Cisco Nexus Dashboard プラットフォームの概要、リリース 3.1.x

目次

プラットフォーム概要

サポートされるサービス

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

Nexus Dashboard クラスタは通常、1つまたは3つのプライマリ ノードで構成されます。また、3 ノード クラスタの場合、プライマリ ノードで障害が発生した際に簡単にクラスタを回復させられるよう、いくつかの ワーカー ノードをプロビジョニングして、水平スケーリングや スタンバイ ノードを有効化できます。このリリースでサポートされるワーカー ノードとスタンバイ ノードの最大数については、Cisco Nexus Dashboard 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。*追加のノードを使用してクラスタを拡張する方法の詳細については、 インフラストラクチャの管理 を参照してください。

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 worker」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。

Nexus Dashboard ソフトウェアへの root アクセスは、Cisco TAC のみに制限されています。一連の操作とトラブルシューティング コマンドを有効にするために、すべての Nexus Dashboard 展開のために
特別なユーザー rescue-user が作成されます。 使用可能な rescue-user コマンドの詳細については
『Nexus Dashboard User Guide』の「Troubleshooting」の章を参照してください。

このガイドでは、Nexus Dashboard の使用方法について説明します。ハードウェアのインストールについては、 *Nexus Dashboard Hardware Setup Guide* を参照してください。展開プランと Nexus Dashboard ソフトウェアのインストールについては、*Nexus Dashboard Deployment Guide* を参照してください。

サービス

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 などのサービスを展開するには、 Nexus Dashboard 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、これらのサービスのイメージを手動でダウンロードしてプラットフォームにアップロードし、インストール操作を実行してから使用する必要があります。

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

利用可能なフォームファクタ

Cisco Nexus Dashboardのこのリリースは、さまざまなフォームファクタを使用して展開できます。ただし、すべてのノードに同じフォームファクタを使用する必要があります。同じクラスタ内で異なるフォームファクタを混在させることはサポートされていません。物理フォームファクタは現在、クラスタノード用に 2 つの異なる UCS サーバー（UCS-C220-M5 および UCS-C225-M6）をサポートしており、同じクラスタ内で混在させることができます。

> すべてのサービスがすべてのフォーム ファクタでサポートされているわけではありません。展開を計画するときは、Nexus Dashboard クラスタ サイジング ツールでフォーム ファクタとクラスタのサイズ要件を確認してください。

- Cisco Nexus Dashboardの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 Dashboard 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)

  次の2つのリソースプロファイルのいずれかを備えたVMware ESX仮想マシンを使用してNexus Dashboardクラスタを展開できる仮想フォームファクタ。

  - データ ノード：Nexus Dashboard 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 Dashboard 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

- Linux KVM (.qcow2)

  Linux KVM仮想マシンを使用して、Nexus Dashboardクラスタを展開できる仮想フォームファクタ。

- Amazon Web Services (.ami)

  AWSインスタンスを使用して、Nexus Dashboard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)

  Azureインスタンスを使用して、Nexus Dashboardクラスタを展開できるクラウドフォームファクタ。

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

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

クラスタ サイジングの注意事項

前述のように、Nexus Dashboard クラスタは、最初に 1 つまたは 3 つのプライマリ ノードを使用して展開されます。実行するサービスの種類と数によっては、初期展開後にクラスタに追加の 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、指定のユースケースに基づく推奨ノード数については、*Nexus Dashboard キャパシティ プラン* ツールを参照してください。

ヒ

単一ノード クラスタは、限られた数のサービスでサポートされており、最初の展開後に 3 ノード クラスタに拡張することはできません。
3ノードクラスタのみが追加のワーカーノードをサポートします。
単一ノードクラスタを展開していて、3ノードクラスタに拡張するか、ワーカーノードを追加する場合は、基本の3ノードクラスタとして再展開する必要があります。
3 ノード クラスタの場合、クラスタが動作し続けるには、少なくとも 2 つのプライマリ ノードが必要です。2 つのマスター ノードに障害が発生すると、クラスタはオフラインになり、このガイドで説明されているように回復するまで使用できません。

クラスタへのワーカーノードの追加については、「ワーカーノードの管理」を参照して

ください。クラスタへのスタンバイ ノードの追加方法については、「スタンバイノード

の管理」を参照してください。

サポートされるアプリケーションの完全なリストおよび関連する互換性情報については、「*データ センター ネットワーク サービス互換性マトリックス*」を参照してください。

要件と注意事項

次のセクションでは、クラスタの設定とブートストラップ中にすでに完了しているいくつかの展開要件と、クラスタの使用時およびサービスの展開時に必要になる可能性のある参照情報について説明します。

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

Nexus Dashboard 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。

Nexus Dashboard は、DNS クライアントとリゾルバーの両方として機能します。内部サービス向けには、DNS リゾルバーとして機能する内部の Core DNS サーバーを使用します。また、DNS

クライアントとしても動作して、イントラネット内またはインターネットの外部ホストに到達できるようにするためには、

外部 DNS サーバーを構成する必要があります。

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

リリース 3.0(1) 以降、Nexus Dashboard は対称キーを使用した NTP 認証もサポートしています。各キーを複数の NTP サーバーに割り当てることができる NTP キーを設定できます。NTP 認証の有効化と構成については、後のセクションで展開手順の一部として説明します。

BGP 構成と永続的な IP

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

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

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

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

- ピアルータが、ノードのレイヤ 3 ネットワーク間でアドバタイズされた永続的 IP を交換することを確

認します。

- 後続のセクションで説明するように、クラスタの展開時に BGP を有効にするか、[永続 IP アドレス] で説明するように、Nexus ダッシュボード GUI で後で有効にするかを選択します。
  [永続 IP アドレス] で説明するように、Nexus ダッシュボード GUI で後で有効にするかを選択します。
- 割り当てる永続的な IP アドレスが、ノードの管理サブネットまたはデータサブネットと重複しないようにしてください。

Nexus ダッシュボード外部ネットワーク

Cisco Nexus Dashboard 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 Dashboard を設定するときは、2 つの Nexus Dashboard 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 Dashboard 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。

データネットワーク	管理ネットワーク
• Nexus Dashboardノードのクラスタリング • アプリケーション間の通信 • Nexus DashboardノードからCisco APICノードへの通信 たとえば、Nexus Dashboard Insightsサービスなどのネットワークトラフィックです。	• Nexus Dashboard GUIへのアクセス • SSHを使用したNexus Dashboard 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) 「サービス 管理」の説明に従ってNexus Dashboard アプリ ストアからアプリケーションをインストールするには、管理ネットワーク経由でページ（https://dcappcenter.cisco.com）にアクセスできる必要があります。 • Intersight デバイス コネクタ

2つのネットワークには次の要件があります。

- すべての新しい Nexus Dashboard 展開では、管理ネットワークとデータネットワークが異なるサブネットに存在する必要があります。
- 物理クラスタの場合、管理ネットワークは各ノードの CIMC 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 Dashboard Insights サービスの場合、データネットワークは、各ファブリックおよび APIC のインバンドネットワークに IP 到達可能性を提供する必要があります。
- Nexus Dashboard InsightsとAppDynamicsの統合では、データネットワークがAppDynamicsコント

ローラにIP到達可能性を提供する必要があります。

- Nexus Dashboard Orchestrator サービスの場合、データ ネットワークは、Cisco APIC サイトに対してインバンドおよび/またはアウトオブバンド IP 到達可能性を持ちますが、Cisco NDFC サイトに対してはインバンド到達可能性が必要です。
- データ ネットワーク インターフェイスで、Nexus Dashboard トラフィックに使用できる最小 MTU が 1500 である必要があります。

