

Cisco Nexus Dashboard 展開とアップグレード ガイド、リリース 4.3.x

最終更新：2026 年 11 月 2 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)

© 2026 Cisco Systems, Inc. All rights reserved.



目 次

Trademarks ?

第 1 章 **新機能と更新情報** 1

新機能および変更情報 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

Nexus Dashboard の展開の概要 5

サポートされているノード タイプと機能について 9

第 3 章 **前提条件とガイドライン** 13

全般的な前提条件とガイドライン 13

Nexus Dashboard データ ネットワークと管理ネットワークの前提条件 18

Nexus Dashboard 内部アプリおよびサービス ネットワークの前提条件 20

LAN 展開の前提条件 21

LAN 展開のためのネットワークの前提条件 21

LAN 展開で ACI ファブリックをオンボーディングするための前提条件 22

LAN 展開での NX-OS、 IOS XR、およびIOS XE デバイスのオンボーディングに関する前提条件 24

LAN 展開用の通信ポート 25

SAN 展開の前提条件 39

SAN 展開のためのネットワークの前提条件 39

SAN 展開用の通信ポート 40

Nexus Dashboardの 永続 IP アドレス 52

BGP 構成と永続的な IP アドレス 60
ラウンド トリップ時間の要件 60
Nexus Dashboard ストレージの前提条件（仮想フォーム ファクタ） 61
ファブリック接続 63

第 II 部： クラスタの展開 73

第 4 章 インストール前のチェックリスト 75
インストール前チェックリスト 75

第 5 章 物理アプライアンスとしての展開 81
物理アプライアンスとして Nexus Dashboard を展開する場合の前提条件と注意事項 81
Cisco Integrated Management Controller IP アドレスの構成 83
Cisco Integrated Management Controller に対する Serial over LAN の有効化 84
物理アプライアンスの概要とケーブル接続 84
ND-NODE-G5S（UCS-C225-M8）。 84
ND-NODE-G5L（UCS-C225-M8）について 85
ステータス LED およびボタン 88
物理ノードのケーブル接続 93
ND-NODE-G5S（UCS-C225-M8）。 97
ND-NODE-G5S（UCS-C225-M8）について 97
物理ノードのケーブル接続 105
ND-NODE-L4 （UCS-C225-M6） 109
ND-NODE-L4（UCS-C225-M6）について 109
物理ノードのケーブル接続 117
SE-NODE-G2 （UCS-C220-M5）。 120
SE-NODE-G2（UCS-C220-M5）について 120
物理ノードのケーブル接続 131
物理アプライアンスとしての Nexus Dashboard の展開 134

第 6 章 VMware ESX の展開 145

VMware ESX で Nexus Dashboard クラスタを展開するための前提条件と注意事項 145
VMware vCenter を使用した Nexus ダッシュボードの展開 148
VMware ESXi での Nexus ダッシュボードの展開 165

第 7 章 **Linux KVMでの展開 179**
Linux KVM で Nexus Dashboard クラスタを展開するための前提条件と注意事項 179
Linux KVM ストレージ デバイスの I/O 遅延の確認 180
システム リソースを理解する 181
QCOW2 イメージのデプロイメント スクリプトについて 181
QCOW2 イメージのデプロイメント スクリプトの前提条件 182
QCOW2 イメージのデプロイメント スクリプトを使用します 183
オプションの展開後のタスク 189
Linux KVM での Nexus ダッシュボードの展開 190

第 8 章 **Nutanix での仮想 Nexus Dashboard（vND）の展開 203**
Nutanix での vND の展開に関する前提条件と注意事項 203
Nutanix ストレージ デバイスの I/O 遅延の確認 204
システム リソースを理解する 205
QCOW2 イメージのデプロイメント スクリプトについて 206
QCOW2 イメージのデプロイメント スクリプトの前提条件 207
QCOW2 イメージのデプロイメント スクリプトを使用します 208
オプションの展開後のタスク 214
Nutanix に Nexus Dashboard クラスタをインストールする 215

第 9 章 **Amazon Web Services（AWS）での仮想 Nexus Dashboard（vND）の展開 239**
AWS パブリッククラウドでの vND のホスティングについて 239
Amazon Web Services で Nexus Dashboard クラスタを展開するための前提条件と注意事項 241
Nexus Dashboard クラスタ向け Amazon Web サービスの準備 243
Amazon Web Services（AWS）に仮想 Nexus Dashboard（vND）を展開する 244
ノードの交換（RMA） 252

第 III 部： このリリースへのアップグレードまたは移行 257

第 10 章 Nexus Dashboard 3.2.2m クラスタのこのリリースへのアップグレード 259

既存の Nexus Dashbaord クラスターをアップグレードするための前提条件と注意事項 259

(オプション)別々の NDFC および NDI クラスタを単一の共同ホストNexus Dashboardクラスターに変換する 265

サポートされているアップグレード パス 266

Nexus Dashboard のアップグレード 268

アップグレード後の情報とタスク 272

アップグレードのトラブルシューティング 278

第 11 章 このリリースへの Nexus Dashboard 4.x クラスタのアップグレード 279

既存の Nexus Dashbaord クラスターをアップグレードするための前提条件と注意事項 279

サポートされているアップグレード パス 282

Nexus Dashboard のアップグレード 284

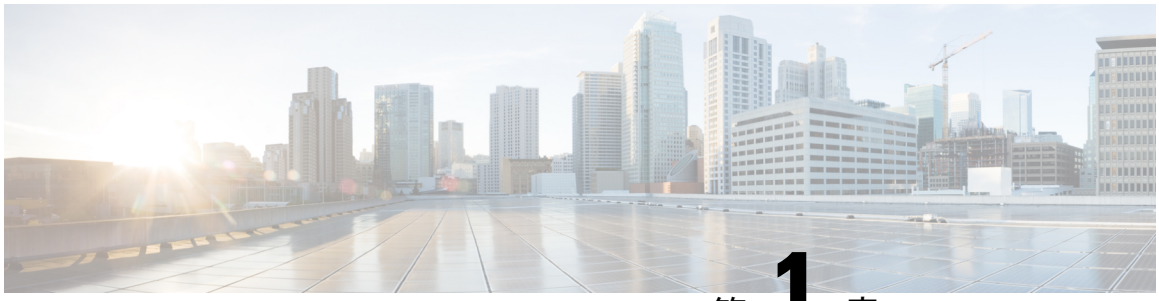
アップグレードのトラブルシューティング 288

第 12 章 DCNM から ND への移行 289

DCNM から ND への移行 289

第 13 章 NDB から ND への移行 291

NDB から ND への移行 291



第 1 章

新機能と更新情報

• 新機能および変更情報 （1 ページ）

新機能および変更情報

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

表 *1*：最新のアップデート

リリース	新機能またはアップデート	参照先
4.3.1	ESXi 9.0.2 のサポート	VMware ESX で Nexus Dashboard クラスタを展開する場合、 ESXi 9.0.2 のサポートが使用可能になりました。 • vSphere 9.0.2 での vND のサポート • vCenter 9.0.2 の VMware 統合のサポート 詳細については、「VMware ESX の展開 （145 ページ）」を参照してください。

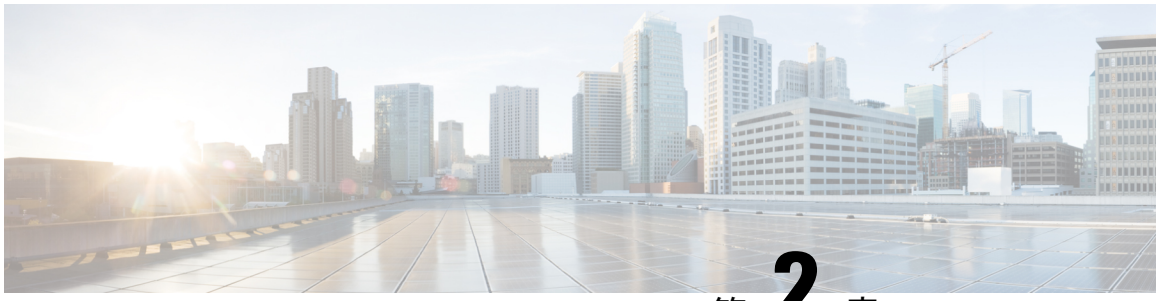
リリース	新機能またはアップデート	参照先
4.3.1	QCOW2イメージの展開スクリプト	RHELやNutanixを含むKVMベースの環境全体でNexus Dashboardをより一貫して展開できるようになります。QCOW2イメージに、セットアップを簡素化し、互換性を検証し、サポートされているプラットフォーム間での一貫したデプロイメントを促進する、デプロイメントの検証とオーケストレーションスクリプトが含まれるようになりました。 詳細については、「QCOW2 イメージのデプロイメント スクリプトについて （181 ページ）」を参照してください。



第 I 部

Nexus Dashboard の展開の準備

- 展開の概要と要件 （5 ページ）
- 前提条件とガイドライン （13 ページ）



第 2 章

展開の概要と要件

• Nexus Dashboard の展開の概要 （5 ページ）

Nexus Dashboard の展開の概要

Nexus Dashboard プラットフォーム

Cisco Nexus Dashboard は、複数のデータ センター ファブリックのための中央管理コンソールで、ネットワーク ポリシーと運用のためのリアルタイム分析、可視性、保証を実現し、Cisco ACI や NX-OS などのデータ センター ファブリックのポリシー オーケストレーションを提供しています。

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

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

統合 Nexus Dashboard のデプロイメント

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

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

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

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

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

ハードウェアとソフトウェアのスタック

Nexus Dashboardは、ソフトウェアフレームワーク（Nexus Dashboard）がプリインストールされた、特殊なCisco UCSサーバ（Nexus Dashboardプラットフォーム）のクラスタとして提供されます。Cisco Nexus Dashboard ソフトウェアスタックは、ハードウェアから分離して、多数の仮想フォームファクタで展開できます。このドキュメントでは、「Nexus Dashboard worker」はハードウェアを指し、「Nexus Dashboard」はソフトウェア スタックと GUI コンソールを指します。さらに、「物理Nexus Dashboard」または「pND」という用語を使用して、Nexus Dashboard ソフトウェア スタックが事前にインストールされている Cisco UCS 物理アプライアンス ハードウェアを指し、「リモート対応 Nexus Dashboard」または「vND」という用語を指します。をデータ ノードとアプリケーション ノードをサポートするリモート対応フォームファクタに追加します。

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

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

利用可能なフォームファクタ

Cisco Nexus Dashboardのこのリリースは、さまざまなフォームファクタを使用して展開できます。ただし、すべてのノードに同じフォーム ファクタを使用する必要があります。同じクラスタ内で異なるフォーム ファクタのノードを混在させることはサポートされていません。物理フォーム ファクタは、現在 4 機種の異なる Cisco UCS サーバをサポートしています（`SE-NODE-G2`、`ND-NODE-L4`、`ND-NODE-G5S`、および`ND-NODE-G5L`）。同じクラスタ内に `SE-NODE-G2` サーバと `ND-NODE-L4` サーバを混在させることはできますが、 `SE-NODE-G2` サーバと `ND-NODE-L4` サーバで、`ND-NODE-L4` サーバと同じクラスタに `ND-NODE-G5S` サーバを混在させることはできません。

- 物理アプライアンス（`.iso`）：このフォームファクタは、Cisco Nexus Dashboard ソフトウェア スタックがプレインストールされた、Cisco UCS 物理アプライアンス ハードウェアを指します。

  このドキュメントの後半のセクションでは、既存の物理アプライアンスハードウェアでソフトウェアスタックを設定してクラスタを展開する方法について説明します。Nexus Dashboard ハードウェアのセットアップについては、特定の UCS モデルの *Nexus Dashboard ハードウェア セットアップ ガイド*を参照してください。

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

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

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

  AWS パブリック クラウド上で仮想 Nexus Dashboard（vND）を実行するためのサポートも提供されています。詳細については、「Amazon Web Services（AWS）での仮想 Nexus Dashboard（vND）の展開 （239 ページ）」を参照してください。

  Nexus Dashboard リリース 4.2(1) 以降では、Nutanix 上で仮想 Nexus Dashboard (vND) を実行するサポートも提供されます。詳細については、「Nutanix での仮想 Nexus Dashboard（vND）の展開 （203 ページ）」を参照してください。

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

スケールとクラスタ サイジングのガイドライン

基本的な Nexus Dashboard の展開は、通常、クラスタを起動するために必要な 1 つまたは 3 つの プライマリ ノードで構成されます。スケール要件に応じて、3 ノード以上のクラスターを最大 3 つの セカンダリ ノードを追加して拡張し、より高いスケールをサポートできます。クラスタへのセカンダリ ノードの追加は、クラスタのデプロイメント中に行う必要があり、クラスターの初期化後に追加することはできません。

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

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

スケールとクラスター サイジングの制限

次の制限は、スケーリングとクラスターのサイジングに適用されます。

- ND-NODE-G5L（UCS-C225-M8）ノードは、3ノード クラスター構成でのみ使用できます。
- 4 クラスター ノードの展開。ここでクラスターの構成は次のとおりです。
  - 3 つの仮想ノード（データ）、および
  - 1 つのスタンバイ ノード

  サポートする構成。スタンバイ ノードを使用せずにこのクラスターを再展開します。クラスター内のいずれかのノードに障害が発生した場合は、新しいノードを再インストールし、**[管理（Administration >）] [システム（System）] [ステータス（Status）] > [ノード（Nodes）]**に移動してから、**[アクション（Actions）] > [再登録（Re-Register）]**をクリックして、再インストールしたノードをクラスターに戻します。
- 単一ノード展開は、初期の展開後に 3 ノード クラスタに拡張することはできません。

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

- 単一ノード展開では、追加の セカンダリ ノードまたは スタンバイ ノードはサポートされません。
- 3 ノード クラスタの場合、クラスタが動作し続けるには、少なくとも 2 つのプライマリ ノードが必要です。

  詳細については、「*Cisco Nexus Dashboard* を使用した高可用性サービスの展開」を参照してください。
- 既存のクラスタ全体のサイズを変更するために、プライマリ ノードまたはセカンダリ ノードを動的に追加または削除することはできません。クラスタのサイズを変更するには、クラスターをバックアップし、クラスタを必要なサイズに再構築してから、設定を復元する必要があります。新しいクラスタ サイズが、デプロイメントでサポートされているスケールおよび機能の要件を満たしていることを確認します。
- クラスタ サイズの変更が必要な場合は、一度に 1 つのセカンダリ ノードだけを削除します。クラスターが正常な状態に戻るまで待ってから、次のセカンダリ ノードを削除します。Nexus Dashboard GUI で、または acs health コマンドを実行して、クラスタの正常性を確認します。複数のセカンダリ ノードを同時に削除したり、クラスタの収束中に削除したりしないでください。
- 検証済みのスケールの場合、 Nexus Dashboard クラスタを初期展開する時に全ての必要なワーカー ノードを含める必要があります。追加のワーカー ノードは、既存のクラスタに追加することができます。しかし、現在のリリースでは、初期展開後にワーカー ノードを追加してもクラスタの検証済みスケール キャパシティがダイナミックに増加することはありません。追加ノードは、技術情報の大きいセットに渡ってワークロードを配布することに役立ち、個々のノードへの集中を軽減します。ワーカー ノードが追加された後にスケールのキャパシティを増やす必要がある場合、拡張されたトポロジがスケール構成に反映されるようにクラスタのバックアップと復元ができます。

サポートされているノード タイプと機能について

- Nexus Dashboard には、SE-NODE-G2 （UCS-C220-M5）、ND-NODE-L4（UCS-C225-M6）、ND-NODE-G5S （UCS -C225-M8）、および ND-NODE-G5L（ UCS-C225-M8）など、いくつかのノードタイプが Nexus Dashboard で使用できます。
- ファブリックごとに有効にできる主な機能には、 **Controller** 、 **Telemetry**、および **Orchestration** が含まれます。
- ノードと機能の互換性には、ノードタイプの混在や特定のクラスタでのすべての機能の有効化などのガイドラインと制限事項が適用されます。

サポートされているノード タイプと機能について

Nexus Dashboard で以下のノードタイプを利用できます：

- `ND-NODE-G5S` (UCS-C225-M8)。3 ノードクラスターの製品 ID は `ND-CLUSTERG5L` です：
- `ND-NODE-G5S` (UCS-C225-M8)。3 ノードクラスターの製品 ID は `ND-CLUSTERG5S` です：

- ND-NODE-L4 （UCS-C225-M6）。3 ノードクラスターの製品 ID は ND-CLUSTER-L4です：
- SE-NODE-G2 (UCS-C220-M5)。3 ノード クラスターの製品 ID は SE-CL-L3 です：

（注） SE-NODE-G2（UCS-C220-M5）ノードのサポートは、今後のNexus Dashboard リリースで終了します。このアプライアンスの EOL マイルストーンは、次の場所にあります：

Cisco UCS M5 ラック サーバー（C220 M5、C240 M5、C480 M5）の販売終了およびサポート終了の通知。

今後の Nexus Dashboard リリース ノートには、このアプライアンスがサポートされる最後のリリースに関する詳細が含まれます。

UCS-**C220-M5** ノードの RMA 交換が必要な場合、M6 が引き続きサポートされている間、**UCS-C225-M6** ノードを引き続き交換できます。M6 がマイルストーン終了（EOL）に近づいたら、M6 が EOL に達した後も M5 ノード RMA を継続的にサポートできるように、4.x リリースへのアップグレードを計画する必要があります。

M6 EOL マイルストーンが完了するまで、M5 の RMA 交換は引き続き M6 ノードで履行されます。この移行期間を使用して、4.x リリースへのアップグレードを計画し、完了することをお勧めします。

また、LAN 展開でこれらの機能を活用できます。

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

Nexus Dashboard によって管理される各ファブリックでは、同じ Nexus Dashboard クラスタ内、またはマルチクラスタ フェデレーテッド Nexus Dashboard 展開全体で次の機能を個別に有効にできます。

- Controller

- テレメトリ（Telemetry）
- オーケストレーション

（注） 一部のクラスタ展開形式では、単一クラスタですべての機能を有効にできない場合があります。Nexus Dashboard 展開に固有のサポートされているフォーム ファクタ、スケール、およびクラスタ サイジング要件のクイック リファレンスについては、「Nexus Dashboard Capacity Planning ツール」を参照してください。

注意事項と制約事項：

- クラスタ内で、より新しい ND-NODE-G5L または ND-NODE-G5S （UCS-C225-M8）ノードを、旧式の SE-NODE-G2（UCS-C220-M5）および ND-NODE-L4（UCS-C225-M6）ノードと混在させて使用することはできません。

  さらに、同種の ND-NODE-G5L または ND-NODE-G5S クラスタのみを使用できます。まとめると、次のようになります。

  - ND-NODE-G5L ノードを含むクラスタは、そのクラスタに追加の ND-NODE-G5L ノードのみを持つことができます。
  - ND-NODE-G5S ノードを含むクラスタは、そのクラスタに追加の ND-NODE-G5S ノードのみを持つことができます。

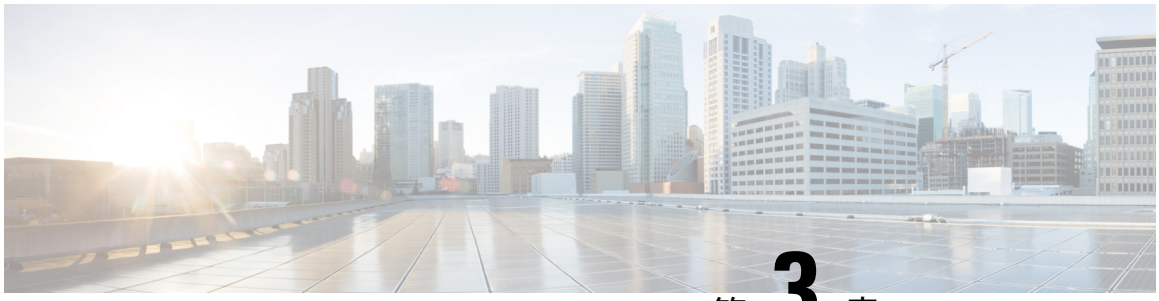
- ND-NODE-G5L ノードは、LAN 展開でのみサポートされています。
- 仮想フォーム ファクタは、 *Cisco Nexus Dashboard Verified Scalability Guide* ので説明しているように、多くのクラスタ サイズおよびタイプですべての機能をサポートしているわけではありません。
- Nexus Dashboard ノードが使用できなくなると、一部のテレメトリ機能が影響を受ける可能性があります。保証、バグ スキャン、ログ収集などのテレメトリのダイナミック ジョブはブロックされ、ノードが復元されるまで実行されません。
- デプロイメントがそのフォーム ファクタでサポートされているスケールの 50% 以下で動作している場合、ノード障害時にテレメトリ機能が完全にサポートされます。たとえば、3vND データ フォーム ファクタは最大 100 台のスイッチをフル スケールでサポートします。デプロイメントに50のスイッチが含まれており、Nexusダッシュボードノードが使用できなくなった場合、テレメトリ サービスは正常に動作し続けます。サポートされているスケールの 50% を超えて動作する展開では、ノード障害時のテレメトリの動作はベスト エフォート ベースで提供され、一部の機能が低下する可能性があります。

Windows 11 VDI クライアントのサイジング

Windows 11 仮想デスクトップ インフラストラクチャ（VDI）環境では、複数のユーザーが同時に UI にアクセスする場合に、十分なクライアント リソースを割り当てて Nexus Dashboard UI の安定したパフォーマンスを提供します。以下の設定は、同時 VDI ユーザー セッションごとにテストおよび検証されています。

これらのサイジング要件は、 Nexus Dashboard UI へのアクセスに使用される VDI クライアント セッションに適用されます。

コンポーネント	ユーザーごとにサポートされる最小構成	ユーザーごとに推奨設定
CPU	8 vCPU	16 vCPU
プロセッサ速度	2.1 GHz 以上	2.1 GHz 以上
プロセッサ	互換性のある 64 ビット プロセッサ（2 コア以上）。 インテル Xeon シルバー 4116 以降	互換性のある 64 ビット プロセッサ（2 コア以上）。 インテル Xeon シルバー 4116 以降
メモリ	8 GB RAM	32 GB RAM
ハードウェア アクセラレーション	有効または無効	有効
ディスプレイの解像度	1280 × 720 ピクセル以上	1280 × 720 ピクセル以上



第 3 章

前提条件とガイドライン

- 全般的な前提条件とガイドライン （13 ページ）
- Nexus Dashboard データ ネットワークと管理ネットワークの前提条件 （18 ページ）
- Nexus Dashboard 内部アプリおよびサービス ネットワークの前提条件 （20 ページ）
- LAN 展開の前提条件 （21 ページ）
- SAN 展開の前提条件 （39 ページ）
- Nexus Dashboardの 永続 IP アドレス （52 ページ）
- ラウンド トリップ時間の要件 （60 ページ）
- Nexus Dashboard ストレージの前提条件（仮想フォーム ファクタ） （61 ページ）
- ファブリック接続 （63 ページ）

全般的な前提条件とガイドライン

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

全般的な展開のガイドラインと制限

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

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

Nexus Dashboard ノードでの展開とアップグレードには、常に、有効な DNS サーバーと NTP サーバーが必要です。

有効な DNS 接続がない場合（到達不能な IP アドレスまたはプレースホルダ IP アドレスを使用している場合など）、システムを正常に展開またはアップグレードできない可能性がありますし、通常のサービスの機能にも影響が及びます。

（注） Nexus Dashboard は、DNS クライアントとリゾルバーの両方として機能します。内部サービス向けには、DNS リゾルバーとして機能する内部の Core DNS サーバーを使用します。また、DNS クライアントとしても動作して、イントラネット内またはインターネットの外部ホストに到達できるようにするためには、外部 DNS サーバーを構成する必要があります。

DNS については次のガイドラインが適用されます。

- Nexus Dashboard リリース 4.3.1 より前のリリースでは、DNS ドメイン名はクラスタ名を使用して作成されていました。Nexus Dashboard リリース 4.3.1 以降、DNS 名は `cluster.case.local` に固定されています。
- 外部 DNS サーバーの場合、 TCPと UDP トラフィックの両方を許可する必要があります。詳細については、LAN 展開用の通信ポート （25 ページ）と SAN 展開用の通信ポート（40 ページ）を参照してください。
- Nexus Dashboard は、ワイルドカード レコードを持つ DNS サーバーはサポートしていません。

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

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

NTP 認証を有効にする場合は、次の注意事項が適用されます。

- Windows サーバを NTP サーバとして使用しないことをお勧めします。
- 対称認証の場合、使用するキーは、NTP サーバーと Nexus Dashboard の両方で同じ構成にする必要があります。

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

  この場合、キーは Nexus Dashboard で 1 回だけ構成してから、複数のサーバーに割り当てる必要があります。
- キー ID が一意である限り、Nexus Dashboard と NTP サーバの両方に複数のキーを設定できます。

- このリリースでは、NTP キーの SHA1、MD5、および AES128CMAC 認証/エンコーディング タイプがサポートされています。

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

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

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

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

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

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

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

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

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

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

IPv4 および IPv6 のサポート

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

IP アドレス構成を定義するとき、以下の注意事項が適用されます。

- クラスタ内のすべてのノードとネットワークは、IPv4 専用、IPv6 専用、またはデュアル スタック IPv4/IPv6 のいずれかの均一な IP 構成を持つ必要があります。
- クラスタを IPv4 専用モードで展開し、デュアル スタック IPv4/IPv6 または IPv6 専用に切り替える場合は、クラスタを再展開する必要があります。
- デュアル スタック構成の場合：
  - データ、管理、アプリ、およびサービス ネットワークはデュアル スタック モードである必要があります。

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

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

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

    AWS パブリック クラウドでの vND 展開プロセスを介して展開されたクラスタは、IPv6 専用またはデュアル スタック モードをサポートしません。
  - ノードを最初に構成するときに、IPv6 管理ネットワーク アドレスを指定する必要があります。

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

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

  IPv6 パケットは、VXLAN の IPv6 パケット内にカプセル化されます。
- すべての内部サービスは IPv6 アドレスを使用します。
- 物理サーバーの CIMC にも IPv6 アドレスが必要です。

特定の接続に必要な URL

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

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

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

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

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

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

Nexus Dashboard はクラスタとして展開され、各サービス ノードは 2 つのネットワークに接続されます。Nexus Dashboard を最初に設定するときは、クラスター ノードごとに、2 つの Nexus Dashboard インターフェイスに 2 つの IP アドレスを指定する必要があります。

- 1 つはデータ ネットワークに接続され、最適なパフォーマンスのためのバックエンド、クラスター、およびインフラ接続に使用されます
- もう 1 つは、管理ネットワークに接続されます。これは、シームレスな GUI とフロントエンド オペレーションのために使用されます。

表 *2:* 外部ネットワークの目的

データ ネットワーク	管理ネットワーク
• Nexus Dashboardノードのクラスタリング • サービス間通信 • Nexus Dashboard ノードから Cisco APIC ノードへの通信 • スイッチおよびオンボード ファブリックのテレメトリ トラフィック	• Nexus ダッシュボード GUI へのアクセス • SSH を介した Nexus Dashboard CLI へのアクセス • DNS および NTP 通信 • Nexus Dashboard ファームウェアのアップロード • Intersight デバイス コネクタ • AAA トラフィック • マルチクラスタ接続

2つのネットワークには次の要件があります。

- 管理ネットワークとデータ ネットワークが異なるサブネットに存在する必要があります。

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

- データ サブネットを変更するにはクラスタを再展開する必要があるため、今後の追加サービスを考慮して、ノードとサービスの必要最低限よりも大きなサブネットを使用することをお勧めします。
- リモート認証を設定する場合、AAA サーバをデータ インターフェイスと同じサブネットに配置することはできません。
- 物理クラスタの場合、管理ネットワークは各ノードの CIMC に TCP ポート 22 および 443 を使用して IP 到達可能性を提供する必要があります。これは、Nexus Dashboard クラスター設定では各ノードの CIMC IP アドレスを使用してノードを設定するためです。
- データ ネットワーク インターフェイスで、Nexus Dashboard トラフィックに使用できる最小 MTU が 1500 である必要があります。

  必要に応じて、ノードが接続されているスイッチでより高い MTU を構成できます。

（注） データ ネットワーク トラフィックに使用されるスイッチ ポートに外部 VLAN タグが構されている場合は、ジャンボ フレームを有効にするか、ノードが接続されているスイッチ ポートで 1504 バイト以上のカスタム MTU を構成する必要があります。

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

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

  - DNS 統合の場合、DNS サーバーへ。

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

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

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

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

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

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

複数の Nexus Dashboard クラスタの展開を計画している場合、同じアプリケーション サブネットとサービス サブネットをそれらに使用できます。

（注） 異なる Nexus ダッシュボード ノードに展開されたコンテナ間の通信は VXLAN でカプセル化され、送信元と宛先としてデータ インターフェイスの IP アドレスを使用します。これは、アプリ ネットワークとサービス ネットワークのアドレスがデータ ネットワークの外部に公開されることはなく、これらのサブネット上のトラフィックは内部でルーティングされ、クラスタ ノードを離れないことを意味します。

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

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

LAN 展開の前提条件

LAN 展開のためのネットワークの前提条件

次のネットワークの前提条件が LAN の導入に適用されます：

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

永続 IP アドレスの詳細については、Nexus Dashboardの 永続 IP アドレス （52 ページ）を参照してください。ブートストラップ プロセス中に、必要最小限の永続 IP アドレスを割り当てる必要があります。追加の永続IPアドレスの割り当ては、クラスタの展開後にGUIの外部サービス プール設定を使用して行うことができます。

LAN 展開で ACI ファブリックをオンボーディングするための前提条件

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

- Cisco ACI ファブリックを管理するためにオーケストレーションを使用する場合は、データ インターフェイスまたは管理インターフェイスから各ファブリックの APIC クラスターのインバンドまたはアウトオブバンド（OOB）インターフェイスまたは両方への接続を確立できます。

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

ACI ファブリックの追加の前提条件

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

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

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

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

5. [API] を展開し、次をクリックします。

これで、クラスター上でオーケストレーション サービスが有効になります。

ACI ファブリックでテレメトリを使用する場合の追加の前提条件

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

LAN 展開用の通信ポート

Nexus Dashboard は、暗号化を備えた TLS または mTLS を使用して、移行中にデータのプライバシーと完全性を保護します。

このセクションで説明されている全てのポートを開きます。

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

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

表 *3 : LAN* 展開用の管理ネットワーク通信ポート

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

サービス	ポート	プロトコル	方向（In/Out）	接続
DHCP	67	UDP	入力	ローカル DHCP サーバーがブートストラップまたは POAP 用に構成されている場合。 （注） POAP の目的でローカル DHCP サーバーとして Nexus Dashboard を使用する場合、すべての Nexus Dashboard マスター ノードの IP アドレスを DHCP リレーとして構成する必要があります。Nexus Dashboard ノードの管理 IP アドレスが DHCP サーバーにバインドされるかどうかは、サーバー設定の LAN デバイス管理接続によって決定されます。
DHCP	68	UDP	発信	
DNS	53	TCP および UDP	アウト	DNS サーバ
HTTP	80	TCP	発信	インターネット/プロキシ
HTTP（PnP）	9666	TCP	入力	Catalyst デバイス用の Cisco プラグ アンド プレイ（PnP）は、Nexus Dashboard HTTP ポート 9666 および HTTPS ポート 9667 を介して実現されます。ポート 9666 の HTTP は、CA 証明書バンドルをデバイスに送信して HTTPS モード用にデバイスを準備するために使用され、実際の PnP はその後ポート 9667 で HTTPS を介して行われます。 POAP のような PnP サービスは、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続 IP アドレスで実行されます。これは、Nexus Dashboard サーバー設定の **[LAN デバイス管理接続（LAN Device Management Connectivity）]** 設定によって制御されます。

サービス	ポート	プロトコル	方向（In/Out）	接続
HTTP（POAP）	80	TCP	入力	POAP 経由のデバイス ゼロタッチ プロビジョニングにのみ使用されます。デバイスは、基本的なインベントリ情報を Nexus Dashboard に送信して (Nexus Dashboard への制限付きの書き込み専用アクセス)、セキュアな POAP 通信を開始できます。Nexus Dashboard ブートストラップまたは POAP は、TFTP または HTTP/HTTPS 用に構成できます。 Nexus Dashboard の SCP-POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続 IP アドレスがあります。これは、Nexus Dashboard サーバー設定の **[LAN デバイス管理接続（LAN Device Management Connectivity）]** 設定によって制御されます。
HTTPS	443	TCP	入力 / 出力	UI、他のクラスタ (マルチクラスタ接続用)、ファブリック、インターネット/プロキシ
HTTPS/HTTP（NX-API）	443/80	TCP	発信	NX-API HTTPS/HTTP クライアントは、構成可能でもあるポート 443/80 でデバイスの NX-API サーバーに接続します。NX-API はオプション機能であり、Nexus Dashboard 機能の限られたセットで使用されます。

サービス	ポート	プロトコル	方向（In/Out）	接続
HTTPS（PnP）	9667	TCP	入力	Catalyst デバイス用の Cisco プラグ アンド プレイ（PnP）は、Nexus Dashboard HTTP ポート 9666 および HTTPS ポート 9667 を介して実現されます。ポート 9666 の HTTP は、CA 証明書バンドルをデバイスに送信して HTTPS モード用にデバイスを準備するために使用され、実際の PnP はその後ポート 9667 で HTTPS を介して行われます。 POAP のような PnP サービスは、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続 IP アドレスで実行されます。これは、Nexus Dashboard サーバー設定の **[LAN デバイス管理接続（LAN Device Management Connectivity）]** 設定によって制御されます。
HTTPS（POAP）	443	TCP	入力	セキュア POAP は、ポート 443 の Nexus Dashboard HTTPS サーバーを使用して実現されます。HTTPS サーバーは SCP-POAP サービスにバインドされ、そのポッドに割り当てられたのと同じ永続 IP アドレスを使用します。 Nexus Dashboard の SCP-POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続 IP アドレスがあります。これは、Nexus Dashboard サーバー設定の **[LAN デバイス管理接続（LAN Device Management Connectivity）]** 設定によって制御されます。
インフラ サービス	30012 30021 30500 ～ 30600	TCP および UDP	入力 / 出力	その他のクラスタ ノード
KMS	9880	TCP	入力 / 出力	その他クラスタ ノードおよび ACI ファブリック

サービス	ポート	プロトコル	方向（In/Out）	接続
LDAP	389 636	TCP	発信	LDAP サーバ
NTP	123	UDP	発信	NTP サーバー
NX-API	8443	TCP	入力 / 出力	NX-OS リリース 9.x 以降を搭載した Cisco MDS 9000 シリーズ スイッチでパフォーマンス モニタリングに使用されます。
RADIUS	1812	TCP	発信	Radius サーバー
SCP	22	TCP	入力 / 出力	SCPは、リモートサーバーへのバックアップファイルのアーカイブなど、デバイスと Nexus Dashboard の間でファイルを転送するさまざまな機能によって使用されます。Nexus Dashboard SCP サービスは、ダウンロードとアップロードの両方の SCP サーバーとして機能します。SCP は、POAP 関連ファイルをダウンロードするために、デバイス上の POAP クライアントによっても使用されます。 Nexus Dashboard の SCP-POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続 IP アドレスがあります。これは、Nexus Dashboard サーバー設定の **[LAN デバイス管理接続（LAN Device Management Connectivity）]** 設定によって制御されます。

サービス	ポート	プロトコル	方向（In/Out）	接続
SCP/テックコレクションを表示	22	TCP	発信	Nexus Dashboard POAP-SCP ポッドの永続 IP アドレスから、テレメトリを実行している別の ND クラスターにテクニカル サポート ファイルを転送します。 Nexus Dashboard の SCP-POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続 IP アドレスがあります。これは、NDFC サーバー設定の **[LAN デバイス管理接続（LAN Device Management Connectivity）]** 設定によって制御されます。
SMTP	25	TCP	発信	SMTPポートは、**[管理（Admin）>] [サーバー設定（Server Settings）]>[全般（General）]**ページで設定できます。 これはオプションの機能です。
SNMP	161	TCP および UDP	アウト	Nexus Dashboard からデバイスへの SNMP トラフィック。
SNMP トラップ	2162	UDP	入力	デバイスから Nexus Dashboard への SNMP トラップは、SNMP-Trap/Syslog サービス ポッドに関連付けられた永続 IP アドレスに向けて送信されます。 Nexus Dashboard の SNMP-Trap-Syslog サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続 IP アドレスがあります。これは、NDFC サーバー設定の **[LAN デバイス管理接続（LAN Device Management Connectivity）]** 設定によって制御されます。
SSH	22	TCP	入力 / 出力	クラスタ ノードの CLI および CIMC

サービス	ポート	プロトコル	方向（In/Out）	接続
TAC アシスト	8884	TCP	入力 / 出力	その他のクラスタ ノード スイッチから **show tech** を収集し、Intersight に情報をアップロードするサービスである TAC Assist に使用されます。このポートは、クラスタ ノード間で **show tech** data を交換するために使用されます。
TACACS	49	TCP	発信	TACACS サーバー
TFTP（POAP）	69	UDP	入力	POAP 経由のデバイス ゼロタッチ プロビジョニングにのみ使用されます。デバイスは、基本的なインベントリ情報を Nexus Dashboard に送信して (Nexus Dashboard への制限付きの書き込み専用アクセス)、セキュアな POAP 通信を開始できます。Nexus Dashboard ブートストラップまたは POAP は、TFTP または HTTP/HTTPS 用に構成できます。 Nexus Dashboard の SCP-POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続 IP アドレスがあります。これは、Nexus Dashboard サーバー設定の **[LAN デバイス管理接続（LAN Device Management Connectivity）]** 設定によって制御されます。

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

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

表 *4 : LAN* 展開用のデータ ネットワーク通信ポート

サービス	ポート	プロトコル	方向（In /Out）	接続
Nexus Dashboard エージェント ポート	30022	TCP	入力 / 出力	Nexus Dashboard でサポートされている SONiC デバイスを管理する場合、このポートを Nexus Dashboard の管理ネットワークとデータ ネットワークの両方に対して開いている必要があります。Nexus Dashboard は、30022 ポートへの Web ソケットを開く SONiC デバイスにエージェントをインストールします。
DHCP	67	UDP	入力	Nexus Dashboard ローカル DHCP サーバーがブートストラップ/POAP 用に構成されている場合。 （注） POAP の目的でローカル DHCP サーバーとして Nexus Dashboard を使用する場合、すべての Nexus Dashboard マスター ノードの IP アドレスを DHCP リレーとして構成する必要があります。Nexus Dashboard ノードのデータ IP アドレスが DHCP サーバーにバインドされるかどうかは、サーバー設定の LAN デバイス管理接続によって決定されます。
DHCP	68	UDP	発信	
DNS	53	TCP および UDP	入力 / 出力	他のクラスタ ノードと DNS サーバー
フローテレメトリ	5640 ～ 5671	UDP	入力	スイッチの帯域内 ファブリックからフロー テレメトリを受信するために使用されます
GRPC（テレメトリ）	50051	TCP	入力	メディア展開用の IP ファブリックおよび一般的な LAN 展開用の PTP のマルチキャスト フローに関連する情報は、ソフトウェア テレメトリを介して、Nexus Dashboard GRPC レシーバー サービス ポッドに関連付けられた永続 IP アドレスにストリーミングされます。

サービス	ポート	プロトコル	方向（In/Out）	接続
HTTP（PnP）	9666	TCP	入力	Catalyst デバイス用の Cisco プラグ アンド プレイ（PnP）は、Nexus Dashboard HTTP ポート 9666 および HTTPS ポート 9667 を介して実現されます。ポート 9666 の HTTP は、CA 証明書バンドルをデバイスに送信して HTTPS モード用にデバイスを準備するために使用され、実際の PnP はその後ポート 9667 で HTTPS を介して行われます。 POAP のような PnP サービスは、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続 IP アドレスで実行されます。これは、Nexus Dashboard サーバー設定の **[LAN デバイス管理接続（LAN Device Management Connectivity）]** 設定によって制御されます。
HTTP（POAP）	80	TCP	入力	POAP 経由のデバイス ゼロタッチ プロビジョニングにのみ使用されます。デバイスは、基本的なインベントリ情報を Nexus Dashboard に送信して (Nexus Dashboard への制限付きの書き込み専用アクセス)、セキュアな POAP 通信を開始できます。Nexus Dashboard ブートストラップまたは POAP は、TFTP または HTTP/HTTPS 用に構成できます。 Nexus Dashboard の SCP-POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続 IP アドレスがあります。これは、Nexus Dashboard サーバー設定の **[LAN デバイス管理接続（LAN Device Management Connectivity）]** 設定によって制御されます。
HTTPS	443	TCP	発信	スイッチと APIC および NX-OS の帯域内

サービス	ポート	プロトコル	方向（In/Out）	接続
HTTPS/HTTP（NX-API）	443/80	TCP	発信	NX-API HTTPS/HTTP クライアントは、構成可能でもあるポート 443/80 でデバイスの NX-API サーバーに接続します。NX-API はオプション機能であり、Nexus Dashboard 機能の限られたセットで使用されます。
HTTPS（PnP）	9667	TCP	入力	Catalyst デバイス用の Cisco プラグ アンド プレイ（PnP）は、Nexus Dashboard HTTP ポート 9666 および HTTPS ポート 9667 を介して実現されます。ポート 9666 の HTTP は、CA 証明書バンドルをデバイスに送信して HTTPS モード用にデバイスを準備するために使用され、実際の PnP はその後ポート 9667 で HTTPS を介して行われます。 POAP のような PnP サービスは、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続 IP アドレスで実行されます。これは、Nexus Dashboard サーバー設定の **[LAN デバイス管理接続（LAN Device Management Connectivity）]** 設定によって制御されます。
HTTPS（POAP）	443	TCP	入力	セキュア POAP は、ポート 443 の Nexus Dashboard HTTPS サーバーを使用して実現されます。HTTPS サーバーは SCP-POAP サービスにバインドされ、そのポッドに割り当てられたのと同じ永続 IP アドレスを使用します。 Nexus Dashboard の SCP-POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続 IP アドレスがあります。これは、Nexus Dashboard サーバー設定の **[LAN デバイス管理接続（LAN Device Management Connectivity）]** 設定によって制御されます。

サービス	ポート	プロトコル	方向（In/Out）	接続
HTTPS（vCenter、Kubernetes、OpenStack、Discovery）	443	TCP	発信	Nexus Dashboard は、VMware vCenter や OpenStack などの登録済み VMM ドメインと、Kubernetes などのコンテナ オーケストレーターから取得した情報を関連付けることにより、統合されたホストおよび物理ネットワーク トポロジ ビューを提供します。 これはオプションの機能です。
ICMP	ICMP	ICMP	入力 / 出力	他のクラスタ ノード、デフォルト ゲートウェイ
インフラ サービス	3379 3380 4430 8989 9090 9969 9979 9989 15223 30002 ～ 30006 30009 ～ 30010 30012 30014-30021 30025 30027 30028	TCP	入力 / 出力	その他のクラスタ ノード
インフラ サービス	30016 30017	TCP および UDP	入力 / 出力	その他のクラスタ ノード
インフラ サービス	30019	UDP	入力 / 出力	その他のクラスタ ノード

サービス	ポート	プロトコル	方向（In/Out）	接続
インフラ サービス	30500 ～ 30600	TCP および UDP	入力 / 出力	その他のクラスタ ノード
Kafka	30001	TCP	入力 / 出力	スイッチと APIC/コントローラの帯域内 IP
KMS	9989	TCP	入力 / 出力	その他クラスタ ノードおよび ACI ファブリック
NFSv3	111	TCP および UDP	入力 / 出力	リモート NFS サーバー
NFSv3	608	UDP	入力 / 出力	リモート NFS サーバー
NFSv3	2049	TCP	入力 / 出力	リモート NFS サーバー
NX-API	8443	TCP	入力 / 出力	NX-OS リリース 9.x 以降を搭載した Cisco MDS 9000 シリーズ スイッチでパフォーマンス モニタリングに使用されます。
SCP	22	TCP	入力 / 出力	SCPは、リモートサーバーへのバックアップファイルのアーカイブなど、デバイスと Nexus Dashboard の間でファイルを転送するさまざまな機能によって使用されます。Nexus Dashboard SCP サービスは、ダウンロードとアップロードの両方の SCP サーバーとして機能します。SCP は、POAP 関連ファイルをダウンロードするために、デバイス上の POAP クライアントによっても使用されます。 Nexus Dashboard の SCP-POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続 IP アドレスがあります。これは、Nexus Dashboard サーバー設定の **[LAN デバイス管理接続（LAN Device Management Connectivity）]** 設定によって制御されます。

サービス	ポート	プロトコル	方向（In/Out）	接続
SCP	22	TCP	発信	Nexus Dashboard POAP-SCP ポッドの永続 IP アドレスから、テレメトリを実行している別の ND クラスターにテクニカル サポート ファイルを転送します。 Nexus Dashboard の SCP-POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続 IP アドレスがあります。これは、NDFC サーバー設定の **[LAN デバイス管理接続（LAN Device Management Connectivity）]** 設定によって制御されます。
SMTP	25	TCP	発信	SMTPポートは、**[管理（Admin）>] [サーバー設定（Server Settings）] > [全般（General）]**ページで設定できます。 これはオプションの機能です。
SNMP	161	TCP および UDP	アウト	Nexus Dashboard からデバイスへの SNMP トラフィック。
SNMP トラップ	2162	UDP	入力	デバイスから Nexus Dashboard への SNMP トラップは、SNMP-Trap/Syslog サービス ポッドに関連付けられた永続 IP アドレスに向けて送信されます。 Nexus Dashboard の SNMP-Trap-Syslog サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続 IP アドレスがあります。これは、NDFC サーバー設定の **[LAN デバイス管理接続（LAN Device Management Connectivity）]** 設定によって制御されます。
SSH	22	TCP	発信	UI、スイッチと APIC のインバンド
SSH	1022	TCP および UDP	入力 / 出力	その他のクラスタ ノード

サービス	ポート	プロトコル	方向（In/Out）	接続
SW テレメトリ	5695 30000 57500 30570	TCP	入力 / 出力	その他のクラスタ ノード ファブリックからさまざまなテレメトリ情報を収集するために使用されます テレメトリおよび NX- OS ベースのスイッチ用に、スイッチと Nexus Dashboard 間にポート 57500 が必要です
テクニカル サポート	2022	TCP	入力	テクニカル サポートをファブリックからクラスタまでにアップロードするためにこれが使われています。
TFTP（POAP）	69	UDP	入力	POAP 経由のデバイス ゼロタッチ プロビジョニングにのみ使用されます。デバイスは、基本的なインベントリ情報を Nexus Dashboard に送信して (Nexus Dashboard への制限付きの書き込み専用アクセス)、セキュアな POAP 通信を開始できます。Nexus Dashboard ブートストラップまたは POAP は、TFTP または HTTP/HTTPS 用に構成できます。 Nexus Dashboard の SCP-POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続 IP アドレスがあります。これは、Nexus Dashboard サーバー設定の **[LAN デバイス管理接続（LAN Device Management Connectivity）]** 設定によって制御されます。
VXLAN	4789	UDP	入力 / 出力	その他のクラスタ ノード

SAN 展開の前提条件

SAN 展開のためのネットワークの前提条件

SAN 展開には、次のネットワークの前提条件が適用されます。

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

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

  この状況では、次のことがわかります。

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

- ユースケースに応じて、次の数の永続 IP アドレスを割り当てる必要があります。永続 IP アドレスの詳細については、Nexus Dashboardの 永続 IP アドレス （52 ページ）を参照してください。

SAN 展開用の通信ポート

Nexus Dashboard は、暗号化を備えた TLS または mTLS を使用して、移行中にデータのプライバシーと完全性を保護します。

次の表に、 SAN 展開での管理ネットワーク通信ポートを示します。

表 *5: SAN* 展開の管理ネットワーク通信ポート

サービス	ポート	プロトコル	方向 イン：クラスタに向かう アウト：クラスタからファブリックまたは外に向かう	接続
DNS	53	TCP および UDP	アウト	DNS サーバ
GRPC（テレメトリ）	33000	TCP	入力	Nexus Dashboard 永続 IP に関連付けられた GRPC トランスポートを介して SAN データ (ストレージ、ホスト、フローなど) を受信する SAN Telemetry サーバー。

サービス	ポート	プロトコル	方向 イン：クラスタに向かう アウト：クラスタからファブリックまたは外に向かう	接続
HTTP	80	TCP	発信	インターネット/プロキシ
HTTPS	443	TCP	入力 / 出力	UI、他のクラスタ (マルチクラスタ接続用)、ファブリック、インターネット/プロキシ
HTTPS（vCenter、Kubernetes、OpenStack、Discovery）	443	TCP	発信	Nexus Dashboard は、VMware vCenter や OpenStack などの登録済み VMM ドメインと、Kubernetes などのコンテナ オーケストレーターから取得した情報を関連付けることにより、統合されたホストおよび物理ネットワーク トポロジ ビューを提供します。 これはオプションの機能です。
ICMP	ICMP	ICMP	入力 / 出力	他のクラスタ ノード、CIMC、デフォルト ゲートウェイ
インフラ サービス	30012 30021 30500 ～ 30600	TCP および UDP	入力 / 出力	その他のクラスタ ノード
KMS	9880	TCP	入力 / 出力	その他クラスタ ノードおよび ACI ファブリック
LDAP	389 636	TCP	発信	LDAP サーバ
NTP	123	UDP	発信	NTP サーバー
NX-API	8443	TCP	入力 / 出力	NX-OS リリース 9.x 以降を搭載した Cisco MDS 9000 シリーズ スイッチでパフォーマンス モニタリングに使用されます。
RADIUS	1812	TCP	発信	Radius サーバー

サービス	ポート	プロトコル	方向 イン：クラスタに向かう アウト：クラスタからファブリックまたは外に向かう	接続
SCP	22	TCP	入力 / 出力	SCPは、リモートサーバーへのバックアップファイルのアーカイブなど、デバイスと Nexus Dashboard の間でファイルを転送するさまざまな機能によって使用されます。Nexus Dashboard SCP サービスは、ダウンロードとアップロードの両方の SCP サーバーとして機能します。SCP は、POAP 関連ファイルをダウンロードするために、デバイス上の POAP クライアントによっても使用されます。 Nexus Dashboard の SCP-POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続 IP アドレスがあります。これは、Nexus Dashboard サーバー設定の **[LAN デバイス管理接続（LAN Device Management Connectivity）]** 設定によって制御されます。
SCP	22	TCP	発信	Nexus Dashboard POAP-SCP ポッドの永続 IP アドレスから、テレメトリを実行している別の ND クラスターにテクニカル サポート ファイルを転送します。 Nexus Dashboard の SCP-POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続 IP アドレスがあります。これは、NDFC サーバー設定の **[LAN デバイス管理接続（LAN Device Management Connectivity）]** 設定によって制御されます。

サービス	ポート	プロトコル	方向 イン：クラスタに向かう アウト：クラスタからファブリックまたは外に向かう	接続
SMTP	25	TCP	発信	SMTPポートは、**[管理（Admin）>][サーバー設定（Server Settings）]>[全般（General）]**ページで設定できます。 これはオプションの機能です。
SNMP	161	TCP および UDP	アウト	Nexus Dashboard からデバイスへの SNMP トラフィック。
SNMP トラップ	2162	UDP	入力	デバイスから Nexus Dashboard への SNMP トラップは、SNMP-Trap/Syslog サービス ポッドに関連付けられた永続 IP アドレスに向けて送信されます。 Nexus Dashboard の SNMP-Trap-Syslog サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続 IP アドレスがあります。これは、NDFC サーバー設定の **[LAN デバイス管理接続（LAN Device Management Connectivity）]**設定によって制御されます。
SSH	22	TCP	入力 / 出力	クラスタ ノードの CLI および CIMC

サービス	ポート	プロトコル	方向 イン：クラスタに向かう アウト：クラスタからファブリックまたは外に向かう	接続
Syslog	514	UDP	入力	Nexus Dashboard が Syslog サーバーとして構成されている場合、デバイスからの syslog は、SNMP-Trap/Syslog サービス ポッドに関連付けられた永続 IP アドレスに向けて送信されます。 Nexus Dashboard の SNMP-Trap-Syslog サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続 IP アドレスがあります。これは、Nexus Dashboard サーバー設定の **[LAN デバイス管理接続（LAN Device Management Connectivity）]** 設定によって制御されます。
TACACS	49	TCP	発信	TACACS サーバー

次の表に、 SAN 展開での管理ネットワーク通信ポートの一覧を示します。

表 *6 : SAN* 展開用のデータ ネットワーク通信ポート

サービス	ポート	プロトコル	方向 イン：クラスタに向かう アウト：クラスタからファブリックまたは外に向かう	接続
DNS	53	TCP および UDP	入力 / 出力	他のクラスタノードと DNS サーバー

サービス	ポート	プロトコル	方向 イン：クラスタに向かう アウト：クラスタからファブリックまたは外に向かう	接続
GRPC（テレメトリ）	33000	TCP	入力	Nexus Dashboard 永続 IP に関連付けられた GRPC トランスポートを介して SAN データ (ストレージ、ホスト、フローなど) を受信する SAN Telemetry サーバー。
HTTPS	443	TCP	発信	スイッチと APIC および NX-OS の帯域内
HTTPS（vCenter、Kubernetes、OpenStack、Discovery）	443	TCP	発信	Nexus Dashboard は、VMware vCenter や OpenStack などの登録済み VMM ドメインと、Kubernetes などのコンテナ オーケストレーターから取得した情報を関連付けることにより、統合されたホストおよび物理ネットワーク トポロジ ビューを提供します。 これはオプションの機能です。
ICMP	ICMP	ICMP	入力 / 出力	他のクラスタ ノード、デフォルト ゲートウェイ

サービス	ポート	プロトコル	方向 イン：クラスタに向かう アウト：クラスタからファブリックまたは外に向かう	接続
インフラサービス	3379 3380 8989 9090 9969 9979 9989 15223 30002 ～ 30006 30009 ～ 30010 30012 30014-30015 30018-30019 30025 30027	TCP	入力 / 出力	その他のクラスタ ノード
インフラサービス	30016 30017	TCP および UDP	入力 / 出力	その他のクラスタ ノード
インフラサービス	30019	UDP	入力 / 出力	その他のクラスタ ノード
インフラサービス	30500 ～ 30600	TCP および UDP	入力 / 出力	その他のクラスタ ノード
KMS	9880	TCP	入力 / 出力	その他クラスタ ノードおよび ACI ファブリック
NFSv3	111	TCP および UDP	入力 / 出力	リモート NFS サーバー

サービス	ポート	プロトコル	方向 ィン：クラスタに向かう アウト：クラスタからファブリックまたは外に向かう	接続
NFSv3	608	UDP	入力 / 出力	リモート NFS サーバー
NFSv3	2049	TCP	入力 / 出力	リモート NFS サーバー
NX-API	8443	TCP	入力 / 出力	NX-OS リリース 9.x 以降を搭載した Cisco MDS 9000 シリーズ スイッチでパフォーマンス モニタリングに使用されます。
SCP	22	TCP	入力 / 出力	SCPは、リモートサーバーへのバックアップファイルのアーカイブなど、デバイスと Nexus Dashboard の間でファイルを転送するさまざまな機能によって使用されます。Nexus Dashboard SCP サービスは、ダウンロードとアップロードの両方の SCP サーバーとして機能します。SCP は、POAP 関連ファイルをダウンロードするために、デバイス上の POAP クライアントによっても使用されます。 Nexus Dashboard の SCP-POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続 IP アドレスがあります。これは、Nexus Dashboard サーバー設定の **[LAN デバイス管理接続（LAN Device Management Connectivity）]** 設定によって制御されます。

サービス	ポート	プロトコル	方向 イン：クラスタに向かう アウト：クラスタからファブリックまたは外に向かう	接続
SCP	22	TCP	発信	Nexus Dashboard POAP-SCP ポッドの永続 IP アドレスから、テレメトリを実行している別の ND クラスターにテクニカルサポート ファイルを転送します。 Nexus Dashboard の SCP-POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続 IP アドレスがあります。これは、NDFC サーバー設定の **[LAN デバイス管理接続（LAN Device Management Connectivity）]** 設定によって制御されます。
SMTP	25	TCP	発信	SMTPポートは、**[管理（Admin）>] [サーバー設定（Server Settings）] > [全般（General）]**ページで設定できます。 これはオプションの機能です。
SNMP	161	TCP および UDP	アウト	Nexus Dashboard からデバイスへの SNMP トラフィック。
SNMP トラップ	2162	UDP	入力	デバイスから Nexus Dashboard への SNMP トラップは、SNMP-Trap/Syslog サービス ポッドに関連付けられた永続 IP アドレスに向けて送信されます。 Nexus Dashboard の SNMP-Trap-Syslog サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続 IP アドレスがあります。これは、NDFC サーバー設定の **[LAN デバイス管理接続（LAN Device Management Connectivity）]** 設定によって制御されます。
SSH	22	TCP	発信	スイッチと APIC の帯域内

サービス	ポート	プロトコル	方向 イン：クラスタに向かう アウト：クラスタからファブリックまたは外に向かう	接続
SSH	1022	TCP および UDP	入力 / 出力	その他のクラスタ ノード
Syslog	514	UDP	入力	Nexus Dashboard が Syslog サーバーとして構成されている場合、デバイスからの syslog は、SNMP-Trap/Syslog サービス ポッドに関連付けられた永続 IP アドレスに向けて送信されます。 Nexus Dashboard の SNMP-Trap-Syslog サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続 IP アドレスがあります。これは、Nexus Dashboard サーバー設定の **[LAN デバイス管理接続（LAN Device Management Connectivity）]** 設定によって制御されます。
VXLAN	4789	UDP	入力 / 出力	その他のクラスタ ノード

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

表 *7:* 単一ノード クラスタでの *SAN* 展開向けの *Nexus Dashboard* ポート

サービス	ポート	プロトコル	方向 イン：クラスタに向かう アウト：クラスタからファブリックまたは外に向かう	接続 （特に明記されていない限り、**LAN** と **SAN** の両方の展開に適用されます）
GRPC（テレメトリ）	33000	TCP	入力	Nexus Dashboard 永続 IP に関連付けられた GRPC トランスポートを介して SAN データ (ストレージ、ホスト、フローなど) を受信する SAN Telemetry サーバー。
HTTPS（vCenter、Kubernetes、OpenStack、Discovery）	443	TCP	発信	Nexus Dashboard は、VMware vCenter や OpenStack などの登録済み VMM ドメインと、Kubernetes などのコンテナ オーケストレーターから取得した情報を関連付けることにより、統合されたホストおよび物理ネットワーク トポロジ ビューを提供します。 これはオプションの機能です。
SCP	22	TCP	入力 / 出力	SCPは、リモートサーバーへのバックアップファイルのアーカイブなど、デバイスと Nexus Dashboard の間でファイルを転送するさまざまな機能によって使用されます。Nexus Dashboard SCP サービスは、ダウンロードとアップロードの両方の SCP サーバーとして機能します。SCP は、POAP 関連ファイルをダウンロードするために、デバイス上の POAP クライアントによっても使用されます。 Nexus Dashboard の SCP-POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続 IP アドレスがあります。これは、Nexus Dashboard サーバー設定の **[LAN デバイス管理接続（LAN Device Management Connectivity）]** 設定によって制御されます。

サービス	ポート	プロトコル	方向 イン：クラスタに向かう アウト：クラスタからファブリックまたは外に向かう	接続 （特に明記されていない限り、**LAN** と **SAN** の両方の展開に適用されます）
SCP	22	TCP	発信	Nexus Dashboard POAP-SCP ポッドの永続 IP アドレスから、テレメトリを実行している別の ND クラスターにテクニカル サポート ファイルを転送します。 Nexus Dashboard の SCP-POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続 IP アドレスがあります。これは、NDFC サーバー設定の **[LAN デバイス管理接続（LAN Device Management Connectivity）]** 設定によって制御されます。
SMTP	25	TCP	発信	SMTPポートは、**[管理（Admin）>] [サーバー設定（Server Settings）]>[全般（General）]**ページで設定できます。 これはオプションの機能です。
SNMP	161	TCP および UDP	アウト	Nexus Dashboard からデバイスへの SNMP トラフィック。
SNMP トラップ	2162	UDP	入力	デバイスから Nexus Dashboard への SNMP トラップは、SNMP-Trap/Syslog サービス ポッドに関連付けられた永続 IP アドレスに向けて送信されます。 Nexus Dashboard の SNMP-Trap-Syslog サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続 IP アドレスがあります。これは、NDFC サーバー設定の **[LAN デバイス管理接続（LAN Device Management Connectivity）]** 設定によって制御されます。

サービス	ポート	プロトコル	方向 イン：クラスタに向かう アウト：クラスタからファブリックまたは外に向かう	接続 （特に明記されていない限り、**LAN** と **SAN** の両方の展開に適用されます）
SSH	22	TCP	発信	SSH は、デバイスにアクセスするための基本的なメカニズムです。
Syslog	514	UDP	入力	Nexus Dashboard が Syslog サーバーとして構成されている場合、デバイスからの syslog は、SNMP-Trap/Syslog サービス ポッドに関連付けられた永続 IP アドレスに向けて送信されます。 Nexus Dashboard の SNMP-Trap-Syslog サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続 IP アドレスがあります。これは、Nexus Dashboard サーバー設定の **[LAN デバイス管理接続（LAN Device Management Connectivity）]** 設定によって制御されます。

Nexus Dashboardの 永続 IP アドレス

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

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

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

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

リリース 4.x での永続 IP アドレスの更新

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

- 必要な IP アドレス数の削減

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

- LAN デバイスの接続性

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

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

- テレメトリのためのレイヤ 3 永続 IP サポート

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

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

LAN 展開：

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

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

SAN 展開：

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

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

新規インストールまたはアップグレード

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

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

留意すべきその他の考慮事項

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

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

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

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

マッピングの更新

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

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

必要な永続 IP アドレスの合計数の決定

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

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

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

新規インストール

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

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

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

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

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

表 *8 :* 永続的な *IP* 要件：*4.x* の新規インストール

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

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

アップグレード：

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

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

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

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

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

表 *9 :* 永続 *IP* の要件：*3.2.x* から *4.x* へのアップグレード

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

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

BGP 構成と永続的な IP アドレス

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

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

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

- ピア ルータが、ノードのレイヤ 3 ネットワーク間でアドバタイズされた永続的 IP アドレスを交換することを確認します。
- データ ネットワークのレイヤ3 隣接関係については、ブートストラップ プロセス中に BGP を構成する必要があります。BGP は管理ネットワークのレイヤ3 隣接関係をサポートしません。
- 割り当てる永続的な IP アドレスが、ノードの管理サブネットまたはデータ サブネットと重複しないようにしてください。

ラウンド トリップ時間の要件

両方のネットワークでノード間の接続が必要です。そして、表示に示されているラウンド トリップ時間（RTT）要件があります。

表 *10 :* クラスタのラウンド トリップ時間の要件

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

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

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

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

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

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

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

主なワークロードの特徴

主なワークロードの特徴は次のとおりです。

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

基準ストレージ要件

基準ストレージ要件は次のとおりです。

容量

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

パフォーマンス

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

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

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

ストレージの設計に関する推奨事項

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

ストレージ メディアの選択と配置

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

リモート ストレージまたは共有ストレージの使用

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

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

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

キャッシング

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

ファブリック接続

ここでは、Nexus Dashboard クラスタ ノードを管理とデータ ネットワークに接続し、クラスタをファブリックに接続する方法について説明します。インバンドテレメトリ機能を有効にするためのファブリックの構成の詳細については、次のドキュメントを参照してください。

