Cisco Nexus ダッシュボード展開ガイド、リリース 2.0.x

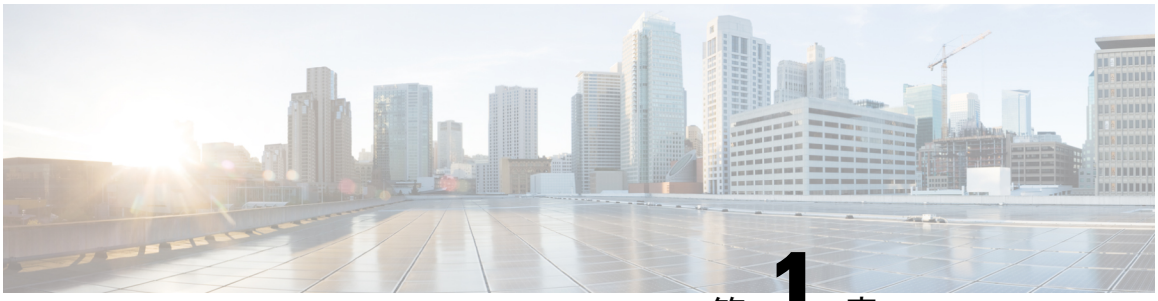
初版：2020 年 10 月 30 日

最終更新：2021 年 6 月 9 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

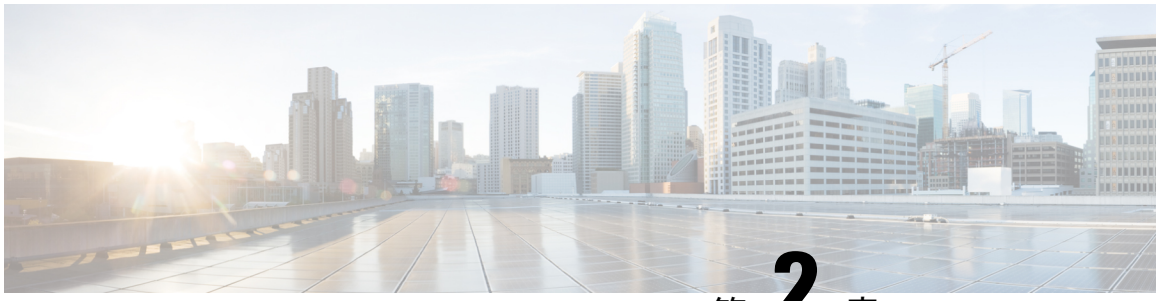
新機能および変更された機能に関する情報

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
2.0.2h	仮想およびクラウド フォーム ファクタの展開情報。	VMware ESX の展開 （31 ページ） Amazon Web Services での展開 （45 ページ） Microsoft Azure での展開 （55 ページ）
2.0.2g	このリリースへのアップグレードに関する追加情報。	Nexus ダッシュボードのアップグレード （61 ページ）
2.0(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 Insights や Nexus Assurance Engine などのシスコ データセンター運用アプリケーションをホストするための共通プラットフォームです。これらのアプリケーションは、すべてのデータセンター サイトで広く利用でき、ネットワーク ポリシーと運用のリアルタイム分析、可視性、および保証を提供します。Cisco Multi-Site Orchestrator は、ホスト アプリケーションとして Nexus ダッシュボードで実行することもできます。

Nexus Dashboard は、これら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クノロジースタックを提供し、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、これらのアプリケーションを実行および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の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。

各 Nexus ダッシュボード クラスタは、3 つのマスターノードで構成されます。物理的な Nexus ダッシュボード クラスタの場合は、最大 4 つのワーカー ノードをプロビジョニングして水平方向のスケーリングを有効にし、最大2つのスタンバイ ノードを使用して、マスターノードに障害が発生した場合にクラスタを簡単に回復できます。仮想クラスタとクラウド クラスタでは、ベース 3 ノード クラスタのみがサポートされます。

（注） このドキュメントでは、3 ノード 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）が事前インストールされた、特殊な Cisco UCS サーバー（Nexus Dashboard プラットフォーム）のクラスタとして提供されます。Cisco Nexus Dashboard ソフトウェアスタックは、ハードウェアから分離して、多数の仮想フォームファクタで展開できます。このドキュメントでは、「Nexus Dashboard プラットフォーム」は具体的に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。

Nexus ダッシュボードと Cisco DCNM

Nexus ダッシュボードは、Cisco DCNM のコンテキストで使用できます。この場合、DCNM は Nexus ダッシュボード ソフトウェア スタックで実行されているアプリケーションではありません。代わりに、DCNM イメージ（.iso）が Nexus ダッシュボード物理サーバに直接インストールされ、Cisco DCNM でインストールおよび実行されているアプリケーションに追加のコンピューティング リソースを提供し、DCNM プラットフォームの水平スケーリングを可能にします。このドキュメントでは、Nexus ダッシュボード ソフトウェア スタックの導入について説明しているため、Nexus ダッシュボード ハードウェアへの DCNM のインストールに関する情報については、展開タイプに適した『Cisco DCNM Installation Guide』を参照してください。

利用可能なフォーム ファクタ

Cisco Nexus ダッシュボード、リリース 2.0.1 および 2.0.2g は、物理アプライアンスとしてのみ展開できます。これは、購入した Nexus ダッシュボード プラットフォーム ハードウェアにすでに展開されているソフトウェア スタックを指します。

Cisco Nexus ダッシュボード、リリース 2.0.2h 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） Nexus ダッシュボード、リリース 2.0.2h は、Multi-Site Orchestrator アプリケーションの仮想フォーム ファクタクラスタのみをサポートします。Nexus Insights などの他のアプリケーションの場合は、物理クラスタを展開する必要があります。

- 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 のソフトウェアスタックが事前に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。

- 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。

以前のバージョンの Nexus ダッシュボードからのアップグレード

すでに Nexus ダッシュボード リリース 2.0.1 以降を実行している場合は、Nexus ダッシュボードのアップグレード （61 ページ）の説明に従って、クラスタ設定とアプリケーションを保持したまま、最新リリースにアップグレードできます。

Application Services Engine からのアップグレード

Application Services Engine リリース 1.1.3d を物理アプライアンスとして実行している場合は、Nexus ダッシュボードにアップグレードして、Nexus ダッシュボードのアップグレード （61 ページ） に説明されているクラスタの設定とアプリケーションを保持できます。

Application Services Engine リリース 1.1.3d を仮想アプライアンスまたはリリース 1.1.3d より前のリリースとして実行している場合、クラスタのステートフル アップグレードまたは移行は Nexus ダッシュボード リリース 2.0.2h 以降でのみサポートされます。リリース 2.0.1 または 2.0.2g を導入する場合は、新しい物理アプライアンス クラスタを導入し、すべてのアプリケーションを再インストールする必要があります。

クラスタサイジングのガイドライン

Nexus Dashboard は、アプリケーションの共同ホスティングをサポートします。実行するアプリケーション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必要があります。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』を参照してください。

最初の 3 ノード 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ダッシュボード GUI から直接入手することもできます。

サポートされるアプリケーション

サポートされるアプリケーションの完全なリスト、および関連する互換性と相互運用性の情報については、『Cisco Day-2 Operations Apps Support Matrix』を参照してください。

次の表に、Nexus ダッシュボード リリース2.xの推奨アプリケーション リリース バージョンの参照先を示します。

表 *2:* アプリケーションの推奨バージョン

Nexus ダッシュボードのリリースとフォームファクタ	Nexus Insights	Multi-Site Orchestrator	Network Assurance Engine
Nexus ダッシュボード、リリース2.0.1 物理クラスタ	5.0(1)	3.2(1)	5.1(1a)
Nexus ダッシュボード、リリース 2.0.2g 物理クラスタ	5.1(1)	3.2(1)	5.1（1b）
Nexus ダッシュボード、リリース 2.0.2h 物理クラスタ	5.1(1)	3.3(1)	5.1（1b）
Nexus ダッシュボード、リリース 2.0.2h 仮想クラスタ	サポート対象外	3.3(1)	サポート対象外

前提条件とガイドライン

Network Time Protocol（NTP）

Nexus ダッシュボード ノードはクロックの同期に NTP を使用するため、環境で NTP サーバを設定する必要があります。

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アプリケーションは、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、導入計画については、このドキュメントに加えて特定のアプリケーションのドキュメントを参照することを推奨します。

- **データ ネットワーク** は次の目的で使用されます。
  - Nexus ダッシュボード ノードのクラスタリング

- アプリケーション間通信
- Cisco APIC、クラウド APIC、および DCNM 通信への Nexus ダッシュボード ノード

たとえば、NAE などの 2 日目運用アプリケーションのネットワーク トラフィック。

- **管理ネットワーク** は次の目的で使用されます。
  - 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 ダッシュボード 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 Dashboard 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。

- 2 つのメジャー インターフェイスは同じサブネットまたは異なるサブネット内に設定できます。

  また、クラスタ内の異なるノードにまたがる各ネットワークのインターフェイスは、異なるサブネットに属することもできます。
- 管理ネットワークは、TCP ポート 22/443 を介して各ノードの CIMC に IP 到達可能性を提供する必要があります。

  Nexus Dashboard 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 Insights および Network Assurance Engine アプリケーションの場合、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 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。
- Multi-Site Orchestrator アプリケーションの場合、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 到達可能性を持つことができますが、Cisco DCNM サイトに対して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 ダッシュボード 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、より高い MTU を設定できます。

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

  Nexusダッシュボードクラスタおよびアプリケーションを展開する場合は、常に最も低いRTT要件を使用する必要があります。たとえば、MSOアプリケーションとNIアプリを共同ホストする場合、サイト接続RTTは50ミリ秒を超えてはなりません。

表 *3 : RTT* 要件

アプリケーション	接続	RTT の最大値
Nexus Dashboard クラスタ	ノード間	150 ミリ秒
マルチサイト オーケストレーション（MSO）	ノード間	150 ミリ秒
	サイトへ	500 ミリ秒
Nexus Insights (NI)	ノード間	50 ミリ秒
	サイトへ	50 ミリ秒
Network Assurance Engine（NAE）	ノード間	50 ミリ秒
	サイトへ	50 ミリ秒

Nexus ダッシュボードの内部ネットワーク

Nexus Dashboard 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。

（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。

通信ポート

Nexus Dashboard クラスタとそのアプリケーションには、次のポートが必要です。

表 *4:*

インターフェイス	ポート番号	ポート タイプ
管理インターフェイス	--	ICMP
	22	TCP
	67	UDP
	69	UDP
	443	TCP
	5555	TCP
	9880	TCP
	30012	TCP
	30021	TCP
	30500 ～ 30600	TCP および UDP

インターフェイス	ポート番号	ポート タイプ
ND ノード間のデータインターフェイス	53	TCP/UDP
	443	TCP
	3379	TCP
	3380	TCP
	4789	UDP
	9969	TCP
	9979	TCP
	9989	TCP
	15223	TCP
	30002 ～ 30006	TCP
	30009 ～ 30010	TCP
	30012	TC
	30015 ～ 30019	TCP
	30017	UDP
	30025	TCP
	30500 ～ 30600	TCP および UDP
APIC のデータインターフェイス	22	TCP
	443	TCP
ND ノードとファブリック間のデータインターフェイス	443	TCP
	2022	TCP
	5640 ～ 5671	UDP
	5965	UDP
	8884	TCP
	9989	TCP
	30000 ～ 30001	TCP

ファブリック接続

ここでは、Nexus ダッシュボード 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 DCNM 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ダッシュボードクラスタ。
- リーフ スイッチに接続された Nexus ダッシュボード ノードは、一般的なホストです。

クラウド APIC 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。

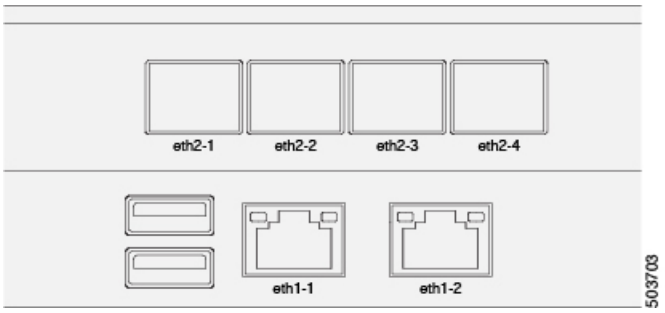
物理ノードのケーブル接続

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。

次の図に、Nexus ダッシュボードの物理ノード インターフェイスを示します。

- `eth1-1` および `eth1-2` は管理ネットワークに接続する必要があります。
- `eth2-1` および `eth2-2` はデータ ネットワークに接続する必要があります。

図 *1:* ノード接続



インターフェイスは Linux ボンドとして設定されます。1 つはデータインターフェイス用、もう 1 つは管理インターフェイス用です。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。ポートチャネルまたは vPC はサポートされません。

Nexusダッシュボードノードがシスコ 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、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コマンドを追加して、データネットワーク上での到達可能性を確保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 Multi-Site 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）インターフェイスのいずれか、またはその両方への接続を確立できます。
- Cisco DCNM ファブリックを管理するために Multi-Site 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 DCNM 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 Insights などの Day-2 Operations アプリケーションを導入する場合は、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 ダッシュボード 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。

- DCNM ファブリックの場合、データ インターフェイスと DCNM 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、DCNM にルートを追加して 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必要があります。

  DCNM UIからルートを追加するには、**Administration** > **Customization** > **Network Preference** > **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 Dashboard 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。

たとえば、Nexus Dashboard ノードの管理インターフェイスとデータ ネットワーク インターフェイスが同じサブネットにある場合など、「L3ネットワーク」と「管理ネットワーク」は同じネットワークインフラストラクチャにすることができます。

