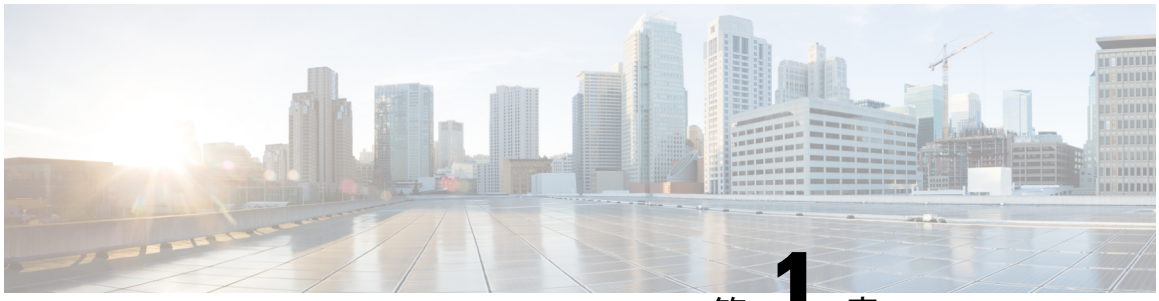
Cisco Nexus Dashboard 展開とアップグレード ガイド、リリース 4.1.x

最終更新：2026 年 6 月 15 日

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

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

目 次



第 1 章

新機能および変更された機能に関する情報

新機能および変更情報

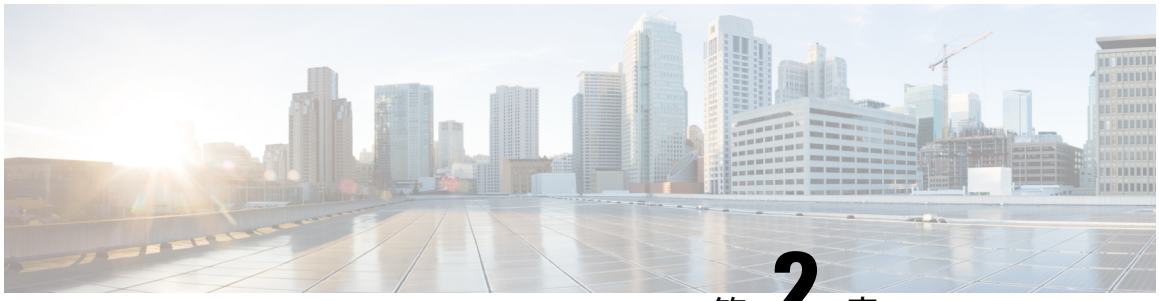
このテーブルは、ガイドが最初に発行されたリリースから現行リリースまでの、このガイドの組織と機能に対する重要な変更の概要を示しています。テーブルは、ガイドに加えられたすべての変更のすべてを網羅したリストを提供しているわけではありません。

表 *1*: 最新のアップデート

リリース	新機能またはアップデート	参照先
4.1.1	このドキュメントの最初のリリース。	N/A

第 I 部

Nexus Dashboard の展開の準備



第 2 章

展開の概要と要件

Nexus Dashboard のデプロイメントの概要

Nexus Dashboard プラットフォーム

Cisco Nexus Dashboard は、複数のデータ センター ファブリックのための中央管理コンソールで、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、保証を実現し、Cisco ACI や NX-OS 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 Dashboard は、シスコが提供するデータ センターの LAN ファブリック、SAN ファブリック、および IP Fabric for Media（IPFM）ネットワークにまたがる ACI および NX-OS デプロイメント向けの包括的な管理ソリューションです。Nexus Dashboard は、IOS-XE スイッチ、IOS-XR ルータ、シスコ以外のデバイスなど、他のデバイスもサポートしています。マルチファブリック コントローラである Nexus Dashboard は、VXLAN EVPN、クラシック 3 層 LAN、FabricPath、LAN 向けのルーテッドベース ファブリックなどの複数の展開モデルを管理すると同時に、これらすべての環境ですぐに使用できる制御、管理、モニタリング、および自動化機能を提供します。さらに、Nexus Dashboard を SAN にインストールすると、Cisco Nexus Dashboard ストレージ固有の機能と分析機能に重点を置いた NX-OS モードで Cisco MDS スイッチと Cisco Nexus ファミリのインフラストラクチャを自動化します。

（注） この文書は、Cisco Nexus Dashboard クラスタを最初に展開し、ファブリックをオンボードする方法について説明します。クラスタが稼働したら、日常の操作に関する Nexus Dashboard の設定と操作に関する記事を参照してください。

統合 Nexus Dashboard のデプロイメント

Nexus Dashboard（ND）プラットフォームと関連サービスは、以前に次の方法で利用できました。

- ND リリース 3.1 より前のリリースでは、 Nexus Dashboard にはプラットフォーム ソフトウェアのみが付属しており、サービスは含まれていませんでした。最初の ND プラットフォームの展開後、サービス（NDI、NDO、NDFC またはそのいずれか）を個別にダウンロード、インストール、および有効化します。
- ND リリース 3.1 および 3.2 では、 Nexus Dashboard は ND プラットフォーム ソフトウェアと個々のサービスのソフトウェアを統合されたパッケージ形式でパッケージ化しました。ただし、サービスは個別に有効にしたままです。ファブリックの管理とインサイトは、まだ統合されていない、独立した 2 つのピースでした。

  さらに、 Nexus Dashboard リリース 3.1 および 3.2 には「展開モード」の概念があり、展開モードを選択することで、Nexus Dashboard で特定のサービスを静的に有効にできます。ただし、展開モードの変更は、データや再インストールを含むサービス全体を消去する破壊的な試みでした。最後に、 Nexus Dashboard リリース 3.1 および 3.2 の単一の Nexus Dashboard クラスタですべてのサービスを実行することはできませんでした。

ND リリース 4.1 以降、プラットフォームと個々のサービスが 1 つの製品に統合されました。サービスを個別に展開および構成する必要がなくなり、個々のサービスをアクティブ化したり、展開モードを静的に構成したりする必要がなくなります。さらに、フォーム ファクタに応じて、以前のリリースでサービスとして出荷されていた機能を Nexus Dashboard で使用できます。独立したサービスの概念がなくなったため、ユーザーエクスペリエンスが統合され、代わりに、単一のダッシュボード ビューからすべての機能を利用できるようになりました。

（注） 展開したクラスタの形式とクラスタ ノードの数によっては、特定の機能（コントローラ、オーケストレータ、テレメトリなど）がユニファイド Nexus Dashboard 製品で使用できない場合があります。 Nexusダッシュボード キャパシティ プランニング ツール の情報を確認して、クラスターインストールで使用できる機能を確認します。

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 Dashboard 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。

このガイドでは、 Nexus Dashboardソフトウェアの初期デプロイメントについて説明します。これは、物理および仮想フォームファクタに共通です。物理クラスターを展開する場合は、UCSサーバーのハードウェアの概要、仕様、およびラッキングの手順について、*Nexus Dashboard* ハードウェア セットアップ ガイドを 参照してください。

（注） Nexus Dashboard ソフトウェアへの root 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 展開のために特別なユーザー `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 ドキュメント ライブラリの「トラブルシューティング」の章を参照してください。

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 ファクタのノード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 3 機種の異なる Cisco UCS サーバーをサポートしています（`SE-NODE-G2`、`ND-NODE-L4`、および `ND-NODE-G5S`）。同じクラスター内に `SE-NODE-G2` サーバーと `ND-NODE-L4` サーバーを混在させることはできますが、 `SE-NODE-G2` サーバーと `ND-NODE-L4` サーバーと同じクラスターに `ND-NODE-G5S` サーバーを混在させることはできません。

- 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、Cisco UCS 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。Nexus Dashboard ハードウェアのセットアップについては、特定の UCS モデルの *Nexus Dashboard ハードウェア セットアップ ガイド*を参照してください。

- 仮想アプライアンス：Nexus Dashboardクラスタを展開できる仮想フォームファクタで、VMware ESX（`.ova`）または RHEL KVM (`.qcow2`）を使用します。

  仮想フォームファクタは、次の 2 つのプロファイルをサポートしています。

  - データ ノード：このプロファイルは、システム要件が高いため、より大規模な展開や統合型のデプロイメント向けに設計されています。
  - アプリ ノード：システム要件が低いこのプロファイルは、セカンダリ ノードとして展開できます。プライマリ ノードとして展開することもできますが、統合型のデプロイメントはサポートしていません。

  さらに、Nexus Dashboard リリース 4.1(1) 以降、AWS パブリッククラウドで仮想 Nexus Dashboard（vND）を実行するためのサポートを利用できます。詳細については、「Amazon Web Services（AWS）での仮想 Nexus Dashboard（vND）の展開 （141 ページ）」を参照してください。

（注） 展開を計画するときは、このドキュメントの次のいずれかのセクションで、展開するフォームファクタに固有の「前提条件とガイドライン」のリストを確認してください。サポートされているフォーム ファクタ、スケール、およびクラスタ サイジングの要件のクイック リファレンスは、Nexus Dashboard クラスタ サイジング ツールで入手できます。

スケールとクラスタ サイジングのガイドライン

基本的な Nexus Dashboard の展開は、通常、クラスタを起動するために必要な 1 つまたは 3 つの プライマリ ノードで構成されます。スケール要件に応じて、3 ノード以上のクラスターを最大 3 つのセカンダリ ノードを追加して拡張し、より高いスケールをサポートできます。

- 物理クラスタの場合、プライマリ ノードに障害が発生した場合にクラスタを容易に回復できるようにするため、最大 2 つの スタンバイ ノードを追加することもできます。
- 仮想クラスタの場合、最大2つのスタンバイ ノードもサポートされますが、コントローラのみまたはオーケストレーションのみの展開の場合は 3 ノードの vND (アプリ) プロファイルでのみサポートされます。

特定のユースケースに必要な追加のセカンダリ ノードの正確な数は、Nexus Dashboard クラスタ サイジング ツールから入手できます。

スケールとクラスター サイジングの制限

次の制限は、スケーリングとクラスターのサイジングに適用されます。

- 単一ノード展開は、初期の展開後に 3 ノード クラスタに拡張することはできません。

  単一ノードクラスターを展開し、それを3ノードクラスターに拡張するか、セカンダリ ノードを追加する場合は、それをバックアップし、新しい 3 ノード ベース クラスターを展開して、後でそのバックアップを復元する必要があります詳細については、「*Nexus Dashboard* のバックアップと復元」を参照してください。

- 単一ノード展開では、追加の セカンダリ ノードまたは スタンバイ ノードはサポートされません。
- 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。

  詳細については、「*Cisco Nexus Dashboard* を使用した高可用性サービスの展開」を参照してください。

サポートされているノード タイプと機能について

これらのノードタイプは、 Nexus Dashboardリリース4.1.1より前のリリースで使用できました。

- SE-NODE-G2 (UCS-C220-M5)。3 ノード クラスターの製品 ID は SE-CL-L3 です：

- ND-NODE-L4 （UCS-C225-M6）。3 ノードクラスターの製品 ID は ND-CLUSTER-L4です：

Nexus Dashboard リリース 4.1.1 以降、このノード タイプも使用できるようになりました。

- ND-NODE-G5S (UCS-C225-M8)。3 ノードクラスターの製品 ID は ND-CLUSTERG5S です：

また、LAN 展開でこれらの機能を活用できます。

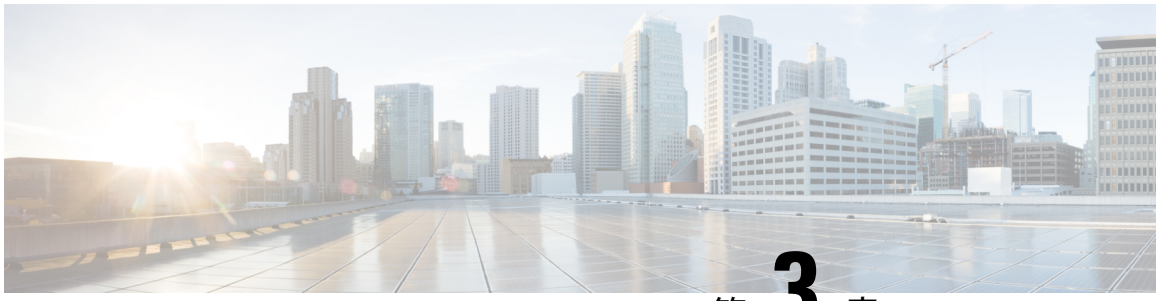
- **Controller**：ファブリック管理とも呼ばれます。この機能は、NX- OS および非 NX OSスイッチ（Catalyst、 ASR など）の管理に使用されます。これには、非 ACI ファブリック タイプの作成、ソフトウェアアップグレードの実行、それらのファブリックでの新しい構成の作成が含まれます。
- **Telemetry**：この機能は、Nexus Dashboard リリース 4.1.1 より前のリリースで Nexus Dashboard Insights によって提供されていた機能と同様のテレメトリ機能を提供します。 **[管理（Manage）] > [ファブリックの（Fabrics）]** でファブリックを作成または編集するときに、 **テレメトリ** 機能を有効にして使用できます。
- **Orchestration**：**オーケストレーション** 機能を Nexus ダッシュボードを介して拡張し、複数の ACI ファブリックを接続し、ネットワークおよびポリシー構成とともにテナントを複数の ACI ファブリックに統合して展開します。 **[管理（Administration）] > [システム設定] > [マルチクラスタ接続（Multi-cluster 接続）] > [接続（Cluster）]** でACI を追加する場合、 **オーケストレーション** 機能を有効にして使用できます。

これらの機能は個別にイネーブルにできますが、場合によってはこれらの複合機能セットの 1 つとしてイネーブルにできます。

- コントローラとテレメトリ
- オーケストレーションとテレメトリ
- コントローラ、テレメトリ、およびオーケストレーション（アプリ ノード クラスターまたは SE-NODE-G2 でクラスターではサポートされていません）

注意事項と制約事項

- Nexus Dashboardリリース4.1.1では、新しい ND-NODE-G5S （UCS -C225-M8）ノードを古い SE-NODE-G2 （UCS -C220-M5）および ND-NODE-L4 とのクラスター内で混在させることはできません。 (UCS-C225-M6) ノード。
- 6 ノードの物理アプライアンス クラスターは主に、テレメトリ機能が有効になっている拡張スケール NX-OS または ACI ファブリック用に設計されており、非テレメトリの展開には推奨されません。
- 仮想フォーム ファクタは、 *Cisco Nexus Dashboard Verified Scalability Guide* ので説明しているように、多くのクラスターサイズおよびタイプですべての機能をサポートしているわけではありません。



第 3 章

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

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

- 4 クラスター ノードの展開。ここでクラスターの構成は次のとおりです。
  - 3 つの仮想ノード（データ）、および
  - 1 つのスタンバイ ノード

  サポートする構成。スタンバイ ノードを使用せずにこのクラスターを再展開します。クラスター内のいずれかのノードに障害が発生した場合は、新しいノードを再インストールし、**[管理（Administration）]** > **[システム（System）]** **[ステータス（Status）]** > **[ノード（Nodes）]**に移動してから、**[アクション（Actions）]** > **[再登録（Re-Register）]** をクリックして、再インストールしたノードをクラスターに戻します。
- 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。

- 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 （23 ページ）と SAN 展開用の通信ポート（39 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 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、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：
  - 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。
- 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 パブリック クラウドでの vNDデプロイメント プロセスを介して展開されたクラスタは、純粋な IPv6 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 *2:* 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。Nexus Dashboard は、データ ネットワーク ポート(bond0)上のICMPパケットを 1 秒あたり 100 パケットにレート制限し、バースト制限を 5 にします。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 （51 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。

- ポッド プロファイル ポリシーは、展開するノードの数に基づいて動的に設定されます。

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。
- フローテレメトリ機能またはトラフィック分析機能を使用する場合には、ACI ファブリック ノード制御ポリシーでテレメトリの優先順位を選択する必要があります。

  Cisco APIC で、テレメトリの優先順位を選択するには、**[ファブリック（Fabric）] > [ファブリック ポリシー（Fabric Policies）] > [ポリシー（Policies）] > [モニタリング（Monitoring）] > [ファブリック ノードの制御（Fabric Node Controls）] > *[<policy-name>]*** > **[機能選択（Feature Selection）]**の順に選択します。<*policy-name*> のモニタリングは、**[ファブリック（Fabric）] > [ファブリック ポリシー（Fabric Policies）] > [スイッチ] > [リーフ/スパイン スイッチ（Leaf/Spine Switches）] > [プロファイル（Profiles）] >** に続ける必要があります。
- フローテレメトリ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。
- 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。

- 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

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、クラスター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
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。 （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 クラスター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。
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 IP アドレスを使用して 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 Nexus Dashboard EPL サービスはピアを形成します。 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。

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
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。
HTTP	80	TCP	発信	インターネット/プロキシ

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、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。
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

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、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 （In/Out）	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
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
SCP	22	TCP	入力 / 出力	SCPは、リモートサーバへのバックアップ 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、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（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、クラスター 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	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、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、クラスター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 *4 : 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
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 IP アドレスを使用して 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 Nexus Dashboard EPL サービスはピアを形成します。 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。
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

サービス	ポート	プロトコル	方向（In/Out）	接続
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。
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、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。
HTTPS	443	TCP	発信	スイッチと APIC および NX-OS の帯域内
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、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。
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。

サービス	ポート	プロトコル	方向 （In/Out）	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
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
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

サービス	ポート	プロトコル	方向（In/Out）	接続
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、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	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（In/Out）	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	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
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

サービス	ポート	プロトコル	方向（In/Out）	接続
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 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 （51 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 *5 : 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。
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

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
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、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	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 *6 : 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、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
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 *7:* 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 ィン：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、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）
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 ィン：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 *8 :* 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 *9 :* 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 *10*：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	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
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
ファブリック スイッチまで	150 ミリ秒

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

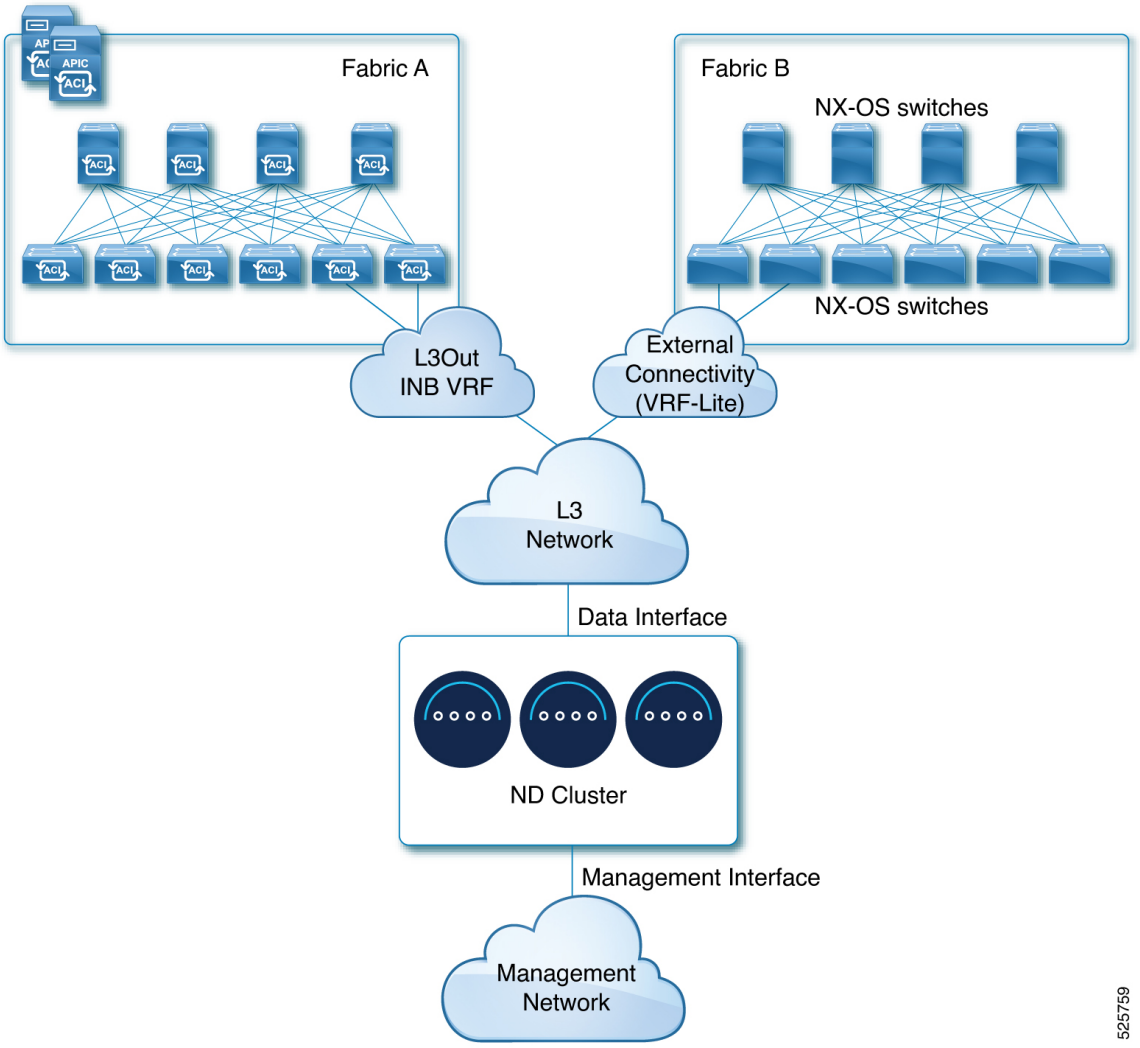
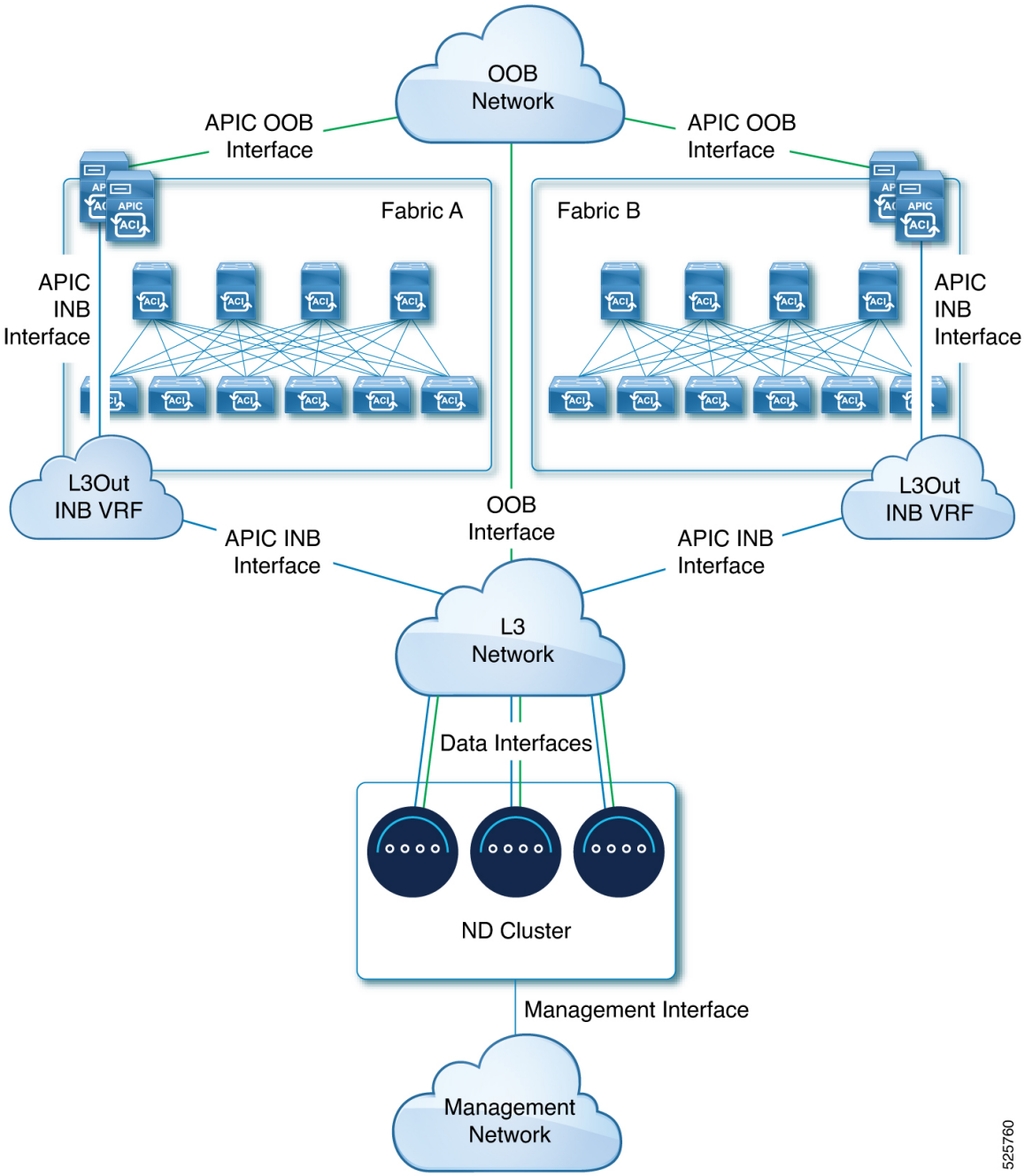


図 *2 : ACI*ファブリックのみを使用したレイヤ *3* ネットワークを使用した接続



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。
- 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、以下の推奨設定があります。
  - 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

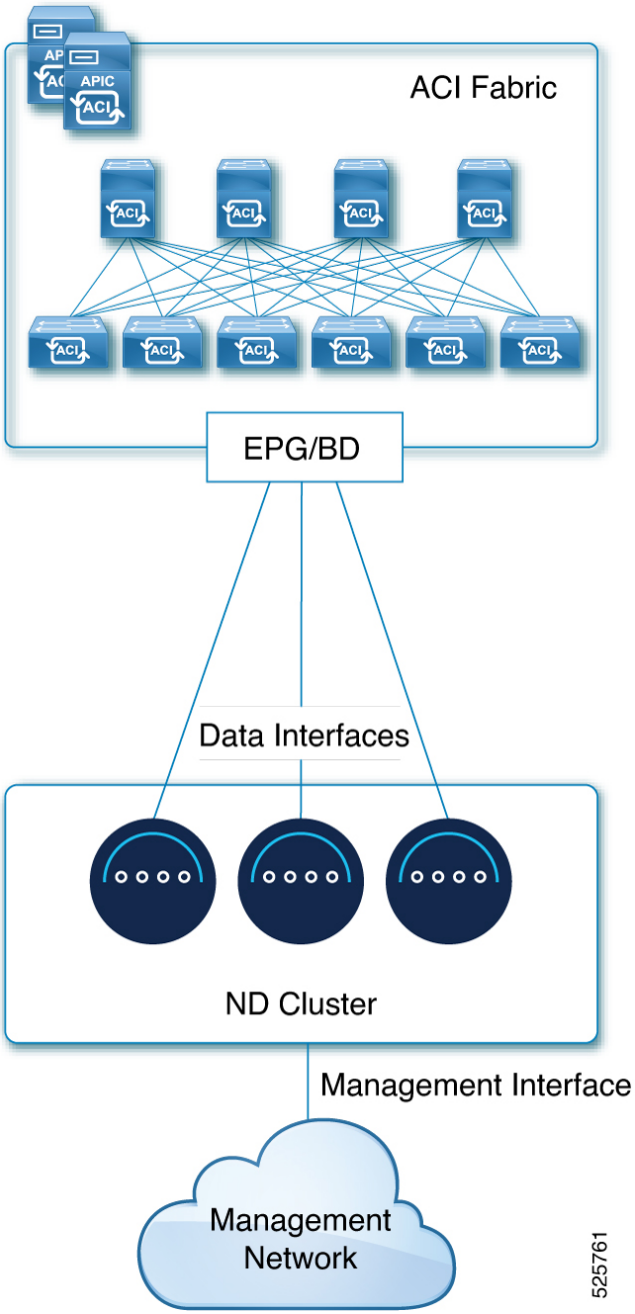


図 *4 : NX- OS* ファブリックに直接接続

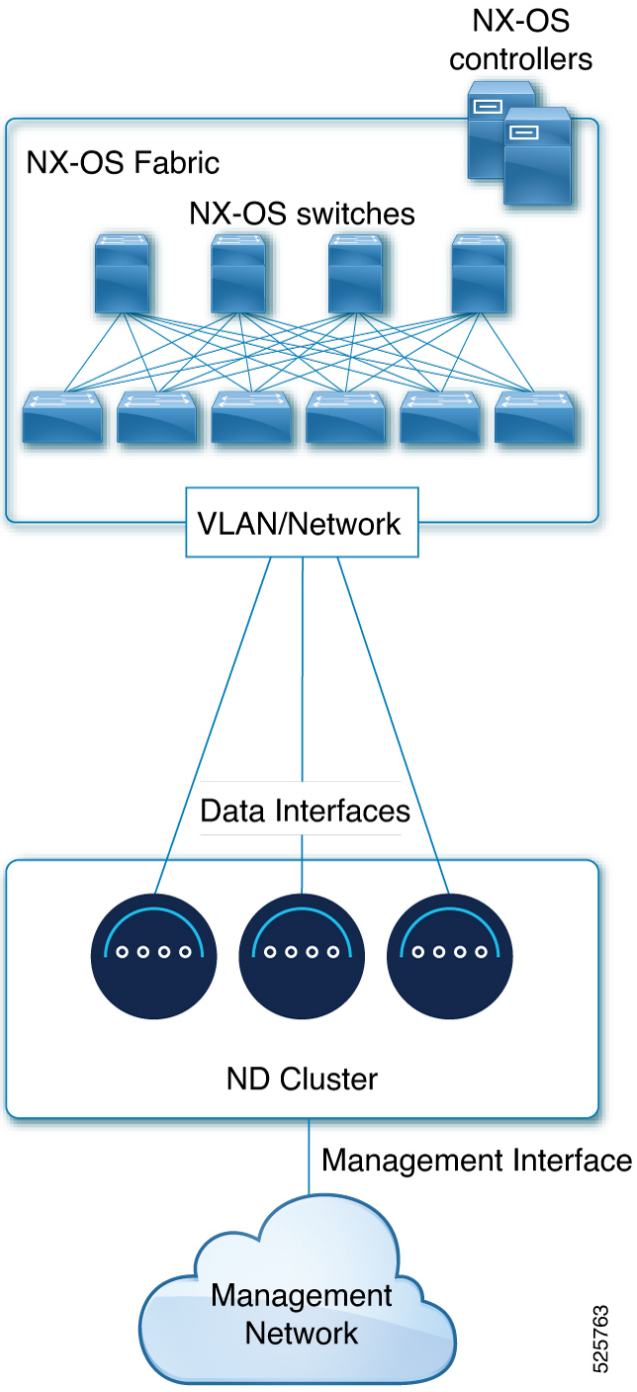
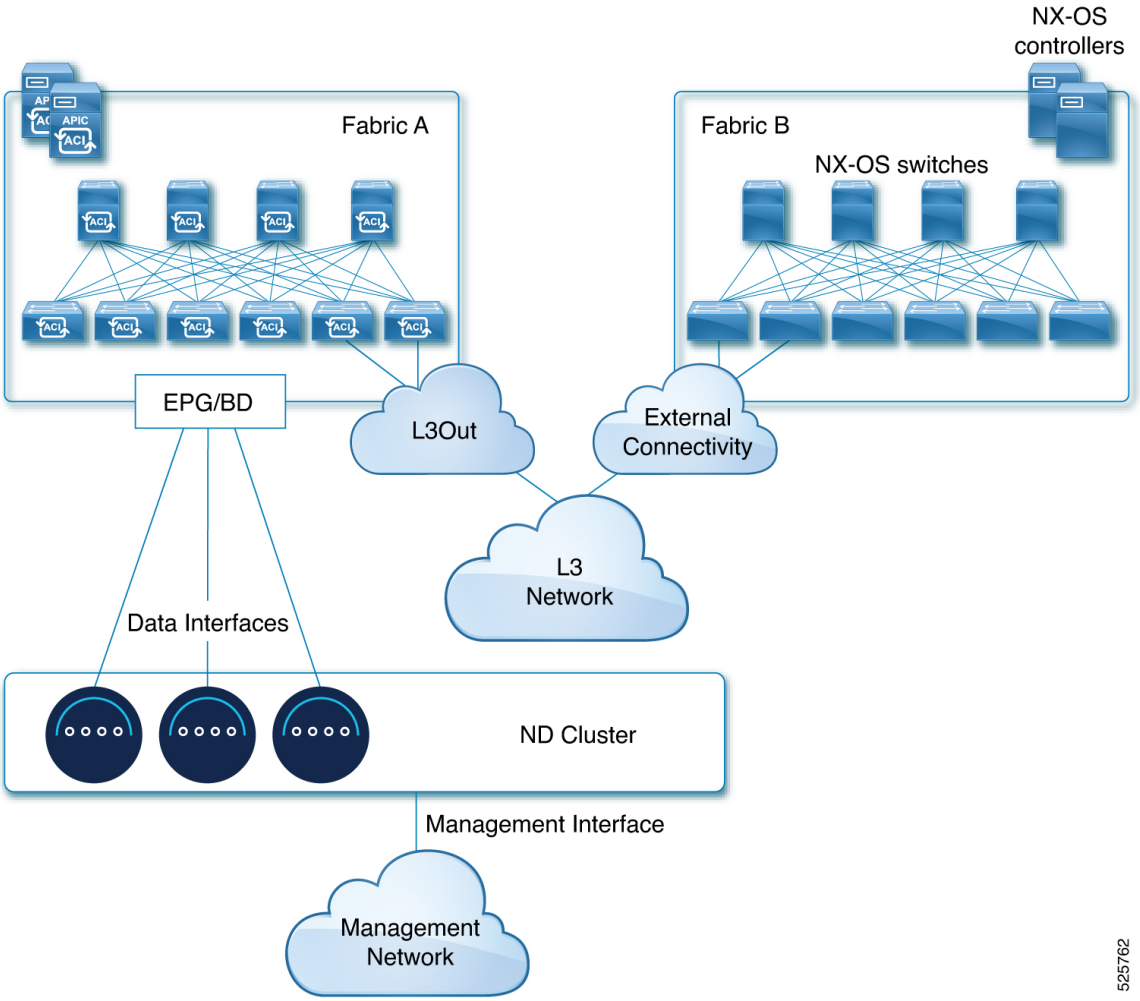
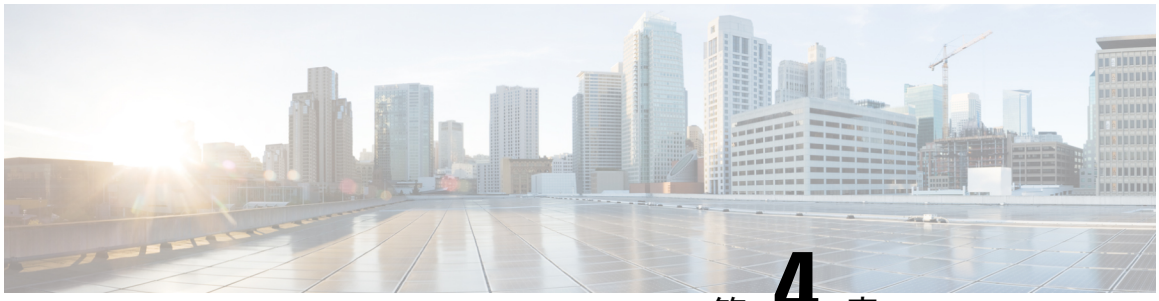


図 *5 : ACI* および *NX- OS* ファブリックに直接接続



第 II 部

クラスタの展開



第 4 章

インストール前のチェックリスト

インストール前チェックリスト

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-Prod-CL01	
Nexus Dashboard の実装タイプ（LAN/SAN）	LAN	
DNS プロバイダー	8.8.8.8	
DNS 検索ドメイン	cisco.com	
NTPプロバイダ	1.1.1.1	
（オプション）**NTP 認証 キー**	123456789	
（オプション） **NTP 認証 ID**	100	
（オプション）**NTP 認証タイプ**	MD5	
Proxy Server	192.168.50.1	
（オプション） **プロキシ サーバ無視ホスト**	10.0.0.1	
（オプション）**プロキシ ユーザー名**	Proxy-user	

パラメータ（Parameters）	例	入力する値
（オプション）**プロキシ パスワード**	P@ssword!123	
アプリ ネットワーク	172.17.0.1/16 (default)[1]	
サービス ネットワーク	100.80.0.0/16 (default)[2]	
（オプション）**アプリ ネットワーク IPv6**	2001:db8:abcd:0012::0/64	
（オプション）**サービス ネットワーク IPv6**	2001:db8:efgh:0012::0/64	

[2] These are the default values and we do not recommend that you change them. If you want to change the values, see the appropriate chapter in the "Deploying the Cluster" part.

