Cisco Nexus ダッシュボード展開ガイド、リリース 2.3.x

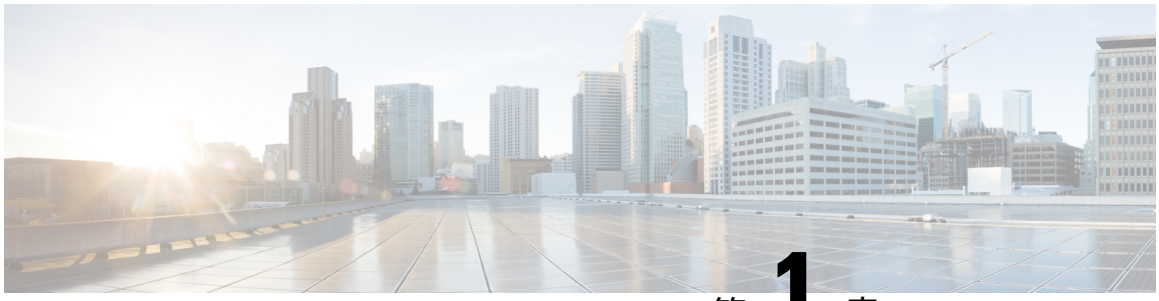
初版：2023 年 1 月 31 日

最終更新：2023 年 3 月 22 日

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

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

目 次



第 1 章

新機能および変更された機能に関する情報

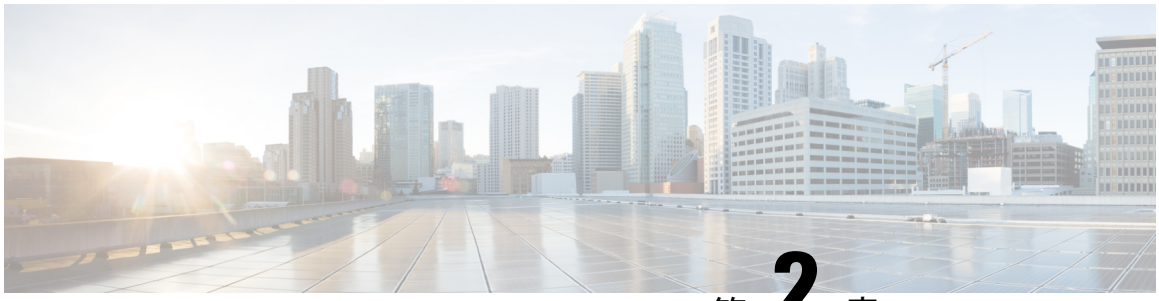
新機能および変更された機能に関する情報

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

表 *1* : 最新のアップデート

リリース	新機能またはアップデート	参照先
2.3(1)	このドキュメントの最初のリリース。	--

新機能および変更された機能に関する情報



第 2 章

展開の概要と要件

デプロイ概要

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

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

Nexus Dashboard クラスタは通常、1 つまたは 3 つのマスターノードで構成されます。また、3 ノードクラスタの場合、マスターノードで障害が発生した際に簡単にクラスタを回復させられるよう、いくつかのワーカーノードをプロビジョニングして、水平スケーリングやスタンバイノードを有効化できます。このリリースでサポートされるワーカー ノードとスタンバイ ノードの最大数については、Cisco Nexus ダッシュボード リリース ノートの「検証済みのスケーラビリティ制限」セクションを参照してください。

（注） このドキュメントでは、ベースクラスタの初期設定について説明します。クラスタが稼働したら、『*Cisco Nexus Dashboard User Guide*』の説明に従って追加ノードを設定して展開できます。このガイドは、Nexus Dashboard GUI から直接入手することもできます。

ハードウェアとソフトウェアのスタック

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

このガイドでは、Nexusダッシュボードソフトウェアの初期導入について説明します。ハードウェアのセットアップについては『*Nexus Dashboard Hardware Setup Guide*』で説明しています。その他の Nexus ダッシュボードの操作手順については、『*Cisco Nexus Dashboard User Guide*』を参照してください。

[サービス（Services）]

Nexus ダッシュボードは、一貫した統一された方法ですべての Nexusダッシュボード製品を使用できるようにするサービスを構築および展開するための標準のアプライアンスプラットフォームです。Insights、Orchestrator、Fabric Controller、Data Broker などのサービスをサブスクライブして使用するには、Nexusダッシュボードプラットフォームを使用して、これらのサービスに必要な容量とライフサイクル管理操作を提供します。

通常、Nexusダッシュボードプラットフォームには、これらのサービスのライフサイクルを管理するために必要なソフトウェアのみが同梱されていますが、実際のサービスはアプライアンスにパッケージ化されていません。データ センターからのパブリック ネットワーク接続を許可している場合は、数回クリックするだけでサービスをダウンロードしてインストールできます。ただし、パブリック ネットワークに接続していない場合は、これらのサービスを手動でダウンロードしてプラットフォームにアップロードし、インストール操作を実行してから使用する必要があります。

物理的な Nexus Dashboard サーバーを購入する場合、一部のサービスを、出荷前にハードウェアに事前インストールすることを選択できます。詳細については、『*Nexus ダッシュボードの注文ガイド*』を参照してください。Nexusダッシュボードの仮想またはクラウドフォームファクターを展開している場合、クラスタの準備が整った後にサービスを個別に展開する必要があることに注意してください。

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を混在させることはサポートされていません。

（注） すべてのサービスがすべてのフォームファクタでサポートされているわけではありません。展開を計画するときは、フォームファクタとクラスタサイズの要件についてCisco Nexus Dashboard クラスタのサイズ設定を確認してください。

- Cisco Nexus ダッシュボード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状態で購入した元の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。元の Cisco Nexus ダッシュボードプラットフォーム ハードウェアのセットアップについては、『*Cisco Nexus Dashboard Hardware Setup Guide*』を参照してください。

- VMware ESX (.ova)

  3つのVMware ESX仮想マシンを使用してNexusダッシュボードクラスタを展開できる仮想フォームファクタ。

- Linux KVM（.qcow2）

  3つのLinux KVM仮想マシンを使用してNexusダッシュボードクラスタを展開できる仮想フォームファクタ。

- Amazon Web Services (.ami)

  3つのAWSインスタンスを使用してNexusダッシュボードクラスタを展開できるクラウドフォームファクタ。

- Microsoft Azure (.arm)

  3 つの Azure インスタンスを使用して Nexus ダッシュボード クラスタを展開できるクラウド フォーム ファクタ。

- 既存のRed Hat Enterprise Linux(RHEL)システムの場合

  リリース2.2(1)以降、既存のRed Hat Enterprise Linuxサーバーで Nexus Dashboardノードを実行できます。

クラスタのサイジングと可用性の注意事項

前述のように、Nexus Dashboard クラスタは、最初に 1 つまたは 3 つのマスター ノードを使用してデプロイされます。実行するサービスの種類と数によっては、クラスタに追加のワーカー ノードを展開することが必要な場合があります。クラスタのサイジング情報と、特定の使用例に基づく推奨ノード数については、Cisco Nexus Dashboard Cluster Sizing ツールを参照してください。

（注）

- 単一ノードクラスタは、限られた数のサービスでサポートされており、最初の展開後に3ノードクラスタに拡張することはできません。
- 追加のワーカーノードをサポートするのは3ノードクラスタのみです。
- 単一ノードクラスターをデプロイし、それを3ノードクラスターに拡張するか、ワーカーノードを追加する場合は、基本の3ノードクラスターとして再デプロイする必要があります。
- 3ノードクラスタの場合、クラスタが動作し続けるには、少なくとも2つのマスターノードが必要です。2つのマスターノードに障害が発生した場合、*Cisco Nexus Dashboard* ユーザー ガイドの説明に従って回復するまで使用できません。

最初のクラスタが稼働したら、*Cisco Nexus* ダッシュボード ユーザー ガイドの説明に従って追加ノードを設定して展開できます。このガイドは、Nexusダッシュボード GUIから直接利用することもできます。

サポートされるサービス

サポートされるアプリケーションと関連する互換性および相互運用性情報の完全なリストについては、『Nexus ダッシュボードおよびサービスの互換性マトリクス』を参照してください。

前提条件とガイドライン

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

Nexus ダッシュボード 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。

（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。

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

Nexus ダッシュボード外部ネットワーク

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

Nexus ダッシュボードにインストールされた個々のサービスは、追加の目的で 2 つのネットワークを使用する場合があるため、展開計画については、このドキュメントに加えて特定のサービスのドキュメントを参照することを推奨します。

表 *2:* 外部ネットワークの目的

Data Network	管理ネットワーク
• Nexus Dashboardノードのクラスタリング • サービス間通信 • Cisco APIC、クラウド ネットワーク コントローラ、および NDFC 通信へのNexus Dashboard ノード たとえば、Nexus ダッシュボード Insights などのサービスのネットワーク トラフィックです。	• Nexus ダッシュボード GUI へのアクセス • SSH を介した Nexus ダッシュボード CLI へのアクセス • DNS および NTP 通信 • Nexus Dashboard ファームウェアのアップロード • Cisco DC App Center（AppStore）へのアクセス Nexus ダッシュボード App Store を使用してアプリケーションをインストールする場合は、https://dcappcenter.cisco.com は管理ネットワーク経由で到達可能である必要があります • Intersight デバイス コネクタ

2つのネットワークには次の要件があります。

- すべての新しい Nexus Dashboard 展開では、管理ネットワークとデータネットワークが異なるサブネットに存在する必要があります。
- 物理クラスタの場合、管理ネットワークは各ノードの CIMI に対して、TCP ポート 22/443 を介して IP 到達可能性を提供する必要があります。

  Nexus Dashboardのクラスタ設定では、各ノードのCIMC IPアドレスを使用してノードを設定します。
- Nexus ダッシュボード Insights サービスの場合、データ ネットワークは、各ファブリックおよび APIC のインバンド ネットワークに IP 到達可能性を提供する必要があります。
- Nexus Dashboard InsightsとAppDynamicsの統合では、データネットワークがAppDynamicsコントローラにIP到達可能性を提供する必要があります。

- Nexus Dashboard Orchestrator サービスの場合、データ ネットワークは、Cisco APIC サイトに対してインバンドおよび/またはアウトオブバンド IP 到達可能性を持ちますが、Cisco NDFC サイトに対してはインバンド到達可能性が必要です。
- 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、高いMTUを設定できます。
- 次の表は、管理ネットワークとデータネットワークのサービス固有の要件をまとめたものです。

（注） 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。このセクションに記載されている要件に加えて、展開を計画している特定のサービスのリリースノートを参照してください。

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

永続的な IP 構成に関連する追加の要件と警告については、特定のサービスのドキュメントを参照することをお勧めします。

表 *3:* サービス固有のネットワーク要件

Nexus Dashboard サービス	管理インターフェイス	データ インターフェイス	永続的 IP の総数
Nexus Dashboard Orchestrator	レイヤ 3 隣接	レイヤ 3 隣接	なし
SFLOW/NetFlow のない Nexus Dashboard Insights（ACI ファブリック）	レイヤ 3 隣接	レイヤ 3 隣接	なし
SFLOW/NetFlow（NDFC ファブリック）のない Nexus Dashboard Insights	レイヤ 3 隣接	レイヤ 2 隣接	IPv4 を使用している場合、データ インターフェイス ネットワーク内の 6 つの IP IPv6 を使用している場合、データ インターフェイス ネットワーク内の 7 つの IP

Nexus Dashboard サービス	管理インターフェイス	データ インターフェイス	永続的 IP の総数
SFLOW/NetFlow（ACI または NDFC ファブリック）を使用した Nexus ダッシュボード Insights	レイヤ 3 隣接	レイヤ 2 隣接	データ インターフェイス ネットワーク内の 6 つの IP

Nexus Dashboard サービス	管理インターフェイス	データ インターフェイス	永続的 IP の総数
Nexus Dashboard ファブリック コントローラ、リリース 12.0(x)	レイヤ 2 隣接	レイヤ 2 隣接	

Nexus Dashboard サービス	管理インターフェイス	データ インターフェイス	永続的 IP の総数
			[**LAN デバイス管理の接続性（LAN Device Management Connectivity**）] が [管理（Management）]（デフォルト） に設定されている場合： • SNMP/Syslog および SCP サービス用の管理ネットワーク内の 2 つの IP • [**EPL**] が有効になっている場合、各ファブリックのデータネットワークに 1 つの追加 IP • [**メディア用の IP ファブリック（IP Fabric for Media**）] が有効になっている場合、テレメトリ用の管理ネットワークに 1 つの追加の IP [**LAN デバイス管理の接続性（LAN Device Management Connectivity**）] が [データ（Data）] に設定されている場合： • SNMP/Syslog および SCP サービス用のデータネットワーク内の 2 つの IP • [**EPL**] が有効になっている場

Nexus Dashboard サービス	管理インターフェイス	データ インターフェイス	永続的 IP の総数
			合、各ファブリックのデータネットワークに 1 つの追加 IP • [**メディア用の IP ファブリック（IP Fabric for Media**）] が有効になっている場合、テレメトリ用のデータネットワークに 1 つの追加の IP

Nexus Dashboard サービス	管理インターフェイス	データ インターフェイス	永続的 IP の総数
Nexus ダッシュボード ファブリック コントローラ、リリース 12.1.1 以降	レイヤ 2 またはレイヤ 3 隣接	レイヤ 2 またはレイヤ 3 隣接	

Nexus Dashboard サービス	管理インターフェイス	データ インターフェイス	永続的 IP の総数
			LAN 展開タイプで **[LAN デバイス管理の接続性（LAN Device Management Connectivity）]** が [管理（Management）]（デフォルト）に設定されたレイヤー 2 モードで動作している場合 • SNMP/Syslog および SCP サービス用の管理ネットワーク内の 2 つの IP • **[EPL]** が有効になっている場合、各ファブリックのデータネットワークに 1 つの追加 IP • **[メディア用の IP ファブリック（IP Fabric for Media）]** が有効になっている場合、テレメトリ用の管理ネットワークに 1 つの追加の IP LAN 展開タイプで **[LAN デバイス管理の接続性（LAN Device Management Connectivity）]** が [データ（Data）]（デフォルト）に設定されたレイヤー 2 モードで動作している場合

Nexus Dashboard サービス	管理インターフェイス	データ インターフェイス	永続的 IP の総数
			• SNMP/Syslog および SCP サービス用のデータ ネットワーク内の 2 つの IP • [**EPL**] が有効になっている場合、各ファブリックのデータ ネットワークに 1 つの追加 IP • [**メディア用の IP ファブリック（IP Fabric for Media**）] が有効になっている場合、テレメトリ用のデータネットワークに 1 つの追加の IP LAN 展開タイプのレイヤ 3 モードで動作している場合：

Nexus Dashboard サービス	管理インターフェイス	データ インターフェイス	永続的 IP の総数
			• [**LAN デバイス管理の接続性（LAN Device Management Connectivity**）] が [データ（Data）] に設定されている必要があります • SNMP/Syslog および SCP サービス用の 2 つの IP • [**EPL**] が有効になっている場合、各ファブリックのデータ ネットワークに 1 つの追加 IP • すべての永続的 IP は、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別のプールの一部である必要があります。 永続的 IP のレイヤ 3 モードの詳細については、ユーザー ガイドの「永続的 IP」のセクションを参照してください。 SAN コントローラ展開タイプのレイヤ 3 モードで動作している場合：

Nexus Dashboard サービス	管理インターフェイス	データ インターフェイス	永続的 IP の総数
			• SSH 用の 1 つの IP • SNMP/Syslog 用の 1 つの IP • SAN Insights 機能用の 1 つの IP メディア モードの IP ファブリックは、レイヤ 3 モードではサポートされていません。
Cisco Nexus Dashboard Data Broker	レイヤ 3 隣接	なし	なし

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

（注） Nexus ダッシュボード クラスタとサービスを展開する場合は、常に最も低い RTT 要件を使用する必要があります。例えば、Insights とオーケストレータ サービスを共同ホストする場合、サイト接続性 RTT は 50ms を超えないようにします。

表 *4 : RTT* 要件

サービス	接続	最大 RTT
Nexus Dashboardクラスタ	ノード間	150 ミリ秒
Nexus Dashboard Orchestrator	ノード間	150 ミリ秒
	サイトへ	APIC サイトの場合：500 ミリ秒 NDFC サイトの場合：150 ミリ秒
Nexus Dashboard Insights	ノード間	50 ミリ秒
	スイッチ	50 ミリ秒

サービス	接続	最大 RTT
Nexusダッシュボード ファブリック コントローラ	ノード間	50 ミリ秒
	スイッチ	50 ミリ秒
Cisco Nexus Dashboard Data Broker	ノード間	150 ミリ秒
	スイッチ	500 ミリ秒

Nexus ダッシュボードの内部ネットワーク

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

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

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

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

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

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

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

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

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

BGP 構成と永続的な IP

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

リリース 2.2(1) 以降、異なるレイヤ 3 ネットワークにクラスタノードを展開する場合でも、永続的な IP 機能がサポートされます。この場合、永続的な IP は、「レイヤー 3 モード」と呼ばれる BGP を介して各ノードのデータリンクからアドバタイズされます。また、IP は、ノードの管理サブネットまたはデータサブネットと重複していないサブネットの一部である必要があります。永続IPがデータネットワークおよび管理ネットワークの外部にある場合、この機能はデフォルトでレイヤ3モードで動作します。IPがそれらのネットワークの一部である場合、機能はレイヤ 2 モードで動作します。

BGP は、クラスタの展開中、またはクラスタの稼働後に Nexus ダッシュボード GUI から有効にすることができます。

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

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

通信ポート

次のセクションでは、Nexus Dashboard クラスタとサービスに必要なポートのリファレンスを示します。

（注） すべてのサービスは、暗号化を備えた TLS または mTLS を使用して、ネットワーク上のデータのプライバシーと完全性を保護します。

Nexus Dashboard ポート

Nexus Dashboard クラスタには、次のポートが必要です。

表 *5 : Nexus Dashboard* ポート（管理ネットワーク）

サービス	ポート	プロトコル	方向 イン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	接続
ICMP	ICMP	ICMP	入力 / 出力	他のクラスタ ノード、CIMC、デフォルト ゲートウェイ
SSH	22	TCP	入力 / 出力	クラスタ ノードの CLI および CIMC
TACACS	49	TCP	発信	TACACS サーバー
DNS	53	TCP/UDP	アウト	DNS サーバ
HTTP	80	TCP	発信	インターネット/プロキシ
NTP	123	UDP	発信	NTP サーバー
HTTPS	443	TCP	入力 / 出力	UI、他のクラスタ (マルチクラスタ接続用)、ファブリック、インターネット/プロキシ
LDAP	389 636	TCP	発信	LDAP サーバ
RADIUS	1812	TCP	発信	Radius サーバー
KMS	9880	TCP	入力 / 出力	その他クラスタ ノードおよび ACI ファブリック
インフラ サービス	30012 30021 30500 ～ 30600	TCP および UDP	入力 / 出力	その他のクラスタ ノード

表 *6 : Nexus Dashboard* ポート（データ ネットワーク）

サービス	ポート	プロトコル	方向 ィン：クラスタに対して ァウト：クラスタからファブリックまたは世界外に対して	接続
ICMP	ICMP	ICMP	入力 / 出力	他のクラスタ ノード、CIMC、デフォルト ゲートウェイ
SSH	22	TCP	発信	スイッチと APIC の帯域内
DNS	53	TCP および UDP	入力 / 出力	他のクラスタノードと DNS サーバー
HTTPS	443	TCP	発信	スイッチと APIC の帯域内
SSH	1022	TCP および UDP	入力 / 出力	その他のクラスタ ノード
VXLAN	4789	UDP	入力 / 出力	その他のクラスタ ノード
KMS	9880	TCP	入力 / 出力	その他クラスタ ノードおよびACI ファブリック

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

Nexus Dashboard Insights ポート

上記の Nexus Dashboard クラスタ ノードに必要なポートに加えて、Nexus Dashboard Insights サービスには次のポートが必要です。

表 *7 : Nexus Dashboard Insights* ポート（データ ネットワーク）

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

Nexus Dashboard Fabric Controller ポート

Nexus Dashboard（ND）クラスタ ノードに必要なポートに加えて、Nexus Dashboard Fabric Controller（NDFC）サービスには次のポートが必要です。

（注） 次のポートは、NDFC サービスからスイッチへの IP 到達可能性を提供するインターフェイスに応じて、Nexus Dashboard 管理ネットワークおよび/またはデータ ネットワーク インターフェイスに適用されます。

表 *8 : Nexus Dashboard Fabric Controller* ポート

サービス	ポート	プロトコル	方向 イン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	接続 （特に明記されていない限り、**LAN** と **SAN** の両方の展開に適用されます）
SSH	22	TCP	発信	SSH は、デバイスにアクセスするための基本的なメカニズムです。
SCP	22	TCP	発信	NDFC バックアップ ファイルをリモート サーバーにアーカイブする SCP クライアント。
SMTP	25	TCP	発信	SMTP ポートは、NDFC の [サーバー設定（Server Settings）] メニューから構成できます。 これはオプションの機能です。
DHCP	67	UDP	入力	NDFC ローカル DHCP サーバーがブートストラップ/POAP 用に構成されている場合。 これは、LAN 展開にのみ適用されます。 （注） POAP の目的でローカル DHCP サーバーとして NDFC を使用する場合、すべての ND マスター ノードの IP を DHCP リレーとして構成する必要があります。ND ノードの管理 IP またはデータ IP が DHCP サーバーにバインドされるかどうかは、NDFC サーバー設定の LAN デバイス管理接続によって決定されます。
DHCP	68	UDP	発信	
SNMP	161	TCP/UDP	アウト	NDFC からデバイスへの SNMP トラフィック。

サービス	ポート	プロトコル	方向 ィン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	接続 （特に明記されていない限り、**LAN** と **SAN** の両方の展開に適用されます）
HTTPS/HTTP（NX-API）	443/80	TCP	発信	NX-API HTTPS/HTTP クライアントは、構成可能でもあるポート 443/80 でデバイスの NX-API サーバーに接続します。NX-API はオプション機能であり、NDFC 機能の限られたセットで使用されます。 これは、LAN 展開にのみ適用されます。
HTTPS（vCenter、Kubernetes、OpenStack、Discovery）	443	TCP	発信	NDFC は、VMware vCenter や OpenStack などの登録済み VMM ドメインと、Kubernetes などのコンテナ オーケストレーターから取得した情報を関連付けることにより、統合されたホストおよび物理ネットワーク トポロジ ビューを提供します。 これはオプションの機能です。

（注） 次のポートは、一部の NDFC サービスで使用される永続的 IP とも呼ばれる外部サービス IP に適用されます。これらの外部サービス IP は、構成された設定に応じて、Nexus Dashboard の管理サブネット プールまたはデータ サブネット プールから取得される場合があります。

表 *9 : Nexus Dashboard Fabric Controller* 永続的 *IP* ポート

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

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

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

サービス	ポート	プロトコル	方向 ィン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	接続 （特に明記されていない限り、**LAN** と **SAN** の両方の展開に適用されます）
BGP	179	TCP	入力 / 出力	エンドポイント ロケーターの場合、有効になっているファブリックごとに、独自の永続的な IP を使用して EPL サービスが生成されます。このサービスは、常に Nexus Dashboard データ インターフェイスに関連付けられています。エンドポイント情報を追跡するために必要な BGP アップデートを取得するために、ファブリック上の適切な BGP エンティティ（通常は BGP ルート リフレクタ）と NDFC EPL サービスはピアを行います。 この機能は、VXLAN BGP EVPN ファブリックの展開にのみ適用されます。 これは、LAN 展開にのみ適用されます。
HTTPS（POAP）	443	TCP	入力	セキュア POAP は、ポート 443 の NDFC HTTPS サーバーを介して実現されます。HTTPS サーバーは SCP-POAP サービスにバインドされ、そのポッドに割り当てられたのと同じ永続的 IP を使用します。 NDFC の SCP-POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続的な IP があります。これは、NDFC サーバー設定の [LAN デバイス管理接続（LAN Device Management Connectivity）] 設定によって制御されます。 これは、LAN 展開にのみ適用されます。

サービス	ポート	プロトコル	方向 イン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	接続 （特に明記されていない限り、**LAN** と **SAN** の両方の展開に適用されます）
Syslog	514	UDP	入力	NDFC が Syslog サーバーとして構成されている場合、デバイスからの Syslog は、SNMP-Trap/Syslog サービス ポッドに関連付けられた永続的な IP に向けて送信されます。 NDFC の SNMP-Trap-Syslog サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続的な IP があります。これは、NDFC サーバー設定の [LAN デバイス管理接続（LAN Device Management Connectivity）] 設定によって制御されます。
SCP	2022	TCP	発信	NDFC POAP-SCP ポッドの永続的な IP から、Nexus Dashboard Insights を実行している別の ND クラスターにテクニカル サポート ファイルを転送します。 NDFC の SCP-POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続的な IP があります。これは、NDFC サーバー設定の LAN デバイス管理接続設定によって制御されます。

サービス	ポート	プロトコル	方向 ィン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	接続 （特に明記されていない限り、**LAN** と **SAN** の両方の展開に適用されます）
SNMP トラップ	2162	UDP	入力	デバイスから NDFC への SNMP トラップは、SNMP-Trap/Syslog サービス ポッドに関連付けられた永続的な IP に向けて送信されます。 NDFC の SNMP-Trap-Syslog サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続的な IP があります。これは、NDFC サーバー設定の [LAN デバイス管理接続（LAN Device Management Connectivity）] 設定によって制御されます。
GRPC（テレメトリ）	33000	TCP	入力	NDFC 永続的 IP に関連付けられた GRPC トランスポートを介して SAN データ (ストレージ、ホスト、フローなど) を受信する SAN Insights Telemetry サーバー。 これは、SAN 展開でのみ有効です。
GRPC（テレメトリ）	50051	TCP	入力	メディア展開用の IP ファブリックおよび一般的な LAN 展開用の PTP のマルチキャスト フローに関連する情報は、ソフトウェアテレメトリを介して、NDFC GRPC レシーバー サービス ポッドに関連付けられた永続的 IP にストリーミングされます。 これは、LAN およびメディア展開でのみ有効です。

SAN 展開向けの Nexus Dashboard Fabric Controller ポート

Nexus Dashboard Fabric Controller は、単一ノードまたは 3 ノードの Nexus Dashboard クラスタに導入できます。単一ノード クラスタでの NDFC SAN 展開には、次のポートが必要です。

表 *10 :* 単一ノード クラスタでの *SAN* 展開向けの *Nexus Dashboard Fabric Controller* ポート

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

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

（注） 次のポートは、一部の NDFC サービスで使用される、永続的 IP とも呼ばれる外部サービス IP に適用されます。これらの外部サービス IP は、構成された設定に応じて、Nexus Dashboard の管理サブネット プールまたはデータ サブネット プールから取得される場合があります。

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

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

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

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

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。

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。

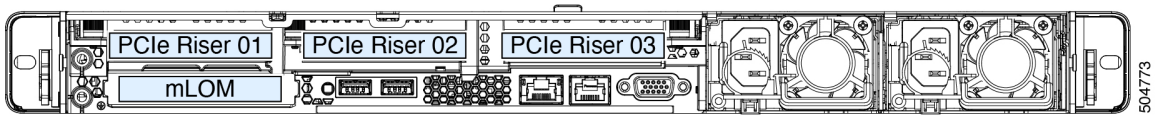
Cisco Cloud Network Controller ファブリックの場合は、レイヤ 3 ネットワーク経由で接続する必要があります。

