



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](#) (1 ページ)
- [物理ノードのケーブル接続](#) (5 ページ)
- [物理アプライアンスとしての Nexus ダッシュボードの展開](#) (7 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 クラスターの展開に進む前に、次の手順を実行する必要があります。

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

サービス固有のドキュメントは、次のリンクで見つけることができます。

- [Nexus Dashboard ファブリック コントローラ、リリース ノート](#)
- [Nexus Dashboard Insights リリース ノート](#)
- [Nexus Dashboard Orchestrator リリース ノート](#)
- 使用しているサーバーのモデルに対応した、[Cisco Nexus Dashboard ハードウェア セットアップガイド](#)の説明に従って、以下のハードウェアを使用しており、サーバがラックに接続されていることを確認します。

物理アプライアンス フォーム ファクタは、UCS-C220-M5 (SE-NODE-G2) および UCS-C225-M6 (ND-NODE-L4) のオリジナルの Cisco Nexus Dashboard プラットフォーム ハードウェアでのみサポートされます。次の表に、サーバの物理的アプライアンス サーバの PID と仕様を示します。

表 1: サポートされる UCS-C220-M5 ハードウェア

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

表 2: サポートされる UCS-C225-M6 ハードウェア

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



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

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

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

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

[Cisco Integrated Management Controller IP アドレスの構成 \(4 ページ\)](#) 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 \(5 ページ\)](#) 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 2.3.2 のイメージがプリインストールされているが、代わりにリリース 3.2.1 を展開する場合は、次の手順に従います。

1. 最初に、リリース 2.3.2 クラスタを[そのリリース](#)の展開ガイドに従って起動します。
2. [既存の ND クラスタをこのリリースへアップグレード](#)の説明に従って、リリース 3.2.1 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ーを展開する前に、Cisco Nexus Dashboard の最新バージョンを使用してノードを再イメージ化することもできます（たとえば、GUI ワークフローを通じたこのリリースへの直接アップグレードをサポートしていないイメージがハードウェアに付属している場合）。このプロセスについては、このリリースの[トラブルシューティング](#)の記事の「ノードの再イメージング」セクションで説明されています。

- 少なくとも3ノードのクラスターが必要です。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 (NIC Redundancy)]** で、**[Active-active [x]]** を選択します。
- d) ホスト名、DNS、デフォルトユーザーパスワード、ポートプロパティ、ポートプロファイルのリセットなどのその他のオプションを表示するには、**F1** を押します。

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

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

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

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

手順

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

ステップ 2 次のコマンドを実行します。

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

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

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

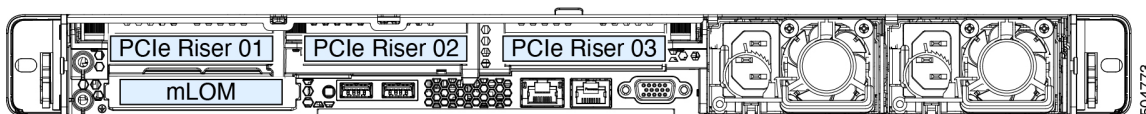
ステップ 3 コマンド出力で、`com0` が SoL の comポートであることを確認します。

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

物理ノードのケーブル接続

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

図 1: ノード接続に使用される mLOM および PCIe ライザー 01 カード



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

- UCS-C220-M5 サーバーには、「PCIe-Riser-01」スロットに 4 ポートの VIC1455 カードが含まれており (上の図を参照)、Nexus Dashboard のデータ ネットワーク接続に使用します。
- UCS-C225-M6 サーバーには、2x10GbE NIC (APIC-P-ID10GC) または 2x25/10GbE SFP28 NIC (APIC-P-I8D25GF)、または「PCIe-Riser-01」スロット (上の図に表示) の VIC1455 カードに含まれており、Cisco Nexus Dashboard のデータ ネットワーク接続に使用します。

ノードを管理ネットワークおよびデータ ネットワークに接続する場合：

- インターフェイスは、アクティブ/スタンバイ モードで実行されている、データインターフェイス用と管理インターフェイス用の Linux ボンドとして設定されます。
- 管理ネットワークの場合：
 - mLOM カードで mgmt0 および mgmt1 を使用する必要があります。
 - すべてのポートが同じ速度 (1G または 10G) である必要があります。
- データ ネットワークの場合：
 - UCS-C220-M5 サーバーでは、VIC1455 カードを使用する必要があります。
 - UCS-C225-M6 サーバーで、2x10GbE NIC (APIC-P-ID10GC)、または 2x25/10GbE SFP28 NIC (APIC-P-I8D25GF)、または VIC1455 カードを使用できます。