（注） 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 *12 :* ノードの詳細

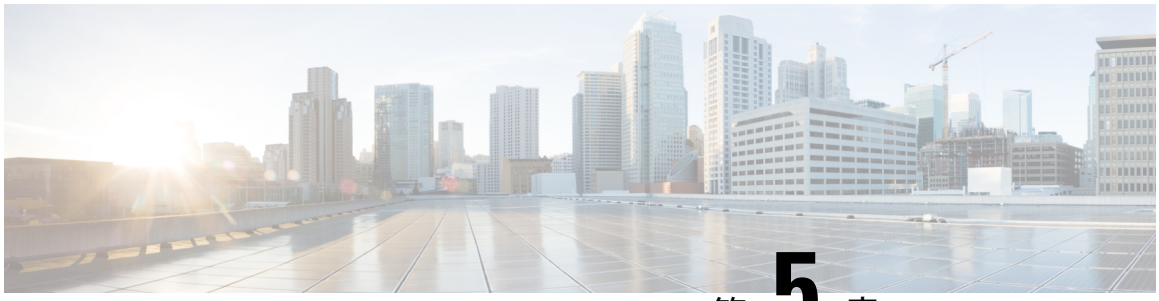
パラメータ（Parameters）	例	入力する値
物理ノードの場合、最初のノードの **CIMC** アドレスとログイン情報	10.196.220.84/24 ユーザ名: admin パスワード：Cisco1234	
物理ノードの場合、2 番目のノードの **CIMC** アドレスとログイン情報	10.196.220.85/24 ユーザ名: admin パスワード：Cisco1234!	
物理ノードの場合、3 番目のノードの **CIMC** アドレスとログイン情報	10.196.220.86/24 ユーザ名: admin パスワード：Cisco1234!	
各ノードのレスキュー ユーザに使用される**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!	

パラメータ（**Parameters**）	例	入力する値
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	
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**（アップストリーム スイッチ ポートの設定が「トランク」で、 VLANがトランク許可リストに追加されている場合にのみ、 VLAN を入力します）	101	
（オプション）BGP を有効にする場合、最初のノードの **ASN**	63331	
（オプション）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	
（オプション）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	
（オプション）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	

パラメータ（**Parameters**）	例	入力する値
（オプション）2番目のノードの**データ ネットワーク VLAN**	101	
（オプション）BGP を有効にする場合、2 番目のノードの**ASN**	63331	
（オプション）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	
（オプション）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	
クラスタ接続（L2/BGP）	L2	
（オプション）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	
（オプション）BGP を有効にする場合、3 番目のノードの**ASN**	63331	
（オプション）BGP を有効にし、純粋な IPv6 展開を使用する場合、**ルータ ID**（IPv4 アドレスの形式）	3.3.3.3	

パラメータ（Parameters）	例	入力する値
（オプション）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	
（オプション）BGP を有効にする場合、3 番目のノードの **BGP ピア**の ASN	55555	

また、クラスターの起動中に永続的な IP アドレスをプログラムする必要があります。詳細については、「Nexus Dashboardの 永続 IP アドレス （51 ページ）」を参照してください。



第 5 章

物理アプライアンスとしての展開

物理アプライアンスとして Nexus Dashboard を展開する場合の前提条件と注意事項

Nexus ダッシュボード クラスタの展開に進む前に、次の手順を実行する必要があります。

- 前提条件とガイドライン（11 ページ）に記載されている前提条件を確認して完了します：
- デプロイメントに影響する可能性のある情報については、 *Cisco Nexus Dashboard*のリリースノートを確認してください。Cisco Nexus Dashboard のドキュメントのランディング ページを参照してください。
- 使用しているサーバーのモデルに対応した、*Cisco Nexus Dashboard* ハードウェア セットアップ ガイドの説明に従って、以下のハードウェアを使用しており、サーバがラックに接続されていることを確認します。

  物理アプライアンス フォーム ファクタは、オリジナルの Cisco Nexus Dashboard プラットフォーム ハードウェア、

  - `SE-NODE-G2` （UCS-C220-M5）。3 ノード クラスター シャーシの製品 ID は、`SE-CL-L3` です。
  - `ND-NODE-L4` （UCS-C225-M6）。3 ノード クラスター シャーシの製品 ID は、`ND-CLUSTER-L4` です。
  - `ND-NODE-G5S` (UCS-C225-M8)。3 ノード クラスター シャーシの製品 ID は `ND-CLUSTERG5S` です。

（注） このハードウェアは、Cisco Nexus Dashboard ソフトウェアのみをサポートします。他のオペレーティングシステムがインストールされている場合、そのノードは Cisco Nexus Dashboard ノードとして使用できなくなります。

- Cisco Integrated Management Controller（CIMC）のサポートされているバージョンを実行していることを確認します。

  CIMC のサポートおよび推奨される最小バージョンは、Cisco Nexus Dashboard リリースのリリース ノート の「互換性」セクションにリストされています。

- サーバーの CIMC の IP アドレスが構成済みであることを確認します。

  Cisco Integrated Management Controller IP アドレスの構成 （79 ページ）を参照してください。

- Serial over LAN（SOL）が CIMC で有効になっていることを確認します。

  Cisco Integrated Management Controller に対する Serial over LAN の有効化 （80 ページ）を参照してください。

  ブートストラップ ピア ノード ポイントでブートストラップが次のエラーで失敗した場合は、SoL の構成が間違っている可能性があります。

  ```
  Waiting for firstboot prompt on NodeX
  ```

- すべてのノードが同じリリース バージョン イメージを実行していることを確認します。

- Cisco Nexus Dashboard ハードウェアに、展開するイメージとは異なるリリースイメージが付属している場合は、まず既存のイメージを含むクラスタを導入してから、必要なリリースにアップグレードすることをお勧めします。

  たとえば、受け取ったハードウェアにリリース 3.2.1 のイメージがプリインストールされているが、代わりにリリース 4.1.1 を展開する場合は、次の手順に従います：

  1. 最初に、リリース 3.2.1 クラスタをそのリリースの展開ガイドに従って起動します。
  2. それから、既存の Nexus Dashboard クラスターのこのリリースへのアップグレード （157 ページ）で説明されているように、リリース 4.1.1 にアップグレードします。

（注） まったく新しい展開の場合は、このドキュメントに戻ってクラスタを展開する前に、Cisco Nexus Dashboard の最新バージョンを使用してノードを再イメージ化することもできます（たとえば、GUI ワークフローを通じたこのリリースへの直接アップグレードをサポートしていないイメージがハードウェアに付属している場合）。このプロセスについては、このリリースのトラブルシューティングの記事の「ノードの再イメージング」セクションで説明されています。

- 少なくとも 1 ノードのクラスターが必要です。展開するサービスの数に応じて、水平スケーリング用に追加のセカンダリ ノードを追加できます。単一クラスター内のセカンダリ ノードとスタンバイ ノードの最大数については、ご使用のリリースのリリース ノートを参照してください。

Cisco Integrated Management Controller IP アドレスの構成

以下の手順に従い、Cisco Integrated Management Controller（CIMC）IP アドレスを構成します。

手順

ステップ 1 サーバの電源をオンにします。

ハードウェア診断が完了すると、機能（Fn）キーによって制御されるさまざまなオプションが表示されます。

ステップ 2 **F8** キーを押して **Cisco IMC 構成ユーティリティ**を起動します。

ステップ 3 次のサブステップに従います。

a) **NIC モード**を専用モードに設定します。

b) **IPv4** IP モードと **IPv6** IP モードのいずれかを選択します。

DHCP を有効にするか無効にするかを選択できます。DHCP を無効にする場合は、静的 IP アドレス、サブネット、およびゲートウェイ情報を指定します。

c) **NIC 冗長性** が [なし（None）] に設定されていることを確認します。

d) ホスト名、DNS、デフォルト ユーザー パスワード、ポート プロパティ、ポート プロファイルのリセットなどのその他のオプションを表示するには、 **F1** を押します。

ステップ 4 **F10** を押して、構成を保存し、サーバーを再起動します。

Cisco Integrated Management Controller に対する Serial over LAN の有効化

Serial over LAN（SoL）は、基本的な構成情報を提供するために物理アプライアンス ノードに接続するのに使用する `connect host` コマンドに必要です。SoL を使用するには、まず Cisco Integrated Management Controller （CIMC）で SoL を有効にする必要があります。

Cisco Integrated Management Controller で Serial over LANを有効にするには、次の手順に従います。

手順

ステップ 1 CIMC IP アドレスを使用してノードに SSH 接続し、サインイン情報を入力します。

ステップ 2 次のコマンドを実行します。

```
Server# scope sol
Server /sol # set enabled yes
Server /sol *# set baud-rate 115200
Server /sol *# commit
Server /sol *#
Server /sol # show

C220-WZP23150D4C# scope sol
C220-WZP23150D4C /sol # show

Enabled Baud Rate(bps)  Com Port SOL SSH Port
------- --------------- -------- -------------
yes     115200          com0     2400
```

ステップ 3 コマンド出力で、 `com0` が SoL の comポートであることを確認します。

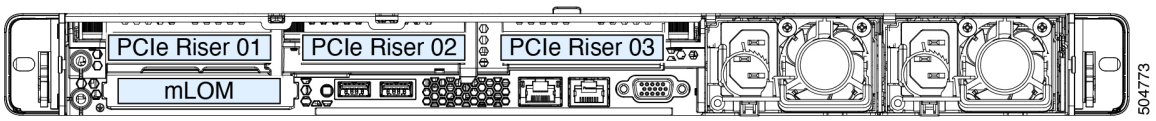
これにより、システムはCIMC CLI から `connect host` コマンドを使用してコンソールをモニタできます。これは、クラスタの起動に必要です。

物理ノードのケーブル接続

物理ノードは、以下の物理サーバーに展開できます：

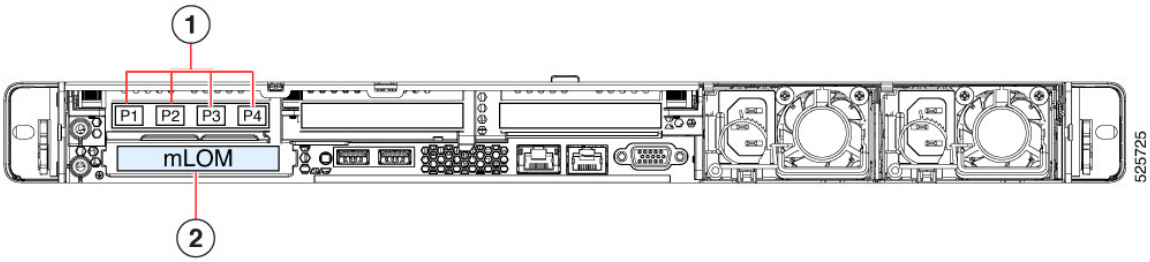
- `SE-NODE-G2` （UCS-C220-M5）および `ND-NODE-L4` （UCS-C225-M6）物理サーバー：

  図 *6 :* ノード接続に使用される *mLOM* および *PCIe* ライザー *01* カード： *`SE-NODE-G2`* （*UCS-C220-M5*）および *`ND-NODE-L4`* （*UCS-C225-M6*）



- ND-NODE-G5S （UCS-C225-M8）の物理サーバーで、これらの接続を行います。

図 7: ノード接続に使用される *mLOM* および *PCIe* ライザー *01* カード：*ND-NODE-G5S*



1	**データ接続**：ポートには、UCSC-P-V5Q50G-D（Cisco UCS VIC 15425 Quad Port 10/25/50G Converged Network Adapter（CNA））PCIE カードの左から右に 1、2、3、4 の番号が付けられています。 サポートされているポート チャネル構成については、以下の「データ ネットワーク接続」情報を参照してください。
2	**管理接続**：モジュール型 LAN on Motherboard（mLOM）の 2 つの MGMT ポート経由。

（注） ND-NODE-G5S サーバーに含まれている OCP カードは、管理目的でのみ 1Gb 銅線接続をサポートします。Nexus Dashboard の他のすべてのネットワーク接続は、4 ポート VIC カード（上の図のコールアウト 1）を活用する必要があります。この VIC カードは 10/25/50Gbps をサポートしており、推奨されている SFP+ ケーブルは SFP-10G-AOC3M ですが、シスコでは 5 m と 7 m のオプションも提供しています。VIC カードでは、データ ネットワーク接続のためにサーバーごとに少なくとも 2 つの接続が必要です。これらの VIC 接続は、サポートされている任意の SFP を活用できますが、Cisco は Nexus Dashboard のシームレスな展開のためにこの接続を推奨しています。

物理ノードは、次のガイドラインに従って展開できます：

- すべてのサーバーに、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。
- ND-NODE-G5S 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。
- ND-NODE-G5S サーバーには、2x10GbE NIC (APIC-P-ID10GC) または 2x25/10GbE SFP28 NIC（APIC-P-I8D25GF）、または「PCIe-Riser-01」スロット（上の図に表示）の VIC1455 カードに含まれており、Cisco Nexus Dashboard のデータ ネットワーク接続に使用します。
- ND-NODE-G5S には、Nexus Dashboard データ ネットワーク接続に使用する「PCIe-Riser-01」スロット (上図参照) に UCSC-P-V5Q50G-D (Cisco UCS VIC 15425 Quad Port 10/25/50G CNA) PCIE カードが含まれています。

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：

- 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（bond0）と管理インターフェイス用（bond1）の Linux ボンドとして設定されます。
- **管理ネットワーク接続**：
  - mLOM カードで `mgmt0` および `mgmt1` を使用する必要があります。
  - すべてのポートが同じ速度（1G または 10G）である必要があります。
- **データ ネットワーク接続**：
  - `SE-NODE-G2` サーバーでは、VIC1455 カードを使用する必要があります。
  - `ND-NODE-L4` サーバーで、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。

（注） 25G Intel NIC を使用して接続する場合は、NIC の設定と一致するようにスイッチポートの FEC 設定を無効にする必要があります。

```
(config-if)# fec off
# show interface ethernet 1/34
Ethernet1/34 is up
admin state is up, Dedicated Interface
  [...]
  FEC mode is off
```

- `ND-NODE-G5S` サーバでは、UCSC-P-V5Q50G-D（Cisco UCS VIC 15425 Quad Port 10/25/50G CNA）PCIe カードは、必要なポート チャネルの組み合わせを介して光ファイバ接続を使用する必要があります。

（注） 25/50 GB の速度で接続する場合は、次の前方誤り訂正（FEC）構成のペアのいずれかが必要です：

Nexus 9000 では	**CIMC** ポート
FEC AUTO	cl74
FC-FEC	cl74
FEC OFF	FEC OFF

- すべてのインターフェイスは、個々のホスト側のスイッチ ポートに接続する必要があります。ファブリック エクステンダ（FEX）、スイッチ ポート チャネル（PC）、およびリモート対応ポート チャネル（vPC）はサポートされていません。

- すべてのポートは同じ速度である必要があります（10G、25G、または 50G のいずれか）。
- `fabric0` ペアの 1 つの物理ポートと `fabric1` ペアの 1 つの物理ポートを活用、ノードをデータ ネットワークに接続します。サポートされているポートのペアリングは次のとおりです：
  - ポート 1（`fabric0`）、ポート2（`fabric1`）
  - ポート 3（`fabric0`）、ポート4（`fabric1`）
- これらの接続のスイッチ ポート チャネルまたは vPC を構成しないでください。上記のサポートされているペアリングは、 VIC カードでのみ有効な物理ポート マッピングを識別します。
- データ ネットワーク接続には、アクティブ スタンバイ モードとして `fabric0` と `fabric1` の両方を使用できます。

（注） 4 ポート カードを使用する場合、ポートの順序は、使用しているサーバーのモデルによって異なります。

- ポート 1 とポート 2 またはポート 3 とポート 4 をペアで使用します。ポート 1/ポート 2 ペアを使用することをお勧めします。
- `SE-NODE-G2` サーバーでは、左から右に、ポート 1、ポート 2、ポート 3、ポート 4 です。
- `ND-NODE-L4m` サーバーでは、左から右に、ポート 4、ポート 3、ポート 2、ポート 1 です。

- ノードを Cisco Catalyst スイッチに接続すると、VLAN が指定されていない場合、パケットは Catalyst スイッチ上で `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。

物理アプライアンスとしての Nexus Dashboard の展開

Nexusダッシュボードの物理ハードウェアを最初に受け取ると、ソフトウェアイメージがプリロードされています。Nexus Dashboard を物理アプライアンスとして展開するには、次の手順に従います。

始める前に

物理アプライアンスとして Nexus Dashboard を展開する場合の前提条件と注意事項 （77 ページ）に記載されている要件とガイドラインを満たしていることを確認します：

手順

ステップ 1 最初のノードの基本情報を設定します。

この手順で説明するように、1 つの（「最初の」）ノードのみを構成する必要があります。他のノードは、次の手順で説明する GUI ベースのクラスタ展開プロセス中に構成され、最初の プライマリ ノードからの設定を受け入れます。他の 2 つの プライマリ ノードには、CIMC IP アドレスが最初の プライマリ ノードから到達可能であり、ログイン クレデンシャルが設定されていることと、データ ネットワーク上でノード間のネットワーク接続が確立されていることを確認する以外に、追加の設定は必要ありません。

a) CIMC 管理 IP を使用してノードに SSH 接続し、`connect host` コマンドを使用してノードのコンソールに接続します。

```
C220-WZP23150D4C# connect host
CISCO Serial Over LAN:
Press Ctrl+x to Exit the session
```

ホストに接続したら、 **Enter** を押して続行します。

b) Nexus Dashboard セットアップ ユーティリティのプロンプトが表示されたら、 **Enter**を押します。

```
Starting Nexus Dashboard setup utility
Welcome to Nexus Dashboard 4.1.1
Press Enter to manually bootstrap your first master node...
```

c) `admin` パスワードを入力して確認します。

このパスワードは、`rescue-user` CLI ログインおよび初期 GUI パスワードに使用されます。

```
Admin Password:
Reenter Admin Password:
```

d) 管理ネットワーク情報を入力します。

```
Management Network:
  IP Address/Mask: 192.168.9.172/24
  Gateway: 192.168.9.1
```

（注）
純粋な IPv6 モードを構成する場合は、代わりに上記の例の IPv6 を入力します。

e) 入力した譲歩をレビューし、確認します。

入力した情報を変更するかどうかを尋ねられます。すべてのフィールドが正しい場合は、 大文字の `N` を入力して続行します。入力した情報を変更する場合は、`y` を入力して基本設定スクリプトを再起動します。

```
Please review the config
Management network:
  Gateway: 192.168.9.1
  IP Address/Mask: 192.168.9.172/24
```

```
Re-enter config? (y/N): N
```

ステップ 2 プロセスが完了するまで待ちます。

最初のノードの管理ネットワーク情報を入力して確認すると、初期セットアップでネットワーキングが設定され、UI が表示されることが分かります。この UI を使用して、他の 2 つのノードを追加して設定し、クラスタの導入を完了します。

```
Please wait for system to boot: [#########################] 100%
System up, please wait for UI to be online.

System UI online, please login to https://192.168.9.172 to continue.
```

ステップ 3 ブラウザを開き、`https://<node-mgmt-ip>` に移動して、GUI を開きます。

残りの設定ワークフローは、ノードの GUI の 1 つから実行します。展開したノードのいずれか 1 つを選択して、ブートストラッププロセスを開始できます。他の 2 つのノードにログインしたり、これらを直接構成したりする必要はありません。

前の手順で入力したパスワードを入力し、**[ログイン（Login）]** をクリックします。

ステップ 4 **[クラスタのブリングアップ（Cluster Bringup）**] ウィザードの **[基本情報（Basic Information）]** ページに、必要な情報を入力します。

a) **[クラスタ名（Cluster Name）]** には、Nexus Dashboard クラスタの名前を入力します。

クラスタ名は、 RFC-1123 の要件に従う必要があります。

b) **[Nexus Dashboard の実装タイプの選択（Nexus Dashboard Implementation type）]**で、**LAN]** または **[SAN]** を選択して、 **[次へ（Next）]**をクリックします。

ステップ 5 **[クラスタのブリングアップ（Cluster Bringup）**] ウィザードの **[構成（Configuration）]** ページで、必要な情報を入力します。

a) （任意） クラスタの IPv6 機能を有効にする場合は、**[IPv6 を有効にする（Enable IPv6）]** チェックボックスをオンにします。

b) をクリックして、1 つ以上の DNS サーバーを追加し、DNS プロバイダーの IP アドレスを入力し、チェックマーク アイコンをクリックします。

c) （任意） **[+ DNS 検索ドメインの追加]**をクリックして、検索ドメインを追加し、DNS 検索ドメインの IP アドレスを入力し、チェックマーク アイコンをクリックします。

d) （任意） NTP サーバー認証を有効にする場合は、**[NTP 認証]** チェックボックスをオンにします。

e) NTP 認証を有効にした場合、**+ Add Key** をクリックし、必要な情報を入力し、チェックマーク アイコンをクリックして情報を保存します。

- **キー**：NTP 認証キーを入力します。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です。次の手順で NTP サーバーを定義します。複数の NTP サーバーで同じ NTP 認証キーを使用できます。
- **ID**： NTP ホストのキー ID を入力します。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**：NTPキーの認証タイプを選択します。

- このキーを信頼したい場合には、**[信頼済み（Trusted）]** チェックボックスをオンにします。信頼できないキーは NTP 認証に使用できません。

NTP認証の要件とガイドラインの完全なリストについては、全般的な前提条件とガイドライン（11 ページ） を参照してください。

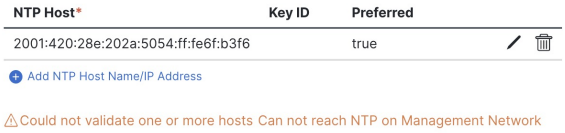
追加のNTPキーを入力する場合は、 **[+ キーの追加（+ Add Key）]** を再度クリックして、情報を入力します。

f) NTP認証を有効にした場合は、 **[+ NTP ホスト名/ IPアドレスの追加（+Add NTP Host Name/ IP Address）]**をクリックし、必要な情報を入力し、チェックマークアイコンをクリックして情報を保存します。

- **NTP ホスト**：IPアドレスを入力する必要があります。完全修飾ドメイン名（FQDN）はサポートされていません。
- **キー ID**：前のサブステップで定義した NTP キーのキー ID を入力します。

  NTP 認証が無効になっている場合、このフィールドはグレー表示されます。
- このホストを優先したい場合は、**[優先（Preferred）]** チェックボックスをオンにします。

（注）
ログインしているノードに IPv4 アドレスのみが設定されているが、前の手順で **[IPv6 を有効にする（Enable IPv6）]** をオンにして NTP サーバーの IPv6 アドレスを指定した場合は、次の検証エラーが表示されます。



これは、ノードに IPv6 アドレスがまだなく、NTP サーバーの IPv6 アドレスに接続できないためです。次の手順で IPv6 アドレスを入力します。この場合、次の手順の説明に従って他の必要な情報の入力を完了し、**[次へ（Next）]** をクリックして次の画面に進み、ノードの IPv6 アドレスを入力します。

追加の NTP サーバーを入力する場合は、 **[+ Add NTP Host Name/IP Address）]** を再度クリックし、情報を入力します。

g) **[プロキシ サーバー（Proxy Server）]** について、プロキシ サーバーの URL または IP アドレスを入力します。

Cisco Cloud に直接接続できないクラスタの場合は、接続を確立するためにプロキシ サーバを構成することをお勧めします。これにより、ファブリック内の非適合ハードウェアおよびソフトウェアにさらされるリスクを軽減できます。

+Add Ignore Host をクリックして、トラフィックがプロキシの使用をスキップする 1 つ以上の接続先 IP アドレスを入力します。

プロキシ サーバーでは、次の URL が有効になっている必要があります：

```
dcappcenter.cisco.com
svc.intersight.com
svc.ucs-connect.com
svc-static1.intersight.com
svc-static1.ucs-connect.com
```

プロキシを構成しない場合は、**[プロキシをスキップ（Skip Proxy）]**をクリックして、**[確認（Confirm）]** をクリックします。

h) （任意）プロキシサーバーで認証が必要な場合は、**[プロキシに必要な認証（Authentication required for Proxy）]** をオンにして、ログイン資格情報を指定します。

i) （任意） **[詳細設定（Advanced Settings）]** カテゴリを展開し、必要に応じて設定を変更します。

詳細設定では、次の設定を行うことができます。

- **アプリ ネットワーク**：Nexus Dashboard でアプリケーションで使用されるアドレス空間です。ターゲット ネットワークの IP アドレスとネットマスクを入力します。
- **サービス ネットワーク**：Nexus Dashboard とそのプロセスで使用される内部ネットワークです。ターゲット ネットワークの IP アドレスとネットマスクを入力します。
- **[アプリ ネットワーク IPv6（App Network IPv6）]**：先ほど **[IPv6 の有効化（Enable IPv6）]** チェックボックスをオンにした場合は、アプリ ネットワークの IPv6 サブネットを入力します。
- **[サービス ネットワーク IPv6（Service Network IPv6）]**：先ほど **[IPv6 を有効にする（Enable IPv6）]** チェックボックスをオンにした場合は、サービス ネットワークの IPv6 サブネットを入力します。

アプリケーションおよびサービス ネットワークの詳細については、全般的な前提条件とガイドライン （11 ページ） を参照してください。

j) [次へ（Next）] をクリックします。

ステップ 6 **[ノードの詳細（Node Details）]** ページで、最初のノードの情報を更新します。

前の手順の初期ノード構成時に現在ログインしているノードの管理ネットワークと IP アドレスを定義しましたが、他のプライマリノードを追加し、クラスタを作成する進む前に、ノードのデータ ネットワーク情報も指定する必要があります。

a) **クラスタ接続** について、クラスタが L3 HAモードで展開されている場合は、**BGP** を選択します。それ以外の場合は、 **L2**を選択します。

テレメトリで使用される永続的な IP アドレス機能には、BGP 構成が必要です。この機能については、BGP 構成と永続的な IP アドレス （59 ページ） と『*Cisco Nexus Dashboard* ユーザーガイド』の「永続的な IP アドレス」セクションで詳しく説明されています。

（注）
BGP をこの時点で、またはクラスタの展開後に Nexus ダッシュボード GUI で有効にすることができます。BGP が構成されている場合は、残りのすべてのノードで BGP を構成する必要があります。ノードのデータネットワークに異なるサブネットがある場合は、ここで BGP を有効にする必要があります。

b) 最初のノードの横にある **[編集（Edit）]**ボタンをクリックします。

ノードの**[シリアル番号（Serial Number）]**、**[管理ネットワーク（Management Network）]**情報、および**[タイプ（Type）]**が自動的に入力されます。ただし、他の情報は入力する必要があります。

c) **[名前（Name）]**に、サービス ノードのノード名を入力します。

ノードの **名前** はホスト名として設定されるため、 RFC-1123 の要件に従う必要があります。

（注）
[名前（Name）]フィールドが編集できない場合には、CIMC の検証を再度実行して、この問題を修正してください。

d) **[タイプ（Type）]**で、 **[プライマリ（Primary）]**を選択します。

クラスタの最初のノードは **[プライマリ（Primary）]** に設定する必要があります。より大規模なスケールを有効にする必要がある場合は、後の手順でセカンダリ ノードを追加します。

e) **[データ ネットワーク（Data Network）]** エリアで、ノードのデータ ネットワークを入力します。

データ ネットワークの IP アドレス、ネットマスク、およびゲートウェイを入力します。オプションで、ネットワークの VLAN ID を指定することもできます。構成に VLAN が不要な場合は、 [VLAN ID] フィールドを空白のままにします。 **データ接続** に **BGP** を選択した場合は、 ASNを入力します。

前のページで IPv6 機能を有効にした場合は、IPv6 アドレス、ネットマスク、およびゲートウェイも入力する必要があります。

（注）
IPv6 情報を提供する場合は、クラスタ ブートストラップ プロセス中に行う必要があります。後で IP アドレス構成を変更するには、クラスタを再展開する必要があります。

クラスタ内のすべてのノードは、 IPv4 のみ、IPv6 のみ、またはデュアル スタック IPv4/IPv6 のいずれかで構成する必要があります。

f) **クラスタ接続** に **BGP** を選択した場合は、 **[BGP ピアの詳細（BGP peer details）]** 領域で、ピアの IPv4 アドレスとASNを入力します。

[+ IPv4 BGP ピアの追加（+ Add IPv4 BGP peer）] をクリックして、ピアを追加できます。

前のページで IPv6 機能を有効にした場合は、ピアの IPv6 アドレスと ASN も入力する必要があります。

g) **[Save]**をクリックして、変更内容を保存します。

ステップ 7 複数ノード クラスタを展開している場合、**[ノードの詳細（Node Details）]** 画面で、**[ノードの追加（Add Node）]** をクリックして、クラスタに 2 番目のノードを追加します。

a) **[展開の詳細（Deployment Details）]** エリアで、2 番目のノードに **[CIMC IP アドレス（CIMC IP Address）]**、**[ユーザー名（Username）]**、**[パスワード（Password）]** を入力します。

（注）
2 番目のノードの**ユーザー名**に対して、管理者ユーザーの ID を入力します。

b) **[検証（Validate）]** をクリックして、ノードへの接続を確認します。

CIMC 接続が検証されると、ノードの [シリアル番号（Serial Number）] が自動的に入力されます。

c) **[名前]**に、ノードの名前を入力します。

ノードの 名前はホスト名として設定されるため、 RFC-1123 の要件に従う必要があります。

d) **[タイプ（Type）]**で、 [プライマリ（Primary）]を選択します。

クラスタの最初の 3 つのノードは [プライマリ（ Primary）] に設定する必要があります。より大規模なスケールを有効にする必要がある場合は、後の手順でセカンダリ ノードを追加します。

e) **[管理ネットワーク（Management Network）]** エリアで、ノードの管理ネットワークの情報を入力します。

管理ネットワークの IP アドレス、ネットマスク、ゲートウェイを指定する必要があります。

前のページで IPv6 機能を有効にした場合は、IPv6 アドレス、ネットマスク、およびゲートウェイも入力する必要があります。

（注）
クラスタ内のすべてのノードは、 IPv4 のみ、IPv6 のみ、またはデュアル スタック IPv4/IPv6 のいずれかで構成する必要があります。

f) **[データ ネットワーク（Data Network）]** エリアで、ノードのデータ ネットワークを入力します。

データ ネットワークの IP アドレス、ネットマスク、およびゲートウェイを入力します。オプションで、ネットワークの VLAN ID を指定することもできます。構成に VLAN が不要な場合は、 [VLAN ID] フィールドを空白のままにします。 **データ接続** に **BGP** を選択した場合は、 ASNを入力します。

前のページで IPv6 機能を有効にした場合は、IPv6 アドレス、ネットマスク、およびゲートウェイも入力する必要があります。

（注）
IPv6 情報を提供する場合は、クラスタ ブートストラップ プロセス中に行う必要があります。後で IP アドレス構成を変更するには、クラスタを再展開する必要があります。

クラスタ内のすべてのノードは、 IPv4 のみ、IPv6 のみ、またはデュアル スタック IPv4/IPv6 のいずれかで構成する必要があります。

g) **クラスタ接続** に **BGP** を選択した場合は、 **[BGP ピアの詳細（BGP peer details）]** 領域で、ピアの IPv4 アドレスとASNを入力します。

[+ IPv4 BGP ピアの追加（+ Add IPv4 BGP peer）] をクリックして、ピアを追加できます。

前のページで IPv6 機能を有効にした場合は、ピアの IPv6 アドレスと ASN も入力する必要があります。

h) **[Save]**をクリックして、変更内容を保存します。

i) クラスタの最後の（3 番目の）プライマリ ノードでこの手順を繰り返します。

ステップ 8 （任意） 前の手順を繰り返して、追加のセカンダリ ノードまたはスタンバイ ノードに関する情報を入力します。

（注）

より高いスケールをサポートするには、展開時に十分な数のセカンダリ ノードを提供する必要があります。特定のユースケースに必要な追加のセカンダリノードの詳しい数については、Nexus Dashboard クラスタ サイジング ツールを参照してください

スタンバイ ノードを今すぐ追加するか、クラスタの展開後に追加するかを選択できます。

ステップ 9 **[ノードの詳細（Node Details）]** ページで、入力した情報を確認してから、**[次へ（Next）]**をクリックします。

ステップ 10 永続的なIPアドレスをさらに追加する場合は、**[永続的な IP（Persistent IPs）]** ページで、**[+ データ サービスの IP アドレスの追加（+ Add Data Service IP Address）]**をクリックし、 IPアドレスを入力して、チェックマークアイコン（）をクリックします。必要な回数だけこのステップを繰り返し、**[次へ（Next）]** をクリックします。

ブートストラッププロセス中に、必要な永続IPアドレスの最小数を設定する必要があります。この手順により、必要に応じて永続的な IP アドレスを追加できます。

ステップ 11 **[概要（Summary）]** ページで設定情報をレビューして確認し、**[保存（Save）]** をクリックし、**[続行（Continue）]** をクリックして正しい展開モードを確認し、クラスタの構築を続行します。

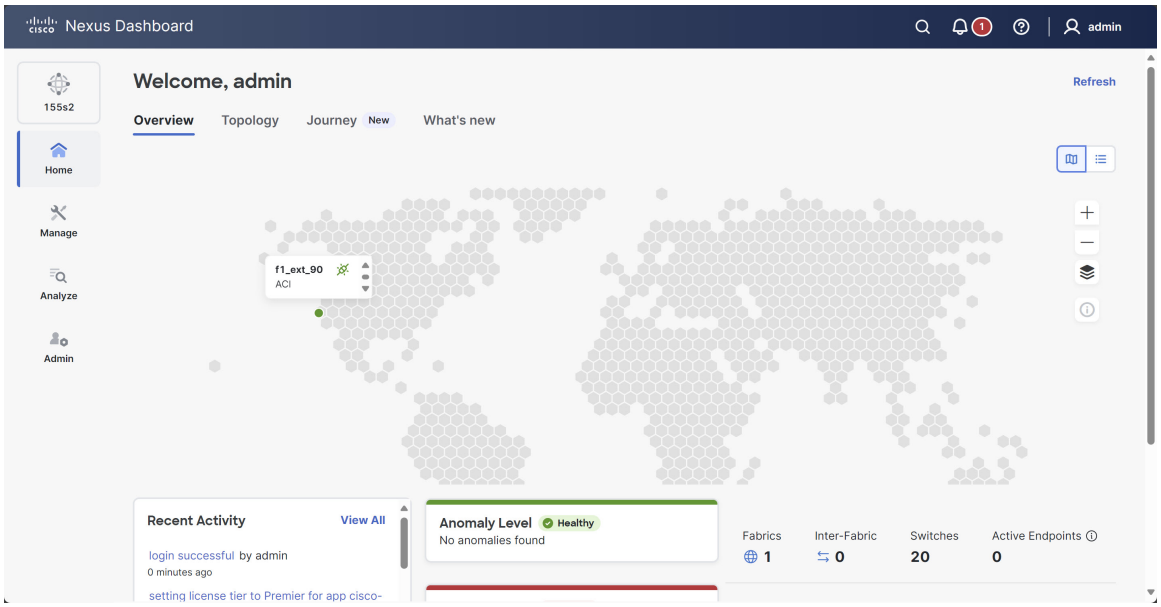
ノードのブート ストラップとクラスタの起動中に、全体的な進捗状況と各ノードの個々の進捗状況がUIに表示されます。ブートストラップの進行状況が表示されない場合は、ブラウザでページを手動で更新し、ステータスを更新してください。

クラスターが形成され、クラスター内のノードの数と起動するすべての機能に応じて、クラスタが形成されるまでに最大 60 分以上かかる場合があります。クラスタの設定が完了すると、ページが Nexus ダッシュボード GUI にリロードされます。

ステップ 12 クラスタが健全であることを検証します。

クラスタが使用可能になったら、ノードの管理 IP アドレスのいずれかを参照してアクセスできます。`admin` ユーザーのデフォルト パスワードは、最初のノードに選択した `rescue-user` のパスワードと同じです。この間、UI は上部に「サービスのインストールが進行中です。Nexus Dashboard の設定タスクは現在無効になっています」という意味のバナーを表示します。

すべてのクラスタが展開され、すべてのサービスが開始されたら **[ホーム（Home）]** > **[概要（Overview）]** ページの **異常レベル（Anomaly Level）** でクラスタが正常であることを確認できます。



または、SSH を使用し、`rescue-user` として、ノード展開中に入力したパスワードを使っていずれかのノードにログインし、`acs health` コマンドを実行してクラスタの状態を確認できます。

- クラスタが収束している間、次の出力が表示されることがあります：

```
$ acs health
k8s install is in-progress
```

```
$ acs health
k8s services not in desired state - [...]
```

```
$ acs health
k8s: Etcd cluster is not ready
```

- クラスタが稼働している場合は、次の出力が表示されます。

```
$ acs health
All components are healthy
```

（注）
場合によっては、ノードの電源を再投入（電源をオフにしてから再度オン）すると、この段階でスタックが停止することがある可能性があります。

```
deploy base system services
```

