Cisco Nexus Dashboard ユーザーガイド、リリース 2.2.x

目次

初版: 2022-05-08
最終更新日: 2022-05-08

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

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』に記載されています。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 Internet Protocol（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。

この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイスにハードコードされている言語、RFP のドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

Cisco および Cisco のロゴは、米国およびその他の国における Cisco およびその関連会社の商標を示します。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。Third-party trademarks mentioned are the property of their respective owners. 「パートナー」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。（1110R）。

新機能および変更された機能に関する情報

次の表に、このガイドの最初に発行されたリリースから現在のリリースまでに、このガイドの編成と機能に加えられた大幅な変更の概要を示します。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	変更	参照先
2.2.1	このドキュメントの初回リリース	–

このドキュメントの最新バージョン

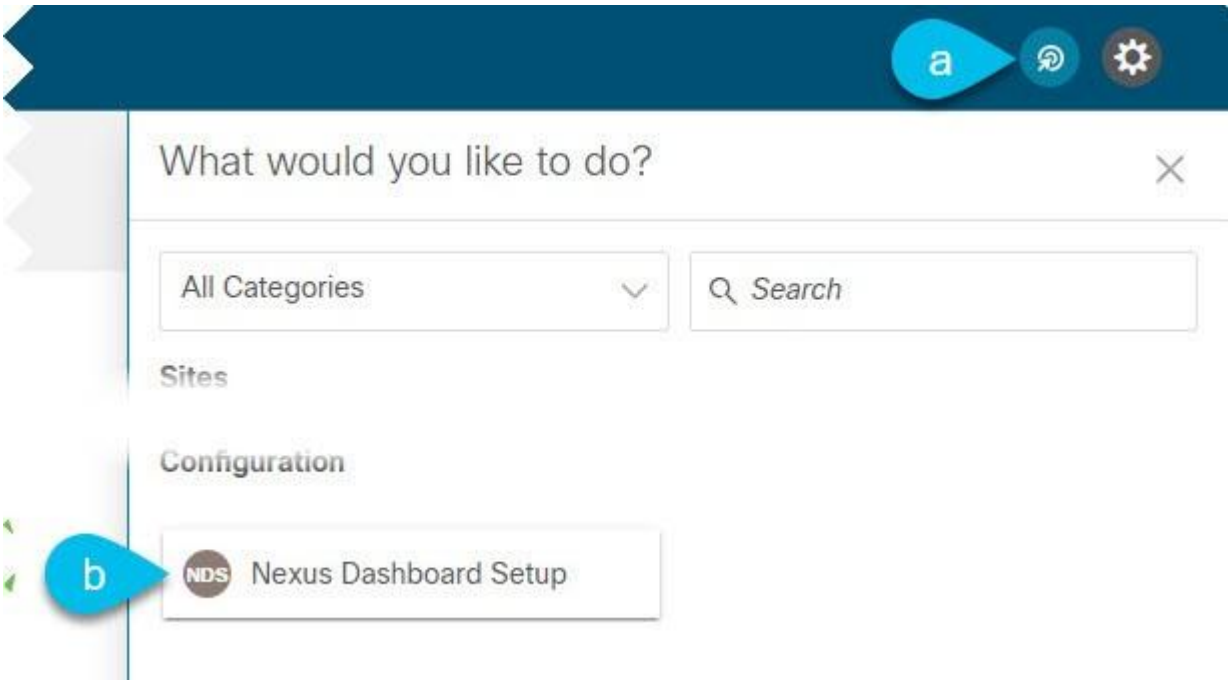
このドキュメントは、Nexus Dashboard GUI およびオンライン（www.cisco.com）から入手できます。このドキュメントの最新版については、 *『Nexus Dashboard ユーザーガイド』*を参照してください。

初回セットアップ

新しい Nexus ダッシュボードクラスタに初めてログインすると、初回セットアップウィザードから基本設定を構成できます。

1. **[最新情報（What's New）]** 画面で、**[設定の開始（Begin Setup）]** をクリックします。
2. 次の 2 つの項のいずれかの説明に従って、サイトを追加し、プロキシを設定します。

初回セットアップウィザードを終了した場合は、Nexus Dashboard の**管理コンソール**のインテントメニューを使用していつでもこのウィザードに戻ることができます。



初回セットアップウィザードをすでに完了している場合は、次の 2 つのセクションをスキップできます。

それ以外の場合は、次の 2 つのことを求めるプロンプトが表示されます。

- プロキシの構成 - インターネットへの接続に使用できるプロキシサーバーを提供できます。

  これは、Cloud APIC サイトを追加するときに必要になる場合があります。その場合、それらのサイトをオンボーディングする前に設定する必要があります。

- サイトの追加 - クラスタで実行されているサービスで使用する 1 つ以上のファブリックをオンボードできます。

プロキシの設定

オンプレミスとクラウドサイトの組み合わせや企業ネットワーク内での Nexus Dashboard クラスタの展開など、特定の展開シナリオでは、インターネットとクラウドサイトへのプロキシを介したアクセスが必要な場合があります。

このリリースでは、単一のプロキシサーバーの追加がサポートされています。

プロキシサーバーを追加するには、次の手順を実行します。

1. **[プロキシ設定（Proxy Configuration）]** タイルで、**[開始（Begin）]** をクリックします。
2. **[セットアップ - プロキシ設定（Setup-Proxy Configuration）]** ページで、**[+サーバーの追加（+Add Server）]** をクリックします。
   a. **[タイプ（Type）]**ドロップダウンから、プロキシするトラフィックのタイプを選択します。
   b. **[サーバー（Server）]** フィールドにプロキシサーバーの完全なアドレスを入力します。

      http://proxy.company.com:80 のように、ポートを指定することもできます。

   c. サーバーにログイン情報が必要な場合は、**ユーザー名**と**パスワード**を入力します。
3. （任意）**[無視するホストの追加（Add Ignore Host）]** をクリックして、プロキシを無視するホストを指定します。

   クラスタがプロキシをバイパスして直接通信する 1 つ以上のホストを追加できます。

サイトの追加

はじめる前に

- ファブリック接続がすでに設定されている必要があります。
- Cisco APIC または Cloud APIC サイトを追加する場合は、サイトでリリース 4.2(4)以降を実行している必要があります。
- Cisco APIC サイトを追加する場合は、Cisco Nexus Dashboard データネットワークの IP 接続用の EPG/L3Out を事前に設定する必要があります。

  詳細については、「ファブリック接続」を参照してください。
- Cisco APIC サイトを追加し、Cisco NIR アプリケーションを展開する場合は、次のことに注意してください。
  - Cisco Nexus Dashboard からデータネットワークを介した Cisco APIC インバンド IP への IP 接続を設定する必要があります。
  - Cisco Nexus Dashboard からリーフノードおよびスパインノードのインバンド IP への IP 接続を設定する必要があります。
- Cisco NDFC または DCNM サイトを追加するには、次のことに注意してください。
  - サイトはリリース 11.5(1)以降を実行している必要があります。
  - ファブリックとスイッチへのレイヤ 3 接続を設定する必要があります。
  - クラスタが AWS または Azure に展開されている場合は、データインターフェイスでインバウンドルールを設定する必要があります。

    これは通常、最初のクラスタ展開中に行われ、「*Cisco Nexus Dashboard Deployment Guide*」で詳細に説明されています。

サイトを追加するには、次の手順を実行します。

1. **[サイトの追加（Add Sites）]** タイルで、**[開始（Begin）]** をクリックします。
2. **[セットアップ - サイトの追加（Setup-Add Sites）]** ページで、**[サイトの追加（Add Site）]** をクリックします。
3. 追加するサイトのタイプを選択します。

Cisco Nexus Dashboard は、3 種類のファブリックすべてのオンボーディングをサポートしますが、サービスと互換性のある特定のファブリックタイプとバージョンについては、「*サービス互換性マトリックス*」を参照してください。

- **ACI** - Cisco APIC によって管理されるオンプレミス ACI サイト向け
- **クラウド ACI** - Cisco Cloud APIC によって管理されるクラウド ACI サイト向け
- **DCNM** - Cisco NDFC または DCNM によって管理されるオンプレミスサイト向け

4. サイトの情報を入力します。

   a. ACI サイトを追加する場合は、次の情報を入力します。

   - **[サイト名（Site Name）]** - このサイトを参照するときに Nexus Dashboard の GUI 全体で使用されます。
   - **[ホスト名（Host Name）]/[IP アドレス（IP Address）]** - Cisco APIC との通信に使用されます。

     このサイトを Nexus Dashboard Orchestrator サービスでのみ使用する場合、APIC のインバンドまたはアウトオブバンド IP アドレスを指定できます。Nexus Dashboard Insights でもこのサイトを使用する場合は、インバンド IP アドレスを指定する必要があります。