  必要に応じて、高いMTUを設定できます。

- Nexus Dashboard は 、サーバーから情報をモニターまたは収集するためのSNMPポーリングをサポートしていません。
- 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。

データ サブネットを変更するにはクラスタを再展開する必要があるため、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。

ノードとサービスに必要な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
にリストされた要件に加えて、展開する予定の特定のサービスに対する
リリース ノートを必ず参考にしてください。

レイヤ2およびレイヤ3接続の永続IPアドレスの割り当ては、『Cisco Nexus Dashboardユーザーガイド』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、そ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。

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

SFLOW/NetFlow（ACI または NDFCファブリック）を使用した Nexus Dashboard Insights	レイヤ 3 隣接	レイヤ 2 隣接	データ インターフェイス ネットワーク内の 6 つの IP
Nexus Dashboard サービス	管理インターフェイス	データ インターフェイス	永続的 **IP** の総数
Nexus Dashboard ファブリック コントローラ、リリース 12.1(3) 以降	レイヤ 2 または レイヤ 3 隣接	レイヤ 2 または レイヤ 3 隣接	LAN 展開タイプで **[LAN** デバイス管理の接続性（LAN Device Management Connectivity）**]** が **[**管理（**Management**）**]**（デフォルト）に設定されたレイヤー 2 モードで動作している場合 ・SNMP/Syslog および SCP サービス用の管理ネットワーク内の 2 つの IP ・**[EPL]** が有効になっている場合、各ファブリックのデータ ネットワークに 1 つの追加 IP ・**[**メディア用の **IP** ファブリック（**IP Fabric for Media**）**]** が有効になっている場合、テレメトリ用の管理ネットワークに 1 つの追加の IP LAN 展開タイプで **[LAN** デバイス管理の接続性（**LAN Device Management Connectivity**）**]** が [データ（Data）]（デフォルト）に設定されたレイヤー 2 モードで動作している場合 ・SNMP/Syslog および SCP サービス用のデータネットワーク内の 2 つの IP ・**[EPL]** が有効になっている場合、各ファブリックのデータ ネットワークに 1 つの追加 IP ・**[**メディア用の **IP** ファブリック（**IP Fabric for Media**）**]** が有効になっている場合、テレメトリ用のデータネットワークに 1 つの追加の IP

Nexus Dashboard サービス	管理インターフェイス	データ インターフェイス	永続的 **IP** の総数
Nexus Dashboard ファブリック コントローラ、リリース 12.1(3) 以降	レイヤ 2 またはレイヤ 3 隣接	レイヤ 2 またはレイヤ 3 隣接	LAN 展開タイプのレイヤ 3 モードで動作している場合： ・**LAN** デバイス管理の接続性 [データ（Data）]に設定する必要があります。 ・SNMP/Syslog および SCP サービス用の 2 つの IP ・**[EPL]** が有効になっている場合、各ファブリックのデータ ネットワークに 1 つの追加 IP ・すべての永続的 IP は、管理サブネットまたはデータ サブネットと重複していない別のプールの一部である必要があります。 永続的 IP のレイヤ 3 モードの詳細については、ユーザー ガイドの <<Persistent IP Addresses>> のセクションを参照してください。 SAN コントローラ展開タイプのレイヤ 3 モードで動作している場合： ・SSH 用の 1 つの IP ・SNMP/Syslog 用の 1 つの IP ・SAN Insights 機能用の 1 つの IP メディア モードの IP ファブリックは、レイヤ 3 モードではサポートされていません。

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

Nexus Dashboard クラスタとアプリケーションを展開する場合は、常に最も低い RTT 要件を使用する必要があります。例えば、Insights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。

アプリケーション	接続	最大 **RTT**
Nexus Dashboardクラスタ	ノード間	150 ミリ秒
Nexus Dashboard Orchestrator	ノード間	150 ミリ秒
	サイトへ	APIC サイトの場合：500 ミリ秒 NDFC サイトの場合：150 ミリ秒

Nexus Dashboard Insights	ノード間	50 ミリ秒
	スイッチ	50 ミリ秒

アプリケーション	接続	最大 **RTT**
Nexus Dashboard ファブリック コントローラ	ノード間	50 ミリ秒
	スイッチ	200 ms*

* POAP（PowerOn Auto Provisioning）は、Nexus Dashboard ファブリック コントローラとスイッチ間で最大 RTT 50 ミリ秒でサポートされます。

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 Dashboard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、展開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 Dashboard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 Dashboard 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。

> 異なる Nexus Dashboard 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、送信と接続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、クラスタノードを離れ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 Dashboard からそのサービスにアクセスすることはできません。
> そのため、これらのネットワークを設定する際、それらが一意であり、Nexus Dashboardクラスタノードからのアクセスが必要になる可能性のある既存のネットワークやサービスと重複しないように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。

IPv4 および IPv6 のサポート

Nexus Dashboard の以前のリリースでは、クラスタ ノードの純粋な IPv4 構成またはデュアル スタック IPv4/IPv6（管理ネットワークのみ）構成がサポートされていました。リリース 3.0(1) 以降、Nexus Dashboard は、クラスタ ノードおよびサービスの純粋な IPv4、純粋な IPv6、またはデュアル スタック IPv4/IPv6 構成をサポートします。

IP 構成を定義するとき、以下のガイドラインが適用されます。

- クラスタ内のすべてのノードとネットワークは、純粋な IPv4、純粋な IPv6、またはデュアル スタック IPv4/IPv6 のいずれかの均一な IP 構成を持つ必要があります。
- デュアル スタック構成の場合：

- 上記のすべてのネットワークは、デュアル スタック モードである必要があります。
- IPv4 データ ネットワークやデュアル スタック管理ネットワークなどの部分的な構成はサポートされていません。
- 物理的なサーバーの CIMC にも IPv6 アドレスが必要です。
- ノードの初期起動時にノードの管理ネットワークに IPv4 または IPv6 アドレスを構成できますが、クラスタのブートストラップ ワークフロー中に両方のタイプの IP を指定する必要があります。
- 管理 IP は、初めてノードにログインしてクラスタのブートストラップ プロセスを開始するために使用されます。
- すべてのノード、ネットワーク、および永続 IP に対して、両方のタイプの IP アドレスを設定する必要があります。
- すべての内部証明書は、IPv4 と IPv6 の両方のサブジェクト代替名（SAN）を含むように生成されます。
- Kubernetes 内部コア サービスは IPv4 モードで開始されます。
- DNS は、IPv4 と IPv6 の両方にサービスを提供して転送し、両方のタイプのレコードをサーバーに提供します。
- ピア接続用の VxLAN オーバーレイは、データ ネットワークの IPv4 アドレスを使用します。
- IPv4 パケットと IPv6 パケットは両方とも、VxLAN の IPv4 パケット内にカプセル化されます。
- UI は、IPv4 と IPv6 の両方の管理ネットワーク アドレスでアクセスできます。