これは、pND（物理 Nexus Dashboard）クラスタの再起動後のノードの `etcd` の問題が原因です。

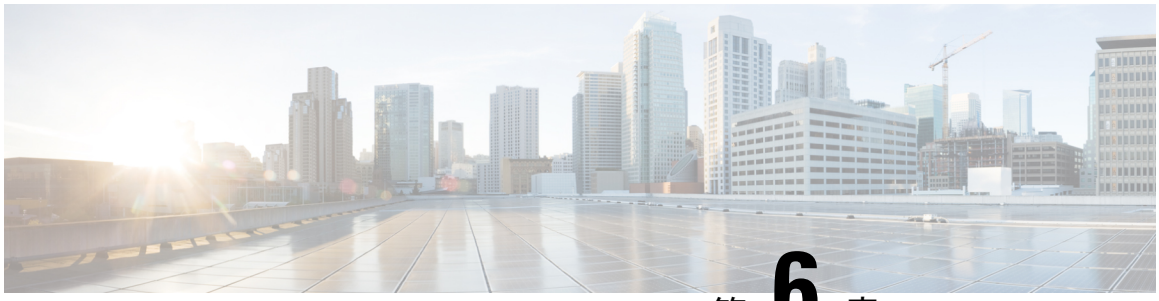
この問題を解決するには、影響を受けるノードで `acs reboot clean` コマンドを入力します。

ステップ 13 （オプション） Cisco Nexus Dashboardクラスター をCisco Intersightに接続、可視性と利点を強化します。詳細な手順については、 「*Cisco Intersightの操作*」 を参照してください。

ステップ 14 Nexus Dashboardを展開した後、設定情報については、このリリースのコレクションページを参照してください。

次のタスク

次のタスクは、ファブリックとファブリック グループを作成することです。 Cisco Nexus Dashboardのコレクション ページ にある、このリリースの 「ファブリックとファブリック グループの作成」の記事を参照してください。



第 6 章

VMware ESX の展開

VMware ESX で Nexus Dashboard クラスタを展開するための前提条件と注意事項

VMware ESX で Nexus ダッシュボード クラスタを展開する前に、次の手順を実行する必要があります。

- ファクターから ESX が拡張性要件をサポートしていることを確認します。

  スケールとサービスのサポートと共同ホスティングは、展開するクラスタのフォーム ファクターと、展開する予定の特定のサービスによって異なります。Nexus ダッシュボード キャパシティ プランニング ツールを使用して、仮想フォーム ファクタが展開要件を満たすことを確認できます。

（注） 一部の展開は、1 つ以上の特定のユース ケースに対して単一の ESX 仮想ノードのみを必要とする場合があります。その場合、キャパシティ プランニング ツールで要件が示されるので、次のセクションの追加のノード展開手順をスキップできます。

- 前提条件とガイドライン （11 ページ） に記載されている一般的な前提条件を確認して完了します。

  この文書は、ベースとなる Nexus Dashboard クラスタを最初に展開する方法について説明します。追加ノード（セカンダリまたはスタンバイなど）で既存のクラスタを拡張する場合は、代わりに*Cisco Nexus* ダッシュボード ユーザー ガイドの「インフラストラクチャの管理」の章を参照してください。これは、Nexus ダッシュボード UI またはオンラインで*Cisco Nexus* ダッシュボード ユーザー ガイドから利用できます。

- Nexus ダッシュボード VM に使用される CPU ファミリが AVX 命令セットをサポートしていることを確認します。
- ディスクの I/O 遅延は 20 ミリ秒以下である必要があります。
- 展開するノードのタイプを選択します：
  - データ ノード：追加のリソースを必要とする 特定のNexus Dashboard 機能向けに設計された、より高いシステム要件を持つノード プロファイル。
  - アプリ ノード：ほとんどの Nexus Dashboard 機能向けに使用できる、リソース フットプリントが小さいノード プロファイル。

（注） 一部の大規模な展開では、追加のセカンダリ ノードが必要になる場合があります。Nexus Dashboard クラスタにセカンダリ ノードを追加する予定の場合には、OVA-App プロファイルを使用してすべてのノード（最初の 3 ノードのクラスタと追加のセカンダリ ノード）を展開できます。詳細なスケール情報は、使用しているリリースの *Cisco Nexus Dashboard* 検証済みスケーラビリティ ガイドで入手できます。

十分なシステム リソースをもつことを確認します。

表 *13* : 展開要件

データ ノードの要件	アプリケーション ノードの要件

• VMware ESXi 7.0、7.0.1、7.0.2、7.0.3、8.0、8.0.2、8.0.3
• VMware vCenter を使用して展開する場合、VMware vCenter 7.0.1、7.0.2、7.0.3、8.0、8.0.2、8.0.3
• 各ノード/VM には、次のものが必要です。
  • 少なくとも 35,200 MHz の物理的に CPU 予約された 32 個の vCPU
  • 物理予約された 128GB の RAM
  • データ ボリューム用の 3TB SSD ストレージとシステム ボリューム用の追加の 50GB
  データノードは、次の最小パフォーマンス要件を満たすストレージに展開する必要があります。
  • SSD は、データストアに直接接続するか、RAID ホストバス アダプタ（HBA）を使用している場合は JBOD モードで接続する必要があります。
  • SSD は、混合使用/アプリケーション用に最適化する必要があります（読み取り最適化ではありません）。
  • 4K ランダム読み取り IOPS：93000
  • 4K ランダム書き込み IOPS：31000
• 各 Nexus ダッシュボードノードは、異なる ESXi サーバに展開することを推奨します。
	• VMware ESXi 7.0、7.0.1、7.0.2、7.0.3、8.0、8.0.2、8.0.3
	• VMware vCenter を使用して展開する場合、VMware vCenter 7.0.1、7.0.2、7.0.3、8.0、8.0.2、8.0.3
	• 各ノード/VM には、次のものが必要です。
	  • 少なくとも 17,600 MHz の物理的 CPU で予約された 16 個の vCPU
	  • 物理予約された 64GB の RAM
	  • データ ボリューム用に 500GB HDD または SSD ストレージ、システム ボリューム用に追加の 50GB
	  一部の機能では、アプリ ノードをより高速な SSD ストレージに展開する必要がありますが、他の機能では HDD をサポートしています。Nexus ダッシュボード キャパシティ プランニング ツールをチェックして、正しいタイプのストレージを使用していることを確認してください。
	• 各 Nexus ダッシュボードノードは、異なる ESXi サーバに展開することを推奨します。

- クラスタ ノードのデータ インターフェイスの VLAN ID を構成する場合は、仮想ゲスト VLAN タギング（VGT）モードの VMware vCenter のデータ インターフェイス ポート グ

ループで VLAN 4095 を有効にする必要があります。Nexus Dashboard データ インターフェイスの VLAN ID を指定する場合、パケットはその VLAN ID を持つ Dot1q タグを伝送する必要があります。vSwitch のポート グループに明示的な VLAN タグを設定し、Nexus Dashboard VM の VNIC にアタッチすると、vSwitch は、パケットをその VNIC に送信する前に、アップリンクからのパケットから Dot1q タグを削除します。仮想 Nexus Dashboard ノードは Dot1q タグを想定しているため、すべての VLAN を許可するには、データ インターフェイス ポート グループで VLAN 4095 を有効にする必要があります。

- 各ノードの VM を展開したら、次のセクションの展開手順で説明されているように、VMware ツールの定期的な時刻同期が無効になっていることを確認します。
- VMware vMotion は Nexus ダッシュボード クラスタ ノードではサポートされていません。
- VMware 分散リソース スケジューラ (DRS) は、Nexus ダッシュボード クラスタ ノードではサポートされていません。

  ESXi クラスタ レベルで DRS を有効にしている場合は、次のセクションで説明するように、展開時に Nexus ダッシュボード VM に対して明示的に無効にする必要があります。
- コンテンツ ライブラリによる展開はサポートされていません。
- VMwareスナップショットは、次の条件下で、リモート対応Nexus Dashboard VMsでサポートされます。
  - スナップショットは、VMsの電源がオフになっている間に作成する必要があります。VMsの電源がオンになっている間のスナップショットの作成はサポートされていません。
  - 同じクラスタの一部であるすべてのVMsのスナップショットは、まとめて作成する必要があります。
  - 以前のスナップショットにロールバックする場合、同じクラスターに属するすべてのVMs を同時にロールバックする必要があります。
- Cisco は、ネストされた仮想化環境の使用をサポートしていません。仮想化ハイパーバイザ（例：ESXi上のKVM）上で動作している仮想マシンにNexus Dashboardを展開することは、サポート対象外の構成であり、パフォーマンスの低下やシステムの不安定化を招く可能性があります。
- ノードを ESXi に直接展開するか、VMware vCenter を使用して展開するかを選択できます。

  VMware vCenter を使用して展開する場合は、VMware vCenter を使用した Nexus ダッシュボードの展開 （97 ページ） で説明されている手順に従います。

  ESXi に直接展開する場合は、VMware ESXi での Nexus ダッシュボードの展開 （112 ページ） で説明されている手順に従います。

VMware vCenter を使用した Nexus ダッシュボードの展開

ここでは、VMware vCenter を使用して Cisco Nexus ダッシュボード クラスタを展開する方法について説明します。ESXi に直接展開する場合は、代わりに VMware ESXi での Nexus ダッシュボードの展開 （112 ページ） で説明されている手順に従ってください。

始める前に

- VMware ESX で Nexus Dashboard クラスタを展開するための前提条件と注意事項 （93 ページ） に記載されている要件とガイドラインを満たしていることを確認します。

手順

ステップ 1 Cisco Nexus Dashboard OVAイメージを取得します。

a) [ソフトウェア ダウンロード（Software Download）] ページを参照します。

https://software.cisco.com/download/home/286327743/type/286328258/

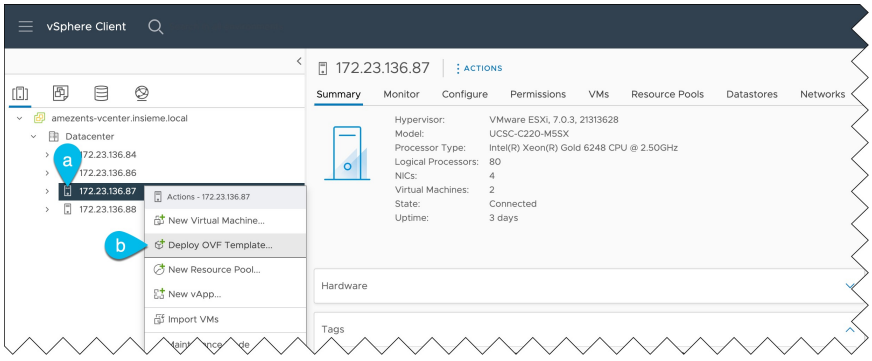
b) 左側のサイドバーから、ダウンロードする Nexus ダッシュボードのリリースバージョンを選択します。

c) Nexus ダッシュボード OVA イメージの横にある**ダウンロード**をクリックします（`nd-dk9.<version>.ova`）。

ステップ 2 VMware vCenter にログインします。

vSphereクライアントのバージョンによっては、設定画面の場所と順序が若干異なる場合があります。次の手順では、VMware vSphere Client 7.0を使用した導入の詳細を示します。

ステップ 3 新しい VM 展開を開始します。

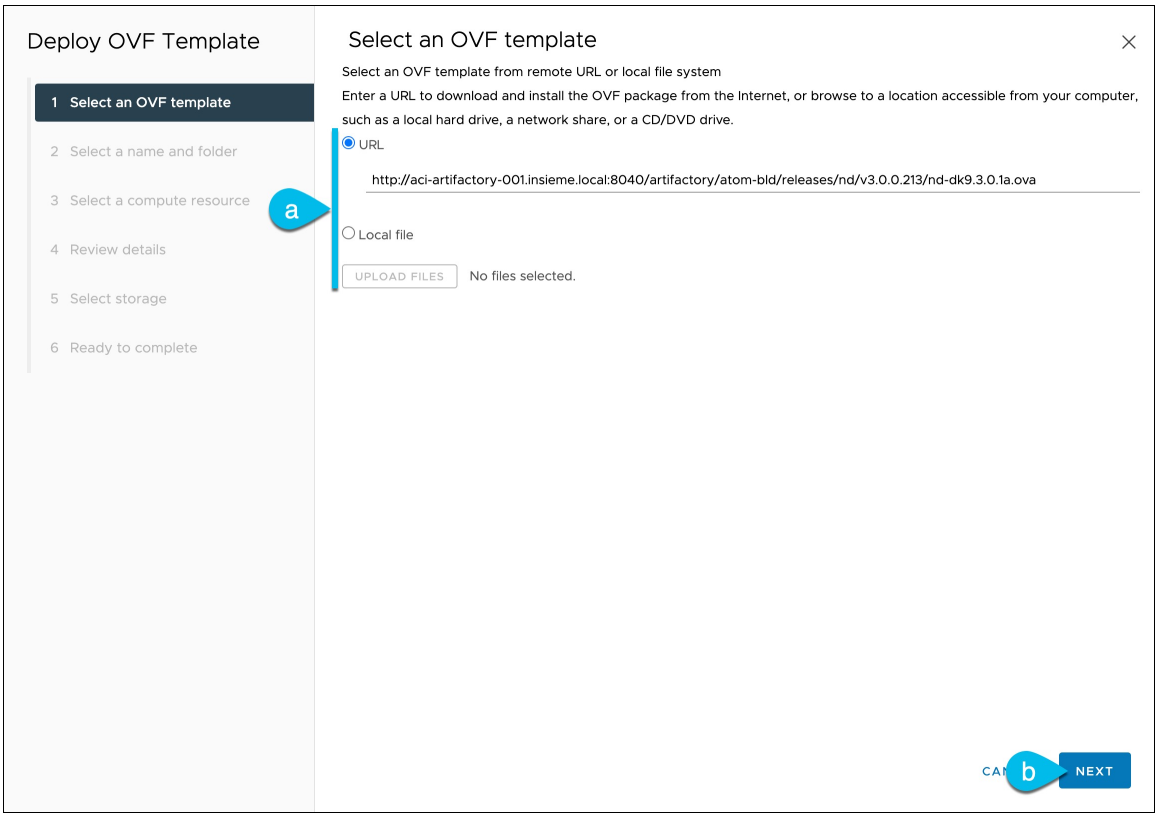


a) VM を展開する ESX ホストを右クリックします。

b) **[OVFテンプレートの展開（Deploy OVF Template）]** を選択します。

[Deploy OVF Template] ウィザードが表示されます。

ステップ 4 **[OVF テンプレートの選択（Select an OVF template）]** 画面で、OVAイメージを指定します。



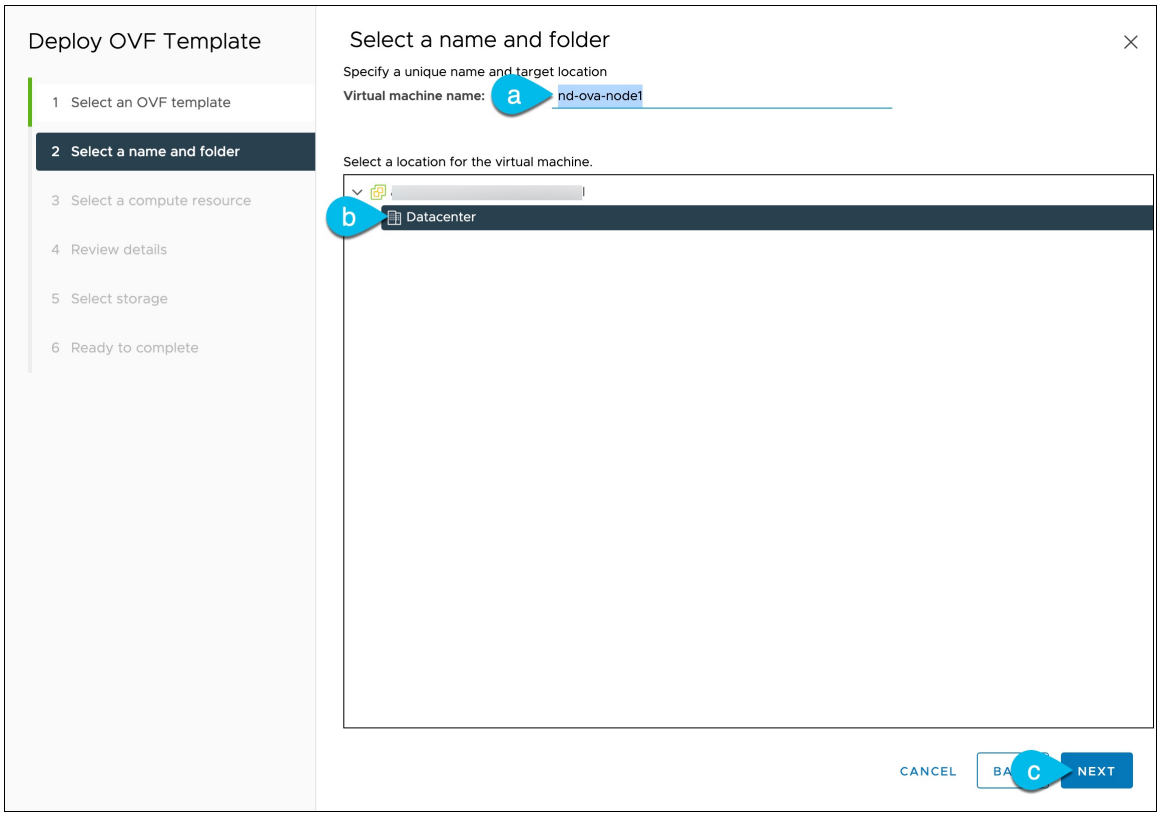
a) イメージの場所を指定します。

環境内の Web サーバでイメージをホストしている場合は、**[URL]** を選択し、イメージの URL を指定します。

イメージがローカルの場合は、**[ローカル ファイル（Local file）]** を選択し、**[ファイルの選択（Choose Files）]** をクリックしてダウンロードしたOVAファイルを選択します。

b) **[次へ（Next）]** をクリックして続行します。

ステップ 5 **[名前とフォルダの選択（Select a name and folder）]** 画面で、VM の名前と場所を入力します。



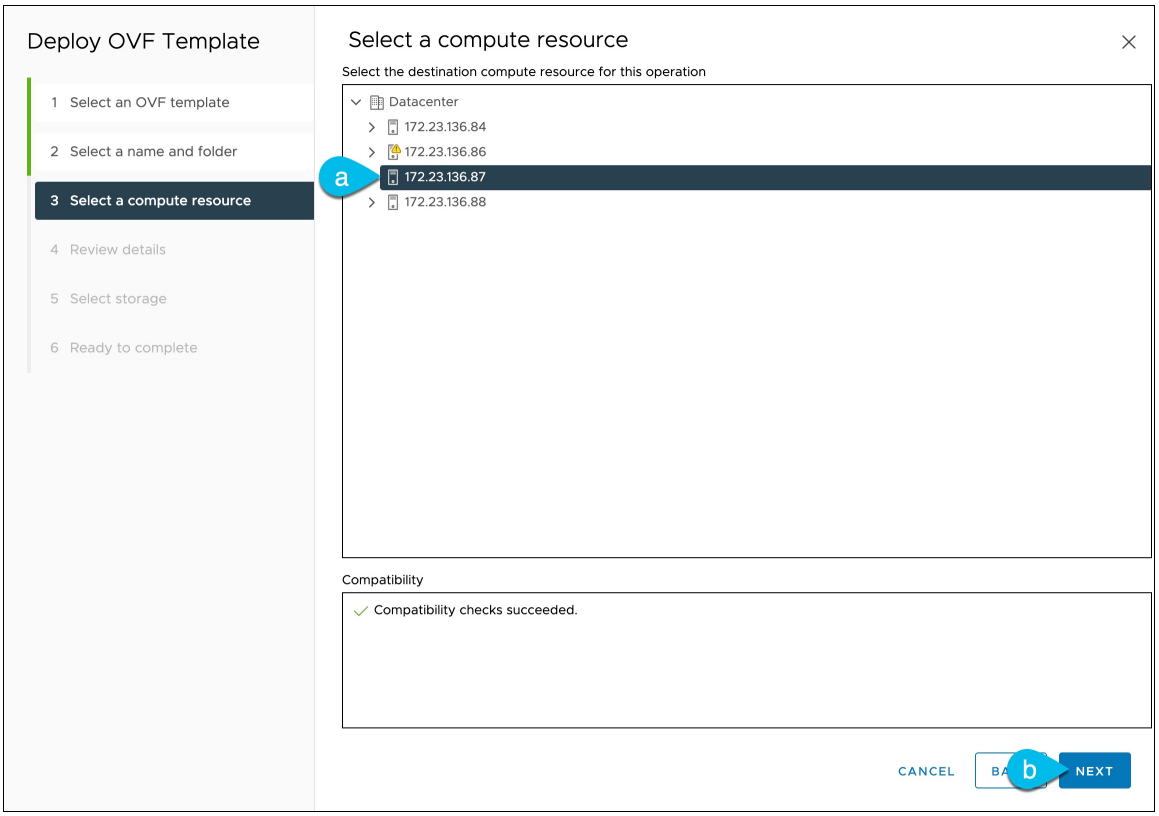
a) 仮想マシンの名前を入力します。

たとえば、`nd-ova-node1` です。

b) 仮想マシンのストレージ場所を選択します。

c) **[次へ（Next）]** をクリックして、続行します。

ステップ 6 **[コンピューティング リソースの選択（Select a compute resource）]** 画面で、ESX ホストを選択します。

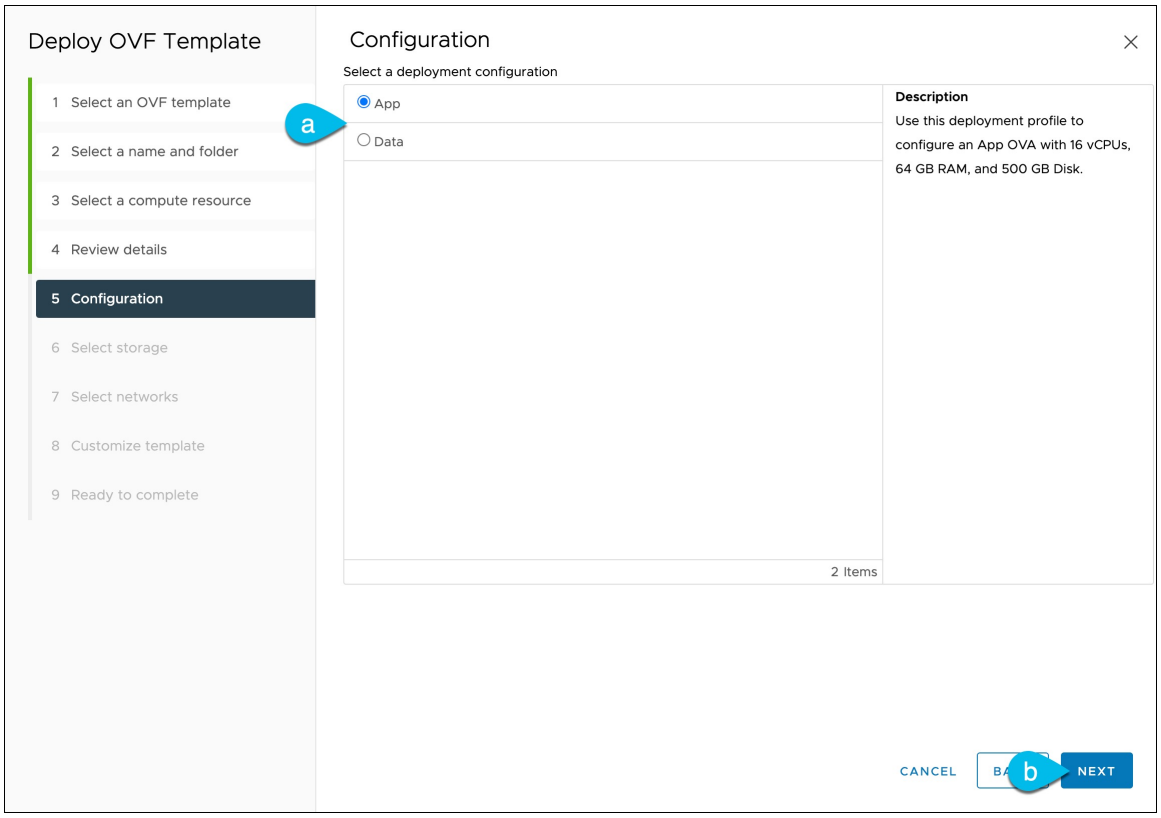


a) 仮想マシンの vCenter データセンターと ESX ホストを選択します。

b) **[次へ（Next）]** をクリックして、続行します。

ステップ 7 **[詳細の確認（Review details）]** 画面で、**[次へ（Next）]** をクリックして続行します。

ステップ 8 [設定] 画面で、展開するノードプロファイルを選択します。

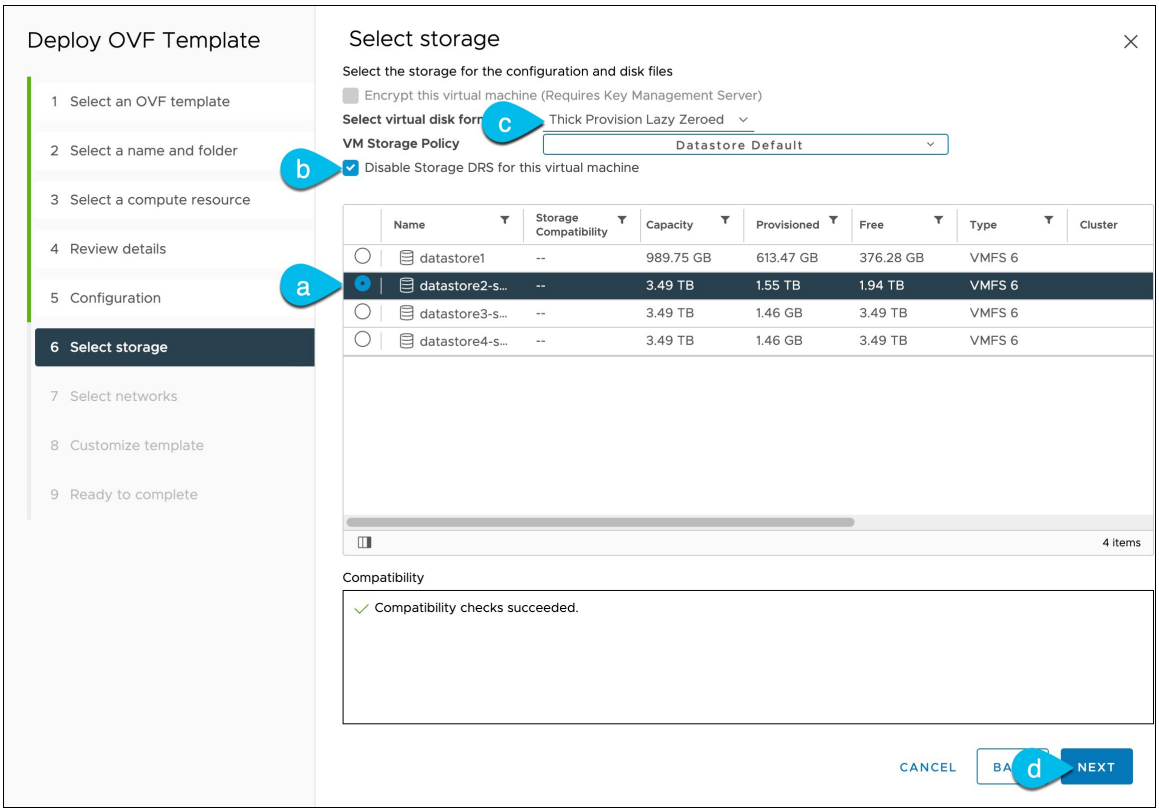


a) ユースケースの要件に基づいて、アプリまたはデータ ノード プロファイルを選択します。

ノードプロファイルの詳細については、「VMware ESX で Nexus Dashboard クラスタを展開するための前提条件と注意事項 （93 ページ）」を参照してください。

b) **[次へ（Next）]** をクリックして、続行します。

ステップ 9 **[ストレージの選択（Select storage）]** 画面で、ストレージ情報を入力します。



a) 仮想マシンのデータストアを選択します。

ノードごとに一意のデータストアを推奨します。

b) **[この仮想マシンのストレージ DRS を無効にする（Disable Storage DRS for this virtual machine）]** チェックボックスをオンにします。

Nexus DashboardはVMware DRSをサポートしていません。

c) **[仮想ディスク フォーマットの選択（Select virtual disk format）]** ドロップダウン リストから [シック プロビジョニング Lazy Zeroed（Thick Provisioning Lazy Zeroed）] を選択します。

d) **[次へ（Next）]** をクリックして、続行します。

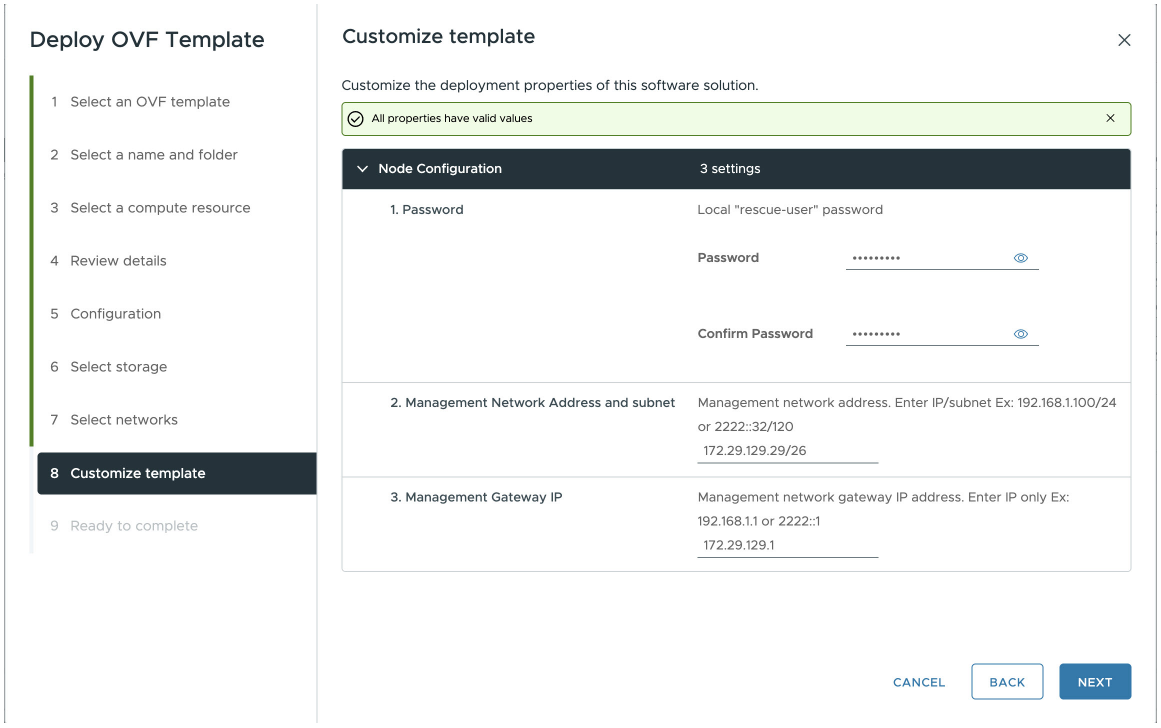
ステップ 10 [**ネットワークの選択**]画面で、Nexusダッシュボードの管理およびデータネットワークのVMネットワークを選択し、[**次へ**] をクリックして続行します。

Nexus Dashboard クラスターには、高可用性向けに構成されたポートを持つ、以下の 2 つのネットワークが必要です：

- **データ ネットワーク**：結合されたポート **fabric0/fabric1** は、 Nexus Dashboard クラスタのデータネットワークに使用されます。
- **管理ネットワーク**：結合されたポート **mgmt0/mgmt1** は、 Nexus Dashboard クラスタの管理ネットワークに使用されます。

これらのネットワークの詳細については、「展開の概要と要件」の章の「全般的な前提条件とガイドライン （11 ページ）」を参照してください。

ステップ 11 **[テンプレートのカスタマイズ（Customize template）]** 画面で、必要な情報を入力します。



a) [アプリ/データ] タイプを選択します。

b) **パスワード**を入力して確認します。

このパスワードは、各ノードの `rescue-user` アカウントに使用されます。

（注）
すべてのノードに同じパスワードを指定する必要があります。同じパスワードを指定しないと、クラスタの作成に失敗します。

c) **管理ネットワーク**の IP アドレスとネットマスクを入力します。

d) **管理ネットワーク**の IP ゲートウェイを入力します。

e) [次へ（Next）] をクリックして次に進みます。

ステップ 12 **[完了準備（Ready to complete）]** 画面で、すべての情報が正しいことを確認し、**[終了（Finish）]** をクリックして最初のノードの展開を開始します。

ステップ 13 以前のステップを繰り返し、追加のノードを展開します。

（注）
単一のノードクラスタを展開している場合は、この手順をスキップできます。

マルチノードク ラスタの場合は、2 つの追加のプライマリ ノードと、特定のユースケースで必要なだけのセカンダリ ノードを展開する必要があります。必要なノードの総数は、 Nexus Dashboard キャパシティ プランニング ツールで確認できます。

最初のノードの VM 展開が完了するのを待つ必要はありません。他の 2 つのノードの展開を同時に開始できます。2 番目と 3 番目のノードを展開する手順は、最初のノードの場合と同じです。

ステップ 14 VM の展開が完了するまで待ちます。

ステップ 15 VMware ツールの定期的な時刻同期が無効になっていることを確認してから、VM を起動します。

時刻の同期を無効にするには、次の手順を実行します。

a) VM を右クリックして、**[設定の編集（Edit Settings）]** を選択します。
b) **[設定の編集（Edit Settings）]** ウィンドウで、**[VMオプション（VM Options）]** タブを選択します。
c) **[VMware ツール（VMware Tools）]** カテゴリを展開し、**[定期的な時刻の同期（Synchronize time periodically）]** オプションのチェックボックスをオフにします。

ステップ 16 ブラウザを開き、`https://<node-mgmt-ip>` に移動して、GUI を開きます。

残りの設定ワークフローは、ノードの GUI の 1 つから実行します。展開したノードのいずれか 1 つを選択して、ブートストラッププロセスを開始できます。他の 2 つのノードにログインしたり、これらを直接構成したりする必要はありません。

前の手順で入力したパスワードを入力し、**[ログイン（Login）]** をクリックします。

ステップ 17 **[クラスタのブリングアップ（Cluster Bringup）**] ウィザードの **[基本情報（Basic Information）]** ページに、必要な情報を入力します。

a) **[クラスタ名（Cluster Name）]** には、Nexus Dashboard クラスタの名前を入力します。

クラスタ名は、 RFC-1123 の要件に従う必要があります。

b) **[Nexus Dashboard の実装タイプの選択（Nexus Dashboard Implementation type）]**で、**LAN]** または **[SAN]** を選択して、 **[次へ（Next）]**をクリックします。

ステップ 18 **[クラスタのブリングアップ（Cluster Bringup）**] ウィザードの **[構成（Configuration）]** ページで、必要な情報を入力します。

a) （任意）クラスタの IPv6 機能を有効にする場合は、**[IPv6 を有効にする（Enable IPv6）]** チェックボックスをオンにします。
b) をクリックして、1 つ以上の DNS サーバーを追加し、DNS プロバイダーの IP アドレスを入力し、チェックマーク アイコンをクリックします。
c) （任意） **[+ DNS 検索ドメインの追加]**をクリックして、検索ドメインを追加し、DNS 検索ドメインの IP アドレスを入力し、チェックマーク アイコンをクリックします。
d) （任意） NTP サーバー認証を有効にする場合は、**[NTP 認証]** チェックボックスをオンにします。
e) NTP 認証を有効にした場合、**+ Add Key** をクリックし、必要な情報を入力し、チェックマーク アイコンをクリックして情報を保存します。

- **キー**：NTP 認証キーを入力します。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です。次の手順で NTP サーバーを定義します。複数の NTP サーバーで同じ NTP 認証キーを使用できます。
- **ID**： NTP ホストのキー ID を入力します。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**：NTPキーの認証タイプを選択します。

- このキーを信頼したい場合には、**[信頼済み（Trusted）]** チェックボックスをオンにします。信頼できないキーは NTP 認証に使用できません。

NTP 認証の要件とガイドラインの完全なリストについては、全般的な前提条件とガイドライン（11 ページ） を参照してください。

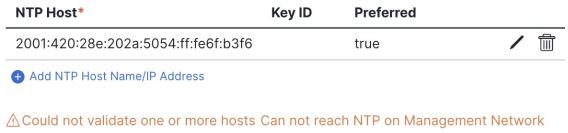
追加のNTPキーを入力する場合は、**[+ キーの追加（+ Add Key）]** を再度クリックして、情報を入力します。

f) NTP認証を有効にした場合は、**[+ NTP ホスト名/ IPアドレスの追加（+Add NTP Host Name/ IP Address）]**をクリックし、必要な情報を入力し、チェックマークアイコンをクリックして情報を保存します。