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

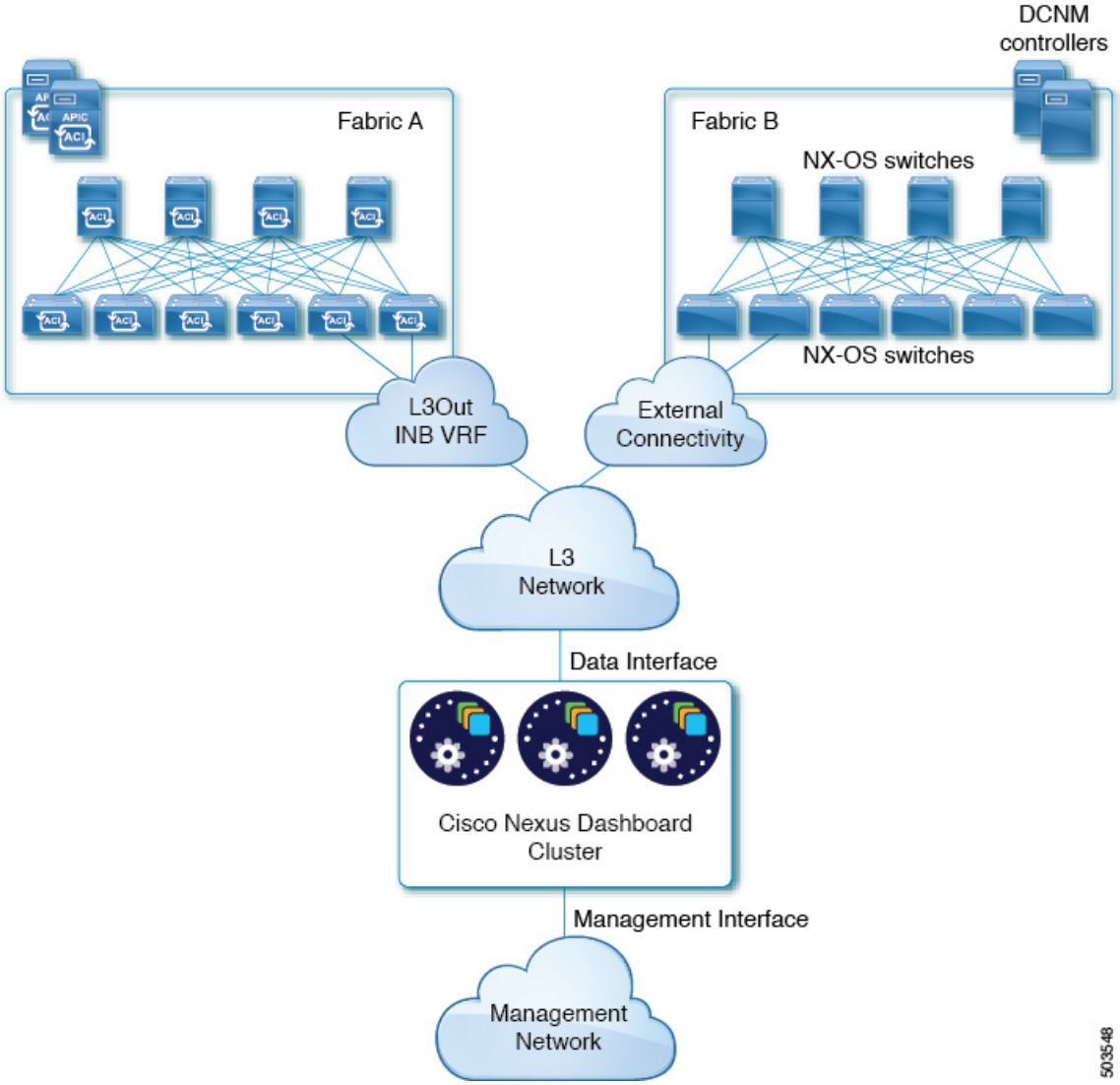
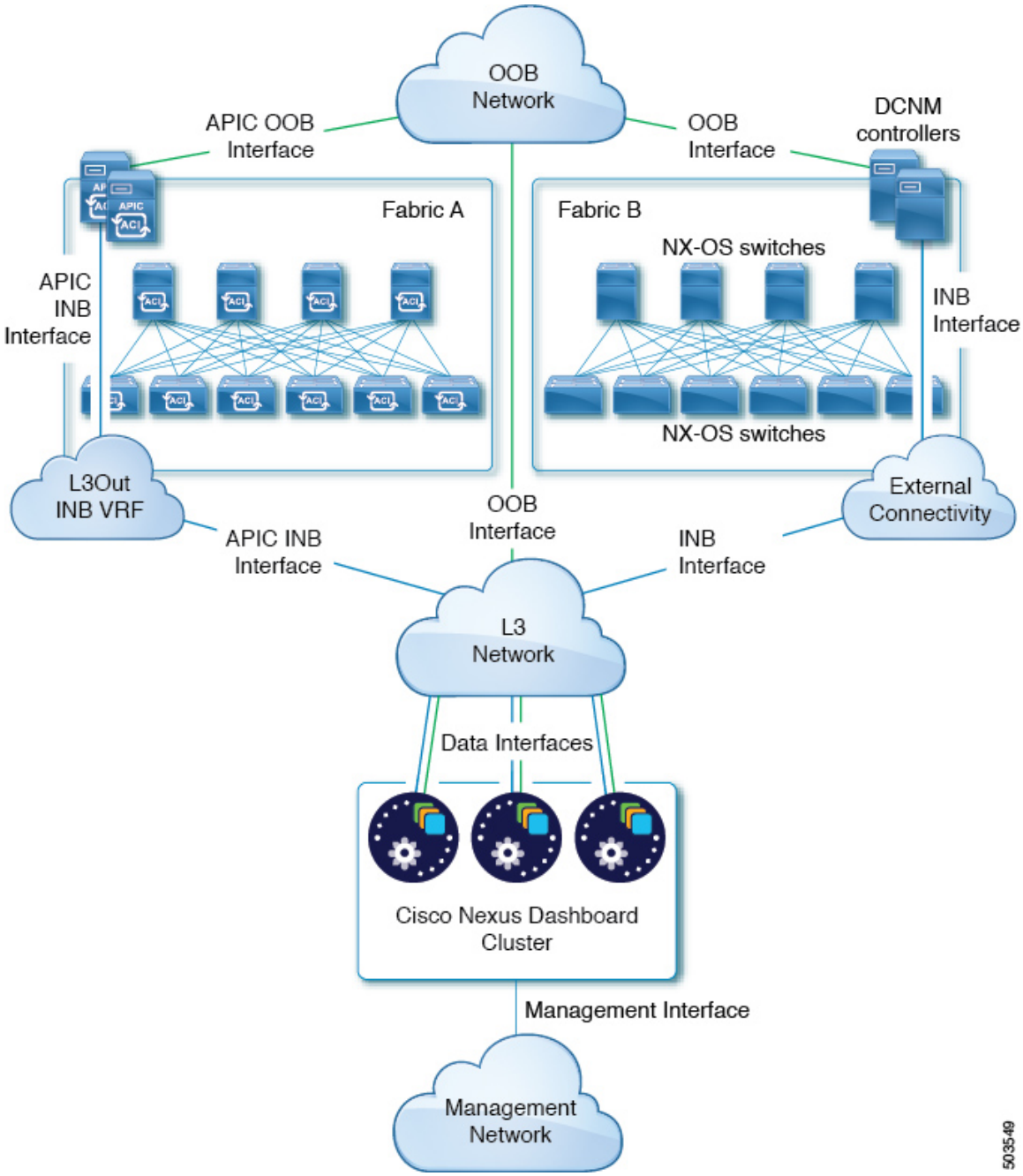


図 *3:* レイヤ *3* ネットワーク経由の接続、マルチサイト オーケストレータ



リーフ スイッチへのノードの直接接続

Nexus ダッシュボード 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ダッシュボード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 Multi-Site 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 Insights または Network Assurance Engine を導入する場合は、各ファブリックのデータ インターフェイスからインバンド 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の 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に対してコントラクトが確立されている必要です。Nexus Dashboard は、管理テナントとインバンド VRF に展開することを推奨します。他のファブリックへの接続は、L3Out を介して確立されます。
- ACI ファブリックを使用して Nexus Insights を展開する場合は、データインターフェイス IP アドレスと ACI ファブリックのインバンド IP アドレスが異なるサブネットに存在する必要があります。

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。
- ACI ファブリックの場合、管理テナントの Cisco Nexus ダッシュボード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）を設定することをお勧めします。

  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。
- ACI ファブリックの場合、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。
- ACIファブリックの場合、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 の間で契約を確立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。

次の 2 つの図に、Nexus Dashboard 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ます。それぞれの主な目的は、Nexus Dashboard 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。

たとえば、Nexus Dashboard ノードの管理インターフェイスとデータ ネットワーク インターフェイスが同じサブネットにある場合など、「L3ネットワーク」と「管理ネットワーク」は同じネットワークインフラストラクチャにすることができます。

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

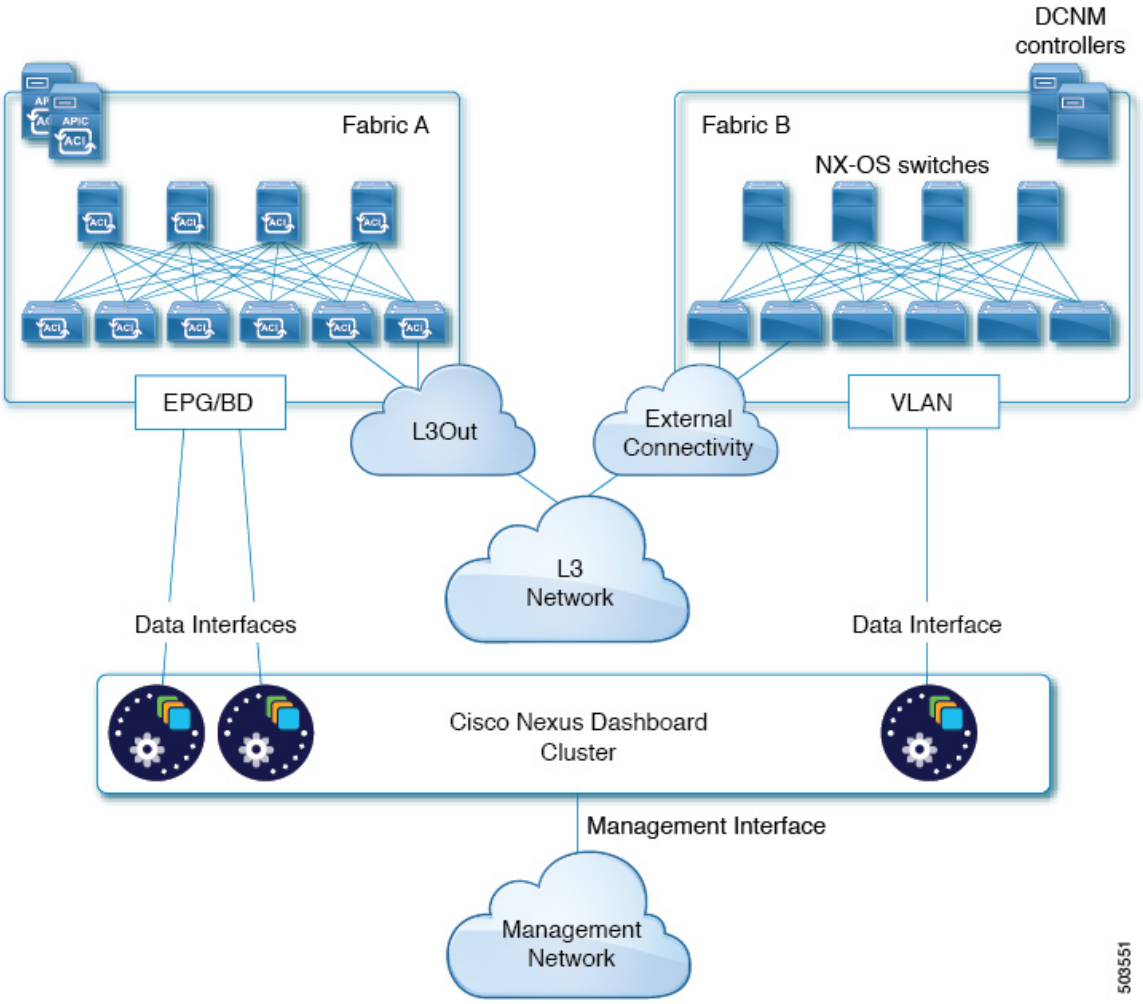
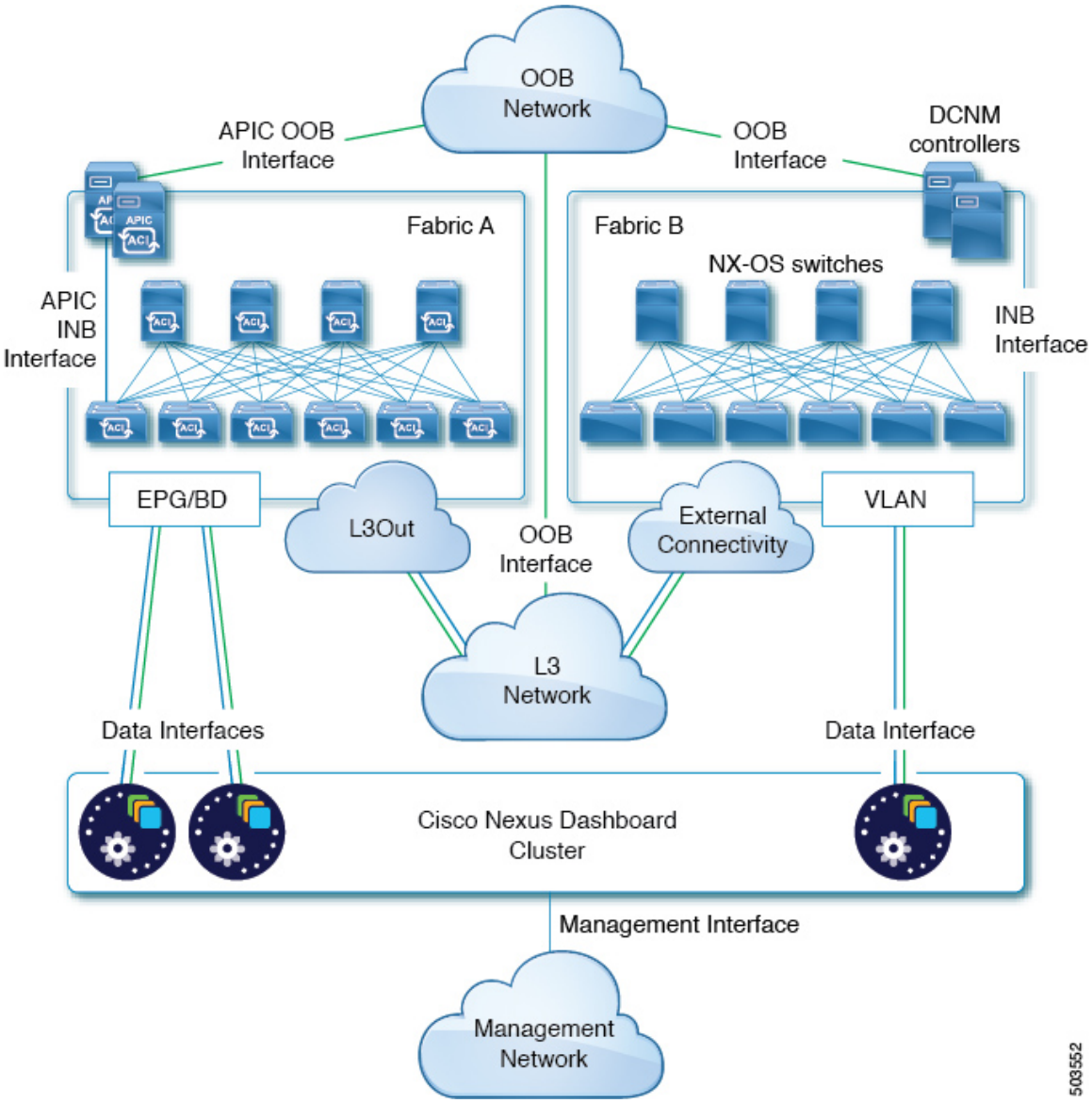


図 *5 :* リーフ スイッチ、*Multi-Site Orchestrator* への直接接続



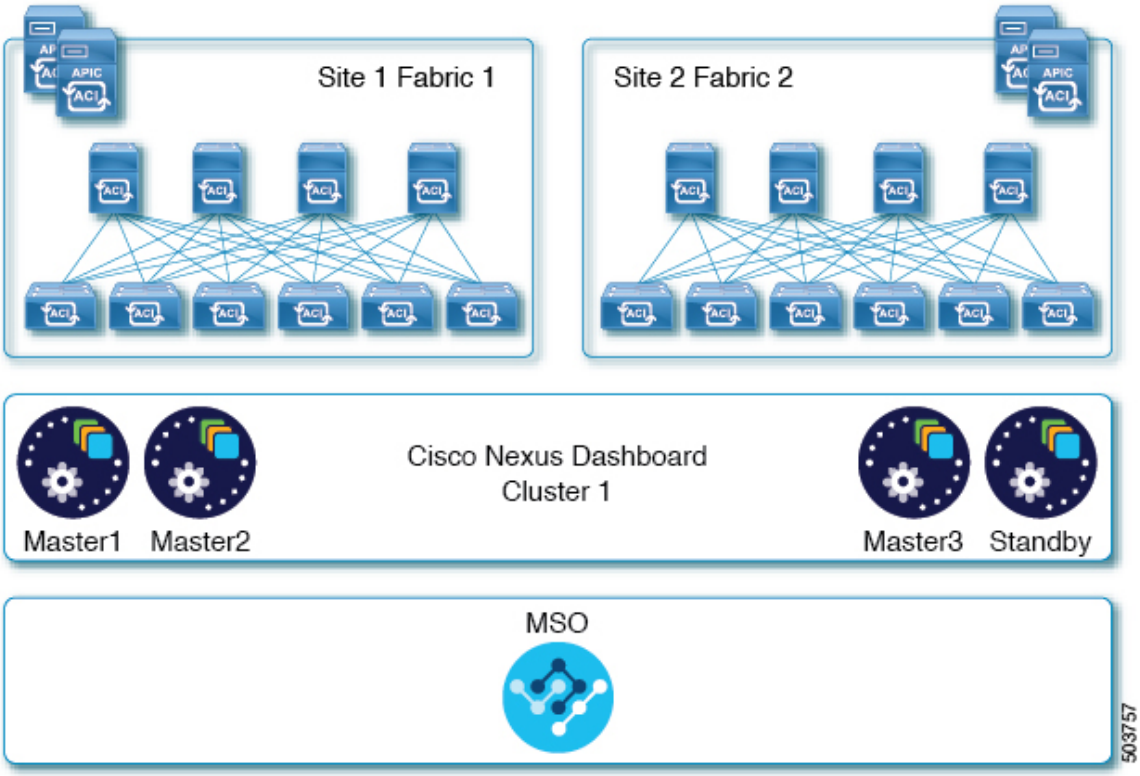
サイト間のノード分散

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。

Nexus Insights および Network Assurance Engine アプリケーションには、一元化された単一サイトの導入をお勧めします。これらのアプリケーションは、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。

