Cisco Nexus Dashboard およびサービスの導入とアップグレード ガイド、リリース 3.1.x

最終更新：2025 年 8 月 4 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。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html. Cisco product warranty information is available at https://www.cisco.com/c/en/us/products/warranty-listing.html. US Federal Communications Commission Notices are found here https://www.cisco.com/c/en/us/products/us-fcc-notice.html.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2024–2024 Cisco Systems, Inc. All rights reserved.

目 次

Trademarks ?

第 1 章 **新機能および変更された機能に関する情報** 1

新機能および変更された機能に関する情報 1

第 I 部： **Nexus Dashboard の展開の準備** 3

第 2 章 **展開の概要と要件** 5

デプロイ概要 5

第 3 章 **前提条件：Nexus Dashboard** 9

前提条件とガイドライン 9

通信ポート 16

ファブリック接続 19

サイト間のノード分散 25

サービスのコロケーションの使用例 27

インストール前のチェックリスト 29

第 4 章 **前提条件：ファブリックコントローラ** 33

ファブリック コントローラの要件 33

Fabric Controller の通信ポート 36

第 5 章 **前提条件：オーケストレータ** 53

Orchestrator の要件 53

Orchestrator の通信ポート 54
オーケストレータのファブリック要件 55
ポッド プロファイルとポリシー グループ 56
ファブリック アクセス グローバル ポリシーの設定 57
ファブリック アクセス インターフェイス ポリシーの設定 59

第 6 章 前提条件：Insights 63
Insights の要件 63
Insights の通信ポート 65
Insights のファブリック要件 66

第 II 部： クラスタの展開 69

第 7 章 物理アプライアンスとしての展開 71
前提条件とガイドライン 71
物理ノードのケーブル接続 75
物理アプライアンスとしての Nexus ダッシュボードの展開 77

第 8 章 VMware ESX の展開 93
前提条件とガイドライン 93
VMware vCenter を使用している Nexus ダッシュボードの展開 97
VMware ESXi での Nexus ダッシュボードの展開 118

第 9 章 Linux KVMでの展開 137
前提条件とガイドライン 137
Linux KVM での Nexus ダッシュボードの展開 138

第 10 章 Amazon Web Services での展開 157
前提条件とガイドライン 157
AWS での Nexus ダッシュボードの展開 159

第 11 章 **Microsoft Azure での展開** 173

前提条件とガイドライン 173

Linux または MacOS での SSH キー ペアの生成 174

Windows での SSH キー ペアの生成 175

Azure での Nexus ダッシュボードの展開 178

第 12 章 **ファブリックのオンボーディング** 191

ACI ファブリックのオンボーディング 191

NDFC ファブリックのオンボーディング 193

NX-OS スイッチのオンボーディング 194

第 III 部： **このリリースへのアップグレードまたは移行** 199

第 13 章 **既存の ND クラスタをこのリリースへアップグレード** 201

前提条件とガイドライン 201

サポート対象のアップグレード パス 204

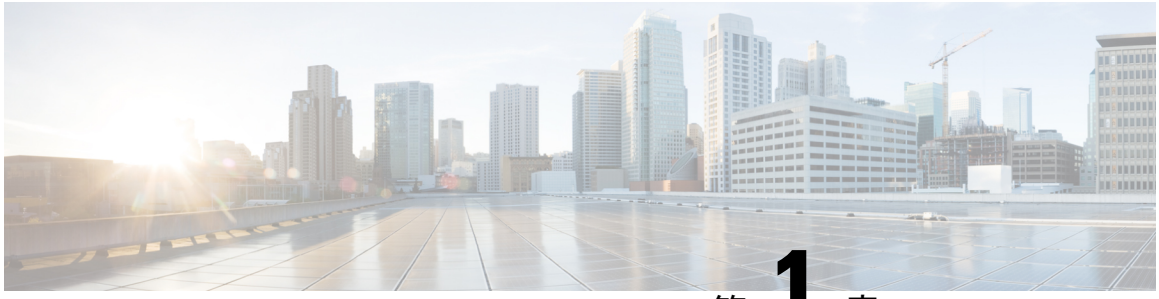
Nexus ダッシュボードのアップグレード 208

アップグレードのトラブルシューティング 212

第 14 章 **DCNM から NDFC への移行** 215

前提条件とガイドライン 215

既存の DCNM 設定の NDFC への移行 217



第 1 章

新機能および変更された機能に関する情報

- 新機能および変更された機能に関する情報 （1 ページ）

新機能および変更された機能に関する情報

次のテーブルは、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

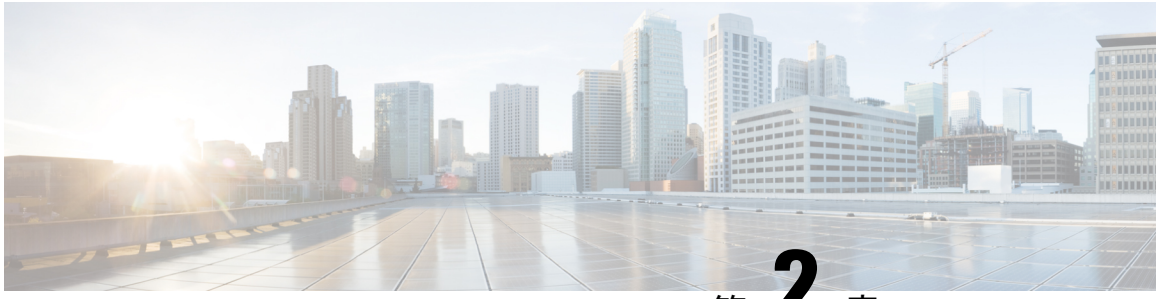
リリース	新機能またはアップデート	参照先
3.1(1)	このドキュメントの最初のリリース。 このリリースの統合された導入ワークフローを反映するために、このドキュメントには、個々のプラットフォームおよびサービスのインストールガイドが統合されています。	--

新機能および変更された機能に関する情報

第 I 部

Nexus Dashboard の展開の準備

- 展開の概要と要件 （5 ページ）
- 前提条件：Nexus Dashboard （9 ページ）
- 前提条件：ファブリックコントローラ （33 ページ）
- 前提条件：オーケストレータ （53 ページ）
- 前提条件：Insights （63 ページ）



第 2 章

展開の概要と要件

- デプロイ概要 （5 ページ）

デプロイ概要

Nexus Dashboardプラットフォーム

Cisco Nexus Dashboard は、複数のデータセンターサイト向けの中央管理コンソールであり、Insights、Orchestrator、Fabric Controller などの Cisco データセンター運用サービスをホストするための共通プラットフォームです。これらのサービスはすべてのデータセンターサイトで利用でき、ネットワークポリシーと運用のためのリアルタイム分析、可視性、保証、また Cisco ACI や Cisco NDFC などのデータセンターファブリックのポリシー オーケストレーションを提供しています。

Nexus Dashboard は、上述のマイクロサービスベースのアプリケーションに共通のプラットフォームと最新のテックスタックを提供し、さまざまな最新アプリケーションのライフサイクル管理を簡素化しながら、これらのアプリケーションを実行し維持するための運用オーバーヘッドを削減します。また、ローカルにホストされているアプリケーションと外部のサードパーティ製アプリケーションの中央統合ポイントも提供します。

（注） このドキュメントでは、Nexus Dashboard クラスタを最初に展開し、1 つ以上のサービスを有効にし、それらのサービスによって管理される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、Nexus Dashboard の設定と操作に関する記事、および日常の操作に関するサービス固有のドキュメントを参照してください。

リリース 3.1(1) での Nexus Dashboard サービスと統合インストール

Nexus ダッシュボードは、一貫した統一された方法ですべての Nexusダッシュボード製品を使用できるようにするサービスを構築および展開するための標準のアプライアンスプラットフォームです。Nexus Dashboard プラットフォームは、Nexus Dashboard サービス（Insights、Orchestrator、Fabric Controller など）を有効にして、ネットワーク ポリシーと運用のリアルタイム分析、可視性、保証を提供できます。また、Cisco ACI、Cisco NDFC、またはコントロー

ラのないスタンドアロン NX-OS スイッチ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実現します。

リリース 3.1(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。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。リリース 3.1(1) 以降、プラットフォームと個々のサービスは単一のイメージに統合され、クラスタの初期設定時に展開して有効にすることができるようになりました。こうして、よりシンプルで合理化されたエクスペリエンスを実現しています。

（注） Nexus Dashboard プラットフォームの以前のリリースでは、多くの場合、個々のサービスの複数のバージョンがサポートされていましたが、統合インストールにより、各 Nexus Dashboard リリースは、各サービスの特定の単一バージョンをサポートし、それらをクラスタの展開時に有効にすることを選択できるようになりました。

さらに、統合インストールにより、クラスタ展開時にサポートされているサービスの組み合わせのみを有効にできるため、サポートされていないサービスの組み合わせが発生する可能性はなくなりました。サービスの共同ホスティングに関する詳細情報は、 Nexus Dashboard クラスタ サイジング ツールで入手できます。

ハードウェアとソフトウェアのスタック

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

このガイドでは、Nexus Dashboard ソフトウェアの初期導入について説明します。これは、物理、仮想、クラウドのフォームファクタに共通です。物理クラスタを展開する場合は、*Nexus Dashboard ハードウェア セットアップ ガイド*で、UCS サーバーのハードウェアの概要、仕様、ラック搭載の方法などについて参照してください。

（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、クラスタ ノード用に 2 つの異なる Cisco UCS サーバー（SE-NODE-G2 と ND-NODE-L4）をサポートしており、これらは同じクラスタ内で混在させることができます。

- 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
  - VMware ESX (.ova)

    VMware ESX仮想マシンを使用して、Nexus Dashboardクラスタを展開できる仮想フォームファクタ。

  - Linux KVM（.qcow2）

    Linux KVM仮想マシンを使用して、Nexus Dashboardクラスタを展開できる仮想フォームファクタ。

- パブリッククラウド
  - Amazon Web Services (.ami)

    AWSインスタンスを使用して、Nexus Dashboardクラスタを展開できるクラウドフォームファクタ。

  - Microsoft Azure (.arm)

    Azureインスタンスを使用して、Nexus Dashboardクラスタを展開できるクラウドフォームファクタ。

（注） すべてのサービスがすべてのフォームファクタでサポートされているわけではなく、一部のフォームファクタは特定のサービスのみをサポートしています。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、サービス、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。サービスとスケールの要件に応じて、 セカンダリ ノードを

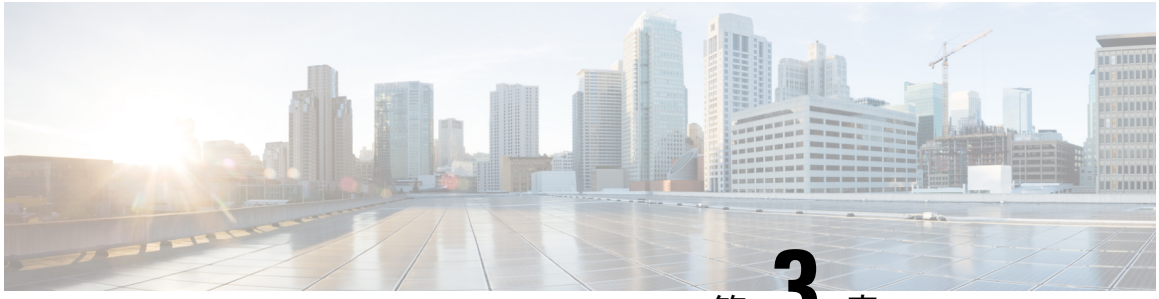
追加して3ノードクラスタを拡張し、サービスの共同ホスティングとより大きなスケールをサポートできます。物理クラスタの場合、プライマリノードに障害が発生した場合にクラスタを容易に回復できるようにするため、最大 2 つの スタンバイ ノードを追加することもできます。

（注）

- 単一ノード展開は、限られた数のサービスでサポートされています。最初の展開後に 3 ノード クラスタに拡張することはできません。
- 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。
- 単一ノード クラスタを展開したものの、それを 3 ノード クラスタに拡張する必要が生じた場合、またはセカンダリ ノードを追加する必要が生じた場合は、基本の 3 ノード クラスタとして再度展開する必要があります。
- 3 ノード クラスタの場合、クラスタが動作し続けるには、少なくとも 2 つのプライマリ ノードが必要です。

  2 つのプライマリ ノードに障害が発生した場合、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」の記事の説明に従って回復するまでは、使用できません。

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。



第 3 章

前提条件：Nexus Dashboard

- 前提条件とガイドライン （9 ページ）
- 通信ポート （16 ページ）
- ファブリック接続 （19 ページ）
- サイト間のノード分散 （25 ページ）
- サービスのコロケーションの使用例 （27 ページ）
- インストール前のチェックリスト （29 ページ）

前提条件とガイドライン

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

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

Nexus 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。

Nexus Dashboard は、ワイルドカード レコードを持つ DNS サーバーはサポートしていません。

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

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

NTP 認証を有効にする場合は、次の注意事項が適用されます。

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

  ID、認証タイプ、およびキー/パスフレーズ自体は、NTP サーバーと Nexus ダッシュボードの両方で一致し、信頼されている必要があります。
- 複数のサーバーが同じキーを使用できます。

  この場合、キーは Nexus Dashboard で 1 回だけ構成してから、複数のサーバーに割り当てる必要があります。
- キー ID が一意である限り、Nexus Dashboard と NTP サーバの両方に複数のキーを設定できます。
- このリリースでは、NTP キーの SHA1、MD5、および AES128CMAC 認証/エンコーディング タイプがサポートされています。

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

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

  このオプションを使用すると、キーが侵害された場合に Nexus Dashboard で特定のキーを簡単に無効にすることができます。
- Nexus Dashboard で一部の NTP サーバーを`優先`としてタグ付けすることを選択できます。

  NTP クライアントは、RTT、応答時間の差異、およびその他の変数を考慮することで、時間の経過に伴う NTP サーバーの「品質」を推定できます。プライマリ サーバーを選択する場合、優先サーバーの優先順位が高くなります。
- `ntpd` を実行している NTP サーバーを使用している場合は、少なくともバージョン 4.2.8p12 を推奨します。
- 以下の制限事項がすべての NTP キーに適用されます。

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

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

Nexus ダッシュボード外部ネットワーク

Nexus Dashboardはクラスタとして展開され、各サービスノードは2つのネットワークに接続されます。最初に Nexus ダッシュボードを設定するときは、2 つの Nexus ダッシュボード インターフェイスに 2 つの IP アドレスを指定する必要があります。1 つはデータ ネットワークに接続し、もう 1 つは管理ネットワークに接続します。

Nexus Dashboard にインストールされる個々のサービスは、次のセクションで説明するように、追加の目的で 2 つのネットワークを使用する場合があります。

表 *2*: 外部ネットワークの目的

Data Network	管理ネットワーク
• Nexus Dashboardノードのクラスタリング • サービス間通信 • Cisco APIC、クラウド ネットワーク コントローラ、および NDFC 通信へのNexus Dashboard ノード たとえば、Nexus ダッシュボード Insights などのサービスのネットワーク トラフィックです。 • スイッチおよびオンボード ファブリックのテレメトリ トラフィック	• Nexus ダッシュボード GUI へのアクセス • SSH を介した Nexus ダッシュボード CLI へのアクセス • DNS および NTP 通信 • Nexus Dashboard ファームウェアのアップロード • Intersight デバイス コネクタ • AAAトラフィック

2つのネットワークには次の要件があります。

- すべての新しい Nexus Dashboard 展開では、管理ネットワークとデータネットワークが異なるサブネットに存在する必要があります。

（注） Nexus Dashboard ファブリック コントローラ サービスだけを実行するNexus Dashboard クラスタは例外です。これは、データ ネットワークと管理ネットワークで同じサブネットを使用して展開できます。

- データ サブネットを変更するにはクラスタを再展開する必要があるため、今後の追加サービスを考慮して、ノードとサービスの必要最低限よりも大きなサブネットを使用することをお勧めします。
- 物理クラスタの場合、管理ネットワークは各ノードの CIMI に対して、TCP ポート 22/443 を介して IP 到達可能性を提供する必要があります。

  Nexus Dashboardのクラスタ設定では、各ノードのCIMC IPアドレスを使用してノードを設定します。
- データ ネットワーク インターフェイスで、Nexus Dashboard トラフィックに使用できる最小 MTU が 1500 である必要があります。

  必要に応じて、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。

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

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

表 *3*: クラスタの *RTT* 要件

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

接続	最大 RTT
あるクラスタ内のノードと別のクラスタ内のノード間（クラスタがマルチクラスタ接続を介して接続されている場合） マルチクラスタ接続の詳細については、『*Cisco Nexus Dashboard インフラストラクチャ管理*』を参照してください。	500 ミリ秒
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

Nexus ダッシュボードの内部ネットワーク

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

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

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

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

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

複数の Nexus 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、アプリケーション オーバーレイとサービス オーバーレイのアドレスがデータ ネットワークの外部に公開されることはなく、これらのサブネット上のトラフィックは内部でルーティングされ、クラスタノードから出ないことを意味します。

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

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

IPv4 および IPv6 のサポート

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

IP 構成を定義するとき、以下のガイドラインが適用されます。

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

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

    管理 IP は、初めてノードにログインしてクラスタのブートストラップ プロセスを開始するために使用されます。
  - Kubernetes 内部コア サービスは IPv4 モードで開始されます。
  - DNS は IPv4 要求と IPv6 要求の両方を処理し、転送します。
  - ピア接続用の VXLAN オーバーレイは、データ ネットワークの IPv4 アドレスを使用します。

    IPv4 パケットと IPv6 パケットは両方とも、VXLAN の IPv4 パケット内にカプセル化されます。
  - UI は、IPv4 と IPv6 の両方の管理ネットワーク アドレスでアクセスできます。
- 純粋な IPv6 構成の場合：
  - 純粋な IPv6 モードは、物理および仮想フォーム ファクタのみでサポートされます。

    AWS および Azure に展開されたクラスタは、純粋な IPv6 モードをサポートしていません。
  - ノードを最初に構成するときに、IPv6 管理ネットワーク アドレスを指定する必要があります。

ノードが起動した後、これらの IP を使用して UI にログインし、クラスタのブートストラップ プロセスを続行します。

- 前述の内部アプリケーションおよびサービス ネットワークに IPv6 CIDR を提供する必要があります。
- 前述のデータ ネットワークと管理ネットワークに IPv6 アドレスとゲートウェイを提供する必要があります。
- すべての内部サービスは IPv6 モードで開始されます。
- ピア接続用の VXLAN オーバーレイは、データ ネットワークの IPv6 アドレスを使用します。

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

BGP 構成と永続的な IP

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

この機能は引き続きサポートされていますが、このリリースでは、異なるレイヤ 3 ネットワークにクラスタ ノードを展開する場合でも、永続的な IP 機能を構成することができます。この場合、永続的な IP は、「レイヤー 3 モード」と呼ばれる BGP を介して各ノードのデータリンクからアドバタイズされます。また、IP は、ノードの管理サブネットまたはデータサブネットと重複していないサブネットの一部である必要があります。永続IPがデータネットワークおよび管理ネットワークの外部にある場合、この機能はデフォルトでレイヤ 3 モードで動作します。IP がそれらのネットワークの一部である場合、機能はレイヤ 2 モードで動作します。BGP は、クラスタの展開中、またはクラスタの稼働後に Nexus ダッシュボード GUI から有効にすることができます。

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

- ピアルータが、ノードのレイヤ 3 ネットワーク間でアドバタイズされた永続的 IP を交換することを確認します。
- 以降のセクションで説明されているように、クラスタの展開時に BGP を有効にするか、インフラストラクチャ管理ドキュメントの「永続的な IP アドレス」セクションで説明されているように、Nexus ダッシュボード GUI で後で有効にするかを選択します。
- 割り当てる永続的な IP アドレスが、ノードの管理サブネットまたはデータ サブネットと重複しないようにしてください。

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

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

通信ポート

Nexus Dashboard クラスタには、次のポートが必要です。

（注） すべてのサービスは、暗号化を備えた TLS または mTLS を使用して、移行中にデータのプライバシーと完全性を保護します。

表 *4 : Nexus Dashboard* ポート（管理ネットワーク）

サービス	ポート	プロトコル	方向 イン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	接続
ICMP	ICMP	ICMP	入力 / 出力	他のクラスタ ノード、CIMC、デフォルト ゲートウェイ
SSH	22	TCP	入力 / 出力	クラスタ ノードの CLI および CIMC
TACACS	49	TCP	発信	TACACS サーバー
DNS	53	TCP/UDP	アウト	DNS サーバ
HTTP	80	TCP	発信	インターネット/プロキシ
NTP	123	UDP	発信	NTP サーバー
HTTPS	443	TCP	入力 / 出力	UI、他のクラスタ (マルチクラスタ接続用)、ファブリック、インターネット/プロキシ
LDAP	389 636	TCP	発信	LDAP サーバ

サービス	ポート	プロトコル	方向 イン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	接続
RADIUS	1812	TCP	発信	Radius サーバー
KMS	9880	TCP	入力 / 出力	その他クラスタ ノードおよび ACI ファブリック
インフラサービス	30012 30021 30500 ～ 30600	TCP および UDP	入力 / 出力	その他のクラスタ ノード

表 *5 : Nexus Dashboard* ポート（データ ネットワーク）

サービス	ポート	プロトコル	方向 イン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	接続
ICMP	ICMP	ICMP	入力 / 出力	他のクラスタ ノード、デフォルト ゲートウェイ
SSH	22	TCP	発信	スイッチと APIC の帯域内
DNS	53	TCP および UDP	入力 / 出力	他のクラスタノードと DNS サーバー
NFSv3	111	TCP および UDP	入力 / 出力	リモート NFS サーバー
HTTPS	443	TCP	発信	スイッチと APIC の帯域内
NFSv3	608	UDP	入力 / 出力	リモート NFS サーバー

サービス	ポート	プロトコル	方向 イン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	接続
SSH	1022	TCP および UDP	入力 / 出力	その他のクラスタ ノード
NFSv3	2049	TCP	入力 / 出力	リモート NFS サーバー
VXLAN	4789	UDP	入力 / 出力	その他のクラスタ ノード
KMS	9880	TCP	入力 / 出力	その他クラスタ ノードおよび ACI ファブリック
インフラサービス	3379 3380 8989 9090 9969 9979 9989 15223 30002 ～ 30006 30009 ～ 30010 30012 30014-30015 30018-30019 30025 30027	TCP	入力 / 出力	その他のクラスタ ノード
インフラサービス	30016 30017	TCP および UDP	入力 / 出力	その他のクラスタ ノード

サービス	ポート	プロトコル	方向 イン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	接続
インフラサービス	30019	UDP	入力 / 出力	その他のクラスタ ノード
インフラサービス	30500 ～ 30600	TCP および UDP	入力 / 出力	その他のクラスタ ノード

ファブリック接続

ここでは、Nexus Dashboard クラスタ ノードを管理ネットワークとデータ ネットワークに接続し、クラスタをファブリックに接続する方法について説明します。

- オンプレミス APIC または NDFC ファブリックの場合、Nexus ダッシュボード クラスタは次の2つの方法のいずれかで接続できます。
  - レイヤ 3 ネットワーク経由でファブリックに接続された Nexus Dashboard クラスタ。
  - リーフ スイッチに接続された Nexus Dashboard ノードは、一般的なホストです。
- Cloud Network Controller ファブリックの場合は、レイヤ 3 ネットワーク経由で接続する必要があります。

外部レイヤ 3 ネットワークを介した接続

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

- Cisco ACI ファブリックのみを管理するために Nexus Dashboard オーケストレータを展開する場合は、データ インターフェイスまたは管理インターフェイスから、各サイトの APIC のインバンドまたはアウトオブバンド（OOB）インターフェイスあるいは両方への接続を確立できます。

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

- Cisco NDFC ファブリックを管理するために Nexus Dashboard Orchestrator を展開する場合は、データインターフェイスから各サイトのNDFCのインバンドインターフェイスへの接続を確立する必要があります。
- Nexus ダッシュボード Insights などの Day-2 Operations アプリケーションを展開する場合は、データ インターフェイスから各ファブリックおよび APIC のインバンド ネットワークへの接続を確立する必要があります。

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

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

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

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

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

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

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

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

図 *1 :* レイヤ *3* ネットワークを介した接続、*2* 日目の運用アプリケーション

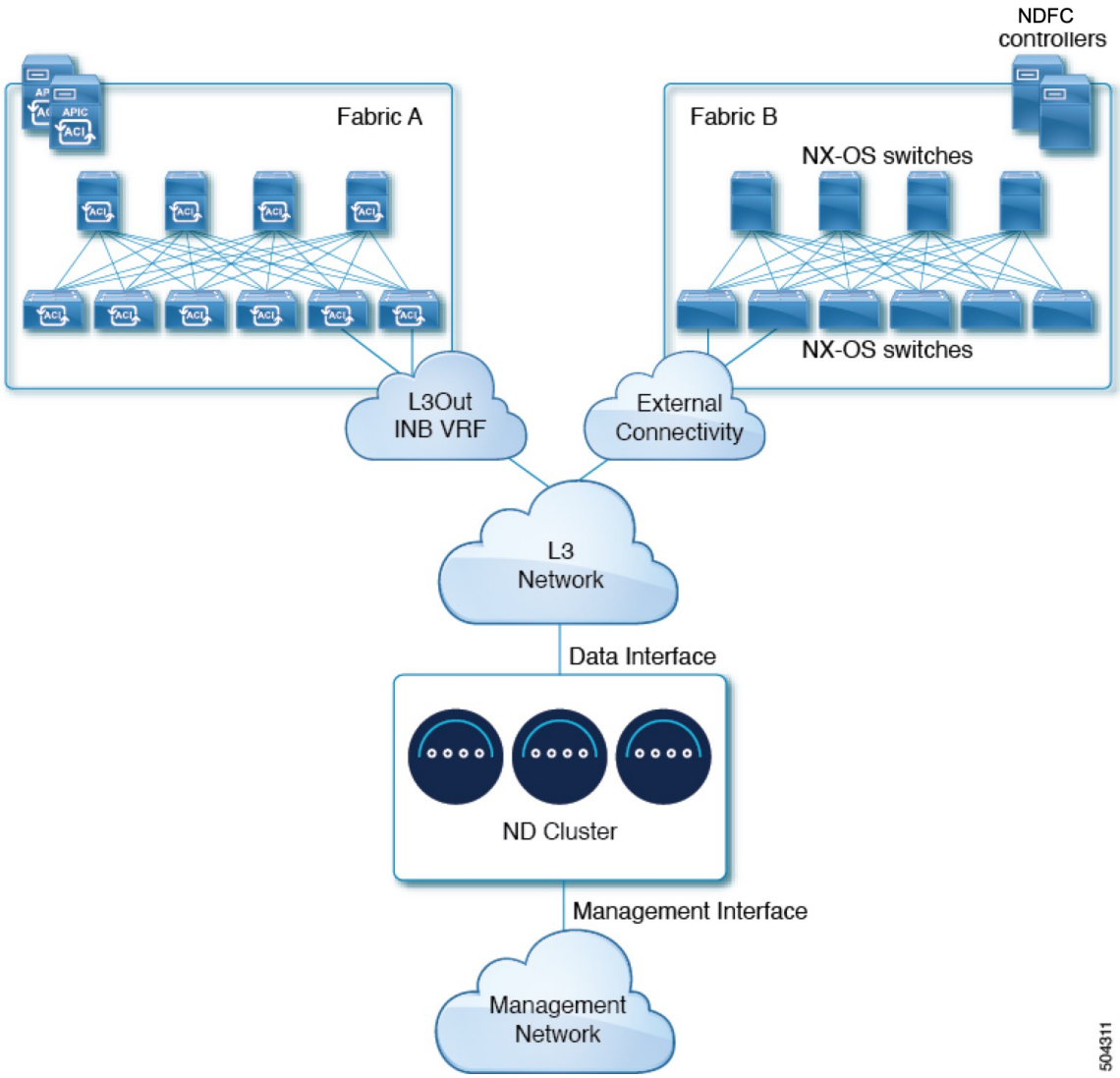
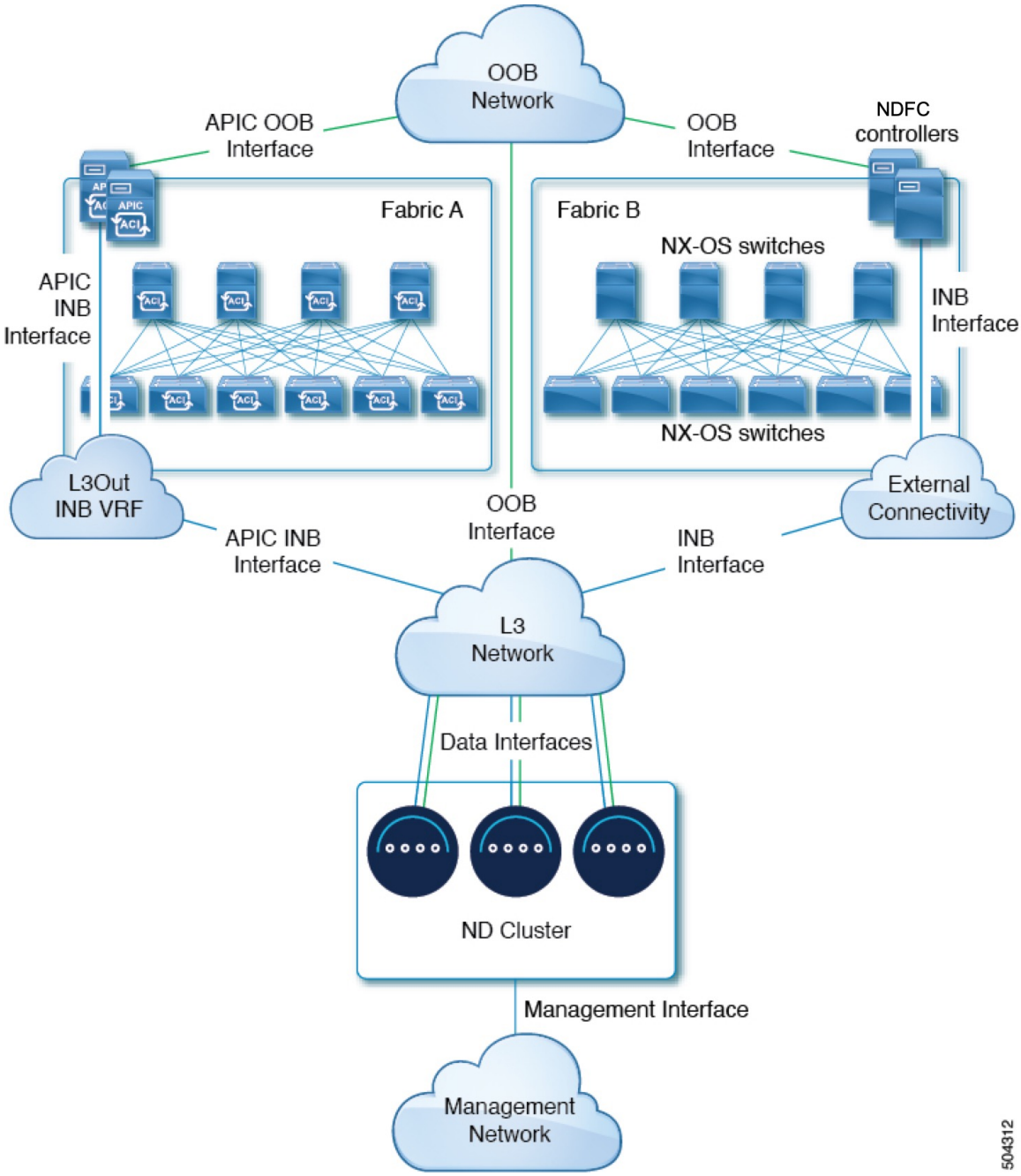


図 *2 :* レイヤ*3*ネットワーク、***Nexus Dashboard Orchestrator***を介した接続



リーフ スイッチへのノードの直接接続

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

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

- Cisco ACI ファブリックのみを管理するために Nexus Dashboard オーケストレータを展開する場合は、データ インターフェイスまたは管理インターフェイスから、各サイトの APIC のインバンドまたはアウトオブバンド（OOB）インターフェイスあるいは両方への接続を確立できます。

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

- Nexus ダッシュボード Insights を展開する場合は、データインターフェイスから各ファブリックのインバンドインターフェイスへの接続を確立する必要があります。

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

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

クラスタをリーフスイッチに直接接続する場合は、次の点に注意してください。

- VMware ESX または Linux KVM で展開する場合、ホストはトランク ポート経由でファブリックに接続する必要があります。

- クラスタのセットアップ中にデータ ネットワークの VLAN ID を指定する場合は、Nexus ダッシュボード インターフェイスと接続されたネットワークデバイスのポートをトランクとして設定する必要があります。

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

- ACI ファブリックの場合：

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

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

  - ファブリックのインバンド管理 EPG と Cisco Nexus ダッシュボード EPG 間のコントラクトを作成する必要があります。

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

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

図 *3:* リーフ スイッチへの直接接続、*2* 日目の運用アプリケーション

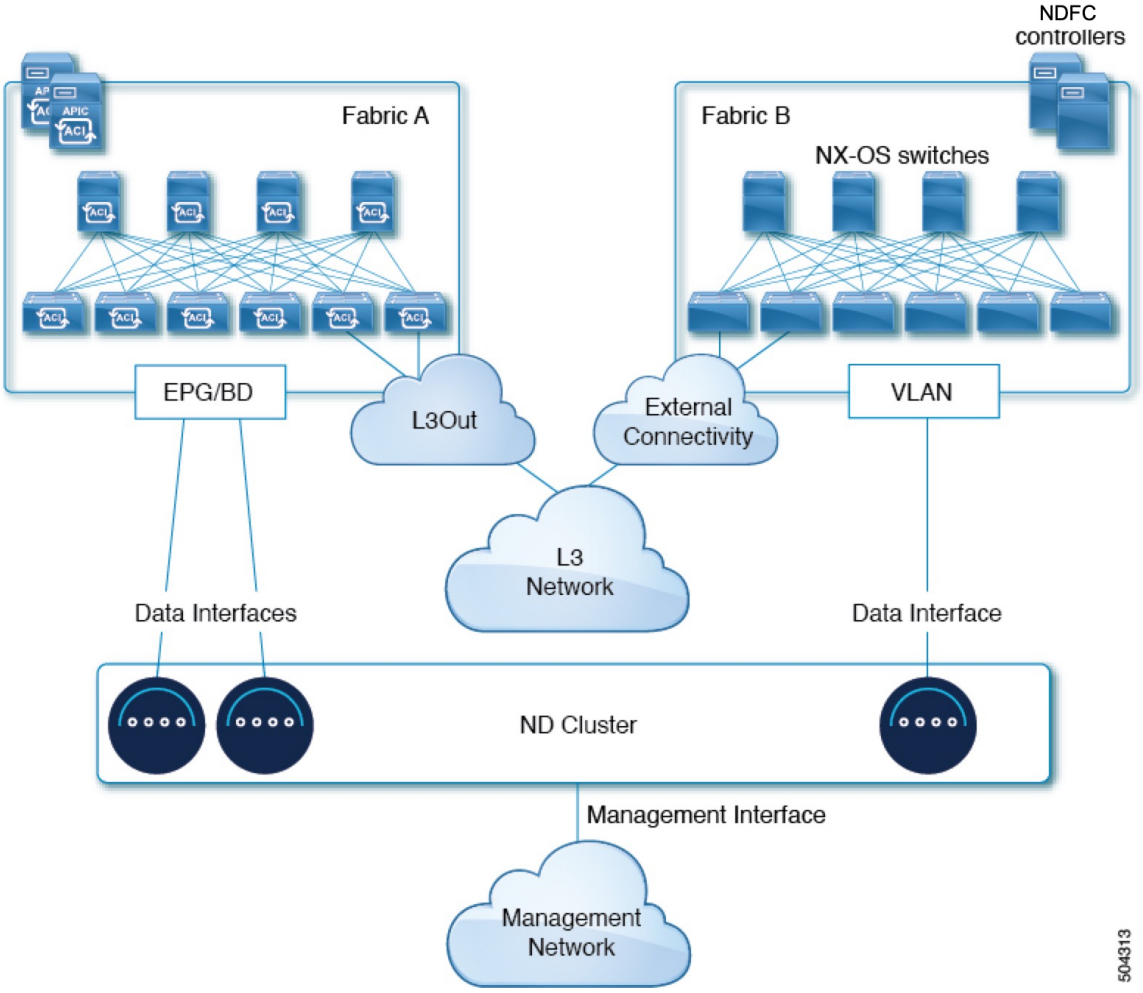
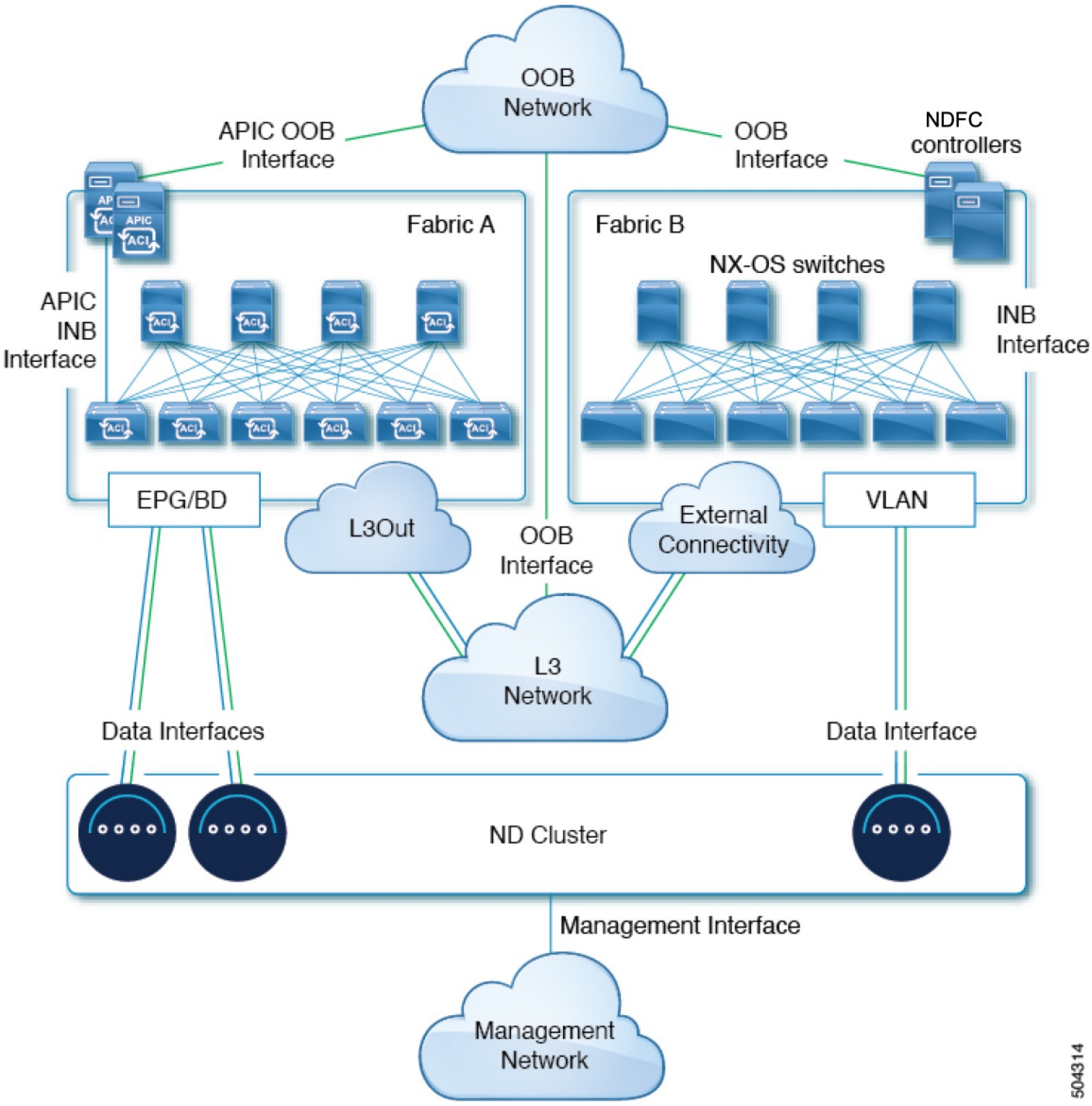


図 *4 :* リーフ スイッチ、*Nexus* ダッシュボード オーケストレータへの直接接続



サイト間のノード分散

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

Nexus Dashboard Insights のノード配布

Nexus Dashboard Insights サービスには、一元化された単一サイトの展開をお勧めします。このサービスは、2 つのプライマリ ノードが使用できない場合には回復をサポートしていないため、

分散クラスタからの冗長性の利点は得られません。むしろ、ノードが異なるサイトにある場合、クラスタで相互接続障害が発生する可能性があります。

ファブリック コントローラのノード分散

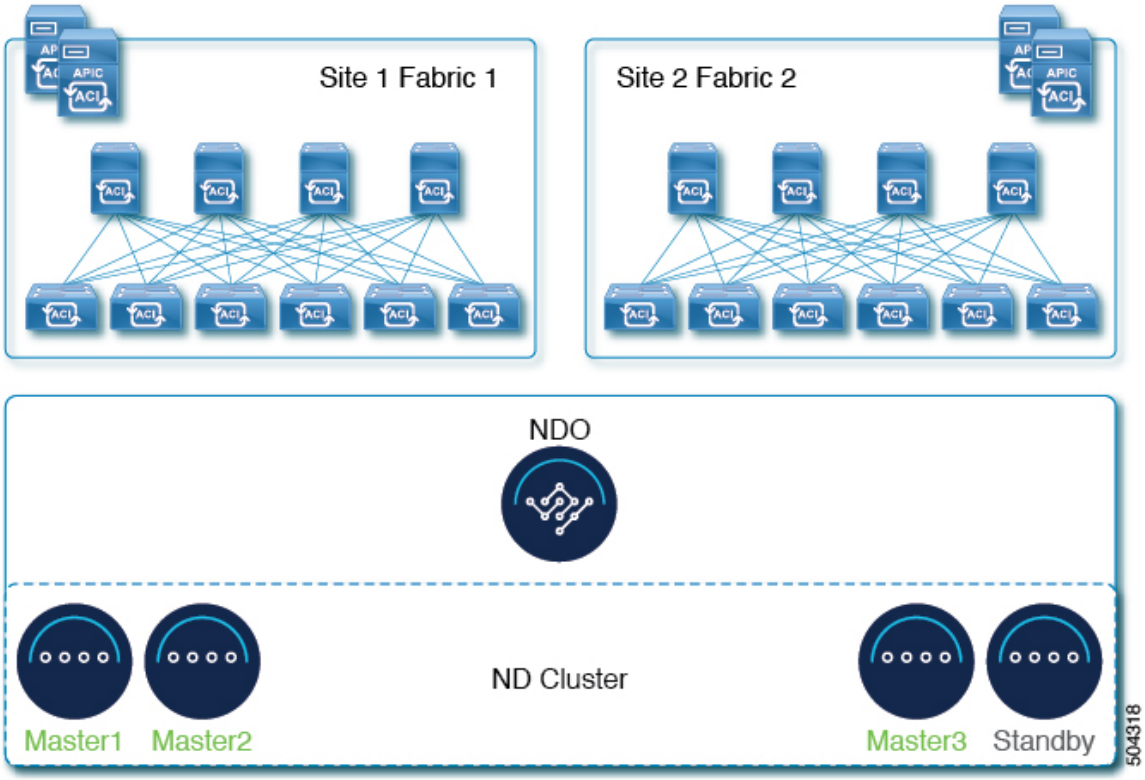
Nexus Dashboard Fabric Controller には、一元化された単一サイトの展開をお勧めします。このサービスは、2 つのプライマリ ノードが使用できない場合には回復をサポートしていないため、分散クラスタからの冗長性の利点は得られません。むしろ、ノードが異なるサイトにある場合、クラスタで相互接続障害が発生する可能性があります。

Nexus Dashboard Orchestrator のノードの分散

Nexus Dashboard Orchestrator の場合は、分散クラスタをお勧めします。クラスタが動作し続けるには、少なくとも 2 つの Nexus Dashboard プライマリ ノードが必要であるため、Nexus Dashboard クラスタを 2 つのサイトに展開する場合は、次の図に示すように、1 つのプライマリ ノードを持つサイトにスタンバイ ノードを展開することを推奨します。

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

図 *5 : Nexus* ダッシュボード オーケストレータの *2* つのサイトにまたがるノードの分散



サービスのコロケーションの使用例

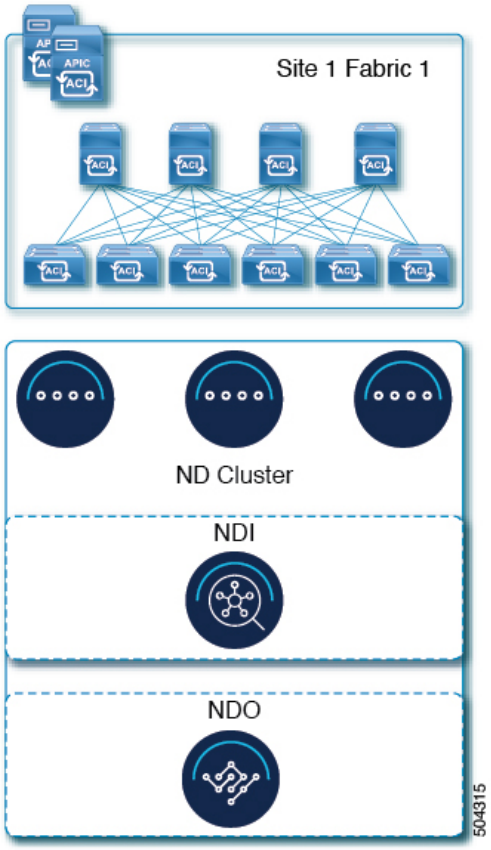
このセクションでは、特定の単一サービスまたは複数サービスの共同ホストの使用例について、いくつかの推奨される展開シナリオについて説明します。

（注） このリリースは、Linux KVM、AWS、Azure、または RHEL に展開されている Nexus ダッシュボードクラスタでの共同ホスティングサービスをサポートしていません。以下のすべてのサービス共同ホスティングのシナリオは、物理フォームファクタまたはVMwareESXクラスタフォームファクタに適用されます。クラスタのサイジングと展開計画の参考情報については、Cisco Nexus Dashboard Cluster Sizing tool を参照してください。

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

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

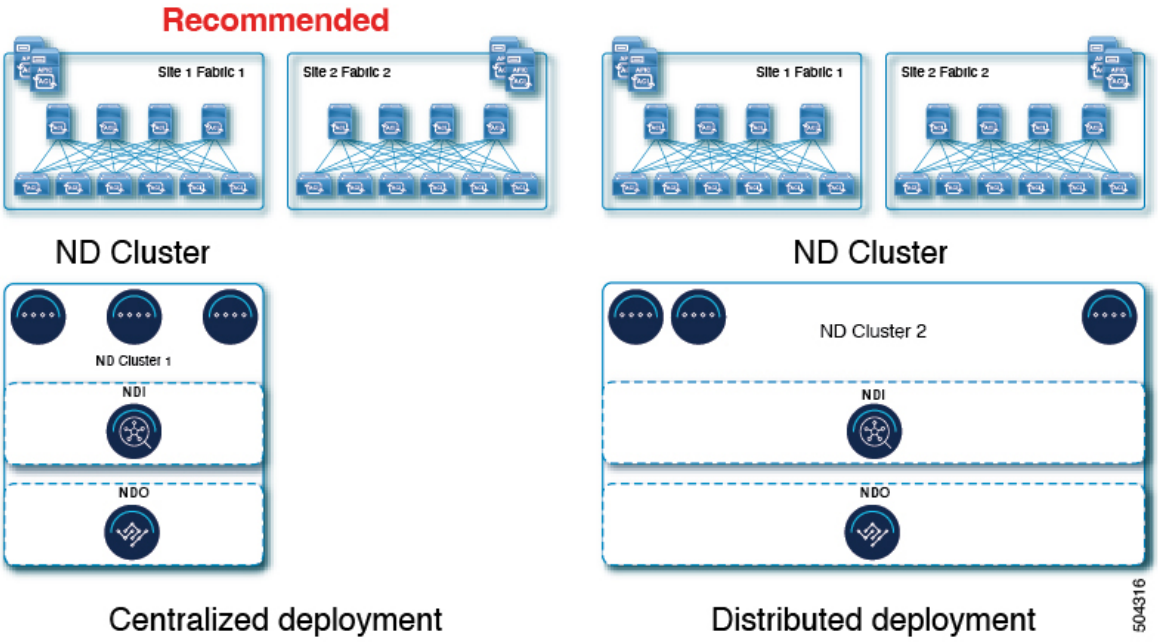
図 *6 :* 単一サイト、*Nexus* ダッシュボード *Insights* およびオーケストレータ



