合、 ICMPメッセージの通過を許可する必要があります。そうしないと、検出プロセスが失敗します。管理インターフェイスの ICMP トラフィックは、平均6パケット/秒、バースト 5 にレート制限されています。モニタリング システムは、パケット損失に関する誤検出アラートを回避するために、この制限を念頭に置いて設定する必要があります。

サービス	ポート	プロトコル	方向（In/Out）	接続
DHCP	67	UDP	入力	ローカル DHCP サーバーがブートストラップまたは POAP 用に構成されている場合。 （注） POAP の目的でローカル DHCP サーバーとして Nexus Dashboard を使用する場合、すべての Nexus Dashboard マスター ノードの IP アドレスを DHCP リレーとして構成する必要があります。Nexus Dashboard ノードの管理 IP アドレスが DHCP サーバーにバインドされるかどうかは、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	
DNS	53	TCP および UDP	アウト	DNS サーバ
HTTP	80	TCP	発信	インターネット/プロキシ
HTTP（PnP）	9666	TCP	入力	Catalyst デバイス用の Cisco プラグ アンド プレイ（PnP）は、Nexus Dashboard HTTP ポート 9666 および HTTPS ポート 9667 を介して実現されます。ポート 9666 の HTTP は、CA 証明書バンドルをデバイスに送信して HTTPS モード用にデバイスを準備するために使用され、実際の PnP はその後ポート 9667 で HTTPS を介して行われます。 POAP のような PnP サービスは、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 IP アドレスで実行されます。これは、Nexus Dashboard 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（In/Out）	接続
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 Nexus Dashboard に送信して (Nexus Dashboard 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。Nexus Dashboard 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。 Nexus Dashboard 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 IP アドレスがあります。これは、Nexus Dashboard 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。
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
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、Nexus Dashboard 機能の限られたセットで使用されます。

サービス	ポート	プロトコル	方向（In/Out）	接続
HTTPS（PnP）	9667	TCP	入力	Catalyst デバイス用の Cisco プラグ アンド プレイ（PnP）は、Nexus Dashboard HTTP ポート 9666 および HTTPS ポート 9667 を介して実現されます。ポート 9666 の HTTP は、CA 証明書バンドルをデバイスに送信して HTTPS モード用にデバイスを準備するために使用され、実際の PnP はその後ポート 9667 で HTTPS を介して行われます。 POAP のような PnP サービスは、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 IP アドレスで実行されます。これは、Nexus Dashboard 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。
HTTPS（POAP）	443	TCP	入力	セキュア POAP は、ポート 443 の Nexus Dashboard HTTPS サーバーを使用して実現されます。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 IP アドレスを使用します。 Nexus Dashboard 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 IP アドレスがあります。これは、Nexus Dashboard 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。
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
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 （In/Out）	接続
LDAP	389 636	TCP	発信	LDAP サーバ
NTP	123	UDP	発信	NTP サーバー
NX-API	8443	TCP	入力 / 出力	NX-OS リリース 9.x 以降を搭載した Cisco MDS 9000 シリーズ スイッチでパフォーマンス モニタリングに使用されます。
RADIUS	1812	TCP	発信	Radius サーバー
SCP	22	TCP	入力 / 出力	SCPは、リモートサーバーへのバックアップファイルのアーカイブなど、デバイスと Nexus Dashboard の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。Nexus Dashboard 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。 Nexus Dashboard 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 IP アドレスがあります。これは、Nexus Dashboard 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（In/Out）	接続
SCP/テックコレクションを表示	22	TCP	発信	Nexus Dashboard POAP-SCP ポッドの永続 IP アドレスから、テレメトリ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。 Nexus Dashboard 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 IP アドレスがあります。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。
SMTP	25	TCP	発信	SMTPポートは、**[管理（Admin）>] [サーバー設定（Server Settings）]>[全般（General）]**ページで設定できます。 これはオプションの機能です。
SNMP	161	TCP および UDP	アウト	Nexus Dashboard からデバイスへの SNMP トラフィック。
SNMP トラップ	2162	UDP	入力	デバイスから Nexus Dashboard 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 IP アドレスに向けて送信されます。 Nexus Dashboard 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 IP アドレスがあります。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。
SSH	22	TCP	入力 / 出力	クラスタ ノードの CLI および CIMC

サービス	ポート	プロトコル	方向（In/Out）	接続
TAC アシスト	8884	TCP	入力 / 出力	その他のクラスタ ノード スイッチから **show tech** を収集し、Intersight に情報をアップロードするサービスである TAC Assist に使用されます。このポートは、クラスタ ノード間で **show tech** data を交換するために使用されます。
TACACS	49	TCP	発信	TACACS サーバー
TFTP（POAP）	69	UDP	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 Nexus Dashboard に送信して (Nexus Dashboard 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。Nexus Dashboard 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。 Nexus Dashboard 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 IP アドレスがあります。これは、Nexus Dashboard 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。

この表に、LAN 展開用の管理ネットワーク通信ポートを示します。**[方向（Direction）]** 列は次のようになっています。

- **In**は、クラスタに向うことを意味します
- **Out**は、クラスタからファブリックまたは外に向かうことを意味します

表 *3 : LAN* 展開用のデータ ネットワーク通信ポート

サービス	ポート	プロトコル	方向（In /Out）	接続
Nexus Dashboard エージェント ポート	30022	TCP	入力 / 出力	Nexus Dashboard でサポートされている SONiC デバイスを管理する場合、このポートを Nexus Dashboard の管理ネットワークとデータ ネットワークの両方に対して開いている必要があります。Nexus Dashboard は、30022 ポートへの Web ソケットを開く SONiC デバイスにエージェントをインストールします。
DHCP	67	UDP	入力	Nexus Dashboard 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。 （注） POAP の目的でローカル DHCP サーバーとして Nexus Dashboard を使用する場合、すべての Nexus Dashboard マスター ノードの IP アドレスを DHCP リレーとして構成する必要があります。Nexus Dashboard ノードのデータ IP アドレスが DHCP サーバーにバインドされるかどうかは、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	
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
フローテレメトリ	5640 ～ 5671	UDP	入力	スイッチの帯域内 ファブリックからフロー テレメトリを受信するために使用されます
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、Nexus Dashboard GRPC レシーバー サービス ポッドに関連付けられた永続 IP アドレスにストリーミングされます。

サービス	ポート	プロトコル	方向（In/Out）	接続
HTTP（PnP）	9666	TCP	入力	Catalyst デバイス用の Cisco プラグ アンド プレイ（PnP）は、Nexus Dashboard HTTP ポート 9666 および HTTPS ポート 9667 を介して実現されます。ポート 9666 の HTTP は、CA 証明書バンドルをデバイスに送信して HTTPS モード用にデバイスを準備するために使用され、実際の PnP はその後ポート 9667 で HTTPS を介して行われます。 POAP のような PnP サービスは、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 IP アドレスで実行されます。これは、Nexus Dashboard 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。
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 Nexus Dashboard に送信して (Nexus Dashboard 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。Nexus Dashboard 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。 Nexus Dashboard 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 IP アドレスがあります。これは、Nexus Dashboard 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。
HTTPS	443	TCP	発信	スイッチと APIC および NX-OS の帯域内