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

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

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



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

- UCS-C220-M5 サーバーでは、左から右に、ポート 1、ポート 2、ポート 3、ポート 4 です。
- UCS-C225-M6 サーバーでは、左から右に、ポート 4、ポート 3、ポート 2、ポート 1 です。

- ノードを Cisco Catalyst スイッチに接続する場合は、`switchport voice vlan dot1p` コマンドをスイッチ インターフェイスに追加する必要があります。

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

物理アプライアンスとしての Nexus ダッシュボードの展開

Nexus ダッシュボードの物理ハードウェアを最初に受け取ると、ソフトウェアイメージがブロードロードされています。ここでは、最初の Nexus Dashboard クラスタを設定して起動する方法について説明します。

始める前に

- [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 \(1 ページ\)](#) に記載されている要件とガイドラインを満たしていることを確認します。

手順

ステップ 1 最初のノードの基本情報を設定します。

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

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

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

ホストに接続したら、**Enter** を押して続行します。

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

```
Starting Nexus Dashboard setup utility
Welcome to Nexus Dashboard 3.2.1
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)

純粋な IPv6 モードを構成する場合は、代わりに上記の例の IPv6 を指定します。

- e) 入力した譲歩をレビューし、確認します。

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

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

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

ステップ2 初期ブートストラップ処理が完了するまで待ちます。

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

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

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

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

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

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

ステップ 4 [クラスタの詳細 (Cluster Details)] を入力します。

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

Cluster Bringup
Answer some questions, select the services you want to enable and have Nexus Dashboard ready to use in a few minutes.

1 Configuration

Configuration
Provide the cluster name and configure the DNS, NTP and Proxy to set up Nexus Dashboard and bring up the user interface

Nexus Dashboard Cluster Name*
a) nd-cluster

Enable IPv6
b) ☐

DNS

DNS Provider IP Address*
c) 171.70.168.183

DNS Search Domain
d)

NTP

NTP Authentication
e) ☐

NTP Host*
f) 171.68.38.65

Proxy
Skip Proxy

Ignore Hosts
g)

Proxy Server*
g)

Authentication required for proxy
☐

Advanced Settings

App Network*
h) 172.17.0.1/16

Service Network*
h) 100.80.0.0/16

App Network IPv6
h) 2000::/108

Service Network IPv6
h) 3000::/108

Next

- a) Nexus ダッシュボード クラスタの [クラスタ名 (Cluster Name)] を入力します。
クラスタ名は、RFC-1123 の要件に従う必要があります。

- b) (オプション) クラスタの IPv6 機能を有効にする場合は、**[IPv6 を有効にする (Enable IPv6)]** チェックボックスをオンにします。
- c) **[+DNS プロバイダの追加 (+Add DNS Provider)]** をクリックして、1 つ以上の DNS サーバを追加します。