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

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

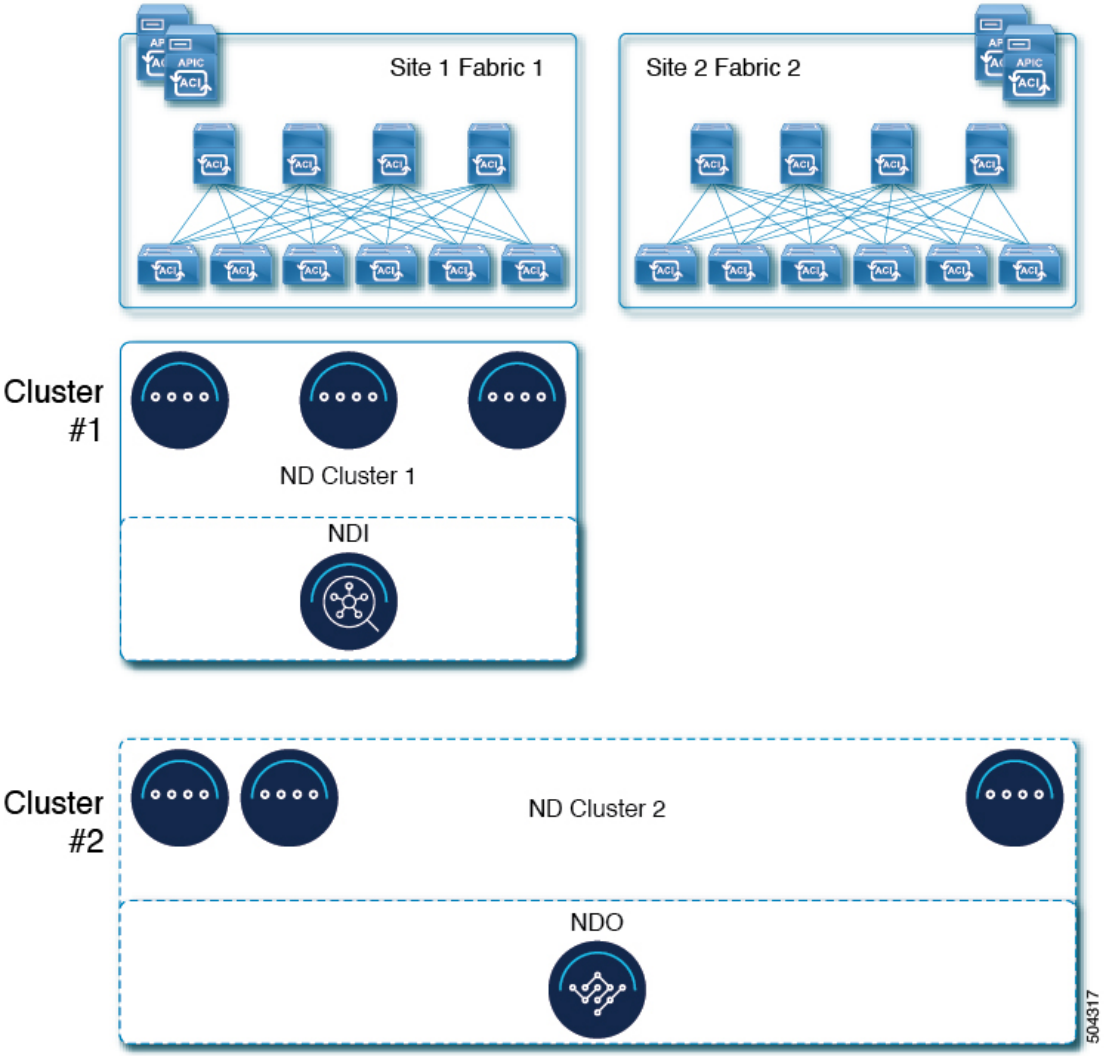
図 *7: Nexus* ダッシュボード *Insights* およびオーケストレータの複数サイト、単一クラスタ



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

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

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



インストール前のチェックリスト

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

表 *6 :* クラスタの詳細

パラメータ（Parameters）	例	入力する値
クラスタ名	nd-cluster	
NTP サーバー	170.78.48.55	

パラメータ（Parameters）	例	入力する値
DNS プロバイダー	170.71.68.83	
DNS 検索ドメイン	cisco.com	
アプリ ネットワーク	172.17.0.0/16	
サービスネットワーク	100.80.0.0/16	

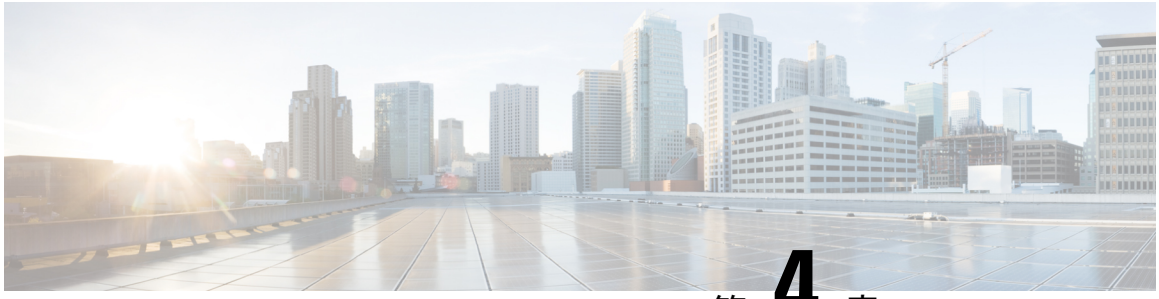
（注） リリース 3.1(1) 以降では、クラスタの初期展開時に、 セカンダリ ノードとスタンバイ ノードを含むすべてのノードを定義できます。わかりやすくするために、次の表では3 ノードの基本クラスタを想定していますが、より大きなクラスタを展開する場合は、すべての追加ノードのノードの詳細も必要です。

表 *7:* ノードの詳細

パラメータ（Parameters）	例	入力する値
物理ノードの場合、最初のノードの **CIMC** アドレスとログイン情報	10.196.220.84/24 ユーザ名: admin パスワード：Cisco1234	
物理ノードの場合、2 番目のノードの **CIMC** アドレスとログイン情報	10.196.220.85/24 ユーザ名: admin パスワード：Cisco1234!	
物理ノードの場合、3 番目のノードの **CIMC** アドレスとログイン情報	10.196.220.86/24 ユーザ名: admin パスワード：Cisco1234!	
各ノードのレスキュー ユーザに使用される**パスワード**と初期 GUIパスワード。 クラスタ内のすべてのノードに同じパスワードを設定することを推奨します。	Welcome2Cisco!	
最初のノードの **管理 IP**	192.168.11.172/24	
最初のノードの**管理ゲートウェイ**	192.168.11.1	

パラメータ（Parameters）	例	入力する値
最初のノードの**データ ネットワーク IP**	192.168.8.172/24	
最初のノードの**データ ネットワーク ゲートウェイ**	192.168.8.1	
（オプション）最初のノードの**データ ネットワーク VLAN**	101	
BGP を有効にする場合、最初のノードの **ASN**	63331	
BGP を有効にし、純粋な IPv6 展開を使用する場合、最初のノードの**ルータ ID**（IPv4 アドレスの形式）	1.1.1.1	
BGP を有効にする場合、最初のノードの **BGP ピア**の IP アドレス	200.11.11.2] または [200:11:11::2	
BGP を有効にする場合、最初のノードの **BGP ピア**の ASN	55555	
2 番目のノードの**管理 IP**	192.168.9.173/24	
2 番目のノードの**管理ゲートウェイ**。	192.168.9.1	
2 番目のノードの**データ ネットワーク IP**	192.168.6.173/24	
2 番目のノードの**データ ネットワーク ゲートウェイ**	192.168.6.1	
（オプション）2番目のノードの**データ ネットワーク VLAN**	101	
BGP を有効にする場合、2 番目のノードの **ASN**	63331	
BGP を有効にし、純粋な IPv6 展開を使用する場合、2番目のノードの**ルータ ID**（IPv4 アドレスの形式）	2.2.2.2	

パラメータ（Parameters）	例	入力する値
BGP を有効にする場合、2 番目のノードの **BGP ピア**の IP アドレス	200.12.12.2] または [200:12:12::2	
BGP を有効にする場合、2 番目のノードの **BGP ピア**の ASN	55555	
3 番目のノードの**管理 IP**	192.168.9.174/24	
3 番目のノードの**管理ゲートウェイ**。	192.168.9.1	
3 番目のノードの**データ ネットワークIP**	192.168.6.174/24	
3 番目のノードの**データ ネットワーク ゲートウェイ**	192.168.6.1	
（オプション）3番目のノードの**データ ネットワーク VLAN**	101	
BGP を有効にする場合、3 番目のノードの **ASN**	63331	
BGP を有効にし、純粋な IPv6 展開を使用する場合、3番目のノードの**ルータ ID**（IPv4 アドレスの形式）	3.3.3.3	
BGP を有効にする場合、3 番目のノードの **BGP ピア**の IP アドレス	200.13.13.2] または [200:13:13::2	
BGP を有効にする場合、3 番目のノードの **BGP ピア**の ASN	55555	



第 4 章

前提条件：ファブリックコントローラ

- ファブリック コントローラの要件 （33 ページ）
- Fabric Controller の通信ポート （36 ページ）

ファブリック コントローラの要件

概要

Nexus Dashboard Fabric Controller（NDFC）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、および IP Fabric for Media（IPFM）ネットワークにまたがるすべての NX-OS 展開向けの包括的な管理ソリューションです。Cisco Nexus Dashboard Fabric Controller 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 Cisco Nexus Dashboard Fabric Controller は、VXLAN EVPN、クラシック 3 層、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、Cisco NDFC を SAN コントローラとして有効にすると、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 ファミリインフラストラクチャを自動化します。

NDFC は主に3つの主要な市場セグメントの制御と管理に焦点を当てています。

- VXLAN、マルチサイト、クラシックイーサネット、外部ファブリックを含むLANネットワークは、スタンドアロン NX-OS を実行する Cisco Nexus スイッチをサポートし、さらに IOS-XR、IOS-XE、隣接ホスト、計算機、仮想マシン、コンテナ管理システムにも対応します。
- スタンドアロン NX-OS を実行する Cisco MDS および Cisco Nexus スイッチの SAN ネットワーキング（ストレージアレイ、さらにはホスト、コンピューティング、仮想マシン、およびコンテナ オーケストレーション システムとの統合を含む）。
- スタンドアロン NX-OS として動作する Cisco Nexus スイッチを実行するマルチキャストビデオ実稼働ネットワークのメディア制御、およびサードパーティ製メディア制御システムの追加統合。

NDFC を含む展開モードを使用して Nexus Dashboard を展開した後、次の手順を実行します。

- **ファブリック検出**：LAN 展開を検出、モニタ、および可視化します。
- **ファブリックコントローラ**：メディア展開用のクラシックイーサネット（vPC）、ルーテッド、VXLAN、および IP ファブリック用の LAN コントローラ。
- **SAN コントローラ**：MDS および Nexus スイッチ用の SAN コントローラ。ストリーミングテレメトリによる拡張 SAN 分析。

ネットワーク要件

（注） このセクションでは、ファブリック コントローラ サービスを有効にする場合の追加の要件とガイドラインについて説明します。前提条件とガイドライン （9 ページ） セクションに記載されているプラットフォーム レベルの要件をすでに満たしていることを確認します。

- Nexus Dashboard リリース 3.1.1 以降、サービスを個別にダウンロードする必要がなくなったため、Cisco DC App Center 接続は Nexus Dashboard から削除されました。

  ファブリック コントローラを展開するには、[ソフトウェアのダウンロード（Software Download）]ページから統合インストール イメージをダウンロードします。個々のサービスのインストール イメージは、Cisco DC App Center から入手できなくなりました。

- 前のセクションで述べたとおり、すべての新しい Nexus Dashboard 展開では、管理ネットワークとデータネットワークが異なるサブネットに存在する必要があります。

（注） SAN コントローラのペルソナだけが、データ ネットワークと管理ネットワークに同じサブネットを使用して Nexus Dashboard に展開できます。

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

表 *8*: ファブリック コントローラの *RTT* 要件

接続	最大 RTT
スイッチ	200 ms*

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

- 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。

LAN 展開タイプで **[LAN デバイス管理の接続性（LAN Device Management Connectivity）]** が ［管理（Management）］に設定されている場合（デフォルト）：

- SNMP/Syslog および SCP サービス用の**管理ネットワーク**内に 2 つの IP
- [EPL] が有効になっている場合、各ファブリックのデータネットワークに 1 つの追加 IP
- メディア用 IP ファブリックが有効になっている場合は、次のいずれかになります。
  - シングル ノード ND のテレメトリ用の **管理ネットワーク** に 1 つの追加 IP
  - 3 ノード ND クラスタのテレメトリ用の **管理ネットワーク** に 3 つの追加 IP

LAN 展開タイプで **[LAN デバイス管理の接続性（LAN Device Management Connectivity）]** が ［データ（Data）］に設定されている場合：

- SNMP/Syslog および SCP サービス用の**データネットワーク**に 2 つの IP
- [EPL] が有効になっている場合、各ファブリックのデータネットワークに 1 つの追加 IP
- メディア用 IP ファブリックが有効になっている場合は、次のいずれかになります。
  - シングル ノードNDのテレメトリ用の **データ ネットワーク** に 1 つの追加 IP
  - マルチノード ND クラスタのテレメトリ用の **データ ネットワーク** に 3 つの追加 IP
- LAN 展開タイプのレイヤ 3 モードで動作している場合は、**[LAN デバイス管理接続（LAN Device Management Connectivity）]** を ［データ（Data）］に設定する必要があり、すべての永続 IP は、ND 管理サブネットまたはデータ サブネットとは重複しない別のプールの一部である必要があります。

SAN コントローラ展開タイプのレイヤ 2 モードで動作している場合：

- SSH 用の 1 つの IP
- SNMP/Syslog 用の 1 つの IP
- SAN Insights の機能に対して、Nexus Dashboard クラスタ ノードごとに 1 つの IP

永続 IP 機能の概要については、前提条件とガイドライン （9 ページ）を参照してください。永続的な IP アドレスの割り当ては、最初のクラスタ展開のときに行うこともできますし、クラスタの展開後に UI の外部サービス プール設定を使用して行うこともできます。

Fabric Controller の通信ポート

上記の Nexus Dashboard クラスタ ノードに必要なポート（前のセクションに記載）に加えて、Fabric Controller サービスには次のポートが必要です。

- 次のポートは、NDFC サービスからスイッチへの IP の到達を可能にしているインターフェイスに応じて、Nexus Dashboard 管理ネットワークとデータ ネットワーク インターフェイスに適用されます。

表 *9 : Nexus Dashboard Fabric Controller* ポート

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

サービス	ポート	プロトコル	方向 ィン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	接続 （特に明記されていない限り、**LAN** と **SAN** の両方の展開に適用されます）
DHCP	67	UDP	入力	NDFC ローカル DHCP サーバーがブートストラップ/POAP 用に構成されている場合。 これは、LAN 展開にのみ適用されます。 （注） POAP の目的でローカル DHCP サーバーとして NDFC を使用する場合、すべての ND マスター ノードの IP を DHCP リレーとして構成する必要があります。ND ノードの管理 IP またはデータ IP が DHCP サーバーにバインドされるかどうかは、NDFC サーバー設定の LAN デバイス管理接続によって決定されます。
DHCP	68	UDP	発信	
SNMP	161	TCP/UDP	アウト	NDFC からデバイスへの SNMP トラフィック。
HTTPS/HTTP（NX-API）	443/80	TCP	発信	NX-API HTTPS/HTTP クライアントは、構成可能でもあるポート 443/80 でデバイスの NX-API サーバーに接続します。NX-API はオプション機能であり、NDFC 機能の限られたセットで使用されます。 これは、LAN 展開にのみ適用されます。

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

- 次のポートは、一部の NDFC サービスで使用される、永続的 IP とも呼ばれる外部サービス IP に適用されます。

  これらの外部サービス IP は、構成された設定に応じて、Nexus Dashboard の管理サブネット プールまたはデータ サブネット プールから取得できます。

表 *10 : Nexus Dashboard Fabric Controller* 永続的 *IP* ポート

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

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

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

サービス	ポート	プロトコル	方向 イン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	接続 （特に明記されていない限り、**LAN** と **SAN** の両方の展開に適用されます）
BGP	179	TCP	入力 / 出力	エンドポイント ロケーターの場合、有効になっているファブリックごとに、独自の永続的な IP を使用して EPL サービスが生成されます。このサービスは、常に Nexus Dashboard データ インターフェイスに関連付けられています。エンドポイント情報を追跡するために必要な BGP アップデートを取得するために、ファブリック上の適切な BGP エンティティ（通常は BGP ルート リフレクタ）と NDFC EPL サービスはピアを行います。 この機能は、VXLAN BGP EVPN ファブリックの展開にのみ適用されます。 これは、LAN 展開にのみ適用されます。

サービス	ポート	プロトコル	方向 ィン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	接続 （特に明記されていない限り、**LAN** と **SAN** の両方の展開に適用されます）
HTTPS（POAP）	443	TCP	入力	セキュア POAP は、ポート 443 の NDFC HTTPS サーバーを介して実現されます。HTTPS サーバーは SCP-POAP サービスにバインドされ、そのポッドに割り当てられたのと同じ永続的 IP を使用します。 NDFC の SCP-POAP サービスには、管理サブネットまたはデータサブネットのいずれかに関連付けられた永続的な IP があります。これは、NDFC サーバー設定の [LAN デバイス管理接続（LAN Device Management Connectivity）] 設定によって制御されます。 これは、LAN 展開にのみ適用されます。
Syslog	514	UDP	入力	NDFC が Syslog サーバーとして構成されている場合、デバイスからの Syslog は、SNMP-Trap/Syslog サービス ポッドに関連付けられた永続的な IP に向けて送信されます。 NDFC の SNMP-Trap-Syslog サービスには、管理サブネットまたはデータサブネットのいずれかに関連付けられた永続的な IP があります。これは、NDFC サーバー設定の [LAN デバイス管理接続（LAN Device Management Connectivity）] 設定によって制御されます。

サービス	ポート	プロトコル	方向 イン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	接続 （特に明記されていない限り、**LAN** と **SAN** の両方の展開に適用されます）
SCP	2022	TCP	発信	NDFC POAP-SCP ポッドの永続的な IP から、Nexus Dashboard Insights を実行している別の ND クラスターにテクニカル サポート ファイルを転送します。 NDFC の SCP-POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続的な IP があります。これは、NDFC サーバー設定の LAN デバイス管理接続設定によって制御されます。
SNMP トラップ	2162	UDP	入力	デバイスから NDFC への SNMP トラップは、SNMP-Trap/Syslog サービス ポッドに関連付けられた永続的な IP に向けて送信されます。 NDFC の SNMP-Trap-Syslog サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続的な IP があります。これは、NDFC サーバー設定の [LAN デバイス管理接続（LAN Device Management Connectivity）] 設定によって制御されます。

サービス	ポート	プロトコル	方向 ィン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	接続 （特に明記されていない限り、**LAN** と **SAN** の両方の展開に適用されます）
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、NDFC 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的な IP で実行されます。これは、NDFC サーバー設定の **[LAN デバイス管理接続（LAN Device Management Connectivity）]** 設定によって制御されます。 これは、LAN 展開にのみ適用されます。
HTTPS（PnP）	9667	TCP	入力	
GRPC（テレメトリ）	33000	TCP	入力	NDFC 永続的 IP に関連付けられた GRPC トランスポートを介して SAN データ (ストレージ、ホスト、フローなど) を受信する SAN Insights Telemetry サーバー。 これは、SAN 展開でのみ有効です。

サービス	ポート	プロトコル	方向 ィン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	接続 （特に明記されていない限り、**LAN** と **SAN** の両方の展開に適用されます）
GRPC（テレメトリ）	50051	TCP	入力	メディア展開用の IP ファブリックおよび一般的な LAN 展開用の PTP のマルチキャスト フローに関連する情報は、ソフトウェア テレメトリを介して、NDFC GRPC レシーバー サービス ポッドに関連付けられた永続的 IP にストリーミングされます。 これは、LAN およびメディア展開でのみ有効です。

- 単一ノード クラスタでの NDFC SAN 展開には、次のポートが必要です。

表 *11 :* 単一ノード クラスタでの *SAN* 展開向けの *Nexus Dashboard Fabric Controller* ポート

サービス	ポート	プロトコル	方向 ィン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	接続 （特に明記されていない限り、**LAN** と **SAN** の両方の展開に適用されます）
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。

サービス	ポート	プロトコル	方向 イン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	接続 （特に明記されていない限り、**LAN** と **SAN** の両方の展開に適用されます）
SCP	22	TCP	発信	NDFC バックアップ ファイルをリモート サーバーにアーカイブする SCP クライアント。
SMTP	25	TCP	発信	SMTP ポートは、NDFC の [サーバー設定（Server Settings）] メニューから構成できます。 これはオプションの機能です。
SNMP	161	TCP/UDP	アウト	NDFC からデバイスへの SNMP トラフィック。

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

- 次のポートは、一部の NDFC サービスで使用される、永続的 IP とも呼ばれる外部サービス IP に適用されます。

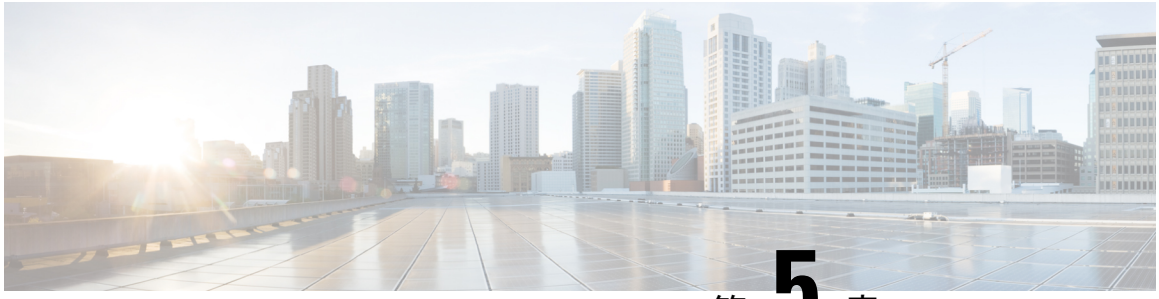
  これらの外部サービス IP は、構成された設定に応じて、Nexus Dashboard の管理サブネット プールまたはデータ サブネット プールから取得できます。

表 *12 :* 単一ノード クラスタでの *SAN* 展開向けの *Nexus Dashboard Fabric Controller* 永続的 *IP* ポート

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

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

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



第 5 章

前提条件：オーケストレータ

- Orchestrator の要件 （53 ページ）
- Orchestrator の通信ポート （54 ページ）
- オーケストレータのファブリック要件 （55 ページ）

Orchestrator の要件

（注） このセクションでは、Orchestrator サービスを有効にする場合の追加の要件とガイドラインについて説明します。前提条件とガイドライン （9 ページ） セクションに記載されているプラットフォーム レベルの要件をすでに満たしていることを確認します。

- Nexus Dashboard リリース 3.1.1 以降、サービスを個別にダウンロードする必要がなくなったため、Cisco DC App Center 接続は Nexus Dashboard から削除されました。

  Orchestrator を展開するには、[ソフトウェアのダウンロード（Software Download）] ページから統合インストール イメージをダウンロードします。個々のサービスのインストール イメージは、Cisco DC App Center から入手できなくなりました。

- Cisco ACI ファブリックを管理するために Nexus Dashboard Orchestrator を展開する場合は、データ インターフェイスまたは管理インターフェイスから各サイトの APIC のインバンドまたはアウトオブバンド（OOB）インターフェイス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。

- Cisco NDFC ファブリックを管理するために Nexus Dashboard Orchestrator を展開する場合は、データネットワークから Cisco NDFC サイトにインバンドで到達できる必要があります。

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

表 *13 : Orchestrator RTT* の要件

接続	最大 RTT
管理対象 APIC サイトへ	500 ミリ秒
管理対象 NDFC サイトへ	150 ミリ秒

Orchestrator の通信ポート

上記の Nexus Dashboard クラスタ ノードに必要なポート（前のセクションに記載）に加えて、Orchestrator サービスには次のポートが必要です。

表 *14 : Nexus Dashboard Orchestrator* ポート（管理ネットワーク）

サービス	ポート	プロトコル	方向 イン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	接続
SCP または SFTP	22	TCP	入力 / 出力	バックアップを保存し、ソフトウェアアップグレード イメージをダウンロードするためのリモート サーバー
HTTP	80	TCP	発信	外部ログストリーミングが有効になっている場合は、Splunk または syslog サーバー
HTTPS	443	TCP	入力 / 出力	外部ログストリーミングが有効になっている場合は、Splunk または syslog サーバー

表 *15 : Nexus Dashboard Orchestrator* ポート（データ ネットワーク）

サービス	ポート	プロトコル	方向 イン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	接続
HTTPS	443	TCP	発信	スイッチと APIC の帯域内

オーケストレータのファブリック要件

次の追加のファブリック関連のガイドラインがオーケストレータ サービスに適用されます。

- Cisco Mini ACI ファブリックは、追加の設定を必要とせずに、一般的なオンプレミス サイトとしてサポートされます。

  このタイプのファブリックの導入と設定に関する詳細情報は、*Cisco Mini ACI ファブリックおよび仮想 APIC*に記述されています。

- リモート リーフ スイッチを含む ACI ファブリックを管理している場合は、次の制限が適用されます。
  - 物理リモート リーフ スイッチのみがサポートされます。
  - -EX および -FX 以降のスイッチのみが、リモート リーフ スイッチとしてサポートされています。
  - リモート リーフは、IPN スイッチを使用しないバックツーバック接続サイトではサポートされていません。
  - 1 つのサイトのリモート リーフ スイッチで別のサイトの L3Out を使用することはできません。
  - あるサイト（ローカル リーフまたはリモート リーフ）と別のサイトのリモート 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。

  また、Nexus Dashboard Orchestrator でサイトを追加して管理するには、その前に次のタスクを実行する必要があります。

  - サイトの APIC でリモート リーフの直接通信を直接有効にする必要があります。

    直接通信を有効にするには、サイトの APIC にログインし、**[システム（System）]** > **[システム設定（System Settings）]** > **[ファブリック全体の設定（Fabric Wide Setting）]**

を選択し、**[リモート リーフ直接トラフィック転送を有効にする（Enable Remote Leaf Direct Traffic Forwarding）]** をオンにします。

（注） 有効にした後は、このオプションを無効にすることはできません。

- リモート リーフ スイッチの外部 TEP プールを設定する必要があります。

  1 つ以上の外部 TEP プールを設定するには、サイトの APIC にログインし、**[ファブリック（Fabric）]** > **[インベントリ（Inventory）]** > **[ポッド ファブリック セットアップ ポリシー（Pod Fabric Setup Policy）]**に移動します。次に、サブネットを設定するポッドをダブルクリックし、**[外部 TEP（External TEP）]** 領域で **[+]** をクリックします。最後に、**[IP]**アドレスと**[予約アドレスの数（Reserve Address Count）]**を入力し、状態を [アクティブ（Active）] または [非アクティブ（Inactive）] に設定してから、**[更新（Update）]** をクリックしてサブネットを保存します。

  ルーティング可能な TEP プールを設定する場合は、 /22 から /29 の範囲のネットマスクを指定する必要があります。異なる時点を含め、複数の非連続外部 TEP プールを設定できます。

- リモート リーフ スイッチに接続しているレイヤ 3 ルータのインターフェイスに適用されている DHCP リレー設定で、APIC ノード（定義済み外部 TEP プールから割り当てられたもの）のルーティング可能な IP アドレスを追加する必要があります。

  各 APIC ノードのルーティング可能な IP アドレスは、APIC GUI の **[システム（System）]** > **[コントローラ（Controllers）]** > **[<controller-name>]**画面の **[ルーティング可能 IP アドレス（Routable IP Address）]** フィールドに表示されます。

- 次のセクションの説明に従って、ポッド プロファイル、ポリシー グループ、およびファブリック アクセス ポリシーを設定する必要があります。

ポッド プロファイルとポリシー グループ

各サイトの APIC には、ポッド ポリシー グループを持つポッド プロファイルが 1 つ必要です。サイトにポッド ポリシー グループがない場合は、作成する必要があります。通常、これらの設定はすでに存在していて、ファブリックを最初に展開したときに設定したとおりになっているはずです。

手順

ステップ 1 サイトの APIC GUI にログインします。

ステップ 2 ポッド プロファイルにポッド ポリシー グループが含まれているかどうかを確認します。

[ファブリック (Fabric)] > **[ファブリック ポリシー (Fabric Policies)]** > **[ポッド (Pods)]** > **[プロファイル (Profiles)]** > **[ポッドのプロファイルのデフォルト (Pod Profile default)]**に移動します。

ステップ 3 必要であれば、ポッド ポリシー グループを作成します。

a) **[ファブリック (Fabric)]** > **[ファブリック ポリシー (Fabric Policies)]** > **[ポッド (Pods)]** > **[ポリシー グループ (Policy Groups)]**に移動します。

b) **[ポリシー グループ (Policy Groups)]** を右クリックし、**[ポッド ポリシー グループの作成 (Create Pod Policy Groups)]** を選択します。

c) 適切な情報を入力して、[Submit] をクリックします。

ステップ 4 新しいポッド ポリシー グループをデフォルトのポッド プロファイルに割り当てます。

a) **[ファブリック (Fabric)]** > **[ファブリック ポリシー (Fabric Policies)]** > **[ポッド (Pods)]** > **[プロファイル (Profiles)]** > **[ポッド プロファイルのデフォルト (Pod Profile default)]** に移動します。

b) デフォルトのプロファイルを選択します。

c) 新しいポッド ポリシー グループを選択し、**[更新 (Update)]** をクリックします。

ファブリック アクセス グローバル ポリシーの設定

このセクションでは、Nexus Dashboard クラスタにオンボードし、Nexus Dashboard Orchestrator で管理する前に、APIC サイトごとに作成する必要があるグローバル ファブリック アクセス ポリシーの設定について説明します。

手順

ステップ 1 サイトの APIC GUI に直接ログインします。

ステップ 2 メイン ナビゲーション メニューから、**[ファブリック (Fabric)]** > **[アクセス ポリシー (Access Policies)]** を選択します。

サイトを Nexus Dashboard Orchestrator で管理するには、いくつかのファブリック ポリシーを設定する必要があります。APIC の観点からは、ベアメタル ホストを接続していた場合と同様に、ドメイン、AEP、ポリシー グループ、およびインターフェイス セレクタを設定することができます。同じマルチサイト ドメインに属するすべてのサイトに対して、スパイン スイッチ インターフェイスをサイト間ネットワークに接続するための同じオプションを設定する必要があります。

ステップ 3 VLAN プールを指定します。

最初に設定するのは、VLAN プールです。レイヤ 3 サブインターフェイスは VLAN 4 を使用してトラフィックにタグを付け、スパインスイッチをサイト間ネットワークに接続します。

a) 左側のナビゲーション ツリーで、**[プール (Pools)]** > **[VLAN]** を参照します。

b) **[VLAN]** カテゴリを右クリックし、**[VLAN プールの作成 (Create VLAN Pool)]** を選択します。

[**VLAN プールの作成 (CREATE VLAN Pool)**] ウィンドウで、次の項目を指定します。

- [**名前 (name)**] フィールドで、VLAN プールの名前 (たとえば、 `msite`) を指定します。

- [**Allocation Mode (割り当てモード)**]の場合は、[スタティック割り当て(Static Allocation)]を指定します。
- [**Encap ブロック(Encap Blocks)**] の場合は、単一の VLAN 4 だけを指定します。両方の [**Range (範囲)**] フィールドに同じ番号を入力することによって、単一の VLAN を指定できます。

ステップ 4 接続可能アクセス エンティティ プロファイル (AEP) を作成します。

a) 左側のナビゲーションツリーで、**[グローバル ポリシー (Global Policies)]** > **[接続可能なアクセス エントリ プロファイル (Attachable Access Entity Profiles)]** を参照します。

b) **[接続可能なアクセス エンティティ プロファイル (Attachable Access Entry Profiles)]** を右クリックして、**[接続可能なアクセス エンティティ プロファイルの作成 (Create Attachable Access Entity Profiles)]** を選択します。

[接続可能アクセス エンティティ プロファイルの作成(Create Attachable Access Entity Profiles)]] ウィンドウで、AEP の名前 (例：`msite-aep`) を指定します。

c) [**次へ(Next)]**] をクリックして [**送信(Submit)**] します。

インターフェイスなどの追加の変更は必要ありません。

ステップ 5 外部ルーテッド ドメインを設定します。

設定するドメインは、このサイトを追加するときに、Nexus Dashboard Orchestratorから選択するものになります。

a) ナビゲーション ツリーで、**[物理的ドメインと外部ドメイン (Physical and External Domains)]** > **[外部でルーテッド ドメイン (External Routed Domains)]** を参照します。

b) [**外部ルーテッド ドメイン(External Routed Domains)**] カテゴリを右クリックし、[**レイヤ 3 ドメインの作成 (Create Layer 3 Domain)**] を選択します。

[**レイヤ 3 ドメインの作成 (Create Layer 3 Domain)**] ウィンドウで、次の項目を指定します。

- [**名前 (name)**] フィールドで、ドメインの名前を指定します。たとえば、 `msite-l3`です。
- **関連付けられている接続可能エンティティ プロファイル**の場合は、ステップ 4で作成した AEP を選択します。
- **VLAN プール**の場合は、ステップ 3で作成した VLAN プールを選択します。

c) [**送信 (Submit)**] をクリックします。

セキュリティ ドメインなどの追加の変更は必要ありません。

次のタスク

グローバル アクセス ポリシーを設定した後も、ファブリック アクセス インターフェイス ポリシーの設定 （59 ページ） の説明に従って、インターフェイス ポリシーを追加する必要があります。

ファブリック アクセス インターフェイス ポリシーの設定

このセクションでは、各 APIC サイトの Nexus Dashboard Orchestrator で行わなければならないファブリック アクセス インターフェイスの設定について説明します。

始める前に

サイトの APIC では、ファブリック アクセス グローバル ポリシーの設定 （57 ページ） の説明に従って、VLAN プール、AEP、および ドメインなどのグローバル ファブリック アクセス ポリシーを設定しておく必要があります。

手順

ステップ 1 サイトの APIC GUI に直接ログインします。

ステップ 2 メイン ナビゲーション メニューから、**[ファブリック (Fabric)]** > **[アクセス ポリシー (Access Policies)]** を選択します。

前のセクションで設定した VLAN、AEP、およびドメインに加えて、サイト間ネットワーク (ISN) に接続するファブリックのスパイン スイッチ インターフェイスに対してインターフェイス ポリシーを作成します。

ステップ 3 スパイン ポリシー グループを設定します。

a) 左ナビゲーション ツリーで、**[インターフェイス ポリシー (Interface Policie)]** > **[ポリシー グループ (Policy Groups)]** > **[スパイン ポリシー グループ (Spine Policy Groups)]** を参照します。

これは、ベアメタルサーバを追加する方法と類似していますが、リーフ ポリシー グループの代わりにスパイン ポリシー グループを作成する点が異なります。

b) **[スパイン ポリシー グループ (Spine Policy Groups)]** カテゴリーを右クリックして、**[スパイン アクセス ポート ポリシー グループの作成 (Create Spine Access Port Policy Group)]** を選択します。

[**スパイン アクセス ポリシー グループの作成 (Create Spine Access Port Policy Group)**]ウィンドウで、以下のとおり指定します。

- **[名前 (Name)]** フィールドの場合、ポリシー グループの名前を指定します。たとえば `Spine1-PolGrp` です。
- [**リンク レベル ポリシー (Link Level Policy)**] フィールドには、スパイン スイッチと ISN の間のリンク ポリシーを指定します。
- **[CDP ポリシー (CDP Policy)]** の場合、CDP を有効にするかどうかを選択します。
- **[添付したエンティティ プロファイル (Attached Entity Profiel)]**の場合、前のセクションで設定した AEP を選択します。たとえば `msite-aep` です。

c) [**送信 (Submit)**] をクリックします。

セキュリティ ドメインなどの追加の変更は必要ありません。

ステップ 4 スパイン プロファイルを設定します。

a) 左ナビゲーション ツリーで、**[インターフェイス ポリシー (Interface Policies)]** > **[ポリシー グループ (Profiles)]** > **[スパイン ポリシー グループ (Spine Profiles)]** を参照します。

b) **[プロファイル (Profiles)]** カテゴリを右クリックし、**[スパイン インターフェイス プロファイルの作成 (Create Spine Interface Profile]** を選択します。

[スパイン インターフェイス プロファイルの作成 (Create Spine Interface Profile)] ウィンドウで、次のとおり指定します。

- **[名前 (name)]** フィールドに、プロファイルの名前 (`Spine1`など) を指定します。
- **[インターフェイス セレクタ (Interface Selectors)]**では、+ 記号をクリックして、ISN に接続されるスパイン スイッチ上のポートを追加します。次に、**[スパイン アクセス ポート セレクターの作成 (Create Spine Access Port Selector)]** ウィンドウで、次のように指定します。
  - **[名前 (name)]** フィールドに、ポート セレクタの名前を指定します (例: `Spine1`)。
  - **[インターフェイス ID (Interface IDs)]** に、ISN に接続するスイッチ ポートを指定します (例 `5/32`)。
  - **[インターフェイス ポリシー グループ (Interface Policy Group)]** に、前の手順で作成したポリシー グループを選択します (例: `Spine1-PolGrp`)。

それから、**[OK]** をクリックして、ポート セレクタを保存します。

c) **[送信 (Submit)]** をクリックしてスパイン インターフェイス プロファイルを保存します。

ステップ 5 スパイン スイッチ セレクター ポリシーを設定します。

a) 左ナビゲーション ツリーで、**[スイッチ ポリシー (Switch Policies)]** > **[プロファイル (Profiles)]** > **[スパイン プロファイル (Spine Profiles)]** を参照します。

b) **[スパイン プロファイル (Spine Profiles)[** カテゴリを右クリックし、**[スパイン プロファイルの作成 (Create Spine Profile)]** を選択します。

[スパイン インターフェイス プロファイルの作成 (Create Spine Interface Profile)] ウィンドウで、次のように指定します。

- **[名前 (name)]** フィールドに、プロファイルの名前を指定します (例: `Spine1`)。
- **[スパインセレクタ (Spine Selectora)]**で、**[+]** をクリックしてスパインを追加し、次の情報を入力します。
  - **[名前 (name)]** フィールドで、セレクタの名前を指定します (例: `Spine1`) 。
  - **[ブロック (Blocks)]** フィールドで、スパイン ノードを指定します (例: `201`)。

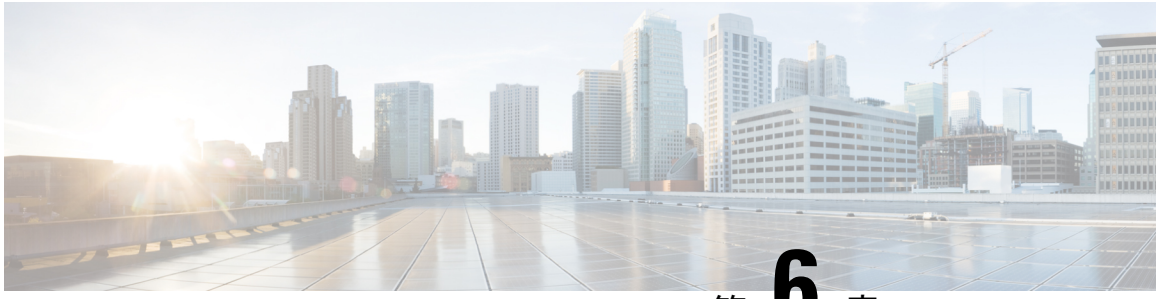
c) **[更新 (Update)]** をクリックして、セレクタを保存します。

d) **[次へ (Next)]** をクリックして、次の画面に進みます。

e) 前の手順で作成したインターフェイス プロファイルを選択します。

たとえば、`Spine1-ISN`などです。

f) **[完了 (Finish)]** をクリックしてスパイン プロファイルを保存します。



第 6 章

前提条件：Insights

- Insights の要件 （63 ページ）
- Insights の通信ポート （65 ページ）
- Insights のファブリック要件 （66 ページ）

Insights の要件

（注） このセクションでは、Insights サービスを有効にする場合の 追加 の要件とガイドラインについて説明します。前提条件とガイドライン （9 ページ） セクションに記載されているプラットフォーム レベルの要件をすでに満たしていることを確認します。

- Nexus Dashboard リリース 3.1.1 以降、サービスを個別にダウンロードする必要がなくなったため、Cisco DC App Center 接続は Nexus Dashboard から削除されました。

  Insight を展開するには、[ソフトウェアのダウンロード（Software Download）] ページから、統合インストール イメージをダウンロードします。個々のサービスのインストール イメージは、Cisco DC App Center から入手できなくなりました。

- Nexus Dashboard Insights サービスの場合、データ ネットワークは、次の接続先に対し IP 到達可能である必要があります。
  - 各ファブリックと APIC のインバンド ネットワーク。
  - DNS サーバー。
  - 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。
  - vCenter 統合の場合は、vCenter への接続。

- AppDynamics 統合の場合は、AppDynamics コントローラへの接続。

- NDFC ファブリックで Insights サービスを使用している場合、または SFLOW/NetFlow を有効にしている場合、データ ネットワーク インターフェイスはレイヤ 2 隣接である必要があります。
- 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 機能の概要については、前提条件とガイドライン （9 ページ）を参照してください。

  ACI ファブリックの場合：

  - Netflow または Panduit PDU 統合を使用しない Nexus Dashboard Insights：データ ネットワークに IP は必要ありません。
  - Panduit PDU 統合を使用する Nexus Dashboard Insights：IPv4 を使用している場合、1 IP。純粋な IPv6 スタックでは統合はサポートされていません。
  - Netflow および Panduit PDU 統合を使用する Nexus Dashboard Insights：IPv4 を使用している場合、データ ネットワーク内に 8 IP。IPv6 を使用している場合、6 IP。
  - Netflow を使用し、Panduit PDU 統合を使用しない Nexus Dashboard Insights：IPv4 を使用している場合、データ ネットワーク内に 8 IP。IPv6 を使用している場合、6 IP。

  NDFC ファブリックの場合：

  - IPv4 を使用している場合、データ ネットワーク内に 8 IP。IPv6 を使用している場合、6 IP。

  スタンドアロンNX-OSスイッチの場合：

  - IPv4 を使用している場合、データ ネットワーク内に 10 IP。IPv6 を使用している場合、8 IP。

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

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

表 *16 : Insights の RTT 要件*

接続	最大 RTT
スイッチ	150 ミリ秒

Insights の通信ポート

上記の Nexus Dashboard クラスタ ノードに必要なポート（前のセクションに記載）に加えて、Insights サービスには次のポートが必要です。

（注） デフォルトでは、Insights は、Nexus Dashboard クラスタノードのデータインターフェイスとスイッチのインバンド IP 間の接続のみを必要とします。ただし、スイッチが使用できなくなった場合、Insights はクラスタ ノードの管理またはデータ インターフェイス（ルート設定に応じて決まる）を使用してスイッチの OOB IP に接続しようとします。

表 *17 : Nexus Dashboard Insights* ポート（データ ネットワーク）

サービス	ポート	プロトコル	方向 イン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	接続
テックコレクションを表示	2022	TCP	入力 / 出力	スイッチと APIC/NDFC の帯域内
フローテレメトリ	5640 ～ 5671	UDP	入力	スイッチの帯域内
TAC アシスト	8884	TCP	入力 / 出力	その他のクラスタ ノード
KMS	9989	TCP	入力 / 出力	その他クラスタ ノードおよび ACI ファブリック
Kafka	30001	TCP	入力 / 出力	スイッチと APIC/NDFC の帯域内 IP
SW テレメトリ	5695 30000 57500 30570	TCP	入力 / 出力	その他のクラスタ ノード

Insights のファブリック要件

ACI ファブリックの追加の前提条件

ACI ファブリックで Insights サービスを使用する場合は、次のことを確認します。

- 同じクラスタ内では、1つのタイプのサイト（ACI、NDFC、またはスタンドアロンNX-OS）のみをオンボードできます。

  同じクラスタ内での ACI と NDFC、ACI と NX-OS、または NDFC と NX-OS の混在オンボーディングはサポートされていません。

- 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。

- Nexus Dashboard Insights でフローテレメトリ機能を使用する計画の場合には、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。

- Nexus Dashboard Insights でフローテレメトリ機能を使用する計画の場合には、Cisco APIC で Precision Time Protocol（PTP）を有効にして、Nexus Dashboard Insights が複数のスイッチからのフローを相互に適切に関連付けることが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、Nexus Dashboard Insights とその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、同じスイッチが Nexus Dashboard Insights のフローマップに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 ダッシュボードのデータ 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。

NDFC 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

NDFC ファブリックまたはスタンドアロン NX-OS スイッチで Insights サービスを使用する場合は、次のことを確認します。

- 同じクラスタ内では、1つのタイプのサイト（ACI、NDFC、またはスタンドアロンNX-OS）のみをオンボードできます。

  同じクラスタ内での ACI と NDFC、ACI と NX-OS、または NDFC と NX-OS の混在オンボーディングはサポートされていません。
- 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、Nexus Dashboard Insights 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。

  管理サイトモードとモニタサイトモードの両方で、サイト内のすべてのノードでPTPが正しく設定されていることを確認する必要があります。NDFC Easy Site Setup の **[詳細（Advanced）]** タブで PTP を有効にするには、**[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します。

PTPグランドマスタークロックは、ネットワークサイト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。Cisco Nexus 9000 シリーズ スイッチを PTP グランドマスターとして使用することはサポートされていません。

（注） ファブリック内の N9k-C93180YC-FX3 スイッチは、PTP GM として使用できます。

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 デバイスは一般に、PTP の標準要件であるナノ秒精度を達成するために GNSS/GPS ソースを備えていますが、Nexus Dashboard Insights とそのフローテレメトリにはマイクロ秒精度で十分であるため、通常は GNSS/GPS ソースは不要です。

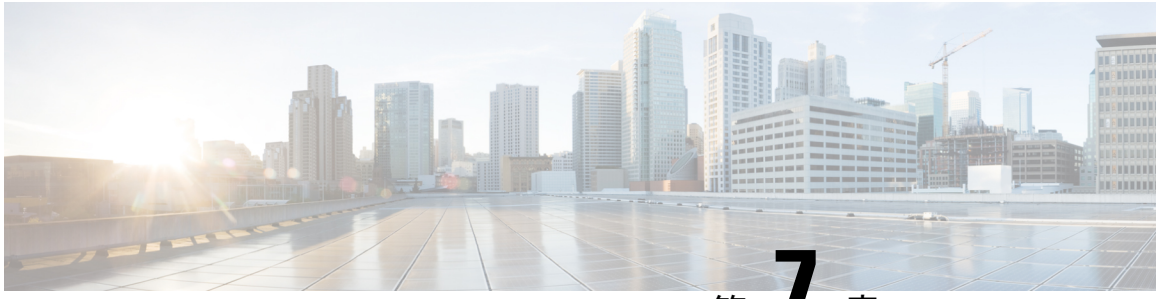
Precision Time Protocol の詳細については、*Cisco NDFC LAN* ファブリック コントローラ 構成ガイドを参照してください。