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

オンプレミス APIC または NDFC ファブリックの場合、Nexus ダッシュボード クラスタは次の 2 つの方法のいずれかで接続できます。

- レイヤ 3 ネットワーク経由でファブリックに接続された Nexus Dashboard クラスタ。
- リーフ スイッチに接続された Nexus Dashboard ノードは、一般的なホストです。

外部レイヤ 3 ネットワークを介した接続

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

- Cisco ACI ファブリックを管理するために Nexus Dashboard Orchestrator を使用する場合は、データ インターフェイスまたは管理インターフェイスから各ファブリックの APIC のイン

バンドまたはアウトオブバンド（OOB）インターフェイスまたは両方への接続を確立できます。

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

- テレメトリを使用する場合は、データ インターフェイスから各ファブリックおよび APIC のインバンド ネットワークへの接続を確立する必要があります。

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

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

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

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

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

次の 2 つの図は、Nexus Dashboard クラスタをレイヤ 3 ネットワーク経由でファブリックに接続する場合の 2 つの異なるネットワーク接続シナリオを示しています。最初の図は ACI と NX-OS ファブリック混在、2 番目の図は ACI ファブリックのみの場合です。

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

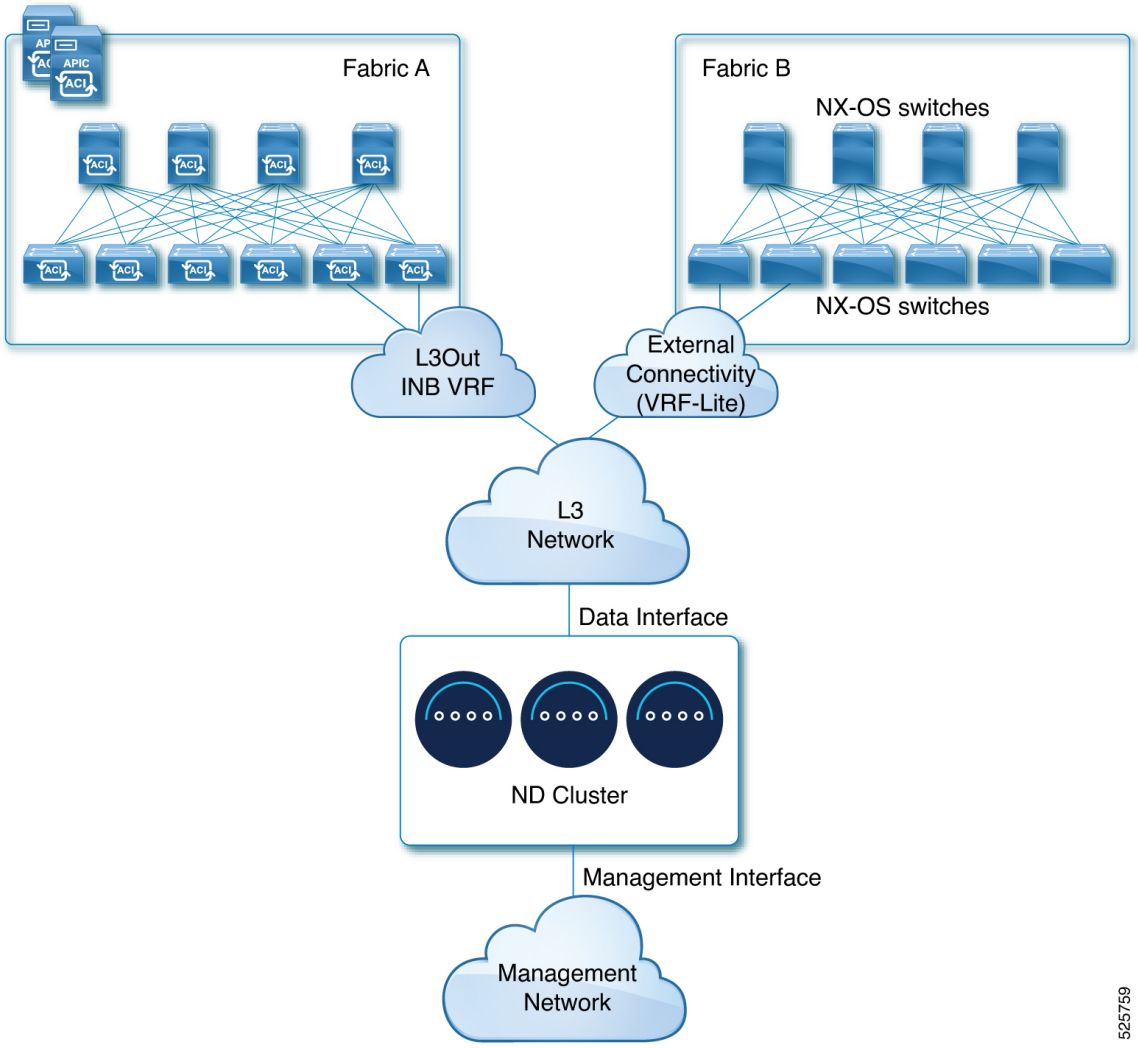
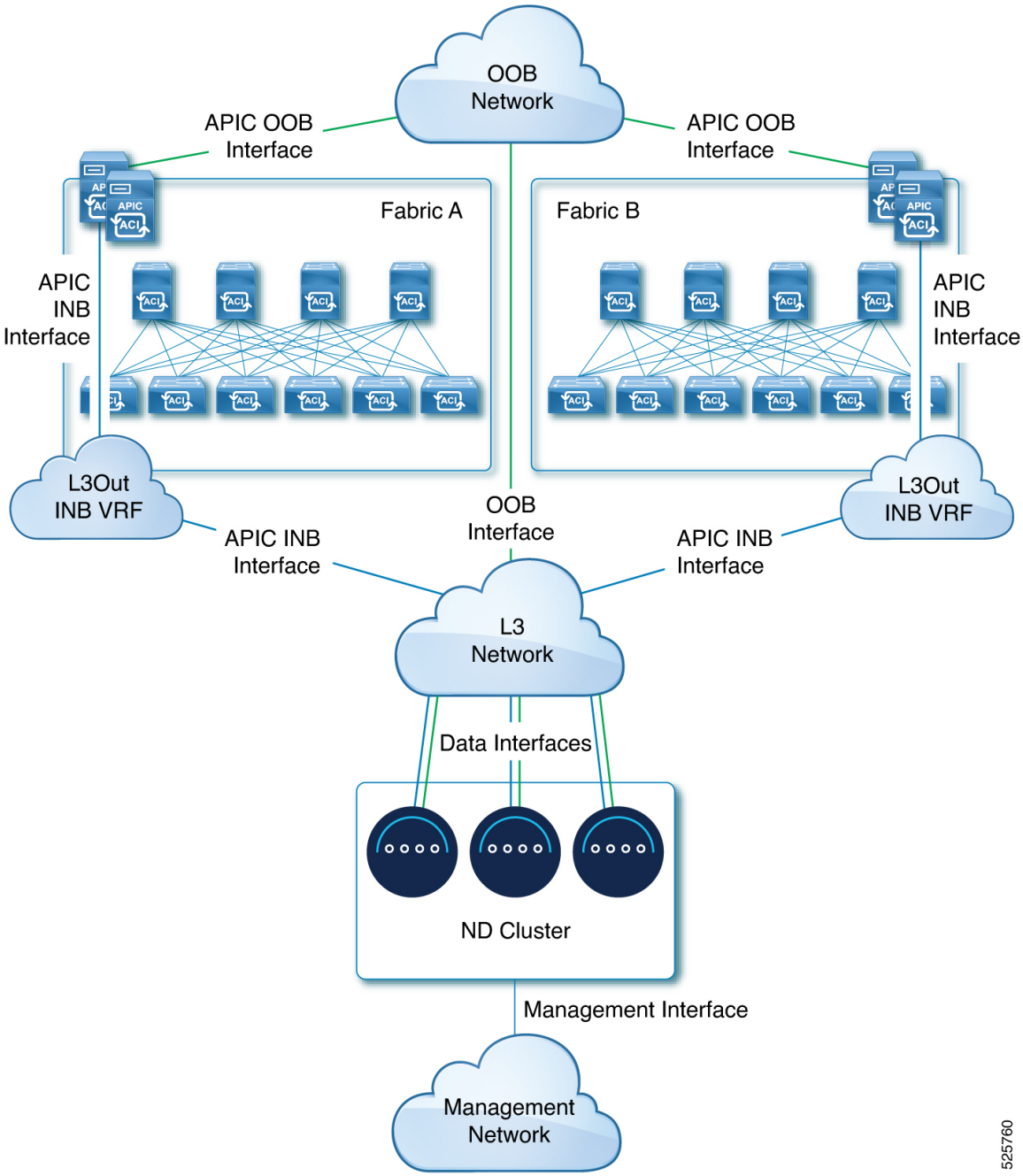


図 *2 : ACI*ファブリックのみを使用したレイヤ *3* ネットワークを使用した接続



リーフ スイッチへのノードの直接接続

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

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

- Cisco ACI ファブリックを管理するために Nexus Dashboard Orchestrator を使用する場合は、データ インターフェイスまたは管理インターフェイスから各ファブリックの APIC のインバンドまたはアウトオブバンド（OOB）インターフェイスまたは両方への接続を確立できます。

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

- テレメトリを使用する場合は、データ インターフェイスから各ファブリックの APIC のインバンドまたはアウトオブバンド（OOB）インターフェイスへの接続を確立できます。ただし、データインターフェイスからアウトオブバンドインターフェイスへの接続を確立する場合は、ルートを追加する必要があります。

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

クラスタをリーフスイッチに直接接続する場合は、次の点に注意してください。

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

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

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

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

- APIC 側の設定では、次には必要な設定があります。

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

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

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

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

次の図は、これらのタイプの接続を示しています。

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

図 *3 : ACI* ファブリックに直接接続

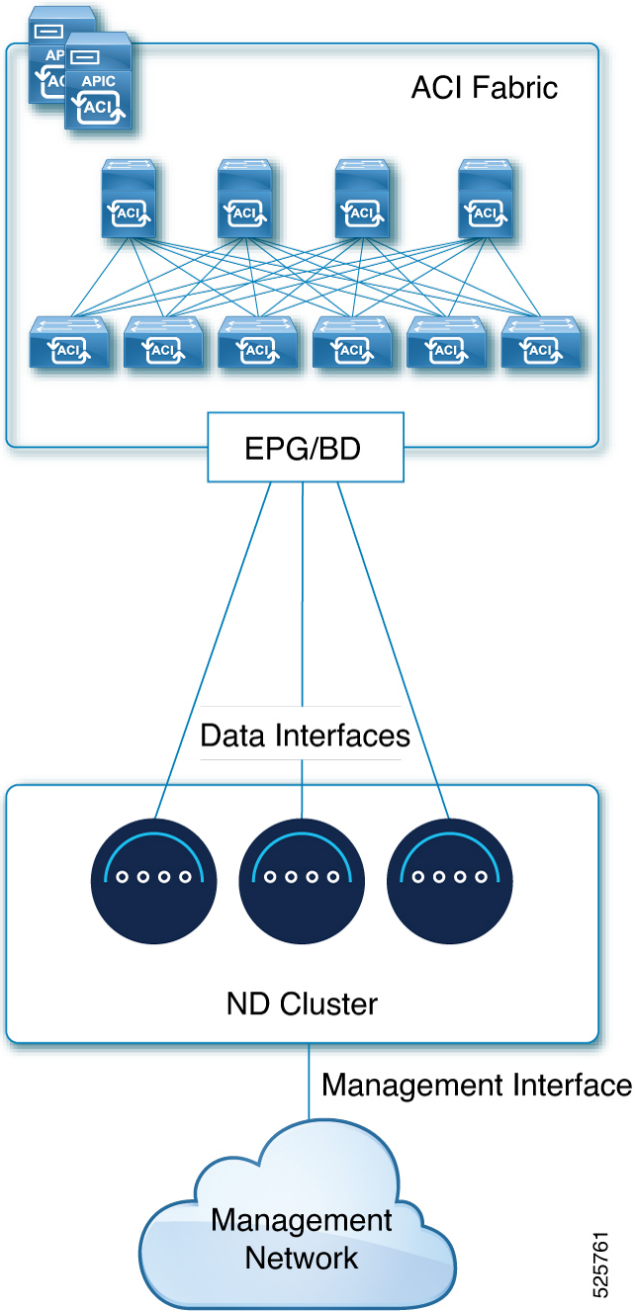


図 *4 : NX- OS* ファブリックに直接接続

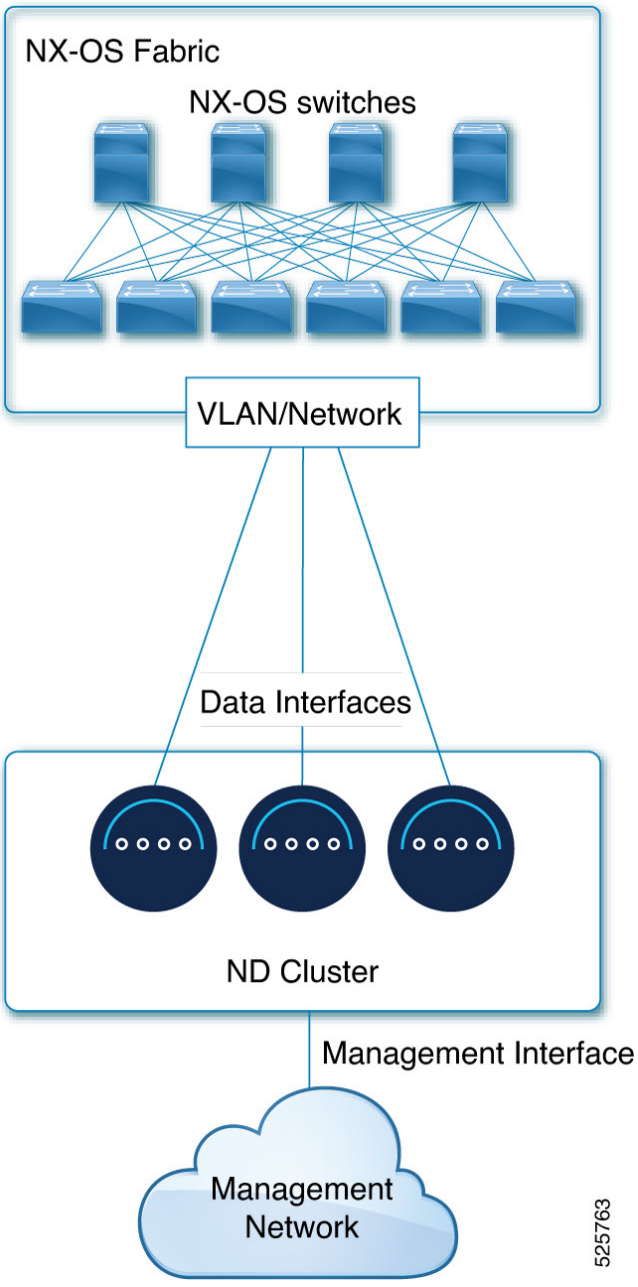
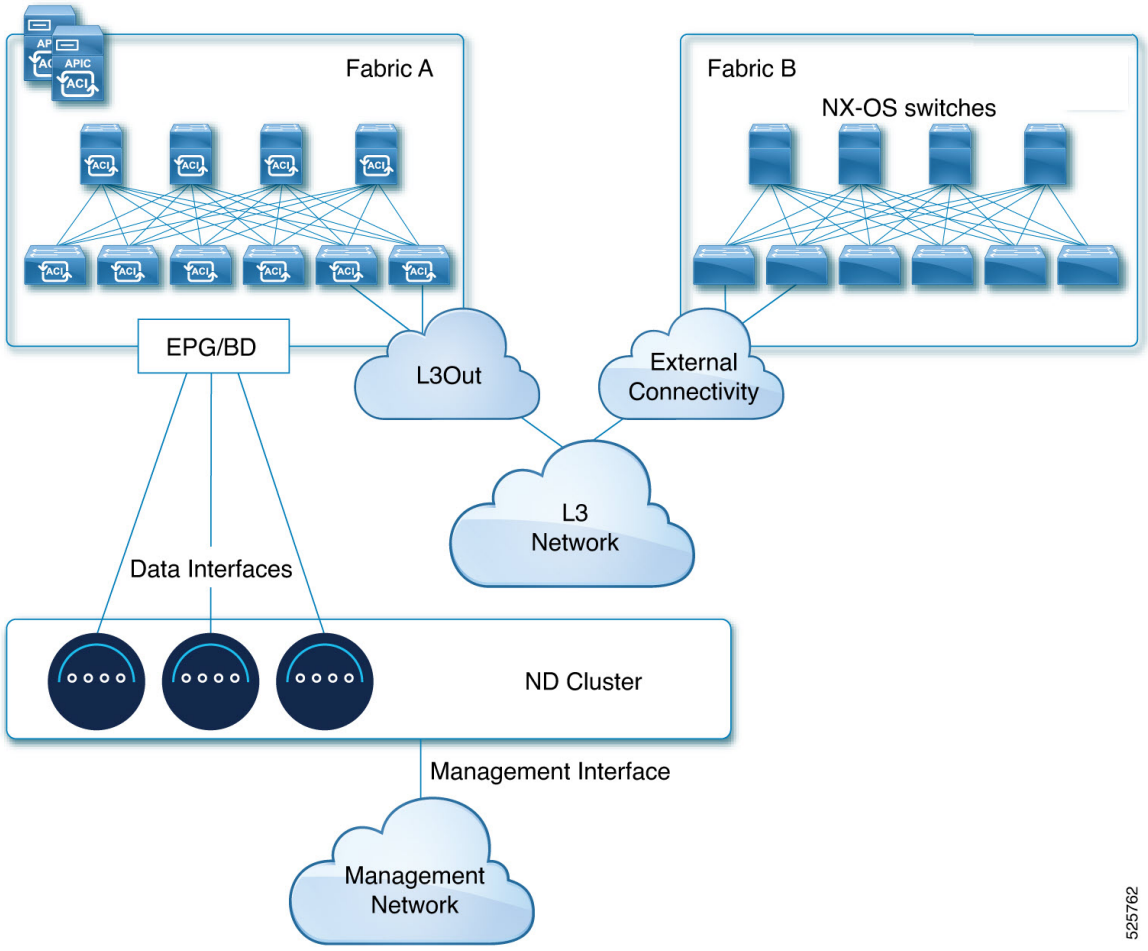


図 *5 : ACI* および *NX- OS* ファブリックに直接接続

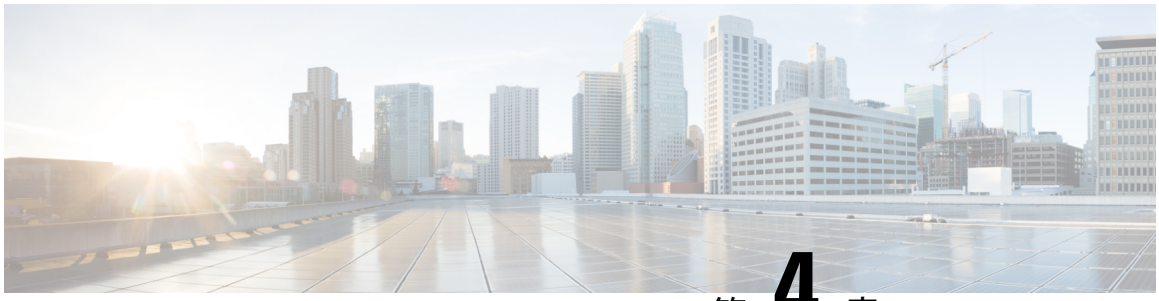




第 II 部

クラスタの展開

- インストール前のチェックリスト （75 ページ）
- 物理アプライアンスとしての展開 （81 ページ）
- VMware ESX の展開 （145 ページ）
- Linux KVMでの展開 （179 ページ）
- Nutanix での仮想 Nexus Dashboard（vND）の展開 （203 ページ）
- Amazon Web Services（AWS）での仮想 Nexus Dashboard（vND）の展開 （239 ページ）



第 4 章

インストール前のチェックリスト

• インストール前チェックリスト （75 ページ）

インストール前チェックリスト

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

表 *11* : クラスタの詳細

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

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

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

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

表 *12 :* ノードの詳細

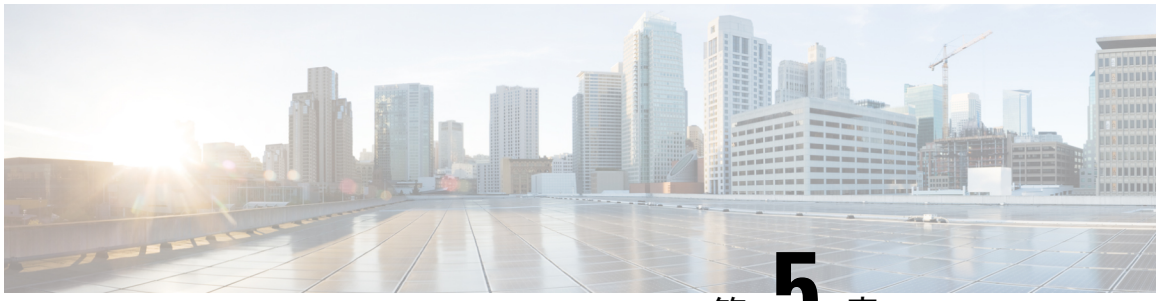
パラメータ（Parameters）	例	入力する値
物理ノードの場合、最初のノードの **CIMC** アドレスとログイン情報	10.196.220.84/24 ユーザ名: admin パスワード：Cisco1234	
物理ノードの場合、2 番目のノードの **CIMC** アドレスとログイン情報	10.196.220.85/24 ユーザ名: admin パスワード：Cisco1234!	
物理ノードの場合、3 番目のノードの **CIMC** アドレスとログイン情報	10.196.220.86/24 ユーザ名: admin パスワード：Cisco1234!	
各ノードのレスキュー ユーザに使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

パラメータ（**Parameters**）	例	入力する値
最初のノードの **管理 IP**	192.168.11.172/24	
最初のノードの**管理ゲートウェイ**	192.168.11.1	
最初のノードの**データ ネットワーク IP**	192.168.8.172/24	
最初のノードの**データ ネットワーク ゲートウェイ**	192.168.8.1	
（オプション）最初のノードの**データ ネットワーク VLAN**（アップストリーム スイッチ ポートの設定が「トランク」で、 VLANがトランク許可リストに追加されている場合にのみ、 VLAN を入力します）	101	
（オプション）BGP を有効にする場合、最初のノードの **ASN**	63331	
（オプション）BGP を有効にし、IPv6 専用の展開を使用する場合、最初のノードの**ルータ ID**（IPv4 アドレスの形式）	1.1.1.1	
（オプション）BGP を有効にする場合、最初のノードの **BGP ピア**の IP アドレス	200.11.11.2	
（オプション）BGP を有効にする場合、最初のノードの **BGP ピア**の ASN	55555	
2 番目のノードの**管理 IP**	192.168.9.173/24	
2 番目のノードの**管理ゲートウェイ**。	192.168.9.1	
2 番目のノードの**データ ネットワーク IP**	192.168.6.173/24	
2 番目のノードの**データ ネットワーク ゲートウェイ**	192.168.6.1	

パラメータ（**Parameters**）	例	入力する値
（オプション）2番目のノードの**データ ネットワーク VLAN**	101	
（オプション）BGP を有効にする場合、2 番目のノードの**ASN**	63331	
（オプション）BGP を有効にし、IPv6 専用の展開を使用する場合、2番目のノードの**ルータ ID**（IPv4 アドレスの形式）	2.2.2.2	
（オプション）BGP を有効にする場合、2 番目のノードの**BGP ピア**の IP アドレス	200.12.12.2	
クラスタ接続（L2/BGP）	L2	
（オプション）BGP を有効にする場合、2 番目のノードの**BGP ピア**の ASN	55555	
3 番目のノードの**管理 IP**	192.168.9.174/24	
3 番目のノードの**管理ゲートウェイ**。	192.168.9.1	
3 番目のノードの**データ ネットワークIP**	192.168.6.174/24	
3 番目のノードの**データ ネットワーク ゲートウェイ**	192.168.6.1	
（オプション）3番目のノードの**データ ネットワーク VLAN**	101	
（オプション）BGP を有効にする場合、3 番目のノードの**ASN**	63331	
（オプション）BGP を有効にし、IPv6 専用の展開を使用する場合、**ルータ ID**（IPv4 アドレスの形式）	3.3.3.3	

パラメータ（Parameters）	例	入力する値
（オプション）BGP を有効にする場合、3 番目のノードの **BGP ピア**の IP アドレス	200.13.13.2	
（オプション）BGP を有効にする場合、3 番目のノードの **BGP ピア**の ASN	55555	

また、クラスターの起動中に永続的な IP アドレスをプログラムする必要があります。詳細については、「Nexus Dashboardの 永続 IP アドレス （52 ページ）」を参照してください。



第 5 章

物理アプライアンスとしての展開

- 物理アプライアンスとして Nexus Dashboard を展開する場合の前提条件と注意事項 （81 ページ）
- 物理アプライアンスの概要とケーブル接続 （84 ページ）
- 物理アプライアンスとしての Nexus Dashboard の展開 （134 ページ）

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

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

- 前提条件とガイドライン（13 ページ）に記載されている前提条件を確認して完了します：
- デプロイメントに影響する可能性のある情報については、 *Cisco Nexus Dashboard*のリリースノートを確認してください。Cisco Nexus Dashboard のドキュメントのランディング ページを参照してください。
- 使用しているサーバーのモデルに対応した、*Cisco Nexus Dashboard* ハードウェア セットアップ ガイドの説明に従って、以下のハードウェアを使用しており、サーバがラックに接続されていることを確認します。

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

  - `SE-NODE-G2` （UCS-C220-M5）。3 ノード クラスター シャーシの製品 ID は、`SE-CL-L3` です。
  - `ND-NODE-L4` （UCS-C225-M6）。3 ノード クラスター シャーシの製品 ID は、`ND-CLUSTER-L4` です。
  - `ND-NODE-G5S` (UCS-C225-M8)。3 ノードクラスター シャーシの製品 ID は `ND-CLUSTERG5S` です。
  - `ND-NODE-G5S` (UCS-C225-M8)。3 ノードクラスター シャーシの製品 ID は `ND-CLUSTERG5L` です。

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

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

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

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

  Cisco Integrated Management Controller IP アドレスの構成 （83 ページ）を参照してください。

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

  Cisco Integrated Management Controller に対する Serial over LAN の有効化 （84 ページ）を参照してください。

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

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

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

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

  たとえば、受け取ったハードウェアにリリース 3.2.1 のイメージがプリインストールされているが、代わりにリリース 4.3.1 を展開する場合は、次の手順に従います：

  1. 最初に、リリース 3.2.1 クラスタをそのリリースの展開ガイドに従って起動します。
  2. 次に、「Nexus Dashboard 3.2.2m クラスタのこのリリースへのアップグレード （259 ページ）」の説明に従って、リリース「4.3.1 」にアップグレードします。

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

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

Cisco Integrated Management Controller IP アドレスの構成

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

手順

ステップ 1 サーバの電源をオンにします。

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

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

ステップ 3 次のサブステップに従います。

a) **NIC モード**を専用モードに設定します。

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

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

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

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

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

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

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

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

手順

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

ステップ 2 次のコマンドを実行します。

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

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

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

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

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

物理アプライアンスの概要とケーブル接続

このセクションでは、サポートされているこれらの Nexus Dashboard 物理アプライアンスの概要とケーブル接続について説明します。

ND-NODE-G5S（UCS-C225-M8）。

これらのセクションでは、`ND-NODE-G5L` （UCS-C225-M8）物理アプライアンスの概要とケーブル接続に関する情報を提供します。

ND-NODE-G5L（UCS-C225-M8）について

このセクションでは、ND-NODE-G5L（UCS-C225-M8）物理アプライアンスの概要について説明します。

ND-NODE-G5L 物理アプライアンスは、 UCS C225 M8 サーバに基づくNexus Dashboard アプライアンスです。Nexus Dashboard ND-NODE-G5L は UCS C225 M8 サーバに基づいていますが、ベースの UCS C225 M8 サーバのようにNexus Dashboard ND-NODE-G5L 内のコンポーネントを交換することはできません。代わりに、 Nexus Dashboard ND-NODE-G5L 内のコンポーネントに障害がある場合は、アプライアンスの返品許可（RMA）操作を実行します。

Nexus Dashboard ND-NODE-G5L は UCS C225 M8 サーバに基づいているため、そのドキュメントの次の章に記載されている情報など、Nexus Dashboard D-NODE-G5L にも適用される重要な UCS *C225 M8* サーバ情報については、『*Cisco UCS C225 M8 Server Installation and Service Guide*』を参照できます。。

- 概要
- サーバーのインストール
- サーバの仕様
- ストレージ コントローラの考慮事項

ただし、 Nexus Dashboard ND-NODE-G5L 内のコンポーネントをベースのUCS C225 M8 サーバのように交換することはできないため、そのドキュメントの次の章はNexus Dashboard ND-NODE-G5L には適用されず、無視する必要があります。

- サーバーの保守
- サーバ コンポーネントのリサイクル
- Cisco UCS Manager 統合に適した設置方法
- GPU の取り付け

次のセクションでは、 Nexus Dashboard ND-NODE-G5Lに適用される情報を提供します。

概要

Cisco Nexus Dashboard は、シスコ データセンター アプリケーションを展開するための共通プラットフォームを提供します。これらのアプリケーションは、ポリシーとインフラストラクチャのリアルタイム分析、可視性、および保証を提供します。

Cisco Nexus Dashboard アプリケーションは、Cisco Nexus Dashboard アプリケーションをインストールしてホストするために必要です。

このアプライアンスでは次のバージョンを構成可能です。

- **ND-NODE-G5L**：シングル ノード アプライアンス
- **ND-CLUSTERG5L**：ND-NODE-G5L と同じ構成を活用するが、3 つのアプライアンスが含まれる 3 ノードバージョン

コンポーネント

ND-NODE-G5Lアプライアンスは、次のコンポーネントで構成されています。

- **ND-M8-MLB**：ND M8 ラック MLB
- **ND-C225-M8S**：UCS C225 M8 ラック（CPU、メモリ、ドライブなし、SFF HDD/ SSD バックプレーン付きの 1U フォームファクタ）
- **CIMC-LATEST-D**：C シリーズ サーバー向け IMC SW（推奨）最新リリース
- **CON-L1NCO-UCSC5M8S**：CX LEVEL 1 8X7XNCDOS UCS C225 M8 Rack w/o CPU mem DRV 1U W
- **ND-RAIL-D**：C220 およびC240 M7/M8 ラック サーバ用ボールベアリング レールキット）
- **ND-CPU-A9655P**：AMD 9655P 2.6GHz 400W 96C/384MB キャッシュ DDR5 6000MT/s
- **ND-M2-I240GB-D**：240GB M.2 ブート SATA Intel SSD
- **ND-M2-HWRAID-D**：ND Cisco ブート最適化 M.2 RAID コントローラ
- **ND-TPM2-002D-D**：ND TPM 2.0 FIPS 140-2 MSW2022 準拠 AMD M8 サーバー
- **ND-RIS1A-225M8**：ND C225 M8 1U Riser 1A PCIe Gen4 x16 HH
- **ND-HD24TB10KJ4-D**：ND 2.4TB 12G SAS 10K RPM SFF HDD（4Kn）
- **ND-SD960GBM3XEPD**：ND 960GB 2.5 インチ Enter Perf 6G SATA Micron G2 SSD (3X)
- **ND-SD32TKA3XEP-D**：3.2TB 2.5 インチ Enter Perf 24G SAS Kioxia PM7 SSD (3X)
- **ND-M-V5Q50GV2-D**：Cisco VIC 15427 4x 10/25/50G mLOM C シリーズ（セキュア ブート付き）
- **ND-FBRS2-C225M8**：C225 M8 Riser2 HH フィラー ブランク
- **ND-FBRS-C220-D**：C220M7 HH ライザー 3 ブランク
- 電源モジュール：
  - C シリーズ サーバー用の 1200W AC チタニウム電源
  - UCS ラック サーバー用 1050W -48V DC 電源
  - APIC サーバー用 1050W -48V DC 電源ユニット（インド）
- **ND-MRX64G2RE5**：64GB DDR5-6400 RDIMM 2Rx4（16Gb）
- **ND-RAID-M1L16**: ND 24G トライモード M1 RAIDコントローラ（4GB FBWC 16Drv 付き）
- **ND-P-ID10GC-D**：Cisco - Intel X710T2LG 2x10 GbE RJ45 PCIe NIC
- **ND-HSLP-C225M8**：ND C225 M8 ヒートシンク
- **ND-BBLKD-M8**：UCS C シリーズ M6 & M8 SFF ドライブ ブランク パネル

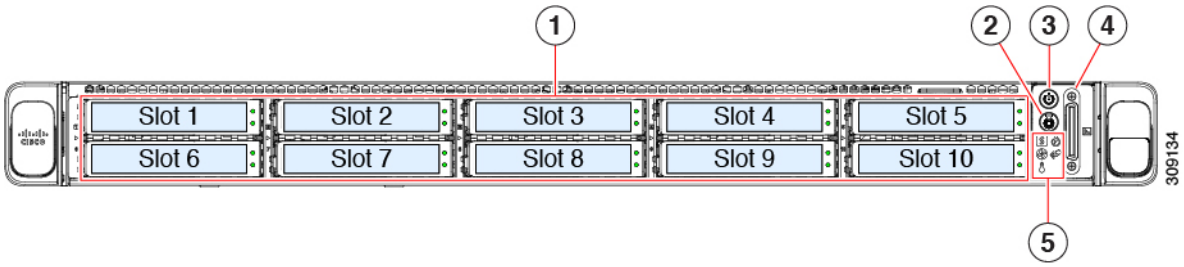
- **ND-DDR5-BLK**：ND DDR5 DIMM ブランク
- **ND-PSU-BLK-D**：M7/M8 サーバ用電源ブランク パネル
- **ND-HPBKT-225M8**：C225 M8 トライモード 24G SAS RAID コントローラ ブラケット
- **CBL- SAS-C225M8**：C225M8 SAS ケーブル、メイン ボードから RAID カード
- **NO-POWER-CORD**：環境に優しいグリーン オプション、電源ケーブルは出荷されません
- **ND-DLOM-01-D**：C シリーズ サーバ用専用モード BIOS 設定
- **CNDL-DESELECT-D**：条件付き選択解除
- **OPTOUT-ENTL-SWAP**：ライセンスは不要：スマートアカウントで権限が更新される

外部機能

ND-NODE-G5L 前面パネルの機能

次の図に、小型フォームファクタのドライブ バージョンのサーバの前面パネルの機構を示します。

図 *6 : ND-NODE-G5L* 前面パネル



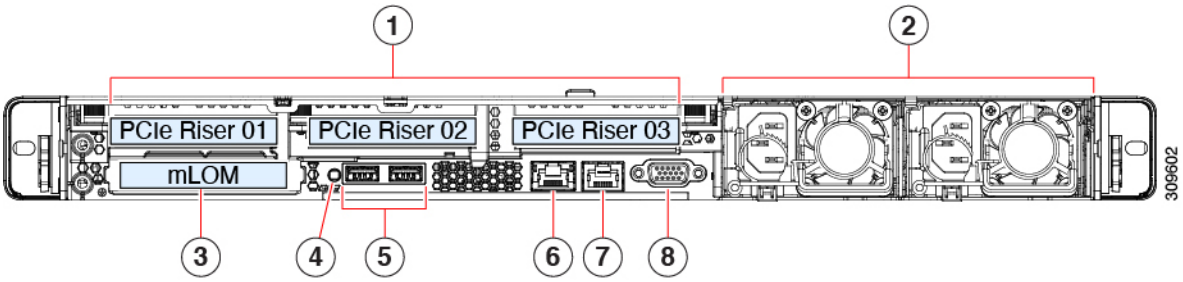
1	ドライブ ベイ 1 ～ 10 は SAS/SATA ハード ディスク ドライブ（HDD）およびソリッド ステート ドライブ（SSD）をサポート。	**2**	ユニット識別ボタン/LED
3	電源ボタン/電源ステータス LED	**4**	KVM コネクタ（1 つの DB-15 VGA コネクタ、1 つの DB-9 シリアルコネクタ、および 2 つの USB 2.0 コネクタを備えた KVM ケーブルで使用）
5	システム LED クラスタ： • ファン ステータス LED • システム ステータス LED • 電源装置ステータス LED • ネットワーク リンク アクティビティ LED • 温度ステータス LED		-

ND-NODE-G5L 背面パネルの機能

背面パネルの機能は、サーバー内の PCIe カードの数とタイプによって異なります。

次の図は、3 ライザー構成のサーバーの背面パネルの機能を示しています。

図 *7*: *ND-NODE-G5L* 背面パネルの *3* ライザーの構成



1	PCIe スロット 3 HH ライザー ケージ構成では、次の PCIe ライザーの組み合わせを使用できます。 • **ライザー 1** : • ライザー 1A（PCIe Gen4） : ハーフハイト、3/4 長、x16。		
2	電源ユニット（PSU）2 台。1+1 電源モードで構成されている場合には冗長化できます。	**3**	モジュラ LAN-on-motherboard（mLOM）カードベイ（x16 PCIe レーン）
4	システム ユニット識別ボタン/LED	**5**	USB 3.0 ポート（2 個）
6	1 GB イーサネット専用管理ポート	**7**	COM ポート（RJ45 コネクタ）
8	VGA ビデオ ポート（DB-15 コネクタ）		

ステータス LED およびボタン

ここでは、前面、背面、および内部の LED の状態について説明します。

前面パネルの LED

図 *8* : 前面パネルの *LED*

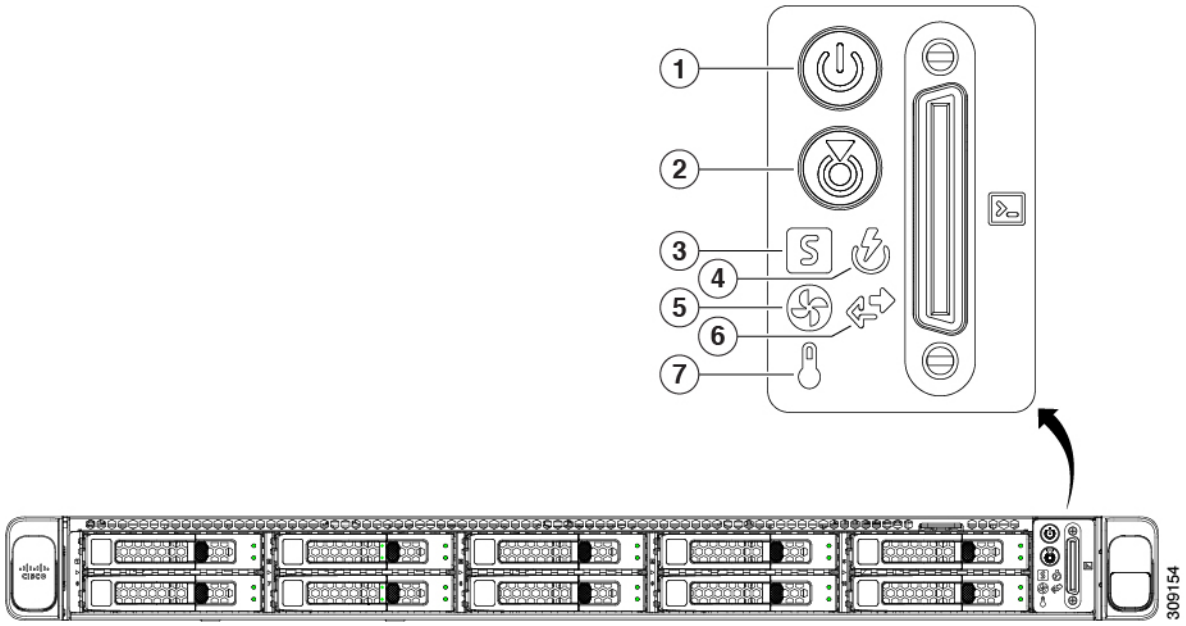


表 *13* : 前面パネル *LED*、状態の定義

	LED 名	状態
1	電源ボタン/LED（）	• 消灯：サーバに AC 電力が供給されていません。 • オレンジ：サーバはスタンバイ電源モードです。Cisco IMC と一部のマザーボード機能にだけ電力が供給されています。 • 緑：サーバは主電源モードです。すべてのサーバコンポーネントに電力が供給されています。
2	ユニット識別（）	• 消灯：ユニット識別機能は使用されていません。 • 青の点滅：ユニット識別機能がアクティブです。

3	システムの状態（）	• 緑：サーバは正常動作状態で稼働しています。 • 緑の点滅：サーバーはシステムの初期化とメモリチェックを行っています。 • オレンジの点灯：サーバは縮退運転状態にあります（軽度な障害）。次に例を示します。 • 電源装置の冗長性が失われている。 • CPU が一致しない。 • 少なくとも1つのCPUに障害が発生している。 • 少なくとも 1 つの DIMM に障害が発生している。 • RAID 構成内の少なくとも 1 台のドライブに障害が発生している。 • オレンジの点滅（2回）：システムボードで重度の障害が発生しています。 • オレンジの点滅（3回）：メモリ（DIMM）で重度の障害が発生しています。 • オレンジの点滅（4回）：CPUで重度の障害が発生しています。
4	電源の状態（）	• 緑：すべての電源装置が正常に動作中です。 • オレンジの点灯：1台以上の電源装置が縮退運転状態にあります。 • オレンジの点滅：1台以上の電源装置が重大な障害発生状態にあります。
5	ファンの状態（）	• 緑：すべてのファン モジュールが正常に動作中です。 • オレンジの点滅：1つ以上のファンモジュールで回復不能なしきい値を超えました。

6	ネットワーク リンク アクティビティ（）	• 消灯：イーサネット LOM ポート リンクがアイドル状態です。 • 緑：1 つ以上のイーサネット LOM ポートでリンクがアクティブになっていますが、アクティビティは存在しません。 • 緑の点滅：1 つ以上のイーサネット LOM ポートでリンクがアクティブになっていて、アクティビティが存在します。
7	温度（）	• 緑：サーバは正常温度で稼働中です。 • オレンジの点灯：1 個以上の温度センサーで重大なしきい値を超えました。 • オレンジの点滅：1 個以上の温度センサーで回復不能なしきい値を超えました。

背面パネルの LED

図 *9* : 背面パネル *LED*

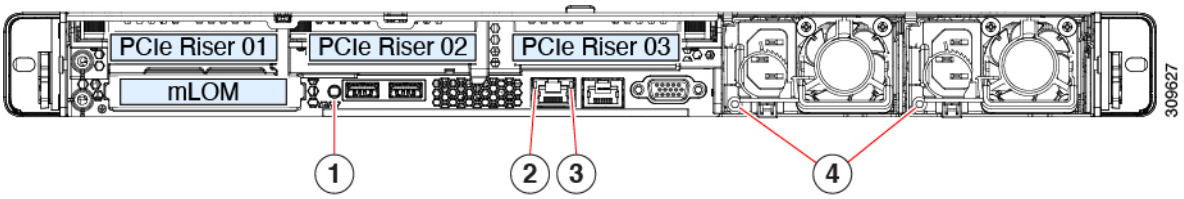


表 *14* : 背面パネル *LED*、状態の定義

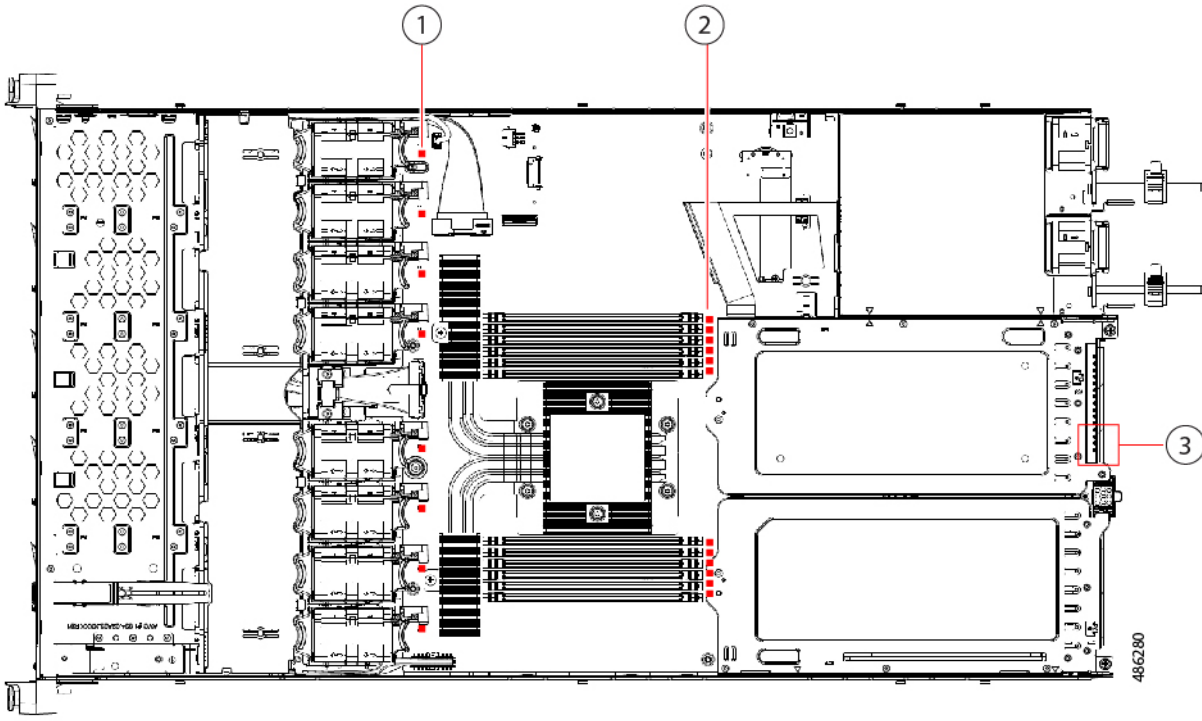
	LED 名	状態
1	背面ユニット識別	• 消灯：ユニット識別機能は使用されていません。 • 青の点滅：ユニット識別機能がアクティブです。
2	1 Gb イーサネット専用管理リンク速度	• 消灯：リンク速度は 10 Mbps です。 • オレンジ：リンク速度は 100 Mbps です。 • 緑：リンク速度は 1 Gbps です。

3	1 Gb イーサネット専用管理リンク ステータス	• 消灯：リンクが確立されていません。 • 緑：リンクはアクティブです。 • 緑の点滅：アクティブなリンクにトラフィックが存在します。
4	電源ステータス（各電源装置に 1 つの LED）	**AC 電源装置**： • 消灯：AC 入力なし（12 V 主電源はオフ、12 V スタンバイ電源オフ）。 • 緑の点滅：12 V 主電源はオフ、12 V スタンバイ電源はオン。 • 緑の点灯：12 V 主電源はオン、12 V スタンバイ電源はオン。 • オレンジの点滅：警告しきい値が検出されましたが、12 V 主電源はオン。 • オレンジの点灯：重大なエラーが検出されました。12 V 主電源はオフです（過電流、過電圧、温度超過などの障害）。 **DC 電源装置**： • 消灯：DC 入力なし（12 V 主電源はオフ、12 V スタンバイ電源はオフ）。 • 緑の点滅：12 V 主電源はオフ、12 V スタンバイ電源はオン。 • 緑の点灯：12 V 主電源はオン、12 V スタンバイ電源はオン。 • オレンジの点滅：警告しきい値が検出されましたが、12 V 主電源はオン。 • オレンジの点灯：重大なエラーが検出されました。12 V 主電源はオフです（過電流、過電圧、温度超過などの障害）。

内部診断 LED

サーバーには、CPU、DIMM、およびファンモジュールの内部障害 LED があります。

図 *10* : 内部診断 *LED* の位置

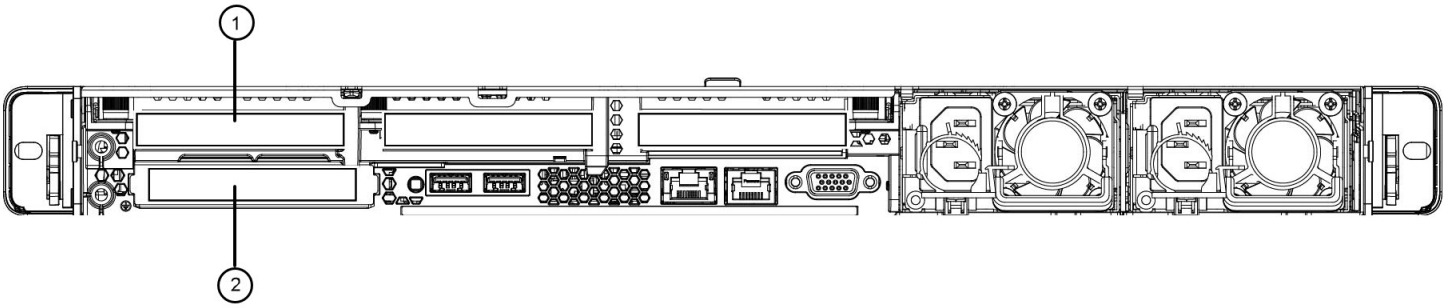


1	ファンモジュール障害 LED（マザーボード上の各ファンコネクタの後方に 1 つ） • オレンジ：ファンに障害が発生しているか、しっかりと装着されていません。 • 緑：ファンは正常です。	2	DIMM 障害 LED（マザーボード上の各 DIMM ソケットの後方に 1 つ） これらの LED は、サーバーがスタンバイ電源モードの場合にのみ動作します。 • オレンジ：DIMM に障害が発生しています。 • 消灯：DIMM は正常です。
3	CPU 障害 LED（背面 USB2 コネクタの横）。 これらの LED は、サーバーがスタンバイ電源モードの場合にのみ動作します。 • オレンジ：CPU に障害が発生しています。 • 消灯オフ: CPU は正常です。	-	

物理ノードのケーブル接続

`ND-NODE-G5L` （UCS-C225-M8）の物理サーバで、これらの接続を行います。

図 *11 :* ノード接続に使用される *mLOM* および *PCIe* ライザー *01* カード：*ND-NODE-G5L*（*UCS-C225-M8*）



1	**管理接続**：PCIe ライザー 01 の場所に取り付けられた UCSC-O-ID10GC PCIe カードの 2 つの MGMT ポート経由。
2	**データ接続**：UCSC-M-V5Q50GV2-D（Cisco UCS VIC 15427 Quad Port 10/25/50G CNA）モジュラーLANオンマザーボード（mLOM）では、ポートは左から右へ 1、2、3、4 の番号が付けられています。 サポートされているポート チャネル構成については、以下の「データ ネットワーク接続」情報を参照してください。

（注） ND-NODE-G5L サーバに含まれている OCP カードは、管理目的でのみ 1Gb 銅線接続をサポートします。Nexus Dashboard の他のすべてのネットワーク接続は、4 ポート VIC カード（上の図のコールアウト 2）を活用する必要があります。この VIC カードは 10/25/50Gbps をサポートしており、推奨されている SFP+ ケーブルは SFP-10G-AOC3M ですが、シスコでは 5 m と 7 m のオプションも提供しています。VIC カードでは、データ ネットワーク接続のためにサーバーごとに少なくとも 2 つの接続が必要です。これらの VIC 接続は、サポートされている任意の SFP を活用できますが、Cisco は Nexus Dashboard のシームレスな展開のためにこの接続を推奨しています。

物理ノードは、次のガイドラインに従って展開できます：

- ND-NODE-G5L には、 Nexus Dashboard 管理ネットワーク接続に使用する UCSC-O-ID10GC PCIe カード（上の図を参照）が付属しています。
- ND-NODE-G5L には、UCSC-M-V5Q50GV2-D（Cisco UCS VIC 15427 クワッド ポート 10/25/50G Converged Network Adapter（CNA））モジュール型 LAN on Motherboard（mLOM）カードも付属しており、これを使用して Nexus Dashboard データされないようにします。

（注） ノードをケーブル接続する前に、「データ ネットワーク接続」で提供される情報を使用して、データ インターフェイスの Cisco UCS VIC カードポートマッピングを確認します。データ インターフェイスは、個々のホスト側のスイッチ ポートに接続する必要があります。これらの接続のスイッチ ポート チャネルまたは vPC を構成しないでください。

- VIC でポート チャネル機能が有効になっていることを確認します。
  - `ND-NODE-L4`（UCS-C225-M6）および `ND-NODE-G5S`（UCS-C225-M8）の場合、ポート チャネル機能は工場出荷時にデフォルトで有効になっています。これらのプラットフォームでは追加の設定は不要ですが、必要に応じて、以下の手順を使用してポート チャネル機能が正しく有効になっているかを確認したり、同機能を有効にしたりすることができます。
  - `SE-NODE-G2`（UCS-C220-M5）では VIC 上のポートチャンネル機能を手動で有効にする必要があります。

1. CIMC にログインします。
2. ハンバーガー アイコンをクリックして、次の場所に移動します。

   [ネットワーキング（Networking）] > [アダプタ カード（Adapter Card）] > [全般（General）] を選択します。
3. **[アダプタ カード プロパティ（Adapter Card Properties）]** エリアでは、**[ポート チャネル（Port Channel）]** フィールドを探します。

   [ポート チャネル（Port Channel）] オプションが無効になっている（チェックボックスにチェックが入っていない）場合は、Nexus Dashboard のデプロイメント プロセスを開始する前に、その機能を有効にしてください（チェックボックスにチェックを入れてください）。

ノードを管理ネットワークおよびデータ ネットワークに接続する場合：

- インターフェイスは、アクティブ/スタンバイ モードで実行されている、データ インターフェイス用（bond0）と管理インターフェイス用（bond1）の Linux ボンドとして構成されます。
- **管理ネットワーク接続**：
  - PCIe カードで `mgmt0` および `mgmt1` を使用する必要があります。
  - すべてのポートが同じ速度（1G または 10G）である必要があります。
- **データ ネットワーク接続**：

- ND-NODE-G5L サーバでは、UCSC-M-V5Q50GV2-D（Cisco UCS VIC 15427 Quad Port 10/25/50G CNA）PCIe カードは、必要なポートチャネルの組み合わせを介して光ファイバ接続を使用する必要があります。

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

N9000 上	Nexus Dashboard アプライアンス（CIMC 経由）上
FEC AUTO	cl74
FC-FEC	cl74
FEC OFF	FEC OFF

- すべてのポートは同じ速度である必要があります（10G、25G、または 50G のいずれか）。
- データ ネットワーク接続用のケーブルを接続します。一方のケーブルを fabric0 に、もう一方のケーブルを fabric1 に接続してください。

  ND-NODE-G5L サーバの fabric0 および fabric1 は、次のポートに対応しています。

  - ポート 1 およびポート 2 は fabric0 に対応します
  - ポート 3 および ポート 4 は fabric1 に対応します

  したがって、これらのポートチャネルの組み合わせのうち、いずれかを使用することができます。

最初のデータ ケーブル（fabric0）	2 番目のデータ ケーブル（fabric1）
[Port-1]	ポート 3
[Port-1]	ポート 4
[Port-2]	ポート 3
[Port-2]	ポート 4

  ポート位置は、図 11 : ノード接続に使用される mLOM および PCIe ライザー 01 カード : ND-NODE-G5L（UCS-C225-M8） （94 ページ） を参照します。

  データ ネットワーク接続には、アクティブ スタンバイとして fabric0 と fabric1 の両方を使用できます。

注意

- これらの接続のスイッチ ポート チャネルまたは vPC を構成しないでください。上記のサポートされているペアリングは、VIC カードでのみ有効な物理ポート マッピングを識別します。
- 上記以外のポート チャネルの組み合わせを使用してデータ ネットワーク接続用の 2 本のケーブルを接続する場合、上流に位置するスイッチで MAC 移動通知が行われ、ポートがフラップします。

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

次のステップ

物理アプライアンスとしての Nexus Dashboard の展開 （134 ページ） に移動して、Nexus Dashboard を展開します。

ND-NODE-G5S（UCS-C225-M8）。

これらのセクションでは、`ND-NODE-G5S` （UCS-C225-M8）物理アプライアンスの概要とケーブル接続に関する情報を提供します。

ND-NODE-G5S（UCS-C225-M8）について

このセクションでは、`ND-NODE-G5S`（UCS-C225-M8）物理アプライアンスの概要について説明します。

`ND-NODE-G5S` 物理アプライアンスは、 UCS C225 M8 サーバに基づくNexus Dashboard アプライアンスです。Nexus Dashboard `ND-NODE-G5S` は UCS C225 M8 サーバに基づいていますが、ベースの UCS C225 M8 サーバのようにNexus Dashboard `ND-NODE-G5S` 内のコンポーネントを交換することはできません。代わりに、Nexus Dashboard `ND-NODE-G5S` 内のコンポーネントに障害がある場合は、アプライアンスの返品許可（RMA）操作を実行します。

Nexus Dashboard `ND-NODE-G5S` は UCS C225 M8 サーバに基づいているため、そのドキュメントの次の章に記載されている情報など、Nexus Dashboard `D-NODE-G5L` にも適用される重要な UCS *C225 M8* サーバ情報については、『*Cisco UCS C225 M8 Server Installation and Service Guide*』を参照できます。。

- 概要
- サーバーのインストール
- サーバの仕様

- ストレージ コントローラの考慮事項

ただし、 Nexus Dashboard ND-NODE-G5S 内のコンポーネントをベースの UCS C225 M8 サーバのように交換することはできないため、そのドキュメントの次の章はNexus Dashboard ND-NODE-G5L には適用されず、無視する必要があります。

- サーバーの保守
- サーバ コンポーネントのリサイクル
- Cisco UCS Manager 統合に適した設置方法
- GPU の取り付け

次のセクションでは、 Nexus Dashboard ND-NODE-G5Sに適用される情報を提供します。

概要

Cisco Nexus Dashboard は、シスコ データセンター アプリケーションを展開するための共通プラットフォームを提供します。これらのアプリケーションは、ポリシーとインフラストラクチャのリアルタイム分析、可視性、および保証を提供します。

Cisco Nexus Dashboard アプリケーションは、Cisco Nexus Dashboard アプリケーションをインストールしてホストするために必要です。

このアプライアンスでは次のバージョンを構成可能です。

- **ND-NODE-G5S**：シングル ノード アプライアンス
- **ND-CLUSTERG5S**：ND-NODE-G5S と同じ構成を活用するが、3 つのアプライアンスが含まれる 3 ノードバージョン

コンポーネント

ND-NODE-G5Sアプライアンスは、次のコンポーネントで構成されています。

- **CIMC-LATEST-D**：C シリーズ サーバー向け IMC SW（推奨）最新リリース
- **ND- CPU-A9454P**：ND AMD 9454P 2.75 GHz 290W 48C/256MB キャッシュ DDR5 4800MT/s
- **ND-M2-240G-D**：ND 240GB M.2 SATA Micron G2 SSD
- **ND-M2-HWRAID-D**：ND Cisco ブート最適化 M.2 RAID コントローラ
- **ND-TPM2-002D-D**：ND TPM 2.0 FIPS 140-2 MSW2022 準拠 AMD M8 サーバー
- **ND-RIS1A-225M8**：ND C225 M8 1U Riser 1A PCIe Gen4 x16 HH
- **ND-HD24TB10KJ4-D**：ND 2.4TB 12G SAS 10K RPM SFF HDD（4Kn）
- **ND-SD960GBM3XEPD**：ND 960GB 2.5 インチ Enter Perf 6G SATA Micron G2 SSD (3X)
- **ND-RAIL-D**：C220およびC240 M7/M8 ラック サーバ用ボールベアリング レールキット）
- 電源モジュール：

- C シリーズ サーバー用の 1200W AC チタニウム電源
- UCS ラック サーバー用 1050W -48V DC 電源
- APIC サーバー用 1050W -48V DC 電源ユニット（インド）

- **ND-MRX32G1RE3**: ND 32GB DDR5-5600 RDIMM 1Rx4 (16Gb)
- **ND-RAID-M1L16**: ND 24G トライモード M1 RAIDコントローラ（4GB FBWC 16Drv 付き）
- **ND-O-ID10GC-D**: Intel X710T2LOCPV3G1L 2x10GbE RJ45 OCP3.0 NIC
- **ND-OCP3-KIT-D**：C2XX OCP 3.0 インタポーザ（メッシュ アセンブリ付き）
- **ND-P-V5Q50G-D**：Cisco VIC 15425 4x 10/25/50G PCIe C シリーズ（セキュア ブート付き）

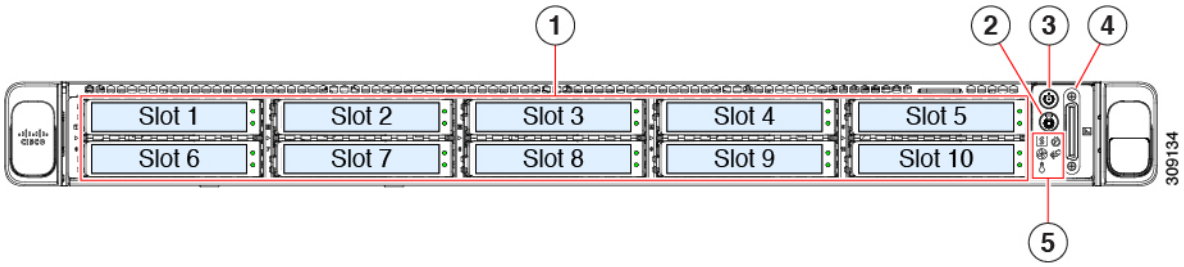
外部機能

ND-NODE-G5S 前面パネルの機能

次の図に、小型フォームファクタのドライブ バージョンのサーバの前面パネルの機構を示します。

LED の状態の定義については、前面パネルの LED （89 ページ）を参照してください。

図 *12 : ND-NODE-G5S* 前面パネル



1	ドライブ ベイ 1 ～ 10 は SAS/SATA ハード ディスク ドライブ（HDD）およびソリッド ステート ドライブ（SSD）をサポート。	**2**	ユニット識別ボタン/LED
3	電源ボタン/電源ステータス LED	**4**	KVM コネクタ（1 つの DB-15 VGA コネクタ、1 つの DB-9 シリアルコネクタ、および 2 つの USB 2.0 コネクタを備えた KVM ケーブルで使用）

5	システム LED クラスタ： • ファン ステータス LED • システム ステータス LED • 電源装置ステータス LED • ネットワーク リンク アクティビティ LED • 温度ステータス LED		-

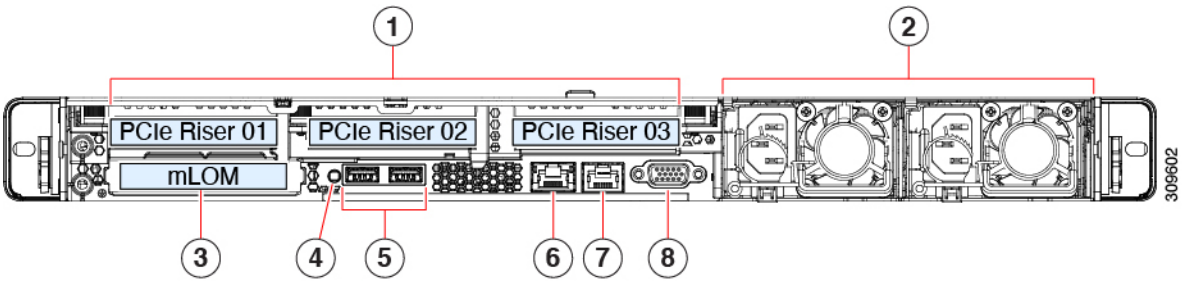
ND-NODE-G5S 背面パネルの機能

背面パネルの機能は、サーバー内の PCIe カードの数とタイプによって異なります。

次の図は、3 ライザー構成のサーバーの背面パネルの機能を示しています。

LED の状態の定義については、背面パネルの LED （91 ページ）を参照してください。

図 *13 : ND-NODE-G5S* 背面パネルの *3* ライザーの構成



1	PCIe スロット 3 HH ライザー ケージ構成では、次の PCIe ライザーの組み合わせを使用できます。 • **ライザー 1** : • ライザー 1A（PCIe Gen4） : ハーフハイト、3/4 長、x16、NCSI、シングル幅 GPU。		
2	電源ユニット（PSU）2 台。1+1 電源モードで構成されている場合には冗長化できます。	3	モジュラ LAN-on-motherboard（mLOM）カード ベイ（x16 PCIe レーン）
4	システム ユニット識別ボタン/LED	5	USB 3.0 ポート（2 個）
6	1 GB イーサネット専用管理ポート	7	COM ポート（RJ45 コネクタ）
8	VGA ビデオ ポート（DB-15 コネクタ）		