     アドレスを指定する場合、URL 文字列の一部としてプロトコル（http:// または https://）を含めないでください。追加すると、サイトの追加に失敗します。

   - **[ユーザー名（User Name）]**と**[パスワード（Password）]** - 追加するサイトで管理者権限を持つユーザーのログイン情報。
   - (任意) **[ログインドメイン（Login Domain）]** - このフィールドを空白にすると、サイトのローカルログインが使用されます。
   - (任意) **[インバンド EPG（In-Band EPG）]** - EPG およびブリッジドメインを介して ACI ファブリックに接続する場合は入力する必要があります。ファブリック接続の詳細については、「ファブリック接続」を参照してください。

     Nexus Dashboard Insights サービスでこのサイトを使用する場合は、ノード管理のインバンド EPG を指定する必要があります。

   b. クラウド ACI サイトを追加する場合は、次の情報を入力します。

   - **[サイト名（Site Name）]** - このサイトを参照するときに Nexus Dashboard の GUI 全体で使用されます。
   - **[ホスト名（Host Name）]/[IP アドレス（IP Address）]** - Cisco クラウド APIC との通信に使用されます。

     アドレスを指定する場合、URL 文字列の一部としてプロトコル（http:// または https://）を含めないでください。追加すると、サイトの追加に失敗します。

   - **[ユーザー名（User Name）]**と**[パスワード（Password）]** - 追加するサイトで管理者権限を持つユーザーのログイン情報。
   - (任意) **[ログインドメイン（Login Domain）]** - このフィールドを空白にすると、サイトのローカルログインが使用されます。

- (任意)**[プロキシの有効化（Enable Proxy）]** - クラウドサイトにプロキシ経由でアクセスできる場合は、この設定を有効にします。

  > プロキシは、Nexus Dashboard のクラスタ設定ですでに設定されている必要があります。詳細については、「プロキシの設定」を参照してください。

c. DCNM サイトを追加する場合は、次の情報を入力します。

- **[ホスト名（Host Name）]/[IP アドレス（IP Address）]** - Cisco NDFC または DCNM との通信に使用されます。
  これは DCNM のインバンド IP アドレスである必要があります。

  > アドレスを指定する場合、URL 文字列の一部としてプロトコル（http:// または https://）を含めないでください。追加すると、サイトの追加に失敗します。

- **[ユーザー名（User Name）]**と**[パスワード（Password）]** - 追加するサイトで管理者権限を持つユーザーのログイン情報。
- **[DCNM 上のサイト（Sites on DCNM）]** - **[サイトの追加（Add Sites）]**をクリックして、指定したコントローラで管理される DCNM ファブリックを選択します。

5. **[追加（Add）]** をクリックして、サイトの追加を終了します。
6. （任意）**[地理的位置（Geographical Location）]** マップをクリックして、サイトの場所を指定します。
7. (任意)他にも追加するサイトがあれば、上記の手順を繰り返します。

ネットワークスケールの設定

リリース 2.2(1)以降、サービスのターゲットスケールを設定でき、Nexus Dashboard クラスタは適切な量のリソースと制限を自動的に割り当てます。

ネットワーク規模を構成するには、次を実行します。

1. **[ネットワークスケール（Network Scale）]**タイルで、**[開始（Begin）]**をクリックします。
2. **[セットアップ-ネットワークスケール（Setup - Network Scale）]**ページで、必要な情報を入力します。

   > ネットワークの規模を変更するには、変更を適用するためにサービスを再起動する必要があります。

a. **[サイトの数（Number of Sites）]**フィールドに、この Nexus Dashboard クラスタが管理する展開のターゲットサイト数を入力します。

デフォルトでは、ネットワークスケールは 10 サイトに設定されています。

b. **[ファブリックノードの数（Number of Fabric Nodes）]**フィールドに、展開のスイッチノードのターゲット数を指定します。

c. **[1 秒あたりのフロー数（Flows per second）]**ドロップダウンメニューから、Nexus Dashboard Insights サービスにおけるターゲットフロー数を選択します。

プラットフォームの概要

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 などのシスコデータセンター運用アプリケーションをホストするための共通プラットフォームです。これらのアプリケーションは、すべてのデータセンターサイトで広く利用でき、ネットワークポリシーと運用のリアルタイム分析、可視性、およびアシュアランスを提供します。Cisco Nexus Dashboard Orchestrator は、ホストされたアプリケーションとして Nexus Dashboard で実行することもできます。

Nexus ダッシュボードは、これらのマイクロサービスベースのアプリケーションに共通のプラットフォームと最新のテクノロジースタックを提供し、さまざまな最新アプリケーションのライフサイクル管理を簡素化し、これらのアプリケーションを実行および維持するための運用オーバーヘッドを削減します。また、ローカルにホストされているアプリケーションとの外部のサード パーティ 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、3 つのマスターノードで構成されます。また、マスターノードで障害が発生した際に簡単にクラスタを回復させられるよう、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やスタンバイノードを有効化できます。追加のノードを使用したクラスタの拡張の詳細については、「インフラストラクチャ管理」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 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 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 Installation 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。

使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 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
- アプリケーションノード - Nexus Dashboard Orchestrator などの非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

- 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

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、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。

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。

サポート対象サービス

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。

ネットワーク接続

Nexus Dashboard はクラスタとして展開され、各サービスノードは 2 つのネットワークに接続されます。Nexus Dashboard の初回設定時に、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され、もう 1 つは管理ネットワークに接続されます。

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 App Store 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

データと管理ネットワーク要件

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 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。

データサブネットを変更するにはクラスタを再展開する必要があるため、今後の追加サービスを考慮して、ノードとサービスの必要最低限よりも大きなサブネットを使用することをお勧めします。このセクションに記載されている要件に加えて、展開を計画している特定のサービスのリリースノートを参照してください。

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	該当なし 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	該当なし
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
SFLOW/NetFlow（ACI または NDFC/DCNM 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 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。 ・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 ・**LAN デバイス管理接続**をデータに設定する場合、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

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

> Nexus Dashboard 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。

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	500 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

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いずれか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。

通信ポート

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

表 2. 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 3. 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	スイッチおよび APIC/NDFC/DCNM の帯域内
VXLAN	4789	TCP	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	接続
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 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
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 4 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
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
SW 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
フローテレメトリ	5695 30000 30570 57500	TCP	入力 / 出力	その他のクラスタ ノード

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。

物理ノードのケーブル接続

仮想またはクラウド フォーム ファクタ クラスタを展開した場合は、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

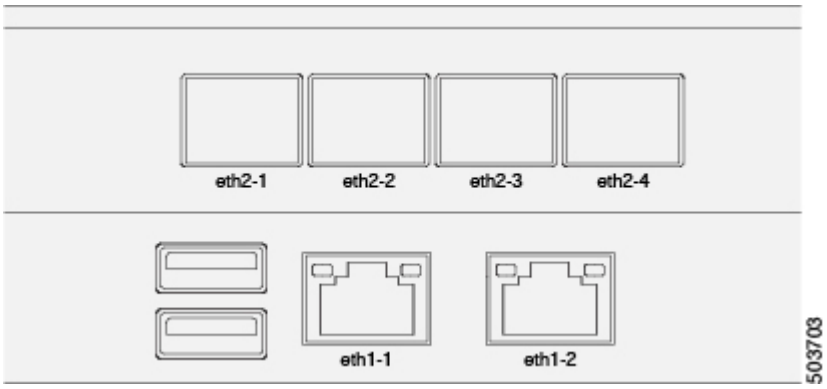


図 1. ノード接続

インターフェイスは、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。ポートチャネルまたは vPC はサポートされません。

外部レイヤ 3 ネットワークを介した接続

Nexus Dashboard に展開されているアプリケーションのタイプに合わせて接続します。

- 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 Orchestrator を展開して Cisco NDFC または 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 Dashboard 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。

- DCNM ファブリックでは、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、DCNM で Nexus Dashboard のデータネットワークにルートを追加する必要があります。

