



Cisco Nexus ダッシュボード展開ガイド、リリース 2.1.x

初版：2021年9月14日

最終更新：2022年9月5日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: <http://www.cisco.com/go/softwareterms>. Cisco product warranty information is available at <http://www.cisco.com/go/warranty>. US Federal Communications Commission Notices are found here <http://www.cisco.com/c/en/us/products/us-fcc-notice.html>.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and-if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com go trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021–2022 Cisco Systems, Inc. All rights reserved.



目次

Trademarks ?

第 1 章	新機能および変更された機能に関する情報 1 新機能および変更された機能に関する情報 1
第 2 章	展開の概要と要件 3 デプロイ概要 3 前提条件とガイドライン 6 ファブリック接続 15 サイト間のノード分散 22 サービスのコロケーションの使用例 26 インストール前のチェックリスト 28
第 3 章	物理アプライアンスとしての展開 31 前提条件とガイドライン 31 Cisco Nexus ダッシュボードを物理アプライアンスとして展開 33
第 4 章	VMware ESX の展開 39 前提条件とガイドライン 39 VMware vCenter を使用している Cisco Nexus ダッシュボードの展開 43 VMware ESXi での Cisco Nexus ダッシュボードの直接展開 52
第 5 章	Linux KVMでの展開 59 前提条件とガイドライン 59

Linux KVM での Cisco Nexus ダッシュボードの展開 60

第 6 章

Amazon Web Services での展開 69

前提条件とガイドライン 69

AWS での Cisco Nexus ダッシュボードの展開 71

第 7 章

Microsoft Azure での展開 79

前提条件とガイドライン 79

Linux または MacOS での SSH キー ペアの生成 80

Windows での SSH キー ペアの生成 81

Azure での Cisco Nexus ダッシュボードの展開 84

第 8 章

Nexus ダッシュボードのアップグレード 91

前提条件とガイドライン 91

Nexus ダッシュボードのアップグレード 92



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 \(1 ページ\)](#)

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
2.1.2	ラスタの初期ブートストラップ中にプロキシ設定を追加しました。	物理アプライアンスとしての展開 (31 ページ) Linux KVMでの展開 (59 ページ) VMware ESX の展開 (39 ページ)
2.1.2	サービスと必要なポートの説明を追加	デプロイ概要 (3 ページ)
2.1.1	このドキュメントの最初のリリース。	--



第 2 章

展開の概要と要件

- デプロイ概要 (3 ページ)
- 前提条件とガイドライン (6 ページ)
- ファブリック接続 (15 ページ)
- サイト間のノード分散 (22 ページ)
- サービスのコロケーションの使用例 (26 ページ)
- インストール前のチェックリスト (28 ページ)

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。

各 Nexus Dashboard クラスタは通常、3 つのマスターノードで構成されます。また、多数のワーカーノードをプロビジョニングして、水平スケーリングを有効にしたり、スタンバイノードでマスターノードで障害が発生した場合に簡単にクラスタを回復したりすることができます。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、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リ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。

リリース 2.1(2) 以降、物理的な Nexus ダッシュボード サーバーを注文する場合、Nexus ダッシュボード Insights および Nexus ダッシュボード オーケストレータ 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、サービスのインストールに変更はなく、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。

- 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。

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 \(91 ページ\)](#) 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、最新リリースに直接アップグレードできます。

Application Services Engineからのアップグレード

Cisco Application Services Engine を実行している場合は、Nexus ダッシュボード リリース 2.1.x にアップグレードする前に、『[Cisco Nexus ダッシュボード展開ガイド、リリース 2.0\(x\)](#)』の説明に従って、Nexus ダッシュボード リリース 2.0.2g 以降にアップグレード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ダッシュボードは、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。

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
<ul style="list-style-type: none"> • 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 APIC、および NDFC/DCNM 通信への Nexus ダッシュボードノード <p>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。</p>	<ul style="list-style-type: none"> • 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 <p>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</p> <ul style="list-style-type: none"> • 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。

- 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 DCNM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ります。そのため、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。

また、2つのインターフェースが同じサブネット内にある場合、いずれかのIPがトラフィックの送信元として使用される可能性があることにも注意してください。たとえば、リモート認証が構成されている場合、2つのインターフェースのいずれかが認証トラフィックの送信元として使用される可能性があるため、管理IPとデータIPの両方を外部認証プロバイダーの許可されたIPアドレスのリストに追加する必要があります。

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	同じサブネットでのデータと管理のサポート
Nexus Dashboard Orchestrator	レイヤ 3 隣接	レイヤ 3 隣接	N/A	○ ただし、2つのネットワークには個別のサブネットを使用することをお勧めします
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	N/A	○ ただし、2つのネットワークには個別のサブネットを使用することをお勧めします

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	同じサブネットでのデータと管理のサポート
SFLOW/NetFlow (NDFC/DCNM 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	いいえ
SFLOW/NetFlow (ACI または NDFC/DCNM 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	いいえ

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	同じサブネットでのデータと管理のサポート
Nexusダッシュボードファブリックコントローラ	レイヤ 2 隣接	レイヤ 2 隣接	次のいずれかが必要です。 <ul style="list-style-type: none"> デフォルトの LAN デバイス管理接続設定を使用する場合、管理ネットワーク内の 2 つの IP データへの LAN デバイス管理接続を設定する場合、データネットワーク内の 2 つの IP さらに、データネットワークの EPL 用にファブリックごとに 1 つの IP	いいえ
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 / DCNM サイトの場合 : 150 ミリ秒
Nexus Dashboard Insights	ノード間	50 ミリ秒
	サイトへ	50 ミリ秒
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
	サイトへ	50 ミリ秒
Cisco Nexus Dashboard Data Broker	ノード間	150 ミリ秒
	サイトへ	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。

通信ポート

Nexus ダッシュボード 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 5: Nexus Dashboard 通信ポート (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

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
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 の通信ポート (データ ネットワーク)

サービス	ポート	プロトコル	方向 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
SSH	22	TCP	発信	スイッチと APIC の帯域内

サービス	ポート	プロトコル	方向 イン：クラスタに対して 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
HTTPS	443	TCP	発信	スイッチおよびAPIC/NDFC/DCNMの帯域内
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
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
Kafka	30001	TCP	入力 / 出力	スイッチのインバンドおよびAPIC/NDFC/DCNM
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

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	30500 ~ 30600	TCP および UDP	入力 / 出力	その他のクラスタノード

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

サービス	ポート	プロトコル	方向 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
テックコレクションを表示	2022	TCP	入力 / 出力	スイッチのインバンドおよび APIC/NDFC/DCNM
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	外部
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
SW テレメトリ	5695 30000 57500 30570	TCP	入力 / 出力	その他のクラスタノード

ファブリック接続

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 NDFC/DCNM ファブリックの場合、Nexus ダッシュボード クラスターは次の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 クラスター。
- 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。

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。

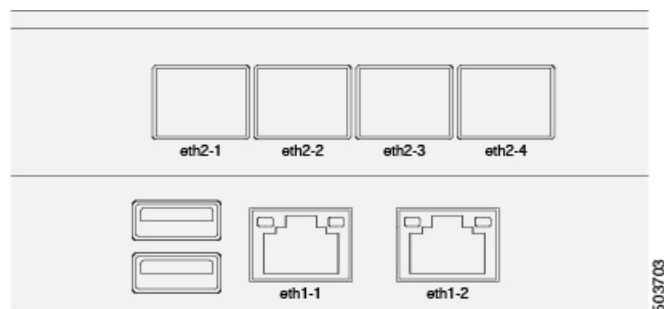
物理ノードのケーブル接続

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

次の図に、Nexus Dashboard 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、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v1an0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 クラスターは、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、クラスター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。
- Nexus Dashboard Orchestrator を展開して Cisco NDFC/DCNM ファブリックを管理する場合は、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 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/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、NDFC/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。

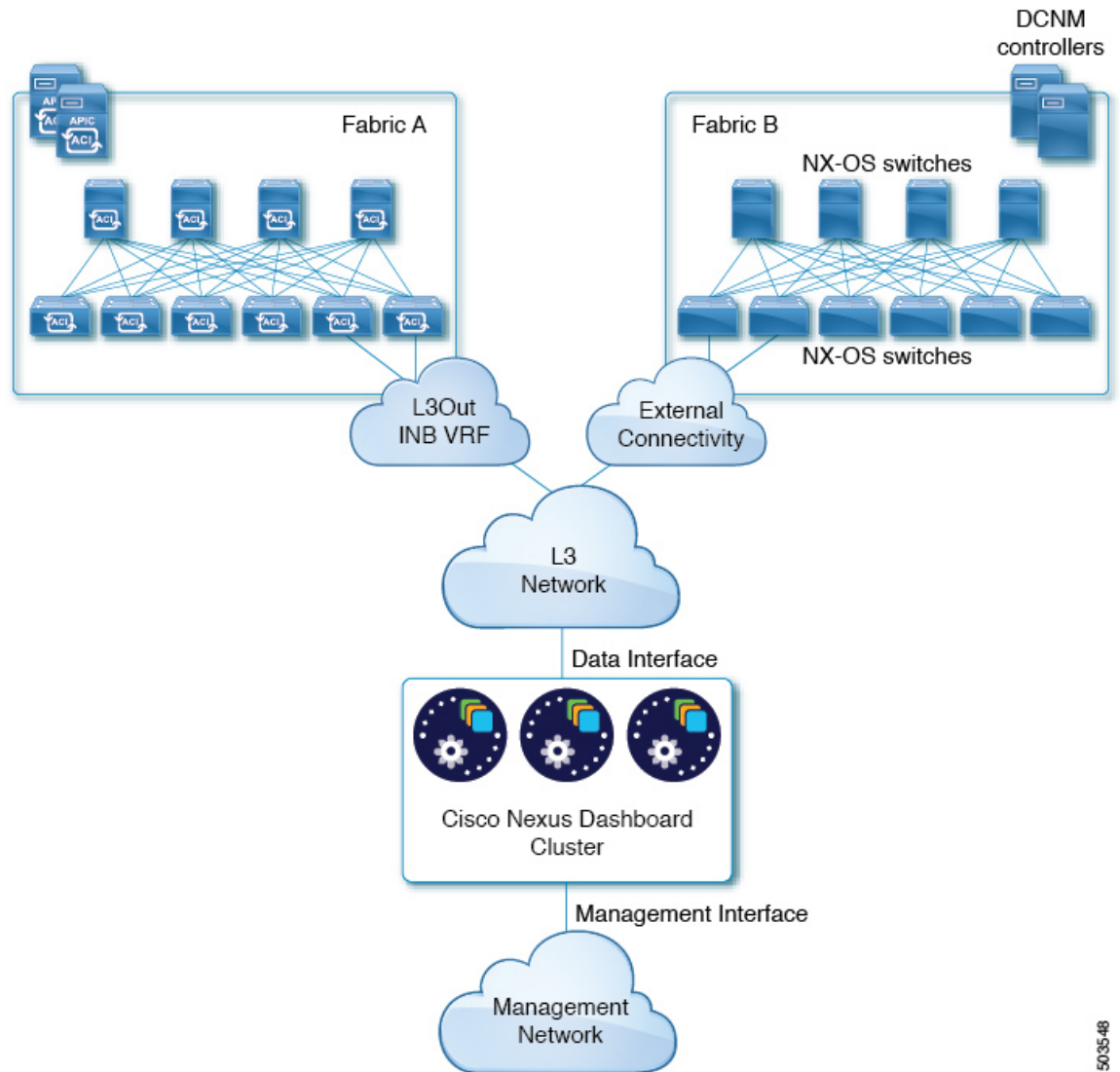
NDFC/DCNM UI からルートを追加するには、[**管理者 (Administration)**] > [**カスタマイズ (Customization)**] > [**ネットワーク設定 (Network Preference)**] > [**インバンド (In-Band) (eth2)**] に移動し、ルートを追加して保存します。