サービス	ポート	プロトコル	方向（In/Out）	接続
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、Nexus Dashboard 機能の限られたセットで使用されます。
HTTPS（PnP）	9667	TCP	入力	Catalyst デバイス用の Cisco プラグ アンド プレイ（PnP）は、Nexus Dashboard HTTP ポート 9666 および HTTPS ポート 9667 を介して実現されます。ポート 9666 の HTTP は、CA 証明書バンドルをデバイスに送信して HTTPS モード用にデバイスを準備するために使用され、実際の PnP はその後ポート 9667 で HTTPS を介して行われます。 POAP のような PnP サービスは、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 IP アドレスで実行されます。これは、Nexus Dashboard 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。
HTTPS（POAP）	443	TCP	入力	セキュア POAP は、ポート 443 の Nexus Dashboard HTTPS サーバーを使用して実現されます。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 IP アドレスを使用します。 Nexus Dashboard 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 IP アドレスがあります。これは、Nexus Dashboard 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 （In/Out）	接続
HTTPS（vCenter、Kubernetes、OpenStack、Discovery）	443	TCP	発信	Nexus Dashboard 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。
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
インフラ サービス	3379 3380 4430 8989 9090 9969 9979 9989 15223 30002 ～ 30006 30009 ～ 30010 30012 30014-30021 30025 30027 30028	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	30019	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（In/Out）	接続
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
Kafka	30001	TCP	入力 / 出力	スイッチと APIC/コントローラの帯域内 IP
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
NFSv3	111	TCP および UDP	入力 / 出力	リモート NFS サーバー
NFSv3	608	UDP	入力 / 出力	リモート NFS サーバー
NFSv3	2049	TCP	入力 / 出力	リモート NFS サーバー
NX-API	8443	TCP	入力 / 出力	NX-OS リリース 9.x 以降を搭載した Cisco MDS 9000 シリーズ スイッチでパフォーマンス モニタリングに使用されます。
SCP	22	TCP	入力 / 出力	SCPは、リモートサーバーへのバックアップファイルのアーカイブなど、デバイスと Nexus Dashboard の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。Nexus Dashboard 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。 Nexus Dashboard 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 IP アドレスがあります。これは、Nexus Dashboard 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（In/Out）	接続
SCP	22	TCP	発信	Nexus Dashboard POAP-SCP ポッドの永続 IP アドレスから、テレメトリ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。 Nexus Dashboard 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 IP アドレスがあります。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。
SMTP	25	TCP	発信	SMTPポートは、**[管理（Admin）>] [サーバー設定（Server Settings）] > [全般（General）]**ページで設定できます。 これはオプションの機能です。
SNMP	161	TCP および UDP	アウト	Nexus Dashboard からデバイスへの SNMP トラフィック。
SNMP トラップ	2162	UDP	入力	デバイスから Nexus Dashboard 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 IP アドレスに向けて送信されます。 Nexus Dashboard 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 IP アドレスがあります。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。
SSH	22	TCP	発信	UI、スイッチと APIC のインバンド
SSH	1022	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（In/Out）	接続
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 ファブリックからさまざまなテレメトリ情報を収集するために使用されます テレメトリおよび NX- OS ベースのスイッチ用に、スイッチと Nexus Dashboard 間にポート 57500 が必要です
テクニカル サポート	2022	TCP	入力	テクニカル サポートをファブリックからクラスタまでにアップロードするためにこれが使われています。
TFTP（POAP）	69	UDP	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 Nexus Dashboard に送信して (Nexus Dashboard 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。Nexus Dashboard 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。 Nexus Dashboard 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 IP アドレスがあります。これは、Nexus Dashboard 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。
VXLAN	4789	UDP	入力 / 出力	その他のクラスタ ノード

SAN 展開の前提条件

SAN 展開のためのネットワークの前提条件

SAN 展開には、次のネットワークの前提条件が適用されます。

- SAN 展開では、管理ネットワークとデータ ネットワークは同じサブネットを使用できます。

- 永続的な IP アドレスは、BGP が構成されたレイヤ 2 隣接およびレイヤ 3 隣接のデータネットワークでのみサポートされます。ただし、同じサブネットを使用するように管理ネットワークとデータネットワークを構成すると、レイヤ 3 隣接関係は使用できません。これは、データネットワーク層 3 隣接関係のブートストラッププロセス中に BGP を構成する必要があるのに、管理ネットワークは BGP が構成されている状態でのレイヤ 3 隣接関係をサポートしていないためです。

  この状況では、次のことがわかります。

  - 同じサブネットを使用するように管理ネットワークとデータ ネットワークを構成する場合は、代わりにレイヤ 2 隣接を活用。または、
  - 管理ネットワークとデータネットワークに異なるサブネットを活用。管理ネットワークでレイヤ 2 隣接を構成し、データネットワークで構成された BGP とのレイヤ 3 隣接を構成できます。

- ユースケースに応じて、次の数の永続 IP アドレスを割り当てる必要があります。永続 IP アドレスの詳細については、Nexus Dashboardの 永続 IP アドレス （40 ページ）を参照してください。

SAN 展開用の通信ポート

Nexus Dashboard 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。

次の表に、 SAN 展開での管理ネットワーク通信ポートを示します。

表 *4: SAN* 展開の管理ネットワーク通信ポート

サービス	ポート	プロトコル	方向 イン：クラスタに向かう アウト：クラスタからファブリックまたは外に向かう	接続
DNS	53	TCP および UDP	アウト	DNS サーバ
GRPC（テレメトリ）	33000	TCP	入力	Nexus Dashboard 永続 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 Telemetry サーバー。

サービス	ポート	プロトコル	方向 イン：クラスタに向かう アウト：クラスタからファブリックまたは外に向かう	接続
HTTP	80	TCP	発信	インターネット/プロキシ
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
HTTPS（vCenter、Kubernetes、OpenStack、Discovery）	443	TCP	発信	Nexus Dashboard 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。
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
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
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
LDAP	389 636	TCP	発信	LDAP サーバ
NTP	123	UDP	発信	NTP サーバー
NX-API	8443	TCP	入力 / 出力	NX-OS リリース 9.x 以降を搭載した Cisco MDS 9000 シリーズ スイッチでパフォーマンス モニタリングに使用されます。
RADIUS	1812	TCP	発信	Radius サーバー

サービス	ポート	プロトコル	方向 イン：クラスタに向かう アウト：クラスタからファブリックまたは外に向かう	接続
SCP	22	TCP	入力 / 出力	SCPは、リモートサーバーへのバックアップファイルのアーカイブなど、デバイスと Nexus Dashboard の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。Nexus Dashboard 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。 Nexus Dashboard 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 IP アドレスがあります。これは、Nexus Dashboard 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	22	TCP	発信	Nexus Dashboard POAP-SCP ポッドの永続 IP アドレスから、テレメトリ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。 Nexus Dashboard 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 IP アドレスがあります。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：クラスタに向かう アウト：クラスタからファブリックまたは外に向かう	接続
SMTP	25	TCP	発信	SMTPポートは、**[管理（Admin）>][サーバー設定（Server Settings）]>[全般（General）]**ページで設定できます。 これはオプションの機能です。
SNMP	161	TCP および UDP	アウト	Nexus Dashboard からデバイスへの SNMP トラフィック。
SNMP トラップ	2162	UDP	入力	デバイスから Nexus Dashboard 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 IP アドレスに向けて送信されます。 Nexus Dashboard 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 IP アドレスがあります。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。
SSH	22	TCP	入力 / 出力	クラスタ ノードの CLI および CIMC

サービス	ポート	プロトコル	方向 イン：クラスタに向かう アウト：クラスタからファブリックまたは外に向かう	接続
Syslog	514	UDP	入力	Nexus Dashboard 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 IP アドレスに向けて送信されます。 Nexus Dashboard 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 IP アドレスがあります。これは、Nexus Dashboard 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。
TACACS	49	TCP	発信	TACACS サーバー

次の表に、 SAN 展開での管理ネットワーク通信ポートの一覧を示します。

表 *5: SAN* 展開用のデータ ネットワーク通信ポート

サービス	ポート	プロトコル	方向 イン：クラスタに向かう アウト：クラスタからファブリックまたは外に向かう	接続
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

サービス	ポート	プロトコル	方向 イン：クラスタに向かう アウト：クラスタからファブリックまたは外に向かう	接続
GRPC（テレメトリ）	33000	TCP	入力	Nexus Dashboard 永続 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 Telemetry サーバー。
HTTPS	443	TCP	発信	スイッチと APIC および NX-OS の帯域内
HTTPS（vCenter、Kubernetes、OpenStack、Discovery）	443	TCP	発信	Nexus Dashboard 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。
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