物理ノードのケーブル接続

（注） 仮想またはクラウド フォーム ファクタ クラスタを展開する場合は、このセクションをスキップできます。

物理ノードは、次のネットワーク カードを使用して、UCS-C220-M5 および UCS-C225-M6 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、「`PCIe-Riser-01`」スロット（上の図に表示）に 2x10GbE NIC (`APIC-P-ID10GC`) または 2x25/10GbE SFP28 NIC（`APIC-P-I8D25GF`）が含まれており、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：

- 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。
- UCS-C220-M5 サーバーのデータ ネットワークでは、VIC1455 カードを使用する必要があります。
  - すべてのポートは、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。

- インターフェイスは、Nexus ダッシュボードの `fabric0` に対応するポート 1/ポート 2、および `fabric1` に対応するポート 3/ポート 4 を使用して Linux ボンドとして構成されます。

  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） インターフェイスの各ペアに対して許可される接続は 1 つだけです。たとえば、1 本のケーブルをポート 1 またはポート 2 **のいずれか**に接続し、別のケーブルをポート 3 またはポート 4 **のいずれか**に接続することができます。同じペアから両方のインターフェイスを接続しないでください。

- UCS-C220-M6 サーバーのデータ ネットワークの場合、2x10GbE NIC（`APIC-P-ID10GC`）または 2x25/10GbE SFP28 NIC（`APIC-P-I8D25GF`）を使用する必要があります。
  - 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。
  - Nexus Dashboard ノードとファブリックの間で 25G 接続を使用する場合は、銅線ケーブルを使用する必要があります。

    互換性のあるトランシーバ オプションのリストについては、*Cisco 25GBASE SFP28 モジュール データ シート* を参照してください。
  - 2 つのポートは、Nexus ダッシュボードの `fabric0` と `fabric1` にそれぞれ対応します。

    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。

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。すべてのインターフェイスは個々のホストポートに接続する必要があります。PortChannelおよびvPCはサポートされていません。

Nexus ダッシュボード ノードが 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。

外部レイヤ 3 ネットワークを介した接続

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

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

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

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

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

  ACI ファブリックでの外部接続の設定については、『Cisco APIC Layer 3 Networking Configuration Guide』を参照してください。
- NDFC ファブリックの場合、データインターフェイスと NDFC のインバンドインターフェイスが異なるサブネットにある場合は、Nexus ダッシュボードのデータネットワークアドレスに到達するためのルートを NDFC で追加する必要があります。

  NDFC UI からルートを追加するには、**[管理者（Administration）]** > **[カスタマイズ（Customization）]** > **[ネットワーク設定（Network Preference）]** > **[インバンド（In-Band）（eth2）]**に移動し、ルートを追加して保存します。
- クラスタのセットアップ中にデータ インターフェイスの VLAN ID を指定する場合、その VLANを許可するトランクとしてホスト ポートを設定する必要があります。

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

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

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

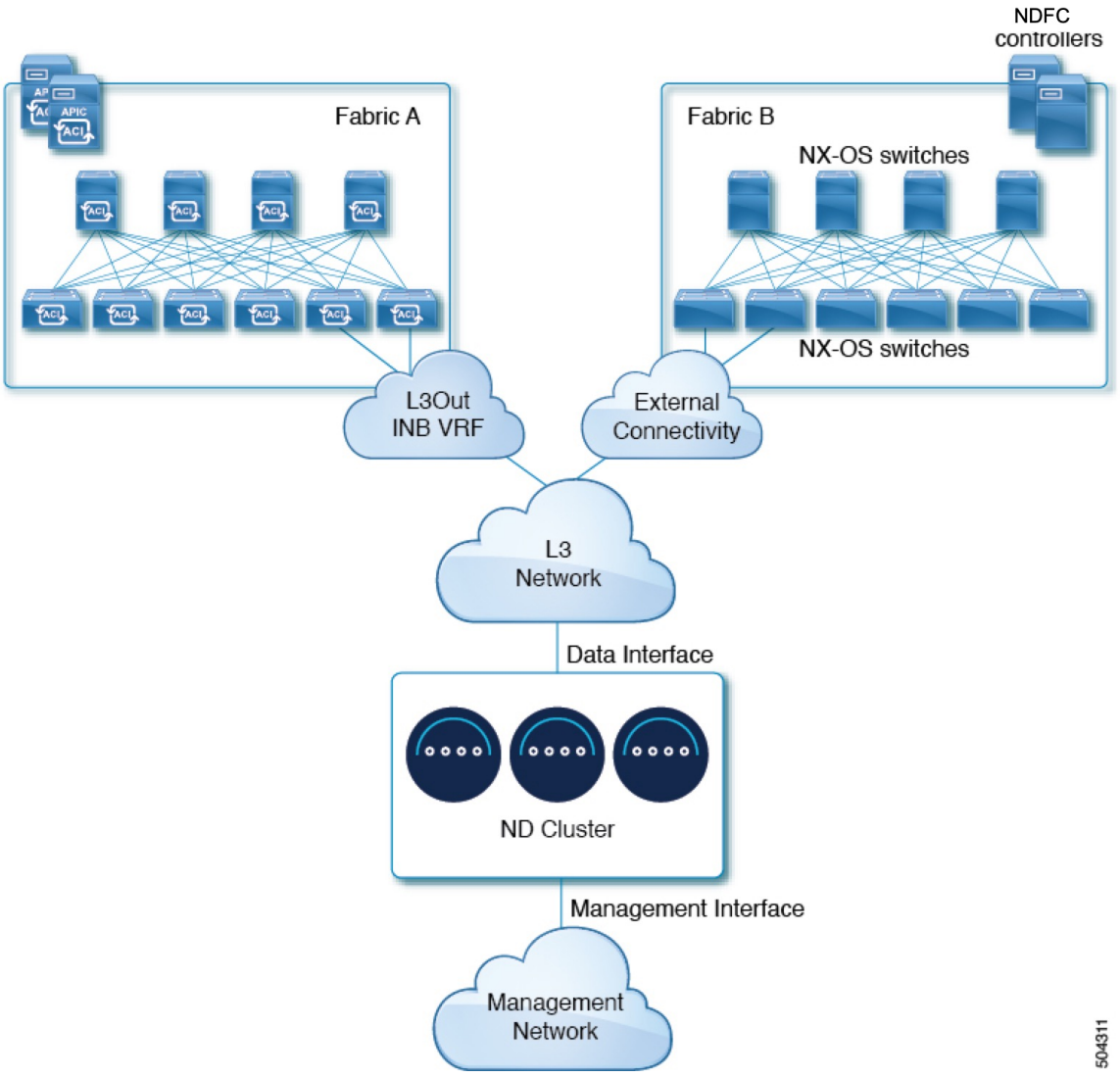
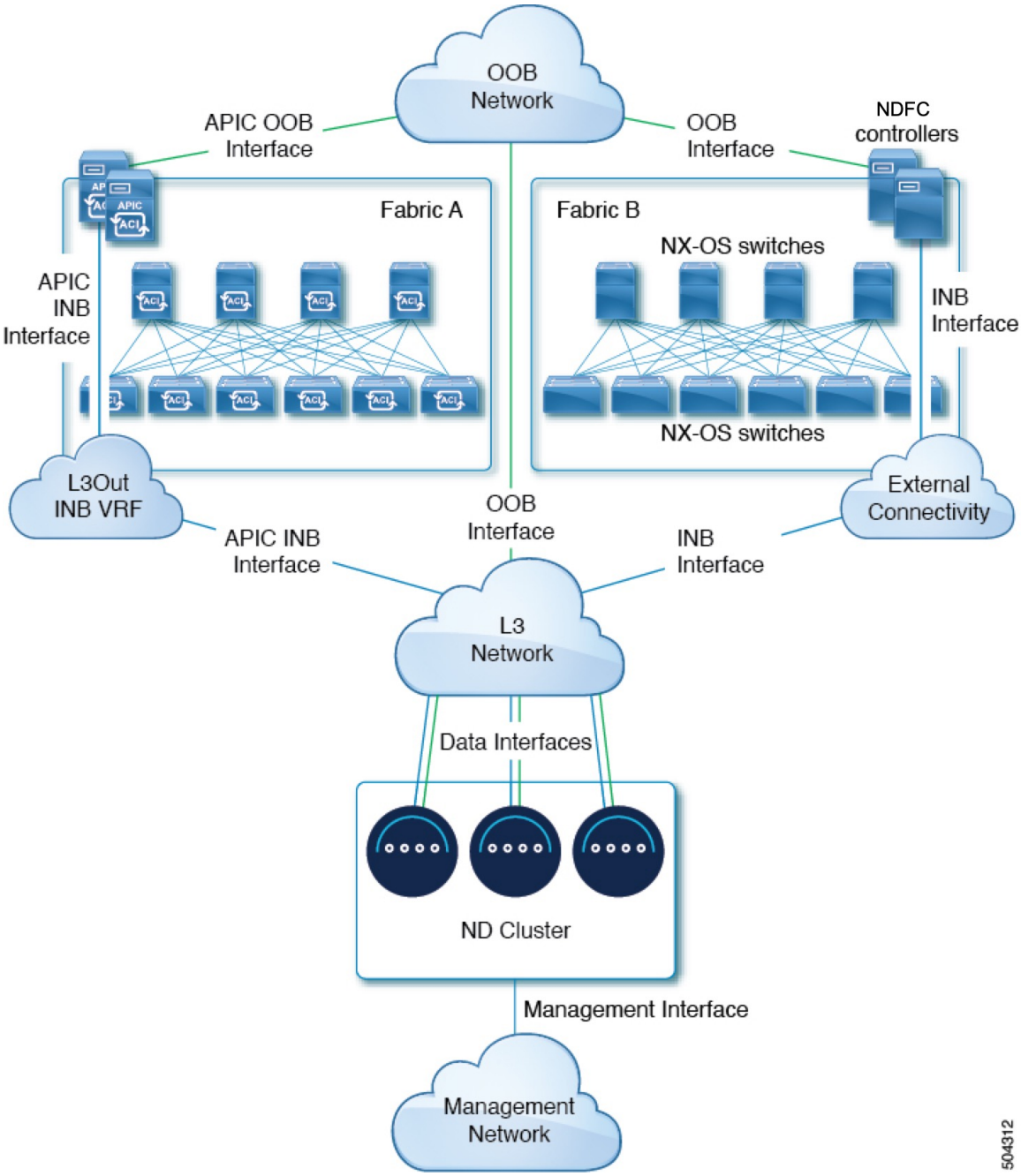


図 *3 :* レイヤ*3*ネットワーク、*Nexus Dashboard Orchestrator*を介した接続



リーフ スイッチへのノードの直接接続

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

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

- Cisco ACIファブリックのみを管理するためにNexus Dashboard Orchestratorを展開する場合は、データインターフェイスから各サイトの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。
- Nexus ダッシュボード Insights を展開する場合は、データインターフェイスから各ファブリックのインバンドインターフェイスへの接続を確立する必要があります。

  ACIファブリックの場合、データインターフェイスIPサブネットはファブリック内のEPG / BDに接続し、管理テナントのローカルインバンドEPGに対して確立されたコントラクトが必要です。Nexusダッシュボードは、管理テナントおよびインバンドVRFに導入することを推奨します。他のファブリックへの接続は、L3Out経由で確立されます。
- ACIファブリックを使用してNexus Dashboard Insightsを展開する場合は、データインターフェイスのIPアドレスとACIファブリックのインバンドIPアドレスは、異なるサブネット内にある必要があります。

クラスタをリーフスイッチに直接接続する場合は、次の点に注意してください。

- VMware ESX または Linux KVM で展開する場合、ホストはトランク ポート経由でファブリックに接続する必要があります。
- クラスタのセットアップ中にデータ ネットワークの VLAN ID を指定する場合は、Nexus ダッシュボード インターフェイスと接続されたネットワークデバイスのポートをトランクとして設定する必要があります。

  ただし、ほとんどの場合、VLAN をデータ ネットワークに割り当てないことを推奨します。この場合、ポートをアクセス モードで設定する必要があります。
- ACI ファブリックの場合：
  - 管理テナントのCisco Nexus Dashboard接続用にブリッジドメイン(BD)、サブネット、およびエンドポイントグループ(EPG)を設定することを推奨します。

    Nexus Dashboardはインバンドvrfのインバンドepgへの接続を必要とするため、管理テナントでEPGを作成すると、ルートリークが不要になります。
  - ファブリックのインバンド管理 EPG と Cisco Nexus ダッシュボード EPG 間のコントラクトを作成する必要があります。
  - 複数のファブリックが Nexus ダッシュボード クラスタのアプリケーションでモニタされている場合、デフォルトルートまたは他の ACI ファブリックインバンド EPG への特定のルートを持つ L3Out をプロビジョニングし、クラスタ EPG と L3Out の外部 EPG の間でコントラクトを確立する必要があります。

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

図 *4 :* リーフ スイッチへの直接接続、*2* 日目の運用アプリケーション

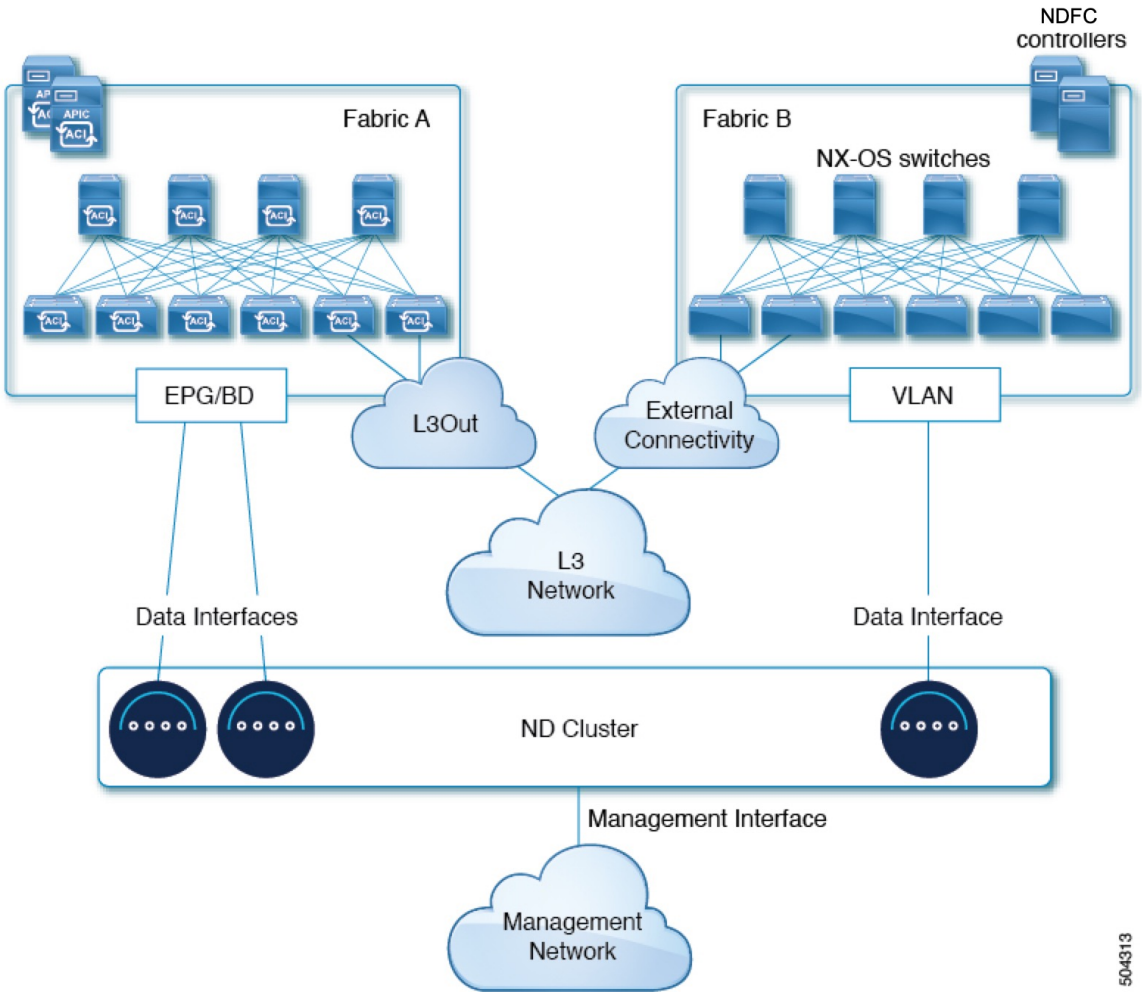
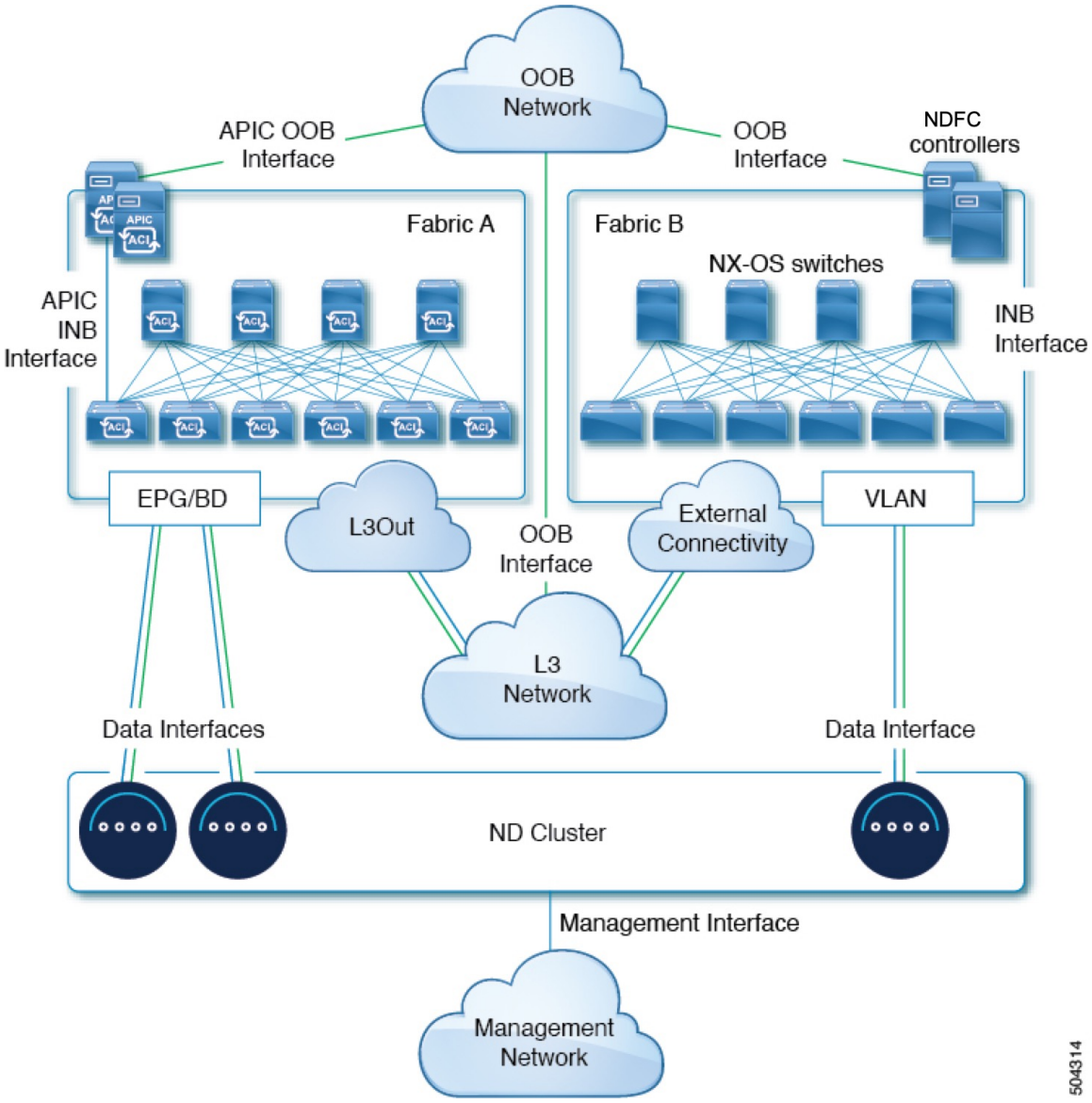


図 *5:* リーフ スイッチ、*Nexus* ダッシュボード オーケストレータへの直接接続



サイト間のノード分散

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

（注） 次のセクションのこのダイアグラムは、物理または仮想の Nexus Dashboard クラスター ノードで考えられる展開シナリオのいくつか例を示しています。特定のユース ケースに必要な正確なノード数の詳細については、Nexus Dashboard キャパシティ プランニング ツールを参照してください。

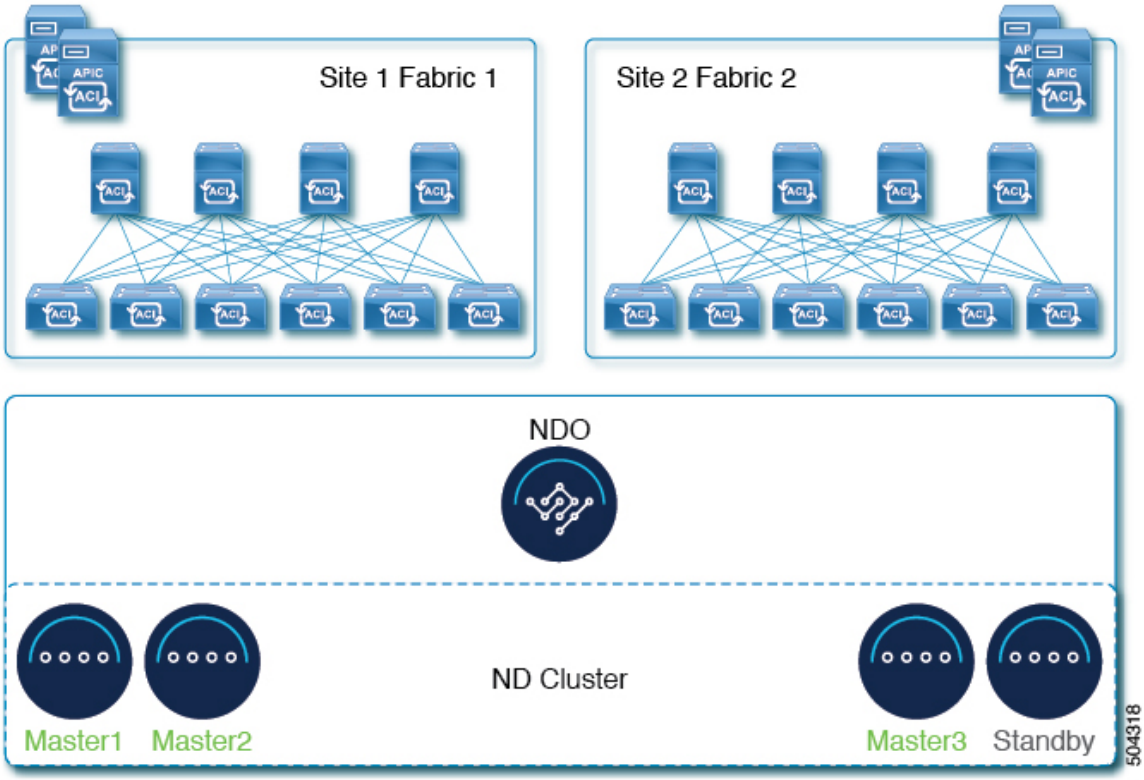
Nexus Dashboard Insights のノード配布

Nexus Dashboard Insights サービスには、一元化された単一サイトの展開をお勧めします。このサービスは、ノードが異なるサイトにある場合に、クラスタを相互接続障害にさらす可能性がある分散クラスタの冗長性の利点を得ることができません。

Nexus Dashboard Orchestrator のノードの分散

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

図 *6 : Nexus* ダッシュボード オーケストレータの *2* つのサイトにまたがるノードの分散



ファブリック コントローラのノード分散

Nexus Dashboard ファブリック コントローラの場合、複数のサイトがある場合は、集中型の単一サイト クラスタまたは分散クラスタのいずれかを展開できます。クラスタが動作し続けるには、少なくとも 2 つの Nexus Dashboard マスター ノードが必要であるため、Nexus Dashboard クラスタを 2 つのサイトに展開する場合は、次の図に示すように、1 つのマスター ノードを持つサイトにスタンバイ ノードを展開することを推奨します。

（注） 集中型の単一サイト クラスタの場合、スタンバイ ノードなしでデプロイできます。ただし、分散クラスタの場合は、マスター ノードが最も少ないサイトにスタンバイ ノードを追加することをお勧めします。

次の図は、NDFC サービスを備えた物理（4 ノード）または仮想（4 ノードまたは 6 ノード）の Nexus Dashboard クラスタの可能な展開シナリオの 2 つの例を示しています。特定のユースケースに必要な正確なノード数の詳細については、Nexus Dashboard キャパシティ プランニング ツールを参照してください。