情報を入力した後、チェックマーク アイコンをクリックして保存します。

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

情報を入力した後、チェックマーク アイコンをクリックして保存します。

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

次のフィールドで、以下の情報を提供します。

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

(注)

情報を入力した後、チェックマーク アイコンをクリックして保存します。

NTP 認証の要件とガイドラインの完全なリストについては、[すべての有効なサービスの前提条件と注意事項](#) を参照してください。

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

次のフィールドで、以下の情報を提供します。

- **NTP ホスト** : IP アドレスを指定する必要があります。完全修飾ドメイン名 (FQDN) はサポートされていません。
 - **キー ID** : このサーバーの NTP 認証を有効にする場合は、前の手順で定義した NTP キーのキー ID を指定します。
- NTP 認証が無効になっている場合、このフィールドはグレー表示されます。
- この NTP サーバーを **[優先 (Preferred)]** にするかどうかを選択します。

情報を入力した後、チェックマーク アイコンをクリックして保存します。

(注)

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

NTP Host*	Key ID	Preferred
2001:420:28e:202a:5054:ff:fe6f:b3f6		true

[Add NTP Host Name/IP Address](#)

△ Could not validate one or more hosts Can not reach NTP on Management Network

これは、ノードに IPv6 アドレスがまだなく（次の手順で指定します）、NTP サーバーの IPv6 アドレスに接続できないためです。

この場合、次の手順の説明に従って他の必要な情報の入力を完了し、[次へ (Next)] をクリックして次の画面に進み、ノードの IPv6 アドレスを入力します。

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

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

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

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

プロキシ サーバーでは、次の URL が有効になっている必要があります。

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

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

- h) (オプション) プロキシ サーバで認証が必要な場合は、[プロキシで認証が必要 (Authentication required for Proxy)] を [はい (Yes)] に変更し、ログイン資格情報を指定します。
- i) (オプション) [詳細設定 (Advanced Settings)] カテゴリを展開し、必要に応じて設定を変更します。

詳細設定では、次の設定を行うことができます。

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

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

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

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

アプリケーションおよびサービスネットワークについては、このドキュメントの前の [すべての有効なサービスの前提条件と注意事項](#) の項で説明します。

j) **[次へ (Next)]** をクリックして続行します。

ステップ 5 **[ノードの詳細 (Node Details)]** 画面で、最初のノードの情報を更新します。

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

Cluster Bringup
Answer some questions, select the services you want to enable and have Nexus Dashboard ready to use in a few minutes.

Node Details
Register Nexus Dashboard nodes to form a cluster and adjust their settings to allow communication between them and to your fabrics.
[Learn More](#)

The diagram illustrates the network topology: three Nexus Dashboard nodes (Node 1, Node 2, Node 3) are connected to a central L2/L3 switch, which is connected to a Data Network. Each node also connects to a Management Network. The nodes are labeled with their serial numbers and IP addresses.

Serial Number	Name	Type	Management Network	Data Network