- 純粋な IPv6 構成の場合：
  - ノードを最初に構成するときに、IPv6 管理ネットワーク アドレスを指定する必要があります。
  - ノード（物理、仮想、またはクラウド）が起動した後、これらの IP を使用して UI にログインし、クラスタのブートストラップ プロセスを続行します。
  - 前述の内部アプリケーションおよびサービス ネットワークに IPv6 CIDR を提供する必要があります。
  - 前述のデータ ネットワークと管理ネットワークに IPv6 アドレスとゲートウェイを提供する必要があります。
  - すべての内部証明書は、IPv6 サブジェクト代替名 (SAN) を含むように生成されます。
  - すべての内部サービスは IPv6 モードで開始されます。
  - ピア接続用の VxLAN オーバーレイは、データ ネットワークの IPv6 アドレスを使用します。
  - IPv6 パケットは、VxLAN の IPv6 パケット内にカプセル化されます。
  - すべての内部サービスは IPv6 アドレスを使用します。

通信ポート：**Nexus Dashboard**

Nexus Dashboard クラスタには、次のポートが必要です。

ヒ

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

表 1. 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	接続
ICMP	ICMP	ICMP	入力 / 出力	他のクラスタ ノード、CIMC、デフォルト ゲートウェイ
SSH	22	TCP	入力 / 出力	クラスタ ノードの CLI および CIMC
TACACS	49	TCP	発信	TACACS サーバー
DNS	53	TCP/UDP	アウト	DNS サーバ
HTTP	80	TCP	発信	インターネット/プロキシ
NTP	123	UDP	発信	NTP サーバー
HTTPS	443	TCP	入力 / 出力	UI、他のクラスタ (マルチクラスタ接続用)、ファブリック、インターネット/プロキシ
LDAP	389 636	TCP	発信	LDAP サーバ
RADIUS	1812	TCP	発信	Radius サーバー
KMS	9880	TCP	入力 / 出力	その他クラスタ ノードおよび ACI ファブリック
インフラサービス	30012 30021 30500-30600	TCP および UDP	入力 / 出力	その他のクラスタ ノード

表 2. 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	接続
SSH	22	TCP	発信	スイッチと APIC の帯域内
HTTPS	443	TCP	発信	スイッチと APIC の帯域内
SSH	1022	TCP および UDP	入力 / 出力	その他のクラスタ ノード
VXLAN	4789	TCP	入力 / 出力	その他のクラスタ ノード
KMS	9880	TCP	入力 / 出力	その他クラスタ ノードおよび ACI ファブリック

サービス	ポート	プロトコル	方向	接続
インフラサービス	3379 3380 8989 9090 9969 9979 9989 15233 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	スイッチと APIC/NDFC の帯域内
インフラサービス	30016 30017	TCP および UDP	入力 / 出力	その他のクラスタ ノード
インフラサービス	30500-30600	TCP および UDP	入力 / 出力	その他のクラスタ ノード

通信ポート：Nexus Dashboard Insights

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

表 3. 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	接続
Techcollection を表示	2022	TCP	入力 / 出力	スイッチと APIC/NDFC の帯域内
フローテレメトリ	5640 ~ 5671	UDP	入力	スイッチの帯域内
TAC アシスト	8884	TCP	入力 / 出力	その他のクラスタ ノード
KMS	9989	TCP	入力 / 出力	その他クラスタ ノードおよび ACI ファブリック
SW テレメトリ	5695 30000 30570 57500	TCP	入力 / 出力	その他のクラスタ ノード

通信ポート：**Nexus Dashboard** ファブリック コントローラ

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

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

表 4. Nexus Dashboard ファブリック コントローラ通信ポート

サービス	ポート	プロトコル	方向	接続
SSH	22	TCP	発信	SSH は、デバイスにアクセスするための基本的なメカニズムです。
SCP	22	TCP	発信	NDFC バックアップ ファイルをリモート サーバーにアーカイブする SCP クライアント。
SMTP	25	TCP	発信	SMTP ポートは、NDFC の [サーバー設定（Server Settings）] メニューから構成できます。 これはオプションの機能です。
DHCP	67	UDP	入力	NDFC ローカル DHCP サーバーがブートストラップ/POAP 用に構成されている場合。これは、LAN 展開にのみ適用されます。 注：POAP の目的でローカル DHCP サーバーとして NDFC を使用する場合、すべての ND マスター ノードの IP を DHCP リレーとして構成する必要があります。ND ノードの管理 IP またはデータ IP が DHCP サーバーにバインドされるかどうかは、NDFC サーバー設定の LAN デバイス管理接続によって決定されます。
DHCP	68	UDP	発信	
SNMP	161	TCP/UDP	アウト	NDFC からデバイスへの SNMP トラフィック。
HTTPS/HTTP（NX-API）	443/80	TCP	発信	NX-API HTTPS/HTTP クライアントは、構成可能でもあるポート 443/80 でデバイスの NX-API サーバーに接続します。NX-API はオプション機能であり、NDFC 機能の限られたセットで使用されます。 これは、LAN 展開にのみ適用されます。
HTTPS（vCenter, Kubernetes, OpenStack, Discovery）	443	TCP	発信	NDFC は、VMware vCenter や OpenStack などの登録済み VMM ドメインと、Kubernetes などのコンテナ オーケストレーターから取得した情報を関連付けることにより、統合されたホストおよび物理ネットワーク トポロジ ビューを提供します。 これはオプションの機能です。

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

表 5. Nexus Dashboard Fabric Controller 永続的 IP ポート

サービス	ポート	プロトコル	方向	接続
SCP	22	TCP	入力	SCP は、デバイスと NDFC サービス間でファイルを転送するさまざまな機能によって使用されます。NDFC SCP サービスは、ダウンロードとアップロードの両方の SCP サーバーとして機能します。SCP は、POAP 関連ファイルをダウンロードするために、デバイス上の POAP クライアントによっても使用されます。 NDFC の SCP-POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続的な IP があります。これは、NDFC サーバー設定の [LAN デバイス管理接続（LAN Device Management Connectivity）] 設定によって制御されます。
TFTP（POAP）	69	TCP	入力	POAP 経由のデバイス ゼロタッチ プロビジョニングにのみ使用されます。デバイスは、基本的なインベントリ情報を NDFC に送信して (NDFC への制限付きの書き込み専用アクセス)、セキュアな POAP 通信を開始できます。NDFC ブートストラップまたは POAP は、TFTP または HTTP/HTTPS 用に構成できます。 NDFC の SCP-POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続的な IP があります。これは、NDFC サーバー設定の [LAN デバイス管理接続（LAN Device Management Connectivity）] 設定によって制御されます。 これは、LAN 展開にのみ適用されます。

サービス	ポート	プロトコル	方向	接続
HTTP（POAP）	80	TCP	入力	POAP 経由のデバイス ゼロタッチ プロビジョニングにのみ使用されます。デバイスは、基本的なインベントリ情報を NDFC に送信して (NDFC への制限付きの書き込み専用アクセス)、セキュアな POAP 通信を開始できます。NDFC ブートストラップまたは POAP は、TFTP または HTTP/HTTPS 用に構成できます。 NDFC の SCP-POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続的な IP があります。これは、NDFC サーバー設定の [LAN デバイス管理接続（LAN Device Management Connectivity）] 設定によって制御されます。 これは、LAN 展開にのみ適用されます。
BGP	179	TCP	入力 / 出力	エンドポイント ロケーターの場合、有効になっているファブリックごとに、独自の永続的な IP を使用して EPL サービスが生成されます。このサービスは、常に Nexus Dashboard データ インターフェイスに関連付けられています。エンドポイント情報を追跡するために必要な BGP アップデートを取得するために、ファブリック上の適切な BGP エンティティ（通常は BGP ルート リフレクタ）と NDFC EPL サービスはピアを行います。 この機能は、VXLAN BGP EVPN ファブリック の展開にのみ適用されます。 これは、LAN 展開にのみ適用されます。
HTTPS（POAP）	443	TCP	入力	セキュア POAP は、ポート 443 の NDFC HTTPS サーバーを介して実現されます。 HTTPS サーバーは SCP-POAP サービスにバインドされ、そのポッドに割り当てられたのと同じ永続的 IP を使用します。 NDFC の SCP-POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続的な IP があります。これは、NDFC サーバー設定の [LAN デバイス管理接続（LAN Device Management Connectivity）] 設定によって制御されます。 これは、LAN 展開にのみ適用されます。