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。

第 II 部

クラスタの展開

- 物理アプライアンスとしての展開 （71 ページ）
- VMware ESX の展開 （93 ページ）
- Linux KVMでの展開 （137 ページ）
- Amazon Web Services での展開 （157 ページ）
- Microsoft Azure での展開 （173 ページ）
- ファブリックのオンボーディング （191 ページ）



第 7 章

物理アプライアンスとしての展開

- 前提条件とガイドライン （71 ページ）
- 物理ノードのケーブル接続 （75 ページ）
- 物理アプライアンスとしての Nexus ダッシュボードの展開 （77 ページ）

前提条件とガイドライン

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：Nexus Dashboard （9 ページ） に記載されている一般的な前提条件およびサービス固有の前提条件を確認して完了します。
- 展開予定のサービスのリリース ノートに説明されている追加の前提条件を確認し、条件を満たすようにしてください。

  サービス固有のドキュメントは、次のリンクで見つけることができます。

  - Nexus Dashboard ファブリック コントローラ、リリース ノート
  - Nexus Dashboard Insights リリース ノート
  - Nexus Dashboard Orchestrator リリース ノート
- 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、UCS-C220-M5（`SE-NODE-G2`）および UCS-C225-M6（`ND-NODE-L4`）のオリジナルの Cisco Nexus Dashboard プラットフォーム ハードウェアでのみサポートされます。

（注） UCS-C225-M6（ND-NODE-L4）ノードと ACI サイトを含むクラスタで 3.1.1k ソフトウェアの新規仮想メディア インストールを実行すると、NDI または NDO へのサイトのオンボーディングが失敗するという既知の問題が存在します。。この問題の回避策は、ソフトウェアの **3.1.1l** バージョンの新規インストールを実行することです。リリース 3.1.1k から 3.1.1l にアップグレードしても問題は解決しないので、注意してください。この問題を解決するには、3.1.1l ソフトウェアの新規インストールを実行する必要があります。

次の表に、サーバの物理的アプライアンス サーバの PID と仕様を示します。

表 ***18 :*** サポートされる ***UCS-C220-M5*** ハードウェア

プロセス ID（Process ID）	ハードウェア
SE-NODE-G2=	• Cisco UCS C220 M5シャーシ • 2 X 10 コア 2.2 GHz Intel Xeon Silver CPU • 256 GB の RAM • 4 x 2.4-TB HDD 400-GB SSD 1.2 TB NVME ドライブ • Cisco UCS 仮想インターフェイス カード 1455（4x25G ポート） • 1050W 電源モジュール
SE-CL-L3	3 台の `SE-NODE-G2=` アプライアンスのクラスタ。

表 *19* : サポートされる *UCS-C225-M6* ハードウェア

プロセス ID（Process ID）	ハードウェア
ND-NODE-L4=	• Cisco UCS C225 M6 シャーシ • 2.8 GHz AMD CPU • 256 GB の RAM • 4 x 2.4-TB HDD 960-GB SSD 1.6 TB NVME ドライブ • Intel X710T2LG 2x10 GbE（銅） • 次のいずれかが必要です。 • Intel E810XXVDA2 2x25/10 GbE（光ファイバ） • Cisco UCS 仮想インターフェイスカード 1455（4x25G ポート） • 1050W 電源モジュール
ND-CLUSTER-L4	3 台の `ND-NODE-L4=` アプライアンスのクラスタ。

（注） 上記のハードウェアは、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。

  CIMC IP アドレスを構成するには、次の手順を実行します。

  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。

  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。

3. 次の情報を入力します。
   - **NIC モード**を専用モードに設定します。
   - **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。
   - 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。
4. **F10** を押して、構成を保存し、サーバーを再起動します。

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

  SoL は、基本的な構成情報を提供するために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、最初に CIMC で SoL を有効にする必要があります。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。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
```

- 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 2.3.2 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 3.1.1 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 2.3.2 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. 既存の ND クラスタをこのリリースへアップグレード（201 ページ）の説明に従って、リリース 3.1.1 にアップグレードします。

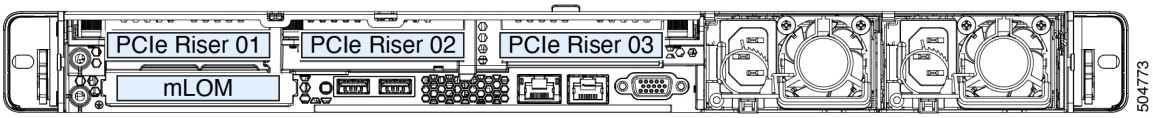
（注） まったく新しい展開の場合は、このドキュメントに戻ってクラスタを展開する前に、Cisco Nexus Dashboard の最新バージョンを使用してノードを再イメージ化することもできます（たとえば、GUI ワークフローを通じたこのリリースへの直接アップグレードをサポートしていないイメージがハードウェアに付属している場合）。このプロセスについては、このリリースのトラブルシューティングの記事の「ノードの再イメージング」セクションで説明されています。

- 少なくとも 3 ノードのクラスタが必要です。展開するサービスのタイプと数に応じて、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。

物理ノードのケーブル接続

物理ノードは、次のガイドラインに従って、UCS-C220-M5（SE-NODE-G2）および UCS-C225-M6（ND-NODE-L4）物理サーバーに展開できます。

図 9: ノード接続に使用される *mLOM* および *PCIe* ライザー *01* カード



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

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と管理インターフェイス用の Linux ボンドとして設定されます。
- 管理ネットワークの場合：
  - mLOM カードで mgmt0 および mgmt1 を使用する必要があります。
  - 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 ネットワークの場合：
  - UCS-C220-M5 サーバーでは、VIC1455 カードを使用する必要があります。
  - UCS-C225-M6 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
```

- すべてのインターフェイスは、個々のホストに向けたスイッチ ポートに接続する必要があります。PortChannel (PC) および Virtual PortChannel (vPC) はサポートされていません。
- すべてのポートは、10G または 25G のいずれかの同じ速度である必要があります。
- ポート 1 は Nexus Dashboard の `fabric0` に対応し、ポート 2 は `fabric1` に対応します。

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

（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。

- UCS-C220-M5 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。
- UCS-C225-M6 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場合は、 `switchport voice vlan dot1p` コマンドをスイッチ インターフェイスに追加する必要があります。

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

物理アプライアンスとしての Nexus ダッシュボードの展開

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。ここでは、最初の Nexus Dashboard クラスタを設定して起動する方法について説明します。

始める前に

- 前提条件とガイドライン （71 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 3.1.1k
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 を指定します。

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 初期ブートストラップ処理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。

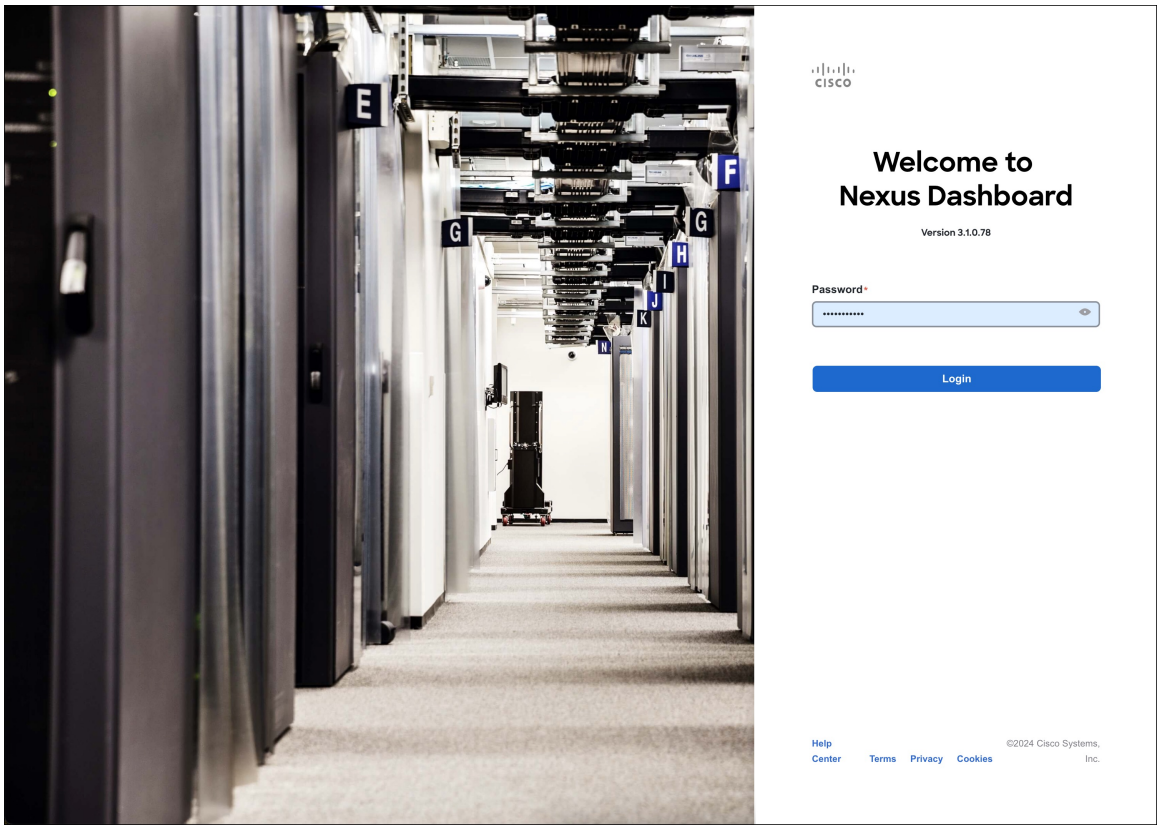
```
Please wait for system to boot: [#########################] 100%
System up, please wait for UI to be online.

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。

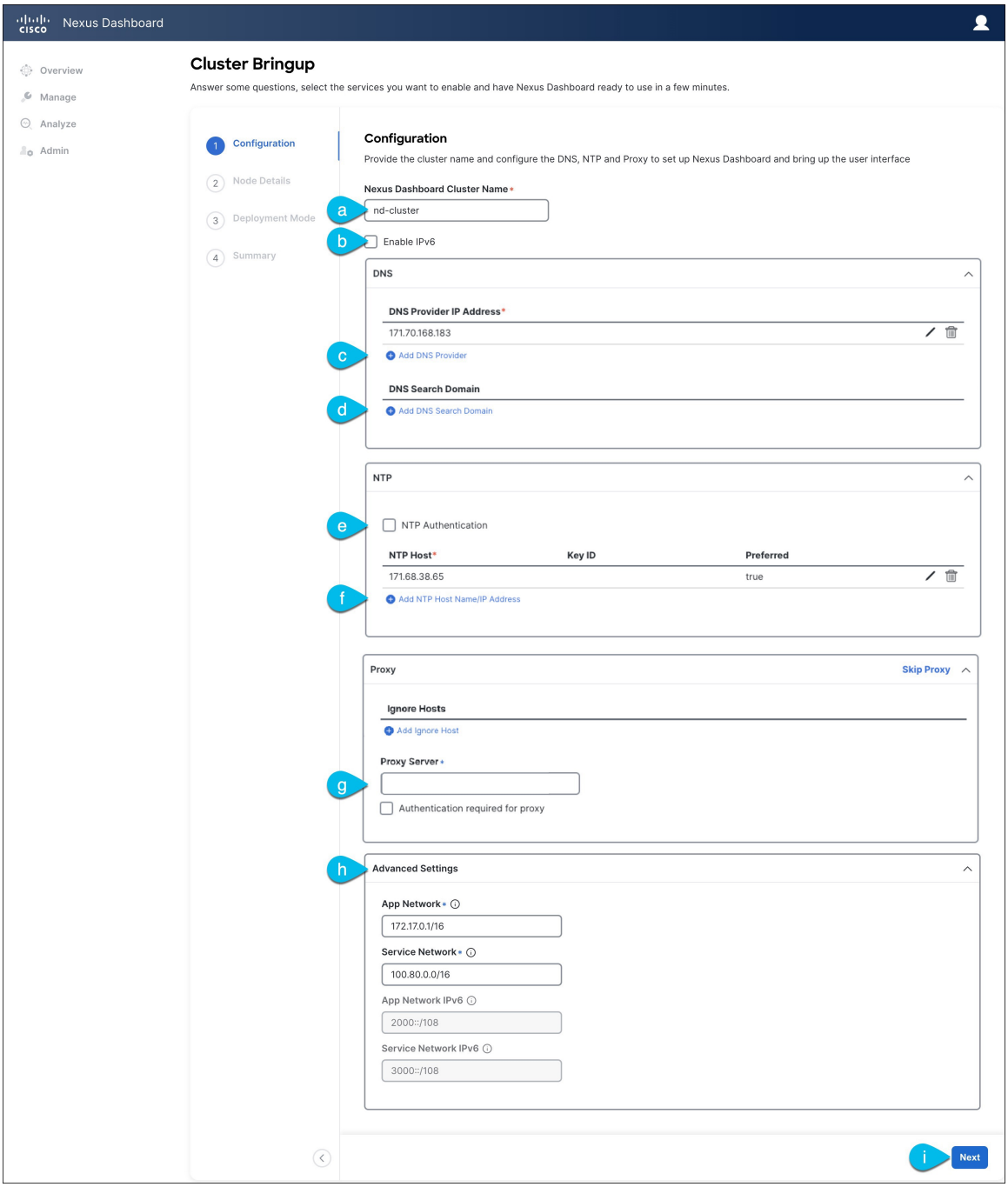
残りの設定ワークフローは、ノードの GUI の 1 つから実行します。展開したノードのいずれか 1 つを選択して、ブートストラッププロセスを開始できます。他の 2 つのノードにログインしたり、これらを直接構成したりする必要はありません。

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 **[クラスタの詳細（Cluster Details）]** を入力します。

[クラスタ起動（Cluster Bringup）] ウィザードの **[クラスタの詳細（Cluster Details）]** 画面で、次の情報を入力します。



a) Nexus ダッシュボード クラスタの **[クラスタ名（Cluster Name）]** 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) （オプション）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。

c) **[+DNS プロバイダの追加（+Add DNS Provider）]** をクリックして、1 つ以上の DNS サーバを追加します。

情報を入力した後、チェックマーク アイコンをクリックして保存します。

d) （オプション）**[+DNS 検索ドメインの追加（+Add DNS Search Domain ）]** をクリックして、検索ドメインを追加します。

情報を入力した後、チェックマーク アイコンをクリックして保存します。

e) （オプション）NTP サーバー認証を有効にする場合には、**[NTP 認証（NTP Authentication）]** チェックボックスをオンにし、**[NTP キーの追加（Add NTP Key）]**をクリックします。

次のフィールドで、以下の情報を提供します。

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

（注）
情報を入力した後、チェックマーク アイコンをクリックして保存します。

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、前提条件とガイドライン （9 ページ） を参照してください。

f) **[+ NTP ホスト名/IP アドレスの追加（+Add NTP Host Name/IP Address）]** をクリックして、1 つ以上の NTP サーバを追加します。

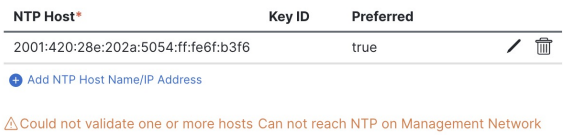
次のフィールドで、以下の情報を提供します。

- **NTP ホスト**：IP アドレスを指定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**：このサーバーの NTP 認証を有効にする場合は、前の手順で定義した NTP キーのキー ID を指定します。

  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 NTP サーバーを **[優先（Preferred）]** にするかどうかを選択します。

情報を入力した後、チェックマーク アイコンをクリックして保存します。

（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（次の手順で指定します）、NTP サーバーの IPv6 アドレスに接続できないためです。

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 サーバーを指定する場合は、**[+NTP ホストの追加（+Add NTP Host）]** を再度クリックし、このサブステップを繰り返します。

g) **[プロキシ サーバー（Proxy Server）]** を指定し、**[検証（Validate）]** をクリックします。

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。

[+無視するホストを追加（+Add Ignore Host）] をクリックして、プロキシをスキップする 1 つ以上の IP アドレス通信を提供することもできます。

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
```

プロキシ設定をスキップする場合は、**[プロキシをスキップ（Skip Proxy）]** をクリックします。

h) (オプション) プロキシ サーバで認証が必要な場合は、**[プロキシで認証が必要（Authentication required for Proxy）]** を **[はい（Yes）]** に変更し、ログイン資格情報を指定します。

i) (オプション) **[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。

- カスタム **App Network** と **Service Network** を提供します。

  アプリケーション オーバーレイ ネットワークは、Nexus ダッシュボードで実行されるアプリケーションのサービスで使用されるアドレス空間を定義します。このフィールドには、デフォルトの `172.17.0.1/16` 値が事前に入力されています。

  サービス ネットワークは、Nexus ダッシュボードとそのプロセスで使用される内部ネットワークです。このフィールドには、デフォルトの `100.80.0.0/16` 値が事前に入力されています。

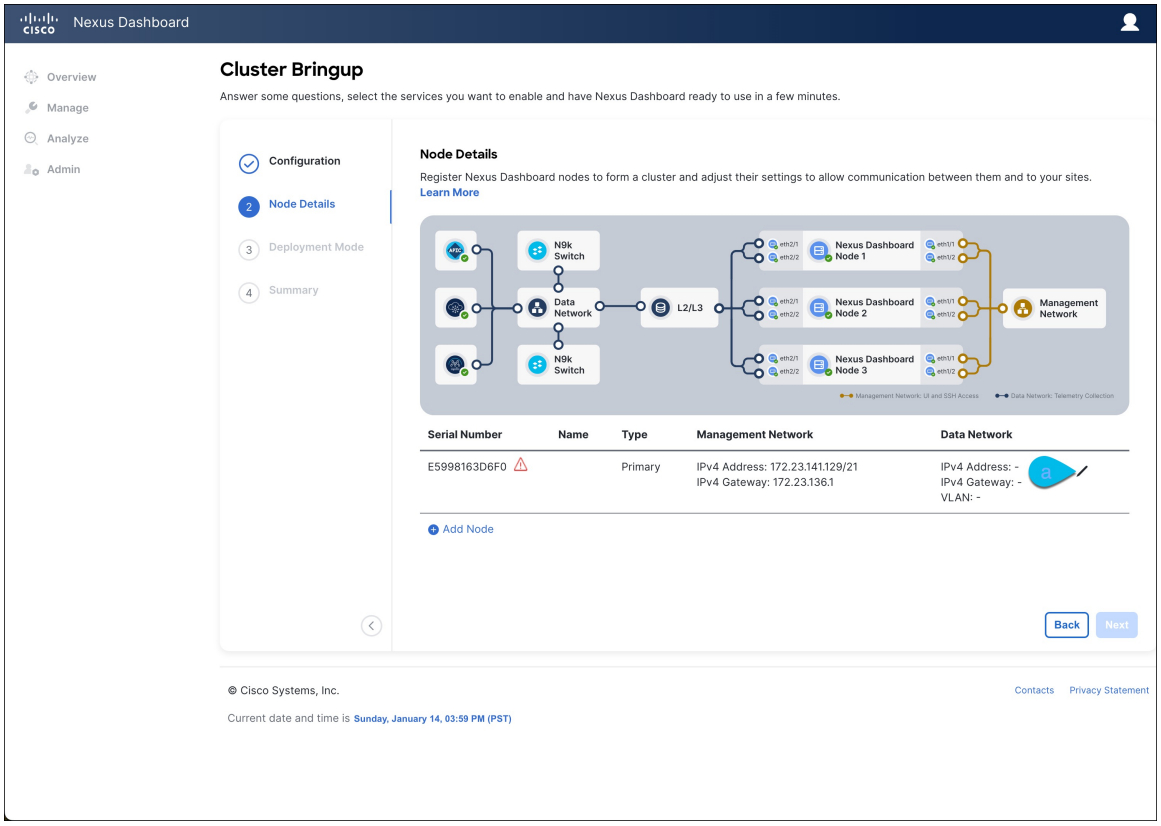
  以前に **[IPv6 を有効にする（Enable IPv6）]** オプションをオンにした場合は、アプリケーション ネットワークとサービス ネットワークの IPv6 サブネットを定義することもできます。

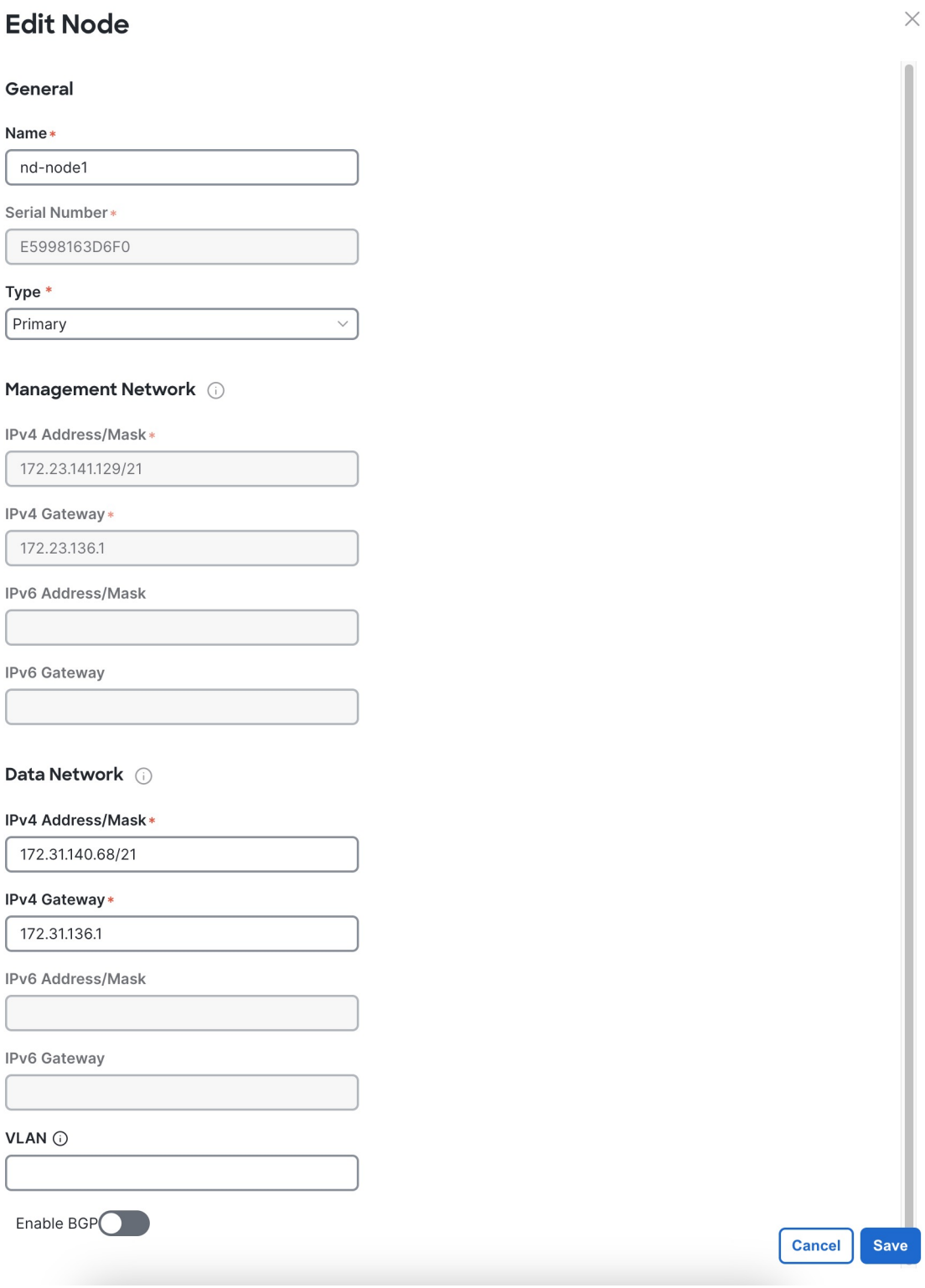
  アプリケーションおよびサービスネットワークについては、このドキュメントの前の 前提条件とガイドライン （9 ページ） の項で説明します。

j) [次へ（Next）] をクリックして続行します。

ステップ 5 **[ノードの詳細（Node Details）]** 画面で、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) 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、他の情報は手動で入力する必要があります。

b) ノードの **[名前（Name）]** 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。

c) **[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。サービスの共同ホスティングや、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。

d) **[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。

e) （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。

Insights やファブリック コントローラなどの、一部のサービスで使用される永続的な IP 機能には、BGP 構成が必要です。この機能については、前提条件とガイドライン （9 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**。

f) **[Save]**をクリックして、変更内容を保存します。

ステップ 6 [**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 **[CIMC IP アドレス（CIMC IP Address）]**、**[ユーザー名（Username）]**、**[パスワード（Password）]** を指定します。

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) ノードの **[名前（Name）]** 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）]** 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。サービスの共同ホスティングや、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**の情報を提供します。

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。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）
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。

g) （任意）必要に応じて、データ ネットワークの **BGP を有効にします**。

Insights やファブリック コントローラなどの、一部のサービスで使用される永続的な IP 機能には、BGP 構成が必要です。この機能については、前提条件とガイドライン （9 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**。

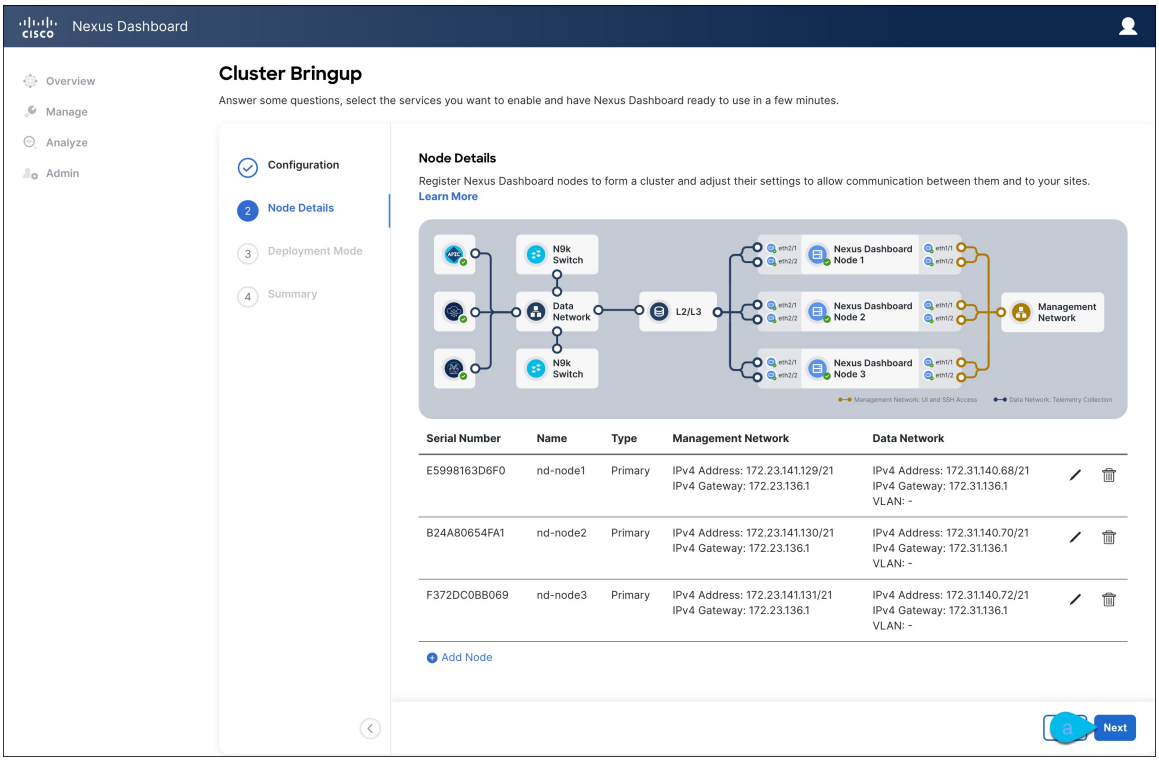
h) **[Save]**をクリックして、変更内容を保存します。
i) クラスタの最後の（3 番目の）プライマリ ノードでこの手順を繰り返します。

ステップ 7 （オプション）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）
クラスタで複数のサービスを同時に有効にするか、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 8 **[ノードの詳細（Node Details）]** ページで、入力した情報を確認し、**[次へ（Next）]** をクリックして続行します。



ステップ 9 クラスタの**展開モード**を選択します。

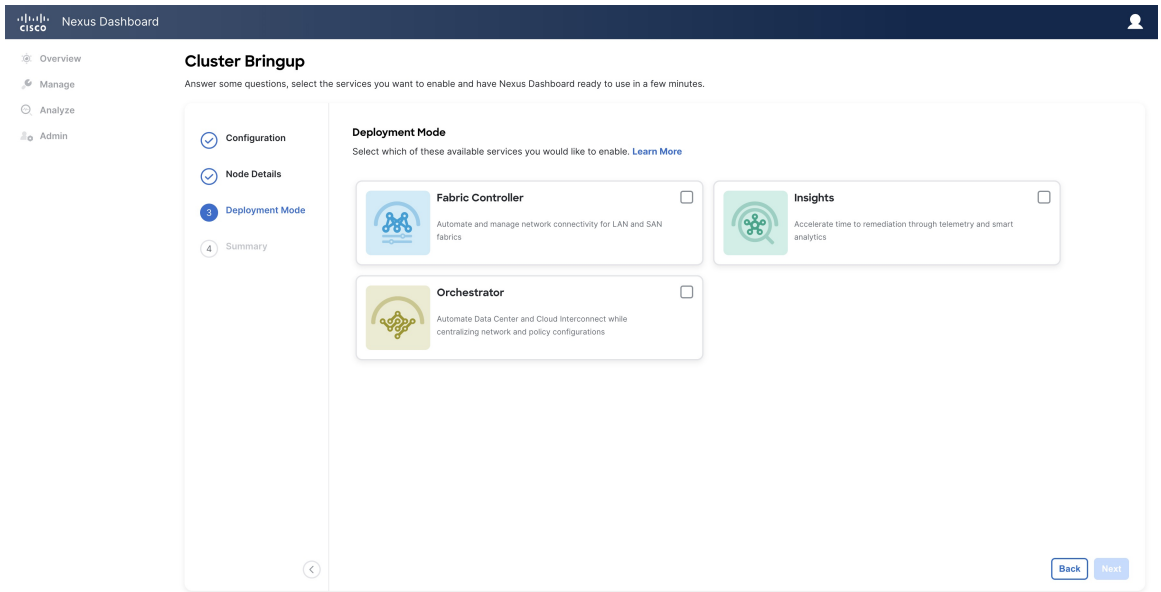
a) 有効にするサービスを選択します。

リリース 3.1(1) より前では、クラスタの初期展開が完了した後に、個々のサービスをダウンロードしてインストールする必要がありました。今では、初期インストール時にサービスを有効にするように選択できます。

（注）
クラスタ内のノードの数によっては、一部のサービスまたは共同ホスティングのシナリオがサポートされない場合があります。必要な数のサービスを選択できない場合は、**[戻る（Back）]** をクリックし、前の手順で十分な数のセカンダリ ノードを指定したことを確認します。

クラスタの展開後に展開モードを変更することはできないため、このドキュメントの前の章で説明されているサービス固有の前提条件をすべて満たしていることを確認する必要があります。

- Nexus Dashboard ファブリック コントローラの前提条件
- Nexus Dashboard オーケストレータの前提条件
- Nexus Dashboard Insights の前提条件



b) ファブリック コントローラまたは Insights を含む展開モードを選択した場合は、**[永続サービス IP/プールの追加（Add Persistent Service IPs/Pools）]** をクリックして、Insights またはファブリック コントローラ サービスに必要な 1 つ以上の永続 IP を指定します。

永続 IP の詳細については、 前提条件とガイドライン （9 ページ） セクションおよびサービス固有の要件の章を参照してください。

c) [次へ（Next）] をクリックして続行します。

ステップ 10 **[概要（Summary）]** 画面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。

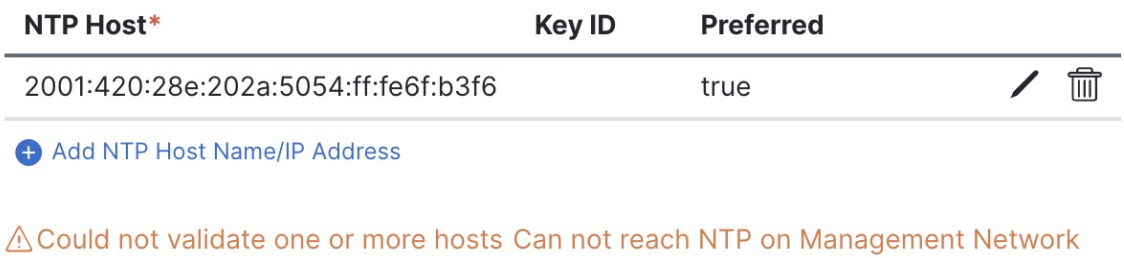
ノードのブート ストラップとクラスタの起動中に、全体的な進捗状況と各ノードの個々の進捗状況がUIに表示されます。ブートストラップの進行状況が表示されない場合は、ブラウザでページを手動で更新し、ステータスを更新してください。

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。

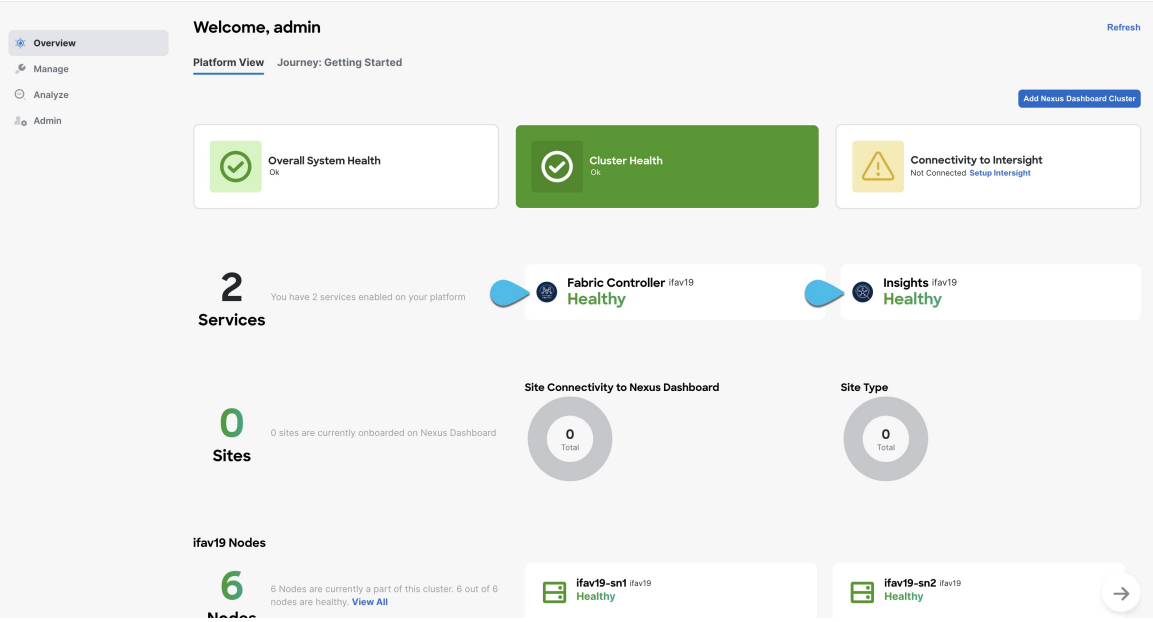
ステップ 11 クラスタが健全であることを検証します。

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、**[概要（Overview）]** ページ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、ノード展開中に指定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。

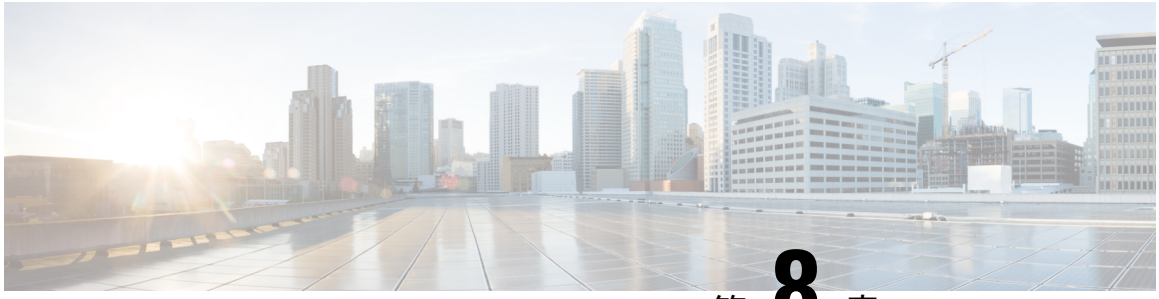
```
deploy base system services
```

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 12 Nexus Dashboard とサービスを展開したら、設定と操作の記事の説明に従って各サービスを設定できます。

- ファブリック コントローラについては、*NDFC*ペルソナ設定 のホワイトペーパーとドキュメントライブラリを参照してください。
- Orchestrator については、 ドキュメント ページを参照してください。
- Insights については、 ドキュメント ライブラリを参照してください。



第 8 章

VMware ESX の展開

- 前提条件とガイドライン （93 ページ）
- VMware vCenter を使用している Nexus ダッシュボードの展開 （97 ページ）
- VMware ESXi での Nexus ダッシュボードの展開 （118 ページ）

前提条件とガイドライン

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 が拡張性とサービス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、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） 一部のサービス (Nexus Dashboard Fabric Controller など) 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：Nexus Dashboard （9 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 ダッシュボード クラスタを最初に展開する方法について説明するものである点に留意してください。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。

- 展開予定のサービスのリリース ノートに説明されている追加の前提条件を確認し、条件を満たすようにしてください。
- 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。
- VMware ESXで展開する場合、2種類のノードを展開できます。
  - データノード：追加のリソースを必要とする特定のサービス向けに設計された、より高いシステム要件を持つノード プロファイル。
  - アプリケーション ノード：ほとんどのサービスに使用できる、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 Nexus Dashboard ファブリックコントローラの展開では、追加のセカンダリ ノードが必要になる場合があります。NDFC 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 ファブリック コントローラの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 *20* : 導入要件

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、8.0.2
• vCenter を使用して展開する場合、VMware vCenter 7.0.1、7.0.2、7.0.3、8.0.2
• 各 VM には次のものが必要です。
  • 少なくとも 2.2 GHz の物理予約された 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 Dashboardノードは、異なるESXiサーバー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、8.0.2
	• vCenter を使用して展開する場合、VMware vCenter 7.0.1、7.0.2、7.0.3、8.0.2
	• 各 VM には次のものが必要です。
	  • 少なくとも 2.2 GHz の物理予約された 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
	  一部のサービスでは、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、他のサービスでは 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。
	  （注）
	  Nexus Dashboard リリース3.0(1i) および Nexus Dashboard Insights リリース6.3(1)以降では、Insights サービスにOVA-Appノード プロファイルを使用できます。ただし、Insights のホスティングに使用されるノード VM を展開する場合は、デフォルトの 500 GB のディスク要件から 1536 GB に変更する必要があります。
	• 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 を設定する場合は、仮想ゲスト VLAN タギング（VGT）モードの 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。vND 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。

- Nexus ダッシュボードはプラットフォーム インフラストラクチャであるため、すべてのサービスを停止することはできません。

  つまり、デバッグ目的などで、仮想マシンのスナップショットを作成する場合、スナップショットではすべての Nexus ダッシュボード サービスが実行されている必要があります。

- ノードを ESXi に直接展開するか、vCenter を使用して展開するかを選択できます。

  vCenter を使用して展開する場合は、VMware vCenter を使用している 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 （118 ページ） で説明されている手順に従います。

（注） OVA-App ノード プロファイルを使用して Nexus Dashboard Insights を展開する場合は、vCenter を使用して展開する必要があります。

Nexus Dashboard Insightsには、OVA-Appノード プロファイルのデフォルト値よりも大きなディスク サイズが必要です。OVA-App ノードプロファイルを使用して NDI を展開する場合は、VM の展開時に OVA-App ノードのデフォルトのディスク サイズを 500GB から 1.5TB に変更する必要があります。ディスク サイズのカスタマイズは、VMware vCenter を介して展開する場合にのみサポートされます。Insights の詳細な要件については、Nexus Dashboard Capacity Planningツールを参照してください。

VMware vCenter を使用している 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 （118 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

- 前提条件とガイドライン （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/

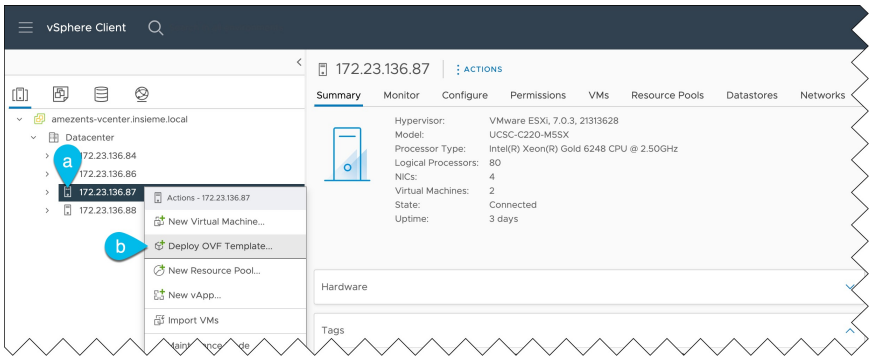
b) 左側のサイドバーから、ダウンロードする Nexus ダッシュボードのリリースバージョンを選択します。