サービス	ポート	プロトコル	方向 イン：クラスタに向かう アウト：クラスタからファブリックまたは外に向かう	接続
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	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
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
NFSv3	111	TCP および 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：クラスタに向かう アウト：クラスタからファブリックまたは外に向かう	接続
NFSv3	608	UDP	入力 / 出力	リモート NFS サーバー
NFSv3	2049	TCP	入力 / 出力	リモート NFS サーバー
NX-API	8443	TCP	入力 / 出力	NX-OS リリース 9.x 以降を搭載した Cisco MDS 9000 シリーズ スイッチでパフォーマンス モニタリングに使用されます。
SCP	22	TCP	入力 / 出力	SCPは、リモートサーバーへのバックアップファイルのアーカイブなど、デバイスと Nexus Dashboard の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。Nexus Dashboard 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。 Nexus Dashboard 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 IP アドレスがあります。これは、Nexus Dashboard 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：クラスタに向かう アウト：クラスタからファブリックまたは外に向かう	接続
SCP	22	TCP	発信	Nexus Dashboard POAP-SCP ポッドの永続 IP アドレスから、テレメトリ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。 Nexus Dashboard 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 IP アドレスがあります。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。
SMTP	25	TCP	発信	SMTPポートは、**[管理（Admin）>] [サーバー設定（Server Settings）] > [全般（General）]**ページで設定できます。 これはオプションの機能です。
SNMP	161	TCP および UDP	アウト	Nexus Dashboard からデバイスへの SNMP トラフィック。
SNMP トラップ	2162	UDP	入力	デバイスから Nexus Dashboard 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 IP アドレスに向けて送信されます。 Nexus Dashboard 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 IP アドレスがあります。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。
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：クラスタに向かう アウト：クラスタからファブリックまたは外に向かう	接続
SSH	1022	TCP および UDP	入力 / 出力	その他のクラスタ ノード
Syslog	514	UDP	入力	Nexus Dashboard 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 IP アドレスに向けて送信されます。 Nexus Dashboard 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 IP アドレスがあります。これは、Nexus Dashboard 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。
VXLAN	4789	UDP	入力 / 出力	その他のクラスタ ノード

次の表に、シングルノード クラスタでの Nexus Dashboard SAN 展開に必要なポートを示します。

表 *6 :* 単一ノード クラスタでの *SAN* 展開向けの *Nexus Dashboard* ポート

サービス	ポート	プロトコル	方向 イン：クラスタに向かう アウト：クラスタからファブリックまたは外に向かう	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）
GRPC（テレメトリ）	33000	TCP	入力	Nexus Dashboard 永続 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 Telemetry サーバー。
HTTPS（vCenter、Kubernetes、OpenStack、Discovery）	443	TCP	発信	Nexus Dashboard 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。
SCP	22	TCP	入力 / 出力	SCPは、リモートサーバーへのバックアップファイルのアーカイブなど、デバイスと Nexus Dashboard の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。Nexus Dashboard 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。 Nexus Dashboard 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 IP アドレスがあります。これは、Nexus Dashboard 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：クラスタに向かう アウト：クラスタからファブリックまたは外に向かう	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	発信	Nexus Dashboard POAP-SCP ポッドの永続 IP アドレスから、テレメトリ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。 Nexus Dashboard 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 IP アドレスがあります。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。
SMTP	25	TCP	発信	SMTPポートは、**[管理（Admin）>] [サーバー設定（Server Settings）]>[全般（General）]**ページで設定できます。 これはオプションの機能です。
SNMP	161	TCP および UDP	アウト	Nexus Dashboard からデバイスへの SNMP トラフィック。
SNMP トラップ	2162	UDP	入力	デバイスから Nexus Dashboard 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 IP アドレスに向けて送信されます。 Nexus Dashboard 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 IP アドレスがあります。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：クラスタに向かう アウト：クラスタからファブリックまたは外に向かう	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。
Syslog	514	UDP	入力	Nexus Dashboard 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 IP アドレスに向けて送信されます。 Nexus Dashboard 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 IP アドレスがあります。これは、Nexus Dashboard 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。

Nexus Dashboardの 永続 IP アドレス

永続 IP アドレス（外部サービス IP アドレスとも呼ばれる）は、Nexus ダッシュボード クラスター内のさまざまなコントローラおよびテレメトリ機能に使用される IP アドレスです。「永続」という用語が使用されるのは、ノードまたはポッドに障害が発生した場合にサービスが異なる Nexus Dashboard ノード間を移動する可能性があるものの、ファブリック内のスイッチによって参照されるサービスの IP アドレスが保持されるためです。これにより、Nexus ダッシュボード関連の障害イベントが発生した場合にスイッチの設定更新が不要になります。永続 IP アドレスは、展開される機能に応じて、管理サブネットとデータ サブネットの両方でプログラムできます。

次の場所に移動して、 Nexus Dashboard で設定された永続 IP アドレスを表示できます。

Admin > **System Settings** > **General**

外部プール 並べて表示するを見つけ、 **外部プール** 並べて表示するの左下の領域に **ある [すべて表示（View all）]** をクリックして、設定された永続的なIPアドレスをNexusダッシュボードに表示します。

リリース 4.x での永続 IP アドレスの更新

このセクションでは、永続 IP アドレスの Nexus Dashboard リリース 4.x での変更に関する情報を提供します。また、Nexus Dashboard リリース 4.x へのアップグレードに進む前に、永続的な IP アドレスを特定の数に更新する方法についても説明します。

- 必要な IP アドレス数の削減

  リリース 4.1.1 以降、以前の Nexus Dashboard リリースで排他的 IP アドレスが必要であった一部のサービスが他のサービスにマージされました。たとえば、Nexus ダッシュボードノードごとに、データ ネットワーク上のソフトウェア テレメトリ、フロー テレメトリ、および IPFM テレメトリ コレクタがマージされ、コレクタ サービスごとに 1 つの IP アドレスで 3 つの機能をすべて果たすようになりました。

- LAN デバイスの接続性

  LAN デバイス接続のタイプ（データまたは管理）は、**[管理（Administration）] > [システム設定（System Settings）] > [ファブリック管理（Fabric management）] > [詳細設定（Advanced settings）] > [管理（Administration）] > [LAN デバイス管理の接続性（LAN Device Management Connectivity）]**で設定できます。

  リリース 4.1.1 より前のリリースでは、LAN デバイス接続のデフォルト設定は [管理（Management）] でした。リリース 4.1.1 以降、このデフォルトは [データ（Data）] に変更されました。ただし、 Nexus Dashboard リリース 3.2.x から 4.x にアップグレードする場合、LAN デバイス接続のユーザー構成は保持されます。

- テレメトリのためのレイヤ 3 永続 IP サポート

  Nexus Dashboard リリース 4.1.1 以降、テレメトリコレクタ X の永続 IP は、レイヤ 3 隣接 Nexus Dashboard クラスタでサポートされます。レイヤ 3 BGP のデプロイメントの詳細については、以下を参照してください。

Nexus Dashboard リリース 4.x では、永続 IP アドレスの数とサービスへのマッピング方法が変更されました。次のサービスは、 Nexus Dashboard の永続 IP アドレスを使用します。

LAN 展開：

- テレメトリ コレクタ x：データ ネットワークでは、1 ノード クラスターの場合は 1 つの永続 IP アドレス、3 ノード以上のクラスターの場合は 3 つの永続 IP アドレスが必要です。
- SNMP トラップおよび syslog 受信者：LAN デバイスの接続タイプがデータに設定されている場合はデータ ネットワーク上の 1 つの永続 IP アドレス、LAN デバイスの接続タイプが管理に設定されている場合は管理ネットワーク上の 1 つの永続 IP アドレス。
- スイッチ ブートストラップ サービス（POAP/ PnP ）：LAN デバイスの接続タイプがデータに設定されている場合はデータ ネットワーク上の 1 つの永続 IP アドレス、LAN デバイスの接続タイプが管理に設定されている場合は管理ネットワーク上の 1 つの永続 IP アドレス。
- （オプション）エンドポイント ロケータ（EPL）：EPL が有効になっている各ファブリックのデータ ネットワーク上の 1 つの永続 IP アドレス。EPL 機能は、特定の Nexus ダッシュボードクラスターで最大 4 つのファブリックに対して有効にできます。