Multi-Site Orchestrator の展開に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 ダッシュボード マスター ノードが必要であるため、物理的な Nexus ダッシュボード 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*: マルチサイト 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



仮想 Nexus ダッシュボード クラスタを導入している場合、スタンバイ ノードはサポートされません。ノードの1つに障害が発生した場合は、「*Cisco Nexus* ダッシュボード ユーザガイド」の「仮想ノードの交換」の章で説明されているとおり、新しい仮想ノードを呼び出して交換する必要があります。

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 *5*: 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	--	--	--
2	M1、M2	M3、 S1	--	--
3	M1	M2	M3	--
4	M1	M2	M3	S1

アプリのコロケーションの使用例

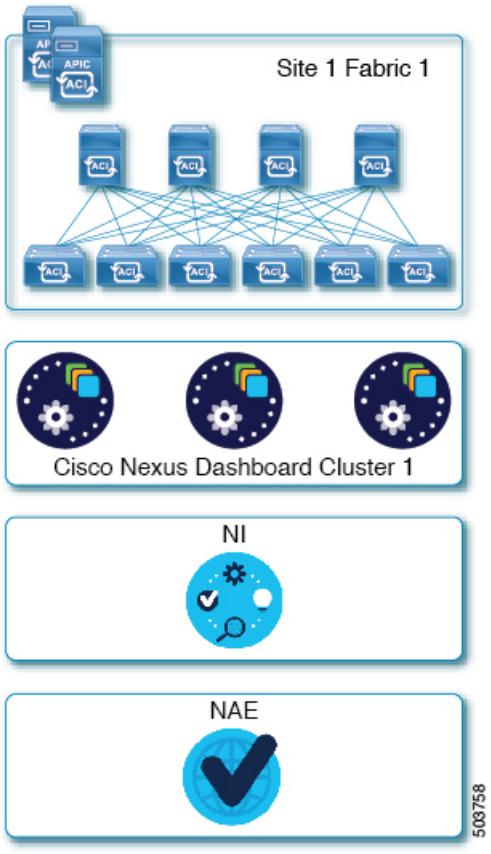
このセクションでは、特定の単一アプリまたは複数アプリの共同ホスティングの使用例について、いくつかの推奨される導入シナリオについて説明します。

（注） このリリースでは、仮想またはクラウドフォームファクタのアプリケーションの共同ホスティングはサポートされていません。以下のすべてのアプリケーション共同ホスティングのシナリオは、物理 Nexus ダッシュボード クラスタにのみ適用されます。

単一サイト、Nexus Insights および Network Assurance Engine

Nexus Insights と Network Assurance Engine アプリケーションを使用する単一サイトのシナリオでは、単一の物理 Nexus ダッシュボード クラスタを導入し、両方のアプリケーションをホストすることができます。

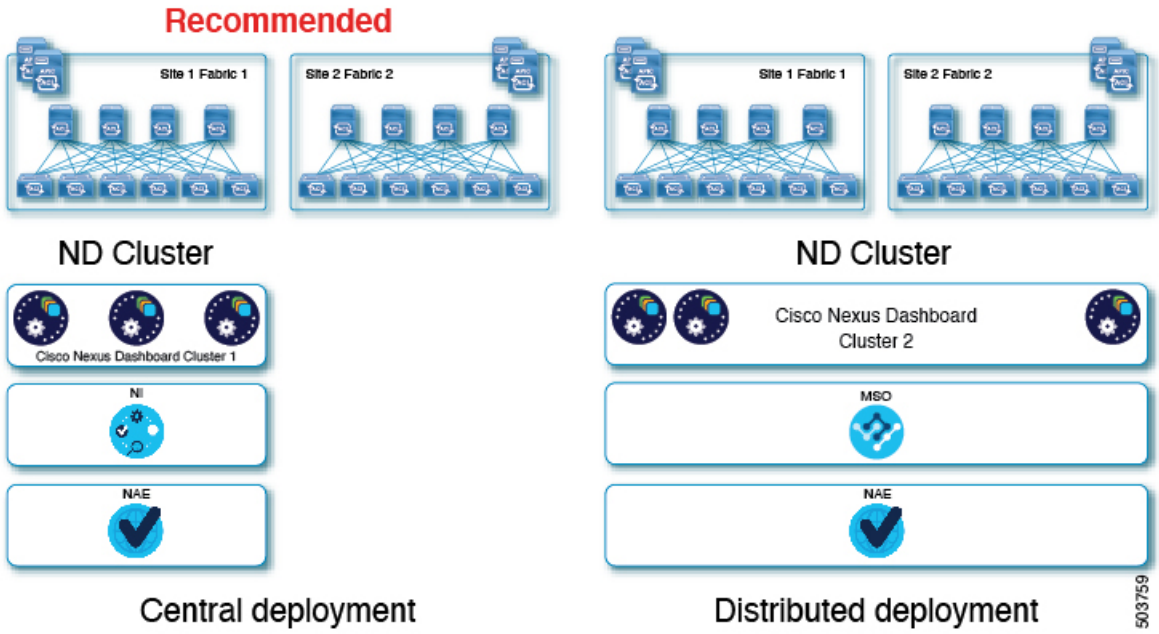
図 *7*: 単一サイト、*Nexus Insights* および *Network Assurance Engine*



複数のサイト、Nexus Insights、Network Assurance Engine

Nexus Insights と Network Assurance Engine アプリケーションを使用する複数サイトのシナリオでは、単一の Nexus ダッシュボード クラスタを、両方のアプリケーションをホストすることで導入できます。この場合、ノードはサイト間で分散できますが、これらのアプリケーション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、左側の導入オプションを推奨します。

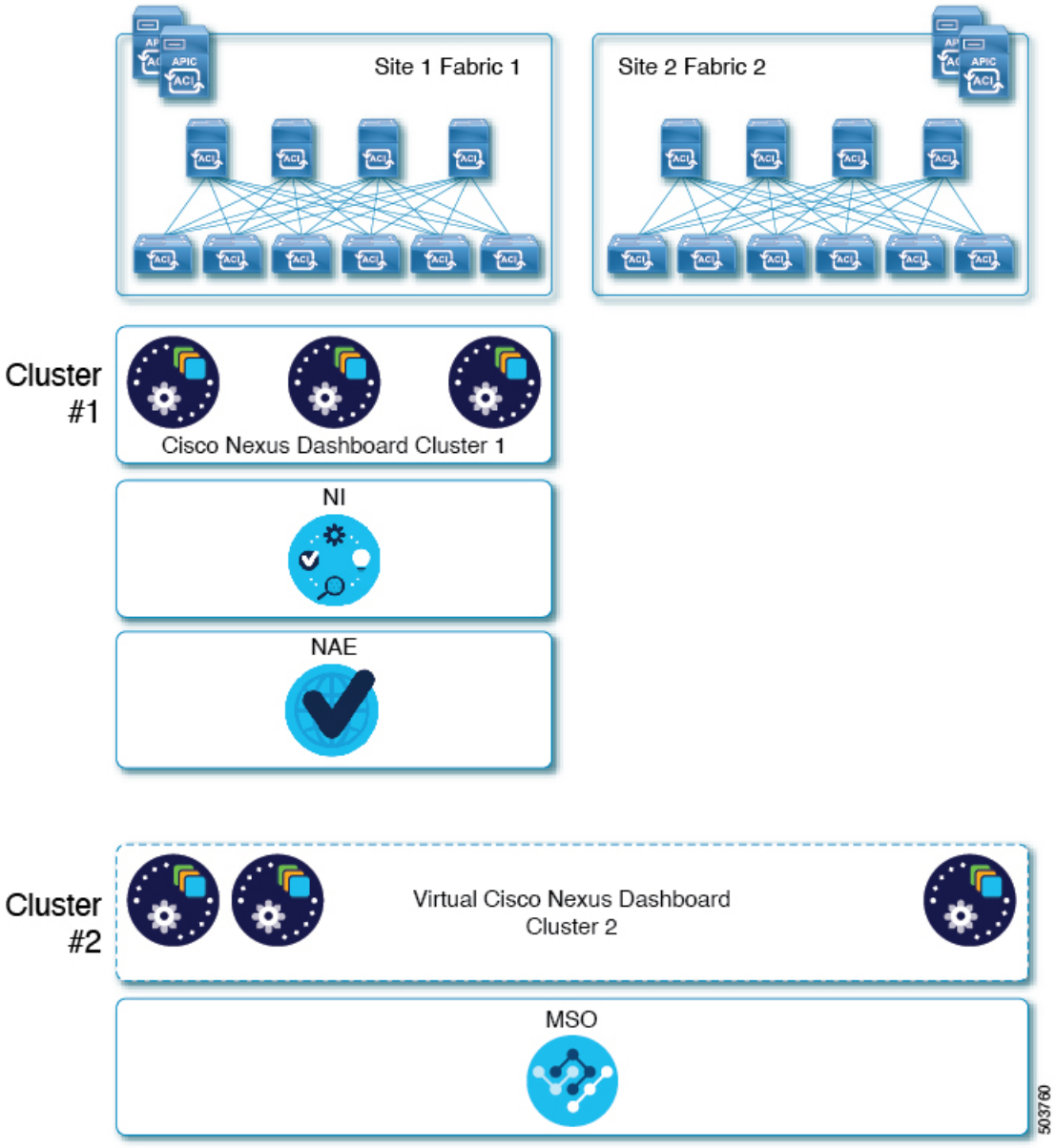
図 *8*: 単一サイト、*Nexus Insights* および *Network Assurance Engine*



複数のサイト、Nexus Insights、Network Assurance Engine、および Multi-Site Orchestrator

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 Multi-Site Orchestrator アプリケーション専用で、サイト全体に分散されたノードです。

図 *9* : 単一サイト、*Nexus Insights* および *Network Assurance Engine*



インストール前チェックリスト

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

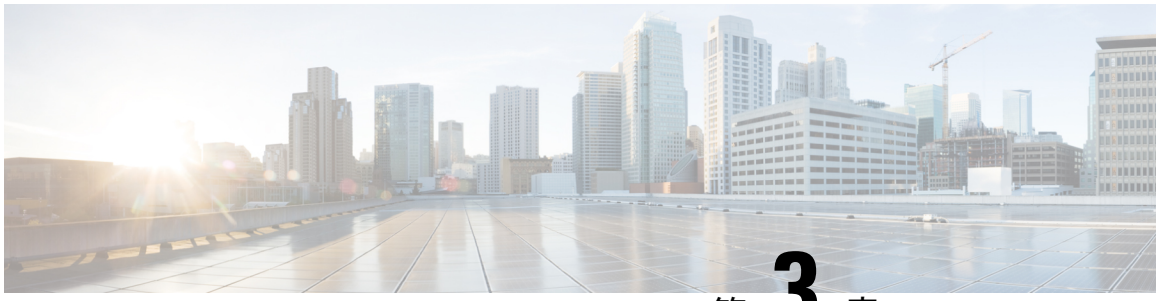
表 *6:* クラスタの詳細

パラメータ	例	入力する値
クラスタ名	nd-cluster	
NTP サーバ（NTP Server）	171.68.38.65	
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	172.17.0.1/16	
サービス ネットワーク	100.80.0.0/16	

表 *7:* ノードの詳細

パラメータ	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（USERNAME）]：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（USERNAME）]：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（USERNAME）]：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	

パラメータ	例	入力する値
最初のノードの**データ ネットワーク IP**	192.168.6.172/24	
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	
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	
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	



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。

- 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。

  このセクションでは、3 ノードの 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します。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、代わりに、『*Cisco Nexus* ダッシュボード ユーザ ガイド』の「追加ノードの展開」を参照してください。

  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、サーバを完全に再イメージ化する場合は、『Cisco Nexus Dashboard User Guide』の「*Re-Imaging Nodes*」の項を参照してください。

  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。

- 『*Cisco Nexus Dashboard Hardware Installation Guide*』の説明に従って、正しい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、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 *8*: サポート対象ハードウェア

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 • 4 X 2.4 TB HDD 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。

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。

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

  推奨バージョン：CIMC リリース 4.1(3b)。

  サポートされる最小バージョン：CIMC、リリース4.0(1a)。

- 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 2.0.2 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（61 ページ）の説明に従って、リリース 2.0.2 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最大 4 つのワーカー ノードを追加できます。

Cisco Nexus ダッシュボードを物理アプライアンスとして展開

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 （25 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。

次の設定は、クラスタの最初のノードでのみ実行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、最初のノードから CIMC IP アドレスに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。