- 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 を指定する場合は、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。

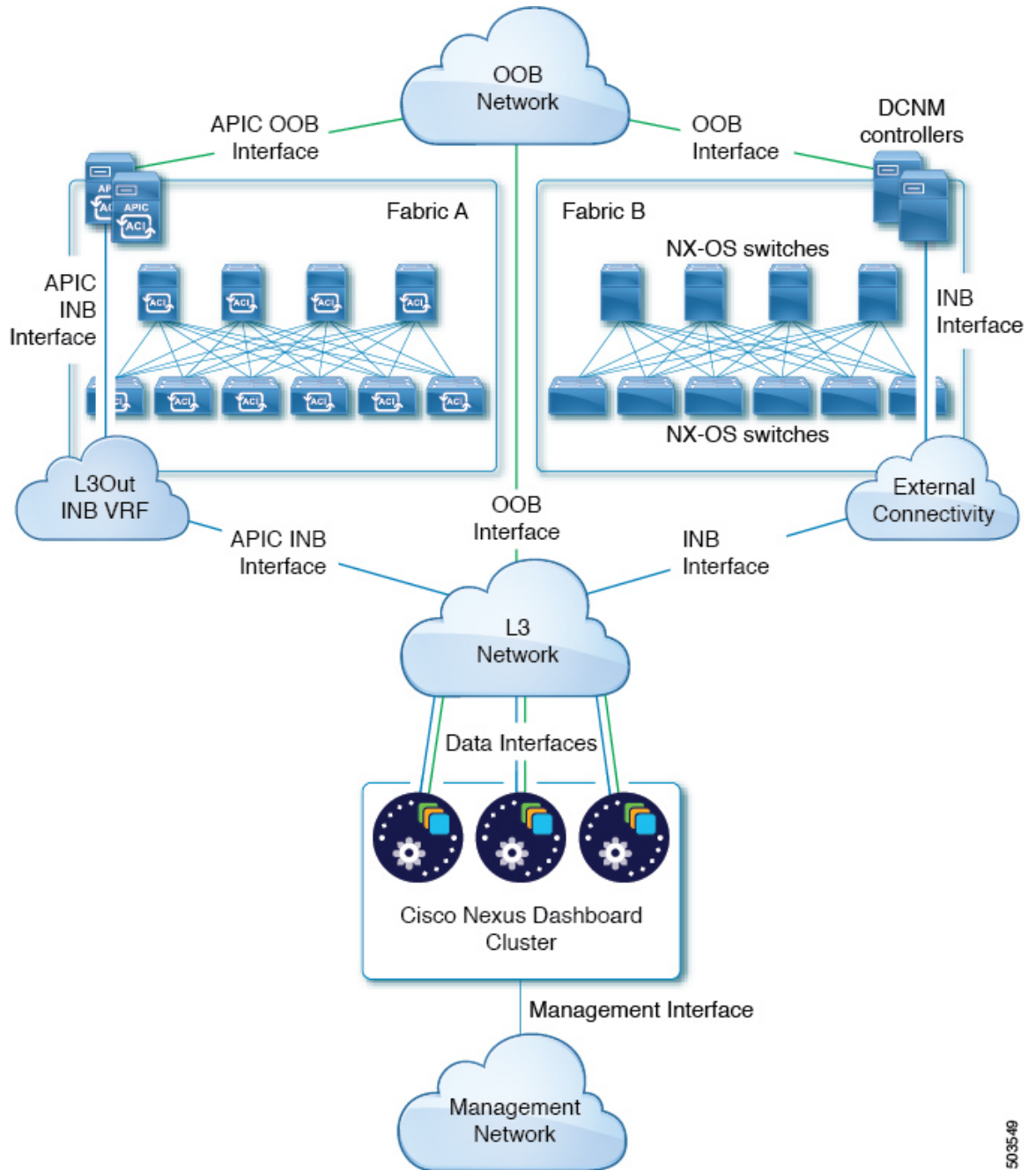
ただし、ほとんどの一般的な導入では、VLAN ID を空のままにして、ホスト ポートをアクセス モードに設定できます。

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



503548

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、ファブリック内の間

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。

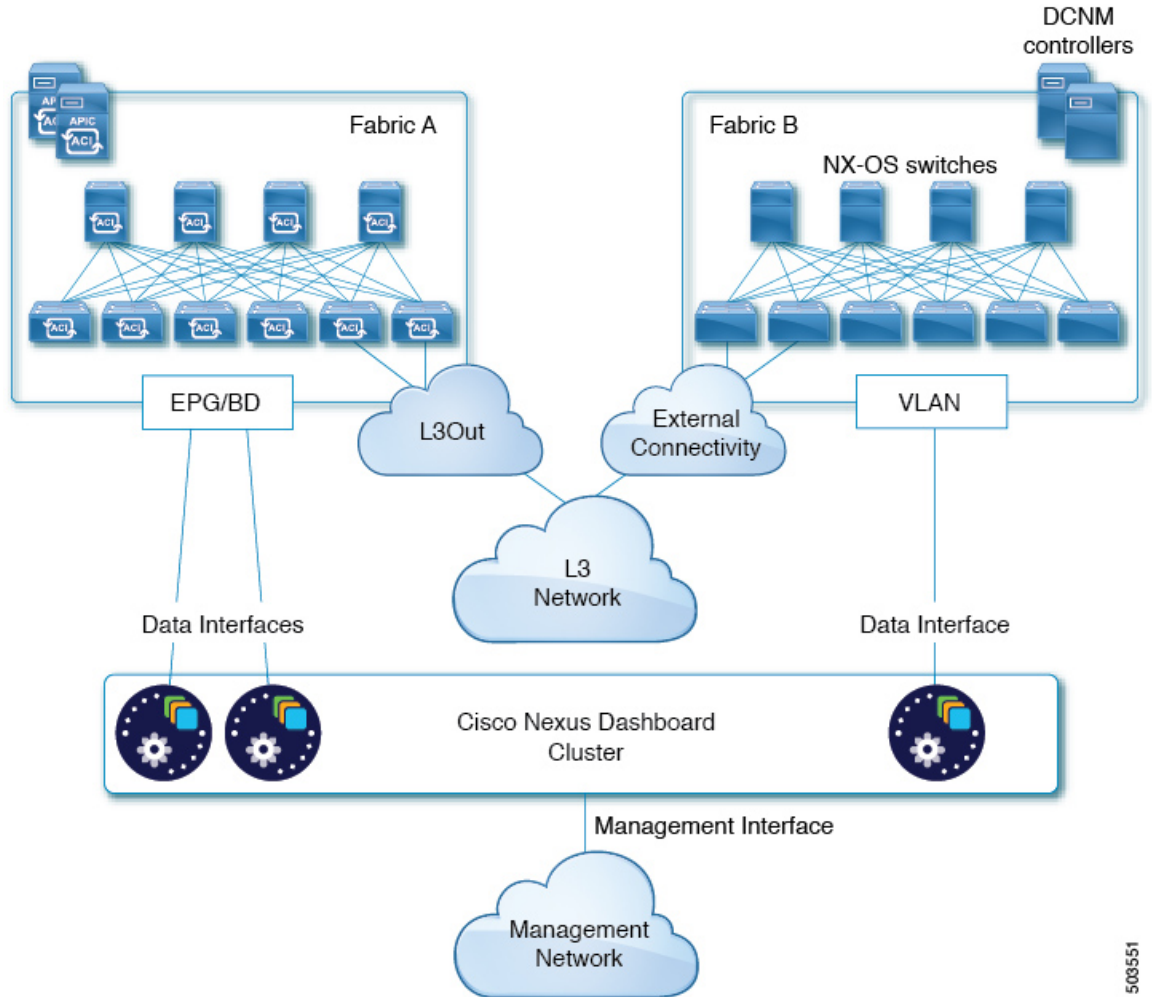
Nexus Dashboard はインバンド VRF のインバンド EPG への接続を必要とするため、管理テナントで EPG を作成すると、ルートリークが不要になります。

- 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ーされている場合、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。

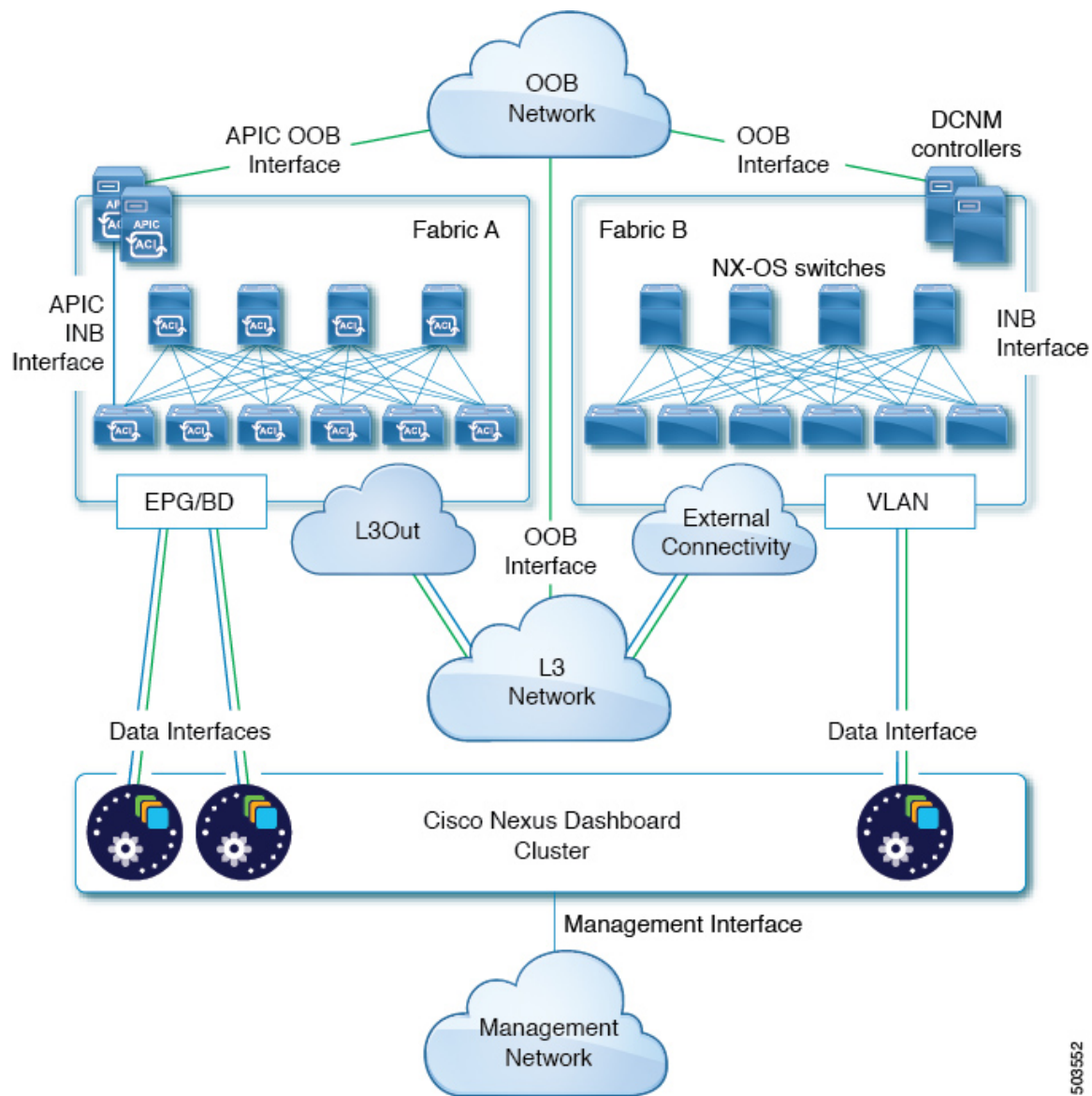
「L3ネットワーク」と「管理ネットワーク」は同じネットワークインフラストラクチャにすることができます。たとえば、Nexusダッシュボードノードの管理とデータネットワークインターフェイスが同じサブネットにある場合です。