図 *7: Nexus Dashboard* ファブリック コントローラの *2* つのサイトにまたがるノードの分散（*4* ノード クラスタ）

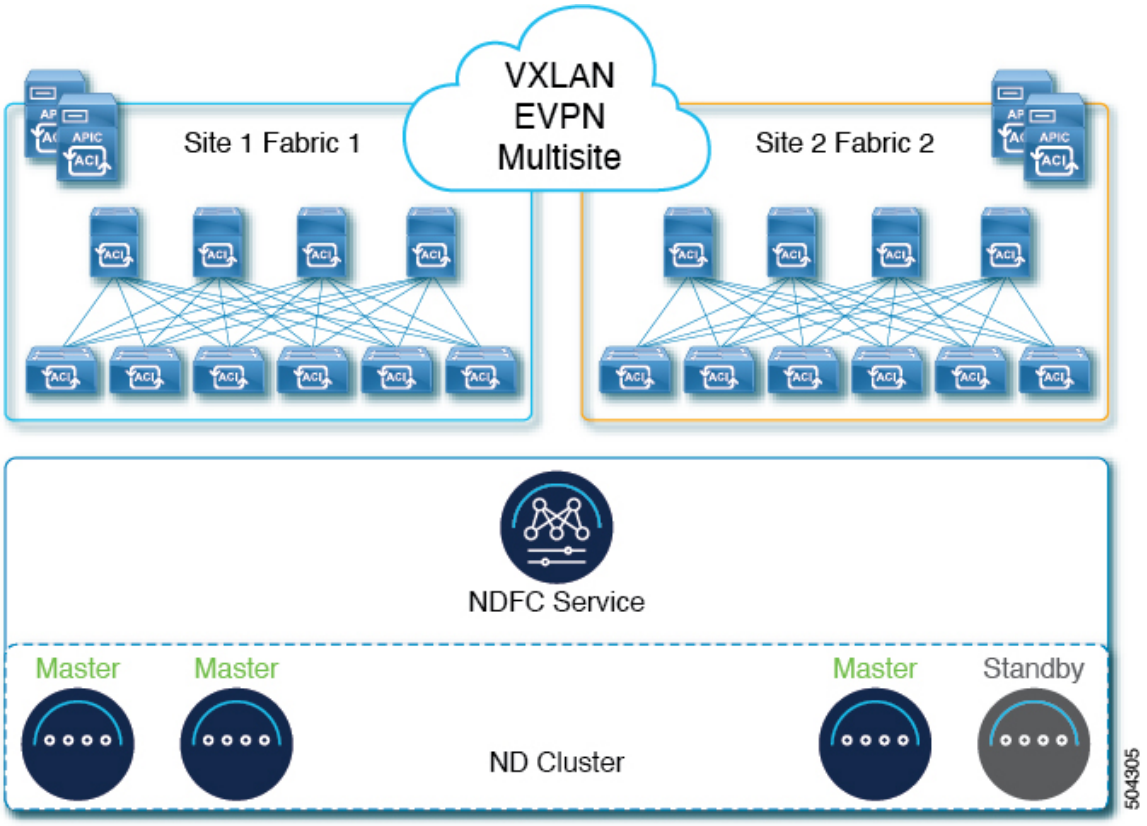
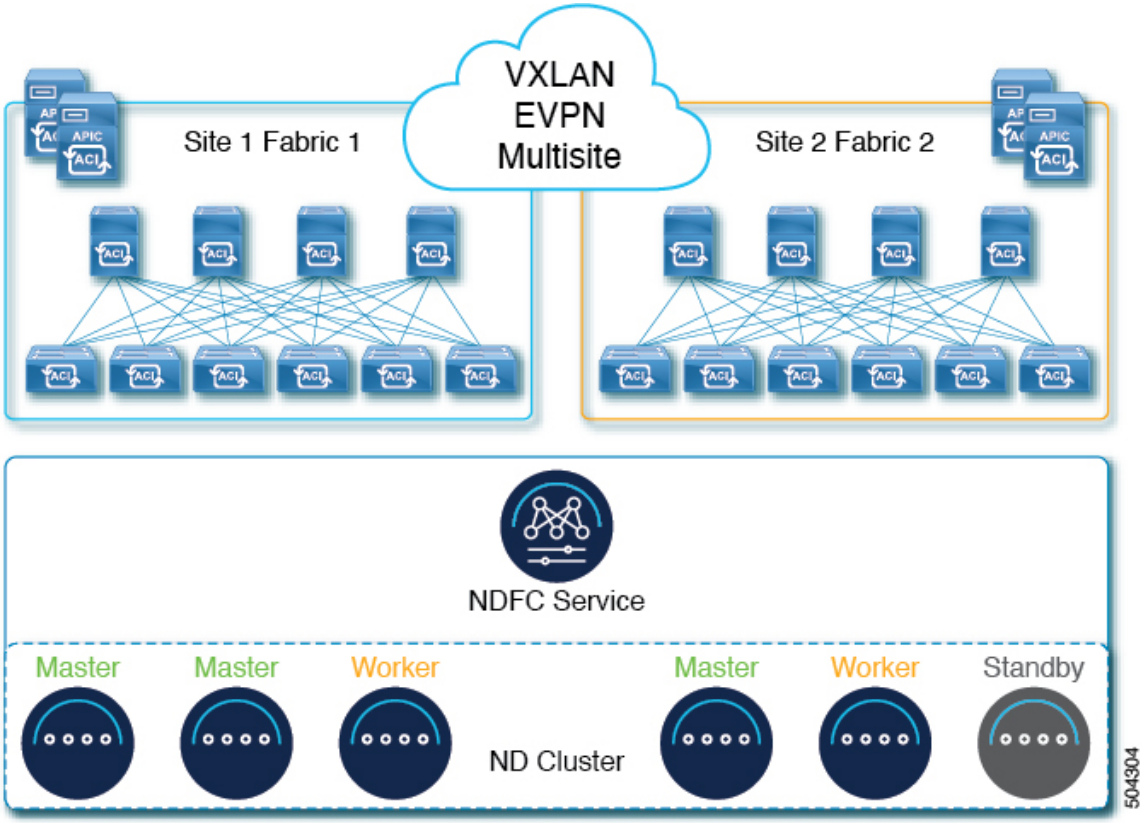


図 *8 : Nexus Dashboard* ファブリック コントローラの *2* つのサイトにまたがるノードの分散（*6* ノード クラスタ）



サイト間の Nexus ダッシュボード ノードの分散

次の表に、複数のサイトにまたがる物理的な Nexus ダッシュボード マスター（M1、M2、M3）およびスタンバイ（S1）ノードの分散でサポートされる追加のシナリオをまとめます。

表 *12 :* サイト間の *Nexus* ダッシュボード ノードの分散

サイト数	サイト 1 のノード	サイト 2 のノード	サイト 3 のノード	サイト 4 のノード
1	M1、M2、M3、S1	--	--	--
2	M1、M2	M3、 S1	--	--
3	M1、S1* *スタンバイノードは 3 つのサイトのいずれか 1 つに追加可能	M2	M3	--
4	M1	M2	M3	S1

サービスのコロケーションの使用例

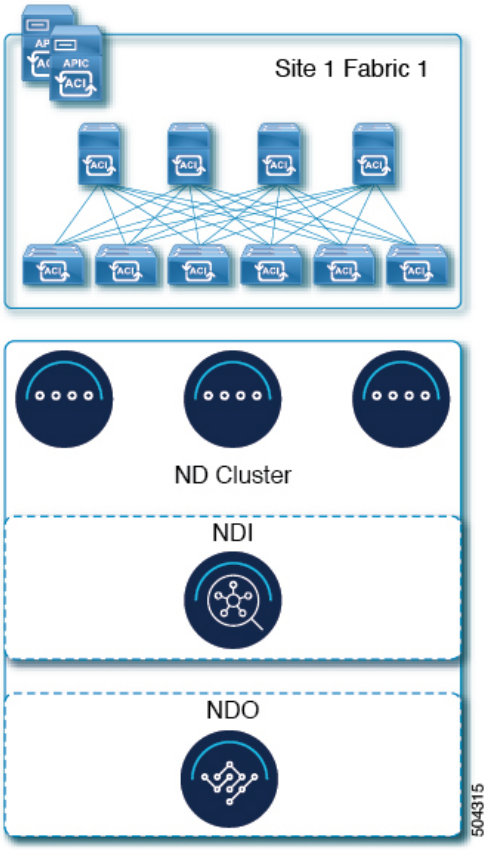
このセクションでは、特定の単一サービスまたは複数サービスの共同ホストの使用例について、いくつかの推奨される展開シナリオについて説明します。

（注） このリリースは、Linux KVM、AWS、Azure、または RHEL に展開されている Nexus ダッシュボードクラスタでの共同ホスティングサービスをサポートしていません。以下のすべてのサービス共同ホスティングのシナリオは、物理フォームファクタまたは VMware ESX クラスタフォームファクタに適用されます。

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

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

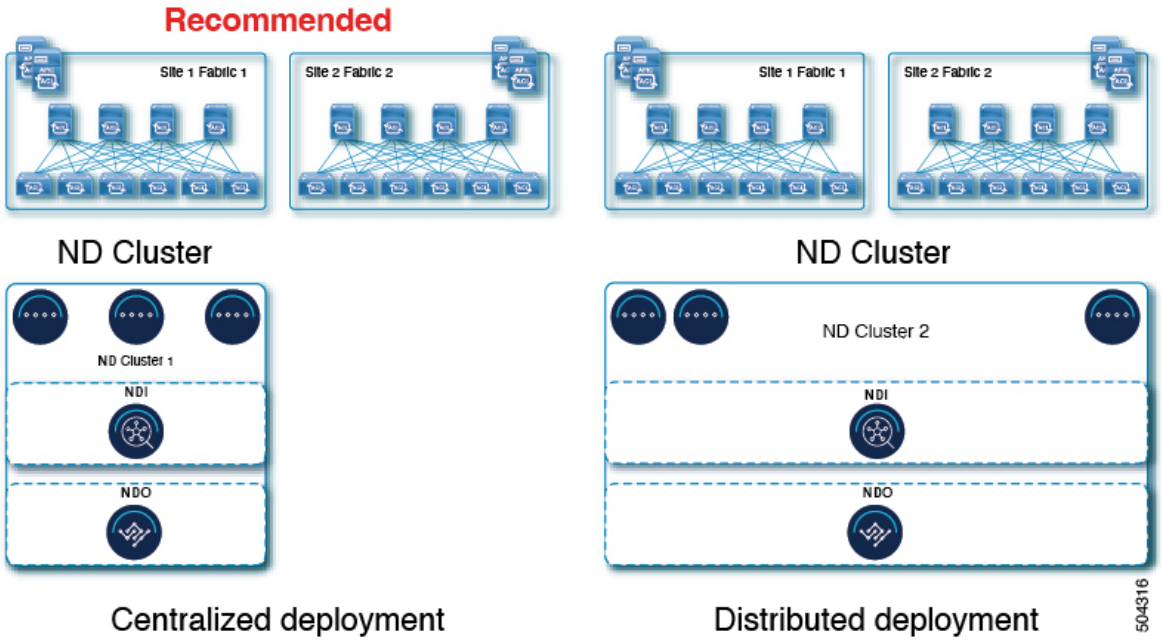
図 *9*: 単一サイト、*Nexus* ダッシュボード *Insights* およびオーケストレータ



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

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

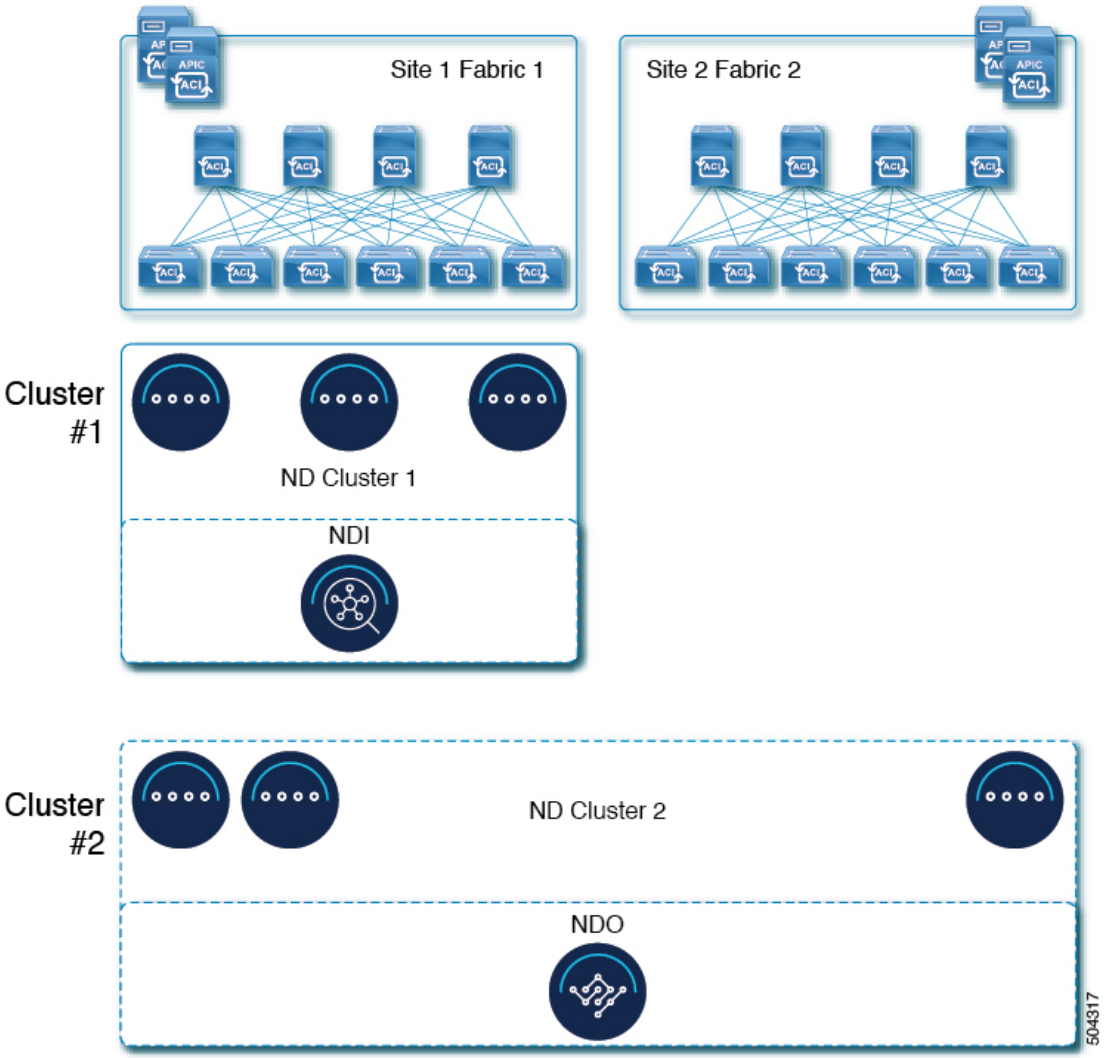
図 *10 : Nexus* ダッシュボード *Insights* およびオーケストレータの複数サイト、単一クラスタ



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

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

図 *11 : Nexus* ダッシュボード *Insights* およびオーケストレータの複数のサイト、複数のクラスタ



インストール前のチェックリスト

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

表 *13 :* クラスタの詳細

パラメータ（Parameters）	例	入力する値
クラスタ名	nd-cluster	
NTP サーバー	171.68.38.65	

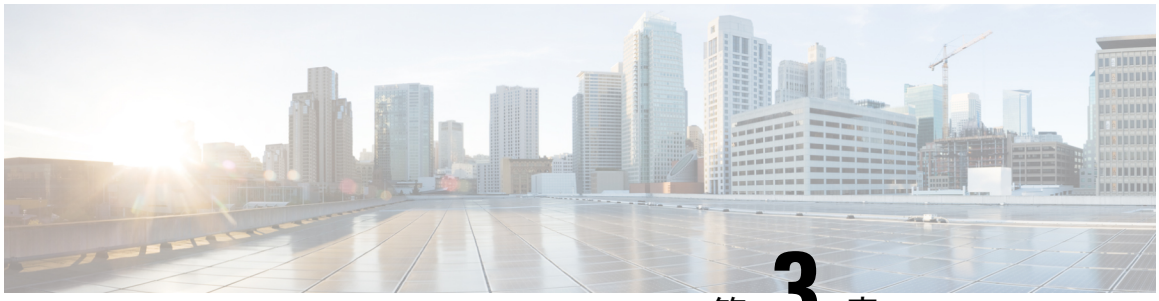
パラメータ（Parameters）	例	入力する値
DNS プロバイダー	64.102.6.247 171.70.168.183	
DNS 検索ドメイン	cisco.com	
アプリ ネットワーク	172.17.0.0/16	
サービスネットワーク	100.80.0.0/16	

表 *14 :* 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	10.195.219.84/24 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	10.195.219.85/24 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	10.195.219.86/24 ユーザ名: admin パスワード：Cisco1234	
各ノードのレスキュー ユーザに使用される**パスワード**と初期 GUIパスワード。 クラスタ内のすべてのノードに同じパスワードを設定することを推奨します。	Welcome2Cisco!	
最初のノードの **管理 IP**	192.168.9.172/24	
最初のノードの**管理ゲートウェイ**	192.168.9.1	
最初のノードの**データ ネットワーク IP**	192.168.6.172/24	
最初のノードの**データ ネットワーク ゲートウェイ**	192.168.6.1	
（オプション）最初のノードの**データ ネットワーク VLAN**	101	

パラメータ（**Parameters**）	例	入力する値
（オプション）最初のノードの **ASN**	63331	
（オプション）最初のノードの **BGP ピア**の IP アドレス	200.11.11.2 または 200:11:11::2	
（オプション）最初のノードの **BGP ピア**の ASN	55555	
2 番目のノードの**管理 IP**	192.168.9.173/24	
2 番目のノードの**管理ゲートウェイ**。	192.168.9.1	
2 番目のノードの**データ ネットワーク IP**	192.168.6.173/24	
2 番目のノードの**データ ネットワーク ゲートウェイ**	192.168.6.1	
（オプション）2番目のノードの**データ ネットワーク VLAN**	101	
（オプション）2番目のノードの **ASN**	63331	
（オプション）2番目のノードの **BGP ピア**の IP アドレス	200.12.12.2 または 200:12:12::2	
（オプション）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	

パラメータ（**Parameters**）	例	入力する値
（オプション）3番目のノードの **ASN**	63331	
（オプション）3番目のノードの **BGP ピア**の IP アドレス	200.13.13.2 または 200:13:13::2	
（オプション）3番目のノードの **BGP ピア**の ASN	55555	



第 3 章

物理アプライアンスとしての展開

前提条件とガイドライン

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。

- 展開の概要と要件 （3 ページ） に記載されている一般的な前提条件を確認して完了します。

  この文書は、ベースとなるNexusダッシュボードクラスタを最初に展開する方法について説明するものである点に留意してください。追加ノード（従業員またはスタンバイ）で既存のクラスタを拡張する場合は、『*Cisco Nexus* ダッシュボード ユーザ 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 ガイド』から利用できます。

  手動リカバリ用にレスキューユーザとしてログインできない場合など、サーバーを完全に再イメージ化する場合は、『Cisco Nexus ダッシュボード ユーザ ガイド』の「トラブルシューティング」の章を参照してください。

- 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。

- 『*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 および UCS-C225-M6 の元の Nexus ダッシュボード 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 *15* : サポートされる *UCS-C220-M5* ハードウェア

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

表 *16* : サポートされる *UCS-C225-M6* ハードウェア

PID	ハードウェア
ND-NODE-L4=	• UCS C225 M6 シャーシ • 2.8GHz AMD CPU • 256 GB の RAM • 2.4TB HDD X 4 960GB SSD 1.6TB NVME ドライブ • Intel X710T2LG 2x10 GbE（銅） Intel E810XXVDA2 2x25/10 GbE（光ファイバ） • 1050W 電源装置
ND-CLUSTER-L4	3 台の ND-NODE-L4= アプライアンスのクラスタ。

（注） 上記のハードウェアは、Nexus ダッシュボード 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Nexus Dashboardノードとして使用できなくなります。

UCS-C225-M6 サーバーは、Nexus Dashboard リリース 2.3(2) 以降でサポートされています。

- 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、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。

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

  SOL は、基本的な構成情報を提供するためにノードに接続するのに使用する `connect host` コマンドに必要です。

- 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。

- Nexus ダッシュボード ハードウェアに、導入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、目的の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 2.0.1 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 2.1.1 を展開する場合は、次の手順に従います。

  - 最初に、次のセクションの説明に従って、リリース 2.0.1 クラスタを起動します。
  - 次に、Nexusダッシュボードのアップグレード（137ページ）の説明に従って、リリース 2.1.1 にアップグレードします。

少なくとも 3 ノードのクラスタが必要です。展開するアプリケーションのタイプと数に応じて、水平スケーリング用に追加のワーカー ノードを追加できます。単一クラスター内のワーカー ノードとスタンバイ ノードの最大数については、ご使用のリリースのリリース ノートを参照してください。

物理アプライアンスとしての Nexus ダッシュボードの展開

Nexusダッシュボードの物理ハードウェアを最初に受け取ると、ソフトウェアイメージがプリロードされています。ここでは、最初の 3 ノードの Nexus ダッシュボード クラスタを設定して起動する方法について説明します。

始める前に

- 前提条件とガイドライン （55 ページ） で説明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てください。

ステップ 1 最初のノードの基本情報を設定します。

クラスタのノードでのみ次の設定を完了する必要があります。2 番目と 3 番目のマスター ノードでは、電源がオンになっており、CIMC は IP アドレスとログイン資格情報で設定され、CIMC IP は最初のノードから到達できることを確認します。

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。

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` 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:
```

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) 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

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。

管理ネットワーク情報を入力して確認すると、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。

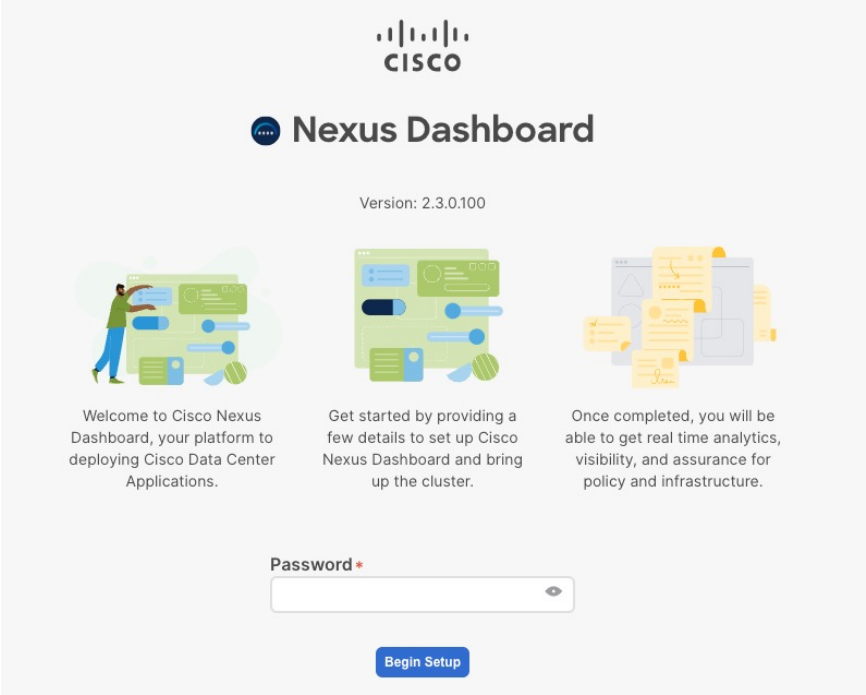
```
Please wait for system to boot: [#########################] 100%
System up, please wait for UI to be online.
```

```
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、**[セットアップの開始（Begin Setup）]** 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。

初期セットアップ ウィザードの **[クラスタの詳細（Cluster Details）]** 画面で、次の情報を入力します。

a) Nexus ダッシュボード クラスタの **[クラスタ名（Cluster Name）]** を入力します。

b) **[+ NTP ホストの追加（+Add NTP Host）]** をクリックして、1 つ以上の NTP サーバを追加します。

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。

IP アドレスを入力したら、緑色のチェックマーク アイコンをクリックして保存します。

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。

IP アドレスを入力したら、緑色のチェックマーク アイコンをクリックして保存します。

d) **[プロキシ サーバ（Proxy Server）]** を指定します。

Cisco クラウドへの直接接続を持たないクラスタの場合、プロキシ サーバを設定して接続を確立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準拠の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。

プロキシ構成をスキップする場合は、フィールドの横にある情報 **(i)** アイコンをクリックしてから、**[スキップ（Skip）]** をクリックします。

e) (オプション)プロキシサーバで認証が必要な場合は、**[プロキシに必要な認証（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。

f) (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。

- **[+DNS 検索ドメインを追加（+Add DNS Search Domain）]** をクリックして、1 つ以上の検索ドメインを指定します。

  IP アドレスを入力したら、緑色のチェックマーク アイコンをクリックして保存します。

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

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

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

  アプリケーションおよびサービスネットワークについては、このドキュメントの前の 前提条件とガイドライン （6 ページ） の項で説明します。

g) [**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、ノードの情報を入力します。

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

b) [**パスワード（Password）**] フィールドに、このノードのパスワードを入力し、[**検証（Validate）**] をクリックします。

これにより、ノードの [**シリアル番号（Serial Number）**] と [**管理ネットワーク（Management Network）**] の情報が自動入力されます。

c) ノードの**名前**を入力します。

d) ノードの**データ ネットワーク**情報を入力します。

管理ネットワーク情報には、最初のノードに指定した情報があらかじめ入力されています。

データネットワークの IP アドレス/ネットマスク（たとえば、`172.31.140.58/24`）とゲートウェイ（たとえば、`172.31.140.1`）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。

e) （オプション）管理およびデータ ネットワークの IPv6 情報を指定します。

Nexus ダッシュボードは、管理およびデータネットワークの IPv4 またはデュアルスタック IPv4/IPv6 のいずれかをサポートします。

（注） IPv6 情報を指定する場合は、このクラスタブートストラップのプロセス中に行う必要があります。IPv4 スタックのみを使用してクラスタを展開し、後で IPv6 情報を追加する場合は、クラスタを再度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スタックまたはデュアル IPv4/IPv6スタックのいずれかで設定する必要があります。

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

NDFC ファブリックを使用した Nexus ダッシュボード Insights などの一部のサービスで必要な永続的な IP 機能には、BGP 構成が必要です。この機能については、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。

- 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。

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。

[ノードの詳細（Node Details）] ウィンドウが開きます。

a) ノードの**名前**を入力します。

b) **[CIMC の詳細（CIMC Details）]**セクションで、ノードの CIMC IP アドレスとログイン クレデンシャルを入力し、**[確認（Verify）]** をクリックします。

IP アドレスとログイン資格情報は、そのノードを設定するために使用されます。

c) ノードの**管理ネットワーク**情報を指定します。

管理ネットワーク 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。

d) ノードの**データ ネットワーク**情報を入力します。

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。

e) （任意）管理およびデータネットワークのIPv6情報を指定します。

リリース2.1.1以降、Nexusダッシュボードは管理およびデータネットワークのデュアルスタックIPv4 / IPv6をサポートします。

（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。IPv4 スタックのみを使用してクラスタを展開し、後で IPv6 情報を追加する場合は、クラスタを再度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スタックまたはデュアル IPv4/IPv6スタックのいずれかで設定する必要があります。

f) **[保存 (Save)]**をクリックして、変更内容を保存します。

ステップ 7 前の手順を繰り返して、3番目のノードを追加します。

ステップ 8 [**次へ（Next**）] をクリックして続行します。

ステップ 9 **[確認（Confirmation）]** 画面で **[確認（Confirm）]** をクリックして、クラスタを作成します。

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。

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 10 クラスタが健全であることを検証します。

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

3 つすべてのノードの準備ができたら、SSH を使用して任意の 1 つのノードにログインし、次のコマンドを実行してクラスタの状態を確認できます。

a) クラスタが稼働していることを確認します。

任意のノードにログインし、`acs health` コマンドを実行することで、クラスタ展開の現在のステータスを確認できます。

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。

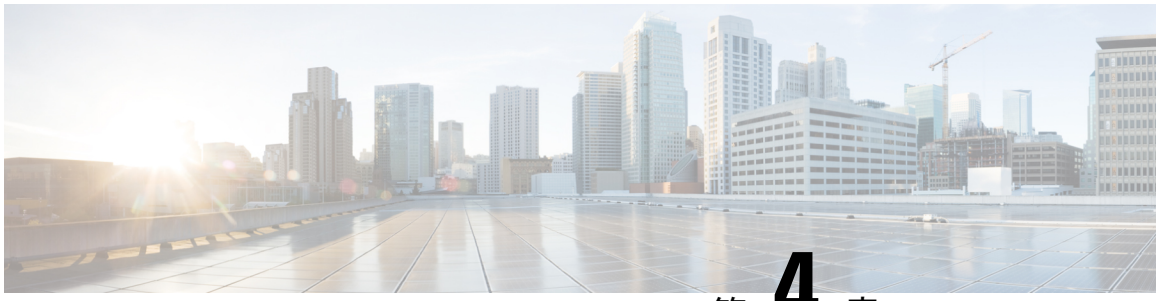
```
$ acs health
All components are healthy
```

b) Nexus ダッシュボード GUI にログインします。

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。管理者ユーザのデフォルト パスワードは、Nexus ダッシュボード クラスタの最初のノードに選択したレスキュー ユーザ パスワードと同じです。

ステップ 11 クラスタの **ネットワーク 拡張** パラメータを構成。

これは、*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管理** > **クラスタ構成** セクションに説明されています。 これは、Nexus ダッシュボードのヘルプセンターからも直接利用可能です。



第 4 章

VMware ESX の展開

前提条件とガイドライン

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

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

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

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

- 展開の概要と要件 （3 ページ） に記載されている一般的な前提条件を確認して完了します。

  この文書は、ベースとなる Nexus ダッシュボード クラスタを最初に展開する方法について説明するものである点に留意してください。追加ノード（従業員またはスタンバイ）で既存のクラスタを拡張する場合は、『*Cisco Nexus* ダッシュボード ユーザ 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 ガイド』から利用できます。

- 展開予定のサービスのリリース ノートに説明されている追加の前提条件を確認し、条件を満たすようにしてください。
- VMware ESXで展開する場合、2種類のノードを展開できます。
  - データ ノード：Nexus ダッシュボード Insightsなどのデータ集約型アプリケーション向けに設計されたノードプロファイル
  - アプリ ノード：Nexus ダッシュボード オーケストレータなどの非データ集約型アプリケーション用に設計されたノード プロファイル