  DCNM 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。

「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。

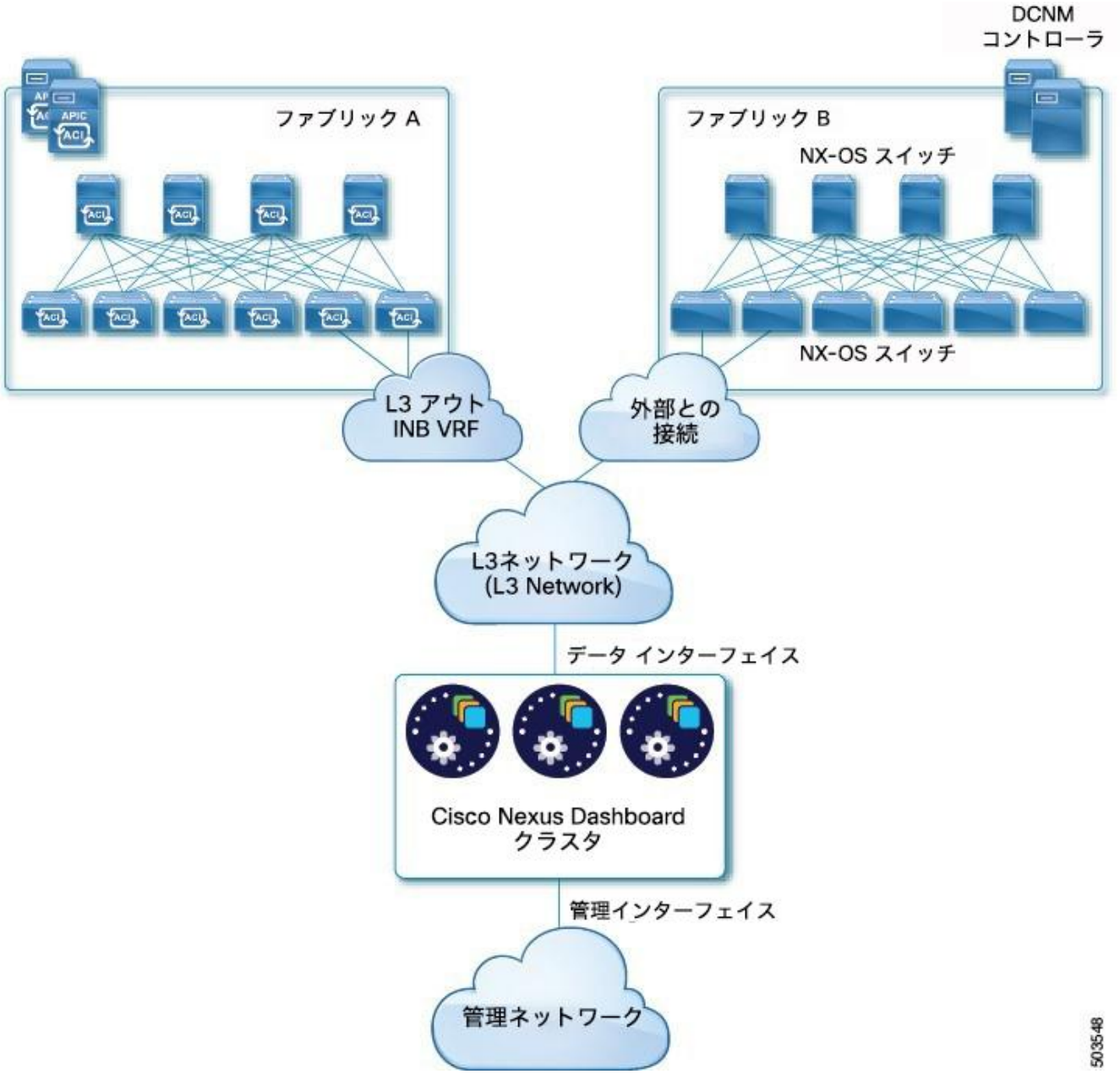


図 2 外部レイヤ 3 ネットワーク経由の接続、2 日目の運用サービス

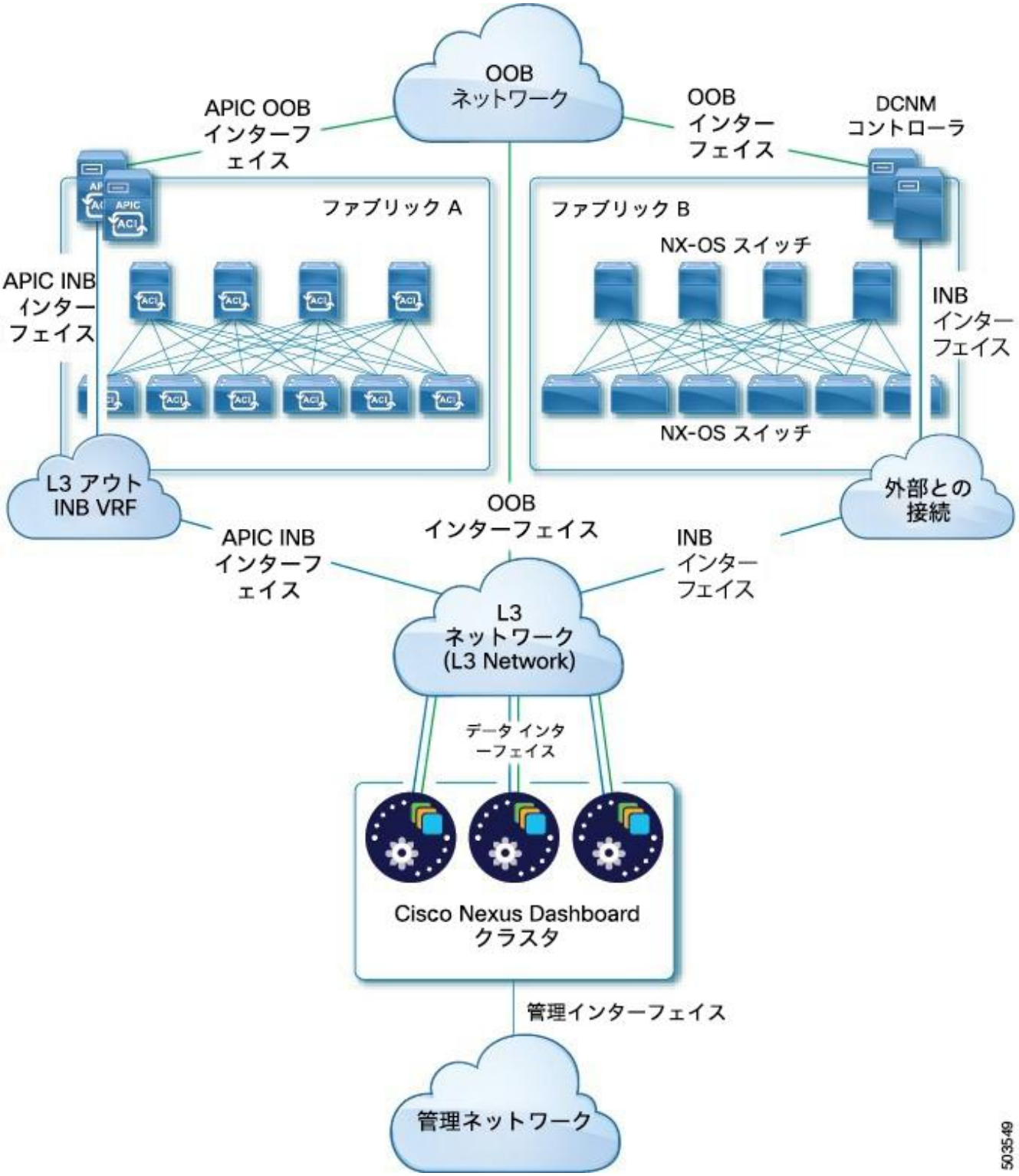


図 3. 外部レイヤ 3 ネットワーク、Nexus Dashboard Orchestrator を使用した接続

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。

「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。

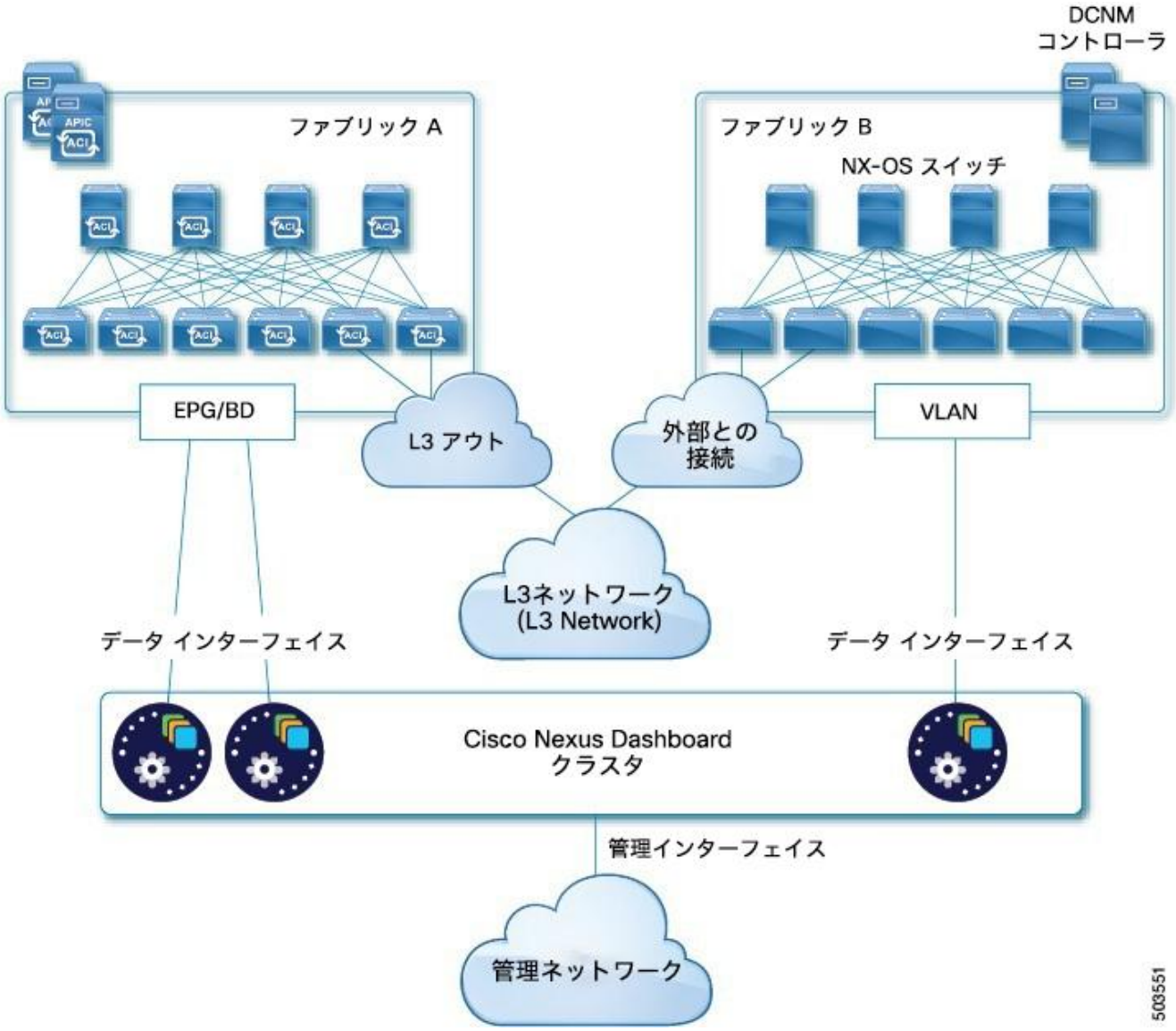


図 4 EPG / BD 経由の接続、2 日目の運用サービス

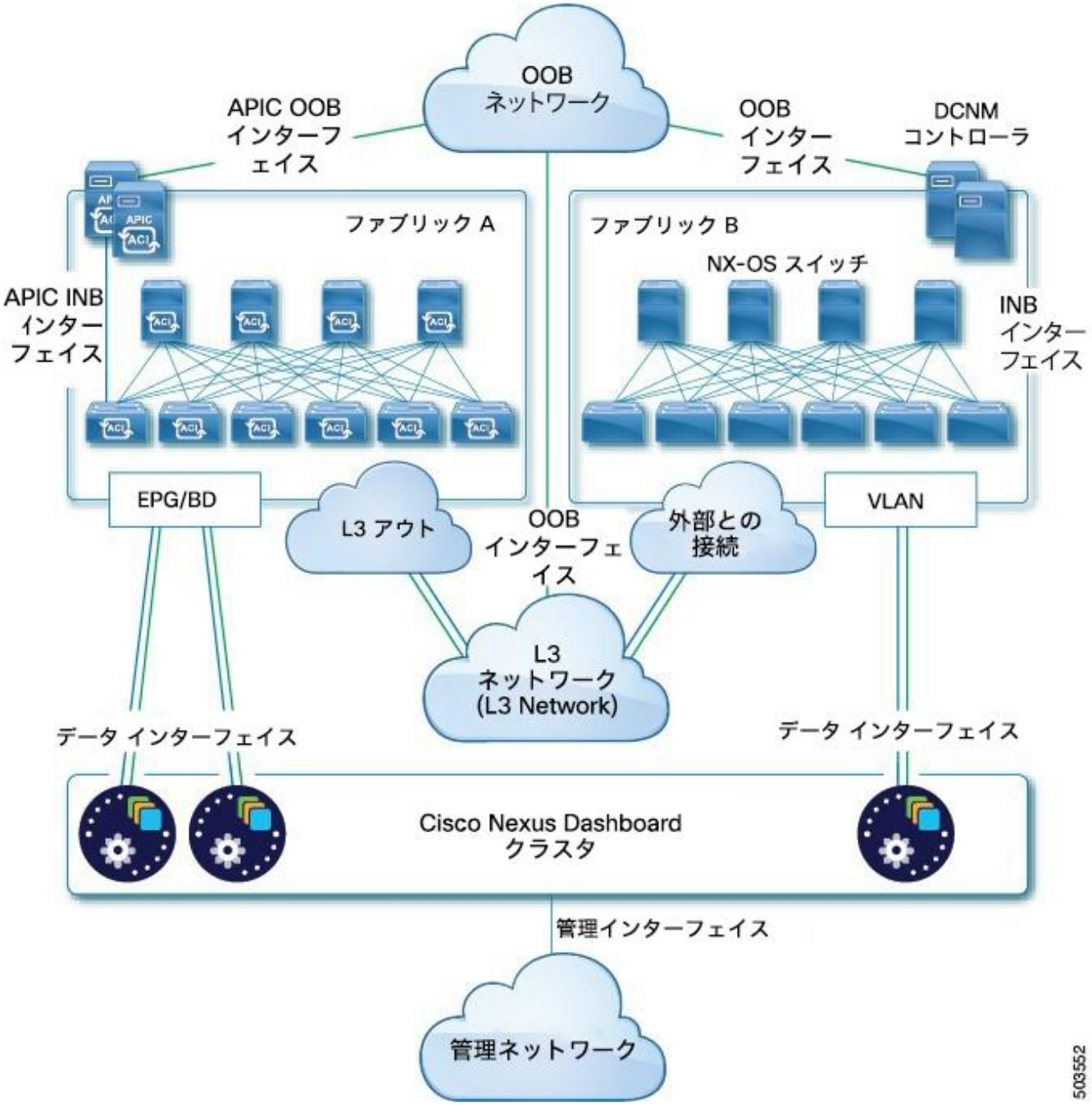


図 5 EPG / BD、Nexus Dashboard Orchestrator を介した接続

GUI の概要

Nexus ダッシュボードクラスタを展開した後、その GUI を使用して残りのすべてのアクションを実行できます。Cisco Nexus Dashboard 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>
```

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。

- **[ホーム（Home）]** ボタンを使用すると、現在表示しているページまたはサービスから **[ワンビュー（One View）]** ページ（次のセクションで説明）に戻ります。
- **[フィードバック（Feedback）]** ボタンを使用すると、ソフトウェアの使用中にフィードバックや提案を送信したり、問題を報告したりできます。
- **[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。
- ***[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、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。

  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。

One View ページ

Nexus Dashboard クラスタにログインすると最初に表示されるページが、**[ワンビュー（One View）]** です。このページには、現在の Nexus Dashboard クラスタのステータス、サイト、サービス、リソース使用状況に関する情報が表示されます。

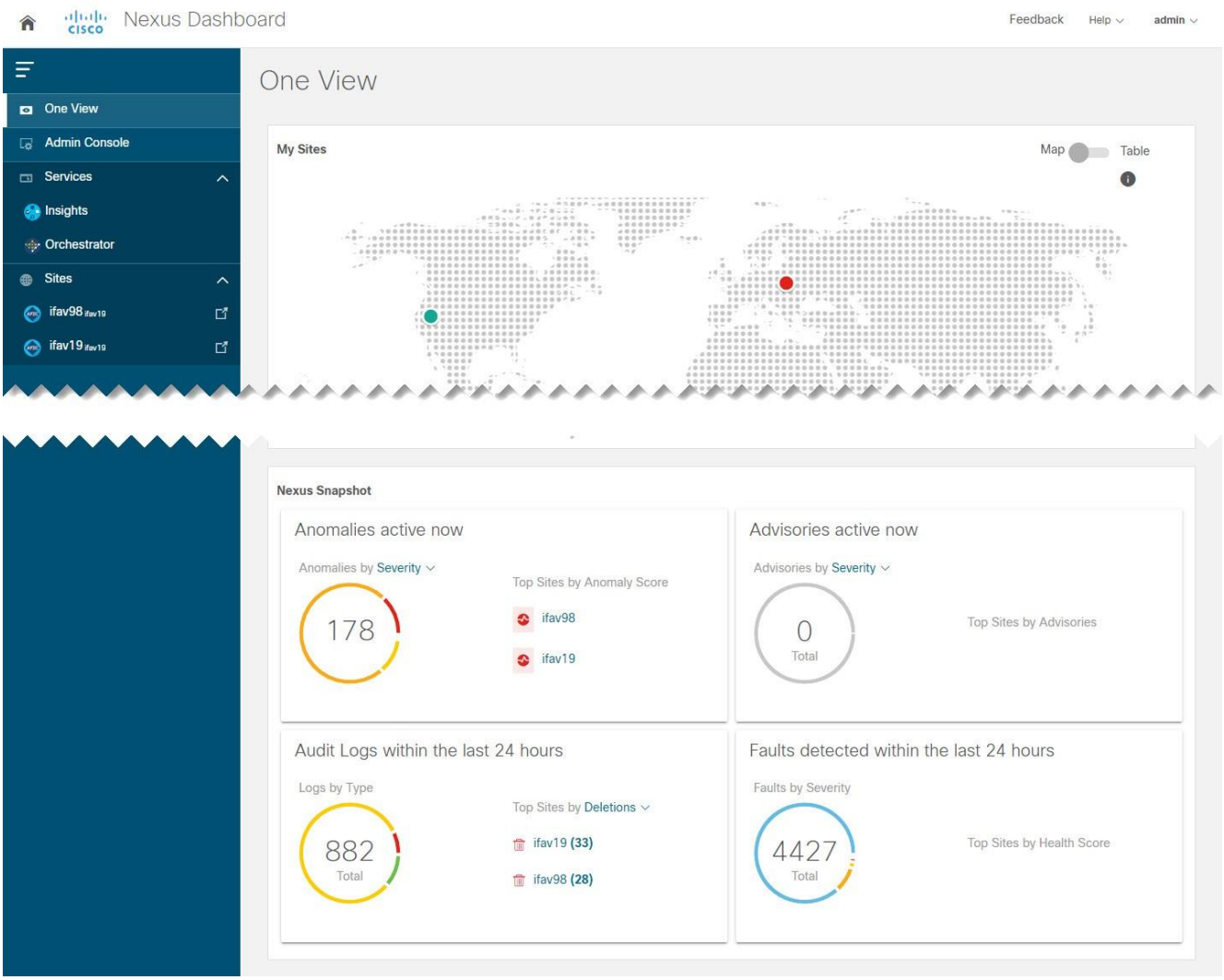


図 6 ワンビュー

ここでは、ダッシュボードユーザーのクラスタ全体(またはマルチクラスタ接続の場合はすべてのクラスタ)のステータス概要を 1 つの場所に表示できます。**Nexus スナップショット**の情報は、Nexus Dashboard Insights サービスでのみ利用できることに注意してください。

UI の左上隅にある **[ホーム（Home）]** アイコンをクリックすると、いつでも [ワンビュー（One View）] ページにアクセスできます。

[管理コンソール（Admin Console）] ページ

ログイン後、[ワンビュー（One View）] ページで **[管理コンソール（Admin Console）]** をクリックすると、Nexus Dashboard クラスタの**管理コンソール**に移動できます。管理コンソールの **[概要（Overview）]** 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、リソース使用状況に関する情報が表示されます。

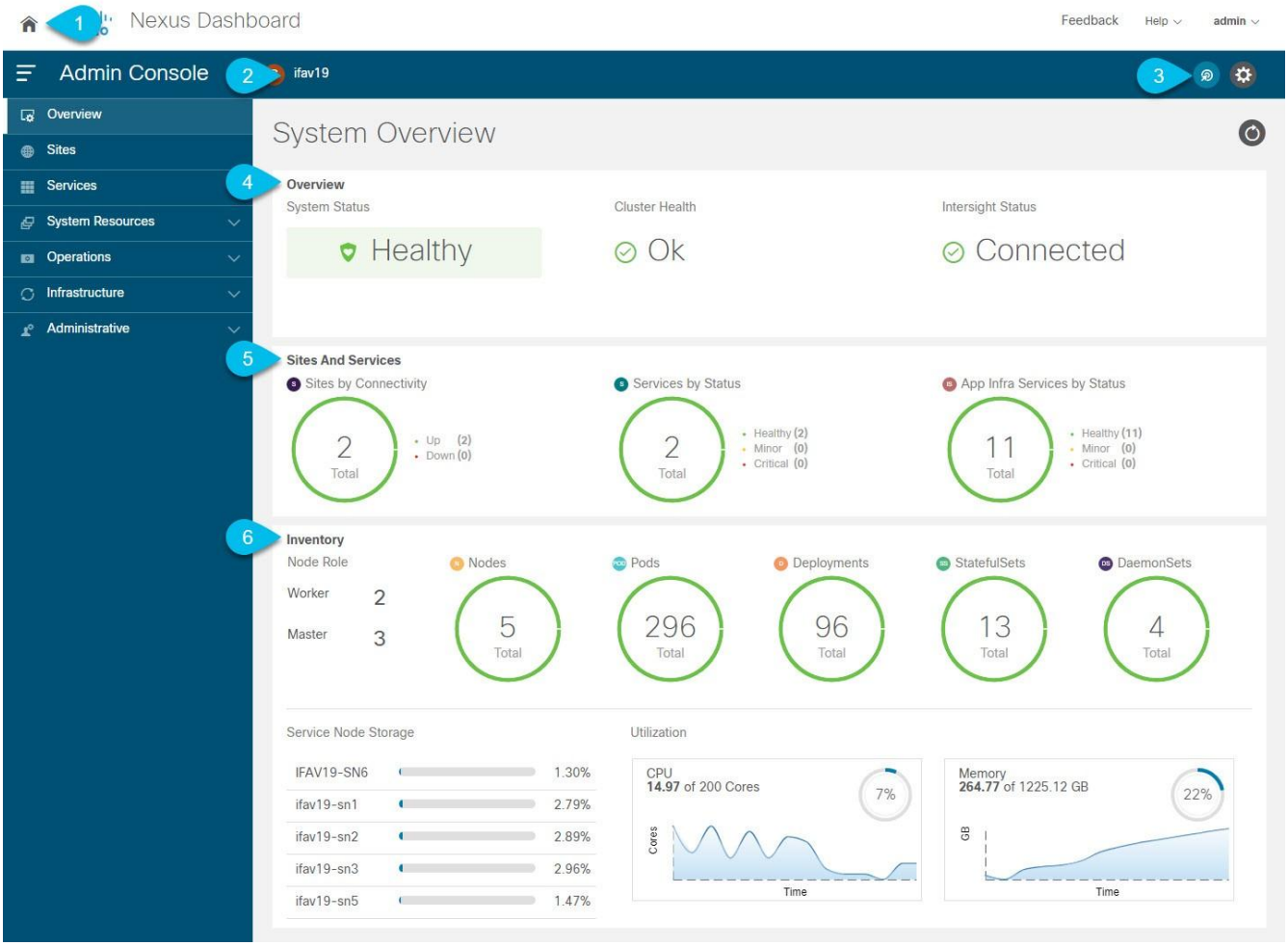


図 7 システムの概要

1. グローバル **[ホーム（Home）]** アイコンから、Nexus Dashboard のホーム画面に簡単に戻ってさまざまなコンポーネント間を移動できます。
    - **[ワンビュー（One View）]** ページ（上で説明済み）は、接続されているすべてのクラスタ、サイト、サービスを単一画面で一元管理（SPOG）できるようにするものです。

      マルチクラスタ展開では、**[ワンビュー（One View）]** にすべてのクラスタで使用可能なリソースとサービスすべてが表示されます。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。

    - **[管理コンソール（Admin Console）]**（上図）で、Nexus Dashboard クラスタを設定および管理できます。
    - **[サービス（Services）]** からは、クラスタで使用可能なすべてのサービスにワンクリックでアクセスできます。

      マルチクラスタ展開では、**[サービス（Services）]** にすべてのクラスタのすべてのサービスが含まれています。

    - **[サイト（Sites）]** は、クラスタにオンボードされているサイトのコントローラ UI にワンクリックでアクセスできるサイトです。

      マルチクラスタ展開では、**[サイト（Sites）]** にすべてのクラスタのすべてのサイトが含まれています。

2. **[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。

   マルチクラスタ展開では、クラスタの名前をクリックして、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。

3. **インテント**アイコンから、サイトやノードの追加、クラスタのアップグレード、ユーザーの作成など、一般的なタスクにアクセスできます。
