物理アプライアンスとしての展開

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

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

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

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

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

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

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

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

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

  Cisco Integrated Management Controller IP アドレスの構成 （3 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 （4 ページ）を参照してください。

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

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

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

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

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

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

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

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

Cisco Integrated Management Controller IP アドレスの構成

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

手順

ステップ 1 サーバの電源をオンにします。

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

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

ステップ 3 次のサブステップに従います。

a) **NIC モード**を専用モードに設定します。

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

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

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

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

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

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

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

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

手順

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

ステップ 2 次のコマンドを実行します。

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

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

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

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

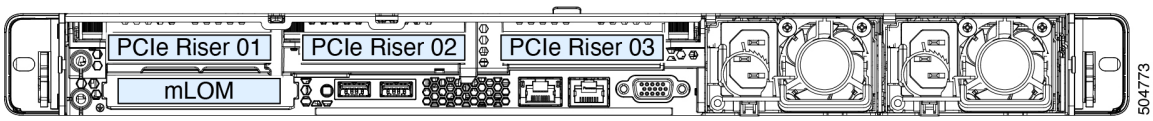
これにより、システムはCIMC CLI から `connect host` コマンドを使用してコンソールをモニタできます。これは、クラスタの起動に必要です。

物理ノードのケーブル接続

物理ノードは、以下の物理サーバーに展開できます：

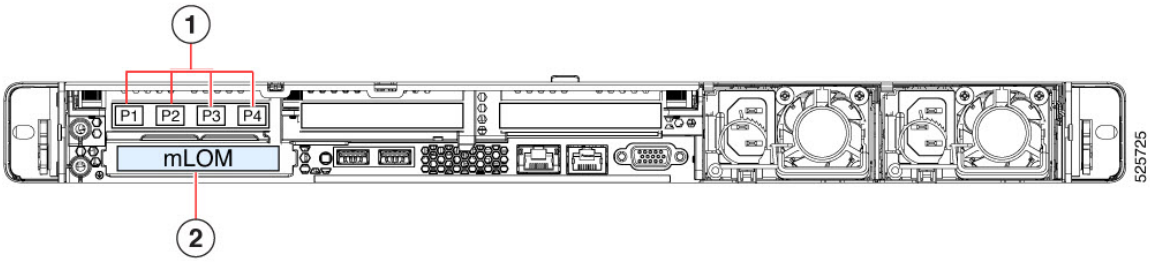
- `SE-NODE-G2` （UCS-C220-M5）および `ND-NODE-L4` （UCS-C225-M6）物理サーバー：

図 *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： *`SE-NODE-G2`* （*UCS-C220-M5*）および *`ND-NODE-L4`* （*UCS-C225-M6*）



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

図 2: ノード接続に使用される *mLOM* および *PCIe* ライザー *01* カード：*ND-NODE-G5S*



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

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

物理ノードは、次のガイドラインに従って展開できます：

- すべてのサーバーに、Nexus Dashboard 管理ネットワークへの接続に使用する Modular LAN on Motherboard（mLOM）カードが付属しています。
- ND-NODE-G5S サーバーには、「PCIe-Riser-01」スロットに 4 ポートの VIC1455 カードが含まれており (上の図を参照)、Nexus Dashboard のデータ ネットワーク接続に使用します。
- ND-NODE-G5S サーバーには、2x10GbE NIC (APIC-P-ID10GC) または 2x25/10GbE SFP28 NIC（APIC-P-I8D25GF）、または「PCIe-Riser-01」スロット（上の図に表示）の VIC1455 カードに含まれており、Cisco Nexus Dashboard のデータ ネットワーク接続に使用します。
- ND-NODE-G5S には、Nexus Dashboard データ ネットワーク接続に使用する「PCIe-Riser-01」スロット (上図参照) に UCSC-P-V5Q50G-D (Cisco UCS VIC 15425 Quad Port 10/25/50G CNA) PCIE カードが含まれています。

ノードを管理ネットワークおよびデータ ネットワークに接続する場合：

- インターフェイスは、アクティブ/スタンバイ モードで実行されている、データ インターフェイス用（bond0）と管理インターフェイス用（bond1）の Linux ボンドとして設定されます。
- **管理ネットワーク接続**：
  - mLOM カードで `mgmt0` および `mgmt1` を使用する必要があります。
  - すべてのポートが同じ速度（1G または 10G）である必要があります。
- **データ ネットワーク接続**：
  - `SE-NODE-G2` サーバーでは、VIC1455 カードを使用する必要があります。
  - `ND-NODE-L4` サーバーで、2x10GbE NIC (`APIC-P-ID10GC`)、または 2x25/10GbE SFP28 NIC (`APIC-P-I8D25GF`)、または VIC1455 カードを使用できます。