- **NTP ホスト**：IP アドレスを入力する必要があります。完全修飾ドメイン名（FQDN）はサポートされていません。
- **キー ID**：前のサブステップで定義した NTP キーのキー ID を入力します。

  NTP 認証が無効になっている場合、このフィールドはグレー表示されます。
- このホストを優先したい場合は、**[優先（Preferred）]** チェックボックスをオンにします。

（注）
ログインしているノードに IPv4 アドレスのみが設定されているが、前の手順で **[IPv6 を有効にする（Enable IPv6）]** をオンにして NTP サーバーの IPv6 アドレスを指定した場合は、次の検証エラーが表示されます。



これは、ノードに IPv6 アドレスがまだなく、NTP サーバーの IPv6 アドレスに接続できないためです。次の手順で IPv6 アドレスを入力します。この場合、次の手順の説明に従って他の必要な情報の入力を完了し、**[次へ（Next）]** をクリックして次の画面に進み、ノードの IPv6 アドレスを入力します。

追加の NTP サーバーを入力する場合は、**[+ Add NTP Host Name/IP Address）]** を再度クリックし、情報を入力します。

g) **[プロキシ サーバー（Proxy Server）]** について、プロキシ サーバーの URL または IP アドレスを入力します。

Cisco Cloud に直接接続できないクラスタの場合は、接続を確立するためにプロキシ サーバを構成することをお勧めします。これにより、ファブリック内の非適合ハードウェアおよびソフトウェアにさらされるリスクを軽減できます。

+Add Ignore Host をクリックして、トラフィックがプロキシの使用をスキップする 1 つ以上の接続先 IP アドレスを入力します。

プロキシ サーバーでは、次の URL が有効になっている必要があります：

```
dcappcenter.cisco.com
svc.intersight.com
svc.ucs-connect.com
svc-static1.intersight.com
svc-static1.ucs-connect.com
```

プロキシを構成しない場合は、**[プロキシをスキップ（Skip Proxy）]**をクリックして、**[確認（Confirm）]** をクリックします。

h) （任意）プロキシサーバーで認証が必要な場合は、**[プロキシに必要な認証（Authentication required for Proxy）]** をオンにして、ログイン資格情報を指定します。

i) （任意）**[詳細設定（Advanced Settings）]** カテゴリを展開し、必要に応じて設定を変更します。

詳細設定では、次の設定を行うことができます。

- **アプリ ネットワーク**：Nexus Dashboard でアプリケーションで使用されるアドレス空間です。ターゲット ネットワークの IP アドレスとネットマスクを入力します。
- **サービス ネットワーク**：Nexus Dashboard とそのプロセスで使用される内部ネットワークです。ターゲット ネットワークの IP アドレスとネットマスクを入力します。
- **[アプリ ネットワーク IPv6（App Network IPv6）]**：先ほど **[IPv6 の有効化（Enable IPv6）]** チェックボックスをオンにした場合は、アプリ ネットワークの IPv6 サブネットを入力します。
- **[サービス ネットワーク IPv6（Service Network IPv6）]**：先ほど **[IPv6 を有効にする（Enable IPv6）]** チェックボックスをオンにした場合は、サービス ネットワークの IPv6 サブネットを入力します。

アプリケーションおよびサービス ネットワークの詳細については、全般的な前提条件とガイドライン （11 ページ） を参照してください。

j) [次へ（Next）] をクリックします。

ステップ 19 **[ノードの詳細（Node Details）]** ページで、最初のノードの情報を更新します。

前の手順の初期ノード構成時に現在ログインしているノードの管理ネットワークと IP アドレスを定義しましたが、他のプライマリ ノードを追加し、クラスタを作成する進む前に、ノードのデータ ネットワーク情報も指定する必要があります。

a) **クラスタ接続** について、クラスタが L3 HAモードで展開されている場合は、**BGP** を選択します。それ以外の場合は、 **L2**を選択します。

テレメトリで使用される永続的な IP アドレス機能には、BGP 構成が必要です。この機能については、BGP 構成と永続的な IP アドレス （59 ページ） と『*Cisco Nexus Dashboard* ユーザーガイド』の「永続的な IP アドレス」セクションで詳しく説明されています。

（注）
BGP をこの時点で、またはクラスタの展開後に Nexus ダッシュボード GUI で有効にすることができます。BGP が構成されている場合は、残りのすべてのノードで BGP を構成する必要があります。ノードのデータネットワークに異なるサブネットがある場合は、ここで BGP を有効にする必要があります。

b) 最初のノードの横にある **[編集（Edit）]**ボタンをクリックします。

ノードの**[シリアル番号（Serial Number）]**、**[管理ネットワーク（Management Network）]**情報、および**[タイプ（Type）]**が自動的に入力されます。ただし、他の情報は入力する必要があります。

c) **[名前（Name）]**に、サービス ノードのノード名を入力します。

ノードの **名前** はホスト名として設定されるため、 RFC-1123 の要件に従う必要があります。

（注）
[名前（Name）]フィールドが編集できない場合には、CIMC の検証を再度実行して、この問題を修正してください。

d) **[タイプ（Type）]**で、**[プライマリ（Primary）]**を選択します。

クラスタの最初のノードは **[プライマリ（Primary）]** に設定する必要があります。より大規模なスケールを有効にする必要がある場合は、後の手順でセカンダリ ノードを追加します。

e) **[データ ネットワーク（Data Network）]** エリアで、ノードのデータ ネットワークを入力します。

データ ネットワークの IP アドレス、ネットマスク、およびゲートウェイを入力します。オプションで、ネットワークの VLAN ID を指定することもできます。構成に VLAN が不要な場合は、 [VLAN ID] フィールドを空白のままにします。 **データ接続** に **BGP** を選択した場合は、 ASNを入力します。

前のページで IPv6 機能を有効にした場合は、IPv6 アドレス、ネットマスク、およびゲートウェイも入力する必要があります。

（注）
IPv6 情報を提供する場合は、クラスタ ブートストラップ プロセス中に行う必要があります。後で IP アドレス構成を変更するには、クラスタを再展開する必要があります。

クラスタ内のすべてのノードは、 IPv4 のみ、IPv6 のみ、またはデュアル スタック IPv4/IPv6 のいずれかで構成する必要があります。

f) **クラスタ接続** に **BGP** を選択した場合は、 **[BGP ピアの詳細（BGP peer details）]** 領域で、ピアの IPv4 アドレスとASNを入力します。

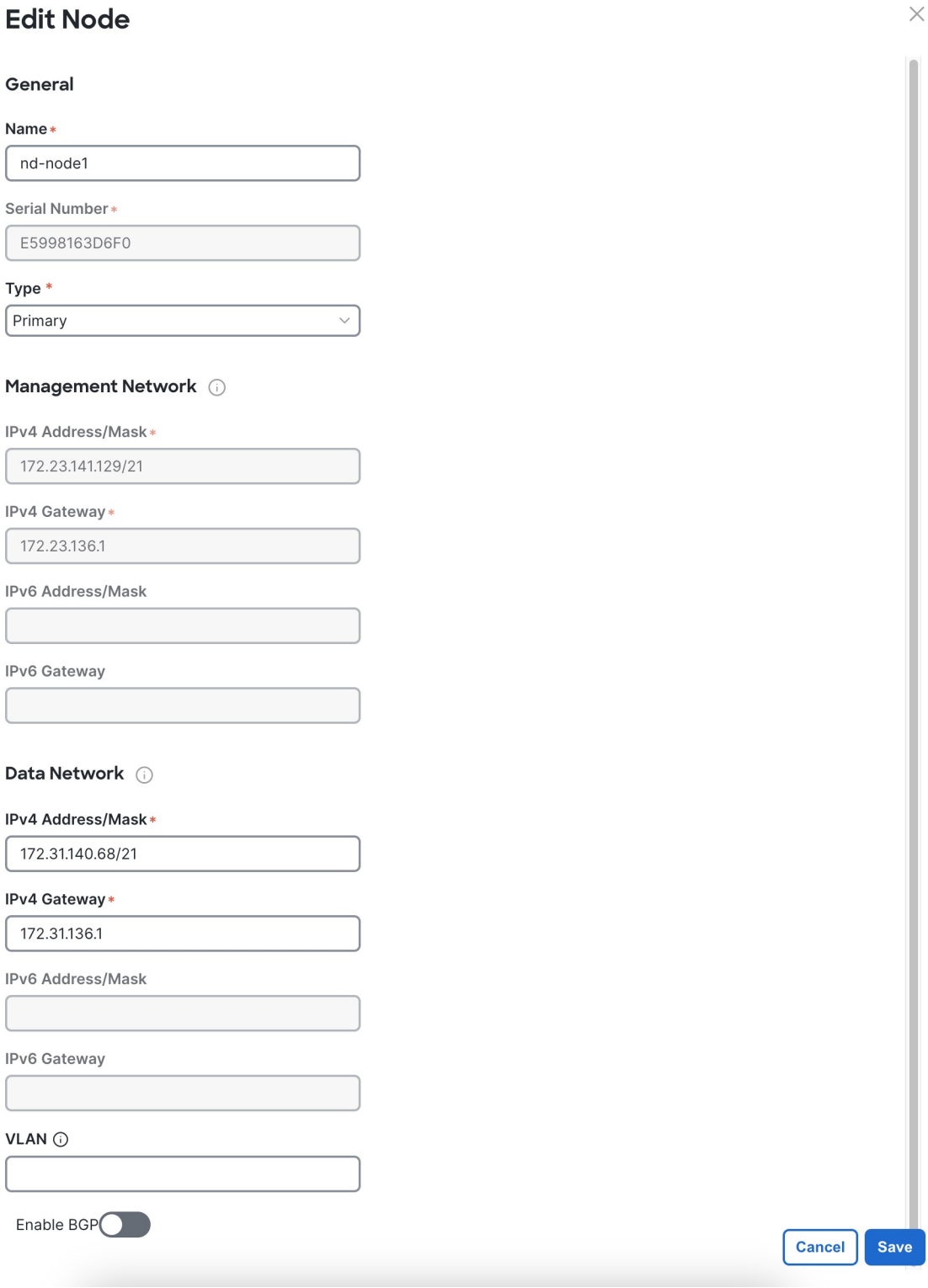
[+ IPv4 BGP ピアの追加（+ Add IPv4 BGP peer）] をクリックして、ピアを追加できます。

前のページで IPv6 機能を有効にした場合は、ピアの IPv6 アドレスと ASN も入力する必要があります。

g) **[Save]**をクリックして、変更内容を保存します。

ステップ 20 [**ノードの詳細（Node Details**）] 画面で、[**ノードの追加（Add Node**）] をクリックして、クラスタに 2 番目のノードを追加します。

単一ノード クラスタを展開する場合は、この手順をスキップします。



a) **[展開の詳細（Deployment Details）]** エリアで、2 番目のノードに **[管理 IP アドレス（Management IP Address）]** および **[パスワード（Password）]** を指定します。

ノードの初期構成手順で、管理ネットワーク情報とパスワードを定義しました。

b) **[検証（Validate）]** をクリックして、ノードへの接続を確認します。

接続が検証されると、ノードの**シリアル番号**と**管理ネットワーク**情報が自動的に入力されます。

c) ノードの **[名前（Name）]** を入力します。

d) **[タイプ（Type）]** ドロップダウンから `[プライマリ（Primary）]` を選択します。

クラスタの最初の 3 つのノードは `[プライマリ（ Primary）]` に設定する必要があります。より大規模なスケールを有効にする必要がある場合は、後の手順でセカンダリ ノードを追加します。

e) **[データ ネットワーク（Data Network）]** エリアで、ノードの**データ ネットワーク**を提供します。

データ ネットワークの IP アドレス、ネットマスク、およびゲートウェイを指定する必要があります。オプションで、ネットワークの VLAN ID を指定することもできます。ほとんどの導入では、[VLAN ID] フィールドを空白のままにできます。

前の画面で IPv6 機能を有効にした場合は、IPv6 アドレス、ネットマスク、およびゲートウェイも入力する必要があります。

（注）
IPv6 情報を提供する場合は、クラスタ ブートストラップ プロセス中に行う必要があります。後で IP 構成を変更するには、クラスタを再展開する必要があります。

クラスタ内のすべてのノードは、 IPv4 のみ、IPv6 のみ、またはデュアル スタック IPv4/IPv6 のいずれかで構成する必要があります。

f) （オプション）クラスタが L3 HA モードで展開されている場合は、データ ネットワークの **[BGP を有効にする（Enable BGP）]** をオンにします。

永続 IP アドレス機能には BGP 設定が必要です。この機能については、BGP 構成と永続的な IP アドレス （59 ページ） と『*Cisco Nexus Dashboard* ユーザーガイド』の「永続的な IP アドレス」セクションで詳しく説明されています。

（注）
BGP をこの時点で、またはクラスタの展開後に Nexus ダッシュボード GUI で有効にすることができます。

BGP を有効にする際、次の情報も入力する必要があります。

- このノードの **ASN**（BGP 自律システム番号）。

  すべてのノードに同じ ASN を構成することも、ノードごとに異なる ASN を構成することもできます。

- 純粋な IPv6 の場合、このノードの**ルータ ID**。

  ルータ ID は、`1.1.1.1` などの IPv4 アドレスである必要があります。

- ピアの IPv4 または IPv6 アドレスとピアの ASN を含む **BGP ピアの詳細**。

g) **[Save]**をクリックして、変更内容を保存します。

h) クラスタの最後の（3 番目の）プライマリ ノードでこの手順を繰り返します。

ステップ 21 （任意）前の手順を繰り返して、追加のセカンダリ ノードまたはスタンバイ ノードに関する情報を入力します。

（注）
より高いスケールをサポートするには、展開時に十分な数のセカンダリ ノードを提供する必要があります。特定のユースケースに必要な追加のセカンダリノードの詳しい数については、Nexus Dashboard クラスタ サイジング ツールを参照してください

スタンバイ ノードを今すぐ追加するか、クラスタの展開後に追加するかを選択できます。

ステップ 22 **[ノードの詳細（Node Details）]** ページで、入力した情報を確認してから、**[次へ（Next）]**をクリックします。

ステップ 23 永続的なIPアドレスをさらに追加する場合は、**[永続的な IP（Persistent IPs）]** ページで、**[+ データ サービスの IP アドレスの追加（+ Add Data Service IP Address）]**をクリックし、 IPアドレスを入力して、チェックマークアイコン（）をクリックします。必要な回数だけこのステップを繰り返し、**[次へ（Next）]** をクリックします。

ブートストラッププロセス中に、必要な永続IPアドレスの最小数を設定する必要があります。この手順により、必要に応じて永続的な IP アドレスを追加できます。

ステップ 24 **[概要（Summary）]** ページで設定情報をレビューして確認し、**[保存（Save）]** をクリックし、**[続行（Continue）]** をクリックして正しい展開モードを確認し、クラスタの構築を続行します。

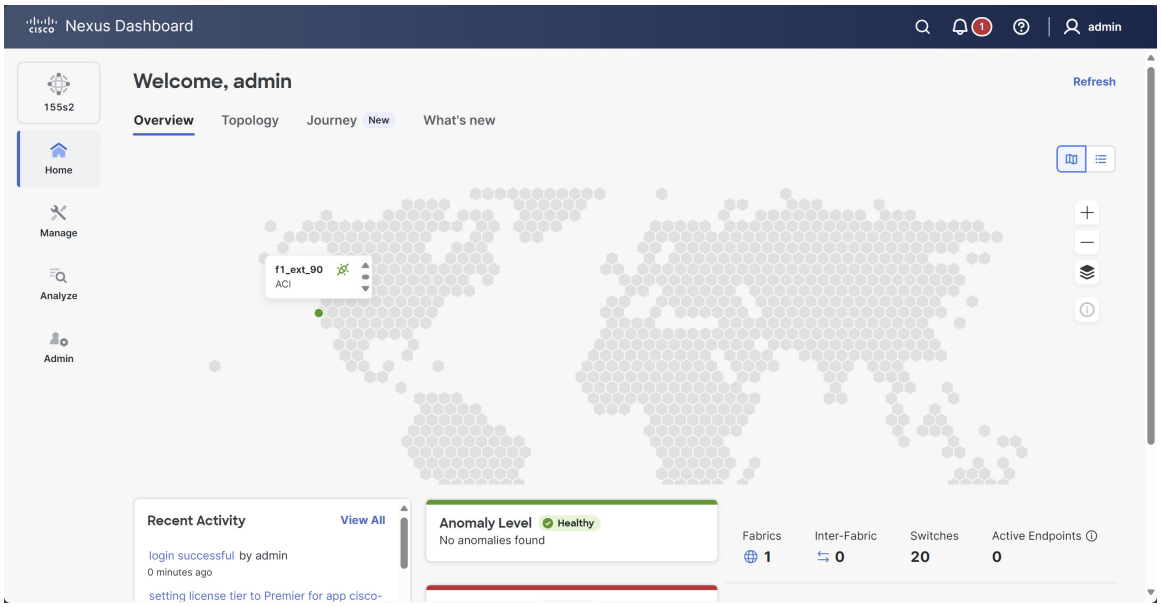
ノードのブート ストラップとクラスタの起動中に、全体的な進捗状況と各ノードの個々の進捗状況がUIに表示されます。ブートストラップの進行状況が表示されない場合は、ブラウザでページを手動で更新し、ステータスを更新してください。

クラスターが形成され、クラスター内のノードの数と起動するすべての機能に応じて、クラスタが形成されるまでに最大 60 分以上かかる場合があります。クラスタの設定が完了すると、ページが Nexus ダッシュボード GUI にリロードされます。

ステップ 25 クラスタが健全であることを検証します。

クラスタが使用可能になったら、ノードの管理 IP アドレスのいずれかを参照してアクセスできます。`admin` ユーザーのデフォルト パスワードは、最初のノードに選択した `rescue-user` のパスワードと同じです。この間、UI は上部に「サービスのインストールが進行中です。Nexus Dashboard の設定タスクは現在無効になっています」という意味のバナーを表示します。

すべてのクラスタが展開され、すべてのサービスが開始されたら**[ホーム（Home）]**>**[概要（Overview）]** ページの **異常レベル（Anomaly Level）** でクラスタが正常であることを確認できます。



または、SSH を使用し、`rescue-user` として、ノード展開中に入力したパスワードを使っていずれかのノードにログインし、`acs health` コマンドを実行してクラスタの状態を確認できます。

- クラスタが収束している間、次の出力が表示されることがあります：

```
$ acs health
k8s install is in-progress
```

```
$ acs health
k8s services not in desired state - [...]
```

```
$ acs health
k8s: Etcd cluster is not ready
```

- クラスタが稼働している場合は、次の出力が表示されます。

```
$ acs health
All components are healthy
```

（注）
場合によっては、ノードの電源を再投入（電源をオフにしてから再度オン）すると、この段階でスタックが停止することがある可能性があります。

```
deploy base system services
```

これは、pND（物理 Nexus Dashboard）クラスタの再起動後のノードの `etcd` の問題が原因です。

この問題を解決するには、影響を受けるノードで `acs reboot clean` コマンドを入力します。

ステップ 26 （オプション） Cisco Nexus DashboardクラスターをCisco Intersightに接続、可視性と利点を強化します。詳細な手順については、 「*Cisco Intersightの操作*」 を参照してください。

ステップ 27 Nexus Dashboardを展開した後、設定情報については、このリリースのコレクションページを参照してください。

次のタスク

次のタスクは、ファブリックとファブリック グループを作成することです。 Cisco Nexus Dashboardのコレクション ページ にある、このリリースの 「ファブリックとファブリック グループの作成」の記事を参照してください。

VMware ESXi での Nexus ダッシュボードの展開

ここでは、VMware ESXi で Cisco Nexus ダッシュボード クラスタを展開する方法について説明します。vCenter を使用して展開する場合は、代わりに VMware ESXi での Nexus ダッシュボードの展開 （112 ページ） で説明されている手順に従ってください。

始める前に

- VMware ESX で Nexus Dashboard クラスタを展開するための前提条件と注意事項 （93 ページ） に記載されている要件とガイドラインを満たしていることを確認します。

手順

ステップ 1 Cisco Nexus Dashboard OVAイメージを取得します。

a) [ソフトウェア ダウンロード（Software Download）] ページを参照します。

https://software.cisco.com/download/home/286327743/type/286328258/

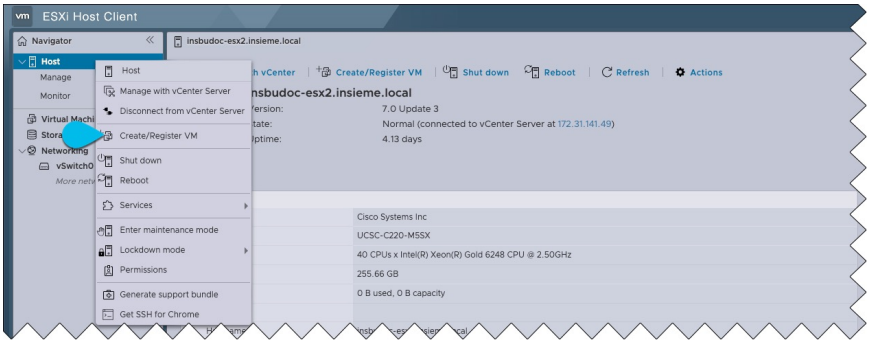
b) 左側のサイドバーから、ダウンロードする Nexus ダッシュボードのリリースバージョンを選択します。

c) Nexus ダッシュボード OVA イメージの横にある**ダウンロード**をクリックします（`nd-dk9.<version>.ova`）。

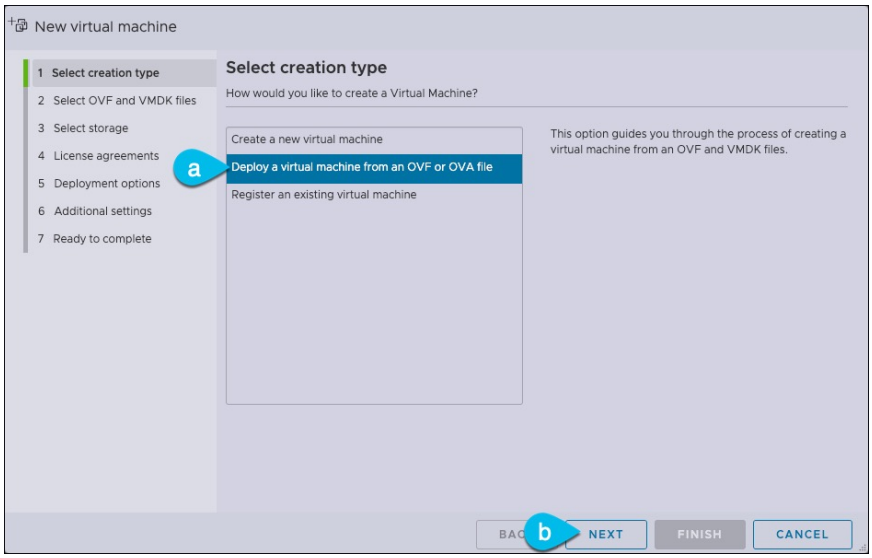
ステップ 2 VMware ESXi にログインします。

ESXiサーバのバージョンによっては、設定画面の場所と順序が若干異なる場合があります。次の手順では、VMware ESXi 7.0を使用した導入の詳細を示します。

ステップ 3 ホストを右クリックし、**[VM の作成/登録（Create/Register VM）]** を選択します。



ステップ 4 **[作成タイプの選択（Select creation type）]** 画面で、`[OVF または OVA ファイルから仮想マシンを展開する（Deploy a virtual machine from an OVF or OVA file）]` を選択し、**[次へ（Next）]** をクリックします。



ステップ 5 **[OVF と VMDK ファイルの選択（Select OVF and VMDK files）]** 画面で、最初の手順でダウンロードした仮想マシン名（`nd-ova-node1` など）とOVAイメージを入力し、**[次へ（Next）]** をクリックします。

ステップ 6 **[ストレージの選択（Select storage）]** 画面で、VM のデータストアを選択し、**[次へ（Next）]** をクリックします。

ステップ 7 **[OVF と VMDK ファイルの選択（Select OVF and VMDK files）]** 画面で、最初の手順でダウンロードした仮想マシン名（`nd-node1` など）とOVAイメージを入力し、**[次へ（Next）]** をクリックします。

ステップ 8 **[展開オプション（Deployment options）]** を指定します。

[展開オプション（Deployment options）] 画面で、次の情報を入力します。

- **[ネットワーク マッピング（Network mappings）]** ドロップダウンから、Nexus Dashboard の管理（`mgmt0`）およびデータ（`fabric0`）インターフェイスのネットワークを選択します。

  Nexus Dashboard ネットワークについては、全般的な前提条件とガイドライン （11 ページ） で説明しています。

- **[展開タイプ（Deployment type）]** ドロップダウンから、ノードプロファイル（`[アプリケーション（App）]` または `[データ（Data）]`）を選択します。

  ノード プロファイルについては、VMware ESX で Nexus Dashboard クラスタを展開するための前提条件と注意事項 （93 ページ） を参照してください。

- **[ディスク プロビジョニング タイプ（Disk provisioning type）]** で、`[シック（Thick）]` を選択します。

- **[自動的に電源をオンにする（Power on automatically）]** オプションを無効にします。

ステップ 9 **[完了準備（Ready to complete）]** 画面で、すべての情報が正しいことを確認し、**[終了（Finish）]** をクリックして最初のノードの展開を開始します。

ステップ 10 以前のステップを繰り返し、2 番目と 3 番目のノードを展開します。

（注）
単一のノードクラスタを展開している場合は、この手順をスキップできます。

最初のノードの展開が完了するのを待つ必要はありません。他の 2 つのノードの展開を同時に開始できます。

ステップ 11 VM の展開が完了するまで待ちます。

ステップ 12 VMware ツールの定期的な時刻同期が無効になっていることを確認してから、VM を起動します。

時刻の同期を無効にするには、次の手順を実行します。

a) VM を右クリックして、**[設定の編集（Edit Settings）]** を選択します。
b) **[設定の編集（Edit Settings）]** ウィンドウで、**[VMオプション（VM Options）]** タブを選択します。
c) **[VMware ツール（VMware Tools）]** カテゴリを展開し、**[ホストとゲスト時刻の同期（Synchronize guest time with host）]** オプションをオフにします。

ステップ 13 ノードのコンソールのいずれかを開き、ノードの基本情報を設定します。

a) 初期設定を開始します。

初回セットアップユーティリティの実行を要求するプロンプトが表示されます。

```
[ OK ] Started atomix-boot-setup.
       Starting Initial cloud-init job (pre-networking)...
       Starting logrotate...
       Starting logwatch...
       Starting keyhole...
[ OK ] Started keyhole.
[ OK ] Started logrotate.
[ OK ] Started logwatch.

Press any key to run first-boot setup on this console...
```

b) `admin` パスワードを入力して確認します。

このパスワードは、`rescue-user` SSH ログインおよび初期 GUI パスワードに使用されます。

（注）
すべてのノードに同じパスワードを指定する必要があります。指定しない場合、クラスタ作成に失敗します。

```
Admin Password:
Reenter Admin Password:
```

c) 管理ネットワーク情報を入力します。

```
Management Network:
  IP Address/Mask: 192.168.9.172/24
  Gateway: 192.168.9.1
```

d) 最初のノードのみ、「クラスタ リーダー」として指定します。

クラスタ リーダー ノードにログインして、設定を完了し、クラスタの作成を完了します。

```
Is this the cluster leader?: y
```

e) 入力した譲歩をレビューし、確認します。

入力した情報を変更するかどうかを尋ねられます。すべてのフィールドが正しい場合は、nを選択して続行します。入力した情報を変更する場合は、yを入力して基本設定スクリプトを再起動します。

```
Please review the config
Management network:
  Gateway: 192.168.9.1
  IP Address/Mask: 192.168.9.172/24
Cluster leader: no

Re-enter config? (y/N): n
```

ステップ 14 以前のステップを繰り返し、追加のノードを展開します。

単一のノードクラスタを展開している場合は、この手順をスキップできます。

マルチノードク ラスタの場合は、2 つの追加のプライマリ ノードと、特定のユースケースで必要なだけのセカンダリ ノードを展開する必要があります。必要なノードの総数は、 Nexus Dashboard キャパシティ プランニング ツールで確認できます。

最初のノードの設定が完了するのを待つ必要はありません。他の 2 つのノードの設定を同時に開始できます。

（注）
すべてのノードに同じパスワードを指定する必要があります。指定しない場合、クラスタ作成に失敗します。

追加のノードを展開する手順は同じですが、**クラスタ リーダー**ではないことを示す必要がある点が異なります。

ステップ 15 ブラウザを開き、`https://<node-mgmt-ip>` に移動して、GUI を開きます。

残りの設定ワークフローは、ノードの GUI の 1 つから実行します。展開したノードのいずれか 1 つを選択して、ブートストラッププロセスを開始できます。他の 2 つのノードにログインしたり、これらを直接構成したりする必要はありません。

前の手順で入力したパスワードを入力し、**[ログイン（Login）]** をクリックします。

ステップ 16 **[クラスタのブリングアップ（Cluster Bringup）**] ウィザードの **[基本情報（Basic Information）]** ページに、必要な情報を入力します。

a) **[クラスタ名（Cluster Name）]** には、Nexus Dashboard クラスタの名前を入力します。

クラスタ名は、 RFC-1123 の要件に従う必要があります。

b) **[Nexus Dashboard の実装タイプの選択（Nexus Dashboard Implementation type）]**で、**LAN]** または **[SAN]** を選択して、 **[次へ（Next）]**をクリックします。

ステップ 17 **[クラスタのブリングアップ（Cluster Bringup）**] ウィザードの **[構成（Configuration）]** ページで、必要な情報を入力します。

a) （任意）クラスタの IPv6 機能を有効にする場合は、**[IPv6 を有効にする（Enable IPv6）]** チェックボックスをオンにします。

b) をクリックして、1 つ以上の DNS サーバーを追加し、DNS プロバイダーの IP アドレスを入力し、チェックマーク アイコンをクリックします。

c) （任意） **[+ DNS 検索ドメインの追加]**をクリックして、検索ドメインを追加し、DNS 検索ドメインの IP アドレスを入力し、チェックマーク アイコンをクリックします。

d) （任意） NTP サーバー認証を有効にする場合は、**[NTP 認証]** チェックボックスをオンにします。

e) NTP 認証を有効にした場合、**+ Add Key** をクリックし、必要な情報を入力し、チェックマーク アイコンをクリックして情報を保存します。

- **キー**：NTP 認証キーを入力します。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です。次の手順で NTP サーバーを定義します。複数の NTP サーバーで同じ NTP 認証キーを使用できます。
- **ID**： NTP ホストのキー ID を入力します。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**：NTPキーの認証タイプを選択します。
- このキーを信頼したい場合には、**[信頼済み（Trusted）]** チェックボックスをオンにします。信頼できないキーは NTP 認証に使用できません。

NTP認証の要件とガイドラインの完全なリストについては、全般的な前提条件とガイドライン（11 ページ） を参照してください。

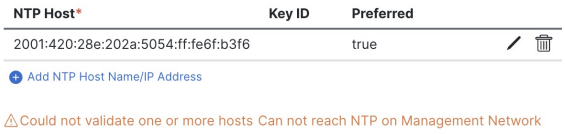
追加のNTPキーを入力する場合は、 **[+ キーの追加（+ Add Key）]** を再度クリックして、情報を入力します。

f) NTP認証を有効にした場合は、 **[+ NTP ホスト名/ IPアドレスの追加（+Add NTP Host Name/ IP Address）]**をクリックし、必要な情報を入力し、チェックマークアイコンをクリックして情報を保存します。

- **NTP ホスト**：IPアドレスを入力する必要があります。完全修飾ドメイン名（FQDN）はサポートされていません。
- **キー ID**：前のサブステップで定義した NTP キーのキー ID を入力します。

  NTP 認証が無効になっている場合、このフィールドはグレー表示されます。
- このホストを優先したい場合は、**[優先（Preferred）]** チェックボックスをオンにします。

（注）
ログインしているノードに IPv4 アドレスのみが設定されているが、前の手順で **[IPv6 を有効にする（Enable IPv6）]** をオンにして NTP サーバーの IPv6 アドレスを指定した場合は、次の検証エラーが表示されます。



これは、ノードに IPv6 アドレスがまだなく、NTP サーバーの IPv6 アドレスに接続できないためです。次の手順で IPv6 アドレスを入力します。この場合、次の手順の説明に従って他の必要な情報

の入力を完了し、**[次へ（Next）]** をクリックして次の画面に進み、ノードの IPv6 アドレスを入力します。

追加の NTP サーバーを入力する場合は、**[+ Add NTP Host Name/IP Address）]** を再度クリックし、情報を入力します。

g) **[プロキシ サーバー（Proxy Server）]** について、プロキシ サーバーの URL または IP アドレスを入力します。

Cisco Cloud に直接接続できないクラスタの場合は、接続を確立するためにプロキシ サーバを構成することをお勧めします。これにより、ファブリック内の非適合ハードウェアおよびソフトウェアにさらされるリスクを軽減できます。

+Add Ignore Host をクリックして、トラフィックがプロキシの使用をスキップする 1 つ以上の接続先 IP アドレスを入力します。

プロキシ サーバーでは、次の URL が有効になっている必要があります：

```
dcappcenter.cisco.com
svc.intersight.com
svc.ucs-connect.com
svc-static1.intersight.com
svc-static1.ucs-connect.com
```

プロキシを構成しない場合は、**[プロキシをスキップ（Skip Proxy）]**をクリックして、**[確認（Confirm）]** をクリックします。

h) （任意）プロキシサーバーで認証が必要な場合は、**[プロキシに必要な認証（Authentication required for Proxy）]** をオンにして、ログイン資格情報を指定します。

i) （任意） **[詳細設定（Advanced Settings）]** カテゴリを展開し、必要に応じて設定を変更します。

詳細設定では、次の設定を行うことができます。

- **アプリ ネットワーク**：Nexus Dashboard でアプリケーションで使用されるアドレス空間です。ターゲット ネットワークの IP アドレスとネットマスクを入力します。
- **サービス ネットワーク**：Nexus Dashboard とそのプロセスで使用される内部ネットワークです。ターゲット ネットワークの IP アドレスとネットマスクを入力します。
- **[アプリ ネットワーク IPv6（App Network IPv6）]**：先ほど **[IPv6 の有効化（Enable IPv6）]** チェックボックスをオンにした場合は、アプリ ネットワークの IPv6 サブネットを入力します。
- **[サービス ネットワーク IPv6（Service Network IPv6）]**：先ほど **[IPv6 を有効にする（Enable IPv6）]** チェックボックスをオンにした場合は、サービス ネットワークの IPv6 サブネットを入力します。

アプリケーションおよびサービス ネットワークの詳細については、全般的な前提条件とガイドライン （11 ページ） を参照してください。

j) [次へ（Next）] をクリックします。

ステップ 18 **[ノードの詳細（Node Details）]** ページで、最初のノードの情報を更新します。

前の手順の初期ノード構成時に現在ログインしているノードの管理ネットワークとIPアドレスを定義しましたが、他のプライマリノードを追加し、クラスタを作成する進む前に、ノードのデータ ネットワーク情報も指定する必要があります。

a) **クラスタ接続** について、クラスタがL3 HAモードで展開されている場合は、**BGP** を選択します。それ以外の場合は、 **L2**を選択します。

テレメトリで使用される永続的なIPアドレス機能には、BGP構成が必要です。この機能については、BGP 構成と永続的な IP アドレス （59 ページ） と『*Cisco Nexus Dashboard* ユーザーガイド』の「永続的なIPアドレス」セクションで詳しく説明されています。

（注）
BGP をこの時点で、またはクラスタの展開後に Nexus ダッシュボード GUI で有効にすることができます。BGP が構成されている場合は、残りのすべてのノードで BGP を構成する必要があります。ノードのデータネットワークに異なるサブネットがある場合は、ここで BGP を有効にする必要があります。

b) 最初のノードの横にある **[編集（Edit）]**ボタンをクリックします。

ノードの**[シリアル番号（Serial Number）]**、**[管理ネットワーク（Management Network）]**情報、および**[タイプ（Type）]**が自動的に入力されます。ただし、他の情報は入力する必要があります。

c) **[名前（Name）]**に、サービス ノードのノード名を入力します。

ノードの **名前** はホスト名として設定されるため、 RFC-1123 の要件に従う必要があります。

（注）
[名前（Name）]フィールドが編集できない場合には、CIMC の検証を再度実行して、この問題を修正してください。

d) **[タイプ（Type）]**で、 **[プライマリ（Primary）]**を選択します。

クラスタの最初のノードは **[プライマリ（Primary）]** に設定する必要があります。より大規模なスケールを有効にする必要がある場合は、後の手順でセカンダリ ノードを追加します。

e) **[データ ネットワーク（Data Network）]** エリアで、ノードのデータ ネットワークを入力します。

データ ネットワークの IP アドレス、ネットマスク、およびゲートウェイを入力します。オプションで、ネットワークの VLAN ID を指定することもできます。構成に VLAN が不要な場合は、 [VLAN ID] フィールドを空白のままにします。**データ接続** に **BGP** を選択した場合は、 ASNを入力します。