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。

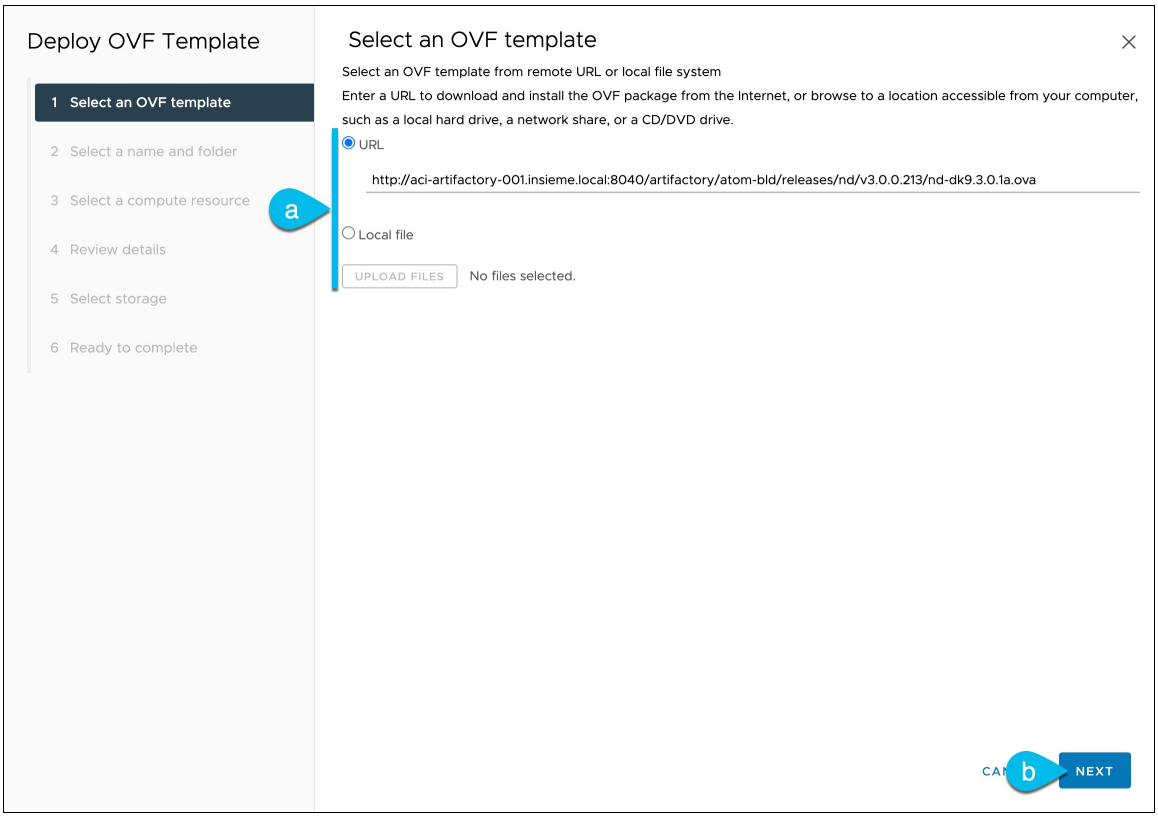


a) VM を展開する ESX ホストを右クリックします。

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。



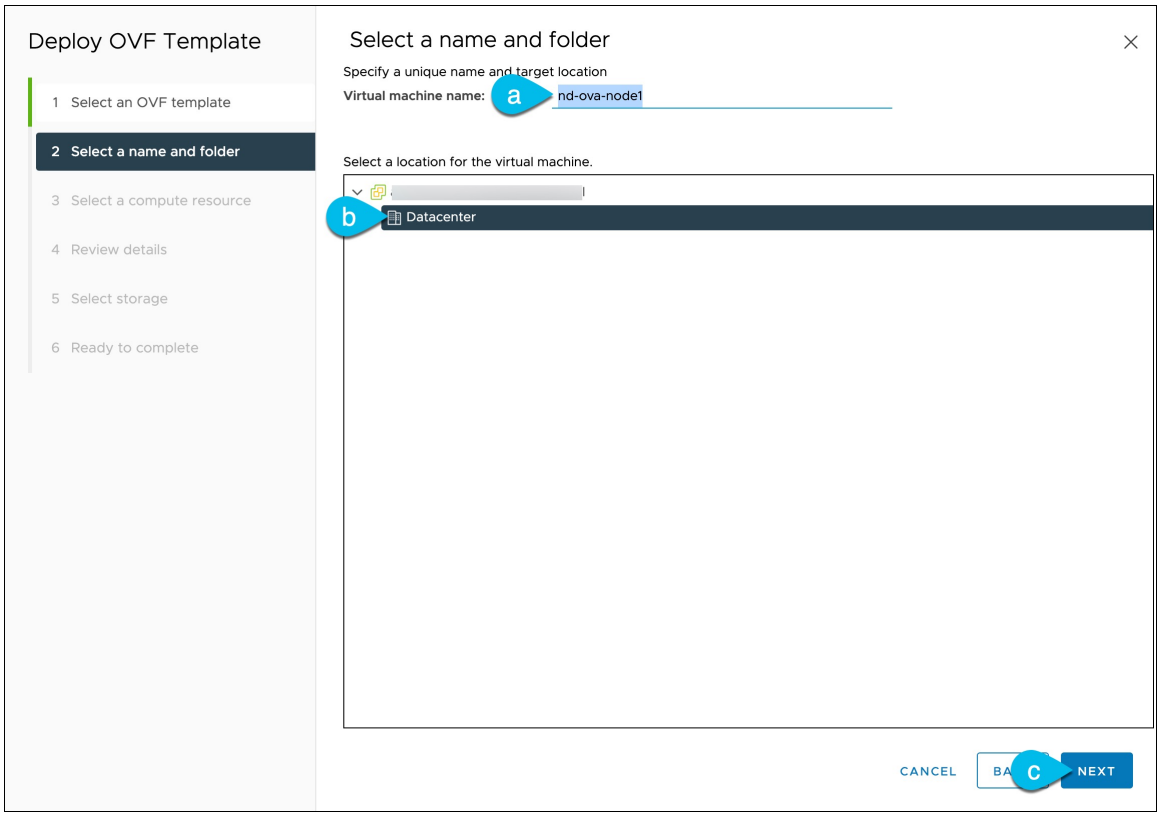
a) イメージの場所を指定します。

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。



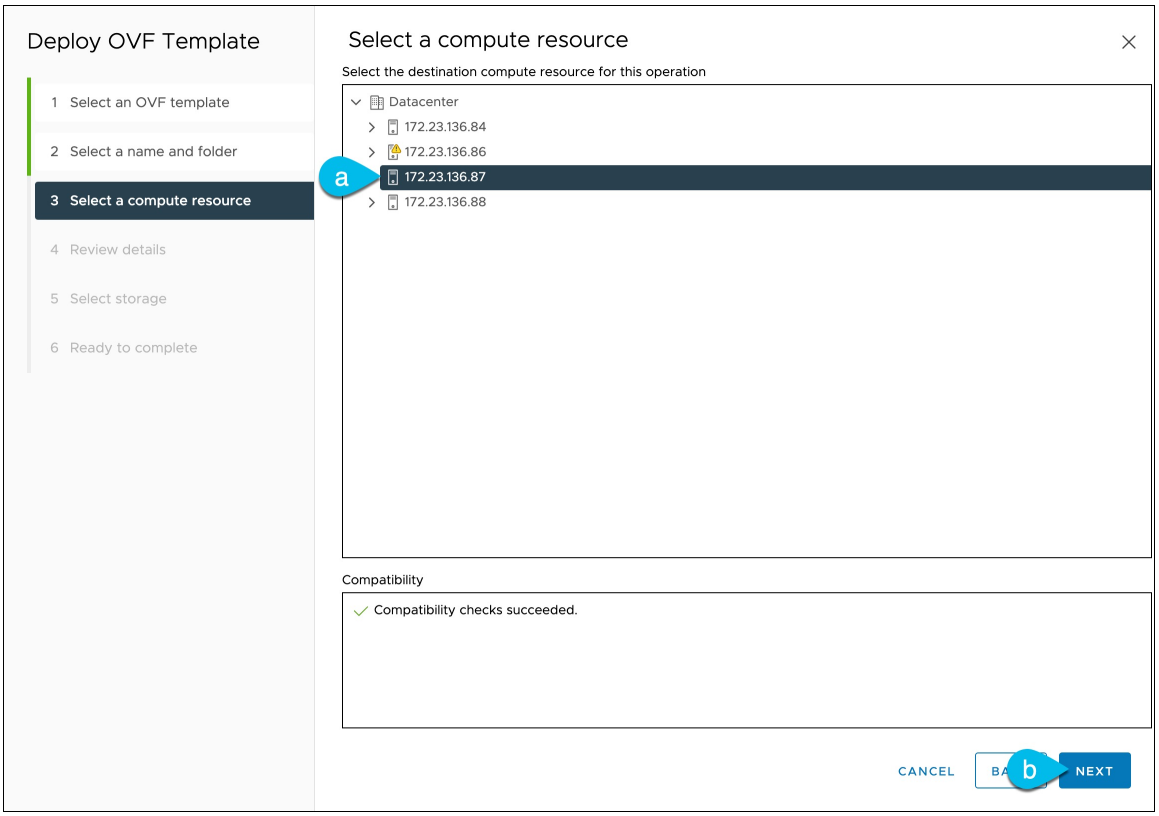
a) 仮想マシンの名前を入力します。

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。

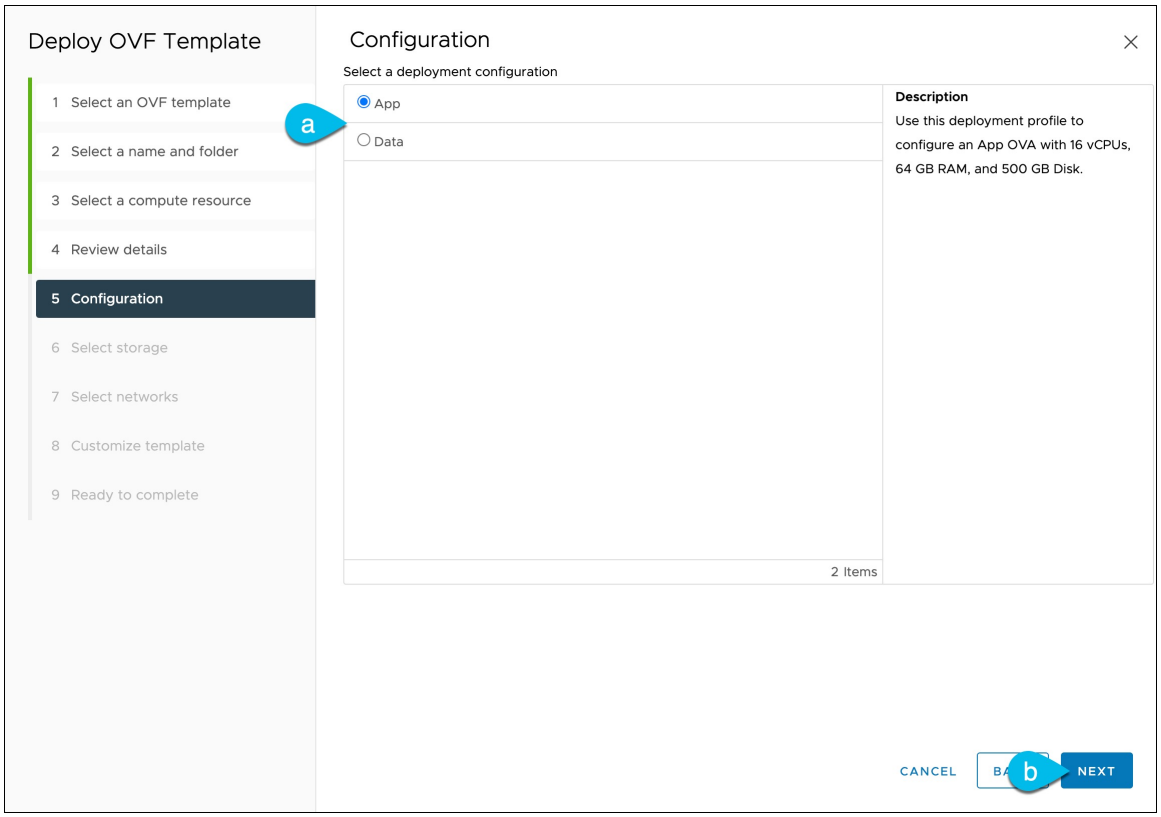


a) 仮想マシンの vCenter データセンターと ESX ホストを選択します。

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。

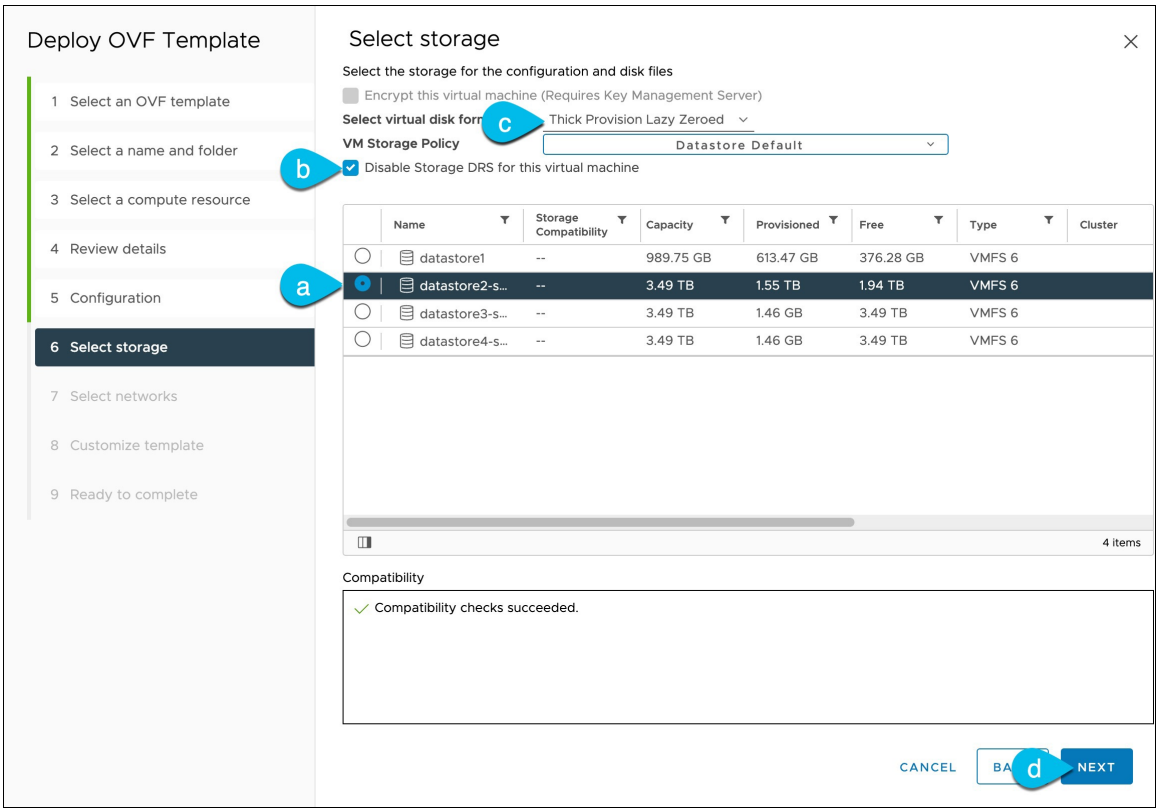


a) ユースケースの要件に基づいて、アプリまたはデータ ノード プロファイルを選択します。

ノードプロファイルの詳細については、「前提条件とガイドライン （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) **[仮想ディスク フォーマットの選択（Select virtual disk format）]** ドロップダウンから [シック プロビジョニング（Thick Provisioning）] を選択します。

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。ESXi クラスタ レベルで DRS が有効になっている場合は、**[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）]** オプションをオンにすることをお勧めします。

c) 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。

d) **[次へ（Next）]** をクリックして、続行します。

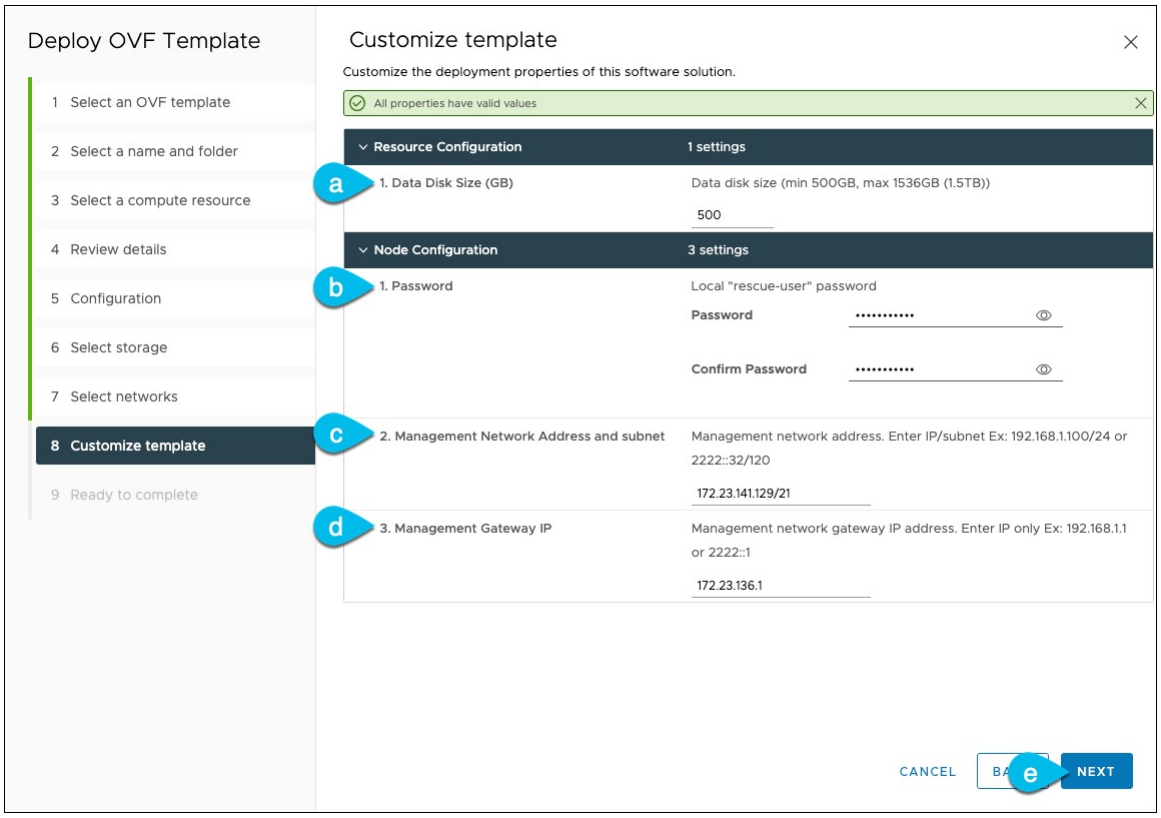
ステップ 10 [**ネットワークの選択**] 画面で、Nexus ダッシュボードの管理およびデータ ネットワークの VM ネットワークを選択し、[**次へ**] をクリックして続行します。

Nexus ダッシュボードクラスタには 2 つのネットワークが必要です。

- **fabric0** は、Nexus ダッシュボードクラスタのデータ ネットワークに使用されます
- **mgmt0** は、Nexus ダッシュボード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「前提条件とガイドライン （9 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) ノードのデータ ボリュームのサイズを指定します。

デフォルト値は、展開するノードのタイプに基づいて事前に入力されます。アプリケーションノードには単一の500 GBディスクがあり、データノードには単一の 3TB ディスクがあります。データ ボリュームに加えて、2 つ目の 50GB のシステム ボリュームも構成されますが、カスタマイズすることはできません。

（注）
ノードのカスタムディスク サイズを指定する場合は、VM の展開時に指定する必要があります。ノードの起動後のディスクのサイズ変更は、Nexus Dashboard ではサポートされていません。

OVA-App ノードプロファイルを使用して Nexus Dashboard Insights を展開する場合は、データディスクサイズをデフォルトの 500GB 値から 1536GB に変更する必要があります。クラスタのサイジング、システム リソース要件、およびノード プロファイルのサポートの詳細については、Nexus Dashboard Capacity Planningを参照してください。

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、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 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。

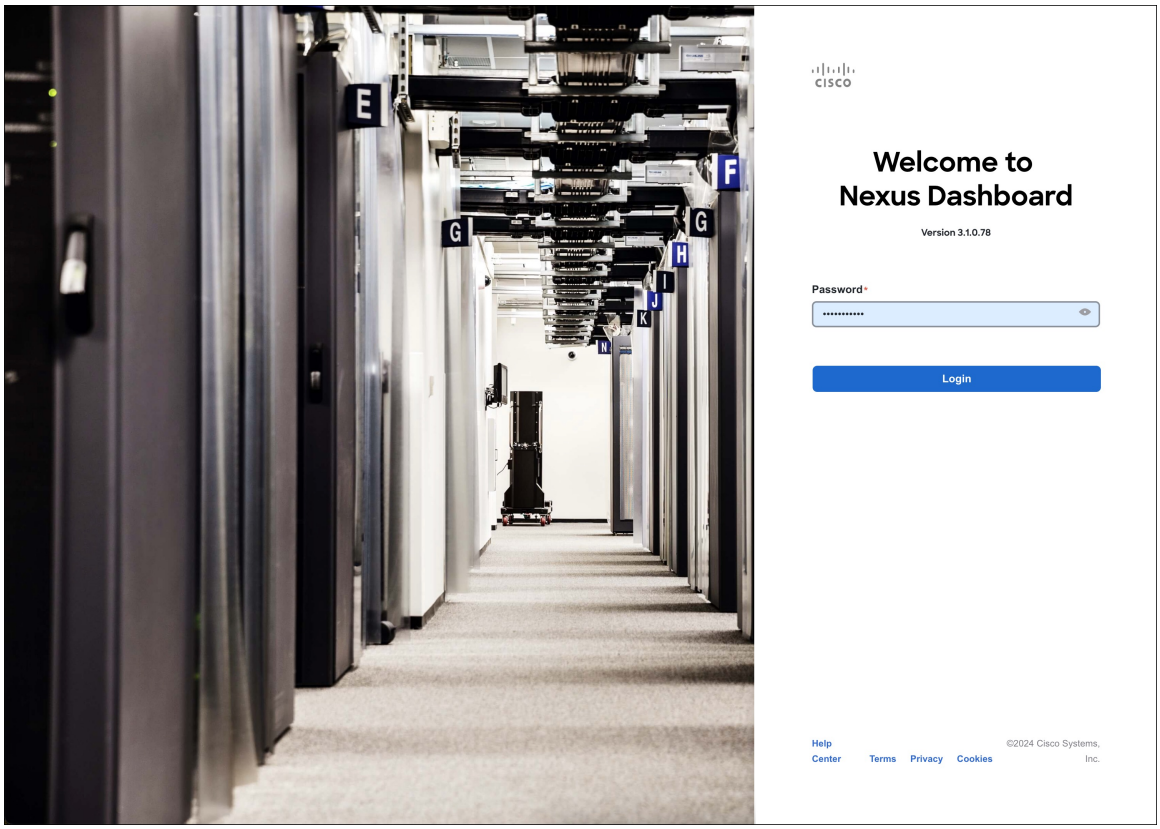
時刻の同期を無効にするには、次の手順を実行します。

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

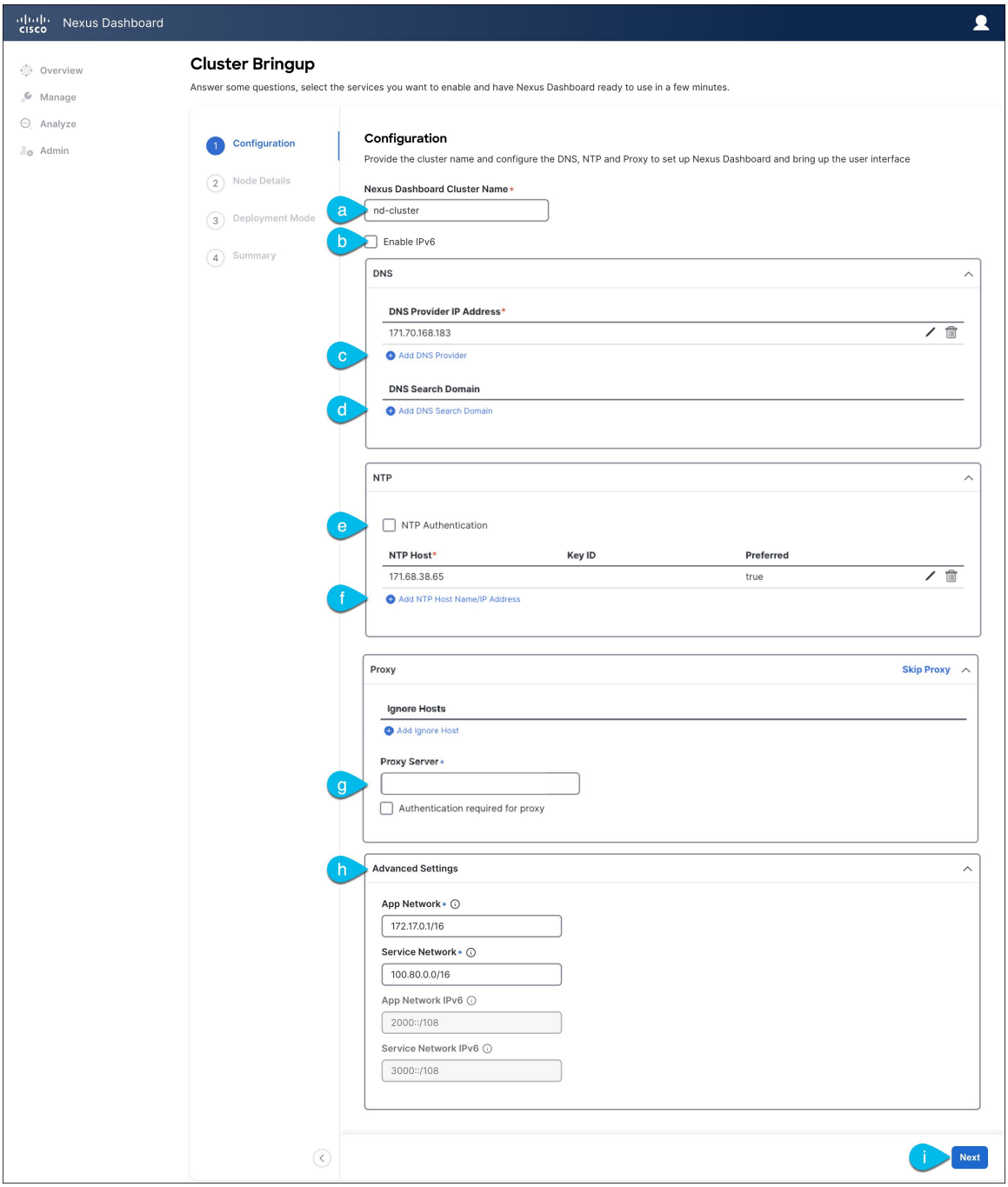
残りの設定ワークフローは、ノードの GUI の 1 つから実行します。展開したノードのいずれか 1 つを選択して、ブートストラッププロセスを開始できます。他の 2 つのノードにログインしたり、これらを直接構成したりする必要はありません。

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 **[クラスタの詳細（Cluster Details）]** を入力します。

[クラスタ起動（Cluster Bringup）] ウィザードの **[クラスタの詳細（Cluster Details）]** 画面で、次の情報を入力します。



a) Nexus ダッシュボード クラスタの **[クラスタ名（Cluster Name）]** 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) （オプション）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。

c) **[+DNS プロバイダの追加（+Add DNS Provider）]** をクリックして、1 つ以上の DNS サーバを追加します。

情報を入力した後、チェックマーク アイコンをクリックして保存します。

d) （オプション）**[+DNS 検索ドメインの追加（+Add DNS Search Domain ）]** をクリックして、検索ドメインを追加します。

情報を入力した後、チェックマーク アイコンをクリックして保存します。

e) （オプション）NTP サーバー認証を有効にする場合には、**[NTP 認証（NTP Authentication）]** チェックボックスをオンにし、**[NTP キーの追加（Add NTP Key）]**をクリックします。

次のフィールドで、以下の情報を提供します。

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

（注）
情報を入力した後、チェックマーク アイコンをクリックして保存します。

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、前提条件とガイドライン （9 ページ） を参照してください。

f) **[+ NTP ホスト名/IP アドレスの追加（+Add NTP Host Name/IP Address）]** をクリックして、1 つ以上の NTP サーバを追加します。

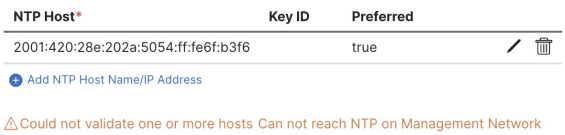
次のフィールドで、以下の情報を提供します。

- **NTP ホスト**：IP アドレスを指定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**：このサーバーの NTP 認証を有効にする場合は、前の手順で定義した NTP キーのキー ID を指定します。

  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 NTP サーバーを **[優先（Preferred）]** にするかどうかを選択します。

情報を入力した後、チェックマーク アイコンをクリックして保存します。

（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（次の手順で指定します）、NTP サーバーの IPv6 アドレスに接続できないためです。

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 サーバーを指定する場合は、**[+NTP ホストの追加（+Add NTP Host）]** を再度クリックし、このサブステップを繰り返します。

g) **[プロキシ サーバー（Proxy Server）]** を指定し、**[検証（Validate）]** をクリックします。

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。

[+無視するホストを追加（+Add Ignore Host）] をクリックして、プロキシをスキップする 1 つ以上の IP アドレス通信を提供することもできます。

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
```

プロキシ設定をスキップする場合は、**[プロキシをスキップ（Skip Proxy）]** をクリックします。

h) (オプション) プロキシ サーバで認証が必要な場合は、**[プロキシで認証が必要（Authentication required for Proxy）]** を **[はい（Yes）]** に変更し、ログイン資格情報を指定します。

i) (オプション) **[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。

- カスタム **App Network** と **Service Network** を提供します。

  アプリケーション オーバーレイ ネットワークは、Nexus ダッシュボードで実行されるアプリケーションのサービスで使用されるアドレス空間を定義します。このフィールドには、デフォルトの `172.17.0.1/16` 値が事前に入力されています。

  サービス ネットワークは、Nexus ダッシュボードとそのプロセスで使用される内部ネットワークです。このフィールドには、デフォルトの `100.80.0.0/16` 値が事前に入力されています。

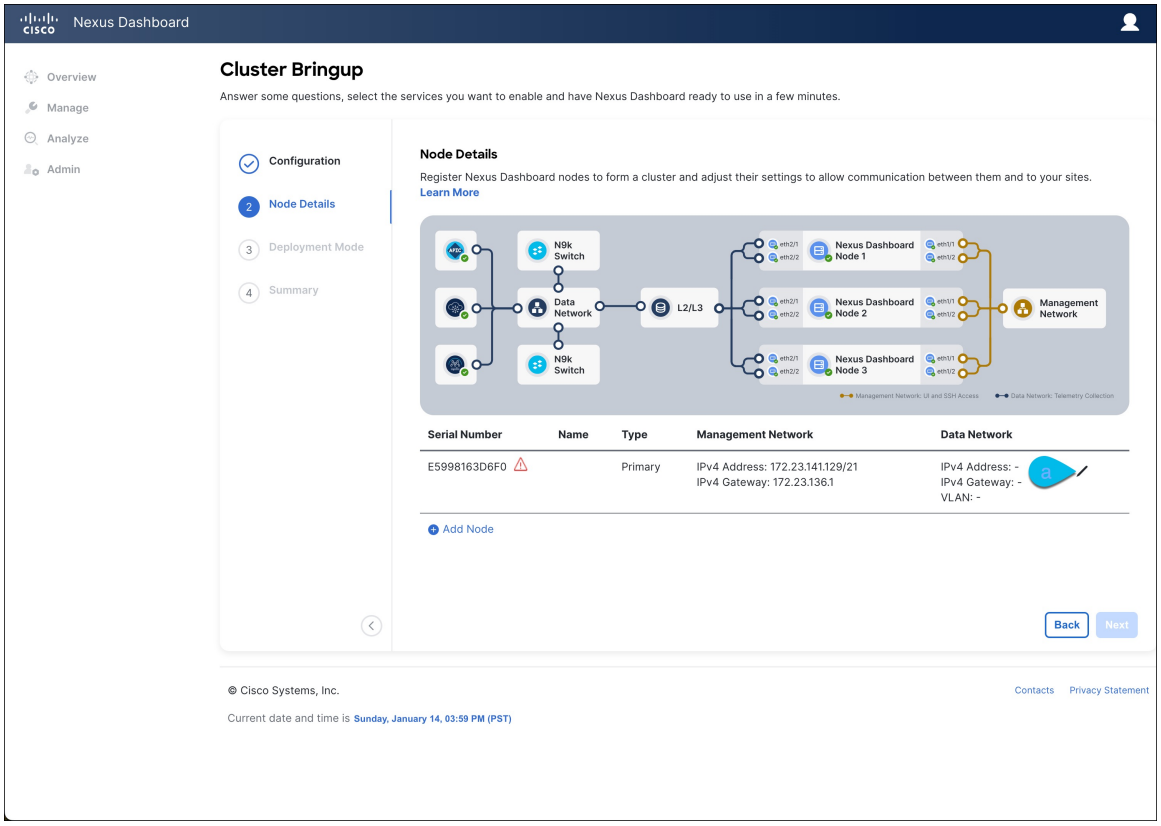
  以前に **[IPv6 を有効にする（Enable IPv6）]** オプションをオンにした場合は、アプリケーション ネットワークとサービス ネットワークの IPv6 サブネットを定義することもできます。

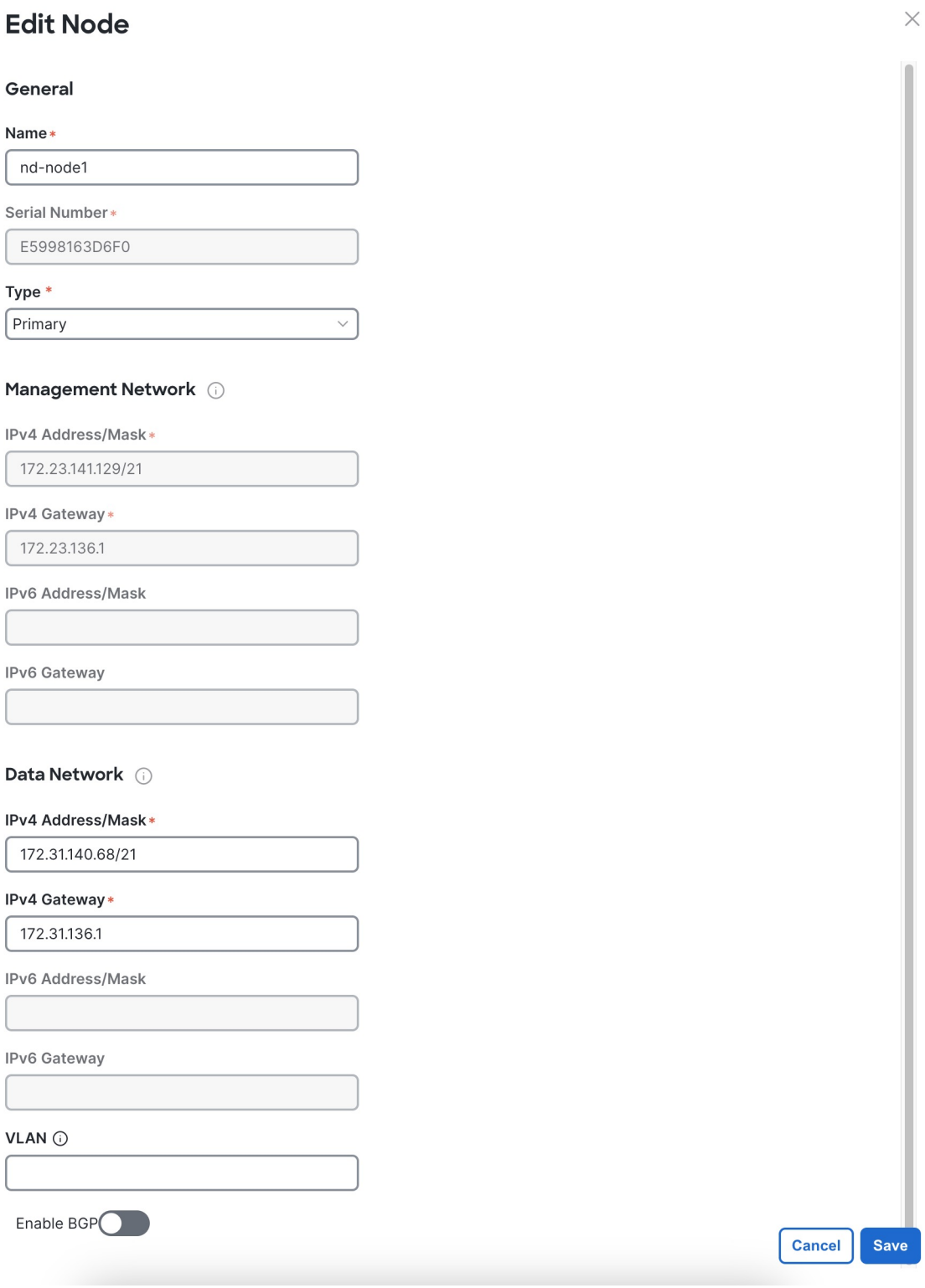
  アプリケーションおよびサービスネットワークについては、このドキュメントの前の 前提条件とガイドライン （9 ページ） の項で説明します。

j) [次へ（Next）] をクリックして続行します。

ステップ 18 **[ノードの詳細（Node Details）]** 画面で、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) 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、他の情報は手動で入力する必要があります。

b) ノードの **[名前（Name）]** 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。

c) **[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。サービスの共同ホスティングや、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。

d) **[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。

e) （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。

Insights やファブリック コントローラなどの、一部のサービスで使用される永続的な IP 機能には、BGP 構成が必要です。この機能については、前提条件とガイドライン （9 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**。

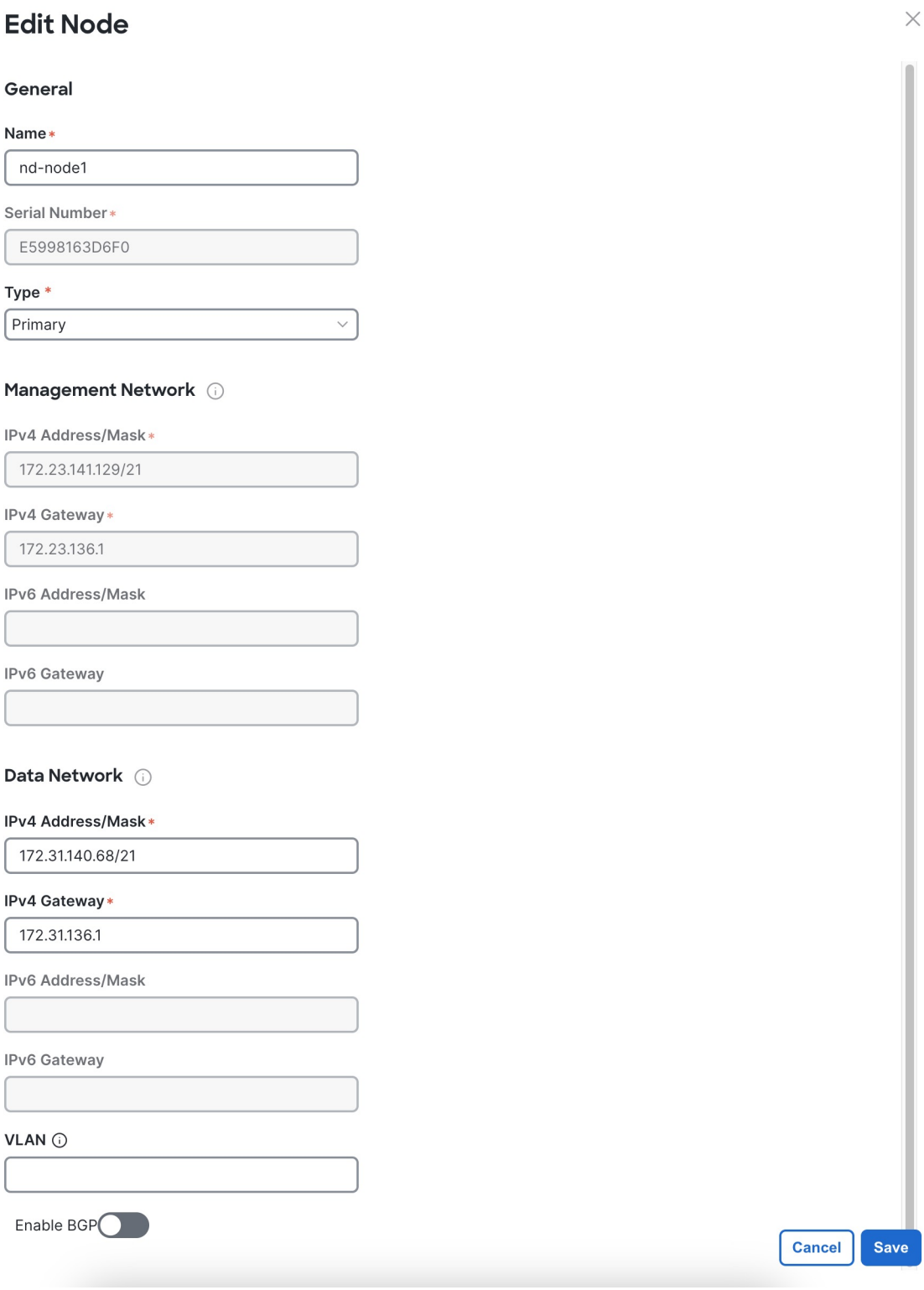
  ルータ ID は、`1.1.1.1` などの IPv4 アドレスである必要があります。

- 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**。

f) **[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。サービスの共同ホスティングや、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) （任意）必要に応じて、データ ネットワークの **BGP を有効にします**。

Insights やファブリック コントローラなどの、一部のサービスで使用される永続的な IP 機能には、BGP 構成が必要です。この機能については、前提条件とガイドライン （9 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。

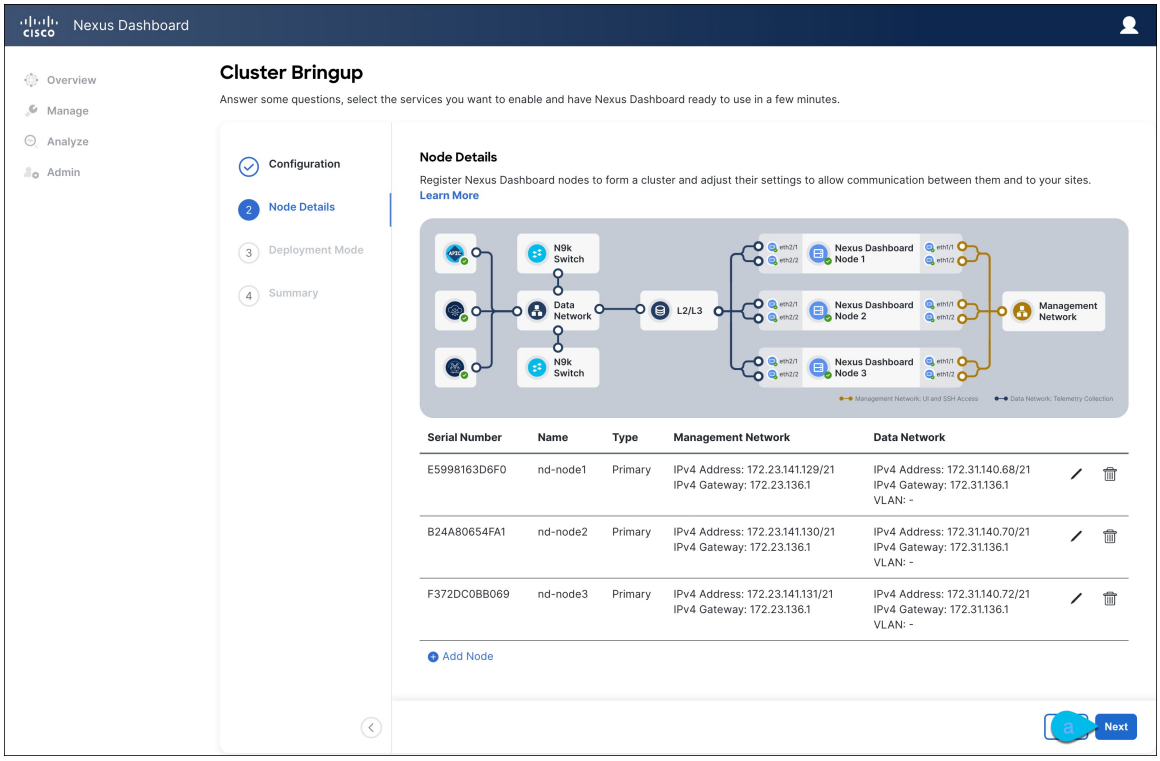
h) クラスタの最後の（3 番目の）プライマリ ノードでこの手順を繰り返します。

ステップ 20 （オプション）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）
クラスタで複数のサービスを同時に有効にするか、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、**[次へ（Next）]** をクリックして続行します。



ステップ 22 クラスタの**展開モード**を選択します。

a) 有効にするサービスを選択します。

リリース 3.1(1) より前では、クラスタの初期展開が完了した後に、個々のサービスをダウンロードしてインストールする必要がありました。今では、初期インストール時にサービスを有効にするように選択できます。

（注）
クラスタ内のノードの数によっては、一部のサービスまたは共同ホスティングのシナリオがサポートされない場合があります。必要な数のサービスを選択できない場合は、**[戻る（Back）]** をクリックし、前の手順で十分な数のセカンダリ ノードを指定したことを確認します。

b) **[永続サービスIP/プールの追加（Add Persistent Service IPs/Pools）]** をクリックして、Insights または ファブリック コントローラ サービスに必要な 1 つ以上の永続 IP を指定します。

永続的 IP の詳細については、ユーザー ガイドの前提条件とガイドライン （9 ページ）のセクションを参照してください。

c) [次へ（Next）] をクリックして続行します。

ステップ 23 **[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。

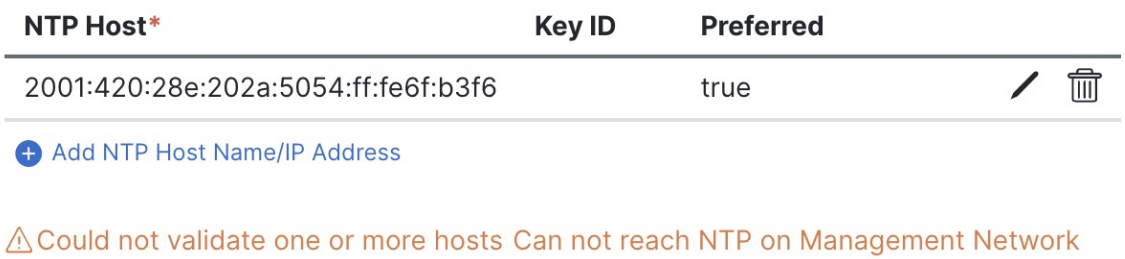
ノードのブート ストラップとクラスタの起動中に、全体的な進捗状況と各ノードの個々の進捗状況がUIに表示されます。ブートストラップの進行状況が表示されない場合は、ブラウザでページを手動で更新し、ステータスを更新してください。

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。

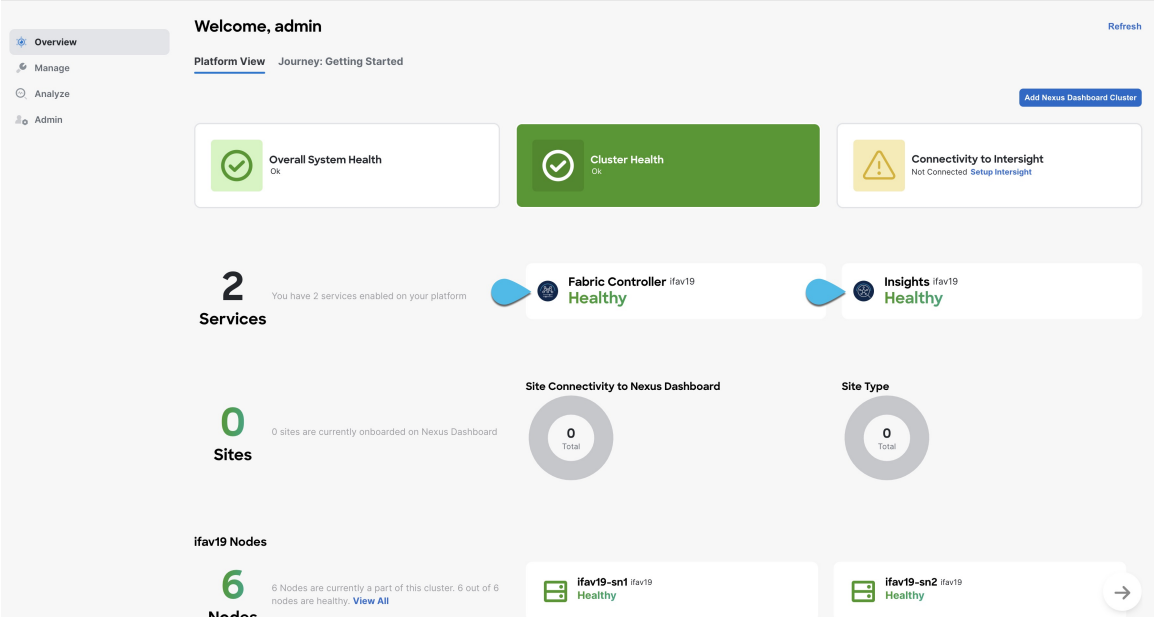
ステップ 24 クラスタが健全であることを検証します。

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、**[概要（Overview）]** ページ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、ノード展開中に指定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。

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 （118 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

- 前提条件とガイドライン （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/

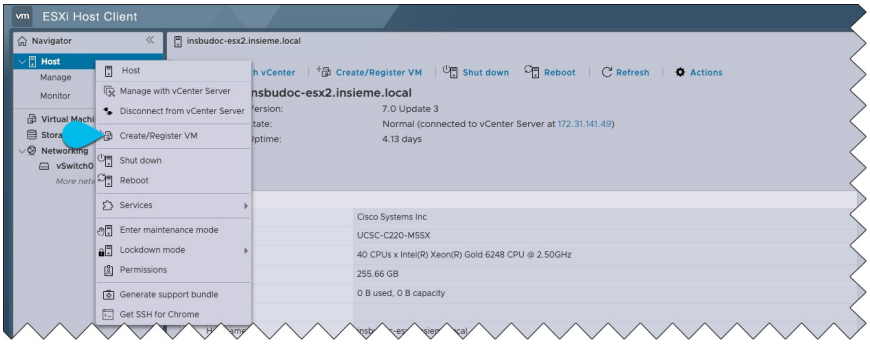
b) 左側のサイドバーから、ダウンロードする Nexus ダッシュボードのリリースバージョンを選択します。

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`）。

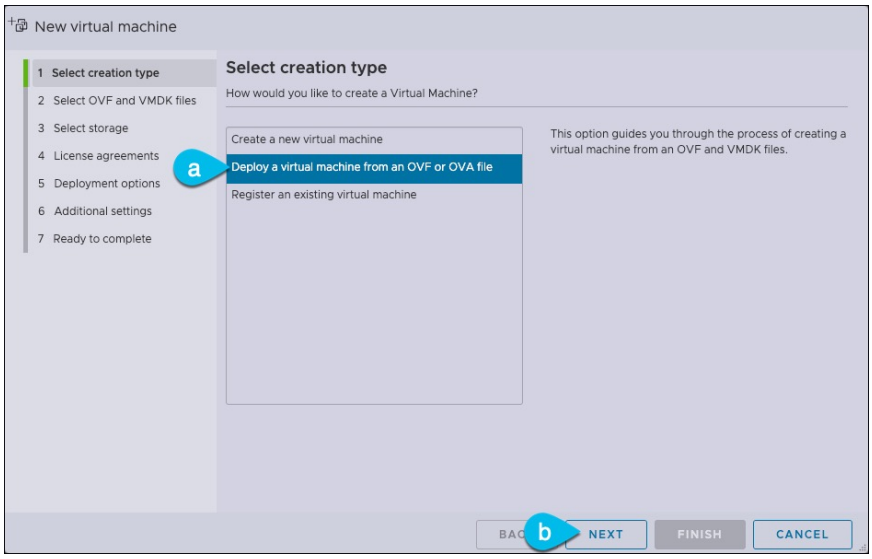
ステップ 2 VMware ESXi にログインします。

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、前提条件：Nexus Dashboard （9 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、前提条件とガイドライン （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。

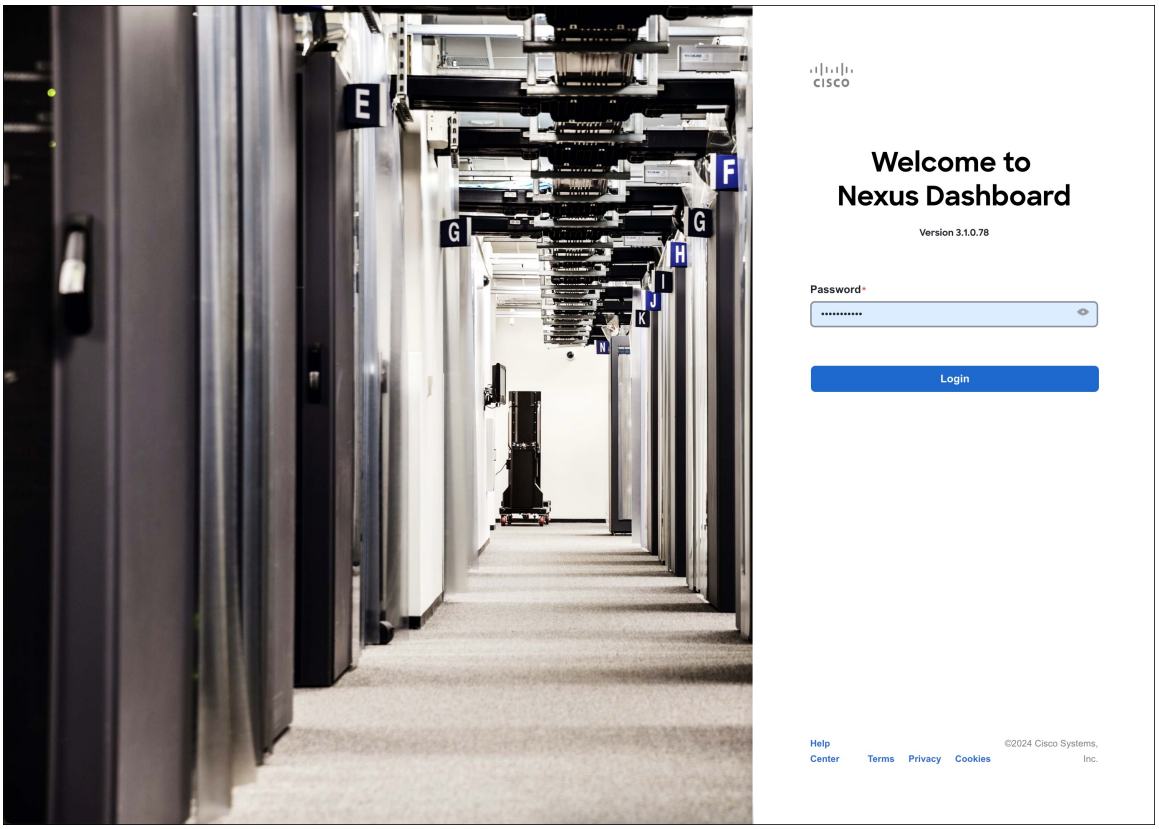
（注）
すべてのノードに同じパスワードを指定する必要があります。指定しない場合、クラスタ作成に失敗します。

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。

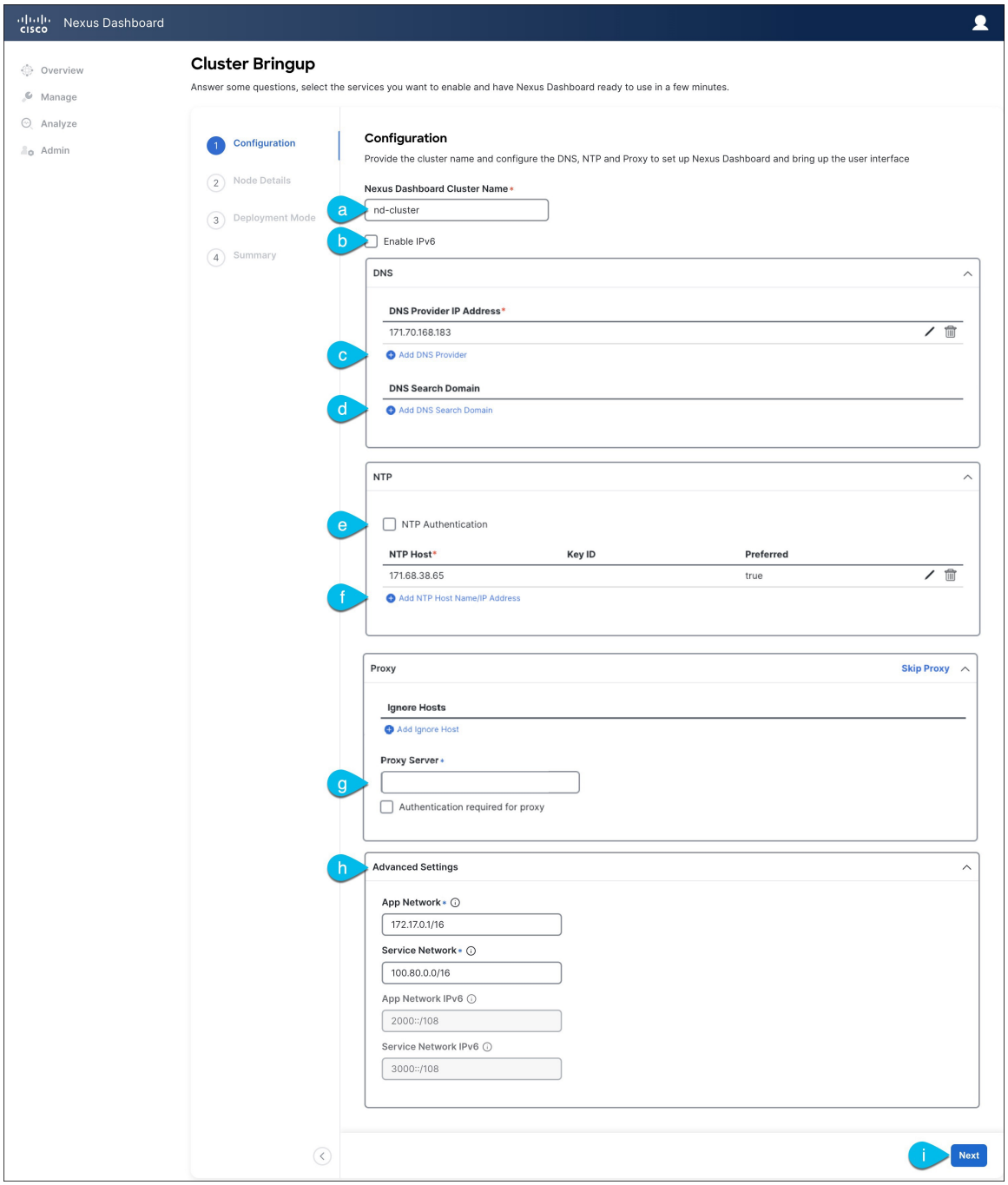
残りの設定ワークフローは、ノードの GUI の 1 つから実行します。展開したノードのいずれか 1 つを選択して、ブートストラッププロセスを開始できます。他の 2 つのノードにログインしたり、これらを直接構成したりする必要はありません。

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 **[クラスタの詳細（Cluster Details）]** を入力します。

[クラスタ起動（Cluster Bringup）] ウィザードの **[クラスタの詳細（Cluster Details）]** 画面で、次の情報を入力します。



a) Nexus ダッシュボード クラスタの **[クラスタ名（Cluster Name）]** 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) （オプション）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。

c) **[+DNS プロバイダの追加（+Add DNS Provider）]** をクリックして、1 つ以上の DNS サーバを追加します。

情報を入力した後、チェックマーク アイコンをクリックして保存します。

d) （オプション）**[+DNS 検索ドメインの追加（+Add DNS Search Domain ）]** をクリックして、検索ドメインを追加します。

情報を入力した後、チェックマーク アイコンをクリックして保存します。

e) （オプション）NTP サーバー認証を有効にする場合には、**[NTP 認証（NTP Authentication）]** チェックボックスをオンにし、**[NTP キーの追加（Add NTP Key）]**をクリックします。

次のフィールドで、以下の情報を提供します。

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

（注）
情報を入力した後、チェックマーク アイコンをクリックして保存します。

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、前提条件とガイドライン （9 ページ） を参照してください。

f) **[+ NTP ホスト名/IP アドレスの追加（+Add NTP Host Name/IP Address）]** をクリックして、1 つ以上の NTP サーバを追加します。

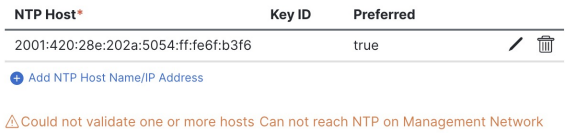
次のフィールドで、以下の情報を提供します。

- **NTP ホスト**：IP アドレスを指定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**：このサーバーの NTP 認証を有効にする場合は、前の手順で定義した NTP キーのキー ID を指定します。

  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 NTP サーバーを **[優先（Preferred）]** にするかどうかを選択します。

情報を入力した後、チェックマーク アイコンをクリックして保存します。

（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（次の手順で指定します）、NTP サーバーの IPv6 アドレスに接続できないためです。

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 サーバーを指定する場合は、**[+NTP ホストの追加（+Add NTP Host）]** を再度クリックし、このサブステップを繰り返します。

g) **[プロキシ サーバー（Proxy Server）]** を指定し、**[検証（Validate）]** をクリックします。

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。

[+無視するホストを追加（+Add Ignore Host）] をクリックして、プロキシをスキップする 1 つ以上の IP アドレス通信を提供することもできます。

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
```