- （オプション）IPFM（メディア用の IP ファブリック） テレメトリ コレクタ x：LAN デバイスの接続がデータに設定されている場合、追加の永続的な IP は必要ありません。ただし、LANデバイスの接続タイプが管理に設定されている場合、管理ネットワークには、1ノードクラスターの場合は 1 つの永続 IP アドレス、3 ノード以上のクラスターの場合は 3 つの永続 IP アドレスが必要です。

SAN 展開：

- SNMPトラップおよび syslog 受信者:データ ネットワーク上の 1 つの永続 IP アドレス。
- スイッチ ブートストラップ サービスデータ ネットワーク上の 1 つの永続 IP アドレス。
- （オプション）SAN Insights receiver-x：データ ネットワークでは、1 ノード クラスタの場合は 1 つの永続 IP アドレス、3 ノード以上のクラスタの場合は 3 つの永続 IP アドレスが必要です。

IPv4 のみの Nexus Dashboard クラスター デプロイメントの場合、上記の各サービスは 1 つの永続 IPv4 アドレスを消費します。IPv6 のみの Nexus Dashboard クラスター展開の場合、各サービスは 1 つの永続 IPv6 アドレスを消費します。デュアルスタック Nexus Dashboard クラスター デプロイメントの場合、永続 IP が必要な各サービスが 1 つの IPv4 アドレスと 1 つの IPv6 アドレスを消費します。

新規インストールまたはアップグレード

必要な永続 IP アドレスの総数は、必ずしも新規インストールまたはアップグレードを実行しているかどうかに基づいて必ずしも変更されるわけではありません。さらに、Nexus Dashboard の新規インストール（グリーンフィールド デプロイメント）の場合、データ ネットワークでのみ永続 IP アドレスを設定する必要があります。クラスターのインストールが完了した後、LAN デバイスの接続タイプをデータから管理に変更できます。

前述のように、以前の Nexus Dashboard リリースと比較して、 Nexus Dashboard 4.x のデフォルト設定に変更があります。Nexus Dashboard 4.x では、デフォルトの LAN デバイス管理の接続性はデータに設定されています。以前のリリースでは管理に設定されていました。統合された Nexus Dashboard の提供に向けた取り組みの一環として、目標は、推奨されるベストプラクティスのデプロイメントをできるだけ簡単にすることです。Nexus Dashboard からスイッチへの到達可能性は、Nexus Dashboard データ インターフェイスを介して行うことを推奨します。Nexus Dashboard 管理インターフェイスは、主に UI/ APIアクセス、およびAAA、DNS、プロキシ、NTP 、Intersight などの到達可能性のために使用されます。最後に、 Nexus Dashboard リリース 3.2.x から Nexus Dashboard リリース 4.x へのインライン アップグレードを実行すると、ユーザーが設定した接続設定が保持されることに注意してください。

留意すべきその他の考慮事項

上記の要因に加えて、永続 IP アドレスに関して留意すべきいくつかの追加の考慮事項があります。

- Nexus Dashboard の展開モード:
  - レイヤ 2：ここでは、クラスター内の Nexus Dashboard ノードはレイヤ 2 隣接です。これは、すべての Nexus Dashboard ノードがそれぞれ同じ管理サブネットとデータ サ

ブネットを共有することを意味します。永続 IP アドレスは、データネットワークまたは管理ネットワークと同じネットワーク上にある必要があります。

- レイヤ3 BGP : このモードでは、クラスター内の Nexus Dashboard ノードはレイヤ 3 隣接です。つまり、クラスター内の各 Nexus Dashboard ノードに、一意の管理サブネットとデータ サブネットが関連付けられます。クラスターを形成するには、ノード間に IP 到達可能性がある必要があります。永続 IP アドレスは、 Nexus Dashboard ノードのデータまたは管理インターフェイス サブネットのいずれかに属するサブネットから取得することはできません。この場合、LAN デバイス管理の接続性はデータに設定する必要があり、変更できません。

マッピングの更新

永続的な IP アドレスのマッピングが更新され、正しいサービス名が表示されるようになりました。

さらに前	新しい
cisco-nir-collectorpersistent1-service	Telemetry collector-1
cisco-nir-collectorpersistent2-service	Telemetry collector-2
cisco-nir-collectorpersistent3-service	Telemetry collector-3
cisco-ndfc-dcnm-poap-data-http-ssh	スイッチのブートストラップ サーバ
cisco-ndfc-dcnm-poap-mgmt-http-ssh	スイッチのブートストラップ サーバ
cisco-ndfc-dcnm-syslog-trap-data	SNMPトラップと syslog レシーバ
cisco-ndfc-dcnm-syslog-trap-mgmt	SNMPトラップと syslog レシーバ
cisco-ndfc-pmn-telemetry-mgmt-worker-0	IPFM telemetry collector-1
cisco-ndfc-pmn-telemetry-mgmt-worker-1	IPFM telemetry collector-2
cisco-ndfc-pmn-telemetry-mgmt-worker-2	IPFM telemetry collector-3
cisco-ndfc-dcnm-san-insight-receiver-1	SAN Insights receiver-1
cisco-ndfc-dcnm-san-insight-receiver-2	SAN Insights receiver-2
cisco-ndfc-dcnm-san-insight-receiver-3	SAN Insights receiver-3

必要な永続 IP アドレスの合計数の決定

必要な永続 IP アドレスの合計数とその取得元のネットワークを決定しようとする際には、上記のすべての要因が考慮されます。最終的な Nexus Dashboard 展開構成を確認して、十分な数の永続 IP アドレスがデプロイメントのための適切なサブネット範囲にあることを確かめてください。また、必要に応じ、追加の永続IPアドレスがあることも確かめてください。これは、

設定した LAN デバイスの接続性のタイプと、エンドポイント ロケータ（EPL）など、有効にする可能性のあるサービスに応じて決まります。

次に、永続 IP アドレスがどのように使用されるかを示すシナリオの例を示します。

新規インストール

まず、クラスターの起動時に、前述のように、クラスターのサイズに基づいて、データネットワーク上に特定の数の永続 IP アドレスが必要になります。

- **物理ノードまたはリモート対応ノードを備えた 1ノードクラスター**：データネットワークで少なくとも **3 つ** の永続的なIPアドレスが必要
- **物理ノードまたはリモート対応ノードを備えた 3ノード以上のクラスター**：データネットワークに少なくとも **5 つ** の永続的なIPアドレスが必要

（注） これらの値は、IPv4 または IPv6 のいずれかで有効ですが、デュアルスタック IPv4 および IPv6 の場合は2倍になります。たとえば、3ノード以上のクラスターの場合、デュアルスタック IPv4 および IPv6 用にデータ ネットワーク上に少なくとも 10 個の永続的な IP アドレスが必要です（5 個の IPv4 および 5 個の IPv6 の永続的 IP アドレス）。

ブートストラップ後、次のシナリオに応じて、必要に応じて永続 IP アドレスを追加する必要がある場合があります。

- LANデバイス接続タイプセットを**Data**に設定した場合、エンドポイント ロケータ（EPL）機能を有効にしない限り、追加の永続IPアドレスは必要ありません。この機能では、EPL が有効になっているファブリックごとにデータ ネットワーク上で 1 つの追加の永続 IP アドレスが必要です。
- LAN デバイスの接続タイプを **Data** から **Management**に変更した場合：
  - Syslog/ SNMP トラップおよびスイッチのブートストラップ機能のために、管理ネットワーク上に 2 つの追加の永続 IP アドレスが必要です。
  - （オプション）エンドポイント ロケータ（EPL）を有効にする場合は、EPLが有効になっているファブリックごとにデータ ネットワーク上に 1 つの永続 IP アドレスが必要です。
  - （オプション）IP Fabric for Media（IPFM）ファブリックが必要な場合は、管理ネットワーク上に 1 ノードクラスターの場合は 1 つの永続 IP アドレス、3 ノード以上のクラスターの場合は 3 つの永続 IP アドレスが必要です。