PCIe スロットの仕様

次の表で、3 通りのライザーの組み合わせにおけるスロットの仕様について説明します。

表 *15 : PCIe* ライザ *1*

スロット番号	電気レーン幅	コネクタの長さ	カードの最大長	カードの高さ（背面パネルの開口部）	NCSI のサポート
1A	Gen4 x16	x24 コネクタ	¾ レングス	ハーフハイト	対応
10 億	第 5 世代 x16	x24 コネクタ	¾ レングス	ハーフハイト	対応

ステータス LED およびボタン

ここでは、前面、背面、および内部の LED の状態について説明します。

前面パネルの *LED*

図 *14 :* 前面パネルの *LED*

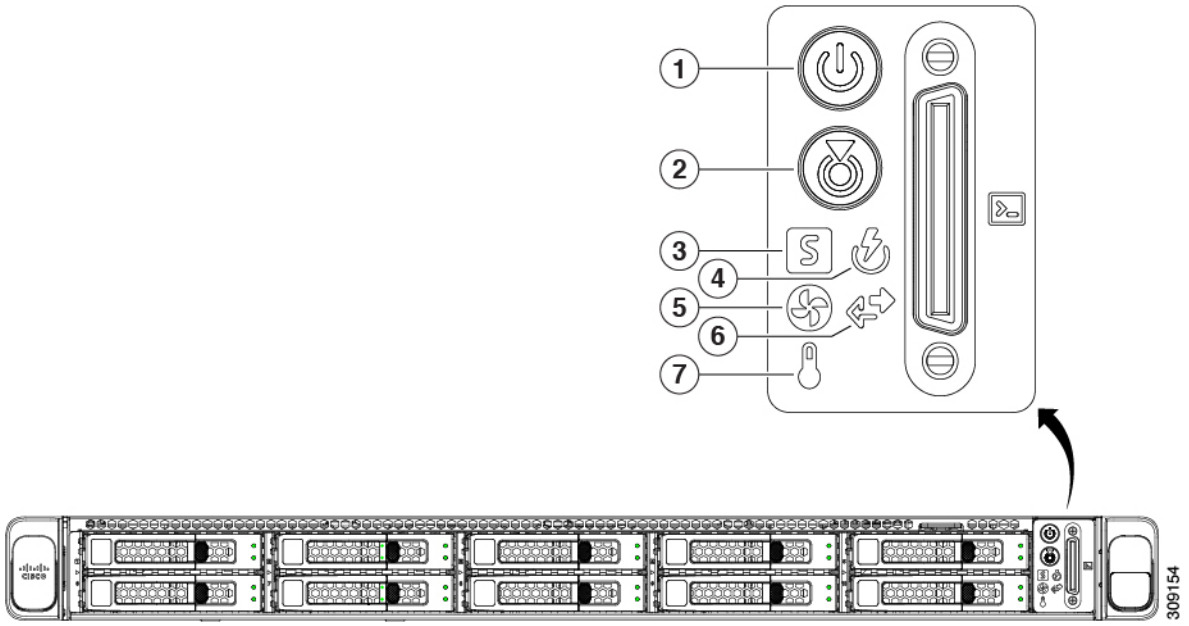


表 *16 :* 前面パネル *LED*、状態の定義

	LED 名	状態
1	電源ボタン/LED（ ）	• 消灯：サーバに AC 電力が供給されていません。 • オレンジ：サーバはスタンバイ電源モードです。Cisco IMC と一部のマザーボード機能にだけ電力が供給されています。 • 緑：サーバは主電源モードです。すべてのサーバコンポーネントに電力が供給されています。

2	ユニット識別（）	• 消灯：ユニット識別機能は使用されていません。 • 青の点滅：ユニット識別機能がアクティブです。

3	システムの状態（）	• 緑：サーバは正常動作状態で稼働しています。
		• 緑の点滅：サーバーはシステムの初期化とメモリチェックを行っています。
		• オレンジの点灯：サーバは縮退運転状態にあります（軽度な障害）。次に例を示します。
		  • 電源装置の冗長性が失われている。
		  • CPU が一致しない。
		  • 少なくとも 1 つの CPU に障害が発生している。
		  • 少なくとも 1 つの DIMM に障害が発生している。
		  • RAID 構成内の少なくとも 1 台のドライブに障害が発生している。
		• オレンジの点滅（2 回）：システムボードで重度の障害が発生しています。
		• オレンジの点滅（3 回）：メモリ（DIMM）で重度の障害が発生しています。
		• オレンジの点滅（4 回）：CPU で重度の障害が発生しています。

4	電源の状態（）	• 緑：すべての電源装置が正常に動作中です。 • オレンジの点灯：1 台以上の電源装置が縮退運転状態にあります。 • オレンジの点滅：1 台以上の電源装置が重大な障害発生状態にあります。
5	ファンの状態（）	• 緑：すべてのファン モジュールが正常に動作中です。 • オレンジの点滅：1 つ以上のファンモジュールで回復不能なしきい値を超えました。

6	ネットワーク リンク アクティビティ（）	• 消灯：イーサネット LOM ポート リンクがアイドル状態です。 • 緑：1 つ以上のイーサネット LOM ポートでリンクがアクティブになっていますが、アクティビティは存在しません。 • 緑の点滅：1 つ以上のイーサネット LOM ポートでリンクがアクティブになっていて、アクティビティが存在します。
7	温度（）	• 緑：サーバは正常温度で稼働中です。 • オレンジの点灯：1 個以上の温度センサーで重大なしきい値を超えました。 • オレンジの点滅：1 個以上の温度センサーで回復不能なしきい値を超えました。

背面パネルの *LED*

図 *15* : 背面パネル *LED*

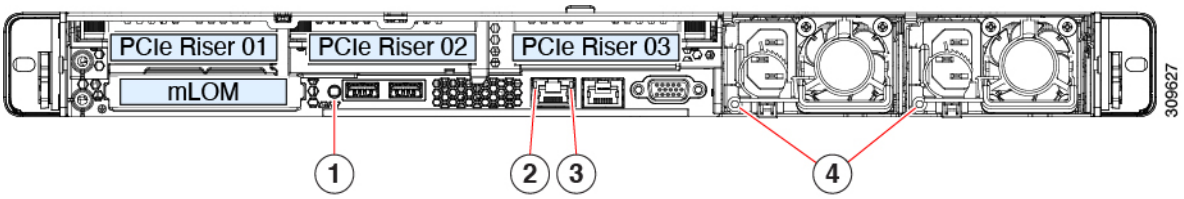


表 *17* : 背面パネル *LED*、状態の定義

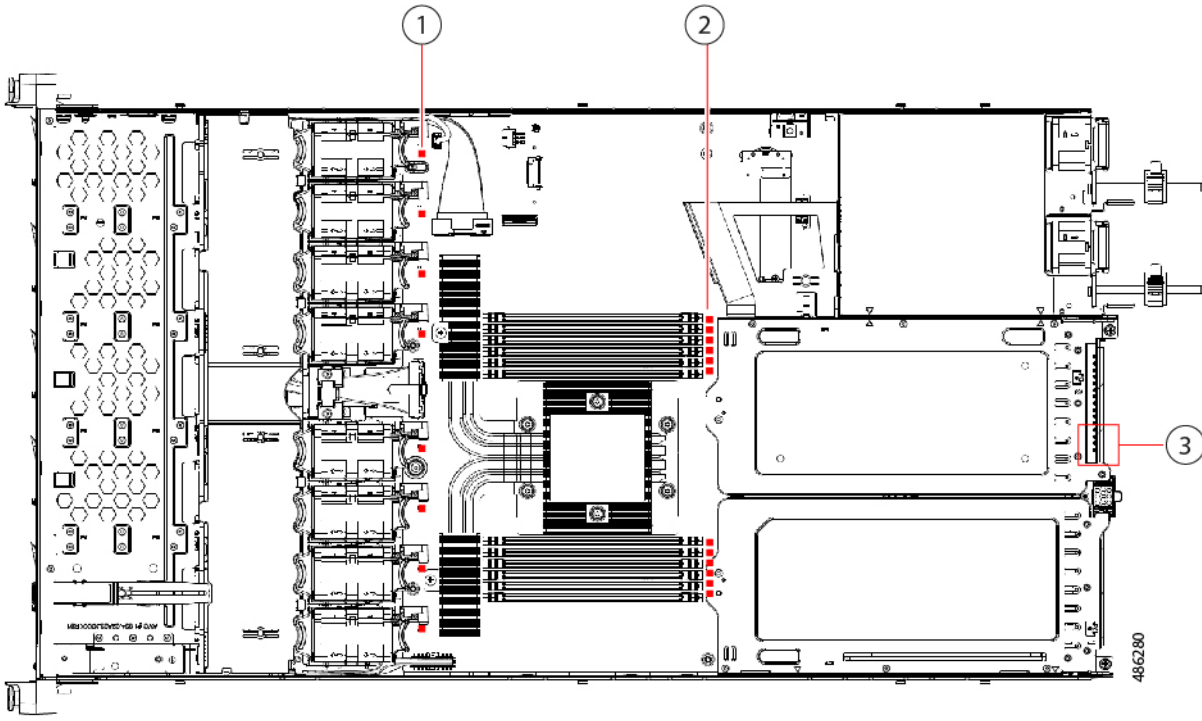
	LED 名	**状態**
1	背面ユニット識別	• 消灯：ユニット識別機能は使用されていません。 • 青の点滅：ユニット識別機能がアクティブです。
2	1 Gb イーサネット専用管理リンク速度	• 消灯：リンク速度は 10 Mbps です。 • オレンジ：リンク速度は 100 Mbps です。 • 緑：リンク速度は 1 Gbps です。

3	1 Gb イーサネット専用管理リンク ステータス	• 消灯：リンクが確立されていません。 • 緑：リンクはアクティブです。 • 緑の点滅：アクティブなリンクにトラフィックが存在します。
4	電源ステータス（各電源装置に 1 つの LED）	**AC 電源装置**： • 消灯：AC 入力なし（12 V 主電源はオフ、12 V スタンバイ電源オフ）。 • 緑の点滅：12 V 主電源はオフ、12 V スタンバイ電源はオン。 • 緑の点灯：12 V 主電源はオン、12 V スタンバイ電源はオン。 • オレンジの点滅：警告しきい値が検出されましたが、12 V 主電源はオン。 • オレンジの点灯：重大なエラーが検出されました。12 V 主電源はオフです（過電流、過電圧、温度超過などの障害）。 **DC 電源装置**： • 消灯：DC 入力なし（12 V 主電源はオフ、12 V スタンバイ電源はオフ）。 • 緑の点滅：12 V 主電源はオフ、12 V スタンバイ電源はオン。 • 緑の点灯：12 V 主電源はオン、12 V スタンバイ電源はオン。 • オレンジの点滅：警告しきい値が検出されましたが、12 V 主電源はオン。 • オレンジの点灯：重大なエラーが検出されました。12 V 主電源はオフです（過電流、過電圧、温度超過などの障害）。

内部診断 *LED*

サーバーには、CPU、DIMM、およびファンモジュールの内部障害 LED があります。

図 *16* : 内部診断 *LED* の位置

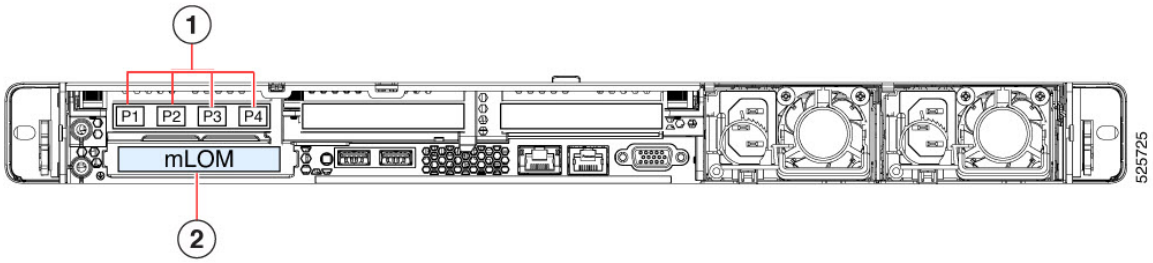


1	ファンモジュール障害 LED（マザーボード上の各ファンコネクタの後方に 1 つ） • オレンジ：ファンに障害が発生しているか、しっかりと装着されていません。 • 緑：ファンは正常です。	2	DIMM 障害 LED（マザーボード上の各 DIMM ソケットの後方に 1 つ） これらの LED は、サーバーがスタンバイ電源モードの場合にのみ動作します。 • オレンジ：DIMM に障害が発生しています。 • 消灯：DIMM は正常です。
3	CPU 障害 LED（背面 USB2 コネクタの横）。 これらの LED は、サーバーがスタンバイ電源モードの場合にのみ動作します。 • オレンジ：CPU に障害が発生しています。 • 消灯オフ: CPU は正常です。	-	

物理ノードのケーブル接続

この図では、`ND-NODE-G5S` （UCS-C225-M8）の物理サーバで、これらの接続を行います。

図 *17 : ノード接続に使用される mLOM および PCIe ライザー 01 カード：ND-NODE-G5S*



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

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

物理ノードは、次のガイドラインに従って展開できます：

- すべてのサーバーに、Nexus Dashboard 管理ネットワークへの接続に使用する Modular LAN on Motherboard（mLOM）カードが付属しています。
- ND-NODE-G5S には、Nexus Dashboard データ ネットワーク接続に使用する「PCIe-Riser-01」スロット (上図参照) に UCSC-P-V5Q50G-D (Cisco UCS VIC 15425 Quad Port 10/25/50G CNA) PCIE カードが含まれています。

（注） ノードをケーブル接続する前に、「データ ネットワーク接続」で提供される情報を使用して、データ インターフェイスの Cisco UCS VIC カードポートマッピングを確認します。データ インターフェイスは、個々のホスト側のスイッチ ポートに接続する必要があります。これらの接続のスイッチ ポート チャネルまたは vPC を構成しないでください。

- VIC でポート チャネル機能が有効になっていることを確認します。
  - `ND-NODE-L4`（UCS-C225-M6）および `ND-NODE-G5S`/`ND-NODE-G5L`（UCS-C225-M8）の場合、ポートチャネル機能は工場出荷時にデフォルトで有効になっています。これらのプラットフォームでは追加の設定は不要ですが、必要に応じて、以下の手順を使用してポートチャネル機能が正しく有効になっているかを確認したり、同機能を有効にしたりすることができます。
  - `SE-NODE-G2`（UCS-C220-M5）では VIC 上のポートチャンネル機能を手動で有効にする必要があります。

1. CIMC にログインします。
2. ハンバーガー アイコンをクリックして、次の場所に移動します。

   [ネットワーキング（Networking）] > [アダプタ カード（Adapter Card）] > [全般（General）] を選択します。
3. **[アダプタ カード プロパティ（Adapter Card Properties）]** エリアでは、**[ポート チャネル（Port Channel）]** フィールドを探します。

   [ポート チャネル（Port Channel）] オプションが無効になっている（チェックボックスにチェックが入っていない）場合は、Nexus Dashboard のデプロイメント プロセスを開始する前に、その機能を有効にしてください（チェックボックスにチェックを入れてください）。

ノードを管理ネットワークおよびデータ ネットワークに接続する場合：

- インターフェイスは、アクティブ/スタンバイ モードで実行されている、データ インターフェイス用（bond0）と管理インターフェイス用（bond1）の Linux ボンドとして構成されます。
- **管理ネットワーク接続**：
  - mLOM カードで `mgmt0` および `mgmt1` を使用する必要があります。
  - すべてのポートが同じ速度（1G または 10G）である必要があります。
- **データ ネットワーク接続**：

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

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

N9000 上	Nexus Dashboard アプライアンス（CIMC 経由）上
FEC AUTO	cl74
FC-FEC	cl74
FEC OFF	FEC OFF

- すべてのポートは同じ速度である必要があります（10G、25G、または 50G のいずれか）。
- データ ネットワーク接続用のケーブルを接続します。一方のケーブルを fabric0 に、もう一方のケーブルを fabric1 に接続してください。

  ND-NODE-G5S サーバの fabric0 および fabric1 は、次のポートに対応しています。

  - ポート 1 およびポート 2 は fabric0 に対応します
  - ポート 3 および ポート 4 は fabric1 に対応します

  したがって、これらのポートチャネルの組み合わせのうち、いずれかを使用することができます。

最初のデータ ケーブル（fabric0）	2 番目のデータ ケーブル（fabric1）
[Port-1]	ポート 3
[Port-1]	ポート 4
[Port-2]	ポート 3
[Port-2]	ポート 4

  ポート位置は、図 17 : ノード接続に使用される mLOM および PCIe ライザー 01 カード : ND-NODE-G5S （106 ページ） を参照します。

  データ ネットワーク接続には、アクティブ スタンバイとして fabric0 と fabric1 の両方を使用できます。

注意

- これらの接続のスイッチ ポート チャネルまたは vPC を構成しないでください。上記のサポートされているペアリングは、VIC カードでのみ有効な物理ポート マッピングを識別します。
- 上記以外のポート チャネルの組み合わせを使用してデータ ネットワーク接続用の 2 本のケーブルを接続する場合、上流に位置するスイッチで MAC 移動通知が行われ、ポートがフラップします。

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

次のステップ

物理アプライアンスとしての Nexus Dashboard の展開 （134 ページ） に移動して、Nexus Dashboard を展開します。

ND-NODE-L4 （UCS-C225-M6）

これらのセクションでは、`ND-NODE-L4`（UCS-C225-M6）物理アプライアンスの概要とケーブル接続情報について説明します。

ND-NODE-L4（UCS-C225-M6）について

このセクションでは、`ND-NODE-L4` （UCS-C225-M6）物理アプライアンスの概要について説明します。

`ND-NODE-L4` 物理アプライアンスは、UCS-C225-M6 サーバに基づく Nexus Dashboard アプライアンスです。Nexus Dashboard `ND-NODE-L4` は UCS-C225-M6 サーバに基づいていますが、ベースの UCS C225 M8 サーバのように Nexus Dashboard `ND-NODE-L4` 内のコンポーネントを交換することはできません。代わりに、Nexus Dashboard `ND-NODE-L4` 内のコンポーネントに障害がある場合は、アプライアンス用の返品許可（RMA）操作を実行します。

Nexus Dashboard `ND-NODE-L4` は UCS C225 M6 サーバに基づいているため、そのドキュメントの次の章に記載されている情報など、Nexus Dashboard `ND-NODE-L4` にも適用される重要な *UCS-C225-M6* サーバ情報については、『*Cisco UCS C225 M6 Server Installation and Service Guide*』を参照できます。。

- 概要
- サーバーのインストール
- サーバの仕様

- ストレージ コントローラの考慮事項

ただし、 Nexus Dashboard ND-NODE-L4 内のコンポーネントをベースの UCS-C225-M6 サーバのように交換することはできないため、そのドキュメントの次の章は Nexus Dashboard ND-NODE-L4 には適用されず、無視する必要があります。

- サーバの保守
- Cisco UCS Manager 統合に適した設置方法
- GPU の取り付け

次のセクションでは、 Nexus Dashboard ND-NODE-L4に適用される情報を提供します。

概要

Cisco Nexus Dashboard は、シスコ データセンター アプリケーションを展開するための共通プラットフォームを提供します。これらのアプリケーションは、ポリシーとインフラストラクチャのリアルタイム分析、可視性、および保証を提供します。

Cisco Nexus Dashboard アプリケーションは、Cisco Nexus Dashboard アプリケーションをインストールしてホストするために必要です。

サーバは次のバージョンで構成可能です。

- ND-NODE-L4 — スモール フォーム ファクタ（SFF）ドライブ、10 ドライブ バックプレーン付き。最大 10 台の 2.5 インチ SAS/SATA ドライブをサポート。ドライブベイ 1 および 2 は NVMe SSD をサポート。

次の PCIe ライザーの組み合わせを使用できます。

- PCIe ライザー 1 に装着された 1 枚のハーフハイト ライザー カード
- PCIe ライザー 1、2、3 に装着された 3 枚のハーフハイト ライザー カード
- ライザー 1 および 3 の 2 枚のフルハイト ライザー カード
- ライザー 1：ライザー 1 をサポート。2 ライザー構成でフルハイト 3/4 レングス カードをサポートするシングル x16 PCIe（または）3 ライザー構成でハーフハイト 3/4 レングス カードおよび Pilot4 からの NC-SIをサポート。
- ライザー 2：ライザー 1 をサポート。3 ライザー構成でハーフハイト 3/4 レングスカードのみをサポートするシングル x16 PCIe をサポートします。
- ライザー 3：ライザー 3A、3B をサポート。以下のオプションを含む PCIe スロット 3：
  - ライザー 3A は、3 ライザー構成と NC-SI でハーフハイト 3/4 レングス カードをサポートするシングル x16 PCIe をサポートします。
  - ライザー 3Bは、2 ライザー構成と NC-SI でフルハイト 3/4 レングス カードをサポートする x16 PCIe をサポートします。

- ネットワーク接続用の 2 つの 10GBase-T イーサネット LAN over Motherboard（LOM）ポート、および 1 つの 1 Gb イーサネット専用管理ポート。
- 1 つの mLOM/VIC カードは、10G/25G/40G/50G/100G 接続を提供します。サポートされるカード：
  - Cisco VIC 1455 VIC PCIE – クアッド ポート 10/25G SFP28（UCSC-PCIE-C25Q-04）

外部機能

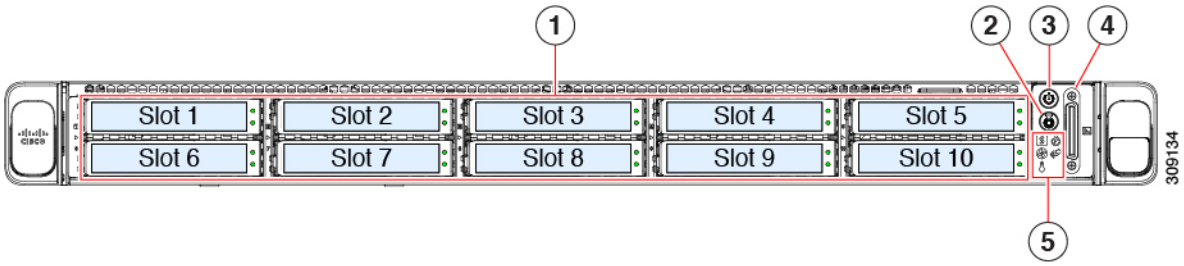
このトピックでは、各サーバー バージョンの外部機能について説明します。

Cisco ND-NODE-L4（SFF ドライブ）前面パネルの機能

次の図に、小型フォームファクタのドライブ バージョンのサーバの前面パネルの機構を示します。

LED の状態の定義については、前面パネルの LED （113 ページ）を参照してください。

図 *18 : ND-NODE-L4（SFF ドライブ）前面パネル*



1 UCSC-C225-M6S バージョン：ドライブ ベイ 1 ～ 10 は SAS/SATA ハード ディスク ドライブ（HDD）およびソリッド ステート ドライブ（SSD）をサポート。オプションとして、ドライブ ベイ 1 ー 4 には最大 4 台の NVMe ドライブを搭載できます。最大で 4 台であること以外に、台数に制限はありません。ドライブ ベイ 5 ー 10 は、SAS/SATA HDD または SSD のみをサポートします。 UCSC-C225-M6N バージョン：ドライブ ベイ 1 ～ 10 は 2.5 インチ NVMe SSD のみをサポートします。	2 ユニット識別ボタン/LED
3 電源ボタン/電源ステータス LED	4 KVM コネクタ （DB-15 VGA X 1、DB-9 シリアル X 1、USB 2.0 X 2 を装備した KVM ケーブルの接続用）

5 システム LED クラスタ： • ファン ステータス LED • システム ステータス LED • 電源装置ステータス LED • ネットワーク リンク アクティビティ LED • 温度ステータス LED	-

Cisco ND-NODE-L4 の背面パネルの機能

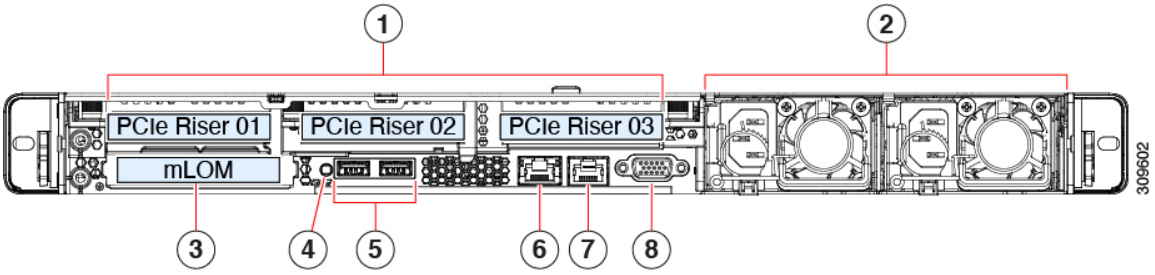
背面パネルの機能は、サーバー内の PCIe カードの数とタイプによって異なります。

デフォルトでは、シングル CPU サーバにはハーフハイト ライザー 1 が 1 つだけ取り付けられており、デュアル CPU サーバは 3 つのハーフハイト ライザーをすべてサポートします。

次の図は、3 ライザー構成のサーバーの背面パネルの機能を示しています。

LED の状態の定義については、背面パネルの LED （115 ページ）を参照してください。

図 *19 : Cisco ND-NODE-L4* 背面パネルの *3* ライザーの構成



次の図は、3 ライザー構成のサーバーの背面パネルの機能を示しています。

1 PCIe スロット 次の PCIe ライザーの組み合わせを使用できます。 • PCIe ライザー 1 に装着された 1 枚のハーフハイト ライザー カード	
2 電源ユニット（PSU）2 台。1+1 電源モードで構成されている場合には冗長化できます。	3 モジュラ LAN-on-motherboard（mLOM）カード ベイ（x16 PCIe レーン）
4 システム ユニット識別ボタン/LED	5 USB 3.0 ポート（2 個）
6 1 GB イーサネット専用管理ポート	7 COM ポート（RJ45 コネクタ）
8 VGA ビデオ ポート（DB-15 コネクタ）	

PCIe スロットの仕様

次の表で、3 通りのライザーの組み合わせにおけるスロットの仕様について説明します。

表 *18 : PCIe* ライザ *1*

スロット番号	電気レーン幅	コネクタの長さ	カードの最大長	カードの高さ（背面パネルの開口部）	NCSI のサポート
1	Gen-3 および 4 x16	x24 コネクタ	¾ レングス	ハーフハイト	対応

ステータス LED およびボタン

ここでは、前面、背面、および内部の LED の状態について説明します。

前面パネルの *LED*

図 *20 :* 前面パネルの *LED*

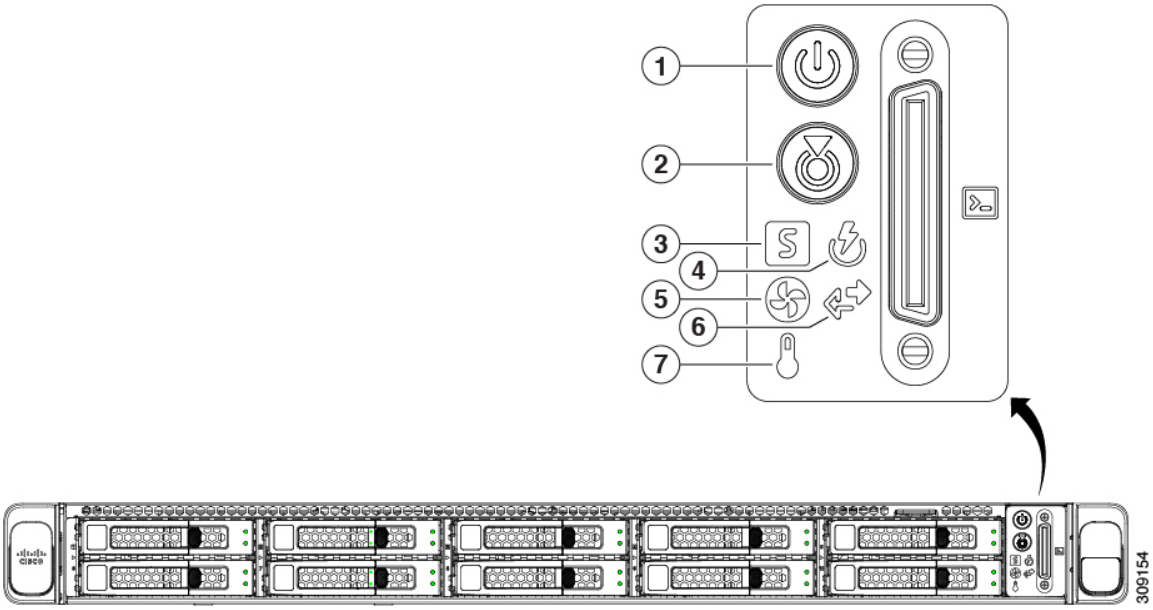


表 *19 :* 前面パネル *LED*、状態の定義

LED 名	状態

1 電源ボタン/LED（）	• 消灯：サーバに AC 電力が供給されていません。 • オレンジ：サーバはスタンバイ電源モードです。Cisco IMC と一部のマザーボード機能にだけ電力が供給されています。 • 緑：サーバは主電源モードです。すべてのサーバコンポーネントに電力が供給されています。
2 ユニット識別（）	• 消灯：ユニット識別機能は使用されていません。 • 青の点滅：ユニット識別機能がアクティブです。

3
システムの状態（）
	• 緑：サーバは正常動作状態で稼働しています。
	• 緑の点滅：サーバーはシステムの初期化とメモリチェックを行っています。
	• オレンジの点灯：サーバは縮退運転状態にあります（軽度な障害）。次に例を示します。
	  • 電源装置の冗長性が失われている。
	  • CPU が一致しない。
	  • 少なくとも 1 つの CPU に障害が発生している。
	  • 少なくとも 1 つの DIMM に障害が発生している。
	  • RAID 構成内の少なくとも 1 台のドライブに障害が発生している。
	• オレンジの点滅（2 回）：システムボードで重度の障害が発生しています。
	• オレンジの点滅（3回）：メモリ（DIMM）で重度の障害が発生しています。
	• オレンジの点滅（4 回）：CPU で重度の障害が発生しています。

4 電源の状態（）	• 緑：すべての電源装置が正常に動作中です。 • オレンジの点灯：1 台以上の電源装置が縮退運転状態にあります。 • オレンジの点滅：1 台以上の電源装置が重大な障害発生状態にあります。

5 ファンの状態	• 緑：すべてのファンモジュールが正常に動作中です。 • オレンジの点滅：1 つ以上のファンモジュールで回復不能なしきい値を超えました。
6 ネットワーク リンク アクティビティ	• 消灯：イーサネット LOM ポート リンクがアイドル状態です。 • 緑：1 つ以上のイーサネット LOM ポートでリンクがアクティブになっていますが、アクティビティは存在しません。 • 緑の点滅：1 つ以上のイーサネット LOM ポートでリンクがアクティブになっていて、アクティビティが存在します。
7 温度	• 緑：サーバは正常温度で稼働中です。 • オレンジの点灯：1 個以上の温度センサーで重大なしきい値を超えました。 • オレンジの点滅：1 個以上の温度センサーで回復不能なしきい値を超えました。

背面パネルの *LED*

図 *21* : 背面パネル *LED*

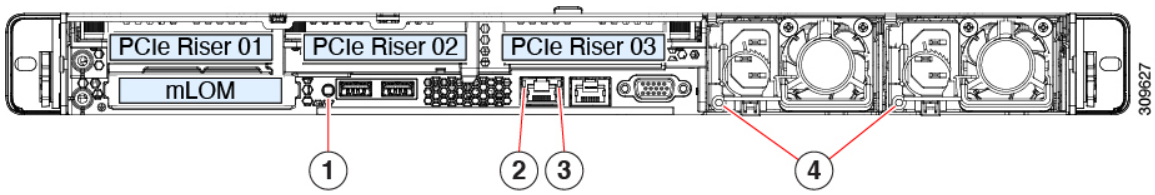


表 *20* : 背面パネル *LED*、状態の定義

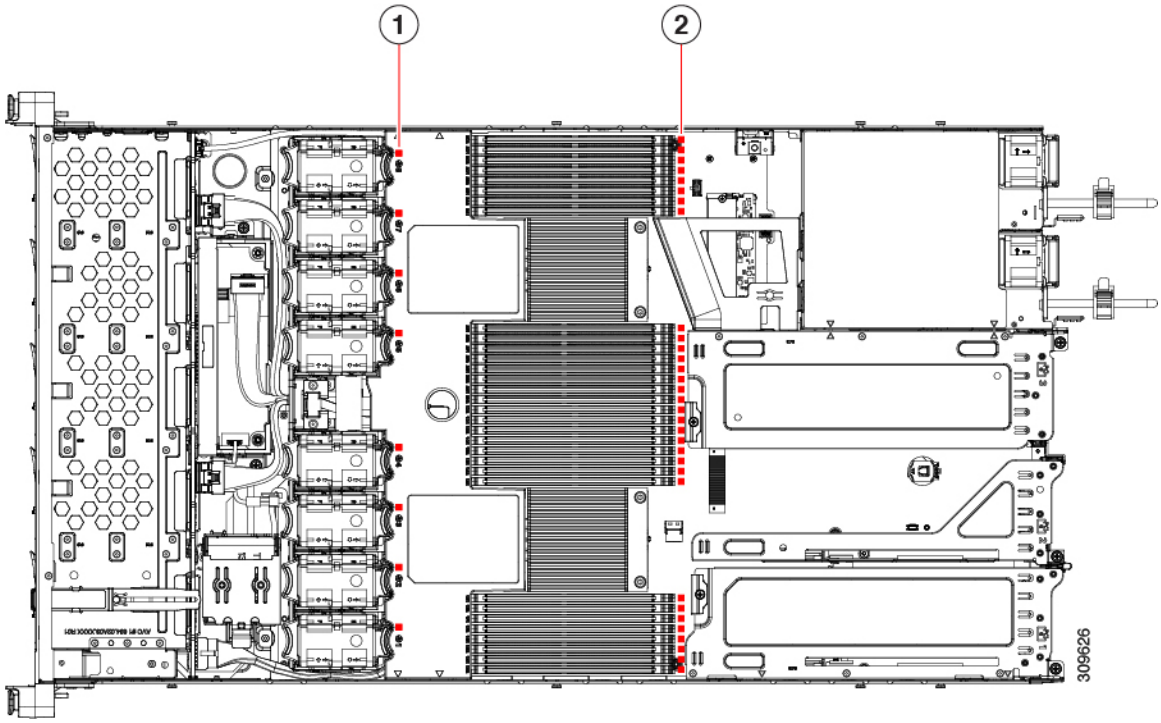
LED 名	状態
1 背面ユニット識別	• 消灯：ユニット識別機能は使用されていません。 • 青の点滅：ユニット識別機能がアクティブです。
2 4 Gb イーサネット専用管理リンク速度	• 消灯：リンク速度は 10 Mbps です。 • オレンジ：リンク速度は 100 Mbps です。 • 緑：リンク速度は 1 Gbps です。

3 1 Gb イーサネット専用管理リンク ステータス	• 消灯：リンクが確立されていません。 • 緑：リンクはアクティブです。 • 緑の点滅：アクティブなリンクにトラフィックが存在します。
4 電源ステータス（各電源装置に 1 つの LED）	**AC 電源装置**： • 消灯：AC 入力なし（12 V 主電源はオフ、12 V スタンバイ電源オフ）。 • 緑の点滅：12 V 主電源はオフ、12 V スタンバイ電源はオン。 • 緑の点灯：12 V 主電源はオン、12 V スタンバイ電源はオン。 • オレンジの点滅：警告しきい値が検出されましたが、12 V 主電源はオン。 • オレンジの点灯：重大なエラーが検出されました。12 V 主電源はオフです（過電流、過電圧、温度超過などの障害）。 **DC 電源装置**： • 消灯：DC 入力なし（12 V 主電源はオフ、12 V スタンバイ電源はオフ）。 • 緑の点滅：12 V 主電源はオフ、12 V スタンバイ電源はオン。 • 緑の点灯：12 V 主電源はオン、12 V スタンバイ電源はオン。 • オレンジの点滅：警告しきい値が検出されましたが、12 V 主電源はオン。 • オレンジの点灯：重大なエラーが検出されました。12 V 主電源はオフです（過電流、過電圧、温度超過などの障害）。

内部診断 *LED*

サーバーには、CPU、DIMM、およびファンモジュールの内部障害 LED があります。

図 *22* : 内部診断 *LED* の位置

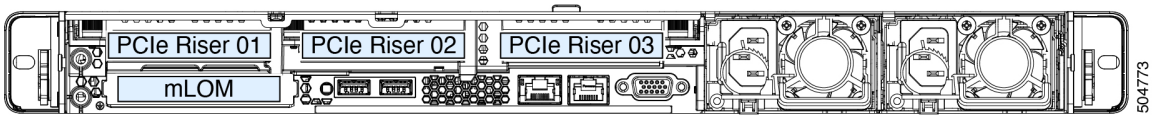


1 ファンモジュール障害 LED（マザーボード上の各ファンコネクタの後方に 1 つ） • オレンジ：ファンに障害が発生しているか、しっかりと装着されていません。 • 緑：ファンは正常です。	2 DIMM 障害 LED（マザーボード上の各 DIMM ソケットの後方に 1 つ） これらの LED は、サーバーがスタンバイ電源モードの場合にのみ動作します。 • オレンジ：DIMM に障害が発生しています。 • 消灯：DIMM は正常です。
3 CPU 障害 LED（マザーボード上の各 CPU ソケットの後方に 1 つ） これらの LED は、サーバーがスタンバイ電源モードの場合にのみ動作します。 • オレンジ：CPU に障害が発生しています。 • 消灯オフ: CPU は正常です。	-

物理ノードのケーブル接続

物理ノードは、ND-NODE-L4（UCS-C225-M6）の物理サーバに展開できます：

図 *23 :* ノード接続に使用される *mLOM* および *PCIe* ライザー *01* カード：*ND-NODE-L4*（*UCS-C225-M6*）



物理ノードは、次のガイドラインに従って展開できます：

- すべてのサーバーに、Nexus Dashboard 管理ネットワークへの接続に使用する Modular LAN on Motherboard（mLOM）カードが付属しています。
- ND-NODE-G5S サーバーには、 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。

（注） ノード をケーブル接続する前に、「データ ネットワーク接続」で提供される情報を使用して、データ インターフェイスのポート マッピングを確認します。データ インターフェイスは、個々のホスト側のスイッチ ポートに接続する必要があります。これらの接続のスイッチ ポート チャネルまたは vPC を構成しないでください。

- VIC でポート チャネル機能が有効になっていることを確認します。
  - ND-NODE-L4（UCS-C225-M6）および ND-NODE-G5S/ND-NODE-G5L（UCS-C225-M8）の場合、ポート チャネル機能は工場出荷時にデフォルトで有効になっています。これらのプラットフォームでは追加の設定は不要ですが、必要に応じて、以下の手順を使用してポート チャネル機能が正しく有効になっているかを確認したり、同機能を有効にしたりすることができます。
  - SE-NODE-G2（UCS-C220-M5）では VIC 上のポートチャンネル機能を手動で有効にする必要があります。

1. CIMC にログインします。
2. ハンバーガー アイコンをクリックして、次の場所に移動します。

   [ネットワーキング（Networking）] > [アダプタ カード（Adapter Card）] > [全般（General）] を選択します。
3. **[アダプタ カード プロパティ（Adapter Card Properties）]** エリアでは、**[ポート チャネル（Port Channel）]** フィールドを探します。

   [ポート チャネル（Port Channel）] オプションが無効になっている（チェックボックスにチェックが入っていない）場合は、Nexus Dashboard のデプロイメント プロセスを開始する前に、その機能を有効にしてください（チェックボックスにチェックを入れてください）。

ノードを管理ネットワークおよびデータ ネットワークに接続する場合：

- インターフェイスは、アクティブ/スタンバイ モードで実行されている、データ インターフェイス用（bond0）と管理インターフェイス用（bond1）の Linux ボンドとして構成されます。
- **管理ネットワーク接続**：
  - mLOM カードで `mgmt0` および `mgmt1` を使用する必要があります。
  - すべてのポートが同じ速度（1G または 10G）である必要があります。
- **データ ネットワーク接続**：
  - `ND-NODE-L4` サーバーで、2x10GbE NIC (`APIC-P-ID10GC`)、または 2x25/10GbE SFP28 NIC (`APIC-P-I8D25GF`)、または VIC1455 カードを使用できます。

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

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

  - すべてのポートは同じ速度である必要があります（10G、25G、または 50G のいずれか）。
  - データ ネットワーク接続用のケーブルを接続します。一方のケーブルを `fabric0` に、もう一方のケーブルを `fabric1` に接続してください。

    `ND-NODE-L4` サーバーの `fabric0` および `fabric1` は、カードのタイプに応じて特定のポートに対応します。
    - 2 ポート Intel カードの場合：
      - ポート 1 は `fabric0` に対応します
      - ポート 2 は `fabric1` に対応します
    - 4 ポート カードの場合：
      - ポート 1 およびポート 2 は `fabric0` に対応します
      - ポート 3 および ポート 4 は `fabric1` に対応します

    したがって、これらのポートチャネルの組み合わせのうち、いずれかを使用することができます。

最初のデータ ケーブル（fabric0）	2 番目のデータ ケーブル（fabric1）
[Port-1]	ポート 3
[Port-1]	ポート 4
[Port-2]	ポート 3
[Port-2]	ポート 4

ND-NODE-L4 サーバで 4 ポート カードを使用する場合は、左から右に、ポート 4、ポート 3、ポート 2、ポート 1 です。

データ ネットワーク接続には、アクティブ スタンバイとして fabric0 と fabric1 の両方を使用できます。

注意

- これらの接続のスイッチ ポート チャネルまたは vPC を構成しないでください。上記のサポートされているペアリングは、VIC カードでのみ有効な物理ポート マッピングを識別します。
- 上記以外のポート チャネルの組み合わせを使用してデータ ネットワーク接続用の 2 本のケーブルを接続する場合、上流に位置するスイッチで MAC 移動通知が行われ、ポートがフラップします。

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

次のステップ

物理アプライアンスとしての Nexus Dashboard の展開 （134 ページ） に移動して、Nexus Dashboard を展開します。

SE-NODE-G2 （UCS-C220-M5）。

このセクションでは、SE-NODE-G2 （UCS-C220-M5）物理アプライアンスの概要とケーブル接続について説明します。

SE-NODE-G2（UCS-C220-M5）について

このセクションでは、SE-NODE-G2 （UCS-C220-M5）物理アプライアンスの概要について説明します。

SE-NODE-G2 物理アプライアンスは、 UCS C220 M5 サーバに基づく Nexus Dashboard アプライアンスです。Nexus Dashboard SE-NODE-G2 は UCS C220 M5 サーバに基づいていますが、ベースの UCS C220 M5 サーバのように Nexus Dashboard SE-NODE-G2 内のコンポーネントを交換することはできません。代わりに、 Nexus Dashboard SE-NODE-G2 内のコンポーネントに障害がある場合は、アプライアンス用の返品許可（RMA）操作を実行します。

Nexus Dashboard SE-NODE-G2 は UCS C220 M5 サーバに基づいているため、 Nexus Dashboard SE-NODE-G2 にも適用される重要な UCS C220 M5 サーバ情報については、『*Cisco UCS UCS M5 Server Installation and Service Guide*』を参照できます（そのドキュメントの次の章に記載されている情報など）。

- 概要
- サーバーのインストール
- サーバの仕様
- ストレージ コントローラの考慮事項

ただし、Nexus Dashboard SE-NODE-G2 内のコンポーネントを、ベース UCS C220 M5 サーバのように交換することはできないため、そのドキュメントの次の章は Nexus Dashboard SE-NODE-G2 には適用されず、無視する必要があります。

- サーバーの保守
- GPU の取り付け
- Cisco UCS Manager 統合に適した設置方法

次のセクションでは、Nexus Dashboard SE-NODE-G2 に適用される情報を提供します。

概要

Cisco Nexus Dashboard は、シスコ データセンター アプリケーションを展開するための共通プラットフォームを提供します。これらのアプリケーションは、ポリシーとインフラストラクチャのリアルタイム分析、可視性、および保証を提供します。

Cisco Nexus Dashboard アプリケーションは、Cisco Nexus Dashboard アプリケーションをインストールしてホストするために必要です。

サーバは次のバージョンで構成可能です。

- SE-CL-L3 —スモール フォーム ファクタ (SFF) ドライブ、10 ドライブ バックプレーン付き。最大 10 台の 2.5 インチ SAS/SATA ドライブをサポート。ドライブベイ 1 および 2 は NVMe SSD をサポート。

外部機能

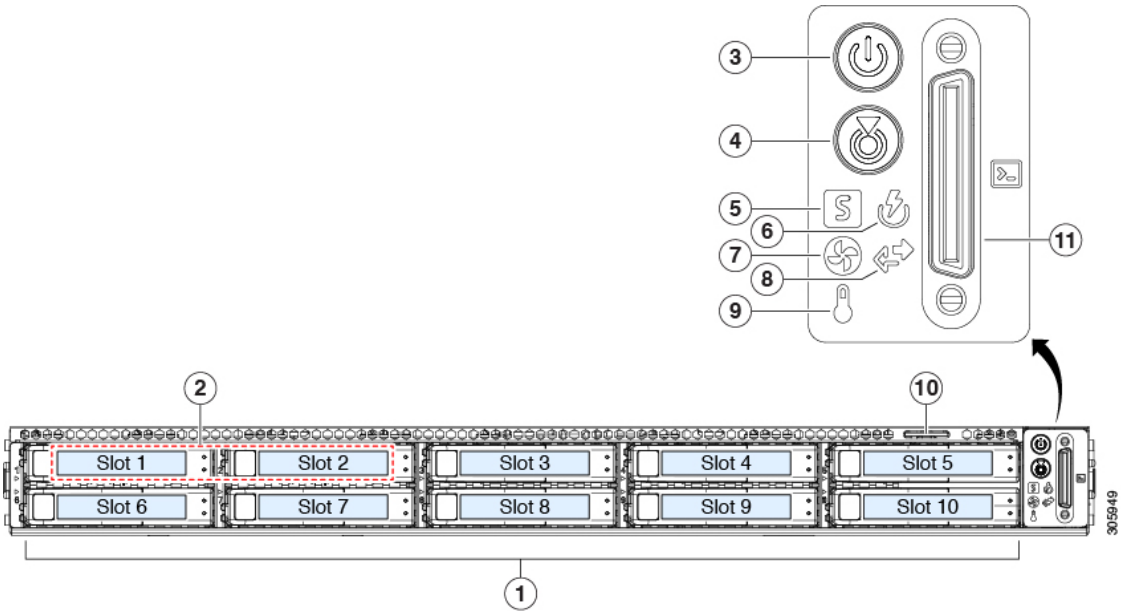
このトピックでは、各サーバー バージョンの外部機能について説明します。

Cisco SE-CL-L3（SFF ドライブ）前面パネルの機能

次の図に、小型フォームファクタのドライブ バージョンのサーバの前面パネルの機構を示します。

LED の状態の定義については、前面パネルの LED （126 ページ）を参照してください。

図 *24 : Cisco SE-CL-L3*（*SFF* ドライブ）前面パネルの機能



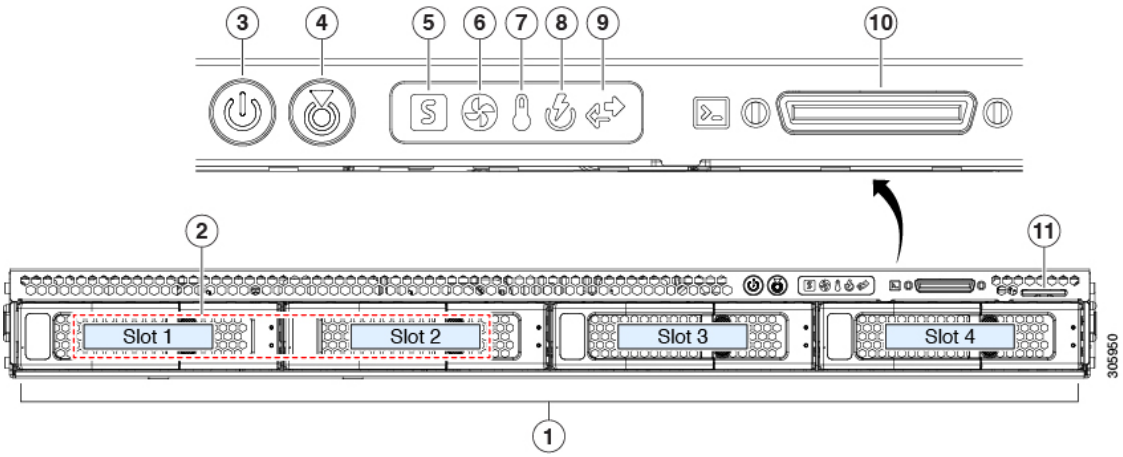
1 ドライブ ベイ 1 ～ 10 は SAS/SATA ハード ディスク ドライブ（HDD）およびソリッド ステート ドライブ（SSD）をサポート。	7 ファン ステータス LED
2 • SE-CL-L3 : ドライブベイ 1 および 2 で NVMe PCIe SSD をサポート。	8 ネットワーク リンク アクティビティ LED
3 電源ボタン/電源ステータス LED	9 温度ステータス LED
4 ユニット識別ボタン/LED	10 引き抜きアセットタグ
5 システム ステータス LED	11 KVM コネクタ （DB-15 VGA 1 個、DB-9 シリアル 1 個、および USB コネクタ 2 個を装備した KVM ケーブルとともに使用）
6 電源ステータス LED	-

31SE-CL-L3（LFF ドライブ）前面パネルの機能

次の図に、大型フォームファクタのドライブバージョンのサーバーの前面パネルの機構を示します。

LED の状態の定義については、「前面パネルの LED （126 ページ）」を参照してください。

図 25 : 31SE-CL-L3（LFF ドライブ）前面パネルの機能



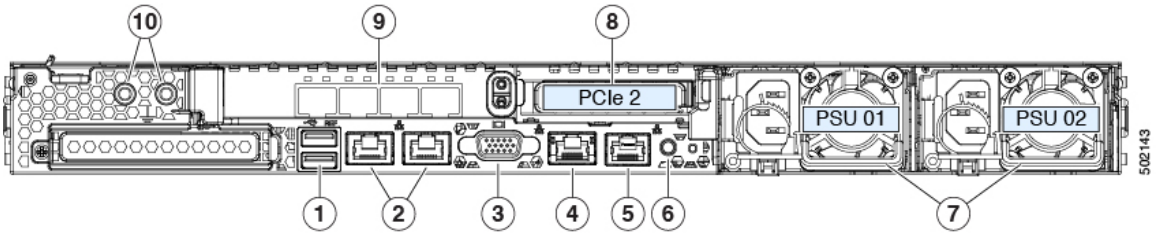
1 ドライブベイ 1 ～ 4 は SAS/SATA HDD および SSD をサポート。	7 温度ステータス LED
2 ドライブベイ 1 および 2 で NVMe PCIe SSD をサポート。 2.5 インチ SSD を使用する場合は、サイズ変換ドライブスレッドが必要です。	8 電源装置ステータス LED
3 電源ボタン/電源ステータス LED	9 ネットワーク リンク アクティビティ LED
4 ユニット識別ボタン/LED	10 KVM コネクタ （DB-15 VGA 1 個、DB-9 シリアル 1 個、および USB コネクタ 2 個を装備した KVM ケーブルとともに使用）
5 システムヘルス LED	11 引き抜きアセット タグ
6 ファン ステータス LED	-

SE-CL-L3 背面パネルの機能

背面パネルの機能は、サーバーのバージョンすべてで同一です。

LED の状態の定義については、背面パネルの LED （129 ページ）を参照してください。

図 *26 : SE-CL-L3* 背面パネル

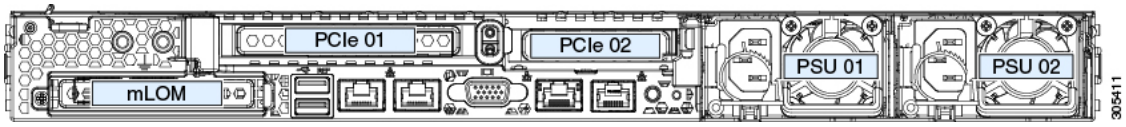


1 USB 3.0 ポート（2 個）	6 背面ユニット識別ボタン/LED
2 デュアル 1 Gb/10 Gb イーサネット ポート（LAN1 と LAN2） デュアル LAN ポートは、リンク パートナーの機能に応じて 1 Gbps および 10 Gbps をサポートできます。 これらはそれぞれ `eth1-1` (`eth0`) および `eth1-2` (`eth1`) に対応します。	7 電源装置（2、1+1 として冗長）
3 VGA ビデオ ポート（DB-15 コネクタ）	8 PCIe ライザー 1/スロット 1（x16 レーン） フロントロード NVMe SSD（x8 レーン）用の PCIe ケーブル コネクタが付属
4 1 Gb イーサネット専用管理ポート	9 クワッド 10 Gb / 25 Gb ポート。 これらは `eth 2-1`～`eth 2-4` に対応します。アクティブ/スタンバイモードでは、4 つのうち 2 つのインターフェイスのみがアクティブになります（`eth2-1 / 2-2` または `eth2-3 / 2-4`）。
5 シリアル ポート（RJ-45 コネクタ）	10 デュアルホール アース ラグ用ネジ穴

PCIe スロットの仕様

サーバには、PCIe カードを水平に取り付けるための 1 つのライザー アセンブリ上に PCIe スロットが 2 つあります。両方のスロットが NCSI プロトコルと 12 V のスタンバイ電源をサポートしています。

図 *27 :* 背面パネル、*PCIe* スロットの番号付け



次の表で、スロットの仕様について説明します。

表 *21 : PCIe* ライザー *1*/スロット *1*

スロット番号	電気レーン幅	コネクタの長さ	カードの最大長	カードの高さ（背面パネルの開口部）	NCSI のサポート
1	Gen-3 x16	x24 コネクタ	¾ レングス	フルハイト	対応
microSD カードスロット	microSD カード用ソケット X 1				

表 *22 : PCIe* ライザー *2*/スロット *2*

スロット番号	電気レーン幅	コネクタの長さ	カードの最大長	カードの高さ（背面パネルの開口部）	NCSI のサポート
2	Gen-3 x16	x24 コネクタ	ハーフ レングス	ハーフ ハイト	Yes
前面パネルの NVMe SSD の PCIe ケーブル コネクタ	Gen-3 x8	ケーブルの他方の端は、前面パネルの NVMe SSD をサポートする前面のドライブバックプレーンに接続します。			

（注） ライザー 2/スロット 2 は、シングル CPU 構成では使用できません。

ステータス LED およびボタン

ここでは、前面、背面、および内部の LED の状態について説明します。

前面パネルの *LED*

図 *28 :* 前面パネルの *LED*

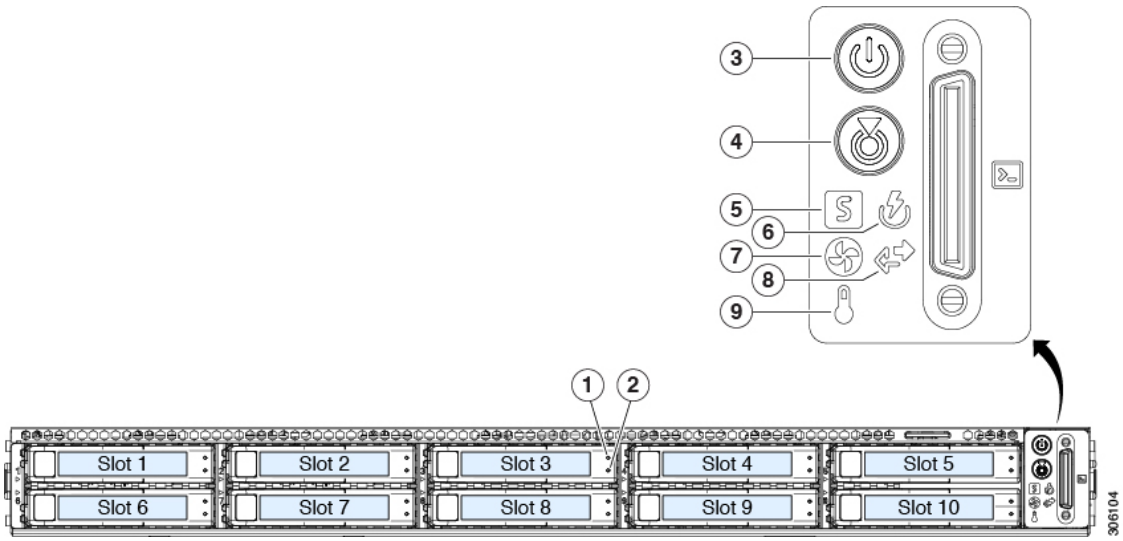


表 *23 :* 前面パネル *LED*、状態の定義

LED 名	状態
1 SAS/SATA ドライブの障害 (注) NVMe ソリッド ステート ドライブ（SSD）ドライブ トレイの LED の動作は、SAS/SATA ドライブ トレイとは異なります。	• 消灯：ハード ドライブは正常に動作中です。 • オレンジ：ドライブ障害が検出されました。 • オレンジの点滅：デバイスの再構成中です。 • 1 秒間隔のオレンジの点滅：ソフトウェアでドライブ位置特定機能がアクティブ化されました。
2 SAS/SATA ドライブ アクティビティ LED	• 消灯：ハード ドライブ トレイにハード ドライブが存在しません（アクセスなし、障害なし）。 • 緑：ハード ドライブの準備が完了しています。 • 緑の点滅：ハード ドライブはデータの読み取り中または書き込み中です。

1 NVMe SSD ドライブ障害 (注) NVMe ソリッド ステート ドライブ（SSD）ドライブ トレイの LED の動作は、SAS/SATA ドライブ トレイとは異なります。	• 消灯：ドライブは使用されておらず、安全に取り外すことができます。 • 緑色：ドライブは使用中で、正常に機能しています。 • 緑の点滅：ドライバは挿入後の初期化中、またはイジェクト コマンドの後のアンロード中です。 • オレンジ：ドライブで障害が発生しています。 • オレンジの点滅：ソフトウェアでドライブ検出コマンドが発行されました。
2 NVMe SSD アクティビティ	• 消灯：ドライブが動作していません。 • 緑の点滅：ドライブは動作中です。
3 電源ボタン/LED	• 消灯：サーバに AC 電力が供給されていません。 • オレンジ：サーバはスタンバイ電源モードです。Cisco IMC と一部のマザーボード機能にだけ電力が供給されています。 • 緑：サーバは主電源モードです。すべてのサーバ コンポーネントに電力が供給されています。
4 ユニット識別	• 消灯：ユニット識別機能は使用されていません。 • 青の点滅：ユニット識別機能がアクティブです。

5 システム ヘルス	• 緑：サーバは正常動作状態で稼働しています。
	• 緑の点滅：サーバーはシステムの初期化とメモリチェックを行っています。
	• オレンジの点灯：サーバは縮退運転状態にあります（軽度な障害）。次に例を示します。
	  • 電源装置の冗長性が失われている。
	  • CPU が一致しない。
	  • 少なくとも 1 つの CPU に障害が発生している。
	  • 少なくとも 1 つの DIMM に障害が発生している。
	  • RAID 構成内の少なくとも 1 台のドライブに障害が発生している。
	• オレンジの点滅（2 回）：システムボードで重度の障害が発生しています。
	• オレンジの点滅（3回）：メモリ（DIMM）で重度の障害が発生しています。
	• オレンジの点滅（4 回）：CPU で重度の障害が発生しています。

6 電源の状態	• 緑：すべての電源装置が正常に動作中です。 • オレンジの点灯：1 台以上の電源装置が縮退運転状態にあります。 • オレンジの点滅：1 台以上の電源装置が重大な障害発生状態にあります。
7 ファンの状態	• 緑：すべてのファンモジュールが正常に動作中です。 • オレンジの点滅：1 つ以上のファンモジュールで回復不能なしきい値を超えました。
8 ネットワーク リンク アクティビティ	• 消灯：イーサネット LOM ポート リンクがアイドル状態です。 • 緑：1つ以上のイーサネットLOMポートでリンクがアクティブになっていますが、アクティビティは存在しません。 • 緑の点滅：1つ以上のイーサネットLOMポートでリンクがアクティブになっていて、アクティビティが存在します。

9 温度	• 緑：サーバは正常温度で稼働中です。 • オレンジの点灯：1 個以上の温度センサーで重大なしきい値を超えました。 • オレンジの点滅：1 個以上の温度センサーで回復不能なしきい値を超えました。