プロキシ設定をスキップする場合は、**[プロキシをスキップ（Skip Proxy）]** をクリックします。

h) (オプション) プロキシ サーバで認証が必要な場合は、**[プロキシで認証が必要（Authentication required for Proxy）]** を **[はい（Yes）]** に変更し、ログイン資格情報を指定します。

i) (オプション) **[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。

- カスタム **App Network** と **Service Network** を提供します。

  アプリケーション オーバーレイ ネットワークは、Nexus ダッシュボードで実行されるアプリケーションのサービスで使用されるアドレス空間を定義します。このフィールドには、デフォルトの `172.17.0.1/16` 値が事前に入力されています。

  サービス ネットワークは、Nexus ダッシュボードとそのプロセスで使用される内部ネットワークです。このフィールドには、デフォルトの `100.80.0.0/16` 値が事前に入力されています。

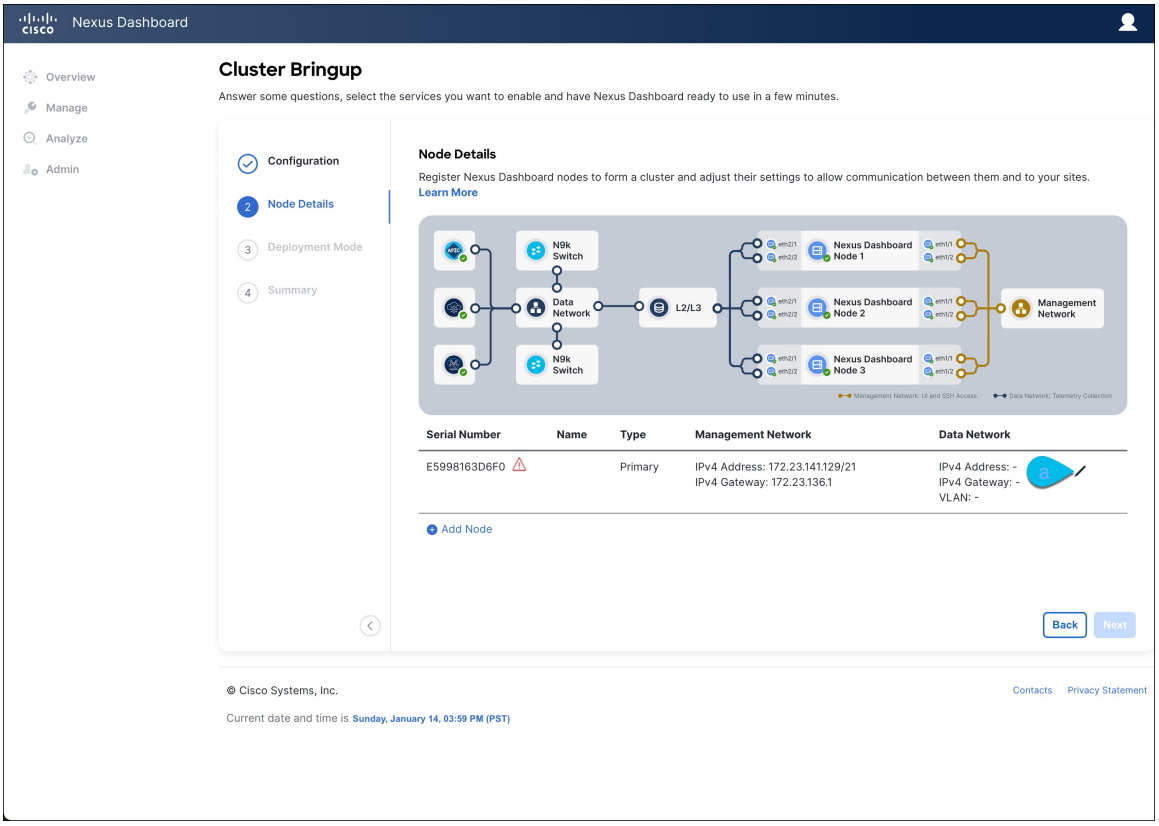
  以前に **[IPv6 を有効にする（Enable IPv6）]** オプションをオンにした場合は、アプリケーション ネットワークとサービス ネットワークの IPv6 サブネットを定義することもできます。

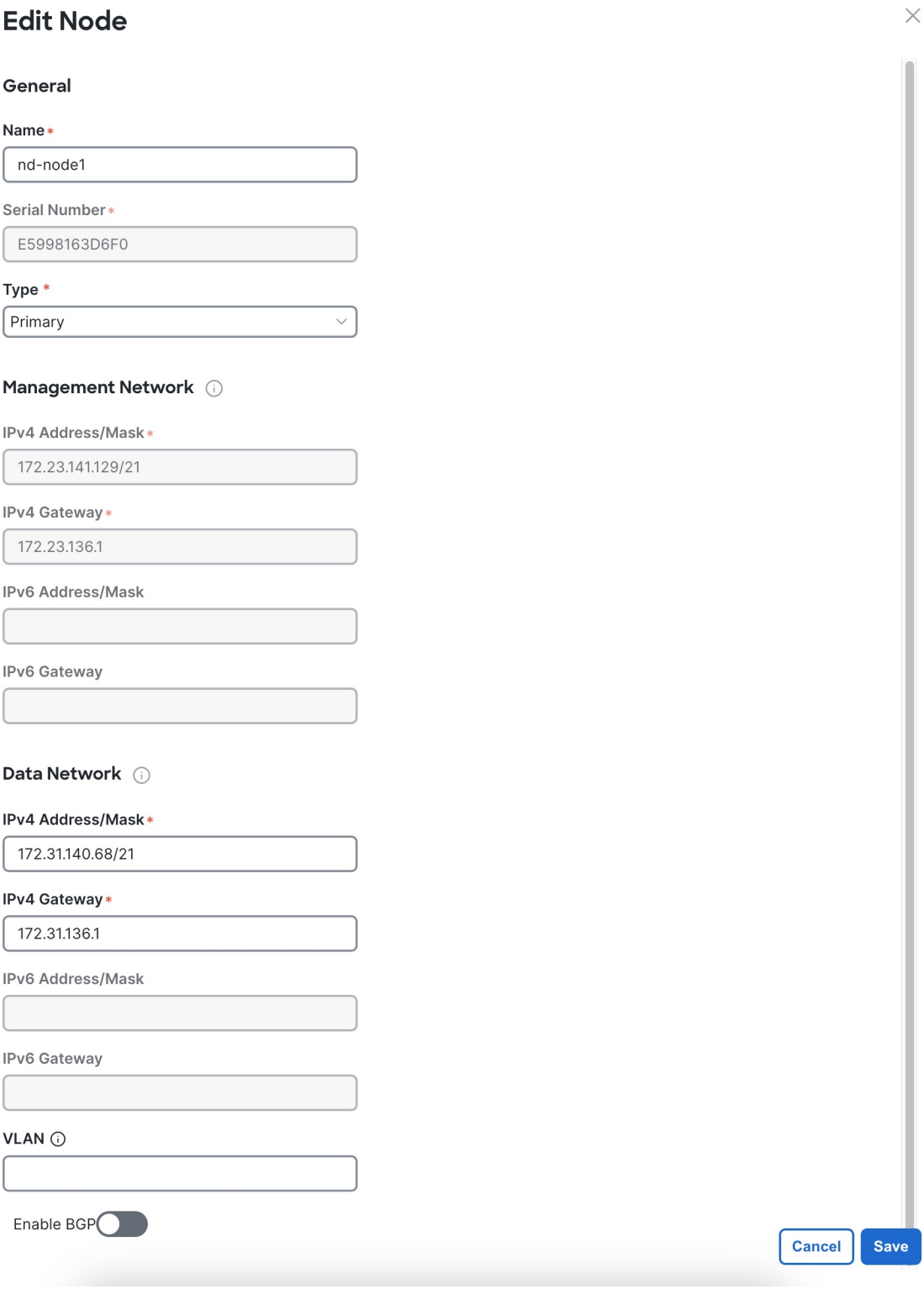
  アプリケーションおよびサービスネットワークについては、このドキュメントの前の 前提条件とガイドライン （9 ページ） の項で説明します。

j) [次へ（Next）] をクリックして続行します。

ステップ 17 **[ノードの詳細（Node Details）]** 画面で、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) 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、他の情報は手動で入力する必要があります。

b) ノードの **[名前（Name）]** 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。

c) **[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。サービスの共同ホスティングや、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。

d) **[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。

e) （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。

Insights やファブリック コントローラなどの、一部のサービスで使用される永続的な IP 機能には、BGP 構成が必要です。この機能については、前提条件とガイドライン （9 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**。

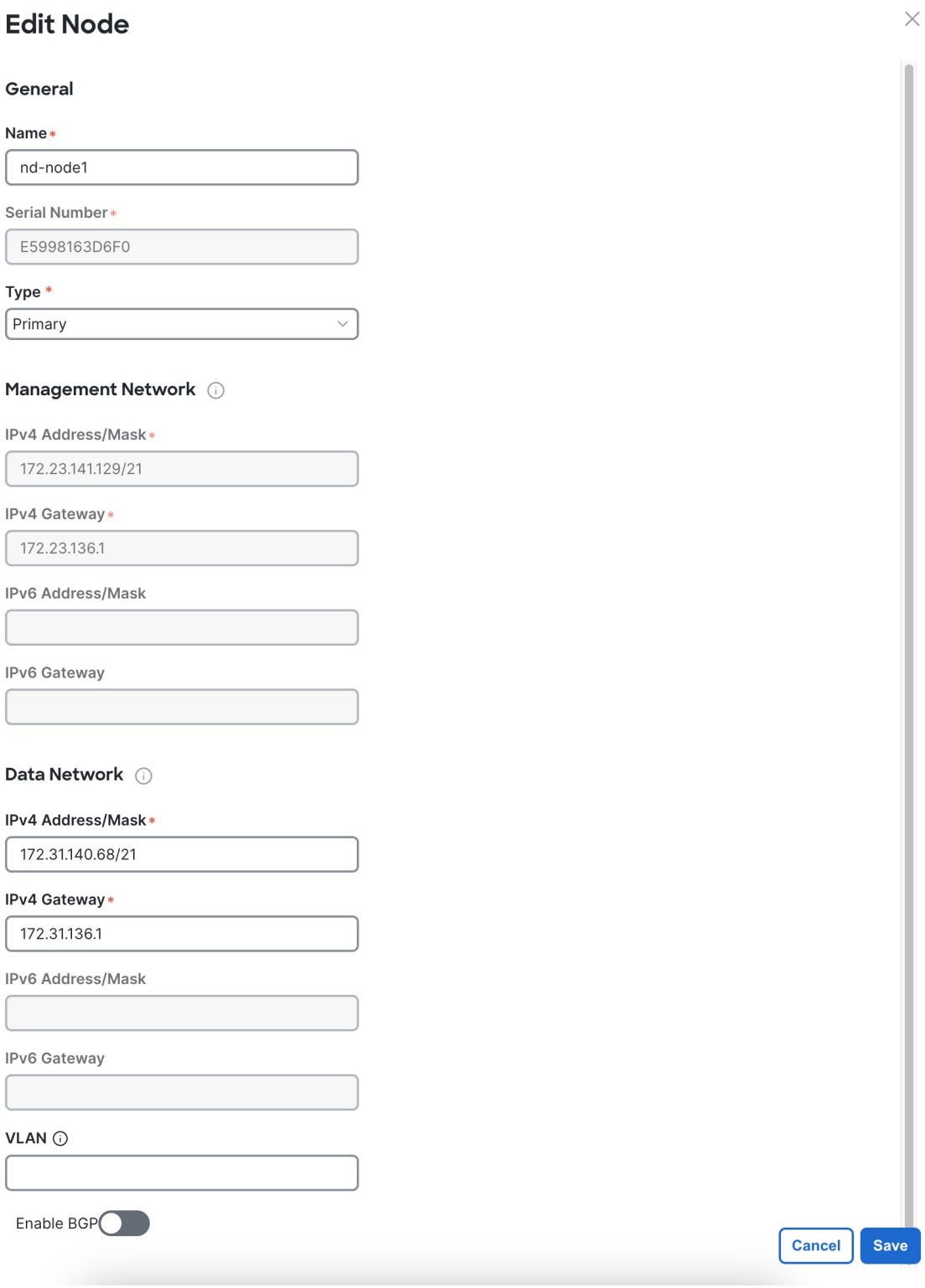
  ルータ ID は、`1.1.1.1` などの IPv4 アドレスである必要があります。

- 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**。

f) **[Save]**をクリックして、変更内容を保存します。

ステップ 18 [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。サービスの共同ホスティングや、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) （任意）必要に応じて、データ ネットワークの **BGP を有効にします**。

Insights やファブリック コントローラなどの、一部のサービスで使用される永続的な IP 機能には、BGP 構成が必要です。この機能については、前提条件とガイドライン （9 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。

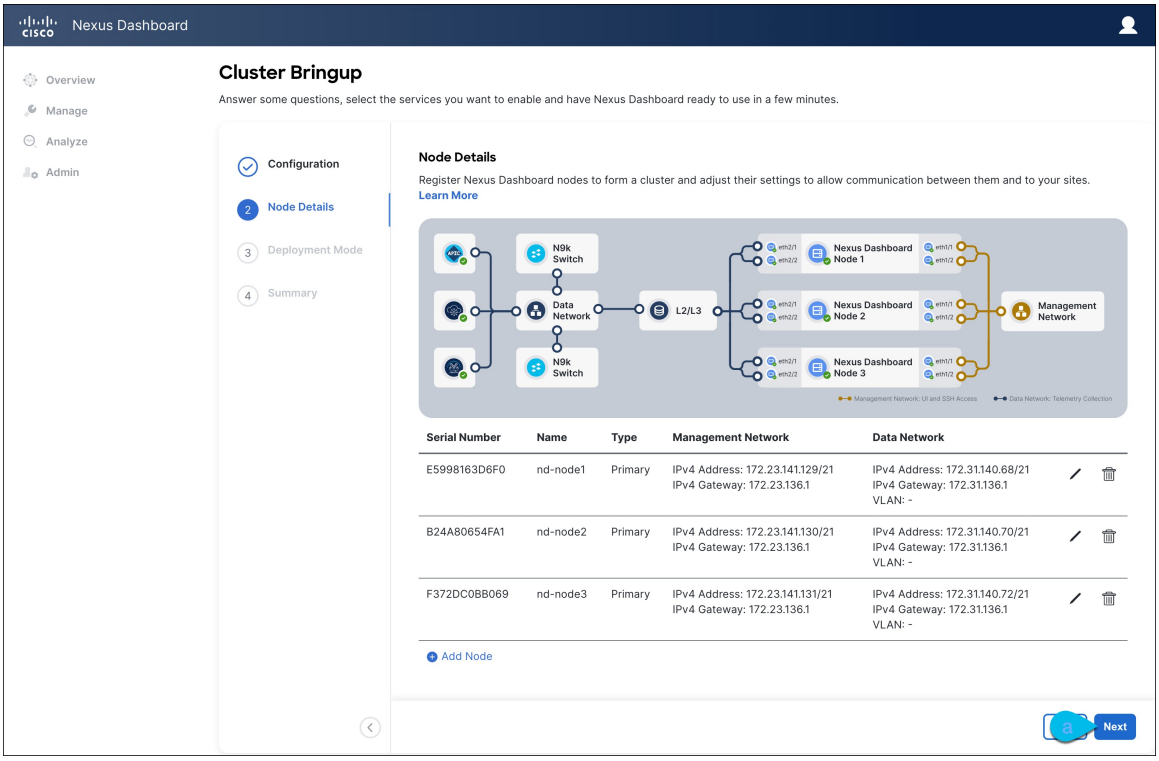
h) クラスタの最後の（3 番目の）プライマリ ノードでこの手順を繰り返します。

ステップ 19 （オプション）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）
クラスタで複数のサービスを同時に有効にするか、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 20 **[ノードの詳細（Node Details）]** ページで、入力した情報を確認し、**[次へ（Next）]** をクリックして続行します。



ステップ 21 クラスタの**展開モード**を選択します。

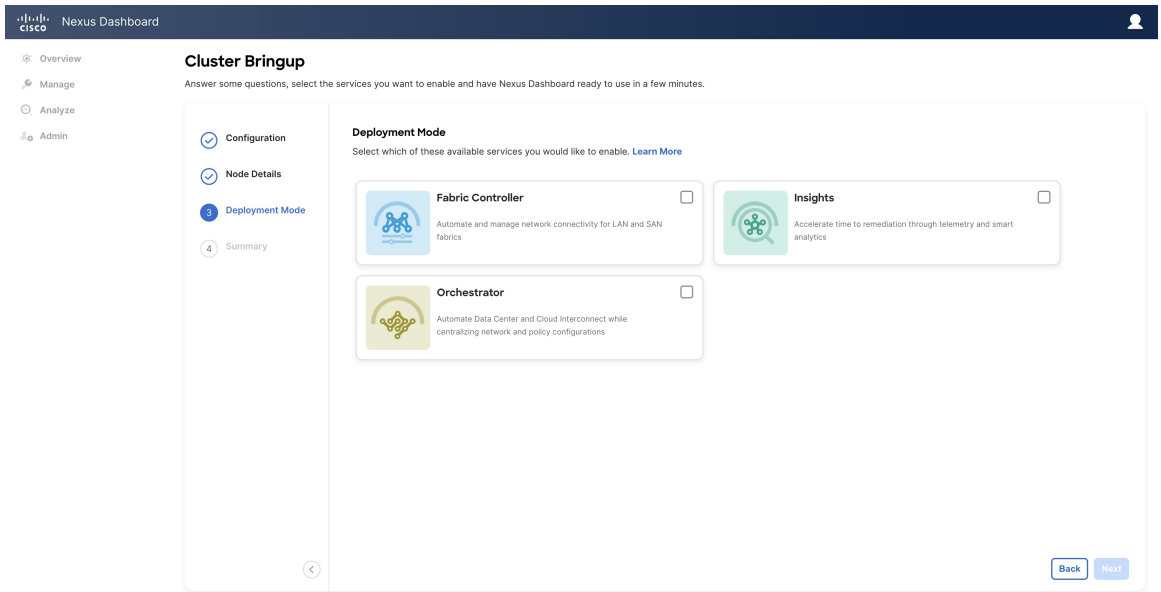
a) 有効にするサービスを選択します。

リリース 3.1(1) より前では、クラスタの初期展開が完了した後に、個々のサービスをダウンロードしてインストールする必要がありました。今では、初期インストール時にサービスを有効にするように選択できます。

（注）
クラスタ内のノードの数によっては、一部のサービスまたは共同ホスティングのシナリオがサポートされない場合があります。必要な数のサービスを選択できない場合は、**[戻る（Back）]** をクリックし、前の手順で十分な数のセカンダリ ノードを指定したことを確認します。

クラスタの展開後に展開モードを変更することはできないため、このドキュメントの前の章で説明されているサービス固有の前提条件をすべて満たしていることを確認する必要があります。

- Nexus Dashboard ファブリック コントローラの前提条件
- Nexus Dashboard オーケストレータの前提条件
- Nexus Dashboard Insights の前提条件



b) ファブリック コントローラまたは Insights を含む展開モードを選択した場合は、**[永続サービス IP/プールの追加（Add Persistent Service IPs/Pools）]** をクリックして、Insights またはファブリック コントローラ サービスに必要な 1 つ以上の永続 IP を指定します。

永続 IP の詳細については、 前提条件とガイドライン （9 ページ） セクションおよびサービス固有の要件の章を参照してください。

c) [次へ（Next）] をクリックして続行します。

ステップ 22 **[概要（Summary）]** 画面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。

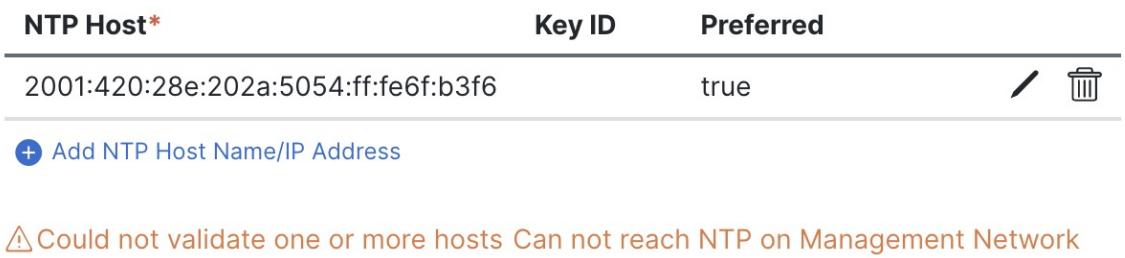
ノードのブート ストラップとクラスタの起動中に、全体的な進捗状況と各ノードの個々の進捗状況がUIに表示されます。ブートストラップの進行状況が表示されない場合は、ブラウザでページを手動で更新し、ステータスを更新してください。

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。

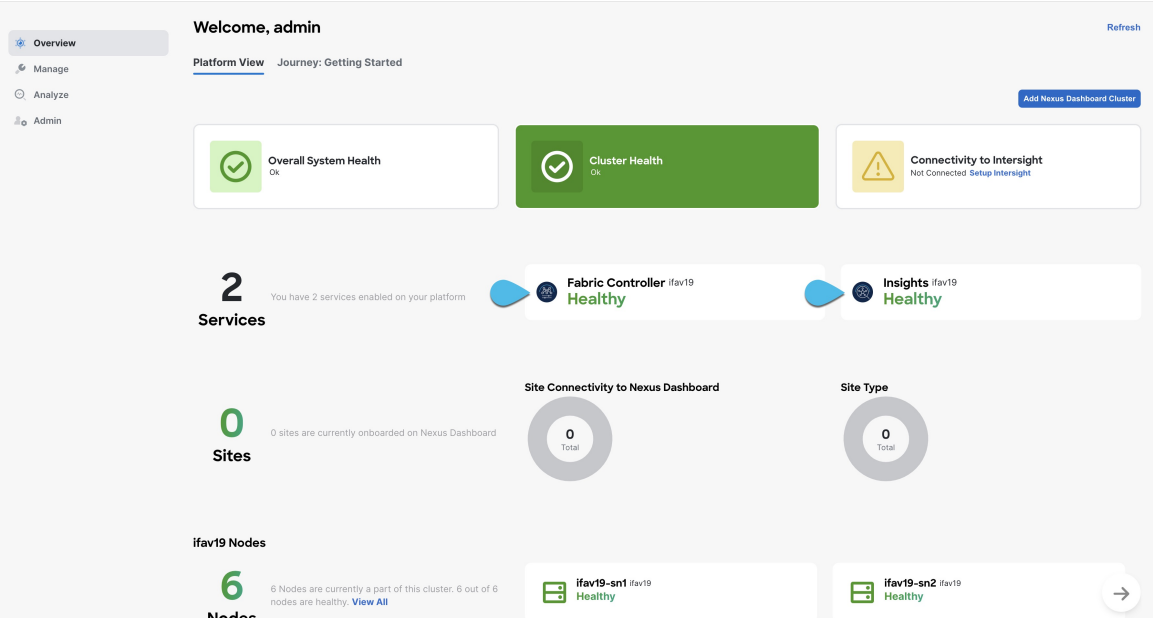
ステップ 23 クラスタが健全であることを検証します。

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、**[概要（Overview）]** ページ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、ノード展開中に指定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
```

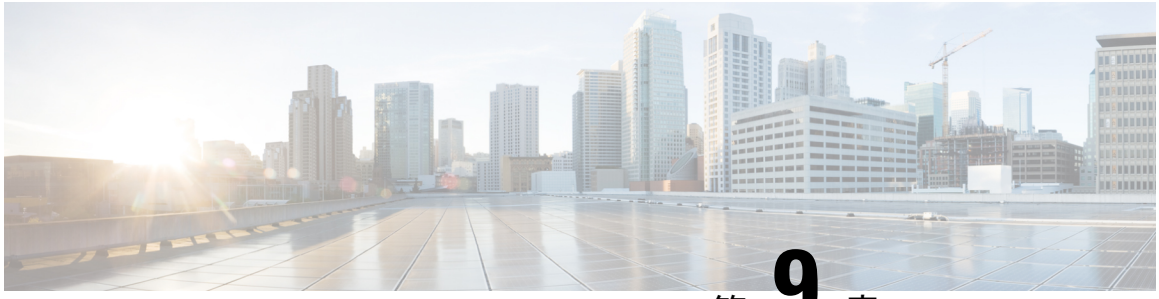
（注）

There may be an issue during the bootstrap process on 3-node vND (ESX) clusters which can cause the 'acs health' command to show the following error: `'k8s: services not in desired state - aaamgr,cisco-intersightdc,eventmonitoring,infra-kafka,kafka,mongodb,sm,statscollect'`

Cisco TAC に連絡し、オープン バグ ID CSCwf65557 を参照してケースをオープンし、各ノードで回避策コマンドを実行するための `root` アクセスを要求します。

ステップ 24 Nexus Dashboard とサービスを展開したら、設定と操作の記事の説明に従って各サービスを設定できます。

- ファブリック コントローラについては、*NDFC*ペルソナ設定 のホワイトペーパーとドキュメントライブラリを参照してください。
- Orchestrator については、 ドキュメント ページを参照してください。
- Insights については、 ドキュメント ライブラリを参照してください。



第 9 章

Linux KVMでの展開

- 前提条件とガイドライン （137 ページ）
- Linux KVM での Nexus ダッシュボードの展開 （138 ページ）

前提条件とガイドライン

Linux KVM で Nexus ダッシュボード クラスタを展開する前に、次の作業を行う必要があります。

- ファクターから KVM 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：Nexus Dashboard （9 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。
- 展開予定のサービスのリリース ノートに説明されている追加の前提条件を確認し、条件を満たすようにしてください。
- 十分なシステム リソースをもつことを確認します。

表 *21* : 導入要件

要 件

• KVM の展開は、Nexus Dashboard ファブリック コントローラでのみサポートされます。
• CentOS 7.9 または Red Hat Enterprise Linux 8.6 に展開する必要があります。
• Kernel および KVM のサポートされるバージョンが必要です。
  • CentOS 7.9 の場合、Kernel バージョン `3.10.0-957.el7.x86_64` および KVM バージョン `libvirt-4.5.0-23.el7_7.1.x86_64`
  • RHEL 8.6 の場合、Kernel バージョン `4.18.0-372.9.1.el8.x86_64` および KVM バージョン `libvert 8.0.0`
• 16 vCPU
• 64 GB の RAM
• 550 GBのディスク
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。
• 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。
I/O レイテンシを確認するには：
1. テスト ディレクトリを作成します。
`test-data` のような名前にします。
2. 次のコマンドを実行します。
`# fio --rw=write --ioengine=sync --fdatasync=1 --directory=test-data --size=22m --bs=2300 --name=mytest`
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。
• 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 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

- 前提条件とガイドライン（137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 最初のノードに必要なディスクイメージを作成します。

ダウンロードしたベース `qcow2` イメージのスナップショットを作成し、そのスナップショットをノードの VM のディスク イメージとして使用します。また、ノードごとに2番目のディスクイメージを作成する必要があります。

a) KVM ホストに `root` ユーザとしてログインします。

b) ノードのスナップショット用のディレクトリを作成します。

次の手順は、`/home/nd-node1` ディレクトリにスナップショットを作成することを前提としています。

```
# mkdir -p /home/nd-node1/
# cd /home/nd-node1
```

c) スナップショットを作成します。

次のコマンドで、`/home/nd-base//nd-dk9.<version>.qcow2` を以前のステップで作成したベースイメージの場所に置換します。

```
# qemu-img create -f qcow2 -b /home/nd-base/nd-dk9.<version>.qcow2
/home/nd-node1/nd-node1-disk1.qcow2
```

（注）
RHEL 8.6 で展開する場合は、宛先スナップショットの形式を定義するための追加のパラメータも指定する必要があります。その場合は、上記のコマンドを次のように更新します。

```
# qemu-img create -f qcow2 -b /home/nd-base/nd-dk9.2.1.1a.qcow2
/home/nd-node1/nd-node1-disk1.qcow2 -F qcow2
```

d) ノードの追加ディスクイメージを作成します。

各ノードには 2 つのディスクが必要です。ベースの Nexus ダッシュボード`qcow2`イメージのスナップショットと、2 番目の 500GB ディスクです。

```
# qemu-img create -f qcow2 /home/nd-node1/nd-node1-disk2.qcow2 500G
```

ステップ 4 前のステップを繰り返して、2 番目と 3 番目のノードのディスク イメージを作成します。

次の手順に進む前に、次の準備が必要です。

- 1 つ目のノードの場合、2 つのディスクイメージがある `/home/nd-node1/` ディレクトリ：
  - `/home/nd-node1/nd-node1-disk1.qcow2` は、ステップ 1でダウンロードしたベース `qcow2` イメージのスナップショットです。
  - `/home/nd-node1/nd-node1-disk2.qcow2`。これは、作成した新しい 500GB のディスクです。
- 2 つ目のノードの場合、2つのディスクイメージがある/ home / nd-node2 /ディレクトリ。
  - `/home/nd-node2/nd-node2-disk1.qcow2` は、ステップ 1 でダウンロードした基本 `qcow2` イメージのスナップショットです。
  - `/home/nd-node2/nd-node2-disk2.qcow2`。これは、作成した新しい 500GB のディスクです。
- 3 つ目のノードの場合、2 つのディスク イメージがある `/home/nd-node3/` ディレクトリ。
  - `/home/nd-node1/nd-node3-disk1.qcow2`。ステップ 1 でダウンロードしたベース `qcow2` イメージのスナップショットです。
  - `/home/nd-node1/nd-node3-disk2.qcow2`。これは、作成した新しい 500GB のディスクです。

ステップ 5 最初のノードの VM を作成します。

a) KVM コンソールを開き、**[新しい仮想マシン（New Virtual Machine）]** をクリックします。

コマンド ラインから `virt-manager` コマンドを使用して KVM コンソールを開くことができます。

b) **[新しい VM（New VM）]** 画面で、**[既存のディスク イメージのインポート（import existing disk image）]** オプションを選択し、**[転送（Forward）]** をクリックします。

c) **[既存のストレージ パスを指定（Provide existing storage path）]**フィールドで **[参照（Browse）]** をクリックし、`nd-node1-disk1.qcow2` ファイルを選択します。

各ノードのディスクイメージは、それぞれのディスクパーティションに保存することを推奨します。

d) **OS タイプ**と**バージョン**に対して `[Generic]` を選択し、**[転送]** をクリックします。

e) 64GB のメモリと 16 個の CPU を指定し、**[転送（Forward）]** をクリックします。

f) 仮想マシンの**名前**（例：`nd-node1`）を入力し、**[インストール前に構成をカスタマイズする（Customize configuration before install）]**オプションをオンにします。次に、[完了（Finish）] をクリックします。

（注）
ノードに必要なディスクとネットワークカードをカスタマイズできるようにするには、**[インストール前に構成をカスタマイズする]** チェックボックスをオンにする必要があります。

[VMの詳細]ウィンドウが開きます。

[VMの詳細]ウィンドウで、NICのデバイスモデルを変更します。

a) **NIC <mac>** を選択します。
b) **[デバイス モデル]** で、`[e1000]` を選択します。
c) **[ネットワーク ソース（Network Source）]** で、ブリッジ デバイスを選択し、「mgmt」ブリッジの名前を指定します。

VMの詳細ウィンドウで、2番目のNICを追加します。

a) [ハードウェアを追加（Add Hardware）] をクリックします。
b) **[新しい仮想ハードウェアの追加（Add new virtual hardware）]** ウィンドウで、**[ネットワーク]** を選択します。
c) **[ネットワーク ソース（Network Source）]** で、ブリッジ デバイスを選択し、作成した「データ」ブリッジの名前を指定します。
d) デフォルトの **MAC アドレス** の値のままにします。
e) **[デバイス モデル]** で、`[e1000]` を選択します。

[VMの詳細（VM details）] ウィンドウで、2 番目のディスク イメージを追加します。

a) [ハードウェアを追加（Add Hardware）] をクリックします。
b) **[新しい仮想ハードウェアの追加]** 画面で、**[ストレージ]** を選択します。
c) ディスクのバス ドライバについては、`[IDE]` を選択します。
d) **[カスタム ストレージの選択または作成（Select or create custom storage）]** を選択し、**[管理（Manage）]** をクリックして、作成した `nd-node1-disk2.qcow2` ファイルを選択します。
e) **[終了（Finish）]** をクリックして 2 番目のディスクを追加します。

（注）
仮想マシン マネージャの UI で `[ホスト CPU 設定のコピー（Copy host CPU configuration）]` オプションが有効になっていることを確認します。

最後に、**[インストールの開始（Begin Installation）]** をクリックして、ノードのVMの作成を終了します。

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。

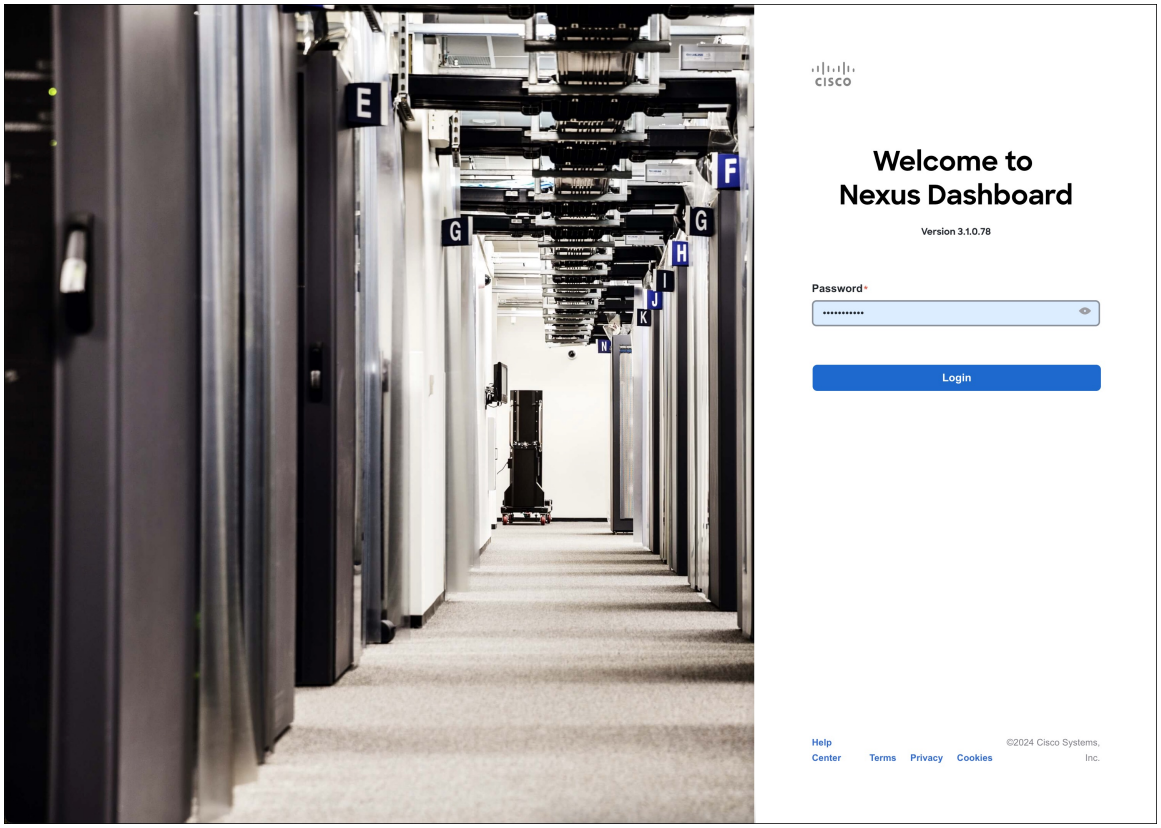
```
Please wait for system to boot: [##########################] 100%
System up, please wait for UI to be online.