前のページで IPv6 機能を有効にした場合は、IPv6 アドレス、ネットマスク、およびゲートウェイも入力する必要があります。

（注）
IPv6 情報を提供する場合は、クラスタ ブートストラップ プロセス中に行う必要があります。後で IP アドレス構成を変更するには、クラスタを再展開する必要があります。

クラスタ内のすべてのノードは、 IPv4 のみ、IPv6 のみ、またはデュアル スタック IPv4/IPv6 のいずれかで構成する必要があります。

f) **クラスタ接続** に **BGP** を選択した場合は、**[BGP ピアの詳細（BGP peer details）]** 領域で、ピアの IPv4 アドレスとASNを入力します。

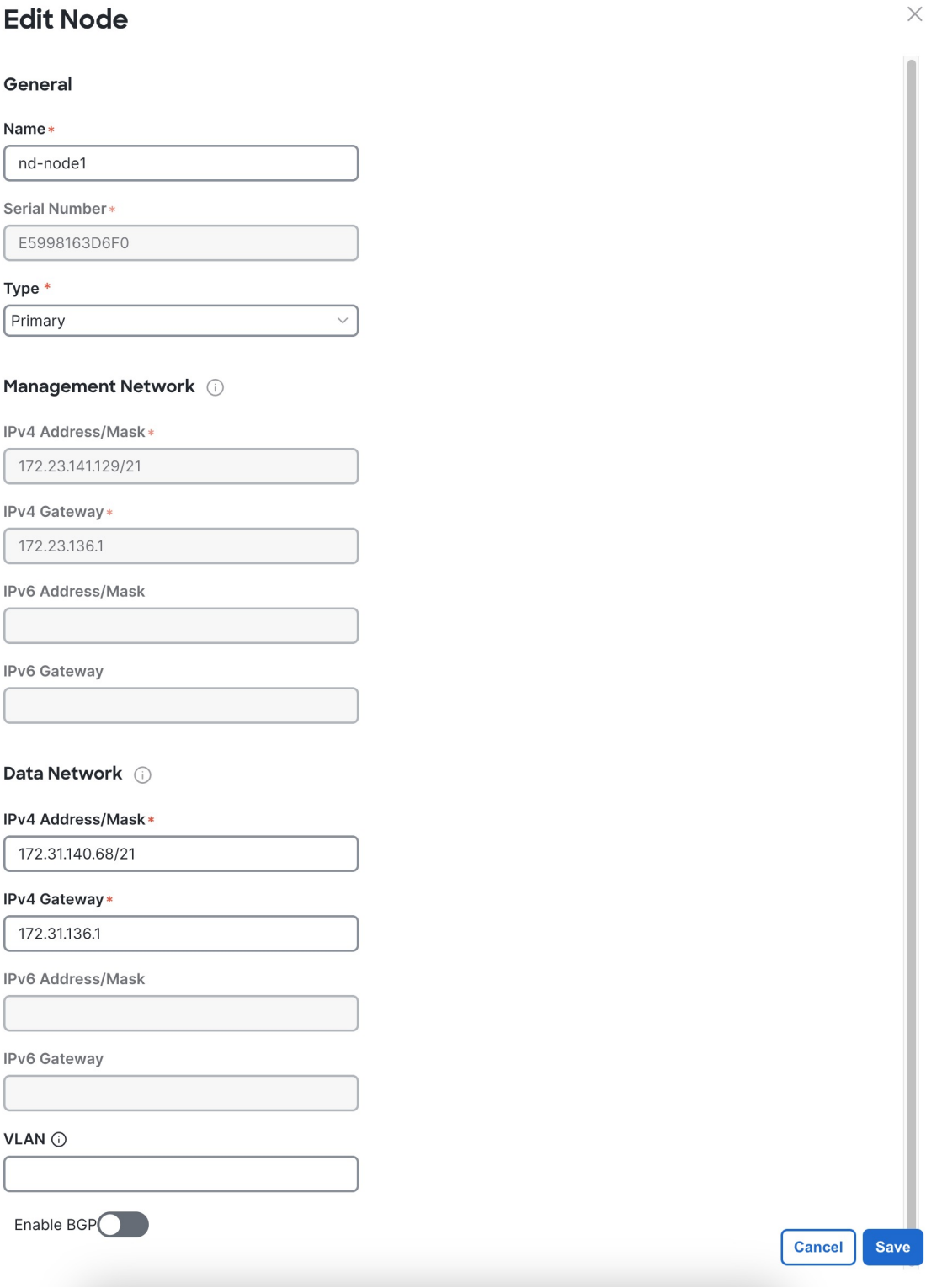
[+ IPv4 BGP ピアの追加（+ Add IPv4 BGP peer）] をクリックして、ピアを追加できます。

前のページで IPv6 機能を有効にした場合は、ピアの IPv6 アドレスと ASN も入力する必要があります。

g) **[Save]**をクリックして、変更内容を保存します。

ステップ 19 [**ノードの詳細（Node Details**）] 画面で、[**ノードの追加（Add Node**）] をクリックして、クラスタに 2 番目のノードを追加します。

単一ノード クラスタを展開する場合は、この手順をスキップします。



a) **[展開の詳細（Deployment Details）]** エリアで、2 番目のノードに **[管理 IP アドレス（Management IP Address）]** および **[パスワード（Password）]** を指定します。

ノードの初期構成手順で、管理ネットワーク情報とパスワードを定義しました。

b) **[検証（Validate）]** をクリックして、ノードへの接続を確認します。

接続が検証されると、ノードの**シリアル番号**と**管理ネットワーク**情報が自動的に入力されます。

c) ノードの **[名前（Name）]** を入力します。

d) **[タイプ（Type）]** ドロップダウンから `[プライマリ（Primary）]` を選択します。

クラスタの最初の 3 つのノードは `[プライマリ（ Primary）]` に設定する必要があります。より大規模なスケールを有効にする必要がある場合は、後の手順でセカンダリ ノードを追加します。

e) **[データ ネットワーク（Data Network）]** エリアで、ノードの**データ ネットワーク**を提供します。

データ ネットワークの IP アドレス、ネットマスク、およびゲートウェイを指定する必要があります。オプションで、ネットワークの VLAN ID を指定することもできます。ほとんどの導入では、[VLAN ID] フィールドを空白のままにできます。

前の画面で IPv6 機能を有効にした場合は、IPv6 アドレス、ネットマスク、およびゲートウェイも入力する必要があります。

（注）
IPv6 情報を提供する場合は、クラスタ ブートストラップ プロセス中に行う必要があります。後で IP 構成を変更するには、クラスタを再展開する必要があります。

クラスタ内のすべてのノードは、 IPv4 のみ、IPv6 のみ、またはデュアル スタック IPv4/IPv6 のいずれかで構成する必要があります。

f) （オプション）クラスタが L3 HA モードで展開されている場合は、データ ネットワークの **[BGP を有効にする（Enable BGP）]** をオンにします。

永続 IP アドレス機能には BGP 設定が必要です。この機能については、BGP 構成と永続的な IP アドレス （59 ページ） と『*Cisco Nexus Dashboard* ユーザーガイド』の「永続的な IP アドレス」セクションで詳しく説明されています。

（注）
BGP をこの時点で、またはクラスタの展開後に Nexus ダッシュボード GUI で有効にすることができます。

BGP を有効にする際、次の情報も入力する必要があります。

- このノードの **ASN**（BGP 自律システム番号）。

  すべてのノードに同じ ASN を構成することも、ノードごとに異なる ASN を構成することもできます。

- 純粋な IPv6 の場合、このノードの**ルータ ID**。

  ルータ ID は、`1.1.1.1` などの IPv4 アドレスである必要があります。

- ピアの IPv4 または IPv6 アドレスとピアの ASN を含む **BGP ピアの詳細**。

g) **[Save]**をクリックして、変更内容を保存します。

h) クラスタの最後の（3 番目の）プライマリ ノードでこの手順を繰り返します。

ステップ 20 （任意）前の手順を繰り返して、追加のセカンダリ ノードまたはスタンバイ ノードに関する情報を入力します。

（注）
より高いスケールをサポートするには、展開時に十分な数のセカンダリ ノードを提供する必要があります。特定のユースケースに必要な追加のセカンダリノードの詳しい数については、Nexus Dashboard クラスタ サイジング ツールを参照してください

スタンバイ ノードを今すぐ追加するか、クラスタの展開後に追加するかを選択できます。

ステップ 21 **[ノードの詳細（Node Details）]** ページで、入力した情報を確認してから、**[次へ（Next）]**をクリックします。

ステップ 22 永続的なIPアドレスをさらに追加する場合は、**[永続的な IP（Persistent IPs）]** ページで、**[+ データ サービスの IP アドレスの追加（+ Add Data Service IP Address）]**をクリックし、IPアドレスを入力して、チェックマークアイコン（）をクリックします。必要な回数だけこのステップを繰り返し、**[次へ（Next）]** をクリックします。

ブートストラッププロセス中に、必要な永続IPアドレスの最小数を設定する必要があります。この手順により、必要に応じて永続的な IP アドレスを追加できます。

ステップ 23 **[概要（Summary）]** ページで設定情報をレビューして確認し、**[保存（Save）]** をクリックし、**[続行（Continue）]** をクリックして正しい展開モードを確認し、クラスタの構築を続行します。

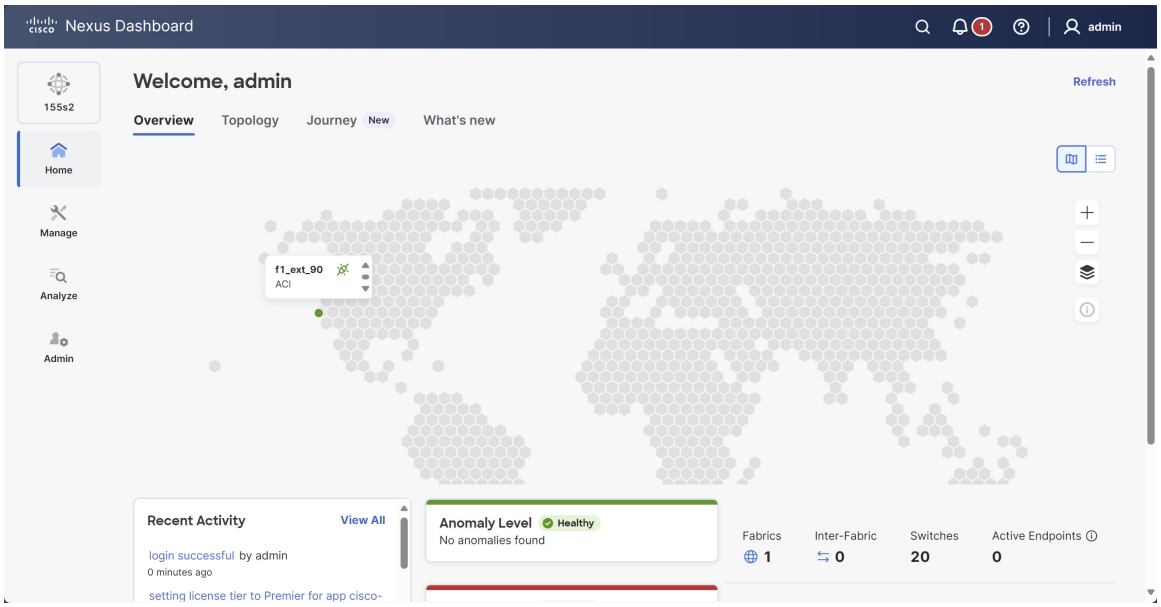
ノードのブート ストラップとクラスタの起動中に、全体的な進捗状況と各ノードの個々の進捗状況がUIに表示されます。ブートストラップの進行状況が表示されない場合は、ブラウザでページを手動で更新し、ステータスを更新してください。

クラスターが形成され、クラスター内のノードの数と起動するすべての機能に応じて、クラスタが形成されるまでに最大 60 分以上かかる場合があります。クラスタの設定が完了すると、ページが Nexus ダッシュボード GUI にリロードされます。

ステップ 24 クラスタが健全であることを検証します。

クラスタが使用可能になったら、ノードの管理 IP アドレスのいずれかを参照してアクセスできます。`admin` ユーザーのデフォルト パスワードは、最初のノードに選択した `rescue-user` のパスワードと同じです。この間、UI は上部に「サービスのインストールが進行中です。Nexus Dashboard の設定タスクは現在無効になっています」という意味のバナーを表示します。

すべてのクラスタが展開され、すべてのサービスが開始されたら**[ホーム（Home）]**>**[概要（Overview）]** ページの **異常レベル（Anomaly Level）** でクラスタが正常であることを確認できます。



または、SSH を使用し、`rescue-user` として、ノード展開中に入力したパスワードを使っていずれかのノードにログインし、`acs health` コマンドを実行してクラスタの状態を確認できます。

- クラスタが収束している間、次の出力が表示されることがあります：

```
$ acs health
k8s install is in-progress
```

```
$ acs health
k8s services not in desired state - [...]
```

```
$ acs health
k8s: Etcd cluster is not ready
```

- クラスタが稼働している場合は、次の出力が表示されます。

```
$ acs health
All components are healthy
```

（注）
場合によっては、ノードの電源を再投入（電源をオフにしてから再度オン）すると、この段階でスタックが停止することがある可能性があります。

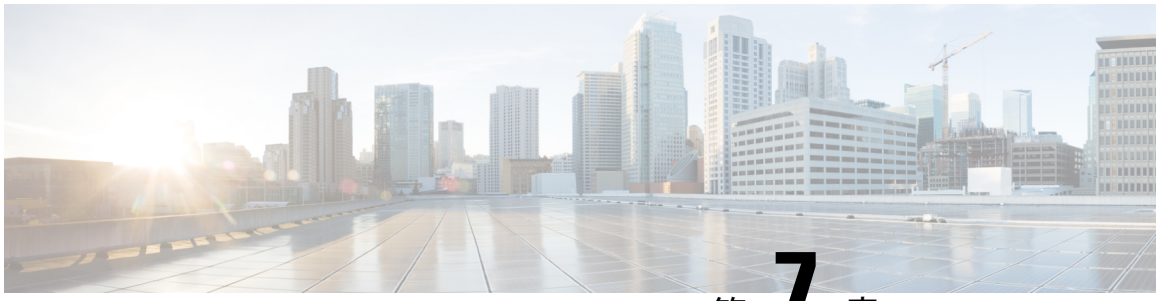
```
deploy base system services
```

これは、pND（物理 Nexus Dashboard）クラスタの再起動後のノードの `etcd` の問題が原因です。

この問題を解決するには、影響を受けるノードで `acs reboot clean` コマンドを入力します。

ステップ 25 （オプション） Cisco Nexus DashboardクラスターをCisco Intersightに接続、可視性と利点を強化します。詳細な手順については、 「*Cisco Intersightの操作*」 を参照してください。

ステップ 26 Nexus Dashboardを展開した後、設定情報については、このリリースのコレクションページを参照してください。



第 7 章

Linux KVMでの展開

Linux KVM で Nexus Dashboard クラスタを展開するための前提条件と注意事項

Linux KVM で Nexus Dashboard クラスタの展開に進む前に、KVM が次の前提条件を満たしている必要があり、次の注意事項に従う必要があります。

- KVM フォーム ファクタが拡張性要件をサポートする必要があります。

  クラスタ フォーム ファクタに基づいて、拡張性サポートおよび共同ホストは変わります。Nexus ダッシュボード キャパシティ プランニング ツールを使用して、仮想フォーム ファクタが展開要件を満たすことを確認できます。

- 前提条件とガイドライン （11 ページ） に記載されている一般的な前提条件を確認して完了します。

- Nexus Dashboard VM に使用される CPU ファミリが AVX 命令セットをサポートしている必要があります。

- KVM には十分なシステム リソースが必要です。また、各ノードには専用のディスク パーティションが必要です。詳細については、「システム リソースを理解する （127ページ）」を参照してください。

- ディスクの I/O 遅延は 20 ミリ秒以下である必要があります。

  「Linux KVM ストレージ デバイスの I/O 遅延の確認 （126 ページ）」を参照してください。

- Cisco は、ネストされた仮想化環境の使用をサポートしていません。仮想化ハイパーバイザ（例：ESXi上のKVM）上で動作している仮想マシンにNexus Dashboardを展開すること

は、サポート対象外の構成であり、パフォーマンスの低下やシステムの不安定化を招く可能性があります。

- KVM の導入は、NX- OS および ACI ファブリックのみならず、SAN の展開でサポートされています。
- Red Hat Enterprise Linux 8.8、8.10、または 9.4 に展開する必要があります。
- OS のリブート時にNexus Dashboard を稼働させるには、RHEL ホスト オペレーティング システムの `fstab設定` ファイルに UUID を追加する必要があります。これが、RHEL オペレーティング システムの再起動時にNexus Dashboard を保持できる唯一の方法です。
- また、 Nexus Dashboad の展開に必要な次のネットワーク ブリッジをホスト レベルで構成する必要があります。
  - 管理網ブリッジ（mgmt-bridge）： Nexus Dashboad を管理するための外部ネットワーク。
  - データ網ブリッジ（data-bridge）： Nexus Dashboad 内でクラスタリングを形成するために使用される内部ネットワーク。
- 各 Nexus Dashboard ノードは異なる KVM ハイパーバイザに展開することを推奨します。

Linux KVM ストレージ デバイスの I/O 遅延の確認

Linux KVM に Nexus Dashboard クラスタを展開する場合、KVM のストレージ デバイスの遅延は 20 ミリ秒未満である必要があります。

Linux KVM ストレージ デバイスの I/O 遅延を確認するには、次の手順を実行します。

手順

ステップ 1 テスト ディレクトリを作成します。

たとえば、 `test-data`という名前のディレクトリを作成します。

ステップ 2 フレキシブル I/O テスター（FIO）を実行します。

```
# fio --rw=write --ioengine=sync --fdatasync=1 --directory=test-data --size=22m --bs=2300 --name=mytest
```

ステップ 3 コマンドの実行後に、`fsync/fdatasync/sync_file_range` セクションの `99.00th=[<value>]` が 20 ミリ秒未満であることを確認します。

システム リソースを理解する

Linux KVM に Nexus ダッシュボード クラスターを展開する場合、KVM には十分なシステム リソースが必要です。仮想 Nexus Dashboard KVM では複数のフォーム ファクタがサポートされており、各ノードに必要なシステム リソースの量はフォーム ファクタによって異なります。

表 *14*: ノード当たりのリソース要件

フォーム ファクタ	vCPU の数	RAM サイズ	ディスク サイズ
1 ノードKVM（アプリ）	16	64 GB	550 GB
1 ノードKVM（データ）	32	128 GB	3 TB
3 ノードKVM（アプリ）	16	64 GB	550 GB
3 ノードKVM（データ）	32	128 GB	3 TB

Linux KVM での Nexus ダッシュボードの展開 （127 ページ）の手順を実行するときに、フォーム ファクタに関する上記の情報を知っておく必要があります

Linux KVM での Nexus ダッシュボードの展開

ここでは、Linux KVM で Cisco Nexus ダッシュボード クラスタを展開する方法について説明します。

始める前に

- Linux KVM で Nexus Dashboard クラスタを展開するための前提条件と注意事項 （125 ページ） に記載されている要件とガイドラインを満たしていることを確認します。

手順

ステップ 1 Cisco Nexus ダッシュボード イメージをダウンロードします。

a) [ソフトウェア ダウンロード（Software Download）] ページを参照します。

https://software.cisco.com/download/home/286327743/type/286328258

b) **[Nexus ダッシュボード ソフトウェア]** をクリックします。

c) 左側のサイドバーから、ダウンロードする Nexus ダッシュボードのバージョンを選択します。

d) Linux KVM の Cisco Nexus ダッシュボードイメージをダウンロードします（`nd-dk9.<version>.qcow2`）。

ステップ 2 ノードをホストする Linux KVM サーバーにイメージをコピーします。

scp を使用してイメージをコピーできます。次に例を示します。

```
# scp nd-dk9.<version>.qcow2 root@<kvm-host-ip>:/home/nd-base
```

次の手順は、イメージを /home/nd-base ディレクトリにコピーしたことを前提としています。

ステップ 3 各 KVM ホストで次の構成を行います。

a) /etc/libvirt/qemu.conf を編集、 Nexus Dashboard の展開に使用する予定のストレージの所有権に基づいて、ユーザーとグループが正しく設定されていることを確認します。

これは、デフォルトの libvirtdとは異なるディスク ストレージ パスを使用する場合にのみ必要です。

b) /etc/libvirt/libvirt.conf を編集、 uri_default のコメントを外します。

c) ルートから systemctl restart libvirtd コマンドを使用して設定を更新した後、 libvirtd サービスを再起動します。

ステップ 4 KVMホストにルートユーザーとしてログインし、各ノードで必要なディスクイメージを作成するために次の手順を実行します。

システム リソースを理解する （127 ページ） で説明されているとおり、2 つのディスク イメージを作成するには、合計 550 GB または 3 TB の SSD ストレージが必要です。

- ダウンロードした QCOW2 イメージに基づいてディスクを起動します。
- データ ディスク：

a) VMディスクを保存するのに十分な空き容量があるディレクトリ（例：/home/nd-node1）があることを確認するか、ストレージ ディスク（raw ディスクまたは LVM）を /opt/cisco/nd ディレクトリにマウントしてください。

b) ルート ディレクトリの下に /root/create_vm.sh として次のスクリプトを作成します。

（注）
この情報を手動で入力する場合は、これらの行の後に空白がないことを確認します。

システム リソースを理解する （127 ページ）に記載されている情報に基づき、次のとおり、スクリプトを作成します。

- 1ノードまたは 3ノードKVM（**アプリ**）フォームファクタの場合：

```
#!/bin/bash -ex

# Configuration
# Name of Nexus Dashboard Virtual machine
name=nd1

# Path of Nexus Dashboard QCOW2 image.
nd_qcow2=/home/nd-base/nd-dk9.4.1.1g.qcow2

# Disk Path to storage Boot and Data Disks.
data_disk=/opt/cisco/nd/data

# Management Network Bridge
mgmt_bridge=mgmt-bridge
```

```
# Data Network bridge
data_bridge=data-bridge

# Data Disk Size
data_size=500G

# CPU Cores
cpus=16

# Memory in units of MB.
memory=65536

# actual script
rm -rf $data_disk/boot.img
/usr/bin/qemu-img convert -f qcow2 -O raw $nd_qcow2 $data_disk/boot.img
rm -rf $data_disk/disk.img
/usr/bin/qemu-img create -f raw $data_disk/disk.img $data_size
virt-install \
--import \
--name $name \
--memory $memory \
--vcpus $cpus \
--os-type generic \
--osinfo detect=on,require=off \
--check path_in_use=off \
--disk path=${data_disk}/boot.img,format=raw,bus=virtio \
--disk path=${data_disk}/disk.img,format=raw,bus=virtio \
--network bridge=$mgmt_bridge,model=virtio \
--network bridge=$data_bridge,model=virtio \
--console pty,target_type=serial \
--noautoconsole \
--autostart
```

- 1ノードまたは3ノードKVM（**データ**）フォームファクタの場合：

```
#!/bin/bash -ex

# Configuration
# Name of Nexus Dashboard Virtual machine
name=nd1

# Path of Nexus Dashboard QCOW2 image.
nd_qcow2=/home/nd-base/nd-dk9.4.1.1g.qcow2

# Disk Path to storage Boot and Data Disks.
data_disk=/opt/cisco/nd/data

# Management Network Bridge
mgmt_bridge=mgmt-bridge

# Data Network bridge
data_bridge=data-bridge

# Data Disk Size
data_size=3072G

# CPU Cores
cpus=32

# Memory in units of MB.
memory=131072

# actual script
```

```
rm -rf $data_disk/boot.img
/usr/bin/qemu-img convert -f qcow2 -O raw $nd_qcow2 $data_disk/boot.img
rm -rf $data_disk/disk.img
/usr/bin/qemu-img create -f raw $data_disk/disk.img $data_size
virt-install \
--import \
--name $name \
--memory $memory \
--vcpus $cpus \
--os-type generic \
--osinfo detect=on,require=off \
--check path_in_use=off \
--disk path=${data_disk}/boot.img,format=raw,bus=virtio \
--disk path=${data_disk}/disk.img,format=raw,bus=virtio \
--network bridge=$mgmt_bridge,model=virtio \
--network bridge=$data_bridge,model=virtio \
--console pty,target_type=serial \
--noautoconsole \
--autostart
```

ステップ 5 `create_vm.sh` スクリプトを実行可能にし、これらのコマンドを使用して実行します。

```
# chmod +x /root/create_vm.sh
# /root/create_vm.sh
```

ステップ 6 以前のステップを繰り返し、2 番目と 3 番目のノードを展開して、すべての VM を開始します。

（注）
単一のノードクラスタを展開している場合は、この手順をスキップできます。

ステップ 7 ノードのコンソールのいずれかを開き、ノードの基本情報を設定します。

a) いずれかのキーを押して、初期設定を開始します。

初回セットアップユーティリティの実行を要求するプロンプトが表示されます。

```
[ OK ] Started atomix-boot-setup.
       Starting Initial cloud-init job (pre-networking)...
       Starting logrotate...
       Starting logwatch...
       Starting keyhole...
[ OK ] Started keyhole.
[ OK ] Started logrotate.
[ OK ] Started logwatch.

Press any key to run first-boot setup on this console...
```

b) `admin` パスワードを入力して確認します。

このパスワードは、`rescue-user` SSH ログインおよび初期 GUI パスワードに使用されます。

（注）
すべてのノードに同じパスワードを指定する必要があります。指定しない場合、クラスタ作成に失敗します。

```
Admin Password:
Reenter Admin Password:
```

c) 管理ネットワーク情報を入力します。

```
Management Network:
  IP Address/Mask: 192.168.9.172/24
  Gateway: 192.168.9.1
```

d) 最初のノードのみ、「クラスタ リーダー」として指定します。

クラスタ リーダー ノードにログインして、設定を完了し、クラスタの作成を完了します。

```
Is this the cluster leader?: y
```

e) 入力した譲歩をレビューし、確認します。

入力した情報を変更するかどうかを尋ねられます。すべてのフィールドが正しい場合は、nを選択して続行します。入力した情報を変更する場合は、yを入力して基本設定スクリプトを再起動します。

```
Please review the config
Management network:
  Gateway: 192.168.9.1
  IP Address/Mask: 192.168.9.172/24
Cluster leader: yes

Re-enter config? (y/N): n
```

ステップ 8 前の手順を繰り返して、2 番目と 3 番目のノードの初期情報を構成します。

最初のノードの設定が完了するのを待つ必要はありません。他の 2 つのノードの設定を同時に開始できます。

（注）
すべてのノードに同じパスワードを指定する必要があります。指定しない場合、クラスタ作成に失敗します。

2 番目と 3 番目のノードを展開する手順は同じですが、**クラスタ リーダー**ではないことを示す必要がある点が異なります。

ステップ 9 初期ブートストラップ プロセスを待機して、すべてのノードで完了します。

管理ネットワーク情報を入力して確認すると、最初のノード（クラスタ リーダー）初期設定でネットワーキングが設定され、UI が表示されます。この UI を使用して、他の 2 つのノードを追加し、クラスタの展開を完了します。

```
Please wait for system to boot: [#########################] 100%
System up, please wait for UI to be online.

System UI online, please login to https://192.168.9.172 to continue.
```

ステップ 10 ブラウザを開き、`https://<node-mgmt-ip>` に移動して、GUI を開きます。

残りの設定ワークフローは、ノードの GUI の 1 つから実行します。展開したノードのいずれか 1 つを選択して、ブートストラッププロセスを開始できます。他の 2 つのノードにログインしたり、これらを直接構成したりする必要はありません。

前の手順で入力したパスワードを入力し、**[ログイン（Login）]** をクリックします。

ステップ 11 **[クラスタのブリングアップ（Cluster Bringup）**] ウィザードの **[基本情報（Basic Information）]** ページに、必要な情報を入力します。

a) **[クラスタ名（Cluster Name）]** には、Nexus Dashboard クラスタの名前を入力します。

クラスタ名は、 RFC-1123 の要件に従う必要があります。

b) **[Nexus Dashboard の実装タイプの選択（Nexus Dashboard Implementation type）]**で、**LAN]** または **[SAN]** を選択して、 **[次へ（Next）]**をクリックします。

ステップ 12 **[クラスタのブリングアップ（Cluster Bringup）**] ウィザードの **[構成（Configuration）]** ページで、必要な情報を入力します。

a) （任意） クラスタの IPv6 機能を有効にする場合は、**[IPv6 を有効にする（Enable IPv6）]** チェックボックスをオンにします。

b) をクリックして、1 つ以上の DNS サーバーを追加し、DNS プロバイダーの IP アドレスを入力し、チェックマーク アイコンをクリックします。

c) （任意） **[+ DNS 検索ドメインの追加]**をクリックして、検索ドメインを追加し、DNS 検索ドメインの IP アドレスを入力し、チェックマーク アイコンをクリックします。

d) （任意） NTP サーバー認証を有効にする場合は、**[NTP 認証]** チェックボックスをオンにします。

e) NTP 認証を有効にした場合、**+ Add Key** をクリックし、必要な情報を入力し、チェックマーク アイコンをクリックして情報を保存します。

- **キー**：NTP 認証キーを入力します。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です。次の手順で NTP サーバーを定義します。複数の NTP サーバーで同じ NTP 認証キーを使用できます。
- **ID**： NTP ホストのキー ID を入力します。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**：NTPキーの認証タイプを選択します。
- このキーを信頼したい場合には、**[信頼済み（Trusted）]** チェックボックスをオンにします。信頼できないキーは NTP 認証に使用できません。

NTP認証の要件とガイドラインの完全なリストについては、全般的な前提条件とガイドライン（11 ページ） を参照してください。

追加のNTPキーを入力する場合は、 **[+ キーの追加（+ Add Key）]** を再度クリックして、情報を入力します。

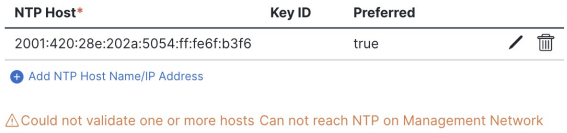
f) NTP認証を有効にした場合は、 **[+ NTP ホスト名/ IPアドレスの追加（+Add NTP Host Name/ IP Address）]**をクリックし、必要な情報を入力し、チェックマークアイコンをクリックして情報を保存します。

- **NTP ホスト**：IPアドレスを入力する必要があります。完全修飾ドメイン名（FQDN）はサポートされていません。
- **キー ID**：前のサブステップで定義した NTP キーのキー ID を入力します。

  NTP 認証が無効になっている場合、このフィールドはグレー表示されます。
- このホストを優先したい場合は、**[優先（Preferred）]** チェックボックスをオンにします。

（注）

ログインしているノードに IPv4 アドレスのみが設定されているが、前の手順で **[IPv6 を有効にする（Enable IPv6）]** をオンにして NTP サーバーの IPv6 アドレスを指定した場合は、次の検証エラーが表示されます。



これは、ノードに IPv6 アドレスがまだなく、NTP サーバーの IPv6 アドレスに接続できないためです。次の手順で IPv6 アドレスを入力します。この場合、次の手順の説明に従って他の必要な情報の入力を完了し、**[次へ（Next）]** をクリックして次の画面に進み、ノードの IPv6 アドレスを入力します。

追加の NTP サーバーを入力する場合は、**[+ Add NTP Host Name/IP Address）]** を再度クリックし、情報を入力します。

g) **[プロキシ サーバー（Proxy Server）]** について、プロキシ サーバーの URL または IP アドレスを入力します。

Cisco Cloud に直接接続できないクラスタの場合は、接続を確立するためにプロキシ サーバを構成することをお勧めします。これにより、ファブリック内の非適合ハードウェアおよびソフトウェアにさらされるリスクを軽減できます。

+Add Ignore Host をクリックして、トラフィックがプロキシの使用をスキップする 1 つ以上の接続先 IP アドレスを入力します。

プロキシ サーバーでは、次の URL が有効になっている必要があります：

```
dcappcenter.cisco.com
svc.intersight.com
svc.ucs-connect.com
svc-static1.intersight.com
svc-static1.ucs-connect.com
```

プロキシを構成しない場合は、**[プロキシをスキップ（Skip Proxy）]**をクリックして、**[確認（Confirm）]** をクリックします。

h) （任意）プロキシサーバーで認証が必要な場合は、**[プロキシに必要な認証（Authentication required for Proxy）]** をオンにして、ログイン資格情報を指定します。

i) （任意）**[詳細設定（Advanced Settings）]** カテゴリを展開し、必要に応じて設定を変更します。

詳細設定では、次の設定を行うことができます。

- **アプリ ネットワーク**：Nexus Dashboard でアプリケーションで使用されるアドレス空間です。ターゲット ネットワークの IP アドレスとネットマスクを入力します。
- **サービス ネットワーク**：Nexus Dashboard とそのプロセスで使用される内部ネットワークです。ターゲット ネットワークの IP アドレスとネットマスクを入力します。
- **[アプリ ネットワーク IPv6（App Network IPv6）]**：先ほど **[IPv6 の有効化（Enable IPv6）]** チェックボックスをオンにした場合は、アプリ ネットワークの IPv6 サブネットを入力します。

- **[サービス ネットワーク IPv6（Service Network IPv6）]**：先ほど **[IPv6 を有効にする（Enable IPv6）]** チェックボックスをオンにした場合は、サービス ネットワークの IPv6 サブネットを入力します。

アプリケーションおよびサービス ネットワークの詳細については、全般的な前提条件とガイドライン （11 ページ） を参照してください。

j) [次へ（Next）] をクリックします。

ステップ 13 **[ノードの詳細（Node Details）]** ページで、最初のノードの情報を更新します。

前の手順の初期ノード構成時に現在ログインしているノードの管理ネットワークと IP アドレスを定義しましたが、他のプライマリ ノードを追加し、クラスタを作成する進む前に、ノードのデータ ネットワーク情報も指定する必要があります。

a) **クラスタ接続** について、クラスタが L3 HAモードで展開されている場合は、**BGP** を選択します。それ以外の場合は、 **L2**を選択します。

テレメトリで使用される永続的な IP アドレス機能には、BGP 構成が必要です。この機能については、BGP 構成と永続的な IP アドレス （59 ページ） と『*Cisco Nexus Dashboard* ユーザーガイド』の「永続的な IP アドレス」セクションで詳しく説明されています。

（注）
BGP をこの時点で、またはクラスタの展開後に Nexus ダッシュボード GUI で有効にすることができます。BGP が構成されている場合は、残りのすべてのノードで BGP を構成する必要があります。ノードのデータネットワークに異なるサブネットがある場合は、ここで BGP を有効にする必要があります。

b) 最初のノードの横にある **[編集（Edit）]**ボタンをクリックします。

ノードの**[シリアル番号（Serial Number）]**、**[管理ネットワーク（Management Network）]**情報、および**[タイプ（Type）]**が自動的に入力されます。ただし、他の情報は入力する必要があります。

c) **[名前（Name）]**に、サービス ノードのノード名を入力します。

ノードの **名前** はホスト名として設定されるため、 RFC-1123 の要件に従う必要があります。

（注）
[名前（Name）]フィールドが編集できない場合には、CIMC の検証を再度実行して、この問題を修正してください。

d) **[タイプ（Type）]**で、 **[プライマリ（Primary）]**を選択します。

クラスタの最初のノードは **[プライマリ（Primary）]** に設定する必要があります。より大規模なスケールを有効にする必要がある場合は、後の手順でセカンダリ ノードを追加します。

e) **[データ ネットワーク（Data Network）]** エリアで、ノードのデータ ネットワークを入力します。

データ ネットワークの IP アドレス、ネットマスク、およびゲートウェイを入力します。オプションで、ネットワークの VLAN ID を指定することもできます。構成に VLAN が不要な場合は、 [VLAN ID] フィールドを空白のままにします。**データ接続** に **BGP** を選択した場合は、 ASNを入力します。

前のページで IPv6 機能を有効にした場合は、IPv6 アドレス、ネットマスク、およびゲートウェイも入力する必要があります。

（注）
IPv6 情報を提供する場合は、クラスタ ブートストラップ プロセス中に行う必要があります。後で IP アドレス構成を変更するには、クラスタを再展開する必要があります。

クラスタ内のすべてのノードは、 IPv4 のみ、IPv6 のみ、またはデュアル スタック IPv4/IPv6 のいずれかで構成する必要があります。

f) **クラスタ接続** に **BGP** を選択した場合は、 **[BGP ピアの詳細（BGP peer details）]** 領域で、ピアの IPv4 アドレスとASNを入力します。