サービス	ポート	プロトコル	方向	接続
Syslog	514	UDP	入力	NDFC が Syslog サーバーとして構成されている場合、デバイスからの Syslog は、SNMP-Trap/Syslog サービス ポッドに関連付けられた永続的な IP に向けて送信されます。NDFC の SNMP-Trap-Syslog サービスには、管理サブネットまたはデータサブネットに関連付けられた永続 IP があります。 これは、NDFC サーバー設定の [LAN デバイス管理接続（LAN Device Management Connectivity）] 設定によって制御されます。
SCP	2022	TCP	発信	NDFC POAP-SCP ポッドの永続的な IP から、Nexus Dashboard Insights を実行している別の ND クラスターにテクニカル サポート ファイルを転送します。 NDFC の SCP-POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続的な IP があります。これは、NDFC サーバー設定の LAN デバイス管理接続設定によって制御されます。
SNMP トラップ	2162	UDP	入力	デバイスから NDFC への SNMP トラップは、SNMP-Trap/Syslog サービス ポッドに関連付けられた永続的な IP に向けて送信されます。 NDFC の SNMP-Trap-Syslog サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続的な IP があります。 これは、NDFC サーバー設定の [LAN デバイス管理接続（LAN Device Management Connectivity）] 設定によって制御されます。
GRPC（テレメトリ）	33000	TCP	入力	NDFC 永続的 IP に関連付けられた GRPC トランスポートを介して SAN データ (ストレージ、ホスト、フローなど) を受信する SAN Insights Telemetry サーバー。 これは、SAN 展開でのみ有効です。
GRPC（テレメトリ）	50051	TCP	入力	メディア展開用の IP ファブリックおよび一般的な LAN 展開用の PTP のマルチキャスト フローに関連する情報は、ソフトウェア テレメトリを介して、NDFC GRPC レシーバー サービス ポッドに関連付けられた永続的 IP にストリーミングされます。 これは、LAN およびメディア展開でのみ有効です。

通信ポート：SAN 展開用 Nexus Dashboard ファブリック コントローラ

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

表 6. 単一ノード クラスタでの SAN 展開向けの Nexus Dashboard Fabric Controller ポート

サービス	ポート	プロトコル	方向	接続
SSH	22	TCP	発信	SSH は、デバイスにアクセスするための基本的なメカニズムです。
SCP	22	TCP	発信	NDFC バックアップ ファイルをリモート サーバーにアーカイブする SCP クライアント。
SMTP	25	TCP	発信	SMTP ポートは、NDFC の [サーバー設定（Server Settings）] メニューから構成できます。 これはオプションの機能です。
SNMP	161	TCP/UDP	アウト	NDFC からデバイスへの SNMP トラフィック。
HTTPS（vCenter, Kubernetes, OpenStack, Discovery）	443	TCP	発信	NDFC は、VMware vCenter や OpenStack などの登録済み VMM ドメインと、Kubernetes などのコンテナ オーケストレーターから取得した情報を関連付けることにより、統合されたホストおよび物理ネットワーク トポロジ ビューを提供します。 これはオプションの機能です。

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

表 7. 単一ノード クラスタでの SAN 展開向けの Nexus Dashboard Fabric Controller 永続的 IP ポート

サービス	ポート	プロトコル	方向	接続
SCP	22	TCP	入力	SCP は、デバイスと NDFC サービス間でファイルを転送するさまざまな機能によって使用されます。NDFC SCP サービスは、ダウンロードとアップロードの両方で機能します。

サービス	ポート	プロトコル	方向	接続
Syslog	514	UDP	入力	NDFC が Syslog サーバーとして構成されている場合、デバイスからの syslog は、SNMP-Trap/Syslog サービス ポッドに関連付けられた永続的 IP に向けて送信されます。NDFC の SNMP-Trap-Syslog サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続的な IP があります。 これは、NDFC サーバー設定の [LAN デバイス管理接続（LAN Device Management Connectivity）] 設定によって制御されます。
SNMP トラップ	2162	UDP	入力	デバイスから NDFC への SNMP トラップは、SNMP-Trap/Syslog サービス ポッドに関連付けられた永続的な IP に向けて送信されます。 NDFC の SNMP-Trap-Syslog サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続的な IP があります。
GRPC（テレメトリ）	33000	TCP	入力	NDFC 永続的 IP に関連付けられた GRPC トランスポートを介して SAN データ (ストレージ、ホスト、フローなど) を受信する SAN Insights Telemetry サーバー。 これは、SAN 展開でのみ有効です。

ファブリック接続

Nexus Dashboardクラスタは、次の2つの方法でファブリックに接続できます。

- レイヤ 3 ネットワーク経由でファブリックに接続された Nexus Dashboard クラスタ。
- リーフ スイッチに接続された Nexus Dashboard ノードは、一般的なホストです。

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

外部レイヤ 3 ネットワークを介した接続

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

- Cisco ACI ファブリックのみを管理するために Nexus Dashboard オーケストレータを展開する場合は、データ インターフェイスから各サイトの APIC のインバンドまたはアウトオブバンド（OOB）インターフェイスまたは両方への接続を確立できます。
- Cisco NDFC ファブリックを管理するために Nexus Dashboard Orchestrator を展開する場合は、データインターフェイスから各サイトの NDFC のインバンドインターフェイスへの接続を確立する必要があります。
- Nexus ダッシュボード Insights などの Day-2 Operations アプリケーションを展開する場合は、データ インターフェイスから各ファブリックおよび APIC のインバンド ネットワークへの接続を確立する必要があります。

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

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

  ACI ファブリックでの外部接続の設定については、『*Cisco APIC Layer 3 Networking Configuration Guide*』を参照してください。

- NDFC ファブリックの場合、データ インターフェイスと NDFC のインバンドインターフェイスが異なるサブネットにある場合は、Nexus Dashboard のデータ ネットワークのルートを NDFC 上に追加する必要があります。

  NDFC UI からルートを追加するには、**[**管理（**Administration**）**] > [**カスタマイズ（**Customization**）**] > [**ネットワーク設定（**Network Preference**）**] > [**インバンド **(eth2)**（**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、ホストポートはそのVLANを許可するトランクとして設定する必要があります。

  ただし、ほとんどの一般的な展開では、VLAN IDを空白のままにして、アクセスモードでホストポートを設定できます。

次の2つの図は、外部レイヤ3ネットワーク経由でNexus Dashboardクラスタを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。