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。

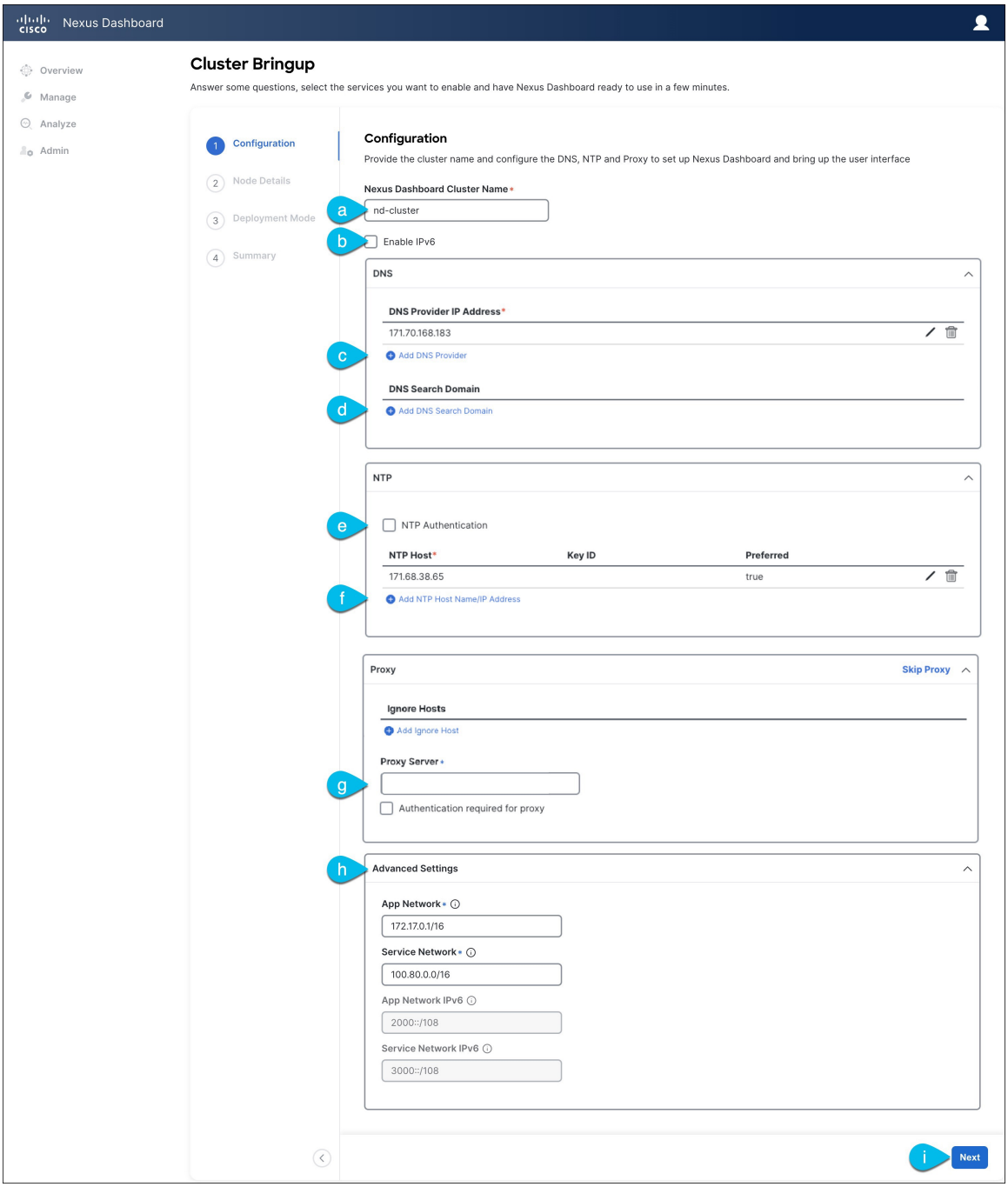
残りの設定ワークフローは、ノードの GUI の 1 つから実行します。展開したノードのいずれか 1 つを選択して、ブートストラッププロセスを開始できます。他の 2 つのノードにログインしたり、これらを直接構成したりする必要はありません。

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 **[クラスタの詳細（Cluster Details）]** を入力します。

[クラスタ起動（Cluster Bringup）] ウィザードの **[クラスタの詳細（Cluster Details）]** 画面で、次の情報を入力します。



a) Nexus ダッシュボード クラスタの **[クラスタ名（Cluster Name）]** 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) （オプション）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。

c) **[+DNS プロバイダの追加（+Add DNS Provider）]** をクリックして、1 つ以上の DNS サーバを追加します。

情報を入力した後、チェックマーク アイコンをクリックして保存します。

d) （オプション）**[+DNS 検索ドメインの追加（+Add DNS Search Domain ）]** をクリックして、検索ドメインを追加します。

情報を入力した後、チェックマーク アイコンをクリックして保存します。

e) （オプション）NTP サーバー認証を有効にする場合には、**[NTP 認証（NTP Authentication）]** チェックボックスをオンにし、**[NTP キーの追加（Add NTP Key）]**をクリックします。

次のフィールドで、以下の情報を提供します。

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

（注）
情報を入力した後、チェックマーク アイコンをクリックして保存します。

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、前提条件とガイドライン （9 ページ） を参照してください。

f) **[+ NTP ホスト名/IP アドレスの追加（+Add NTP Host Name/IP Address）]** をクリックして、1 つ以上の NTP サーバを追加します。

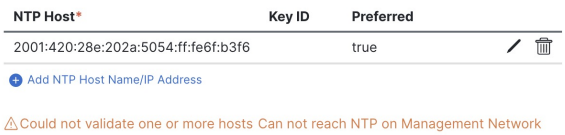
次のフィールドで、以下の情報を提供します。

- **NTP ホスト**：IP アドレスを指定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**：このサーバーの NTP 認証を有効にする場合は、前の手順で定義した NTP キーのキー ID を指定します。

  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 NTP サーバーを **[優先（Preferred）]** にするかどうかを選択します。

情報を入力した後、チェックマーク アイコンをクリックして保存します。

（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（次の手順で指定します）、NTP サーバーの IPv6 アドレスに接続できないためです。

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 サーバーを指定する場合は、**[+NTP ホストの追加（+Add NTP Host）]** を再度クリックし、このサブステップを繰り返します。

g) **[プロキシ サーバー（Proxy Server）]** を指定し、**[検証（Validate）]** をクリックします。

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。

[+無視するホストを追加（+Add Ignore Host）] をクリックして、プロキシをスキップする 1 つ以上の IP アドレス通信を提供することもできます。

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
```

プロキシ設定をスキップする場合は、**[プロキシをスキップ（Skip Proxy）]** をクリックします。

h) (オプション) プロキシ サーバで認証が必要な場合は、**[プロキシで認証が必要（Authentication required for Proxy）]** を **[はい（Yes）]** に変更し、ログイン資格情報を指定します。

i) (オプション) **[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。

- カスタム **App Network** と **Service Network** を提供します。

  アプリケーション オーバーレイ ネットワークは、Nexus ダッシュボードで実行されるアプリケーションのサービスで使用されるアドレス空間を定義します。このフィールドには、デフォルトの `172.17.0.1/16` 値が事前に入力されています。

  サービス ネットワークは、Nexus ダッシュボードとそのプロセスで使用される内部ネットワークです。このフィールドには、デフォルトの `100.80.0.0/16` 値が事前に入力されています。

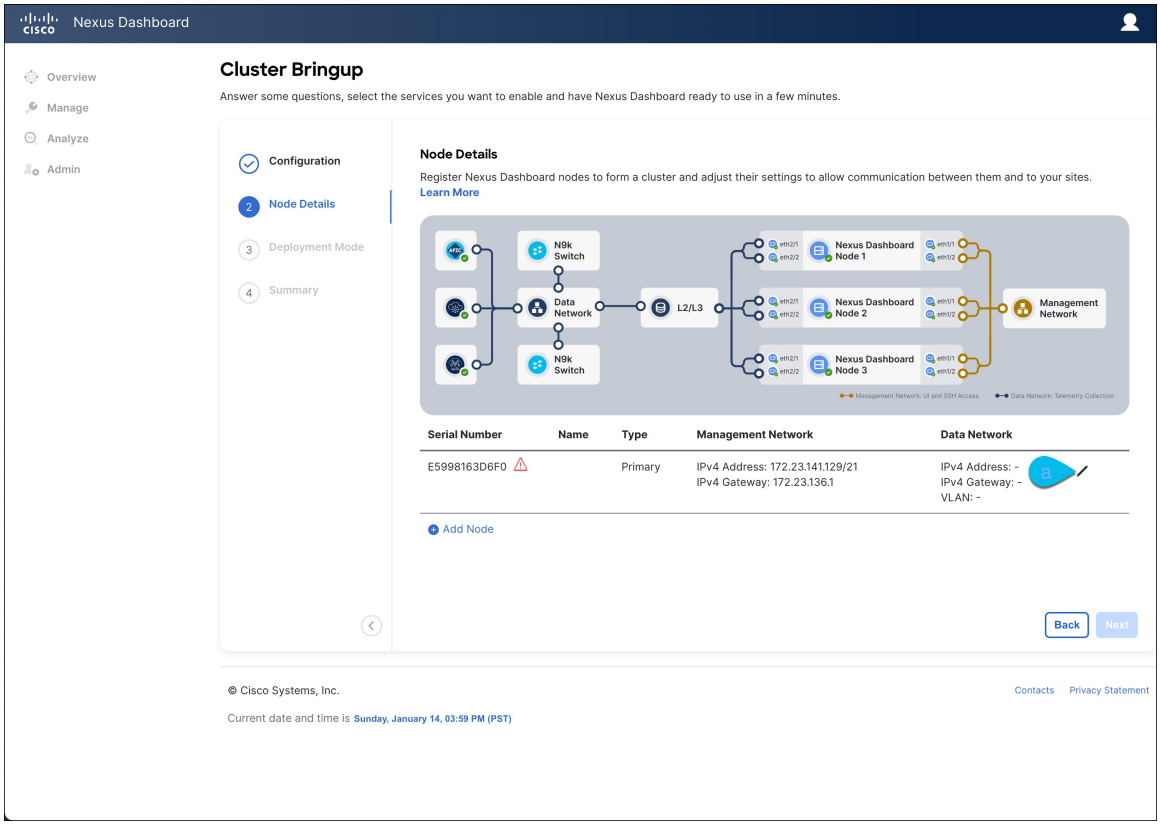
  以前に **[IPv6 を有効にする（Enable IPv6）]** オプションをオンにした場合は、アプリケーション ネットワークとサービス ネットワークの IPv6 サブネットを定義することもできます。

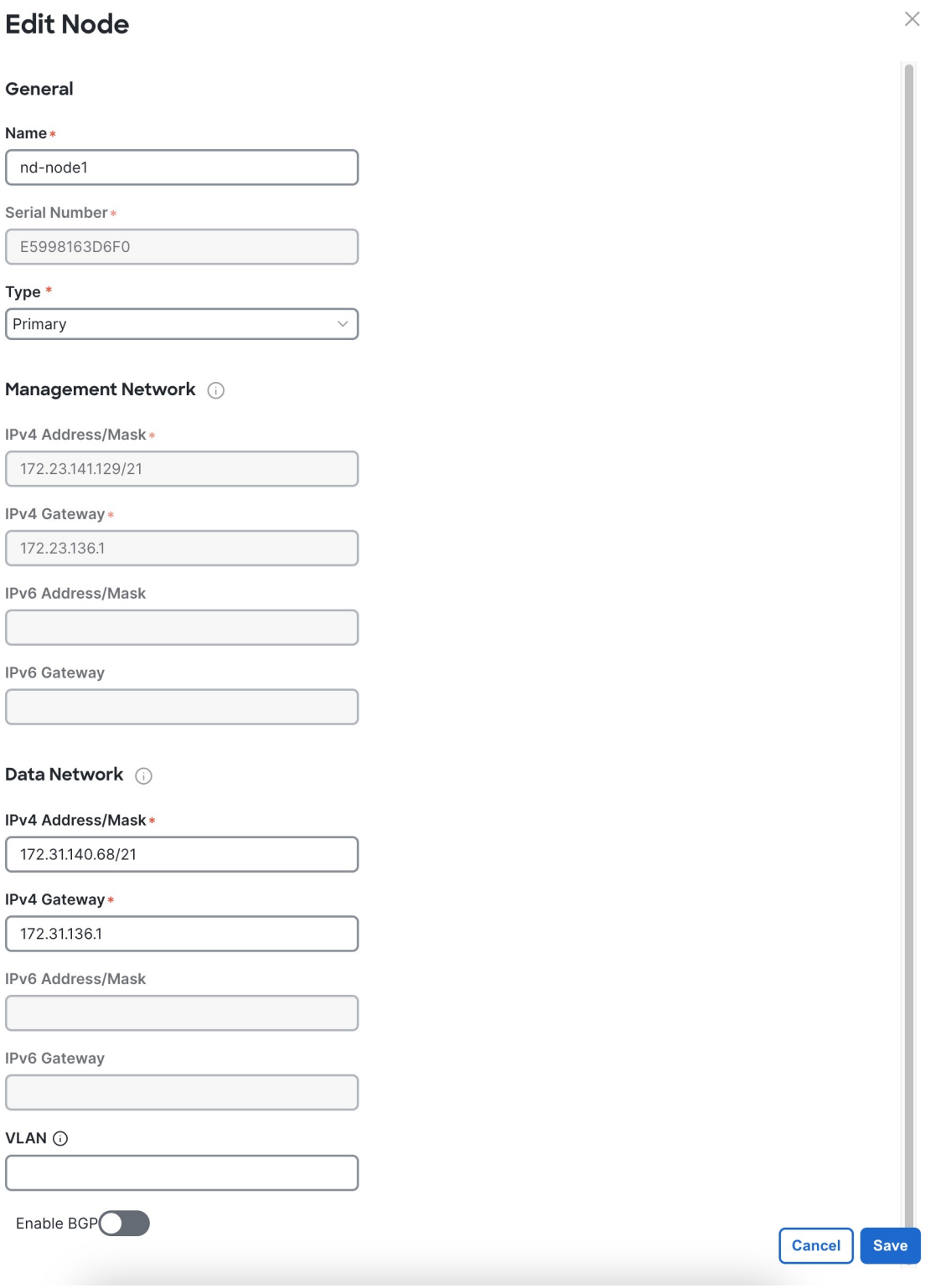
  アプリケーションおよびサービスネットワークについては、このドキュメントの前の 前提条件とガイドライン （9 ページ） の項で説明します。

j) [次へ（Next）] をクリックして続行します。

ステップ 12 **[ノードの詳細（Node Details）]** 画面で、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) 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、他の情報は手動で入力する必要があります。

b) ノードの **[名前（Name）]** 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。

c) **[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。サービスの共同ホスティングや、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。

d) **[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。

e) （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。

Insights やファブリック コントローラなどの、一部のサービスで使用される永続的な IP 機能には、BGP 構成が必要です。この機能については、前提条件とガイドライン （9 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**。

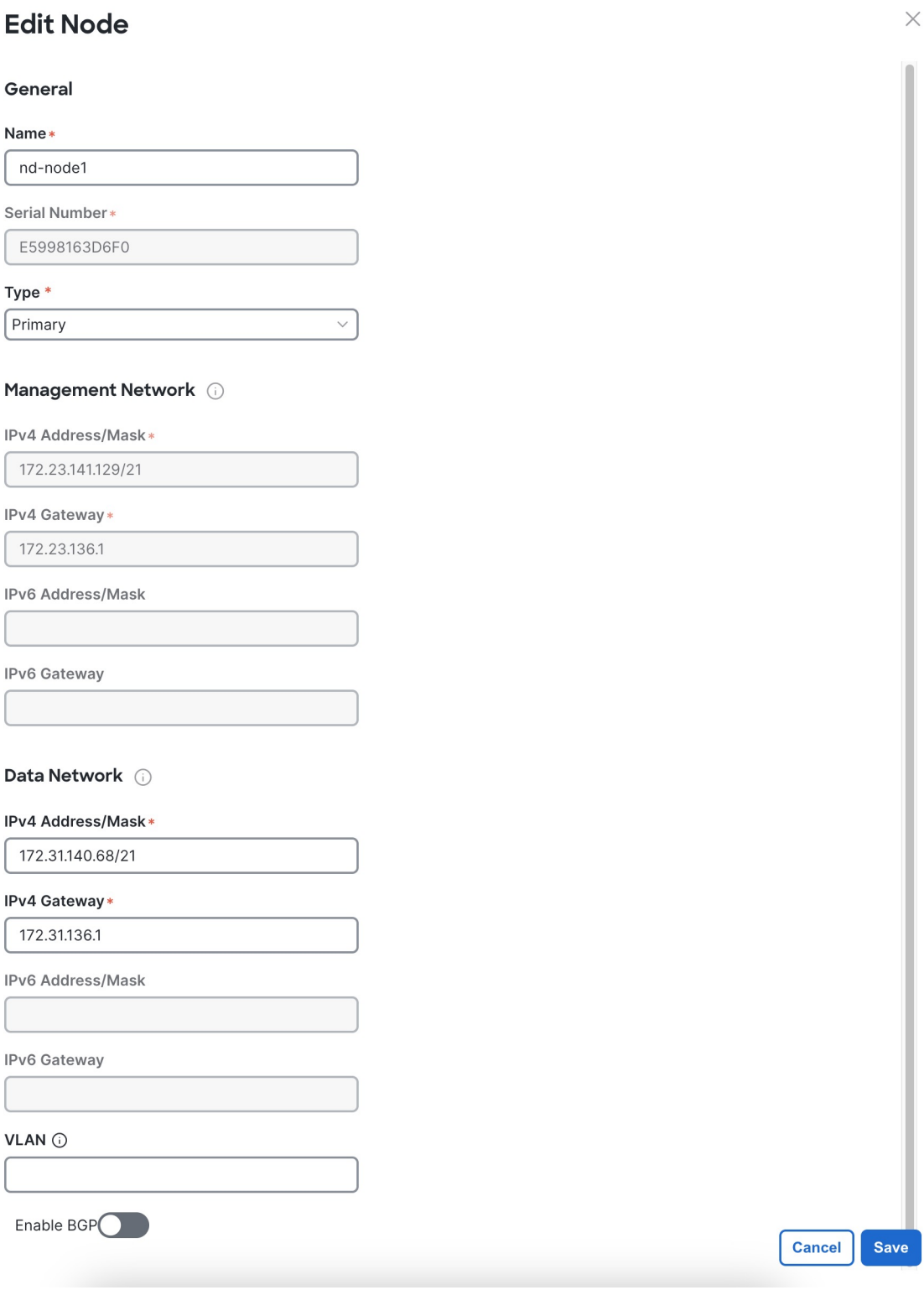
  ルータ ID は、`1.1.1.1` などの IPv4 アドレスである必要があります。

- 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**。

f) **[Save]**をクリックして、変更内容を保存します。

ステップ 13 [**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。サービスの共同ホスティングや、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) （任意）必要に応じて、データ ネットワークの **BGP を有効にします**。

Insights やファブリック コントローラなどの、一部のサービスで使用される永続的な IP 機能には、BGP 構成が必要です。この機能については、前提条件とガイドライン （9 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**。

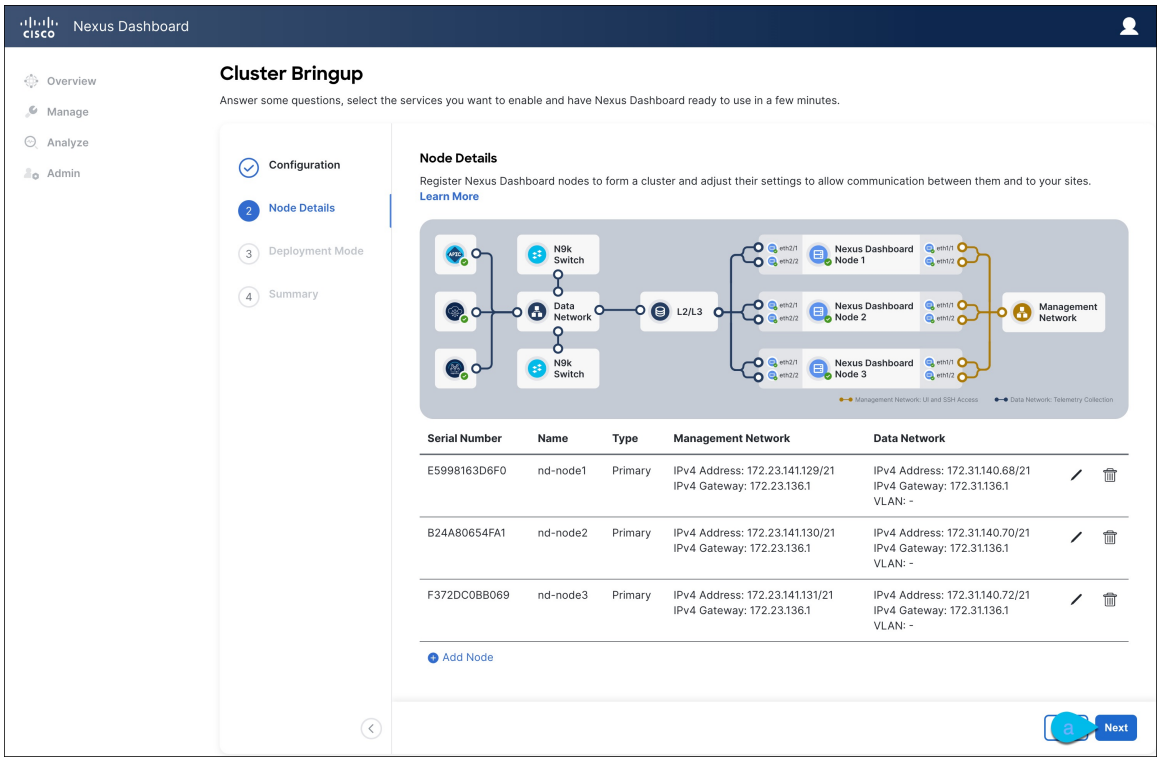
  ルータ ID は、`1.1.1.1` などの IPv4 アドレスである必要があります。

- 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 14 **[ノードの詳細（Node Details）]** ページで、入力した情報を確認し、**[次へ（Next）]** をクリックして続行します。



ステップ 15 クラスタの**展開モード**を選択します。

a) 有効にするサービスを選択します。

リリース 3.1(1) より前では、クラスタの初期展開が完了した後に、個々のサービスをダウンロードしてインストールする必要がありました。今では、初期インストール時にサービスを有効にするように選択できます。

（注）
クラスタ内のノードの数によっては、一部のサービスまたは共同ホスティングのシナリオがサポートされない場合があります。必要な数のサービスを選択できない場合は、**[戻る（Back）]** をクリックし、前の手順で十分な数のセカンダリ ノードを指定したことを確認します。

b) **[永続サービスIP/プールの追加（Add Persistent Service IPs/Pools）]** をクリックして、Insights または ファブリック コントローラ サービスに必要な 1 つ以上の永続 IP を指定します。

永続的 IP の詳細については、ユーザー ガイドの前提条件とガイドライン （9 ページ）のセクションを参照してください。

c) [次へ（Next）] をクリックして続行します。

ステップ 16 **[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。

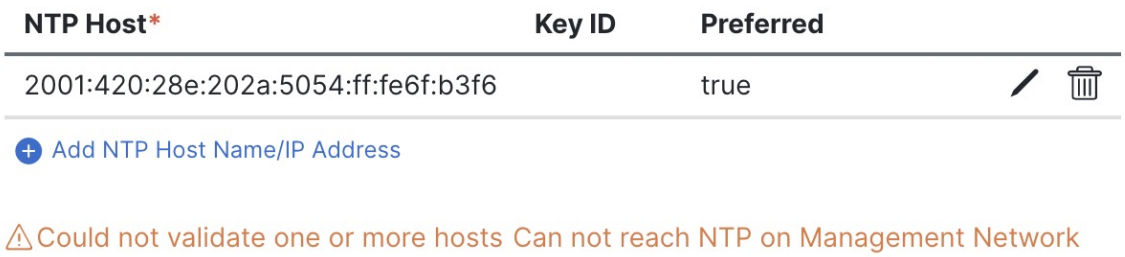
ノードのブート ストラップとクラスタの起動中に、全体的な進捗状況と各ノードの個々の進捗状況がUIに表示されます。ブートストラップの進行状況が表示されない場合は、ブラウザでページを手動で更新し、ステータスを更新してください。

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。

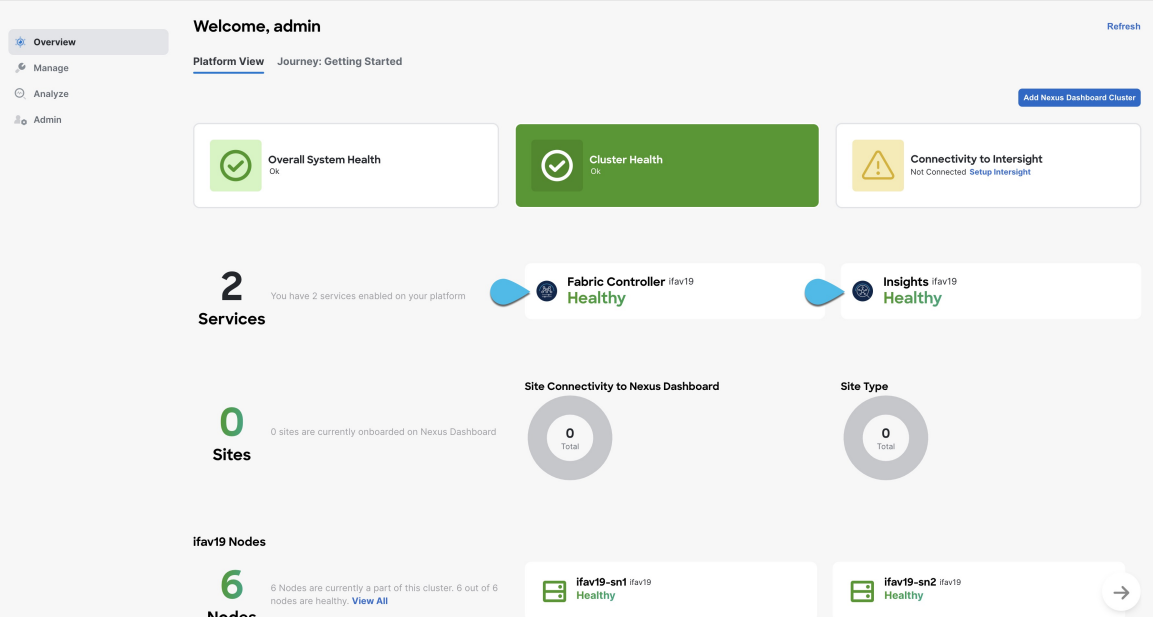
ステップ 17 クラスタが健全であることを検証します。

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、**[概要（Overview）]** ページ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、ノード展開中に指定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。

第 10 章

Amazon Web Services での展開

- 前提条件とガイドライン （157 ページ）
- AWS での Nexus ダッシュボードの展開 （159 ページ）

前提条件とガイドライン

（注） クラウドホスト型フォームファクタに展開できるのは、Nexus Dashboard オーケストレータ サービスのみです。

Amazon Web Services（AWS）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 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。

- デプロイ概要 （5 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（`m5.2xlarge`）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。
- 6 つ以上の AWS Elastic IP アドレスが必要です。

  一般的な Nexus ダッシュボードの導入は 3 つのノードで構成され、各ノードには管理およびデータネットワーク用に 2 つの AWS Elastic IP アドレスが必要です。

デフォルトでは、AWS アカウントの Elastic IP の制限は低いため、増加を要求する必要があります。IP 制限の増加を要求するには、次の手順を実行します。

1. AWS コンソールで、**[Computer]** > **[EC2]** の順に移動します。
2. EC2 ダッシュボードで、**[Network & Security]** > **[Elastic IPs]** をクリックし、すでに使用されている Elastic IP の数を確認します。
3. EC2 ダッシュボードで、**[制限（Limits）]** をクリックし、許可されている **EC2-VPC Elastic IP** の最大数を確認します。

   使用する IP の数を制限から減算します。必要に応じて、**[制限の増加を要求（Request limit 増加）]** をクリックして追加の Elastic IP を要求します。

- VPC（仮想プライベート クラウド）を作成します。

  VPC は、Amazon EC2 インスタンスなどの AWS オブジェクトによって入力される AWS クラウドの分離された部分です。VPC を作成するには:

  1. AWS コンソールで、**[Networking & Content Delivery Tools] [VPC]**に移動します。
  2. VPC ダッシュボードで **[Your VPCs]** をクリックし、**[Create VPC]** を選択します。次に、**名前タグ**と **IPv4 CIDR ブロック** を指定します。

     CIDR ブロックは VPC の IPv4 アドレスの範囲であり、`/16`〜`/24` の範囲である必要があります。たとえば、`10.9.0.0/16` です。

- インターネット ゲートウェイを作成し、VPC に接続します。

  インターネット ゲートウェイは、VPC がインターネットに接続できるようにする仮想ルータです。インターネット ゲートウェイを作成するには:

  - [VPC ダッシュボード（VPC Dashboard）] > **[インターネット ゲートウェイ（Internet Gateway）]** の順にクリックしてから、**[インターネット ゲートウェイの作成（Create Internet Gateway）]** をクリックします。次に、**名前タグ**を入力します。
  - **[インターネット ゲートウェイ（Internet Gateways）]** 画面で、作成したインターネット ゲートウェイを選択し、**[アクション]** > **[VPC をアタッチ]** を選択します。最後に、**[使用可能な VPC（Available VPCs）]** ドロップダウンから、作成した VPC を選択し、**[インターネット ゲートウェイのアタッチ（Attach Internet Gateway）]** をクリックします。

- ルート テーブルを作成します。

  ルートテーブルは、VPC およびインターネット ゲートウェイ内のサブネットを Nexus ダッシュボード クラスタに接続するために使用されます。ルート テーブルを作成するには、次の手順を実行します。

  - VPC ダッシュボードで、**[ルート テーブル（Route Tables）]** をクリックし、**[ルート（Routes）]** タブを選択して、**[ルートの編集（Edit routes）]** をクリックします。

- **[ルートの編集（Edit routes）]** 画面で、**[ルートの追加（Add route）]** をクリックし、`0.0.0.0/0` の宛先を作成します。**[ターゲット（Target）]** ドロップダウンから `[インターネット ゲートウェイ（Target Internet Gateway）]` から、作成したゲートウェイを選択します。最後に、**[ルートの保存（Save Routes）]** をクリックします。

- キー ペアを作成します。

  キー ペアは、プライベート キーとパブリック キーで構成され、インスタンスへの接続時に ID を証明するために使用されるセキュリティ クレデンシャルとして使用されます。キー ペアを作成するには:

  - **[すべてのサービス（All services）]** > **[コンピュート（Compute）]** > **[EC2]**に移動します。
  - EC2 ダッシュボードで、**[ネットワークとセキュリティ（Network & Security）]** > **[キーペア（Key pairs）]** をクリックします。次に、**[キー ペアの作成 (Create Key Pair)]** をクリックします。
  - キー ペアの名前を入力し、**pem** ファイル形式を選択して、**[キー ペアの作成 (Create Key Pair)]** をクリックします。

    これにより、`.pem` 秘密キー ファイルがシステムにダウンロードされます。ファイルを安全な場所に移動します。EC2インスタンスのコンソールに初めてログインするときに使用する必要があります。

（注） デフォルトでは、PEMベースのログインのみが各ノードで有効になっています。GUI セットアップ ウィザードで要求されるパスワードを使用してノードにSSHで接続できるようにするには、生成されたキーを使用して各ノードにログインし、以下のセットアップセクションの説明に従って必要なコマンドを実行することにより、パスワードベースのログインを明示的に有効にする必要があります。

AWS での Nexus ダッシュボードの展開

ここでは、Amazon Web Services (AWS) 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

- 前提条件とガイドライン （157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) [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 ダッシュボード**を検索し、結果をクリックします。

f) 製品ページで、**[続行して登録（Continue to Subscribe）]** をクリックします。

g) [条件に同意する（Accept Terms）] をクリックします。

サブスクリプションが処理されるまでに数分かかる場合があります。

h) 最後に、**[設定を続行 (Continue to Configuration)]** 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) **[配送方法（Delivery Method）]**ドロップダウンから、`[Cisco Nexus Dashboard for Cloud]` を選択します。

b) **[ソフトウェア バージョン（Software Version）]** ドロップダウンから、展開するバージョンを選択します。

c) **[リージョン（Region）]** ドロップダウンから、テンプレートを展開する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。

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

この製品 ページが表示され、設定の概要が表示され、クラウド形成テンプレートを起動できます。

ステップ 3 **[アクションの選択（Choose Action）]** から、`[CloudFormation の起動（Launch CloudFormation）]` を選択し、**[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 4 スタックを作成します。

a) **[前提条件 - テンプレートの準備（Prerequisite-Prepare template）]** 領域で、`[テンプレート準備完了（Template is ready）]` を選択します。

b) **[テンプレートの指定（Specify Template）]** フィールドで、テンプレート ソースとして `[Amazon S3 URL]` を選択します。

これは、自動的に入力されます。

c) [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 5 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) **[VPC ID]** ドロップダウンから、作成した VPC を選択します。

たとえば、`vpc-038f83026b6a48e98（10.176.176.0/24）`です。

c) **ND クラスタ サブネット ブロック**で、VPC サブネット CIDR ブロックを指定します。

定義した VPC CIDR からサブネットを選択します。より小さいサブネットを提供することも、CIDR 全体を使用することもできます。CIDR は `/24` または `/25` サブネットにすることができ、可用性ゾーン全体で使用されるようにセグメント化されます。

たとえば、`10.176.176.0/24` です。

d) **[可用性ゾーン（Availability Zones）]** ドロップダウンから、1 つ以上の使用可能なゾーンを選択します。

3 つの可用性ゾーンを選択することをお勧めします。2 つの可用性ゾーンのみをサポートするリージョンの場合、クラスタの 2 番目と 3 番目のノードは 2 番目の可用性ゾーンで起動します。

e) **[可用性ゾーンの数（Number of Availability Zones）]** ドロップダウンから、前のサブステップで追加したゾーンの数を選択します。

この番号が、前のサブステップで選択した可用性ゾーンの数と一致していることを確認します。

f) **データ インターフェイス EIP サポート**を有効にします。

このフィールドは、ノードの外部接続を有効にします。AWS 以外の Cisco ACI ファブリックとの通信には、外部接続が必要です。

g) **[パスワード（Password）]** および **[パスワードの確認（Confirm Password）]** フィールドに、パスワードを提供します。

このパスワードは、Nexus ダッシュボードの`レスキュー ユーザ`ログインと、GUI の`管理者ユーザ`の初期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。

h) **[SSH key pair]** ドロップダウンから、作成したキーペアを選択します。

i) **[アクセス制御（Access control）]** フィールドに、クラスタへのアクセスを許可する外部ネットワークを指定します。

たとえば、`0.0.0.0/0` は、どこからでもクラスタにアクセスできます。

j) [**次へ（Next）**] をクリックして続行します。

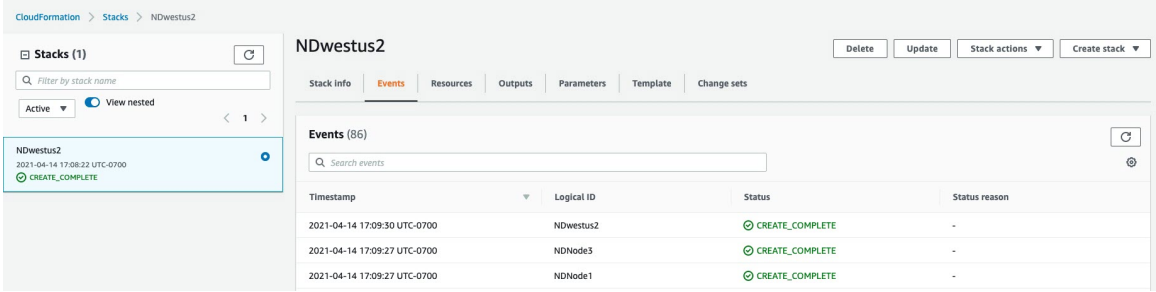
ステップ 6 **[詳細オプション（Advanced options）]** 画面で、**[次へ（Next）]**をクリックします。

ステップ 7 **[レビュー（Review）]** 画面で、テンプレート設定を確認し、**[スタックの作成（Create stack）]** をクリックします。

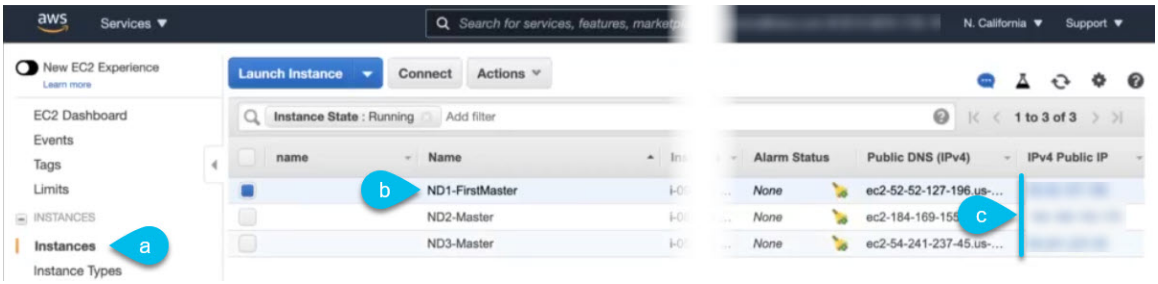
ステップ 8 展開が完了するのを待ってから、VM を起動します。

[CloudFormation] 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 9 すべてのノードのパブリック IP アドレスを書き留めます。



a) すべてのインスタンスが展開されたら、AWS コンソールの **EC2** > **Instances** ページに移動します。

b) FirstMaster とラベル付けされているノードを書き留めます。

このノードのパブリック IP アドレスを使用して、クラスタ設定を完了します。

c) すべてのノードのパブリック IP アドレスを書き留めます。

次の手順で、この情報を GUI ブートストラップ ウィザードに提供します。

ステップ 10 すべてのノードでパスワードベースのログインを有効にします。

デフォルトでは、PEM ベースのログインのみが各ノードで有効になっています。パスワードを使用して SSH をノードに接続できるようにするには、GUI セットアップ ウィザードで要求されるように、パスワードベースのログインを明示的に有効にする必要があります。

（注）
次の手順で説明するクラスタブートストラップに進む前に、すべてのノードでパスワードベースのログインを有効にする必要があります。そうしないと、クラスタ設定を完了できません。

a) パブリック IP アドレスと PEM ファイルを使用して、インスタンスの 1 つに SSH で接続します。

このために作成した PEM ファイルを 前提条件とガイドライン（157 ページ） の一部として使用します。

```
# ssh -i <pem-file-name>.pem rescue-user@<node-public-ip>
```

b) パスワードベースのログインを有効にします。

各ノードで、次のコマンドを実行します。

```
# acs login-prompt enable
```

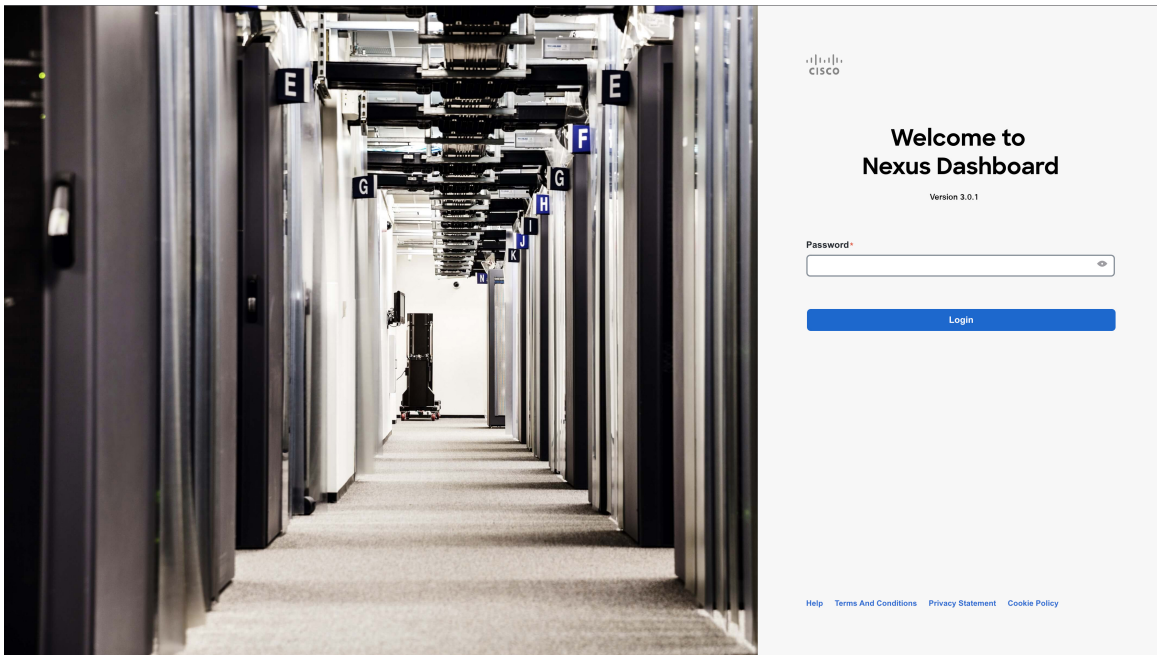
c) 他の 2 つのインスタンスについて、この手順を繰り返します。

ステップ 11 ブラウザを開き、`https://<first-node-public-ip>` に移動して、GUI を開きます。

（注）
最初のノード（`FirstMaster`）のパブリック IP アドレスを使用する必要があります。そうしないと、クラスタ構成を完了できません。

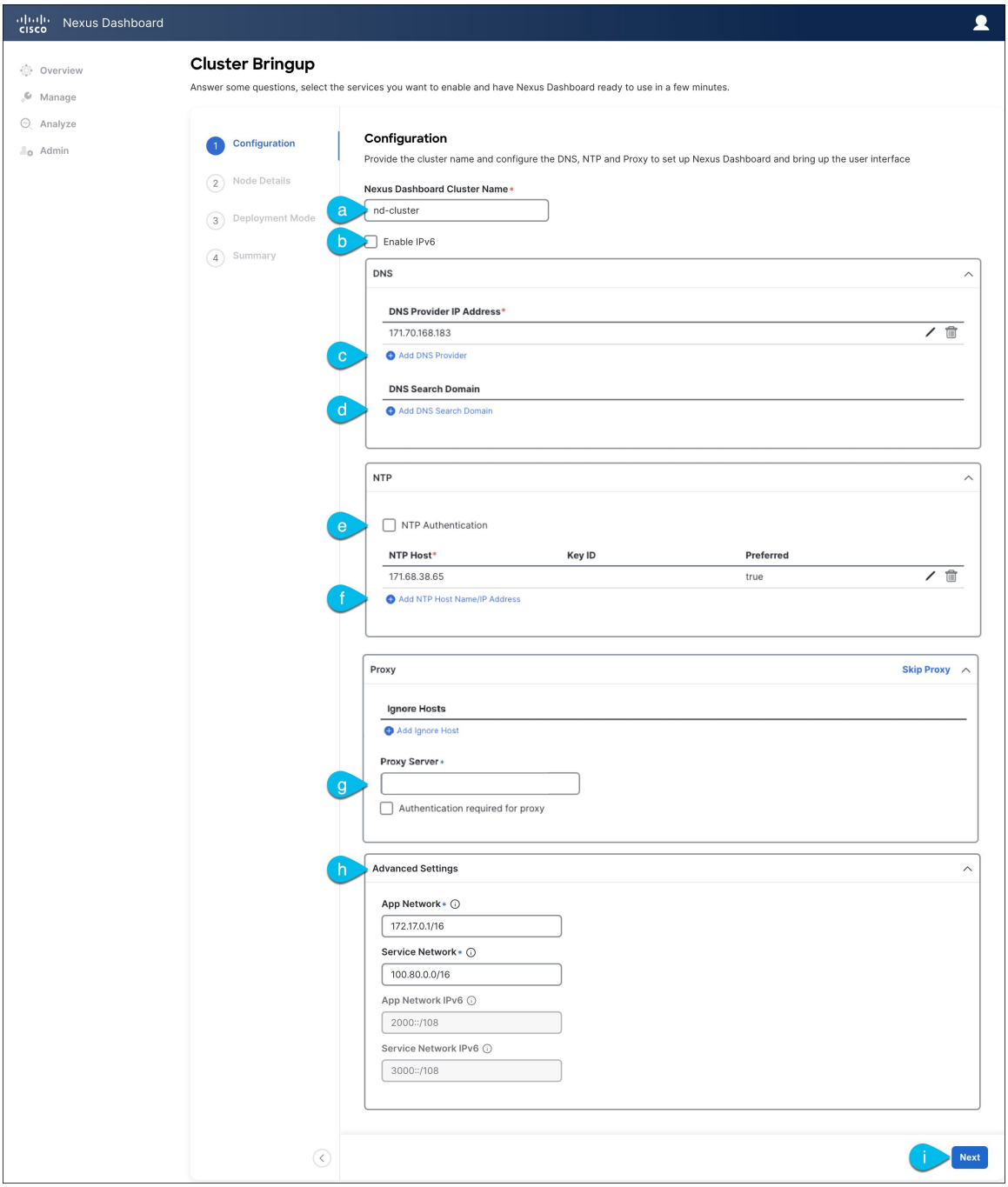
残りの設定ワークフローは、最初のノードの GUI から実行します。他の 2 つのノードに直接ログインまたは設定する必要はありません。

最初のノードに指定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 12 **[クラスタの詳細（Cluster Details）]** を入力します。

[クラスタ起動（Cluster Bringup）] ウィザードの **[クラスタの詳細（Cluster Details）]** 画面で、次の情報を入力します。



a) Nexus ダッシュボード クラスタの **[クラスタ名（Cluster Name）]** 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) （オプション）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。

c) **[+DNS プロバイダの追加（+Add DNS Provider）]** をクリックして、1 つ以上の DNS サーバを追加します。

情報を入力した後、チェックマーク アイコンをクリックして保存します。

d) （オプション）**[+DNS 検索ドメインの追加（+Add DNS Search Domain ）]** をクリックして、検索ドメインを追加します。

情報を入力した後、チェックマーク アイコンをクリックして保存します。

e) （オプション）NTP サーバー認証を有効にする場合には、**[NTP 認証（NTP Authentication）]** チェックボックスをオンにし、**[NTP キーの追加（Add NTP Key）]**をクリックします。

次のフィールドで、以下の情報を提供します。

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

（注）
情報を入力した後、チェックマーク アイコンをクリックして保存します。

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、前提条件とガイドライン （9 ページ） を参照してください。

f) **[+ NTP ホスト名/IP アドレスの追加（+Add NTP Host Name/IP Address）]** をクリックして、1 つ以上の NTP サーバを追加します。

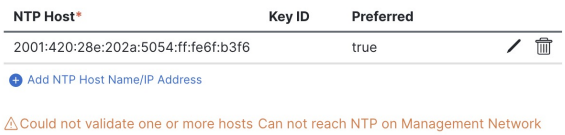
次のフィールドで、以下の情報を提供します。

- **NTP ホスト**：IP アドレスを指定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**：このサーバーの NTP 認証を有効にする場合は、前の手順で定義した NTP キーのキー ID を指定します。

  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 NTP サーバーを **[優先（Preferred）]** にするかどうかを選択します。

情報を入力した後、チェックマーク アイコンをクリックして保存します。

（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（次の手順で指定します）、NTP サーバーの IPv6 アドレスに接続できないためです。

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 サーバーを指定する場合は、**[+NTP ホストの追加（+Add NTP Host）]** を再度クリックし、このサブステップを繰り返します。

g) **[プロキシ サーバー（Proxy Server）]** を指定し、**[検証（Validate）]** をクリックします。

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。

[+無視するホストを追加（+Add Ignore Host）] をクリックして、プロキシをスキップする 1 つ以上の IP アドレス通信を提供することもできます。

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
```

プロキシ設定をスキップする場合は、**[プロキシをスキップ（Skip Proxy）]** をクリックします。

h) (オプション) プロキシ サーバで認証が必要な場合は、**[プロキシで認証が必要（Authentication required for Proxy）]** を **[はい（Yes）]** に変更し、ログイン資格情報を指定します。

i) (オプション) **[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。

- カスタム **App Network** と **Service Network** を提供します。

  アプリケーション オーバーレイ ネットワークは、Nexus ダッシュボードで実行されるアプリケーションのサービスで使用されるアドレス空間を定義します。このフィールドには、デフォルトの `172.17.0.1/16` 値が事前に入力されています。

  サービス ネットワークは、Nexus ダッシュボードとそのプロセスで使用される内部ネットワークです。このフィールドには、デフォルトの `100.80.0.0/16` 値が事前に入力されています。

  以前に **[IPv6 を有効にする（Enable IPv6）]** オプションをオンにした場合は、アプリケーション ネットワークとサービス ネットワークの IPv6 サブネットを定義することもできます。

  アプリケーションおよびサービスネットワークについては、このドキュメントの前の 前提条件とガイドライン （9 ページ） の項で説明します。

j) [**次へ（Next）**] をクリックして続行します。

ステップ 13 **[ノードの詳細（Node Details）]** 画面で、ノードの情報を入力します。

a) 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。

b) ノードの**名前**を入力します。

管理ネットワークと**データ ネットワーク**の情報は、クラスタを展開する前に構成した VPC サブネットから既に入力されています。

クラスタは、指定された VPC CIDR から 6 つのサブネットを作成し、そこからデータと管理ネットワークがクラスタの 3 つのノードに割り当てられます。

c) IPv6 アドレスと VLAN フィールドは空白のままにします。

Cloud Nexus ダッシュボード クラスタは、これらのオプションをサポートしていません。

d) **[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。

[ノードの詳細（Node Details）] ウィンドウが開きます。

a) ノードの**名前**を入力します。

b) **[資格情報（Credentials）]** セクションで、ノードの**パブリック IP アドレス**とテンプレートの展開時に指定したパスワードを入力し、**[検証（Verify）]** をクリックします。

IP アドレスとパスワードは、そのノードの**管理ネットワーク**と**データ ネットワーク**情報を取得するために使用され、下のフィールドに入力されます。

c) **[保存 (Save)]**をクリックして、変更内容を保存します。

ステップ 15 前の手順を繰り返して、3番目のノードを追加します。

ステップ 16 **[ノードの詳細（Node Details）]** ページで、**[次へ（Next）]** をクリックして続行します。

ステップ 17 クラスタの**展開モード**を選択します。

a) 有効にするサービスを選択します。

リリース 3.1(1) より前では、クラスタの初期展開が完了した後に、個々のサービスをダウンロードしてインストールする必要がありました。今では、初期インストール時にサービスを有効にするように選択できます。

（注）
クラスタ内のノードの数によっては、一部のサービスまたは共同ホスティングのシナリオがサポートされない場合があります。必要な数のサービスを選択できない場合は、**[戻る（Back）]** をクリックし、前の手順で十分な数のセカンダリ ノードを指定したことを確認します。

b) **[永続サービスIP/プールの追加（Add Persistent Service IPs/Pools）]** をクリックして、Insights または ファブリック コントローラ サービスに必要な 1 つ以上の永続 IP を指定します。

永続的 IP の詳細については、ユーザー ガイドの前提条件とガイドライン （9 ページ）のセクションを参照してください。

c) [次へ（Next）] をクリックして続行します。

ステップ 18 **[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。

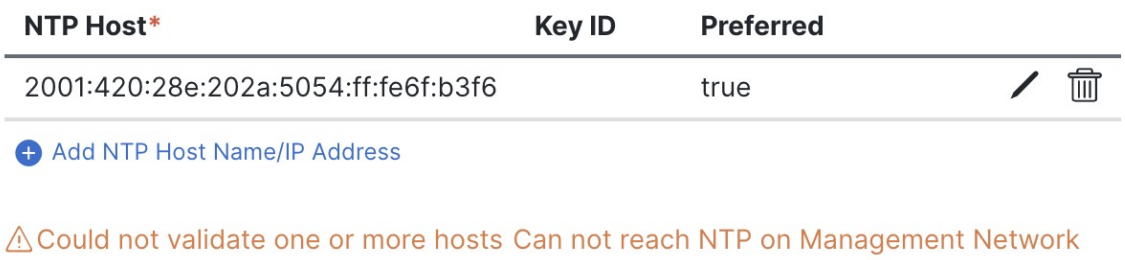
ノードのブート ストラップとクラスタの起動中に、全体的な進捗状況と各ノードの個々の進捗状況がUIに表示されます。ブートストラップの進行状況が表示されない場合は、ブラウザでページを手動で更新し、ステータスを更新してください。