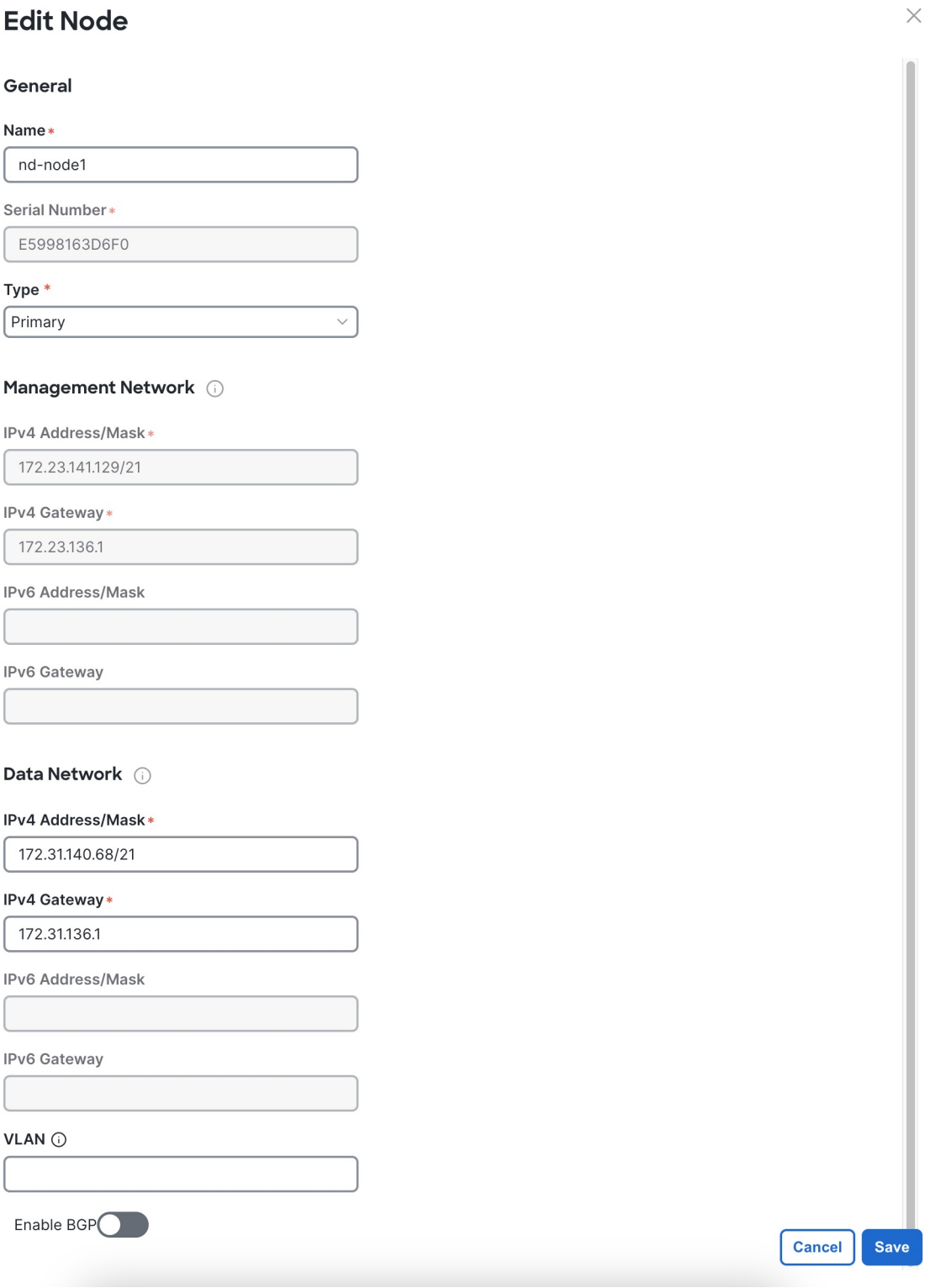
[+ IPv4 BGP ピアの追加（+ Add IPv4 BGP peer）] をクリックして、ピアを追加できます。

前のページで IPv6 機能を有効にした場合は、ピアの IPv6 アドレスと ASN も入力する必要があります。

g) **[Save]**をクリックして、変更内容を保存します。

ステップ 14 [**ノードの詳細（Node Details**）] 画面で、[**ノードの追加（Add Node**）] をクリックして、クラスタに 2 番目のノードを追加します。

単一ノード クラスタを展開する場合は、この手順をスキップします。



a) **[展開の詳細（Deployment Details）]** エリアで、2 番目のノードに **[管理 IP アドレス（Management IP Address）]** および **[パスワード（Password）]** を指定します。

ノードの初期構成手順で、管理ネットワーク情報とパスワードを定義しました。

b) **[検証（Validate）]** をクリックして、ノードへの接続を確認します。

接続が検証されると、ノードの**シリアル番号**と**管理ネットワーク**情報が自動的に入力されます。

c) ノードの **[名前（Name）]** を入力します。

d) **[タイプ（Type）]** ドロップダウンから `[プライマリ（Primary）]` を選択します。

クラスタの最初の 3 つのノードは `[プライマリ（ Primary）]` に設定する必要があります。より大規模なスケールを有効にする必要がある場合は、後の手順でセカンダリ ノードを追加します。

e) **[データ ネットワーク（Data Network）]** エリアで、ノードの**データ ネットワーク**を提供します。

データ ネットワークの IP アドレス、ネットマスク、およびゲートウェイを指定する必要があります。オプションで、ネットワークの VLAN ID を指定することもできます。ほとんどの導入では、[VLAN ID] フィールドを空白のままにできます。

前の画面で IPv6 機能を有効にした場合は、IPv6 アドレス、ネットマスク、およびゲートウェイも入力する必要があります。

（注）
IPv6 情報を提供する場合は、クラスタ ブートストラップ プロセス中に行う必要があります。後で IP 構成を変更するには、クラスタを再展開する必要があります。

クラスタ内のすべてのノードは、 IPv4 のみ、IPv6 のみ、またはデュアル スタック IPv4/IPv6 のいずれかで構成する必要があります。

f) （オプション）クラスタが L3 HA モードで展開されている場合は、データ ネットワークの **[BGP を有効にする（Enable BGP）]** をオンにします。

永続 IP アドレス機能には BGP 設定が必要です。この機能については、BGP 構成と永続的な IP アドレス （59 ページ） と『*Cisco Nexus Dashboard* ユーザーガイド』の「永続的な IP アドレス」セクションで詳しく説明されています。

（注）
BGP をこの時点で、またはクラスタの展開後に Nexus ダッシュボード GUI で有効にすることができます。

BGP を有効にする際、次の情報も入力する必要があります。

- このノードの **ASN**（BGP 自律システム番号）。

  すべてのノードに同じ ASN を構成することも、ノードごとに異なる ASN を構成することもできます。

- 純粋な IPv6 の場合、このノードの**ルータ ID**。

  ルータ ID は、`1.1.1.1` などの IPv4 アドレスである必要があります。

- ピアの IPv4 または IPv6 アドレスとピアの ASN を含む **BGP ピアの詳細**。

g) **[Save]**をクリックして、変更内容を保存します。

h) クラスタの最後の（3 番目の）プライマリ ノードでこの手順を繰り返します。

ステップ 15 **[ノードの詳細（Node Details）]** ページで、入力した情報を確認してから、**[次へ（Next）]**をクリックします。

ステップ 16 クラスタの**展開モード**を選択します。

a) **[永続的サービスIP/プールの追加]** をクリックして、必要な永続的IPアドレスを指定します。

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 （51 ページ）のセクションを参照してください：

b) [次へ（Next）] をクリックして続行します。

ステップ 17 **[サマリー（Summary）]** 画面で設定情報を見直して確認し、**[保存（Save）]** をクリックしてクラスタを構築します。

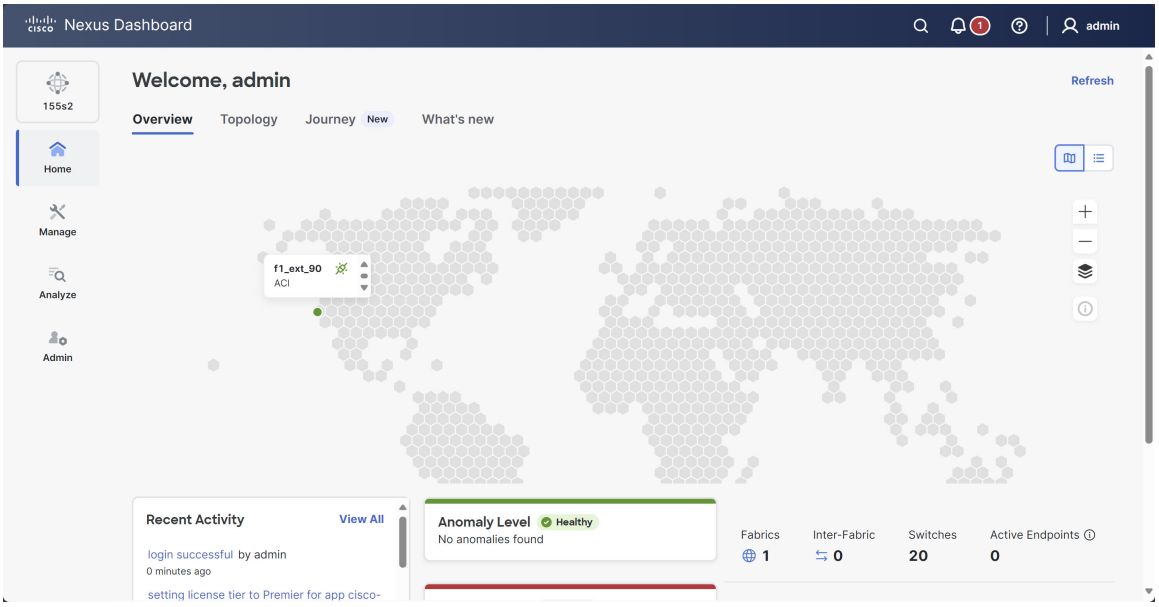
ノードのブート ストラップとクラスタの起動中に、全体的な進捗状況と各ノードの個々の進捗状況がUIに表示されます。ブートストラップの進行状況が表示されない場合は、ブラウザでページを手動で更新し、ステータスを更新してください。

クラスタが形成され、すべてのサービスが開始されるまでに最大30分かかる場合があります。クラスタの設定が完了すると、ページが Nexus ダッシュボード GUI にリロードされます。

ステップ 18 クラスタが健全であることを検証します。

クラスタが使用可能になったら、ノードの管理 IP アドレスのいずれかを参照してアクセスできます。`admin` ユーザーのデフォルト パスワードは、最初のノードに選択した `rescue-user` のパスワードと同じです。この間、UI は上部に「サービスのインストールが進行中です。Nexus Dashboard の設定タスクは現在無効になっています」という意味のバナーを表示します。

すべてのクラスタが展開され、すべてのサービスが開始されたら**[ホーム（Home）]**>**[概要（Overview）]** ページの **異常レベル（Anomaly Level）** でクラスタが正常であることを確認できます。



または、SSH を使用し、`rescue-user` として、ノード展開中に入力したパスワードを使っていずれかのノードにログインし、`acs health` コマンドを実行してクラスタの状態を確認できます。

- クラスタが収束している間、次の出力が表示されることがあります：

```
$ acs health
k8s install is in-progress

$ acs health
k8s services not in desired state - [...]

$ acs health
k8s: Etcd cluster is not ready
```

- クラスタが稼働している場合は、次の出力が表示されます。

```
$ acs health
All components are healthy
```

（注）
場合によっては、ノードの電源を再投入（電源をオフにしてから再度オン）すると、この段階でスタックが停止することがある可能性があります。

```
deploy base system services
```

これは、pND（物理 Nexus Dashboard）クラスタの再起動後のノードの `etcd` の問題が原因です。

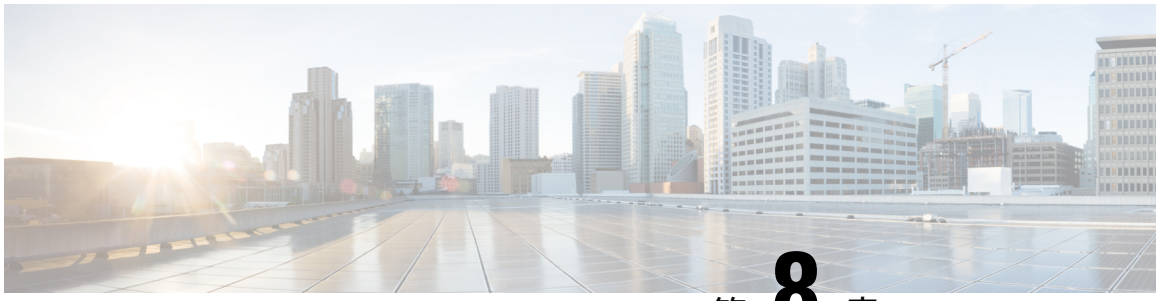
この問題を解決するには、影響を受けるノードで `acs reboot clean` コマンドを入力します。

ステップ 19 （オプション） Cisco Nexus DashboardクラスターをCisco Intersightに接続、可視性と利点を強化します。詳細な手順については、 「*Cisco Intersightの操作*」 を参照してください。

ステップ 20 Nexus Dashboardを展開した後、設定情報については、このリリースのコレクションページを参照してください。

次のタスク

次のタスクは、ファブリックとファブリック グループを作成することです。 Cisco Nexus Dashboardのコレクション ページ にある、このリリースの 「ファブリックとファブリック グループの作成」の記事を参照してください。



第 8 章

Amazon Web Services（AWS）での仮想 Nexus Dashboard（vND）の展開

AWS パブリッククラウドでの vND のホスティングについて

この機能を使用すると、AWS パブリッククラウドで仮想 Nexus Dashboard（vND）を実行できます。このソリューションのコンポーネントは次のとおりです。

- Virtual Nexus Dashboard
- Nexus 9000 スイッチ
- 2 つの Catalyst 8000 シリーズ ルータ、または Nexus ダッシュボードが vND からオンプレミス データセンターへの VXLAN トンネルを終端して永続 IP アドレス（PIP）トラフィックに使用できる別のタイプのデバイス（Nexus 9000 スイッチなど）
- AWS パブリック クラウド アカウント

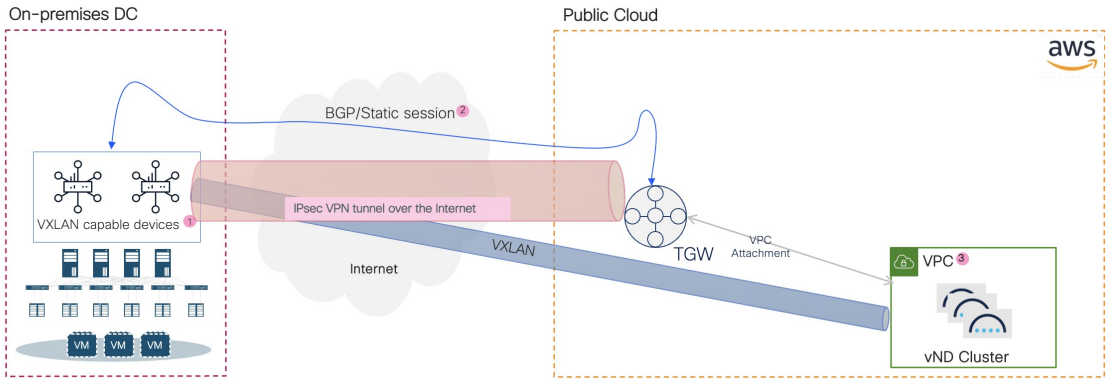
AWS パブリック クラウドでの vND の展開方法を理解する

AWS パブリッククラウドに vND を展開する場合、手動でのブートストラップは不要です。代わりに、Nexus Dashboard のブートストラップが自動的にブートストラップを実行します。AWS パブリッククラウドで vND デプロイメントプロセスを完了すると、仮想プライベートクラウド（VPC）の 3 つの可用性ゾーン（AZ）にわたる、可用性の高い 3 ノードクラスターが自動的に作成されます。Nexus Dashboard GUIで、**[管理（Administration）] [** > **システムステータ**

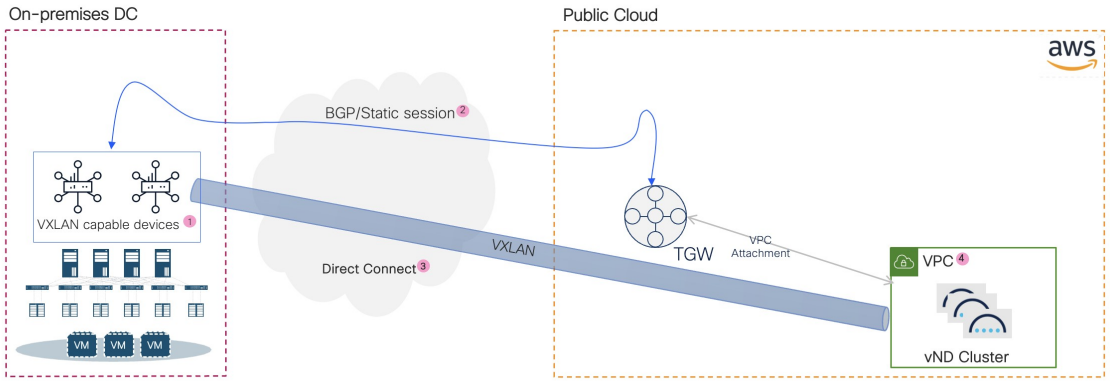
ス（System Status）]>[概要（Overview）]に移動し、[クラスタノード（Cluster nodes）]領域での 3 ノードクラスターに関する情報を表示します。

トポロジの例

次の図は、トポロジの例を示しています。



1 On-premises device with VXLAN support for example, Catalyst 8000 series router, Nexus 9000
2 BGP / static session for ND data IP reachability
3 VPC in AWS terminology stands for virtual private cloud and is an equivalent of VRF



1 On-premises device with VXLAN support for example, Catalyst 8000 series router, Nexus 9000
2 BGP / static session for ND data IP reachability
3 Direct connect takes the role of a private transport for carrying data
4 VPC in AWS terminology stands for virtual private cloud and is an equivalent of VRF

ここで、

- オンプレミスのデータセンターと AWS パブリッククラウドの間の接続は、直接接続（実稼働環境に推奨）または 2 つの間の IPSec トンネル（追加のオーバーヘッドとして PoC またはラボ用）のいずれかを使用して実現されます。
- 2 つのオンプレミスルータは、次のいずれかになります。
  - 直接接続を使用する場合は、 Nexus 9000 スイッチなどの 2 つの物理スイッチを使用できます。

- IPSec トンネルを使用している場合、この場合は VXLAN トンネルを終端するため、VXLAN サポートが有効な Cisco 8000 ファミリのネットワーク アプライアンスを使用できます。

- トランジット ゲートウェイは、Nexus Dashboard ノードをホストする VPC（アプリ VPC）に接続するためのトランジット ゲートウェイ アタッチメントと、トランジット ゲートウェイで終端する別のトランジット ゲートウェイ添付ファイル、VPN 添付ファイルまたはルータを作成するために使用されます。

（注） Catalyst 8000V（C8000V）は、シスコ クラウド サービス ルータ（CSR）1000V の進化型としてリリースされました。このドキュメントでは、C8000V を VXLAN 対応エッジ デバイスの例として使用します。詳細については、*Cisco Catalyst 8000V Edge* ソフトウェアのリリース ノートを参照してください。

Amazon Web Services で Nexus Dashboard クラスタを展開するための前提条件と注意事項

Amazon Web Services（AWS）で仮想 Nexus Dashboard クラスタを展開する前に、次の手順を実行する必要があります。

（注） AWS でサポートされる vND タイプは、32vCPU、128G RAM、3TB SSD （GP3）、および 10G のネットワーク スループットのみの vND データです。

- この機能は、単一の製品としてNexus Dashboard を備えた AWS の 3ノード仮想クラスタ（データ）でサポートされています（IPv4 のみ）。
- この機能では、NX- OSファブリックのみがサポートされます。また、次の機能が有効になっている場合のみサポートされます。
  - コントローラ
  - テレメトリ、次の制限あり：
    - アウトオブバンドのみ
    - トラフィック分析、ただしフロー テレメトリなし

  オーケストレーション機能は、この機能ではサポートされていません。
- この機能は、LAN ファブリックでのみサポートされています。メディア用の IP ファブリック（IPFM）または SAN ファブリックではサポートされません。

（注） AI ファブリックは LAN ファブリックと見なされます。AWS の vND でのこのタイプのファブリックの展開は、ソリューションの観点からは制限されていません。AI ファブリックの基本的な要件は、デバイスと vND 間の遅延が50 ミリ秒を超えないようにすることです。

- セカンダリ/ワーカーノードは、この機能ではサポートされていません。3 つのプライマリ ノードと 1 つのスタンバイ ノードのみがサポートされます。
- クラスターあたりのスケール：単一の 3 ノード vNDクラスター上で 100 個のスイッチ
- AWS に vND を展開した後は、トンネルエンドポイントに割り当てられた IP アドレスまたは VNI を変更することはできません。
- Nexus Dashboard vND を展開する前に、オンプレミス サイトを準備して、Catalyst 8000 シリーズ ルータまたはNexus 9000 スイッチのペアを展開しておくことがベストです。これにより、Nexus Dashboard vND のデプロイメントの間に、必要な BDI と TEP IP アドレスを提供できます。必要に応じて、 Nexus Dashboard vND を展開した後にオンプレミス ネットワーク アプライアンスを展開できますが、その場合、 Nexus Dashboard vND のデプロイメント時に提供したのと同じ情報を使用してオンプレミスデバイスを設定する必要があります。両方の場所で同じ設定情報を提供しない場合は、 Nexus Dashboard vNDを再インストールする必要があります。
- オンプレミスの VXLAN 対応デバイスが正しく構成されていることを確認します。
  - データプレーン：入力レプリケーション
  - コントロールプレーン：フラッディングと学習
- ファクターから AWS が拡張性とサービス要件をサポートしていることを確認します。

  クラスタ フォーム ファクタに基づいて、拡張性とサービス サポートおよび共同ホストは異なります。Nexus ダッシュボード キャパシティ プラン ツールを使用して、仮想フォーム ファクタが展開要件を満たすことを確認できます。
- 全般的な前提条件とガイドライン （11 ページ） に記載されている一般的な前提条件を確認して完了します。
- 展開する予定のサービスのリリース ノートに記載されている追加の前提条件を確認して完了します。
- AWS アカウントに適切なアクセス権限があること。

  Nexus ダッシュボード クラスタをホストするには、複数の Elastic Compute Cloud（`m5.8xlarge`）のインスタンスを起動できる必要があります。
- Nexus ダッシュボード VM に使用される CPU ファミリが AVX 命令セットをサポートしていることを確認します。

- Nexus Dashboard クラスタ向け Amazon Web サービスの準備 （145 ページ）の手順を実行します。

Nexus Dashboard クラスタ向け Amazon Web サービスの準備

Nexus Dashboard vND をAmazon Web Services（AWS）に展開する前に、次の前提条件に従ってAWS を展開できるように準備します。

- AWS とその仕組みについて理解してください。
- （オプション）AWS とオンプレミスのデータセンター間の接続（理想的には、直接接続）を確立します。
- Nexus ダッシュボード ノードのデプロイメントに使用するリージョンを特定します。
- このデプロイメントに使用する既存の VPC を選択するか、新しい VPC を作成します。
- 外部アクセスを有効化します、

  これは、Elastic IP アドレスを vND 管理インターフェイスにマッピングし、 GUI と SSH に外部からアクセスするために必要です。選択した接続方法に応じて、外部アクセスを有効にするためにインターネット ゲートウェイを作成して VPC に接続する必要がある場合と、不要な場合があります。

  - **Option 1**：イーサネットインターフェイスプロセッサ（EIP）を使用して管理インターフェイスを接続します。この場合は、インターネット ゲートウェイが必要です。
  - **Option 2**：プライベート IP アドレスを使用します。この場合、インターネットゲートウェイは必要ありません。

- セキュリティ グループを更新して、次のような必要なサービスにパブリック IP アドレスまたは範囲からアクセスできるようにします。

  - HTTPS（TCP ポート 443）：Nexus Dashboard GUI にアクセスする場合
  - SSH（TCPポート 22）：vND ノードへセキュアなリモート ログインを行う場合

  これは、 GUI と SSH にアクセスして Nexus Dashboard ノードにアクセスできるようにするために必要です。

- 6 つのサブネットを作成します：

  - ノードごとに管理用のサブネット 1 セット（3）：最小 /28
  - ノードごとにデータ用のサブネット 1 セット（3）：最小 /28

  特定のノードの管理とデータのサブネットは、同じ可用性ゾーンに存在する必要があります。

- vND のデプロイメントに使用可能な十分な AWS Elastic IPアドレス があることを確認します。

  このインストールでは、ノードごとに 1 つずつ、合計 3 つの AWS Elastic IP アドレスが必要です。各 AWS Elastic IP アドレスは、vND UI やSSH へのアクセスなど、管理サービスにアクセスするために使用されます。

- 管理サブネットの IP アドレスは、デプロイメントの一部として AWS Elastic IP アドレスにマッピングされるため、これらの管理サブネットには外部アクセスが必要です。データサブネットは、vNDからVXLANトンネル（永続的なポッドによって使用される）の終端に使用されるオンプレミスのデバイスおよびオンプレミスの Catalyst 8000 シリーズ ルータ（または Nexus 9000 スイッチなどの他のデバイス）に到達できる必要があります。

- AWS によって所有されておらず、PIP（永続的な IP アドレス）によって使用されるオンプレミスのデータセンター（ただしまだ使用されていない）から取得される /28（100.100.100.0/28 など）のサブネット 1 つ。ここでそのサブネットの 100.100.100.1 と 100.100.100.2 は、オンプレミス データセンター デバイス（Catalyst 8000 または Nexus 9000 スイッチ）の BDI IP アドレスである必要があり、残りの IP アドレスは vND 永続ポッド（トラップ、テレメトリコレクタなど）によって使用されます。

- 適切に機能させるために、オンプレミスデバイスはこれらの永続的 IP アドレスと Nexus ダッシュボード データ IP アドレスに到達できる必要があります。

- vND ノードが相互に通信してクラスターを形成し、外部およびオンプレミスのデバイスと通信できるように、必要なすべての IP アドレスとポートを使用してセキュリティ グループを作成します。

- デプロイメント用に 1 つの EC2 キーペアを設定します。

（注） 前提条件の一部としてこの設定を完了します。ただし、EC2 キーペアは現在使用されておらず、現時点でサポートされているオプションはユーザー/パスワードのみです。

Amazon Web Services（AWS）に仮想 Nexus Dashboard（vND）を展開する

ここでは、Amazon Web Services (AWS) で仮想 Nexus Dashboard（vND）を展開する方法について説明します。

始める前に

- Amazon Web Services で Nexus Dashboard クラスタを展開するための前提条件と注意事項（143 ページ） に記載されている要件とガイドラインを満たしていることを確認します。

手順

ステップ 1 AWS Marketplace で Cisco Nexus ダッシュボード製品に登録します。

a) AWS アカウントにログインし、AWS Management Console に移動します。

管理コンソールは https://console.aws.amazon.com/ で入手できます。

b) **[サービス]** > **[AWS マーケットプレイス サブスクリプション（Services AWS Marketplace Subscriptions）]**に移動します。

c) **[サブスクリプションの管理（Manage Subscriptions）]** をクリックします。

d) **[製品の検出（Discover products）]** をクリックします。

e) **Cisco Nexus Dashboard - Cloud**を検索し、結果をクリックします。

f) **[購入の表示（View Purchase）]** オプションをクリックし、 **[登録（Subscribe）]**まで下にスクロールしてクリックします。

g) 製品ページで、 **[サブスクリプションの表示（View subscription）]**をクリックします。

h) **[サブスクリプションの管理（Manage subscriptions）]** ページで、 **[Cisco Nexus Dashboard-Cloud（Cisco Nexus Dashboard - Cloud）]**の行を見つけ、その行で **[起動（Launch）]** をクリックします。

ステップ 2 ソフトウェア オプションと地域を選択します。

a) **[Cisco Nexus Dashboard - Cloud]** の **[このソフトウェアを構成する（Configure this software）]**ページで、次を選択します。

- **履行オプション（Fulfillment option）** ：デフォルトの [**Nexus Dashboard - Cloud Deployment）]** の 選択をそのままにします。
- **ソフトウェア バージョン**：ドロップダウンリストから使用可能な最新の 4.1.1 オプションを選択します。
- **リージョン**：テンプレートを展開する適切なリージョンを選択します。

  これは、VPC を作成したのと同じリージョンである必要があります。

b) **[続行して起動する（Continue to Launch）]** をクリックします

c) **[Cisco Nexus Dashboard - Cloud]** の [**このソフトウェアの起動（Launch this software）]**ページで、**[アクションの選択（Choose Action）]** フィールドを見つけ、ドロップダウン リストから **[CloudFormation の起動（Launch CloudFormation）]** を選択して、 **[起動（Launch）]**をクリックします。

[Create Stack（スタックの作成）] ページが表示されます。

ステップ 3 スタック設定を完了します。

a) **[スタックの作成（Create stack）]** ページのオプションはそのままにします。

（注）
提供されているテンプレートに変更を加えないでください。スマート デフォルト テンプレート構成を使用することによってのみ、クラスタを正常に形成できます。

- **前提条件 -テンプレートを準備**：「既存のテンプレートを選択（Choose an existing template）」オプションを「そのまま」にします。
- **[テンプレートの指定（Specify Template）]**：[Amazon S3 URL] オプションはそのままにします。
- **Amazon S3 URL**：事前設定された URL エントリをそのままにします。

b) [**次へ（Next）**] をクリックして続行します。

[スタック詳細の指定（Specify stack details）] ページが表示されます。

ステップ 4 スタックの詳細を指定します。

a) **スタック名**を入力します。

b) **[パラメータ（Parameters）]** 領域に表示される情報を確認し、必要に応じて変更を加えます。

ほとんどの場合、この vND CFT の一部である構成に基づいて、事前に入力されたフィールドをそのままにすることができます。

- **[Nexus Dashboard クラスタ名（Nexus Dashboard Cluster Name）]** フィールドに、クラスタ名を入力します。
- **[ファブリック展開モード（Fabric Deployment Mode）]** フィールドで、デフォルトの**[LAN]** オプションは、 Nexus Dashboard 4.1.1 リリースでサポートされている唯一のオプションです。
- **[VPC 識別子（VPC identifier）]**フィールドに、VPC 識別子を入力します。

  アプリケーションの VPC がこのフィールドに自動的に入力されます。このフィールドの VPC を変更する場合は、次で別の VPC を選択します： **VPC dashboard** > **[仮想プライベート クラウド（Virtual private cloud）]** > **[使用中の VPC（Your VPCs）]**
- **[セキュリティ グループ ID（Security Group Identifier）]** フィールドに、セキュリティグループ IDを入力します。

  これは事前に作成されたセキュリティ グループで、ポート 22 および 443 への入力アクセスを許可する必要があります。
- **[インスタンス タイプ（Instance Type）]**フィールドで、ノード インスタンスの EC2 インスタンス タイプを指定します。
- **[AMI ID（AMI Identifier）]**フィールドで、Nexus Dashboard の AWS AMI を指定します。
- **[パスワード（Password）]** フィールドに、 Nexus Dashboard ノードの管理者パスワードを入力します。

  Nexus Dashboard ノードの管理者パスワードには、少なくとも 1 つの文字、数字、特殊文字（@$!%*#?&）を含める必要があり、長さは 8～64 文字にする必要があります。
- （オプション）**キーペア名（Key Pair Name）** フィールドで、 Nexus Dashboard への SSH アクセスを有効にする既存の SSH キーペアの名前を指定します。

c) **[DNS 構成（DNS Configuration）]** エリアで、必要に応じて設定情報を入力します。

- **[プライマリ DNS サーバー IP'（Primary DNS Server IP）]**フィールドに、プライマリ DNS サーバーの IP アドレスを入力します。
- **[セカンダリ DNS サーバー IP（Secondary DNS Server IP）]** フィールドに、セカンダリ DNS サーバーの IP アドレスを入力します。
- **[検索ドメイン名（Search Domain Name）]** フィールドに、検索ドメイン名を入力します。

d) (オプション) **[プロキシの設定（Proxy Configuration）]** エリアに必要な情報を入力します。

- **[プロキシ タイプ（Proxy Type）]**フィールドで、プロキシタイプ（ HTTP や HTTPS など）を指定します。
- **[プロキシ URL（Proxy URL）]** フィールドに、プロトコルとポートを含む完全なプロキシ URL を指定します。例：`http://proxy.example.com:8080`。
- **[プロキシ ユーザー名（Proxy Username）]** フィールドで、認証が必要な場合はプロキシのユーザー名を指定します。
- **[プロキシ パスワード（Proxy Password）]** 認証が必要な場合は、 フィールドでプロキシ パスワードを指定します。
- **[プロキシ無視ホスト IP（Proxy Ignore Hosts IP）]**フィールドで、プロキシが無視するホスト IP アドレスを指定します。

  このフィールドには 1 つのエントリのみが許可されます（たとえば、192.168.10.101）。

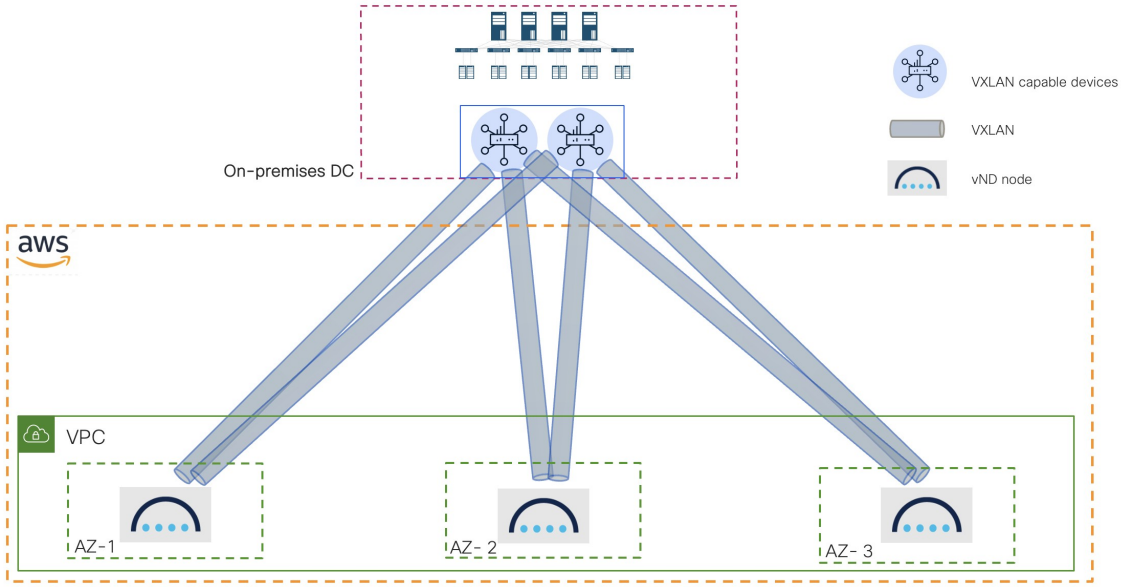
e) **[NTP 構成（NTP Configuration）]**エリアで、必要に応じて設定情報を入力します。

- **[NTP サーバー ホスト（NTP Server Host）]**フィールドで、NTP サーバー ホストを指定します。
- **[NTP サーバー キー識別子（NTP Server Key Identifier）]** フィールドで、 NTPサーバーキー識別子を指定します。
- **[NTPサーバー優先（NTP Server Preferred）]** フィールドで、サーバーが優先される場合は `true` を選択します。
- **[NTP キー識別子（NTP Key Identifier）]** フィールドで、NTP キーの識別子を指定します。
- **[NTP キー（NTP Key）]**フィールドで、 NTP キーのキーを指定します。
- **[NTP キー認証（NTP Key Authentication Type）]**フィールドで、 NTP キーの認証タイプ（MDS や SHA1 など）を指定します。
- **[信頼されている NTP キー（NTP Key Trusted）]** フィールドで、 NTP キーが信頼できるかどうかを `true` または `false` で指定します。

f) **[Cisco VXLAN 対応デバイス（Cisco VXLAN Capable Device）]** 領域に必要な情報を入力します。

- **[デバイス VXLAN ID（Device VXLAN Identifier） (VNI)]** フィールドに、Cisco VXLAN 対応デバイス（IPSec トンネルを使用している場合）または Nexus 9000 スイッチ（直接接続を使用している場合）と Nexus Dashboard ノード間のVXLAN トンネルに使用する VNI 値を入力します。

この図に示すように、Cisco VXLAN 対応デバイスと Nexus Dashboard ノード（vND）間のすべての VXLAN トンネルに単一の VNI 値が使用されます。



- **[デバイス 1 ブリッジ ドメイン IP（Device 1 Bridge Domain IP）]** および **[デバイス 2 ブリッジ ドメイン IP（Device 2 Bridge Domain IP）]** フィールドに、両方の Cisco VXLAN 対応デバイスのブリッジ ドメイン IP アドレスを入力します。