4. **[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）] ステータスをクリックすると、クラスタ内に問題がある場合に詳細を確認できます。

5. **[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。

6. **[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。

> **[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。

[サイト（Sites）] ページ

左側のナビゲーションペインの **[サイト（Sites）]** 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）]** - オンボーディング時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。

[サービス（Services）] ページ

左側のナビゲーションペインの **[サービス（Services）]** 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。

[システムリソース（System Resources）] ページ

左側のナビゲーションペインの **[システムリソース（System Resources）]** カテゴリには、クラスタを構成するノードやクラスタで使用される Kubernetes API オブジェクトなどのクラスタリソースが表示されます。

カテゴリには、次のサブカテゴリが含まれます。

- **[ノード（Nodes）]** - クラスタ内のすべてのマスターノード、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。
- **[ポッド（Pods）]** - コンピューティングの基本単位であるポッドに関する情報を表示します。

  ポッドは、一緒にスケジュールされ、通常は静的なコンテナのグループです。サービスの展開方法を変更する必要がある場合、既存のポッドの設定を変更する代わりに、新しいポッドが新しい設定で作成され、古いポッドは破棄されます。

- **[名前空間（Namespaces）]** - 他の API オブジェクトのグループを編成するために使用される Kubernetes 名前空間に関する情報を提供します。

  名前空間を使用すると、名前空間内のすべてのオブジェクトを一度に操作したり、特定のユーザーまたはロールへのアクセスを制限したりできます。

- **[サービス（Services）]** - クラスタで実行されているサービス（または動的に変化するポッドとコンテナのセット）に関する情報を表示します。

  各サービスは、複数のポッドとコンテナで構成されます。これらは、クラスタのスケーリングまたはリカバリ中に作成、破棄、または変更される場合がありますが、サービス名をつけることで、基本となる設定に関係なく特定のサービスに静的にアクセスできるようになります。

- 展開、ステートフルセット、およびデーモンセットは、ポッドのセットを展開する方法と場所を説明する方法をサービス開発者に提供します。
  - **[展開（Deployments）]** - オブジェクトの中で最も一般的。展開されるポッドのコピーの数とノードのタイプに関する制約を設定する機能を持つポッドのセットを定義します。
  - **[DaemonSets]** - Kubernetes クラスタ内のすべてのホストで実行されるポッドを定義します。ノードがクラスタに追加されるたびに自動的に作成されます。
  - **[StatefulSets]** - 特定のストレージボリュームを持つ予測可能なホストで実行する必要があるポッドを定義します。これらのポッドがダウンすると、同じ永続的な識別子を使用して同じ場所に再作

成されるため、以前のインカネーションと同じストレージボリュームを使用できます。

[操作（Operations）] ページ

左側のナビゲーションペインの **[操作（Operations）]** カテゴリには、Nexus Dashboard で実行できるアクションが表示されます。

カテゴリには、次のサブカテゴリが含まれます。

- **[ファームウェア管理（Firmware Management）]** - クラスタ（ファームウェア）のアップグレードまたはダウングレードを実行する際に使用します。
- **[テクニカルサポート（Tech Support）]** - テクニカルサポートの収集は管理者が実行できます。
- **[監査ログ（Audit Logs）]** - 監査ログはユーザーがトリガーする設定変更です。
- **[バックアップと復元（Backup and Restore）]** - バックアップおよび復元された設定が表示されます。

[インフラストラクチャ（Infrastructure）] ページ

左側のナビゲーションペインの **[インフラストラクチャ（Infrastructure）]** カテゴリでは、Nexus Dashboard クラスタ、Cisco Intersight コネクタ、アプリケーション インフラ サービスを管理できます。

- **[クラスタ設定（Cluster 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）を設定できし、クラスタの現在の問題があれば表示します。
- **[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。
- **[Intersight]** - Cisco Intersight デバイスコネクタ設定にアクセスできます。

  Cisco NI サービスは、サービスノードで設定および使用可能なサービスを Intersight Device Connector に依存します。

- **[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。

[管理（Administrative）] ページ

左側のナビゲーションペインの **[管理（Administrative）]** カテゴリで、認証とユーザーを管理できます。