背面パネルの *LED*

図 *29* : 背面パネル *LED*

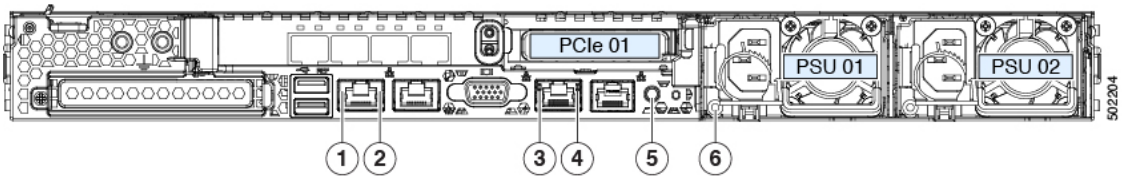


表 *24* : 背面パネル *LED*、状態の定義

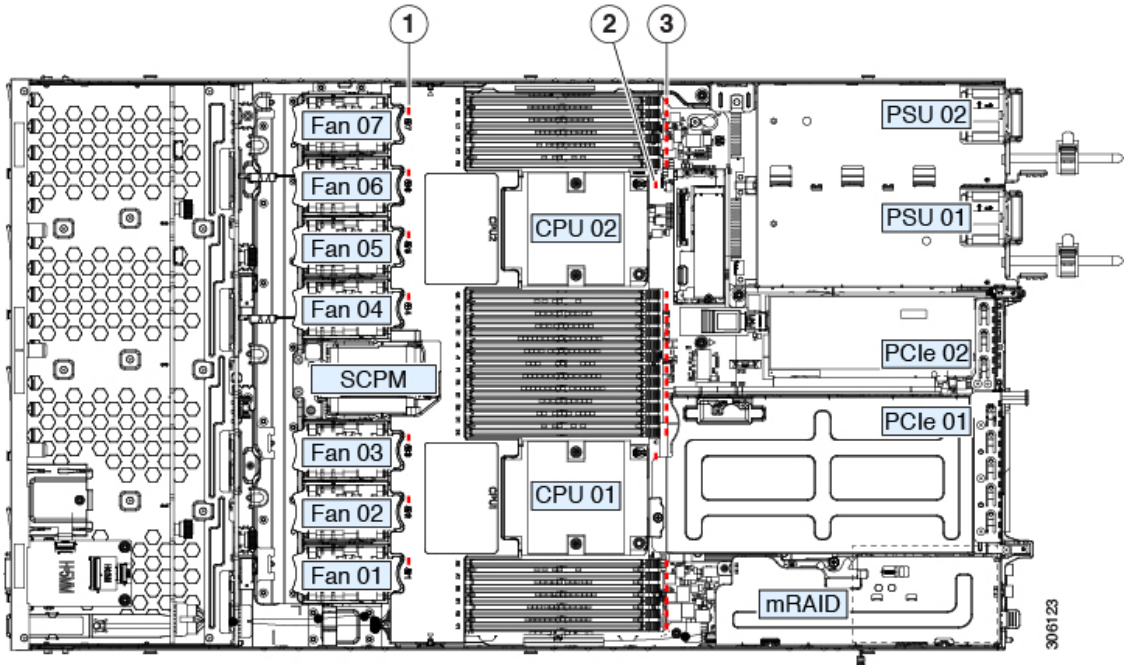
LED 名	状態
1 Gb/10 Gb イーサネット リンク速度（LAN1 と LAN2 の両方）	• オレンジ：リンク速度は 100 Mbps です。 • オレンジ：リンク速度は 1 Gbps です。 • 緑：リンク速度は 10 Gbps です。
2 Gb/10 Gb イーサネット リンク ステータス（LAN1 と LAN2 の両方）	• 消灯：リンクが確立されていません。 • 緑：リンクはアクティブです。 • 緑の点滅：アクティブなリンクにトラフィックが存在します。
3 Gb イーサネット専用管理リンク速度	• 消灯：リンク速度は 10 Mbps です。 • オレンジ：リンク速度は 100 Mbps です。 • 緑：リンク速度は 1 Gbps です。
4 Gb イーサネット専用管理リンク ステータス	• 消灯：リンクが確立されていません。 • 緑：リンクはアクティブです。 • 緑の点滅：アクティブなリンクにトラフィックが存在します。

5 背面ユニット識別	• 消灯：ユニット識別機能は使用されていません。 • 青の点滅：ユニット識別機能がアクティブです。
6 電源ステータス（各電源装置に 1 つの LED）	**AC 電源装置**： • 消灯：AC 入力なし（12 V 主電源はオフ、12 V スタンバイ電源オフ）。 • 緑の点滅：12 V 主電源はオフ、12 V スタンバイ電源はオン。 • 緑の点灯：12 V 主電源はオン、12 V スタンバイ電源はオン。 • オレンジの点滅：警告しきい値が検出されましたが、12 V 主電源はオン。 • オレンジの点灯：重大なエラーが検出されました。12 V 主電源はオフです（過電流、過電圧、温度超過などの障害）。 **DC 電源装置**： • 消灯：DC 入力なし（12 V 主電源はオフ、12 V スタンバイ電源はオフ）。 • 緑の点滅：12 V 主電源はオフ、12 V スタンバイ電源はオン。 • 緑の点灯：12 V 主電源はオン、12 V スタンバイ電源はオン。 • オレンジの点滅：警告しきい値が検出されましたが、12 V 主電源はオン。 • オレンジの点灯：重大なエラーが検出されました。12 V 主電源はオフです（過電流、過電圧、温度超過などの障害）。

内部診断 *LED*

サーバーには、CPU、DIMM、およびファンモジュールの内部障害 LED があります。

図 *30* : 内部診断 *LED* の位置

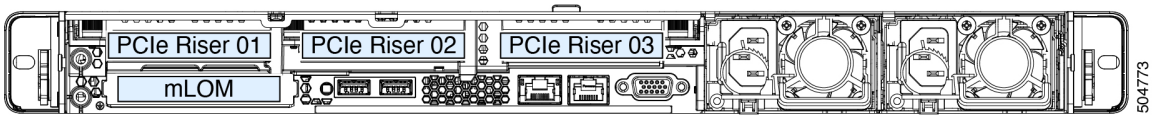


1 ファンモジュール障害 LED（マザーボード上の各ファンコネクタの後方に 1 つ） • オレンジ：ファンに障害が発生しているか、しっかりと装着されていません。 • 緑：ファンは正常です。	3 DIMM 障害 LED（マザーボード上の各 DIMM ソケットの後方に 1 つ） これらの LED は、サーバーがスタンバイ電源モードの場合にのみ動作します。 • オレンジ：DIMM に障害が発生しています。 • 消灯：DIMM は正常です。
2 CPU 障害 LED（マザーボード上の各 CPU ソケットの後方に 1 つ） これらの LED は、サーバーがスタンバイ電源モードの場合にのみ動作します。 • オレンジ：CPU に障害が発生しています。 • 消灯オフ: CPU は正常です。	-

物理ノードのケーブル接続

物理ノードは、`SE-NODE-G2`（UCS-C220-M5）の物理サーバに展開できます：

図 *31 :* ノード接続に使用される *mLOM* および *PCIe* ライザー *01* カード：*SE-NODE-G2*（*UCS-C220-M5*）



物理ノードは、次のガイドラインに従って展開できます：

- すべてのサーバーに、Nexus Dashboard 管理ネットワークへの接続に使用する Modular LAN on Motherboard（mLOM）カードが付属しています。
- ND-NODE-G5S サーバーには、「PCIe-Riser-01」スロットに 4 ポートの VIC1455 カードが含まれており (上の図を参照)、Nexus Dashboard のデータ ネットワーク接続に使用します。

（注） ノード をケーブル接続する前に、「データ ネットワーク接続」で提供される情報を使用して、データ インターフェイスの Cisco UCS VIC カードポートマッピングを確認します。データインターフェイスは、個々のホスト側のスイッチポートに接続する必要があります。これらの接続のスイッチ ポート チャネルまたは vPC を構成しないでください。

- VIC でポート チャネル機能が有効になっていることを確認します。
  - ND-NODE-L4（UCS-C225-M6）および ND-NODE-G5S（UCS-C225-M8）の場合、ポートチャネル機能は工場出荷時にデフォルトで有効になっています。これらのプラットフォームでは追加の設定は不要ですが、必要に応じて、以下の手順を使用してポートチャネル機能が正しく有効になっているかを確認したり、同機能を有効にしたりすることができます。
  - SE-NODE-G2（UCS-C220-M5）では VIC 上のポートチャンネル機能を手動で有効にする必要があります。

1. CIMC にログインします。
2. ハンバーガー アイコンをクリックして、次の場所に移動します。

   [ネットワーキング（Networking）] > [アダプタ カード（Adapter Card）] > [全般（General）] を選択します。
3. **[アダプタ カード プロパティ（Adapter Card Properties）]** エリアでは、**[ポート チャネル（Port Channel）]** フィールドを探します。

   [ポート チャネル（Port Channel）] オプションが無効になっている（チェックボックスにチェックが入っていない）場合は、Nexus Dashboard のデプロイメント プロセスを開始する前に、その機能を有効にしてください（チェックボックスにチェックを入れてください）。

ノードを管理ネットワークおよびデータ ネットワークに接続する場合：

- インターフェイスは、アクティブ/スタンバイ モードで実行されている、データ インターフェイス用（bond0）と管理インターフェイス用（bond1）の Linux ボンドとして構成されます。
- **管理ネットワーク接続**：
  - mLOM カードで `mgmt0` および `mgmt1` を使用する必要があります。
  - すべてのポートが同じ速度（1G または 10G）である必要があります。
- **データ ネットワーク接続**：
  - `SE-NODE-G2` サーバーでは、VIC1455 カードを使用する必要があります。
  - すべてのポートは同じ速度である必要があります（10G、25G、または 50G のいずれか）。
  - データ ネットワーク接続用のケーブルを接続します。一方のケーブルを `fabric0` に、もう一方のケーブルを `fabric1` に接続してください。

    `SE-NODE-G2` の `fabric0` および `fabric1` は、次のポートに対応しています。
    - ポート 1 およびポート 2 は `fabric0` に対応します
    - ポート 3 および ポート 4 は `fabric1` に対応します

    したがって、これらのポートチャネルの組み合わせのうち、いずれかを使用することができます。

最初のデータ ケーブル（**`fabric0`**）	２番目のデータ ケーブル（**`fabric1`**）
[Port-1]	ポート 3
[Port-1]	ポート 4
[Port-2]	ポート 3
[Port-2]	ポート 4

    `SE-NODE-G2` サーバで 4 ポート カードを使用する場合は、左から右に、ポート 1、ポート 2、ポート 3、ポート 4 です。

    データ ネットワーク接続には、アクティブ スタンバイとして `fabric0` と `fabric1` の両方を使用できます。

注意

- これらの接続のスイッチ ポート チャネルまたは vPC を構成しないでください。上記のサポートされているペアリングは、VIC カードでのみ有効な物理ポート マッピングを識別します。
- 上記以外のポート チャネルの組み合わせを使用してデータ ネットワーク接続用の 2 本のケーブルを接続する場合、上流に位置するスイッチで MAC 移動通知が行われ、ポートがフラップします。

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

次のステップ

物理アプライアンスとしての Nexus Dashboard の展開 （134 ページ） に移動して、Nexus Dashboard を展開します。

物理アプライアンスとしての Nexus Dashboard の展開

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

始める前に

物理アプライアンスとして Nexus Dashboard を展開する場合の前提条件と注意事項 （81 ページ） に記載されている要件とガイドラインを満たしていることを確認します：

手順

ステップ 1 最初のノードの基本情報を設定します。

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

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

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

ホストに接続したら、 **Enter** を押して続行します。

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

```
Starting Nexus Dashboard setup utility
Welcome to Nexus Dashboard 4.2.1
Press Enter to manually bootstrap your first master node...
```

c) `admin` パスワードを入力して確認します。

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

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

d) 管理ネットワーク情報を入力します。

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

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

e) 入力した譲歩をレビューし、確認します。

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

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

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

ステップ 2 プロセスが完了するまで待ちます。

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

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

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

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

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

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

ステップ 4 ログイン後、 **Meet Nexus Dashboard** の ウェルカム画面を確認し、 **ジャーニー** 画面に進みます。**クラスタの起動** 手順の下の **Go** をクリックして、ブートストラップ プロセスを開始します。

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

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

クラスタ名は、 RFC-1123 の要件に従う必要があります。

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

ステップ 6 **[クラスタのブリングアップ（Cluster Bringup）**] ウィザードの **[構成（Configuration）]** ページで、必要な情報を入力します。

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

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

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

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

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

- **キー**：NTP 認証キーを入力します。Nexus Dashboard と NTP サーバ間の NTP トラフィックを認証するために使用される暗号キーです。次の手順で NTP サーバーを定義します。複数の NTP サーバーで同じ NTP 認証キーを使用できます。
- **ID**： NTP ホストのキー ID を入力します。各 NTP キーに一意のキー ID を割り当てる必要があります。この ID は、NTP パケットの検証時に使用する適切なキーを識別するために使用されます。
- **認証タイプ**：NTPキーの認証タイプを選択します。
- このキーを信頼したい場合には、**[信頼済み（Trusted）]** チェックボックスをオンにします。信頼できないキーは NTP 認証に使用できません。

NTP認証の要件とガイドラインの完全なリストについては、全般的な前提条件とガイドライン （13 ページ） を参照してください。

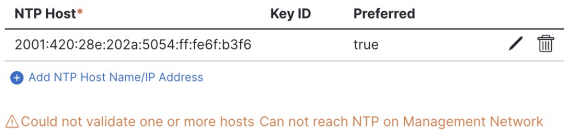
追加のNTPキーを入力する場合は、 **[+ キーの追加（+ Add Key）]** を再度クリックして、情報を入力します。

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

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

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

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



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

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

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

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

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

プロキシ サーバでは、永続 URL を許可する必要があります：

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

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

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

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

詳細設定では、次の設定を行うことができます。

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

アプリケーションおよびサービス ネットワークの詳細については、全般的な前提条件とガイドライン （13 ページ） を参照してください。

j) [次へ（Next）] をクリックします。

ステップ 7 **[ノードの詳細（Node Details）]** ページで、最初のノードの情報を更新します。

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

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

テレメトリで使用される永続的な IP アドレス機能には、BGP 構成が必要です。この機能の詳細については、BGP 構成と永続的な IP アドレス （60 ページ） および Nexus Dashboardの 永続 IP アドレス （52 ページ） セクションで説明します。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

g) **[Save]**をクリックして、変更内容を保存します。

ステップ 8 複数ノードクラスタを展開している場合、**[ノードの詳細（Node Details）]** 画面で、**[ノードの追加（Add Node）]** をクリックして、クラスタに 2 番目のノードを追加します。

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

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

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

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

c) **[名前]**に、ノードの名前を入力します。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

h) **[Save]**をクリックして、変更内容を保存します。

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

ステップ 9 （任意） 前の手順を繰り返して、追加のセカンダリ ノードまたはスタンバイ ノードに関する情報を入力します。

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

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

ステップ 10 **[ノードの詳細（Node Details）]** ページで、入力した情報を確認してから、**[次へ（Next）]**をクリックします。

ステップ 11 永続的なIPアドレスをさらに追加する場合は、**[永続的な IP（Persistent IPs）]** ページで、**[+ データ サービスの IP アドレスの追加（+ Add Data Service IP Address）]**をクリックし、 IPアドレスを入力して、チェックマークアイコン（）をクリックします。必要な回数だけこのステップを繰り返し、**[次へ（Next）]** をクリックします。

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

ステップ 12 **[概要（Summary）]** ページで設定情報をレビューして確認し、**[保存（Save）]** をクリックし、**[続行（Continue）]** をクリックして正しい展開モードを確認し、クラスタの構築を続行します。

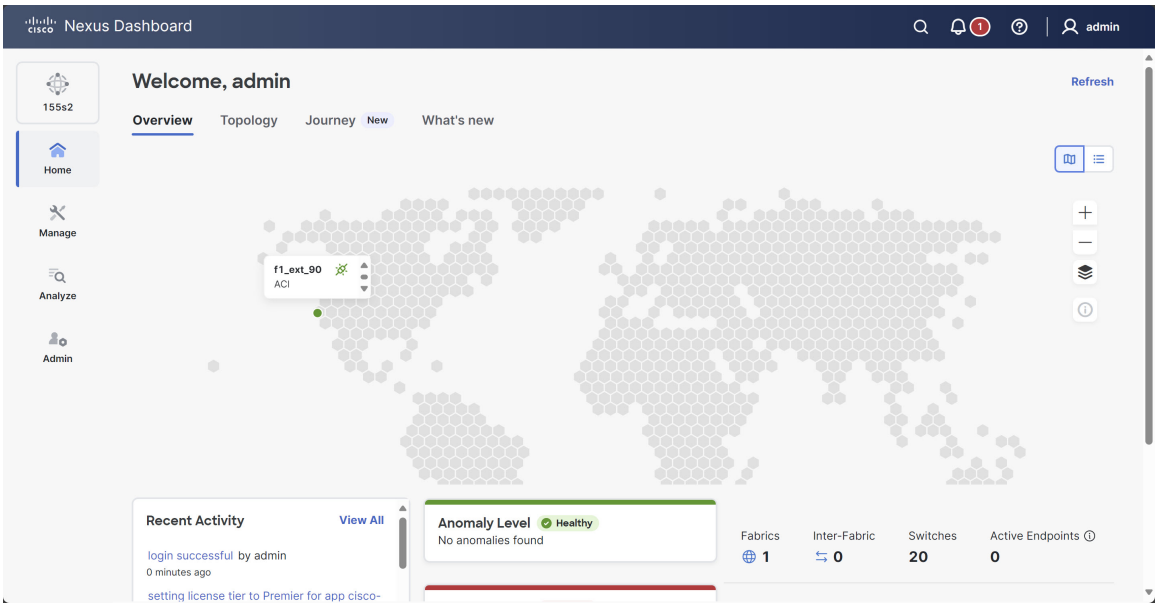
ノードのブート ストラップとクラスタの起動中に、全体的な進捗状況と各ノードの個々の進捗状況がUIに表示されます。ブートストラップの進行状況が表示されない場合は、ブラウザでページを手動で更新し、ステータスを更新してください。

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

ステップ 13 クラスタが健全であることを検証します。

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

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



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

- クラスタが収束している間、次の出力が表示されることがあります：

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

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

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

- クラスタが稼働している場合は、次の出力が表示されます。

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

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

```
deploy base system services
```

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

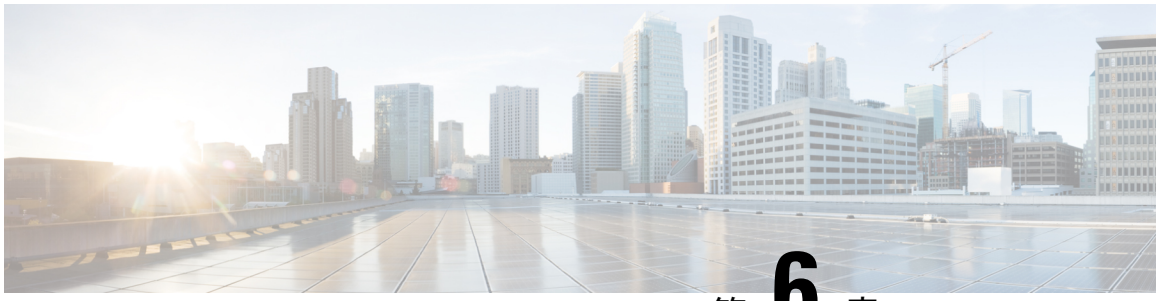
この問題を解決するには、影響を受けるノードで `acs reboot clean` コマンドを入力します。

ステップ 14 （オプション） Cisco Nexus DashboardクラスターをCisco Intersightに接続、可視性と利点を強化します。詳細な手順については、「*Cisco Intersightの操作*」 を参照してください。

ステップ 15 Nexus Dashboardを展開した後、設定情報については、このリリースのコレクションページを参照してください。

次のタスク

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



第 6 章

VMware ESX の展開

- VMware ESX で Nexus Dashboard クラスタを展開するための前提条件と注意事項 （145 ページ）
- VMware vCenter を使用した Nexus ダッシュボードの展開 （148 ページ）
- VMware ESXi での Nexus ダッシュボードの展開 （165 ページ）

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

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

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

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

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

- 前提条件とガイドライン （13 ページ） に記載されている一般的な前提条件を確認して完了します。

  この文書は、ベースとなる Nexus Dashboard クラスタを最初に展開する方法について説明します。追加ノード（セカンダリまたはスタンバイなど）で既存のクラスタを拡張する場合は、代わりに*Cisco Nexus* ダッシュボード ユーザー ガイドの「インフラストラクチャの管

理」の章を参照してください。これは、Nexus ダッシュボード UI またはオンラインで*Cisco Nexus ダッシュボード ユーザー ガイド*から利用できます。

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

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

十分なシステム リソースをもつことを確認します。

表 *25* : 展開要件

データ ノードの要件	アプリケーション ノードの要件

• VMware ESXi 7.0、7.0.1、7.0.2、7.0.3、8.0、8.0.2、8.0.3、9.0.2
• VMware vCenter を使用して展開する場合、VMware vCenter 7.0.1、7.0.2、7.0.3、8.0、8.0.2、8.0.3、9.0.2
• 各ノード/VM には、次のものが必要です。
  • 少なくとも 35,200 MHz の物理的に CPU 予約された 32 個の vCPU
  • 物理予約された 128GB の RAM
  • データ ボリューム用の 3TB SSD ストレージとシステム ボリューム用の追加の 50GB
  データノードは、次の最小パフォーマンス要件を満たすストレージに展開する必要があります。
  • SSD は、データストアに直接接続するか、RAID ホストバス アダプタ（HBA）を使用している場合は JBOD モードで接続する必要があります。
  • SSD は、混合使用/アプリケーション用に最適化する必要があります（読み取り最適化ではありません）。
  • 4K ランダム読み取り IOPS : 93000
  • 4K ランダム書き込み IOPS : 31000
• 各 Nexus ダッシュボードノードは、異なる ESXi サーバに展開することを推奨します。
	• VMware ESXi 7.0、7.0.1、7.0.2、7.0.3、8.0、8.0.2、8.0.3、9.0.2
	• VMware vCenter を使用して展開する場合、VMware vCenter 7.0.1、7.0.2、7.0.3、8.0、8.0.2、8.0.3、9.0.2
	• 各ノード/VM には、次のものが必要です。
	  • 少なくとも 17,600 MHz の物理的 CPU で予約された 16 個の vCPU
	  • 物理予約された 64GB の RAM
	  • データ ボリューム用に 500GB HDD または SSD ストレージ、システム ボリューム用に追加の 50GB
	  一部の機能では、アプリ ノードをより高速な SSD ストレージに展開する必要がありますが、他の機能では HDD をサポートしています。Nexus Dashboard キャパシティ プランニング ツールをチェックして、正しいタイプのストレージを使用していることを確認してください。
	• 各 Nexus Dashboard 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 データ インターフェイスの VLAN ID を構成する場合は、仮想ゲスト VLAN タギング（VGT）モードの VMware vCenter のデータ インターフェイス ポート グループで

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

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

  ESXi クラスタ レベルで DRS を有効にしている場合は、次のセクションで説明するように、展開時に Nexus ダッシュボード VM に対して明示的に無効にする必要があります。
- コンテンツ ライブラリによる展開はサポートされていません。
- VMware スナップショットは、電源がオフになっている Nexus Dashboard VM でのみサポートされており、同じクラスタに属するすべての Nexus Dashboard VM で同時に実行する必要があります。ロールバックが必要な場合、全ての Nexus Dashboard VM は、同時にまとめてロール バックする必要があります。

  VM のスナップショットはサポートされません。
- Cisco は、ネストされた仮想化環境の使用をサポートしていません。仮想化ハイパーバイザ（例：ESXi上のKVM）上で動作している仮想マシンに Nexus Dashboard を展開することは、サポート対象外の構成であり、パフォーマンスの低下やシステムの不安定化を招く可能性があります。
- ノードを ESXi に直接展開するか、VMware vCenter を使用して展開するかを選択できます。

  VMware vCenter を使用して展開する場合は、VMware vCenter を使用した Nexus ダッシュボードの展開 （148 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 （165 ページ） で説明されている手順に従います。

VMware vCenter を使用した Nexus ダッシュボードの展開

ここでは、VMware vCenter を使用して Cisco Nexus ダッシュボード クラスタを展開する方法について説明します。ESXi に直接展開する場合は、代わりに VMware ESXi での Nexus ダッシュボードの展開 （165 ページ） で説明されている手順に従ってください。

始める前に

- VMware ESX で Nexus Dashboard クラスタを展開するための前提条件と注意事項（145 ページ） に記載されている要件とガイドラインを満たしていることを確認します。

手順

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

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

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

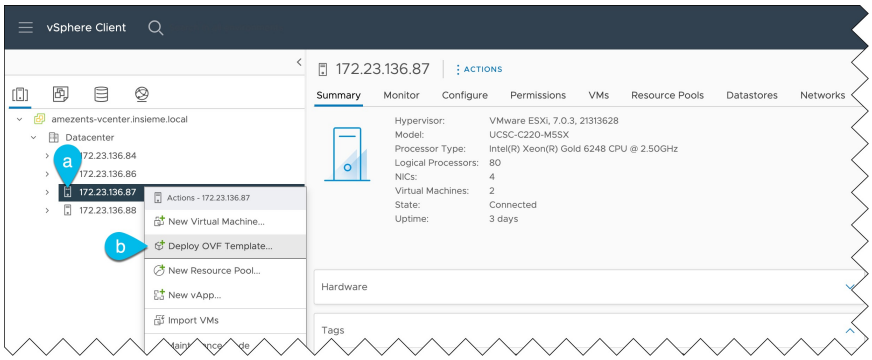
b) 左側のサイドバーから、ダウンロードする Nexus ダッシュボードのリリースバージョンを選択します。

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

ステップ 2 VMware vCenter にログインします。

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

ステップ 3 新しい VM 展開を開始します。

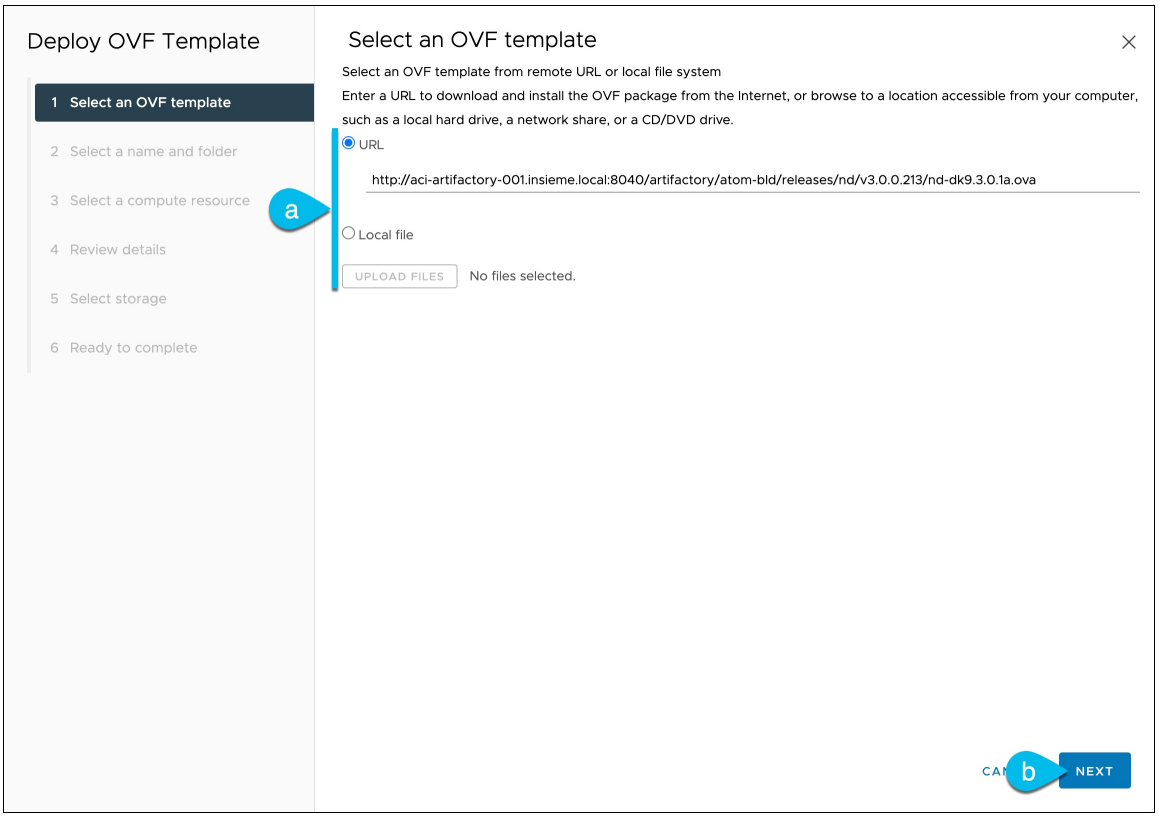


a) VM を展開する ESX ホストを右クリックします。

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

[Deploy OVF Template] ウィザードが表示されます。

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



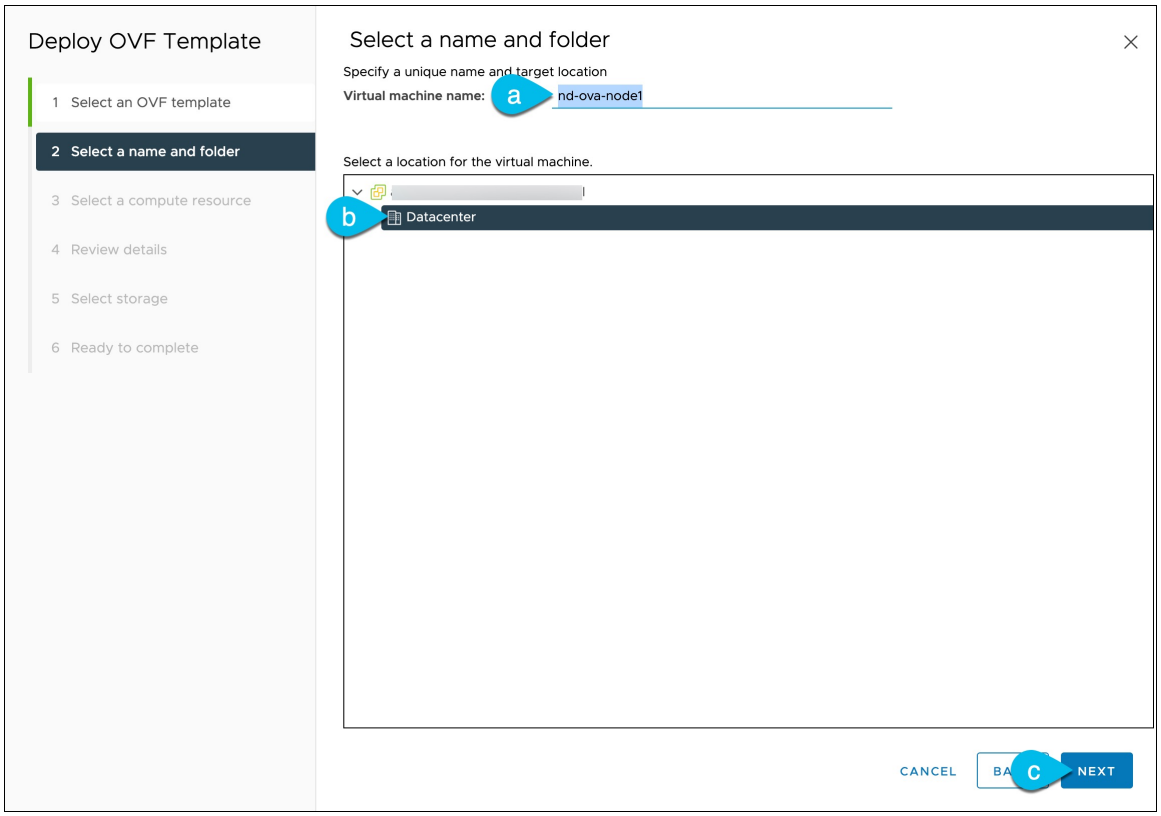
a) イメージの場所を指定します。

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

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

b) **[次へ（Next）]** をクリックして続行します。

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



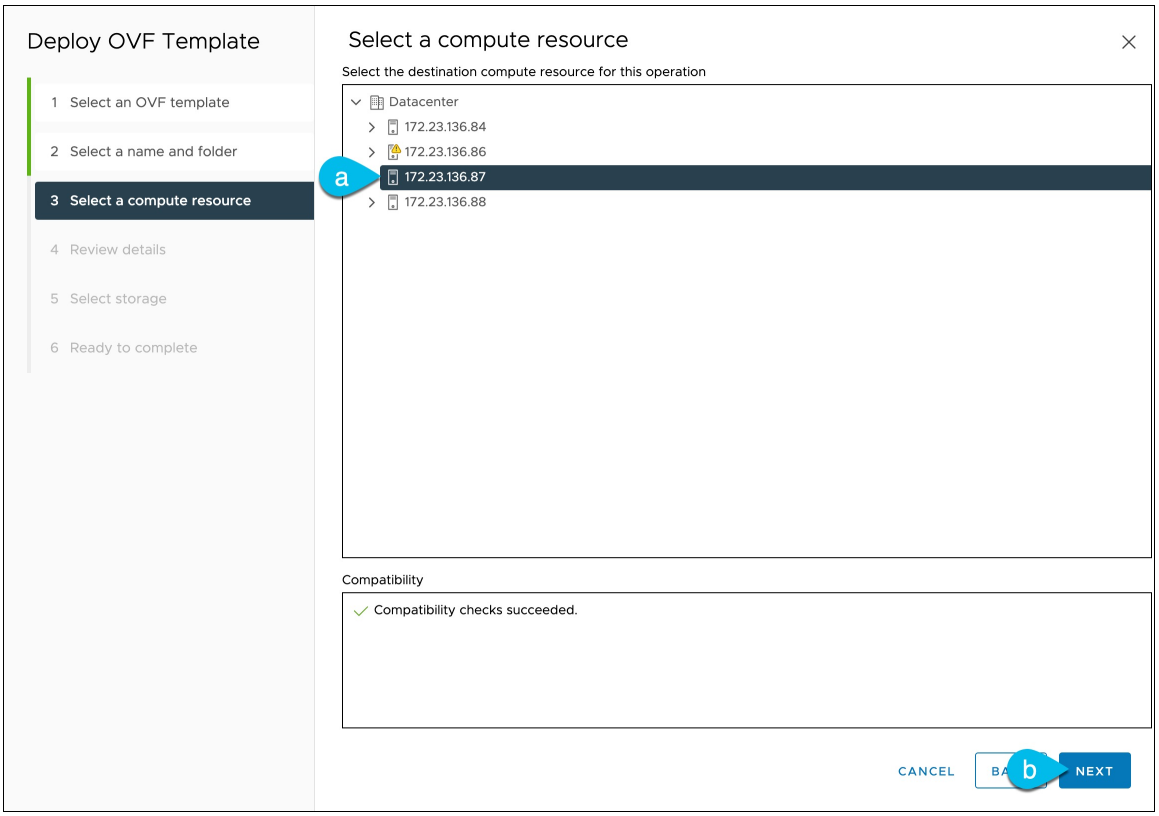
a) 仮想マシンの名前を入力します。

たとえば、`nd-ova-node1` です。

b) 仮想マシンのストレージ場所を選択します。

c) **[次へ（Next）]** をクリックして、続行します。

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

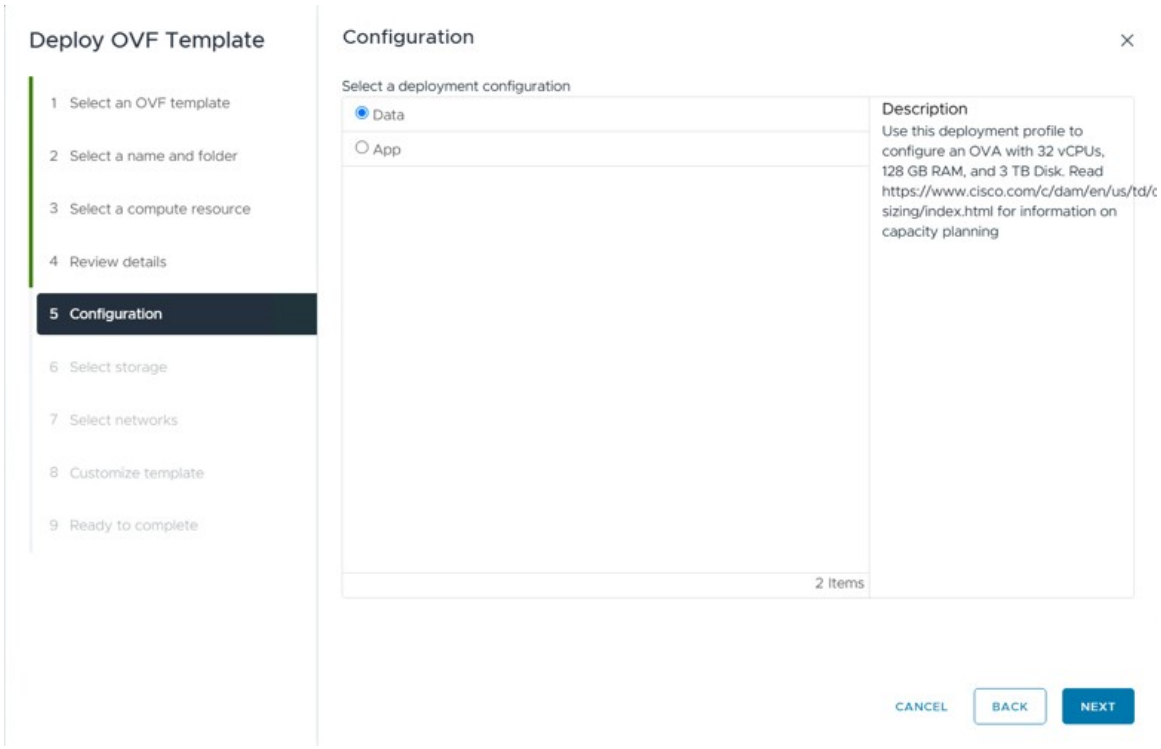


a) 仮想マシンの vCenter データセンターと ESX ホストを選択します。

b) **[次へ（Next）]** をクリックして、続行します。

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

ステップ 8 [設定] 画面で、展開するノードプロファイルを選択します。

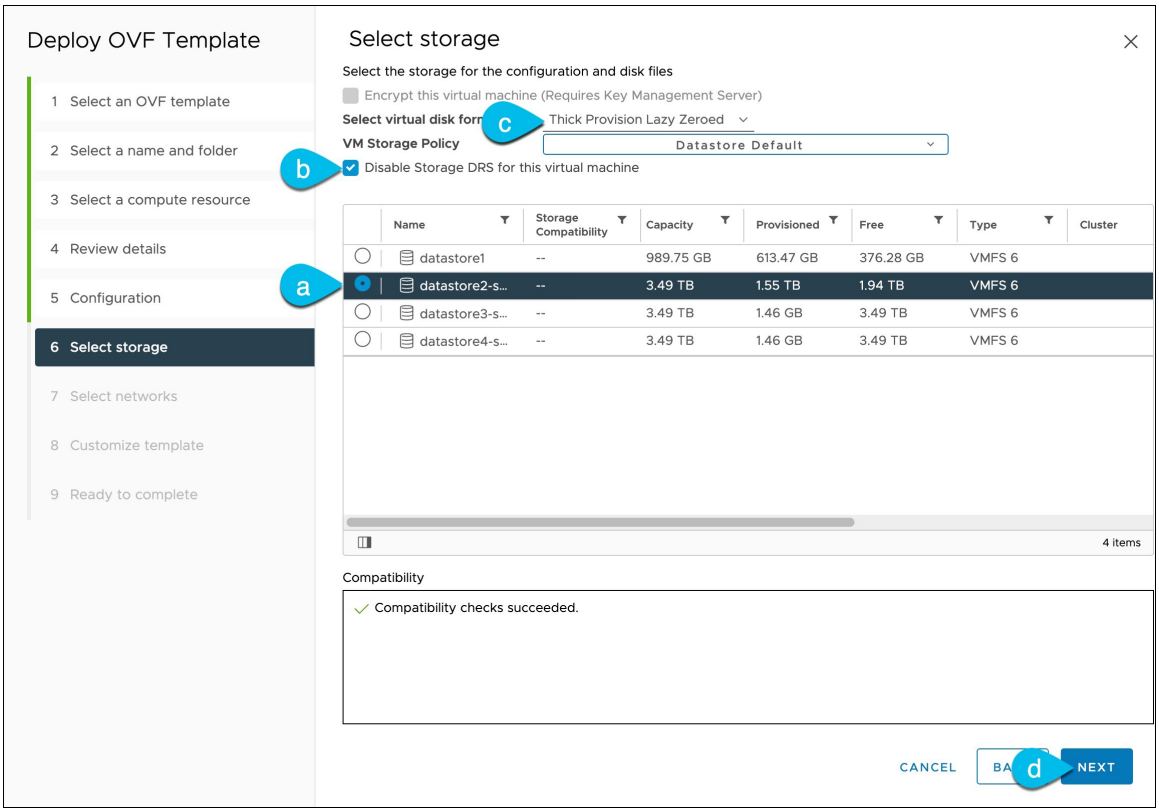


a) ユースケースの要件に基づいて、アプリまたはデータ ノード プロファイルを選択します。

ノードプロファイルの詳細については、「VMware ESX で Nexus Dashboard クラスタを展開するための前提条件と注意事項 （145 ページ）」を参照してください。

b) **[次へ（Next）]** をクリックして、続行します。

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



a) 仮想マシンのデータストアを選択します。

ノードごとに一意のデータストアを推奨します。

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

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

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

d) **[次へ（Next）]** をクリックして、続行します。

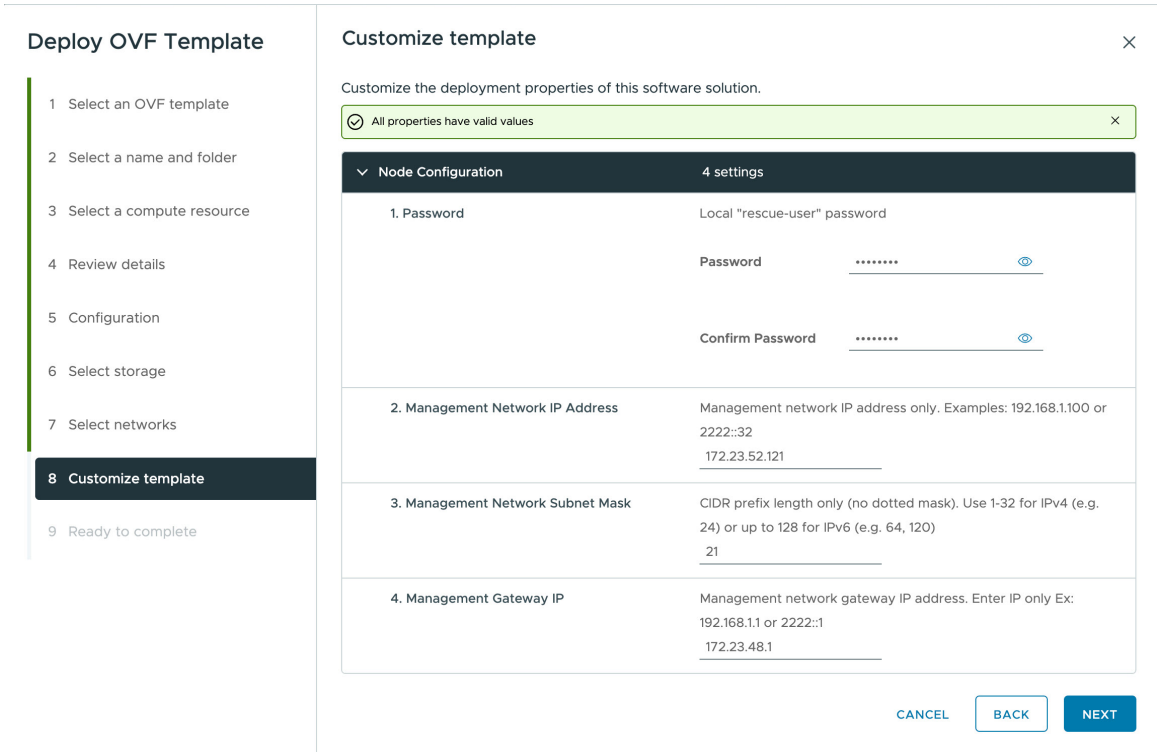
ステップ 10 [**ネットワークの選択**]画面で、Nexusダッシュボードの管理およびデータネットワークのVMネットワークを選択し、[**次へ**] をクリックして続行します。

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

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

これらのネットワークの詳細については、「展開の概要と要件」の章の「全般的な前提条件とガイドライン （13 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) **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。

b) **管理ネットワークの IP アドレス**を入力します。

たとえば、`192.168.1.100` などです。

c) **管理ネットワーク サブネット マスク**を入力します。

このエントリは、 CIDR プレフィックス長のみである必要があります。例：

- IPv4 の場合は`24` または `32`
- IPv6 は、最大`128` です。

d) **管理ゲートウェイ IP** を入力します。

e) [次へ（Next）] をクリックして次に進みます。

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

ステップ 13 以前のステップを繰り返し、追加のノードを展開します。

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

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

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

ステップ 14 VM の展開が完了するまで待ちます。

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

時刻の同期を無効にするには、次の手順を実行します。

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

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

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

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

ステップ 17 ログイン後、 **Meet Nexus Dashboard** の ウェルカム画面を確認し、 **ジャーニー** 画面に進みます。**クラスタの起動** 手順の下の **Go** をクリックして、ブートストラップ プロセスを開始します。

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

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

クラスタ名は、 RFC-1123 の要件に従う必要があります。

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

ステップ 19 **[クラスタのブリングアップ（Cluster Bringup）**] ウィザードの **[構成（Configuration）]** ページで、必要な情報を入力します。

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

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

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

- **キー**：NTP 認証キーを入力します。Nexus Dashboard と NTP サーバ間の NTP トラフィックを認証するために使用される暗号キーです。次の手順で NTP サーバーを定義します。複数の NTP サーバーで同じ NTP 認証キーを使用できます。
- **ID**： NTP ホストのキー ID を入力します。各 NTP キーに一意のキー ID を割り当てる必要があります。この ID は、NTP パケットの検証時に使用する適切なキーを識別するために使用されます。
- **認証タイプ**：NTPキーの認証タイプを選択します。
- このキーを信頼したい場合には、**[信頼済み（Trusted）]** チェックボックスをオンにします。信頼できないキーは NTP 認証に使用できません。

NTP認証の要件とガイドラインの完全なリストについては、全般的な前提条件とガイドライン（13 ページ） を参照してください。

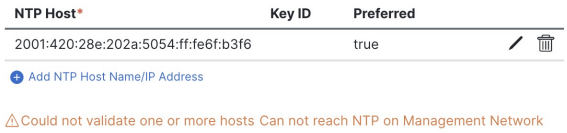
追加のNTPキーを入力する場合は、**[+ キーの追加（+ Add Key）]** を再度クリックして、情報を入力します。

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

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

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

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



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

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

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

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

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

プロキシ サーバでは、永続 URL を許可する必要があります：

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

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

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

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

詳細設定では、次の設定を行うことができます。

- **アプリ ネットワーク**：Nexus Dashboard でアプリケーションで使用されるアドレス空間です。ターゲット ネットワークの IP アドレスとネットマスクを入力します。
- **サービス ネットワーク**：Nexus Dashboard とそのプロセスで使用される内部ネットワークです。ターゲット ネットワークの IP アドレスとネットマスクを入力します。

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

アプリケーションおよびサービス ネットワークの詳細については、全般的な前提条件とガイドライン （13 ページ） を参照してください。

j) [次へ（Next）] をクリックします。

ステップ 20 **[ノードの詳細（Node Details）]** ページで、最初のノードの情報を更新します。

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

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

テレメトリで使用される永続的な IP アドレス機能には、BGP 構成が必要です。この機能の詳細については、BGP 構成と永続的な IP アドレス （60 ページ） およびNexus Dashboardの 永続 IP アドレス （52 ページ） セクションで説明します。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

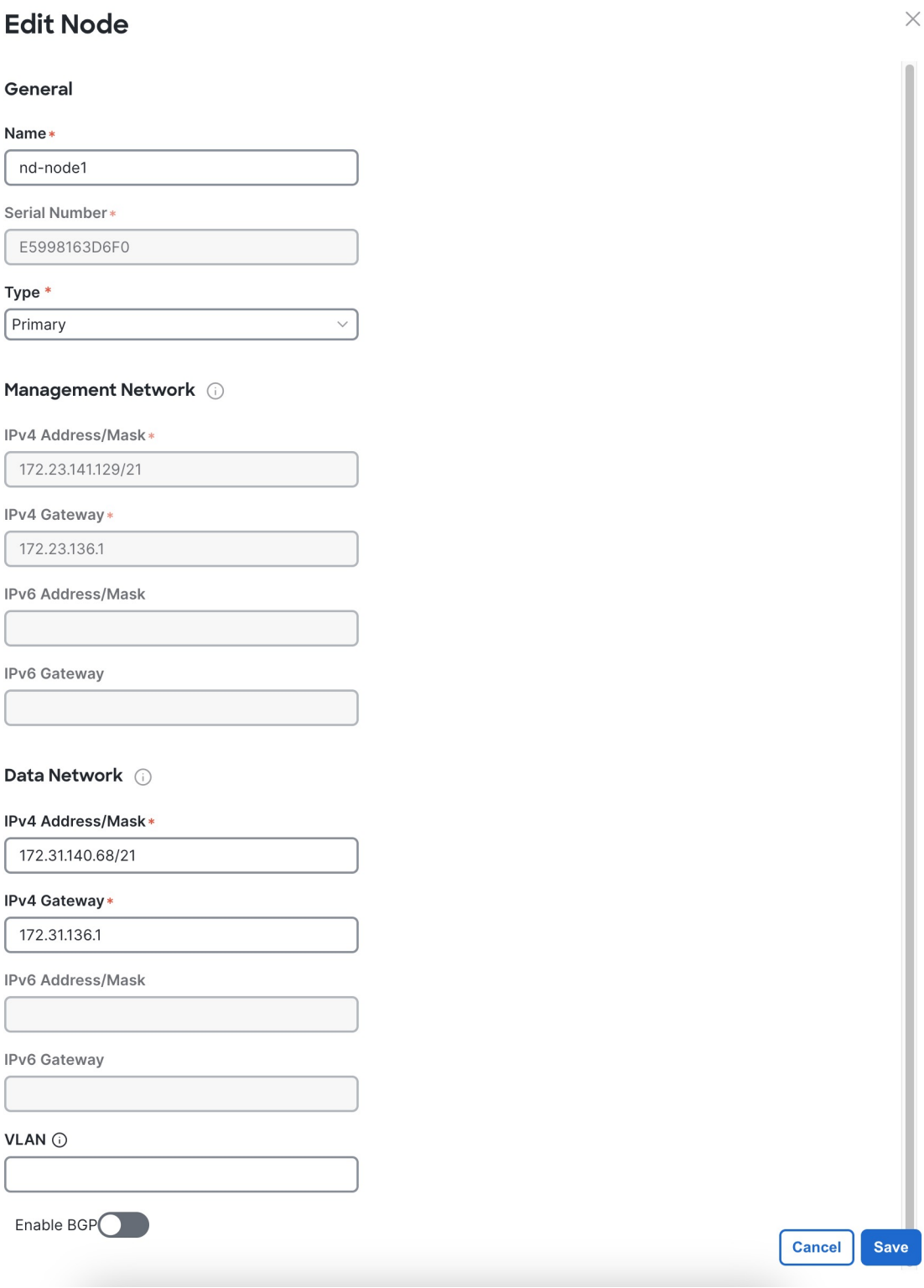
[+ IPv4 BGP ピアの追加（+ Add IPv4 BGP peer）] をクリックして、ピアを追加できます。

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

g) **[Save]**をクリックして、変更内容を保存します。

ステップ 21 [**ノードの詳細（Node Details**）] 画面で、[**ノードの追加（Add Node**）] をクリックして、クラスタに 2 番目のノードを追加します。

単一ノード クラスタを展開する場合は、この手順をスキップします。



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

ノードの初期構成手順で、管理ネットワーク情報とパスワードを定義しました。

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

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

c) ノードの **[名前（Name）]** を入力します。

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

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

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

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

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

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

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

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

永続 IP アドレス機能には BGP 設定が必要です。この機能については、BGP 構成と永続的な IP アドレス （60 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。

- IPv6 専用の場合、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 22 （任意）前の手順を繰り返して、追加のセカンダリ ノードまたはスタンバイ ノードに関する情報を入力します。

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

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

ステップ 23 **[ノードの詳細（Node Details）]** ページで、入力した情報を確認してから、**[次へ（Next）]**をクリックします。

ステップ 24 永続的なIPアドレスをさらに追加する場合は、**[永続的な IP（Persistent IPs）]** ページで、**[+ データ サービスの IP アドレスの追加（+ Add Data Service IP Address）]**をクリックし、IPアドレスを入力して、チェックマークアイコン（）をクリックします。必要な回数だけこのステップを繰り返し、**[次へ（Next）]** をクリックします。

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

ステップ 25 **[概要（Summary）]** ページで設定情報をレビューして確認し、**[保存（Save）]** をクリックし、**[続行（Continue）]** をクリックして正しい展開モードを確認し、クラスタの構築を続行します。

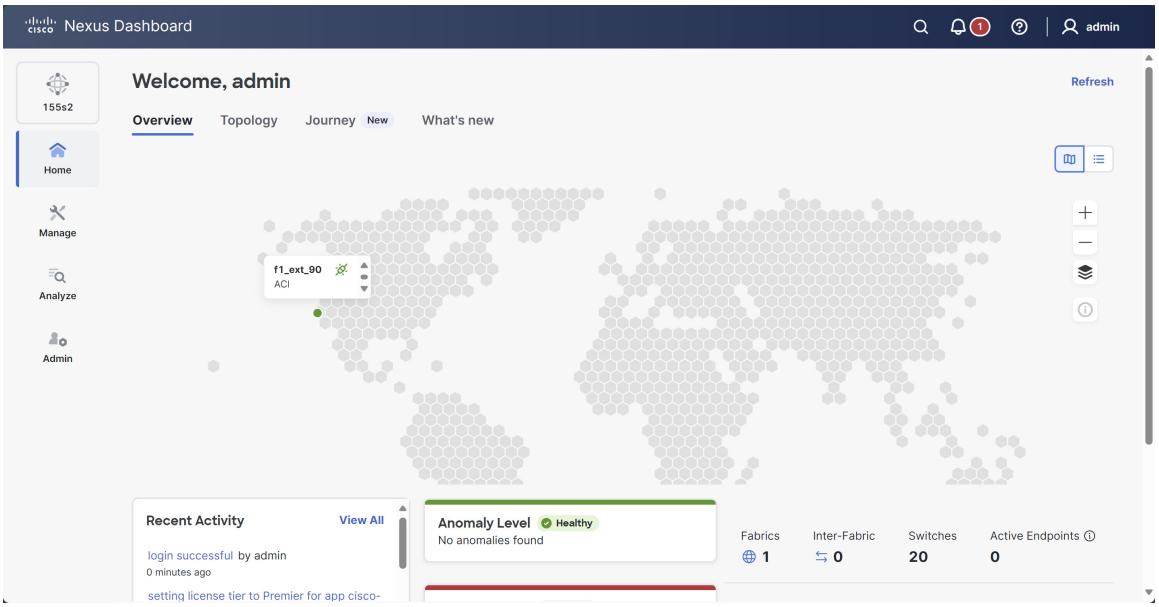
ノードのブート ストラップとクラスタの起動中に、全体的な進捗状況と各ノードの個々の進捗状況がUIに表示されます。ブートストラップの進行状況が表示されない場合は、ブラウザでページを手動で更新し、ステータスを更新してください。

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

ステップ 26 クラスタが健全であることを検証します。

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

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



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

- クラスタが収束している間、次の出力が表示されることがあります：

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

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

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

- クラスタが稼働している場合は、次の出力が表示されます。

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

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

`deploy base system services`

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

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

ステップ 27 （オプション） Cisco Nexus DashboardクラスターをCisco Intersightに接続、可視性と利点を強化します。詳細な手順については、「*Cisco Intersightの操作*」 を参照してください。

ステップ 28 Nexus Dashboardを展開した後、設定情報については、このリリースのコレクションページを参照してください。

次のタスク

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

VMware ESXi での Nexus ダッシュボードの展開

ここでは、VMware ESXi で Cisco Nexus ダッシュボード クラスタを展開する方法について説明します。vCenter を使用して展開する場合は、代わりに VMware ESXi での Nexus ダッシュボードの展開 （165 ページ） で説明されている手順に従ってください。

始める前に

- VMware ESX で Nexus Dashboard クラスタを展開するための前提条件と注意事項（145 ページ） に記載されている要件とガイドラインを満たしていることを確認します。

手順

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

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

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

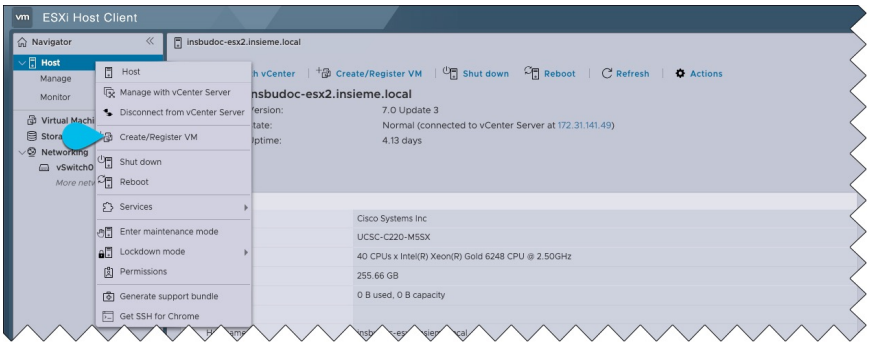
b) 左側のサイドバーから、ダウンロードする Nexus ダッシュボードのリリースバージョンを選択します。

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

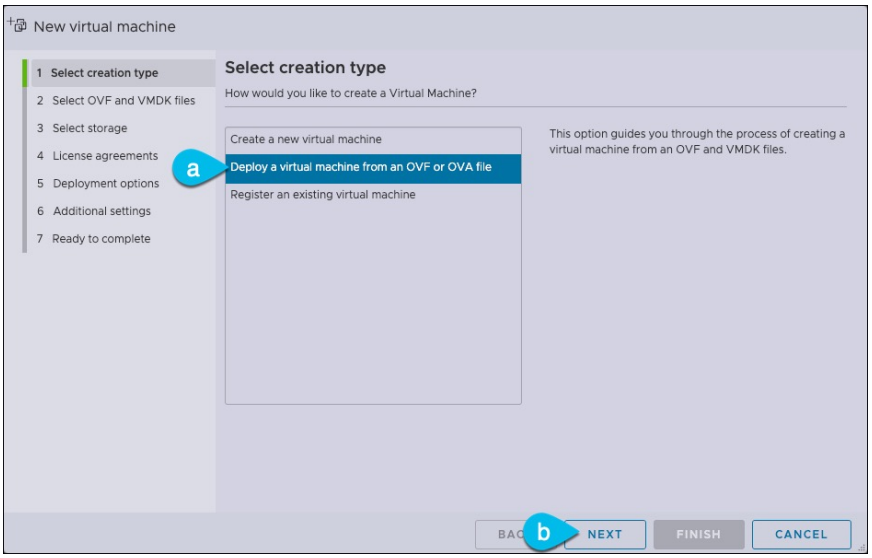
ステップ 2 VMware ESXi にログインします。

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

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



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



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

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

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

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

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

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

  Nexus Dashboard ネットワークについては、全般的な前提条件とガイドライン （13 ページ） で説明しています。

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

ノード プロファイルについては、VMware ESX で Nexus Dashboard クラスタを展開するための前提条件と注意事項 （145 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 ログイン後、 **Meet Nexus Dashboard** の ウェルカム画面を確認し、 **ジャーニー** 画面に進みます。**クラスタの起動** 手順の下の **Go** をクリックして、ブートストラップ プロセスを開始します。

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

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

クラスタ名は、 RFC-1123 の要件に従う必要があります。

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

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

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

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

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

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

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

- **キー**：NTP 認証キーを入力します。Nexus Dashboard と NTP サーバ間の NTP トラフィックを認証するために使用される暗号キーです。次の手順で NTP サーバーを定義します。複数の NTP サーバーで同じ NTP 認証キーを使用できます。
- **ID**： NTP ホストのキー ID を入力します。各 NTP キーに一意のキー ID を割り当てる必要があります。この ID は、NTP パケットの検証時に使用する適切なキーを識別するために使用されます。
- **認証タイプ**：NTPキーの認証タイプを選択します。
- このキーを信頼したい場合には、**[信頼済み（Trusted）]** チェックボックスをオンにします。信頼できないキーは NTP 認証に使用できません。

NTP認証の要件とガイドラインの完全なリストについては、全般的な前提条件とガイドライン（13 ページ） を参照してください。

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

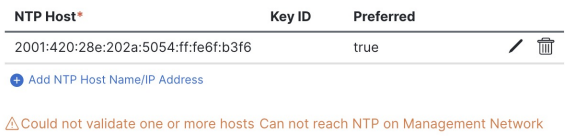
f) NTP認証を有効にした場合は、 **[+ NTP ホスト名/ IPアドレスの追加（+Add NTP Host Name/ IP Address）]**をクリックし、必要な情報を入力し、チェックマークアイコンをクリックして情報を保存します。

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

NTP 認証が無効になっている場合、このフィールドはグレー表示されます。

- このホストを優先したい場合は、**[優先（Preferred）]** チェックボックスをオンにします。

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



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

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

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

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

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

プロキシ サーバでは、永続 URL を許可する必要があります：

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

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

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

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

詳細設定では、次の設定を行うことができます。

- **アプリ ネットワーク**：Nexus Dashboard でアプリケーションで使用されるアドレス空間です。ターゲット ネットワークの IP アドレスとネットマスクを入力します。
- **サービス ネットワーク**：Nexus Dashboard とそのプロセスで使用される内部ネットワークです。ターゲット ネットワークの IP アドレスとネットマスクを入力します。

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

アプリケーションおよびサービス ネットワークの詳細については、全般的な前提条件とガイドライン （13 ページ） を参照してください。

j) [次へ（Next）] をクリックします。

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

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

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

テレメトリで使用される永続的な IP アドレス機能には、BGP 構成が必要です。この機能の詳細については、BGP 構成と永続的な IP アドレス （60 ページ） およびNexus Dashboardの 永続 IP アドレス （52 ページ） セクションで説明します。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

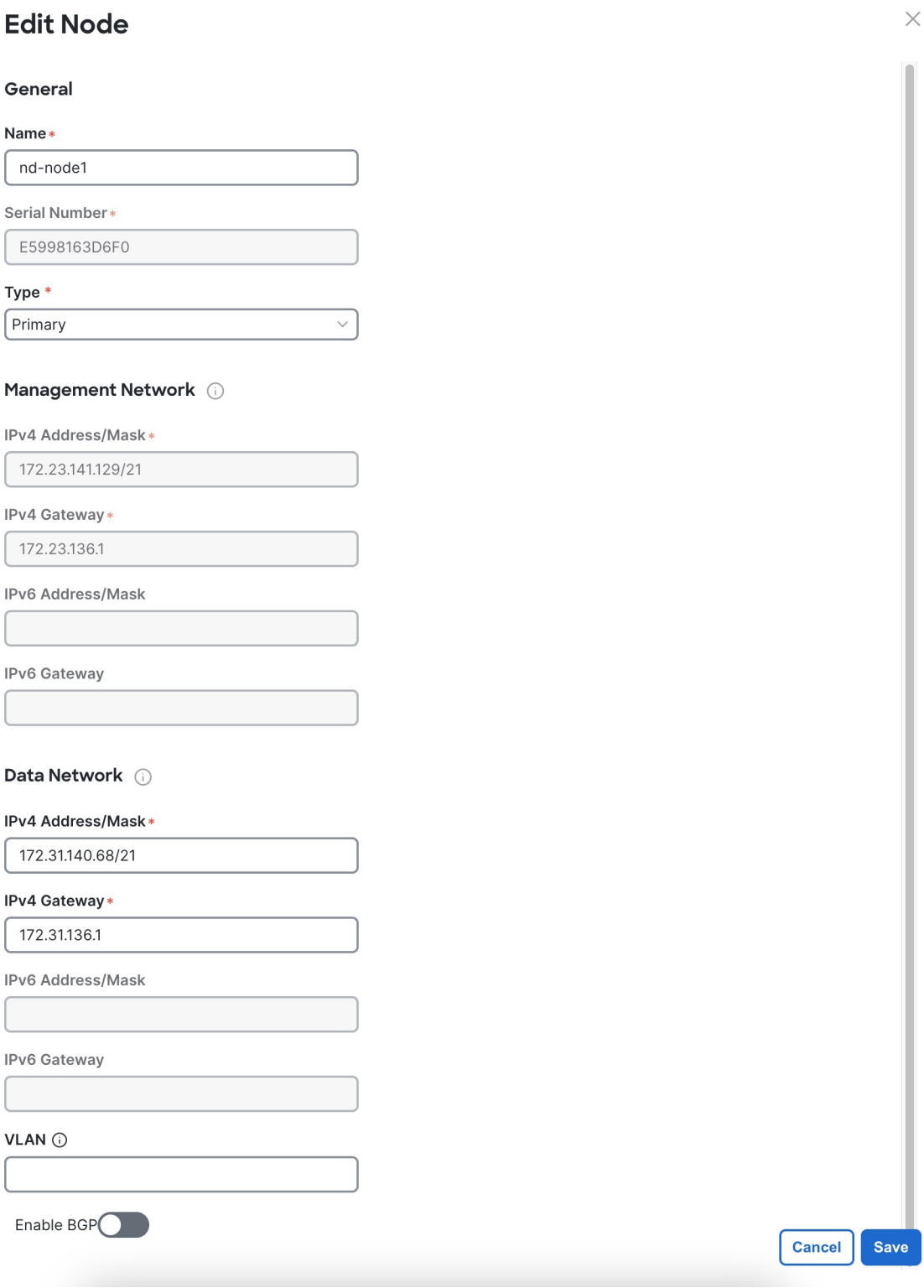
[+ IPv4 BGP ピアの追加（+ Add IPv4 BGP peer）] をクリックして、ピアを追加できます。