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



509551

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



503552

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。

Nexus ダッシュボード インサイトのノード配布

Nexus ダッシュボード 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。

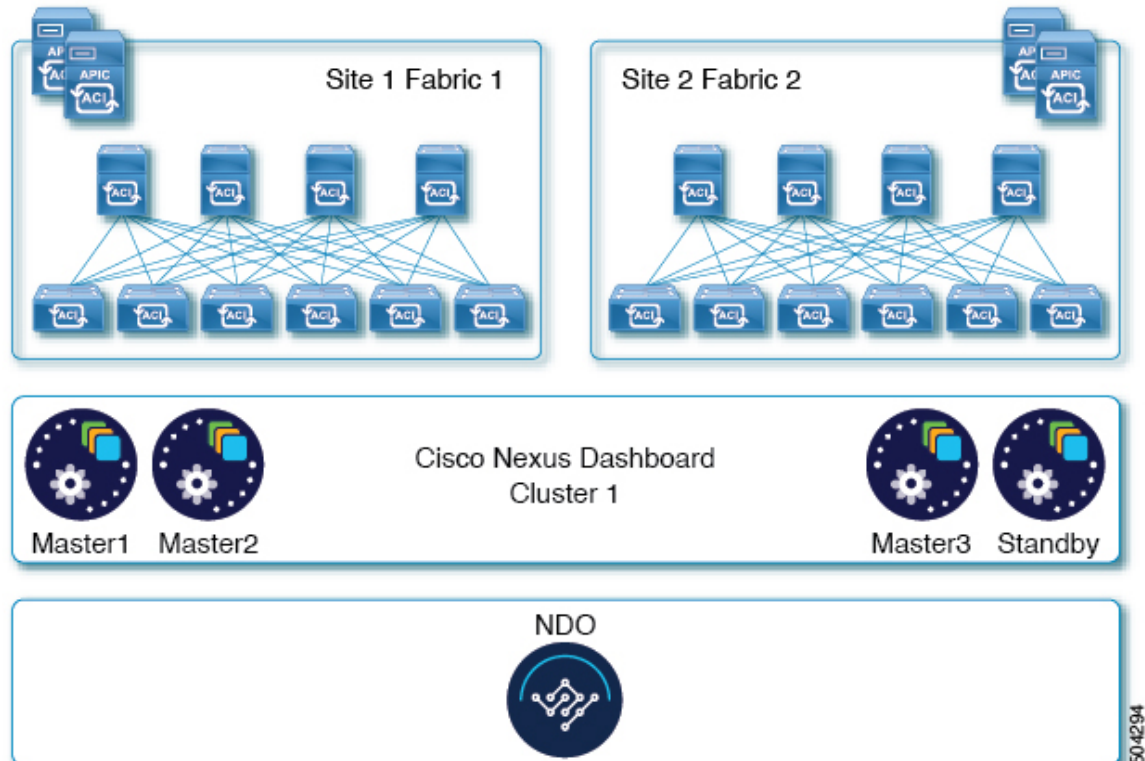
Nexus ダッシュボード オーケストレータ および ファブリック コントローラのノード配布

Nexus Dashboard Orchestrator と Nexus ダッシュボード ファブリック コントローラについては、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。



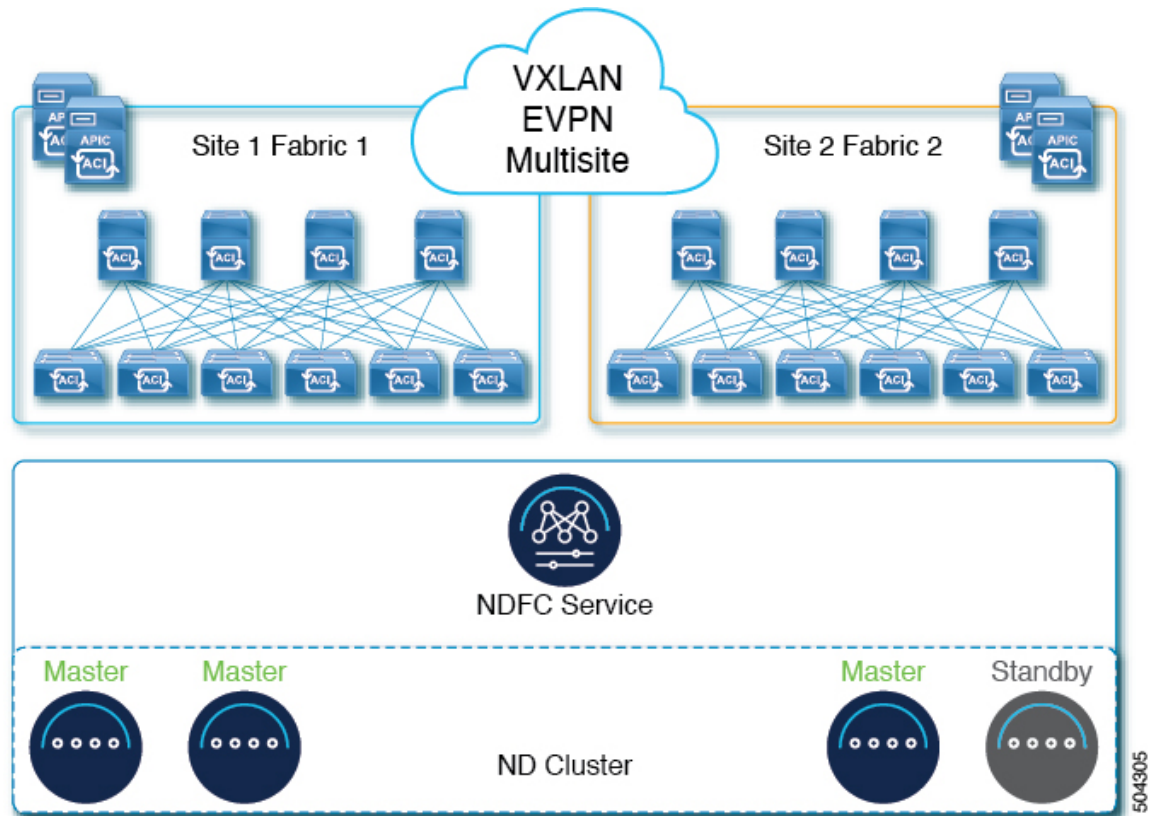
- (注) 次の図は、NDO または NDFC サービスを使用した物理または仮想 Nexus ダッシュボード クラスタの可能な展開シナリオのいくつかの例を示しています。特定のユースケースに必要なノード数の詳細については、[Nexus ダッシュボード キャパシティ プランニング ツール](#)を参照してください。

図 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



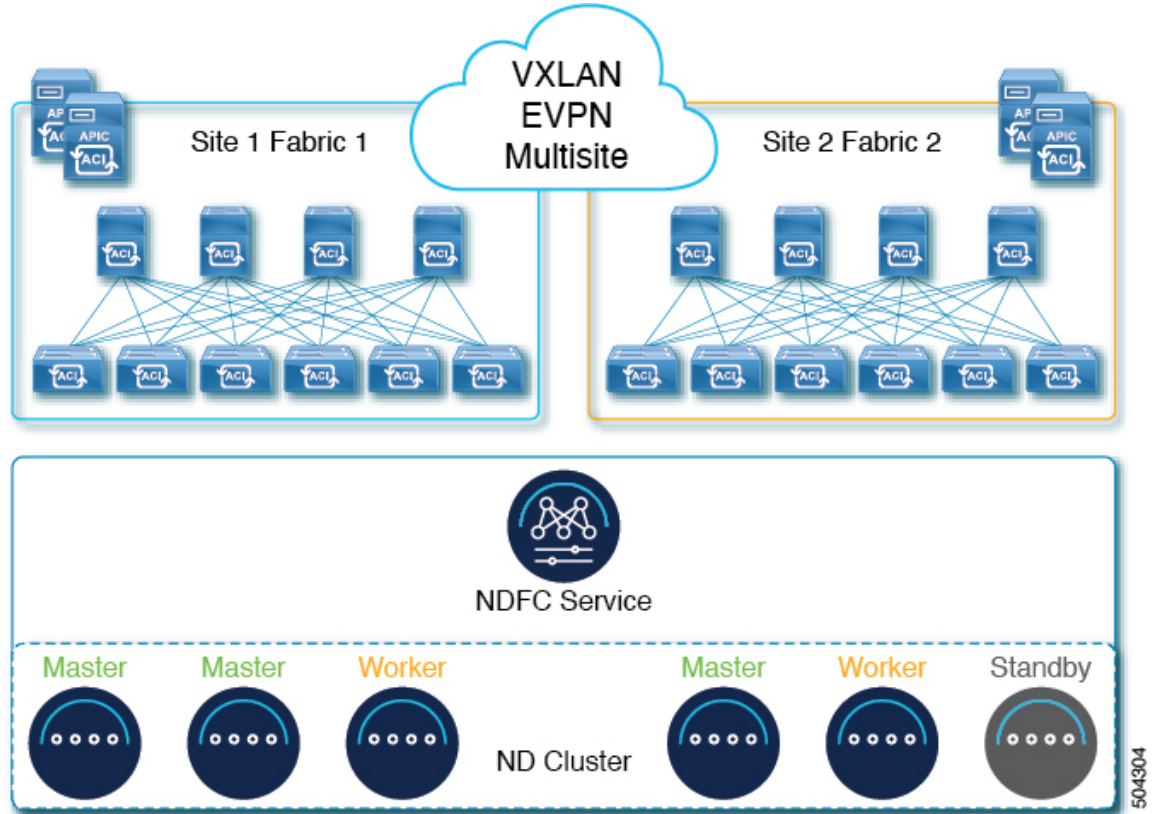
504294

図 7: Nexus Dashboard Fabric Controller の 2つのサイトにまたがるノードの分散 (4ノード)



504305

図 8 : Nexus Dashboard Fabric Controller の 2つのサイトにまたがるノードの分散 (6 ノード)



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 8 : 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。

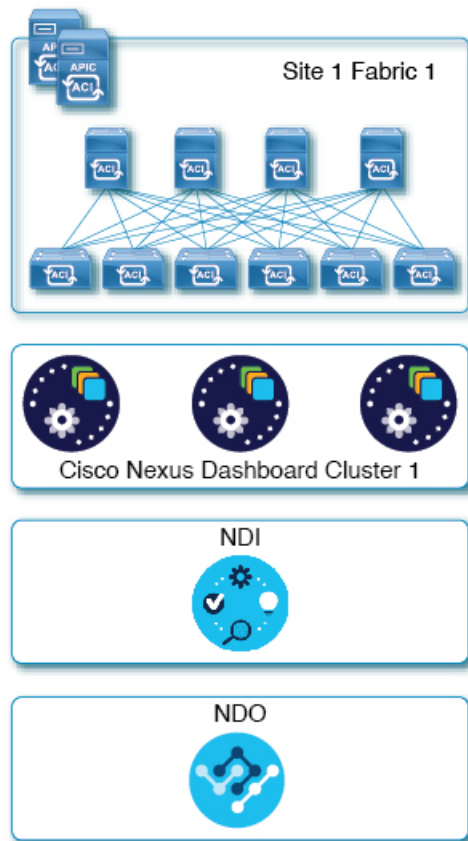


- (注) このリリースは、Linux KVM、AWS または、Azure に展開されている Nexus ダッシュボード クラスタでの共同ホスティングサービスをサポートしていません。以下のすべてのサービス共同ホスティングのシナリオは、物理フォームファクタまたは VMware ESX クラスタフォームファクタに適用されます。