表 *7:* 永続的な *IP* 要件：*4.x* の新規インストール

ND ノード数	LAN デバイス管理の接続性	必須の永続IPアドレス	オプションの永続IPアドレス	他の一般的な永続IPアドレス
1	Data は[1]	データ ネットワークに 3 つ	該当なし	EPL が有効になっているファブリックごとのデータ ネットワークに 1 つ
	管理	管理ネットワークに 2 つ データ ネットワークに 1 つ	IPFM ファブリック用管理ネットワークに 1 つ	
3以上	Data [1]	データ ネットワークに 5 つ	N/A	
	管理	管理ネットワークに 2 つ データ ネットワークに 3 つ	IPFM ファブリックの管理ネットワークに 3 つ	

[1] ND ブートストラップ プロセス中のデフォルト オプション セットを示します

アップグレード：

ここで、 Nexus Dashboard 3.2.x から 4.x にアップグレードするとします。Nexus Dashboard 4.x で必要な永続 IP アドレスの数は、実行していたサービスと Nexus Dashboard 3.2.x でのサービスの設定方法、および Nexus Dashboard 4.1 でのクラスターーのサイズによって異なります。Nexus Dashboard 3.2.x リリースで設定した LAN デバイス管理の接続性は、 Nexus Dashboard 4.x リリースへのインラインアップグレードを実行するときはそのまま保持されることに注意してください。

- Nexus Dashboard 3.2.x システムで実行中の **NDFC** のみがある場合、および
  - **Data** を Nexus Dashboard 3.2.x の LAN デバイス接続のタイプとして設定している場合、および
    - Nexus Dashboard 4.x にアップグレードする 1 ノード クラスターがある場合、データ ネットワーク上に 3 つの永続 IP アドレスが必要です。
    - Nexus Dashboard 4.x にアップグレードする 3 ノード以上のクラスターがある場合、データ ネットワーク上に 5 つの永続 IP アドレスが必要です。
  - **Management** を Nexus Dashboard 3.2.x の LAN デバイス接続のタイプとして設定している場合、および
    - Nexus Dashboard 4.x にアップグレードする 1ノード クラスターがある場合、管理ネットワークにはすでに 2 または 3 つの永続 IP アドレスがあるはずです（IPFM / PTP 機能が有効になっている場合は追加の IP が必要です）。さらに、データ

ネットワークに 1 つの永続 IP アドレスが必要です。そうでないと、4.x へのアップグレードはアップグレード前の検証手順中に失敗します。

- Nexus Dashboard 4.x にアップグレードする 3 ノード以上のクラスターがある場合、管理ネットワークにはすでに 2 つまたは 5 つの永続 IP アドレスがあるはずです（IPFM/PTP機能が有効になっている場合は、3つの追加のIPが必要です）。データ ネットワークに次の 3 つの永続 IP アドレスを構成する必要があります。そうして初めて、4.x へのアップグレードを続行できます。

- Nexus Dashboard 3.2.x システムで実行している **NDI** のみがある場合、および
  - Nexus Dashboard 4.x にアップグレードする 1ノード クラスターがある場合、データ ネットワークにはすでに 4 つの永続 IP アドレスが構成されているはずです。4.x へのアップグレード後には、3つの永続IPアドレスのみが使用されます。残りは再利用できます。
  - Nexus Dashboard 4.x にアップグレードする 3 ノード以上のクラスターがある場合、スタンドアロンNX-OS展開をサポートするための2つの追加データIPと、データ ネットワークの 8 つの永続 IP アドレスがすでに構成されているはずです。4.x へのアップグレード後には、これらのデータ IP アドレスのうち 5 つだけが使用されます。残りは再利用できます。
- Nexus Dashboard 3.2.xシステムで実行している **NDO** のみがある場合、 Nexus Dashboard 3.2.x システムに永続IPアドレスはありません。Nexus Dashboard 4.x にアップグレードする際、Nexus Dashboard 4.x にアップグレードする 3ノード クラスターがある場合、アップグレードを続行するには、データ ネットワーク上に 5 つの永続 IP アドレスが必要です。
- Nexus Dashboard 3.2.x システムに **NDO** および **NDI** 展開モードがあり、3 ノード以上のクラスターを Nexus Dashboard 4.x にアップグレードする場合は、データ ネットワークにすでに 8 つの永続 IP アドレスが設定されていることになります。4.x へのアップグレード後は、これらのデータ永続 IP アドレスのうち 5 つだけが使用されます。残りの永続 IP アドレスは再利用できます。
- Nexus Dashboard 3.2.x システムに **NDFC** と **NDI** の展開モードだけがあり、3 ノード以上の物理 ND クラスターを Nexus Dashboard 4.x にアップグレードする場合は、LAN デバイス管理接続設定に基づいて 2 つのオプションがあります。
  - **Management** を Nexus Dashboard 3.2.x の LAN デバイス接続のタイプとして設定していた場合、すでに NDI のデータ ネットワークに 8 つの永続 IP アドレス、NDFC の管理ネットワークに 2 つの永続 IP アドレスが設定されています。4.x へのアップグレード後、管理サブネットの永続 IP アドレスは 2 つ使用され、データ永続的 IP アドレスは 3 つだけ使用されます。残りの永続 IP アドレスは再利用できます。
  - **Data** を Nexus Dashboard 3.2.x の LAN デバイス接続のタイプとして設定していた場合、すでに NDI のデータ ネットワークに 8 つの永続 IP アドレス、NDFC に追加で 2 つの永続 IP アドレスが設定されています。4.x へのアップグレード後は、これらのデータ永続 IP アドレスのうち 5 つだけが使用されます。残りの永続 IP アドレスは再利用できます。

表 *8 :* 永続 *IP* の要件：*3.2.x* から *4.x* へのアップグレード

ND 3.2.x のデプロイメントモード	ND ノード数	LAN デバイス管理の接続性	ND 3.2.x の永続 IP アドレスの要件	ND 4.x の永続 IP アドレスの要件
NDFC	1	データ	データ ネットワークに 2 つ、加えてIPFM/PTP が有効な場合はデータ ネットワークに 1 つ	データ ネットワークに 3 つ
		管理	管理ネットワークに 2 つ、加えてIPFM/PTP が有効な場合は管理ネットワークに 1 つ	管理ネットワークに 2 つ、IPFM ファブリック用管理ネットワークに 1 つ データ ネットワークに 1 つ
NDFC	3以上	データ	データ ネットワークに 2 つ、加えてIPFM/PTP が有効な場合はデータ ネットワークに 3 つ	データ ネットワークに 5 つ
		管理	管理ネットワークに 2 つ、加えてIPFM/PTP が有効な場合は管理ネットワークに 3 つ	管理ネットワークに 2 つ、加えてIPFM ファブリック用管理ネットワークに 3 つ データ ネットワークに 3 つ
NDFC + NDI	3 物理	データ	データ ネットワークに 10	データ ネットワークに 5 つ
		管理	管理ネットワークに 2 つ データ ネットワークに 8 つ	管理ネットワークに 2 つ、加えてIPFM ファブリック用管理ネットワークに 3 つ データ ネットワークに 3 つ
NDI	1	N/A	データ ネットワークに 3 つ	データ ネットワークに 3 つ
NDI	3以上	該当なし	データ ネットワークに 10	データ ネットワークに 5 つ
NDO	3	該当なし	なし	データ ネットワークに 5 つ
NDO + NDI	3以上	該当なし	データ ネットワークに 8 つ	データ ネットワークに 5 つ

（注） EPL の永続 IP アドレスの要件は、リリース 4.x でも リリース 3.2.x と同じです。

BGP 構成と永続的な IP アドレス

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ものに対しては、1つ以上の永続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 アドレス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 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 アドレス 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 アドレス機能を構成することができます。この場合、永続的な IP アドレスは、「レイヤ 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アドレスは、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 アドレス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アドレス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 Dashboard GUI から有効にすることができます。