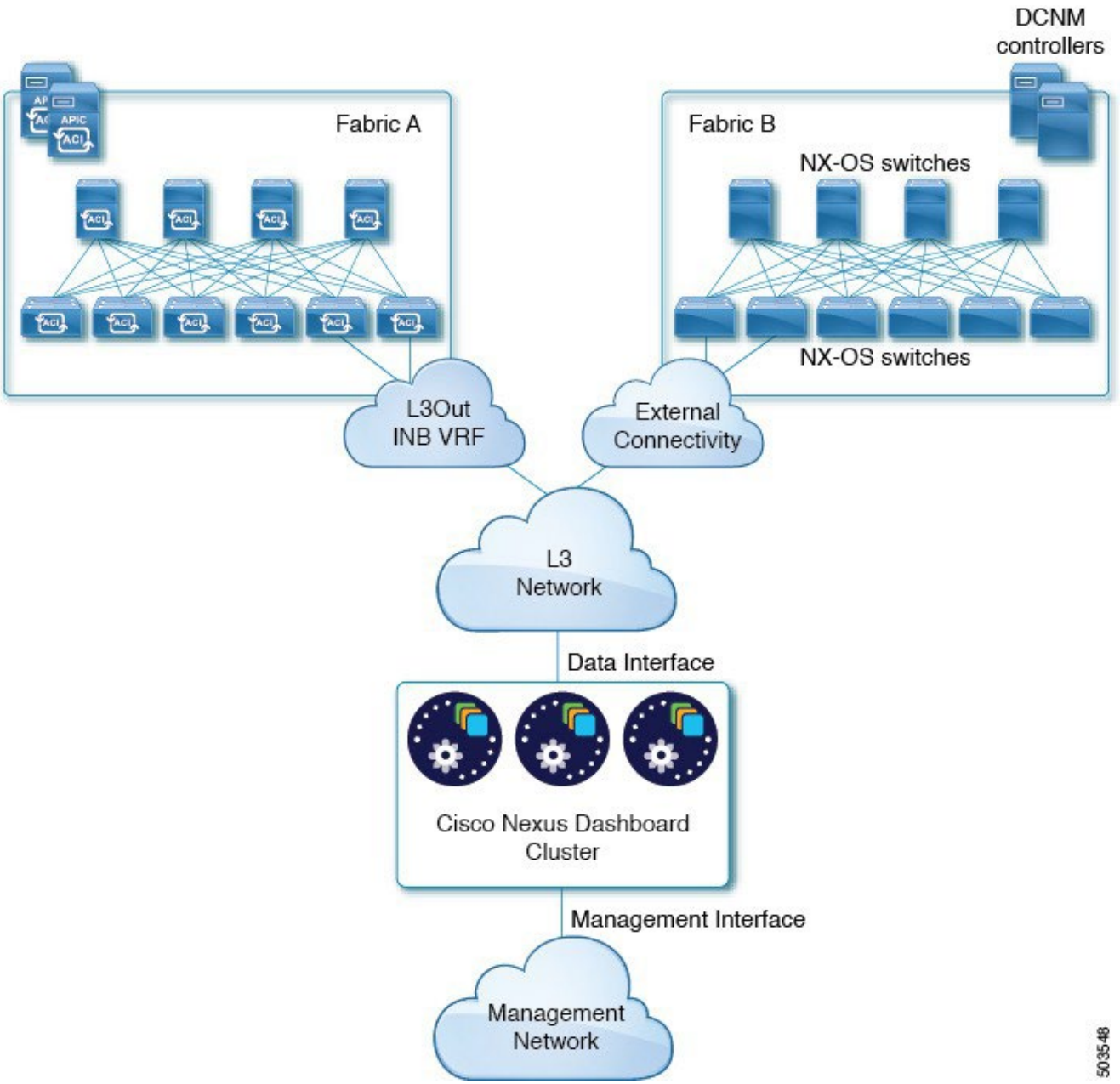

図 1. 外部レイヤ3ネットワーク経由の接続、2日目の運用サービス

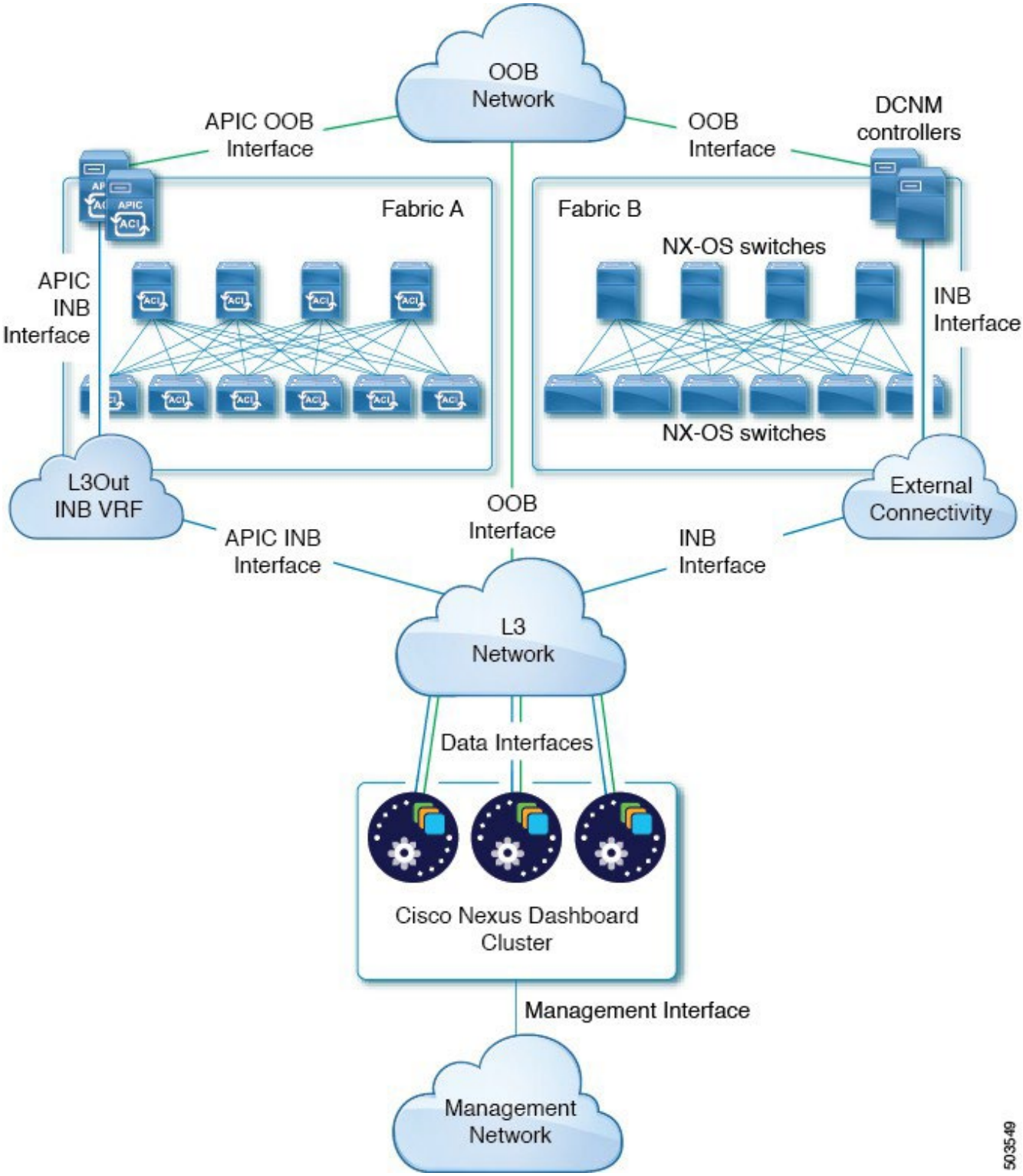

図 2 外部レイヤ3ネットワーク、Nexus Dashboard Orchestratorを使用した接続

リーフスイッチへのノードの直接接続

Nexus Dashboard クラスタをファブリックの 1 つに直接接続することもできます。これにより、クラスタとファブリックのインバンド管理が容易になりますが、クラスタを特定のファブリックに結び付け、外部接続を介して他のファブリックに到達できるようにする必要があります。これにより、クラスタが特定のファブリックに依存するようになるため、ファブリック内の問題が Nexus Dashboard の接続に影響を与える可能性があります。前の例と同様に、接続はNexusダッシュボードに展開されたアプリケーションのタイプによって異なります。