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。

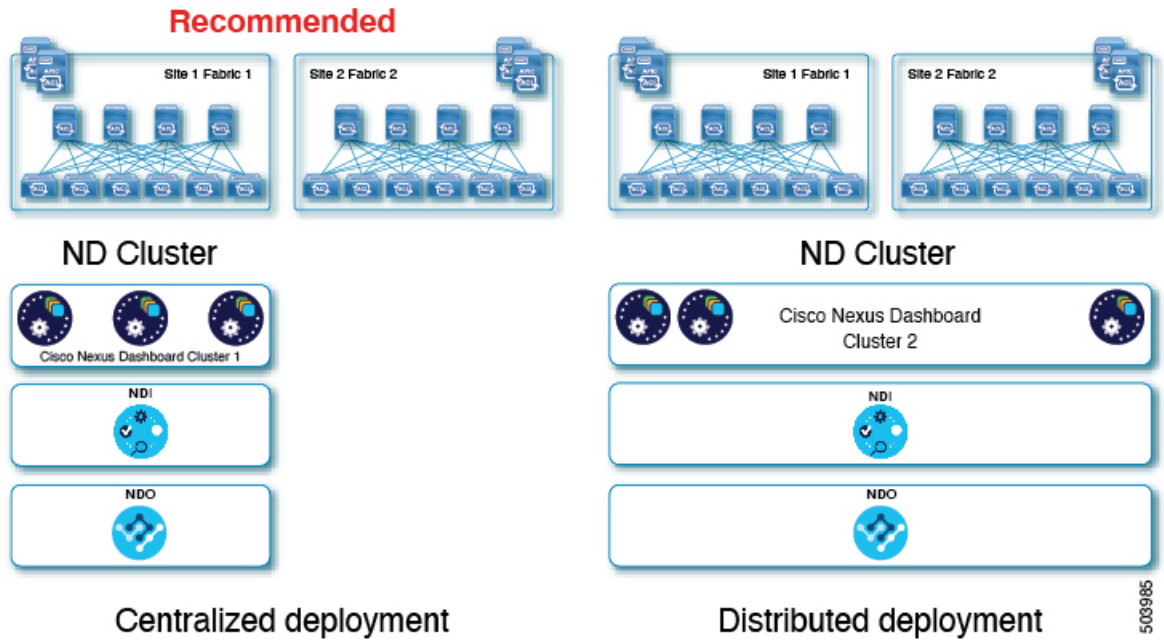
図 9: 単一サイト、Nexus ダッシュボード Insights およびオーケストレータ



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。

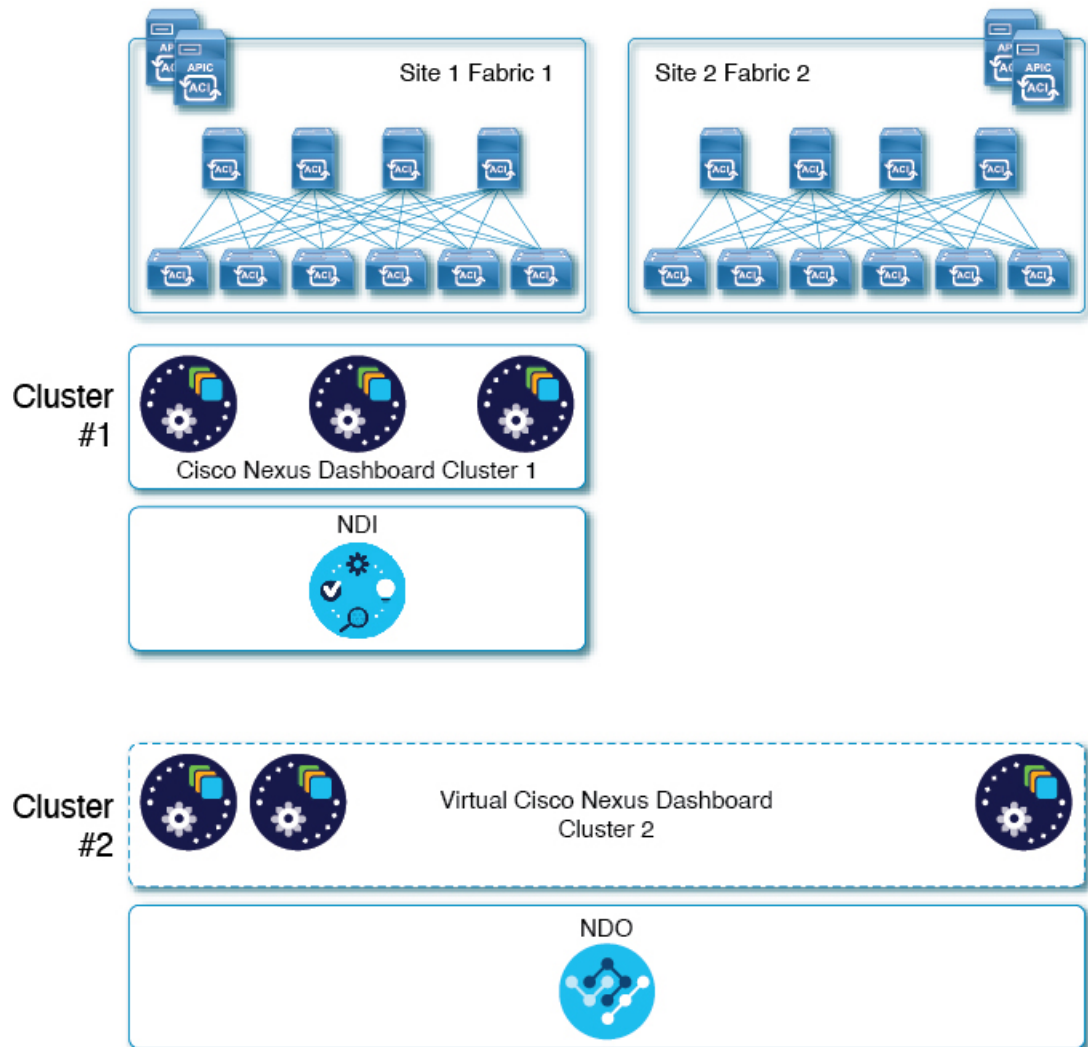
図 10: Nexus ダッシュボード Insights およびオーケストレータの複数サイト、単一クラスタ



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 9: 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	172.17.0.1/16	
サービスネットワーク	100.80.0.0/16	

表 10: 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
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 \(31 ページ\)](#)
- [Cisco Nexus ダッシュボードを物理アプライアンスとして展開 \(33 ページ\)](#)

前提条件とガイドライン

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

- [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 クラスター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）で既存のクラスターを拡張する場合は、『[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。

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。
- 『[Cisco Nexus ダッシュボード ハードウェア 設置ガイド](#)』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、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 11: サポート対象ハードウェア

PID	ハードウェア
SE-NODE-G2	<ul style="list-style-type: none"> • 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。



(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。

- 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。

推奨バージョン: CIMC、リリース 4.2(2a)。

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 2.1.1 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 \(91 ページ\)](#) 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。

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 \(31 ページ\)](#) 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://<first-node-management-ip>` に移動して、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)]** 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。

- 最初のノードの横にある **[編集 (Edit)]** ボタンをクリックします。
- ノードの名前を入力します。
- 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、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。

- 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。

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。

- e) [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ヤルを入力し、[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なら、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 同じクラスタで複数のアプリケーションをホストする予定の場合、App Infra サービス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アプリケーションのみをホストする予定の場合、このステップをスキップします。

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 \(39 ページ\)](#)
- [VMware vCenter を使用している Cisco Nexus ダッシュボードの展開 \(43 ページ\)](#)
- [VMware ESXi での Cisco Nexus ダッシュボードの直接展開 \(52 ページ\)](#)

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。

ただし、アプリ ノードとデータ ノードを混在させてデプロイする必要がある場合、たとえば、Nexus ダッシュボード Insights を展開する予定の場合や、同じクラスターで複数のサービスを共同ホストする予定がある場合は、初期クラスターの 3 つのマスターノードとしてデータ ノードが最初に展開されていることを確認する必要があります。次に、『Cisco Nexus ダッシュボード ユーザ ガイド』の説明に従って、App ノードをワーカーノードとして追加できます。

- **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

十分なシステム リソースをもつことを確認します。

表 12: 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 2.1.x	<ul style="list-style-type: none"> • VMware ESXi 6.5、6.7、または 7.0 • VMware vCenter 6.x (vCenter を使用して展開する場合) • 各 VM には以下が必要です。 <ul style="list-style-type: none"> • 32 vCPU • 128 GB 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 すべてのデータ 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。 • 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。 	<ul style="list-style-type: none"> • VMware ESXi 6.5、6.7、または 7.0 • VMware vCenter 6.x (vCenter を使用して展開する場合) • 各 VM には以下が必要です。 <ul style="list-style-type: none"> • 16 vCPU • 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。

- 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。
- 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 Cisco Nexus ダッシュボードの展開 \(43 ページ\)](#) 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 Cisco Nexus ダッシュボードの直接展開 \(52 ページ\)](#) で説明されている手順に従います。

ESX ホストネットワーク接続

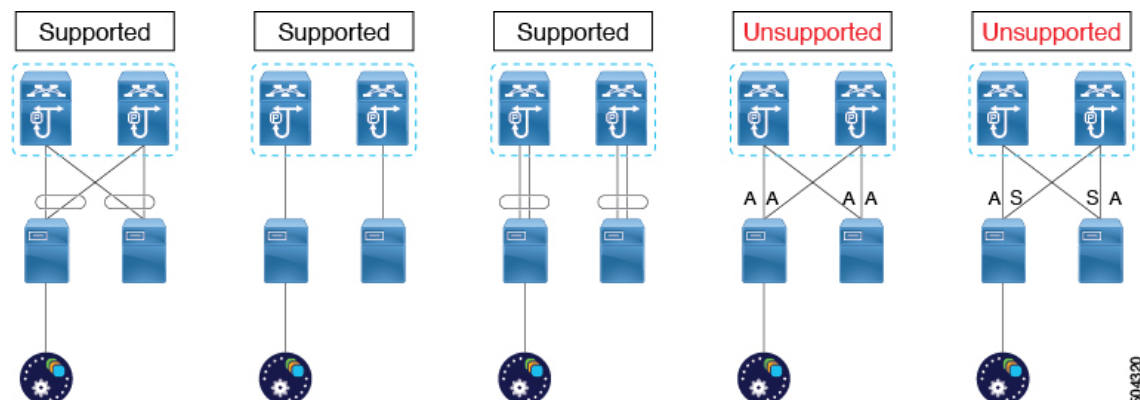
Nexus ダッシュボード Insights またはファブリック コントローラ サービスをインストールし、永続的な IP 機能を使用する予定の場合は、クラスタノードが展開されている ESX ホストに、単一の論理アップリンクが存在することを確実にする必要があります。つまり、単一のリンク、PC、または vPC を介して接続されます。PC/vPC のないデュアルアクティブ/アクティブ (A/A) またはアクティブ/スタンバイ (A/S) リンクではありません。