（注） クラスタにワーカー ノードを追加する予定の場合：

- NDFC の場合、初期クラスタとワーカー ノードの両方をアプリ ノードにすることができます。

  詳細なスケール情報は、使用しているリリースの *Cisco Nexus Dashboard* ファブリック コントローラの検証済みスケーラビリティ ガイドで入手できます。

- 他のすべてのサービスまたは共同ホスティングのシナリオでは、データ ノードを使用して最初のクラスタを展開する必要があります。

十分なシステム リソースをもつことを確認します。

表 *17 :* 導入要件

Nexus Dashboard バージョン	データノードの要件	アプリケーションノードの要件
リリース 2.3.x		

Nexus Dashboard バージョン	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
		• vCenter を使用して展開する場合、VMware vCenter 7.0.1、7.0.2
		• 各 VM には次のものが必要です。
		  • 少なくとも 2.2 GHz の物理予約された 16 個の vCPU
		  • 物理予約された 64GB の RAM
		  • データ ボリューム用に 500GB HDD または SSD ストレージ、システム ボリューム用に追加の 50GB
		  一部のサービスでは、アプリ ノードをより高速な SSD ストレージに展開する必要がありますが、他のサービスでは HDD をサポートしています。Nexus ダッシュボード キャパシティ プランニング ツールをチェックして、正しいタイプのストレージを使用していることを確認してください。
		• 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。

Nexus Dashboard バージョン	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
	• vCenter を使用して展開する場合、VMware vCenter 7.0.1、7.0.2
	• 各 VM には次のものが必要です。
	  • 少なくとも 2.2 GHz の物理予約された 32 個の vCPU
	  • 物理予約された 128GB の RAM
	  • データ ボリューム用の 3TB SSD ストレージとシステム ボリューム用の追加の 50GB
	  データノードは、次の最小パフォーマンス要件を満たすストレージに展開する必要があります。
	  • SSD は、データストアに直接接続するか、RAID ホストバスアダプタ（HBA）を使用している場合は JBOD モードで接続する必要があります。
	  • SSD は、混合使用/アプリケーション用に最適化する必要があります（読み取り最適化ではありませ	

Nexus Dashboard バージョン	データノードの要件	アプリケーションノードの要件
	ん）。 • 4K ランダム読み取り IOPS：93000 • 4K ランダム書き込み IOPS：31000 • 各Nexus Dashboardノードは、異なるESXiサーバーに展開することを推奨します。	

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

  つまり、デバッグ目的などで、仮想マシンのスナップショットを作成する場合、スナップショットではすべてのNexusダッシュボードサービスが実行されている必要があります。
- ノードを ESXi に直接展開するか、vCenter を使用して展開するかを選択できます。

  vCenter を使用して展開する場合は、VMware vCenter を使用している Nexus ダッシュボードの展開 （70 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 （81 ページ） で説明されている手順に従います。

VMware vCenter を使用している Nexus ダッシュボードの展開

ここでは、VMware vCenter を使用して Cisco Nexus ダッシュボード クラスタを展開する方法について説明します。ESXi に直接展開する場合は、代わりに VMware ESXi での Nexus ダッシュボードの展開 （81 ページ） で説明されている手順に従ってください。

始める前に

- 前提条件とガイドライン （65 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。

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/

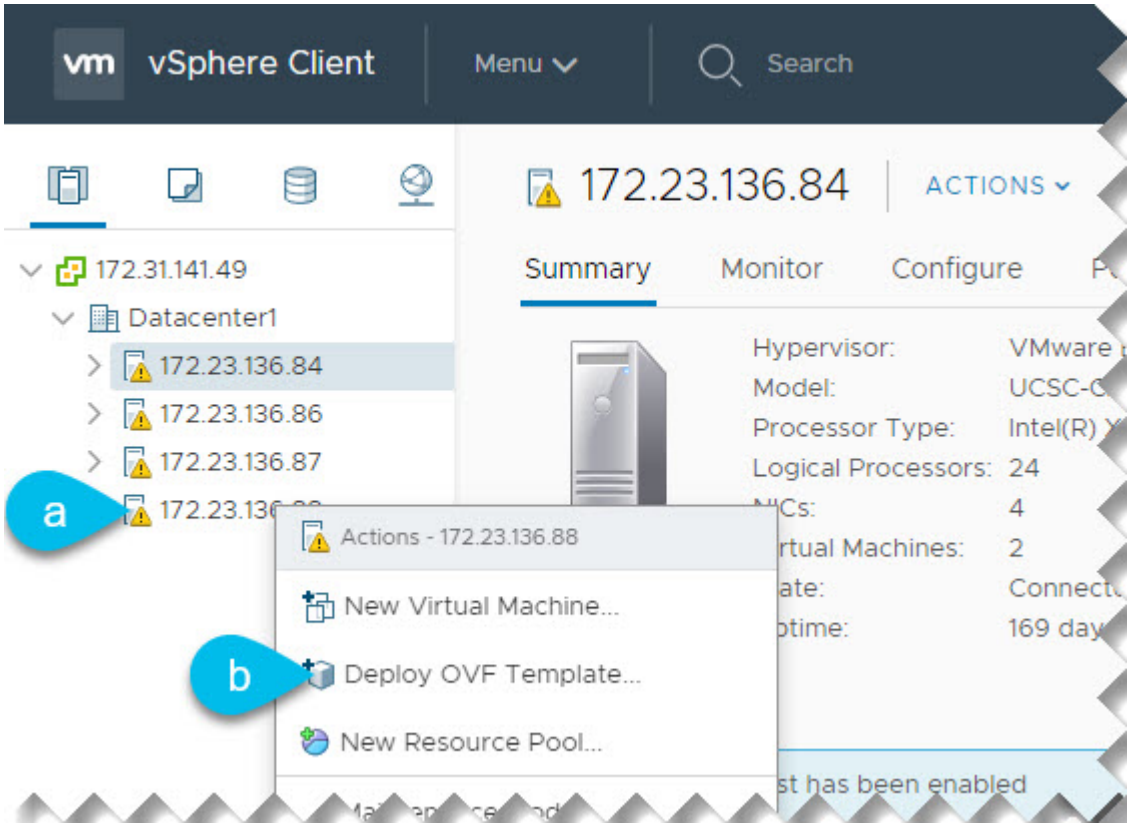
b) 左側のサイドバーから、ダウンロードする Nexus ダッシュボードのリリースバージョンを選択します。

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 6.7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。

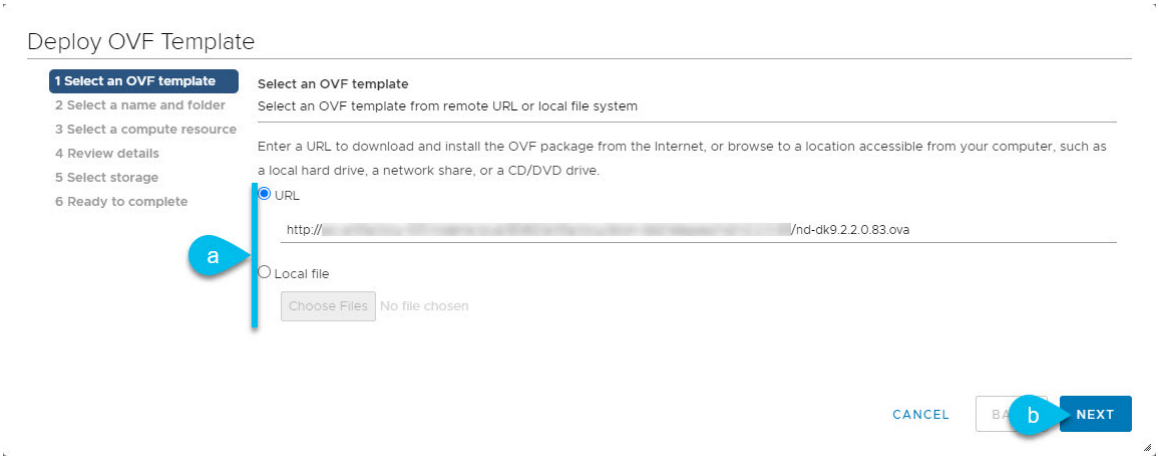


a) 展開する ESX ホストを右クリックします。

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。



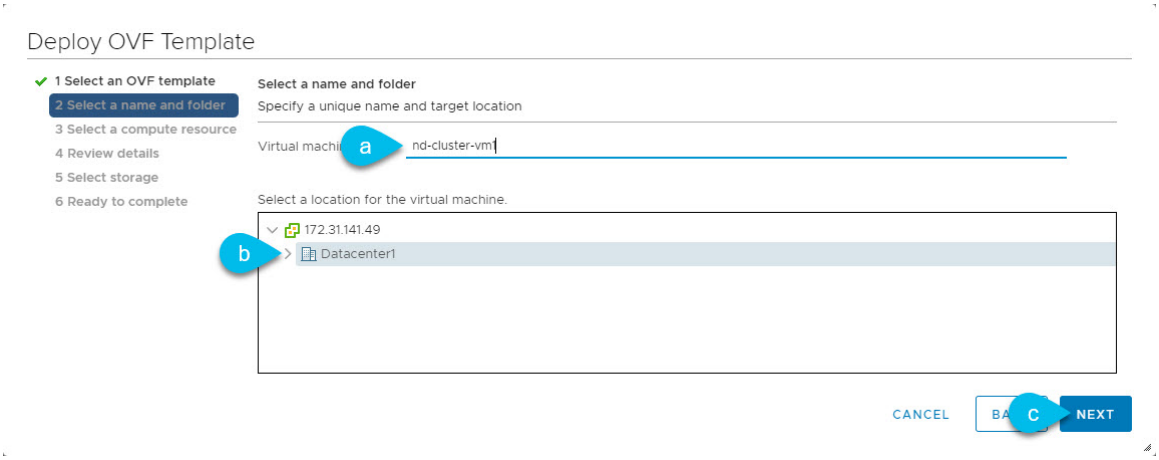
a) 画像を提供します。

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。

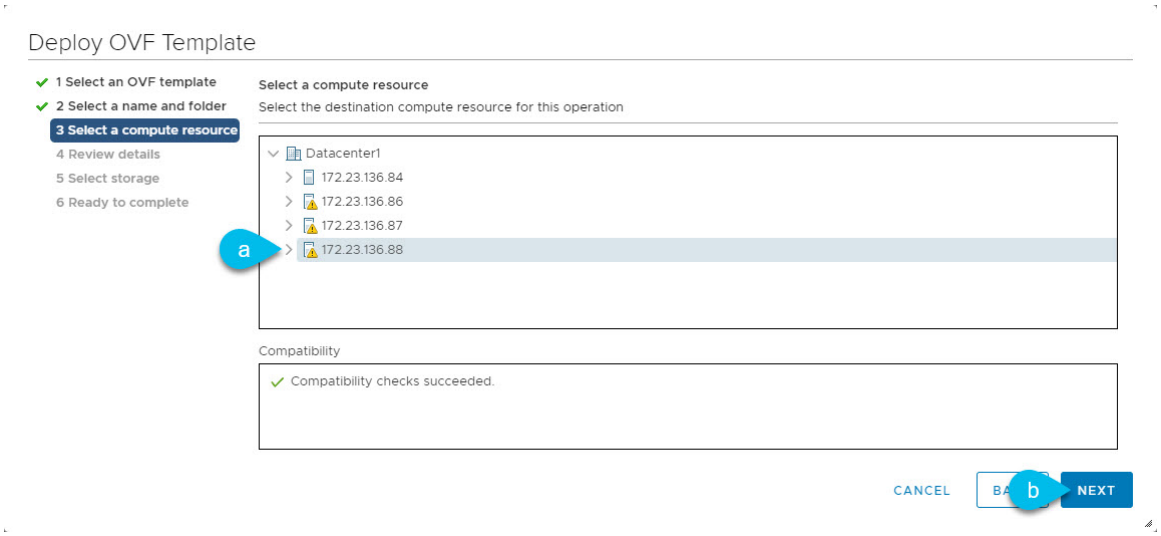
b) **[次へ（Next）]** をクリックして続行します。

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。
b) 仮想マシンのストレージ場所を選択します。
c) **[次へ（Next）]** をクリックして、続行します。

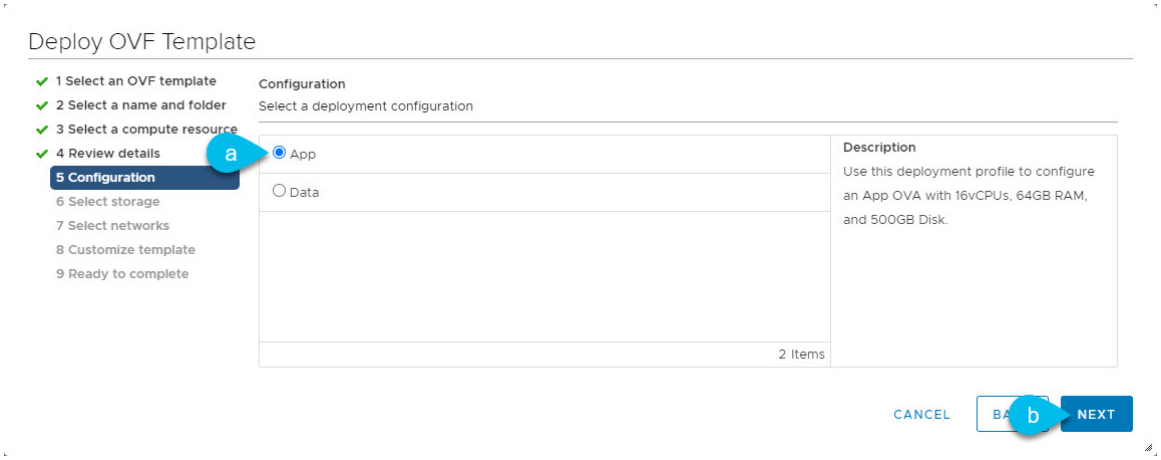
ステップ 6 **[コンピューティング リソースの選択（Select a compute resource）]** 画面で、ESX ホストを選択します。



a) 仮想マシンの vCenter データセンターと ESX ホストを選択します。
b) **[次へ（Next）]** をクリックして、続行します。

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

ステップ 8 [設定] 画面で、展開するノードプロファイルを選択します。

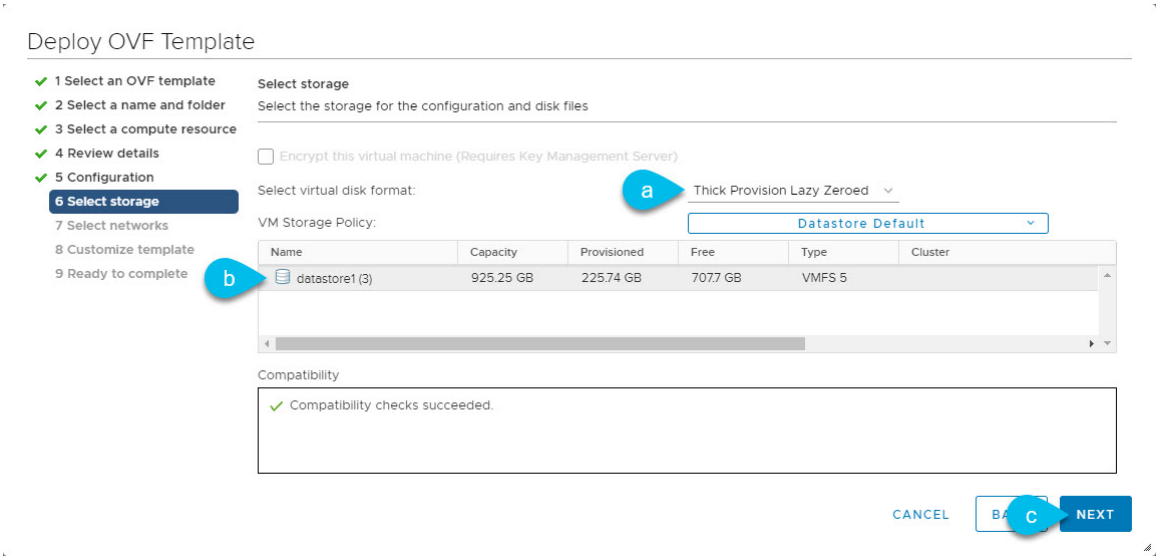


a) ユースケースの要件に基づいて、アプリまたはデータ ノード プロファイルを選択します。

ノードプロファイルの詳細については、「前提条件とガイドライン （65 ページ）」を参照してください。

b) **[次へ（Next）]** をクリックして、続行します。

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



a) [**仮想ディスクフォーマットの選択**]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**）] を選択します。

b) 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。

c) **[次へ（Next）]** をクリックして、続行します。

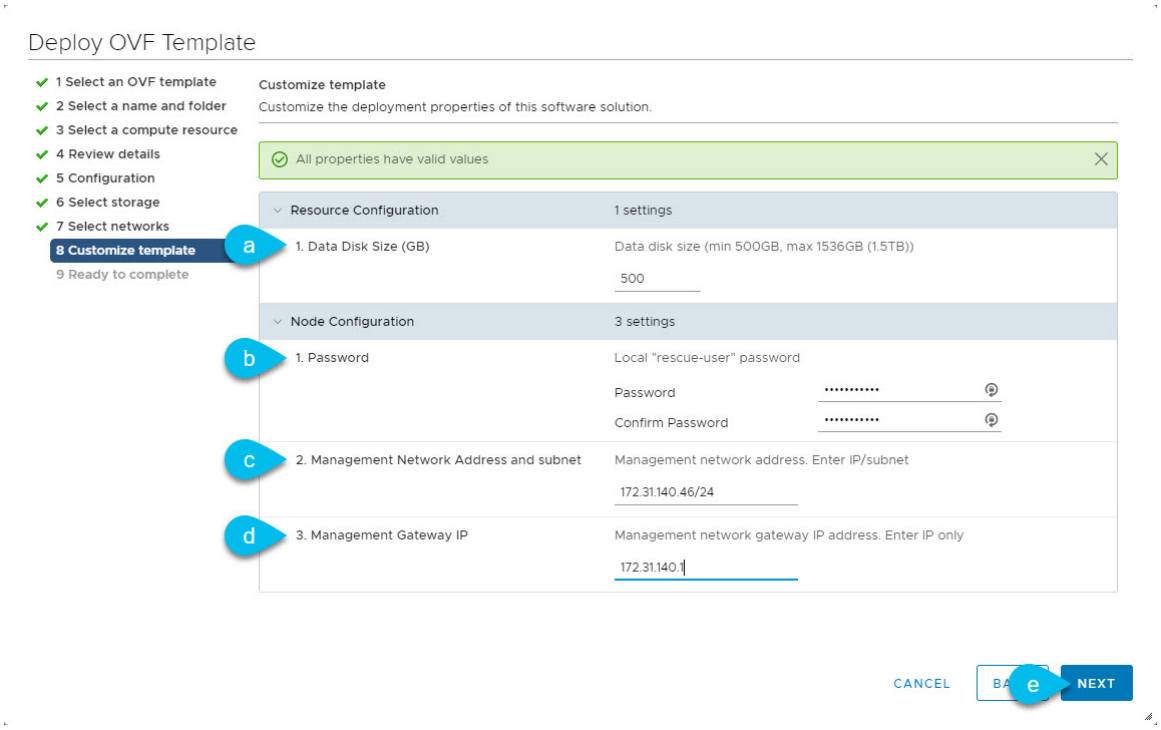
ステップ 10 [**ネットワークの選択**]画面で、Nexus ダッシュボードの管理およびデータ ネットワークの VM ネットワークを選択し、[**次へ**] をクリックして続行します。

Nexus ダッシュボードクラスタには 2 つのネットワークが必要です。

- **fabric0** は、Nexus ダッシュボードクラスタのデータ ネットワークに使用されます
- **mgmt0** は、Nexus ダッシュボードクラスタの管理ネットワークに使用されます。

これらのネットワークの詳細については、「展開の概要と要件」の章の「前提条件とガイドライン （6 ページ）」を参照してください。

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



a) ノードのデータ ボリュームのサイズを指定します。

必要なデータ ボリュームにはデフォルト値を使用することを推奨します。

デフォルト値は、展開するノードのタイプに基づいて事前に入力されます。アプリケーションノードには単一の500 GBディスクがあり、データノードには単一の 3TB ディスクがあります。

データ ボリュームに加えて、2 つ目の 50GB のシステム ボリュームも設定されますが、カスタマイズすることはできません。

b) **パスワード**を入力して確認します。

このパスワードは、各ノードの `rescue-user` アカウントに使用されます。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が、2番目と3番目のノードに異なるパスワードを指定することもできます。ノードにそれぞれ異なるパスワードを指定した場合、GUI の管理者ユーザーの初期パスワードには、クラスタをブートストラップするために**ステップ *16*** で使用したノードのパスワードを使用します。

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

d) **管理ネットワーク**の IP ゲートウェイを入力します。

e) [次へ（Next）] をクリックして次に進みます。

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

ステップ 13 以前のステップを繰り返し、2 番目と 3 番目のノードを展開します。

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

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

ステップ 14 VM の展開が完了するまで待ちます。

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

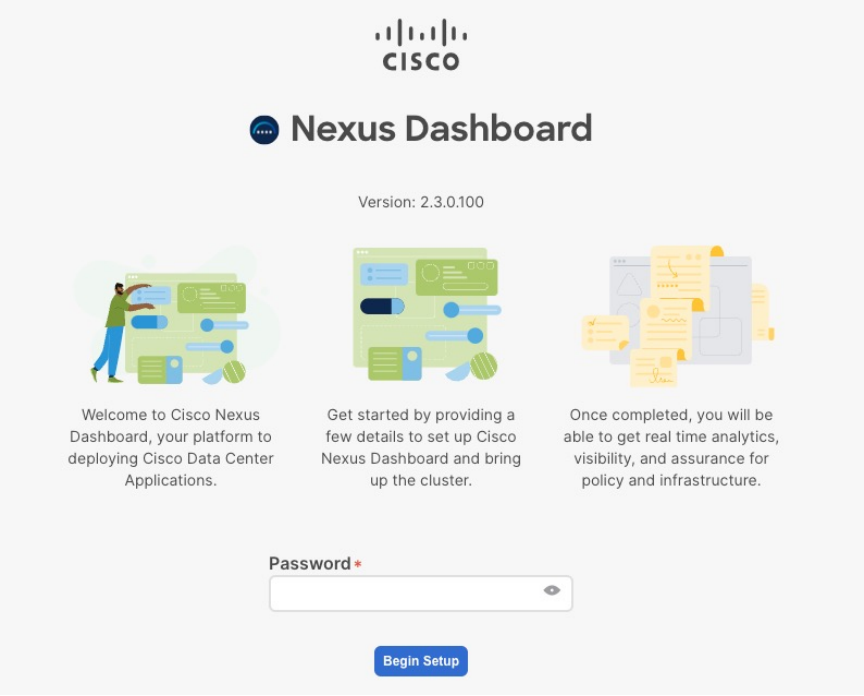
時刻の同期を無効にするには、次の手順を実行します。

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

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

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

前の手順で入力したパスワードを入力し、**[セットアップの開始（Begin Setup）]** をクリックします。



ステップ 17 **[クラスタの詳細（Cluster Details）]** を入力します。

初期セットアップ ウィザードの **[クラスタの詳細（Cluster Details）]** 画面で、次の情報を入力します。

a) Nexus ダッシュボード クラスタの **[クラスタ名（Cluster Name）]** を入力します。
b) **[+ NTP ホストの追加（+Add NTP Host）]** をクリックして、1 つ以上の NTP サーバを追加します。

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。

IP アドレスを入力したら、緑色のチェックマーク アイコンをクリックして保存します。

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。

IP アドレスを入力したら、緑色のチェックマーク アイコンをクリックして保存します。

d) **[プロキシ サーバ（Proxy Server）]** を指定します。

Cisco クラウドへの直接接続を持たないクラスタの場合、プロキシサーバを設定して接続を確立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準拠の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。

プロキシ構成をスキップする場合は、フィールドの横にある情報 **(i)** アイコンをクリックしてから、**[スキップ（Skip）]** をクリックします。

e) (オプション)プロキシサーバで認証が必要な場合は、**[プロキシに必要な認証（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。

f) (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。

- **[+DNS 検索ドメインを追加（+Add DNS Search Domain）]** をクリックして、1 つ以上の検索ドメインを指定します。

  IP アドレスを入力したら、緑色のチェックマーク アイコンをクリックして保存します。

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

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

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

  アプリケーションおよびサービスネットワークについては、このドキュメントの前の 前提条件とガイドライン （6 ページ） の項で説明します。

g) [**次へ（Next）**] をクリックして続行します。

ステップ 18 **[ノードの詳細（Node Details）]** 画面で、ノードの情報を入力します。

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

b) [**パスワード（Password）**] フィールドに、このノードのパスワードを入力し、[**検証（Validate）**] をクリックします。

これにより、ノードの [**シリアル番号（Serial Number）**] と [**管理ネットワーク（Management Network）**] の情報が自動入力されます。

c) ノードの**名前**を入力します。

d) ノードの**データ ネットワーク**情報を入力します。

管理ネットワーク情報には、最初のノードに指定した情報があらかじめ入力されています。

データネットワークの IP アドレス/ネットマスク（たとえば、172.31.140.58/24）とゲートウェイ（たとえば、172.31.140.1）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。

e) （オプション）管理およびデータ ネットワークの IPv6 情報を指定します。

Nexus ダッシュボードは、管理およびデータネットワークの IPv4 またはデュアルスタック IPv4/IPv6 のいずれかをサポートします。

（注） IPv6 情報を指定する場合は、このクラスタブートストラップのプロセス中に行う必要があります。IPv4 スタックのみを使用してクラスタを展開し、後で IPv6 情報を追加する場合は、クラスタを再度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スタックまたはデュアル IPv4/IPv6スタックのいずれかで設定する必要があります。

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

NDFC ファブリックを使用した Nexus ダッシュボード Insights などの一部のサービスで必要な永続的な IP 機能には、BGP 構成が必要です。この機能については、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。

- 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。

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

（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して、手順 21 に進めます。

[ノードの詳細（Node Details）] ウィンドウが開きます。

a) [**展開の詳細**（**Deployment Details**）] セクションで、ノードの VM を展開するときに構成したレスキューユーザーのノードの**管理 IP アドレス**と**パスワード**を入力し、[**検証**（**Verify**）] をクリックします。

これにより、ノードの [**シリアル番号**（**Serial Number**）] と [**管理ネットワーク**（**Management Network**）] の情報が自動入力されます。

b) ノードの**名前**を入力します。

c) ノードの**データ ネットワーク** IP アドレスとゲートウェイを指定します。

[**管理ネットワーク（Management Network**）] 情報には、前のサブステップで指定した IP アドレスとログイン情報に基づいてノードから取得した情報が事前に入力されます。