- **[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。
- **[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。
- **[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。

サイト管理

Cisco Nexus Dashboard を使用すると、複数の CiscoACI、Cisco NDFC または DCNM ファブリックを個別のサイトとして同じクラスタにオンボードできます。ファブリックがオンボードされると、同じ Cisco Nexus Dashboard クラスタで実行されているアプリケーションで使用できるようになります。

サイトを追加するには、そのコントローラのインバンドまたはアウトオブバンドの IP アドレスとログイン情報が必要です。サイトのオンボーディングに使用する IP アドレスのタイプは、サイトを使用する Nexus ダッシュボードサービスによって異なります。詳細については、次のセクションで説明します。Cisco Nexus Dashboard クラスタに追加されたサイトは、デフォルトではサービスで有効化されていないため、各サービスの GUI から直接明示的に有効化する必要があります。

Nexus Dashboard に 1 つ以上のサイトをオンボードした後、左側のナビゲーションサイドバーから **[サイト（Sites）]** を選択すると、オンボードしたサイトを Nexus Dashboard GUI で表示できます。**[サイト（Sites）]** ページでサイト名の横にある **[開く（Open）]** リンクをクリックして、サイトの GUI を直接起動することもできます。

リモート認証を使用して Nexus Dashboard にログインし、起動するサイトで同じログインドメインとユーザーが設定されている場合は、再認証することなくサイトの GUI に自動的にログインできます。

サイトの追加

はじめる前に

- ファブリック接続がすでに設定されている必要があります。
- Cisco APIC または Cloud APIC サイトを追加する場合は、サイトでリリース 4.2(4)以降を実行している必要があります。
- Cisco APIC サイトを追加する場合は、Cisco Nexus Dashboard データネットワークの IP 接続用の EPG/L3Out を事前に設定する必要があります。

  詳細については、「ファブリック接続」を参照してください。

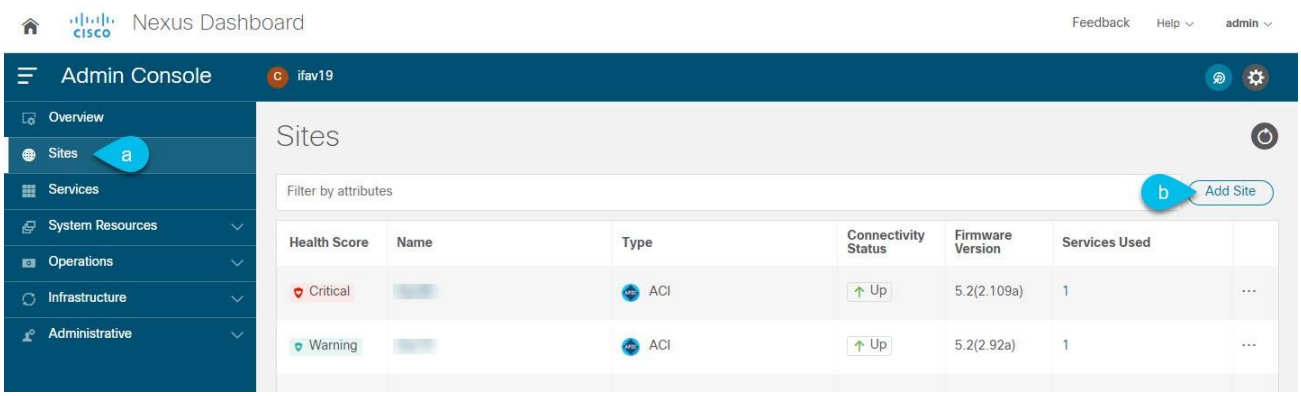
- Cisco APIC サイトを追加し、Cisco NIR アプリケーションを展開する場合は、次のことに注意してください。
  - Cisco Nexus Dashboard からデータネットワークを介した Cisco APIC インバンド IP への IP 接続を設定する必要があります。
  - Cisco Nexus Dashboard からリーフノードおよびスパインノードのインバンド IP への IP 接続を設定する必要があります。
- Cisco NDFC または DCNM サイトを追加するには、次のことに注意してください。
  - サイトはリリース 11.5(1)以降を実行している必要があります。
  - ファブリックとスイッチへのレイヤ 3 接続を設定する必要があります。
  - クラスタが AWS または Azure に展開されている場合は、データインターフェイスでインバウンドルールを設定する必要があります。

    これは通常、最初のクラスタ展開中に行われ、「 *Cisco Nexus Dashboard Deployment Guide*」で詳細に説明されています。

サイトを追加するには、次の手順を実行します。

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。

2. メイン ナビゲーション メニューから、**[管理コンソール（Admin Console）]** を選択します。
3. サイトを追加します。

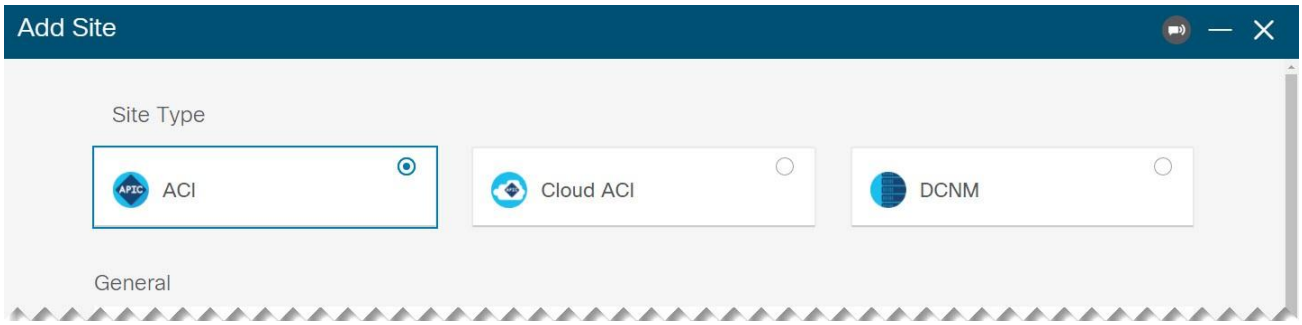


   a. メイン ナビゲーション メニューから **[サイト（Sites）]** を選択します。
   b. メインペインの右上にある **[サイトの追加（Add Site）]** をクリックします。

      [サイトの追加（Add Site）] 画面が開きます。

4. 追加するサイトのタイプを選択します。

   Cisco Nexus Dashboard は、3 種類のファブリックすべてのオンボーディングをサポートしますが、サービスと互換性のある特定のファブリックタイプとバージョンについては、「*サービス互換性マトリックス*」を参照してください。



   - **ACI** - Cisco APIC によって管理されるオンプレミス ACI サイト向け
   - **クラウド ACI** - Cisco Cloud APIC によって管理されるクラウド ACI サイト向け
   - **DCNM** - Cisco NDFC または DCNM によって管理されるオンプレミスサイト向け

5. サイトの情報を入力します。
   a. ACI サイトを追加する場合は、次の情報を入力します。
      - **[サイト名（Site Name]** - このサイトを参照するときに Nexus Dashboard の GUI 全体で使用されます。
      - **[ホスト名（Host Name）]/[IP アドレス（IP Address）]** - Cisco APIC との通信に使用されます。

        このサイトを Nexus Dashboard Orchestrator サービスでのみ使用する場合、APIC のインバンドまたはアウトオブバンド IP アドレスを指定できます。Nexus Dashboard Insights でもこのサイトを使用する場合は、インバンド IP アドレスを指定する必要があります。