次の図は、ノードが展開されている ESX ホストのサポートされているネットワーク接続構成とサポートされていないネットワーク接続構成をまとめたものです。

- ESX ホストが直接接続されている場合、次の構成がサポートされます。
 - PC または vPC を使用したポートグループまたは仮想スイッチの A/A アップリンク
 - ポートグループまたは仮想スイッチの単一のアップリンク
 - ポートグループまたは仮想スイッチのアップリンクに使用されるポートチャネル。

PC または vPC を使用しないポートグループまたは仮想スイッチの A/A または A/S アップリンクはサポートされていません

図 12: ESX ホスト接続 (直接)



- ESX ホストが UCS ファブリック インターコネクト（または同等のもの）を介して接続されている場合、次の構成がサポートされます。

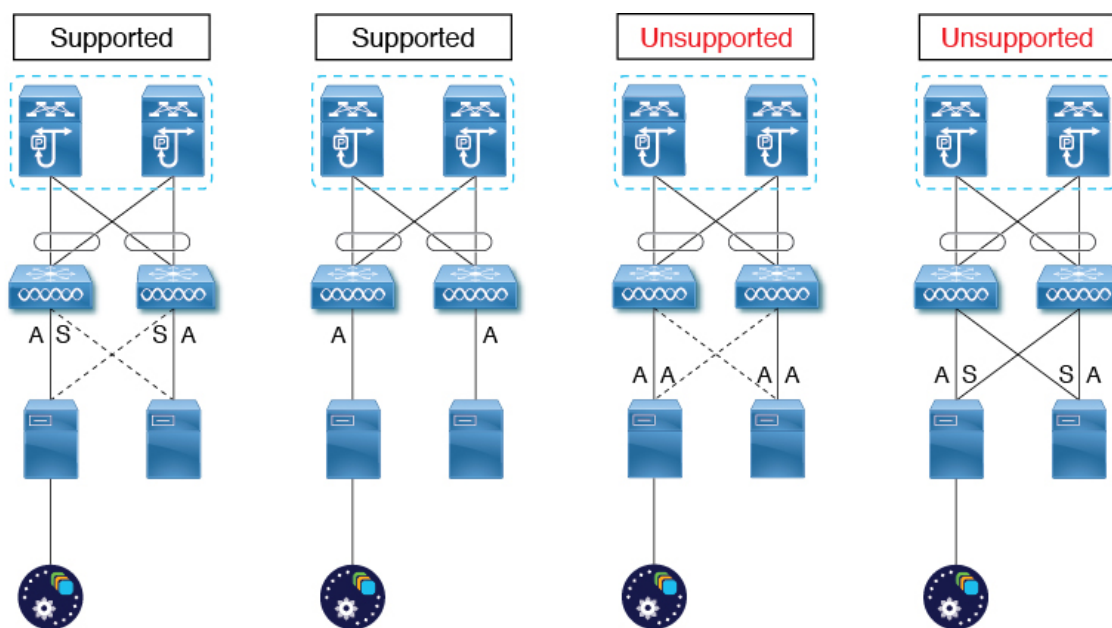
- PC または vPC を使用しない UCS ファブリック インターコネクト レベルでのポートグループまたは仮想スイッチの A/S アップリンク

この場合、アクティブ/スタンバイリンクは、ESXi ハイパーバイザレベルではなく、Cisco UCS のファブリック フェールオーバーなどのサーバー技術に基づいています。

- ポートグループまたは仮想スイッチの単一のアップリンク

PC または vPC を使用しないハイパーバイザレベルでのポートグループまたは仮想スイッチの A/A または A/S アップリンクは、サポートされていません

図 13: UCS 接続（ファブリックインターコネクト使用）



504319

VMware vCenter を使用している 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。ESXi に直接展開する場合は、代わりに [VMware ESXi での Cisco Nexus ダッシュボードの直接展開](#)（52 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](#)（39 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://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) ダウンロードする Nexus Dashboard のバージョンを選択します。

d) 適切な 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>.ova) 。

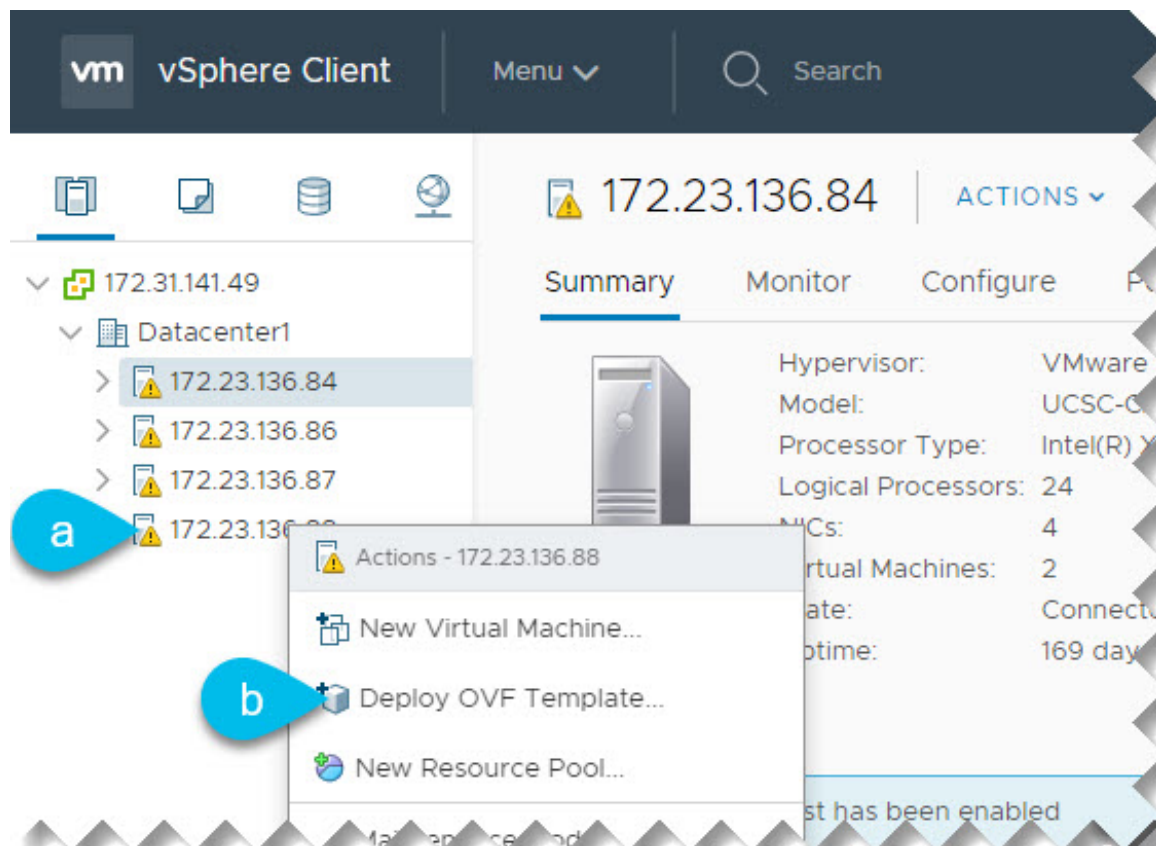
データ ノードの場合、以下をダウンロードします (nd-dk9.<version>-data.ova.)

App ノードの場合、以下をダウンロードします (nd-dk9.<version>-app.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。

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。

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。

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。

Deploy OVF Template

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。

Deploy OVF Template

Name	Capacity	Provisioned	Free	Type	Cluster
datstore1	922.75 GB	426.17 GB	772.35 GB	VMFS 5	

a) [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。

- 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 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。

Deploy OVF Template

1 Select an OVF template
 2 Select a name and folder
 3 Select a compute resource
 4 Review details
 5 Select storage
 6 Select networks
 7 **Customize template**
 8 Ready to complete

Customize template
Customize the deployment properties of this software solution.

Resource Configuration	1 settings
1. Data Disk Size (GB)	Data disk size (min 3TB, max 6TB) 3072
Node Configuration	4 settings
1. Password	Local "rescue-user" password Password: Confirm Password:
2. Management Network Address and subnet	Management network address. Enter IP/subnet 192.168.10.11/24
3. Management Gateway IP	Management network gateway IP address. Enter IP only 192.168.10.1
4. Cluster Leader	Is this node the cluster leader to run bootstrap UI? (Only one node in the cluster must be leader) <input checked="" type="checkbox"/>

CANCEL BACK NEXT

- 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。
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。
- c) 管理ネットワークの IP アドレス、ネットマスク、およびゲートウェイを入力します。

- d) これが展開する最初のノードである場合は、[クラスタ リーダー (Cluster Leader)] チェックボックスをオンにします。

クラスタ内の 1 つのノードのみがリーダーになる必要があります。クラスタ リーダーの管理 IP アドレスを使用して、ブラウザの GUI ウィザードを使用してクラスタの作成を完了します。

- e) [次へ (Next)] をクリックして次に進みます。

ステップ 11 [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 12 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。

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。

- (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 (Cluster Leader)] のチェックボックスをオフのままにする必要がある点異なります。

ステップ 13 3 つすべての VM の展開が完了するまで待ちます。

ステップ 14 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。

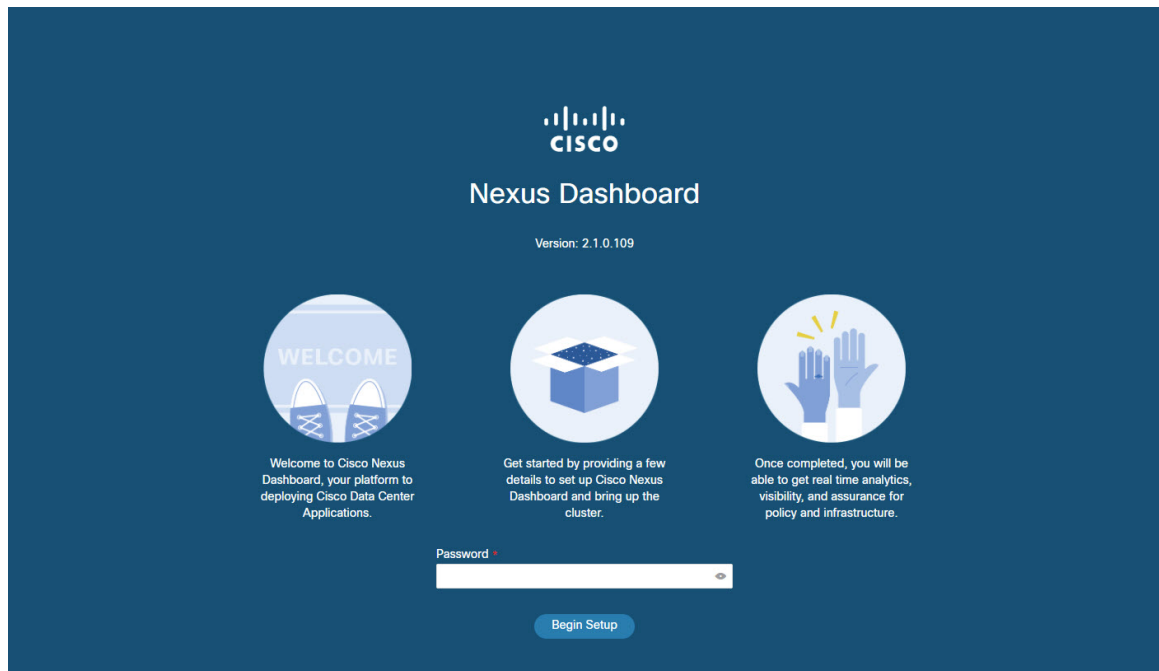
時刻の同期を無効にするには、次の手順を実行します。

- VM を右クリックして、[設定の編集 (Edit Settings)] を選択します。
- [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。
- [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 15 ブラウザを開き、<https://<first-node-management-ip>> に移動して、GUI を開きます。

残りの構成ワークフローは、最初のノード (クラスタ リーダー (Cluster Leader)) 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 16 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 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。

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

- (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。

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。

- [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。

- ノードの **名前** を入力します。
- [資格情報 (Credentials)]** セクションで、ノードの **管理ネットワーク IP アドレス** と **ログイン資格情報** 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、そのノードの情報をプルするために使用されます。

- 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。

管理ネットワーク情報には、前のサブステップで指定したIPアドレスとクレデンシャル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、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。

- 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。

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。

- 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 20 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 21 [次へ (Next)] をクリックして続行します。

ステップ 22 [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 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なら、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** 同じクラスタで複数のアプリケーションをホストする予定の場合、App Infra サービス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アプリケーションのみをホストする予定の場合、このステップをスキップします。

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 から入手できます。

VMware ESXi での Cisco Nexus ダッシュボードの直接展開

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 Cisco Nexus ダッシュボードの直接展開 \(52 ページ\)](#) 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 \(39 ページ\)](#) 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://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) ダウンロードする Nexus Dashboard のバージョンを選択します。
 d) 適切な 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>.ova) 。

データ ノードの場合、以下をダウンロードします (nd-dk9.<version>-data.ova.