E5998163D6F0		Primary	IPv4 Address: 172.23.141.129/21 IPv4 Gateway: 172.23.136.1	IPv4 Address: - IPv4 Gateway: - VLAN: -

[Add Node](#)

[Back](#) [Next](#)

© Cisco Systems, Inc.
Current date and time is Sunday, January 14, 03:59 PM (PST)

[Contacts](#) [Privacy Statement](#)

Edit Node



General

Name *

nd-node1

Serial Number *

E5998163D6F0

Type *

Primary

Management Network ⓘ

IPv4 Address/Mask *

172.23.141.129/21

IPv4 Gateway *

172.23.136.1

IPv6 Address/Mask

IPv6 Gateway

Data Network ⓘ

IPv4 Address/Mask *

172.31.140.68/21

IPv4 Gateway *

172.31.136.1

IPv6 Address/Mask

IPv6 Gateway

VLAN ⓘ

Enable BGP ☐

Cancel

Save

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

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

- b) ノードの [名前 (Name)] を入力します。

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

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

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

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

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

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

(注)

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

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

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

Insights やファブリック コントローラなどの、一部のサービスで使用する永続的な IP 機能には、BGP 構成が必要です。この機能については、[すべての有効なサービスの前提条件と注意事項](#)と『[Cisco Nexus Dashboard ユーザーガイド](#)』の「永続的な IP アドレス」セクションで詳しく説明されています。

(注)

BGP をこの時点で、またはクラスタの展開後に Nexus ダッシュボード GUI で有効にすることができます。BGP が構成されている場合は、残りのすべてのノードで BGP を構成する必要があります。

BGP を有効にする際、次の情報も入力する必要があります。

- このノードの **ASN** (BGP 自律システム番号)。

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

- 純粋な IPv6 の場合、このノードの **ルータ ID**。

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

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

- f) **[Save]**をクリックして、変更内容を保存します。

ステップ 6 **[ノードの詳細 (Node Details)]** 画面で、**[ノードの追加 (Add Node)]** をクリックして、クラスタに 2 番目のノードを追加します。

単一ノードクラスタを展開する場合は、この手順をスキップします。

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

(注)

2 番目のノードの **[ユーザー名 (Username)]** フィールドに、管理者ユーザー識別子 (ローカルユーザー管理の識別子 1) 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) ノードの **[名前 (Name)]** を入力します。

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

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

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

- e) **[管理ネットワーク (Management Network)]** エリアで、ノードの**管理ネットワーク**の情報を提供します。

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

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

(注)

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

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

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

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