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。

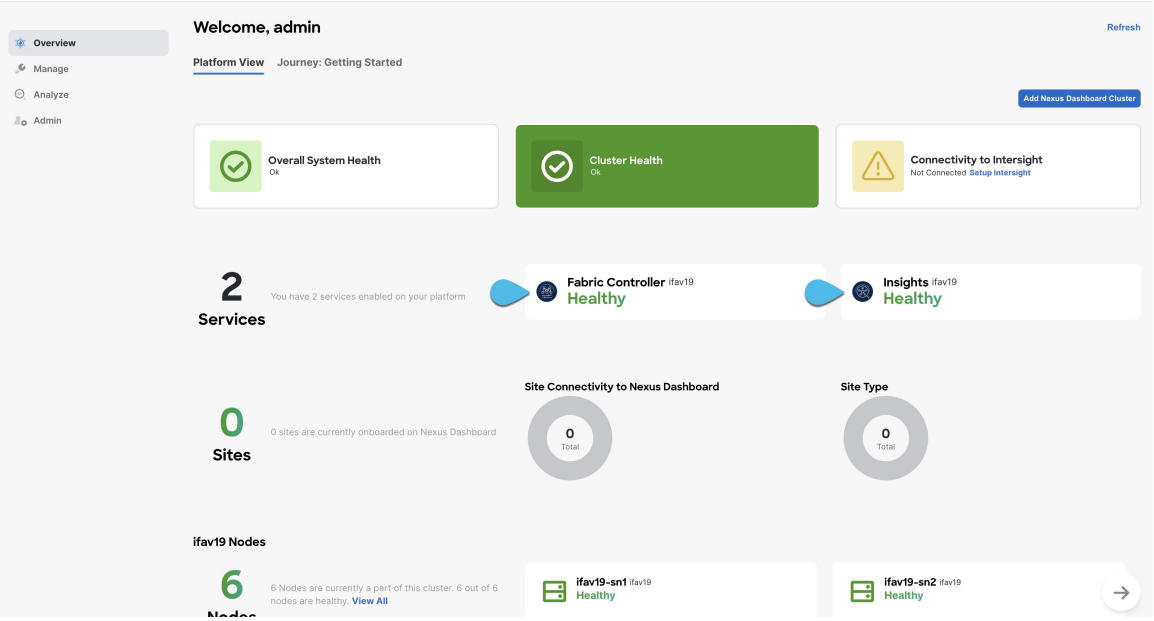
ステップ 19 クラスタが健全であることを検証します。

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、**[概要（Overview）]** ページ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、ノード展開中に指定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
```

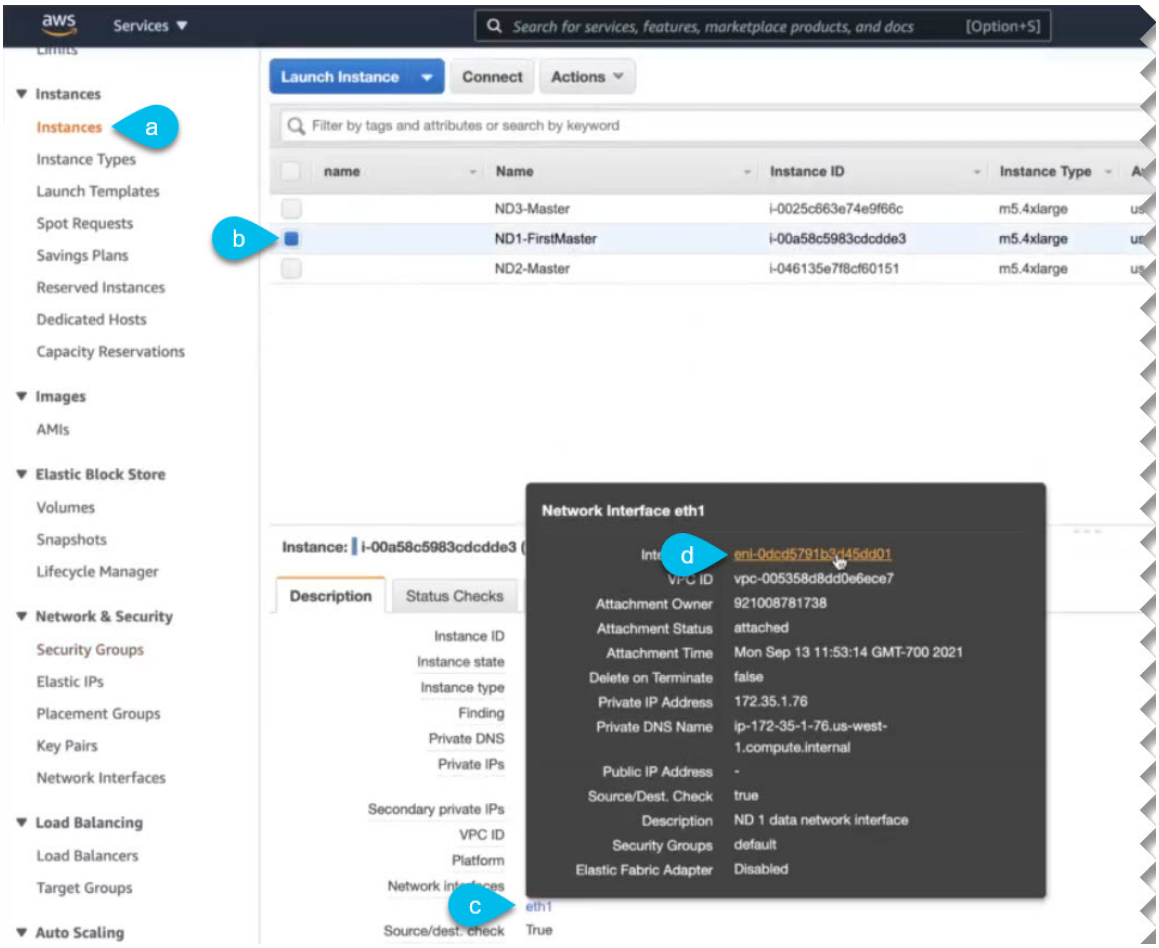
これは、pND（物理 Nexus Dashboard）クラスタの再起動後のノードの `etcd` の問題が原因です。

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 20 必要なポートでノードのセキュリティ グループを更新します。

この手順では、Cisco NDFC サイトのオンボーディングに必要なポート設定で Nexus ダッシュボード ノードのインスタンスを更新する方法について説明します。Nexus ダッシュボード クラスタへの NDFC サイトのオンボーディングを計画していない場合は、この手順をスキップできます。

いずれかのノードのデータ インターフェイスに移動します。



a) AWS コンソールで、**[インスタンス（Instances）]** に移動します。

b) Nexus ダッシュボード インスタンスの 1 つを選択します。

デフォルトのセキュリティ グループに変更を加えるため、ノードの 1 つを選択するだけで済みます。

c) データ インターフェイスをクリックします（`eth1`）。

d) **[インターフェイス ID（Interface ID）]** をクリックします。

[ネットワークインターフェイス（Network Interface）] ページが開きます。

e) **[ネットワーク インターフェイス（Network Interface）]** ページで、インターフェイスの [セキュリティ グループ（`Security groups`）] 列の **[デフォルト（default）]** をクリックします。

新しいルールを追加します。

a) デフォルトのセキュリティ グループのページで、**[インバウンド ルール（Inbound rules）]** タブを選択します。

b) **[インバウンド ルールの編集（Edit Inbound Rules）]** をクリックします。

c) **[インバウンド ルールの編集（Edit inbound rules）]** ページで、**[ルールの追加（Add rule）]** をクリックして新しいインバウンド セキュリティ ルールを追加し、ポート 443 でのインバウンド通信を許可するための詳細を指定します。

新しいルールについて、次の情報を提供します。

- **[タイプ（Type）]** で、[カスタム TCP（Custom TCP）] を選択します。
- **[ポート範囲（Port range）]** に 443 を入力します。
- **[ソース（Source）]** には、Nexus ダッシュボードにオンボードする予定の NDFC コントローラの IP アドレスを指定します。

d) 引き続き **[インバウンド ルールの編集（Edit inbound rules）]** ページで、**[ルールの追加（Add rule）]** をクリックして別のインバウンド セキュリティ ルールを追加し、ポート 9092 でのインバウンド通信を許可するための詳細を指定します。

新しいルールについて、次の情報を提供します。

- **[タイプ（Type）]** で、[カスタム TCP（Custom TCP）] を選択します。
- **[ポート範囲（Port range）]** には、9092 と入力します。
- **[ソース（Source）]** には、Nexus ダッシュボードにオンボードする予定の NDFC コントローラの IP アドレスを指定します。

第 11 章

Microsoft Azure での展開

- 前提条件とガイドライン （173 ページ）
- Azure での Nexus ダッシュボードの展開 （178 ページ）

前提条件とガイドライン

（注） クラウドホスト型フォームファクタに展開できるのは、Nexus Dashboard オーケストレータ サービスのみです。

Microsoft Azure で Nexus ダッシュボード クラスタを展開する前に、次の作業を行う必要があります。

- ファクターから Azure 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。

- デプロイ概要 （5 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。
- Azure アカウントとサブスクリプションに適切なアクセス権限を持っている。
- Nexus ダッシュボード クラスタ リソースのリソース グループを作成しました。

（注） リソース グループは空である必要があり、既存のオブジェクトが含まれていない必要があります。既存のオブジェクトを持つリソース グループは、Nexus ダッシュボードの展開には使用できません。

リソース グループを作成するには:

- Azureポータルで、**[すべてのリソース（All Resources）]**>**[リソース グループ（Resource Groups）]** に移動します。
- 新しいメディア リソース グループを作成するには、**[+追加（+Add）]** をクリックします。
- **[リソース グループの作成（Create a resource group）]** 画面で、Nexus ダッシュボード クラスタに使用するサブスクリプションの名前、リソースグループの名前（`nd-cluster` など）、およびリージョンを入力します。

- 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。
- SSH キー ペアを生成します。

  キー ペアは秘密キーと公開キーで構成され、Nexus ダッシュボード ノードを作成するときに、公開キーを入力するように求められます。

（注） クラスタの展開手順中に一般的な SSH ログインを有効にするには、各ノードへの 1 回限りのログイン用の公開キーを作成するのと同じマシンを使用する必要があります。

SSH キーの作成については、以下の Linux または MacOS での SSH キー ペアの生成 （174 ページ） および Windows での SSH キー ペアの生成 （175 ページ） セクションで説明します。

Linux または MacOS での SSH キー ペアの生成

次の手順では、Linux または MacOS で SSH 公開キーと秘密キーのペアを生成する方法について説明します。Windows で SSH 公開キーと秘密キーのペアを生成する手順については、を参照してください。Windows での SSH キー ペアの生成 （175 ページ）

手順

ステップ 1 Linux 仮想マシンまたは Mac で、ssh-keygen を使用して公開キーと秘密キーのペアを作成し、出力をファイルに送信します。

```
# ssh-keygen -f filename
```

次に例を示します。

```
# ssh-keygen -f azure_key
```

次のような出力が表示されます。パスフレーズを入力するように求められたら、テキストを入力せずに Enter キーを押します（パスフレーズがないようにフィールドを空のままにします）。

```
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in azure_key.
Your public key has been saved in azure_key.pub.
The key fingerprint is:
SHA256:gTsQIIAadjgNsgcguifIloh4XGpVWMdcXVV6U0dyBNs
...
```

ステップ 2 保存した公開キーファイルと秘密キーファイルを見つけます。

```
# ls
```

2 つのファイルが表示されます。

- 拡張子が .pub のファイルには、公開キー情報が含まれています。
- 同じ名前でサフィックスのないファイルに秘密キー情報が含まれている

たとえば、出力を azure_key という名前のファイルに送信すると、次の出力が表示されます。

```
# ls
azure_key
azure_key.pub
```

その場合、次のようになります。

- azure_key.pub ファイルには、公開キー情報が含まれています。
- azure_key ファイルには秘密キー情報が含まれています。

ステップ 3 公開キーファイルを開き、そのファイルから公開キー情報をコピーします。末尾にusername @ hostname 情報は含めません。

（注）
秘密キーファイルは、インストールプロセスでは使用されません。ただし、SSH を介して Nexus ダッシュボード ノードにログインするなど、その他の理由で必要になる場合があります。

Windows での SSH キー ペアの生成

次の手順では、WindowsでSSH公開キーと秘密キーのペアを生成する方法について説明します。LinuxでSSH公開キーと秘密キーのペアを生成する手順については、を参照してください。Linux または MacOS での SSH キー ペアの生成 （174 ページ）

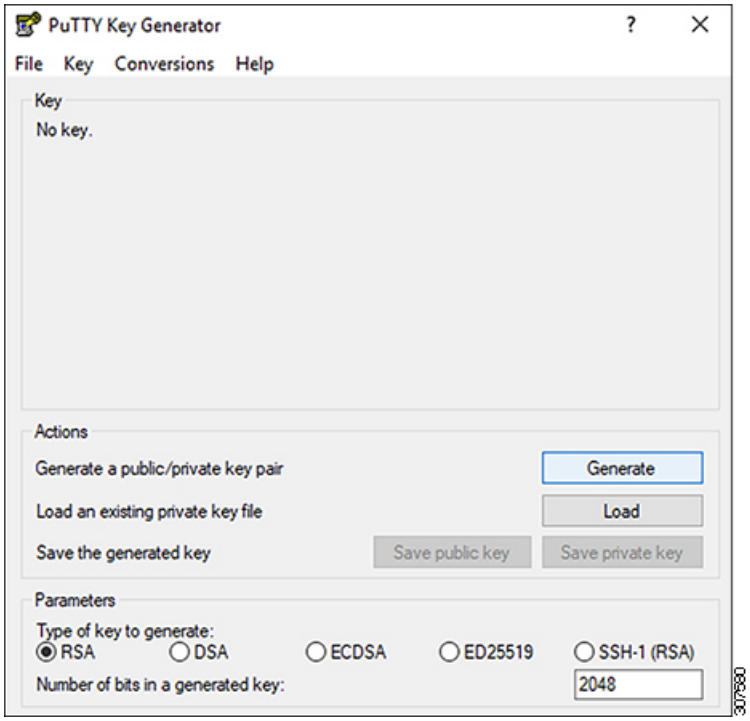
手順

ステップ 1 PuTTYキージェネレータ（puttygen）をダウンロードしてインストールします。

https://www.puttygen.com/download-putty

ステップ 2 **Windows** > **[スタート]** > **[すべてのプログラム]** > **[PuTTY]** > **[PuTTYgen]** に移動して、PuTTY キージェネレータを実行します。

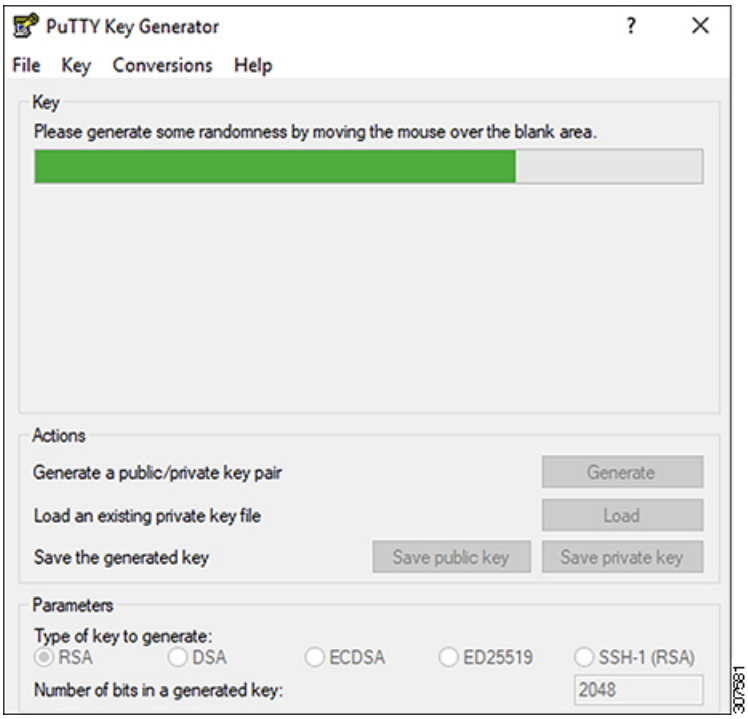
画面にPuTTYキージェネレータのウィンドウが表示されます。



ステップ 3 **[生成（Generate）]** をクリックします。

公開キーを生成するために空白領域にマウスを移動するように求める画面が表示されます。

ステップ 4 空白領域の周囲にカーソルを移動して、公開キーのランダムな文字を生成します。



ステップ 5 公開キーを保存します。

a) 公開キーファイルを保存するラップトップ上のフォルダに移動し、この公開キーのテキストファイルを作成します。

b) PuTTYキージェネレータの情報をコピーします。

次の内容を含めて、ウィンドウに公開キー情報をコピーします。

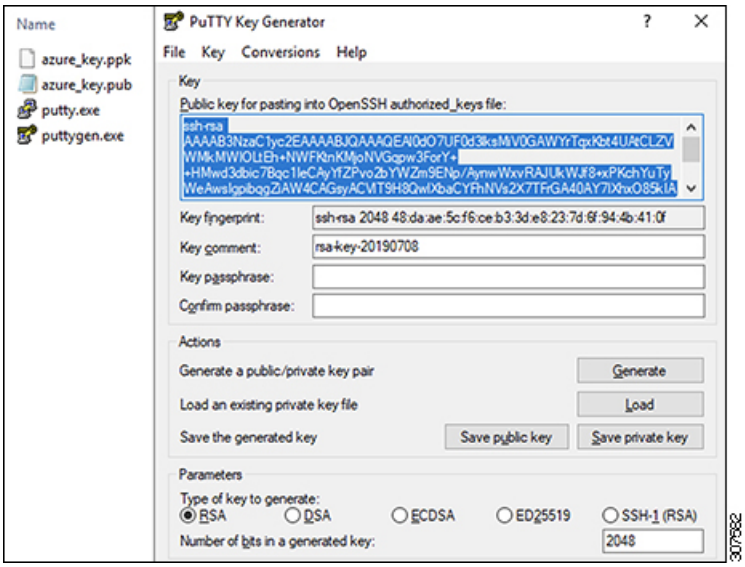
- 公開キーの先頭にssh-rsaテキストを含める。
- 末尾の次のテキスト文字列を除外します。

```
== rsa-key-<date-stamp>
```

== rsa-key-を含まないようにキーを切り捨てます。<date-stamp>末尾のテキスト文字列。

（注）
次の一連の手順では、公開キー情報をAzure ARMテンプレートに貼り付けます。フォームがこの形式のキーを受け入れない場合は、キーの末尾に==を追加します。一部の地域ではこの形式が必要になるためです。

キーが正しい形式でない場合、Nexus ダッシュボードはインストールを完了しません。



c) で作成した公開キーテキストファイルに情報を貼り付け、ファイルを保存して、一意のファイル名を付けます。5.a （177 ページ）

この公開キーテキストファイルには、1行のテキストのキーが含まれています。次の一連の手順では、この公開キーテキストファイルの情報が必要になります。

（注）
PuTTYキージェネレータの[公開キーの保存（Save public key）]オプションを使用して公開キーを保存しないでください。これにより、複数行のテキストを含む形式でキーが保存されます。これは、Nexus ダッシュボード展開プロセスと互換性がありません。

ステップ 6 秘密キーを保存します。

a) **[プライベート キーの保存（Save private key）]** をクリックします。

パスフレーズなしでファイルを保存するかどうかを確認する画面が表示されます。この画面で **[はい（Yes）]** をクリックします。

b) ラップトップのフォルダに移動し、一意のファイル名を付けて秘密キーファイルを保存します。

（注）
秘密キーファイルは、インストールプロセスでは使用されません。ただし、SSH を介して Nexus ダッシュボード ノードにログインするなど、その他の理由で必要になる場合があります。

Azure での Nexus ダッシュボードの展開

このセクションでは、Microsoft Azure 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

- 前提条件とガイドライン （173 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 Azure Marketplace で Cisco Nexus ダッシュボード製品に登録します。

a) Azure アカウントにログインし、https://azuremarketplace.microsoft.com に移動します

b) 検索フィールドに「`Cisco Nexus ダッシュボード`」と入力し、表示されるオプションを選択します。

[Nexus ダッシュボードの Azure Marketplace] ページにリダイレクトされます。

c) **[今すぐ取得（Get it now）]** をクリックします。

d) **[プランを選択（Select a plan）]** ドロップダウンで、バージョンを選択し、**[作成（Create）]** をクリックします。

ステップ 2 **基本**情報を提供します。

a) **[サブスクリプション（Subscription）]** ドロップダウンから、これに使用するサブスクリプションを選択します。

b) **[リソース グループ（Resource group）]** ドロップダウンから、このために作成したリソース グループを 前提条件とガイドライン （173 ページ） の一部として選択します。

c) **[リージョン（Region）]** ドロップダウンから、テンプレートを展開するリージョンを選択します。

d) **[パスワード (Password)]** および **[パスワードの確認 (Confirm Password)]** フィールドにノードの管理パスワードを入力します。

このパスワードは、Nexus ダッシュボードの`レスキュー ユーザ`ログインと、GUI の`管理者ユーザ`の初期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。

e) **[SSH 公共キー（SSH public key）]** フィールドに、前提条件とガイドライン （173 ページ） セクションの一部として生成したキーペアの公開キーを貼り付けます。

f) **[次へ (Next)]** をクリックして、次の画面に進みます。

ステップ 3 **ND 設定**情報を提供します。

a) **クラスタ名** を指定します。

b) **[イメージ バージョン（Image Version）]** ドロップダウンで、正しいバージョンが選択されていることを確認します。

c) **[仮想ネットワーク名（Virtual Network Name）]** フィールドに、クラスタ用に作成される VNET の名前を指定します。

VNET はまだ存在していてはならず、展開時に作成されます。既存の VNET を指定すると、展開を続行できません。

d) **[サブネット アドレス プレフィックス（Subnet Address Prefix）]** フィールドで、VNET 内のサブネットを指定します。

サブネットは /24 サブネットである必要があり、VNET の作成時に定義したデフォルトの VNET サブネットとは異なる必要があります。

e) **[外部サブネット（External Subnets）]** フィールドに、クラスタへのアクセスを許可する外部ネットワークを指定します。

たとえば、0.0.0.0/0 は、どこからでもクラスタにアクセスできます。

f) **[次へ (Next)]** をクリックして、次の画面に進みます。

ステップ 4 **[確認 + 作成（Review + create）]**ページで情報を確認し、**[作成（Create）]** をクリックします。

ステップ 5 展開が完了するのを待ってから、VM を起動します。

ステップ 6 すべてのノードのパブリック IP アドレスを書き留めます。

すべてのインスタンスが展開されたら、Azure コンソールに移動し、各 VM を選択して、すべてのノードのパブリック IP アドレスを書き留めます。次の手順で、この情報を GUI ブートストラップ ウィザードに提供します。

また、どちらが「最初の」ノードであるかに注意してください。これは、ノードの VM 名 vm-**node1**-*<cluster-name>*によって示されます。このノードのパブリック IP アドレスを使用して、クラスタ設定を完了します。

ステップ 7 すべてのノードでパスワードベースのログインを有効にします。

デフォルトでは、キーベースの SSH ログインのみが各ノードで有効になっています。パスワードを使用して SSH をノードに接続できるようにするには、GUI セットアップ ウィザードで要求されるように、パスワードベースのログインを明示的に有効にする必要があります。

（注）
次の手順で説明するクラスタブートストラップに進む前に、すべてのノードでパスワードベースのログインを有効にする必要があります。そうしないと、クラスタ設定を完了できません。

a) rescue-user としてノードの 1 つに SSH でログインします。

（注）
前提条件とガイドライン（173 ページ）セクションで展開用の公開キーを作成するために使用したのと同じマシンを使用する必要があります。

テンプレートの基本設定で指定したパスワードを使用して、**rescue-user** としてログインできます。

```
# ssh rescue-user@<node-public-ip>
```

b) パスワードベースのログインを有効にします。

```
# acs login-prompt enable
```

c) 他の 2 つのノードについて、この手順を繰り返します。

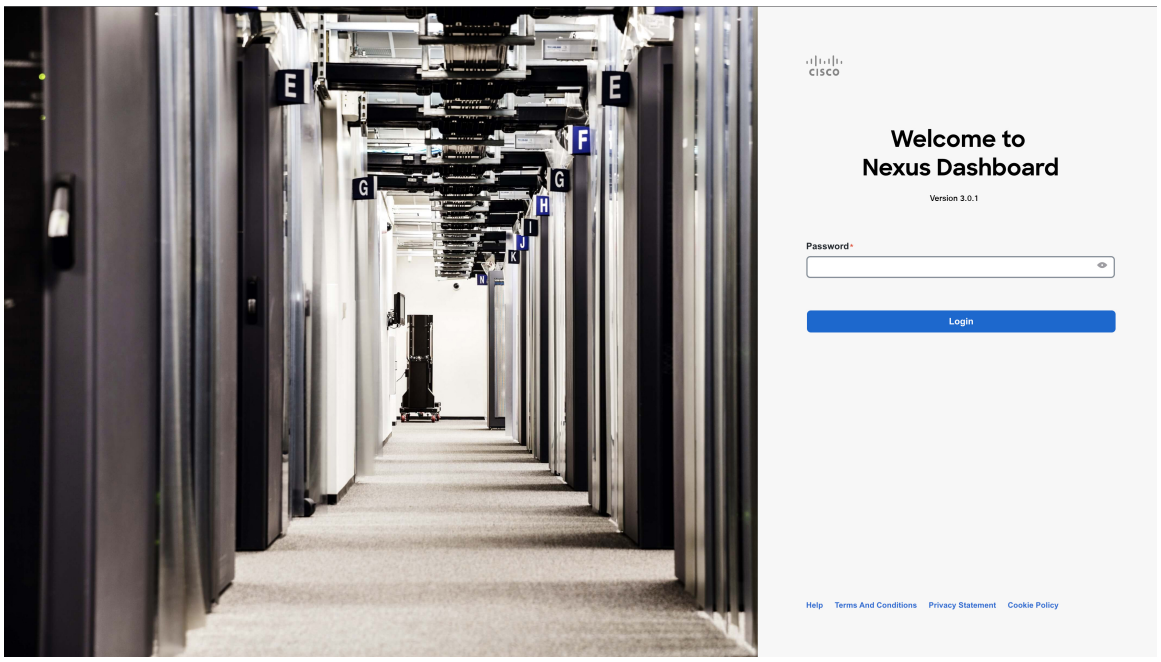
ステップ 8 ブラウザを開き、https://<first-node-public-ip> に移動して、GUI を開きます。

（注）

最初のノード（`vm-node1-<cluster-name>`）のパブリック IP アドレスを使用する必要があります。そうしないと、クラスタ設定を完了できません。

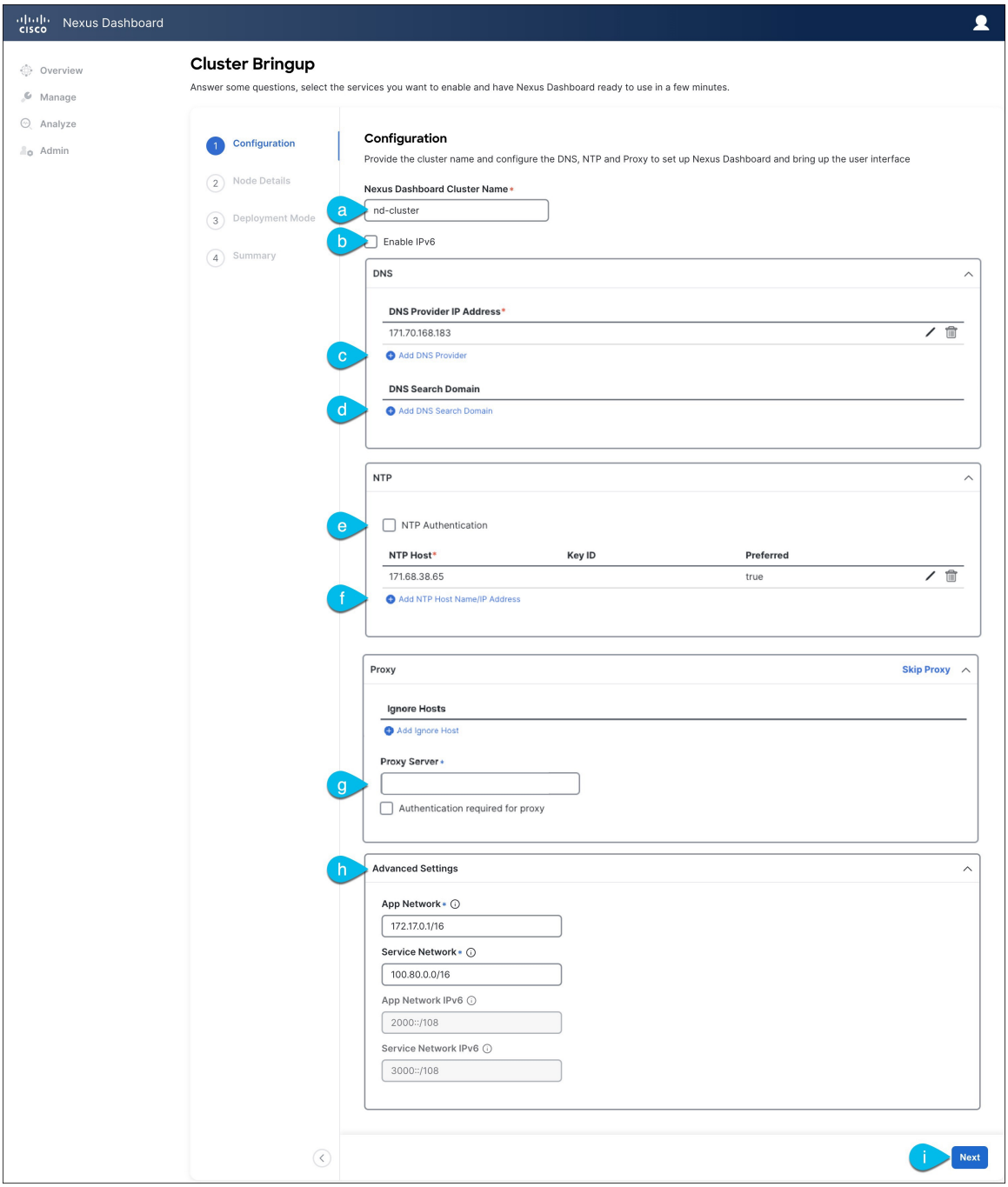
残りの設定ワークフローは、最初のノードの GUI から実行します。他の 2 つのノードに直接ログインまたは設定する必要はありません。

最初のノードに指定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 9 **[クラスタの詳細（Cluster Details）]** を入力します。

[クラスタ起動（Cluster Bringup）] ウィザードの **[クラスタの詳細（Cluster Details）]** 画面で、次の情報を入力します。



a) Nexus ダッシュボード クラスタの **[クラスタ名（Cluster Name）]** 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) （オプション）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。

c) **[+DNS プロバイダの追加（+Add DNS Provider）]** をクリックして、1 つ以上の DNS サーバを追加します。

情報を入力した後、チェックマーク アイコンをクリックして保存します。

d) （オプション）**[+DNS 検索ドメインの追加（+Add DNS Search Domain ）]** をクリックして、検索ドメインを追加します。

情報を入力した後、チェックマーク アイコンをクリックして保存します。

e) （オプション）NTP サーバー認証を有効にする場合には、**[NTP 認証（NTP Authentication）]** チェックボックスをオンにし、**[NTP キーの追加（Add NTP Key）]**をクリックします。

次のフィールドで、以下の情報を提供します。

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

（注）
情報を入力した後、チェックマーク アイコンをクリックして保存します。

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、前提条件とガイドライン （9 ページ） を参照してください。

f) **[+ NTP ホスト名/IP アドレスの追加（+Add NTP Host Name/IP Address）]** をクリックして、1 つ以上の NTP サーバを追加します。

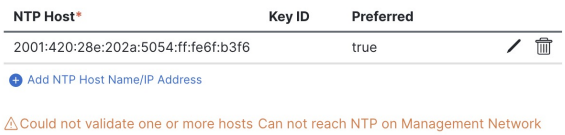
次のフィールドで、以下の情報を提供します。

- **NTP ホスト**：IP アドレスを指定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**：このサーバーの NTP 認証を有効にする場合は、前の手順で定義した NTP キーのキー ID を指定します。

  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 NTP サーバーを **[優先（Preferred）]** にするかどうかを選択します。

情報を入力した後、チェックマーク アイコンをクリックして保存します。

（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（次の手順で指定します）、NTP サーバーの IPv6 アドレスに接続できないためです。

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 サーバーを指定する場合は、**[+NTP ホストの追加（+Add NTP Host）]** を再度クリックし、このサブステップを繰り返します。

g) **[プロキシ サーバー（Proxy Server）]** を指定し、**[検証（Validate）]** をクリックします。

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。

[+無視するホストを追加（+Add Ignore Host）] をクリックして、プロキシをスキップする 1 つ以上の IP アドレス通信を提供することもできます。

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
```

プロキシ設定をスキップする場合は、**[プロキシをスキップ（Skip Proxy）]** をクリックします。

h) (オプション) プロキシ サーバで認証が必要な場合は、**[プロキシで認証が必要（Authentication required for Proxy）]** を **[はい（Yes）]** に変更し、ログイン資格情報を指定します。

i) (オプション) **[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。

- カスタム **App Network** と **Service Network** を提供します。

  アプリケーション オーバーレイ ネットワークは、Nexus ダッシュボードで実行されるアプリケーションのサービスで使用されるアドレス空間を定義します。このフィールドには、デフォルトの `172.17.0.1/16` 値が事前に入力されています。

  サービス ネットワークは、Nexus ダッシュボードとそのプロセスで使用される内部ネットワークです。このフィールドには、デフォルトの `100.80.0.0/16` 値が事前に入力されています。

  以前に **[IPv6 を有効にする（Enable IPv6）]** オプションをオンにした場合は、アプリケーション ネットワークとサービス ネットワークの IPv6 サブネットを定義することもできます。

  アプリケーションおよびサービスネットワークについては、このドキュメントの前の 前提条件とガイドライン （9 ページ） の項で説明します。

j) [**次へ（Next）**] をクリックして続行します。

ステップ 10 **[ノードの詳細（Node Details）]** 画面で、ノードの情報を入力します。

a) 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。

b) ノードの**名前**を入力します。

管理ネットワークと**データ ネットワーク**の情報は、クラスタを展開する前に構成したVNETサブネットから既に入力されています。

クラスタは、指定された VNET から 6 つのサブネットを作成し、そこからデータと管理ネットワークがクラスタの 3 つのノードに割り当てられます。

c) IPv6 アドレスと VLAN フィールドは空白のままにします。

Cloud Nexus ダッシュボード クラスタは、これらのオプションをサポートしていません。

d) **[Save]**をクリックして、変更内容を保存します。

ステップ 11 **[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。

[ノードの詳細（Node Details）] ウィンドウが開きます。

a) ノードの**名前**を入力します。

b) **[資格情報（Credentials）]** セクションで、ノードの**パブリック IP アドレス**とテンプレートの展開時に指定したパスワードを入力し、**[検証（Verify）]** をクリックします。

IP アドレスとパスワードは、そのノードの**管理ネットワーク**と**データ ネットワーク**情報を取得するために使用され、下のフィールドに入力されます。

c) **[保存 (Save)]**をクリックして、変更内容を保存します。

ステップ 12 前の手順を繰り返して、3番目のノードを追加します。

ステップ 13 **[ノードの詳細（Node Details）]** ページで、**[次へ（Next）]** をクリックして続行します。

ステップ 14 クラスタの**展開モード**を選択します。

a) 有効にするサービスを選択します。

リリース3.1(1)より前では、クラスタの初期展開が完了した後に、個々のサービスをダウンロードしてインストールする必要がありました。今では、初期インストール時にサービスを有効にするように選択できます。

（注）
クラスタ内のノードの数によっては、一部のサービスまたは共同ホスティングのシナリオがサポートされない場合があります。必要な数のサービスを選択できない場合は、**[戻る（Back）]** をクリックし、前の手順で十分な数のセカンダリ ノードを指定したことを確認します。

b) **[永続サービスIP/プールの追加（Add Persistent Service IPs/Pools）]** をクリックして、Insights または ファブリック コントローラ サービスに必要な 1 つ以上の永続 IP を指定します。

永続的 IP の詳細については、ユーザー ガイドの前提条件とガイドライン （9 ページ）のセクションを参照してください。

c) [次へ（Next）] をクリックして続行します。

ステップ 15 **[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。

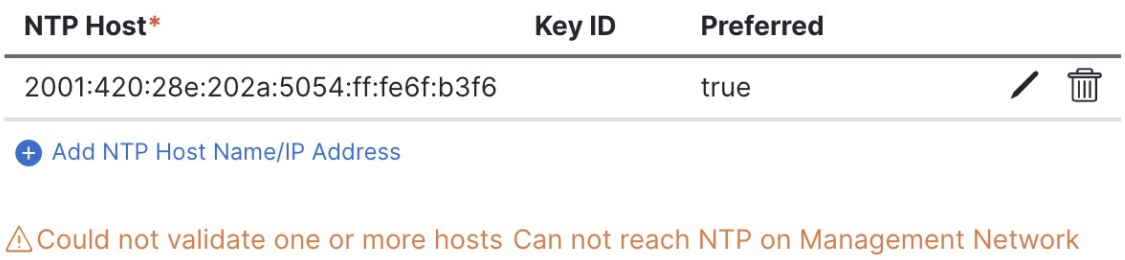
ノードのブート ストラップとクラスタの起動中に、全体的な進捗状況と各ノードの個々の進捗状況がUIに表示されます。ブートストラップの進行状況が表示されない場合は、ブラウザでページを手動で更新し、ステータスを更新してください。

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。

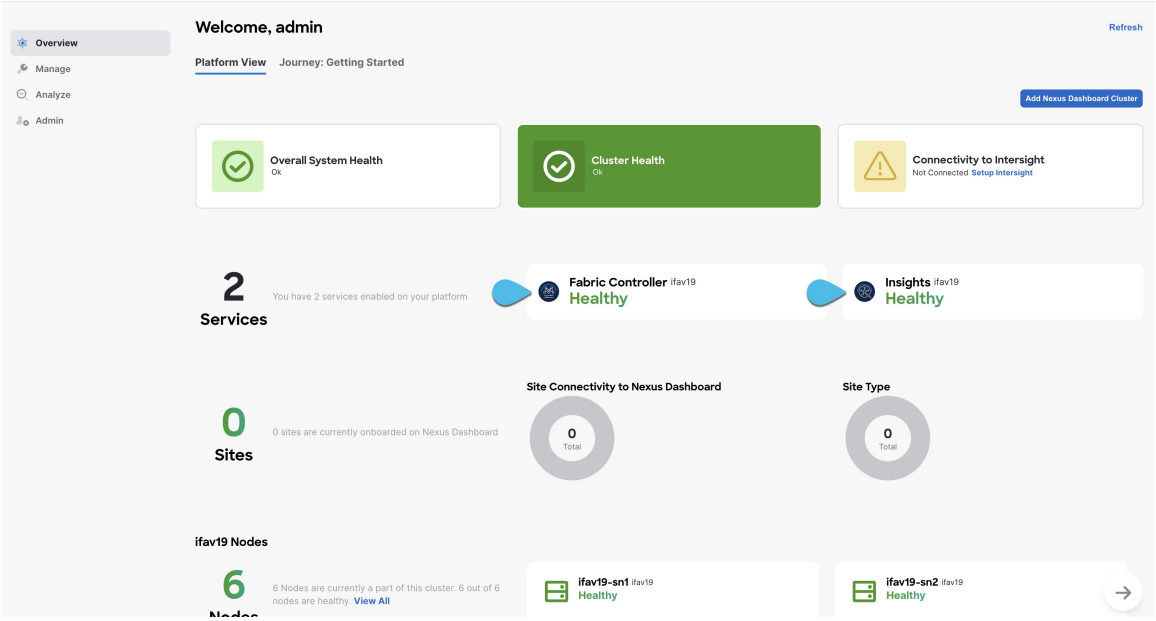
ステップ 16 クラスタが健全であることを検証します。

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、**[概要（Overview）]** ページ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、ノード展開中に指定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。

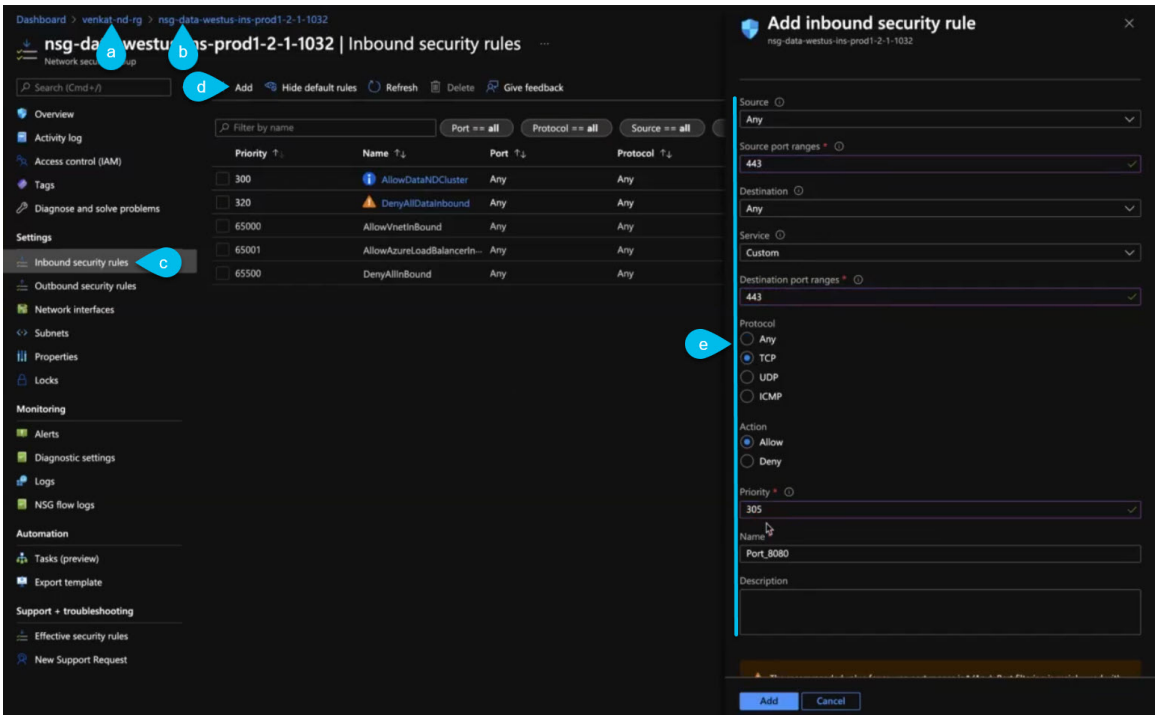
```
deploy base system services
```

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 17 必要なポートでノードのセキュリティ グループを更新します。

この手順では、Cisco NDFC サイトのオンボーディングに必要なポート設定で Nexus ダッシュボード ノードのインスタンスを更新する方法について説明します。Nexus ダッシュボード クラスタへの NDFC サイトのオンボーディングを計画していない場合は、この手順をスキップできます。



a) Azure ポータルで、Nexus ダッシュボードを展開したリソース グループに移動します。

これは、手順 2 で選択したのと同じリソース グループです。

b) ノードのデータ インターフェイスにアタッチされているセキュリティ グループを選択します。

セキュリティ グループの名前は `nsg-data-<region>-...` で始まります。。

c) セキュリティ グループの設定ナビゲーション バーで、**[受信セキュリティ ルール（Inbound security rules）]** を選択します。

d) **[+ 追加（+Add）]** をクリックして新しいインバウンド セキュリティ ルールを追加し、ポート 443 でのインバウンド通信を許可する詳細を指定します。

新しいルールについて、次の情報を提供します。

- **[送信元（Source）]** で、[任意（Any）] を選択します。
- **[送信元ポート範囲（Source port ranges）]** には、443 と入力します。
- **[宛先（Destination）]** で、[任意（Any）] を選択します。
- **[宛先ポート範囲（Destination port ranges）]** に、443 と入力します。
- **[プロトコル（Protocol）]** には、[TCP] を選択します。
- **[アクション（Action）]** で、[許可（Allow）] を選択します。
- **[優先度（Priority）]** で、300 ～ 320 の優先度を選択します。

  たとえば、305 です。
- ルールの**名前**を指定します。

e) **[+ 追加（+Add）]** をクリックして新しいインバウンド セキュリティ ルールを追加し、ポート 9092 でのインバウンド通信を許可する詳細を指定します。

前のサブステップを繰り返して、次の詳細を含む別のルールを追加します。

- **[送信元（Source）]** で、[任意（Any）] を選択します。
- **[送信元ポート範囲（Source port ranges）]** には、9092 と入力します。
- **[宛先（Destination）]** で、[任意（Any）] を選択します。
- **[宛先ポート範囲（Destination port ranges）]** に、9092 と入力します。
- **[プロトコル（Protocol）]** には、[TCP] を選択します。
- **[アクション（Action）]** で、[許可（Allow）] を選択します。
- **[優先度（Priority）]** で、300 〜 320 の優先度を選択します。

  例えば、310。
- ルールの**名前**を指定します。

第 12 章

ファブリックのオンボーディング

- ACI ファブリックのオンボーディング （191 ページ）
- NDFC ファブリックのオンボーディング （193 ページ）
- NX-OS スイッチのオンボーディング （194 ページ）

ACI ファブリックのオンボーディング

このセクションでは、1 つ以上の ACI ファブリックを Nexus Dashboard にオンボードする方法について説明します。

始める前に

- 同じクラスタ内では、1つのタイプのサイト（ACI、NDFC、またはスタンドアロンNX-OS）のみをオンボードできます。

  同じクラスタ内での ACI と NDFC、ACI と NX-OS、または NDFC と NX-OS の混在オンボーディングはサポートされていません。

- ファブリック接続 （19 ページ）で説明しているように、ファブリック接続がすでに設定されている必要があります。
- ファブリック接続 （19 ページ）で説明されているように、Nexus Dashboard データ ネットワーク IP 接続の EPG/L3Out は、すでに設定されている必要があります。
- Nexus Dashboard から。データネットワークを介した Cisco APIC インバンド IP への IP 接続がすでに設定されている必要があります。
- Nexus Dashboard から、データネットワークを介したリーフ ノードおよびスパイン ノードのインバンド IP への IP 接続がすでに設定されている必要があります。

手順

ステップ 1 **[管理（Manage）] > [サイト（Sites）]**に移動します。

ステップ 2 [サイトの追加（Add Site）] をクリックします。

これにより、サイトのオンボーディング ワークフローが開始します。

ステップ 3 **[サイトの追加（Add Site）]** 画面で、**[コントローラベースのサイト（Controller Based Site）]** を選択します。

Insights サービスがインストールされていない場合、この選択は表示されず、サイトのオンボーディングはデフォルトでこのオプションになります。

ステップ 4 サイト情報を入力します。

- **[ホスト名/IP アドレス（Host Name/IP Address）]**： Cisco APIC との通信に使用する IP アドレスを入力します。

  （注）
  アドレスを指定する場合、URL 文字列の一部としてプロトコル（`http://` または `https://`）を含めないでください。追加すると、サイトのオンボーディングに失敗します。

- **[ユーザー名（User Name）]** と **[パスワード（Password）]**：追加するサイトで管理者権限を持つユーザーのログイン情報。
- （オプション）**[ログイン ドメイン（Login Domain）]**：このフィールドを空白にすると、サイトのローカル ログインが使用されます。
- （オプション）**[ピア証明書を検証（Validate Peer Certificate）]**：Nexus Dashboard が、接続先ホスト（例えばサイト コントローラ）の証明書が有効であることと、信頼されている認証局（CA）に署名されていることを検証できるようにします。

  （注）
  このオプションを使用してサイトを追加する前に Nexus ダッシュボードに証明書が既にインポートされていることが必要です。証明書をまだ追加していなければ、オンボーディング ワークフローをキャンセルし、まず Nexus Dashboard ドキュメント ライブラリの「管理者のタスク」の記事に記されている手順に従います。証明書をインポートしたら、ここに説明されている方法でサイトを追加します。有効な証明書をインポートせずに [ピア証明書を検証（Validate Peer Certificate）] オプションを有効にすると、サイトのオンボードは失敗します。

- （オプション）このサイトのコントローラへの接続にプロキシが必要な場合は、**[プロキシの使用（Use Proxy）]** オプションを有効にします。

  プロキシは、Nexus Dashboard の **管理コンソール**ですでに設定されている必要があります。

ステップ 5 追加のサイトの **[詳細（Details）]**を入力します。

- **[名前（Name）]**：サイトの説明となる名前。
- **[場所（Location）]**：サイトの地理的な場所。このオプションは、オンプレミス サイトでのみ使用できます。