初回のセットアップ ユーティリティを実行するように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。

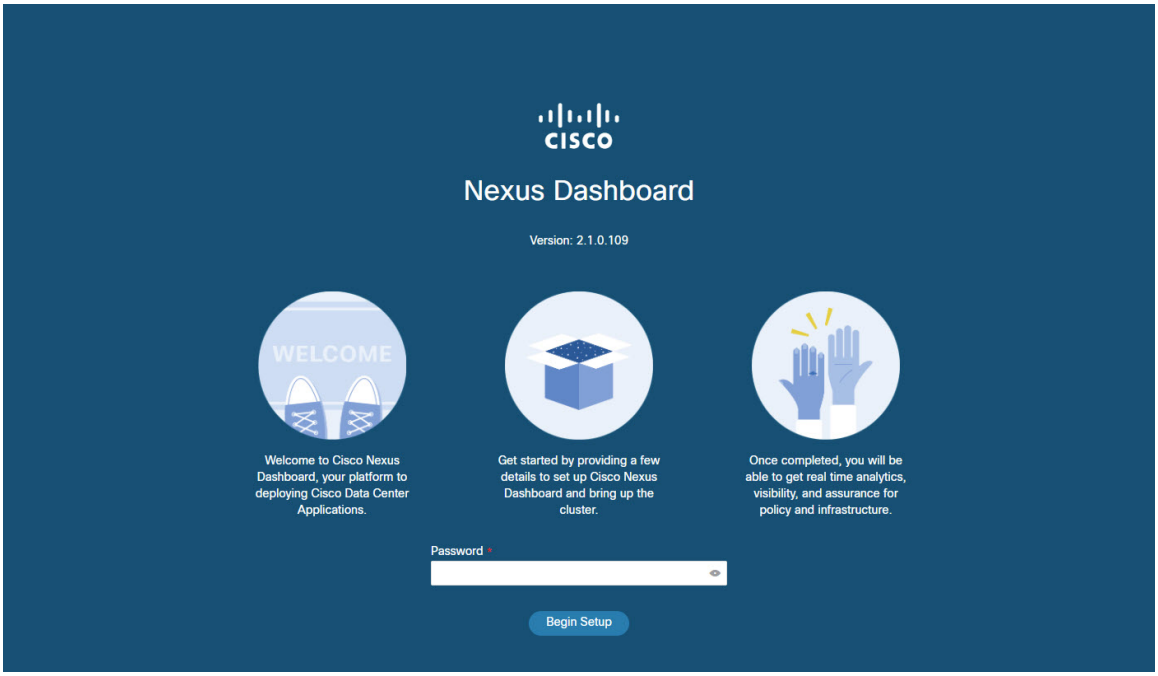
```
Please wait for system to boot: [#########################] 100%
System up, please wait for UI to be online.

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

ステップ 3 ノードの管理IPアドレスを参照してGUIを開きます。

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。

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）]** 画面で、クラスタ情報を入力します。

a) クラスタ **名** を指定します。

b) **[NTP ホストの追加（Add NTP Host）]** をクリックし、NTPサーバ情報を入力します。

c) [Add DNS Provider]をクリックし、DNSサーバ情報を入力します。

d) （オプション）**[詳細設定の表示（View Advanced Settings）]** メニューを展開し、DNS 検索ドメインと内部ネットワーク（アプリケーションとサービス）を設定します。

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。

e) [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) 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。

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。

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 6 クラスタにノードを追加するには、**[ノードの追加（Add Node）]** をクリックします。

[ノードの詳細（Node Details）] ウィンドウが開きます。

a) ノードの CIMC の詳細を入力し、**[検証（Verify）]**をクリックします。

ノードの CIMC の IP アドレスとログイン情報は、シリアル番号などのノードの情報を取得するために使用されます。

b) ノードの**名前**を入力します。

c) ノードの**管理ネットワーク** IP アドレスとゲートウェイを入力します。

d) 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。

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) [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、最大で20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。

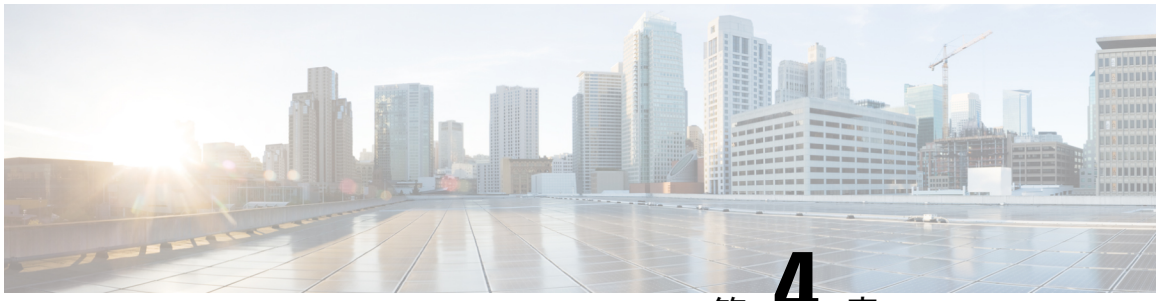
クラスタが使用可能になったら、ノードの管理 IP アドレスのいずれかを参照してアクセスできます。管理者ユーザのデフォルト パスワードは、Nexus ダッシュボード クラスタの最初のノードに選択したレスキュー ユーザ パスワードと同じです。

ステップ 11 リリース 2.0.2 を展開し、同じクラスタで複数のアプリケーションをホストする場合は、App Infra Services の展開プロファイルを設定します。

リリース 2.0.1 を展開した場合、または Nexus ダッシュボード クラスタで単一のアプリケーションのみをホストしている場合は、この手順をスキップします。

同じクラスタに複数のアプリケーションをホストする場合は、アプリケーションとファブリック サイズの組み合わせに適した展開プロファイルを使用して、 App Infra Services を設定する必要があります。

クラスタのアップグレードが完了したら、 『*Cisco Nexus Dashboard User Guide*』の「App Infra Services」セクションに記載されている手順に従ってください。このガイドは、製品の GUI からも入手できます。



第 4 章

VMware ESX の展開

前提条件とガイドライン

仮想展開は、Nexus Dashboard リリース 2.0.2h 以降でサポートされています。以前のリリースでは、物理アプライアンスとしての展開 （25 ページ） で説明されている物理フォーム ファクタのみがサポートされています。

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。

- 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。

  この文書は、3 ノード 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のでご注意ください。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、代わりに、『*Cisco Nexus* ダッシュボード ユーザ ガイド』の「追加ノードの展開」を参照してください。

  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。

- ESX フォーム ファクタが拡張性とアプリケーションの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、拡張性とアプリケーションの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。

- 十分なシステム リソースをもつことを確認します。

表 *9*: 展開（導入）要件

Nexus ダッシュボード バージョン	要件

リリース 2.0.2h
以前のリリースはサポートされていません。
	• VMware vCenter 6.x
	• VMware ESXi 6.5 または 6.7
	• 各 VM には以下が必要です。
	  • 16 vCPU
	  • 64 GB の RAM
	  • 500 GB のディスク
	• 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。

- 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 ESX での Cisco 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。

始める前に

- 前提条件とガイドライン （31 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 の OVA イメージを取得します。

a) [Software Download] ページを参照します。

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 Dashboard のバージョンを選択します。

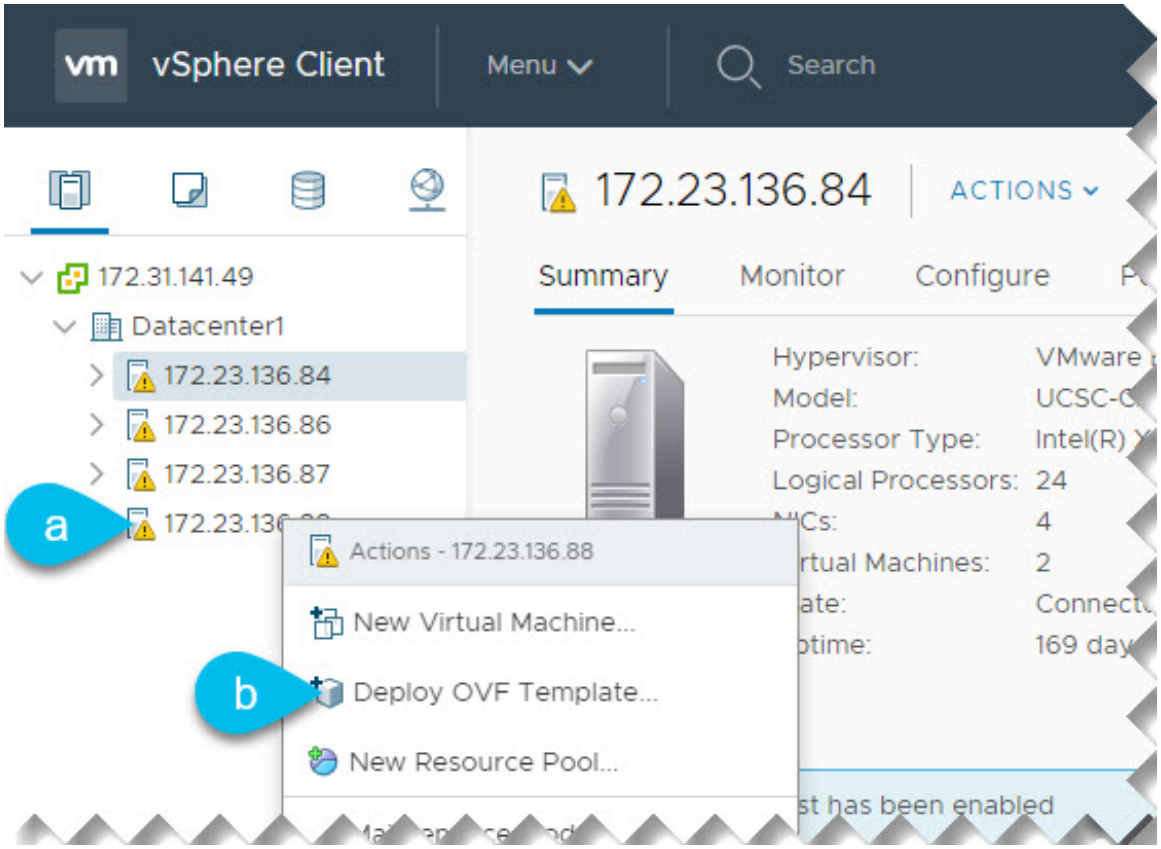
d) Cisco Nexus ダッシュボード イメージ（`nd-dk9.<version>.ova`）。

ステップ 2 VMware vCenter にログインします。

ESX ホストに OVA を直接展開することはできません。vCenter を使用して展開する必要があります。

（注） 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 を使用した展開の詳細を示します。

ステップ 3　新しい VM 展開を開始します。

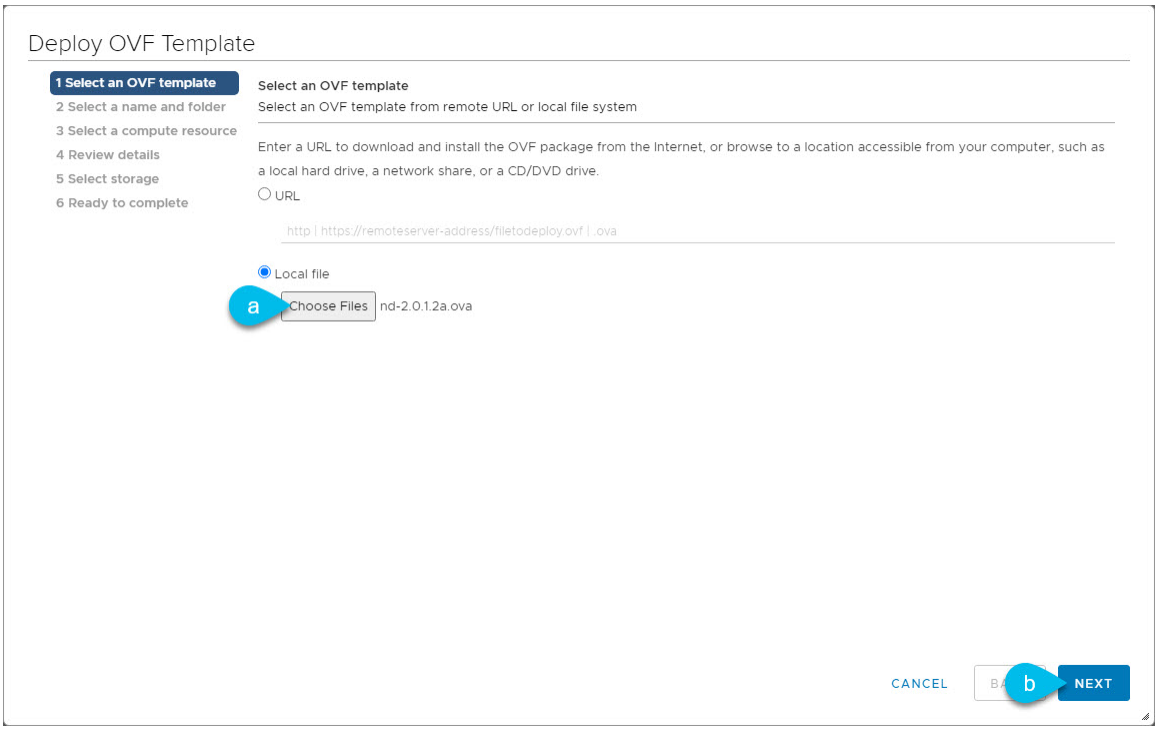


a)　展開する ESX ホストを右クリックします。