App ノードの場合、以下をダウンロードします (nd-dk9.<version>-app.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。

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 3 つすべての 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。

- VM を右クリックして、[設定の編集 (Edit Settings)] を選択します。
- [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。
- [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。

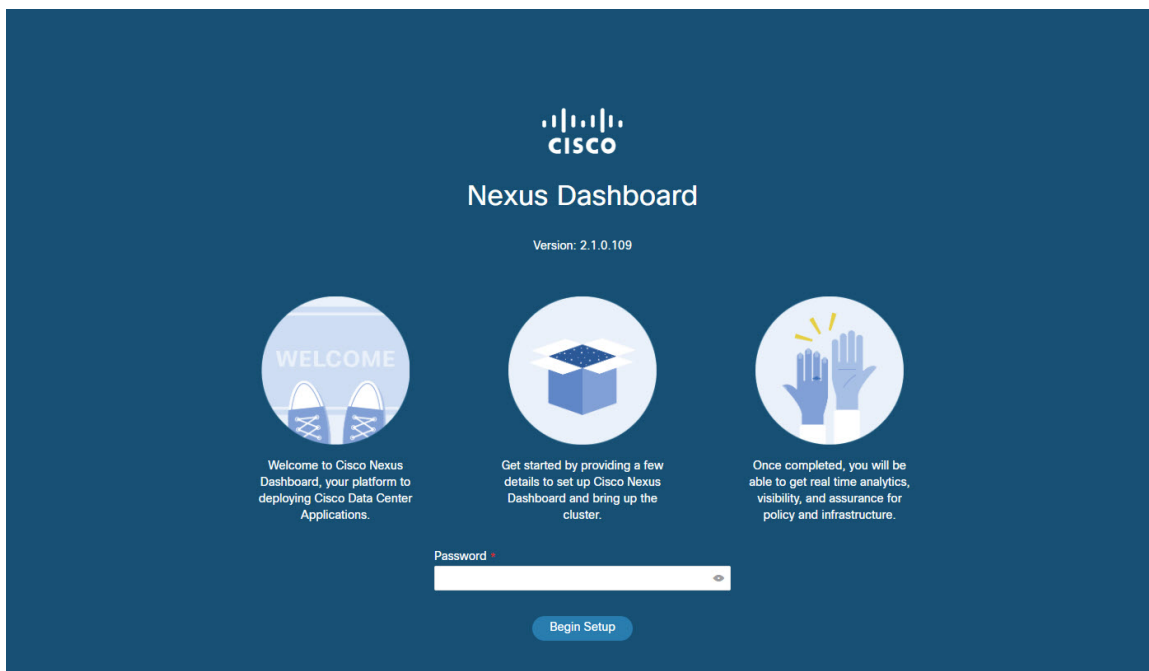
```
Please review the config
Management network:
  Gateway: 192.168.9.1
  IP Address/Mask: 192.168.9.172/24
Cluster leader: no
```

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

ステップ 14 ブラウザを開き、<https://<first-node-management-ip>> に移動して、GUI を開きます。

残りの構成ワークフローは、最初のノード（クラスタ リーダー (Cluster Leader)）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 15 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 16 [**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 17 **[ノードの詳細 (Node Details)]** 画面で、ノードの情報を入力します。

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

- (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。

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。

- [Save]** をクリックして、変更内容を保存します。

ステップ 18 **[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。

- ノードの **名前** を入力します。
- [資格情報 (Credentials)]** セクションで、ノードの **管理ネットワーク IP** アドレスとログイン資格情報を入力し、**[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、そのノードの情報をプルするために使用されます。

- 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。

管理ネットワーク情報には、前のサブステップで指定したIPアドレスとクレデンシャル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、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。

- 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。

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。

- 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 19 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 20 [次へ (Next)] をクリックして続行します。

ステップ 21 [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 22 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なら、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 23** 同じクラスタで複数のアプリケーションをホストする予定の場合、App Infra サービス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アプリケーションのみをホストする予定の場合、このステップをスキップします。

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 から入手できます。



第 5 章

Linux KVMでの展開

- [前提条件とガイドライン \(59 ページ\)](#)
- [Linux KVM での Cisco Nexus ダッシュボードの展開 \(60 ページ\)](#)

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 13: 導入要件

オーケストレーター バージョン	要件
リリース 2.1.1	<ul style="list-style-type: none"> Linux カーネル 3.10.0-957.el7.x86_64 以降、libvirt-4.5.0-23.el7_7.1.x86_64 以降 16 vCPU 48 GB の RAM 800 GB 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。 次のコマンドを使用して、I/O 遅延を確認できます。 <pre># fio --rw=write --ioengine=sync --fdatasync=1 --directory=test-data_with_se --size=22m --bs=2300 --name=mytest</pre>また、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。 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 Cisco 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 \(59 ページ\)](#) 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>

- 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-dk9.2.1.1a.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-dk9.2.1.1a.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-dk9.2.1.1a.qcow2  
/home/nd-node1/nd-node1-disk1.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。

- node1 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。
- node2 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。
- node3 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。

- 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。
- [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。
- [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。
- 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。
- 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。
- 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。

- NIC <mac>** を選択します。
- [デバイス モデル]** で、[e1000] を選択します。
- [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。

- [ハードウェアを追加 (Add Hardware)]** をクリックします。
- [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。
- [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。
- デフォルトの **MAC アドレス** の値のままにします。
- [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) ディスクのバス ドライバについては、[IDE] を選択します。
- d) [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。
- e) [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) 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: no
```

```
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。

2 番目と 3 番目のノードを展開する手順は同じですが、**クラスター リーダー**ではないことを示す必要があります。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（クラスター リーダー）初期設定でネットワークが設定され、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、クラスターの展開を完了します。

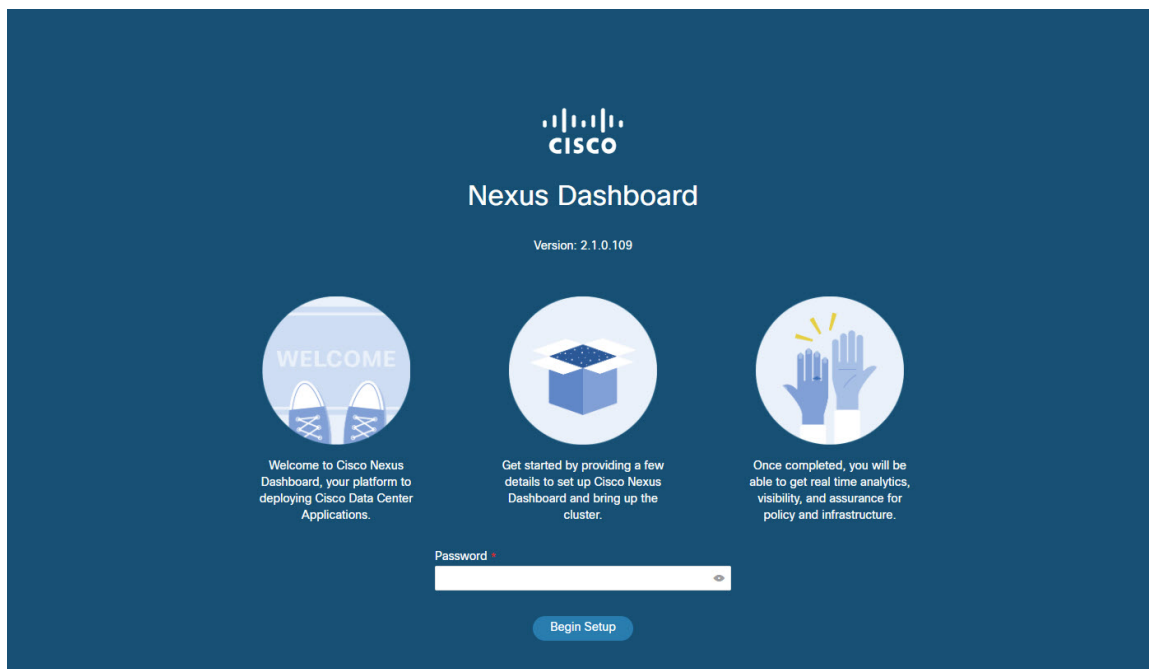
```
Please wait for system to boot: [#####] 100%
System up, please wait for UI to be online.
```

```
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://<first-node-management-ip>` に移動して、GUI を開きます。

残りの構成ワークフローは、最初のノード（クラスター リーダー (Cluster Leader)）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 11 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 12 **[クラスターの詳細 (Cluster Details)]** を入力します。

初期セットアップ ウィザードの **[クラスターの詳細 (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 13 [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。
- 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、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。

- 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。

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。

- e) [Save]をクリックして、変更内容を保存します。

ステップ 14 [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、ノードの管理ネットワーク IP アドレスとログイン資格情報を入力し、[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、そのノードの情報をプルするために使用されます。

- 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。

管理ネットワーク情報には、前のサブステップで指定した IP アドレスとクレデンシャル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、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。

- 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。

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。

- 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 15 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 16 [次へ (Next)] をクリックして続行します。

ステップ 17 [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 18 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なら、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](#) (69 ページ)
- [AWS での Cisco Nexus ダッシュボードの展開](#) (71 ページ)

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する必要があります。

- 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~/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 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 \(69 ページ\)](#) 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。
- 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。

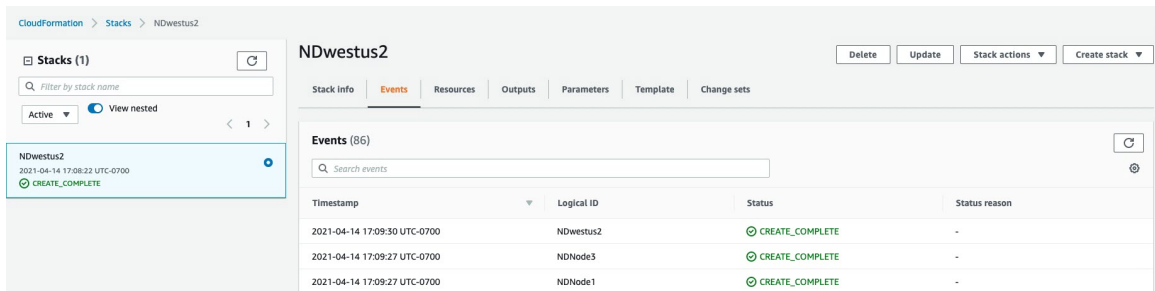
ステップ 6 **[詳細オプション (Advanced options)]** 画面で、**[次へ (Next)]** をクリックします。

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。

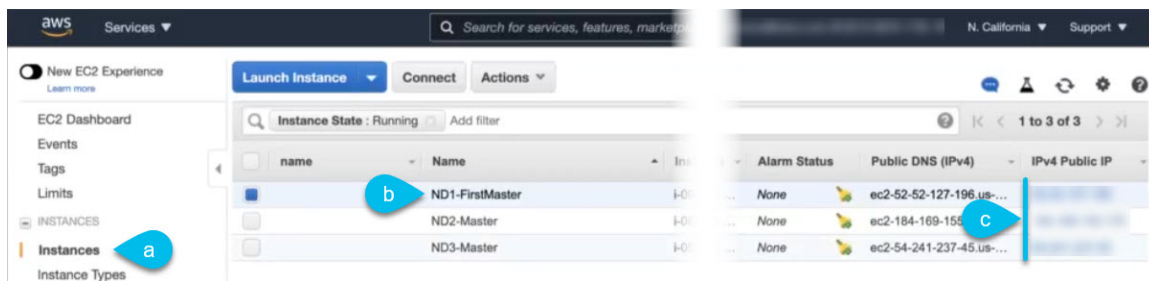
[CloudFormation] ページでインスタンスの展開のステータス (CREATE_IN_PROGRESS など) を表示できません。ページの右上隅にある更新ボタンをクリックすると、ステータスを更新できます。

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。



Timestamp	Logical ID	Status	Status reason
2021-04-14 17:09:30 UTC-0700	NDwestus2	CREATE_COMPLETE	-
2021-04-14 17:09:27 UTC-0700	NDNode3	CREATE_COMPLETE	-
2021-04-14 17:09:27 UTC-0700	NDNode1	CREATE_COMPLETE	-

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 \(69 ページ\)](#) 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
```