ステップ 6 **[概要（Summary）]** ページで情報を確認し、**[保存（Save）]** をクリックしてサイトの追加を完了します。

NDFC ファブリックのオンボーディング

このセクションでは、1 つ以上の NDFC ファブリックを Nexus Dashboard にオンボードする方法について説明します。

（注） クラスタを展開したら、**[ファブリック コントローラ（Fabric Controller）]** > **[システム設定（System Settings）]** > **[機能管理（Feature Management）]**に移動し、サポートされているモードのいずれかを選択して、NDFC 展開ペルソナを設定します。

NDFC サービスでファブリックを作成すると、Nexus Dashboard にサイトとして自動的に追加されます。次の手順は、各サービスが個別のクラスタに展開されているファブリックコントローラと Insights コロケーションのユース ケースで、異なる Nexus Dashboard クラスタからサイトをオンボーディングする場合にのみ必要です。

始める前に

- 同じクラスタ内では、1つのタイプのサイト（ACI、NDFC、またはスタンドアロンNX-OS）のみをオンボードできます。

  同じクラスタ内での ACI と NDFC、ACI と NX-OS、または NDFC と NX-OS の混在オンボーディングはサポートされていません。

- ファブリック接続 （19 ページ）で説明しているように、ファブリック接続がすでに設定されている必要があります。
- ファブリックとスイッチへのレイヤ 3 接続がすでに設定されている必要があります。
- クラスタが AWS または Azure に展開されている場合は、データ インターフェイスでインバウンド ルールを設定する必要があります。

手順

ステップ 1 **[管理（Manage）]** > **[サイト（Sites）]**に移動します。

ステップ 2 [サイトの追加（Add Site）] をクリックします。

これにより、サイトのオンボーディング ワークフローが開始します。

ステップ 3 **[サイトの追加（Add Site）]** 画面で、**[コントローラベースのサイト（Controller Based Site）]** を選択します。

ステップ 4 サイト情報を入力します。

- **[ホスト名/IP アドレス（Host Name/IP Address）]**： Cisco NDFC との通信に使用する IP アドレスを入力します。

（注）
NDFC サイトの場合、これは NDFC のインバンド IP アドレスである必要があります。

アドレスを指定する場合、URL 文字列の一部としてプロトコル（`http://` または `https://`）を含めないでください。追加すると、サイトのオンボーディングに失敗します。

- **[ユーザー名（User Name）]** と **[パスワード（Password）]**：追加するサイトで管理者権限を持つユーザーのログイン情報。
- （オプション）**[ログインドメイン（Login Domain）]**：このフィールドを空白にすると、サイトのローカル ログインが使用されます。
- （オプション）**[ピア証明書を検証（Validate Peer Certificate）]**：Nexus Dashboard が、接続先ホスト（例えばサイトコントローラ）の証明書が有効であることと、信頼されている認証局（CA）に署名されていることを検証できるようにします。

  （注）
  このオプションを使用してサイトを追加する前に Nexus ダッシュボードに証明書が既にインポートされていることが必要です。証明書をまだ追加していなければ、オンボーディング ワークフローをキャンセルし、まず Nexus Dashboard ドキュメント ライブラリの「管理者」の記事に記されている手順に従います。証明書をインポートしたら、ここに説明されている方法でサイトを追加します。有効な証明書をインポートせずに [ピア証明書を検証（Validate Peer Certificate）] オプションを有効にすると、サイトのオンボードは失敗します。

ステップ 5 追加のサイトの **[詳細（Details）]**を入力します。

- **[名前（Name）]**：サイトの説明となる名前。
- **[場所（Location）]**：サイトの地理的な場所。このオプションは、オンプレミス サイトでのみ使用できます。

ステップ 6 **[概要（Summary）]** ページで情報を確認し、**[保存（Save）]** をクリックしてサイトの追加を完了します。

NX-OS スイッチのオンボーディング

ここでは、1 つ以上のスタンドアロン NX-OS スイッチを Nexus ダッシュボードにオンボードする方法について説明します。

（注） コントローラ（APICやNDFCなど）を使用せずにスタンドアロンNX-OSスイッチをオンボーディングする場合、次の制限が適用されます。

- 同じクラスタ内では、1つのタイプのサイト（ACI、NDFC、またはスタンドアロンNX-OS）のみをオンボードできます。

  同じクラスタ内での ACI と NDFC、ACI と NX-OS、または NDFC と NX-OS の混在オンボーディングはサポートされていません。

- Nexus Dashboard Insights サービスのみがスタンドアロン NX-OS スイッチをサポートします。

- NX-OS スイッチのオンボーディングをサポートするのは、物理 Nexus Dashboard クラスタのみです。

- スタンドアロン NX-OS スイッチをオンボードするのと同じ Nexus ダッシュボード クラスタに NDFC サービスをインストールしないでください。

- スタンドアロン NX-OS スイッチをオンボーディングする前に、以下のステップ 3 で説明するように、クラスタで「NX-OS スイッチディスカバリ」を有効にする必要があります。

  NX-OS スイッチ検出の有効化は、管理者ユーザーが行う必要があります。

- また、データネットワークに 10 個の永続 IP（IPv4 を使用している場合）および 8 個の IP（IPv6 を使用している場合）を設定する必要があります。

  永続IPは、 **[Nexusダッシュボード（Nexus Dashboard）]** > **[管理コンソール（Admin Console）]** > **[システム設定（System Settings）]** > **[外部サービスプール（External Service Pools）]** > **[データサービス IP（ Data Service IPs）]** ページで設定できます。

- すべての NX-OS スイッチで NX-OS スイッチの自動検出のための Cisco Discovery Protocol（CDP）を有効にする必要があります。

- NX-OS スイッチの自動検出はスイッチの管理インターフェイスを使用するため、Nexus Dashboard を NX-OS スイッチの管理ネットワークへ到達できるように設定する必要があります。

  Nexus Dashboard のデータ ネットワークを NX-OS スイッチのインバンド ネットワークへ到達できるように設定する必要があります。

手順

ステップ 1 **[管理（Manage）]** > **[サイト（Sites）]**に移動します。

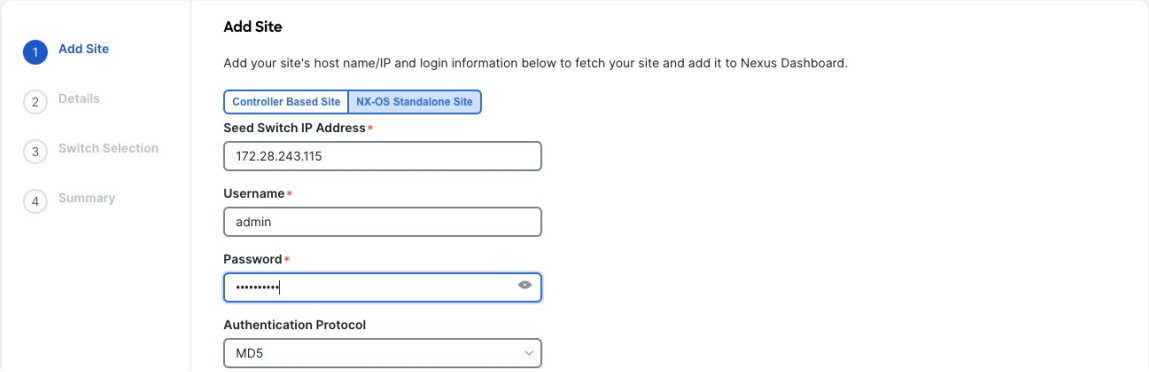
ステップ 2 [サイトの追加（Add Site）] をクリックします。

これにより、サイトのオンボーディング ワークフローが開始します。

ステップ 3 **[サイトの追加（Add Site）]** 画面で、**[NX-OS スタンドアロン サイト（NX-OS Standalone Site）]** を選択します。

（注）
コントローラなしでNX-OSスイッチを初めてオンボーディングする場合は、**[NX-OS 検出の有効化（Enable NX-OS Discovery）]** をクリックします。

ステップ 4 サイト情報を入力します。



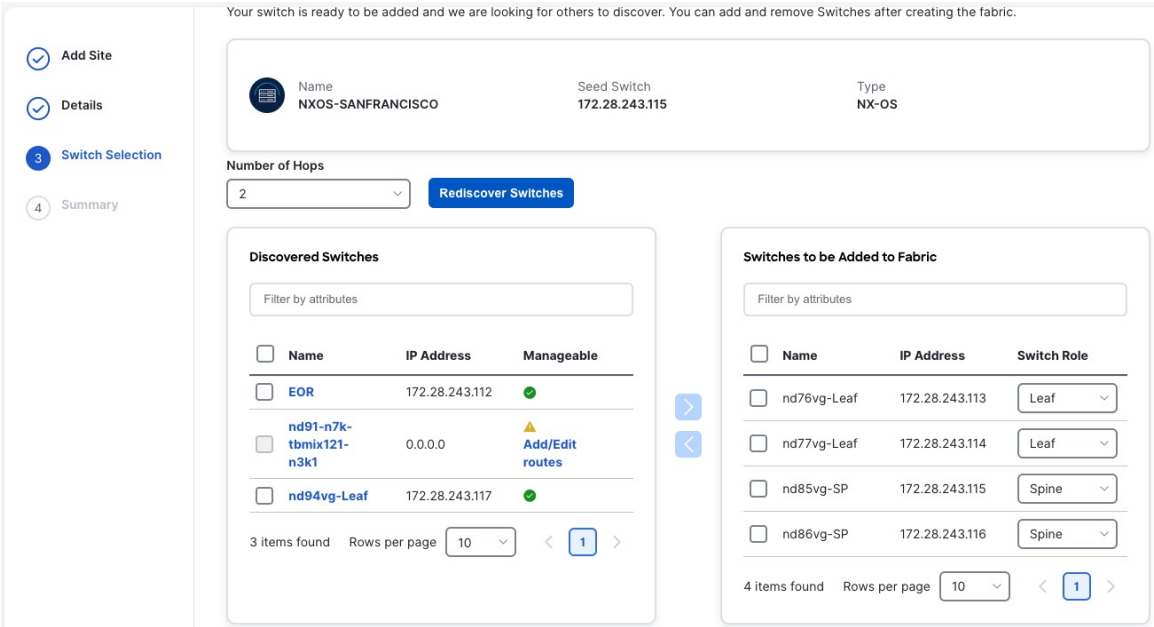
- **[シード スイッチ IP アドレス（Seed Switch IP Address）]**：サイト内の他のスイッチを検出するために使用されるシード スイッチの IP アドレスを指定します。
- **[ユーザー名（Username）]** と **[パスワード（Password）]**：シード スイッチのログイン クレデンシャル。

ステップ 5 追加のサイトの **[詳細（Details）]**を入力します。

- **[名前（Name）]**：サイトの説明となる名前。
- **[場所（Location）]**：サイトの地理的な場所。このオプションは、オンプレミス サイトでのみ使用できます。

ステップ 6 **[スイッチの選択（Switch Selection）]** ページで、サイトに追加する 1 台以上のスイッチを選択します。

スイッチ検出プロセスのデフォルトでは、シード スイッチから 2 ホップ離れたスイッチが表示されます。デフォルトの設定は、**[ホップ数（Number of Hops）]** ドロップダウンを使用し、**[スイッチの再検出（Rediscover Switches）]** をクリックして変更できます。



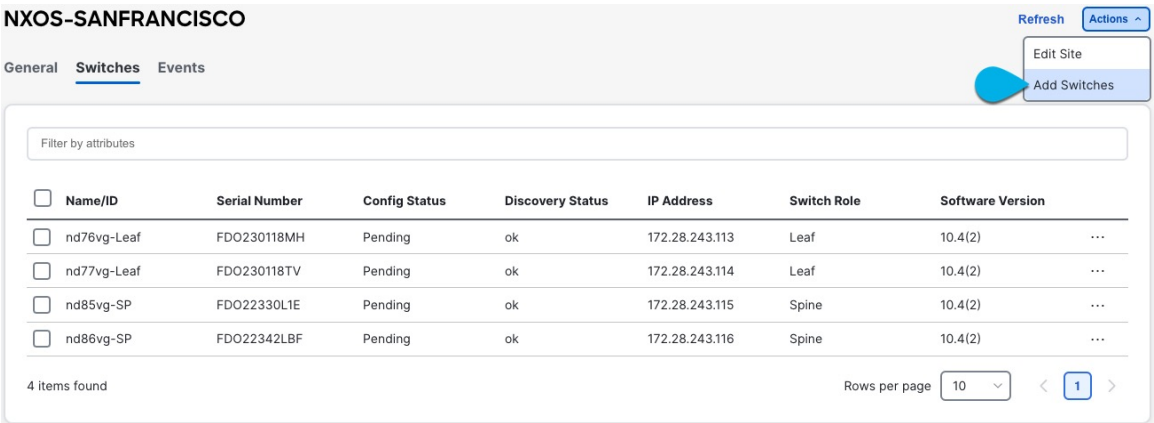
スイッチが検出されたら、左側のリストでサイトに追加するすべてのスイッチを選択し、右矢印をクリックして右側のリストに移動します。

スイッチはデフォルトの リーフ ロールで追加されますが、必要に応じて他のロールに変更できます。**[次へ（Next ）]** をクリックして続行します。

ステップ 7 **[概要（Summary）]** ページで情報を確認し、**[保存（Save）]** をクリックしてサイトの追加を完了します。

ステップ 8 （オプション）既存のスタンドアロン NX-OS サイトにスイッチを追加します。

まずサイトを追加した後に、GUI でサイトを選択して **[スイッチを追加（Add Switches）]** を選択します。



第 III 部

このリリースへのアップグレードまたは移行

- 既存の ND クラスタをこのリリースへアップグレード （201 ページ）
- DCNM から NDFC への移行 （215 ページ）

第 13 章

既存の ND クラスタをこのリリースへアップグレード

- 前提条件とガイドライン （201 ページ）
- サポート対象のアップグレード パス （204 ページ）
- Nexus ダッシュボードのアップグレード （208 ページ）
- アップグレードのトラブルシューティング （212 ページ）

前提条件とガイドライン

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。
- このリリースにアップグレードすると、クラスタで有効になっているサービスの数を変更できなくなることに注意してください。

  リリース3.1.1以降、各クラスタには、有効なサービスの組み合わせを定義する「展開モード」があり、サービスの組み合わせをクラスタの展開またはアップグレード後に変更することはできません。つまり、このリリースにアップグレードした後、クラスタを再展開せずにサービスの追加や削除を行うことはできません。クラスタ内のサービスを追加または削除する予定の場合は、本リリースにアップグレードする前に行うことをお勧めします。

（注） 場合によっては、本リリースでサポートされている展開モードが、以前のリリースではサポートされていなかった場合があります（たとえば、Insights と Orchestrator の共存は、リリース 3.0.1 の仮想クラスタではサポートされていません）。このような場合、現在のクラスタに単一のサービス（Insights など）が展開されていて、アップグレード後に別のサービス（Orchestrator など）を追加するには、次の手順を実行します。

1. 現在のクラスタ内の既存の Insights サービスを無効にします。
2. 現在のクラスタに追加の Orchestrator サービスをインストールします。
3. 現在のクラスタで Orchestrator サービスを有効にします。

   この時点で、Insights と Orchestrator の両方が現在のクラスタにあって、Insights は無効になり、Orchestrator は有効になります。現在のリリースでサポートされている設定でない場合は、両方のサービスを同時に有効にしないでください。
4. Orchestrator サービスを無効にして、アップグレードを続行します。

- 4 ノードまたは 5 ノードの物理クラスタで Nexus Dashboard Insights サービスを実行している場合は、通常どおりにクラスタとサービスをこのリリースにアップグレードし、4 ノードまたは 5 ノードクラスタを引き続き使用できます。

  Nexus Dashboard Insights を搭載したNexus Dashboard の本リリースで、グリーンフィールド展開を行う場合は、3 ノードおよび 6 ノードのプロファイルのみがサポートされます。ただし、現在のスケールを変更せずに、既存の 4 ノードまたは 5 ノードクラスタを以前のリリースからアップグレードする場合は、本リリースで引き続き使用できます。

- 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。

- Linux KVM 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、**Virtual Machine Manager** の UI で [ホスト CPU 設定のコピー（Copy host CPU configuration）] オプションを有効にする必要があります。

  このリリースは、次のカーネルおよび KVM バージョンを搭載した CentOS 7.9 または Red Hat Enterprise Linux 8.6 をサポートします。

- CentOS 7.9 の場合、Kernel バージョン `3.10.0-957.el7.x86_64` および KVM バージョン `libvirt-4.5.0-23.el7_7.1.x86_64`
- RHEL 8.6 の場合、Kernel バージョン `4.18.0-372.9.1.el8.x86_64` および KVM バージョン `libvert 8.0.0`

- 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 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。

- Nexus Dashboard リリース 3.0(1) またはそれ以降を実行して、リリース 3.2(1) に直接アップグレードする必要があります。

  それより前のバージョンの Nexus Dashboard を実行している場合は、それぞれの展開ガイドの説明に従って、最初にリリース 3.0(1) または 3.1(1) にアップグレードする必要があります。

- 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。

- リリース 3.0(1) からアップグレードする場合、このリリースにアップグレードする前に、クラスタで実行されているすべてのサービスを無効にする必要があります。

  リリース 3.1(1) からアップグレードする場合は、サービスを無効化にする必要はありません。

リリース3.1(1)の統合インストールイメージにより、既存のすべてのサービスのため、構成を保持しながら、この Nexus Dashboard リリースと互換性のあるバージョンに自動的にアップグレードされることに注意してください。また、アップグレードが完了すると、サービスは自動的に再度有効になります。

- アップグレードを続行する前に、データを保護し、潜在的なリスクを最小限に抑えるために、アップグレードの前にNexusダッシュボードとサービスの構成バックアップを実行する必要があります。
- アップグレードの進行中には、セカンダリまたはスタンバイノードを追加するなど、構成変更がクラスタに対して行われていないことを確認します。
- 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してサービスを再インストールする必要があります。

サポート対象のアップグレード パス

Nexus Dashboard リリース3.1(1) より前では、プラットフォーム ソフトウェアと個々のサービスは、サポートされている特定のバージョンの組み合わせの範囲内で、相互に独立してアップグレードできました。そのため、以前のリリースのドキュメントには、各アップグレード段階ですべてのコンポーネント間の互換性を確保するために、複数のリリースにわたる特定のアップグレード パスが記載されていました。

この要件は、Nexus Dashboard と個々のサービス間のより緊密な結合により、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があるため、削除されました。その結果、現在 Nexus Dashboard ソフトウェアの必要最小限のバージョン（前提条件とガイドライン（201 ページ）に記載）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このリリースに直接アップグレードできます。

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 *22*：

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
3.0(1)	ファブリック コントローラ：12.1(3) Orchestrator：4.2(x) Insights：6.3(1)	次のセクションの説明に従って、リリース 3.1.1 に直接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。
2.3(2d)	ファブリック コントローラ：12.1(2) Orchestrator：4.1(x) Insights:：6.2(x)	**1.** Orchestrator リリース4.1(1) 以前を実行している場合は、最初に Orchestrator サービスをリリース4.1(2) にアップグレードします。 Orchestrator サービスを有効にしていない場合は、この手順をスキップします。 （注）Orchestrator サービスが有効になっているNexus Dashboardリリース2.3.2dからアップグレードする場合、 Nexus Dashboard 3.1(1) に直接アップグレードするには、Orchestrator サービスがバージョン 4.1(2) 以降である必要があります。 **2.** リリース 2.3(2d) からリリース 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。

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(2b)	ファブリック コントローラ：12.1(2) Orchestrator：4.1(x) Insights:：6.2(x)	**1.** 『*Nexus Dashboard 展開ガイド、リリース 2.3.x*』の説明に従って、 Nexus Dashboard プラットフォーム**のみ**をリリース 2.3(2d) にアップグレードします。 **2.** Orchestrator リリース4.1(1) 以前を実行している場合は、最初に Orchestrator サービスをリリース4.1(2) にアップグレードします。 Orchestrator サービスを有効にしていない場合は、この手順をスキップします。 （注）Orchestrator サービスが有効になっているNexus Dashboardリリース2.3.2dからアップグレードする場合、 Nexus Dashboard 3.1(1) に直接アップグレードするには、Orchestrator サービスがバージョン 4.1(2) 以降である必要があります。 **3.** リリース2.3(2d) からリリース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。

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(2b) より前のリリース	ファブリック コントローラ：12.1(1) 以前 Orchestrator：4.0(2) 以前 インサイト：6.1(3) 以前	**1.** 『*Nexus Dashboard 展開ガイド、リリース 2.3.x*』の説明に従って、 Nexus Dashboard プラットフォームをリリース 2.3(2d) にアップグレードします。 **2.** サービス固有のドキュメントに記載されているアップグレード パスまたは最小バージョン要件を使用して、以前に行ったように、個々のサービスを Nexus Dashboard リリース2.3(2d) と互換性のあるバージョンにアップグレードします。 • ファブリック コントローラ • オーケストレータ • [Insights]https://www.cisco.com/c/en/us/support/data-center-analytics/nexus-insights/products-installation-guides-list.html **3.** リリース 2.3(2d) からリリース 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。

Nexus ダッシュボードのアップグレード

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。

（注） 次の手順は、Nexus Dashboard リリース 3.0(1) からのアップグレード ワークフローを示しています。リリース 2.3(x) からアップグレードする場合、UI は若干異なる場合がありますが、アップグレードのワークフローと機能は同じです。

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。前提条件とガイドライン （201 ページ）

手順

ステップ 1 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) 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。

c) ターゲットとするリリース用の 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。

d) イメージを自分の環境内の Web サーバーでホストします。

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 クラスタにインストールされている既存のサービスを無効にします。

（注）

クラスタのアップグレードをする前にすべてのサービスを無効化する必要があります。サービスを無効にしても、サービスを削除しないでください。無効化されたサービスは、アップグレードプロセスが完了すると自動的に再アクティブ化されます。

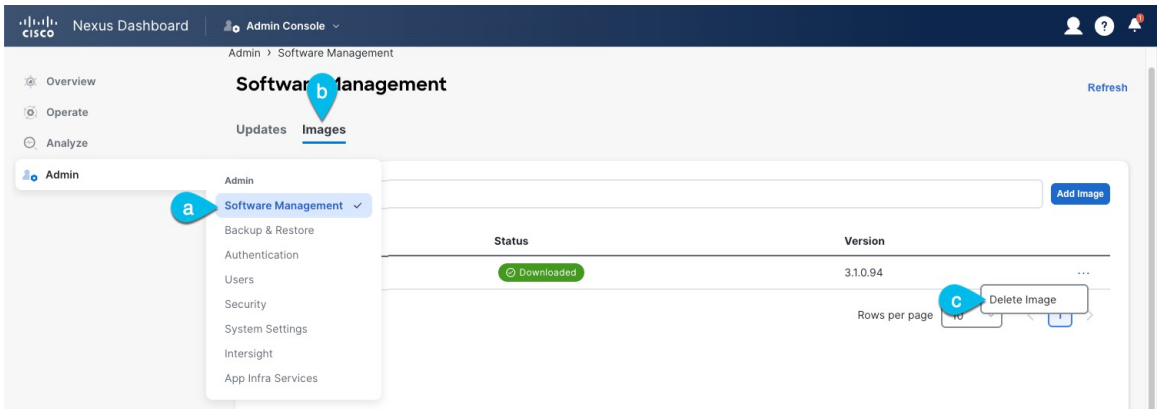
a) メイン ナビゲーション メニューから、**[サービス（Services）]**（リリース 2.3.2）または **[操作（Operate）]** > **[サービス（Services）]**（リリース 3.0.1 以降）を選択します。
b) サービスのタイルで、アクション（**...**）メニューをクリックし、**[無効化（Disable）]** を選択します。
c) クラスタに展開されているすべてのサービスについて、この手順を繰り返します。

ステップ 4 クラスタから既存の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。

以前にクラスタを現在のバージョンにアップグレードしたことがある場合は、以前のアップグレードイメージをすべて削除する必要があります。

（注）
リリース 2.3.2 では、このページは代わりに **[操作（Operations）]** > **[ファームウェア管理（Firmware Management）]** の下にあります。



a) **[管理（Admin）]** > **[ソフトウェア管理（Software Management）]** に移動します。
b) **[イメージ]** タブを選択します。
c) 既存のアップグレードイメージの横にあるアクション メニュー（**...**）から、**[イメージの削除（Delete Image）]** を選択します。
d) すべての既存の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 5 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（Admin ）]** > **[ソフトウェアの管理（Software Management）]**ページの **[イメージ（Images）]** タブで、**[イメージの追加（Add Image）]** をクリックします。
b) **[ソフトウェアイメージの追加（Add Software Image）]** ウィンドウで、イメージがマシン上で **[ローカル（Local）]** であるか、Web サーバー上の **[リモート（Remote）]** であるかを選択します。
c) **[ファイルの選択（Choose file）]** をクリックするか、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。
d) **[アップロード（Upload）]** をクリックして、イメージを追加します。
e) イメージ ステータスが「ダウンロード済み」に変わるのを待ちます。

イメージが Nexus ダッシュボード クラスタにアップロードされ、解凍されて処理され、アップグレードに使用できるようになります。プロセス全体に数分かかる場合があり、**[イメージ（Images）]** タブでプロセスのステータスを確認できます。

ステップ 6 アップグレードをセットアップします。

a) **[管理（Admin）]** > **[ソフトウェア管理（Software Management）]** に移動します。

（注）
リリース 2.3.2 では、このページは代わりに **[操作（Operations）]** > **[ファームウェア管理（Firmware Management）]** の下にあります。

b) **[更新]** タブを選択します。

c) **[更新の設定（Set Up Update）]** をクリックします。

（注）
以前にクラスタをアップグレードしたことがある場合、ページには代わりに以前のアップグレードの詳細が表示されます。その場合は、ページの右上にある **[詳細の変更（Modify Details）]** ボタンをクリックして、新しいアップグレード情報を提供します。

[ファームウェアの更新（Update Firmware）] ダイアログボックスが開きます。

d) **[セットアップ（Setup）]** > **[バージョン選択（Version selection）]** 画面で、アップロードしたファームウェア バージョンを選択し、**[次へ（Next）]** をクリックします。

e) **[セットアップ（Setup）]** > **[確認（Confirmation）]** 画面で、詳細を確認し、**[検証（Validate）]** をクリックします。

セットアップは、アップグレードを確実に成功させるために、いくつかの準備段階と検証段階を経ます。終了するまでに数分かかる場合があります。

f) 検証が完了したら、**[インストール（Install）]** をクリックします。

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。後で更新ステータスを確認するには、**[ソフトウェア管理（Software Management）]** 画面に移動し、**[続行（Continue）]** をクリックします。

このステップには最大 20 分間かかります。これにより、必要な Kubernetes イメージとサービスがセットアップされますが、クラスタは新しいバージョンに切り替わりません。次の手順で新しいイメージをアクティブ化するまで、クラスタは既存のバージョンを実行し続けます。

ステップ 7 新しい画像をアクティブにします。

アップグレード画面から移動したことがない場合は、**[アクティブ化（Activate）]**をクリックして新しいイメージをアクティブ化します。

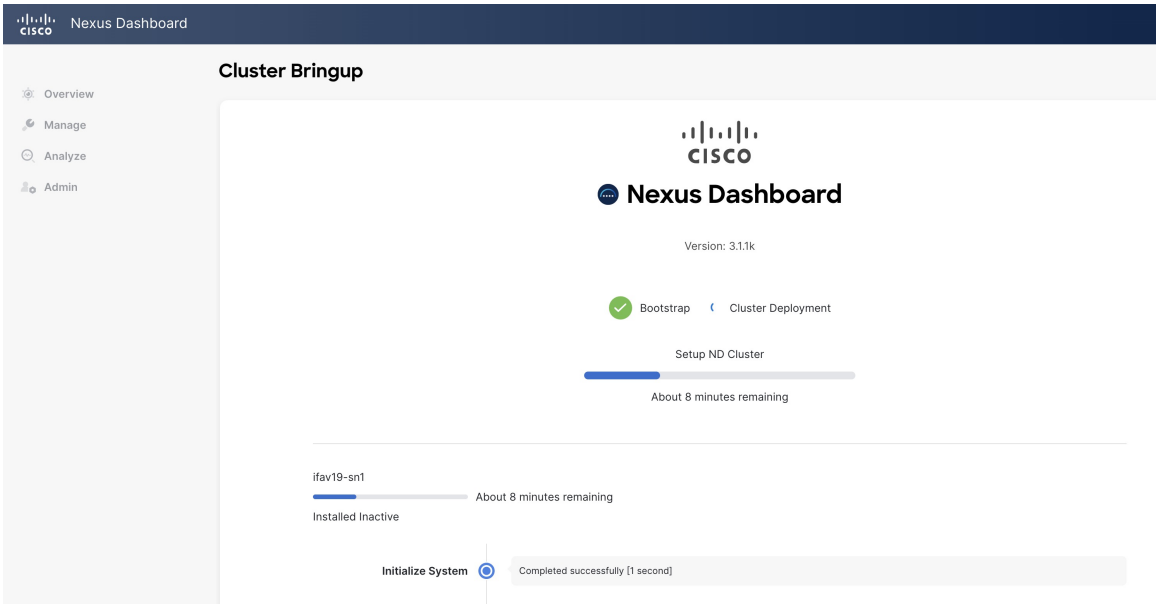
a) 移動したことがある場合には、**[管理（Admin）]** > **[ソフトウェア管理（Software Management）]**に移動します。

リリース 2.3.2 では、このページは代わりに **[操作（Operations）]** > **[ファームウェア管理（Firmware Management）]** の下にあります。

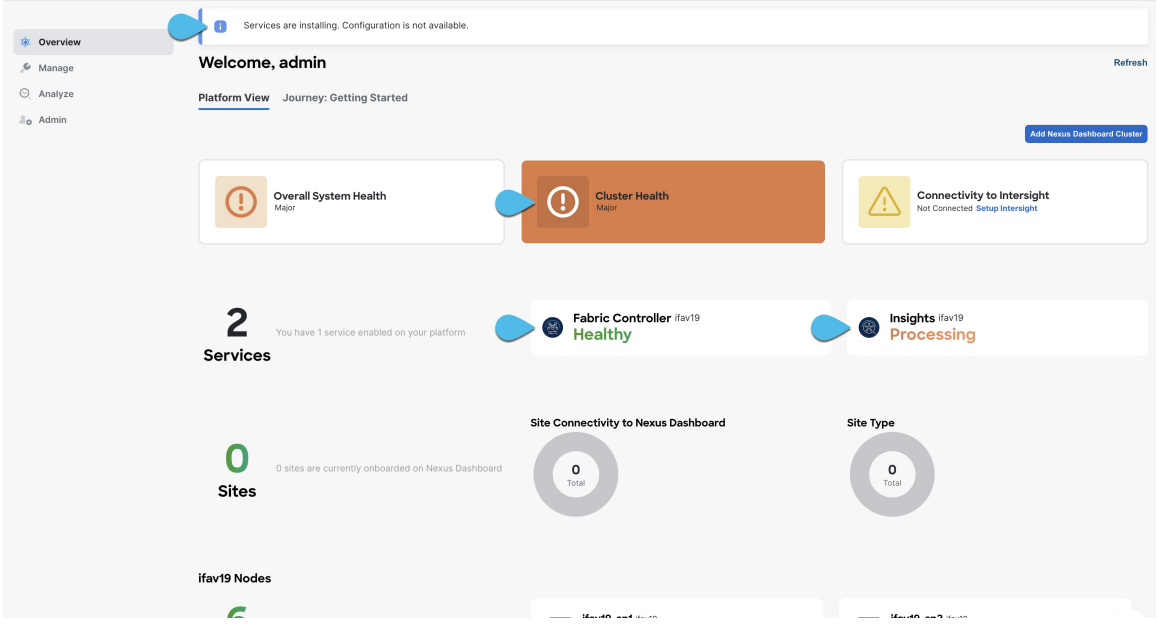
b) **[最終更新ステータス（Last Update Status）]** タイルで、**[続行（Continue）]** をクリックします。

c) **[ファームウェア アップデート（Firmware Update）]** > **[インストール（Install）]** 画面で、**[アクティブ化（Activate）]** をクリックします。

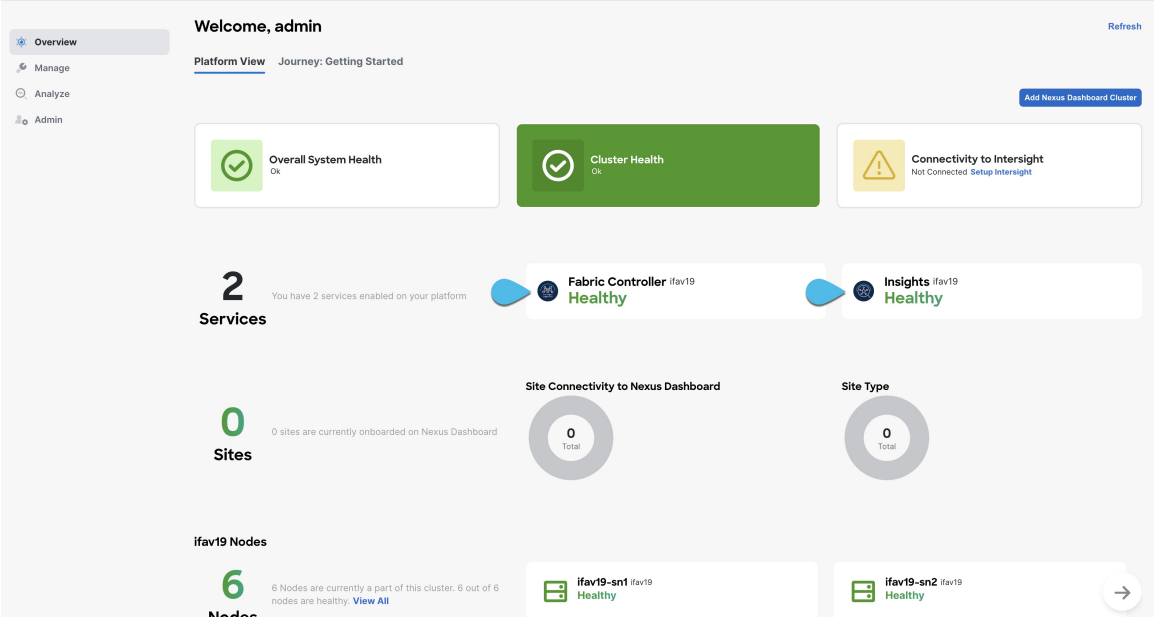
[アクティブ化（Activate）] をクリックすると、クラスタはバックグラウンドサービスを停止します。これには数分かかる場合があります。その後、再起動します。アクティブ化の段階ですべてのノードが同時に再起動し、ノードの再起動後にすべてのクラスタサービスが開始されるので、GUI が使用可能になるまでにさらに最大 20 分かかる場合があることに注意してください。



[概要（Overview）] ページで進行状況とサービスステータスを確認できます。



アップグレードが完了すると、既存のサービスが **[概要（Overview）]** ページに `[正常（Healthy）]` と表示されます。



ステップ 8 (オプション) 新しい UCS-C225-M6 ハードウェアに移行します。

（注）
Nexus ダッシュボード ノードを新しい UCS-C225-M6 サーバーに置き換える予定がない場合は、この手順をスキップできます。

UCS-C220-M5 ハードウェアを使用して展開された既存の Nexus ダッシュボード クラスタを移行するには、新しい UCS-C225-M6 ノードを `stadby` ノードとして既存のクラスタに追加し、古いノードの 1 つをフェイルオーバーするだけです。次に、古いクラスターの残りのノードについて、一度に 1 ノードずつプロセスを繰り返します。スタンバイ ノードの追加と使用については、Nexus Dashboard ドキュメント ライブラリの「インフラストラクチャ管理」の記事で詳しく説明されています。

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。それでも、GUI を使用して問題を解決できなかった場合は、 `rescue-user` としてノードにログインし、このセクションで説明されているコマンドを実行することで、手動でアップグレードを再試行できます。

手順

ステップ 1 すべての Nexus Dashboard クラスタ ノードに `rescue-user` としてログインします。

すべてのノードで同時にリカバリコマンドを実行する必要があるため、次の手順に進む前に各ノードにログインしてください。

ステップ 2 すべてのノードに `rescue-user` としてログインしていることを確認します。

ステップ 3 特定のシナリオに応じて必要なコマンドを実行します。

1 つ以上のノードが再起動せず、古いリリースがまだ実行されているためにアップグレードに失敗する場合は、手動アップグレードを試行できます。ただし、手動アップグレードには Cisco TAC のみが生成できるルートアクセスが必要なため、Cisco TAC に連絡して手動アップグレードのサポートを受ける必要があります。

ステップ 4 すべてのノードでインストーラが完了するまで待ちます。

ステップ 5 `acs reboot` コマンドを使用して、すべてのノードを同時に再起動します。

ノードの再起動後、UI にログインして、通常の UI ベースのアップグレードと同様にブートストラップの進行状況を確認できます。

ステップ 6 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。

ブートストラップ 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（Manage）]** > **[ソフトウェアの管理（Software Management）]**ページで現在の実行中バージョンを確認できます。

さらに、**[分析（Analyze）]** > **[サービス ステータス（Service Status ）]**ページで、サービスのステータスを確認します。

第 14 章

DCNM から NDFC への移行

- 前提条件とガイドライン （215 ページ）
- 既存の DCNM 設定の NDFC への移行 （217 ページ）

前提条件とガイドライン

（注） ファブリック コントローラ サービスで Nexus Dashboard をすでに実行している場合は、このセクションをスキップし、代わりに 既存の ND クラスタをこのリリースへアップグレード （201 ページ） の説明に従ってアップグレードしてください。

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 NDFC 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. ファブリック コントローラ（NDFC）サービスを使用して、新しい Nexus Dashboard クラスタを展開します。

   以前のリリースでは、クラスタがすでに展開された後にサービスをインストールし、有効にする必要がありましたが、このリリースでは、統合インストールの導入により、クラスタの初期展開時にサービスを有効にすることに注意してください。
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） アップグレードに進む前に、各ファブリックのログイン情報を検証します。

これは、 **[Web UI]** > **[管理（Administration）]** > **[ログイン情報の管理（Credentials Manage）]** > **[SAN のログイン情報（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。

ペルソナ互換性

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、ペルソナ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。

DCNM 11.5（4）からのバックアップ	アップグレード後の NDFC でのペルソナの有効化
OVA/ISO/SE での DCNM 11.5（4）ローカルエリア ネットワーク（LAN）ファブリックの展開	ファブリック コントローラ + ファブリック ビルダー
OVA/ISO/SE でのDCNM 11.5（4）PMN の展開	ファブリック コントローラ +メディアの IP ファブリック（IPFM）
OVA/ISO/SE での DCNM 11.5（4）SAN の展開	SAN コントローラ
Linux での DCNM 11.5（4）SAN の展開	SAN コントローラ
Windows での DCNM 11.5（4）SAN の展開	SAN コントローラ

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。

（注） SAN Insights および VMM Visualizer 機能は、復元後に有効になりません。 Nexus Dashboard ファブリック コントローラ UI の **[設定（Settings）]** > **[機能管理（Feature Management）]** ページで有効にするように選択できます。

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 詳細については、Cisco Nexus Dashboard ユーザー ガイドを参照してください。	サポート対象
コンテナ オーケストレータ (K8s) ビジュアライザ	サポート対象
vCenter による VMM の可視性	サポート対象
構成された Nexus Dashboard Orchestrator	未サポート
設定されたプレビュー フィーチャー	サポート対象外
SAN インストールの LAN スイッチ	サポート対象外
IPv6 で検出されたスイッチ	サポート対象外

DCNM 11.5（4）の機能	アップグレードのサポート
DCNM トラッカー	サポート対象外
ファブリックのバックアップ	未サポート
レポート定義とレポート	未サポート
スイッチのイメージとイメージ管理ポリシー	サポート対象外
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
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。

既存の DCNM 設定の NDFC 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) NDFC ダウンロードページに移動します。

https://software.cisco.com/download/home/281722751/type/282088134/

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_12_2_1_Upgrade_Tool_OVA_ISO.zip`

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
Linux または Windows	DCNM_To_NDFC_12_2_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_12_2_1_Upgrade_Tool_LIN_WIN.zip
Archive:  DCNM_To_NDFC_12_2_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。

```
# ls -l
total 4624
-rw-rw-r-- 1 root root    1422 Aug 11  2023 ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM
-rwxr-xr-x 1 root root   16788 Feb 26 15:57 cisco_x509_verify_release.py3
-rw-r--r-- 1 root root 2344694 Feb 27 07:51 DCNM_To_NDFC_12_2_1_Upgrade_Tool_OVA_ISO.zip
-rwxr-xr-x 1 root root 2359065 Feb  2 09:19 DCNM_To_NDFC_Upgrade_Tool_OVA_ISO
-rw-rw-r-- 1 root root     256 Feb 26 16:54 DCNM_To_NDFC_Upgrade_Tool_OVA_ISO.signature

# ./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_12_2_1_Upgrade_Tool_OVA_ISO.zip
Archive:  DCNM_To_NDFC_12_2_1_Upgrade_Tool_OVA_ISO.zip
inflating: DCNM_To_NDFC_Upgrade_Tool_OVA_ISO
extracting: DCNM_To_NDFC_Upgrade_Tool_OVA_ISO.signature
inflating: ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM
inflating: cisco_x509_verify_release.py3
```

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 -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。

バックアップ ツールは、過去 90 日間の Performance Management データを収集します。

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
```

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。

- Windowsの場合：

```
G:\DCNM_To_NDFC_Upgrade_Tool_LIN_WIN>DCNMBackup.bat
DCNMBackup.bat
Enter DCNM root directory [C:\Program Files\Cisco Systems\dcm]:

Initializing, please wait...

*******************************************************************************

Welcome to DCNM-to-NDFC Upgrade Tool for Linux/Windows.

This tool will analyze this system and determine whether you can move to NDFC 12.2.1 or not.

If upgrade to NDFC 12.2.1 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:
….
2024-02-26 17:57:32,247 [main] INFO  DCNMBackup - Creating final tar.gz file....
2024-02-26 17:57:32,649 [main] INFO  DCNMBackup - Final tar.gz elapsed time: 402 in ms
2024-02-26 17:57:32,650 [main] INFO  DCNMBackup - Backup done.
2024-02-26 17:57:32,657 [main] INFO  DCNMBackup - Log file: backup.log
2024-02-26 17:57:32,658 [main] INFO  DCNMBackup - Backup file:
backup11_win57_20240226-172247.tar.gz
```

- Linuxの場合：

```
# ./DCNMBackup.sh
Enter DCNM root directory [/usr/local/cisco/dcm]:

Initializing, please wait...

*******************************************************************************

Welcome to DCNM-to-NDFC Upgrade Tool for Linux/Windows.

This tool will analyze this system and determine whether you can move to NDFC 12.2.1 or not.
```

```
If upgrade to NDFC 12.2.1 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:
2024-02-27 07:53:46,562 [main] INFO  DCNMBackup - Inside init() method
2024-02-27 07:53:46,564 [main] INFO  DCNMBackup - Loading properties....
2024-02-27 07:53:46,649 [main] INFO  DCNMBackup - Inside checkLANSwitches...
2024-02-27 07:53:46,732 [main] INFO  fms.db - set database url
as:jdbc:postgresql://localhost:5432/dcmdb
2024-02-27 07:53:46,887 [main] INFO  DCNMBackup - LAN Switch count: 0
2024-02-27 07:53:46,889 [main] INFO  DCNMBackup - Inside exportDBTables...
2024-02-27 07:53:46,892 [main] INFO  DCNMBackup - Exporting ---------> statistics
2024-02-27 07:53:46,903 [main] INFO  DCNMBackup - Exporting ---------> sequence
2024-02-27 07:53:46,964 [main] INFO  DCNMBackup - Exporting ---------> clustersequence
2024-02-27 07:53:46,965 [main] INFO  DCNMBackup - Exporting ---------> logicsvr_fabric
……….
2024-02-27 07:53:49,147 [main] INFO  DCNMBackup - Creating final tar.gz file....
2024-02-27 07:53:49,183 [main] INFO  DCNMBackup - Final tar.gz elapsed time: 35 in ms
2024-02-27 07:53:49,183 [main] INFO  DCNMBackup - Backup done.
2024-02-27 07:53:49,183 [main] INFO  DCNMBackup - Log file: backup.log
2024-02-27 07:53:49,183 [main] INFO  DCNMBackup - Backup file:
backup11_onefiveseven.cisco.com_20240227-72149.tar.gz
```

- OVA の場合：

```
# ./DCNM_To_NDFC_Upgrade_Tool_OVA_ISO
*******************************************************************************

Welcome to DCNM-to-NDFC Upgrade Tool for OVA/ISO.

This tool will analyze this system and determine whether you can move to
NDFC 12.2.1 or not.

If upgrade to NDFC 12.2.1 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 NDFC 12.2.1

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 backup file
Done.
Backup file: backup11_host108_20240227-153940.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、ファブリック コントローラ サービス、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 ファブリック コントローラ UI 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。

  https://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）]** > **[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。

  https://smartreceiver.cisco.com に ping を送信すると、最新のサブネットを見つけることができます。次に例を示します。

```
$ ping smartreceiver.cisco.com
PING smartreceiver.cisco.com (146.112.59.81): 56 data bytes
64 bytes from 146.112.59.81: icmp_seq=0 ttl=52 time=48.661 ms
64 bytes from 146.112.59.81: icmp_seq=1 ttl=52 time=44.730 ms
64 bytes from 146.112.59.81: icmp_seq=2 ttl=52 time=48.188 ms
```

さらに、NDFC 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。

a) admin アカウントで Nexus Dashboard にログインします。

b) 上部のドロップダウンメニューから、**[ファブリック コントローラ（Fabric Controller）]** を選択します。

c) 左のナビゲーション メニューから**[管理（Admin）]** > **[バックアップおよび復元（Backups & Restore）]** を選択します。

d) メイン ペインで、**[復元（Restore）]** をクリックします。

e) **[今すぐ復元（Restore Now）]** ウィンドウで詳細を入力します。

- 前の手順で作成したバックアップに基づいて、**[設定のみ（Config Only）]** または **[フル（Full）]** を選択します。
- バックアップ ファイルが保存されている **[ソース（Source）]** を選択し、ファイルをアップロードするか、リモート サーバーの場所とパスを指定します。
- 設定のバックアップ時に指定した **[暗号キー（Encryption Key）]** を入力します。
- **[外部サービス IP 設定を無視（Ignore External Service IP Configuration ）]** オプションがオフになっていることを確認します。

f) **[次へ（Next）]** をクリックして情報を確認し、**[復元（Restore）]** で設定を復元します。

復元の進行中、UI はロックされます。復元に必要な時間は、バックアップ ファイルのデータによって異なります。

復元が正常に完了したら、**[ページのリロード（Reload the page）]** をクリックするか、ブラウザ ページを更新して復元を完了し、Nexus Dashboard ファブリックコントローラの使用を開始します。

ステップ 7 アップグレード後のタスクを完了します。

a) SAN コントローラ ペルソナを使用している場合：

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**[操作（Operations）]** > **[ライセンス管理（License Management）]** > **[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) ファブリック コントローラ ペルソナを使用している場合：

DCNM 11.5(4) からアップグレードする場合、次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。

- エンドポイント ロケータを再設定する必要があります
- IPAM 統合を再設定する必要があります

- アラーム ポリシーを再設定する必要があります
- カスタム トポロジを再作成して保存する必要があります
- ファブリックで PM 収集を再度有効にする必要があります
- スイッチ イメージをアップロードする必要があります

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。
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。**Web UI の [LAN]-[Fabrics]-[Fabrics]** で、[Fabric]をダブルクリックして **[Fabric Overview]** を表示します。**[ファブリック アクション（Fabrics Actions）]**ドロップダウン リストから、**[設定の再計算（Recalculate Config）]** 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。**Web UI の [LAN]-[Fabrics]-[Fabrics]** で、[Fabric]をダブルクリックして **[Fabric Overview]** を表示します。**[ファブリック アクション（Fabrics Actions）]**ドロップダウン リストから、**[設定の再計算（Recalculate Config）]** 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

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。