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。

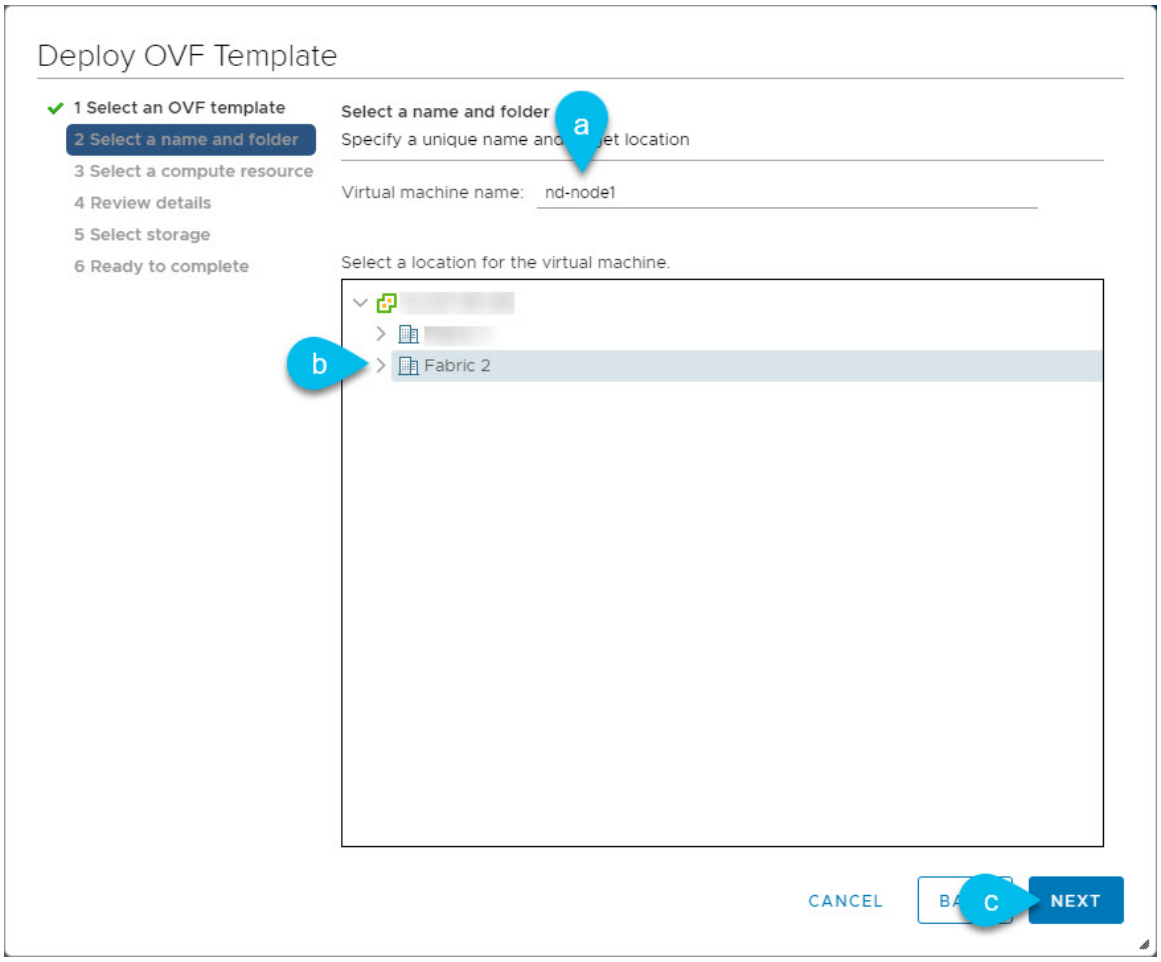
ステップ 4　**[OVF テンプレートの選択（Select an OVF template）]** 画面で、OVAイメージの場所を指定します。



a) **[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。

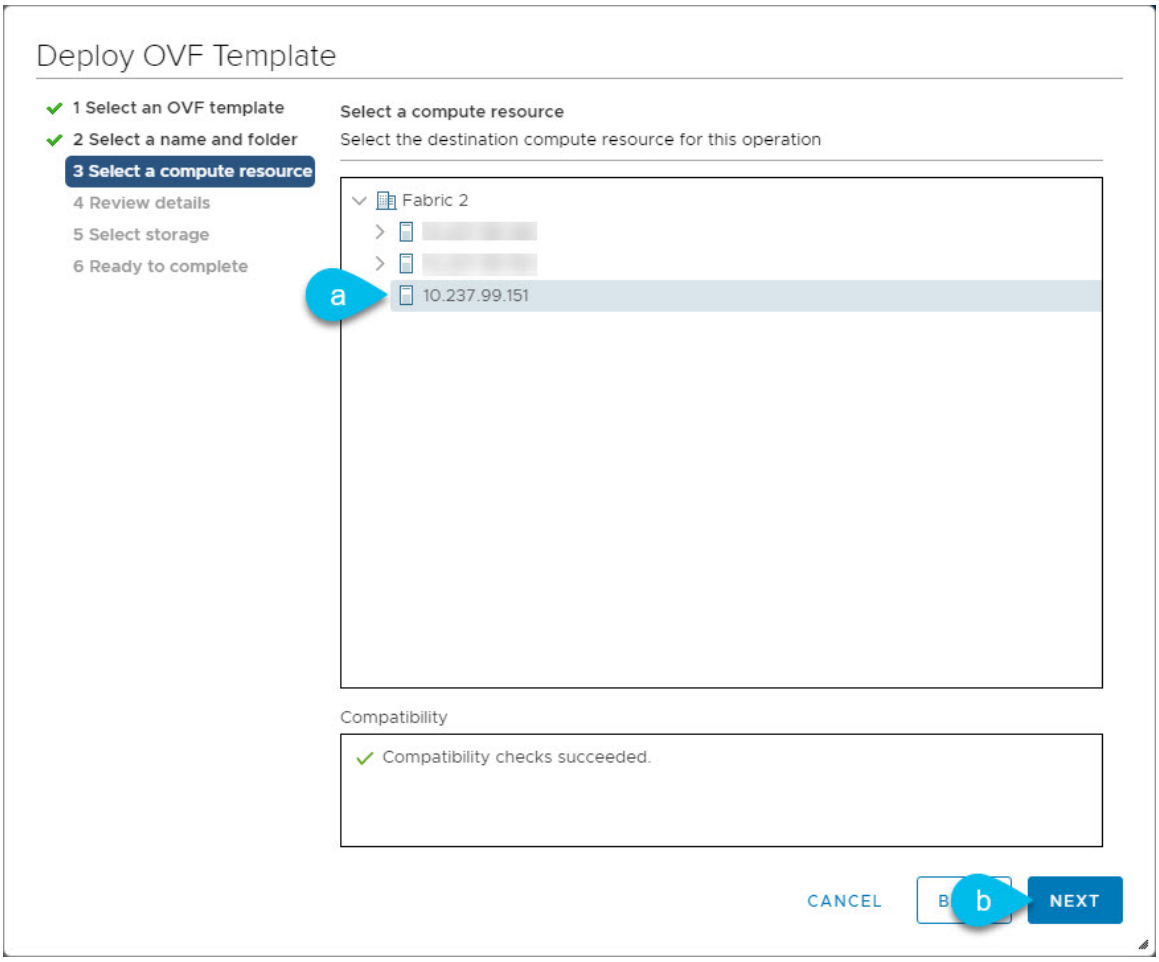
b) [次へ（Next）] をクリックして続行します。

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。

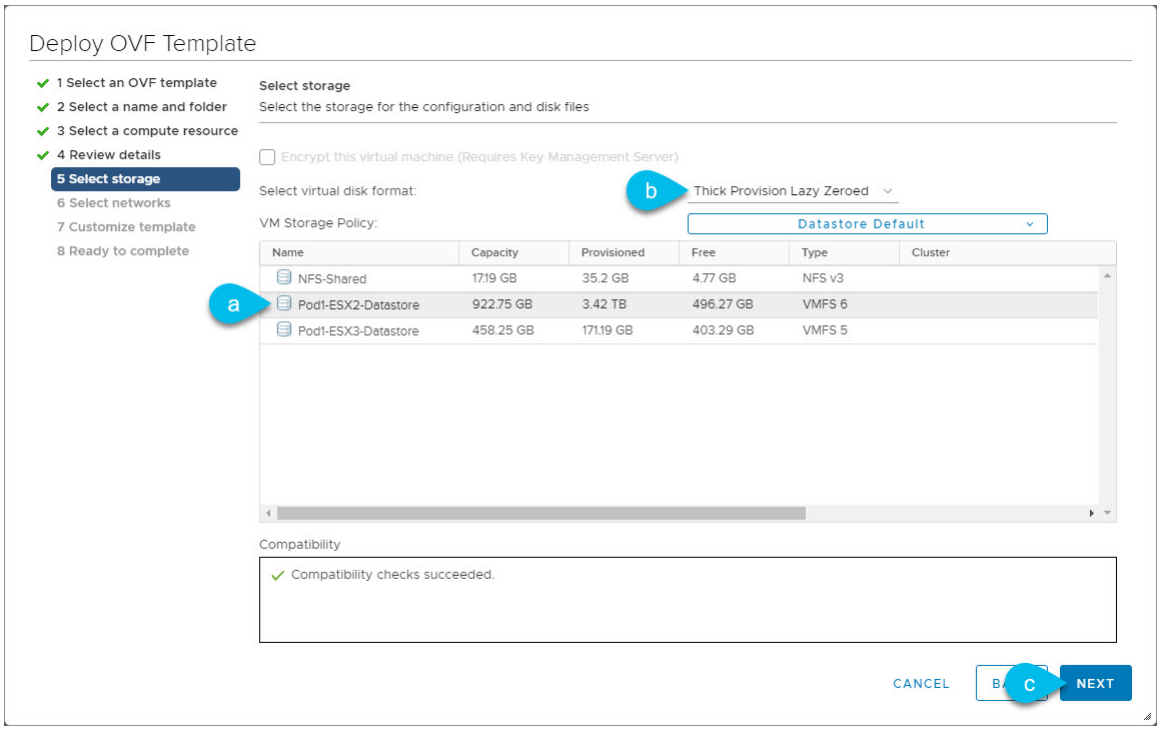


a) 仮想マシンの vCenter データセンターと ESX ホストを選択します。

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



a) 仮想マシンのデータストアを選択します。

ノードごとに一意のデータストアを推奨します。

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

c) **[次へ（Next）]** をクリックして、続行します。

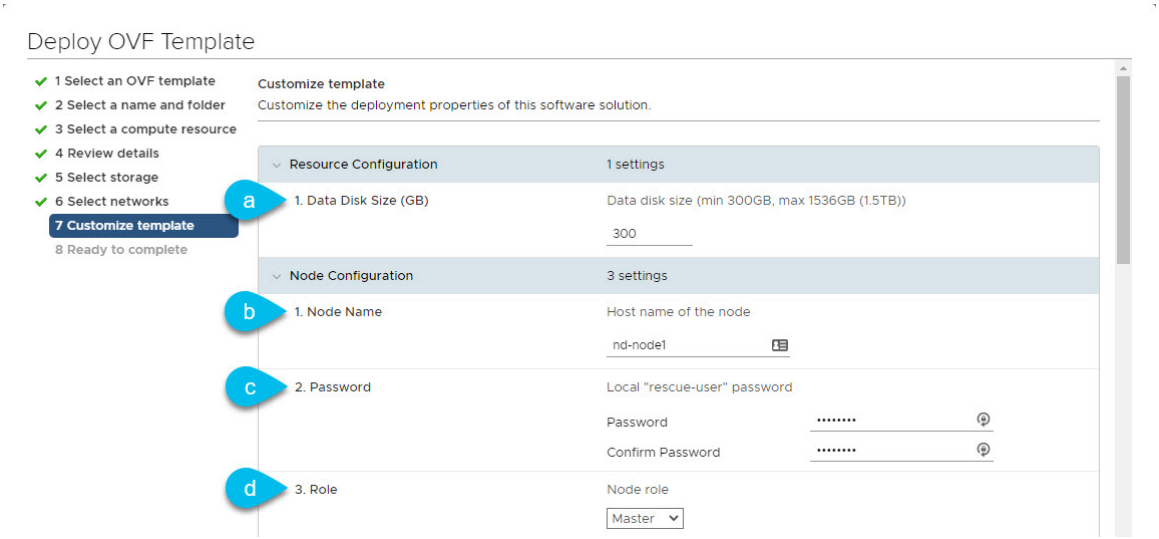
ステップ 9 **[ネットワークの選択（Select Networks）]** 画面で、デフォルト値を受け入れ、**[次へ（Next）]** をクリックして続行します。

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 10 **[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。

（注） 次のいくつかの手順は、使用している vSphere クライアントのバージョンによって異なる順序で表示される場合があります。記載されている順序と例では、VMware vSphere 6.7 を使用しています。

[リソース設定（Resource Configuration）] および **[ノード設定（Node Configuration）]** カテゴリで、次の詳細を入力します。



a) ノードのデータディスクのサイズを指定します。

必要なデータディスクにはデフォルト値を使用することを推奨します。

b) **ノード名** を入力します。

これはノードのホスト名になります。完全修飾ドメイン名（FQDN）は使用しないでください。

たとえば、`nd-node1`

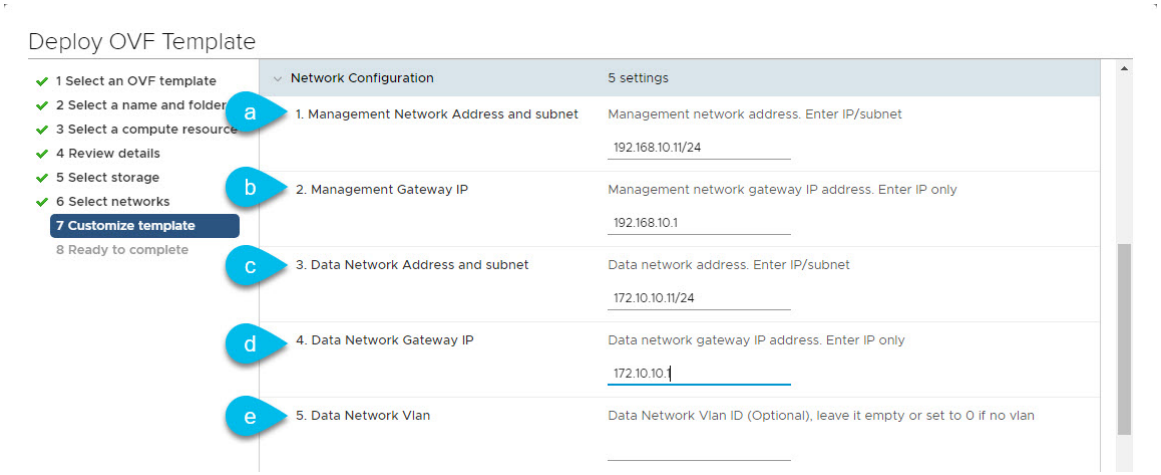
c) **パスワード**を入力して確認します。

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。別のパスワードを指定すると、最初のノードのパスワードが GUI の `admin` ユーザの初期パスワードとして使用されます。

d) **[ロール（Role）]** ドロップダウンから、`[マスター（Master）]` を選択します。

最初にクラスタを展開する場合、3 つのノードすべてがマスターである必要があります。ワーカーノードとスタンバイノードの追加については、『*Cisco Nexus Dashboard User Guide*』を参照してください。

[ネットワーク設定（Network Configuration）] カテゴリで、次の詳細を入力します。



a) ノードの**管理アドレスとサブネット**を入力します。

管理 IP アドレスをデータ ネットワーク IP アドレスと同じまたは異なるサブネットにすることができます。

たとえば、`192.168.10.11/24` です。

b) **管理ゲートウェイ IP** を入力します。

たとえば、`192.168.10.1` と入力します。

c) **データ ネットワーク アドレスとサブネット** を入力します。

データ ネットワーク IP アドレスを管理 IP アドレスと同じまたは異なるサブネットにすることができます。

たとえば、`172.10.10.11/24` と入力します。

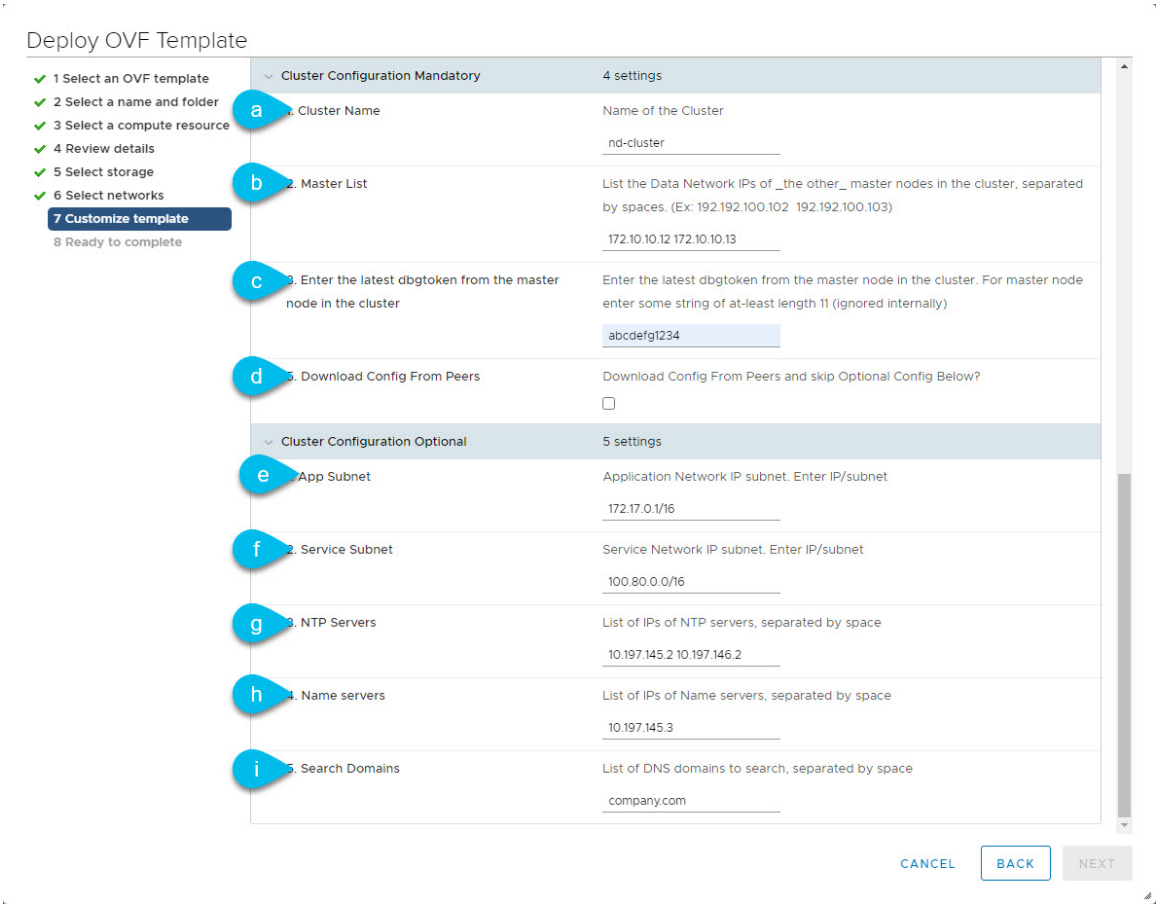
d) **データ ネットワーク ゲートウェイ**を入力します。

たとえば、`172.10.1.1` です。

e) （オプション）データ トラフィックが VLAN 上にある場合は、**データ ネットワーク VLAN** を指定します。

ほとんどの展開では、このフィールドを空白のままにすることができます。データ ネットワークの VLAN ID を指定する場合は、このフィールドに `100` などを入力できます。

[必須のクラスタ設定（Cluster Configuration Mandatory）] カテゴリと **[オプションのクラスタ設定（Cluster Configuration Optional）]** カテゴリで、次の詳細を入力します。



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

この名前は、すべてのノードで同じである必要があります。

たとえば、`nd-cluster` です。

b) In the **Master List** field, provide the data network IP addresses of the other 2 nodes you will configure for your cluster.

リスト内の各 IP アドレスは、スペースで区切る必要があります。

たとえば、3つのノードすべてのデータネットワークIPアドレスが172.10.10.11、172.10.1.12、および172.10.10.13の場合、最初のノードのこのフィールドの値は172.10.10.12 172.10.10.13になります。

c) **[dbgtoken]** フィールドに値を入力します。

これは展開する最初のノードであるため、このフィールドに 11 文字の値を入力します（`abcdef12345` など）。他の 2 つのノードを展開する場合は、このフィールドを使用して最初のノードからトークンを提供し、設定を簡素化します。

d) **[ピアからの設定のダウンロード（Download Config From Peers）]** チェックボックスはオフのままにします。

このオプションは、他の 2 つのノードを設定するときに使用します。

e) **アプリ サブネット**を入力します。

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。

f) **サービス サブネット**を入力します。

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。

g) **NTP サーバ**情報を入力します。

たとえば、`10.197.145.2 10.197.146.2` です。

h) **ネーム サーバ**情報を入力します。

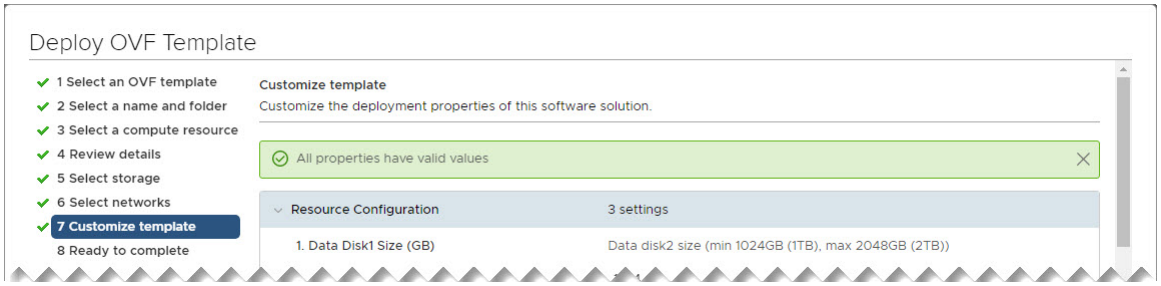
たとえば、`10.197.145.3` です。

i) （オプション）**検索ドメイン**情報を入力します。

たとえば、`company.com` のように入力します。

ステップ 11 すべての情報が有効であることを確認し、**[次へ（Next）]** をクリックして続行します。

[テンプレートのカスタマイズ（Customize template）] 画面を完了すると、上部に確認バナーが表示されます。



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 VM の展開が完了するまで待ち、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 14 最初のノードのコンソールにレスキュー ユーザとしてログインします。

VM の導入時に OVF テンプレートで指定したパスワードを使用します。

ステップ 15 `dbgtoken` を取得します。

次のコマンドを実行します。