データネットワークの IP アドレス/ネットマスク（たとえば、`172.31.141.58/24`）とゲートウェイ（たとえば、`172.31.141.1`）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。

d) （任意）管理およびデータネットワークのIPv6情報を指定します。

Nexus ダッシュボードは、管理およびデータネットワークの IPv4 またはデュアルスタック IPv4/IPv6 のいずれかをサポートします。

（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。IPv4 スタックのみを使用してクラスタを展開し、後で IPv6 情報を追加する場合は、クラスタを再度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スタックまたはデュアル IPv4/IPv6スタックのいずれかで設定する必要があります。

e) （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**。

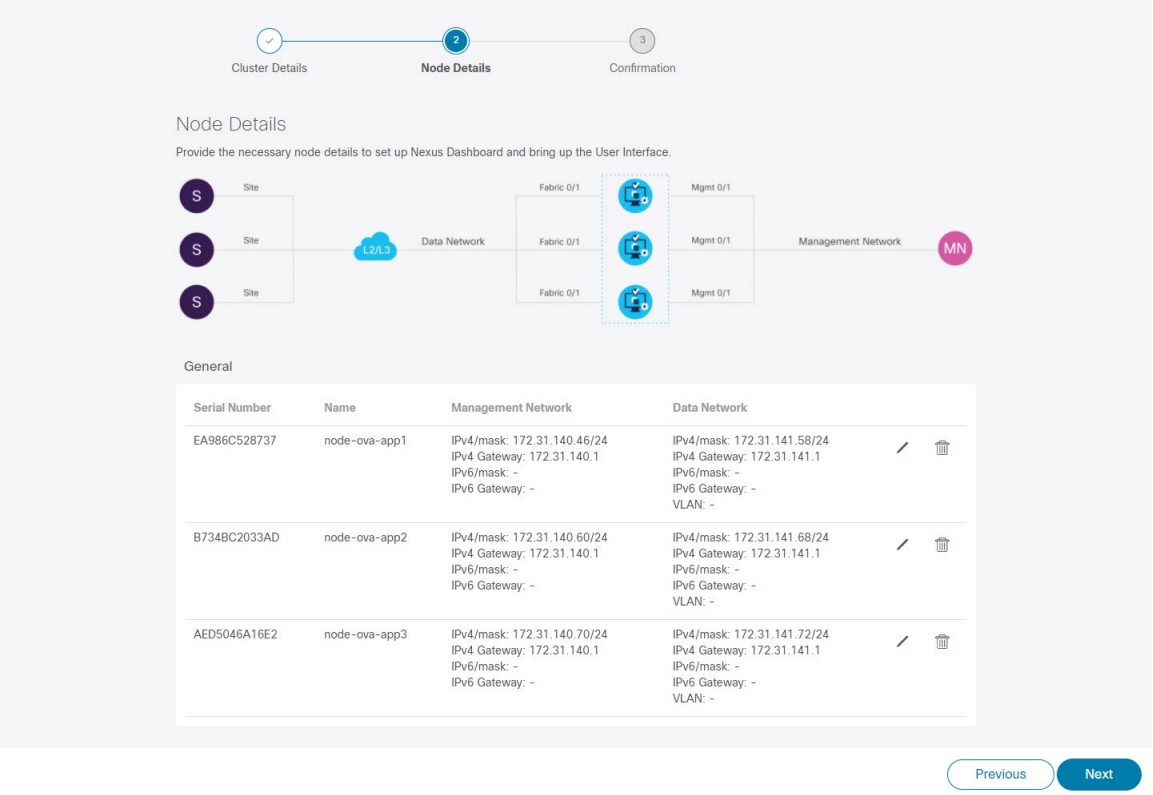
f) **[保存 (Save)]**をクリックして、変更内容を保存します。

ステップ 20 前の手順を繰り返して、3番目のノードを追加します。

（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して、手順 21 に進めます。

ステップ 21 **[ノードの詳細（Node Details）]** 画面で、**[次へ（Next）]** をクリックして続行します。

クラスタ内の 3 つのノードすべての情報を入力したら、ブートストラッププロセスの次の画面に進みます。



ステップ 22 [**確認（Confirmation**）] 画面で設定情報を確認し、[**構成（Configure**）] をクリックしてクラスタを作成します。

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

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

ステップ 23 クラスタが健全であることを検証します。

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

3 つすべてのノードの準備ができたら、SSH を使用して任意の 1 つのノードにログインし、次のコマンドを実行してクラスタの状態を確認できます。

a) クラスタが稼働していることを確認します。

任意のノードにログインし、`acs health` コマンドを実行することで、クラスタ展開の現在のステータスを確認できます。

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
```

b) Nexus ダッシュボード GUI にログインします。

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。管理者ユーザのデフォルト パスワードは、Nexus ダッシュボード クラスタの最初のノードに選択したレスキュー ユーザ パスワードと同じです。

ステップ 24 クラスタの **ネットワーク 拡張** パラメータを構成。

これは、*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管理** > **クラスタ構成** セクションに説明されています。これは、Nexus ダッシュボードのヘルプセンターからも直接利用可能です。

VMware ESXi での Nexus ダッシュボードの展開

ここでは、VMware ESXi で Cisco Nexus ダッシュボード クラスタを展開する方法について説明します。vCenter を使用して展開する場合は、代わりに VMware ESXi での Nexus ダッシュボードの展開 （81 ページ） で説明されている手順に従ってください。

始める前に

- 前提条件とガイドライン （65 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。

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 6.7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-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）]** 画面で、[ディスク プロビジョニング：シック（Disk Provisioning：Thick）] を選択し、[自動化をオン（Power on automatic）] オプションをオフにして、**[次へ（Next）]** をクリックして続行します。

2 つのネットワークがあり、**fabric0** はデータネットワークに使用され、**mgmt0** は管理ネットワークに使用されます。

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。

```
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。

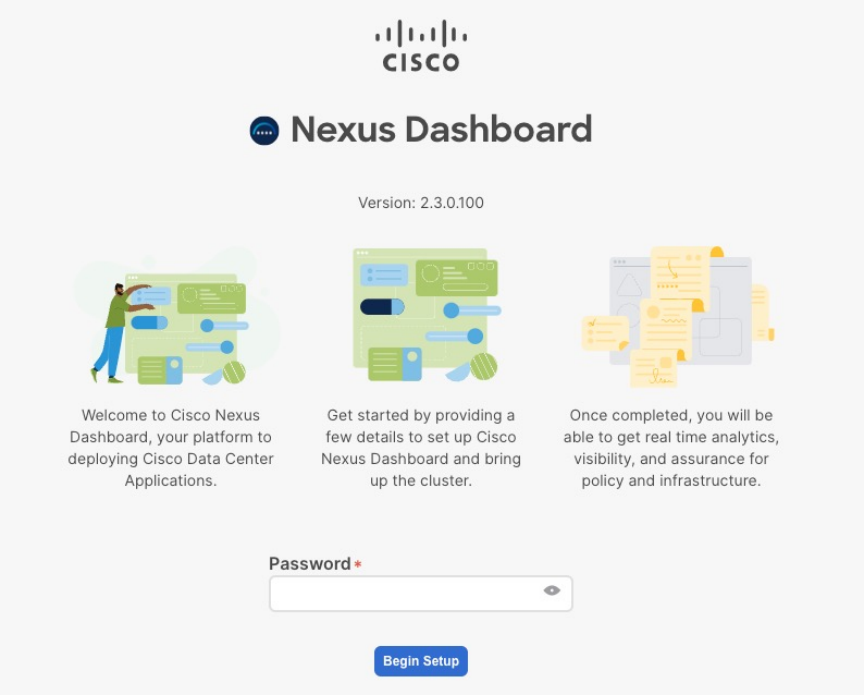
```
Please review the config
Management network:
  Gateway: 192.168.9.1
  IP Address/Mask: 192.168.9.172/24
Cluster leader: no

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

ステップ 14 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、**[セットアップの開始（Begin Setup）]** をクリックします。



ステップ 15 **[クラスタの詳細（Cluster Details）]** を入力します。

初期セットアップ ウィザードの **[クラスタの詳細（Cluster Details）]** 画面で、次の情報を入力します。

a) Nexus ダッシュボード クラスタの **[クラスタ名（Cluster Name）]** を入力します。

b) **[+ NTP ホストの追加（+Add NTP Host）]** をクリックして、1 つ以上の NTP サーバを追加します。

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。

IP アドレスを入力したら、緑色のチェックマーク アイコンをクリックして保存します。

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。

IP アドレスを入力したら、緑色のチェックマーク アイコンをクリックして保存します。

d) **[プロキシ サーバ（Proxy Server）]** を指定します。

Cisco クラウドへの直接接続を持たないクラスタの場合、プロキシサーバを設定して接続を確立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準拠の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。

プロキシ構成をスキップする場合は、フィールドの横にある情報 **(i)** アイコンをクリックしてから、**[スキップ（Skip）]** をクリックします。

e) (オプション)プロキシサーバで認証が必要な場合は、**[プロキシに必要な認証（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。

f) (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。

- **[+DNS 検索ドメインを追加（+Add DNS Search Domain）]** をクリックして、1 つ以上の検索ドメインを指定します。

  IP アドレスを入力したら、緑色のチェックマーク アイコンをクリックして保存します。

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

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

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

  アプリケーションおよびサービスネットワークについては、このドキュメントの前の 前提条件とガイドライン （6 ページ） の項で説明します。

g) **[次へ（Next）]** をクリックして続行します。

ステップ 16 **[ノードの詳細（Node Details）]** 画面で、ノードの情報を入力します。

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

b) **[パスワード（Password）]** フィールドに、このノードのパスワードを入力し、**[検証（Validate）]** をクリックします。

これにより、ノードの **[シリアル番号（Serial Number）]** と **[管理ネットワーク（Management Network）]** の情報が自動入力されます。

c) ノードの**名前**を入力します。

d) ノードの**データ ネットワーク**情報を入力します。

管理ネットワーク情報には、最初のノードに指定した情報があらかじめ入力されています。

データネットワークの IP アドレス/ネットマスク（たとえば、`172.31.140.58/24`）とゲートウェイ（たとえば、`172.31.140.1`）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。

e) （オプション）管理およびデータ ネットワークの IPv6 情報を指定します。

Nexus ダッシュボードは、管理およびデータネットワークの IPv4 またはデュアルスタック IPv4/IPv6 のいずれかをサポートします。

（注） IPv6 情報を指定する場合は、このクラスタブートストラップのプロセス中に行う必要があります。IPv4 スタックのみを使用してクラスタを展開し、後で IPv6 情報を追加する場合は、クラスタを再度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スタックまたはデュアル IPv4/IPv6スタックのいずれかで設定する必要があります。

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

NDFC ファブリックを使用した Nexus ダッシュボード Insights などの一部のサービスで必要な永続的な IP 機能には、BGP 構成が必要です。この機能については、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。

- 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。

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。

（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。

[ノードの詳細（Node Details）] ウィンドウが開きます。

a) [**展開の詳細**（**Deployment Details**）] セクションで、ノードの VM を展開するときに構成したレスキューユーザーのノードの**管理 IP アドレス**と**パスワード**を入力し、[**検証**（**Verify**）] をクリックします。

これにより、ノードの [**シリアル番号**（**Serial Number**）] と [**管理ネットワーク**（**Management Network**）] の情報が自動入力されます。

b) ノードの**名前**を入力します。

c) ノードの**データ ネットワーク** IP アドレスとゲートウェイを指定します。

[**管理ネットワーク**（**Management Network**）] 情報には、前のサブステップで指定した IP アドレスとログイン情報に基づいてノードから取得した情報が事前に入力されます。

データネットワークの IP アドレス/ネットマスク（たとえば、`172.31.141.58/24`）とゲートウェイ（たとえば、`172.31.141.1`）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。

d) （任意）管理およびデータネットワークのIPv6情報を指定します。

Nexus ダッシュボードは、管理およびデータネットワークの IPv4 またはデュアルスタック IPv4/IPv6 のいずれかをサポートします。

（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。IPv4 スタックのみを使用してクラスタを展開し、後で IPv6 情報を追加する場合は、クラスタを再度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スタックまたはデュアル IPv4/IPv6スタックのいずれかで設定する必要があります。

e) （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**。

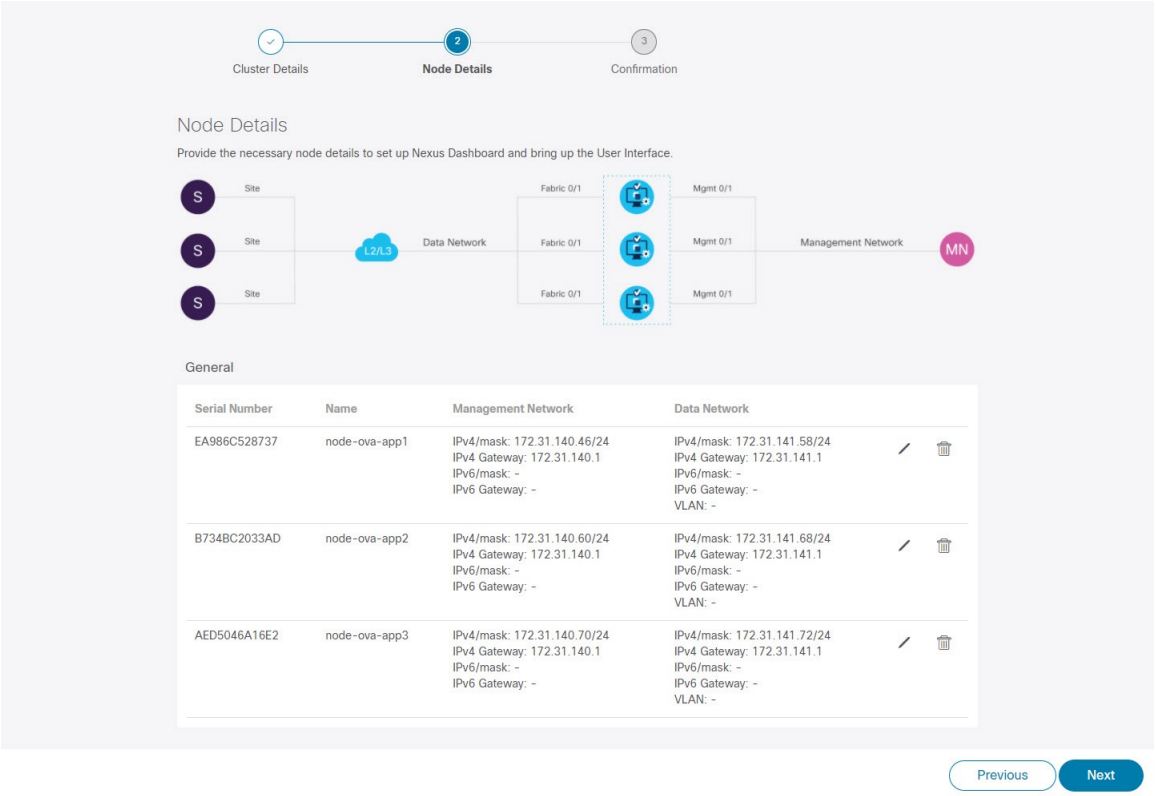
f) **[保存 (Save)]**をクリックして、変更内容を保存します。

ステップ 18 前の手順を繰り返して、3番目のノードを追加します。

（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 19　**[ノードの詳細（Node Details）]** 画面で、**[次へ（Next）]** をクリックして続行します。

クラスタ内の 3 つのノードすべての情報を入力したら、ブートストラッププロセスの次の画面に進みます。



ステップ 20　**[確認（Confirmation）]** 画面で設定情報を確認し、**[構成（Configure）]** をクリックしてクラスタを作成します。

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 21　クラスタが健全であることを検証します。

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

3 つすべてのノードの準備ができたら、SSH を使用して任意の 1 つのノードにログインし、次のコマンドを実行してクラスタの状態を確認できます。

a)　クラスタが稼働していることを確認します。

任意のノードにログインし、`acs health` コマンドを実行することで、クラスタ展開の現在のステータスを確認できます。

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。

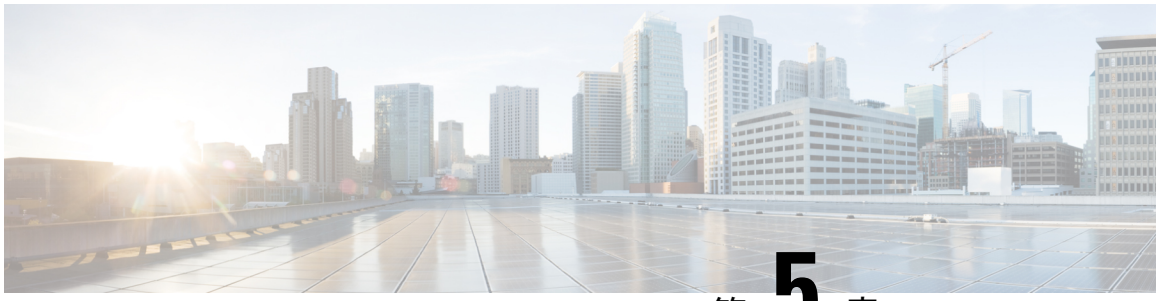
```
$ acs health
All components are healthy
```

b) Nexus ダッシュボード GUI にログインします。

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。管理者ユーザのデフォルト パスワードは、Nexus ダッシュボード クラスタの最初のノードに選択したレスキュー ユーザ パスワードと同じです。

ステップ 22 クラスタの **ネットワーク 拡張** パラメータを構成。

これは、*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管理** > **クラスタ構成** セクションに説明されています。 これは、Nexus ダッシュボードのヘルプセンターからも直接利用可能です。



第 5 章

Linux KVMでの展開

前提条件とガイドライン

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

- ファクターから KVM が拡張性とサービス要件をサポートしていることを確認します。

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

- 展開の概要と要件 （3 ページ） に記載されている一般的な前提条件を確認して完了します。

- 展開予定のサービスのリリース ノートに説明されている追加の前提条件を確認し、条件を満たすようにしてください。

- 十分なシステム リソースをもつことを確認します。

表 *18 :* 導入要件

オーケストレータ バージョン	要件
リリース 2.3.x	

オーケストレータ バージョン	要件

	• サポートされている Linux 流通：
	  • Nexus Dashboard Orchestrator の場合、CentOS Linux に展開する必要があります
	  • Nexus ダッシュボード ファブリック コントローラの場合、CentOS または Red Hat Enterprise Linux に展開する必要があります。
	• カーネルと KVM のサポートされているバージョン：
	  • カーネル `3.10.0-957.el7.x86_64` 以降
	  • KVM `libvirt-4.5.0-23.el7_7.1.x86_64` 以降
	• 16 vCPU
	• 64 GB の RAM
	• 500 GB のディスク
	各ノードには専用のディスク パーティションが必要です。
	• ディスクの I/O 遅延は 20 ミリ秒以下である必要があります。
	I/O レイテンシを確認するには：
	1. テストディレクトリを作成します。
	`test-data` のような名前にします。
	2. 次のコマンドを実行します。
	`# fio --rw=write --ioengine=sync --fdatasync=1 --directory=test-data --size=22m --bs=2300 --name=mytest`
	3. コマンドの実行後に、`fsync/fdatasync/sync_file_range` セクションの `99.00th=[<value>]` が 20 ミリ秒未満であることを確認します。

オーケストレータ バージョン	要件
	• 各 Nexus ダッシュボード ノードは異なる KVM サーバに展開することを推奨します。

Linux KVM での Nexus ダッシュボードの展開

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

始める前に

- 前提条件とガイドライン （89 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。

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

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

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

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

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

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

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

`scp` を使用してイメージをコピーできます。次に例を示します。

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

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

ステップ 3 最初のノードに必要なディスクイメージを作成します。

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

a) KVM ホストに `root` ユーザとしてログインします。

b) ノードのスナップショット用のディレクトリを作成します。

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

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

c) スナップショットを作成します。

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

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

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

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

d) ノードの追加ディスクイメージを作成します。

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

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

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

次の手順に進む前に、次の準備が必要です。

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

ステップ 5 最初のノードの VM を作成します。

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

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

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

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

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

d) **OS タイプ**と**バージョン**に対して [Generic] を選択し、**[転送]** をクリックします。
e) 64GB のメモリと 16 個の CPU を指定し、**[転送（Forward）]** をクリックします。
f) 仮想マシンの**名前**（例：nd-node1）を入力し、**[インストール前に構成をカスタマイズする（Customize configuration before install）]**オプションをオンにします。次に、[完了（Finish）] をクリックします。

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

[VMの詳細]ウィンドウが開きます。

[VMの詳細]ウィンドウで、NICのデバイスモデルを変更します。

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

VMの詳細ウィンドウで、2番目のNICを追加します。

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

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

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

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

ステップ 6 前のステップを繰り返して、2 番目と 3 番目のノードの VM を作成し、それからすべての VM を開始します。

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。

```
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 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） 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、**[セットアップの開始（Begin Setup）]** をクリックします。

ステップ 11 **[クラスタの詳細（Cluster Details）]** を入力します。

初期セットアップ ウィザードの **[クラスタの詳細（Cluster Details）]** 画面で、次の情報を入力します。

a) Nexus ダッシュボード クラスタの **[クラスタ名（Cluster Name）]** を入力します。

b) **[+ NTP ホストの追加（+Add NTP Host）]** をクリックして、1 つ以上の NTP サーバを追加します。

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。

IP アドレスを入力したら、緑色のチェックマーク アイコンをクリックして保存します。

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。

IP アドレスを入力したら、緑色のチェックマーク アイコンをクリックして保存します。

d) **[プロキシ サーバ（Proxy Server）]** を指定します。

Cisco クラウドへの直接接続を持たないクラスタの場合、プロキシサーバを設定して接続を確立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準拠の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。

プロキシ構成をスキップする場合は、フィールドの横にある情報 **(i)** アイコンをクリックしてから、**[スキップ（Skip）]** をクリックします。

e) (オプション)プロキシサーバで認証が必要な場合は、**[プロキシに必要な認証（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。

f) (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。

- **[+DNS 検索ドメインを追加（+Add DNS Search Domain）]** をクリックして、1 つ以上の検索ドメインを指定します。

  IP アドレスを入力したら、緑色のチェックマーク アイコンをクリックして保存します。

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

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

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

  アプリケーションおよびサービスネットワークについては、このドキュメントの前の 前提条件とガイドライン （6 ページ） の項で説明します。

g) [**次へ（Next）**] をクリックして続行します。

ステップ 12 **[ノードの詳細（Node Details）]** 画面で、ノードの情報を入力します。

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

b) [**パスワード（Password）**] フィールドに、このノードのパスワードを入力し、[**検証（Validate）**] をクリックします。

これにより、ノードの [**シリアル番号（Serial Number）**] と [**管理ネットワーク（Management Network）**] の情報が自動入力されます。

c) ノードの**名前**を入力します。

d) ノードの**データ ネットワーク**情報を入力します。

管理ネットワーク情報には、最初のノードに指定した情報があらかじめ入力されています。

データネットワークの IP アドレス/ネットマスク（たとえば、`172.31.140.58/24`）とゲートウェイ（たとえば、`172.31.140.1`）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。

e) （オプション）管理およびデータ ネットワークの IPv6 情報を指定します。

Nexus ダッシュボードは、管理およびデータネットワークの IPv4 またはデュアルスタック IPv4/IPv6 のいずれかをサポートします。

（注） IPv6 情報を指定する場合は、このクラスタブートストラップのプロセス中に行う必要があります。IPv4 スタックのみを使用してクラスタを展開し、後で IPv6 情報を追加する場合は、クラスタを再度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スタックまたはデュアル IPv4/IPv6スタックのいずれかで設定する必要があります。

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

NDFC ファブリックを使用した Nexus ダッシュボード Insights などの一部のサービスで必要な永続的な IP 機能には、BGP 構成が必要です。この機能については、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。

- 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。

ステップ 13 [**ノードの詳細**（**Node Details**）] 画面で、[**ノードの追加**（**Add Node**）] をクリックして、クラスタに 2 番目のノードを追加します。

[ノードの詳細（Node Details）] ウィンドウが開きます。

a) [**展開の詳細**（**Deployment Details**）] セクションで、ノードの VM を展開するときに構成したレスキューユーザーのノードの**管理 IP アドレス**と**パスワード**を入力し、[**検証**（**Verify**）] をクリックします。

これにより、ノードの [**シリアル番号**（**Serial Number**）] と [**管理ネットワーク**（**Management Network**）] の情報が自動入力されます。

b) ノードの**名前**を入力します。

c) ノードの**データ ネットワーク** IP アドレスとゲートウェイを指定します。

[**管理ネットワーク**（**Management Network**）] 情報には、前のサブステップで指定した IP アドレスとログイン情報に基づいてノードから取得した情報が事前に入力されます。

データネットワークの IP アドレス/ネットマスク（たとえば、`172.31.141.58/24`）とゲートウェイ（たとえば、`172.31.141.1`）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。

d) （任意）管理およびデータネットワークのIPv6情報を指定します。

Nexus ダッシュボードは、管理およびデータネットワークの IPv4 またはデュアルスタック IPv4/IPv6 のいずれかをサポートします。

（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。IPv4 スタックのみを使用してクラスタを展開し、後で IPv6 情報を追加する場合は、クラスタを再度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スタックまたはデュアル IPv4/IPv6スタックのいずれかで設定する必要があります。

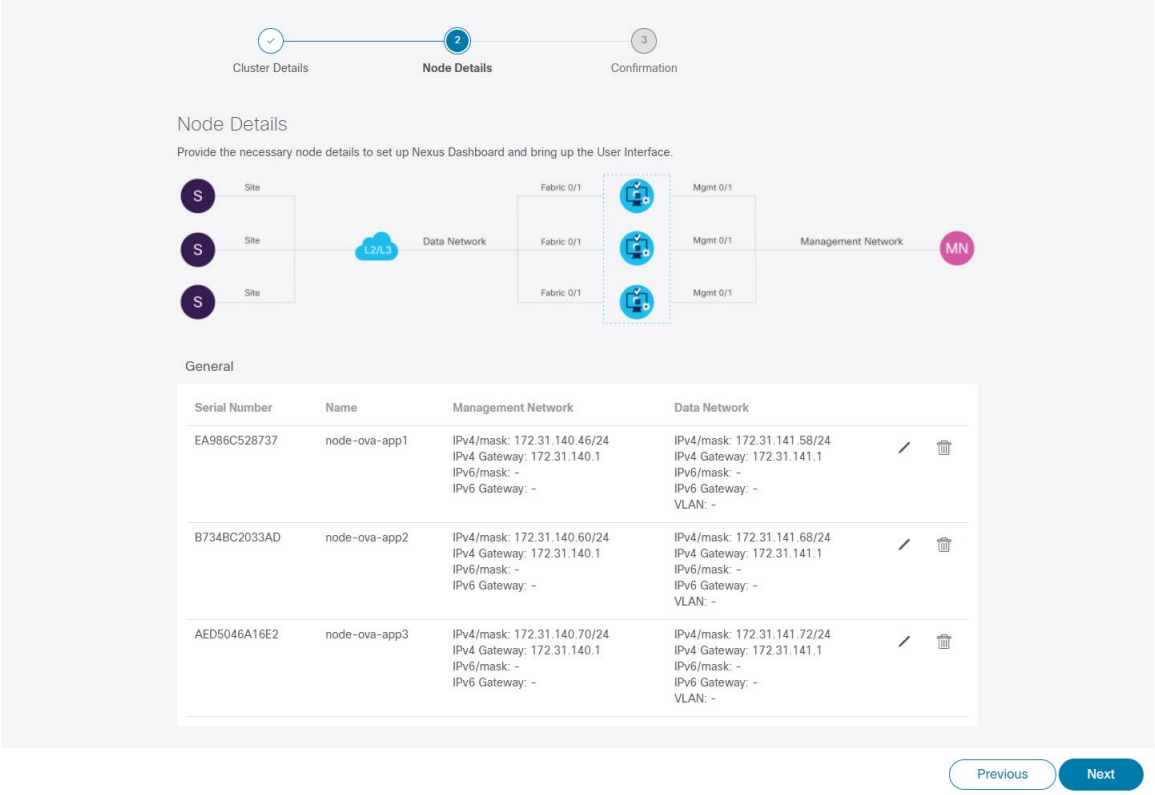
e) （任意）必要に応じて、データ ネットワークの **BGP を有効にします**。

f) **[保存 (Save)]**をクリックして、変更内容を保存します。

ステップ 14 前の手順を繰り返して、3番目のノードを追加します。

ステップ 15 **[ノードの詳細（Node Details）]** 画面で、**[次へ（Next）]** をクリックして続行します。

クラスタ内の 3 つのノードすべての情報を入力したら、ブートストラッププロセスの次の画面に進みます。



ステップ 16 **[確認（Confirmation）]** 画面で設定情報を確認し、**[構成（Configure）]** をクリックしてクラスタを作成します。