(注)

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

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

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

Insights やファブリック コントローラなどの、一部のサービスで使用する永続的な IP 機能には、BGP 構成が必要です。この機能については、[すべての有効なサービスの前提条件と注意事項](#)と『[Cisco Nexus Dashboard ユーザーガイド](#)』の「永続的な IP アドレス」セクションで詳しく説明されています。

(注)

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

BGP を有効にする際、次の情報も入力する必要があります。

- このノードの **ASN** (BGP 自律システム番号)。
すべてのノードに同じ ASN を構成することも、ノードごとに異なる ASN を構成することもできます。
- 純粋な IPv6 の場合、このノードの **ルータ ID**。
ルータ ID は、1.1.1.1 などの IPv4 アドレスである必要があります。
- ピアの IPv4 または IPv6 アドレスとピアの ASN を含む **BGP ピアの詳細**。

- h) **[Save]** をクリックして、変更内容を保存します。

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

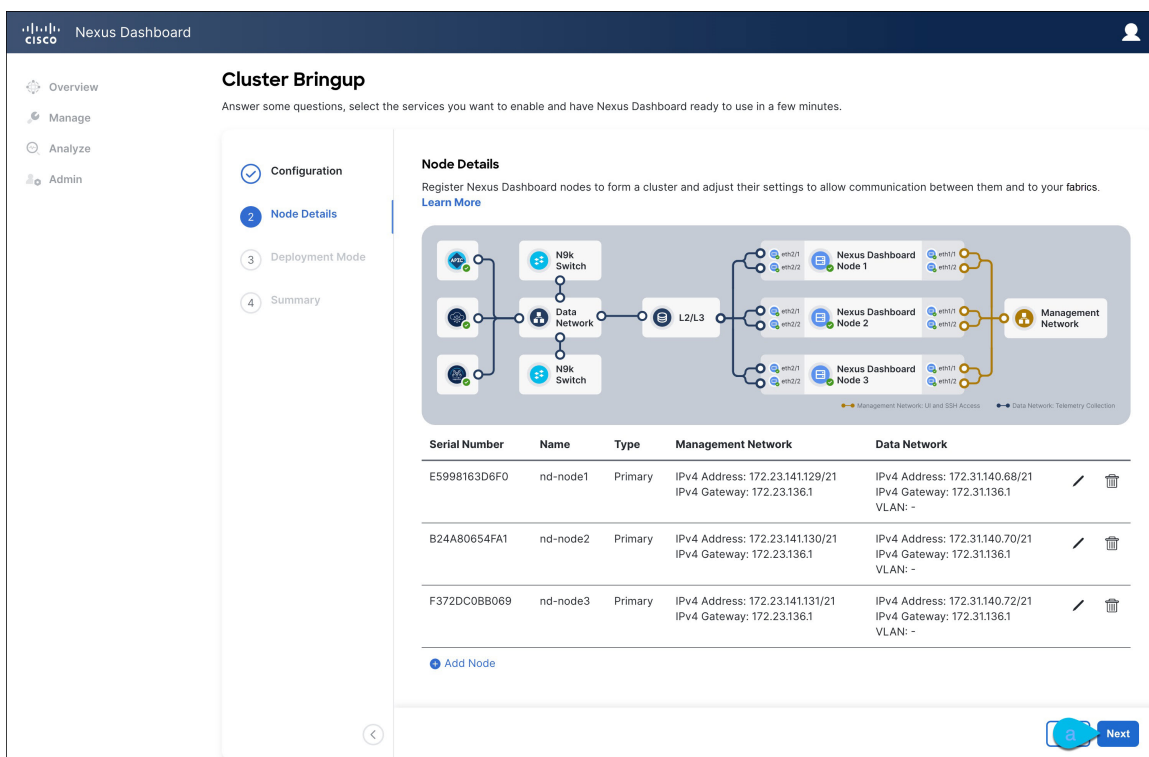
ステップ 7 (オプション) 前の手順を繰り返して、追加のセカンダリ ノードまたはスタンバイ ノードに関する情報を入力します。

(注)

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

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

ステップ 8 **[ノードの詳細 (Node Details)]** ページで、入力した情報を確認し、**[次へ (Next)]** をクリックして続行します。



ステップ 9 クラスタの展開モードを選択します。

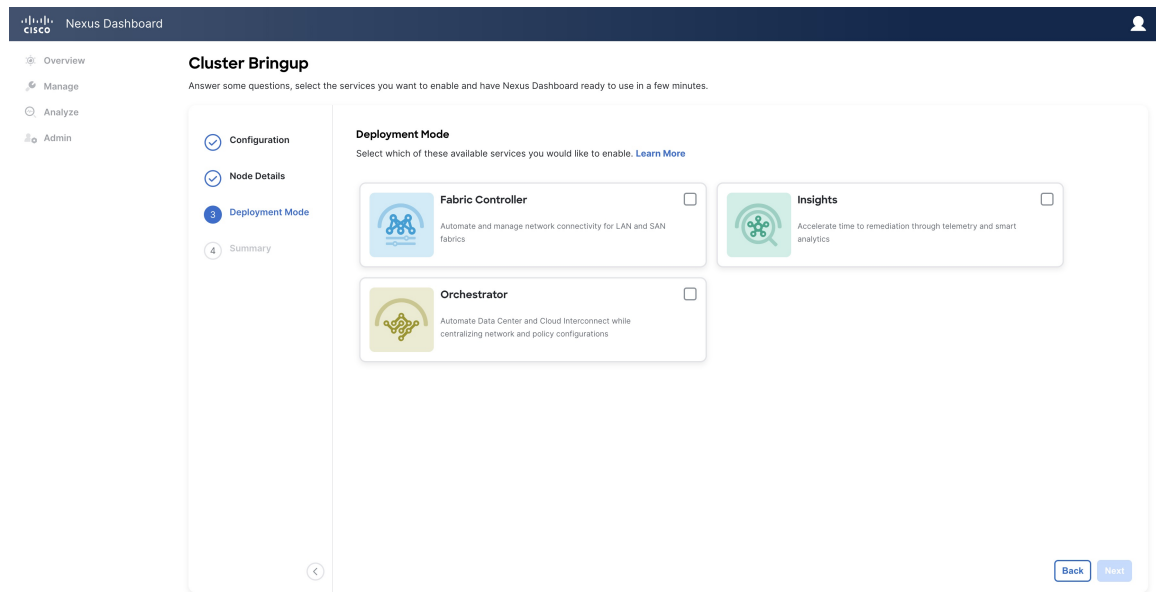
a) 有効にするサービスを選択します。

(注)

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

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

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



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

必要に応じてこの時点でこのステップをスキップでき、クラスタが起動した後に永続的な IP を追加できることに注意してください。永続 IP の詳細については、[すべての有効なサービスの前提条件と注意事項](#) セクションおよびサービス固有の要件の章を参照してください。

- c) [次へ (Next)] をクリックして続行します。

ステップ 10 [概要 (Summary)] 画面で設定情報をレビューして確認し、**[保存 (Save)]** をクリックし、**[続行 (Continue)]** をクリックして正しい展開モードを確認し、クラスタの構築を続行します。

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

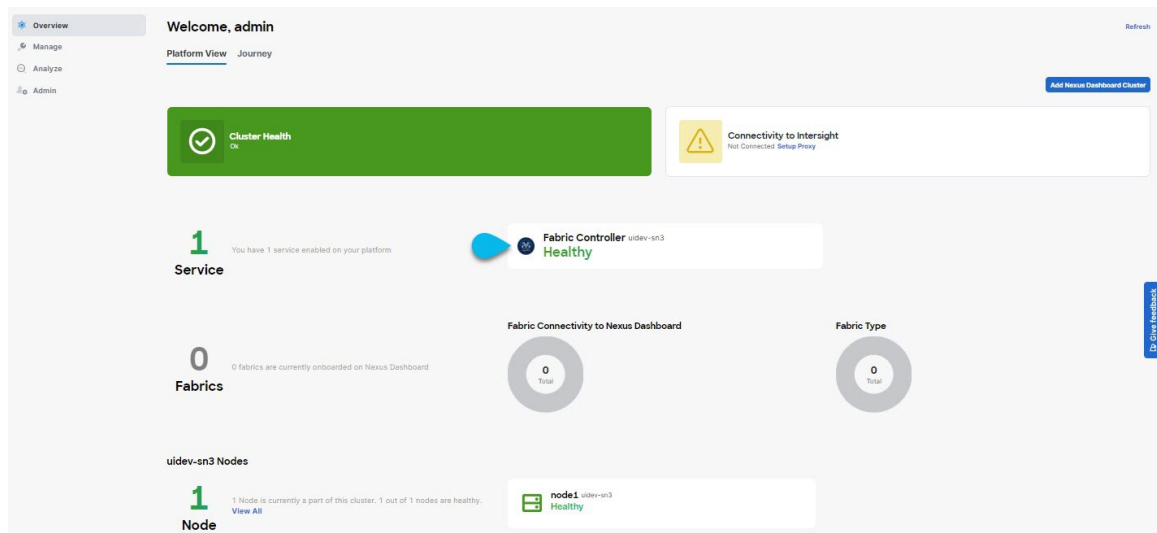
クラスタが形成され、すべてのサービスが開始されるまでに最大 30 分かかる場合があります。クラスタの設定が完了すると、ページが Nexus ダッシュボード GUI にリロードされます。

ステップ 11 クラスタが健全であることを検証します。

展開モードに応じて、クラスタが形成されすべてのサービスが開始されるまでに最大 30 分かかる場合があります。

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

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



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

- クラスタが収束している間、次の出力が表示されることがあります。

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

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

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

- クラスタが稼働している場合は、次の出力が表示されます。

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

(注)

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

```
deploy base system services
```

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

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

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

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

- Insights については、[ドキュメント ライブラリ](#)を参照してください。
-

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。