```
$ acs debug-token
09GZ1PMB8CML
```

このトークンをメモし、他の 2 つのノードを展開するために使用します。

トークンは 30 分ごとに期限切れになり、更新されるため、2 番目と 3 番目のノードを展開する準備ができたらトークンを取得してください。

ステップ 16 2 番目のノードを展開します。

2 番目と 3 番目のノードを展開する手順は似ていますが、最初のノードから `dbgtoken` を使用して一部の設定をスキップできる点が異なります。

a) ステップ 2ー9 を繰り返して、2 番目のノードの展開を開始します。

ノードごとに異なる ESX ホストを使用することを推奨します。

b) **[クラスタ設定（Cluster Configuration）]** 画面で、次の情報を入力します。

- **ノード名**

  完全修飾ドメイン名（FQDN）（Fully Qualified Domain Name (FQDN) を使用しないでください。

- **[パスワード（Password）]**

  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。別のパスワードを指定すると、最初のノードのパスワードが GUI の `admin` ユーザの初期パスワードとして使用されます。

- **[ロール（Role）]**

  最初にクラスタを展開する場合、3 つのノードすべてがマスターである必要があります。

- **管理ネットワーク アドレスとサブネット**
- **管理 IP ゲートウェイ**
- **データ ネットワーク アドレスとサブネット**
- **データ ネットワーク ゲートウェイ**
- （オプション）データ トラフィックが VLAN 上にある場合は、**データ ネットワーク VLAN** を指定します。
- **クラスタ名**

  この名前は、すべてのノードで同じである必要があります。たとえば、`nd-cluster` です。

- **マスター リスト**

  Provide the data network IP addresses of the other 2 nodes in your cluster separated by a space.

たとえば、3つのノードすべてのデータネットワークIPアドレスが172.10.10.11、172.100.10.12、および172.10.10.13の場合、2番目のノードのこのフィールドの値は172.10.10.11 172.10.10.13になります。

- 最初のノードから取得した **dbgtoken** を入力します。

  トークンは 30 分ごとに期限切れになり、更新されます。続行する前に、最初のノードから最新の有効なトークンを取得してください。たとえば、`09GZ1PMB8CML` です。

- **ピアからのダウンロード設定**の確認

  2 番目と 3 番目のノードは、`dbgtoken`を使用して最初のノードから共通の設定パラメータをダウンロードします。

c) **[オプションのクラスタ設定（Cluster Configuration Optional）]** フィールドをスキップし、**[次へ（Next）]** をクリックして続行します。

d) **[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 2 番目のノードの展開を開始します。

ステップ 17 前の手順を繰り返して、3 番目のノードを展開します。

ステップ 18 2 番目と 3 番目のノードの VM の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 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 - [...]
```

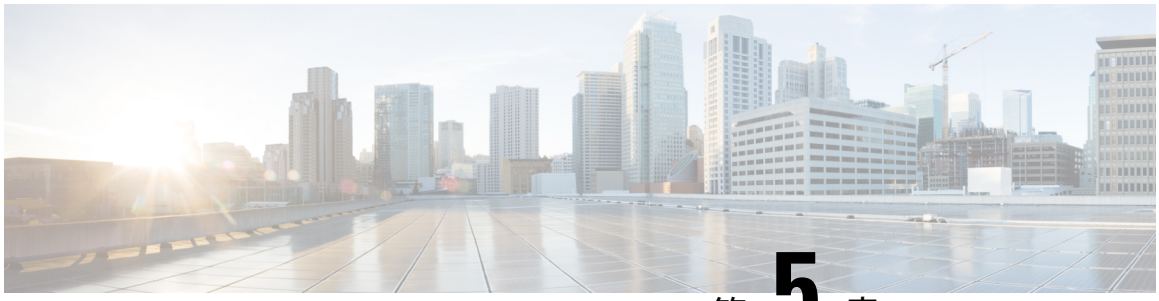
```
$ acs health
k8s: Etcd cluster is not ready
```

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。



第 5 章

Amazon Web Services での展開

前提条件とガイドライン

クラウド展開は、Nexus ダッシュボード リリース 2.0.2b 以降でサポートされています。以前のリリースは 物理アプライアンスとしての展開 （25 ページ） で説明された物理フォーム ファクタのみをサポートします。

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

- 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。
- AWS フォーム ファクタが規模とアプリケーションの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、拡張性とアプリケーションの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。

- 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`/28` 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。

  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ノードに SSH 接続できるようにするには、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。これを行うには、最初にPEMファイルを使用して各ノードに個別にログインし、次のコマンドを実行します。

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

AWS での Cisco 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 （45 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) [サブスクリプションの管理（Manage Subscriptions）] をクリックします。

d) **[製品の検出（Discover products）]** をクリックします。

e) **Cisco Nexus 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。

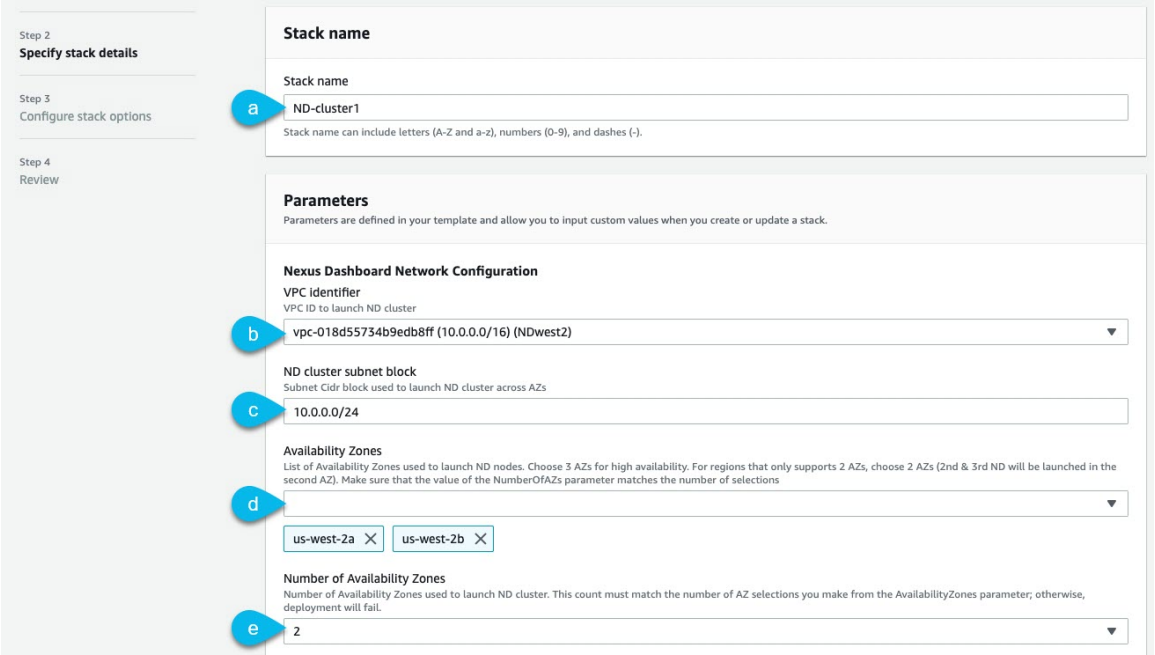
a) **[前提条件 - テンプレートの準備（Prerequisite-Prepare template）]** 領域で、`[テンプレート準備完了（Template is ready）]` を選択します。
b) **[テンプレートの指定（Specify Template）]** フィールドで、テンプレート ソースとして `[Amazon S3 URL]` を選択します。

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。

たとえば、`10.176.176.0/24` です。

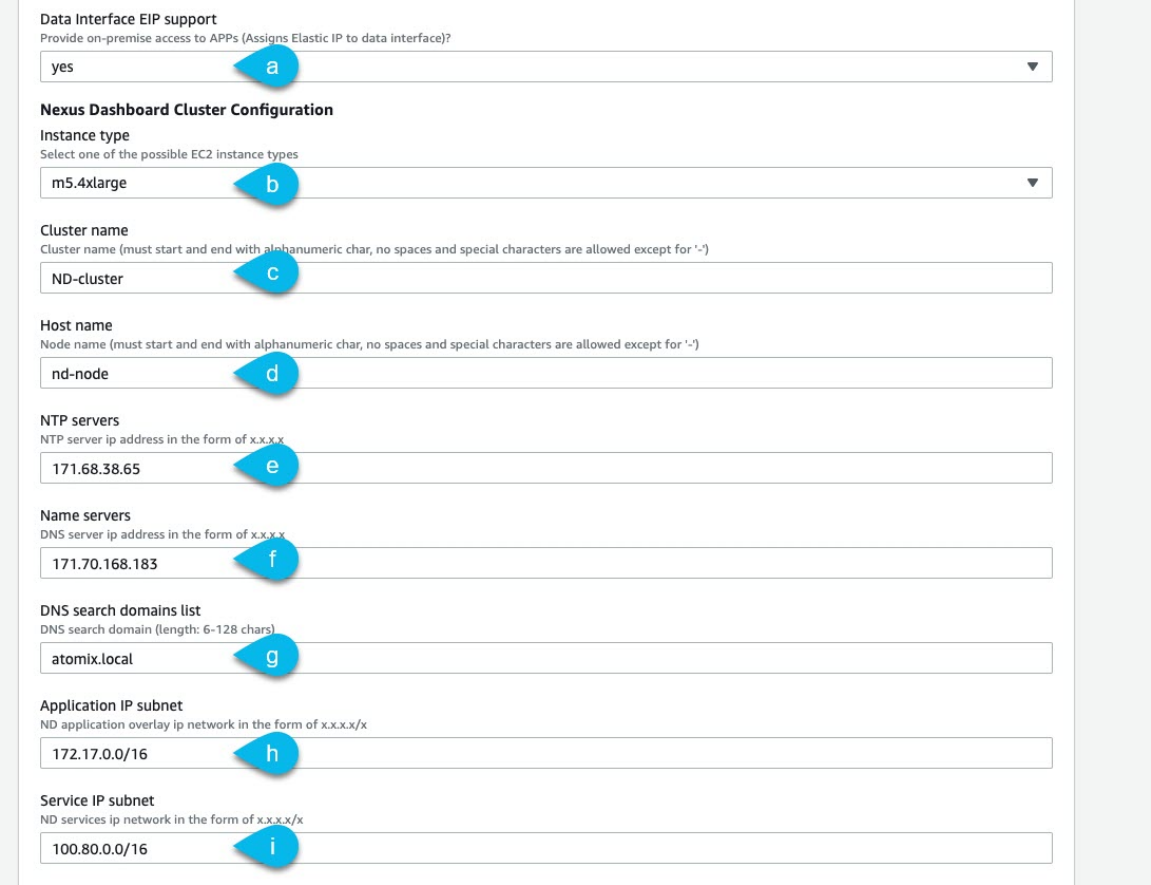
d) **[可用性ゾーン（Availability Zones）]** ドロップダウンから、1 つ以上の使用可能なゾーンを選択します。

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。

残りのノード情報を入力します。



a) **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。

b) **[インスタンス タイプ（Instance type）]** から、`[m5.2xlarge]` を選択します。

c) **クラスタ名** を指定します。

クラスタ名は、展開するすべてのノードで同じである必要があります。

d) **ホスト名**のプレフィックスを入力します。

テンプレートは、各ノードが**ホスト名**プレフィックスを使用し、`-1`、`-2`、および`-3`を追加して各ノードに一意のホスト名を作成する 3 ノードクラスタを展開します。

e) **NTP サーバ**情報を入力します。

f) **ネーム サーバ**情報を入力します。

g) （オプション）**DNS 検索ドメイン リスト**を指定します。

h) **アプリケーション IP サブネット**を指定します。

たとえば、`10.101.0.0/16` です。

i) **サービス IP サブネット**を指定します。

このサービス 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。

たとえば、`10.102.0.0/16` です。

最後に、ログイン情報とアクセス情報を入力します。

a) **[パスワード (Password)]** フィールドに、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。

b) **[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。

c) **[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。

d) [次へ（Next）] をクリックして続行します。

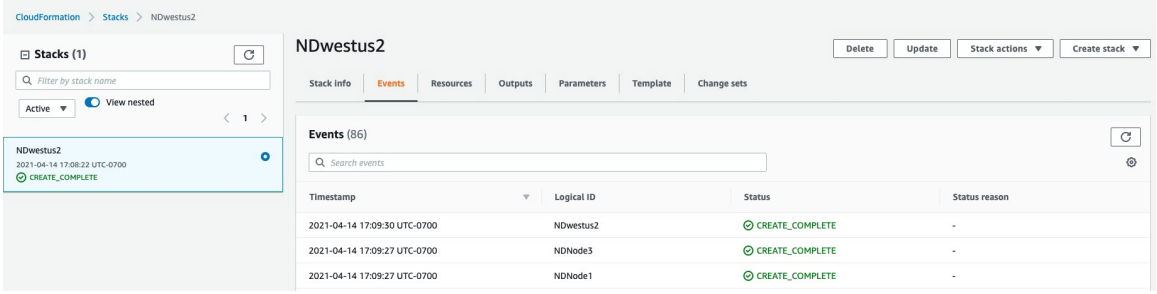
ステップ 6 **[詳細オプション（Advanced options）]** 画面で、**[次へ（Next）]**をクリックします。