BGP を有効にして永続 IP アドレス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 アドレスを交換することを確認します。
- データ ネットワークのレイヤ3 隣接関係については、ブートストラップ プロセス中にBGPを構成する必要があります。BGPは管理ネットワークのレイヤ3隣接関係をサポートしません。
- 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。

ラウンド トリップ時間の要件

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、表示に示されているラウンド トリップ時間（RTT）要件があります。

表 *9:* クラスタのラウンド トリップ時間の要件

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

接続	最大 RTT
マルチクラスタ接続（クラスタ間接続）を使用してクラスタが接続されている場合、あるクラスタ内のノードと別のクラスタ内のノードとの間の接続。 マルチクラスタ接続の詳細については、「クラスタ接続」を参照	500 ミリ秒
外部 Domain Name System（DNS）サーバと Nexus ダッシュボード クラスタ間	5 秒
クラスタ ノードとスイッチ間	150 ミリ秒

Nexus Dashboard ストレージの前提条件（仮想フォーム ファクタ）

ドキュメントのこのセクションでは、Cisco Nexus Dashboard 展開のストレージインフラストラクチャ（VMware、KVM、Nutanix など）を設計するためのガイダンスを提供します。

Nexus Dashboard は、ネットワークデバイスからの高頻度のテレメトリとフロー データを処理する機能を提供します。その結果、ストレージは次のことを保証する上で重要な役割を果たします。

- 信頼性の高いデータの取り込み
- 正確な分析とインサイト
- 大規模なシステム パフォーマンス

このセクションでは、実稼働環境で推奨されるストレージ特性、期待されるパフォーマンス、およびアーキテクチャ上の考慮事項の概要について説明します。

主なワークロードの特徴

主なワークロードの特徴は次のとおりです。

- 持続的なスループット要件による書き込み集約型の取り込み
- 混合 I/O パターン：
  - シーケンス書き込み（データ取り込み）
  - ランダムな読み取り/書き込み（クエリと分析）
- 遅延の影響を受けやすい操作（特に取り込み時）

基準ストレージ要件

基準ストレージ要件は次のとおりです。

容量

- ストレージ容量：2 個のストレージディスクが必要です。
  - 起動ディスクとして使用される 50G サイズのディスク
  - データを保存する別のディスク
- データのサイズは、プラットフォームのフレーバーによって異なります。例: 仮想データには 3 TB のディスクが必要です。

パフォーマンス

Nexus Dashboard のストレージを設計するには、容量だけでなくパフォーマンスにも注意を払う必要があります。次のことを確保する必要があります。

- 同期遅延が 10 ミリ秒未満。
- 実際のスループットと IOPS 要件はスケールに依存し、次のように異なります。
  - IOPS：1.5K io/s ~ 80K io/s（持続）
  - スループット：10 MB/s ~ 1.5 GB/s（持続）

Nexus Dashboard から `acs diag diskio /dev/sdb` コマンドを使用して、ディスク I/O の遅延を確認することもできます。

ストレージの設計に関する推奨事項

これらの要件を満たすために、これらは Nexus Dashboard のストレージを設計するための推奨事項です。

ストレージ メディアの選択と配置

実稼働環境への展開では、NVMe または SSD を使用することを強くお勧めします。配置の観点から、ダイレクトアタッチストレージ（DAS）は通常、最も予測可能な結果を提供します。RAID コントローラを使用している場合、オーバーヘッドを最小限に抑えるために JBOD モードで設定します。

リモート ストレージまたは共有ストレージの使用

パフォーマンス要件を常に満たしている場合、リモート ストレージ ソリューション（SAN、NAS、ソフトウェア デファインド ストレージ プラットフォームなど）を使用できます。ストレージは、短時間のバースト時だけでなく、必要な IOPS とスループットを継続的に提供する必要があることに注意してください。多くの場合、ローカルに接続されたストレージは、Nexus Dashboard ワークロードに最も一貫性のある予測可能なパフォーマンスを提供します。

- 共有ストレージの場合、他のワークロードが原因でパフォーマンスの変動が発生し、リソースの競合によって遅延が急増する可能性があります。

- したがって、専用ディスクを使用し、Nexus Dashboard クラスタ内の他のノードや他のワークロードと共有しないことをお勧めします。

キャッシング

- Nexus Dashboard の観点からは、すべての書き込みがハイパーバイザを介してフラッシュされます。したがって、パフォーマンスを実現する上でキャッシングが重要な役割を果たします。
- キャッシュがないと、4KB の書き込みはすべて物理メディアまで書き込まれる必要があります。キャッシュ ポリシーのライト スルーではなく、常にライト バックを有効にする必要があります。
- 通常、ハードウェア ベンダーは、データの完全性を保証するためにデフォルトをライト スルーに設定します。たとえば、その正確な秒時に電源コードが引き抜かれた場合や建物の電源が失われた場合、データはすでにディスク上にあります。完全に安全です。
- 最近のシステムはバッテリ（BBU）を使用し、バッテリまたは SuperCap が正常な場合にのみキャッシュを使用します。バッテリに障害が発生した場合、または充電中の場合にディスク コントローラが自動的にフォールバックにフォールバックするようにプロビジョニングされていることを確認してください。

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。インバンドテレメトリ機能を有効にするためのファブリックの構成の詳細については、次のドキュメントを参照してください。

- Cisco ACI ファブリックの Cisco Nexus Dashboard Insights の準備
- *Cisco Nexus Dashboard* でのテレメトリによる *Nexus* ファブリックの展開

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。

外部レイヤ 3 ネットワークを介した接続

Nexus Dashboard 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、すべてのファブリック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 ファブリックを管理するために Nexus Dashboard Orchestrator を使用する場合は、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ファブリックの 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。

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。

- テレメトリを使用する場合は、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。

- 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。最初の図は ACI と NX-OS ファブリック混在、2 番目の図は ACI ファブリックのみの場合です。