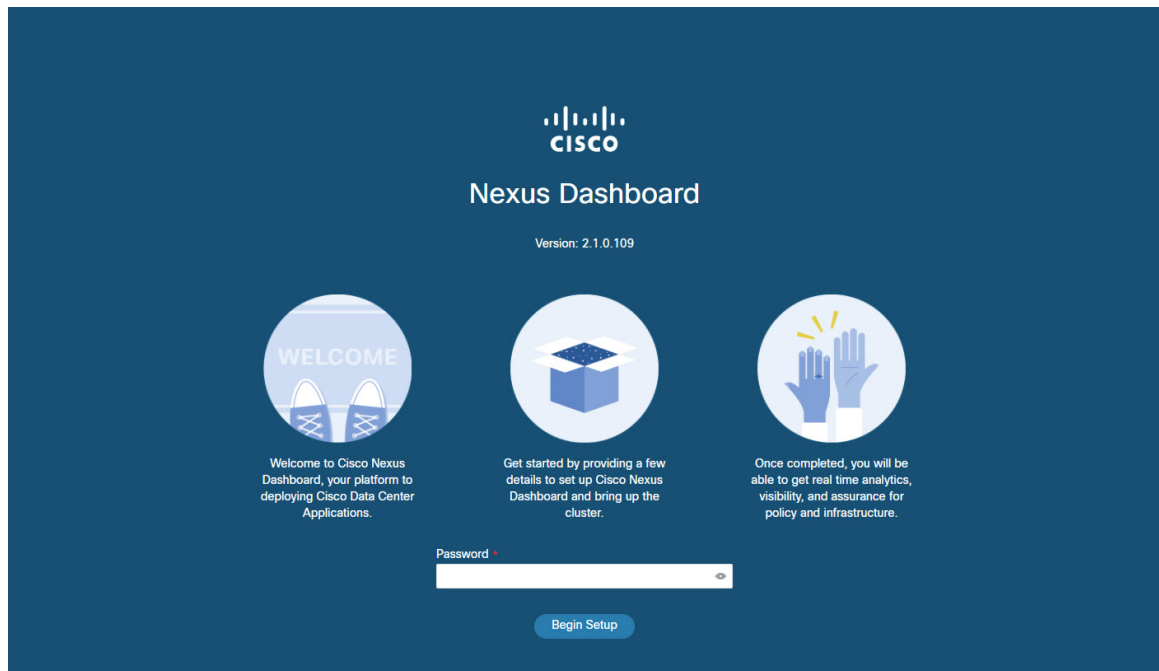
- c) 他の 2 つのインスタンスについて、この手順を繰り返します。

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。

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

- 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。

- [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。

- ノードの**名前**を入力します。
- [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。

- [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なら、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 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なら、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 7 章

Microsoft Azure での展開

- [前提条件とガイドライン](#) (79 ページ)
- [Azure での Cisco Nexus ダッシュボードの展開](#) (84 ページ)

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 \(80 ページ\)](#) および [Windows での SSH キー ペアの生成 \(81 ページ\)](#) 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 \(81 ページ\)](#)

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:gTsQIIAadjgNsgcguifIloh4XGpVWMdcXV6U0dyBNs
...
```

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

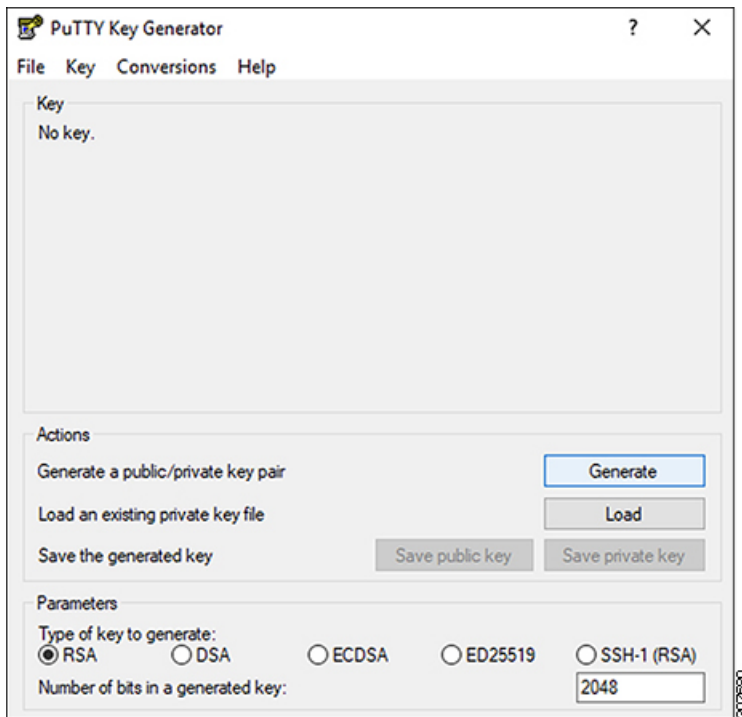
次の手順では、WindowsでSSH公開キーと秘密キーのペアを生成する方法について説明します。LinuxでSSH公開キーと秘密キーのペアを生成する手順については、[を参照してください](#)。Linux または MacOS での SSH キー ペアの生成 (80 ページ)

ステップ 1 PuTTYキージェネレーター (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 キージェネレーターを実行します。

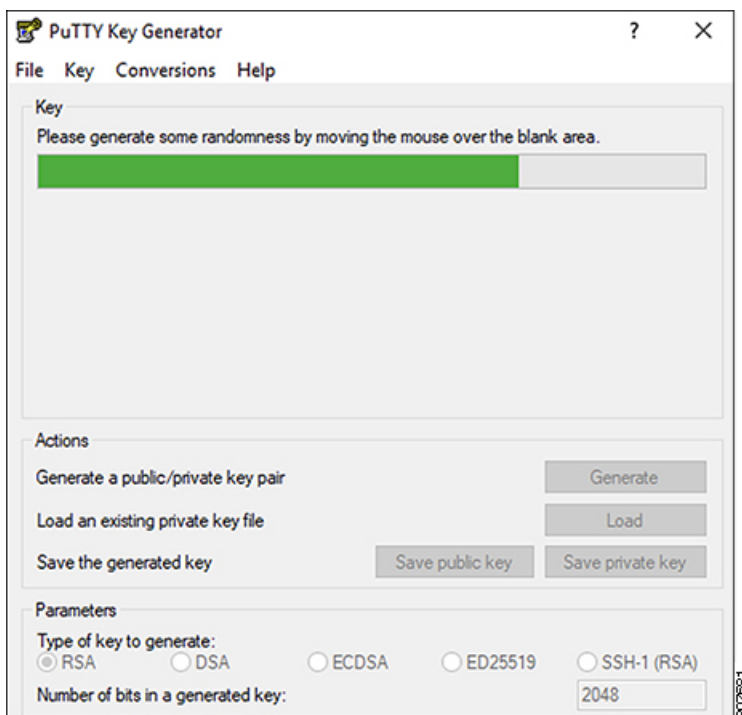
画面にPuTTYキージェネレーターのウィンドウが表示されます。



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。

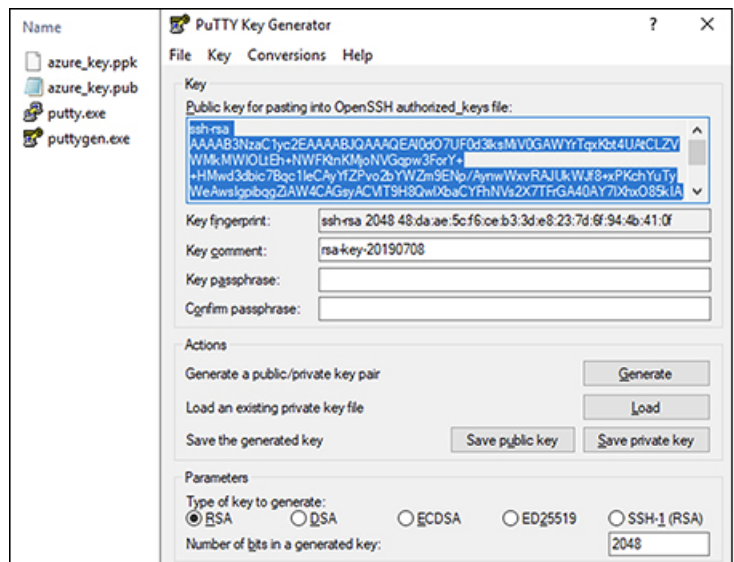
- 公開キーの先頭にssh-rsaテキストを含める。
- 末尾の次のテキスト文字列を除外します。

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

== rsa-key-を含め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 (83 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 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 \(79 ページ\)](#) 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。

- Azure アカウントにログインし、<https://azuremarketplace.microsoft.com> に移動します
- 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。
- [今すぐ取得 (Get it now)]** をクリックします。
- [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。

- [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。
- [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 \(79 ページ\)](#) の一部として選択します。
- [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。
- [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。
- [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 \(79 ページ\)](#) 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。
- [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 \(79 ページ\)](#) 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
```