        アドレスを指定する場合、URL 文字列の一部としてプロトコル（http:// または https://）を含めないでください。追加すると、サイトの追加に失敗します。

- **[ユーザー名（User Name）]と[パスワード（Password）]** - 追加するサイトで管理者権限を持つユーザーのログイン情報。
- (任意) **[ログインドメイン（Login Domain）]** - このフィールドを空白にすると、サイトのローカルログインが使用されます。
- (任意) **[インバンド EPG（In-Band EPG）]** - EPG およびブリッジドメインを介して ACI ファブリックに接続する場合は入力する必要があります。ファブリック接続の詳細については、「ファブリック接続」を参照してください。

  Nexus Dashboard Insights サービスでこのサイトを使用する場合は、ノード管理のインバンド EPG を指定する必要があります。

b. クラウド ACI サイトを追加する場合は、次の情報を入力します。

- **[サイト名（Site Name）]** - このサイトを参照するときに Nexus Dashboard の GUI 全体で使用されます。
- **[ホスト名（Host Name）]/[IP アドレス（IP Address）]** - Cisco クラウド APIC との通信に使用されます。

  アドレスを指定する場合、URL 文字列の一部としてプロトコル（http:// または https://）を含めないでください。追加すると、サイトの追加に失敗します。
- **[ユーザー名（User Name）]と[パスワード（Password）]** - 追加するサイトで管理者権限を持つユーザーのログイン情報。
- (任意) **[ログインドメイン（Login Domain）]** - このフィールドを空白にすると、サイトのローカルログインが使用されます。
- (任意)**[プロキシの有効化（Enable Proxy）]** - クラウドサイトにプロキシ経由でアクセスできる場合は、この設定を有効にします。

  プロキシは、Nexus Dashboard のクラスタ設定ですでに設定されている必要があります。プロキシが管理ネットワーク経由で到達可能な場合は、プロキシ IP アドレスに対して静的管理ネットワークルートも追加する必要があります。プロキシとルートの設定の詳細については、「クラスタ 設定」を参照してください。

c. DCNM サイトを追加する場合は、次の情報を入力します。

- **[ホスト名（Host Name）]/[IP アドレス（IP Address）]** - Cisco NDFC または DCNM との通信に使用されます。

  これは DCNM のインバンド IP アドレスである必要があります。

  アドレスを指定する場合、URL 文字列の一部としてプロトコル（http:// または https://）を含めないでください。追加すると、サイトの追加に失敗します。
- **[ユーザー名（User Name）]と[パスワード（Password）]** - 追加するサイトで管理者権限を持つユーザーのログイン情報。
- **[DCNM 上のサイト（Sites on DCNM）]** - **[サイトの追加（Add Sites）]**をクリックして、指定したコントローラで管理される DCNM ファブリックを選択します。

6. **[追加（Add）]** をクリックして、サイトの追加を終了します。
7. （任意）**[地理的位置（Geographical Location）]** マップをクリックして、サイトの場所を指定します。
8. (任意)他にも追加するサイトがあれば、上記の手順を繰り返します。

サイトの編集

拠点を編集するには、次の手順を実行します。

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. メイン ナビゲーション メニューから、**[管理コンソール（Admin Console）]** を選択します。
3. メイン ナビゲーション メニューから **[サイト（Sites）]** を選択します。
4. 編集するサイトの **[アクション（Actions）]**（**...**）メニューから、**[サイトの編集（Edit Site）]** を選択します。

   [サイトの編集（Edit Site）] 画面が開きます。

5. **[サイトの編集（Edit Site）]** ウィンドウで必要な変更を加えます。
   - セキュリティドメインを削除するには、既存のドメインの横にある **[削除（Delete）]** アイコンをクリックします。
   - 1 つ以上のセキュリティドメインを追加するには、**[+セキュリティドメインの追加（+Add Security Domain）]** をクリックします。
   - サイトを再プロビジョニングするには、**[サイトの再登録（Re-register Site）]** チェックボックスをオンにして、必要な情報を入力します。

     Nexus Dashboard Orchestrator で使用される Cisco Cloud APIC サイトで Cloud APIC のパブリック IP アドレスが変更された場合、サイトの再登録が必要になる場合があります。

     Orchestrator サービスによって管理される DCNM ファブリックの IP アドレス情報を変更した場合にも、このオプションを使用できます。

     Nexus Dashboard Insights サービスでは、サイトの再登録はサポートされていません。
6. **[保存 (Save)]** をクリックして、変更内容を保存します。

サイトの削除

はじめる前に

- Nexus Dashboard にインストールされているアプリケーションでサイトが使用されていないことを確認します。

  サイトを削除すると、そのサイトを使用しているすべてのアプリケーションが中断されます。
- Cisco ACI ファブリックがサイトとして Nexus Dashboard に追加されている場合、いくつかのポリシーが Cisco APIC で作成されている可能性があります。オンボードされているサイトを削除することなく Nexus Dashboard をクリーンリブートしても、Cisco APIC で作成されたポリシーは削除されません。Cisco APIC でこれらのポリシーをクリーンアップするには、サイトを再度追加して削除する必要があります。