図 *1* : *ACI*ファブリックと *NX- OS*ファブリックが混在する、レイヤ *3* ネットワークを使用した接続

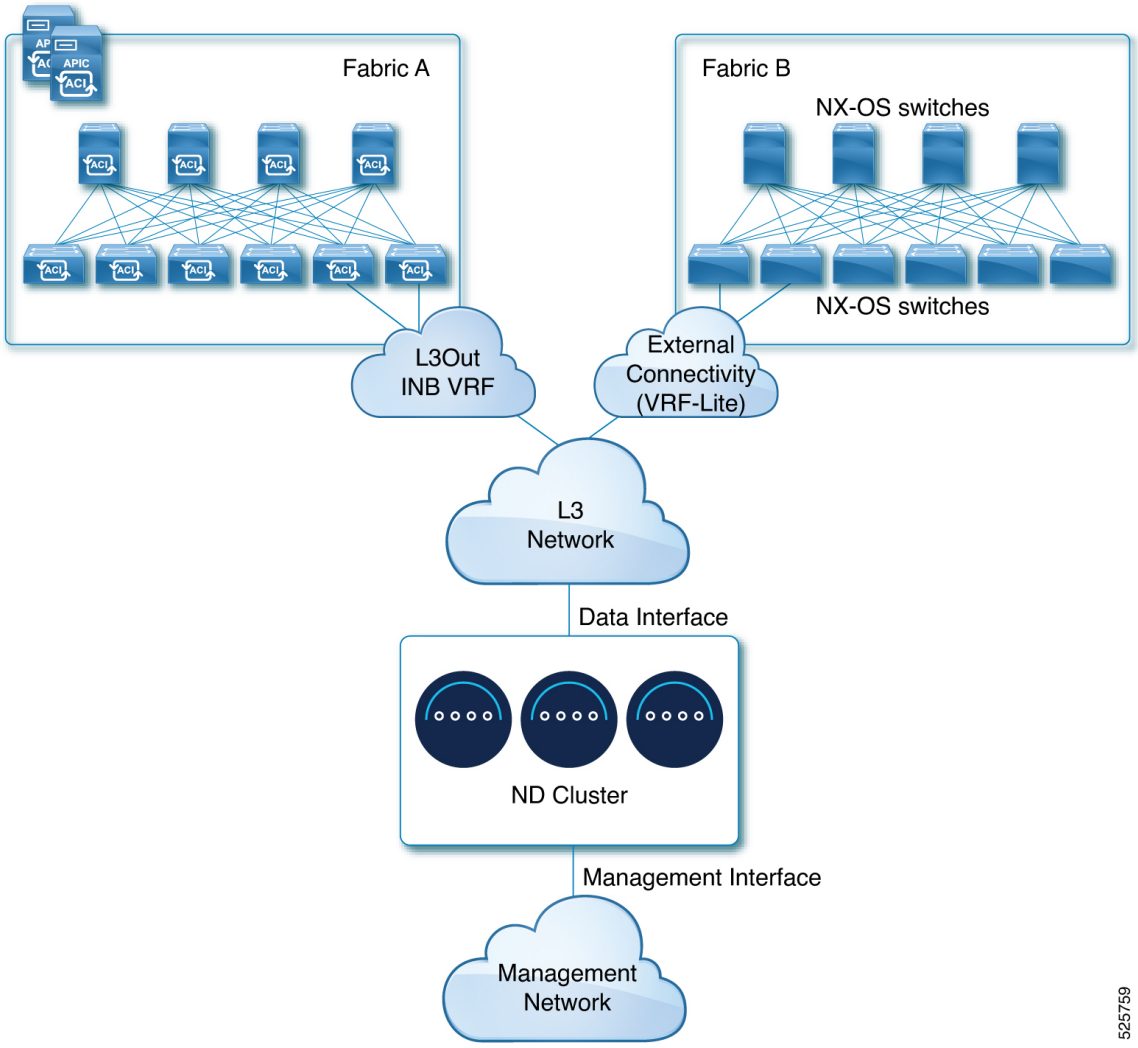
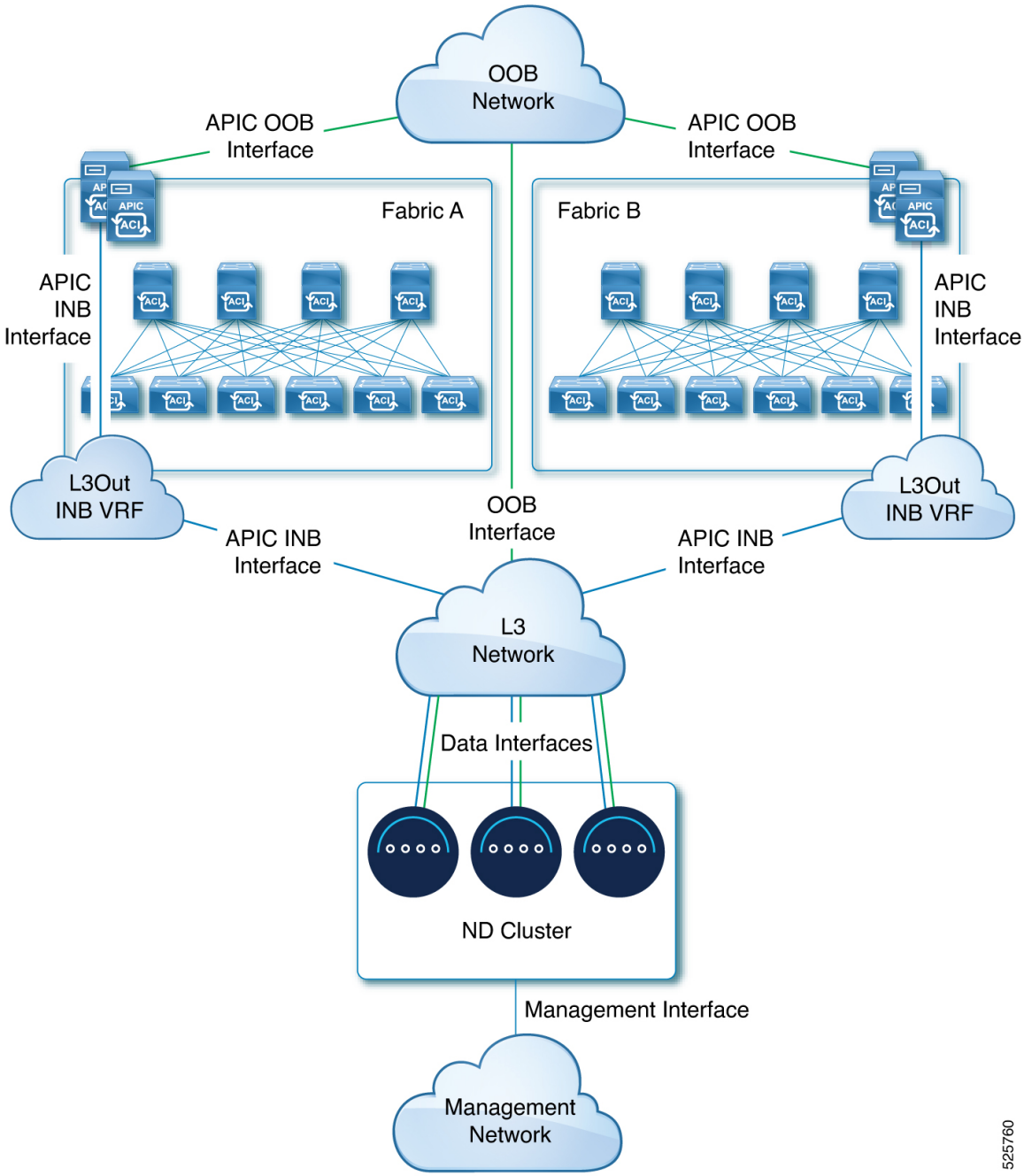


図 *2 : ACI*ファブリックのみを使用したレイヤ *3* ネットワークを使用した接続



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ファブリックを管理するためにNexus Dashboard Orchestratorを使用する場合は、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ファブリックの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。

  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。

- テレメトリを使用する場合は、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。ただし、データインターフェイスからアウトオブバンドインターフェイスへの接続を確立する場合は、ルートを追加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/またはブリッジ ドメインに接続し、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。

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。

- Nexus DashboardをNX-OSリーフ スイッチに直接接続し、それらのスイッチもNexus Dashboardで管理する場合、スイッチを新しいファブリックに追加する前にクラスタをブートストラップできるように、CLIを使用してデータ ネットワークの構成を手動でプロビジョニングする必要があります。このシナリオのため、Nexus Dashboardが接続されているファブリックを同じNexus Dashboardで管理する予定の場合、この方法で新しいファブリックを展開することはお勧めしません。

- 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、Nexus Dashboard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。

- APIC側の設定では、次には必要な設定があります。

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

    Nexus Dashboardはインバンド VRFの管理テナント内のデフォルトのインバンド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。