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

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

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

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

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

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

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

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

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

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

物理アプライアンスとしての Nexus Dashboard の展開

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

始める前に

物理アプライアンスとして Nexus Dashboard を展開する場合の前提条件と注意事項 （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 4.1.1
Press Enter to manually bootstrap your first master node...
```

c) `admin` パスワードを入力して確認します。

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

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

d) 管理ネットワーク情報を入力します。

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

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

e) 入力した譲歩をレビューし、確認します。

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

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

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

ステップ 2 プロセスが完了するまで待ちます。

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

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

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

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

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

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

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

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

クラスタ名は、 RFC-1123 の要件に従う必要があります。

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

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

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

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

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

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

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

- **キー**：NTP 認証キーを入力します。Nexus Dashboard と NTP サーバ間の NTP トラフィックを認証するために使用される暗号キーです。次の手順で NTP サーバーを定義します。複数の NTP サーバーで同じ NTP 認証キーを使用できます。
- **ID**： NTP ホストのキー ID を入力します。各 NTP キーに一意のキー ID を割り当てる必要があります。この ID は、NTP パケットの検証時に使用する適切なキーを識別するために使用されます。
- **認証タイプ**：NTPキーの認証タイプを選択します。

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

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

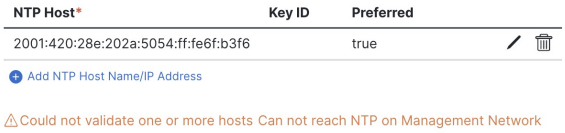
追加のNTPキーを入力する場合は、 **[+ キーの追加（+ Add Key）]** を再度クリックして、情報を入力します。

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

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

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

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



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

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

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

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

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

プロキシ サーバーでは、次の URL が有効になっている必要があります：

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

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

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

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

詳細設定では、次の設定を行うことができます。

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

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

j) [次へ（Next）] をクリックします。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

g) **[Save]**をクリックして、変更内容を保存します。

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

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

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

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

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

c) **[名前]**に、ノードの名前を入力します。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

h) **[Save]**をクリックして、変更内容を保存します。

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

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

（注）

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

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

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

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

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

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

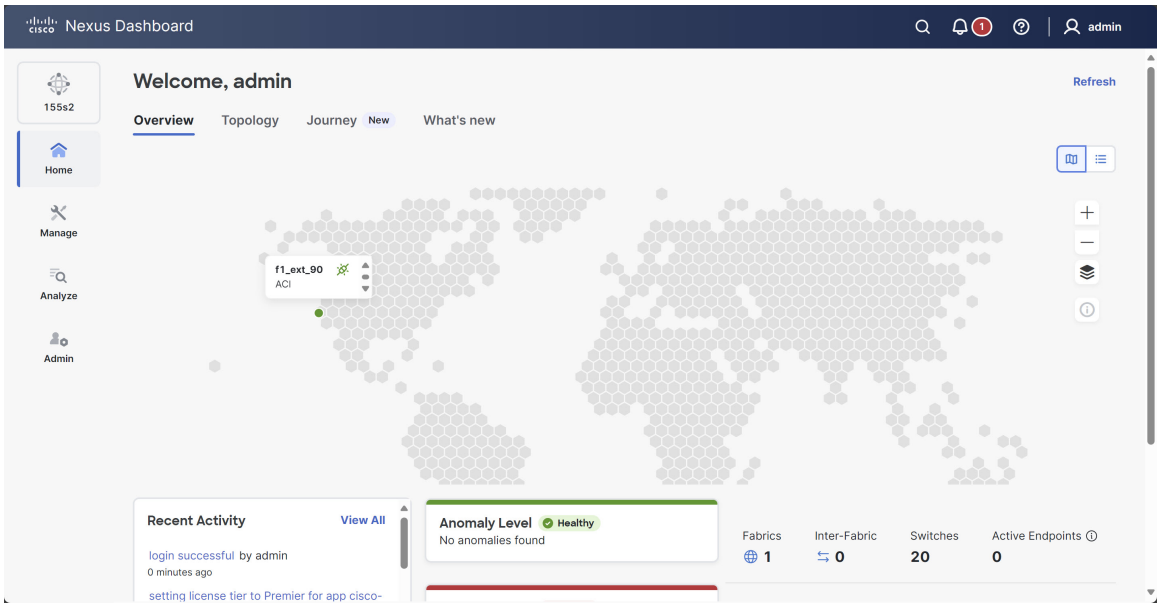
ノードのブート ストラップとクラスタの起動中に、全体的な進捗状況と各ノードの個々の進捗状況がUIに表示されます。ブートストラップの進行状況が表示されない場合は、ブラウザでページを手動で更新し、ステータスを更新してください。

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

ステップ 12 クラスタが健全であることを検証します。

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

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



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

- クラスタが収束している間、次の出力が表示されることがあります：

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

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

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

- クラスタが稼働している場合は、次の出力が表示されます。

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

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

```
deploy base system services
```

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

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

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

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

次のタスク

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

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。