1 つまたは複数のサイトを削除するには、次の手順を実行します。

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. メイン ナビゲーション メニューから、**[管理コンソール（Admin Console）]** を選択します。
3. メイン ナビゲーション メニューから **[サイト（Sites）]** を選択します。
4. 削除するサイトの **[アクション（Actions）]**（**...**）メニューから、**[サイトの削除（Remove Site）]** を選択します。
5. **[削除の確認（Confirm Delete）]** ウィンドウに、サイトのログイン情報を入力します。
6. **[OK]** をクリックしてサイトを削除します。

サービス管理

Cisco Nexus Dashboard を使用すると、**[サービス（Services）]** GUI ページから、すべてのサービスのライフサイクル全体を管理できます。このページでは、Cisco DC App Center を探索し、Nexus Dashboard で使用可能なすべてのサービスを把握することもできます。

App Store を使用したサービスのインストール

[App Store]画面では、Cisco DC App Center からサービスを直接展開できます。

はじめる前に

- サービスをインストールするには管理者権限が必要です。
- Cisco DC App Center は、管理ネットワークを介して直接、またはプロキシ設定を使用して Nexus Dashboard から到達可能である必要があります。

  プロキシの設定については、「クラスタ設定」を参照してください。

- App Store を使用してインストールできるのは、最新バージョンのサービスのみであることに注意してください。

  App Store で入手可能な最新バージョンより前のバージョンのサービスをインストールするには、「サービスの手動インストール」で説明されている手順に従って手動インストールします。

- サービスをインストールする前に、クラスタが正常であることを確認してください。

App Store からサービスをインストールするには、次の手順を実行します。

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. **App Store** からサービスをインストールします。

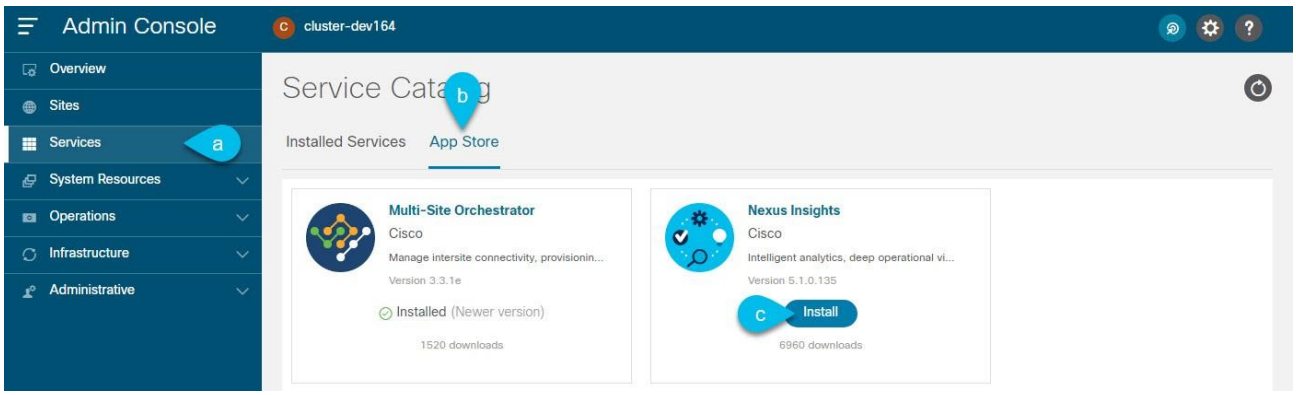


図 8 App Store からのサービスのインストール

a. メイン ナビゲーション メニューから **[サービス（Services）]** を選択します。
b. メインペインで、**[App Store]** タブを選択します。
c. インストールするサービスのタイルで、**[インストール（Install）]** をクリックします。

   Nexus Dashboard は、Cisco DC App Center からサービスを直接ダウンロードし、インストールします。プロセスが完了すると、サービスが **[サービス（Services）]** ページで使用可能になります。

   サービスによっては、最長 20 分かかる場合があります。

3. サービスを開始します。

   デフォルトでは、サービスがインストールされた後は無効な状態のままです。「サービスの有効化」で説明されている手順に従って、有効化します。

   サービスによっては、最長 20 分かかる場合があります。

サービスの手動インストール

または、DC App Center からサービスを手動でダウンロードし、 Nexus Dashboard にアップロードしてインストールすることもできます。

はじめる前に

- サービスをインストールするには管理者権限が必要です。
- サービスをインストールする前に、クラスタが正常であることを確認してください。

サービスを手動でインストールするには、次の手順を実行します。

1. サービスのイメージをダウンロードします。
   a. Cisco DC App Center にアクセスします。
   b. **[アプリケーションの検索...（Search for apps...）]** フィールドに、ダウンロードするサービスの名前を入力し、Enter を押します。

      たとえば、「ネットワークインサイト」です。

   c. 検索結果ページで、サービスをクリックします。
   d. そのサービスのページで、**[ダウンロード（Download）]** をクリックします。
   e. **[ライセンス契約（License Agreement）]** ウィンドウで、**[同意してダウンロード（Agree and download）]** をクリックします。

      これにより、サービスのイメージファイルがシステムにダウンロードされます。
2. Nexus Dashboard の GUI にログインします。
3. メイン ナビゲーション メニューから、**[管理コンソール（Admin Console）]** を選択します。
4. サービスイメージをアップロードします。
   a. メイン ナビゲーション メニューから **[サービス（Services）]** を選択します。
   b. メインペインの右上で **[アクション（Actions）]** メニューをクリックし、**[アプリのアップロード（Upload App）]** を選択します。
   c. ダウンロードしたイメージファイルを選択します。

      http サービスまたはローカルマシンからサービスをアップロードすることもできます。

      ローカルイメージをアップロードするには、**[ローカル（Local）]** を選択し、**[ファイルの選択（Choose File）]** をクリックして、ローカルシステムにダウンロードしたサービスイメージを選択します。

      リモートサーバを使用するには、[リモート（Remote）] を選択し、イメージファイルの URL を指定します。