次の図は、これらのタイプの接続を示しています。

- ACI ファブリックに直接接続
- NX- OS ファブリックに直接接続
- ACI および NX- OS ファブリックに直接接続

図 *3 : ACI* ファブリックに直接接続

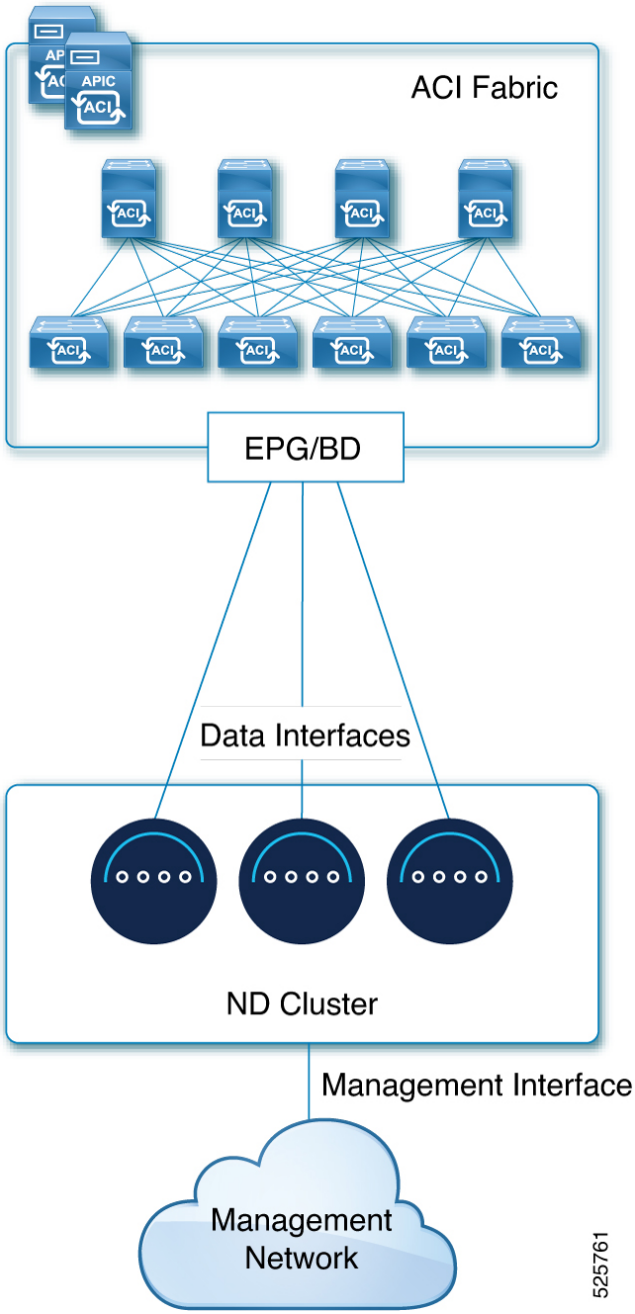


図 *4 : NX- OS* ファブリックに直接接続

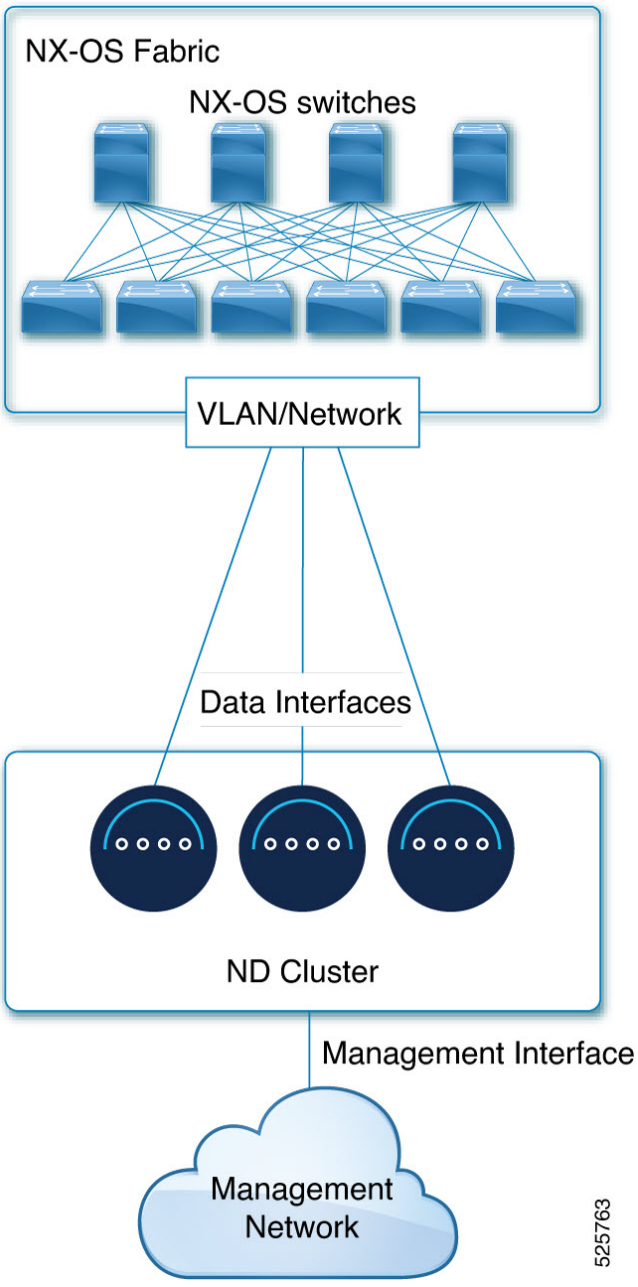
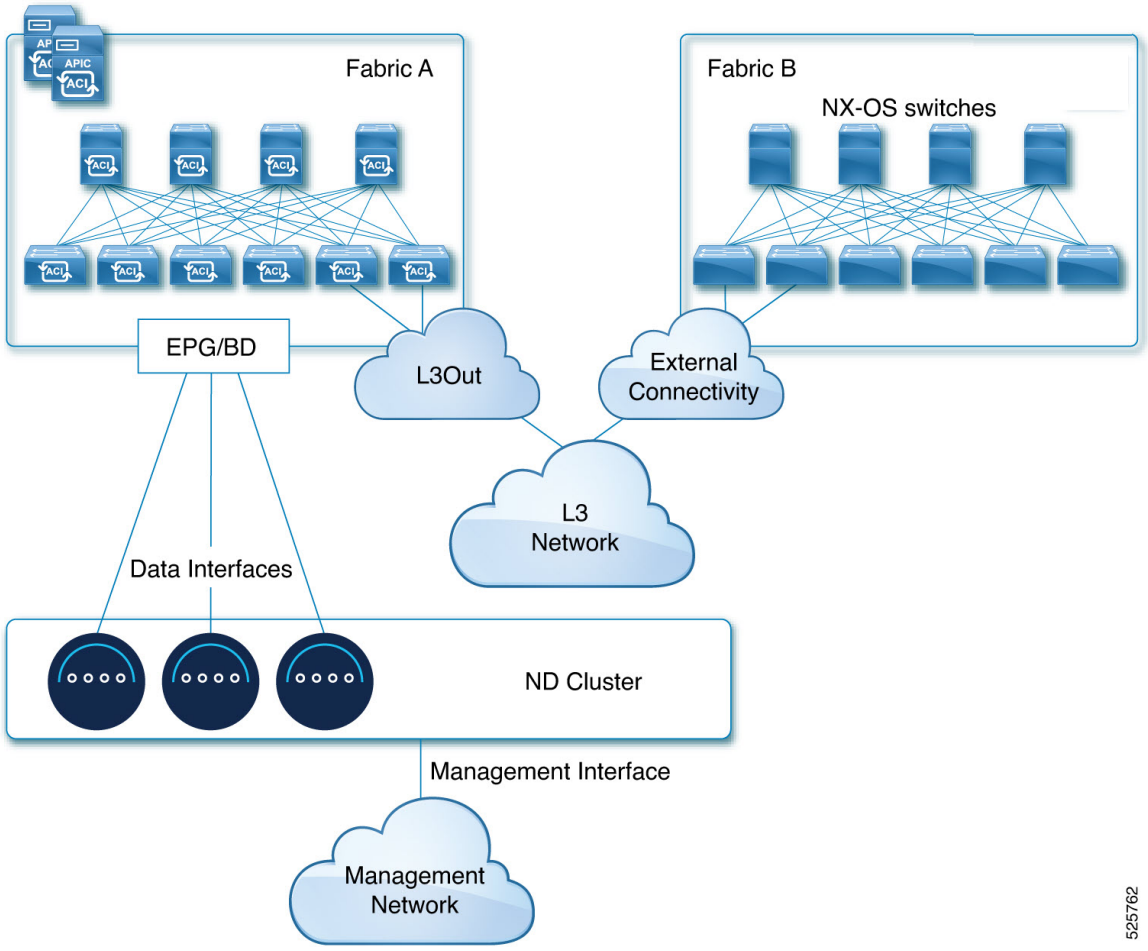


図 *5 : ACI* および *NX- OS* ファブリックに直接接続



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。