- Cisco ACIファブリックのみを管理するためにNexus Dashboard Orchestratorを展開する場合は、データインターフェイスから各サイトのAPICのインバンドまたはアウトオブバンド(OOB)インターフェイスへの接続を確立できます。
- Nexus Dashboard InsightsまたはNetwork Assurance Engineを展開する場合は、各ファブリックのデータインターフェイスからインバンドインターフェイスへの接続を確立する必要があります。

  ACIファブリックの場合、データインターフェイス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 IP アドレスと ACI ファブリックのインバンド IP アドレスが異なるサブネットに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、Nexus Dashboard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、一般的には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 Dashboard 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サービスエンジンクラスタ上のアプリで監視されている場合、デフォルトルートまたは他のACIファブリックのインバンド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結ぶ必要があります。

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

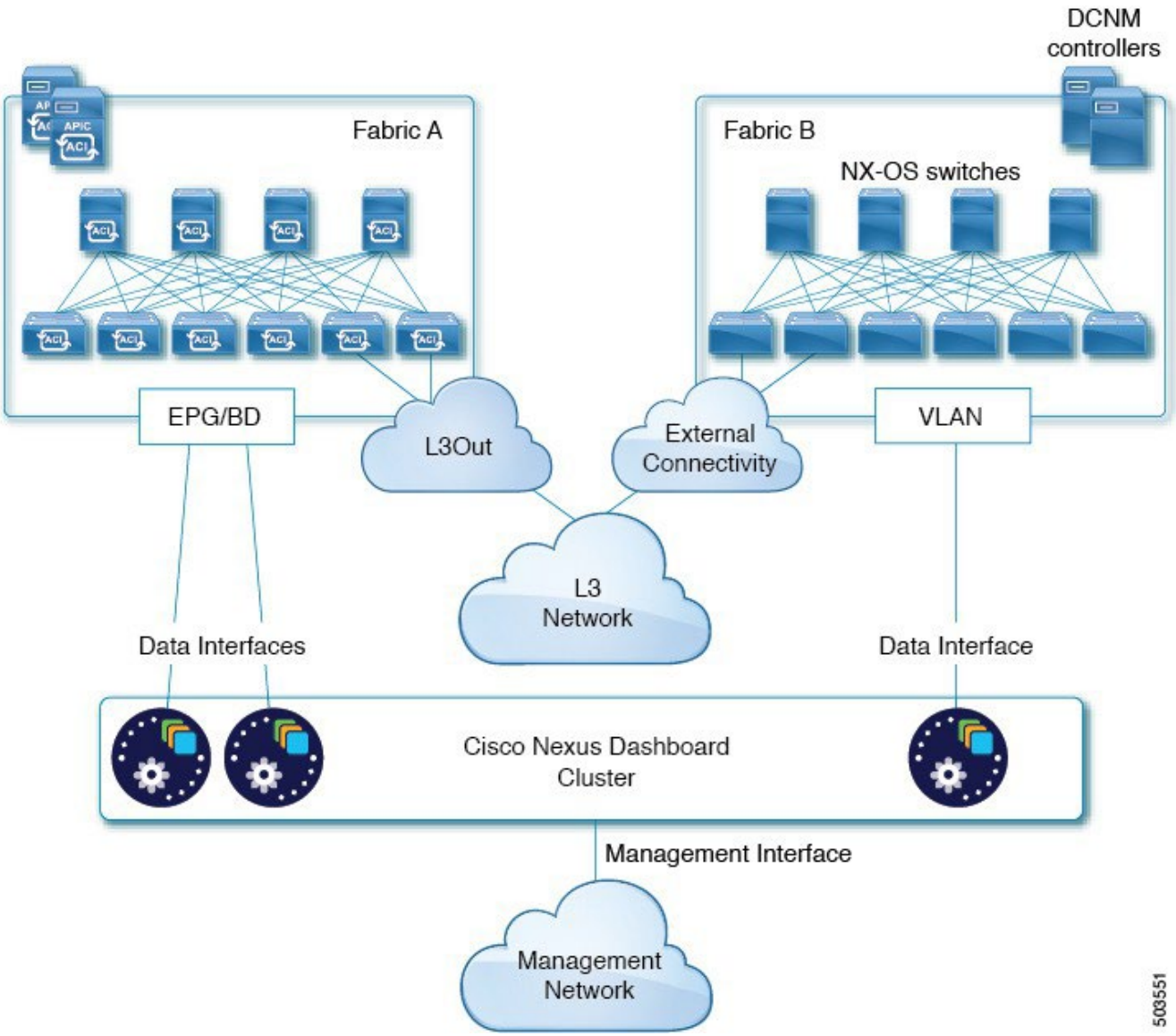

図 3. EPG / BD経由の接続、2日目の運用サービス

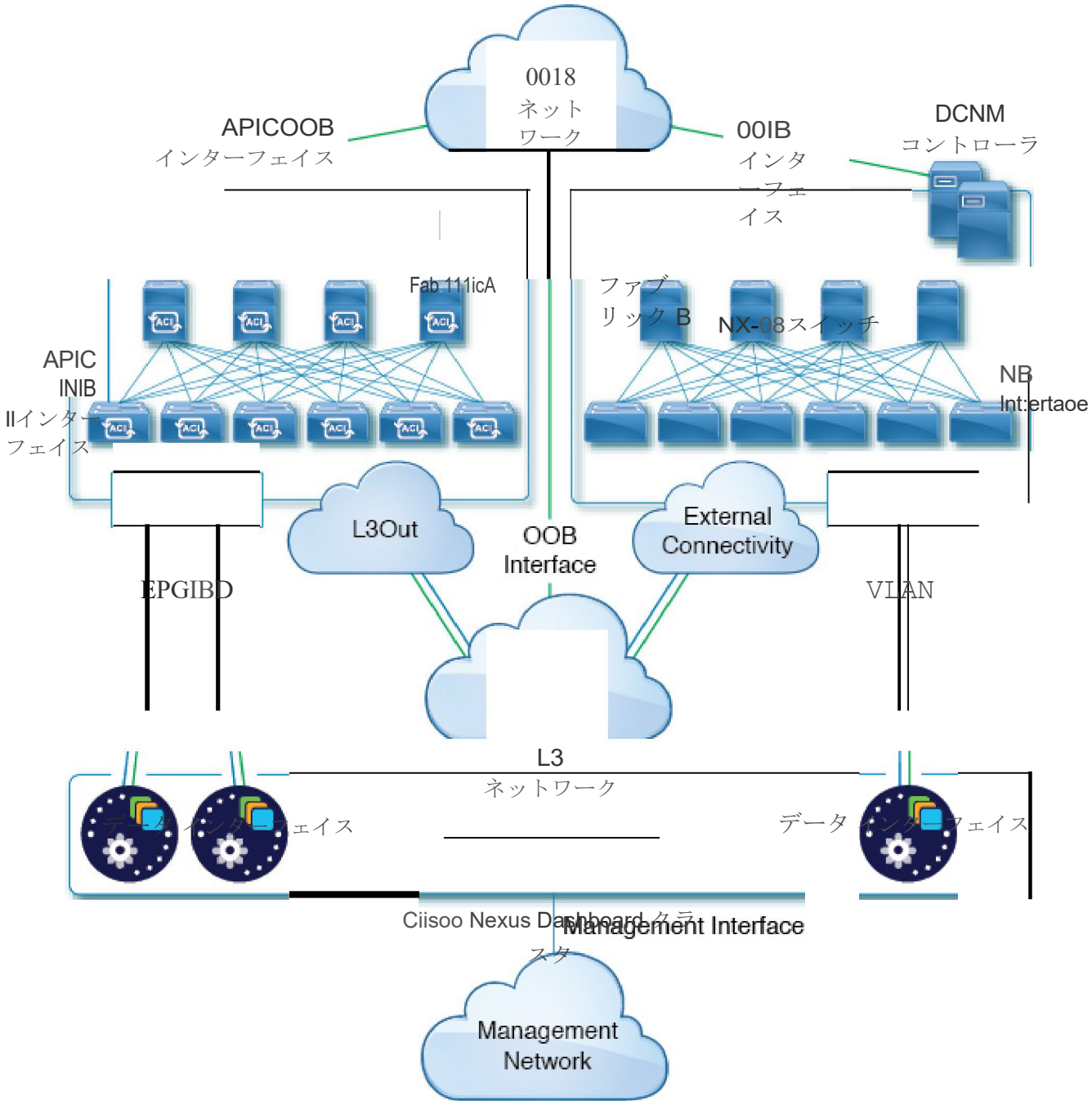

図 4 EPG / BD、Nexus Dashboard Orchestratorを介した接続

GUI の概要

Admin Console

Nexus Dashboard クラスタを展開した後、その GUI を使用して残りのアクションをすべて実行できます。Cisco Nexus DashboardのGUIにアクセスするには、ノードの管理IPアドレスのいずれかを参照します。

```
https://<node-mgmt-ip>
```

ヒ

NexusダッシュボードGUIにログインしているユーザの権限に応じて、ユーザがアクセスを許可されているオブジェクトと設定のみがUIに表示されます。次のセクションで、管理者ユーザーに表示される GUI 要素すべてについて説明します。ユーザー設定と権限の詳細については、「ユーザー」を参照してください。

ナビゲーションバーとユーザー設定