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

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

ステップ 17 クラスタが健全であることを検証します。

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

3 つすべてのノードの準備ができたら、SSH を使用して任意の 1 つのノードにログインし、次のコマンドを実行してクラスタの状態を確認できます。

a) クラスタが稼働していることを確認します。

任意のノードにログインし、`acs health` コマンドを実行することで、クラスタ展開の現在のステータスを確認できます。

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 - [...]
```

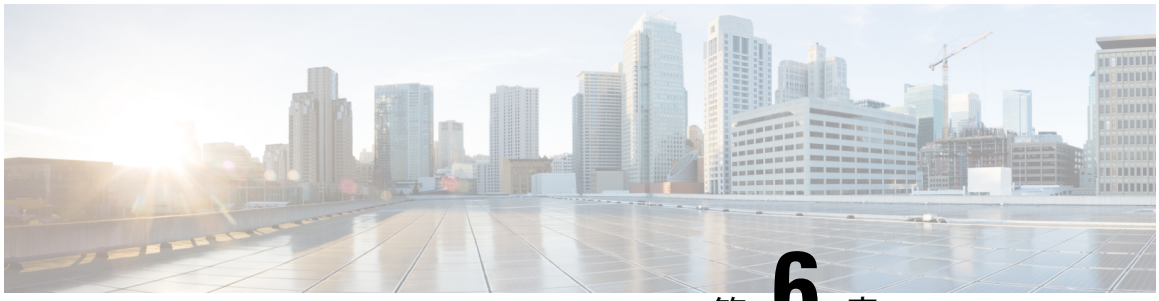
```
$ acs health
k8s: Etcd cluster is not ready
```

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
```

b) Nexus ダッシュボード GUI にログインします。

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。管理者ユーザのデフォルトパスワードは、Nexus ダッシュボードクラスタの最初のノードに選択したレスキュー ユーザ パスワードと同じです。



第 6 章

Amazon Web Services での展開

前提条件とガイドライン

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

- ファクターから AWS が拡張性とサービス要件をサポートしていることを確認します。

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

- デプロイ概要 （3 ページ） に記載されている一般的な前提条件を確認して完了します。

- 展開する予定のサービスのリリース ノートに記載されている追加の前提条件を確認して完了します。

- AWS アカウントに適切なアクセス権限があること。

  Nexus ダッシュボード クラスタをホストするには、複数の Elastic Compute Cloud（`m5.2xlarge`）のインスタンスを起動できる必要があります。

- 6 つ以上の AWS Elastic IP アドレスが必要です。

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

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

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

3. EC2 ダッシュボードで、**[制限（Limits）]** をクリックし、許可されている **EC2-VPC Elastic IP** の最大数を確認します。

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

- VPC（仮想プライベート クラウド）を作成します。

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

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

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

- インターネット ゲートウェイを作成し、VPC に接続します。

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

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

- ルート テーブルを作成します。

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

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

- キー ペアを作成します。

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

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

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

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

AWS での Nexus ダッシュボードの展開

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

始める前に

- 前提条件とガイドライン （101 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。

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

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

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

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

c) [Manage Subscriptions] をクリックします。
d) **[製品の検出（Discover products）]** をクリックします。
e) **Cisco Nexus ダッシュボード**を検索し、結果をクリックします。
f) 製品ページで、**[続行して登録（Continue to Subscribe）]** をクリックします。
g) [条件に同意する（Accept Terms）] をクリックします。

サブスクリプションが処理されるまでに数分かかる場合があります。

h) 最後に、**[設定を続行 (Continue to Configuration)]** をクリックします。

ステップ 2 ソフトウェア オプションと地域を選択します。

a) **[配送方法（Delivery Method）]** ドロップダウンから、`[Cisco Nexus Dashboard for Cloud]` を選択します。
b) **[ソフトウェア バージョン（Software Version）]** ドロップダウンから、展開するバージョンを選択します。
c) **[リージョン（Region）]** ドロップダウンから、テンプレートを展開するリージョンを選択します。

これは、VPC を作成したのと同じリージョンである必要があります。

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

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

ステップ 3 **[アクションの選択（Choose Action）]** から、`[CloudFormation の起動（Launch CloudFormation）]` を選択し、**[起動（Launch）]** をクリックします。

[Create Stack（スタックの作成）] ページが表示されます。

ステップ 4 スタックを作成します。

a) **[前提条件 - テンプレートの準備（Prerequisite-Prepare template）]** 領域で、`[テンプレート準備完了（Template is ready）]` を選択します。
b) **[テンプレートの指定（Specify Template）]** フィールドで、テンプレート ソースとして `[Amazon S3 URL]` を選択します。

これは、自動的に入力されます。

c) [**次へ（Next）**] をクリックして続行します。

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

ステップ 5 スタックの詳細を指定します。

a) **スタック名**を入力します。
b) **[VPC ID]** ドロップダウンから、作成した VPC を選択します。

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

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

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

たとえば、10.176.176.0/24 です。

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

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

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

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

f) **データ インターフェイス EIP サポート**を有効にします。

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

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

このパスワードは、Nexus ダッシュボードのレスキュー ユーザ ログインと、GUI の管理者ユーザの初期パスワードに使用されます。

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

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

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

たとえば、0.0.0.0/0 は、どこからでもクラスタにアクセスできます。

j) [**次へ（Next）**] をクリックして続行します。

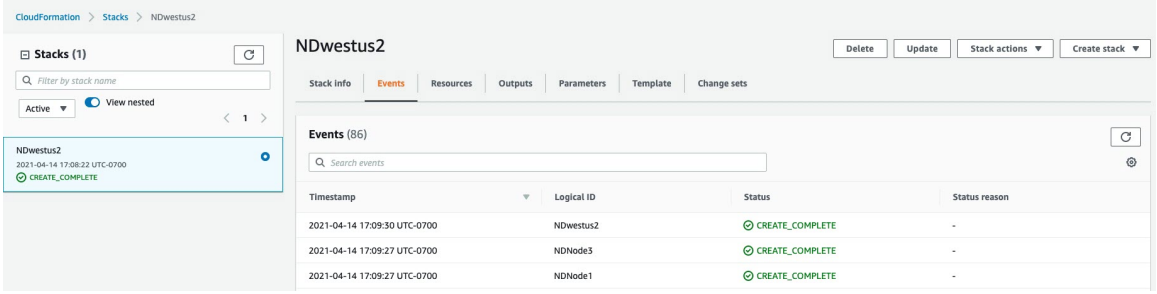
ステップ 6 **[詳細オプション（Advanced options）]** 画面で、**[次へ（Next）]**をクリックします。

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

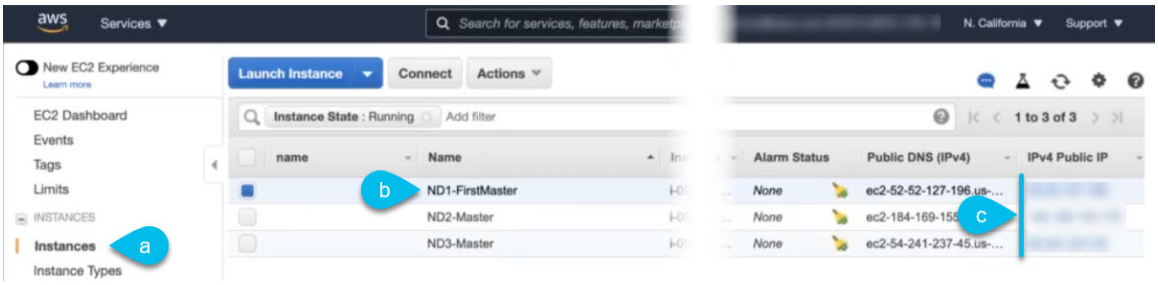
ステップ 8 展開が完了するのを待ってから、VM を起動します。

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

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



ステップ 9 すべてのノードのパブリック IP アドレスを書き留めます。



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

b) `FirstMaster` とラベル付けされているノードを書き留めます。

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

c) すべてのノードのパブリック IP アドレスを書き留めます。

次の手順で、この情報を GUI ブートストラップ ウィザードに提供します。

ステップ 10 すべてのノードでパスワードベースのログインを有効にします。

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

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

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

このために作成した PEM ファイルを 前提条件とガイドライン（101 ページ） の一部として使用します。

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

b) パスワードベースのログインを有効にします。

各ノードで、次のコマンドを実行します。

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

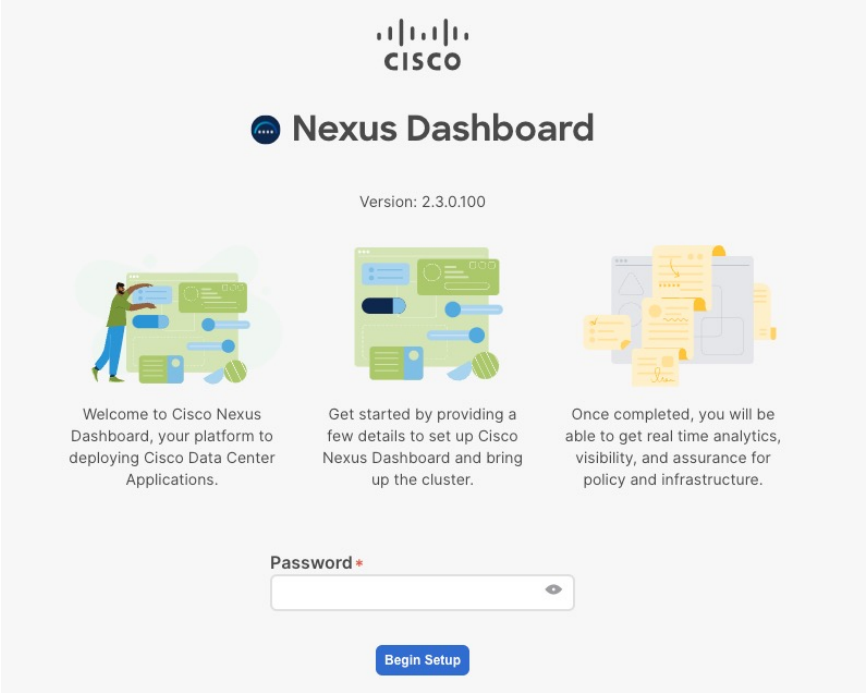
c) 他の 2 つのインスタンスについて、この手順を繰り返します。

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

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

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

テンプレートの展開時に指定したパスワードを入力し、**[セットアップの開始（Begin Setup）]** をクリックします。



ステップ 12 最初のノードで入力したパスワードを入力し、**[セットアップの開始（Begin Setup）]** をクリックします。

ステップ 13 **[クラスタの詳細（Cluster Details）]** を入力します。

初期セットアップ ウィザードの **[クラスタの詳細（Cluster Details）]** 画面で、次の情報を入力します。

a) Nexus ダッシュボード クラスタの **[クラスタ名（Cluster Name）]** を入力します。

b) **[+ NTP ホストの追加（+Add NTP Host）]** をクリックして、1 つ以上の NTP サーバを追加します。

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。

IP アドレスを入力したら、緑色のチェックマーク アイコンをクリックして保存します。

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。

IP アドレスを入力したら、緑色のチェックマーク アイコンをクリックして保存します。

d) **[プロキシ サーバ（Proxy Server）]** を指定します。

Cisco クラウドへの直接接続を持たないクラスタの場合、プロキシサーバを設定して接続を確立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準拠の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。

プロキシ構成をスキップする場合は、フィールドの横にある情報 **(i)** アイコンをクリックしてから、**[スキップ（Skip）]** をクリックします。

e) (オプション)プロキシサーバで認証が必要な場合は、**[プロキシに必要な認証（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。

f) (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。

- **[+DNS 検索ドメインを追加（+Add DNS Search Domain）]** をクリックして、1 つ以上の検索ドメインを指定します。

  IP アドレスを入力したら、緑色のチェックマーク アイコンをクリックして保存します。

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

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

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

  アプリケーションおよびサービスネットワークについては、このドキュメントの前の 前提条件とガイドライン （6 ページ） の項で説明します。

g) **[次へ（Next）]** をクリックして続行します。

ステップ 14 **[ノードの詳細（Node Details）]** 画面で、ノードの情報を入力します。

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

b) ノードの**名前**を入力します。

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

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

c) IPv6 アドレスと VLAN フィールドは空白のままにします。

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

d) **[Save]**をクリックして、変更内容を保存します。

ステップ 15 **[ノードの追加（Add Node）]** をクリックして、クラスタに 2 番目のノードを追加します。

[ノードの詳細（Node Details）] ウィンドウが開きます。

a) ノードの**名前**を入力します。

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

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

c) **[保存 (Save)]**をクリックして、変更内容を保存します。

ステップ 16 前の手順を繰り返して、3番目のノードを追加します。

ステップ 17 [**次へ（Next**）] をクリックして続行します。

ステップ 18 **[確認（Confirmation）]** 画面で **[確認（Confirm）]** をクリックして、クラスタを作成します。

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。

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

ステップ 19 クラスタが健全であることを検証します。

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

3 つすべてのノードの準備ができたら、SSH を使用して任意の 1 つのノードにログインし、次のコマンドを実行してクラスタの状態を確認できます。

a) クラスタが稼働していることを確認します。

任意のノードにログインし、`acs health` コマンドを実行することで、クラスタ展開の現在のステータスを確認できます。

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
```

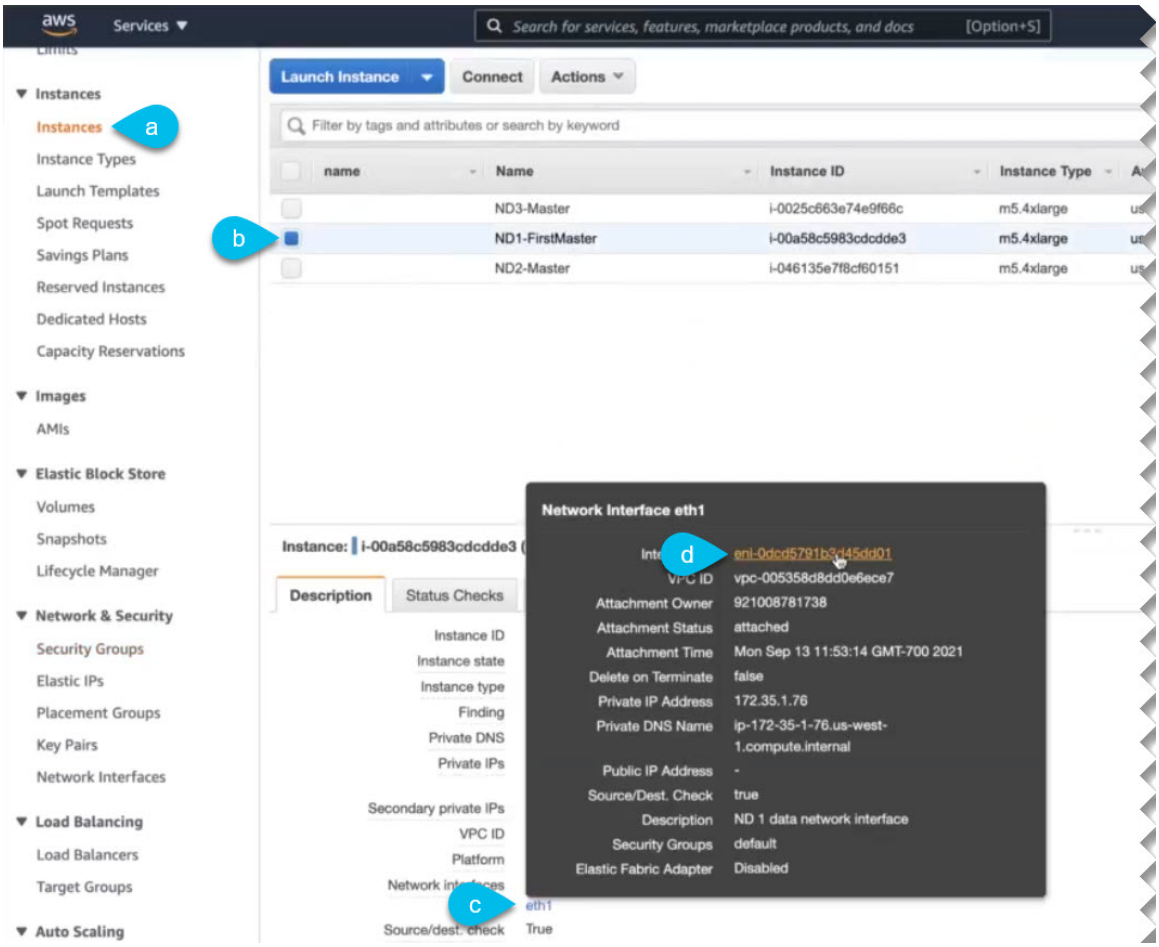
b) Nexus ダッシュボード GUI にログインします。

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。管理者ユーザのデフォルト パスワードは、Nexus ダッシュボード クラスタの最初のノードに選択したレスキュー ユーザ パスワードと同じです。

ステップ 20 必要なポートでノードのセキュリティ グループを更新します。

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

いずれかのノードのデータ インターフェイスに移動します。



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

b) Nexus ダッシュボード インスタンスの 1 つを選択します。

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

c) データ インターフェイスをクリックします（`eth1`）。

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

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

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

新しいルールを追加します。

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

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

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

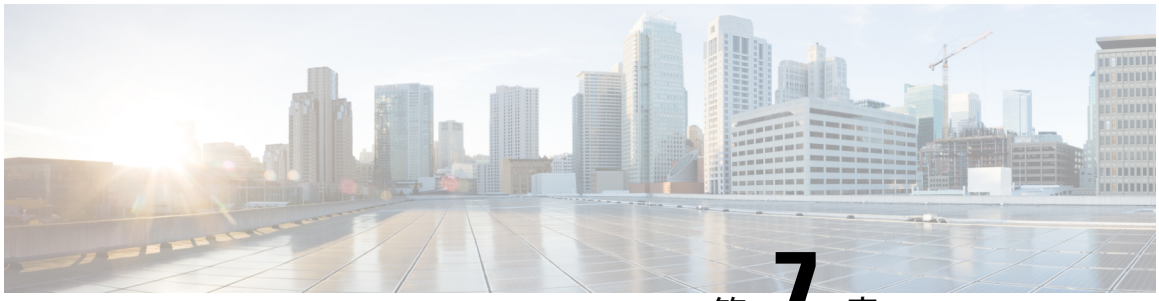
新しいルールについて、次の情報を提供します。

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

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

新しいルールについて、次の情報を提供します。

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



第 7 章

Microsoft Azure での展開

前提条件とガイドライン

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

- ファクターから Azure が拡張性とサービス要件をサポートしていることを確認します。

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

- デプロイ概要 （3 ページ） に記載されている一般的な前提条件を確認して完了します。
- 展開する予定のサービスのリリース ノートに記載されている追加の前提条件を確認して完了します。
- Azure アカウントとサブスクリプションに適切なアクセス権限を持っている。
- Nexus ダッシュボード クラスタ リソースのリソース グループを作成しました。

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

リソース グループを作成するには:

- Azureポータルで、**[すべてのリソース（All Resources）]**>**[リソース グループ（Resource Groups）]** に移動します。

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

- SSH キー ペアを生成します。

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

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

SSH キーの作成については、以下の Linux または MacOS での SSH キー ペアの生成 （114 ページ） および Windows での SSH キー ペアの生成 （115 ページ） セクションで説明します。

Linux または MacOS での SSH キー ペアの生成

次の手順では、Linux または MacOS で SSH 公開キーと秘密キーのペアを生成する方法について説明します。Windows で SSH 公開キーと秘密キーのペアを生成する手順については、を参照してください。Windows での SSH キー ペアの生成 （115 ページ）

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

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

次に例を示します。

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

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

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

ステップ 2 保存した公開キーファイルと秘密キーファイルを見つけます。