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 インスタンスの展開が完了するのを待ってから、インスタンスを起動します。

[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。



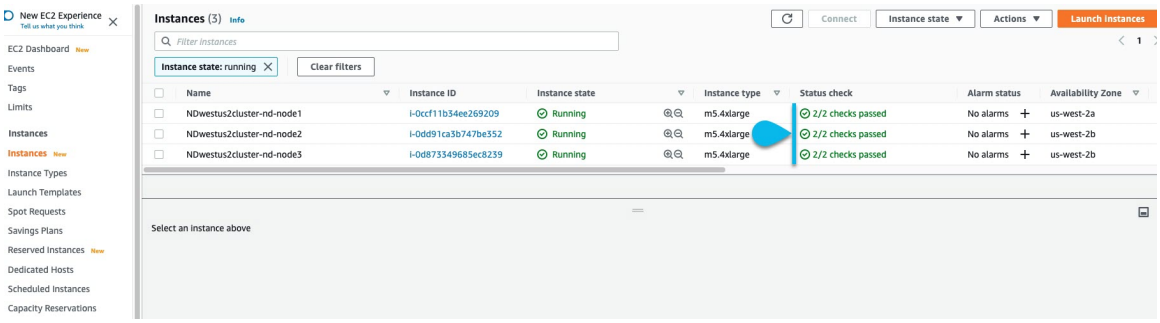
ステップ 9 クラスタが健全であることを検証します。

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 つのノードすべてのステータスが `CREATE_COMPLETE` になったら、次のサブステップに進み、クラスタの状態を確認します。

a) AWS EC2 インスタンスが稼働していることを確認します。

[サービス（Services）] > [EC2] に移動します。次に、**[ステータス チェック（Status Checks）]** タブに `2/2` チェックが表示されることを確認します。



b) いずれかのノードにログインします。

次のコマンドでキーペアを作成するときに、ダウンロードした秘密キー `.pem` ファイルを使用する必要があります。

```
$ ssh -i <pem-file-name>.pem rescue-user@<node-ip-address>
```

c) 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
```

d) Nexus ダッシュボード GUI にログインします。

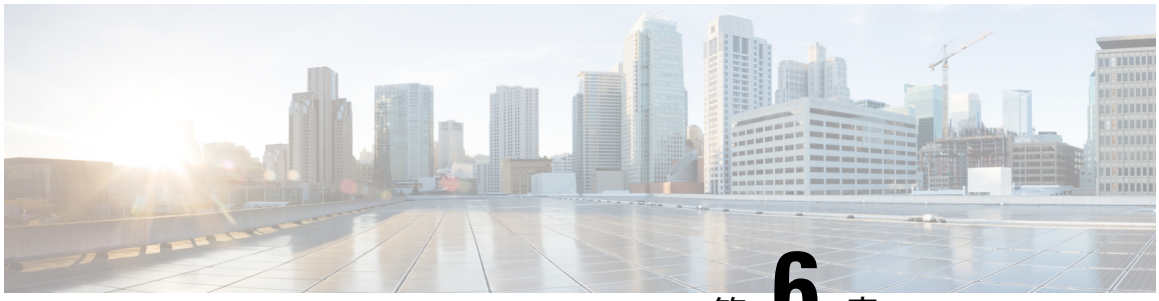
クラスタが使用可能になったら、ノードの管理IPアドレスのいずれかを参照してアクセスできます。管理者ユーザのデフォルト パスワードは、Nexus ダッシュボード クラスタの最初のノードに選択したレスキュー ユーザ パスワードと同じです。

初めてログインしたとき、パスワードを変更するよう求められます。

ステップ 10 （オプション）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ノードに SSH 接続できるようにするには、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。これを行うには、最初にPEMファイルを使用して各ノードに個別にログインし、次のコマンドを実行します。

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



第 6 章

Microsoft Azure での展開

前提条件とガイドライン

クラウド展開は、Nexus ダッシュボード リリース 2.0.2b 以降でサポートされています。以前のリリースは 物理アプライアンスとしての展開 （25 ページ） で説明された物理フォーム ファクタのみをサポートします。

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

- 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。
- Azure フォーム ファクタが規模とアプリケーションの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、拡張性とアプリケーションの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。
- 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。
- 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 VM に接続するときに ID を確認するためのセキュリティ クレデンシャルとして使用されます。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。

  `putty` などの外部ユーティリティを使用して、クラスタのキー ペアを生成できます。

Azure での Cisco 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 （55 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。

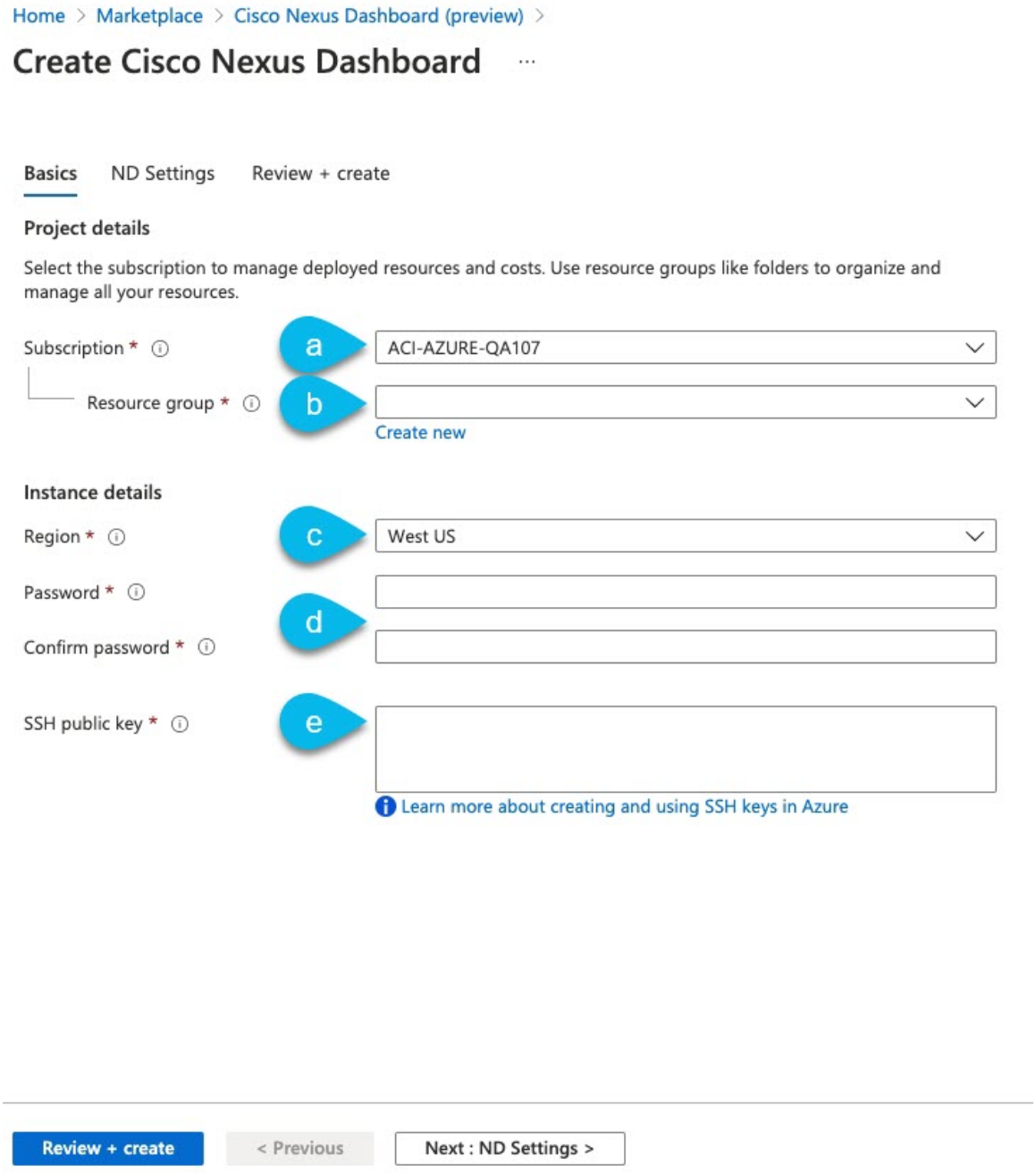
ステップ 1 Azure Marketplace で Cisco Nexus ダッシュボード製品に登録します。

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 **[Basics]** タブで、サブスクリプションの詳細、リージョン、およびパスワードを入力します。



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、クラスタの既存のリソース グループを選択するか、**[新規作成（Create new）]** をクリックして作成します。

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。

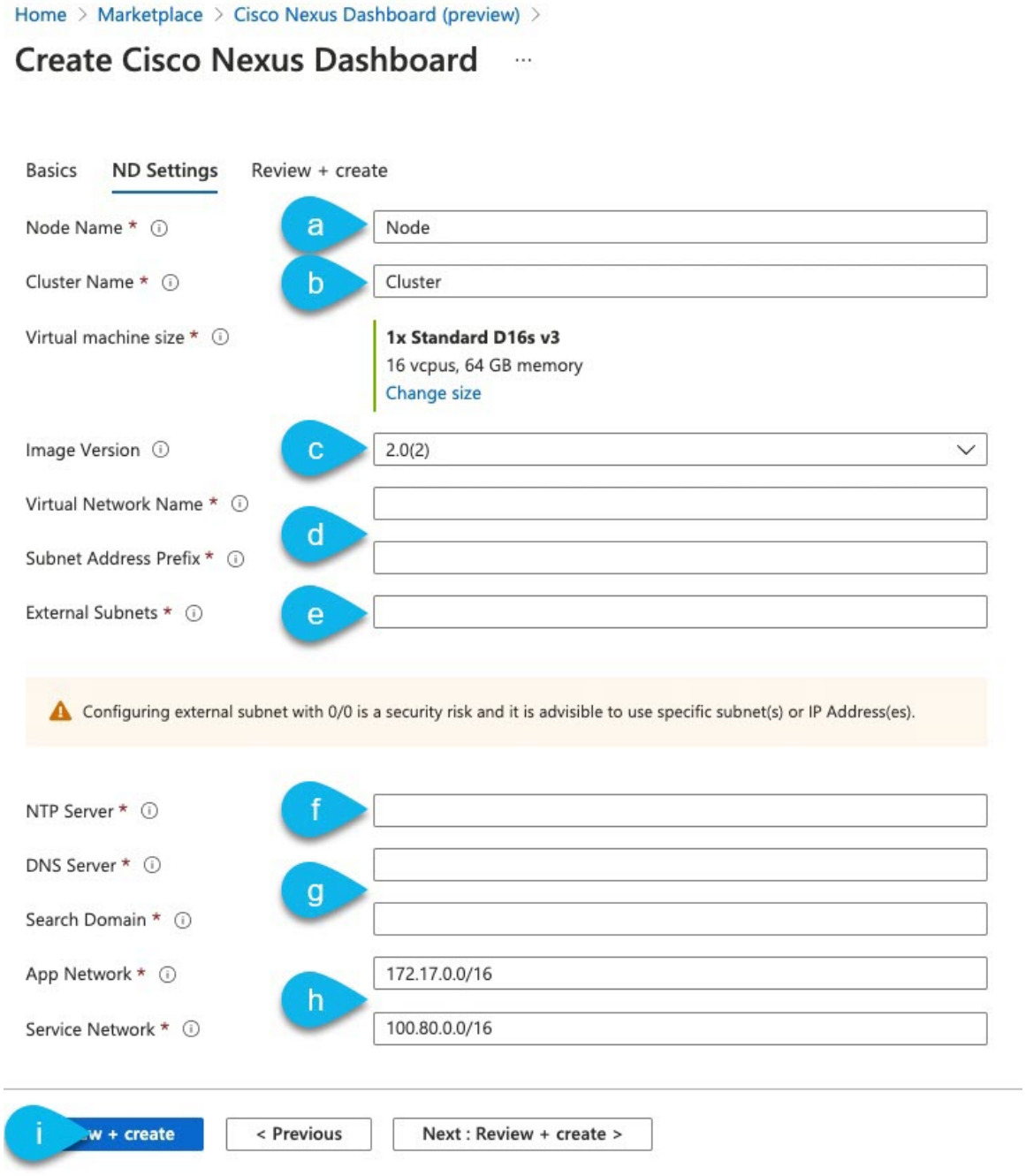
これは、リソース グループと VNET を作成したのと同じリージョンである必要があります。

d) ノードのパスワードを入力して確認します。

これは、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同じです。

e) **[SSH public key]**フィールドに、前提条件とガイドライン （55 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。

ステップ 3 **ND設定**クラスタの詳細を入力します。



a) **ノード名** を入力します。

テンプレートは、**ノード名**プレフィックスを使用し、各ノードに一意のホスト名を作成するために1、2、および 3 を追加した各ノードで 3 ノード クラスタを展開します。

b) **クラスタ名** を指定します。

クラスタ名は、展開するすべてのノードで同じである必要があります。

c) **[イメージ バージョン（Image Version）]** ドロップダウンで、最新のリリースが選択されていることを確認します。

d) **[仮想ネットワーク名（Virtual Network Name）]** フィールドと **[サブネット アドレス プレフィックス（Subnet Address Prefix）]** フィールドに VNET の名前を入力し、その VNET 内のサブネットを選択します。

入力した名前の VNET が存在しない場合は、作成されます。

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) **NTP サーバ**情報を入力します。

g) **DNS サーバ**と**検索ドメイン**情報を指定します。

h) **アプリケーション ネットワーク**と**サービス ネットワーク**を提供します。

これらは、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。

たとえば、`172.17.0.1/16` および `100.80.0.0/16` です。

i) **[確認して作成（Review + create）]** 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 4 VM の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 5 （任意）パスワードベースの SSH 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ノードに SSH 接続できるようにするには、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。これを行うには、Azure から各ノードの VM コンソールに接続し、クラスタの導入時に指定したパスワードを使用してレスキュー ユーザとしてログインし、次のコマンドを実行します。

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

ステップ 6 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。

a) いずれかのノードにログインします。

```
$ ssh rescue-user@<node-ip-address>
```

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
```