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

g) **[Save]**をクリックして、変更内容を保存します。

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

単一ノード クラスタを展開する場合は、この手順をスキップします。



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

ノードの初期構成手順で、管理ネットワーク情報とパスワードを定義しました。

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

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

c) ノードの **[名前（Name）]** を入力します。

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

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

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

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

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

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

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

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

永続 IP アドレス機能には BGP 設定が必要です。この機能については、BGP 構成と永続的な IP アドレス （60 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。

- IPv6 専用の場合、このノードの**ルータ ID**。

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

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

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

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

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

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

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

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

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

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

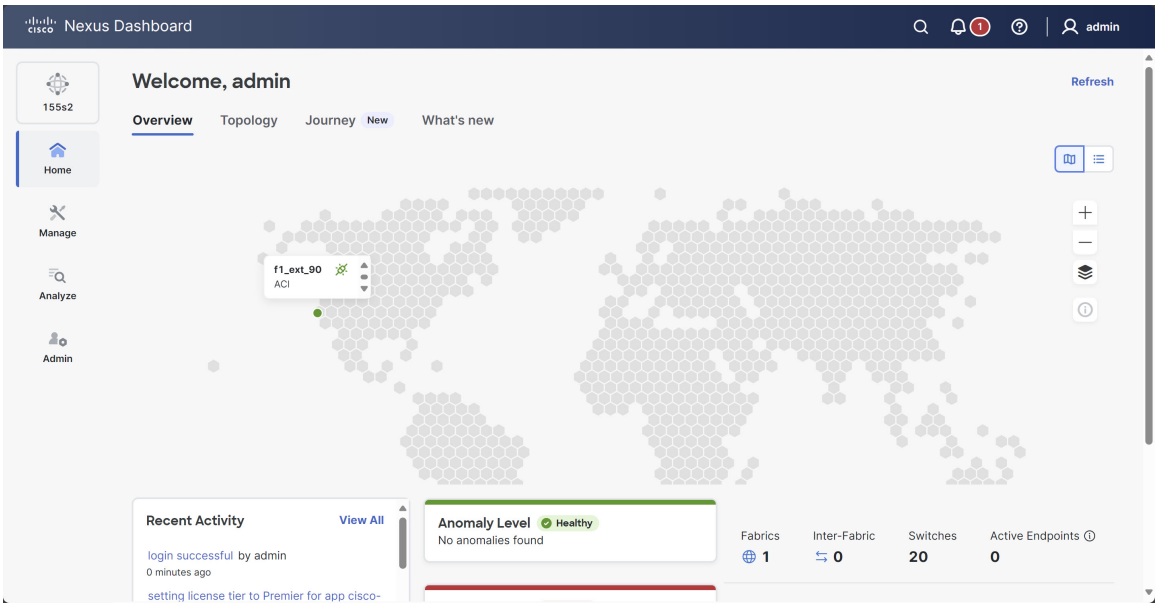
ノードのブート ストラップとクラスタの起動中に、全体的な進捗状況と各ノードの個々の進捗状況がUIに表示されます。ブートストラップの進行状況が表示されない場合は、ブラウザでページを手動で更新し、ステータスを更新してください。

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

ステップ 25 クラスタが健全であることを検証します。

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

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



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

- クラスタが収束している間、次の出力が表示されることがあります：

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

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

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

- クラスタが稼働している場合は、次の出力が表示されます。

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

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

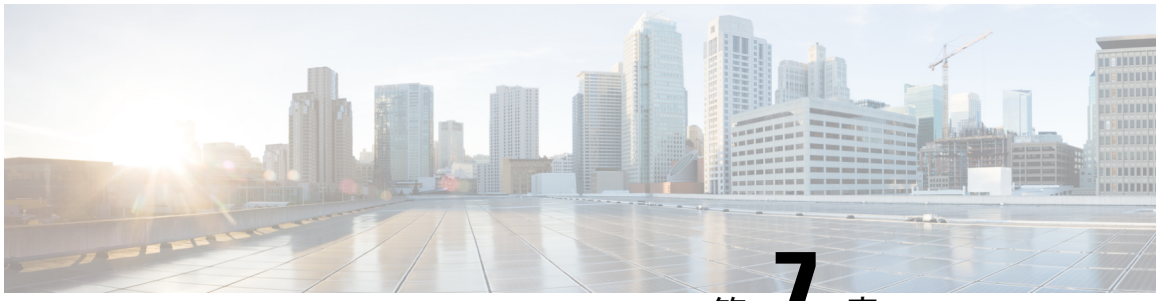
```
deploy base system services
```

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

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

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

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



第 7 章

Linux KVMでの展開

- Linux KVM で Nexus Dashboard クラスタを展開するための前提条件と注意事項 （179 ページ）
- QCOW2 イメージのデプロイメント スクリプトについて （181 ページ）
- Linux KVM での Nexus ダッシュボードの展開 （190 ページ）

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

（注） ユーザーがLinux KVMホストにパッチを適用、アップグレード、または変更するときにNexus Dashboard の可用性を維持するためのプラットフォーム レベルのガイダンスについては、『*Cisco Nexus Dashboard on KVM*』 ドキュメントを参照してください。

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

- KVM フォーム ファクタが拡張性要件をサポートする必要があります。

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

- 前提条件とガイドライン （13 ページ） に記載されている一般的な前提条件を確認して完了します。

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

- KVM には十分なシステムリソースが必要です。また、各ノードには専用のディスクパーティションが必要です。詳細については、「システム リソースを理解する （181 ページ）」を参照してください。

- ディスクの I/O 遅延は 20 ミリ秒以下である必要があります。

  「Linux KVM ストレージ デバイスの I/O 遅延の確認 （180 ページ）」を参照してください。

- Cisco は、ネストされた仮想化環境の使用をサポートしていません。仮想化ハイパーバイザ（例：ESXi上のKVM）上で動作している仮想マシンにNexus Dashboardを展開することは、サポート対象外の構成であり、パフォーマンスの低下やシステムの不安定化を招く可能性があります。

- デフォルトでは、多くの RAID コントローラが ライト スルー モードに設定されています。このモードでは、オペレーティング システムの成功を確認する前に、コントローラはデータが SSD フラッシュに物理的に書き込まれることを確認します。

  すべての同期書き込みに必要な「ハンドシェイク」により、ディスク I/O 遅延は推奨値を超えてスパイク可能性があります。これは通常、 Nexus Dashboard でテレメトリが有効になっている場合に発生し、高いディスク I/O を必要とします。

  ディスク I/O のパフォーマンスを最適化するには、 RAIDコントローラのオンボードRAMを高速バッファとして使用する必要があります。「書き込みポリシー」が ライトバック (WB) に設定されていることを確認します。これにより、コントローラはオンボードキャッシュを使用して書き込みをすぐに確認できます。

- KVM の導入は、NX- OS および ACI ファブリックのみならず、SAN の展開でサポートされています。

- Red Hat Enterprise Linux 8.8、8.10、または 9.4 に展開する必要があります。また、すべてのノードが同じ Linux バージョンで実行されていることを強く推奨します。

- OS のリブート時にNexus Dashboardを稼働させるには、RHEL ホスト オペレーティング システムの `fstab設定` ファイルにUUIDを追加する必要があります。これが、RHEL オペレーティング システムの再起動時にNexus Dashboard を保持できる唯一の方法です。

- また、 Nexus Dashboad の展開に必要な次のネットワーク ブリッジをホスト レベルで構成する必要があります。

  - 管理網ブリッジ（mgmt-bridge）： Nexus Dashboad を管理するための外部ネットワーク。

  - データ網ブリッジ（data-bridge）： Nexus Dashboad 内でクラスタリングを形成するために使用される内部ネットワーク。

- 各 Nexus Dashboard ノードは異なる KVM ハイパーバイザに展開することを推奨します。

Linux KVM ストレージ デバイスの I/O 遅延の確認

Linux KVM に Nexus Dashboard クラスタを展開する場合、KVM のストレージ デバイスの遅延は 20 ミリ秒未満である必要があります。QCOW2 イメージに `kvm_deployer` デプロイメント スクリプトを使用する場合は、「QCOW2 イメージのデプロイメント スクリプトについて （181 ページ）」で説明されているように、パフォーマンス検証手順でこれを実行します。

手動で Linux KVM ストレージ デバイスの I/O 遅延を確認したい場合は、次の手順を実行します。

手順

ステップ 1 テスト ディレクトリを作成します。

たとえば、 `test-data`という名前のディレクトリを作成します。

ステップ 2 フレキシブル I/O テスター（FIO）を実行します。

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

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

システム リソースを理解する

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

表 *26*: ノード当たりのリソース要件

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

Linux KVM での Nexus ダッシュボードの展開 （190 ページ）の手順を実行するときに、フォーム ファクタに関する上記の情報を知っておく必要があります

QCOW2 イメージのデプロイメント スクリプトについて

Nexus Dashboard は、RHEL や Nutanix など、さまざまな環境での KVM 仮想化をサポートしています。Nexus Dashboard の展開は通常、QCOW2 イメージを使用して行われます。しかし、

KVM のバリアントとホスト構成が多様であるため、サポートされているバージョンの追跡と最適なデバイスエミュレーションのパフォーマンス確保に課題が生じています。

QCOW2 イメージのデプロイメント スクリプトは、QCOW2 イメージにパッケージ化されたデプロイメントの検証およびオーケストレーション スクリプトを提供することで、これらの課題に対処します。このスクリプトは、デプロイメント プロセスを合理化、互換性を確保し、サポートされているプラットフォーム間で一貫したパフォーマンス標準を維持するように設計されています。

主な機能

QCOW2 イメージのデプロイメント スクリプトの主な機能は次のとおりです。

- **プラットフォーム互換性チェック**：基盤となるホストのオペレーティング システムがサポートされているディストリビューションとバージョンであることを確認します。
- **リソース検証**： ホストが CPU、メモリ、ストレージ リソースなどの最小コンピューティング要件を満たしているかどうかを評価します。
- **パフォーマンス検証**：
  - **ディスク I/O と網の遅延**： ディスク I/O やネットワーク I/O の遅延などの主要なパフォーマンス インジケータを測定し、適格な範囲内にあることを確認します。
  - **デバイス エミュレーション:** 適切なデバイス エミュレーション（ネットワーク インターフェイスやリモート対応ディスク デバイスなど）が最適なパフォーマンスのために使用可能であることを確認します。
- **展開のオーケストレーション**： 単一ノードとマルチノードの両方のクラスタのデプロイメント プロセスを自動化し、適切なデバイス マッピング（ネットワークやストレージ デバイスなど）でリモート対応マシンをオーケストレーションします。

ストレージは最も一般的なボトルネックであるため、このスクリプトではストレージを「パフォーマンス層」に分類します。

- **ディスクのタイプと配置（SSD/NVMe）**： 高 IOP ワークロードを検証します。
- **RAID 対 JBOD**： 書き込み速度を検証します。
- **リモート ストレージ（iSCSI/ FC/NFS）**： 「Pre-Flight Latency Check」を実行します。
  - **同期遅延**： 標準規格アプリケーションの場合は 10 ミリ秒未満、高性能データベースの場合は 1 ミリ秒未満である必要があります。
  - **IOPS 検証**： 一時的な `FIO` テストを使用して、必要な IOS を確認します。

QCOW2 イメージのデプロイメント スクリプトの前提条件

QCOW2 イメージのデプロイメント スクリプトの前提条件

要件	詳細
ND qcow2 image	Nexus Dashboard `.qcow2` イメージ ファイルへのローカル パス
ネットワーク情報	3 管理 IP + ゲートウェイ
Go toolchain	送信元から構築するには、Go 1.22+ を使用します（または、事前作成のバイナリを使用します。）

QCOW2 イメージのデプロイメント スクリプトを使用します

手順

ステップ 1 デプロイメント スクリプトを含む tar ファイルを見つけます。

tar ファイルは、QCOW2 イメージと同じ場所に用意する必要があります。たとえば、4.3.1 リリース以降の Nexus Dashboard のソフトウェア ダウンロード サイト には、次のように QCOW2 イメージのデプロイメントスクリプトを含む tar ファイルが QCOW2 イメージ自体と同じエリアに表示されます。

```
nd-dk9.4.3.1.175.qcow2.tar.gz
```

ステップ 2 デプロイメント スクリプトを含む tar ファイルをダウンロードします。

ステップ 3 qcow2 tar ファイルを解凍します。

例：

```
tar -xzvf nd-dk9.4.3.1.175.qcow2.tar.gz
```

tar ファイルを抽出し、ディレクトリの内容をリストした後、次のような出力が表示されます。

```
#ls -lrt
total 24730576
-rwxr-xr-x 1 root root    35991736 May  5 23:35 kvm_deployer
-rw-r--r-- 1 root root 12651498496 May 17 03:44 nd-dk9.4.3.1.175.qcow2
-rw-r--r-- 1 root root 12636610743 May 18 22:44 nd-dk9.4.3.1.175.qcow2.tar.gz
```

ステップ 4 **kvm_deployer config** コマンドを使用して、デプロイメント スクリプトで使用する yaml ファイルを作成します。

デプロイメントのタイプに基づいて、各段階で適切な選択をしてください。

- たとえば、1 ノードの yaml ファイルを生成するには：

```
# ./kvm_deployer config

Configure Nexus Dashboard deployment:
 Deployment Platform (kvm/nutanix): kvm
 Image Path (qcow2): /home/nd-base/nd-dk9.4.3.1.58.qcow2
 Cluster Size: 1
 VM Type (app/data/large/xlarge): app
 Admin Password:
Configure current node:
 KVM Host:
  Management Network Bridge: nd_mgmt
```

```
  Data Network Bridge: nd_data
  Disk Path (device or mount point, absolute path): /home/nd-node1
 Nexus Dashboard:
  VM Name (lowercase, numbers, dashes, max 63 chars): node1
  Management Network (e.g., 192.168.1.100/24): 192.168.1.128/25
  Management Gateway IP: 192.168.1.129
[□] Configuration Summary:
 Deployment Platform        : kvm
 Image Path (qcow2)         : /home/nd-base/nd-dk9.4.3.1.58.qcow2
 Admin Password             : [hidden]
 VM Type                    : app
 VMs:
  VM Name                    : node1
   Disk Path                  : /home/nd-node1
   Management Network Bridge  : nd_mgmt
   Data Network Bridge        : nd_data
   Management Network         : 192.168.1.128/25
   Management Gateway IP      : 192.168.1.129
 Proceed with current config? (y/n): y
 File name to save configuration: kvm_1node_deploy.yaml
```

- 3 ノードの yaml ファイルを生成する場合：

```
# ./kvm_deployer config
Configure Nexus Dashboard deployment:
 Deployment Platform (kvm/nutanix): kvm
 Image Path (qcow2): /home/nd-base/nd-dk9.4.3.1.175.qcow2
 Cluster Size: 3
 VM Type (app/data/large/xlarge): app
 Admin Password:
Configure current node:
 KVM Host:
  Management Network Bridge: nd_mgmt
  Data Network Bridge: nd_data
  Disk Path (device or mount point, absolute path): /home/nd-node1
 Nexus Dashboard:
  VM Name (lowercase, numbers, dashes, max 63 chars): node1
  Management Network (e.g., 192.168.1.100/24): 192.168.1.128/25
  Management Gateway IP: 192.168.1.129
Configure remote to deploy vm (2):
 KVM Host:
  IP Address: 192.168.1.133
  Username (ssh): root
. Password (ssh: root):
  Management Network Bridge: nd_mgmt
  Data Network Bridge: nd_data
  Disk Path (device or mount point, absolute path): /home/nd-node2
 Nexus Dashboard:
  VM Name (lowercase, numbers, dashes, max 63 chars): node2
  Management Network (e.g., 192.168.1.100/24): 192.168.1.128/25
  Management Gateway IP: 192.168.1.130
Configure remote to deploy vm (3):
 KVM Host:
  IP Address: 192.168.1.133
  Username (ssh): root
. Password (ssh: root):
  Management Network Bridge: nd_mgmt
  Data Network Bridge: nd_data
  Disk Path (device or mount point, absolute path): /home/nd-node3
 Nexus Dashboard:
  VM Name (lowercase, numbers, dashes, max 63 chars): node3
  Management Network (e.g., 192.168.1.100/24): 192.168.1.128/25
  Management Gateway IP: 192.168.1.131
```

```
[□] Configuration Summary:
 Deployment Platform        : kvm
 Image Path (qcow2)         : /home/nd-base/nd-dk9.4.3.1.175.qcow2
 Admin Password             : [hidden]
 VM Type                    : app
 VMs:
  VM Name                    : node1
   Disk Path                  : /home/nd-node1
   Management Network Bridge  : nd_mgmt
   Data Network Bridge        : nd_data
   Management Network         : 192.168.1.128/25
   Management Gateway IP      : 192.168.1.129
  Host OS IP Address         : 192.168.1.133
  Host OS Username           : root
  Host OS Password           : [hidden]
  VM Name                    : node2
   Disk Path                  : /home/nd-node2
   Management Network Bridge  : nd_mgmt
   Data Network Bridge        : nd_data
   Management Network         : 192.168.1.128/25
   Management Gateway IP      : 192.168.1.130
  Host OS IP Address         : 192.168.1.133
  Host OS Username           : root
  Host OS Password           : [hidden]
  VM Name                    : node3
   Disk Path                  : /home/nd-node3
   Management Network Bridge  : nd_mgmt
   Data Network Bridge        : nd_data
   Management Network         : 192.168.1.128/25
   Management Gateway IP      : 192.168.1.131
 Proceed with current config? (y/n): y
 File name to save configuration: kvm_3node_deploy.yaml
```

ステップ 5 （オプション）必要に応じて、テキストエディタを使用して yaml ファイルに保存された情報を検証します。

たとえば、前述の 3 ノードの例では、yaml ファイルには次のような情報が含まれます。

```
deployment_type: kvm
image_path: /home/nd-base/nd-dk9.4.3.1.175.qcow2
cluster_size: "3"
vms:
- name: node1
  disk_path: /home/nd-node1
  management_network: 192.168.1.128/25
  management_gateway: 192.168.1.129
  management_bridge: nd_mgmt
  data_bridge: nd_data
  host_ip: ""
  host_user: ""
  host_password: ""
- name: node2
  disk_path: /home/nd-node2
  management_network: 192.168.1.135/25
  management_gateway: 192.168.1.129
  management_bridge: nd_mgmt
  data_bridge: nd_data
  host_ip: 192.168.1.133
  host_user: root
  host_password: <host_password>
- name: node3
  disk_path: /home/nd-node3
  management_network: 192.168.1.136/25
```

```
  management_gateway: 192.168.1.129
  management_bridge: nd_mgmt
  data_bridge: nd_data
  host_ip: 192.168.1.133
  host_user: root
  host_password: <hostpword>
flavor: app
admin_password: <adminpword>
```

ステップ 6 yaml ファイルを入力として使用して、デプロイメント スクリプトを実行します。

```
./kvm_deployer deploy --config kvm_3node_deploy.yaml
```

次のような出力が表示されます。

```
Deploying VM node1 using kvm
  Cleanup old images
  [□] Cleaned image /home/nd-node1/boot.img
  [□] Cleaned image /home/nd-node1/disk.img
  [□] Cleaned image /home/nd-node1/config-drive.img
  Creating boot disk, it can take several minutes, pls wait
  [□] Boot disk created successfully
  Creating raw disk, it can take several minutes, pls wait
  [□] Raw disk created successfully
  Creating configuration drive
  [□] Configuration drive created successfully

  Starting VM
  [□] VM started successfully
[□] KVM VM: node1 deployed successfully
Deploying VM node2 using kvm
 Copying file /home/nd-base/nd-dk9.4.3.1.175.qcow2 to /home/nd-node2/nd-dk9.4.3.1.175.qcow2
 [□] File /home/nd-base/nd-dk9.4.3.1.175.qcow2 copied to /home/nd-node2/nd-dk9.4.3.1.175.qcow2
  Cleanup old images
  [□] Cleaned image /home/nd-node2/boot.img
  [□] Cleaned image /home/nd-node2/disk.img
  [□] Cleaned image /home/nd-node2/config-drive.img
  Creating boot disk, it can take several minutes, pls wait
  [□] Boot disk created successfully
  Creating raw disk, it can take several minutes, pls wait
  [□] Raw disk created successfully
  Creating configuration drive
  Copying file /home/nd-node1/node2-bootstrap.json to /home/nd-node2/apic-sn-cfg-mount/bootstrap.json

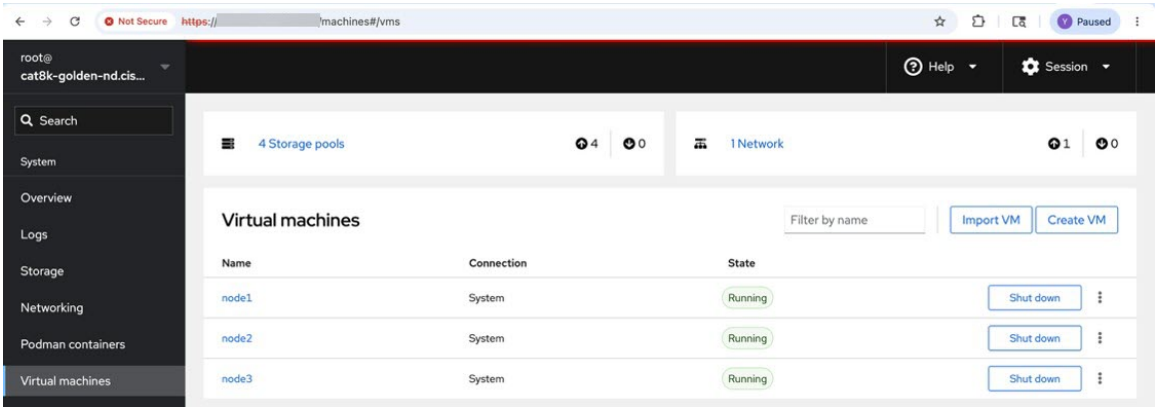
  [□] File /home/nd-node1/node2-bootstrap.json copied to
/home/nd-node2/apic-sn-cfg-mount/bootstrap.json
  [□] Configuration drive created successfully
  Starting VM
  [□] VM started successfully
[□] KVM VM: node2 deployed successfully
Deploying VM node3 using kvm
 Copying file /home/nd-base/nd-dk9.4.3.1.175.qcow2 to /home/nd-node3/nd-dk9.4.3.1.175.qcow2
 [□] File /home/nd-base/nd-dk9.4.3.1.175.qcow2 copied to /home/nd-node3/nd-dk9.4.3.1.175.qcow2
  Cleanup old images
  [□] Cleaned image /home/nd-node3/boot.img
  [□] Cleaned image /home/nd-node3/disk.img
  [□] Cleaned image /home/nd-node3/config-drive.img
  Creating boot disk, it can take several minutes, pls wait
  [□] Boot disk created successfully
  Creating raw disk, it can take several minutes, pls wait
  [□] Raw disk created successfully
  Creating configuration drive
  Copying file /home/nd-node1/node3-bootstrap.json to /home/nd-node3/apic-sn-cfg-mount/bootstrap.json

  [□] File /home/nd-node1/node3-bootstrap.json copied to
```

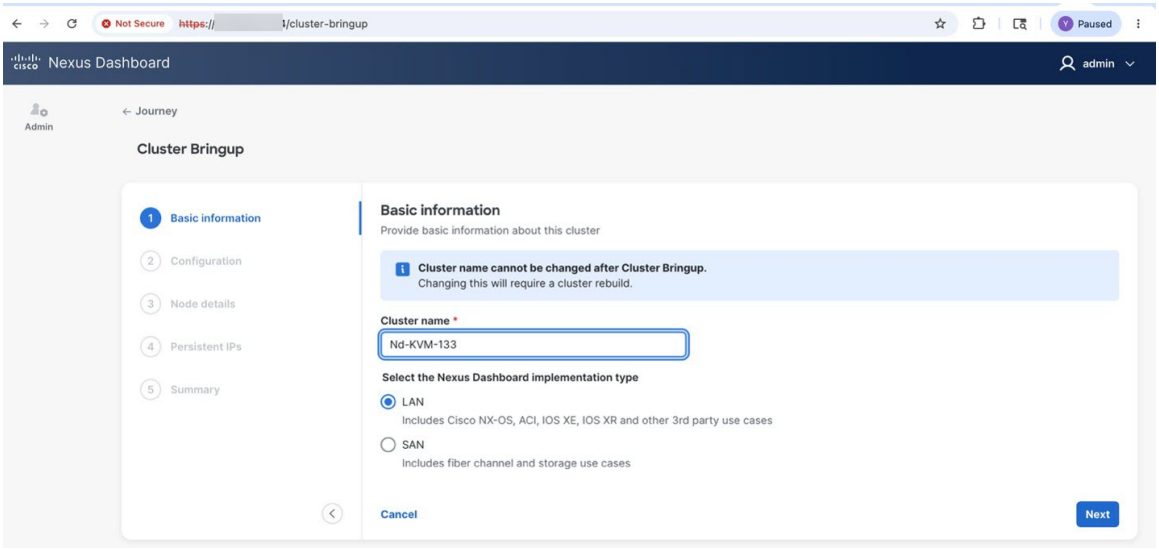
```
/home/nd-node3/apic-sn-cfg-mount/bootstrap.json
  [□] Configuration drive created successfully
  Starting VM
  [□] VM started successfully
[□] KVM VM: node3 deployed successfully
```

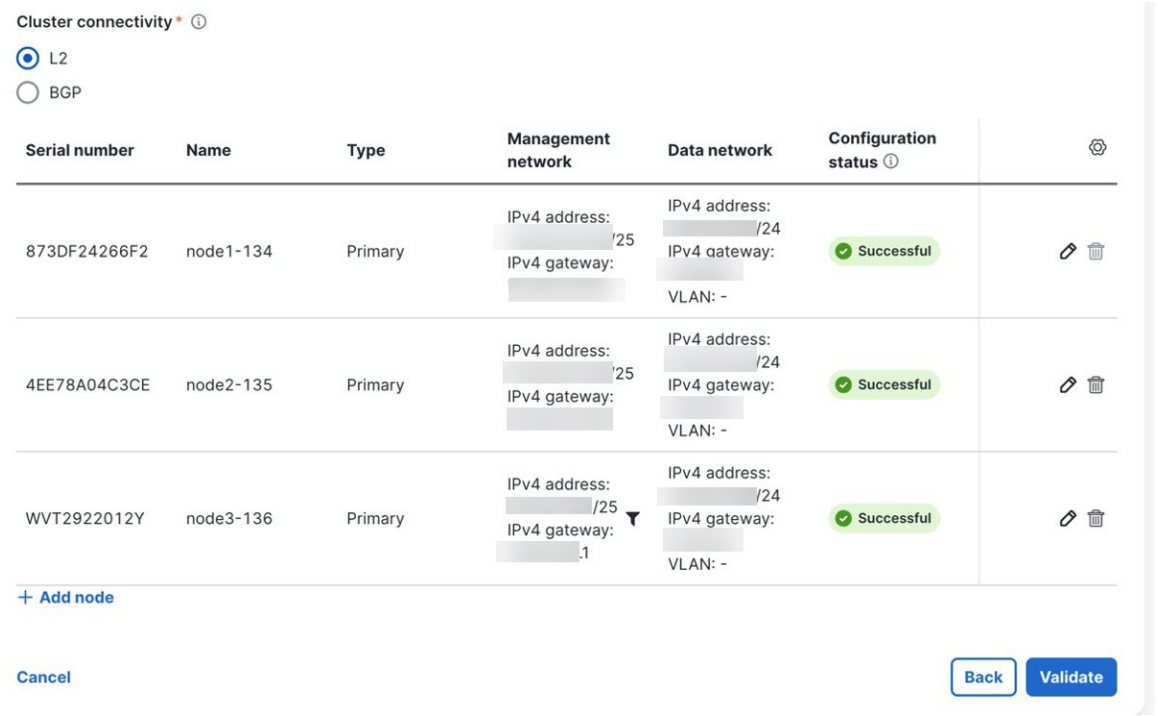
ステップ 7 展開後の手順を完了します。

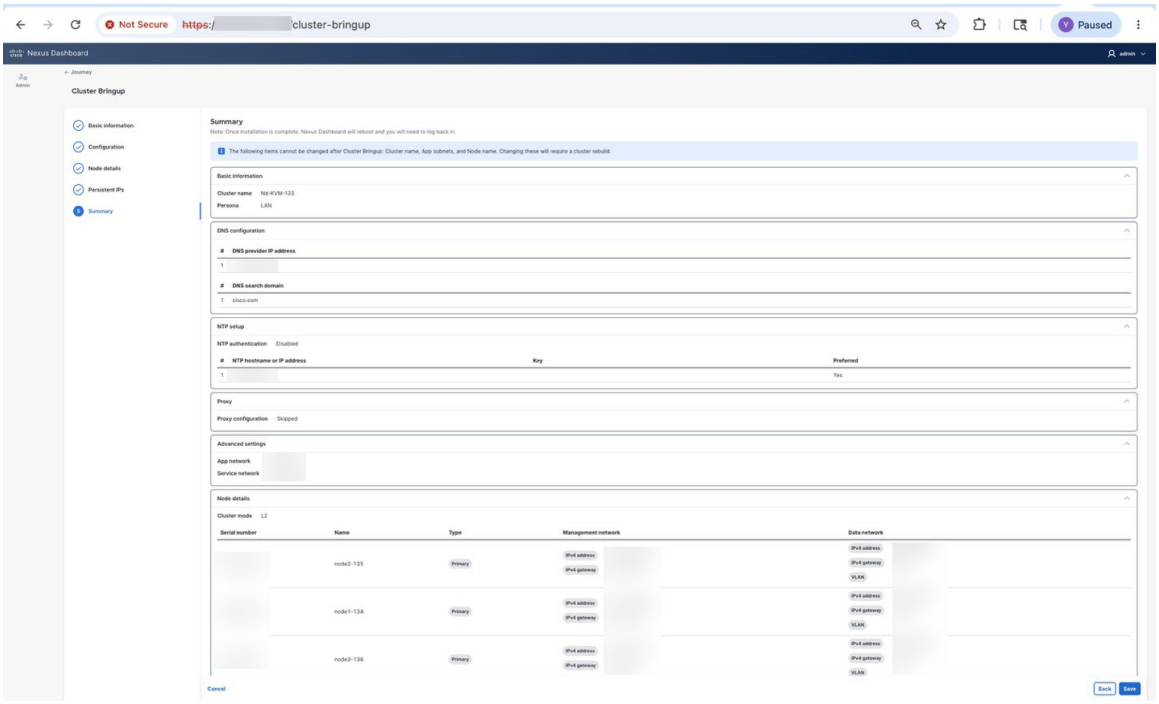
a) **RHEL ホストでのVMs の確認**：www:// を開きます<RHEL_host _ip>:9090 を実行し、3 つすべての VMs の電源がオンで、正常であることを確認します。



b) **クラスタの形成**：すべてのノードが実行されたら、設定の管理IPアドレスを使用して、Nexus Dashboard UI を介して Nexus Dashboard クラスタのセットアップを完了します。




Cluster connectivity *
L2
BGP
Serial number
Name
Type
Management network
Data network
Configuration status
873DF24266F2
node1-134
Primary
IPv4 address: /25
IPv4 gateway:
IPv4 address: /24
IPv4 gateway:
VLAN: -
Successful
4EE78A04C3CE
node2-135
Primary
IPv4 address: /25
IPv4 gateway:
IPv4 address: /24
IPv4 gateway:
VLAN: -
Successful
WVT2922012Y
node3-136
Primary
IPv4 address: /25
IPv4 gateway: .1
IPv4 address: /24
IPv4 gateway:
VLAN: -
Successful
+ Add node
Cancel
Back
Validate


Not Secure
https:/ cluster-bringup
Paused
Nexus Dashboard
Cluster Bringup
Basic information
Configuration
Node details
Persistent IPs
Summary
Summary
Basic information
DNS configuration
NTP setup
Proxy
Advanced settings
Node details
Cancel
Back
Save

オプションの展開後のタスク

トラブルシューティング

症状	検証
Authentication failure（認証失敗）	設定でユーザ名 および パスワードを確認します
VM が IP を取得できない	cloud-init `management_network`が有効な CIDR 表記法および正しいゲートウェイであることを確認します。

デプロイメントを破棄します

デプロイメントを破棄したい場合このコマンドを入力します：

```
./kvm_deployer destroy --config <yaml-filename>.yaml
```

例：

```
$ kvm_deployer destroy --config kvm_3node_deploy.yaml
Destroying VM node1 using nutanix
Destroying VM node1 using nutanix
 Looking for VM: node1
 Found VM node1 with UUID: 94fe9518-5196-4807-a6cc-183d1abe760e
 Powering off VM: 94fe9518-5196-4807-a6cc-183d1abe760e
 VM power off request submitted
 Deleting VM: 94fe9518-5196-4807-a6cc-183d1abe760e
 VM deletion task submitted: 8178938b-5014-474b-b168-34c3bf5b1577
 Waiting for task completion: 8178938b-5014-474b-b168-34c3bf5b1577
  Task status: RUNNING, progress: 0%
  Task status: SUCCEEDED, progress: 100%
 [□] Task completed successfully (status: SUCCEEDED)
 [□] VM deleted successfully
[□] VM node1 destroyed successfully
Destroying VM node2 using nutanix
Destroying VM node2 using nutanix
 Looking for VM: node2
 Found VM node2 with UUID: f1424251-182d-4518-9acc-f06ba89d4883
 Powering off VM: f1424251-182d-4518-9acc-f06ba89d4883
 VM power off request submitted
 Deleting VM: f1424251-182d-4518-9acc-f06ba89d4883
 VM deletion task submitted: a8d41687-3d84-4a38-91cc-5dfee0688351
 Waiting for task completion: a8d41687-3d84-4a38-91cc-5dfee0688351
  Task status: RUNNING, progress: 0%
  Task status: SUCCEEDED, progress: 100%
 [□] Task completed successfully (status: SUCCEEDED)
 [□] VM deleted successfully
[□] VM node2 destroyed successfully
Destroying VM node3 using nutanix
Destroying VM node3 using nutanix
 Looking for VM: node3
 Found VM node3 with UUID: 8cdc2037-fc83-43af-90f6-869c00aa2fdc
 Powering off VM: 8cdc2037-fc83-43af-90f6-869c00aa2fdc
 VM power off request submitted
 Deleting VM: 8cdc2037-fc83-43af-90f6-869c00aa2fdc
 VM deletion task submitted: 710c58a7-0728-4c4e-b63a-f6d90e3b2669
 Waiting for task completion: 710c58a7-0728-4c4e-b63a-f6d90e3b2669
  Task status: RUNNING, progress: 0%
  Task status: SUCCEEDED, progress: 100%
 [□] Task completed successfully (status: SUCCEEDED)
```

```
 [□] VM deleted successfully
[□] VM node3 destroyed successfully
$
```

Linux KVM での Nexus ダッシュボードの展開

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

始める前に

- Linux KVM で Nexus Dashboard クラスタを展開するための前提条件と注意事項 （179 ページ） に記載されている要件とガイドラインを満たしていることを確認します。

手順

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

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

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

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

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

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

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

`scp` を使用してイメージをコピーできます。次に例を示します。

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

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

ステップ 3 各 KVM ホストで次の構成を行います。

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

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

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

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

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

システム リソースを理解する （181 ページ） で説明されているとおり、2 つのディスク イメージを作成するには、合計 550 GB または 3 TB の SSD ストレージが必要です。

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

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

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

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

システム リソースを理解する （181 ページ） に記載されている情報に基づき、次のとおり、スクリプトを作成します。

- 1ノードまたは3ノードKVM（**アプリ**）フォームファクタの場合：

```
#!/bin/bash -ex

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

# Path of Nexus Dashboard QCOW2 image.
nd_qcow2=/home/nd-base/nd-dk9.4.2.1g.qcow2

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

# Management Network Bridge
mgmt_bridge=mgmt-bridge

# Data Network bridge
data_bridge=data-bridge

# Data Disk Size
data_size=500G

# CPU Cores
cpus=16

# Memory in units of MB.
memory=65536

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

```
--disk path=${data_disk}/disk.img,format=raw,bus=virtio \
--network bridge=$mgmt_bridge,model=virtio \
--network bridge=$data_bridge,model=virtio \
--console pty,target_type=serial \
--noautoconsole \
--autostart
```

- 1ノードまたは3ノードKVM（**データ**）フォームファクタの場合：

```
#!/bin/bash -ex

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

# Path of Nexus Dashboard QCOW2 image.
nd_qcow2=/home/nd-base/nd-dk9.4.2.1g.qcow2

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

# Management Network Bridge
mgmt_bridge=mgmt-bridge

# Data Network bridge
data_bridge=data-bridge

# Data Disk Size
data_size=3072G

# CPU Cores
cpus=32

# Memory in units of MB.
memory=131072

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

（注） 自動PCI割り当てによって、管理インターフェイスとデータインターフェイスがそれぞれ 00:03.0 と 00:04.0 に配置されていない場合、接続が失敗する可能性があります。その場合、これらの二つの --ネットワーク ラインを交換します：

```
--network bridge=$mgmt_bridge,model=virtio \
--network bridge=$data_bridge,model=virtio \
```

これらのラインと交換します：

```
--network bridge=$mgmt_bridge,model=virtio,address.type=pci,address.bus=0,address.slot=3
 \
--network bridge=$data_bridge,model=virtio,address.type=pci,address.bus=0,address.slot=4
 \
```

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

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

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

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

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

a) いずれかのキーを押して、初期設定を開始します。

初回セットアップユーティリティの実行を要求するプロンプトが表示されます。

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

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

b) admin パスワードを入力して確認します。

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

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

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

c) 管理ネットワーク情報を入力します。

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

d) 最初のノードのみ、「クラスタ リーダー」として指定します。

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

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

e) 入力した譲歩をレビューし、確認します。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ステップ 11 ログイン後、 **Meet Nexus Dashboard** の ウェルカム画面を確認し、 **ジャーニー** 画面に進みます。**クラスタの起動** 手順の下の **Go** をクリックして、ブートストラップ プロセスを開始します。

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

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

クラスタ名は、 RFC-1123 の要件に従う必要があります。

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

ステップ 13 **[クラスタのブリングアップ（Cluster Bringup）**] ウィザードの **[構成（Configuration）]** ページで、必要な情報を入力します。

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

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

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

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

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

- **キー**：NTP 認証キーを入力します。Nexus Dashboard と NTP サーバ間の NTP トラフィックを認証するために使用される暗号キーです。次の手順で NTP サーバーを定義します。複数の NTP サーバーで同じ NTP 認証キーを使用できます。
- **ID**： NTP ホストのキー ID を入力します。各 NTP キーに一意のキー ID を割り当てる必要があります。この ID は、NTP パケットの検証時に使用する適切なキーを識別するために使用されます。
- **認証タイプ**：NTPキーの認証タイプを選択します。
- このキーを信頼したい場合には、**[信頼済み（Trusted）]** チェックボックスをオンにします。信頼できないキーは NTP 認証に使用できません。

NTP認証の要件とガイドラインの完全なリストについては、全般的な前提条件とガイドライン （13 ページ） を参照してください。

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

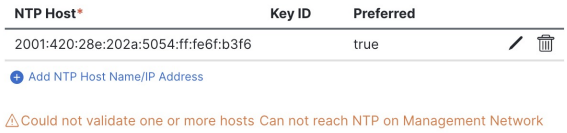
f) NTP認証を有効にした場合は、 **[+ NTP ホスト名/ IPアドレスの追加（+Add NTP Host Name/ IP Address）]**をクリックし、必要な情報を入力し、チェックマークアイコンをクリックして情報を保存します。

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

NTP 認証が無効になっている場合、このフィールドはグレー表示されます。

- このホストを優先したい場合は、**[優先（Preferred）]** チェックボックスをオンにします。

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



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

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

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

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

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

プロキシ サーバでは、永続 URL を許可する必要があります：

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

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

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

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

詳細設定では、次の設定を行うことができます。

- **アプリ ネットワーク**：Nexus Dashboard でアプリケーションで使用されるアドレス空間です。ターゲット ネットワークの IP アドレスとネットマスクを入力します。

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

アプリケーションおよびサービス ネットワークの詳細については、全般的な前提条件とガイドライン （13 ページ） を参照してください。

j) [次へ（Next）] をクリックします。

ステップ 14 **[ノードの詳細（Node Details）]** ページで、最初のノードの情報を更新します。

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

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

テレメトリで使用される永続的な IP アドレス機能には、BGP 構成が必要です。この機能の詳細については、BGP 構成と永続的な IP アドレス （60 ページ） および Nexus Dashboardの 永続 IP アドレス （52 ページ） セクションで説明します。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

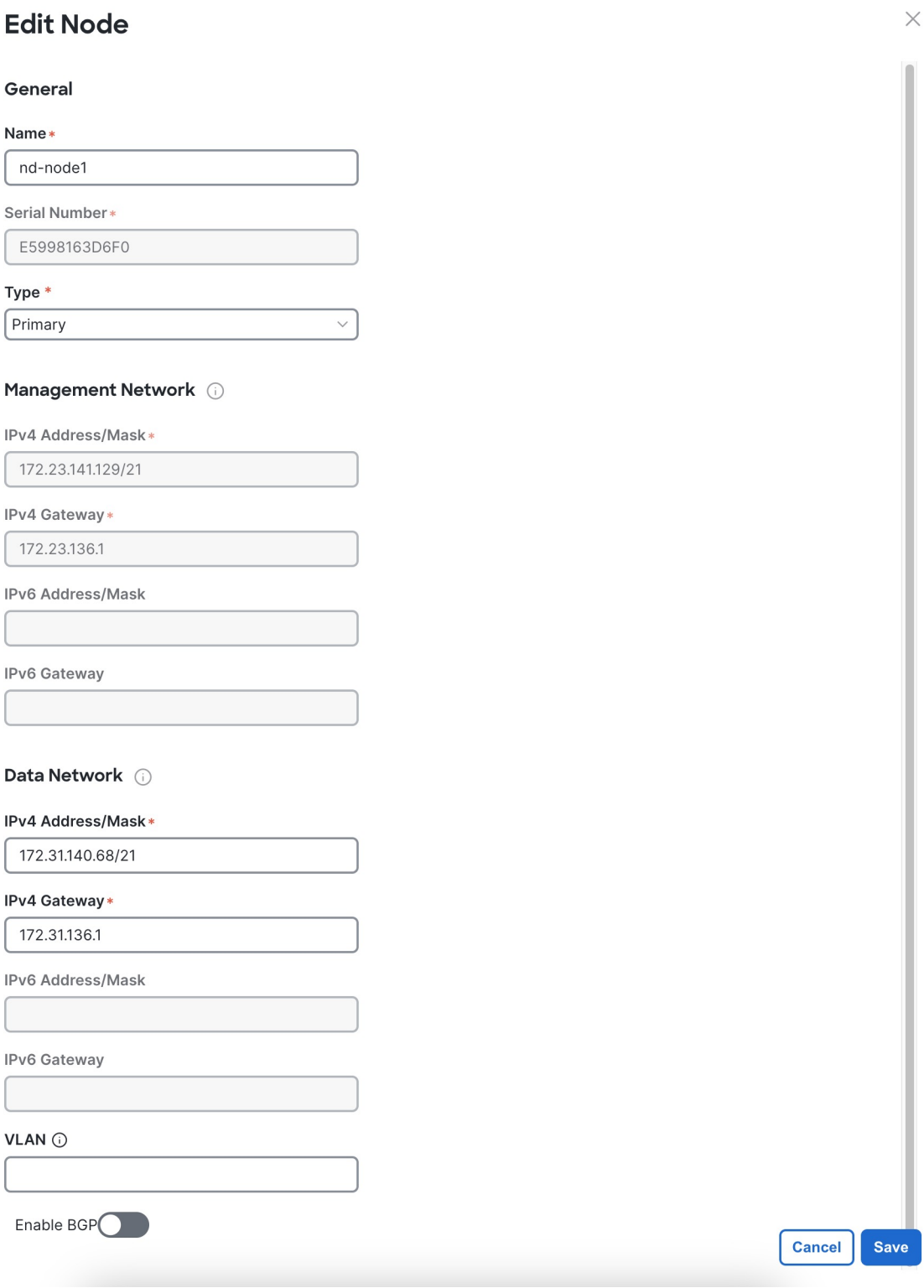
[+ IPv4 BGP ピアの追加（+ Add IPv4 BGP peer）] をクリックして、ピアを追加できます。

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

g) **[Save]**をクリックして、変更内容を保存します。

ステップ 15 [**ノードの詳細（Node Details）**] 画面で、[**ノードの追加（Add Node**）] をクリックして、クラスタに 2 番目のノードを追加します。

単一ノード クラスタを展開する場合は、この手順をスキップします。



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

ノードの初期構成手順で、管理ネットワーク情報とパスワードを定義しました。

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

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

c) ノードの **[名前（Name）]** を入力します。

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

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

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

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

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

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

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

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

永続 IP アドレス機能には BGP 設定が必要です。この機能については、BGP 構成と永続的な IP アドレス （60 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。

- IPv6 専用の場合、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 16 **[ノードの詳細（Node Details）]** ページで、入力した情報を確認してから、**[次へ（Next）]**をクリックします。

ステップ 17 クラスタの**展開モード**を選択します。

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

永続 IP アドレスの詳細については、Nexus Dashboardの 永続 IP アドレス （52 ページ）のセクションを参照してください：

b) [次へ（Next）] をクリックして続行します。

ステップ 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。

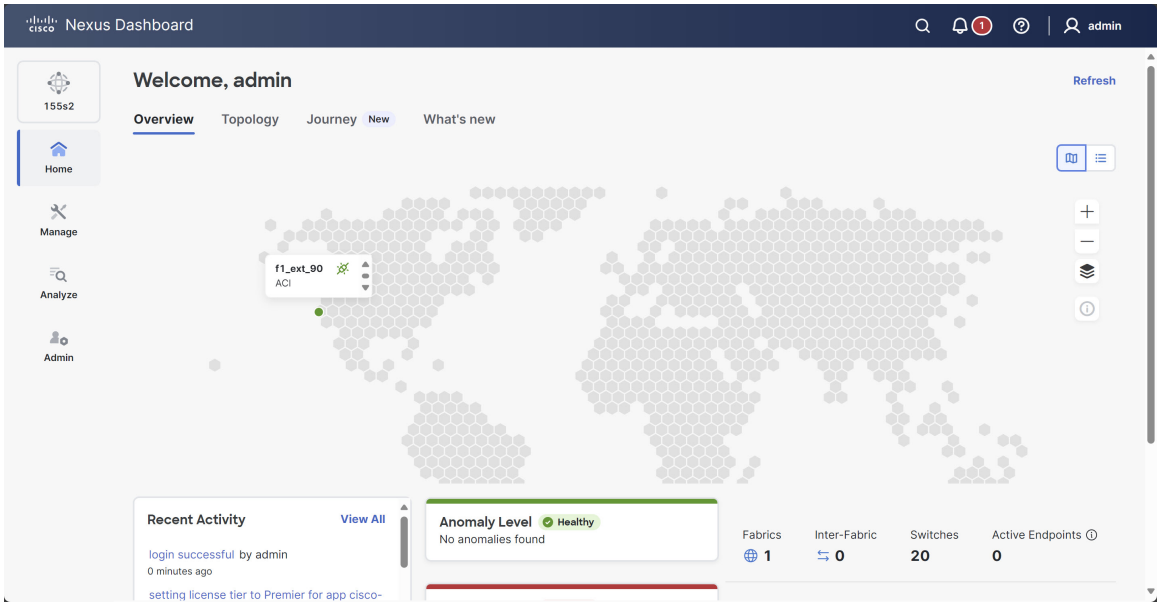
ノードのブート ストラップとクラスタの起動中に、全体的な進捗状況と各ノードの個々の進捗状況がUIに表示されます。ブートストラップの進行状況が表示されない場合は、ブラウザでページを手動で更新し、ステータスを更新してください。

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。

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

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



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

- クラスタが収束している間、次の出力が表示されることがあります：

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

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

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

- クラスタが稼働している場合は、次の出力が表示されます。

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



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

`deploy base system services`

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

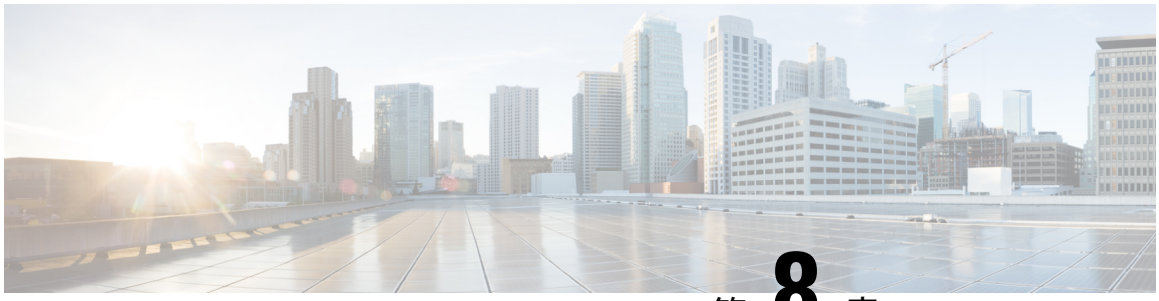
この問題を解決するには、影響を受けるノードで `acs reboot clean` コマンドを入力します。

ステップ 20 （オプション） Cisco Nexus DashboardクラスターをCisco Intersightに接続、可視性と利点を強化します。詳細な手順については、 「*Cisco Intersight*の操作」 を参照してください。

ステップ 21 Nexus Dashboardを展開した後、設定情報については、このリリースのコレクションページを参照してください。

次のタスク

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



第 8 章

Nutanix での仮想 Nexus Dashboard（vND）の展開

- Nutanix での vND の展開に関する前提条件と注意事項 （203 ページ）
- QCOW2 イメージのデプロイメント スクリプトについて （206 ページ）
- Nutanix に Nexus Dashboard クラスタをインストールする （215 ページ）

Nutanix での vND の展開に関する前提条件と注意事項

Nutanix Hyperconverged Infrastructure (HCI) にリモート対応 Nexus Dashboard (vND) を展開できるようになりました。

Nutanix での vND の展開に進む前に、次の前提条件と注意事項に従う必要があります。

- Nutanix 上の vNDs は、単一ノードと 3 ノードの展開の両方をサポートします。基礎となる Nutanix クラスタは、必要なノードとワークロードをホストするのに十分なリソースがある限り、任意のサイズにすることができます。
- コントローラ、テレメトリ、およびオーケストレーション機能を有効にすることができます。詳細については、『*Cisco Nexus Dashboard Verified Scalability Guide, Release 4.2.1*』を参照してください。
- クラスタ フォーム ファクタに基づいて、拡張性サポートおよび共同ホストは変わります。Nexus Dashboard キャパシティ プランニング ツールを使用して、仮想フォーム ファクタが展開要件を満たすことを確認できます。
- 前提条件とガイドライン （13 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。
- 管理インターフェイスとデータ インターフェイスは、両方のサブネットが `VLAN Basic` または `VLAN` のいずれかである同じタイプのサブネットで作成する必要があります。管理インターフェイスとデータ インターフェイスに異なるサブネットタイプが使用されている場合、Nutanix での vND の展開は失敗します。
- Nexus Dashboard VM に使用される CPU ファミリが AVX 命令セットをサポートしている必要があります。

- Nutanixノードには十分なシステム リソースが必要であり、Nutanix システム ストレージ デバイスの I/O遅延は20 ミリ秒未満である必要があります。
  - システム リソースの詳細については、「システム リソースを理解する （205 ページ）」を参照してください。1ノード（データ）と3ノード（データ）リモート対応プロファイルのみがサポートされます。最大のパフォーマンスと信頼性を実現するために、各ノードでこれらのリソースを明示的に予約する必要があります。
  - I/O遅延の詳細については、「Nutanix ストレージ デバイスの I/O 遅延の確認 （204 ページ）」を参照してください。
- Nutanix 展開での vND は、LAN および SAN 展開でサポートされています。
- Nexus Dashboard は、Nutanix Hyperconverged Infrastructure (HCI) にのみ展開する必要があります。詳細については、「https://www.cisco.com/site/us/en/products/computing/hyperconverged/nutanix/index.html」を参照してください。
- サポートされている Nutanix ソフトウェア リリース：

Acropolis オペレーティング システム（AOS）	Acropolis Hypervisor（AHV）	Prism Central
6.10.x	20230302.x	2024.2.x
7.3.x	10.3.x	7.3.x

- 各 Nexus Dashboard ノードを個別の Acropolis ハイパーバイザ ホストに展開することを強くお勧めします。
- ライブ移行はサポートされていません（ Nexus Dashboard VM でこれを無効にする必要があります）。

Nutanix ストレージ デバイスの I/O 遅延の確認

（注） その他の有用な情報については、「*Nutanix での Fio のパフォーマンス ベンチマーク化*」を参照してください。

Nutanix Hyperconverged Infrastructure (HCI) にNexus Dashboard クラスタを展開する場合、Nutanix ストレージ デバイスの遅延は 20 ミリ秒未満である必要があります。QCOW2 イメージに `kvm_deployer` デプロイメント スクリプトを使用する場合は、「QCOW2 イメージのデプロイメント スクリプトについて （181 ページ）」で説明されているように、パフォーマンス検証手順でこれを実行します。

手動で Nutanix ストレージ デバイスの I/O 遅延を確認したい場合は、次の手順を実行します。

手順

ステップ 1 fio パケットをインストールします。

```
# sudo apt-get install fio
```

ステップ 2 test-data フォルダを作成します。

たとえば、 `test-data`という名前のフォルダを作成します。

```
# mkdir test-data
```

ステップ 3 フレキシブル I/O テスター（FIO）テスト 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
```

ステップ 4 コマンドの実行後に、`fsync/fdatasync/sync_file_range` セクションの `99.00th=[<value>]` が 20 ミリ秒未満であることを確認します。

システム リソースを理解する

Nutanix に Nexus Dashboard クラスタを展開する場合、十分なシステム リソースがあることを確認する必要があります。Nutanix に Nexus Dashboard クラスタを展開する際には複数のフォーム ファクタがサポートされており、各ノードに必要なシステム リソースの量はフォーム ファクタによって異なります。

（注） Nutanix でのリモート対応 Nexus Dashboard （vND）の展開は、以下に示すようにデータ ノードでのみサポートされます。Nutanix での vND の展開は、アプリ ノードではサポートされていません。

表 *27*: ノード当たりのリソース要件

フォーム ファクタ	vCPU の数	RAM	ディスク サイズ	CPU あたりのコア数
1-ノード vND（データ）	32	128 GB	3077 GB	1
3-ノード vND（データ）	32	128 GB	3077 GB	1

Nutanix に Nexus Dashboard クラスタをインストールする （215 ページ）の手順を実行するときに、フォーム ファクタに関する上記の情報を知っておく必要があります

QCOW2 イメージのデプロイメント スクリプトについて

Nexus Dashboard は、RHEL や Nutanix など、さまざまな環境での KVM 仮想化をサポートしています。Nexus Dashboard の展開は通常、QCOW2 イメージを使用して行われます。しかし、KVM のバリアントとホスト構成が多様であるため、サポートされているバージョンの追跡と最適なデバイスエミュレーションのパフォーマンス確保に課題が生じています。

QCOW2 イメージのデプロイメント スクリプトは、QCOW2 イメージにパッケージ化されたデプロイメントの検証およびオーケストレーション スクリプトを提供することで、これらの課題に対処します。このスクリプトは、デプロイメント プロセスを合理化、互換性を確保し、サポートされているプラットフォーム間で一貫したパフォーマンス標準を維持するように設計されています。

主な機能

QCOW2 イメージのデプロイメント スクリプトの主な機能は次のとおりです。

- **プラットフォーム互換性チェック**：基盤となるホストのオペレーティング システムがサポートされているディストリビューションとバージョンであることを確認します。
- **リソース検証**： ホストが CPU、メモリ、ストレージ リソースなどの最小コンピューティング要件を満たしているかどうかを評価します。
- **パフォーマンス検証**：
  - **ディスク I/O と網の遅延**： ディスク I/O やネットワーク I/O の遅延などの主要なパフォーマンス インジケータを測定し、適格な範囲内にあることを確認します。
  - **デバイス エミュレーション:** 適切なデバイス エミュレーション（ネットワーク インターフェイスやリモート対応ディスク デバイスなど）が最適なパフォーマンスのために使用可能であることを確認します。
- **展開のオーケストレーション**： 単一ノードとマルチノードの両方のクラスタのデプロイメント プロセスを自動化し、適切なデバイス マッピング（ネットワークやストレージ デバイスなど）でリモート対応マシンをオーケストレーションします。

ストレージは最も一般的なボトルネックであるため、このスクリプトではストレージを「パフォーマンス層」に分類します。

- **ディスクのタイプと配置（SSD/NVMe）**： 高 IOP ワークロードを検証します。
- **RAID 対 JBOD**： 書き込み速度を検証します。
- **リモート ストレージ（iSCSI/ FC/NFS）**： 「Pre-Flight Latency Check」を実行します。
  - **同期遅延**： 標準規格アプリケーションの場合は 10 ミリ秒未満、高性能データベースの場合は 1 ミリ秒未満である必要があります。
  - **IOPS 検証**： 一時的な `FIO` テストを使用して、必要な IOS を確認します。

QCOW2 イメージのデプロイメント スクリプトの前提条件

QCOW2 イメージのデプロイメント スクリプトの前提条件

要件	詳細
Nutanix Prism Central	デプロイヤを実行しているマシンからポート 9440（HTTPS）で到達可能
Nutanix Prism 要素	ポート 9440（HTTPS）で到達可能。ストレージ、ネットワーキング、および VM コンソール アクセスに使用される
Prism ログイン情報	イメージの作成、サブネットのリスト、および VM の管理権限を持つユーザー アカウント
ND qcow2 イメージ	Nexus Dashboard `.qcow2` イメージ ファイルへのローカル パス
ネットワーク情報	Prism で設定されたサブネット名、および 3 つの管理 IP + ゲートウェイ
Go toolchain	送信元から構築するには、Go 1.22+ を使用します（または、事前作成のバイナリを使用します。）

Prism Central と Prism Element の違いを理解する

デプロイメント スクリプトでは、イメージのアップロード、VM の作成、ライフサイクル管理など、すべての API 操作に **Prism Central**（PC）を使用します。構成ファイルの IP とログイン情報が必要です。

Prism Element（PE）は個々の Nutanix クラスタを管理し、次の場合に役立ちます。

- ストレージ コンテナとディスク使用率の表示
- クラスタ レベルでのネットワーク/サブネット設定の確認
- 起動問題をトラブルシューティングするための VM シリアル コンソールへのアクセス
- ホストレベルの正常性とハードウェアのステータスのモニタリング

インターフェイス	[URL（URL）]	必要なとき
Prism Central	www/*prism_cent_ralip*:9440	VMs の展開、管理、および破棄。イメージのアップロード。サブネット名の確認。
Prism Element	www/*prism_element_ip*:9440	ストレージ コンテナ、ネットワーク設定、VM コンソール アクセス、ホストの正常性の確認

QCOW2 イメージのデプロイメント スクリプトを使用します

手順

ステップ 1 デプロイメント スクリプトを含む tar ファイルを見つけます。

tar ファイルは、QCOW2 イメージと同じ場所に用意する必要があります。たとえば、4.3.1 リリース以降の Nexus Dashboard のソフトウェア ダウンロード サイト には、次のように QCOW2 イメージのデプロイメントスクリプトを含む tar ファイルが QCOW2 イメージ自体と同じエリアに表示されます。

```
nd-dk9.4.3.1.175.qcow2.tar.gz
```

ステップ 2 デプロイメント スクリプトを含む tar ファイルをダウンロードします。

ステップ 3 tar ファイルを解凍します。

例：

```
tar -xzvf nd-dk9.4.3.1.175.qcow2.tar.gz
```

tar ファイルを抽出し、ディレクトリの内容をリストした後、次のような出力が表示されます。

```
#ls -lrt
total 24730576
-rwxr-xr-x 1 root root    35991736 May  5 23:35 kvm_deployer
-rw-r--r-- 1 root root 12651498496 May 17 03:44 nd-dk9.4.3.1.175.qcow2
-rw-r--r-- 1 root root 12636610743 May 18 22:44 nd-dk9.4.3.1.175.qcow2.tar.gz
```

ステップ 4 **kvm_deployer config** コマンドを使用して、デプロイメント スクリプトで使用する yaml ファイルを作成します。

デプロイメントのタイプに基づいて、各段階で適切な選択をしてください。

- たとえば、1 ノードの yaml ファイルを生成するには：

```
# ./kvm_deployer config
Configure Nexus Dashboard deployment:
 Deployment Platform (kvm/nutanix): nutanix
 Image Path (qcow2): /home/nd-base/nd-dk9.4.3.1.175.qcow2
 Cluster Size: 1
 VM Type (app/data/large/xlarge): data
 Admin Password:
Configure Nutanix platform settings:
 Prism Central IP: 192.168.94.164
 Nutanix Username: admin
 Nutanix Password:
 Cluster Name: sit_reg1_nutanix
 Network Name: mgmt
 VCPUs per Socket (default: 2): (current: 0): 2
Configure VM (1) for Nutanix:
  VM Name (lowercase, numbers, dashes, max 63 chars): node1
  Management Network (e.g., 192.168.1.100/24): 192.168.94.166/24
  Management Gateway IP: 192.168.94.1
[□] Configuration Summary:
 Deployment Platform        : nutanix
 Image Path (qcow2)         : /home/nd-base/nd-dk9.4.3.1.175.qcow2
 Admin Password             : [hidden]
 VM Type                    : data
```

```
 Nutanix Configuration:
  Prism Central IP            : 192.168.94.164
  Username                    : admin
  Password                    : [hidden]
  Cluster Name                : sit_reg1_nutanix
  Network Name                : mgmt
  VCPUs per Socket            : 2
 VMs:
  VM Name                    : node1
   Management Network         : 192.168.94.166/24
   Management Gateway IP      : 192.168.94.1
 Proceed with current config? (y/n): y
 File name to save configuration: nutanix_1node_deploy.yaml
```

- 3 ノードの yaml ファイルを生成する場合：