```
# ls
```

2 つのファイルが表示されます。

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

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

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

その場合、次のようになります。

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

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

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

Windows での SSH キー ペアの生成

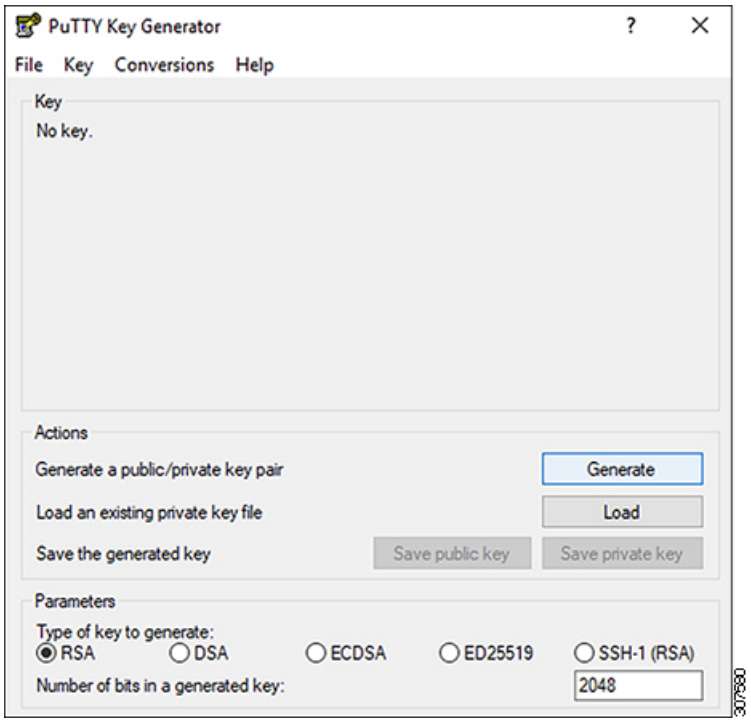
次の手順では、WindowsでSSH公開キーと秘密キーのペアを生成する方法について説明します。LinuxでSSH公開キーと秘密キーのペアを生成する手順については、を参照してください。Linux または MacOS での SSH キー ペアの生成 （114 ページ）

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

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

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

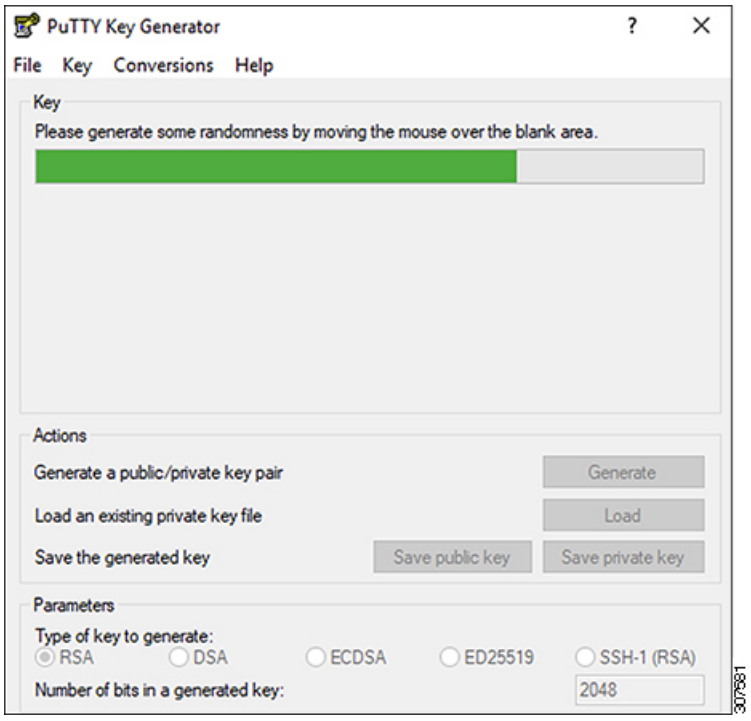
画面にPuTTYキージェネレータのウィンドウが表示されます。



ステップ 3 **[生成（Generate）]** をクリックします。

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

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



ステップ 5 公開キーを保存します。

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

b) PuTTYキージェネレータの情報をコピーします。

次の内容を含めて、ウィンドウに公開キー情報をコピーします。

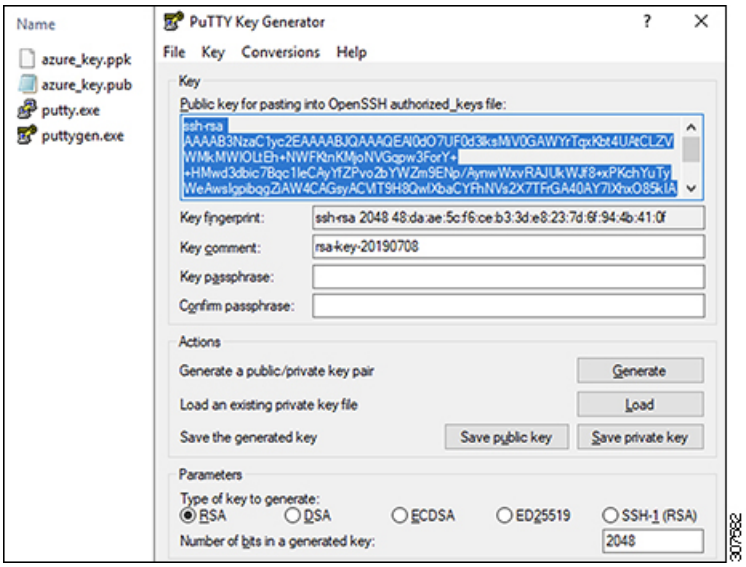
- 公開キーの先頭にssh-rsaテキストを含める。
- 末尾の次のテキスト文字列を除外します。

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

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

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

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



c) で作成した公開キーテキストファイルに情報を貼り付け、ファイルを保存して、一意のファイル名を付けます。5.a （117 ページ）

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

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

ステップ 6 秘密キーを保存します。

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

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

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

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

Azure での Nexus ダッシュボードの展開

このセクションでは、Microsoft Azure で Cisco Nexus ダッシュボード クラスタを展開する方法について説明します。

始める前に

- 前提条件とガイドライン （113 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。

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

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

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

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

c) **[今すぐ取得（Get it now）]** をクリックします。

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

ステップ 2 **基本**情報を提供します。

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

b) **[リソース グループ（Resource group）]** ドロップダウンから、このために作成したリソース グループを 前提条件とガイドライン （113 ページ） の一部として選択します。

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

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

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

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

e) **[SSH 公共キー（SSH public key）]**フィールドに、前提条件とガイドライン （113 ページ） セクションの一部として生成したキーペアの公開キーを貼り付けます。

f) **[次へ (Next)]** をクリックして、次の画面に進みます。

ステップ 3 **ND 設定**情報を提供します。

a) **クラスタ名** を指定します。

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

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

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

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

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

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

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

f) **[次へ (Next)]** をクリックして、次の画面に進みます。

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

ステップ 5 展開が完了するのを待ってから、VM を起動します。

ステップ 6 すべてのノードのパブリック IP アドレスを書き留めます。

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

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

ステップ 7 すべてのノードでパスワードベースのログインを有効にします。

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

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

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

（注） 前提条件とガイドライン（113ページ）セクションで展開用の公開キーを作成するために使用したのと同じマシンを使用する必要があります。

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

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

b) パスワードベースのログインを有効にします。

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

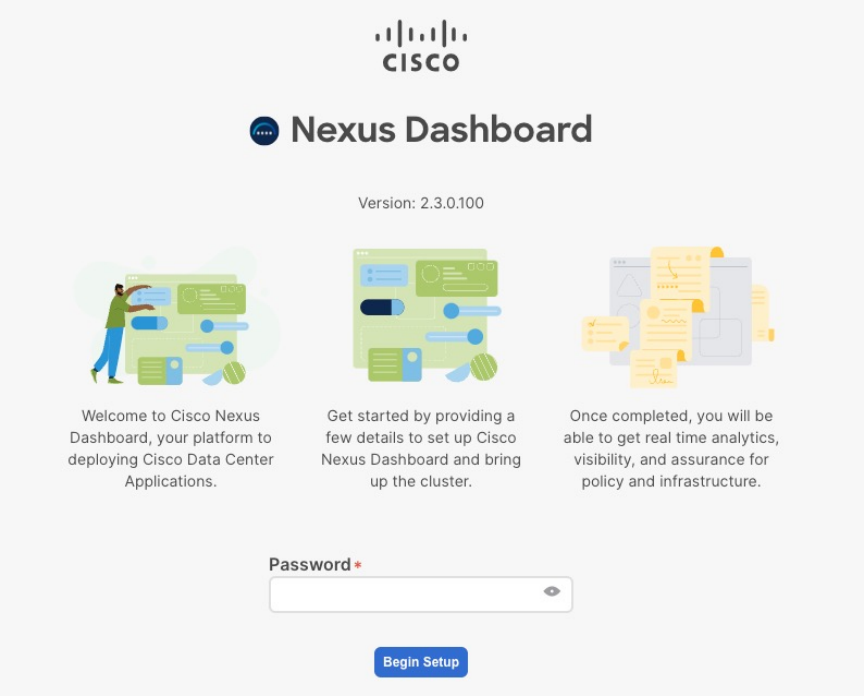
c) 他の 2 つのノードについて、この手順を繰り返します。

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

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

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

テンプレートの展開時に指定したパスワードを入力し、**[セットアップの開始（Begin Setup）]** をクリックします。



ステップ 9 最初のノードで入力したパスワードを入力し、**[セットアップの開始（Begin Setup）]** をクリックします。

ステップ 10 **[クラスタの詳細（Cluster Details）]** を入力します。

初期セットアップ ウィザードの **[クラスタの詳細（Cluster Details）]** 画面で、次の情報を入力します。

a) Nexus ダッシュボード クラスタの **[クラスタ名（Cluster Name）]** を入力します。
b) **[+ NTP ホストの追加（+Add NTP Host）]** をクリックして、1 つ以上の NTP サーバを追加します。

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。

IP アドレスを入力したら、緑色のチェックマーク アイコンをクリックして保存します。

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。

IP アドレスを入力したら、緑色のチェックマーク アイコンをクリックして保存します。

d) **[プロキシ サーバ（Proxy Server）]** を指定します。

Cisco クラウドへの直接接続を持たないクラスタの場合、プロキシサーバを設定して接続を確立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準拠の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。

プロキシ構成をスキップする場合は、フィールドの横にある情報 **(i)** アイコンをクリックしてから、**[スキップ（Skip）]** をクリックします。

e) (オプション) プロキシサーバで認証が必要な場合は、**[プロキシに必要な認証（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。

f) (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。

- **[+DNS 検索ドメインを追加（+Add DNS Search Domain）]** をクリックして、1 つ以上の検索ドメインを指定します。

  IP アドレスを入力したら、緑色のチェックマーク アイコンをクリックして保存します。

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

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

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

  アプリケーションおよびサービスネットワークについては、このドキュメントの前の 前提条件とガイドライン （6 ページ） の項で説明します。

g) [**次へ（Next）**] をクリックして続行します。

ステップ 11 **[ノードの詳細（Node Details）]** 画面で、ノードの情報を入力します。

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

b) ノードの**名前**を入力します。

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

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

c) IPv6 アドレスと VLAN フィールドは空白のままにします。

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

d) **[Save]**をクリックして、変更内容を保存します。

ステップ 12 **[ノードの追加（Add Node）]** をクリックして、クラスタに 2 番目のノードを追加します。

[ノードの詳細（Node Details）] ウィンドウが開きます。

a) ノードの**名前**を入力します。

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

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

c) **[保存 (Save)]**をクリックして、変更内容を保存します。

ステップ 13 前の手順を繰り返して、3番目のノードを追加します。

ステップ 14 [**次へ（Next）**] をクリックして続行します。

ステップ 15 **[確認（Confirmation）]** 画面で **[確認（Confirm）]** をクリックして、クラスタを作成します。

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。

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

ステップ 16 クラスタが健全であることを検証します。

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

3 つすべてのノードの準備ができたら、SSH を使用して任意の 1 つのノードにログインし、次のコマンドを実行してクラスタの状態を確認できます。

a) クラスタが稼働していることを確認します。

任意のノードにログインし、`acs health` コマンドを実行することで、クラスタ展開の現在のステータスを確認できます。

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。

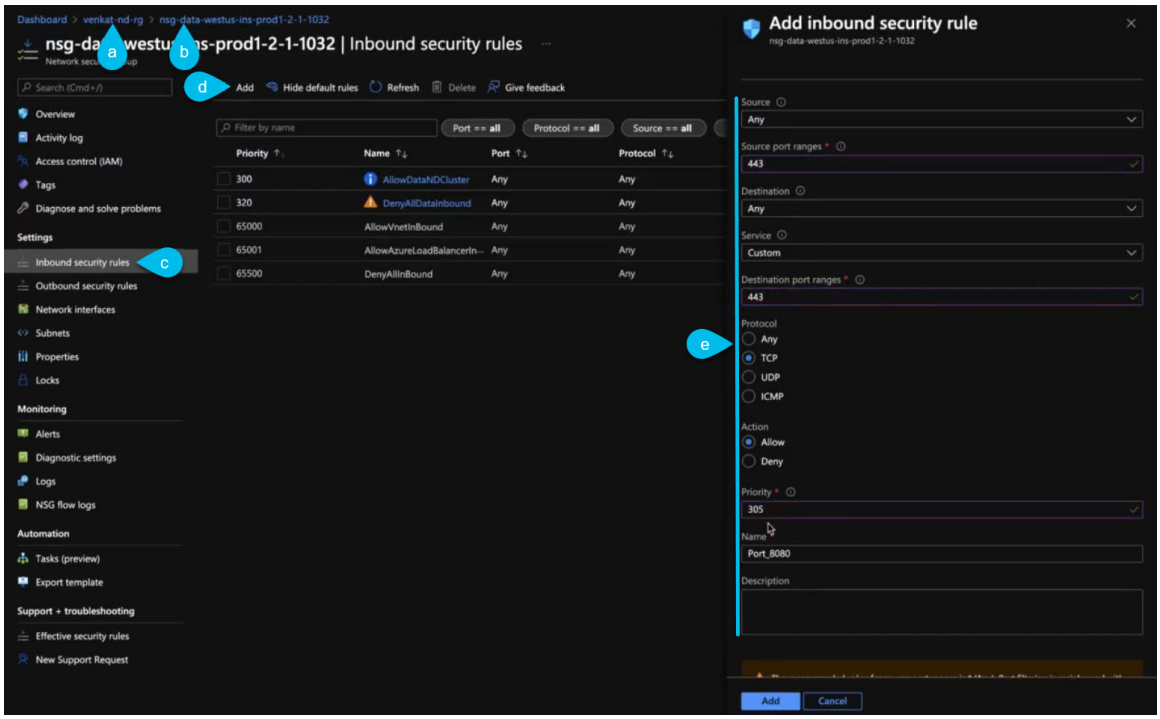
```
$ acs health
All components are healthy
```

b) Nexus ダッシュボード GUI にログインします。

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。管理者ユーザのデフォルト パスワードは、Nexus ダッシュボード クラスタの最初のノードに選択したレスキュー ユーザ パスワードと同じです。

ステップ 17 必要なポートでノードのセキュリティ グループを更新します。

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



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

これは、手順 2 で選択したのと同じリソース グループです。

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

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

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

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

新しいルールについて、次の情報を提供します。

- **[送信元（Source）]** で、[任意（Any）] を選択します。
- **[送信元ポート範囲（Source port ranges）]** には、443 と入力します。
- **[宛先（Destination）]** で、[任意（Any）] を選択します。

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

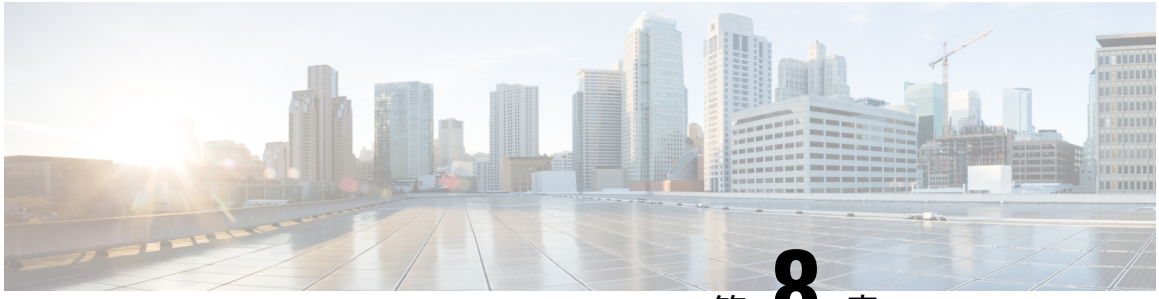
  たとえば、305 です。
- ルールの**名前**を指定します。

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

前のサブステップを繰り返して、次の詳細を含む別のルールを追加します。

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

  例えば、310。
- ルールの**名前**を指定します。



第 8 章

既存の Red Hat Enterprise Linux インストールでの展開

前提条件とガイドライン

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

- デプロイ概要 （3 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。

  このガイドは Nexus ダッシュボード UI から、または『*Cisco Nexus* ダッシュボード ユーザガイド』でオンラインから入手可能です。

- 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。

- サーバーで Red Hat Enterprise Linux（RHEL）リリース 8.4 または、8.6 が実行されていることを確認します。

  Nexus ダッシュボードのこのリリースは、RHEL の物理展開と仮想展開のどちらもサポートしています。

（注） ラボやテストなどの非運用展開の場合、既存の Red Hat Enterprise Linux インストールでの Nexus ダッシュボードの展開 （128 ページ）セクションの**手順 4** で追加のパラメータをインストーラに渡すことで、他の Linux 流通に展開できます。

```
./nd-installer setup ./examples/nd-linux-input.yaml
skip-os-version-check
```

- RHEL では、単一ノードまたは 3 ノード（すべてのマスターノード）クラスタのみ展開することができます。

  このクラスタフォームファクタでは、ワーカーノードまたはスタンバイノードの追加はサポートされていません。

- RHEL で展開されたクラスタは、Nexus ダッシュボード ファブリック コントローラ（NDFC）、リリース 12.1(1) 以降のサービスと **SAN コントローラ**の展開タイプのみをサポートします。

  他の Nexus ダッシュボードサービスまたは別の展開タイプの NDFC を実行する場合は、他のフォームファクタの 1 つを展開する必要があります。Nexus ダッシュボードクラスタのフォーム ファクタごとにサポートされるサービスの詳細については、「Cisco Nexus ダッシュボードクラスタのサイズ」および「Nexus ダッシュボードとサービスの互換性マトリックス」を参照してください。

- 次のシステム レベルの要件が満たされていることを確認します。

  - インストーラで指定し、ノードの管理とトラブルシューティングに使用できる、各クラスタノードの既存の Linux ユーザー。

    Nexus ダッシュボードノードのシステムに接続できるシステムユーザーは 1 人だけです。詳細については、展開後に「RHEL での Nexus ダッシュボード展開に関するトラブルシューティング （136 ページ）」を参照してください。

  - すべてのノードのシステムクロックを同期する必要があります。

    `chrony` などのシステムユーティリティを使用すると、ノード間での正確な時刻同期を確実に行うことができます。

（注） デフォルトでは、RHEL の Nexus ダッシュボードインストーラは、`chrony` を使用してシステムクロックが同期されていることを確認します。別のシステムを使用してクロックを同期する場合は、インストール時に `./nd-installer setup input.yaml` **`skip-ntp-check`** を使用して、デフォルトの検証を無視することができます。

  - Skopeo パッケージがインストールされています。

    Skopeo はこのドキュメントの範囲外ですが、簡単に言うと、`yum install skopeo` コマンドを使用してパッケージをインストールすることができます。

  - スワップファイルが無効になっています。

    スワップを無効にするには、`/etc/fstab` ファイルからそのエントリを削除し、サーバーを再起動します。

  - `firewalld` および `libvirt` サービスが停止し、無効になっています。

（注） Nexus ダッシュボードソフトウェアを展開すると、次の追加のシステムレベルの変更が適用され、追加のディレクトリおよびクラスタ独自の SSH サーバーからの実行可能ファイルが許可されます。

```
/usr/bin/chcon -R -t bin_t /mnt/atom
/usr/bin/chcon -R -t bin_t /mnt/linux
/usr/bin/chcon -R -t bin_t /opt/apic-sn

/usr/bin/chcon -t ssh_home_t -R
/data/services/issh/ssh_host_rsa_key
/usr/bin/chcon -t ssh_home_t -R /data/services/issh/intssh
/usr/sbin/semanage port -a -t ssh_port_t -p tcp 1022
```

- 十分なシステムリソースがあることを確認します。

  RHELで展開する場合、展開できるノードには2 種類あります。

表 *19 :* 導入要件

Nexus Dashboard バージョン	デフォルト ノード プロファイル	大規模ノードプロファイル
リリース 2.3.x	• 16 vCPU • 64 GB の RAM • データボリューム用に 500GB SSD ストレージ、システムボリューム用に追加の 100GB。 すべてのノードは SSD またはより高速なストレージに展開する必要があります。 • RHEL の管理インターフェイスに加えて 2 つのネットワーク インターフェイス。	• 32 vCPU • 128 GBのRAM • データボリューム用に 3TB SSD ストレージ、システムボリューム用に追加の 100GB。 データボリュームは、ドライブがオペレーティングシステムに単一のデバイスとして認識されている限り、複数のドライブの組み合わせ（RAID 構成など）にすることができます。 すべてのノードは SSD またはより高速なストレージに展開する必要があります。 • RHEL の管理インターフェイスに加えて 2 つのネットワーク インターフェイス。

既存の Red Hat Enterprise Linux インストールでの Nexus ダッシュボードの展開

ここでは、RHEL で Nexus ダッシュボードクラスタを設定して起動する方法について説明します。

始める前に

- 前提条件とガイドライン （125 ページ） に記載されている要件とガイドラインを満たしていることを確認します。

ステップ 1 Cisco Nexus ダッシュボード ソフトウェア アーカイブ パッケージ（tarball）を入手します。

a) [ソフトウェアのダウンロード]ページに移動します。

https://www.cisco.com/c/en/us/support/data-center-analytics/nexus-dashboard/series.html

b) [ダウンロード（Downloads）] タブをクリックします。

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

d) Nexus ダッシュボードの tarball の横にある**ダウンロード**アイコンをクリックします（`nd-rhel-<version>.tar`）。

ステップ 2 ダウンロードしたアーカイブを解凍します。

```
tar -xvf nd-rhel-<version>.tar
```

ステップ 3 `yaml` インストールファイルを変更します。

ディストリビューションの tarball には、サンプルの YAML ファイル（`./nd-linux/examples/nd-linux-input.yaml`）が含まれています。これを変更して、展開に適した値を指定できます。

たとえば、次のサンプルのノード構成 YAML ファイルでは、指定する必要がある特定のフィールドが強調表示されています。

- `blkdev` の場合、ノードのイメージボリュームとデータボリュームに SSD デバイスを指定します。

  イメージ用とデータ用の 2 つのデバイスを指定する必要があります。YAML ファイル内のデバイスの順序は関係ありません。小さい方のディスクがイメージに使用され、大きい方のディスクがデータに使用されます。

  （注） 両方のデバイスが消去され、Nexus ダッシュボードノードに使用されます。

  ノードデバイスの詳細については、「前提条件とガイドライン （125 ページ）」を参照してください。

- `oobNetwork` に、管理ネットワーク情報を入力します。

- アップリンクに、クラスタの管理とデータネットワークに使用されるネットワークインターフェイスの名前を指定します。

  これらのインターフェイスは、Nexus ダッシュボード専用にする必要があります。

- ipNet に、ノードの管理ネットワークの IPv4 アドレスとネットマスクを、172.23.152.214/24 の形式で指定します。

- gatewayIP に、ノードの管理ネットワーク IPv4 ゲートウェイを入力します。

- ipv6Net に、ノードの管理ネットワーク IPv6 アドレスとネットマスクを、2001:420:286:2000:6:15:152:220/112 の形式で指定します。

  クラスタにデュアルスタック IPv4/IPv6 を構成していない場合は、このパラメータを省略できます。

- gatewayIPv6 に、ノードの管理ネットワーク IPv6 ゲートウェイを入力します。

  クラスタにデュアルスタック IPv4/IPv6 を構成していない場合は、このパラメータを省略できます。

- inbandNetwork には、残りの構成は GUI ブートストラップ プロセス中に定義されるため、[アップリンク] セクションでインターフェイスのみを指定する必要があります。

- firstMaster には、ノードの 1 つだけが true に設定され、他の 2 つのノードが false に設定されているようにします。

  GUI を使用してクラスタ ブートストラップ プロセスを完了するには、firstMaster ノードを使用します。

- clusterName には、クラスタの名前を指定します。

- installProfile には、[デフォルト（Default）] または [大（Large）] を選択します。

  ノードプロファイル要件の詳細については、「前提条件とガイドライン（125 ページ）」を参照してください。

- serviceUser には、Nexus ダッシュボードノードの管理とトラブルシューティングに使用される既存の Linux アカウント名を指定します。

  （注） serviceUser は、システムの root ユーザーとは異なる必要があります。

```
# Node Definition
# 'Master' / 'Worker' / 'Standby'. Only Master supported in 2.2
nodeRole: Master

# Block devices. Can be complete device or partition. Should meet profile requirements.
blkdev:
  - type: SSD
    name: "/dev/sdb"
  - type: SSD
    name: "/dev/sdc"

# Networking
# ND needs exclusively 2 interfaces. Has to be separate from the linux management interface.
oobNetwork:
```

```
   uplinks:
  - ens924
  ipNet: 172.23.152.214/24
  gatewayIP: 172.23.152.1
  ipv6Net: 2001:420:286:2000:6:15:152:220/112
  gatewayIPv6: 2001:420:286:2000:6:15:152:1

# Just the interface for the inbandNetwork, rest can be provided at ND bootstrap UI
inbandNetwork:
  uplinks:
  - ens956

# 'true' for one of the masters in a cluster
firstMaster: true

clusterName: nd-cluster

#Installation Profile. Default / Large. Large is used for NDFC SAN installations
installProfile: Default

#Linux username. Cannot be root. Only this user will have privileges to execute certain ND diag
commands.
serviceUser: nduser
```

ステップ 4 Nexus ダッシュボード ノード ソフトウェアをインストールします。

```
cd nd-linux
./nd-installer setup ./examples/nd-linux-input.yaml
```

Nexus ダッシュボードクラスタの管理者アカウントに使用される、パスワードを入力するように求められます。

（注） デフォルトでは、インストーラは chrony を使用してシステムクロックが同期されていることを確認します。別のシステムを使用してクロックを同期する場合は、デフォルトの検証をバイパスするために./nd-installer setup./examples/nd-linux-input.yaml **skip-ntp-check** を使用することができます。

ステップ 5 これまで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。

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。

最初のノードのインストール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。

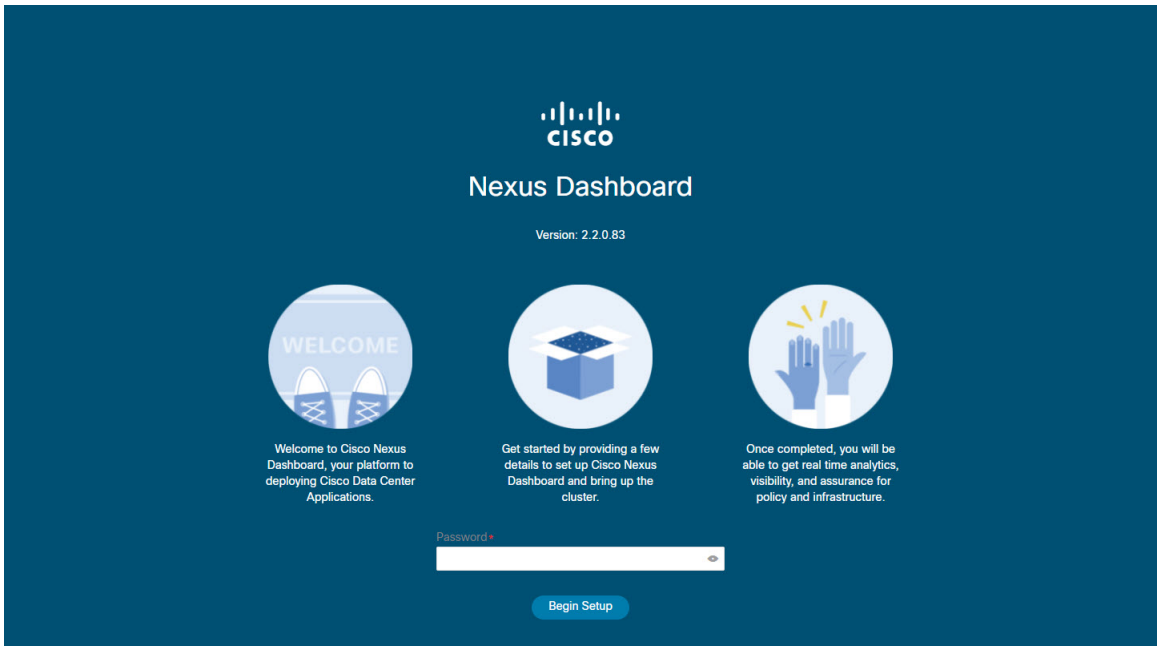
（注） 2 番目と 3 番目のノードの構成 YAML ファイルでノードの詳細を指定する時に、firstMaster パラメータが false に設定されていることを確認してください。

ステップ 6 3 つすべてノードの展開が完了するまで待ちます。

ステップ 7 ブラウザを開き、https://<first-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。firstMaster として指定したノードに指定した IP アドレスを使用する必要があります。

前の手順で入力したパスワードを入力し、**[セットアップの開始（Begin Setup）]** をクリックします。



ステップ 8 **[クラスタの詳細（Cluster Details）]** を入力します。

初期セットアップ ウィザードの **[クラスタの詳細（Cluster Details）]** 画面で、次の情報を入力します。

a) Nexus ダッシュボード クラスタの **[クラスタ名（Cluster Name）]** を入力します。

b) **[+ NTP ホストの追加（+Add NTP Host）]** をクリックして、1 つ以上の NTP サーバを追加します。

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。

IP アドレスを入力したら、緑色のチェックマーク アイコンをクリックして保存します。

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。

IP アドレスを入力したら、緑色のチェックマーク アイコンをクリックして保存します。

d) **[プロキシ サーバ（Proxy Server）]** を指定します。

Cisco クラウドへの直接接続を持たないクラスタの場合、プロキシ サーバを設定して接続を確立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準拠の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。

プロキシ構成をスキップする場合は、フィールドの横にある情報 **(i)** アイコンをクリックしてから、**[スキップ（Skip）]** をクリックします。

e) (オプション) プロキシ サーバで認証が必要な場合は、**[プロキシに必要な認証（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。

f) (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。

- **[+DNS 検索ドメインを追加（+Add DNS Search Domain）]** をクリックして、1 つ以上の検索ドメインを指定します。

IP アドレスを入力したら、緑色のチェックマーク アイコンをクリックして保存します。

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

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

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

  アプリケーションおよびサービスネットワークについては、このドキュメントの前の 前提条件とガイドライン （6 ページ） の項で説明します。

g) [**次へ（Next）**] をクリックして続行します。

ステップ 9 **[ノードの詳細（Node Details）]** 画面で、ノードの情報を入力します。

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

b) [**パスワード（Password）**] フィールドに、このノードのパスワードを入力し、[**検証（Validate）**] をクリックします。

これにより、ノードの [**名前（Name）**]、[**シリアル番号(Serial Number)**]、および [**管理ネットワーク（Management Network）**] の情報が自動入力されます。

ノードの [**名前（Name）**] には、ノードソフトウェアがインストールされている RHEL サーバーのホスト名が使用されます。

c) ノードの**データ ネットワーク**情報を入力します。

管理ネットワーク情報には、最初のノードに指定した情報があらかじめ入力されています。

データネットワークの IP アドレス/ネットマスク（たとえば、`172.31.140.58/24`）とゲートウェイ（たとえば、`172.31.140.1`）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。

d) （オプション）管理およびデータ ネットワークの IPv6 情報を指定します。

Nexus ダッシュボードは、管理およびデータネットワークの IPv4 またはデュアルスタック IPv4/IPv6 のいずれかをサポートします。

（注） IPv6 情報を指定する場合は、このクラスタブートストラップのプロセス中に行う必要があります。IPv4 スタックのみを使用してクラスタを展開し、後で IPv6 情報を追加する場合は、クラスタを再度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スタックまたはデュアル IPv4/IPv6スタックのいずれかで設定する必要があります。

e) （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**。

NDFC ファブリックを使用した Nexus ダッシュボード Insights などの一部のサービスで必要な永続的な IP 機能には、BGP 構成が必要です。この機能については、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。

- 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 10 [**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。

[ノードの詳細（Node Details）] ウィンドウが開きます。

a) [**展開の詳細**（**Deployment Details**）] セクションで、ノードの**管理 IP アドレス**と**パスワード**を入力し、[**検証**（**Verify**）] をクリックします。

これは、ステップ 4 のインストール中に `./nd-installer setup` コマンドに指定したパスワードです。

IP とパスワードを確認すると、ノードの [**名前**（**Name**）]、[**シリアル番号(Serial Number)**]、および [**管理ネットワーク**（**Management Network**）] の情報が自動入力されます。

ノードの [**名前**（**Name**）] には、ノードソフトウェアがインストールされている RHEL サーバーのホスト名が使用されます。

b) ノードの**名前**を入力します。

c) ノードの**データ ネットワーク** IP アドレスとゲートウェイを指定します。

[**管理ネットワーク**（**Management Network**）] 情報には、前のサブステップで指定した IP アドレスとログイン情報に基づいてノードから取得した情報が事前に入力されます。

データネットワークの IP アドレス/ネットマスク（たとえば、`172.31.141.58/24`）とゲートウェイ（たとえば、`172.31.141.1`）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。

d) （任意）管理およびデータネットワークのIPv6情報を指定します。

Nexus ダッシュボードは、管理およびデータネットワークの IPv4 またはデュアルスタック IPv4/IPv6 のいずれかをサポートします。

（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。IPv4 スタックのみを使用してクラスタを展開し、後で IPv6 情報を追加する場合は、クラスタを再度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スタックまたはデュアル IPv4/IPv6スタックのいずれかで設定する必要があります。

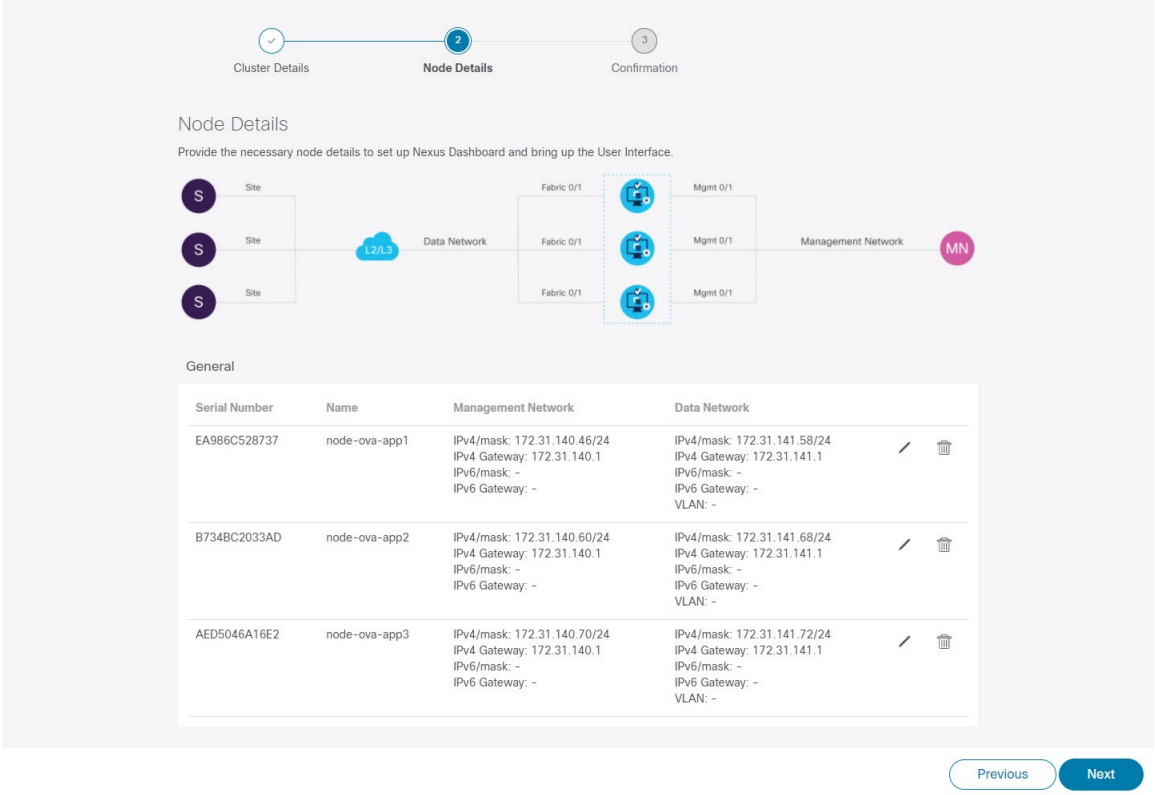
e) （任意）必要に応じて、データ ネットワークの **BGP を有効にします**。

f) **[保存 (Save)]**をクリックして、変更内容を保存します。

ステップ 11 前の手順を繰り返して、3番目のノードを追加します。

ステップ 12 **[ノードの詳細（Node Details）]** 画面で、**[次へ（Next）]** をクリックして続行します。

クラスタ内の 3 つのノードすべての情報を入力したら、ブートストラッププロセスの次の画面に進みます。



ステップ 13 **[確認（Confirmation）]** 画面で設定情報を確認し、**[構成（Configure）]** をクリックしてクラスタを作成します。

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 14 クラスタが健全であることを検証します。

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

3 つすべてのノードの準備ができたら、構成 YAML で指定した `serviceUser` を使用して、SSH を介して任意の 1 つのノードにログインし、次のコマンドを実行してクラスタの状態を確認できます。

a) Linux システムにログインした後、`/usr/bin/attach-nd` コマンドを使用してノードに接続します。

このコマンドは、`serviceUser` ユーザーのみが使用できます。

b) クラスタが稼働していることを確認します。

任意のノードにログインし、`acs health` コマンドを実行することで、クラスタ展開の現在のステータスを確認できます。

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
```

c) Nexus ダッシュボード GUI にログインします。

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。管理者ユーザーのデフォルトのパスワードは、ステップ 4 のインストール中に `./nd-installer setup` コマンドに指定したパスワードと同じです。