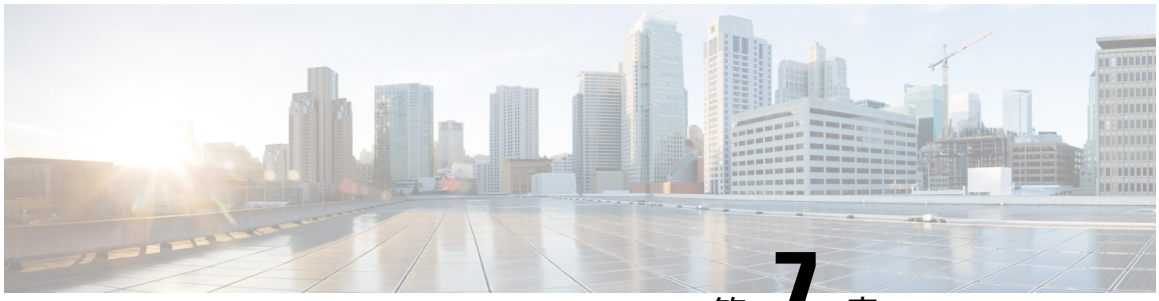
クラスタが稼働している場合は、次の出力が表示されます。

```
$ 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。

初めてログインしたとき、パスワードを変更するよう求められます。



第 7 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 Dashboard 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。
- Cisco Nexus ダッシュボード、リリース 2.0.1 以降を実行している必要があります。

  Cisco Application Services Engine を実行している場合は、代わりに Application Services Engine からのアップグレード （65 ページ） で説明されている手順に従います。
- 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。

  物理サーバー、VMware ESX OVA、または Azure または AWS クラウドを使用してクラスタを展開したかどうかに関係なく、ターゲット リリースの ISO イメージを使用してアップグレードします。
- 現在の Nexus ダッシュボードクラスタが正常であることを確認します。

  Nexus ダッシュボード GUI の **[システム概要（System 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` コマンドを実行します。
- アップグレードの前にクラスタにインストールされているアプリケーションを無効にし、アップグレードが正常に完了した後に再度有効にする必要があります。

  アプリケーションを再度有効にする前に、『*Cisco Nexus Dashboard User Guide*』の「App Infra Services」セクションの説明に従って、App Infra Services 展開プロファイルを設定する必要があります。
- リリース 2.0.2 にアップグレードした後は、すべてのアプリケーションを最新バージョンにアップグレードすることをお勧めします。

Nexus ダッシュボードのアップグレード

- リリース 2.0.2 からのダウングレードはサポートされていません。

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 （61 ページ）

ステップ 1 Nexus Dashboard イメージをダウンロードします。

a) [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 ダッシュボードのバージョンを選択します。

c) Cisco Nexus ダッシュボード イメージ（`nd-dk9.<version>.iso`）。

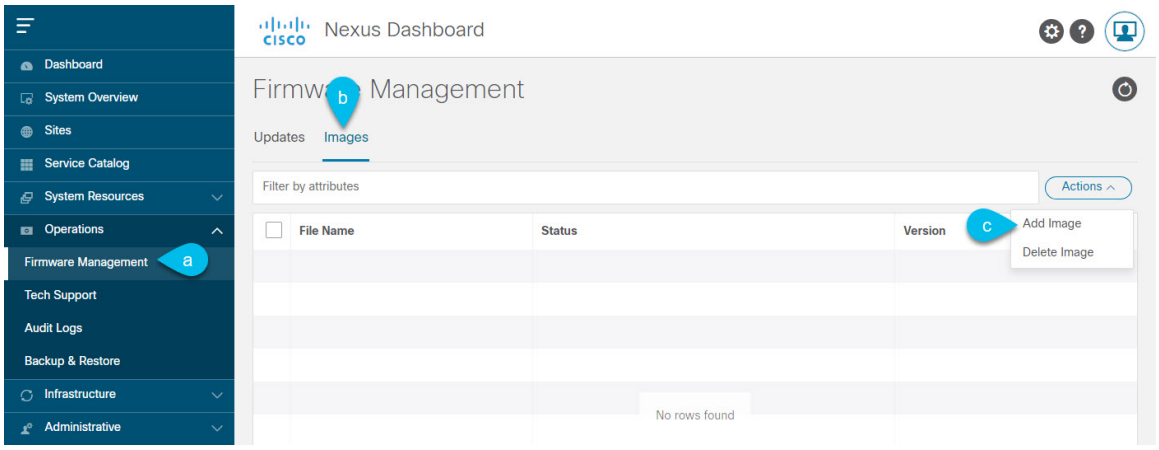
（注） 最初のクラスタ展開に VMware ESX `.ova` イメージまたはクラウド プロバイダーのマーケットプレイスを使用した場合でも、すべてのアップグレードで `.iso` イメージをダウンロードする必要があります。

d) （任意）環境内の Web サーバーでイメージをホストします。

イメージを Nexus Dashboard クラスタにアップロードする際に、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 ダッシュボードGUIに管理者ユーザとしてログインします。

ステップ 3 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。

Nexus ダッシュボードのアップグレード

b) **[イメージ]** タブを選択します。
c) **[アクション（Actions）]** メニューから、**[イメージの追加（Add Image）]**をクリックします。

ステップ 4 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 イメージを選択します。

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。

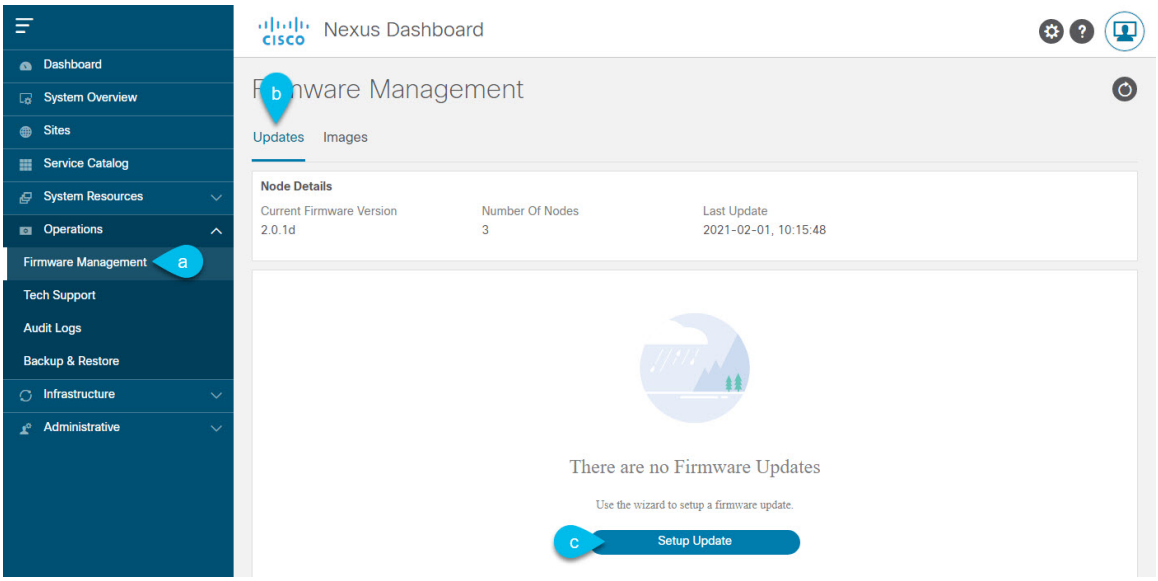
c) **[アップロード（Upload）]** をクリックして、イメージを追加します。

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 5 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 6 更新を設定します。



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) **[更新]** タブを選択します。
c) **[更新のセットアップ（Setup Update）]** をクリックします。

[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 7 アップグレードイメージを選択します。

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、**[インストールの開始（Begin 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。このプロセスは、全体で最大 20 分かかる場合があります。

ステップ 8 新しい画像をアクティブにします。

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、**[詳細の表示（View Details）]** をクリックします。

c) [Activate] をクリックします。

d) **[アクティブ化確認]** ウィンドウで、**[続行]** をクリックします。

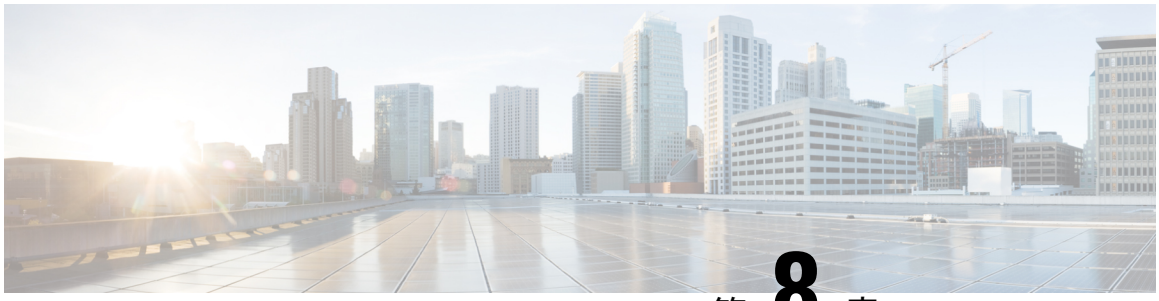
すべてのクラスタサービスが起動し、GUI が使用可能になるまでに、さらに最大 20 分かかる場合があります。このページは、プロセスが完了すると、自動的に再ロードされます。

ステップ 9 同じクラスタで複数のアプリケーションをホストしている場合は、App Infra Services の展開プロファイルを設定します。

Nexus ダッシュボードクラスタで単一のアプリケーションのみをホストしている場合は、この手順をスキップします。

同じクラスタに複数のアプリケーションをホストする場合は、アプリケーションとファブリック サイズの組み合わせに適した展開プロファイルを使用して、 App Infra Services を設定する必要があります。

クラスタのアップグレードが完了したら、 『*Cisco Nexus Dashboard User Guide*』の「App Infra Services」セクションに記載されている手順に従ってください。このガイドは、製品の GUI からも入手できます。



第 8 章

Application Services Engine からのアップグレード

前提条件とガイドライン

既存の Cisco Application Services Engine リリース 1.1.3 クラスタを Cisco Nexus ダッシュボードに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。
- Cisco Application Services Engine リリース 1.1.3d を物理アプライアンスとして実行している必要があります。

  すでに Cisco Nexus ダッシュボードを実行している場合は、代わりに Nexus ダッシュボードのアップグレード （61 ページ） に記載されている手順に従います。

  Application Services Engine の以前のリリースからのアップグレードはサポートされていません。このドキュメントの前の章で説明されているように、新しいクラスタを展開する必要があります。

  Application Services Engine が VMware ESX、Linux KVM、または Amazon Web Services に展開されている場合は、Nexus ダッシュボードにアップグレードできません。
- 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。

  物理サーバー、VMware ESX OVA、または Azure または AWS クラウドを使用してクラスタを展開したかどうかに関係なく、ターゲット リリースの ISO イメージを使用してアップグレードします。
- 現在の Application Services Engine が正常であることを確認します。

- 既存の Application Services Engine クラスタに無効なアプリケーションがある場合は、それらを削除してから Nexus ダッシュボードにアップグレードすることをお勧めします。
- Application Services Engine クラスタで Multi-Site Orchestrator アプリケーションを実行している場合は、クラスタを Nexus ダッシュボードにアップグレードする前にアンインストールする必要があります。

  Nexus ダッシュボードで実行している Multi-Site Orchestrator への移行は、プラットフォームのアップグレード、アプリケーションのインストール、設定の復元、クラウドサイトのアップグレードなど、複数の手順で構成されます。『*Multi-Site Deployment Guide*』の「Migrating Existing Cluster to Nexus Dashboard」の章で説明されている MSO移行手順に従うことを強く推奨します。
- Nexus Dashboard リリース 2.0.2 にアップグレードした後は、すべてのアプリケーションを最新バージョンにアップグレードすることをお勧めします。
- Nexus Dashboard リリース 2.0.2 からのダウングレードはサポートされていません。

Application Services Engine からのアップグレード

ここでは、既存の Application Services Engine リリース 1.1.3d クラスタを Nexus ダッシュボードにアップグレードする方法について説明します。

始める前に

- で説明している前提条件をすべて満たしていることを確認します。前提条件とガイドライン （61 ページ）

ステップ 1 Nexus Dashboard イメージをダウンロードします。

a) [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 ダッシュボードのバージョンを選択します。

c) Cisco Nexus ダッシュボード イメージ（`nd-dk9.<version>.iso`）。

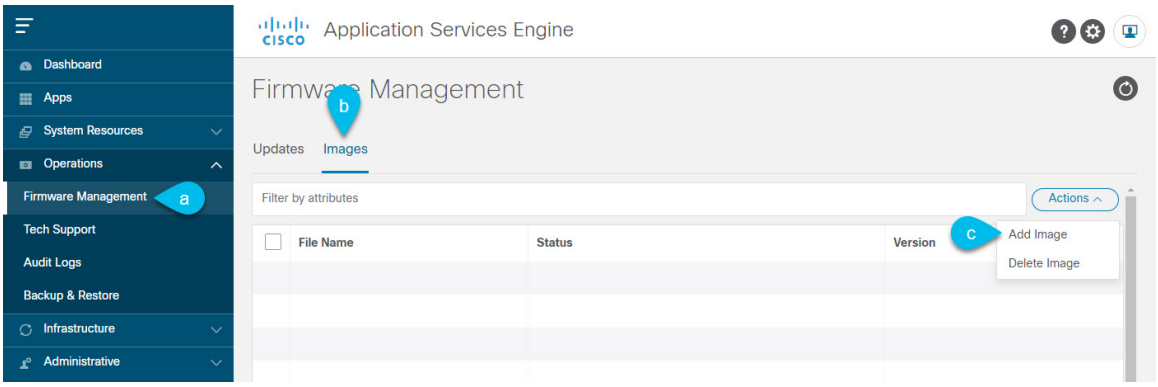
（注） 最初のクラスタ展開に VMware ESX `.ova` イメージまたはクラウド プロバイダーのマーケットプレイスを使用した場合でも、すべてのアップグレードで `.iso` イメージをダウンロードする必要があります。

d) （任意）環境内の Web サーバーでイメージをホストします。

イメージを Nexus Dashboard クラスタにアップロードする際に、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 Application Services Engine GUI に管理者ユーザとしてログインします。

ステップ 3 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) **[アクション（Actions）]** メニューから、**[イメージの追加（Add Image）]**をクリックします。

ステップ 4 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 イメージを選択します。

   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。

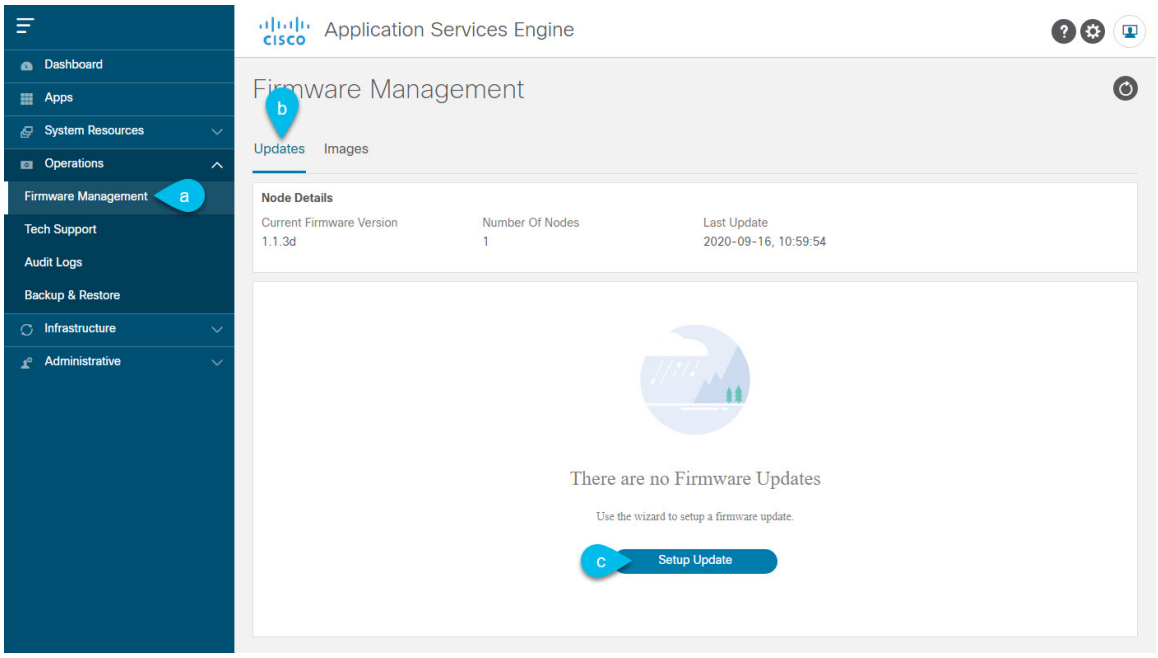
   イメージが Application Services Engine クラスタにアップロードされ、展開されて処理され、アップグレードに使用できるようになります。プロセス全体に数分かかる場合があり、**[イメージ（Images）]** タブでプロセスのステータスを確認できます。

ステップ 5 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 6 更新を設定します。

Application Services Engine からのアップグレード



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) **[更新のセットアップ（Setup Update）]** をクリックします。

ステップ 7 更新の詳細を入力します。

a) **[バージョンの選択（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) **[確認（Confirmation）]** 画面で詳細を確認し、**[インストールの開始（Begin 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。

ステップ 8 新しい画像をアクティブにします。

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、**[詳細の表示（View Details）]** をクリックします。
c) [Activate] をクリックします。
d) **[アクティブ化確認]** ウィンドウで、**[続行]** 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。