```
# ./kvm_deployer config
Configure Nexus Dashboard deployment:
 Deployment Platform (kvm/nutanix): nutanix
 Image Path (qcow2): /home/nd-base/nd-dk9.4.3.1.175.qcow2
 Cluster Size: 3
 VM Type (app/data/large/xlarge): data
 Admin Password:
Configure Nutanix platform settings:
 Prism Central IP: 192.168.94.164
 Nutanix Username: admin
 Nutanix Password:
 Cluster Name: sit_reg1_nutanix
 Network Name: mgmt
 VCPUs per Socket (default: 2): (current: 0): 2
Configure VM (1) for Nutanix:
  VM Name (lowercase, numbers, dashes, max 63 chars): node1
  Management Network (e.g., 192.168.1.100/24): 192.168.94.166/24
  Management Gateway IP: 192.168.94.1
Configure VM (2) for Nutanix:
  VM Name (lowercase, numbers, dashes, max 63 chars): node2
  Management Network (e.g., 192.168.1.100/24): 192.168.94.167/24
  Management Gateway IP: 192.168.94.1
Configure VM (3) for Nutanix:
  VM Name (lowercase, numbers, dashes, max 63 chars): node3
  Management Network (e.g., 192.168.1.100/24): 192.168.94.168/24
  Management Gateway IP: 192.168.94.1
[□] Configuration Summary:
 Deployment Platform        : nutanix
 Image Path (qcow2)         : /home/nd-base/nd-dk9.4.3.1.175.qcow2
 Admin Password             : [hidden]
 VM Type                    : data
 Nutanix Configuration:
  Prism Central IP            : 192.168.94.164
  Username                    : admin
  Password                    : [hidden]
  Cluster Name                : sit_reg1_nutanix
  Network Name                : mgmt
  VCPUs per Socket            : 2
 VMs:
  VM Name                    : node1
   Management Network         : 192.168.94.166/24
   Management Gateway IP      : 192.168.94.1
  VM Name                    : node2
   Management Network         : 192.168.94.167/24
   Management Gateway IP      : 192.168.94.1
  VM Name                    : node3
   Management Network         : 192.168.94.168/24
   Management Gateway IP      : 192.168.94.1
```

```
Proceed with current config? (y/n): y
File name to save configuration: nutanix_3node_deploy.yaml
```

ステップ 5 （オプション）必要に応じて、テキストエディタを使用して yaml ファイルに保存された情報を検証します。

たとえば、前述の 3 ノードの例では、yaml ファイルには次のような情報が含まれます。

```
# cat nutanix_3node_deploy.yaml
deployment_type: nutanix
image_path: /var/www/html/ND_IMAGES/nd-dk9.4.3.1.75.qcow2
cluster_size: "3"
vms:
- name: node1
  disk_path: ""
  management_network: 192.168.94.166/24
  management_gateway: 192.168.94.1
  management_bridge: ""
  data_bridge: ""
  host_ip: ""
  host_user: ""
  host_password: ""
- name: node2
  disk_path: ""
  management_network: 192.168.94.167/24
  management_gateway: 192.168.94.1
  management_bridge: ""
  data_bridge: ""
  host_ip: ""
  host_user: ""
  host_password: ""
- name: node3
  disk_path: ""
  management_network: 192.168.94.168/24
  management_gateway: 192.168.94.1
  management_bridge: ""
  data_bridge: ""
  host_ip: ""
  host_user: ""
  host_password: ""
flavor: data
admin_password:
nutanix:
  prism_central_ip: 192.168.94.164
  username: admin
  password:
  cluster_name: sit_reg1_nutanix
  vcpus_per_socket: 2
  network_name: mgmt
  data_network_name: data
#
```

ステップ 6 yaml ファイルを入力として使用して、デプロイメント スクリプトを実行します。

```
./kvm_deployer deploy --config nutanix_3node_deploy.yaml
```

次のような出力が表示されます。

```
Deploying VM node1 using kvm
  Cleanup old images
  [□] Cleaned image /home/nd-node1/boot.img
  [□] Cleaned image /home/nd-node1/disk.img
  [□] Cleaned image /home/nd-node1/config-drive.img
```

```
  Creating boot disk, it can take several minutes, pls wait
  [□] Boot disk created successfully
  Creating raw disk, it can take several minutes, pls wait
  [□] Raw disk created successfully
  Creating configuration drive
  [□] Configuration drive created successfully

  Starting VM
  [□] VM started successfully
[□] KVM VM: node1 deployed successfully
Deploying VM node2 using kvm
 Copying file /home/nd-base/nd-dk9.4.3.1.175.qcow2 to /home/nd-node2/nd-dk9.4.3.1.175.qcow2
 [□] File /home/nd-base/nd-dk9.4.3.1.175.qcow2 copied to /home/nd-node2/nd-dk9.4.3.1.175.qcow2
  Cleanup old images
  [□] Cleaned image /home/nd-node2/boot.img
  [□] Cleaned image /home/nd-node2/disk.img
  [□] Cleaned image /home/nd-node2/config-drive.img
  Creating boot disk, it can take several minutes, pls wait
  [□] Boot disk created successfully
  Creating raw disk, it can take several minutes, pls wait
  [□] Raw disk created successfully
  Creating configuration drive
  Copying file /home/nd-node1/node2-bootstrap.json to /home/nd-node2/apic-sn-cfg-mount/bootstrap.json

  [□] File /home/nd-node1/node2-bootstrap.json copied to
/home/nd-node2/apic-sn-cfg-mount/bootstrap.json
  [□] Configuration drive created successfully
  Starting VM
  [□] VM started successfully
[□] KVM VM: node2 deployed successfully
Deploying VM node3 using kvm
 Copying file /home/nd-base/nd-dk9.4.3.1.175.qcow2 to /home/nd-node3/nd-dk9.4.3.1.175.qcow2
 [□] File /home/nd-base/nd-dk9.4.3.1.175.qcow2 copied to /home/nd-node3/nd-dk9.4.3.1.175.qcow2
  Cleanup old images
  [□] Cleaned image /home/nd-node3/boot.img
  [□] Cleaned image /home/nd-node3/disk.img
  [□] Cleaned image /home/nd-node3/config-drive.img
  Creating boot disk, it can take several minutes, pls wait
  [□] Boot disk created successfully
  Creating raw disk, it can take several minutes, pls wait
  [□] Raw disk created successfully
  Creating configuration drive
  Copying file /home/nd-node1/node3-bootstrap.json to /home/nd-node3/apic-sn-cfg-mount/bootstrap.json

  [□] File /home/nd-node1/node3-bootstrap.json copied to
/home/nd-node3/apic-sn-cfg-mount/bootstrap.json
  [□] Configuration drive created successfully
  Starting VM
  [□] VM started successfully
[□] KVM VM: node3 deployed successfully
```

展開を実行すると、ツールは VM ごとに次の手順を実行します。

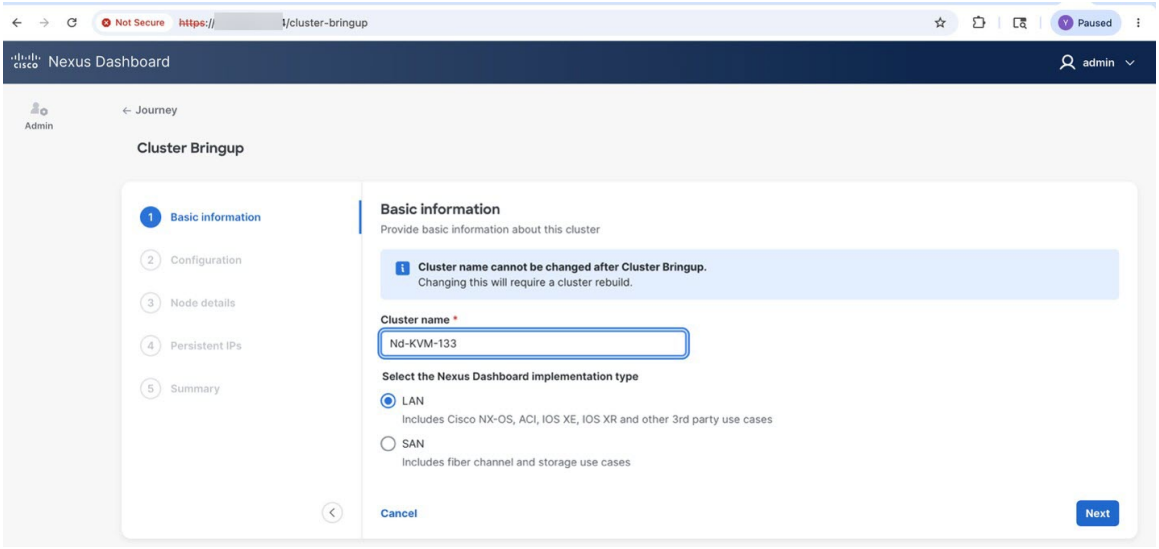
1. イメージのアップロード：qcow2 イメージが Prism Central にすでに存在するかどうかを確認します（ファイル名が一致）。存在しない場合、 はそれをアップロードし、アクティブになるまで待機します。
2. サブネット解決：network-name（および設定されている場合は data-network-name）を Prism サブネット UUID に解決します。
3. VM の作成：次の機能を使用して、電源オフ状態で VM を作成します。

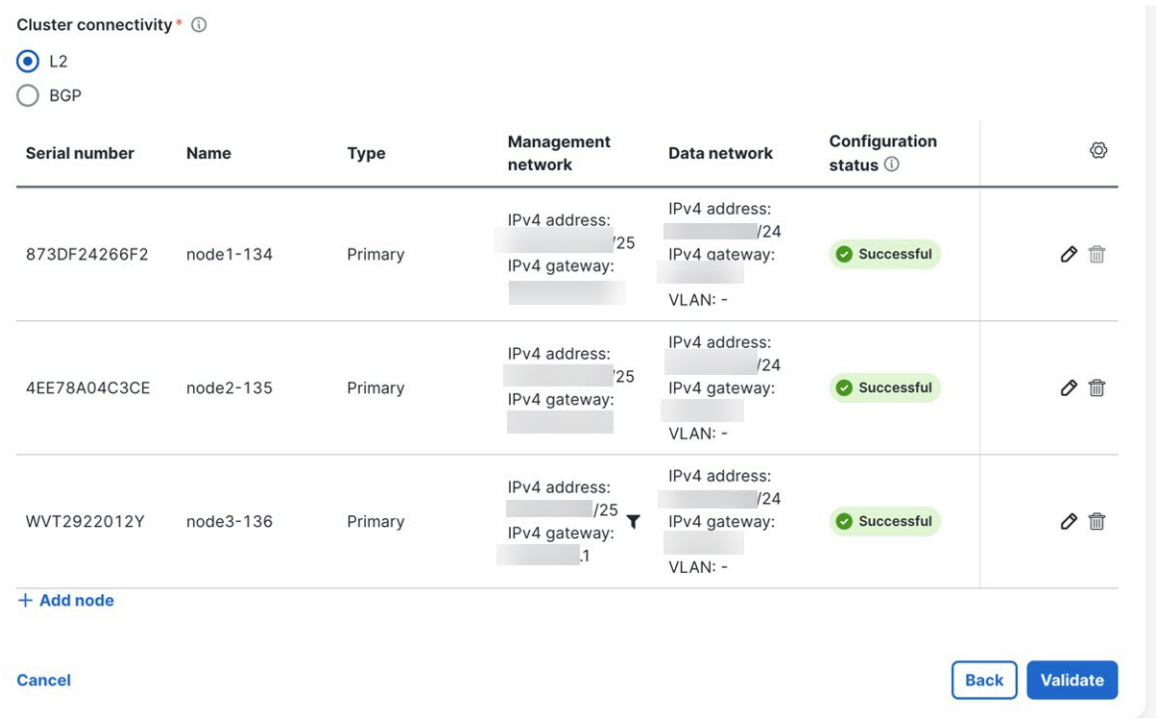
- アップロードされたイメージから複製された起動ディスク
- セカンダリ 3077 GiB raw データディスク
- 解決済みのサブネットにアタッチされている NIC
- 管理者パスワード、管理 IP、およびゲートウェイを伝送する cloud-init ユーザー データ

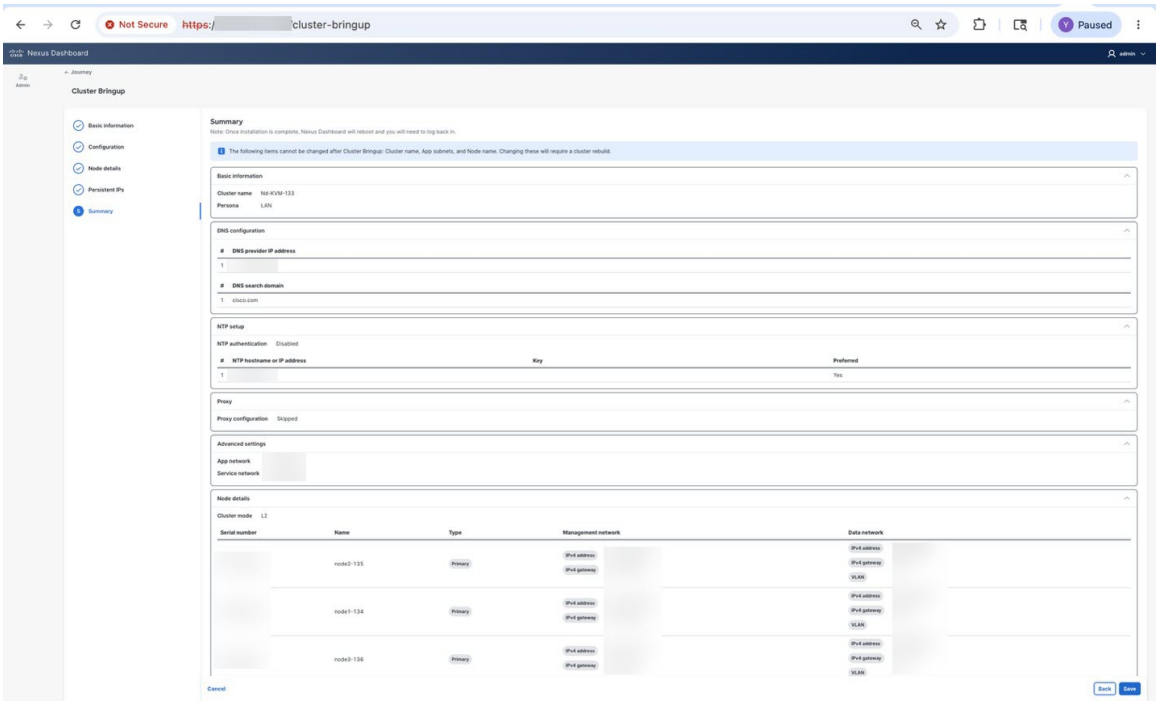
4. 電源オン：VM の電源をオンにして、タスクが完了するまで待ちます。

ステップ 7 展開後の手順を完了します。

a) **クラスタの形成**：すべてのノードが実行されたら、設定の管理 IP アドレスを使用して、Nexus Dashboard UI を介して Nexus Dashboard クラスタのセットアップを完了します。




Cluster connectivity *
L2
BGP
Serial number
Name
Type
Management network
Data network
Configuration status
873DF24266F2
node1-134
Primary
IPv4 address:
/25
IPv4 gateway:
IPv4 address:
/24
IPv4 gateway:
VLAN: -
Successful
4EE78A04C3CE
node2-135
Primary
IPv4 address:
/25
IPv4 gateway:
IPv4 address:
/24
IPv4 gateway:
VLAN: -
Successful
WVT2922012Y
node3-136
Primary
IPv4 address:
/25
IPv4 gateway:
.1
IPv4 address:
/24
IPv4 gateway:
VLAN: -
Successful
+ Add node
Cancel
Back
Validate


Not Secure
https:/
cluster-bringup
Paused
Nexus Dashboard
admin
Cluster Bringup
Basic information
Configuration
Node details
Persistent IPs
Summary
Summary
Basic information
DNS configuration
NTP setup
Proxy
Advanced settings
Node details
Cancel
Back
Save

オプションの展開後のタスク

トラブルシューティング

症状	検証
接続が拒否 / タイムアウトされました。	Prism Central がマシンからポート 9440 で到達可能であることを確認する
Authentication failure（認証失敗）	設定でユーザ名 および パスワードを確認します
イメージのアップロードがハングする	`image-path` が 有効な qcow2 ファイルを指し、Prism に十分なストレージがあることを確認します。
サブネットが見つかりません	`network-name` が Prism Central に表示されているサブネット名と正確に一致することを確認します。
VM が IP を取得していません	cloud-init `management_network` が有効な CIDR 表記法および正しいゲートウェイであることを確認します。
VM が起動時にスタックする	Prism Elementt (`https://<prism_element_ip>:9440`) を使用して VM シリアル コンソールを開いて起動ログを確認します
ストレージの問題	Prism Element で使用可能なストレージ コンテナとディスク容量を確認する

デプロイメントを破棄します

デプロイメントを破棄したい場合このコマンドを入力します：

```
./kvm_deployer destroy --config <yaml-filename>.yaml
```

例：

```
$ kvm_deployer destroy --config nutanix_3node_deploy.yaml
Destroying VM node1 using nutanix
Destroying VM node1 using nutanix
 Looking for VM: node1
 Found VM node1 with UUID: 94fe9518-5196-4807-a6cc-183d1abe760e
 Powering off VM: 94fe9518-5196-4807-a6cc-183d1abe760e
 VM power off request submitted
 Deleting VM: 94fe9518-5196-4807-a6cc-183d1abe760e
 VM deletion task submitted: 8178938b-5014-474b-b168-34c3bf5b1577
 Waiting for task completion: 8178938b-5014-474b-b168-34c3bf5b1577
  Task status: RUNNING, progress: 0%
  Task status: SUCCEEDED, progress: 100%
 [□] Task completed successfully (status: SUCCEEDED)
 [□] VM deleted successfully
[□] VM node1 destroyed successfully
Destroying VM node2 using nutanix
Destroying VM node2 using nutanix
 Looking for VM: node2
 Found VM node2 with UUID: f1424251-182d-4518-9acc-f06ba89d4883
 Powering off VM: f1424251-182d-4518-9acc-f06ba89d4883
 VM power off request submitted
 Deleting VM: f1424251-182d-4518-9acc-f06ba89d4883
```

```
 VM deletion task submitted: a8d41687-3d84-4a38-91cc-5dfee0688351
 Waiting for task completion: a8d41687-3d84-4a38-91cc-5dfee0688351
  Task status: RUNNING, progress: 0%
  Task status: SUCCEEDED, progress: 100%
 [□] Task completed successfully (status: SUCCEEDED)
 [□] VM deleted successfully
[□] VM node2 destroyed successfully
Destroying VM node3 using nutanix
Destroying VM node3 using nutanix
 Looking for VM: node3
 Found VM node3 with UUID: 8cdc2037-fc83-43af-90f6-869c00aa2fdc
 Powering off VM: 8cdc2037-fc83-43af-90f6-869c00aa2fdc
 VM power off request submitted
 Deleting VM: 8cdc2037-fc83-43af-90f6-869c00aa2fdc
 VM deletion task submitted: 710c58a7-0728-4c4e-b63a-f6d90e3b2669
 Waiting for task completion: 710c58a7-0728-4c4e-b63a-f6d90e3b2669
  Task status: RUNNING, progress: 0%
  Task status: SUCCEEDED, progress: 100%
 [□] Task completed successfully (status: SUCCEEDED)
 [□] VM deleted successfully
[□] VM node3 destroyed successfully
$
```

Nutanix に Nexus Dashboard クラスタをインストールする

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）] ページに移動します。

b) 左側のナビゲーション ウィンドウで、ダウンロードする Nexus Dashboard のリリースを選択します。

Nutanix 展開は、Nexus ダッシュボード リリース 4.2 以降でサポートされています。

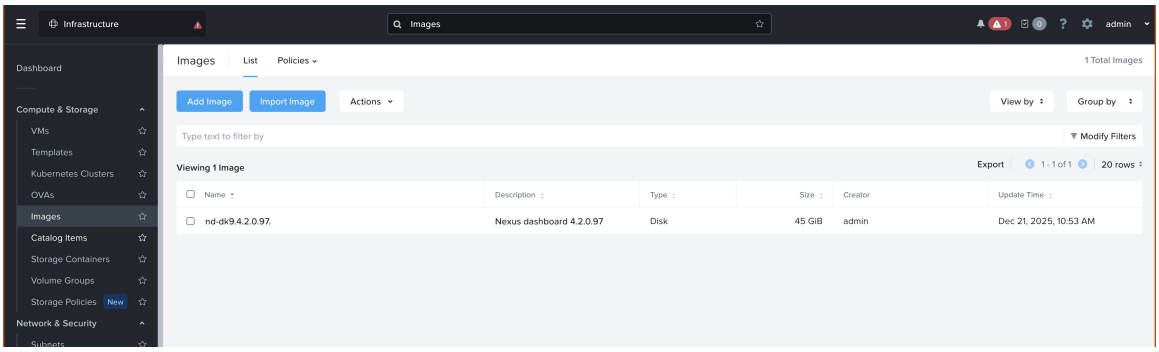
c) Linux KVM の Cisco Nexus ダッシュボードイメージをダウンロードします（`nd-dk9.<version>.qcow2`）。

Nutanix はLinux KVM と同じ `qcow2` イメージを使用します。

ステップ 2 ダウンロードした `qcow2` イメージを、 HTTP または HTTPS 経由で Prism Central からアクセス可能な Web サーバにコピーします。

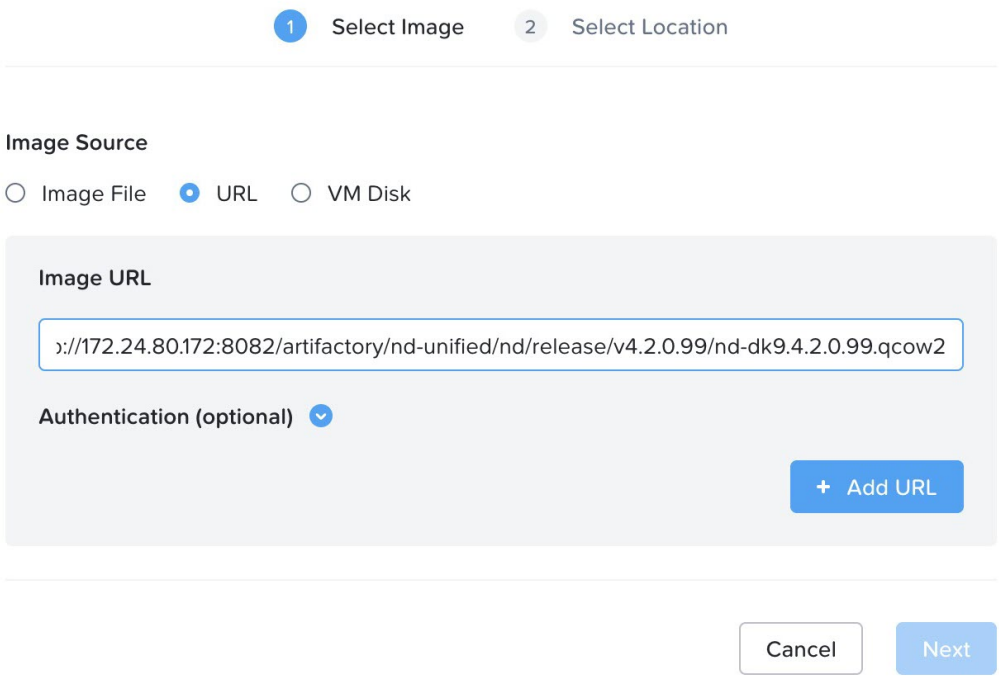
ステップ 3 Prism Central UI にアクセスします。

ステップ 4 **[インフラストラクチャ（Infrastructure）]** > **[コンピューティングとストレージ（Compute & Storage）]** > **[イメージ （Images）]** に移動し、 **[イメージの追加（Add Image）]**をクリックします。

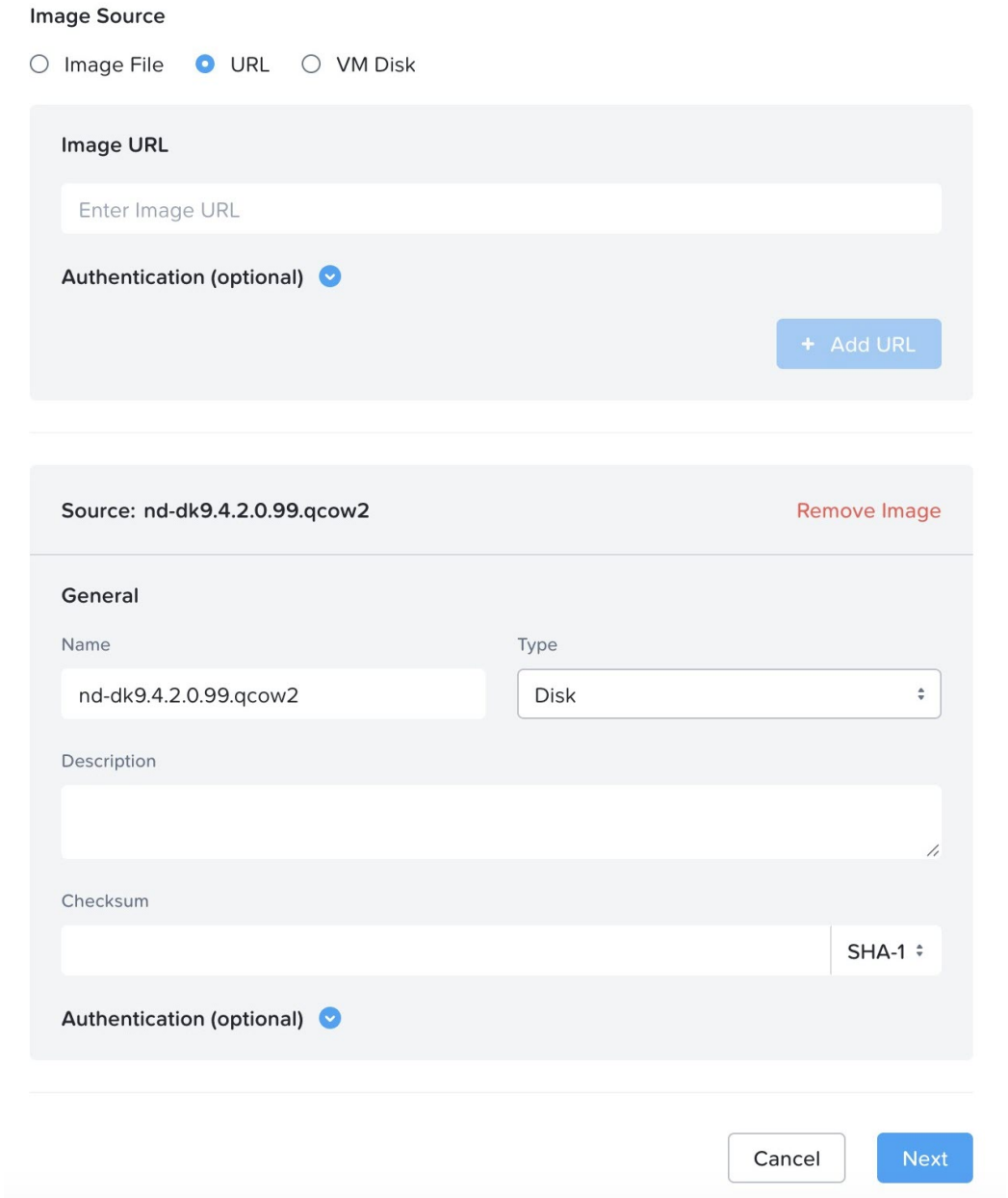


ステップ 5 **[URL]** オプションをクリックし、 Nexus Dashboard qcow2 イメージへの URL パスを入力して、 **[URLの追加（Add URL）]**をクリックします。

（注） Nexus Dashboard qcow2 イメージは 2 GB を超えているため、 **イメージ ファイル** オプションを使用してこのイメージを追加することはできません。



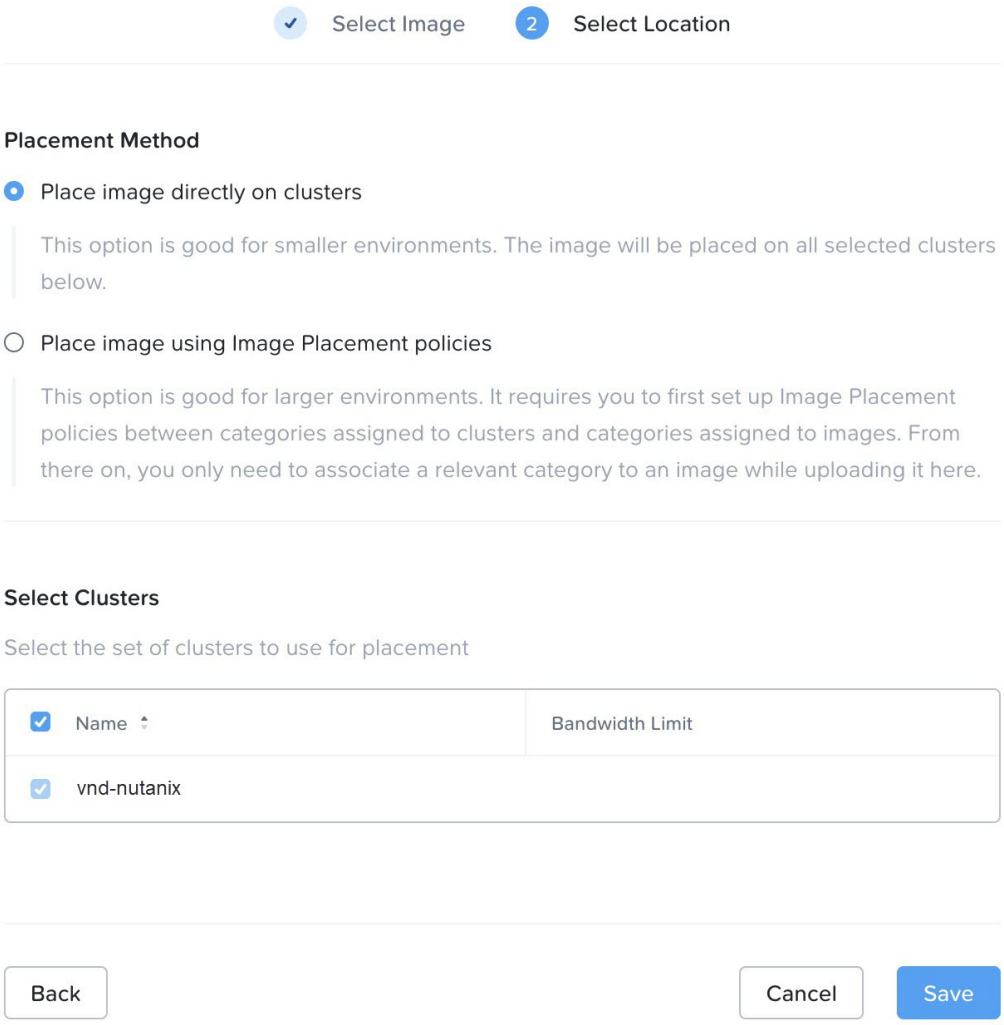
ステップ 6 イメージ情報がウィンドウに表示されたら、 **[次へ（Next）]**をクリックします。



ステップ 7 2 でこれらの構成を行います。**[ロケーション（Location）]** ウィンドウを選択します。

- **[配置メソッド（Placement Method）]** 領域で、**[イメージをクラスタに直接配置（Place image directly on clusters）]**をクリックします。
- 配置に使用するクラスタを選択し、**[保存（Save）]**をクリックします。

イメージのアップロードには、速度によって数分かかる場合があります。プロセスが完了してから、次のステップに進みます。

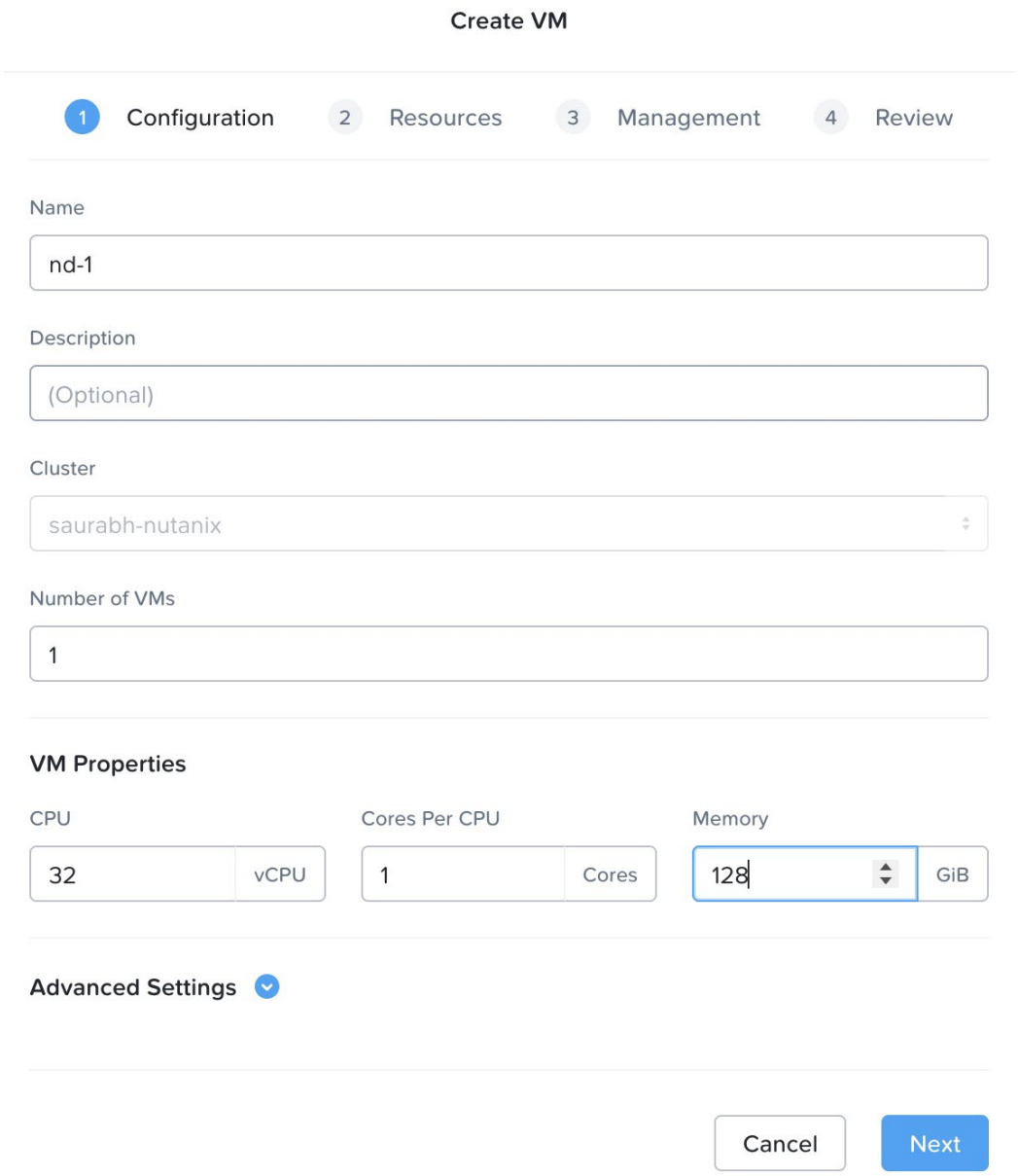


ステップ 8 vND VM の展開

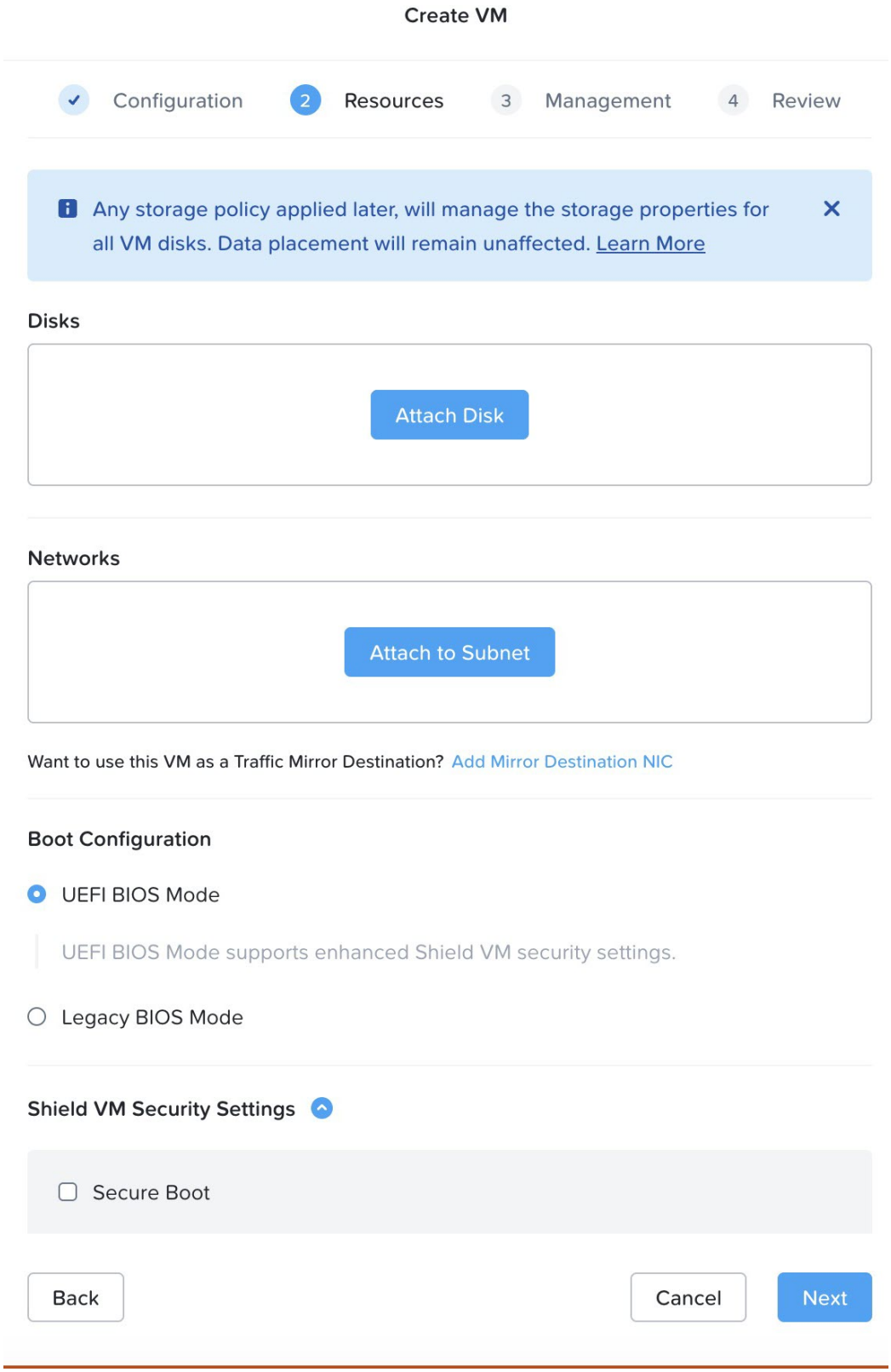
a) **[インフラストラクチャ（Infrastructure）] [コンピューテ > ィングとストレージ（Compute & Storage） >] [VMs]**に移動し、**[VM の作成（Create VM）]**をクリックします。

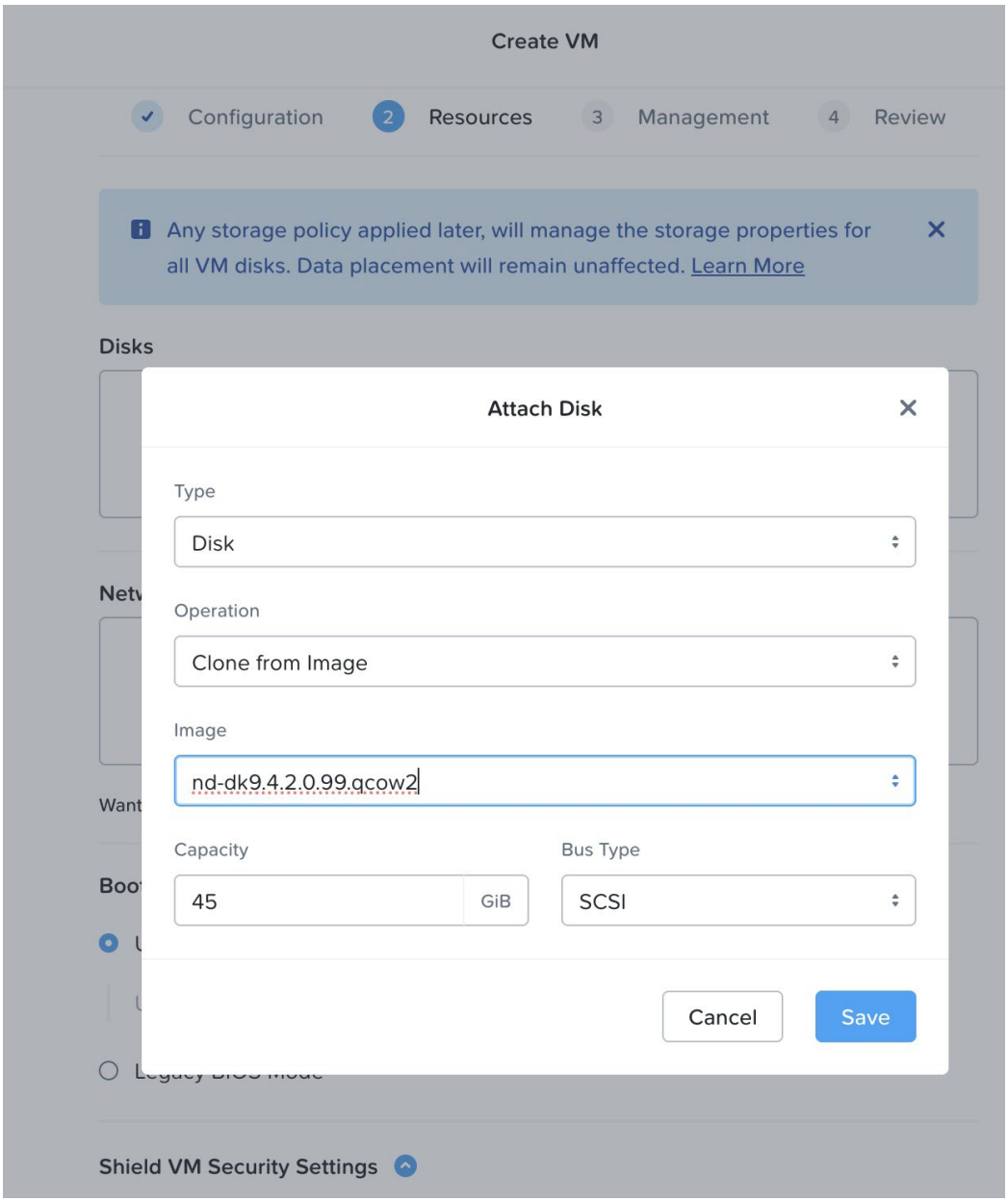
b) **1 で、[構成（Configuration）]** ウィンドウで、 Nexus Dashboard に必要な CPU とメモリの値を入力し、**[次へ（Next）]**をクリックします。

これらの値については、システム リソースを理解する （205 ページ） に記載されている情報を活用します。



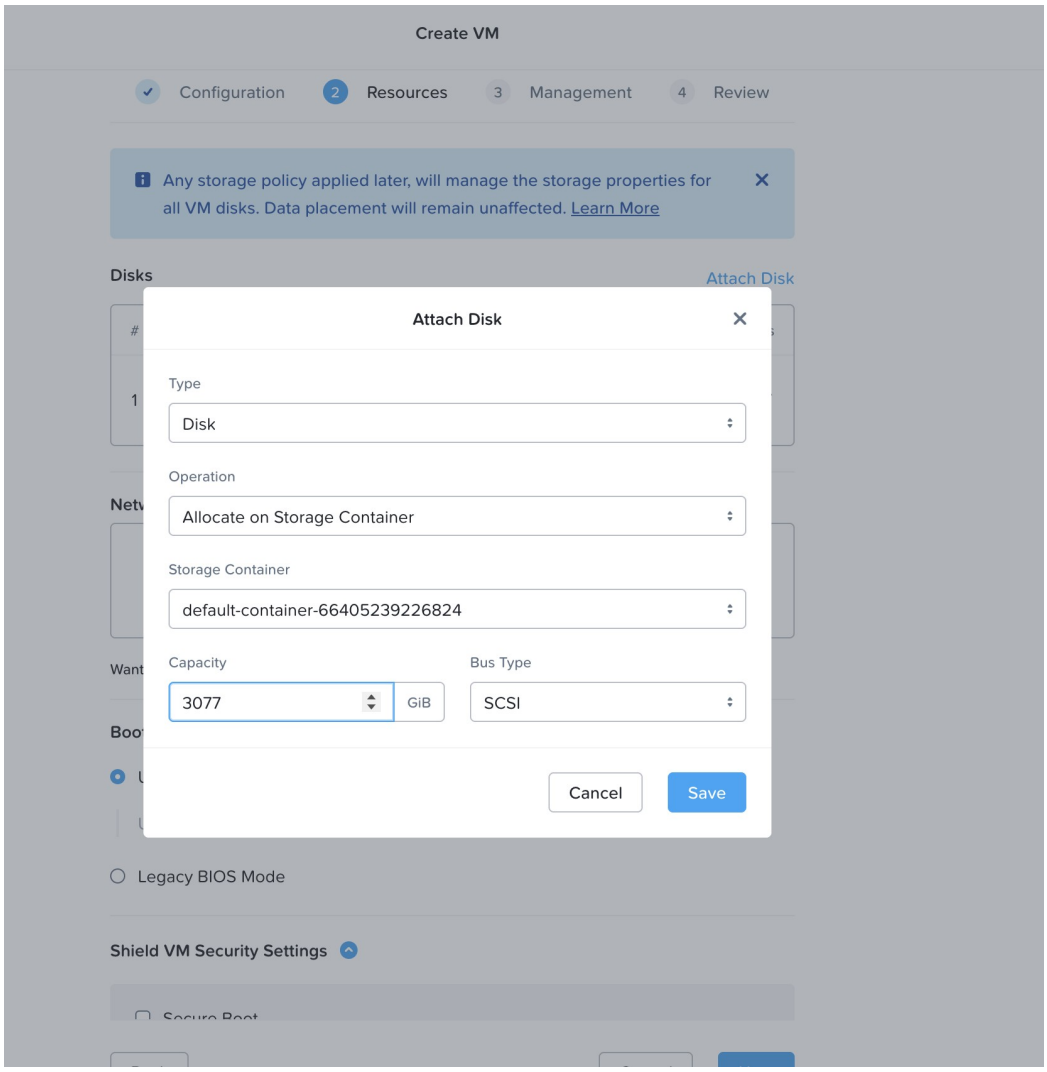
c) **2** で、**[**リソース（**Resources**）**]** ウィンドウで、**[**ディスク接続（**Attach Disk**）**]** をクリックしてブートディスクを VM に接続し、**[**保存（**Save**）**]**をクリックします。


Create VM
Configuration
2
Resources
3
Management
4
Review
Any storage policy applied later, will manage the storage properties for all VM disks. Data placement will remain unaffected. Learn More
Disks
Attach Disk
Networks
Attach to Subnet
Want to use this VM as a Traffic Mirror Destination? Add Mirror Destination NIC
Boot Configuration
UEFI BIOS Mode
UEFI BIOS Mode supports enhanced Shield VM security settings.
Legacy BIOS Mode
Shield VM Security Settings
Secure Boot
Back
Cancel
Next



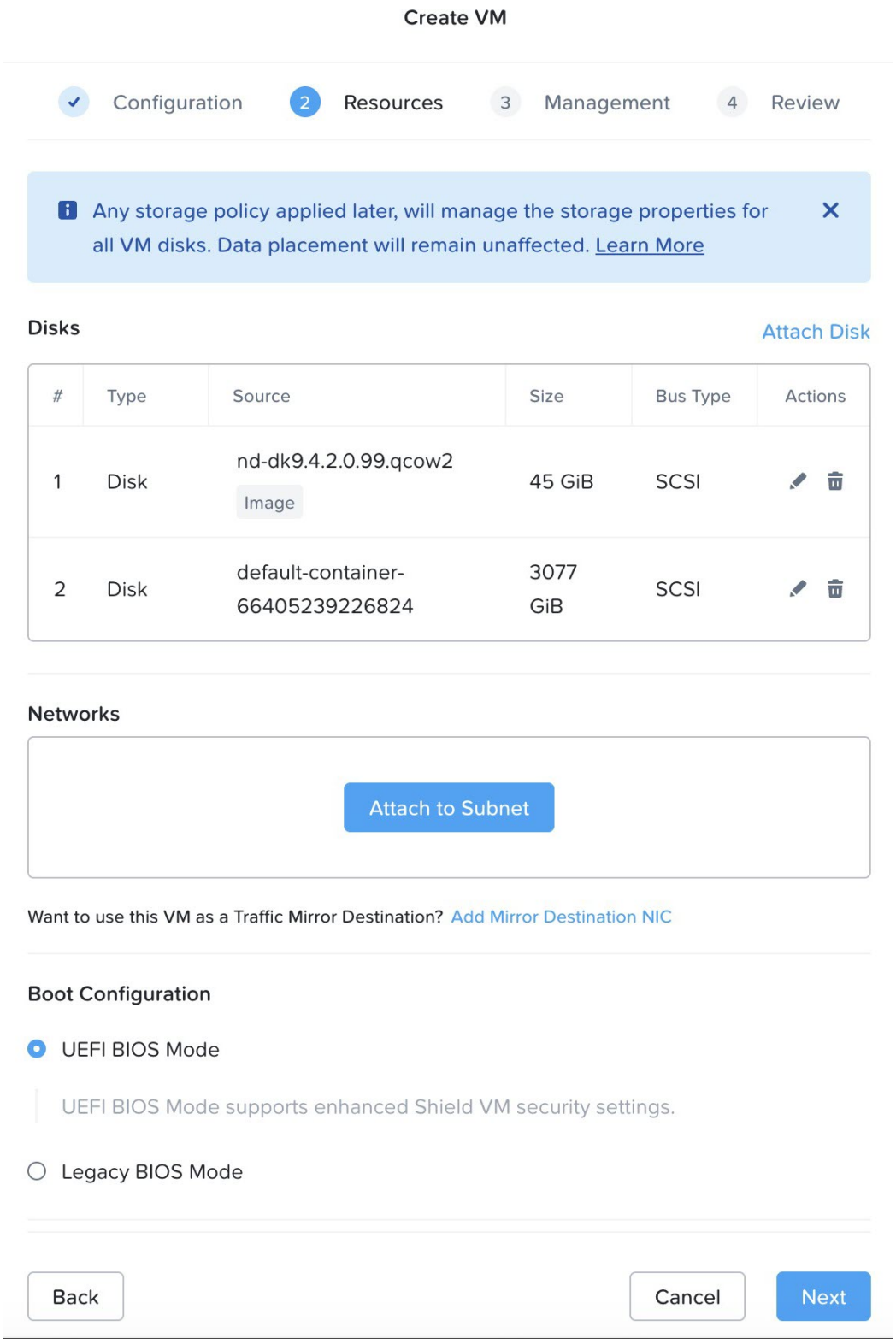
d) **2 で、[リソース（Resources）]** ウィンドウで、**[ディスク接続（Attach Disk）]** をクリックし、セカンダリ ディスクを追加します。

詳細については、「システム リソースを理解する （205 ページ）」を参照してください。



e) **2 で、[リソース（Resources）]** ウィンドウで、**[サブネットへ接続（Attach to Subnet）]** をクリックし、最初のサブネットの に必要な構成を行います。

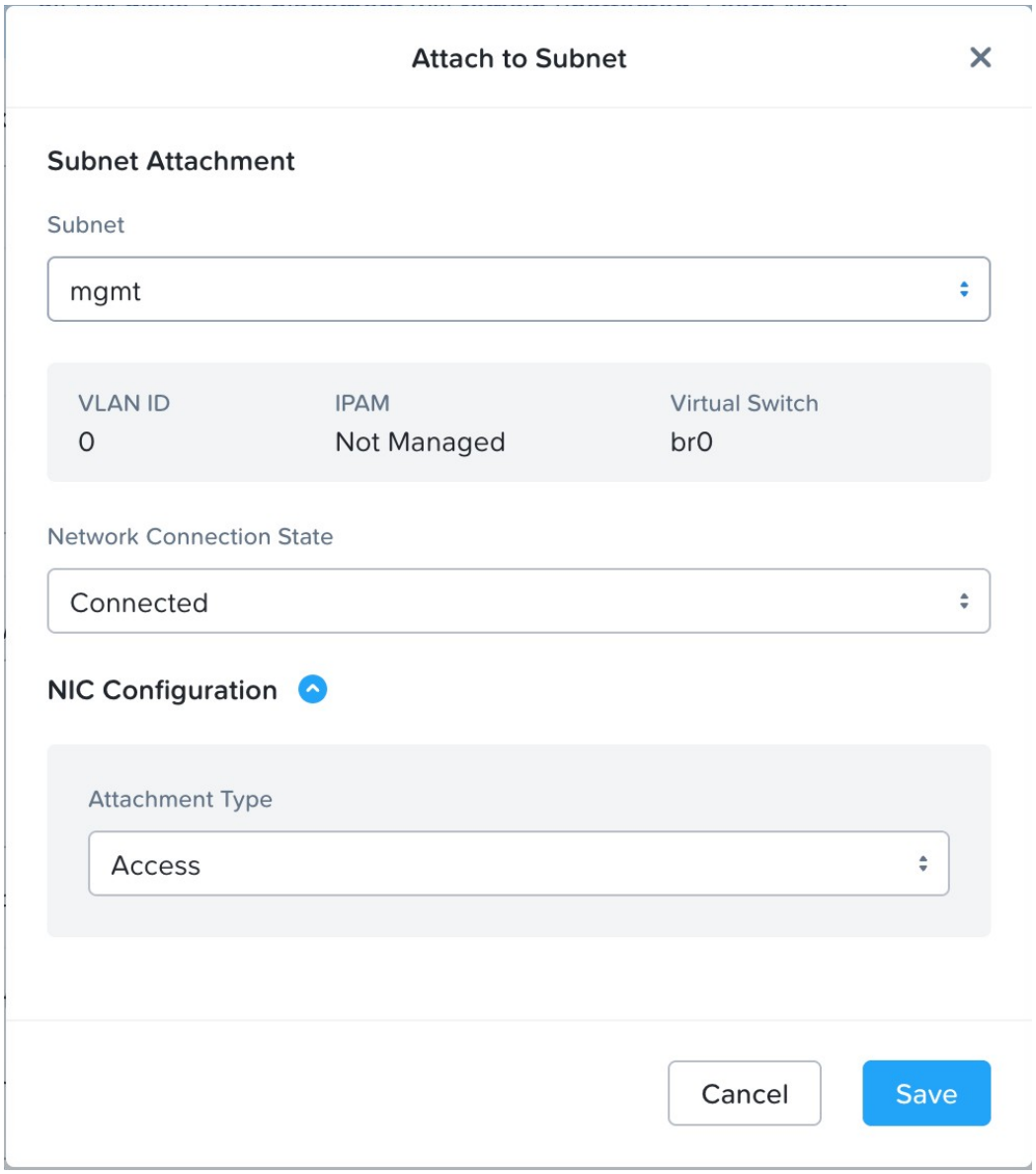
（注） 管理インターフェイスとデータ インターフェイスは、両方のサブネットが `VLAN Basic` または `VLAN` のいずれかである同じタイプのサブネットで作成する必要があります。管理インターフェイスとデータ インターフェイスに異なるサブネットタイプが使用されている場合、Nutanix での vND の展開は失敗します。



- **[サブネット（SUBNET）]** フィールドに、サブネットを入力します。

- **[接続タイプ（Attachment type）]** フィールドのエントリを環境を反映するように構成します。

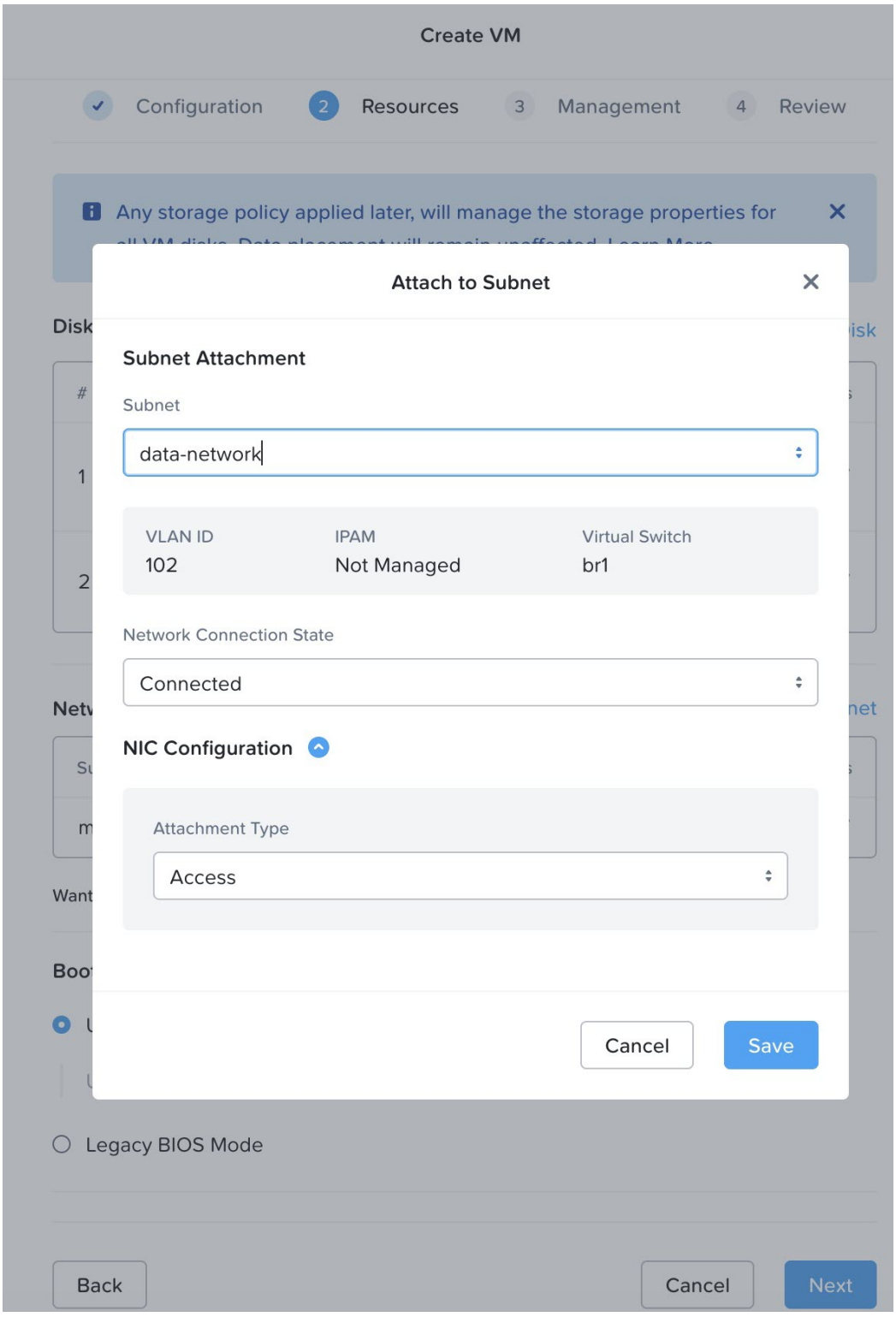
このウィンドウで構成を完了したら、**[保存（Save）]** をクリックします。



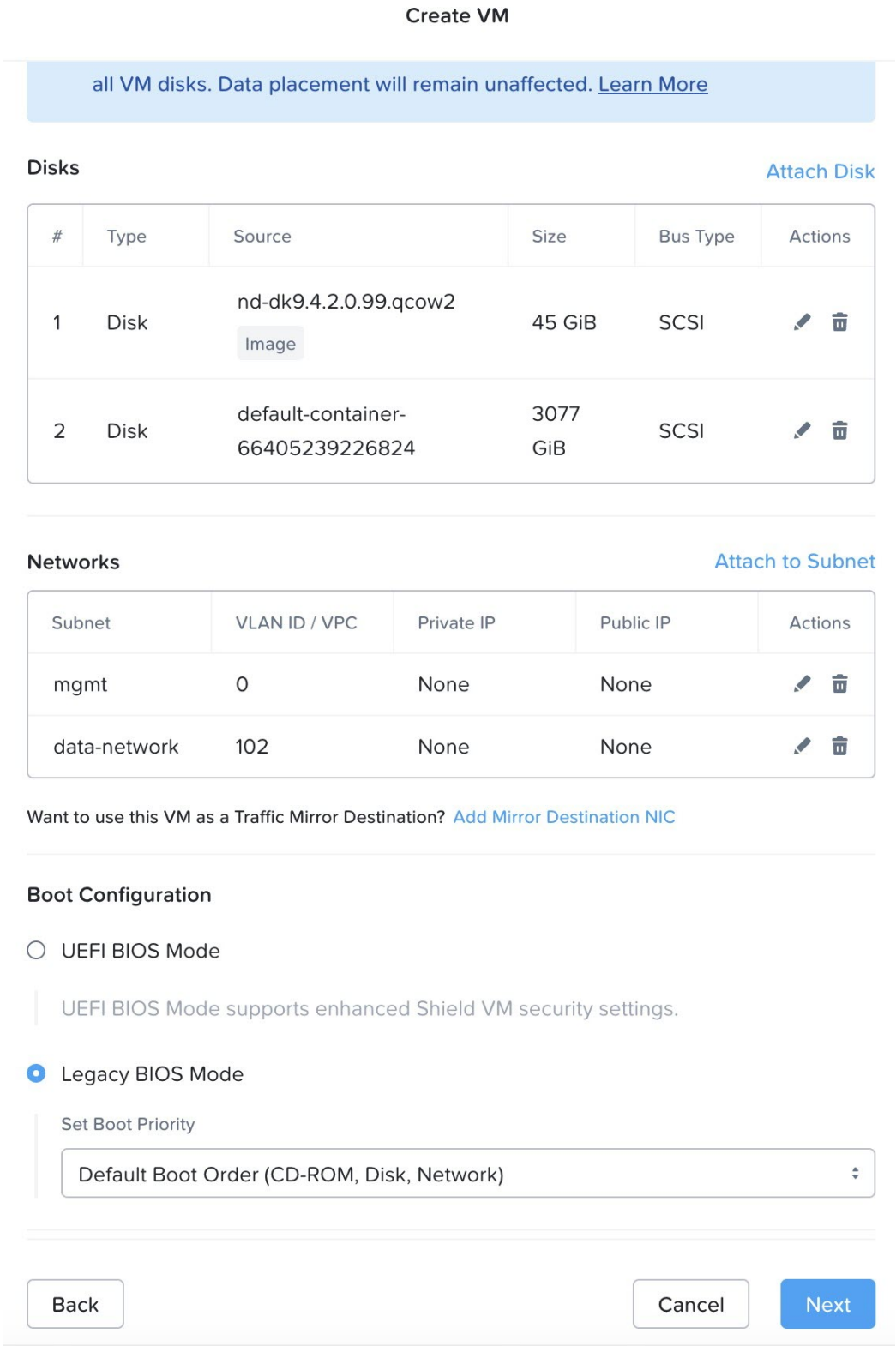
f) **2 で、[リソース（Resources）]** ウィンドウで、**[サブネットへ接続（Attach to Subnet）]** をクリックし、2 番目のサブネットに必要な構成を行います。

- **[サブネット (Subnet)]** フィールドに、データ サブネットを入力します。
- **[接続タイプ（Attachment type）]** フィールドのエントリを環境を反映するように構成します。

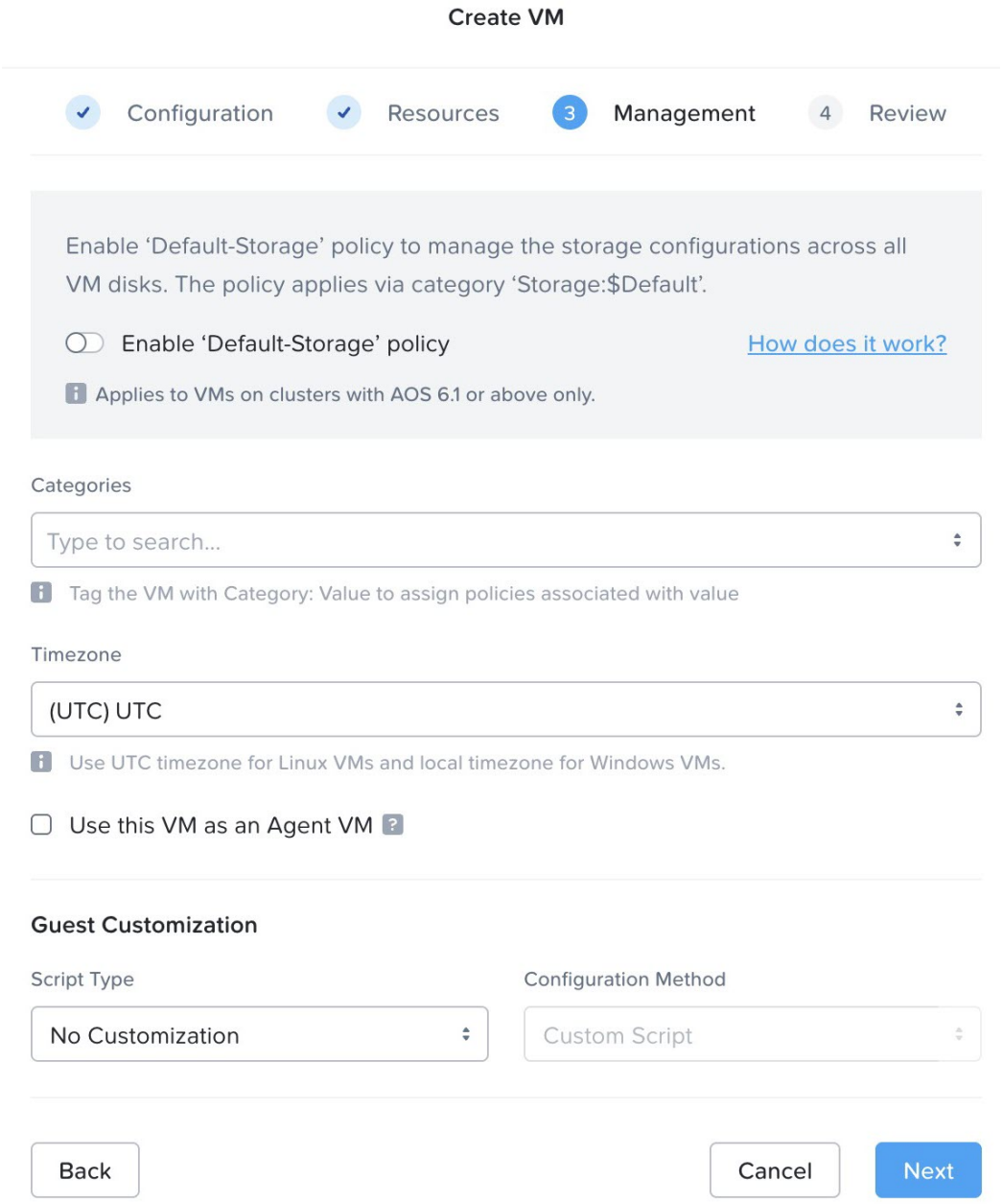
このウィンドウで構成を完了したら、**[保存（Save）]** をクリックします。



g) **2** で、**[**リソース（**Resources**）ウィンドウの **[**ブート構成（**Boot Configuration**）**]** 領域で、**[**レガシー **BIOS** モード（**Legacy BIOS Mode**）**]** を選択して、選択を確認します。

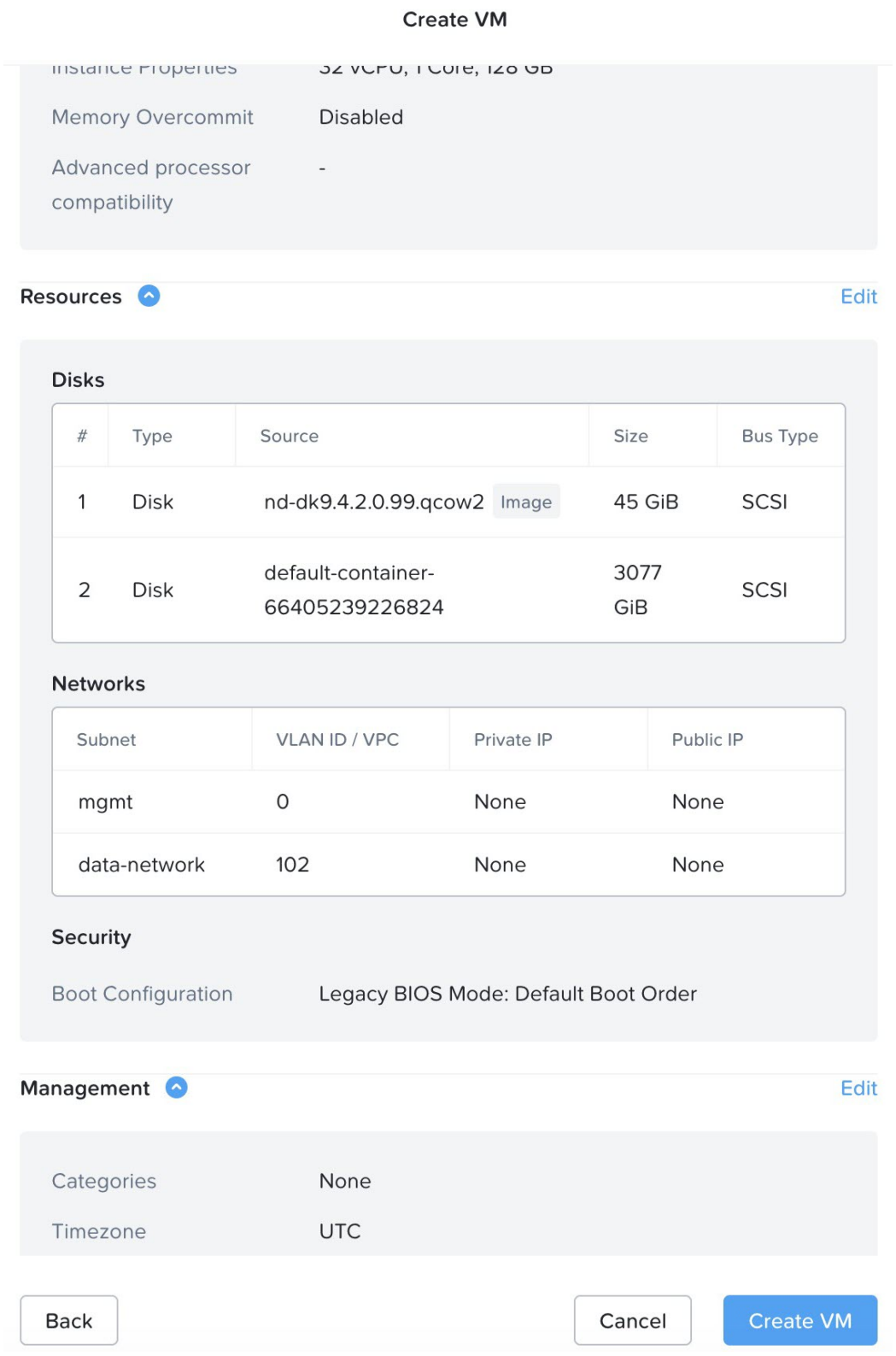

Create VM
all VM disks. Data placement will remain unaffected. Learn More
Disks
Attach Disk
Type Source Size Bus Type Actions
1 Disk nd-dk9.4.2.0.99.qcow2 Image 45 GiB SCSI
2 Disk default-container-66405239226824 3077 GiB SCSI
Networks
Attach to Subnet
Subnet VLAN ID / VPC Private IP Public IP Actions
mgmt 0 None None
data-network 102 None None
Want to use this VM as a Traffic Mirror Destination? Add Mirror Destination NIC
Boot Configuration
UEFI BIOS Mode
UEFI BIOS Mode supports enhanced Shield VM security settings.
Legacy BIOS Mode
Set Boot Priority
Default Boot Order (CD-ROM, Disk, Network)
Back
Cancel
Next

h) **[管理（Management）]** ウィンドウをナビゲートし、変更を加えることなく **[次へ（Next）]** をクリックします。

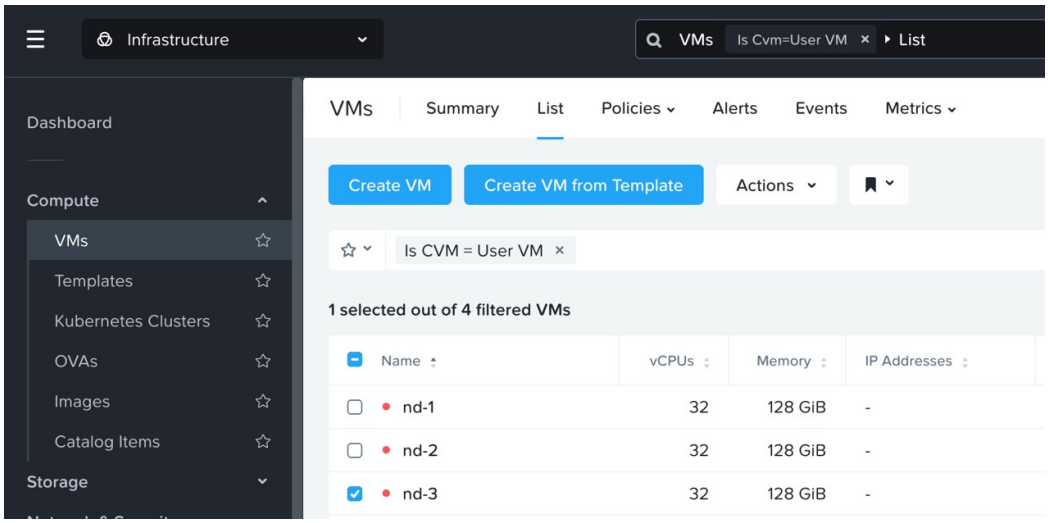


i) **[VMを作成（Create VM）]** をクリックします。

展開後に VM の電源をオンにしないでください。


Create VM
Instance Properties
32 vCPU, 1 Core, 128 GB
Memory Overcommit
Disabled
Advanced processor compatibility
-
Resources
Edit
Disks
Type Source Size Bus Type
1 Disk nd-dk9.4.2.0.99.qcow2 Image 45 GiB SCSI
2 Disk default-container-66405239226824 3077 GiB SCSI
Networks
Subnet VLAN ID / VPC Private IP Public IP
mgmt 0 None None
data-network 102 None None
Security
Boot Configuration
Legacy BIOS Mode: Default Boot Order
Management
Edit
Categories
None
Timezone
UTC
Back
Cancel
Create VM

j) 3 ノード クラスタに展開している場合は、クラスタ内の各 Nexus Dashboard ノードに対してこれらの手順を繰り返します。



k) シリアル コンソールを VM に接続します。

Nexus Dashboard には、構成とブートストラップのためのシリアル ポートが必要です。新しいシリアル ポートを管理および追加するには、 SSH を使用して CVM CLI にログオンします。

（注） その他の有用な情報については、 「*Serial Console Redirection to a Telnet Port*」を 参照してください。