Nexus ダッシュボードソフトウェアのアンインストール

Nexusダッシュボードノードソフトウェアが展開されると、アンインストーラが `/usr/bin` ディレクトリにコピーされます。

任意の時点でソフトウェアをアンインストールする場合、ルートユーザーとして次のコマンドを実行します。

```
/usr/bin/nd-installer uninstall
```

（注） SSHを使用してRHELシステムにログインする場合、アンインストールするには、システムの管理 IP アドレスに接続する必要があります。 Nexus ダッシュボードの管理 IP アドレスは使用しないでください。

これにより、ソフトウェアが削除され、インストールプロセス中に行われたファイルシステムの変更が元に戻されます。

RHEL での Nexus ダッシュボード展開に関するトラブルシューティング

このセクションでは、RHEL に展開された Nexus ダッシュボードソフトウェアの一般的なトラブルシューティング手順について説明します。

ステップ 1 インストール ログを確認します。

Nexus ダッシュボードのインストールログは、次のディレクトリにあります。

```
/logs/ndlinux/
```

ステップ 2 インストールが完了したら、Nexus ダッシュボード環境にアクセスします。

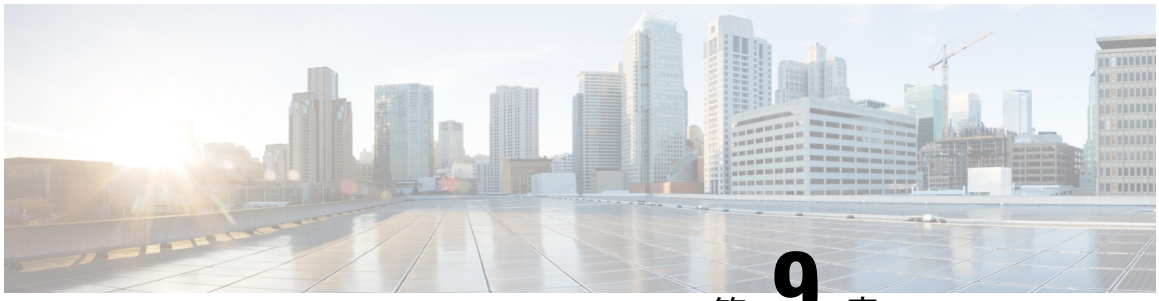
a) インストール時に YAML 構成ファイルで指定した Nexus ダッシュボードユーザーを使用して、RHEL システムにログインします。

b) Nexus ダッシュボード環境にアクセスします。

```
/usr/bin/attach-nd
```

c) 一般的な Nexus ダッシュボードのトラブルシューティング コマンドを使用します。

Nexus ダッシュボード環境にアクセスすると、『*Cisco Nexus ダッシュボード ユーザーガイド*』の「トラブルシューティング」セクションで説明されている、すべての一般的な Nexus ダッシュボードコマンドを使用できます。



第 9 章

Nexus ダッシュボードのアップグレード

前提条件とガイドライン

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

- アップグレードに影響する可能性のある動作、ガイドライン、および問題の変更については、ターゲット リリースのリリース ノートを必ずお読みください。

  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 ファクタで同じです。ただし、既存のクラスタが物理サーバー、VMware ESX、Linux KVM、Azure、または AWS を使用して展開されている場合は、ターゲット リリースの ISO イメージ（`nd-dk9.<version> .iso`）アップグレードします。既存のクラスターが Red Hat Enterprise Linux に展開されている場合は、RHEL 固有のイメージ（`nd-rhel- .tar` ）。

- 既存のクラスタで実行するサービスのリリース ノートおよびアップグレード ガイドを確認し、アップグレードに影響する可能性がある動作、注意事項、問題でサービス固有の変更について対象のリリースで実行を計画する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 ファブリック コントローラ、アップグレード ガイド
  - Nexus Dashboard Insights リリース ノート
  - Nexus Dashboard Insights アップグレード ガイド
  - Nexus Dashboard Orchestrator リリース ノート
  - Nexus Dashboard Orchestrator アップグレード ガイド

- 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* ユーザー ガイド の「トラブルシューティング」セクションで詳しく説明されています。

- アップグレードを続行する前に、データを保護し、潜在的なリスクを最小限に抑えるために、アップグレードの前にNexusダッシュボードとサービスの構成バックアップを実行する必要があります。
- 2.3(x) リリースにアップグレードするために必要な Nexus Dashboard の最小リリースは、クラスタにデプロイした特定のサービスによって異なります。

  詳細については、上記にリンクされているサービス固有のリリース ノートとアップグレード ガイドを確認してください。
- リリース 2.3(x) にアップグレードする前に、クラスタで実行されているすべてのサービスを無効にする必要があります。
  - Nexus Dashboard を同じリリース内の 1 つのパッチから別のパッチにアップグレードする場合 (たとえば、2.3.2b から 2.3.2d に)、Nexus Dashboard のアップグレードが完了したら、サービスを再度有効にします。
  - Nexus Dashboard をあるリリースから別のリリース (たとえば、2.3.1 から 2.3.2) にアップグレードする場合、既存のサービスはターゲットの Nexus Dashboard リリースと互換性がない可能性があります。プラットフォームのアップグレードが完了しました。

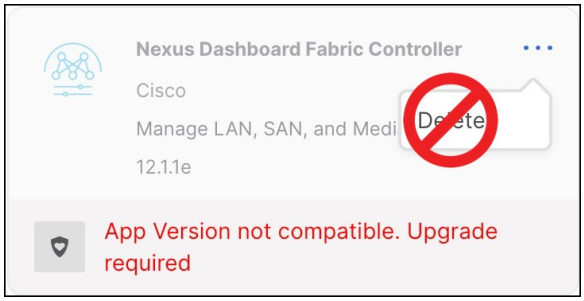
    Nexus ダッシュボードとサービスの相互運用性サポートの完全なリストについては、「Nexus ダッシュボードとサービスの互換性マトリクス」またはこのセクションで前に示したサービス特有のアップグレード ガイドを参照してください。

（注）

- Nexus Dashboard ファブリック コントローラの場合、クラスタがアップグレードされた後で、サービスも同様にアップグレードするまでサービスを無効にしたままにする必要があります。

  Nexus Dashboard クラスタがアップグレードされた後で、既存のバージョンのサービスが互換性のない アプリ バージョンとともにリストされる場合があります。アップグレードが必要です。 警告です。

  ファブリック コントローラ アップグレード イメージをアップロードする前にこのバージョンを**削除または再度有効にする**必要があります。新しいバージョンをアップロードしたら、古いリリースを削除する前に、それを有効にしてサービスのアップグレードを完了する必要があります。新しいリリースがアクティブ化される前に古いサービス バージョンを削除すると、アップグレードが失敗する可能性があります。

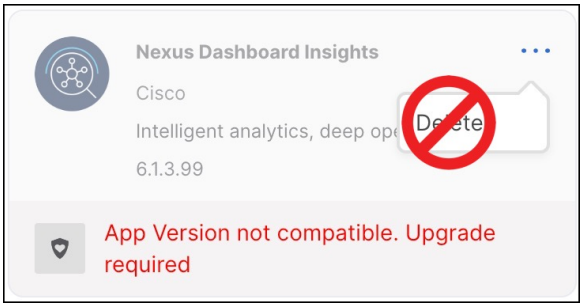


- Nexus Dashboard Insights の場合、クラスタがアップグレードされた後で、サービスも同様にアップグレードするまでサービスを無効にしたままにする必要があります。

  Nexus Dashboard クラスタがアップグレードされた後で、既存のバージョンのサービスが互換性のない アプリ バージョンとともにリストされる場合があります。アップグレードが必要です。 警告です。

  Insights のアップグレード イメージをアップロードする前にこのバージョンを**削除または再度有効にする**必要があります。新しいバージョンをアップロードしたら、古いリリースを削除する前に、それを有効にしてサービスのアップグレードを完了する必要があります。新しいリリースがアクティブ化される前に古いサービス バージョンを削除すると、アップグレードが失敗する可能性があります。

Nexus ダッシュボードのアップグレード



- Nexus Dashboard Orchestrator の場合、新しいバージョンをアップロードしてアクティブ化する前に、既存のバージョンを再度有効にする必要があります。

- 有効な DNS および NTP サーバーが構成され、すべてのクラスター ノードから到達可能である必要があります。
- 現在の Nexus ダッシュボードクラスタが正常であることを確認します。

  Nexus ダッシュボードの**管理コンソール（Admin Console）**の **[概要（Overview）]** ページでシステムのステータスを確認するか、`rescue-user` としてノードの1つにログインし、`acs health` コマンドを実行して `All components are healthy` が返ってくることを確認します。
- アップグレードが進行中にワーカーまたはスタンバイ ノードを追加するなど、設定変更がクラスタに対して行われていないことを確認します。
- Nexus Dashboard ではプラットフォームのダウングレードはサポートされていません。

  以前のリリースにダウングレードするには、新しいクラスタを展開してサービスを再インストールする必要があります。

Nexus ダッシュボードのアップグレード

ここでは、既存の Nexus ダッシュボード クラスタをアップグレードする方法について説明します。

始める前に

- で説明している前提条件をすべて満たしていることを確認します。前提条件とガイドライン （137 ページ）

ステップ 1 Nexusダッシュボードイメージをダウンロードします。

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

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

Nexus ダッシュボードのアップグレード

b) ダウンロードするNexusダッシュボードのバージョンを選択します。
c) ターゲットとするリリース用の Cisco Nexus ダッシュボード イメージをダウンロードします。

（注）
- Nexus ダッシュボードが Red Hat Enterprise Linux に展開されている場合は、`.tar` イメージ (`nd-rhel-<version> .tar`) を使用してアップグレードを実行します。

  RHEL の展開の詳細については、既存の Red Hat Enterprise Linux インストールでの展開 （125 ページ）を参照してください。

- 他のすべてのフォームファクターについては、`.iso`イメージ（`nd-dk9.<version>.iso`）を使用してアップグレードを実行します。

  たとえば、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（VMware ESX での展開のための `.ova` イメージなど）、またはクラウドプロバイダーのマーケットプレースを使用していた場合であっても、アップグレードでは `.iso` イメージを使用する必要があります。

d) （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。

イメージをNexusダッシュボード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。

ステップ 2 現在の Nexus Dashboard GUI に管理者ユーザーとしてログインして、**管理コンソール**に移動します。

ステップ 3 クラスタにインストールされている既存のサービスを無効にします。

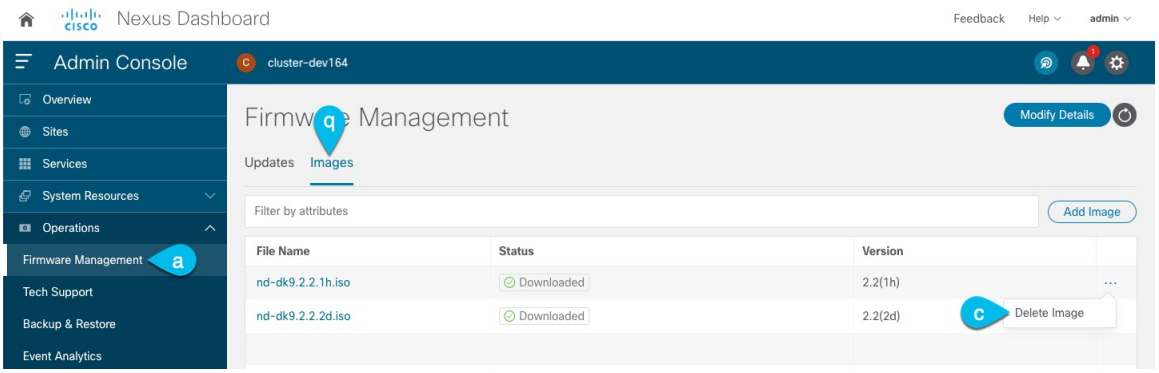
（注） クラスタのアップグレードをする前にすべてのサービスを無効化する必要があります。

a) メイン ナビゲーション メニューから **[サービス（Services）]** を選択します。
b) サービスのタイルで、**[アクション] (...)** メニューをクリックし、**[無効化]** を選択します。
c) クラスタに展開されている他のすべてのサービスについて、この手順を繰り返します。

ステップ 4 クラスタから既存のアップグレード イメージを削除します。

クラスタを初めてアップグレードする場合は、この手順をスキップできます。

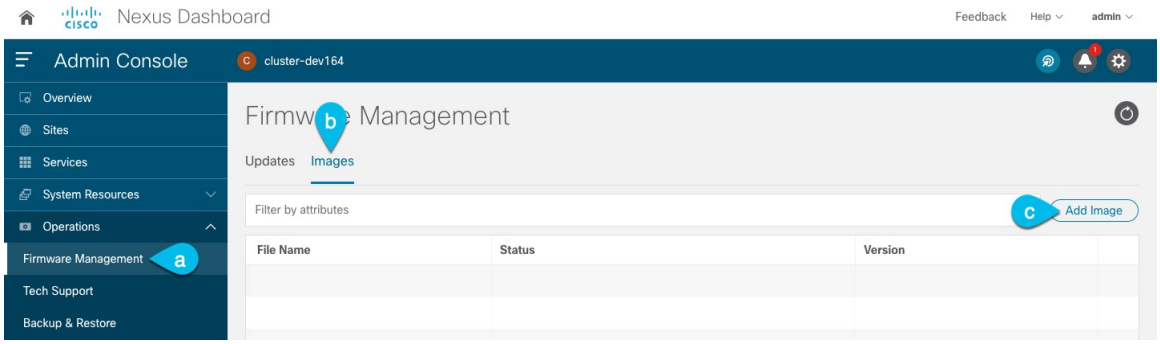
以前にクラスタを現在のバージョンにアップグレードしたことがある場合は、以前のアップグレードで使用されたアップグレード イメージを削除する必要があります



a) **[Operations（オペレーション）]** > **[ファームウェア管理（Firmware Management）]** に移動します。

b) **[イメージ]** タブを選択します。
c) 既存のアップグレードイメージの横にあるアクション メニュー（...）から、**[イメージの削除（Delete Image）]** を選択します。
d) すべての既存のアップグレード イメージについて、この手順を繰り返します。

ステップ 5 新しいイメージをクラスタにアップロードします。



a) **[Operations（オペレーション）]** > **[ファームウェア管理（Firmware Management）]** に移動します。
b) **[イメージ]** タブを選択します。
c) [Add Image] をクリックします。

ステップ 6 新しいイメージを選択します。

a) **[ファームウェア イメージの追加（Add Firmware Image）]**ウィンドウで、**[ローカル（Local）]** を選択します。

   または、ウェブ サーバでイメージをホストした場合は、代わりに**[リモート（Remote）]** を選択します。

b) **[ファイルの選択（Select file）]** をクリックし、最初の手順でダウンロードした `.iso` または `.tar` イメージを選択します。

   RHEL での展開の場合、`.tar` ファイルを使用してアップグレードします。他のすべての展開ファクターの場合、`.iso` ファイルを使用します。

   リモート イメージのアップロードを選択した場合は、リモート サーバ上のイメージのファイル パスを指定します。

c) **[アップロード（Upload）]** をクリックして、イメージを追加します。

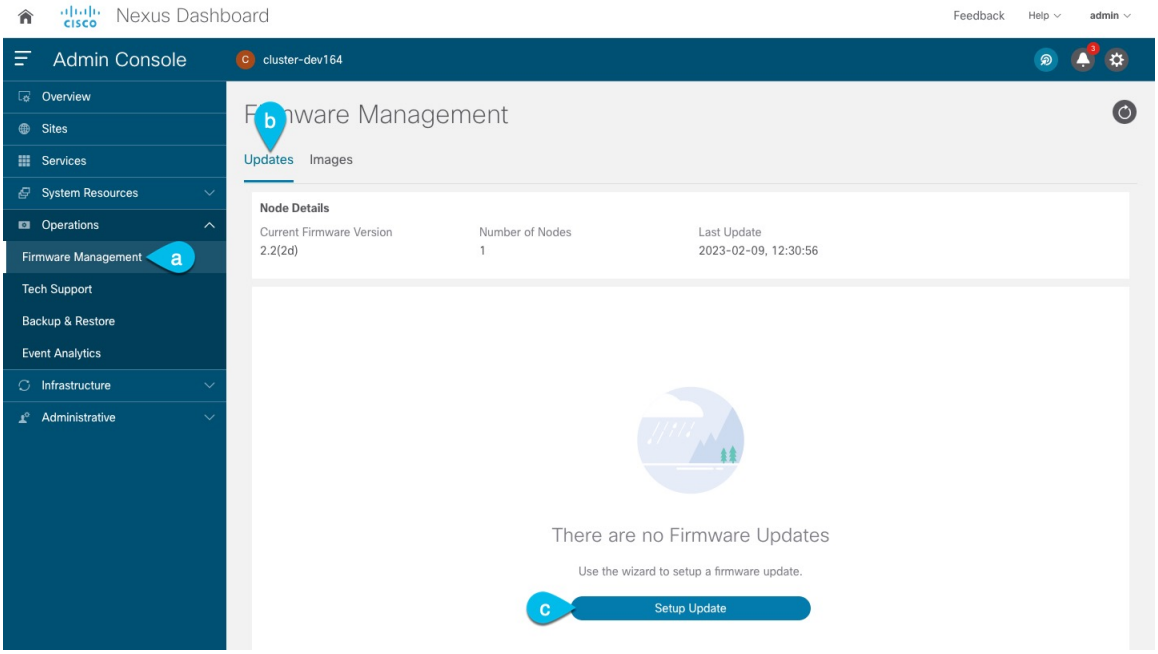
   イメージが Nexus ダッシュボード クラスタにアップロードされ、解凍されて処理され、アップグレードに使用できるようになります。プロセス全体に数分かかる場合があり、**[イメージ（Images）]** タブでプロセスのステータスを確認できます。

ステップ 7 イメージ ステータスが「ダウンロード済み」に変わるのを待ちます。

イメージでイメージのダウンロードの進行状況を確認できます。

ステップ 8 更新を設定します。

Nexus ダッシュボードのアップグレード



a) **[Operations（オペレーション）]** > **[ファームウェア管理（Firmware Management）]** に移動します。
b) **[更新]** タブを選択します。
c) **[更新の設定（Set Up Update）]** をクリックします。

（注） 以前にクラスタをアップグレードしたことがある場合、ページには代わりに以前のアップグレードの詳細が表示されます。その場合は、ページの右上にある **[詳細の変更（Modify Details）]** ボタンをクリックして、新しいアップグレード情報を提供します。

[ファームウェアの更新（Update Firmware）] ダイアログボックスが開きます。

ステップ 9 アップグレードを開始します。

a) **[ファームウェアの更新（Firmware Update）]** > **[バージョン選択（Version selection）]** 画面で、アップロードしたファームウェア バージョンを選択し、**[次へ（Next）]** をクリックします。
b) **[ファームウェアの更新（Firmware Update）]** > **[確認（Confirmation）]** 画面で、詳細を確認し、**[検証（Validate）]** をクリックします。

セットアップは、アップグレードを確実に成功させるために、いくつかの準備段階と検証段階を経ます。終了するまでに数分かかる場合があります。

c) 検証が完了したら、**[インストール（Install）]** をクリックします。

インストールの進行状況ウィンドウが表示されます。更新中は、この画面から移動できます。後で更新ステータスを確認するには、**[ファームウェア管理（Firmware Management）]** 画面に移動し、**[最終更新ステータス（Last Update Status）]** タイルで **[詳細の表示（View Details）]** をクリックします。

これにより、必要な Kubernetes イメージとサービスが設定されますが、クラスタは新しいバージョンに切り替わりません。次の手順で新しいイメージをアクティブ化するまで、クラスタは既存のバージョンを実行し続けます。このステップは、最大で 20 分程度かかる場合があります。

ステップ 10 新しい画像をアクティブにします。

アップグレード画面から移動したことがない場合は、**[アクティブ化（Activate）]** をクリックして新しいイメージをアクティブ化します。

そうでない場合は、次のようになります。

a) **[オペレーション（Operations）]** > **[ファームウェア管理（Firmware Management）]** 画面に戻ります。

b) **[最終更新ステータス（Last Update Status）]** タイルで、**[続行（Continue）]** をクリックします。

一部の以前の Nexus ダッシュボード バージョンでは、このリンクは代わりに **[詳細の表示（View Details）]** と呼ばれる場合があります。

c) **[ファームウェア アップデート（Firmware Update）]の** > **[インストール（Install）]** 画面で、**[アクティブ化（Activate）]** をクリックします。

すべてのクラスタサービスが起動し、GUI が使用可能になるまでに、さらに最大 20 分かかる場合があります。このページは、プロセスが完了すると、自動的に再ロードされます。

ステップ 11 クラスタに展開されている個々のサービスをアップグレードします。

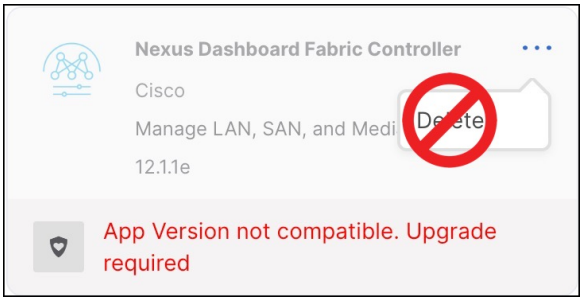
アップグレードするサービスに固有のアップグレード ガイドを必ず読んでください。

- Nexus Dashboard ファブリック コントローラ、アップグレード ガイド
- Nexus Dashboard Insights アップグレード ガイド
- Nexus Dashboard Orchestrator アップグレード ガイド

（注） サービスをアップグレードする場合：

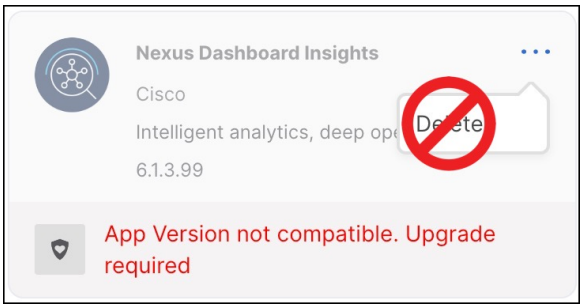
- Nexus Dashboard ファブリック コントローラの場合、クラスタのアップグレード後も、サービスをアップグレードするまで、サービスを無効にしておく必要があります。

  Nexus Dashboard クラスタがアップグレードされた後、サービスの既存のバージョンが、互換性のないアプリ バージョンと共にリストされる場合があります。アップグレードが必要です。警告。ファブリック コントローラのアップグレード イメージをアップロードする前に、このバージョンを**削除または再度有効にしない**でください。



- Nexus Dashboard Insights の場合、クラスタのアップグレード後も、サービスをアップグレードするまで、サービスを無効にしておく必要があります。

  Nexus Dashboard クラスタがアップグレードされた後、サービスの既存のバージョンが、互換性のないアプリ バージョンと共にリストされる場合があります。アップグレードが必要です。警告。Insights アップグレード イメージをアップロードする前に、このバージョンを**削除または再度有効にしない**でください。



- Nexus Dashboard Orchestrator の場合、新しいバージョンをアップロードしてアクティブ化する前に、サービスの既存のバージョンを再度有効にする必要があります。

ステップ 12 (オプション) 新しい UCS-C225-M6 ハードウェアに移行します。

（注） Nexus ダッシュボード ノードを新しい UCS-C225-M6 サーバーに置き換える予定がない場合は、この手順をスキップできます。

新しいハードウェアへの移行を計画している場合は、前の手順で説明したように、最初に既存のクラスタをリリース 2.3(1) 以降にアップグレードする必要があります。

UCS-C220-M5 ハードウェアを使用して展開された既存の Nexus ダッシュボード クラスタを移行するには、新しい UCS-C225-M6 ノードを `stadby` ノードとして既存のクラスタに追加し、古いノードの 1 つをフェイルオーバーするだけです。

次に、古いクラスターの残りのノードについて、一度に 1 ノードずつプロセスを繰り返します。`stadby` ノードの追加と使用については、*Nexus Dashboard* ユーザー ガイドの「インフラストラクチャ管理」の章で詳しく説明されています。

Nexus ダッシュボードのアップグレード

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。