Nexus Dashboard UIとインストールされているサービスにアクセスすると、画面の上部に常に共通のナビゲーションバーが表示されます。

- **Nexus Dashboard** のタイトルは、現在表示しているページまたはサービスから Nexus Dashboard の概要 ページに戻ります。
- [サービス スイッチャ（**Service Switcher**）] ドロップダウンでは、Nexus Dashboard 管理コンソールと展開されたサービスの間を移動できます。
- **[**ユーザー（**user**）**]** メニューでは、ログアウト、現在ログインしているユーザーのパスワードの変更、API キーの管理、1 つまたは複数のユーザー固有設定を行うことができます。
  - **[**ログイン時にようこそ画面を表示（**Show Welcome Screen On Login**）**]** は、現在のユーザーがログインするたびに新機能の画面を表示するかを切り替えます。
  - **[**タイムゾーン設定（**Time Zone Preference**）**]** を使用すると、現在ログインしているユーザーのタイムゾーンを指定できるため、地理的に異なる場所にいる複数のユーザーの UI に時間固有の情報がより便利に表示されるようになります。

    [自動（Automatic）] に設定すると、ローカルブラウザのタイムゾーンが使用されます。これはデフォルト設定で、Nexus Dashboard の過去のリリースと同じ動作をします。

    [手動（Manual）] に設定すると、地図から地理的位置を選択でき、それに応じて最も近いタイムゾーンが設定されます。

    タイムゾーンの変換はUIでのみ実行され、バックエンドとAPIは、保存されている形式(通常はUTC)でタイムスタンプを返し続けます。

ヒ

このリリースは、Nexus DashboardおよびInsightsサービスのグローバルタイムゾーンの設定のみをサポートします。他のサービスは、自動または内部で設定されたタイムゾーン設定を引き続き使用できます。Nexus Dashboard Insightsサービスのタイムゾーン設定は絶対的です。つまり、地理的に異なる地域に複数のサイトがある場合、すべてのソースタイムゾーンが設定されたタイムゾーンにマッピングされます。

- [ヘルプ（**Help**）] メニューから、バージョン情報、現在のリリースの新機能、Nexus Dashboard のドキュメント、インストール済みサービスにアクセスできます。
- [通知（**Notifications** ）] アイコンには、注意が必要なクラスタの動作と正常性に関する新しい通知のリストが表示されます。

この **[概要]** ページには、現在の Nexus Dashboard クラスタのステータス、サイト、サービス、およびリソースの使用状況に関する情報が表示されます。