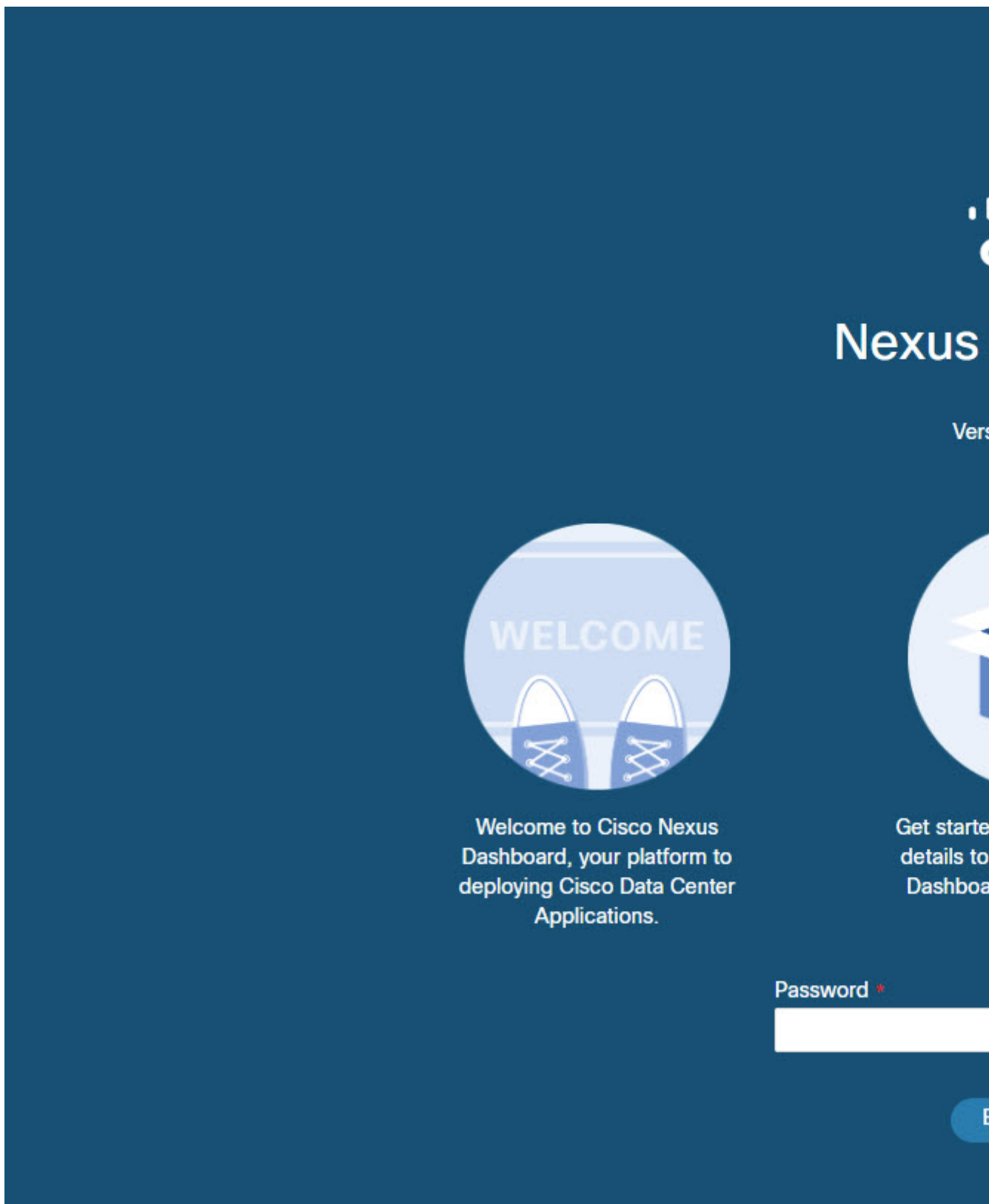
c) 他の 2 つのノードについて、この手順を繰り返します。

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標準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れば、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 8 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 \(91 ページ\)](#)
- [Nexus ダッシュボードのアップグレード \(92 ページ\)](#)

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。クラスタを展開した際に物理サーバー、VMware ESX OVA、Azure、あるいはAWSクラウドを使用したかどうかに関係なく、対象リリースのISOイメージを使用してアップグレードします。

- 既存のクラスタで実行するサービスのリリースノートを確認し、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。
- Cisco Nexus ダッシュボード リリース 2.0.1d 以降を実行する必要があります。

Cisco Application Services Engine を実行している場合は、リリース 2.1.1 にアップグレードする前に、『[Cisco Nexus ダッシュボード展開ガイド、リリース 2.0.x](#)』の説明に従って Nexus ダッシュボードにアップグレードする必要があります。アプリケーションサービスエンジンクラスタを Nexus ダッシュボード リリース 2.0.2h にアップグレードしてから、リリース 2.1.x にアップグレードすることをお勧めします。

- 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状態を確認するか、`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。

- 既存の設定のバックアップを作成します。

- Nexus Insights サービスを実行している場合は、アップグレードの前に無効にし、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。

サービスを無効にした後、アップグレードを続行する前に、クラスタが安定して正常であることを確認してください。

サービスを再度有効化する前に、『Cisco Nexus ダッシュボード ユーザ ガイド』の「アプリ インフラ サービス」セクションで説明されているように、アプリ インフラ サービス 展開プロファイルがお使いの展開に適切に設定されてい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。
- リリース 2.1.1 以前からアップグレードする場合は、新しいイベント モニタリング ページを UI に正しく表示するために、ブラウザのキャッシュをクリアする必要がある場合があります。
- このリリースにアップグレードした後に、すべてのアプリケーションを最新のバージョンにアップグレードすることを推奨します。

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](#)」を参照してください。

- リリース 2.1.x 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 \(91 ページ\)](#)

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>

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

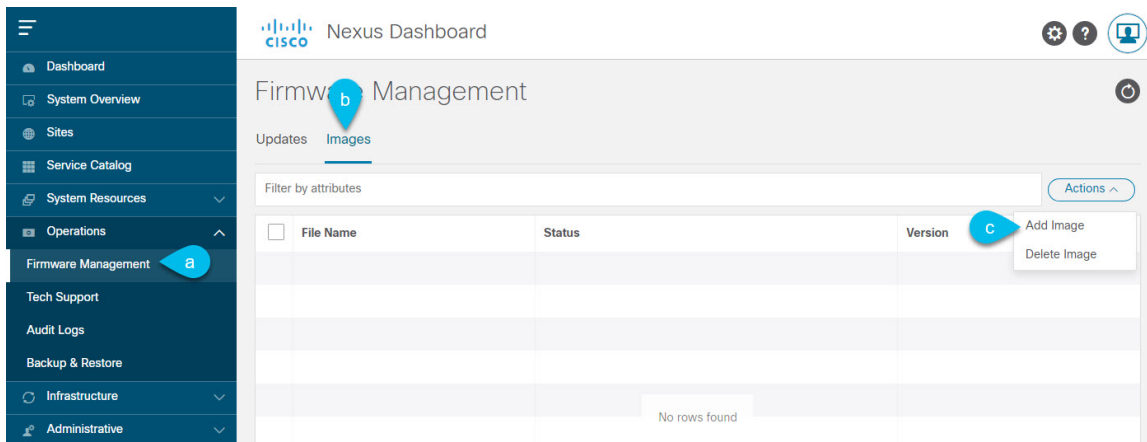
(注) 最初のクラスタ展開に VMware ESX .ova イメージまたはクラウドプロバイダーのマーケットプレイスを使用した場合でも、すべてのアップグレードで .iso イメージをダウンロードする必要があります。

- d) (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 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。



- [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。
- [イメージ] タブを選択します。
- [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。

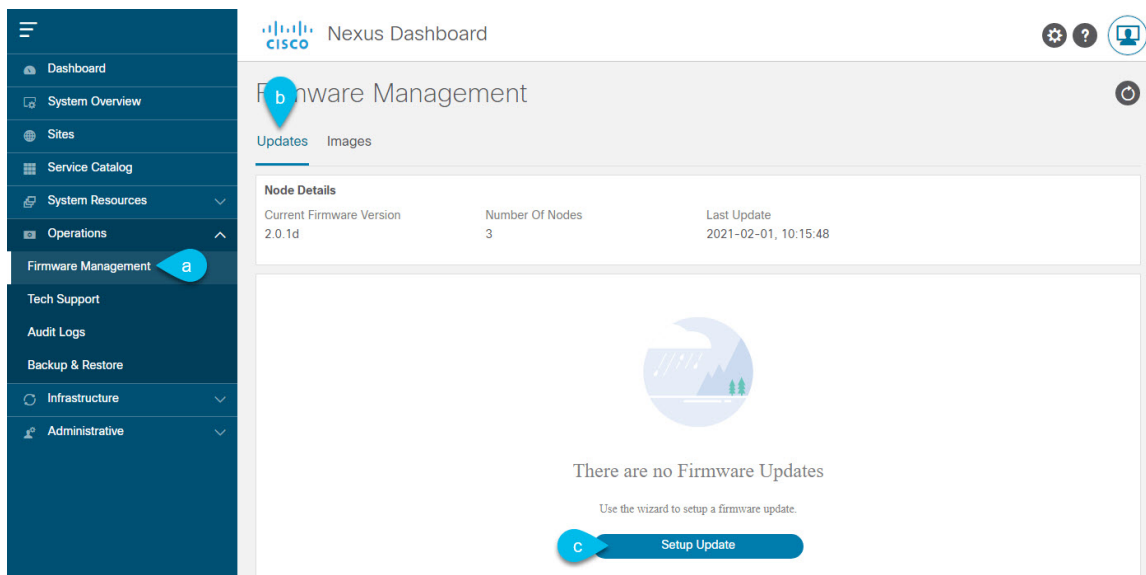
ステップ 4 新しいイメージを選択します。

- [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。
- [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。
- [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ます、[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。



- [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。
- [更新] タブを選択します。
- [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。

- [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。
- [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。

- [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。
- [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。
- [Activate] をクリックします。
- [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 VMware ESX に展開された仮想クラスタをアップグレードした場合は、ノードを新しいプロファイルに変換します。

(注) 物理クラスタをアップグレードした場合は、この手順をスキップしてください。

リリース 2.1(1)以降、Nexus ダッシュボードは、VMware ESX に展開された仮想ノードに対して2つの異なるノードプロファイルをサポートします。アップグレード後、既存のクラスタのすべてのノードを新しいプロファイルの1つに変換する必要があります。

- **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 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

選択するプロファイルは、使用例のシナリオによって異なります。

- Nexus ダッシュボード オーケストレータ サービスのみを実行する予定の場合は、すべてのノードをアプリ ノードプロファイルに変換します。
- Nexus ダッシュボード Insights または共同ホストアプリケーションを実行する予定の場合は、ノードをデータ プロファイルに変換する必要があります。

ノードを新しいプロファイルに変換するには、そのプロファイルを使用して新しいノードを展開し、既存のノードを一度に1つずつ置き換えます。

- a) ノードの1つを停止します。
一度に1つのノードを置き換える必要があります。
- b) アプリまたはデータ プロファイル OVA を使用して、VMware ESX に新しいノードを展開します。
新しいノードを展開するときは、置き換えるノードとまったく同じネットワーク設定パラメータを使用する必要があります。また、OVF パラメータの **[クラスタ リーダー (Cluster Leader)]** チェックボックスがオフのままになっていることも確認する必要があります。
- c) 既存の Nexus ダッシュボード GUI にログインします。
残りの正常なマスター ノードのいずれかの管理IPアドレスを使用できます。
- d) 左側のナビゲーションペインから、**[システム リソース (System Resources)] > [ノード (Nodes)]** を選択します。
交換するノードが **[非アクティブ (Inactive)]** としてリスト化されます。
- e) 置換する非アクティブ マスター ノードの隣にある **(...)** メニューをクリックして、**[置換 (Replace)]** を選択します。
[置換 (Replace)] ウィンドウが開きます。
- f) ノードの **管理 IP アドレス** と **パスワード** を入力し、**[確認 (Verify)]** をクリックします。
クラスタは新しいノードの管理 IP アドレスに接続し、接続性を確認します。
- g) **[置換 (Replace)]** をクリックします。

ノードが設定されてクラスタに参加するまでに、最大で20分かかる場合があります。

h) クラスタが正常になるのを待ってから、他の2つのノードに対してこの手順を繰り返します。

ステップ 10 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 から入手できます。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。