  デバイスのブリッジドメイン IP アドレスは、**[Nexus Dashboard ポッドで使用されるプライベート IP サブネット（Private IP Subnet for Nexus Dashboard Pods）]** フィールドで指定したサブネットからのものである必要があります：たとえば、**[Nexus Dashboard ポッドのプライベート IP サブネット（Private IP Subnet for Nexus Dashboard Pods）]** フィールドに `100.100.100.0/28` と入力した場合、デバイスのブリッジドメインIPアドレスとして `100.100.100.1` および `100.100.100.2` を入力できます。

- **[デバイス 1 トンネル エンドポイント IP（Device 1 Tunnel Endpoint IP）]** および **[デバイス 2 トンネル エンドポイント IP（Device 2 Tunnel Endpoint IP）]** フィールドに、両方の Cisco VXLAN 対応デバイスのトンネル エンドポイント IP アドレス（データ IP アドレス）を入力します。

- **[Nexus Dashboard ポッドのプライベート IP サブネット（Private IP Subnet for Nexus Dashboard Pods）]** フィールドに、 Nexus Dashboard ポッドで使用されるプライベート IP サブネットを入力します。

  IPサブネットのサイズは、`100.100.100.0/28` である必要があります。

  （注）
  この項のこの手順では、Cisco VXLAN 対応デバイスは展開されません。ルールは、 Nexus Dashboard にエッジデバイスとの接続を確立するために必要なすべての変数があることを確認するだけです。

g) **[Nexus Dashboard ノード 1 構成（Nexus Dashboard Node 1 Configuration）]**、**[Nexus Dashboard ノード 2 構成（Nexus Dashboard Node 2 Configuration）]**、および **[Nexus Dashboard ノード 3 構成（Nexus Dashboard Node 3 Configuration）]** 領域で、クラスタ内の各 vND ノードに必要な情報を入力します。

- **ND ノード *x* ホスト名**：各 Nexus Dashboard ノードのホスト名を入力します。
- **ND ノード *x* 管理サブネット**：各 Nexus Dashboard ノードの最初の管理サブネットを入力します。
- **ND ノード *x* 静的管理 IP**：上記で入力した管理サブネットの静的管理 IP アドレスを、 Nexus Dashboard ノードごとに入力します。

  このフィールドに入力した IP アドレスがまだ使用されていないことを確認します。
- **ND ノード *x* 管理サブネット ネットマスク**：各 Nexus Dashboard ノードの最初の管理サブネット ネットマスクを CIDR 形式（16～28）で入力します。
- **ND ノード *x* 管理サブネット ゲートウェイ**：上記で入力した管理サブネット上の最初の管理デフォルト ゲートウェイを、Nexus Dashboard ノードに対して入力します。

  これは通常、サブネットの最初のアドレスです。
- **ND ノード *x* データ サブネット**：各 Nexus Dashboard ノードの最初のデータ サブネットを入力します。
- **ND ノード *x* 静的データ IP**:：上記で入力した管理サブネットの静的データ IP アドレスを、Nexus Dashboard ノードごとに入力します。

  このフィールドに入力した IP アドレスがまだ使用されていないことを確認します。
- **ND ノード *x* データ サブネット ネットマスク**：各 Nexus Dashboard ノードの最初のデータ サブネット ネットマスクを CIDR 形式（16～28）で入力します。
- **ND ノード *x* データ サブネット ゲートウェイ**：上記で入力した管理サブネット上の最初のデータ デフォルトゲートウェイを、Nexus Dashboard ノードに対して入力します。

  これは通常、サブネットの最初のアドレスです。

h) **[Kubernetes網構成（オプション）（Kubernetes Network Configuration (Optional)）]** 領域で、必要に応じて構成情報を入力します。

- **[Kubernetesサービスネットワーク（Kubernetes Service Network）]** フィールドで、Kubernetes サービス ネットワークのネットワーク アドレスを指定します。

  CIDR 範囲は「/16」固定です。
- **[Kubernetes アプリ ネットワーク（Kubernetes App Network）]** フィールドに、kubernetes アプリ ネットワークのネットワーク アドレスを入力します。

  CIDR 範囲は「/16」固定です。

i) [**次へ（Next）**] をクリックして続行します。

ステップ 5 **[スタック構成オプション（Configure stack options）]** ページで、必要に応じて、このページに記載されている情報を確認および変更します。

a) **[スタック障害オプション（Stack failure options）]** で、**[プロビジョニングの失敗時の動作（Behavior on provisioning failure）]** の選択を [正常にプロビジョニングされたリソースを保持する（**Preserve successfully provisioned resources**）] に変更することをお勧めします。

b) **[スタック オプションの構成（Configure stack opushon ）]** ページで情報の確認または変更が完了したら、**[次へ（Next）]** をクリックします。

ステップ 6 **[確認して作成（Review and create）]** ページで、テンプレート設定情報を確認してから、**[送信（Submit）]** をクリックします。

ステップ 7 展開が完了するのを待ってから、VM を起動します。

[CloudFormation] > **[スタック（Stacks）]** ページでインスタンスの展開のステータス（`CREATE_IN_PROGRESS` など）を表示できます。ページの右上隅にある更新ボタンをクリックすると、ステータスを更新できます。

スタックのステータスが `CREATE_COMPLETE` に変わったら、次の手順に進むことができます。

ステップ 8 **[CloudFormation]** [> **[スタック（Stacks）]** の下のスタックで、**[出力（Outputs）]** タブをクリックして、クラスタ内の 3 つの vND のパブリック IP アドレスを表示します。

（注）
CloudFormation テンプレートは、クラスター内の接続を処理します。すべての変数が正しく入力されている場合、ノードは自動的にクラスターを形成します。

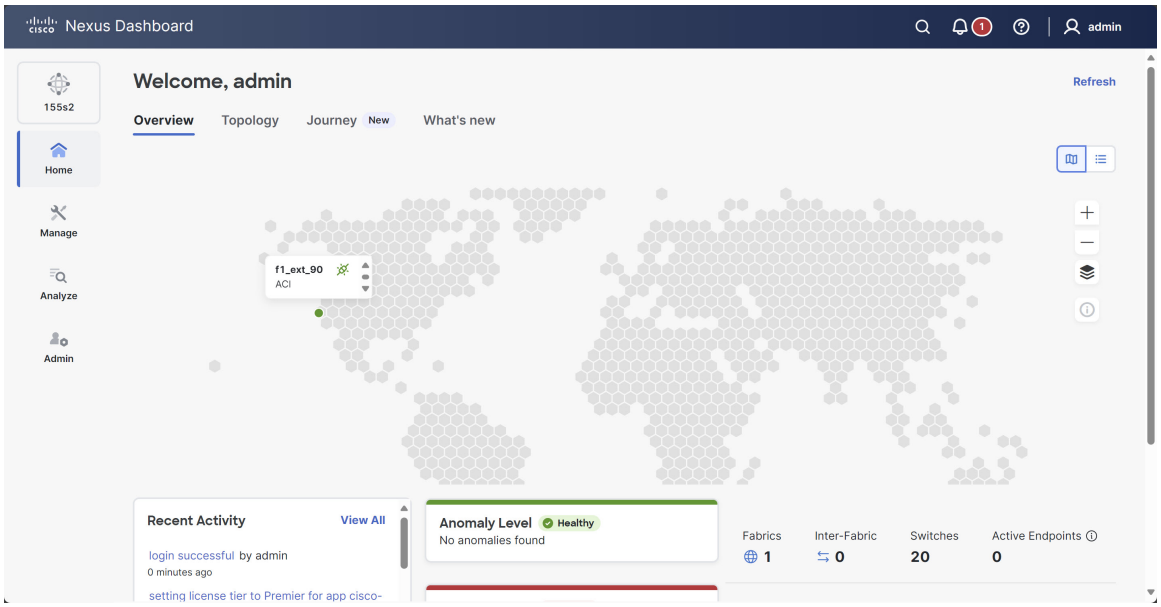
ステップ 9 前の手順にリストされているパブリック IP アドレスのいずれかを使用して、Nexus Dashboard GUI にログインします。

（注）
VM を起動してから、パブリック IP アドレスの 1 つを使用して Nexus Dashboard GUI にログインできるまでに約 40 分かかる場合があります。

ステップ 10 クラスタが健全であることを検証します。

クラスタが使用可能になったら、ノードの管理 IP アドレスのいずれかを参照してアクセスできます。`admin` ユーザーのデフォルト パスワードは、最初のノードに選択した `rescue-user` のパスワードと同じです。この間、UI は上部に「サービスのインストールが進行中です。Nexus Dashboard の設定タスクは現在無効になっています」という意味のバナーを表示します。

すべてのクラスタが展開され、すべてのサービスが開始されたら **[ホーム（Home）]** > **[概要（Overview）]** ページの **異常レベル（Anomaly Level）** でクラスタが正常であることを確認できます。



または、SSH を使用し、`rescue-user` として、ノード展開中に入力したパスワードを使っていずれかのノードにログインし、`acs health` コマンドを実行してクラスタの状態を確認できます。

- クラスタが収束している間、次の出力が表示されることがあります：

```
$ acs health
k8s install is in-progress
```

```
$ acs health
k8s services not in desired state - [...]
```

```
$ acs health
k8s: Etcd cluster is not ready
```

- クラスタが稼働している場合は、次の出力が表示されます。

```
$ acs health
All components are healthy
```

（注）
場合によっては、ノードの電源を再投入（電源をオフにしてから再度オン）すると、この段階でスタックが停止することがある可能性があります。

```
deploy base system services
```

これは、pND（物理 Nexus Dashboard）クラスタの再起動後のノードの `etcd` の問題が原因です。

この問題を解決するには、影響を受けるノードで `acs reboot clean` コマンドを入力します。

ステップ 11 （オプション） Cisco Nexus DashboardクラスターをCisco Intersightに接続、可視性と利点を強化します。詳細な手順については、 「*Cisco Intersightの操作*」 を参照してください。

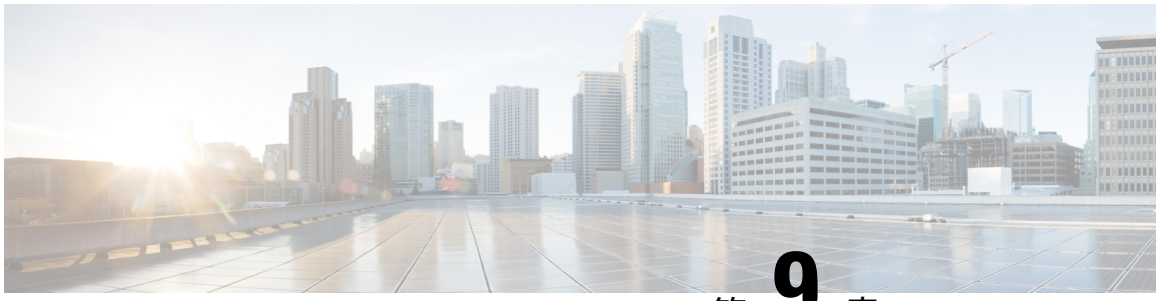
ステップ 12 Nexus Dashboardを展開した後、設定情報については、このリリースのコレクションページを参照してください。

次のタスク

次のタスクは、ファブリックとファブリック グループを作成することです。 Cisco Nexus Dashboardのコレクション ページ にある、このリリースの 「ファブリックとファブリック グループの作成」の記事を参照してください。

第 III 部

このリリースへのアップグレードまたは移行



第 9 章

既存の Nexus Dashboard クラスターのこのリリースへのアップグレード

既存の Nexus Dashbaord クラスターをアップグレードするための前提条件と注意事項

既存のNexusダッシュボードクラスタをアップグレードする前に、次の手順を実行します。

- アップグレードに影響する可能性のある動作、ガイドライン、および問題の変更については、ターゲット リリースのリリース ノートを必ずお読みください。
- Nexus Dashboard リリース 4.1.1 にアップグレードする前に、次の手順を実行します。
  - NTPとDNSサービスが設定されていることを確認します。システムを正常にアップグレードするには、少なくとも 1 つの NTP と DNS が必要です。
  - 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ことを確認する必要があります。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場合にアップグレードは失敗します。
  - Nexus Dashboard のアップグレードを実行する前に、 Nexus Dashboard のアップグレードNexus の検証スクリプトを使用することを強くお勧めします。Nexus Dashboard アップグレード前検証スクリプトは、 Nexus Dashboard のアップグレードの成功に影響を与えることが特定された既知の問題についてさまざまなチェックを実行する Python スクリプトです。スクリプトは継続的に更新され、現場で検出された新しいアップグレード関連の問題を軽減するため、継続的に更新および維持されます。

スクリプト機能および環境での使用方法の詳細については、https://github.com/datacenter/Nexus-Dashboardを参照してください。

- `acs クラスタ`が健全であることを検証します。

  1. `ssh -l rescue-user [management-ip-of-nd]` を使用してNexusダッシュボードにアクセスします。
  2. `acs health` コマンドを発行します。

  `acs health`コマンドからの出力には、すべてのコンポーネントが正常であることが表示されるはずです。

```
rescue-user@node1:~$ acs health
======
Status
======
All components are healthy
```

- アップグレードする前に Nexus Dashboard クラスターのバックアップを実行し、バックアップファイルを安全な場所に保存してください。バックアップを実行するためには、「*Nexus Dashboard* とサービスの統合バックアップおよび復元」 を参照してください。このバックアップを、4.1.1 リリースを実行している Nexus Dashboard クラスターに直接復元することはできないことに注意してください。
- 最新のバックアップに障害が発生していた場合、アップグレードは続行されません。アップグレードを進める前に、正常なバックアップがあることを確認してください。バックアップを正常に実行できず、アップグレードできない場合は、 Cisco Technical Assistance Center （TAC） （TAC） に連絡してサポートを受けてください。
- アプリ全体のプロファイル（1.5 TB ディスク）を使用した Nexus ダッシュボード vND クラスタ（単一ノードまたはマルチノード）のアップグレードはサポートされていません。バックアップから通常のアプリ ノード（16 vCPU/64GB RAM/500GB ディスク）またはデータ ノード（32 vCPU/128GB RAM /3TB ディスク）に Nexus Dashboard クラスタを復元し、クラスタを再度アップグレードします。
- NDI または NDFC のいずれかがあり、NDI がリモートで作成された NDFC クラスタのテレメトリを実行する場合、または複数の ND クラスタとのマルチクラスタ接続がある場合は、すべてのクラスタを Nexus Dashboard 4.1.1 にアップグレードする必要があります。マルチクラスタ接続を使用した Nexus Dashboard リリース 3.2x と 4.1.1 のクラスタの混在はサポートされていません。
- 物理的な Nexus Dashboard クラスタをアップグレードしている場合は、ノードにターゲットの Nexus Dashboard リリースでサポートされている最小の CIMC バージョンがあることを確認してください。

  サポートされている CIMC バージョンは、ターゲット リリースの *Nexus Dashboard* リリース ノート にリストされています。

  CIMC アップグレードについては、Nexus Dashboard ドキュメント ライブラリ の「トラブルシューティング」の記事で詳しく説明されています。

- 仮想 Nexus Dashboard クラスターをアップグレードする場合、 Nexus Dashboard は HDD の遅延のチェックを適用して、<30ms であることを確認します。HDD の遅延がさらに高い場合、アップグレードは失敗します。
- VMware ESX に展開された仮想 Nexus Dashboard クラスタをアップグレードする場合は、ESX のバージョンがターゲット リリースで引き続きサポートされていることを確認します。

  このリリースは、VMware ESXi 7.0、7.0.1、7.0.2、7.0.3、8.0、8.0.2、8.0.3 をサポートしています。

（注） ESX サーバーをアップグレードする必要がある場合は、Nexus Dashboard をターゲット リリースにアップグレードする前に行う必要があります。ESX のアップグレードはこのドキュメントの範囲外ですが、簡単に説明すると次のとおりです。

1. 既存の Nexus Dashboard ノード VM を実行している場合に通常行うように、ESX ホストの 1 つをアップグレードします。
2. ホストがアップグレードされた後、Nexus Dashboard クラスタが正常に動作していることを確認します。
3. 他の ESX ホストで 1 つずつアップグレードを繰り返します。
4. すべての ESX ホストがアップグレードされ、既存の Nexus Dashboard クラスタが正常な状態になったら、このドキュメントの説明に従って、Nexus Dashboard をターゲット リリースにアップグレードします。

- 現在の Nexus ダッシュボードクラスタが正常であることを確認します。

  Nexus ダッシュボードの**管理コンソール（Admin Console）**の **[概要（Overview）]** ページでシステムのステータスを確認するか、`rescue-user` としてノードの1つにログインし、`acs health` コマンドを実行して `All components are healthy` が返ってくることを確認します。
- Nexus Dashboard ではプラットフォームのダウングレードはサポートされていません。

  以前のリリースにダウングレードするには、新しいクラスタを展開する必要があります。
- Nexus Dashboard リリース 3.2.1 で `ダッシュボード ユーザー` （app-user）ユーザーロールのみを持っているユーザーがいる場合は、 Nexus Dashboard リリース 4.1.1 へのアップグレード後に `ダッシュボード ユーザー` ロールを持つユーザーで削除するか、Nexus Dashboard リリース 4.1.1 のユーザーの代わりに`Observer` ロールを使用する必要があります。
- 永続 IP アドレスの数とそれらのマッピング方法は、以前のリリースから Nexus Dashboard リリース 4.1.1 で変更されました。Nexus Dashboardの 永続 IP アドレス （51 ページ）を参照して、以前のリリースで必要だった永続的なIPアドレスの数と、 Nexus Dashboard リリー

ス 4.1.1 にアップグレードする前に必要な永続的なIPアドレスの数で特定の更新を行う必要がある永続的な IP アドレスの数を理解してください。

- サービスを提供する任意のペルソナ、特にNexus Dashboard Fabric Controller（NDFC）とNexus Dashboard Insights（NDI）のNexus Dashboard（NDI）があり、以前のリリース（ND 2.2.x 以下など）から ND 3.2.x にアップグレードしている場合、Elasticsearch（ES）インデックスサイズに関する次の重要な情報に注意してください。

  クラスターが ND 2.2.x 以前に展開され、それ以降にアップグレードされた場合、ND 3.2.x から ND 4.1.1 へのアップグレードにより、時系列データベースのインデックスが作成されている可能性があります。このプロセスでは、サイズがこのクラスターの再インデックス化機能のサイズを超えている場合は、Cisco Technical Assistance Center （TAC） に連絡するように求められます。プロセスが再インデックス化できない場合、UI で提供された`acs recover` コマンドを使用して、失敗後にアップグレードを続行できます。

- マルチクラスタ接続が構成されていて、 Nexus Dashboard リリース 3.2.x システムで NDFC と NDI が同じ場所に配置されており、
  - NDFC が 1 つのクラスターで実行されていて、
  - 別のクラスターで NDI が実行されていた場合、

  Nexus Dashboard リリース 4.1.1 へのアップグレードプロセスを開始する前に、クラスタを切断し、フェデレーションを削除することが必要です。これらの手順については、『*Nexus Dashboard Infrastructure Management*』 の「Disconnecting Clusters」および「Deleting the Federation」の項を参照してください。アップグレードが完了したら、アップグレード後のタスクの一環としてマルチクラスタ接続を再度有効にします。

- 異なるデータ サブネットを持つND リリース 4.1.1 より前のクラスターの一部としてNexus Dashboard Orchestrator を使用している場合は、 Nexus Dashboard リリース 4.1.1 にアップグレードする前に、次の構成を行う必要があります。
  - すべてのノードで BGP 設定を追加します
  - 永続 IP アドレスを追加します

  アップグレード前にこれらの項目を設定していないと、アップグレード中のイメージの検証は失敗します。

アップグレード時の設定のばらつきの自動調整

4.2.(1) より前の NDO リリースから ND リリース 4.1.1 にアップグレードする場合は、マルチステップ アップグレードを実行する必要があります。

1. 最初に 4.2(1) より前の NDO リリースを ND 3.0.1i にアップグレードしてから、『Cisco Nexus Dashboard and Services Deployment and Upgrade Guide, Release 3.2.x』の 「Supported Upgrade Paths」 の項の説明に従って、ND リリース 3.2.x に *Cisco Nexus Dashboard* します。。
2. 次に、この章の説明に従って、ND リリース 3.2.x から ND リリース 4.1.1 にアップグレードします。

4.2(1) より前の NDO リリースを ND リリース 3.2.x にアップグレードすると、アプリケーション テンプレートの構成のばらつきが観察される場合があります。これらのばらつきは、NDO リリース 4.2(1) 以降で、以前のバージョンで管理されていなかった新しいアプリケーション テンプレート オブジェクト プロパティの管理がサポートされているために発生します。NDO 4.2(1) によって管理される新しいプロパティのリストについては、Nexus Dashboard Orchestrator 4.2(1) リリース ノートを参照してください。

ND リリース 4.1.1 は、アップグレード プロセスの一環として構成のばらつきの自動調整をサポートしています。Nexus Dashboard は、テンプレートがファブリックと同期しているかどうかをチェックし、必要に応じて、ファブリック値を Nexus Dashboard にインポートして、ばらつきを自動的に解決します。

4.2(1) より前の NDO バージョンからマルチステップのアップグレードパスに従う場合は、ND リリース 3.2.x で検出されたばらつきを無視して、ND リリース 4.1.1 へのアップグレードを続行することをお勧めします。

ND リリース 4.1.1 へのアップグレード後に残ったばらつきは、手動で解決する必要があります。たとえば、構成されたオブジェクトが複数のファブリックにまたがる拡張テンプレートの一部であり、テンプレートレベルのプロパティに異なるファブリックで構成された異なる値がある場合、自動解決できないばらつきが発生します。

（オプション）6 ノード pND クラスタから 3 ノード pND クラスタへの変換

アップグレード プロセスの一部として 6ノードの pND クラスタを 3 ノードのPND に変換する場合（たとえば、 Nexus Dashboard リリース 3.2.2 で 6ノードのpND **コントローラ** を展開している場合、Nexus Dashboard リリース 4.1.1 ではサポートされていません）、 Nexus Dashboard リリース 4.1.1 にアップグレードする前に、次の手順を使用して Nexus Dashboard リリース 3.2.2 でこの変換を行ってください。

Nexus Dashboard リリース 4.1.1 では 6ノードの pND **テレメトリ**のみの展開がサポートされているため、このオプションの手順はこの場合は必要ありません。

1. Nexus Dashboard リリース 3.2.x で 6ノードpNDクラスターのバックアップを実行します。

   詳細については、「*Nexus Dashboard* とサービスの統合バックアップと復元」の記事を参照してください。

2. 既存のプライマリ ノードとクラスタが正常であることを確認し、1 つずつセカンダリ ノードを削除します。

   1. リリース 3.2.x で実行されているNexus Dashboard で、 **[の管理（Manage）]** > **[ノード（Nodes）]**に移動します。
   2. 削除するセカンダリ ノードをオンにします。
   3. **[アクション（Actions）]** メニューから **[削除（Delete）]** を選択してノードを削除します。
   4. **[概要（Overview）]** > **[プラットフォーム（Platform）]** ビュー に移動し、各セカンダリノードが削除された後、クラスターの正常性ステータスが **[GREEN]** と表示されるまで待ちます。

（注） ノードを削除後、Kafka が安定するまでに最大 30 分かかる場合があります。

5. セカンダリノードを削除した後にクラスターの正常性ステータスが **GREEN** と表示されたら、次のセカンダリノードの削除に進みます。

   各セカンダリノードを1 つずつ削除するプロセスを続行し、クラスターのステータスが **GREEN** になるのを待ってから、次のセカンダリノードの削除に進みます。

3. すべてのセカンダリノードを削除したら、クラスターが正常であることを確認してから、Nexus Dashboard リリース 3.2.x で新しいバックアップを実行します。

   詳細については、「*Nexus Dashboard* とサービスの統合バックアップと復元」の記事を参照してください。

4. この章の手順に従って、クラスタを Nexus Dashboard リリース 3.2.x からリリース 4.1.1 にアップグレードします。

サポートされているアップグレード パス

以前のリリースでは、Nexus Dashboard のデプロイメントの概要 （5 ページ） で説明したとおり、Nexus Dashboard にはプラットフォーム ソフトウェアのみが付属しており、サービスは含まれていませんでした。これらのサービスは、最初のプラットフォームの展開後に個別にダウンロード、インストール、および有効化するようになっていました。加えて、Nexus Dashboard リリース 3.1(1)では、Nexus Dashboard と個々のサービス間のより緊密な結合を実現したため、各サービスの単一バージョンのみがプラットフォームの各バージョンと互換性を持つようになりました。その結果、Nexus Dashboard ソフトウェアの必要最小限のバージョンを使用している限り、プラットフォームと現在有効になっているすべてのサービスの両方を Nexus Dashboard リリース 3.1x と 3.2x に直接アップグレードできるようになっていました。

今では、プラットフォームと個々のサービスが単一の製品に統合されました。つまり、サービスを個別に展開、構成、またはアップグレードする必要がなくなりました。

次の表に、特定の展開の組み合わせに関するシナリオの例をいくつか示します。

表 *15*:

現在の Nexus Dashboard リリース	互換性のあるサービス （フォームファクタとクラスタサイズによっては、これらのサービスの 1 つ以上が現在有効になっている場合があります）	アップグレードのワークフロー
3.2(2)	ファブリック コントローラ：12.2(3) Orchestrator：4.4(2) Insights：6.5(2)	次のセクションの説明に従って、リリース 4.1(1) に直接アップグレードします。 リリース 4.1(1) では、すべてのサービスが単一の Nexus Dashboard 製品に統合されています。
3.2(1)	ファブリック コントローラ：12.2(2) Orchestrator：4.4(1) Insights：6.5(1)	次のセクションの説明に従って、リリース 4.1(1) に直接アップグレードします。 リリース 4.1(1) では、すべてのサービスが単一の Nexus Dashboard 製品に統合されています。
3.1(1)	ファブリックコントローラ：12.2(1) Orchestrator：4.3(x) Insights：6.4(1)	**1.** 『*Nexus Dashboard* 展開ガイド、リリース *3.2.x*』の説明に従って、Nexus Dashboard プラットフォームをリリース 3.2(x) にアップグレードします。 すべてのサービスは、プラットフォームとともに自動的にアップグレードされます。 **2.** リリース 3.2(x) からリリース 4.1(1) へのアップグレード リリース 4.1(1) では、すべてのサービスが単一の Nexus Dashboard 製品に統合されています。
3.0(1)	ファブリック コントローラ：12.1(3) Orchestrator：4.2(x) Insights：6.3(1)	**1.** 『*Nexus Dashboard* 展開ガイド、リリース *3.2.x*』の説明に従って、Nexus Dashboard プラットフォームをリリース 3.2(x) にアップグレードします。 すべてのサービスは、プラットフォームとともに自動的にアップグレードされます。 **2.** リリース 3.2(x) からリリース 4.1(1) へのアップグレード リリース 4.1(1) では、すべてのサービスが単一の Nexus Dashboard 製品に統合されています。

現在の Nexus Dashboard リリース	互換性のあるサービス （フォームファクタとクラスタサイズによっては、これらのサービスの 1 つ以上が現在有効になっている場合があります）	アップグレードのワークフロー
2.3(2) 以前	ファブリックコントローラ：12.1(2) 以前 Orchestrator：4.1(x) 以前 Insights：6.2(x) 以前	1. 『*Nexus Dashboard* 展開ガイド、リリース *3.1.x*』の説明に従って、Nexus Dashboard プラットフォームをリリース 3.1(1) にアップグレードします。 すべてのサービスは、プラットフォームとともに自動的にアップグレードされます。 2. 『*Nexus Dashboard* 展開ガイド、リリース *3.2.x*』の説明に従って、リリース 3.1(1) からリリース 3.2(x) にアップグレードします。 すべてのサービスは、プラットフォームとともに自動的にアップグレードされます。 3. リリース 3.2(x) からリリース 4.1(1) へのアップグレード リリース 4.1(1) では、すべてのサービスが単一の Nexus Dashboard 製品に統合されています。

Nexus Dashboard のアップグレード

ここでは、既存の Nexus ダッシュボード クラスタをアップグレードする方法について説明します。

サポートされているアップグレードパス （162 ページ） で説明しているとおり、Nexus Dashboard リリース 4.1(1) に直接アップグレードするには、 Nexus Dashboard リリース 3.2(x) を実行している必要があります。これらのリリースでは、次の重要な点に注意してください。

- **Nexus Dashboard リリース 3.2(x)**：Nexus Dashboard のデプロイメントの概要 （5 ページ） で説明したとおり、これらのNexus Dashboard リリースでは、 Nexus Dashboard は 1 つの製品として利用でき、個々のサービス（Nexus Dashboard Insights、Orchestrator、Fabric Controller など）はNexus Dashboard とは別の個別の製品として利用できました。
- **Nexus Dashboard リリース 4.1(1)**：これは、Nexus Dashboard と上記の個々のサービスが単一の統合製品としてパッケージ化された最初の Nexus Dashboard リリースです。

つまり、アップグレードプロセスは次の段階を経ます：

1. Nexus Dashboard リリース 3.2(x) でアップグレード プロセスを開始します。ここでは、Nexus Dashboard と個々のサービスは別の製品です。

2. 次に、 Nexus Dashboard 4.1(1) にアップグレードします。これで、 Nexus Dashboard と個々のサービスがパッケージ化された単一の統合製品としてアップグレードプロセスを完了します。

始める前に

で説明している前提条件をすべて満たしていることを確認します。 既存の Nexus Dashbaord クラスターをアップグレードするための前提条件と注意事項 （157 ページ）

手順

ステップ 1 Nexus Dashboard リリース 3.2(x) システムで、 Nexus Dashboard 4.1(1) イメージをダウンロードします。

a) [ソフトウェア ダウンロード（Software Download）] ページを参照します。

https://software.cisco.com/download/home/286327743/type/286328258

b) 左側のサイドバーから、ダウンロードする Nexus Dashboard 4.1(1)のリリースバージョンを選択します。

c) ターゲットとする 4.1(1) リリース用の Nexus ダッシュボード イメージをダウンロードします。

（注）
- アップグレード プロセスは、すべての Nexus ダッシュボード フォーム ファクタで同じで、Nexus ダッシュボードISOイメージ（`nd-dk9.<version>.iso`）を使用します。言い換えると、最初の展開で仮想フォーム ファクターを使用していた場合（ESX での展開のための `.ova` イメージなど）やクラウド プロバイダーのマーケット プレースを使用していた場合であっても、アップグレードでは `.iso` イメージを使用する必要があります。
- イメージのダウンロードが完全に失敗した場合は、Nexus Dashboard とイメージ サーバ間のネットワーク接続を確認します。**[管理（Admin）] > [システム設定（System Settings）] > [一般（General）] > [プロキシ構成（Proxy configuration）]** でプロキシ構成を確認します。

d) （オプション）環境内のWebサーバでイメージをホストします。

（注）
環境内のサーバーでイメージをホストすることをお勧めします。イメージを Nexus Dashboard クラスタにアップロードする場合、イメージに直接 URL を指定するオプションがあります。そうすれば、プロセスは相当高速化されます。

ステップ 2 現在の Nexus ダッシュボードの**管理コンソール**に管理者ユーザーとしてログインします。

ステップ 3 クラスタから古く、アクティブでないアップグレード イメージを削除します。

クラスタを初めてアップグレードする場合は、この手順をスキップできます。

a) **[管理（Manager）] > [ソフトウェア管理（Site Software Management）]**に移動します。

b) アップグレードイメージのタイルのゴミ箱アイコンをクリックして、古い非アクティブなアップグレード**イメージ**を削除します。

c) すべての古いアップグレード イメージについて、この手順を繰り返します。

ステップ 4 新しいイメージをクラスタにアップロードします。

a) **[管理（Manager）]** > **[ソフトウェア管理（Site Software Management）]**に移動します。

b) [Add Image] をクリックします。

c) **[ソフトウェアイメージの追加（Add Software Image）]** ウィンドウで、イメージがウェブ サーバーの **[リモート（Remote）]** であるか、マシン上での **[ローカル（Local）]** であるかを選択します。

どちらの場合も、イメージは `.iso` で終わるファイルです。

- **リモート**：最初の手順でダウンロードしたイメージの **URL** を入力します。
- **ローカル**：**[ファイルの選択]** をクリックして、イメージをダウンロードしたローカルフォルダに移動します。

d) **[追加（Image）]** をクリックして、 イメージを追加します。

次に、 Nexus Dashboard はアップグレード イメージをダウンロードしてイメージの処理を開始し、いくつかの準備と検証の段階を経て、アップグレードが正常に行われるようにします。終了するまでに数分かかる場合があります。

（注）
アップグレードのトラブルシューティング （172 ページ）を参照してください。ここには、アップグレードのこの時点で行われる検証のチェックと、問題が生じた場合の対処方法が記されています。

e) 検証が完了すると、**[ソフトウェア管理（Software Management）]** ページのカードに **[インストール（Install）]** ボタンが表示されます。**[インストール（Install）]** をクリックしてソフトウェアをインストールし、アップグレード プロセスを実行します。

インストールの進行状況ウィンドウが表示されます。更新中は、この画面から移動できます。

クラスター内のノードの数によっては、この手順に60分以上かかる場合があります。その間、ノードが再起動し、 GUIにアクセスできなくなります。Nexus Dashboard は、いくつかの段階を経て次の手順を経ます。

- リリース ファームウェアのインストール
- サービスの無効化
- インフラストラクチャ サービスのシャットダウン
- プラットフォーム サービスのアップデート
- インフラストラクチャ サービスの有効化
- サービスの有効化

[詳細（Details）] リンクをクリックして、アップグレードの進行状況とさまざまな段階を確認できます。

（注）
アップグレードプロセス中に問題が発生した場合（インデックスの問題の可能性など）は既存の Nexus Dashbaord クラスターをアップグレードするための前提条件と注意事項（157 ページ）を参照してください。

上記のプロセスが完了したら、 Nexus Dashboard 4.1(1) にアップグレードできているはずです。Nexus Dashboard と個々のサービスが単一の統合製品としてパッケージ化されています。

（注）
展開したクラスター形式とクラスター ノードの数によっては、特定の機能（コントローラ、オーケストレータ、テレメトリなど）が使用できない場合があります。 Nexusダッシュボード キャパシティ プランニング ツール の情報を確認して、クラスターインストールで使用できる機能を確認します。

ステップ 5 ノードのアップグレードタスクが完了したら、ノードが正常であり、UIにログインできることを確認します。

アップグレード プロセスが完了すると、通常どおりに Nexus Dashboard ダッシュボード UI を表示できます。

[概要（Overview）] ページでシステム全体の正常性を確認し、**[管理（Admin）]** > **[システム ソフトウェア（System Software）]**ページで現在の実行中バージョンを確認できます。

次のタスク

必要なアップグレード後のタスクの実行のために、アップグレード後の情報とタスク （167ページ）に進んでください。

アップグレード後の情報とタスク

このセクションでは、 Nexus Dashboard リリース 3.2.x からNexus Dashboard 4.1.1 にアップグレードした後に完了する必要がある変更とタスクに関する情報を示します。

マルチクラスタ接続のアップグレード後のタスクの実行

4.1.1 より前のこれらの設定のいずれかを設定してた場合。Nexus Dashboard：

- Nexus Dashboard Insights がリモートで作成した NDFC ファブリックをオンボーディングしていた場合
- One Manage を使用して複数の NDFC または NDI クラスタを管理および監視していた場合
- 複数の NDFC クラスタを持つマルチクラスタ ファブリック グループがある場合

これらのクラスタが以前のリリースでマルチクラスタ接続を使用してすでに接続されていた場合は、プライマリクラスターで、Nexus Dashboard リリース 4.1.1 にアップグレードしたすべてのクラスタを再登録する必要があります。

さらに、以前のリリースで NDI および NDO の統合があった場合、Nexus Dashboard リリース 4.1.1 ではサポートされません。NDO 統合を活用するには、 Nexus Dashboard リリース 4.1.1 で NDI および NDO クラスタをフェデレートする必要があります。

Nexus Dashboard リリース 3.2.x システムでマルチクラスタ接続が設定されている場合は、アップグレードが完了した後に、マルチクラスタ接続を再度有効にする必要があります。このタスクは、コロケーション環境に NX- OSファブリックがある場合にのみ適用されます。詳細については、 クラスタの接続 を参照してください。

スイッチのファームウェア イメージの再アップロード

リリース 3.2.x でNexus Dashboard にアップロードされたスイッチのファームウェア イメージは、 Nexus Dashboard 4.1.1 にアップグレードするときに引き継がれません。Nexus Dashboard 4.1.1 にアップグレードした後、それらのスイッチのファームウェアイメージを再アップロードしてください。

1. **[管理（Manage）]** > **[ファブリック ソフトウェア（Fabric Software）]** > **[NX-OS/IOS-XE]** > **[イメージ（Images）]** に移動します。
2. **[アクション（Actions）]** ドロップダウンリストから **[アップロード（Upload）]** を選択し、必要なスイッチファームウェアイメージを再アップロードします。

詳細については、 ファブリック ソフトウェアの管理を 参照してください。

異常の問題に対処する

アップグレードが完了したら、**[異常（Anomalies）]** 領域で問題がないかを確認し、一部の NX OSファブリックで **再計算と展開を** 完了するための要求を確認します。