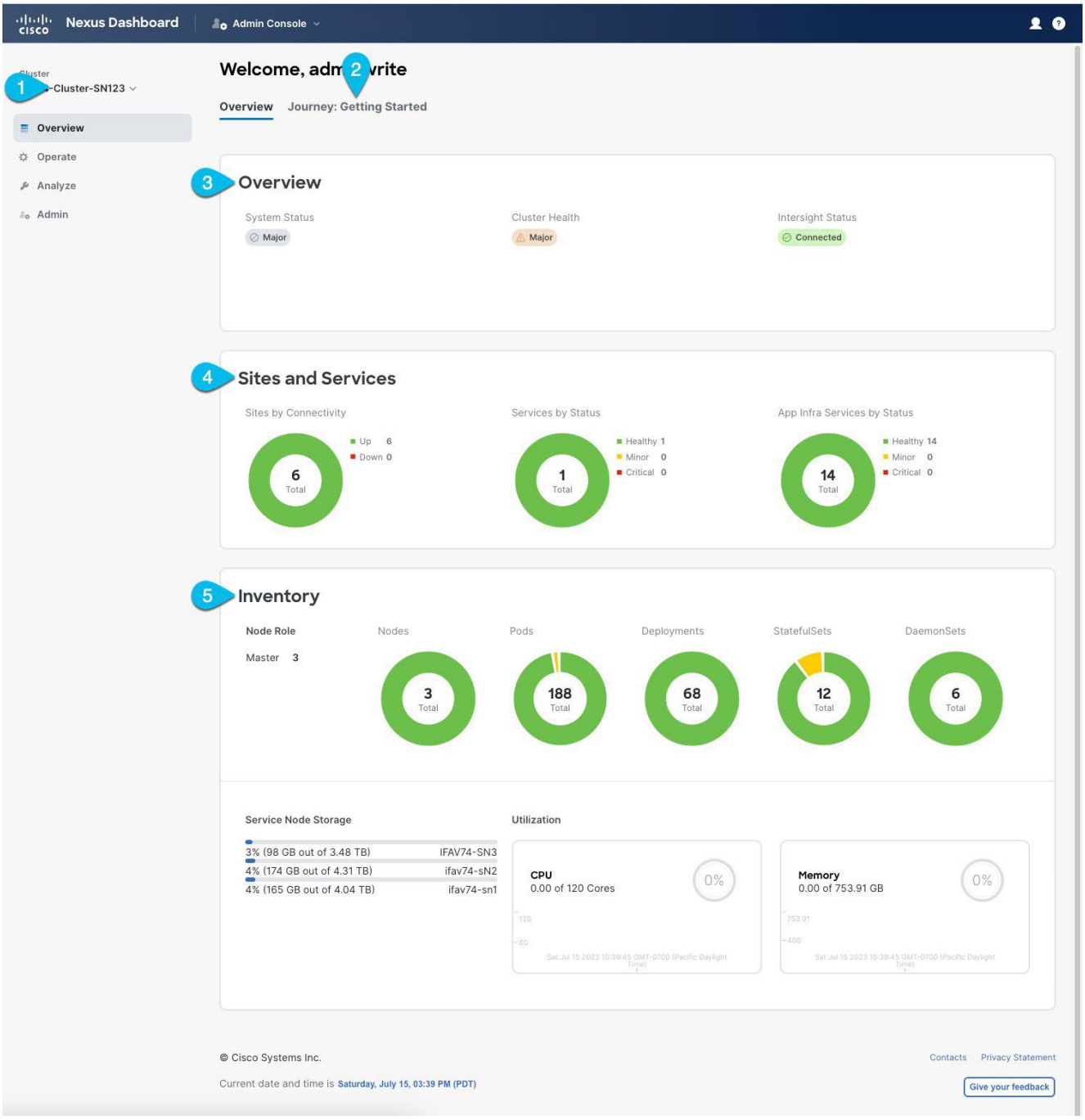

図 5 概要

1. **[現在のクラスタ（Current Cluster）]** には、現在表示されているクラスタの名前が表示されます。

   これはマルチクラスタ展開でのみ有効になり、接続されている別のクラスタにすばやく切り替えることができます。詳細については、「マルチ クラスタ接続」を参照してください。

2. ジャーニー：**[はじめに（Getting Started ）]** タブには、Nexus Dashboardのさまざまな

機能と の初期ワークフローを見つけるのに役立つステップバイステップのガイダンスが用意されています。

3. **[概要（Overview）]** タイルには、システム、クラスタの正常性、Cisco Intersight のステータスが表示されます。

   [クラスタの正常性（Cluster Health）] または **[Intersight ステータス（Intersight Status）]** をクリックすると、それらに問題がある場合に詳細を確認できます。

4. **[サイトとサービス（Sites and Services）]** タイルには、接続ごとにサイトが表示され、ステータスごとにサービスとインフラ サービスが表示されます。

   接続は、サイトがアップ（Up）かダウン（Down）かを示します。

   ステータスは、正常なサービスの数、軽微な障害が発生しているサービスの数、または重大な障害が発生しているサービスの数を示します。

5. **[インベントリ（Inventory）]** タイルには、現在選択しているクラスタのノード、ポッド、展開、およびその他の統計情報の詳細が表示されます。

ヒ **[システム概要（System Overview）]** タブのさまざまな領域をクリックすると、対応する GUI 画面が開き、追加の詳細を表示したり、設定を変更したりできます。

[操作（Operate）] > [サイト（Sites）] ページ

このページでは、単一の場所からサイトをオンボードし、クラスタに展開した任意のサービスからそのサイトを使用できます。

すでにオンボーディングされているすべてのサイトがこのページに表示されます。

- 正常性スコア（Health Score）：サイトのコントローラによって報告された、サイトの現在の正常性ステータス。
- 名前（Name）：導入準備中に指定したサイト名。
- 接続ステータス（**Connectivity Status**）：サイトの接続が確立されている（Up）か、確立されていない（Down）かを示します。
- ファームウェア バージョン（Firmware Version）：サイトで現在実行されているコントローラ ソフトウェアのバージョン。
- 使用サービス（**Services Used**）：指定のサイトを現在使用している

サービスのリスト。オンボーディングサイトの詳細については、「サイト

管理」を参照してください。

[操作（Operate）] > [サービス（Services）] ページ

このページから、Nexus Dashboard のサービスにアクセスして管理できます。

すでにインストールされ、有効になっているサービスは、**[インストール済みサービス（Installed Services）]** タブに表示されます。**[App Store]** タブには、シスコの Data Center アプリケーション センター ページから追加サービスを直接、簡単に展開できます。

サービスの管理の詳細については、「サービス管理」を参照してください。

[操作] > [ノード] ページ

クラスタ内のすべてのプライマリノード、ワーカーノード、スタンバイ ノードに関する情報と、それらのネットワーク設定および CPU/メモリ使用率を表示します。

ページの分析

このカテゴリには、次のページが含まれます。

- 履歴とログ（**History and Logs**）：プラットフォームとサービスからのイベント履歴と監査ログが含まれます。
- テクニカル サポート（**Tech Support**）：管理者は、クラスタおよび展開されたサービスに関するテクニカル サポート情報を収集できます。
- リソース使用率（**Resource Utilization**）：Nexus Dashboard クラスタのリソース使用率に関するリアルタイムの情報が表示されます。

管理ページ

このカテゴリには、次のページが含まれます。

- ソフトウェア管理（**Software Management**）：クラスタ（ファームウェア）のアップグレードを実行できます。
- **[**バックアップと復元（**Backup and Restore**）**]**：クラスタ設定をバックアップまたは復元できます。
- 認証（**Authentication**）：「リモート認証」で説明されているとおり、リモート認証ドメインを設定できます。
- **[**ユーザー（**Users**）**]**：「ユーザー」で説明されているとおり、ローカルの Nexus Dashboard ユーザーを作成および更新したり、Nexus Dashboard に追加したリモート認証サーバーに設定されているユーザーを確認したりできます。
- セキュリティ（**Security**）：キーや証明書などのセキュリティの設定を表示および編集できます。
- システム設定（**System Configuration**）：クラスタの詳細（名前、アプリ サブネット、サービス サブネットなど）を表示し、クラスタ全体の設定（DNS および NTP サーバー、永続的な IP アドレス、ルートなど）を設定でき、クラスタの現在の問題があれば表示します。
- Intersight：Cisco Intersight デバイス コネクタ設定にアクセスできます。
- アプリケーション インフラ サービス（**App Infra Services**）：Nexus Dashboard で実行されているインフラサービスに関する情報を表示し、必要に応じて個々のマイクロサービスの再起動を可能にします。

商標

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザー側の責任となります。

対象製品のソフトウェア ライセンスと限定保証は、製品に添付された『Information Packet』に記載されており、この参照により本マニュアルに組み込まれるものとします。添付されていない場合には、代理店にご連絡ください。

Cisco が採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記代理店は、商品性、特定目的適合、および非侵害の保証、もしくは取り引き、使用、または商慣行から発生する保証を含み、これらに限定することなく、明示または暗黙のすべての保証を放棄します。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアルの中の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際の IP アドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco およびCisco のロゴは、Cisco またはその関連会社の米国およびその他の国における商標または登録商標です。
商標または登録商標です。シスコの商標の一覧は、http://www.cisco.com/ go/trademarks でご確認いただけます。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」という言葉が使用されていても、シスコと他社の間にパートナー関係が存在することを意味するものではありません。（1110R）。

初版： 2023 年 1 月 31 日
最終更新日：2023 年 4 月 11 日

米国本社
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706 USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax：408 527-0883