```
nutanix@NTNX-35b35878-A-CVM:<nodeIP>:~$ acli vm.list
VM name VM UUID
PC-NameOption-1 201b8cf4-7ee6-409b-bb46-fca4265b6f70
nd-1 091c2d79-da94-4370-a77f-eccd998e2095
nd-2 58a04d9e-85da-4476-8735-bc6ed71e31ca
nd-3 c7f8feeb-b1c0-44a0-a5df-0dcfc30b07d8
nutanix@NTNX-35b35878-A-CVM:<nodeIP>:~$ acli vm.serial_port_create nd-1 index=0 type=kServer
VmUpdate: pending
VmUpdate: complete
1nutanix@NTNX-35b35878-A-CVM:<nodeIP>:~$ acli vm.serial_port_create nd-2 index=0 type=kServer
VmUpdate: pending
VmUpdate: complete
nutanix@NTNX-35b35878-A-CVM:<nodeIP>:~$ acli vm.serial_port_create nd-3 index=0 type=kServer
VmUpdate: pending
VmUpdate: complete
nutanix@NTNX-35b35878-A-CVM:<nodeIP>:~$
```

l) Nexus Dashboard VMs の電源をオンにします。

ステップ 9 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: <nodeIP>/<subnet>
  Gateway: <gatewayIP>
```

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: <gatewayIP>
  IP Address/Mask: <nodeIP>/<subnet>
Cluster leader: yes

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

ステップ 10 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 11 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://<gatewayIP>72 to continue.
```

ステップ 12 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 13 ログイン後、 **Meet Nexus Dashboard** の ウェルカム画面を確認し、 **ジャーニー** 画面に進みます。**クラスタの起動** 手順の下の **Go** をクリックして、ブートストラップ プロセスを開始します。

ステップ 14 **[クラスタのブリングアップ（Cluster Bringup）**] ウィザードの **[基本情報（Basic Information）]** ページに、必要な情報を入力します。

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

クラスタ名は、 RFC-1123 の要件に従う必要があります。

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

ステップ 15 **[クラスタのブリングアップ（Cluster Bringup）**] ウィザードの **[構成（Configuration）]** ページで、必要な情報を入力します。

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

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

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

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

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

- **キー**：NTP 認証キーを入力します。Nexus Dashboard と NTP サーバ間の NTP トラフィックを認証するために使用される暗号キーです。次の手順で NTP サーバーを定義します。複数の NTP サーバーで同じ NTP 認証キーを使用できます。
- **ID**： NTP ホストのキー ID を入力します。各 NTP キーに一意のキー ID を割り当てる必要があります。この ID は、NTP パケットの検証時に使用する適切なキーを識別するために使用されます。
- **認証タイプ**：NTPキーの認証タイプを選択します。

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

NTP認証の要件とガイドラインの完全なリストについては、全般的な前提条件とガイドライン （13 ページ） を参照してください。

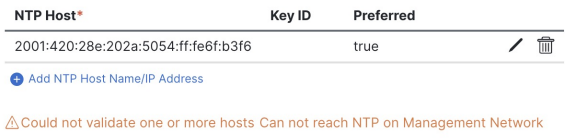
追加のNTPキーを入力する場合は、 **[+ キーの追加（+ Add Key）]** を再度クリックして、情報を入力します。

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

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

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

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



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

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

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

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

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

プロキシ サーバでは、永続 URL を許可する必要があります：

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

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

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

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

詳細設定では、次の設定を行うことができます。

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

アプリケーションおよびサービス ネットワークの詳細については、全般的な前提条件とガイドライン （13 ページ） を参照してください。

j) [次へ（Next）] をクリックします。

ステップ 16 **[ノードの詳細（Node Details）]** ページで、最初のノードの情報を更新します。

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

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

テレメトリで使用される永続的な IP アドレス機能には、BGP 構成が必要です。この機能の詳細については、BGP 構成と永続的な IP アドレス （60 ページ） およびNexus Dashboardの 永続 IP アドレス（52 ページ） セクションで説明します。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

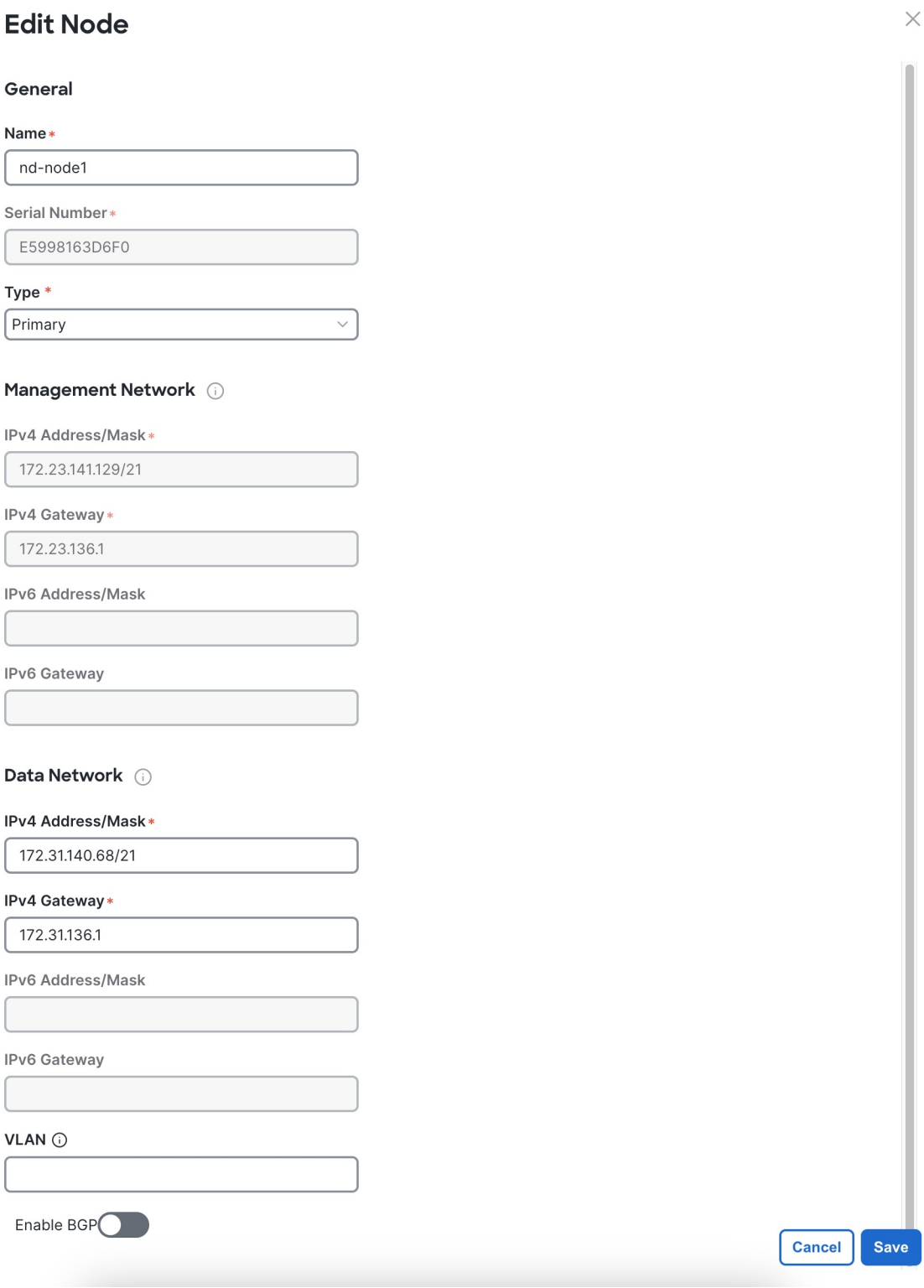
[+ IPv4 BGP ピアの追加（+ Add IPv4 BGP peer）] をクリックして、ピアを追加できます。

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

g) **[Save]**をクリックして、変更内容を保存します。

ステップ 17 [**ノードの詳細（Node Details）**] 画面で、[**ノードの追加（Add Node）**] をクリックして、クラスタに 2 番目のノードを追加します。

単一ノード クラスタを展開する場合は、この手順をスキップします。



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

ノードの初期構成手順で、管理ネットワーク情報とパスワードを定義しました。

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

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

c) ノードの **[名前（Name）]** を入力します。

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

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

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

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

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

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

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

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

永続 IP アドレス機能には BGP 設定が必要です。この機能については、BGP 構成と永続的な IP アドレス （60 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。

- IPv6 専用の場合、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 18 **[ノードの詳細（Node Details）]** ページで、入力した情報を確認してから、**[次へ（Next）]**をクリックします。

ステップ 19 クラスタの**展開モード**を選択します。

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

永続 IP アドレスの詳細については、Nexus Dashboardの 永続 IP アドレス （52 ページ）のセクションを参照してください：

b) [次へ（Next）] をクリックして続行します。

ステップ 20 **[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。

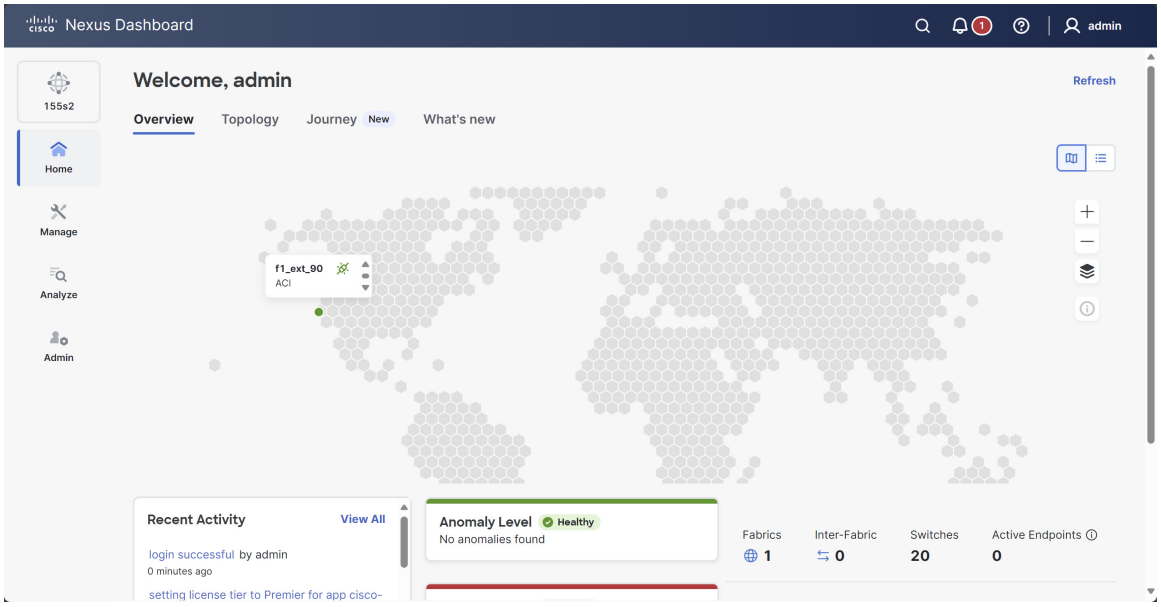
ノードのブート ストラップとクラスタの起動中に、全体的な進捗状況と各ノードの個々の進捗状況がUIに表示されます。ブートストラップの進行状況が表示されない場合は、ブラウザでページを手動で更新し、ステータスを更新してください。

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 Dashboard GUI にリロードされます。

ステップ 21 クラスタが健全であることを検証します。

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

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



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

- クラスタが収束している間、次の出力が表示されることがあります：

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

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

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

- クラスタが稼働している場合は、次の出力が表示されます。

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

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

```
deploy base system services
```

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

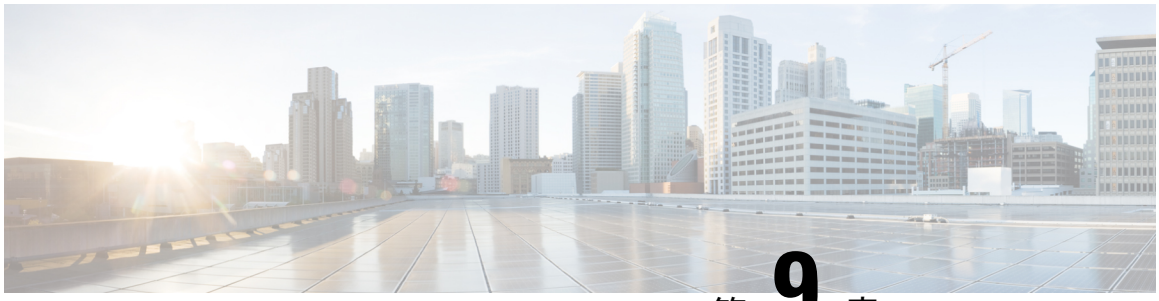
この問題を解決するには、影響を受けるノードで `acs reboot clean` コマンドを入力します。

ステップ 22 （オプション） Cisco Nexus DashboardクラスターをCisco Intersightに接続、可視性と利点を強化します。詳細な手順については、 「*Cisco Intersight*の操作」 を参照してください。

ステップ 23 Nexus Dashboardを展開した後、設定情報については、このリリースのコレクションページを参照してください。

次のタスク

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



第 9 章

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

- AWS パブリッククラウドでの vND のホスティングについて （239 ページ）
- Amazon Web Services で Nexus Dashboard クラスタを展開するための前提条件と注意事項（241 ページ）
- Nexus Dashboard クラスタ向け Amazon Web サービスの準備 （243 ページ）
- Amazon Web Services（AWS）に仮想 Nexus Dashboard（vND）を展開する （244 ページ）
- ノードの交換（RMA） （252 ページ）

AWS パブリッククラウドでの vND のホスティングについて

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

- Virtual Nexus Dashboard
- N9000 スイッチ
- 2 つの Catalyst 8000 シリーズ ルータ、または Nexus ダッシュボードが vND からオンプレミス データセンターへの VXLAN トンネルを終端して永続 IP アドレス（PIP）トラフィックに使用できる別のタイプのデバイス（N9000 スイッチなど）
- AWS パブリック クラウド アカウント

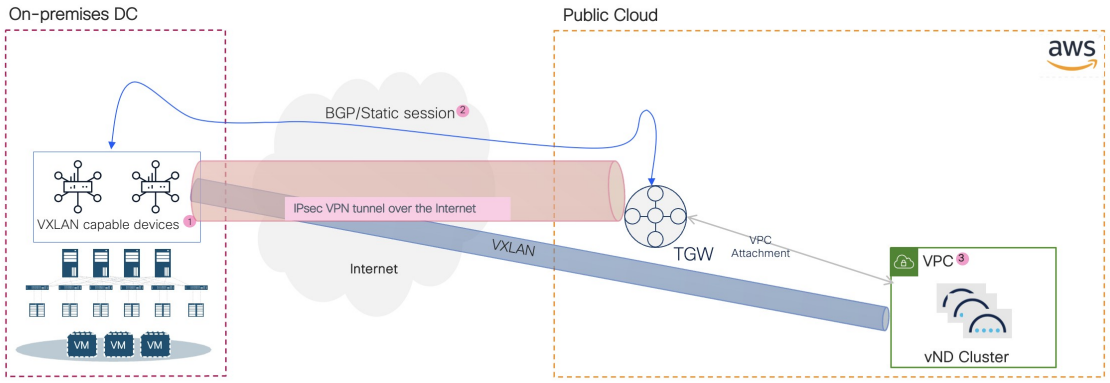
AWS パブリック クラウドでの vND の展開方法を理解する

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

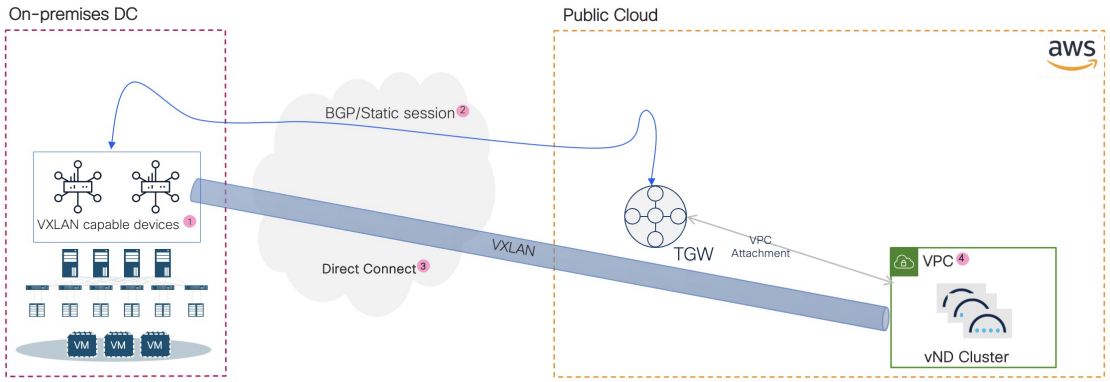
ス（**System Status**）]>[概要（**Overview**）]に移動し、[クラスタノード（**Cluster nodes**）]領域での 3 ノードクラスターに関する情報を表示します。

トポロジの例

次の図は、トポロジの例を示しています。



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



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

ここで、

- オンプレミスのデータセンターと AWS パブリッククラウドの間の接続は、直接接続（実稼働環境に推奨）または 2 つの間の IPSec トンネル（追加のオーバーヘッドとして PoC またはラボ用）のいずれかを使用して実現されます。
- 2 つのオンプレミスルータは、次のいずれかになります。
  - 直接接続を使用する場合は、N9000 スイッチなどの 2 つの物理スイッチを使用できます。

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

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

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

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

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

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

- この機能は、単一の製品としてNexus Dashboard を備えた AWS の 3ノード仮想クラスタ（データ）でサポートされています（IPv4 のみ）。
- この機能では、LAN（NX- OS）および ACI ファブリックがサポートされます。また、次の機能が有効になっている場合のみサポートされます。
  - コントローラ
  - オーケストレーション
  - テレメトリ、次の制限あり：
    - アウトオブバンドのみ
    - トラフィック分析、ただしフロー テレメトリなし
- この機能は、LAN および ACI ファブリックでサポートされています。メディア用の IP ファブリック（IPFM）または SAN ファブリックではサポートされません。

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

- セカンダリ/ワーカーノードは、この機能ではサポートされていません。3 つのプライマリ ノードと 1 つのスタンバイ ノードのみがサポートされます。
- クラスターあたりのスケール：単一の 3 ノード vNDクラスター上で 100 個のスイッチ
- AWS に vND を展開した後は、トンネルエンドポイントに割り当てられた IP アドレスまたは VNI を変更することはできません。
- Nexus Dashboard vND を展開する前に、オンプレミス サイトを準備して、Catalyst 8000 シリーズ ルータまたは N9000 スイッチのペアを展開しておくことがベストです。これにより、Nexus Dashboard vND のデプロイメントの間に、必要な BDI と TEP IP アドレスを提供できます。必要に応じて、 Nexus Dashboard vND を展開した後にオンプレミス ネットワーク アプライアンスを展開できますが、その場合、 Nexus Dashboard vND のデプロイメント時に提供したのと同じ情報を使用してオンプレミスデバイスを設定する必要があります。両方の場所で同じ設定情報を提供しない場合は、 Nexus Dashboard vNDを再インストールする必要があります。
- オンプレミスの VXLAN 対応デバイスが正しく構成されていることを確認します。
  - データプレーン：入力レプリケーション
  - コントロールプレーン：フラッディングと学習
- ファクターから AWS が拡張性とサービス要件をサポートしていることを確認します。

  クラスタ フォーム ファクタに基づいて、拡張性とサービス サポートおよび共同ホストは異なります。Nexus ダッシュボード キャパシティ プラン ツールを使用して、仮想フォーム ファクタが展開要件を満たすことを確認できます。
- 全般的な前提条件とガイドライン （13 ページ） に記載されている一般的な前提条件を確認して完了します。
- 展開する予定のサービスのリリース ノートに記載されている追加の前提条件を確認して完了します。
- AWS アカウントに適切なアクセス権限があること。

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

- Nexus Dashboard クラスタ向け Amazon Web サービスの準備 （243 ページ）の手順を実行します。

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

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

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

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

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

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

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

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

- 6 つのサブネットを作成します：

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

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

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

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

- 管理サブネットの IP アドレスは、デプロイメントの一部として AWS Elastic IP アドレスにマッピングされるため、これらの管理サブネットには外部アクセスが必要です。データサブネットは、vNDからVXLANトンネル（永続的なポッドによって使用される）の終端に使用されるオンプレミスのデバイスおよびオンプレミスの Catalyst 8000 シリーズ ルータ（または N9000 スイッチなどの他のデバイス）に到達できる必要があります。

- AWS によって所有されておらず、PIP（永続的な IP アドレス）によって使用されるオンプレミスのデータセンター（ただしまだ使用されていない）から取得される /28（100.100.100.0/28 など）のサブネット 1 つ。ここでそのサブネットの 100.100.100.1 と 100.100.100.2 は、オンプレミス データセンター デバイス（Catalyst 8000 または N9000 スイッチ）の BDI IP アドレスである必要があり、残りの IP アドレスは vND 永続ポッド（トラップ、テレメトリコレクタなど）によって使用されます。

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

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

- デプロイメント用に 1 つの EC2 キーペアを設定します。

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

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

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

始める前に

- Amazon Web Services で Nexus Dashboard クラスタを展開するための前提条件と注意事項（241 ページ） に記載されている要件とガイドラインを満たしていることを確認します。

手順

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

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

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

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

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

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

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

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

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

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

ステップ 2 ソフトウェア オプションと地域を選択します。

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

- **履行オプション（Fulfillment option）** ：デフォルトの [**Nexus Dashboard - Cloud Deployment）]** の 選択をそのままにします。
- **ソフトウェア バージョン**：ドロップダウンリストから使用可能な最新の 4.2.1 オプションを選択します。
- **リージョン**：テンプレートを展開する適切なリージョンを選択します。

  これは、VPC を作成したのと同じリージョンである必要があります。

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

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

[Create Stack（スタックの作成）] ページが表示されます。

ステップ 3 スタック設定を完了します。

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

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

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

b) [**次へ（Next）**] をクリックして続行します。

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

ステップ 4 スタックの詳細を指定します。

a) **スタック名**を入力します。

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

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

- **[Nexus Dashboard クラスタ名（Nexus Dashboard Cluster Name）]** フィールドに、クラスタ名を入力します。
- **[ファブリック展開モード（Fabric Deployment Mode）]** フィールドで、デフォルトの**[LAN]** オプションは、 Nexus Dashboard 4.2.1 リリースでサポートされている唯一のオプションです。
- **[VPC 識別子（VPC identifier）]**フィールドに、VPC 識別子を入力します。

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

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

  Nexus Dashboard ノードの管理者パスワードには、少なくとも 1 つの文字、数字、特殊文字（@$!%*#?&）を含める必要があり、長さは 8～64 文字にする必要があります。

- （オプション）**キーペア名（Key Pair Name）** フィールドで、 Nexus Dashboard への SSH アクセスを有効にする既存の SSH キーペアの名前を指定します。

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

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

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

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

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

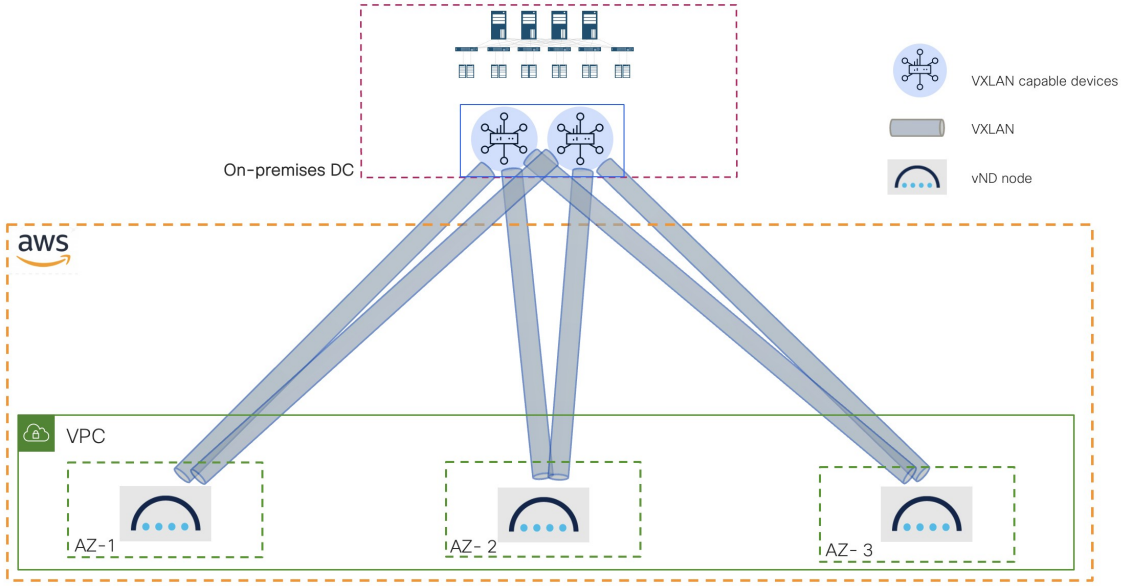
e) **[NTP 構成（NTP Configuration）]**エリアで、必要に応じて設定情報を入力します。

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

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

- **[デバイス VXLAN ID（Device VXLAN Identifier） (VNI)]** フィールドに、Cisco VXLAN 対応デバイス（IPSec トンネルを使用している場合）または N9000 スイッチ（直接接続を使用している場合）と Nexus Dashboard ノード間の VXLAN トンネルに使用する VNI 値を入力します。

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



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

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

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

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

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

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

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

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

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

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

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

  これは通常、サブネットの最初のアドレスです。

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

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

  CIDR 範囲は「/16」固定です。

- **[Kubernetes アプリ ネットワーク（Kubernetes App Network）]** フィールドに、kubernetes アプリネットワークのネットワーク アドレスを入力します。

  CIDR 範囲は「/16」固定です。

i) [**次へ（Next**）] をクリックして続行します。

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

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

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

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

ステップ 7 展開が完了するのを待ってから、VM を起動します。

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

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

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

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

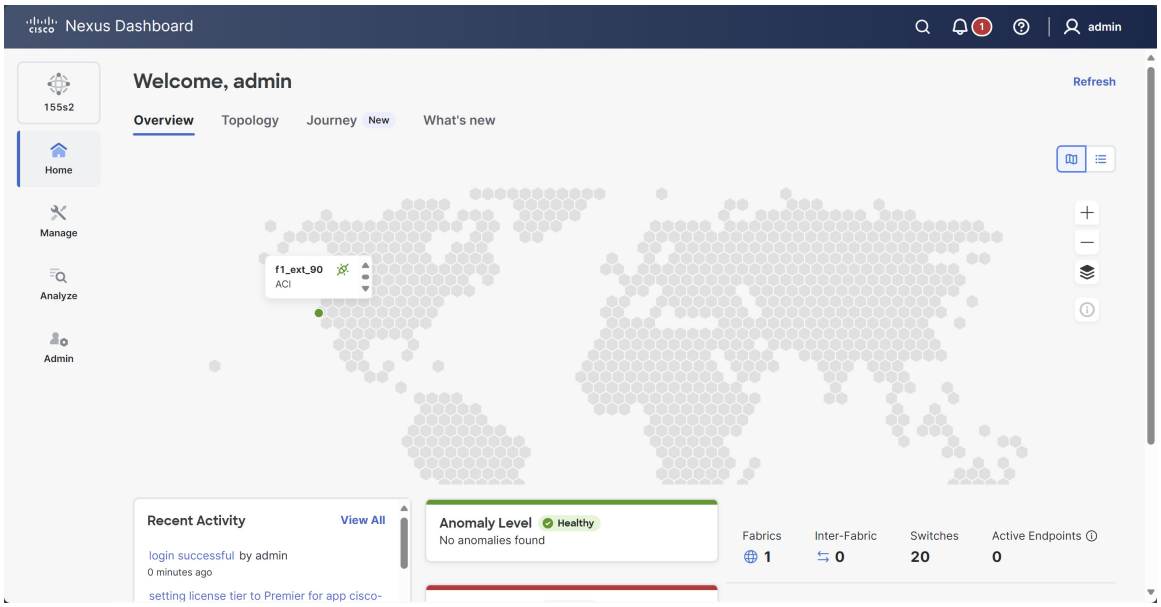
ステップ 9 前の手順にリストされているパブリック IP アドレスのいずれかを使用して、Nexus Dashboard GUI にログインします。

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

ステップ 10 クラスタが健全であることを検証します。

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

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



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

- クラスタが収束している間、次の出力が表示されることがあります：

```
$ acs health
k8s install is in-progress
```

```
$ acs health
k8s services not in desired state - [...]
```

```
$ acs health
k8s: Etcd cluster is not ready
```

- クラスタが稼働している場合は、次の出力が表示されます。

```
$ acs health
All components are healthy
```

（注） 場合によっては、ノードの電源を再投入（電源をオフにしてから再度オン）すると、この段階でスタックが停止することがある可能性があります。

```
deploy base system services
```

これは、pND（物理 Nexus Dashboard）クラスタの再起動後のノードの `etcd` の問題が原因です。

この問題を解決するには、影響を受けるノードで `acs reboot clean` コマンドを入力します。

ステップ 11 （オプション） Cisco Nexus DashboardクラスターをCisco Intersightに接続、可視性と利点を強化します。詳細な手順については、 「*Cisco Intersight*の操作」 を参照してください。

ステップ 12 Nexus Dashboardを展開した後、設定情報については、このリリースのコレクションページを参照してください。

次のタスク

次のタスクは、ファブリックとファブリック グループを作成することです。 Cisco Nexus Dashboardのコレクション ページ にある、このリリースの 「ファブリックとファブリック グループの作成」の記事を参照してください。

ノードの交換（RMA）

AWS ベースの Nexus Dashboard の展開では、ノードが何らかの理由で RMA または交換が必要な場合、新しい交換用ノードをAWS に展開する必要があります。

オンプレミスの物理 Nexus Dashboard（pND）およびリモート対応 Nexus Dashboard（vND）の展開で使用可能な工場出荷時の状態へのリセットとノードの復元オプションは、AWS ベースのノードではサポートされていません。したがって、影響を受けたノードをその場所で回復することはできず、新しいノードとして再展開する必要があります。

元の 3 ノード CloudFormation（CFT）テンプレートを使用して個々のノードを置き換えないでください。単一ノードの交換の場合は、以下に示す専用の単一ノード CFT テンプレートを使用して新しいノードを展開します。

```
{
    "AWSTemplateFormatVersion": "2010-09-09",
    "Description": "This cloud formation template automates the creation and launching
of a Cisco Nexus Dashboard cluster (vND data 32vCPU/128GMem/10G Network/3T Disk) in
multiple Availability Zones (AZs) of AWS. Deployment requires a Application VPC to exist
 in the account from which the cluster will be is launched. For detailed, description
of this template and usage instructions please refer to ND deployment guide.",
    "Metadata": {
        "AWS::CloudFormation::Interface": {
            "ParameterGroups": [
                {
                    "Label": {
                        "default": "Nexus Dashboard Basic Configuration"
                    },
                    "Parameters": [
                        "NDClusterName",
                        "FabricPersona",
                        "VpcId",
                        "SecurityGroupId",
                        "InstanceType",
                        "AMIId",
                        "AdminPassword",
                        "KeyPairName",
                        "ExistingEIPAllocationId1",
                        "ExistingEIPAddress1"
                    ]
                },
```

```
                {
                    "Label": {
                        "default": "Nexus Dashboard Node Configuration"
                    },
                    "Parameters": [
                        "hostNameND1",
                        "SubnetNDMgmt1",
                        "StaticNDMgmt1IP",
                        "SubnetNDMgmt1Netmask",
                        "SubnetNDMgmt1Gateway",
                        "SubnetNDData1",
                        "StaticNDData1IP",
                        "SubnetNDData1Netmask",
                        "SubnetNDData1Gateway"
                    ]
                }
            ],
            "ParameterLabels": {
                "NDClusterName": { "default": "ND Cluster Name" },
                "VpcId": { "default": "VPC identifier" },
                "hostNameND1": { "default": "ND Node Hostname" },
                "SubnetNDMgmt1": { "default": "ND Node Management Subnet" },
                "StaticNDMgmt1IP": { "default": "ND Node Static Management IP" },
               "SubnetNDMgmt1Netmask": { "default": "ND Node Management Subnet Netmask"
},
               "SubnetNDMgmt1Gateway": { "default": "ND Node Management Subnet Gateway"
},
                "SubnetNDData1": { "default": "ND Node Data Subnet" },
                "StaticNDData1IP": { "default": "ND Node Static Data IP" },
                "SubnetNDData1Netmask": { "default": "ND Node Data Subnet Netmask" },
                "SubnetNDData1Gateway": { "default": "ND Node Data Subnet Gateway" },
                "SecurityGroupId": { "default": "Security Group identifier" },
                "InstanceType": { "default": "Instance Type" },
                "AMIId": { "default": "AMI identifier" },
                "AdminPassword": { "default": "Password" },
                "KeyPairName": { "default": "Key Pair Name" },
                "ExistingEIPAllocationId1": { "default": "ND Node 1 EIP Allocation ID."
},
                "ExistingEIPAddress1": { "default": "ND Node 1 Elastic IP." }
            }
        }
    },
    "Parameters": {
        "NDClusterName": {
            "Type": "String",
            "Description": "Nexus Dashboard Cluster name.",
            "MinLength": 1
        },
        "VpcId": {
            "Type": "String",
           "Description": "VpcId of your existing Virtual Private Cloud (VPC) to launch
ND cluster.",
            "ConstraintDescription": "Must be the VPC Id of an existing Virtual Private
Cloud."
        },
        "hostNameND1": {
            "Type": "String",
            "Description": "Specify the hostname for ND Node 1.",
            "Default": "AWSND1"
        },
        "SubnetNDMgmt1": {
            "Type": "AWS::EC2::Subnet::Id",
            "Description": "Select the 1st management subnet for the ND Node 1."
        },
```

```
        "StaticNDMgmt1IP": {
            "Type": "String",
            "Description": "Specify a static management IP address from the selected
subnet. Ensure not in-use already.",
            "AllowedPattern": "^(\\d{1,3})\\.(\\d{1,3})\\.(\\d{1,3})\\.(\\d{1,3})$",
            "Default": "0.0.0.0"
        },
        "SubnetNDMgmt1Netmask": {
            "Type": "String",
            "Description": "Specify the 1st management subnet netmask in CIDR notation
(16-28).",
            "Default": "24",
            "AllowedPattern": "^(1[6-9]|2[0-8])$"
        },
        "SubnetNDMgmt1Gateway": {
            "Type": "String",
            "Description": "Specify the 1st management default gateway on the selected
management subnet. This is typically the first address on the subnet.",
            "AllowedPattern": "^(\\d{1,3})\\.(\\d{1,3})\\.(\\d{1,3})\\.(\\d{1,3})$",
            "Default": "0.0.0.0"
        },
        "SubnetNDData1": {
            "Type": "AWS::EC2::Subnet::Id",
            "Description": "Select the 1st data subnet for the ND Node 1."
        },
        "StaticNDData1IP": {
            "Type": "String",
            "Description": "Specify a static data IP address from the selected subnet.
Ensure not in-use already.",
            "AllowedPattern": "^(\\d{1,3})\\.(\\d{1,3})\\.(\\d{1,3})\\.(\\d{1,3})$",
            "Default": "0.0.0.0"
        },
        "SubnetNDData1Netmask": {
            "Type": "String",
          "Description": "Specify the 1st data subnet netmask in CIDR notation (16-28).",

            "Default": "24",
            "AllowedPattern": "^(1[6-9]|2[0-8])$"
        },
        "SubnetNDData1Gateway": {
            "Type": "String",
          "Description": "Specify the 1st data default gateway on the selected management
 subnet. This is typically the first address on the subnet.",
            "AllowedPattern": "^(\\d{1,3})\\.(\\d{1,3})\\.(\\d{1,3})\\.(\\d{1,3})$",
            "Default": "0.0.0.0"
        },
        "SecurityGroupId": {
            "Type": "AWS::EC2::SecurityGroup::Id",
           "Description": "Pre-created security group to be applied. Must allow ingress
 access for ports 22, 443. Check docs for other needed ports."
        },
        "InstanceType": {
            "Type": "String",
            "Description": "Specify EC2 instance type for the node instances.",
            "AllowedValues": ["m5.8xlarge"],
            "Default": "m5.8xlarge"
        },
        "AMIId": {
            "Type": "AWS::EC2::Image::Id",
            "Description": "Specify the AWS AMI for Nexus Dashboard."
        },
        "AdminPassword": {
            "Type": "String",
            "Description": "Admin user password for ND node (must contain atleast 1
```

```
letter, number and special char @$!%*#?& length: 8-64 chars).",
            "NoEcho": true,
            "MinLength": 8,
            "MaxLength": 64,
            "AllowedPattern":
"^(?=.*[A-Za-z])(?=.*\\d)(?=.*[@$!%*#?&])[A-Za-z\\d@$!%*#?&]{8,64}$"
        },
        "KeyPairName": {
            "Type": "AWS::EC2::KeyPair::KeyName",
           "Description": "Required - Specify Name of an existing SSH KeyPair to enable
 SSH access to ND."
        },
        "ExistingEIPAllocationId1": {
            "Type": "String",
            "Description": "Allocation ID of an existing Elastic IP for ND Node 1."
        },
        "ExistingEIPAddress1": {
            "Type": "String",
            "Description": "Public IP of the existing Elastic IP (e.g., 203.0.113.42)
for ND Node 1.",
            "Default": "0.0.0.0"
        }
    },
    "Resources": {
        "ND1": {
            "Type": "AWS::EC2::Instance",
            "Properties": {
                "InstanceType": { "Ref": "InstanceType" },
                "ImageId": { "Ref": "AMIId" },
                "KeyName": { "Ref": "KeyPairName" },
                "NetworkInterfaces": [
                    {
                        "DeviceIndex": 0,
                        "NetworkInterfaceId": { "Ref": "ND1MgmtENI" }
                    },
                    {
                        "DeviceIndex": 1,
                        "NetworkInterfaceId": { "Ref": "ND1DataENI" }
                    }
                ],
                "EbsOptimized": true,
                "BlockDeviceMappings": [
                    {
                        "DeviceName": "/dev/xvda",
                        "Ebs": { "VolumeType": "gp3", "Iops": 5000 }
                    },
                    {
                        "DeviceName": "/dev/xvdh",
                        "Ebs": {
                            "VolumeSize": 3072,
                            "VolumeType": "gp3",
                            "Iops": 5000
                        }
                    }
                ],
                "Tags": [{ "Key": "Name", "Value": "ND1-Master" }],
                "UserData": {
                    "Fn::Base64": {
                        "Fn::Sub": "{\n \"password\": \"${AdminPassword}\",\n
\"clusterName\": \"${NDClusterName}\",\n \"oobNetwork\": {\n    \"ipSubnet\":
\"${StaticNDMgmt1IP}/${SubnetNDMgmt1Netmask}\",\n    \"gateway\":
\"${SubnetNDMgmt1Gateway}\"\n  }\n}\n"
                    }
                }
```

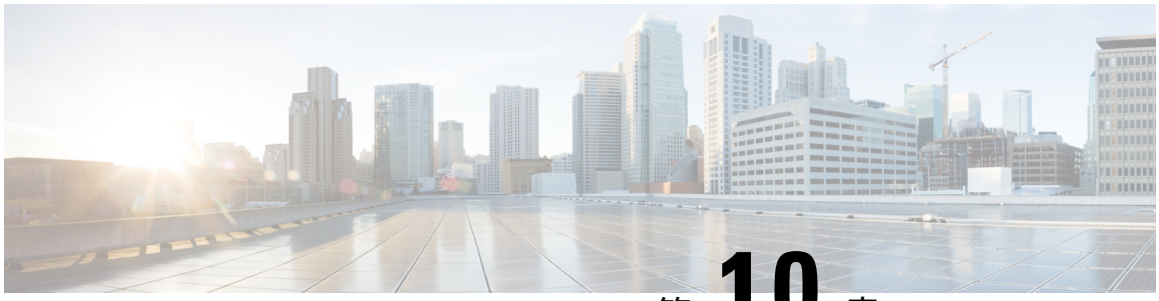
```
                }
            },
            "ND1MgmtENI": {
                "Type": "AWS::EC2::NetworkInterface",
                "Properties": {
                    "SubnetId": { "Ref": "SubnetNDMgmt1" },
                    "PrivateIpAddresses": [
                        {
                            "PrivateIpAddress": { "Ref": "StaticNDMgmt1IP" },
                            "Primary": true
                        }
                    ],
                    "GroupSet": [{ "Ref": "SecurityGroupId" }]
                }
            },
            "EIPAssoc1": {
                "Type": "AWS::EC2::EIPAssociation",
                "Properties": {
                    "NetworkInterfaceId": { "Ref": "ND1MgmtENI" },
                    "AllocationId": { "Ref": "ExistingEIPAllocationId1" }
                }
            },
            "ND1DataENI": {
                "Type": "AWS::EC2::NetworkInterface",
                "Properties": {
                    "SubnetId": { "Ref": "SubnetNDData1" },
                    "PrivateIpAddresses": [
                        {
                            "PrivateIpAddress": { "Ref": "StaticNDData1IP" },
                            "Primary": true
                        }
                    ],
                    "GroupSet": [{ "Ref": "SecurityGroupId" }]
                }
            }
        },
        "Outputs": {
            "ND1PublicIP": {
                "Description": "Public IP of ND Node 1.",
                "Value": { "Ref": "ExistingEIPAddress1" }
            }
        }
}
```



第 III 部

このリリースへのアップグレードまたは移行

- Nexus Dashboard 3.2.2m クラスタのこのリリースへのアップグレード （259 ページ）
- このリリースへの Nexus Dashboard 4.x クラスタのアップグレード （279 ページ）
- DCNM から ND への移行 （289 ページ）
- NDB から ND への移行 （291 ページ）



第 10 章

Nexus Dashboard 3.2.2m クラスタのこのリリースへのアップグレード

（注） この章の手順は、 Nexus Dashboard リリース **3.2.2m** から Nexus Dashboard リリース 4.3.1 にアップグレードする場合に適用されます。

Nexus Dashboard リリース **4.x** から Nexus Dashboard リリース 4.3.1 にアップグレードする場合は、このリリースへの Nexus Dashboard 4.x クラスタのアップグレード （279 ページ） に記載されているアップグレード手順に従ってください。

- 既存の Nexus Dashbaord クラスターをアップグレードするための前提条件と注意事項 （259 ページ）
- (オプション)別々の NDFC および NDI クラスタを単一の共同ホストNexus Dashboardクラスターに変換する （265 ページ）
- サポートされているアップグレード パス （266 ページ）
- Nexus Dashboard のアップグレード （268 ページ）
- アップグレード後の情報とタスク （272 ページ）
- アップグレードのトラブルシューティング （278 ページ）

既存の Nexus Dashbaord クラスターをアップグレードするための前提条件と注意事項

既存のNexusダッシュボードクラスタをアップグレードする前に、次の手順を実行します。

- アップグレードに影響する可能性のある動作、ガイドライン、および問題の変更については、ターゲット リリースのリリース ノートを必ずお読みください。
- Nexus Dashboard リリース 4.3.1 にアップグレードする前に、次の手順を実行します：
  - NTPとDNSサービスが設定されていることを確認します。システムを正常にアップグレードするには、少なくとも 1 つの NTP と DNS が必要です。

- LAN デプロイメントは、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ことを確認する必要があります。管理ネットワークとデータ ネットワークが異なるサブネットに存在する場合にアップグレードは失敗します。

  この制限は、 SAN 展開には適用されないことに注意してください（SAN 展開では、管理ネットワークとデータ ネットワークが同じサブネットに存在する可能性があります）。

- `acs クラスタ`が健全であることを検証します。

  1. `ssh -l rescue-user [management-ip-of-nd]` を使用してNexusダッシュボードにアクセスします。
  2. `acs health` コマンドを発行します。

  `acs health` コマンドからの出力には、すべてのコンポーネントが正常であることが表示されるはずです。