デバイスのログイン情報の設定

Nexus Dashboard リリース 3.2.x システムで共同ホストされた NX- OSファブリックを設定していた場合は、次の手順に従って、 Nexus Dashboard リリース 4.1.1 にアップグレードした後に適切なデバイスのログイン情報が設定されていることを確認します。

1. アップグレードされたNexus Dashboard 4.1.1 システムで、**[管理（Manage）]** > **[デバイス ログイン情報（Device Credentials）]** に移動します。
2. **[デバイス ログイン情報（Device Credentials）]** エリアに表示される情報を確認します。

[デバイス ログイン情報（Device Credentials）] エリアに赤色のテキストで **[設定なし（Not Set）]** が表示されます。

3. **[デバイス ログイン情報（Device Credentials）]** エリアで、**[設定（Set）]** をクリックします。
4. **[デフォルト ログイン情報の設定（Set Default Credentials）]** ページで、必要な情報を入力します。
   - [ユーザー名（Username）]、[パスワード（password）]、および [パスワードの確認（Confirm password）]：必要なユーザー名とパスワードの情報を入力します。
   - 必要に応じて、**[Robot（ロボット）]** ログイン情報を設定するチェックボックスをオンにします。

   次に [**保存（Save**）] をクリックします。

   [デフォルトのログイン情報の設定（Set Default Credentials）] ページに戻り、テキスト **Default Set**が青色で表示されます。

古いクラスタータイプを新しい3ノード仮想クラスター（データ）クラスタータイプに移行する

1.5 TB ディスクを搭載した 4.1.1 より前のクラスタ タイプのアプリ ノードは、Nexus Dashboard リリース 4.1.1 ではサポートされていません。Nexus Dashboard リリース 4.1.1 にアップグレードすると、SE-VIRTUAL-APP-LARGE として表示されます。

さらに、4.1.1 より前のこれらのクラスターは、 Nexus Dashboard リリース 4.1.1 でのグリーンフィールド展開としてはサポートされていませんが、リリース 4.1.1 にアップグレードする場合は次がサポートされます：

- 3 ノード仮想クラスター（1.5 TB ストレージのアプリ ノード）
- 5 ノード仮想クラスター（500G または 1.5TB ストレージのアプリ）

これらの古いクラスタータイプから新しいクラスタータイプ 3ノードのリモート対応クラスター（データ）に移行する場合は、次の手順を使用して新しいクラスタータイプに移行できます。

1. この章で説明されている手順を使用して、古いクラスタータイプをそのままにして、Nexus Dashboard リリース 4.1.1 にアップグレードします。
2. Nexus Dashboardリリース4.1.1にアップグレードしたら、古いクラスター タイプのバックアップを実行します。

   詳細については、「*Nexus Dashboard* のバックアップと復元」を参照してください。

   - 以前のクラスタータイプをバックアップする場合は、 **構成のみ** または **完全** バックアップのオプションを使用できます。
   - 続行する前に、古いクラスターからバックアップを正常に取得したことを確認します。

3. 古いクラスター タイプのクラスターをシャットダウンします。
4. 新しいクラスター タイプ `3 node virtual cluster (data)` のグリーンフィールドの展開を実行します。
   - 新しいクラスターで古いクラスターの名前を再利用します。
   - 仮想データクラスターまたは物理クラスターを展開できます。
   - 古いクラスタータイプのIPアドレスを再利用することも、*Nexus Dashboard* のバックアップと復元 で説明されているように、**[外部サービスの IP 設定を無視する（Ignore External Service IP Configuration）]**チェックボックスをオンにして、新しいクラスターで新しいIPアドレスを使用して復元することもできます。
5. 古い3ノードリモート対応クラスター（アプリ）または5ノードリモート対応クラスター（アプリ）のバックアップを新しい3ノードリモート対応クラスター（データ）に復元します。

   詳細については、「*Nexus Dashboard* のバックアップと復元」を参照してください。

テレメトリ構成の再展開

Nexus Dashboard リリース 4.1.1 にアップグレードすると、NX- OS ファブリックからのソフトウェア テレメトリ ストリーミングを処理するための永続 IP アドレスが変更されます。Nexus Dashboard 4.1.1 へのアップグレード後にテレメトリ操作を再開するには、テレメトリ設定を再展開する必要があります。

1. **[システムのステータス（System Status）]** ページに移動します。

   Admin > **System Status**
2. **[Telemetry]** をクリックし、 **[Telemetry Status]** エリアの **[Fabrics]** タブをクリックします。
3. **ファブリック** テーブルに表示されている情報を確認します。

   NX- OSファブリックの場合、[ファブリック（Fabrics）]テーブルにリストされている 1 つ以上のファブリックで、アップグレード前は**[テレメトリ構成ステータス（Telemetry config status）]** 列に **[保留中の更新（Pending updates）]** のステータスが表示されていることに **注意** してください。

   この状態では、テレメトリ ストリーミングが機能せず、個々の機能のステータス（ソフトウェアテレメトリ、フローコレクション、スイッチ ステータスなど）が無効になるため、無視する必要があります。

（注） **[ファブリック（Fabrics）]**テーブル内の一部のファブリックでは、**[テレメトリ構成ステータス（Telemetry config status）]**列に [**OK]** のステータスが表示され、その他のファブリックのステータスが **[保留中の更新（Pending updates）]**と表示される場合があります。 **[テレメトリステータス（Telemetry status）]**エリアの [**スイッチ（Switches）]** タブをクリックした場合、テレメトリ列に誤った緑色の **[OK]** または **[成功（Success）**] ステータス エントリを **持つ** スイッチが表示される場合があります。これらのスイッチは **、[ファブリック（Fabrics）]** テーブルに表示されます。これは、これらのファブリックのスイッチ レベルで表示される誤ったステータス情報であり、無視する必要があります。

4. **[テレメトリ ステータス（Telemetry status）]**エリアで **[ファブリック（Fabrics）**] タブを選択した状態で、**[テレメトリの再展開（Redeploy テレメトリ）]**をクリックします。

   確認ウィンドウで、**[確認（Confirm）]** をクリックします。

   [確認（Confirm）] をクリックすると、個々の機能のステータスが **[進行中で有効化（Enable in Progress）]**に変わり、累積的な **[Telemetry 設定ステータス（Telemetry Config Status）]** が**[進行中（In Progress）]**に更新されます。

5. **[確認（Confirm）]**をクリックすると、**[システム（System）] [ステータス（Status）]** の下の **[テレメトリ（Telemetry）]** ページの **[ファブリック（Fabrics）]**タブに戻ります。ページの右上隅にある **[更新（Refresh）]** をクリックします。

   確認ページで **[確認（Confirm）]** をクリックした直後にテレメトリステータスが正しく表示されない場合がありますが、**[更新（Refresh）]**をクリックすると正しいテレメトリステータスが に表示されます。

6. もう一度、**ファブリック** テーブルに表示されている情報を確認します。

   [更新（Refresh）]をクリックした後で、次のエリアのステータスが変化することがわかります。

   - 個々の機能のステータスは、**[進行中で有効化（Enable in Progress）]** に変更されます。
   - **[テレメトリ設定ステータス（Telemetry config status）]** 列のファブリックのステータスが、[更新の保留中 （**Pending updates**）] から **[進行中（In Progress）]**に変わります。数分後、ファブリックのステータスは、**[テレメトリ設定ステータス（Telemetry config status）]**列で、自動的に、または**[更新（Refresh）]** を再度クリックした後に、**[OK]** に変わります。

操作が完了すると、個々の機能ステータスは次のようになります。

- `[Enabled]`これはすべてのスイッチで構成のプッシュが成功した場合です。
- `[Enabled Fail]`これはいずれかのスイッチで失敗した場合です。
- `[Enabled Pending]`これは変更制御モードが有効になっている場合です。この場合、**[管理（Manage）]** > **[制御を変更（Change control）]**を使用して変更管理チケットを明示的に

適用します。詳細については、「*Nexus Dashboard* での変更制御とロールバックの使用」を参照してください。

累積 **テレメトリ構成ステータス** は次のように表示されます。

- `OK` すべてのスイッチの構成が成功した場合です。
- `Not OK` 失敗した場合、またはすべてのスイッチの変更制御モードで保留中の場合です。
- `Partial OK` 一部のスイッチで成功し、失敗したか、他のスイッチで変更制御モードで保留中である場合です。

SNMP サーバーのユーザーの変更を確認する

Nexus Dashboard リリース 4.1.1 より前のリリースでは、次に示す例のように、インテントの一部としてパスワードなしで管理対象の NX-OS スイッチで構成された SNMP サーバー ユーザーは、

```
snmp-server user Demo_CMDv5 vdc-operator
snmp-server user DemoOps_admin vdc-operator
snmp-server user DemoOps_admin network-admin
```

は、**再計算および展開** 操作中に差分に表示されませんでした。これらは、特にスイッチが TACACS+などのリモート認証方式に依存している環境では、気付かれないことがよくあります。

Nexus Dashboard リリース 4.1.1 にアップグレードすると、これらの違いが正しく検出され、予想される差分として GUI に表示されるようになります。リリース 4.1.1 へのアップグレード後、次のいずれかを行う必要があります。

- これらの構成をプッシュしてスイッチを同期させるか、
- これらの SNMP ユーザー エントリが不要になった場合は、インテントから削除します。

Performance Manager（PM）の履歴データを表示する

Nexus Dashboard をリリース 3.2.x からリリース 4.1.1 にアップグレードした後、ファブリックでテレメトリを有効にすると、Performance Manager（PM）の履歴データは表示されません。代わりに、システムはその時点から新たな PM データの収集を開始します。

過去の PM データを表示するには、影響を受けるファブリックでテレメトリを無効にします。古い PM データが再表示されます。

アップグレードのトラブルシューティング

前のセクションで説明した、新しいイメージのアクティブ化段階で、すべてのノードが再起動した後、GUI にログインしてアップグレードワークフローのステータスを確認できます。最初は、クラスタの初期展開と同様のブートストラッププロセスを確認できます。ノードが起動すると、GUI の **[概要（Overview）]** ページでサービスのアクティブ化に関する追加情報を確認できます。

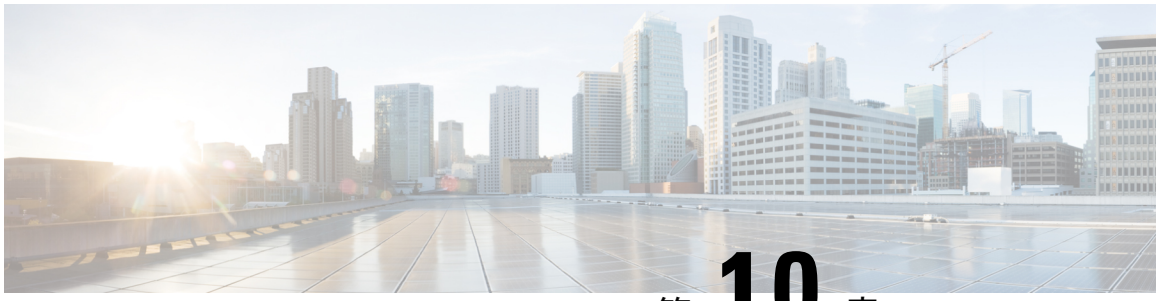
何らかの理由でアップグレードが失敗した場合、GUIにエラーと追加の回避策の手順が表示されます。たとえば、次のようなエラーメッセージが修正とともに表示される場合があります。

```
Failed to activate

Upgrade failed while shutting down the cluster: Operation Timedout, last status: Operation
 Timedout

Please login to one of the primary nodes as 'rescue-user' and follow the steps provided
 by the upgrade recovery
helper by invoking following command: 'acs upgrade recover Cluster Shutdown'. If the
issue persists, please contact Cisco TAC for assistance.
```

問題が解決しない場合は、**[管理（Admin）]**をクリックしてテクニカルサポートにアクセスします。詳細については、「*Cisco* テクニカル サポートの取り扱い」 を参照してください。



第 10 章

DCNM から ND への移行

DCNM から ND への移行の前提条件とガイドライン

DCNM 11.5(4) からのアップグレードは、次のワークフローで構成されます。

1. このセクションに記載されている前提条件とガイドラインが満たされていることを確認します。
2. ターゲット ND リリースに固有の移行ツールを使用して、既存の設定をバックアップします。
3. 新しい Nexus Dashboard クラスターを新規に展開します。
4. ステップ 1 で作成した設定のバックアップを復元します。

（注） アップグレードを実行する前に：

- 各ファブリックのクレデンシャルの検証
  - LAN ファブリックの場合、**[Web UI]** > **[管理（Administration）]** > **[クレデンシャルの管理（Credentials Manage）]** > **[LAN のクレデンシャル（LAN Credentials）]** ページで、各ファブリックを選択し、**[検証（Validate）]** を選択して行います。
  - SAN ファブリックの場合、**[Web UI]** > **[管理（Administration）]** > **[クレデンシャルの管理（Credentials Manage）]** > **[SAN のクレデンシャル（SAN Credentials）]** ページで、各ファブリックを選択し、**[検証（Validate）]** を選択して行います。
- Thousand Eyes 統合アプリケーションなどのアプリケーションを DCNM で実行している場合は、移行手順を進める前にそのアプリケーションを無効化にします。

ファブリック タイプの互換性

適切なアップグレード ツールを使用することで、次の表に示すように、ファブリック タイプのために新しく展開された Nexus Dashboard Fabric Controller に、DCNM リリース 11.5(4) からバックアップされたデータを復元できます。

（注） SAN ファブリックは、 Nexus Dashboardリリース4.1.1 ではほぼ変更されていません。

4.1.1 より前のファブリック		**4.1.1 ファブリック タイプ**
ファブリック テクノロジー	**ファブリック タイプ**	
LAN		
VXLAN EVPN	データ センター VXLAN EVPN	データ センター VXLAN EVPN - iBGP
eBGP VXLAN EVPN	BGP ファブリック	データ センター VXLAN EVPN - eBGP
VXLAN EVPN	キャンパス VXLAN EVPN	キャンパス VXLAN EVPN
eBGP ルーテッド	BGP ファブリック	BGP ファブリック
従来の LAN	拡張クラシック LAN	拡張クラシック LAN
従来の LAN	従来の LAN	レガシー クラシック LAN
Custom	外部接続ネットワーク	外部およびファブリック間接続ネットワーク
Custom	カスタム ネットワーク	外部およびファブリック間接続ネットワーク
Custom	マルチサイト外部ネットワーク	外部およびファブリック間接続ネットワーク
LAN モニター	LAN モニター	外部およびファブリック間接続ネットワーク
VXLAN EVPN	VXLAN EVPN マルチサイト	VXLAN （ファブリック グループ）
マルチファブリック ドメイン	ファブリック グループ	クラシック（ファブリックグループ）
IPFM		
IPFM	IPFM	IPFM

4.1.1 より前のファブリック		4.1.1 ファブリック タイプ
ファブリック テクノロジー	ファブリック タイプ	
LAN		
IPFM	IPFM クラシック	IPFM クラシック
ジェネリック マルチキャスト	IPFM クラシック	IPFM クラシック
マルチファブリック ドメイン	ファブリック グループ	IPFM（ファブリック グループ）

アップグレード後の機能の互換性

次の表に、アップグレード後に DCNM 11.5(4) のバックアップから復元される機能に関連する注意点を示します。

DCNM 11.5（4）の機能	アップグレードのサポート
構成された Nexus Dashboard Insights	11.5(4)から繰り越し
コンテナ オーケストレータ (K8s) ビジュアライザ	11.5(4)から繰り越し
vCenter による VMM の可視性	11.5(4)から繰り越し
構成された Nexus Dashboard Orchestrator	11.5(4)から繰り越されません
設定されたプレビュー フィーチャー	11.5(4)から繰り越されません
SAN インストールの LAN スイッチ	11.5(4)から繰り越されません
IPAMの統合	11.5(4)から繰り越されません
カスタマー トポロジ	11.5(4) から繰り越されません。再作成して保存する必要があります
DCNM トラッカー	11.5(4)から繰り越されません
ファブリックのバックアップ	11.5(4)から繰り越されません
レポート定義とレポート	11.5(4)から繰り越されません
スイッチのイメージとイメージ管理ポリシー	11.5(4)から繰り越されません
SAN CLI テンプレート	11.5(4)から繰り越されません
イメージ/イメージ管理データの切り替え	11.5(4)から繰り越されません

DCNM 11.5（4）の機能	アップグレードのサポート
低速ドレイン データ	11.5(4)から繰り越されません
Infoblox 設定	11.5(4)から繰り越されません
エンドポイント ロケーションの設定	アップグレード後に、エンドポイント ロケータ（EPL）を再構成する必要があります。ただし、履歴データは最大 500 MB まで保持されます。
アラーム ポリシーの設定	11.5(4)から繰り越されません
パフォーマンス管理データ	アップグレード後、最大 90 日間の CPU/メモリ/インターフェイス統計情報が復元されます。ファブリックで再度有効にする必要があります。
温度データ	温度データはバックアップに保存されないため、移行後に復元されません。移行後に温度データ収集を再度有効にする必要があります。

既存の DCNM 設定の ND への移行

このセクションでは、既存の DCNM 11.5(4) 設定をバックアップし、新しい Nexus Dashboard クラスタを展開し、設定を復元して移行を完了する方法について説明します。

手順

ステップ 1 アップグレード ツールをダウンロードします。

a) [Nexus Dashboard] ダウンロード ページに移動します。

https://software.cisco.com/download/home/286327743/type/286328258/

b) **[最新のリリース（Latest Releases）]** リストで、ターゲットとするリリースを選択します。

c) 展開タイプに適したアップグレード ツールをダウンロードします。

DCNM 11.5(4) 展開タイプ	アップグレード ツールのファイル名
ISO/OVA	`DCNM_To_NDFC_4.1.1_Upgrade_Tool_OVA_ISO.zip`
Linux または Windows	`DCNM_To_NDFC_4.1.1_Upgrade_Tool_LIN_WIN.zip`

d) **sysadmin** アカウントを使用して、アップグレード ツール イメージを既存の DCNM 11.5(4) サーバーにコピーします。

ステップ 2 アーカイブを抽出し、Linux/Windows 展開の署名を検証します。

（注）

ISO/OVA アーカイブを使用している場合は、次の手順へスキップします。

a) Python 3 がインストールされていることを確認します。

```
$ python3 --version
Python 3.9.6
```

b) ダウンロードしたアーカイブを解凍します。

```
# unzip DCNM_To_NDFC_4.1.1_Upgrade_Tool_LIN_WIN.zip
Archive: DCNM_To_NDFC_4.1.1_Upgrade_Tool_LIN_WIN.zip
extracting: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip
extracting: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip.signature
inflating: ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM
inflating: cisco_x509_verify_release.py3
```

c) 署名を検証します。

ZIP アーカイブ内にはアップグレード ツールと署名ファイルがあります。アップグレード ツールを検証するには、次のコマンドを使用します。

```
# ./cisco_x509_verify_release.py3 -e ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM -i
DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip -s DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip.signature -v dgst
 -sha512

Retrieving CA certificate from https://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully retrieved and verified crcam2.cer.
Retrieving SubCA certificate from https://www.cisco.com/security/pki/certs/innerspace.cer ...
Successfully retrieved and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully fetched a public key from ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM.
Successfully verified the signature of DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip using
ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM
```

d) 検証スクリプト署名を確認したら、スクリプト自体を抽出します。

```
# unzip DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip
Archive: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip
creating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/log4j2.properties
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/DCNMBackup.sh
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/DCNMBackup.bat
creating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/jarchivelib-0.7.1-jar-with-dependencies.jar
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/bcprov-jdk15on-1.68.jar
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/not-going-to-be-commons-ssl-0.3.20.jar
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/jnm.jar
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/slf4j-simple-1.7.21.jar
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/log4j.properties
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/dcnmbackup.jar
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/sequences.info.oracle
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/tables.info.postgres
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/sequences.info.postgres
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/tables.info.oracle
```

ステップ 3 アーカイブを抽出し、ISO/OVA 展開の署名を検証します。

（注）
Linux/Windows アーカイブを使用している場合は、次の手順にスキップします。

a) ダウンロードしたアーカイブを解凍します。

```
# unzip DCNM_To_NDFC_4.1.1_Upgrade_Tool_OVA_ISO.zip
Archive: DCNM_To_NDFC_4.1.1_Upgrade_Tool_OVA_ISO.zip
inflating: DCNM_To_NDFC_Upgrade_Tool_OVA_ISO_4.1.1
extracting: DCNM_To_NDFC_Upgrade_Tool_OVA_ISO_4.1.1.signature
inflating: cisco_x509_verify_release.py3
inflating: ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM
```

b) 署名を検証します。

ZIP アーカイブ内にはアップグレード ツールと署名ファイルがあります。アップグレード ツールを検証するには、次のコマンドを使用します。

```
# ./cisco_x509_verify_release.py3 -e ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM -i
DCNM_To_NDFC_Upgrade_Tool_OVA_ISO_4.1.1 -s DCNM_To_NDFC_Upgrade_Tool_OVA_ISO.signature -v dgst
 -sha512
Retrieving CA certificate from https://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully retrieved and verified crcam2.cer.
Retrieving SubCA certificate from https://www.cisco.com/security/pki/certs/innerspace.cer ...
Successfully retrieved and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully fetched a public key from ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM.
Successfully verified the signature of DCNM_To_NDFC_Upgrade_Tool_OVA_ISO using
ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM
```

ステップ 4 既存の設定をバックアップします。

a) DCNM リリース 11.5(4) アプライアンス コンソールにログインします。

b) スクリーン セッションを作成します。

次のコマンドは、追加のコマンドを実行するためのセッションを作成します。

```
dcnm# screen
```

このコマンドは、ウィンドウが表示されていない場合、または切断された場合でも実行を続けることに注意してください。

c) スーパー ユーザー（root）アクセス権を取得します。

```
dcnm# su
Enter password: <root-password>
[root@dcnm]#
```

d) OVA および ISO の場合は、アップグレード ツールの実行権限を有効にします。

```
[root@dcnm]# chmod +x ./DCNM_To_NDFC_Upgrade_Tool_OVA_ISO_4.1.1
```

e) 前の手順でダウンロードしたアップグレード ツールを実行します。

- たとえば、 Windowsのリリース 4.1.1 の場合は、次のようになります：

```
C:\DCNM_To_NDFC_Upgrade_Tool_LIN_WIN>DCNMBackup.bat
Enter DCNM root directory [C:\Program Files\Cisco Systems\dcm]:
Initializing, please wait...
********************************************************************************
Welcome to DCNM-to-NexusDashboard Upgrade Tool for Linux/Windows.
This tool will analyze this system and determine whether you can move to Nexus Dashboard
4.1.1 or not.
If upgrade to Nexus Dashboard 4.1.1 is possible, this tool will create files to be used for
 performing the upgrade.
Thank you!
********************************************************************************
This tool will backup config data. Exporting Operational data like Performance(PM) might
take some time.
```

```
Do you want to export operational data also? [y/N]: y
*******************************************************************************
Sensitive information will be encrypted using an encryption key.
This encryption key will have to be provided when restoring
the backup file generated by this tool.
Please enter the encryption key:
Enter it again for verification:
…..
2024-07-25 22:35:34,944 [main] DEBUG
org.apache.http.impl.conn.PoolingHttpClientConnectionManager - Connection [id: 0][route:
{s}->https://127.0.0.1:9200] can be kept alive indefinitely
2024-07-25 22:35:34,944 [main] DEBUG
org.apache.http.impl.conn.DefaultManagedHttpClientConnection - http-outgoing-0: set socket
 timeout to 0
2024-07-25 22:35:34,944 [main] DEBUG
org.apache.http.impl.conn.PoolingHttpClientConnectionManager - Connection released: [id:
0][route: {s}->https://127.0.0.1:9200][total kept alive: 1; route allocated: 1 of 20; total
 allocated: 1 of 20]
2024-07-25 22:35:34,969 [main] INFO DCNMBackup - Total number of Json data entries in
backup/es/pmdb_sanportratedata_daily.data ==> 145
2024-07-25 22:35:35,036 [main] INFO DCNMBackup - ###### Total time to export Daily data: 7
 seconds.
2024-07-25 22:35:35,036 [main] INFO DCNMBackup - ###### Total time to export PM data: 36
seconds.
2024-07-25 22:35:35,169 [main] INFO DCNMBackup - Creating data file...
2024-07-25 22:35:38,083 [main] INFO DCNMBackup - Creating metadata file...
2024-07-25 22:35:38,085 [main] INFO DCNMBackup - Creating final backup archive...
2024-07-25 22:35:38,267 [main] INFO DCNMBackup - Done
```

- たとえば、 Linux用のリリース 4.1.1 の場合は、次のようになります :

```
# ./DCNMBackup.sh
Enter DCNM root directory [/usr/local/cisco/dcm]:
Initializing, please wait...
*******************************************************************************
Welcome to DCNM-to-NexusDashboard Upgrade Tool for Linux/Windows.
This tool will analyze this system and determine whether you can move to Nexus Dashboard
4.1.1 or not.
If upgrade to Nexus Dashboard 4.1.1 is possible, this tool will create files to be used for
 performing the upgrade.
Thank you!

*******************************************************************************

This tool will backup config data. Exporting Operational data like Performance(PM) might
take some time.
Do you want to export operational data also? [y/N]: y
*******************************************************************************
Sensitive information will be encrypted using an encryption key.
This encryption key will have to be provided when restoring
the backup file generated by this tool.

Please enter the encryption key:
Enter it again for verification:
……
2024-07-26 04:04:46,540 [main] INFO DCNMBackup - Total number of Json data entries in
backup/es/pmdb_sanportratedata_daily.data ==> 92
2024-07-26 04:04:46,543 [main] INFO DCNMBackup - ###### Total time to export Daily data: 3
 seconds.
2024-07-26 04:04:46,543 [main] INFO DCNMBackup - ###### Total time to export PM data: 11
seconds.
2024-07-26 04:04:46,958 [main] INFO DCNMBackup - Creating data file...
2024-07-26 04:04:47,456 [main] INFO DCNMBackup - Creating metadata file...
```

```
2024-07-26 04:04:47,467 [main] INFO DCNMBackup - Creating final backup archive...
2024-07-26 04:04:47,478 [main] INFO DCNMBackup - Done.
```

- たとえば、 OVAのリリース 4.1.1 の場合は、次のようになります：

```
# ./DCNM_To_NDFC_Upgrade_Tool_OVA_ISO_4.1.1
********************************************************************************
Welcome to DCNM-to-NexusDashboard Upgrade Tool for OVA/ISO.
This tool will analyze this system and determine whether you can move to
Nexus Dashboard 4.1.1 or not.
If upgrade to Nexus Dashboard 4.1.1 is possible, this tool will create files
to be used for performing the upgrade.
NOTE:
Only backup files created by this tool can be used for upgrading,
older backup files created with 'appmgr backup' CAN NOT be used
for upgrading to Nexus Dashboard 4.1.1
Thank you!

********************************************************************************
Continue? [y/n]: y
Collect operational data (e.g. PM, EPL)? [y/n]: y
Does this DCNM 11.5(4) have DCNM Tracker feature enabled on any switch on any fabric? [y/n]:
 n

Sensitive information will be encrypted using an encryption key.
This encryption key will have to be provided when restoring
the backup file generated by this tool.

Please enter the encryption key:
Enter it again for verification:
……
Adding backup header
Collecting DB table data
Collecting DB sequence data
Collecting stored credentials
Collecting Custom Templates
Collecting CC files
Collecting L4-7-service data
Collecting CVisualizer data
Collecting EPL data
Collecting PM data - WARNING: this will take a while!
Collecting AFW app info
Decrypting stored credentials
Adjusting DB tables
Creating dcnm backup file
Creating final backup file
Done.
Backup file: backup11_sandcnm_20240726-113054.tar.gz
```

ステップ 5 このドキュメントの前の章のいずれかの説明に従って、新規に Nexus Dashboard クラスタを展開します。

Nexus Dashboard プラットフォームおよび上記の導入の章に記載されている特定のフォーム ファクタのすべてのガイドラインと前提条件を満たしていることを確認します。

（注）

- DCNM 設定の復元に進む前に、Nexus Dashboard GUI で、必要な数の永続 IP アドレスを指定する必要があります。
- 既存の設定で Cisco Smart Software Management（CSSM）に直接接続するスマート ライセンスを使用している場合は、新しい Nexus Dashboard に CSSM Web サイトに到達するために必要なルートがあることを確認する必要があります。

`smartreceiver.cisco.com` の IP アドレスのサブネットが、Nexus Dashboard 管理ネットワーク用に、Nexus Dashboard の **[管理（Admin）]** > **[システム設定（System Settings）]** > **[全般（General）]** > **[ルート（Routes）]** ページのルート テーブルに追加されていることを確認します。

最新のサブネットを見つけるには、`smartreceiver.cisco.com` に `nslookup` を実行します。次の例をご覧ください。

```
$ nslookup smartreceiver.cisco.com
Server:         24.233.18.143
Address:        24.233.18.143#53

Name:   smartreceiver.cisco.com
Address: 146.112.59.81
Name:   smartreceiver.cisco.com
Address: 2a04:e4c7:fffe::f
```

Nexus Dashboard のデプロイメントに基づいて、IPv4 アドレスまたは IPv6 アドレスのいずれかを使用できます。

さらに、Nexus Dashboard は新しい製品インスタンスと見なされるため、信頼を再確立する必要があります。期限切れの信頼トークンを使用してバックアップを作成した場合は、アップグレード後にスマート ライセンス設定ウィザードを手動で実行し、有効なトークンを入力する必要があります。

ステップ 6 新しいクラスタで設定のバックアップを復元します。

詳細については、「*Nexus Dashboard のバックアップと復元*」を参照してください。

a) 管理コンソール GUI の統合バックアップと復元ページに移動します。**[管理（Admin）]**>**[バックアップと復元（Backup & Restore）]**。

すでに構成されているバックアップは、**[バックアップ（Backups）]** ページに表示されます。

b) **[復元（Restore）]** スライダ ページにアクセスするには、メインの **[バックアップと復元（Backup and Restore）]** ページの右上隅にある **[復元（Restore）]** をクリックします。

[復元（Restore）] スライド ページが表示されます。

c) 該当する場合、**[送信元（Source）]** フィールドで、復元するバックアップの場所を決定します。

- **構成バックアップ テーブルのアップロード**：[バックアップ ファイル（Backup File）] エリアが表示され、復元するローカル バックアップ ファイルをドラッグ アンド ドロップするか、システム上のローカル エリアに移動して復元するバックアップ ファイルを選択できます。
- **リモート ロケーション**：」

1. **[リモート ロケーション（Remote Location）]** フィールドで、リストからすでに構成されているリモート ロケーションを選択するか（使用可能な場合）、**[リモート ロケーションの作成（Create Remote Location）]** をクリックします。

   [リモート ロケーションの作成（Create Remote Location）] をクリックした場合は、、「*Nexus Dashboard のバックアップと復元*」の「リモート ストレージ ロケーションの作成」の手順に従ってから、ここに戻ります。リモート バックアップ プロセスの一部としてリモート ロケーションを構成しますが、リモート バックアップを構成したクラスタとは異なるクラスタにいる場合、復元プロセスの一部としてリモート ロケーションを設定する必要がある場

合があります。この場合、この時点でリモート ロケーションを再度設定します。これにより、システムは、他のクラスタで構成したリモート バックアップを検出できるようになります。

2. **[リモート パス（Remote Path）]** フィールドに、リモート バックアップが存在するリモート経路を入力します。

d) **[暗号キー（Encryption Key）]** フィールドにバックアップ ファイルに対する暗号キーを入力します。
e) [検証（Validation）]エリアのバックアップの行で、**[検証してアップロード（Validate and Upload）]** をクリックします。
f) 検証の進行状況バーに 100% が表示されると、**[次へ（Next）]** ボタンが現用系になります。[次へ（Next）] をクリックします。
g) DCNM から ND/NDFC にアップグレードする場合、ND/NDFC は常に **外部IP の無視** 設定を無視し、可能な場合は常にバックアップの既存の IP を使用しようとします。それ以外の場合は、新しい IP を使用します。

次の表は、システムが IP アドレスをどのように扱うかについての詳細を示しています。

リリース 11.5(4) の展開タイプ	11.5(4) では、トラップ IP アドレスは以下から収集されます：	LAN デバイス管理の接続性	アップグレード後のトラップ IP アドレス	結果
LAN ファブリック メディア コントローラ	`eth1`（または HA システムの場合 `vip1`）	管理	管理サブネットに属する	Honored 構成の違いは、ありません。対応不要です。

リリース 11.5(4) の展開タイプ	11.5(4) では、トラップ IP アドレスは以下から収集されます：	LAN デバイス管理の接続性	アップグレード後のトラップ IP アドレス	結果
LAN ファブリック メディアコントローラ	eth0（または HA システムの場合 vip0）	管理	管理サブネットに属していない	無視されます。管理プールの別の IP がトラップ IP として使用されます。 構成の違いが作成されます。**[管理（Manage）]>[ファブリック（Fabrics）]** で、[Fabric]をダブルクリックして、**[ファブリックの概要（Fabric Overview）]** を表示します。**[アクション（Actions）]** ドロップダウン リストから、**[再計算と展開（Recalculate and Deploy）]** を選択します。**[構成の展開（Deploy Config）]** をクリックします。
LAN ファブリック メディアコントローラ	eth0（または HA システムの場合 vip0）	データ	データ サブネットに属する	Honored 構成の違いは、ありません。対応不要です。

リリース 11.5(4) の展開タイプ	11.5(4) では、トラップ IP アドレスは以下から収集されます：	LAN デバイス管理の接続性	アップグレード後のトラップ IP アドレス	結果
LAN ファブリック メディアコントローラ	`eth0`（または HA システムの場合 `vip0`）	データ	データサブネットに属していない	無視されます。データプールの別のIPがトラップ IP として使用されます 構成の違いが作成されます。に **[管理（Manage）] > [ファブリック（Fabrics）]** で、ファブリックをダブルクリックして **[ファブリックの概要（Fabric Overview）]** を表示します。**[アクション（Actions）]** ドロップダウン リストから、**[再計算と展開（Recalculate and Deploy）]** を選択します。**[構成の展開（Deploy Config）]** をクリックします。

リリース 11.5(4) の展開タイプ	11.5(4) では、トラップ IP アドレスは以下から収集されます：	LAN デバイス管理の接続性	アップグレード後のトラップ IP アドレス	結果
SAN 管理	OVA/ISO – • `trap.registaddress`（設定されている場合） • eth0（`trap.registaddress` が設定されていない場合） Windows/Linux – • `trap.registaddress`（設定されている場合） • イベントマネージャアルゴリズムに基づくインターフェイス（`trap.registaddress` が設定されていない場合）	N/A	データサブネットに属する	Honored 構成の違いは、ありません。対応不要です。
		N/A	データサブネットに属していない	無視されます。データプールの別のIPがトラップ IP として使用されます

h) [復元（Restore）] をクリックします。

復元プロセスを開始することを確認する警告ウィンドウが表示されます。復元プロセスの実行中は、Nexus Dashboard の機能にアクセスできません。復元プロセスには数分かかる場合があります。

i) 警告ウィンドウで **[復元（Restore）]** をクリックして、復元プロセスを続行します。

別のウィンドウが表示され、復元プロセスの進行状況が表示されます。**[タイプ（Type）]** 列のエントリの横にある矢印をクリックすると、復元プロセスの詳細が表示されます。

j) 復元プロセスが成功すると、[進行状況（Progress）] に 100% と表示され、**[履歴の表示（View History）]** ボタンが現用系になります。

[履歴の表示（View History）] をクリックして **[バックアップと復元（Backup and Restore）]** ウィンドウの **[履歴（History）]**エリアに移動すると、復元プロセスが表示され、**[ステータス（Status）]** 列に **[成功（Success）]** と表示されます。

（注）
新しいND統合バックアップおよび復元機能を使用してバックアップされた構成を復元した後、ND レベルで表示されるNDファブリックの状態が、NDファブリックの実際の状態と同期していない可能性があります。ファブリックのステータスを同期中に戻すには、**[ファブリック概要（Fabric Overview）]** ページで、

ページ上部の **[アクション（Actions）]** をクリックし、**[再計算と展開（Recalculate and Deploy）]** を選択します。

ステップ 7 アップグレード後のタスクを完了します。

a) ND リリース 4.1.1 に SAN デプロイメントがある場合：

バックアップからデータを復元すると、すべての server-smart ライセンスが **OutofCompliance** になります。

UI の**[管理（Admin）]** > **[ライセンス（Licensing）]** > **[スマート（Smart）]** ページから、ポリシーを使用したスマート ライセンシングに移行し、SLP を使用して CCSM との信頼を確立できます。

b) ND リリース 4.1.1 で LAN デプロイメントがある場合：

DCNM 11.5(4) からアップグレードする場合、一部の機能については引き継がれないため、再設定が必要です。詳細については、アップグレード後の機能の互換性 （177 ページ）を参照してください。

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。