```
rescue-user@node1:~$ acs health
======
Status
======
All components are healthy
```

- バックアップと復元のプロセスがアップグレードにどのように影響するかについて、次の重要な注意事項を確認します。
  - アップグレードする前に Nexus Dashboard クラスターのバックアップを実行し、バックアップファイルを安全な場所に保存してください。バックアップを実行するためには、「*Nexus Dashboard* とサービスの統合バックアップおよび復元」 を参照してください。このバックアップを、4.3.1 リリースを実行している Nexus Dashboard クラスタに直接復元することはできないことに注意してください。
  - 最新のバックアップに障害が発生していた場合、アップグレードは続行されません。アップグレードを進める前に、正常なバックアップがあることを確認してください。バックアップを正常に実行できず、アップグレードできない場合は、 Cisco Technical Assistance Center （TAC） （TAC） に連絡してサポートを受けてください。
  - 復元が失敗した場合、アップグレードを実行することはできません。復元が完了したら、 **[履歴の表示（View History）]** をクリックして、 **[バックアップと復元（Backup and Restore）]** ページの **[履歴（History）]** エリアに移動します。これについては、「*Nexus Dashboard* とサービスの統合バックアップと復元」の「Nexus Dashboard 構成の復元」セクションで説明されています。

    ページの **[ステータス（Status）]** 列には、復元プロセスの **[成功（Success）]** が表示されます。 **[ステータス（Status）]** 列に **[成功（Success）]** 以外の値が表示された場合は、クラスタを再展開し、復元プロセスが **[成功（Success）]** となることを確認してから、アップグレードを再度試行してください。

- **管理** > **証明書管理** > **ファブリック証明書** で **NX- API 証明書検証の有効化** フィールドを有効にしていて、 Nexus Dashboard リリース 3.2.2m から 4.3.1 にアップグレードする場合、これらの証明書はアップグレード後に失われる可能性があります。
- Nexus Dashboard リリース 4.3.1 以降、1.5TB ディスク クラスタ タイプのアプリケーション ノードは、グリーンフィールド デプロイメントとしてサポートされなくなりました。
- NDI がリモートで作成された NDFC クラスタに対してテレメトリを実行する場合、あるいは複数の Nexus Dashboard クラスタにまたがるマルチクラスタ接続を使用している場合は、すべてのクラスタをリリース4.3.1にアップグレードしてください。マルチクラスタ接続でリリース 3.2x と 4.3.1 クラスタを混在させて実行しないでください。同じ場所にある NDI および NDFC クラスタもリリース 4.3.1 にアップグレードします。新しい Connected TAC 機能を使用するには、両方のクラスタでリリース 4.3.1 を実行する必要があります。
- 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。
- 仮想 Nexus Dashboard クラスタをアップグレードする場合、 Nexus Dashboard はこれらのチェックを適用します。
  - HDD の遅延をチェックして 30ms 未満であることのチェック。HDD の遅延がさらに高い場合、アップグレードは失敗します。
  - ネットワーク遅延のチェックで、クラスタ ノード内で 50 ミリ秒未満であることを確認します。ネットワークの遅延がさらに高い場合、アップグレードは失敗します。
- VMware ESX に展開された仮想 Nexus Dashboard クラスタをアップグレードする場合は、ESX のバージョンがターゲット リリースで引き続きサポートされていることを確認します。

  このリリースは、VMware ESXi 7.0、7.0.1、7.0.2、7.0.3、8.0、8.0.2、8.0.3 をサポートしています。

（注） ESX サーバーをアップグレードする必要がある場合は、Nexus Dashboard をターゲット リリースにアップグレードする前に行う必要があります。ESX のアップグレードはこのドキュメントの範囲外ですが、簡単に説明すると次のとおりです。

1. 既存の Nexus Dashboard ノード VM を実行している場合に通常行うように、ESX ホストの 1 つをアップグレードします。
2. ホストがアップグレードされた後、Nexus Dashboard クラスタが正常に動作していることを確認します。
3. 他の ESX ホストで 1 つずつアップグレードを繰り返します。
4. すべての ESX ホストがアップグレードされ、既存の Nexus Dashboard クラスタが正常な状態になったら、このドキュメントの説明に従って、Nexus Dashboard をターゲット リリースにアップグレードします。

- 現在の Nexus ダッシュボードクラスタが正常であることを確認します。

  Nexus ダッシュボードの**管理コンソール（Admin Console）**の **[概要（Overview）]** ページでシステムのステータスを確認するか、`rescue-user` としてノードの1つにログインし、`acs health` コマンドを実行して `All components are healthy` が返ってくることを確認します。

- Nexus Dashboard ではプラットフォームのダウングレードはサポートされていません。

  以前のリリースにダウングレードするには、新しいクラスタを展開する必要があります。

- Nexus Dashboard リリース 3.2.x で `ダッシュボード ユーザー` （app-user）ユーザー ロールのみを持っているユーザーがいる場合は、 Nexus Dashboard リリース 4.3.1 へのアップグレード後に `ダッシュボード ユーザー` ロールを持つユーザーで削除するか、Nexus Dashboard リリース 4.3.1 のユーザーの代わりに`Observer` ロールを使用する必要があります。

- 永続 IP アドレスの数とそれらのマッピング方法は、以前のリリースから Nexus Dashboard リリース 4.3.1 で変更されました。Nexus Dashboardの 永続 IP アドレス （52 ページ） を参照して、以前のリリースで必要だった永続的な IP アドレスの数と、Nexus Dashboard リリース 4.3.1 にアップグレードする前に必要な永続的な IP アドレスの数で特定の更新を行う必要がある永続的な IP アドレスの数を理解してください。

- サービスを提供する任意のペルソナ、特にNexus Dashboard Fabric Controller（NDFC）と Nexus Dashboard Insights（NDI）のNexus Dashboard（NDI）があり、以前のリリース（ND 2.2.x 以下など）から ND 3.2.2m にアップグレードしている場合、Elasticsearch（ES）インデックスサイズに関する次の重要な情報に注意してください。

  クラスターが ND 2.2.x 以前に展開され、それ以降にアップグレードされた場合、ND 3.2.2m から ND 4.3.1 へのアップグレードにより、時系列データベースのインデックスが作成されている可能性があります。このプロセスでは、サイズがこのクラスターの再インデックス

化機能のサイズを超えている場合は、Cisco Technical Assistance Center （TAC） に連絡するように求められます。プロセスが再インデックス化できない場合、UI で提供された`acs recover` コマンドを使用して、失敗後にアップグレードを続行できます。

- 同じまたは、異なるデータ サブネットを使用して展開した ND リリース 4.3.1 より前のクラスタの一部として Nexus Dashboard Orchestrator を使用している場合は、Nexus Dashboard リリース 4.3.1 にアップグレードする前に、
  - 永続 IP アドレスを追加する必要があります。Nexus Dashboardの 永続 IP アドレス （52 ページ）を参照してください。
  - さらに、ND リリース 4.3.1 より前のクラスタ ノードが異なるデータ サブネットを使用する場合、すべてのノードに BGP 構成も追加する必要があります。

  アップグレード前にこれらの項目を設定していないと、アップグレード中のイメージの検証は失敗します。
- Nexus Dashboard リリース 4.1x では、 Nexus Dashboard リリース 3.1x または 3.2x では使用できなかった **アクセス** スイッチ ロールが導入されました。
  - **3.x の動作**：テレメトリ エクスポータがループバックをソース インターフェイスとして使用する
  - **4.x の動作**：テレメトリ エクスポータが SVI をソース インターフェイスとして使用する

  この変更は、アップグレード後に自動的にトリガされます。

  フロー テレメトリ エクスポータは、一度作成されたソース インターフェイスの変更を受け入れることができません。これを変更しようとすると（ループバックから SVI）、スイッチでは失敗します。

  Nexus Dashboard リリース 3.1x または 3.2x から 4.x にアップグレードする場合、フロー テレメトリ構成の再展開は、ソース インターフェイスの不一致（ループバック - SVI）が原因で失敗する場合があります。

アップグレード時の設定のばらつきの自動調整

4.2.（1）より前の NDO リリースから ND リリース 4.3.1 にアップグレードする場合は、マルチステップ アップグレードを実行する必要があります。

1. 最初に 4.2（1）より前の NDO リリースを ND 3.0.1i にアップグレードしてから、『*Cisco Nexus Dashboard and Services Deployment and Upgrade Guide, Release 3.2.x*』の 「Supported Upgrade Paths」 の項の説明に従って、ND リリース 3.2.2m にアップグレードします。
2. 次に、この章の説明に従って、ND リリース 3.2.2m から ND リリース 4.3.1 にアップグレードします。

4.2（1）より前の NDO リリースを ND リリース 3.2.2m にアップグレードすると、アプリケーション テンプレートの構成のばらつきが観察される場合があります。これらのばらつきは、

NDO リリース 4.2(1) 以降で、以前のバージョンで管理されていなかった新しいアプリケーション テンプレート オブジェクト プロパティの管理がサポートされているために発生します。NDO 4.2(1) によって管理される新しいプロパティのリストについては、 Nexus Dashboard Orchestrator 4.2(1) リリース ノートを参照してください。

ND リリース 4.3.1 は、アップグレード プロセスの一環として構成のばらつきの自動調整をサポートしています。Nexus Dashboard は、テンプレートがファブリックと同期しているかどうかをチェックし、必要に応じて、ファブリック値を Nexus Dashboard にインポートして、ばらつきを自動的に解決します。

4.2（1）より前の NDO バージョンからマルチステップのアップグレード パスに従う場合は、ND リリース 3.2.2m で検出されたばらつきを無視して、ND リリース 4.3.1 へのアップグレードを続行することをお勧めします。

ND リリース 4.3.1 へのアップグレード後に残ったばらつきは、手動で解決する必要があります。たとえば、構成されたオブジェクトが複数のファブリックにまたがる拡張テンプレートの一部であり、テンプレートレベルのプロパティに異なるファブリックで構成された異なる値がある場合、自動解決できないばらつきが発生します。

（オプション）6 ノード pND クラスタから 3 ノード pND クラスタへの変換

アップグレード プロセスの一部として 6ノードの pND クラスタを 3 ノードのPND に変換する場合（たとえば、 Nexus Dashboard リリース 3.2.2m で 6ノードのpND コントローラ を展開ている場合、Nexus Dashboard リリース 4.1.1 ではサポートされていません）、 Nexus Dashboard リリース 4.1.1 にアップグレードする前に、次の手順を使用して Nexus Dashboard リリース 3.2.2m でこの変換を行ってください。

Nexus Dashboard リリース 4.1.1 では 6ノードの pND **テレメトリ**のみの展開がサポートされているため、このオプションの手順はこの場合は必要ありません。

1. Nexus Dashboard リリース 3.2.2m で 6ノード pND クラスタのバックアップを実行します。

   詳細については、「*Nexus Dashboard* とサービスの統合バックアップと復元」の記事を参照してください。

2. 既存のプライマリ ノードとクラスタが正常であることを確認し、1 つずつセカンダリ ノードを削除します。

   1. リリース 3.2.2m で実行されている Nexus Dashboard で、**[ノード (Nodes）] > [管理（Manage)]** に移動します。
   2. 削除するセカンダリ ノードをオンにします。
   3. **[アクション（Actions）]** メニューから **[削除（Delete）]** を選択してノードを削除します。
   4. **[概要（Overview）] > [プラットフォーム（Platform）] ビュー** に移動し、各セカンダリノードが削除された後、クラスターの正常性ステータスが **[GREEN]** と表示されるまで待ちます。または、acs health コマンドを実行して、クラスタの正常性を確認します。クラスタの状態が正常になるまで、別のセカンダリ ノードを削除しないでください。

（注） ノードを削除後、Kafka が安定するまでに最大 30 分かかる場合があります。

5. セカンダリノードを削除した後にクラスターの正常性ステータスが **GREEN** と表示されたら、次のセカンダリノードの削除に進みます。

   各セカンダリノードを1 つずつ削除するプロセスを続行し、クラスターのステータスが **GREEN** になるのを待ってから、次のセカンダリノードの削除に進みます。

3. すべてのセカンダリノードを削除したら、クラスタが正常であることを確認してから、Nexus Dashboard リリース 3.2.2m で新しいバックアップを実行します。

   詳細については、「*Nexus Dashboard* とサービスの統合バックアップと復元」の記事を参照してください。

4. この章の手順に従って、クラスタを Nexus Dashboard リリース 3.2.2m からリリース 4.3.1 にアップグレードします。

(オプション)別々の NDFC および NDI クラスタを単一の共同ホストNexus Dashboardクラスターに変換する

Nexus Dashboard リリース 3.x の個別の NDFC および NDI クラスタを、アップグレード プロセスの一環としてリリース 4.x の単一の共存型 Nexus Dashboard クラスタに変換する場合は、アップグレード前に以下の手順を実行してください。

たとえば、NDFC を実行している 5 ノード vND クラスタと、 Nexus Dashboard リリース 3.2.2m で NDI を実行している別の 6 ノード vND クラスタがあり、それらを単一の Nexus Dashboard リリース 4.xクラスタにマージする場合、アップグレード前の Nexus Dashboard リリース 3.2.2m の変換手順。

手順

ステップ 1 NDIクラスターで、テレメトリを完全に無効にします。

a) NDIクラスターから NDFC ファブリックを削除します。

b) NDFC および NDI クラスタがフェデレーションされている場合(マルチクラスタ接続を介して接続されている)、クラスタを切断してフェデレーション構成を削除します。

詳細については、*Nexus Dashboard Infrastructure Management*、リリース *3.2.x*を参照してください。

ステップ 2 この章の手順に従って、NDFC を実行している Nexus Dashboard クラスタのみをリリース 3.2.2m からリリース4.x にアップグレードしてください。

ステップ 3 アップグレードが完了したら、すべての NDFC 機能が期待どおりに動作していることを確認します。

ステップ 4 アップグレードした Nexus Dashboard リリース 4.x クラスタのバックアップを実行します。

詳細については、「*Nexus Dashboard* のバックアップと復元」を参照してください。

ステップ 5 ファブリック設定からテレメトリを有効にします。

a) 3 ノード以上の pND クラスタの場合、NDFC アップグレードを確認した後、ファブリック設定から直接テレメトリを有効にします。

b) アップグレードされたデプロイメントが 3 ノード vND アプリケーション クラスタの場合は、新しい 3 ノード データ vND または 6 ノード vND（3 データ + 3 アプリ）クラスタ、または 3 または 6 の pNDクラスタを作成してから、前の手順で作成した Nexus Dashboard リリース 4.x バックアップを復元します。

c) 復元が完了したら、すべての NDFC 機能と特徴を確認し、ファブリック設定からテレメトリを有効にします。

（注） この変換の一環として、別の NDIクラスタを Nexus Dashboard リリース 4.x にアップグレードしないでください。テレメトリは、共同ホストされる展開の準備ができたら、アップグレードした NDFC クラスタから再度有効にする必要があります。

サポートされているアップグレード パス

以前のリリースでは、Nexus Dashboard の展開の概要 （5 ページ） で説明したとおり、Nexus Dashboard にはプラットフォーム ソフトウェアのみが付属しており、サービスは含まれていませんでした。これらのサービスは、最初のプラットフォームの展開後に個別にダウンロード、インストール、および有効化するようになっていました。加えて、Nexus Dashboard リリース 3.1.1では、Nexus Dashboard と個々のサービス間のより緊密な結合を実現したため、各サービスの単一バージョンのみがプラットフォームの各バージョンと互換性を持つようになりました。その結果、Nexus Dashboard ソフトウェアの必要最小限のバージョンを使用している限り、プラットフォームと現在有効になっているすべてのサービスの両方を Nexus Dashboard リリース 3.1x と 3.2x に直接アップグレードできるようになっていました。

Nexus Dashboard リリース 4.1.1 以降、今では、プラットフォームと個々のサービスが単一の製品に統合されました。つまり、サービスを個別に展開、構成、またはアップグレードする必要がなくなりました。

次の表に、特定の展開の組み合わせに関するシナリオの例をいくつか示します。

表 *28* :

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
4.2.1	N/A	このリリースへの Nexus Dashboard 4.x クラスタのアップグレード（279 ページ） の説明に従って、リリース 4.3.1 に直接アップグレードします。
4.1.1	該当なし	このリリースへの Nexus Dashboard 4.x クラスタのアップグレード（279 ページ） の説明に従って、リリース 4.3.1 に直接アップグレードします。
3.2.2m	ファブリック コントローラ：12.2(3) Orchestrator：4.4(2) Insights：6.5(2)	次のセクションの説明に従って、リリース 4.3.1 に直接アップグレードします。 リリース 4.3.1 では、すべてのサービスが単一の Nexus Dashboard 製品に統合されています。
3.2.1	ファブリック コントローラ：12.2(2) Orchestrator：4.4(1) Insights：6.5(1)	**1.** 『*Nexus Dashboard* 展開ガイド、リリース *3.2.x*』の説明に従って、Nexus Dashboard プラットフォームをリリース 3.2.2m にアップグレードします。 すべてのサービスは、プラットフォームとともに自動的にアップグレードされます。 **2.** 以下のセクションで説明されているように、リリース 3.2.2m からリリース 4.3.1 にアップグレードします。 リリース 4.3.1 では、すべてのサービスが単一の Nexus Dashboard 製品に統合されています。
3.1.1	ファブリックコントローラ：12.2(1) Orchestrator：4.3(x) Insights：6.4(1)	**1.** 『*Nexus Dashboard* 展開ガイド、リリース *3.2.x*』の説明に従って、Nexus Dashboard プラットフォームをリリース 3.2.2m にアップグレードします。 すべてのサービスは、プラットフォームとともに自動的にアップグレードされます。 **2.** 以下のセクションで説明されているように、リリース 3.2.2m からリリース 4.3.1 にアップグレードします。 リリース 4.3.1 では、すべてのサービスが単一の Nexus Dashboard 製品に統合されています。

現在の Nexus Dashboard リリース	互換性のあるサービス （フォームファクタとクラスタサイズによっては、これらのサービスの 1 つ以上が現在有効になっている場合があります）	アップグレードのワークフロー
3.0.1	ファブリック コントローラ：12.1(3) Orchestrator：4.2(x) Insights：6.3(1)	1. 『*Nexus Dashboard* 展開ガイド、リリース *3.2.x*』の説明に従って、Nexus Dashboard プラットフォームをリリース 3.2.2m にアップグレードします。 すべてのサービスは、プラットフォームとともに自動的にアップグレードされます。 2. 以下のセクションで説明されているように、リリース 3.2.2m からリリース 4.3.1 にアップグレードします。 リリース 4.3.1 では、すべてのサービスが単一の Nexus Dashboard 製品に統合されています。
2.3.2 以前	ファブリックコントローラ：12.1(2) 以前 Orchestrator：4.1(x) 以前 Insights：6.2(x) 以前	1. 『*Nexus Dashboard* 展開ガイド、リリース *3.1.x*』の説明に従って、Nexus Dashboard プラットフォームをリリース 3.1.1 にアップグレードします。 すべてのサービスは、プラットフォームとともに自動的にアップグレードされます。 2. 『*Nexus Dashboard* 展開ガイド、リリース *3.2.x*』の説明に従って、リリース 3.1.1 からリリース 3.2.2m にアップグレードします。 すべてのサービスは、プラットフォームとともに自動的にアップグレードされます。 3. 以下のセクションで説明されているように、リリース 3.2.2m からリリース 4.3.1 にアップグレードします。 リリース 4.3.1 では、すべてのサービスが単一の Nexus Dashboard 製品に統合されています。

Nexus Dashboard のアップグレード

ここでは、Nexus Dashboard リリース 3.2.2m からNexus Dashboard リリース 4.3.1 にアップグレードする場合に、既存の Nexus Dashboard 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） Nexus Dashboard リリース 4.x からNexus Dashboard リリース 4.3.1 にアップグレードする場合は、このリリースへの Nexus Dashboard 4.x クラスタのアップグレード （279 ページ） のアップグレード手順に従ってください。

サポートされているアップグレードパス （266 ページ） で説明しているとおり、Nexus Dashboard リリース 4.3.1 に直接アップグレードするには、 Nexus Dashboard リリース 3.2.2m を実行している必要があります。これらのリリースでは、次の重要な点に注意してください。

- **Nexus Dashboard リリース 3.2.x**：Nexus Dashboard の展開の概要 （5 ページ） で説明したとおり、これらのNexus Dashboard リリースでは、 Nexus Dashboard は 1 つの製品として利用でき、個々のサービス（ Nexus Dashboard Insights、Orchestrator、Fabric Controller など）はNexus Dashboard とは別の個別の製品として利用できました。
- **Nexus Dashboard リリース 4.1.1**：これは、Nexus Dashboard と上記の個々のサービスが単一の統合製品としてパッケージ化された最初の Nexus Dashboard リリースです。Nexus Dashboard リリース 4.3.1 は、4.1.1 リリースに続くの統合型 Nexus Dashboard リリースの 1 つです。

つまり、アップグレードプロセスは次の段階を経ます：

1. Nexus Dashboard リリース 3.2.2m でアップグレード プロセスを開始します。ここでは、Nexus Dashboard と個々のサービスは別の製品です。
2. 次に、 Nexus Dashboard 4.3.1 にアップグレードします。これで、 Nexus Dashboard と個々のサービスがパッケージ化された単一の統合製品としてアップグレードプロセスを完了します。

始める前に

で説明している前提条件をすべて満たしていることを確認します。 既存の Nexus Dashbaord クラスターをアップグレードするための前提条件と注意事項 （259 ページ）

手順

ステップ 1 Nexus Dashboard リリース 3.2.2m システムで、 Nexus Dashboard 4.3.1 イメージをダウンロードします。

a) [ソフトウェア ダウンロード（Software Download）] ページを参照します。

https://software.cisco.com/download/home/286327743/type/286328258/release/4.3.1

b) 左側のサイドバーから、ダウンロードする Nexus Dashboard 4.3.1 のリリース バージョンを選択します。

c) ターゲットとする 4.3.1 リリース用の Nexus Dashboard イメージをダウンロードします。

（注）
- アップグレードプロセスは、すべての Nexus ダッシュボード フォーム ファクタで同じで、Nexus ダッシュボード ISO イメージ（`nd-dk9.<version>.iso`）を使用します。言い換えると、最初の展開で仮想フォーム ファクターを使用していた場合（ESX での展開のための `.ova` イメージなど）やクラウド プロバイダーのマーケット プレースを使用していた場合であっても、アップグレードでは `.iso` イメージを使用する必要があります。
- イメージのダウンロードが完全に失敗した場合は、Nexus Dashboard とイメージ サーバ間のネットワーク接続を確認します。**[管理（Admin）]**>**[システム設定（System Settings）]**>**[一般（General）]**>**[プロキシ構成（Proxy configuration）]** でプロキシ構成を確認します。

d) （オプション）環境内のWebサーバでイメージをホストします。

（注） 環境内のサーバーでイメージをホストすることをお勧めします。イメージを Nexus Dashboard クラスタにアップロードする場合、イメージに直接 URL を指定するオプションがあります。そうすれば、プロセスは相当高速化されます。

ステップ 2 現在の Nexus ダッシュボードの**管理コンソール**に管理者ユーザーとしてログインします。

ステップ 3 クラスタから古く、アクティブでないアップグレード イメージを削除します。

クラスタを初めてアップグレードする場合は、この手順をスキップできます。

a) **[管理（Manager）]** > **[ソフトウェア管理（Site Software Management）]**に移動します。
b) アップグレードイメージのタイルのゴミ箱アイコンをクリックして、古い非アクティブなアップグレード**イメージ**を削除します。
c) すべての古いアップグレード イメージについて、この手順を繰り返します。

ステップ 4 新しいイメージをクラスタにアップロードします。

a) **[管理（Manager）]** > **[ソフトウェア管理（Site Software Management）]**に移動します。
b) [Add Image] をクリックします。
c) **[ソフトウェアイメージの追加（Add Software Image）]** ウィンドウで、イメージがウェブ サーバーの **[リモート（Remote）]** であるか、マシン上での **[ローカル（Local）]** であるかを選択します。

どちらの場合も、イメージは `.iso` で終わるファイルです。

- **リモート**：最初の手順でダウンロードしたイメージの **URL** を入力します。
- **ローカル**：**[ファイルの選択]** をクリックして、イメージをダウンロードしたローカルフォルダに移動します。

d) **[追加（Image）]** をクリックして、 イメージを追加します。

次に、 Nexus Dashboard はアップグレード イメージをダウンロードしてイメージの処理を開始し、いくつかの準備と検証の段階を経て、アップグレードが正常に行われるようにします。終了するまでに数分かかる場合があります。

（注） アップグレードのトラブルシューティング（278ページ）を参照してください。ここには、アップグレードのこの時点で行われる検証のチェックと、問題が生じた場合の対処方法が記されています。

e) 検証が完了すると、**[ソフトウェア管理（Software Management）]** ページのカードに **[インストール（Install）]** ボタンが表示されます。**[インストール（Install）]** をクリックしてソフトウェアをインストールし、アップグレード プロセスを実行します。

インストールの進行状況ウィンドウが表示されます。更新中は、この画面から移動できます。

クラスター内のノードの数によっては、この手順に60分以上かかる場合があります。その間、ノードが再起動し、 GUIにアクセスできなくなります。Nexus Dashboard は、いくつかの段階を経て次の手順を経ます。

- リリース ファームウェアのインストール
- サービスの無効化
- インフラストラクチャ サービスのシャットダウン
- プラットフォーム サービスのアップデート
- インフラストラクチャ サービスの有効化
- サービスの有効化

[詳細（Details）] リンクをクリックして、アップグレードの進行状況とさまざまな段階を確認できます。

（注） アップグレードプロセス中に問題が発生した場合（インデックスの問題の可能性など）は既存の Nexus Dashbaord クラスターをアップグレードするための前提条件と注意事項（259ページ）を参照してください。

上記のプロセスが完了したら、 Nexus Dashboard 4.3.1 にアップグレードできているはずです。Nexus Dashboard と個々のサービスが単一の統合製品としてパッケージ化されています。

（注） 展開したクラスター形式とクラスター ノードの数によっては、特定の機能（コントローラ、オーケストレータ、テレメトリなど）が使用できない場合があります。 Nexusダッシュボード キャパシティ プランニング ツール の情報を確認して、クラスターインストールで使用できる機能を確認します。

ステップ 5 ノードのアップグレードタスクが完了したら、ノードが正常であり、UIにログインできることを確認します。

アップグレードプロセスが完了すると、通常どおりに Nexus Dashboard ダッシュボード UI を表示できます。

[概要（Overview）] ページでシステム全体の正常性を確認し、**[管理（Admin）]** > **[システム ソフトウェア（System Software）]** ページで現在の実行中バージョンを確認できます。

ステップ 6 DNS のクラスタ名の変更を確認します。

Nexus Dashboard リリース 4.3.1 以降、新規インストールとアップグレードの場合、クラスター DNS は `nd-cluster.case.local` にハードコードされます。以前のリリースから Nexus Dashboard リリース 4.3.1 にアップグレードすると、クラスタ名に基づいて表示される DNS ドメイン名がアップグレード後に変更され、その DNS ドメイン内のクラスタ名ではなく固定クラスタ名（`nd-cluster.case.local`）が表示されます。

次のタスク

必要なアップグレード後のタスクの実行のために、アップグレード後の情報とタスク （272ページ）に進んでください。

アップグレード後の情報とタスク

このセクションでは、 Nexus Dashboard リリース 3.2.2m からNexus Dashboard 4.3.1 にアップグレードした後に完了する必要がある変更とタスクに関する情報を示します。

- マルチクラスタ接続のアップグレード後のタスクの実行 （272 ページ）
- スイッチのファームウェア イメージの再アップロード （273 ページ）
- 異常の問題に対処する （273 ページ）
- デバイスのログイン情報の設定 （273 ページ）
- 古いクラスタータイプを新しい3ノード仮想クラスター（データ）クラスタータイプに移行する （274 ページ）
- テレメトリ構成の再展開 （275 ページ）
- SNMP 関連のタスク （277 ページ）
- ACI ファブリックの再登録 （277 ページ）
- Performance Manager（PM）の履歴データを表示する （278 ページ）
- システム更新通知の表示 （278 ページ）

マルチクラスタ接続のアップグレード後のタスクの実行

4.3.1 より前のこれらの設定のいずれかを設定してた場合。Nexus Dashboard：

- Nexus Dashboard Insights がリモートで作成した NDFC ファブリックをオンボーディングしていた場合
- One Manage を使用して複数の NDFC または NDI クラスタを管理および監視していた場合
- 複数の NDFC クラスタを持つマルチクラスタ ファブリック グループがある場合

これらのクラスタが以前のリリースでマルチクラスタ接続を使用してすでに接続されていた場合は、プライマリクラスターで、Nexus Dashboard リリース 4.3.1 にアップグレードしたすべてのクラスタを再登録する必要があります。

さらに、以前のリリースで NDI および NDO の統合があった場合、Nexus Dashboard リリース 4.3.1 ではサポートされません。NDO 統合を活用するには、 Nexus Dashboard リリース 4.3.1 で NDI および NDO クラスタをフェデレートする必要があります。

Nexus Dashboard リリース 3.2.2m システムでマルチクラスタ接続が設定されている場合は、アップグレードが完了した後に、マルチクラスタ接続を再度有効にする必要があります。このタスクは、コロケーション環境に NX- OSファブリックがある場合にのみ適用されます。詳細については、 クラスタの接続 を参照してください。

スイッチのファームウェア イメージの再アップロード

リリース 3.2.2m で Nexus Dashboard にアップロードされたスイッチのファームウェア イメージは、 Nexus Dashboard 4.3.1 にアップグレードするときに引き継がれません。Nexus Dashboard 4.3.1 にアップグレードした後、それらのスイッチのファームウェアイメージを再アップロードしてください。

1. **[管理（Manage）]** > **[ファブリック ソフトウェア（Fabric Software）]** > **[NX-OS/IOS-XE]** > **[イメージ（Images）]** に移動します。
2. **[アクション（Actions）]** ドロップダウンリストから **[アップロード（Upload）]** を選択し、必要なスイッチファームウェアイメージを再アップロードします。

詳細については、 ファブリックソフトウェアの管理を 参照してください。

異常の問題に対処する

アップグレードが完了したら、**[異常（Anomalies）]** 領域で問題がないかを確認し、一部の NX OSファブリックで **再計算と展開を** 完了するための要求を確認します。

デバイスのログイン情報の設定

Nexus Dashboard リリース 3.2.2m システムで共同ホストされた NX- OS ファブリックを構成していた場合は、次の手順に従って、 Nexus Dashboard リリース 4.3.1 にアップグレードした後に適切なデバイスのログイン情報が構成されていることを確認します。

1. アップグレードされたNexus Dashboard 4.3.1 システムで、**[管理（Manage）]** > **[デバイス ログイン情報（Device Credentials）]** に移動します。
2. **[デバイス ログイン情報（Device Credentials）]** エリアに表示される情報を確認します。

[デバイス ログイン情報（Device Credentials）] エリアに赤色のテキストで **[設定なし（Not Set）]** が表示されます。

3. **[デバイス ログイン情報（Device Credentials）]** エリアで、**[設定（Set）]** をクリックします。
4. **[デフォルト ログイン情報の設定（Set Default Credentials）]** ページで、必要な情報を入力します。
   - [ユーザー名（Username）]、[パスワード（password）]、および [パスワードの確認（Confirm password）]：必要なユーザー名とパスワードの情報を入力します。
   - 必要に応じて、**[Robot（ロボット）]** ログイン情報を設定するチェックボックスをオンにします。

   次に **[保存（Save）]** をクリックします。

   [デフォルトのログイン情報の設定（Set Default Credentials）] ページに戻り、テキスト **Default Set**が青色で表示されます。

古いクラスタータイプを新しい3ノード仮想クラスター（データ）クラスタータイプに移行する

- 4.3.1 より前のこれらのクラスタは、 Nexus Dashboard リリース 4.3.1 でのグリーンフィールド展開としてはサポートされていませんが、リリース 4.3.1 にアップグレードする場合は次がサポートされます：
  - 3 ノード仮想クラスター（1.5 TB ストレージのアプリ ノード）
  - 5 ノード仮想クラスタ（1.5 TB ストレージのアプリ ノード）
- 5 ノード リモート対応クラスタ（アプリ 500G）クラスタ タイプは、 Nexus Dashboard リリース4.3.1 でのグリーンフィールドデプロイメントとしてはサポートされていませんが、リリース 4.3.1にアップグレードする場合はサポートされます。ただし、このクラスタ タイプは次のリリースでアップグレードオプションとしてサポートされないため、次の手順を使用して新しいクラスタ タイプの 3 ノードのリモート対応クラスタ（データ） または 3 ノードの物理クラスタに移行する必要があります。

これらの古いクラスタ タイプから新しいクラスタ タイプ 3 つのノードのリモート対応クラスタ（データ）または、3 つのノードの物理クラスタに移行する場合は、次の手順を使用して新しいクラスタ タイプに移行できます。

1. この章で説明されている手順を使用して、古いクラスタ タイプをそのままにして、 Nexus Dashboard リリース 4.3.1 にアップグレードします。
2. Nexus Dashboardリリース 4.3.1 にアップグレードしたら、古いクラスター タイプのバックアップを実行します。

   詳細については、「*Nexus Dashboard* のバックアップと復元」を参照してください。

- 以前のクラスタータイプをバックアップする場合は、 **構成のみ** または **完全** バックアップのオプションを使用できます。
- 続行する前に、古いクラスターからバックアップを正常に取得したことを確認します。

3. 古いクラスター タイプのクラスターをシャットダウンします。
4. 新しいクラスター タイプ `3 node virtual cluster (data)` のグリーンフィールドの展開を実行します。
   - 新しいクラスターで古いクラスターの名前を再利用します。
   - 仮想データクラスターまたは物理クラスターを展開できます。
   - 古いクラスタータイプのIPアドレスを再利用することも、 *Nexus Dashboard* のバックアップと復元 で説明されているように、 **[外部サービスの IP 設定を無視する（Ignore External Service IP Configuration）]**チェックボックスをオンにして、新しいクラスターで新しいIPアドレスを使用して復元することもできます。
5. 古い `3 つのノードのリモート対応クラスタ（アプリ）` または `5 つのノードのリモート対応クラスタ（アプリ）` のバックアップを新しい `3 つのノードのリモート対応クラスタ（データ）` または、3 つのノードの物理クラスタに復元します。

   詳細については、「*Nexus Dashboard* のバックアップと復元」を参照してください。

テレメトリ構成の再展開

Nexus Dashboard リリース 4.3.1 にアップグレードすると、NX- OS ファブリックからのソフトウェア テレメトリ ストリーミングを処理するための永続 IP アドレスが変更されます。Nexus Dashboard 4.3.1 へのアップグレード後にテレメトリ操作を再開するには、テレメトリ設定を再展開する必要があります。

1. **[システムのステータス（System Status）]** ページに移動します。

   Admin > **System Status**
2. **[Telemetry]** をクリックし、 **[Telemetry Status]** エリアの **[Fabrics]** タブをクリックします。
3. **ファブリック** テーブルに表示されている情報を確認します。

   NX- OSファブリックの場合、[ファブリック（Fabrics）] テーブルにリストされている 1 つ以上のファブリックで、アップグレード前は **[テレメトリ構成ステータス（Telemetry config status）]** 列に **[保留中の更新（Pending updates）]** のステータスが表示されていることに **注意** してください。

   この状態では、テレメトリ ストリーミングが機能せず、個々の機能のステータス（ソフトウェアテレメトリ、フローコレクション、スイッチ ステータスなど）が無効になるため、無視する必要があります。

（注） **[ファブリック（Fabrics）]** テーブル内の一部のファブリックでは、**[テレメトリ構成ステータス（Telemetry config status）]** 列に [**OK]** のステータスが表示され、その他のファブリックのステータスが **[保留中の更新（Pending updates）]**と表示される場合があります。 **[テレメトリステータス（Telemetry status）]** エリアの [**スイッチ（Switches）]** タブをクリックした場合、テレメトリ列に誤った緑色の **[OK]** または **[成功（Success）**] ステータス エントリを **持つ** スイッチが表示される場合があります。これらのスイッチは **、[ファブリック（Fabrics）]** テーブルに表示されます。これは、これらのファブリックのスイッチ レベルで表示される誤ったステータス情報であり、無視する必要があります。

4. **[テレメトリ ステータス（Telemetry status）]** エリアで **[ファブリック（Fabrics）**] タブを選択した状態で、 **[テレメトリの再展開（Redeploy テレメトリ）]**をクリックします。

   確認ウィンドウで、**[確認（Confirm）]** をクリックします。

   [確認（Confirm）] をクリックすると、個々の機能のステータスが **[進行中で有効化（Enable in Progress）]**に変わり、累積的な **[Telemetry 設定ステータス（Telemetry Config Status）]** が**[進行中（In Progress）]**に更新されます。

5. **[確認（Confirm）]**をクリックすると、 **[システム（System）] [ステータス（Status）]** の下の **[テレメトリ（Telemetry）]** ページの **[ファブリック（Fabrics）]**タブに戻ります。ページの右上隅にある **[更新（Refresh）]** をクリックします。

   確認ページで **[確認（Confirm）]** をクリックした直後にテレメトリステータスが正しく表示されない場合がありますが、 **[更新（Refresh）]**をクリックすると正しいテレメトリステータスが に表示されます。

6. もう一度、**ファブリック** テーブルに表示されている情報を確認します。

   [更新（Refresh）] をクリックした後で、次のエリアのステータスが変化することがわかります。

   - 個々の機能のステータスは、**[進行中で有効化（Enable in Progress）]** に変更されます。
   - **[テレメトリ設定ステータス（Telemetry config status）]** 列のファブリックのステータスが、[更新の保留中 （**Pending updates**）] から **[進行中（In Progress）]**に変わります。数分後、ファブリックのステータスは、 **[テレメトリ設定ステータス（Telemetry config status）]**列で、自動的に、または**[更新（Refresh）]** を再度クリックした後に、**[OK]** に変わります。

操作が完了すると、個々の機能ステータスは次のようになります。

- `[Enabled]` これはすべてのスイッチで構成のプッシュが成功した場合です。
- `[Enabled Fail]` これはいずれかのスイッチで失敗した場合です。
- `[Enabled Pending]` これは変更制御モードが有効になっている場合です。この場合、**[管理（Manage）]** > **[制御を変更（Change control）]**を使用して変更管理チケットを明示的に

適用します。詳細については、「*Nexus Dashboard* での変更制御とロールバックの使用」を参照してください。

累積 **テレメトリ構成ステータス** は次のように表示されます。

- `OK` すべてのスイッチの構成が成功した場合です。
- `Not OK` 失敗した場合、またはすべてのスイッチの変更制御モードで保留中の場合です。
- `Partial OK` 一部のスイッチで成功し、失敗したか、他のスイッチで変更制御モードで保留中である場合です。

SNMP 関連のタスク

- **SNMP サーバー ユーザーの変更をを確認します**：Nexus Dashboard リリース 4.3.1 より前のリリースでは、次に示す例のように、インテントの一部としてパスワードなしで管理対象の NX-OS スイッチで構成された SNMP サーバー ユーザー：

  ```
  snmp-server user Demo_CMDv5 vdc-operator
  snmp-server user DemoOps_admin vdc-operator
  snmp-server user DemoOps_admin network-admin
  ```

  は、**再計算および展開** 操作中に差分に表示されませんでした。これらは、特にスイッチが TACACS+などのリモート認証方式に依存している環境では、気付かれないことがよくあります。

  Nexus Dashboard リリース 4.3.1 にアップグレードすると、これらの違いが正しく検出され、予想される差分として GUI に表示されるようになります。リリース 4.3.1へのアップグレード後、次のいずれかを行う必要があります：

  - これらの構成をプッシュしてスイッチを同期させるか、
  - これらの SNMP ユーザー エントリが不要になった場合は、インテントから削除します。

- **無効な SNMP 値を修正します**：Nexus Dashboard は、リリース 4.3.1 の SNMP リスナー IP と受信者の電子メール エントリを検証します。Nexus Dashboard リリース 4.3.1 にアップグレードする前に NDFC のこれら 2 つのフィールドに無効な値が設定されていた場合、このページの **転送されたアラーム データ フィールドの SNMP リスナー IP およびポート** に「`Input is not valid`」 エラーが表示される場合があります。

  [管理（Admin）] > [システム設定（System Settings）] > [ファブリック管理（Fabric management）] > [詳細設定（Advanced settings）] > [アラーム（Alarms）]

  このフィールドの無効なエントリを修正し、**[保存（Save）]** をクリックしてこの問題を解決します。

ACI ファブリックの再登録

リリース 6.1.4 より前のリリースで実行されている ACI ファブリックをオンボードしている場合は、クラスタを 3.x から 4.x にアップグレードした後に、「クラスタの再登録」で説明され

ているようにオンボードされた ACI ファブリックを ACI-Nexus Dashboard 相互起動機能を使用して再登録する必要があります。

Performance Manager（PM）の履歴データを表示する

Nexus Dashboard をリリース 3.2.2m からリリース 4.3.1 にアップグレードした後、ファブリックでテレメトリを有効にすると、Performance Manager（PM）の履歴データは表示されません。代わりに、システムはその時点から新たな PM データの収集を開始します。

過去の PM データを表示するには、影響を受けるファブリックでテレメトリを無効にします。古い PM データが再表示されます。

システム更新通知の表示

リリース 4.2.1 以降、 Nexus Dashboard は、新しい推奨ソフトウェア バージョンが利用可能になったときに通知する自動アラートを提供します。詳細については、 「*Nexus Dashboard* の探索 」の「システムの更新通知」セクションを参照してください。

アップグレードのトラブルシューティング

前のセクションで説明した、新しいイメージのアクティブ化段階で、すべてのノードが再起動した後、GUI にログインしてアップグレードワークフローのステータスを確認できます。最初は、クラスタの初期展開と同様のブートストラッププロセスを確認できます。ノードが起動すると、GUI の **[概要（Overview）]** ページでサービスのアクティブ化に関する追加情報を確認できます。

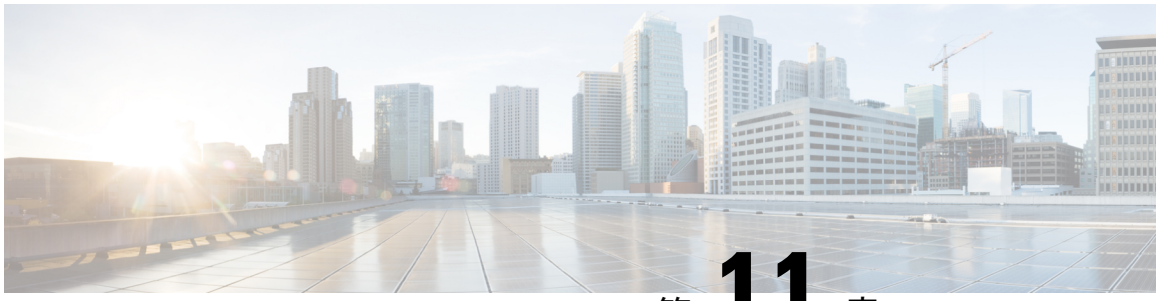
何らかの理由でアップグレードが失敗した場合、GUI にエラーと追加の回避策の手順が表示されます。たとえば、次のようなエラーメッセージが修正とともに表示される場合があります。

```
Failed to activate

Upgrade failed while shutting down the cluster: Operation Timedout, last status: Operation
 Timedout


Please login to one of the primary nodes as 'rescue-user' and follow the steps provided
 by the upgrade recovery
helper by invoking following command: 'acs upgrade recover Cluster Shutdown'. If the
issue persists, please contact Cisco TAC for assistance.
```

問題が解決しない場合は、**[管理（Admin）]** をクリックしてテクニカルサポートにアクセスします。詳細については、 「*Cisco* テクニカル サポートの取り扱い」 を参照してください。



第 11 章

このリリースへの Nexus Dashboard 4.x クラスタのアップグレード

（注） この章の手順は、 Nexus Dashboard リリース **4.x** から Nexus Dashboard リリース 4.3.1 にアップグレードする場合に適用されます。

Nexus Dashboard リリース **3.2.2m** から Nexus Dashboard リリース 4.3.1 にアップグレードする場合は、Nexus Dashboard 3.2.2m クラスタのこのリリースへのアップグレード （259 ページ） に記載されているアップグレード手順に従ってください。

- 既存の Nexus Dashbaord クラスターをアップグレードするための前提条件と注意事項 （279 ページ）
- サポートされているアップグレード パス （282 ページ）
- Nexus Dashboard のアップグレード （284 ページ）
- アップグレードのトラブルシューティング （288 ページ）

既存の Nexus Dashbaord クラスターをアップグレードするための前提条件と注意事項

既存のNexusダッシュボードクラスタをアップグレードする前に、次の手順を実行します。

- アップグレードに影響する可能性のある動作、ガイドライン、および問題の変更については、ターゲット リリースのリリース ノートを必ずお読みください。
- Nexus Dashboard リリース 4.3.1 にアップグレードする前に、次の手順を実行します：
  - NTPとDNSサービスが設定されていることを確認します。システムを正常にアップグレードするには、少なくとも 1 つの NTP と DNS が必要です。
  - LAN デプロイメントは、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ことを確認する必要があります。管理ネットワークとデータ ネットワークが異なるサブネットに存在する場合にアップグレードは失敗します。

この制限は、 SAN 展開には適用されないことに注意してください（SAN 展開では、管理ネットワークとデータ ネットワークが同じサブネットに存在する可能性があります）。

- `acs クラスタ`が健全であることを検証します。

  1. `ssh -l rescue-user [management-ip-of-nd]` を使用してNexusダッシュボードにアクセスします。
  2. `acs health` コマンドを発行します。

  `acs health`コマンドからの出力には、すべてのコンポーネントが正常であることが表示されるはずです。

```
rescue-user@node1:~$ acs health
======
Status
======
All components are healthy
```

- 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。

- マルチクラスタ フェデレーションNexus Dashboard デプロイメントがある場合は、ローカル クラスタをアップグレードする前に、マルチクラスタ グループのプライマリ クラスタを Nexus Dashboard バージョン 4.3.1以降にアップグレードする必要があります。

- バックアップと復元のプロセスがアップグレードにどのように影響するかについて、次の重要な注意事項を確認します。

  - アップグレードする前に Nexus Dashboard クラスターのバックアップを実行し、バックアップ ファイルを安全な場所に保存してください。バックアップを実行するには、「*Nexus Dashboard* のバックアップと復元」を参照してください。
  - 最新のバックアップに障害が発生していた場合、アップグレードは続行されません。アップグレードを進める前に、正常なバックアップがあることを確認してください。バックアップを正常に実行できず、アップグレードできない場合は、 Cisco Technical Assistance Center （TAC） （TAC） に連絡してサポートを受けてください。
  - 復元が失敗した場合、アップグレードを実行することはできません。復元が完了したら、**[履歴の表示（View History）]** をクリックして、**[バックアップと復元（Backup and Restore）]** ページの **[履歴（History）]** エリアに移動します。これについては、「*Nexus Dashboard* とサービスの統合バックアップと復元」の「Nexus Dashboard 構成の復元」セクションで説明されています。

    ページの **[ステータス（Status）]** 列には、復元プロセスの **[成功（Success）]** が表示されます。**[ステータス（Status）]** 列に **[成功（Success）]** 以外の値が表示された場合

は、クラスタを再展開し、復元プロセスが **[成功（Success）]** となることを確認してから、アップグレードを再度試行してください。

- 物理的な Nexus Dashboard クラスタをアップグレードしている場合は、ノードにターゲットの Nexus Dashboard リリースでサポートされている最小の CIMC バージョンがあることを確認してください。

  サポートされている CIMC バージョンは、ターゲット リリースの *Nexus Dashboard* リリース ノート にリストされています。

  CIMC アップグレードについては、Nexus Dashboard ドキュメント ライブラリ の「トラブルシューティング」の記事で詳しく説明されています。

- 仮想 Nexus Dashboard クラスタをアップグレードする場合、 Nexus Dashboard はこれらのチェックを適用します。

  - HDD の遅延をチェックして 30ms 未満であることのチェック。HDD の遅延がさらに高い場合、アップグレードは失敗します。
  - ネットワーク遅延のチェックで、クラスタ ノード内で 50 ミリ秒未満であることを確認します。ネットワークの遅延がさらに高い場合、アップグレードは失敗します。

- VMware ESX に展開された仮想 Nexus Dashboard クラスタをアップグレードする場合は、ESX のバージョンがターゲット リリースで引き続きサポートされていることを確認します。

  このリリースは、VMware ESXi 7.0、7.0.1、7.0.2、7.0.3、8.0、8.0.2、8.0.3 をサポートしています。

（注） ESX サーバーをアップグレードする必要がある場合は、Nexus Dashboard をターゲット リリースにアップグレードする前に行う必要があります。ESX のアップグレードはこのドキュメントの範囲外ですが、簡単に説明すると次のとおりです。

1. 既存の Nexus Dashboard ノード VM を実行している場合に通常行うように、ESX ホストの 1 つをアップグレードします。
2. ホストがアップグレードされた後、Nexus Dashboard クラスタが正常に動作していることを確認します。
3. 他の ESX ホストで 1 つずつアップグレードを繰り返します。
4. すべての ESX ホストがアップグレードされ、既存の Nexus Dashboard クラスタが正常な状態になったら、このドキュメントの説明に従って、Nexus Dashboard をターゲット リリースにアップグレードします。

- Nexus Dashboard ではプラットフォームのダウングレードはサポートされていません。

以前のリリースにダウングレードするには、新しいクラスタを展開する必要があります。

サポートされているアップグレード パス

以前のリリースでは、Nexus Dashboard の展開の概要 （5 ページ） で説明したとおり、Nexus Dashboard にはプラットフォーム ソフトウェアのみが付属しており、サービスは含まれていませんでした。これらのサービスは、最初のプラットフォームの展開後に個別にダウンロード、インストール、および有効化するようになっていました。加えて、Nexus Dashboard リリース 3.1.1では、Nexus Dashboard と個々のサービス間のより緊密な結合を実現したため、各サービスの単一バージョンのみがプラットフォームの各バージョンと互換性を持つようになりました。その結果、Nexus Dashboard ソフトウェアの必要最小限のバージョンを使用している限り、プラットフォームと現在有効になっているすべてのサービスの両方を Nexus Dashboard リリース 3.1x と 3.2x に直接アップグレードできるようになっていました。

Nexus Dashboard リリース 4.1.1 以降、今では、プラットフォームと個々のサービスが単一の製品に統合されました。つまり、サービスを個別に展開、構成、またはアップグレードする必要がなくなりました。

次の表に、特定の展開の組み合わせに関するシナリオの例をいくつか示します。

表 *29 :*

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
4.2.1	N/A	次のセクションの説明に従って、リリース 4.3.1 に直接アップグレードします。
4.1.1	該当なし	次のセクションの説明に従って、リリース 4.3.1 に直接アップグレードします。
3.2.2m	ファブリック コントローラ：12.2(3) Orchestrator：4.4(2) Insights：6.5(2)	Nexus Dashboard 3.2.2m クラスタのこのリリースへのアップグレード （259 ページ） の説明に従って、リリース 4.3.1 に直接アップグレードします。 リリース 4.3.1 では、すべてのサービスが単一の Nexus Dashboard 製品に統合されています。

現在の Nexus Dashboard リリース	互換性のあるサービス （フォームファクタとクラスタサイズによっては、これらのサービスの 1 つ以上が現在有効になっている場合があります）	アップグレードのワークフロー
3.2.1	ファブリック コントローラ：12.2(2) Orchestrator：4.4(1) Insights：6.5(1)	1. 『*Nexus Dashboard* 展開ガイド、リリース *3.2.x*』の説明に従って、Nexus Dashboard プラットフォームをリリース 3.2.2m にアップグレードします。 すべてのサービスは、プラットフォームとともに自動的にアップグレードされます。 2. Nexus Dashboard 3.2.2m クラスタのこのリリースへのアップグレード（259 ページ）で説明されているように、リリース 3.2.2m からリリース 4.3.1 にアップグレードします。 リリース 4.3.1 では、すべてのサービスが単一の Nexus Dashboard 製品に統合されています。
3.1.1	ファブリックコントローラ：12.2(1) Orchestrator：4.3(x) Insights：6.4(1)	1. 『*Nexus Dashboard* 展開ガイド、リリース *3.2.x*』の説明に従って、Nexus Dashboard プラットフォームをリリース 3.2.2m にアップグレードします。 すべてのサービスは、プラットフォームとともに自動的にアップグレードされます。 2. Nexus Dashboard 3.2.2m クラスタのこのリリースへのアップグレード（259 ページ）で説明されているように、リリース 3.2.2m からリリース 4.3.1 にアップグレードします。 リリース 4.3.1 では、すべてのサービスが単一の Nexus Dashboard 製品に統合されています。
3.0.1	ファブリック コントローラ：12.1(3) Orchestrator：4.2(x) Insights：6.3(1)	1. 『*Nexus Dashboard* 展開ガイド、リリース *3.2.x*』の説明に従って、Nexus Dashboard プラットフォームをリリース 3.2.2m にアップグレードします。 すべてのサービスは、プラットフォームとともに自動的にアップグレードされます。 2. Nexus Dashboard 3.2.2m クラスタのこのリリースへのアップグレード（259 ページ）で説明されているように、リリース 3.2.2m からリリース 4.3.1 にアップグレードします。 リリース 4.3.1 では、すべてのサービスが単一の Nexus Dashboard 製品に統合されています。

現在の Nexus Dashboard リリース	互換性のあるサービス （フォームファクタとクラスタサイズによっては、これらのサービスの 1 つ以上が現在有効になっている場合があります）	アップグレードのワークフロー
2.3.2 以前	ファブリックコントローラ：12.1(2) 以前 Orchestrator：4.1(x) 以前 Insights：6.2(x) 以前	1. 『*Nexus Dashboard* 展開ガイド、リリース *3.1.x*』の説明に従って、Nexus Dashboard プラットフォームをリリース 3.1.1 にアップグレードします。 すべてのサービスは、プラットフォームとともに自動的にアップグレードされます。 2. 『*Nexus Dashboard* 展開ガイド、リリース *3.2.x*』の説明に従って、リリース 3.1.1 からリリース 3.2.2m にアップグレードします。 すべてのサービスは、プラットフォームとともに自動的にアップグレードされます。 3. Nexus Dashboard 3.2.2m クラスタのこのリリースへのアップグレード （259 ページ） で説明されているように、リリース 3.2.2m からリリース 4.3.1 にアップグレードします。 リリース 4.3.1 では、すべてのサービスが単一の Nexus Dashboard 製品に統合されています。

Nexus Dashboard のアップグレード

このセクションでは、既存の Nexus Dashboard 4.x クラスタを Nexus Dashboard 4.3.1 リリースにアップグレードする方法について説明します。

始める前に

で説明している前提条件をすべて満たしていることを確認します。 既存の Nexus Dashbaord クラスターをアップグレードするための前提条件と注意事項 （279 ページ）

手順

ステップ 1 Nexus Dashboard リリース 4.x システムで、 Nexus Dashboard 4.3.1 イメージをダウンロードします。

a) [ソフトウェア ダウンロード（Software Download）] ページを参照します。

https://software.cisco.com/download/home/286327743/type/286328258/release/4.3.1

b) 左側のサイドバーから、ダウンロードする Nexus Dashboard 4.3.1 のリリース バージョンを選択します。
c) ターゲットとする 4.3.1 リリース用の Nexus Dashboard イメージをダウンロードします。



（注）
- アップグレード プロセスは、すべての Nexus ダッシュボード フォーム ファクタで同じで、Nexus ダッシュボード ISO イメージ（`nd-dk9.<version>.iso`）を使用します。言い換えると、最初の展開で仮想フォーム ファクターを使用していた場合（ESX での展開のための `.ova` イメージなど）やクラウド プロバイダーのマーケット プレースを使用していた場合であっても、アップグレードでは `.iso` イメージを使用する必要があります。
- イメージのダウンロードが完全に失敗した場合は、Nexus Dashboard とイメージ サーバ間のネットワーク接続を確認します。**[管理（Admin）]**>**[システム設定（System Settings）]**>**[一般（General）]**>**[プロキシ構成（Proxy configuration）]** でプロキシ構成を確認します。

d) （オプション）環境内のWebサーバでイメージをホストします。



（注） 環境内のサーバーでイメージをホストすることをお勧めします。イメージを Nexus Dashboard クラスタにアップロードする場合、イメージに直接 URL を指定するオプションがあります。そうすれば、プロセスは相当高速化されます。

ステップ 2 イメージを追加します。

a) 左のナビゲーション メニューから **[管理 (Admin)]** > **[システム ソフトウェア (System Software)]** を選択します。
b) **[システム ソフトウェア（System Software）]** ページで、**[Nexus Dashboard リリース（Nexus Dashboard Releases）]** エリアに提供されている情報を確認します。
   - 左端の並べて表示するには、現在 Nexus Dashboard にインストールされ実行されているソフトウェア イメージが表示されます。
   - 右端の並べて表示するには、現在 Nexus Dashboard にアップロードされているソフトウェア イメージが表示されます。

   いずれかの並べて表示するで **[新機能（What's new）]** をクリックして特定のリリースで利用可能な新機能を表示するか、**[リリースノート（Release notes）]** をクリックしてその特定のリリースのリリース ノートを表示します。

c) **[Nexus Dashboard リリース（Nexus Dashboard Releases ）]** エリアの右上隅で、**[イメージの追加（Add Image）]** をクリックします。

ステップ 3 **[ソフトウェア イメージの追加（Add Software Image）]** ページでイメージをローカル システムまたはリモート サーバーのどちらに保存するかを選択します。

- ローカル システムからイメージを追加している場合は、**[ローカル（Local）]**をクリックし、**[ファイルを選択（Choose File）]** をクリックして、ローカル システム上のイメージ ファイルに移動して、ローカル システムからイメージ ファイルを選択します。

（注） ローカルマシンからアップロードする場合、アップロード速度が遅いと、セッションがタイムアウトして転送が中断されることがあります。少なくとも40Mbpsのアップロード速度と、セッションタイムアウトを(デフォルトの1200から)1800秒に増やすことをお勧めします。

セッション タイムアウトは、Nexus Dashboard GUI の **[管理（Admin）]** > **[セキュリティ（Administrative Security）]** ページで変更できます。Nexus Dashboard セッションからログアウトした場合、UI に再ログインできるようになるまでに 1 分かかる場合があります。

- リモート ロケーションからイメージを追加する場合、イメージの追加方法を選択します。
  - **HTTP** を選択した場合は、**URL** フィールドにイメージへの完全な URL を入力します。
  - **[SFTP/ SCP]**を選択した場合：
    1. **[リモート ストレージ（Remote Storage）]** フィールドで、リストからすでに構成されているリモート ストレージ ロケーションを選択するか（使用可能な場合）、**[リモート ストレージ ロケーションの作成（Create Remote Storage Location）]** をクリックします。

       [リモート ストレージ ロケーションの作成（Create Remote Storage Location）] をクリックした場合は、「Nexus Dashboard のバックアップと復元」のリモート ストレージ ロケーションの作成セクションの手順に従ってから、ここに戻ります。
    2. **[リモート パス ファイルネーム（Remote Path Filename）]** フィールドに、イメージのリモート パスを入力します。

ステップ 4 [追加（Image）] をクリックして、 イメージを追加します。

右端の並べて表示するには、イメージのアップロードの進行状況が表示されます。次のセクションへ進む前に完了するのを待ってください。

（注） アップグレードのトラブルシューティング（288ページ）を参照してください。ここには、アップグレードのこの時点で行われる検証のチェックと、問題が生じた場合の対処方法が記されています。

a) 検証が完了すると、これらのボタンは、 **システム ソフトウェア** ページの **Nexus Dashboard リリース** エリアのカードに表示されます。

- **工場出荷時のインストール**: **工場出荷時のインストール** オプションを使用すると、ブートストラップ設定を含むすべてのデータが消去されます。その後クラスタを再ブートストラップする必要があります。
- **アップグレード**：以前のリリースからアップグレードする場合は、 **アップグレード** オプションをクリックします。アップグレード前に **初期設定のインストール**を実行する必要はありません。

該当するボタンをクリックして、ソフトウェアをインストールまたはアップグレードします。

インストールの進行状況ウィンドウが表示されます。更新中は、この画面から移動できます。

クラスター内のノードの数によっては、この手順に60分以上かかる場合があります。その間、ノードが再起動し、 GUIにアクセスできなくなります。Nexus Dashboard は、いくつかの段階を経て次の手順を経ます。

- リリース ファームウェアのインストール
- サービスの無効化
- インフラストラクチャ サービスのシャットダウン
- プラットフォーム サービスのアップデート
- インフラストラクチャ サービスの有効化
- サービスの有効化

[詳細（Details）] リンクをクリックして、アップグレードの進行状況とさまざまな段階を確認できます。

（注） アップグレードプロセス中に問題が発生した場合（インデックスの問題の可能性など）は既存の Nexus Dashbaord クラスターをアップグレードするための前提条件と注意事項（279 ページ）を参照してください。

上記のプロセスが完了したら、 Nexus Dashboard 4.3.1 にアップグレードする必要があります。

（注） 展開したクラスター形式とクラスター ノードの数によっては、特定の機能（コントローラ、オーケストレータ、テレメトリなど）が使用できない場合があります。 Nexusダッシュボード キャパシティ プランニング ツール の情報を確認して、クラスターインストールで使用できる機能を確認します。

ステップ 5 ノードのアップグレードタスクが完了したら、ノードが正常であり、UIにログインできることを確認します。

アップグレード プロセスが完了すると、通常どおりに Nexus Dashboard ダッシュボード UI を表示できます。

[概要（Overview）] ページでシステム全体の正常性を確認し、**[管理（Admin）]** > **[システム ソフトウェア（System Software）]**ページで現在の実行中バージョンを確認できます。

ステップ 6 DNS のクラスタ名の変更を確認します。

Nexus Dashboard リリース 4.3.1 以降、新規インストールとアップグレードの場合、クラスター DNS は `nd-cluster.case.local` にハードコードされます。以前のリリースから Nexus Dashboard リリース 4.3.1 に

アップグレードすると、クラスタ名に基づいて表示される DNS ドメイン名がアップグレード後に変更され、その DNS ドメイン内のクラスタ名ではなく固定クラスタ名（`nd-cluster.case.local`）が表示されます。

アップグレードのトラブルシューティング

前のセクションで説明した、新しいイメージのアクティブ化段階で、すべてのノードが再起動した後、GUI にログインしてアップグレードワークフローのステータスを確認できます。最初は、クラスタの初期展開と同様のブートストラッププロセスを確認できます。ノードが起動すると、GUI の **[概要（Overview）]** ページでサービスのアクティブ化に関する追加情報を確認できます。

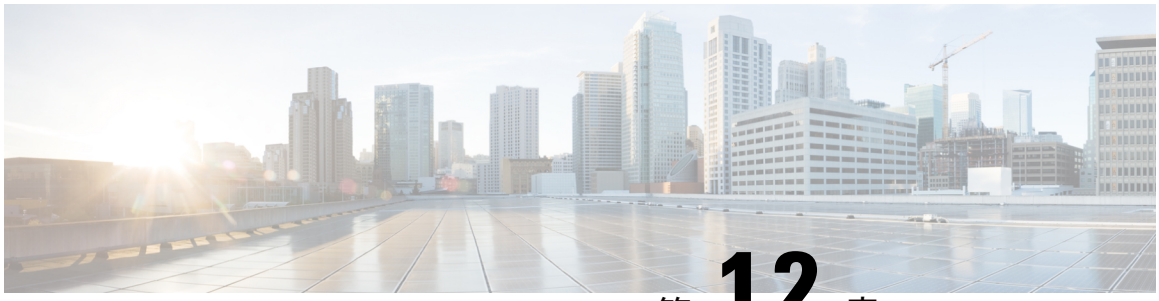
何らかの理由でアップグレードが失敗した場合、GUI にエラーと追加の回避策の手順が表示されます。たとえば、次のようなエラーメッセージが修正とともに表示される場合があります。

```
Failed to activate

Upgrade failed while shutting down the cluster: Operation Timedout, last status: Operation
 Timedout


Please login to one of the primary nodes as 'rescue-user' and follow the steps provided
 by the upgrade recovery
helper by invoking following command: 'acs upgrade recover Cluster Shutdown'. If the
issue persists, please contact Cisco TAC for assistance.
```

問題が解決しない場合は、**[管理（Admin）]** をクリックしてテクニカルサポートにアクセスします。詳細については、「*Cisco* テクニカル サポートの取り扱い」 を参照してください。



第 12 章

DCNM から ND への移行

• DCNM から ND への移行 （289 ページ）

DCNM から ND への移行

DCNM 11.5（4）から Nexus Dashboard 4.3.1 に直接アップグレードすることはできません。代わりに、このワークフローを活用、 DCNM 11.5（4）から Nexus Dashboard 4.3.1にアップグレードします：

1. 最初に、 DCNM 11.5(4) からNexus Dashboard 4.1.1 に、『 *Cisco Nexus Dashboard* 展開とアップグレードガイド、リリース *4.1.x*』の「DCNMから ND への移行」セクションに記載されている手順を使用してアップグレードします。
2. 次に、このリリースへの Nexus Dashboard 4.x クラスタのアップグレード （279 ページ） で提供されている手順を使用して、 Nexus Dashboard 4.1.1 から Nexus Dashboard 4.3.1 にアップグレードします。

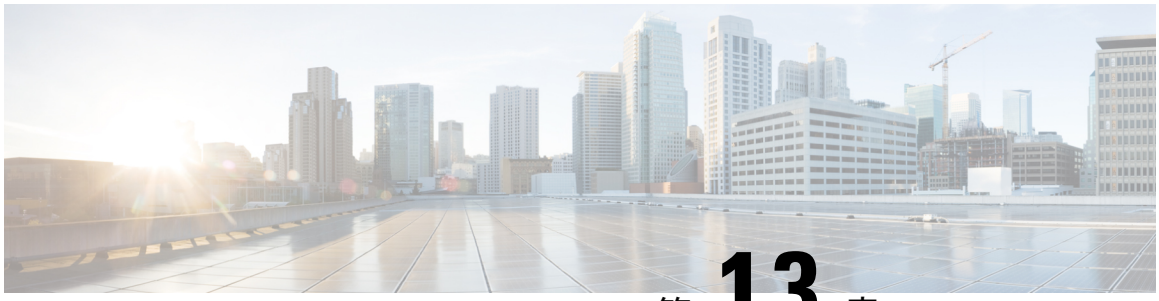
（注） DCNM 11.5 から Nexus Dashboard 4.1.1 にアップグレードした後、 Nexus Dashboard Orchestrator（NDO）アプリが無効になるという問題があります。Nexus Dashboard 4.1.1 から Nexus Dashboard 4.3.1 にアップグレードする前に、手動で NDO（オーケストレータ）アプリを再度有効にする必要があります。そうしないと、アップグレードの事前チェックの失敗が表示されます。

1. **TAC サポートの詳細設定とオプションの表示機能** を有効にします（**[管理（Admin）]**>**[システム設定（System Settings）]** > **[一般（General）]** > **[詳細設定（Advanced Settings）]** > **[TAC サポートの詳細設定とオプションの表示（Display advanced settings and options for TAC suppor）]**）。

   次の手順の **[機能（Features）]** タブを表示するには、 **TAC サポート機能の詳細設定およびオプションの表示** を有効にする必要があります。

2. NDO（オーケストレータ）アプリケーションを手動で再度有効にします**([管理（Admin）]**> **[システム ステータス（System Status）]** > **[機能（Features）]**)。

   その後、必要に応じて、 **TACサポート機能の詳細設定およびオプションの表示を** 再度無効にできます。



第 13 章

NDB から ND への移行

• NDB から ND への移行 （291 ページ）

NDB から ND への移行

現在 NDB 集中型バージョン 3.10.4（または 3.10.5.x）を使用していて、アップグレードする予定の場合は、ND 4.2 の一部として利用可能な NDB バージョンにアップグレードできます。

Nexus Data Broker（NDB）の集中型デプロイメントからNexus Dashboard（ND）に移行するには、次の手順を使用してください。

ND 4.2 への移行でサポートされているパスは次のとおりです。

- NDB 3.10.4 または 3.10.5.x から ND 4.2 への移行。
- リリース 3.10.4 より前の NDB バージョンの場合、ND 4.2 への移行は 2 段階のプロセスです。3.10.4 より前の NDB バージョンは、まず 3.10.4（または 3.10.5.x）にアップグレードする必要があります。このアップグレードでサポートされている NDB バージョンは、3.8.x、3.9.x、3.10.1、3.10.2、3.10.3 です。

  NDB リリース 3.10.4 または 3.10.5.x にアップグレードするための詳細な手順については、それぞれの Nexus Data Broker Deployment Guide を参照してください。

  例: NDB 3.8.1 を ND 4.2 にアップグレードする場合、最初に NDB 3.10.4（または 3.10.5.x）にアップグレードしてから ND 4.2 に移行します。

始める前に

1. Nexus Data Broker GUI にログインし、標準規格の手順を使用して構成ファイルをダウンロードします。

   [管理（Administration）]>[バックアップ/復元（Administration）]>[アクション（Actions）] に移動します。設定はローカル マシンまたはサーバーにバックアップできます。

2. Github にある `backup_converter.sh`ファイルを使用して、NDB構成ファイル（ステップ 1 でダウンロードしたもの）を ND 互換ファイルに変換します。

3. （オプション） ./backup_converter.sh -f {zip_file} -v {ND_version} -k {password} を使用して暗号キーを作成します。スクリプトの実行の手順（Github）を参照してください。この暗号化キーは後から変更できません。バックアップの復元時に同じキーを入力する必要があるため、暗号キーを保存してください。
4. 「Github」から入手可能な「steps_to_generate_ND_format_backup.txt」ファイルに詳述された手順にしたがってください。ファイルには、NDB構成ファイルをND 互換ファイルに変換するための詳細な手順が含まれています。ND 互換ファイルの名前は、cisco-nddb-backup.tar.gzです。

手順

ステップ 1 Nexus Dashboard GUI にログインします。

ステップ 2 **[管理（Administration）]** > **[バックアップ/復元（Backup and Restore[）]** に移動します。

ステップ 3 **[バックアップと復元]** 画面で、**[復元（Restore）]** ボタンをクリックします。

ステップ 4 **復元** 画面で、次のように入力します。

a) **ソース**：バックアップ ファイルの場所
b) **バックアップ ファイル**：変換された ND 互換ファイル。
c) **暗号キー**：事前に作成したカスタム暗号キーを入力します。暗号キーを設定していない場合、デフォルト値の cisco123 が割り当てられます。
d) **[検証とアップロード]** をクリックします。**[ファイル名]** フィールドには、ND 互換ファイル（cisco-nddb-backup.tar.gz）が自動的に入力されます。
e) 検証が完了し、**[次へ（Next）]**をクリックします。

検証の進行状況は緑色のバーで示され、100% が表示されるまで待ちます。

ステップ 5 （復元画面の次のページ）永続的なIP構成を上書きするには、「**このバックアップから永続的なIP構成を復元しない**」チェックボックスをオンにしてください。

チェックボックスをオンにしてください。そうしないと、復元プロセスは失敗します。

ステップ 6 [復元（Restore）] をクリックします。

ステップ 7 **復元開始の** 確認画面で、**[復元]**をクリックします。

確認後、移行プロセスが開始されます。進行状況をモニターできます。さまざまな段階は進行状況バーで示されます。

ステップ 8 [閉じる（Close）] をクリックします。

次のタスク

移行プロセスの後、次の手順を実行します。

1. ND GUI で、**[管理（Manage）]** > **[ファブリック（Fabrics）]** に移動します。

2. 必要な NDB ファブリック（NDB デフォルト、またはスライスを作成した場合は スライス名 は ファブリック名）を選択します。
3. **[アクション（Actions）] > [再計算と展開（Recalculate and Deploy）]** をクリックします。

   これにより、NDB デバイスの構成が更新されます。
4. デバイス モードをチェックします（**管理 > インベントリ**）。この時点で、モードは 「通常（*Normal*）」 として表示されます（移行プロセス中、デバイス モードは *[*移行（*Migration*）*]*と示されます）。

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。