イメージに http URL を指定する場合は、.nap ファイルを解釈せずにそのまま提供するよう Web サーバーを構成する必要があります。通常、これは Web サーバーの httpd.conf 構成ファイルの次の行に拡張を含めることを意味します：AddType application/x-gzip .gz .tgz **.nap**

d. **[アップロード（Upload）]** をクリックしてアプリケーションをアップロードします。

サービスによっては、最長 20 分かかる場合があります。

5. アップロードおよび初期化プロセスが完了するまで待ちます。
6. サービスを開始します。

デフォルトでは、サービスがインストールされた後は無効な状態のままです。「サービスの有効化」で説明されている手順に従って、有効化します。

サービスによっては、最長 20 分かかる場合があります。

サービスの有効化

デフォルトでは、インストールしたサービスは無効な状態です。ここでは、サービスを有効にする方法について説明します。

はじめる前に

- AppStore を使用したサービスのインストールまたはサービスの手動インストールの説明に従ってサービスをインストールしておく必要があります。
- 「クラスタの設定」で説明されているように、ユースケースに適した Network Scale パラメータを設定しておく必要があります。
- サービスを有効にする前に、クラスタが正常であることを確認してください。

サービスを有効にするには、次の手順を実行します。

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. メイン ナビゲーション メニューから **[サービス（Services）]** を選択します。
3. サービスのタイルで、**[開始（Start）]** をクリックします。

リリース 2.2(1)より前のリリースでは、Nexus Dashboard クラスタにサービスをインストールして有効にした場合、その特定のサービスに必要なクラスタリソース(CPU の数とメモリとストレージの量)を定義するサービス展開プロファイルを選択する必要がありました。

リリース 2.2(1)以降、リソースプロファイルの選択は、展開のユースケースに直接関連するいくつかのより直感的なパラメータに削減されました。スイッチやフローの数などのこれらのパラメータは、ファブリックのサイズとユースケースの意図を記述し、クラスタがサービスに必要なリソースをインテリジェントに決定できるようにします。パラメータは「ネットワークスケール」として分類され、サービスを展開する前に[クラスタの設定]画面で指定する必要があります。

さらに、サービスが特定の **App Infra Services** プロファイルを必要とする場合、クラスタは、アプリケーションを開始する前に、要件を満たすためにそのインフラサービスを自動的に更新して再起動します。

クラスタにサービスの実行に必要なリソースが含まれていない場合、サービスは容量削減プロファイルを提供する場合があります。これは、容量削減モードでサービスを実行するかどうかを選択できます。

ただし、開始しようとしているサービスが Nexus Dashboard バージョンと互換性がない場合、またはクラスタサイズが容量削減モードでもサービスを実行するには不十分な場合、クラスタはエラーを返し、そのサービスを開始できません。クラスタの容量が原因でサービスを有効にできない場合は、そのサービスを開始する前に、追加のワーカーノードを展開する必要がある場合があります。

サービスの更新

サービスの更新プロセスは、「App Store を使用した サービスのインストール」または「サービスの手動インストール」で説明されているように、最初の展開プロセスと似ています。

既存のサービスの新しいバージョンをアップロードすると、**[サービス（Services）]** 画面のサービスタイルの **[...]** メニューから使用可能なバージョンのいずれかを選択できます。

既存のサービスを更新するには、次を実行します。

1. 「App Store を使用したサービスのインストール」または「サービスの 手動インストール」の説明に従って、新しいバージョンを展開します。
2. Nexus Dashboard GUI の **[サービス（Services）]** 画面に移動します。
3. 該当するサービスのタイルの **[(...)]** メニューをクリックし、**[利用可能なバージョン（Available Version）]** を選択します。

   または、該当するサービスタイルでバージョン番号をクリックしても、同じメニューを開くことができます。

4. [利用可能なバージョン（Available Version）] ウィンドウが開いたら、新しいバージョンの横にある **[有効化（Activate）]** をクリックします。

サービスの無効化

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. メイン ナビゲーション メニューから **[サービス（Services）]** を選択します。

   Nexus Dashboard にインストールされているすべてのサービスがここに表示されます。

3. 該当するサービスのタイルの **[(...)]** メニューをクリックし、**[無効化（Disable）]** を選択してサービスを無効化します。

サービスの再起動

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. メイン ナビゲーション メニューから **[サービス（Services）]** を選択します。

   Nexus Dashboard にインストールされているすべてのサービスがここに表示されます。

3. 該当するサービスのタイルの **[(...)]** メニューをクリックし、**[再起動（Restart）]** を選択してサービスを再起動します。

サービスのアンインストール

はじめる前に

サービスを削除する前に、サービスを無効にする必要があります。

1. Nexus Dashboard の GUI にログインします。
2. メイン ナビゲーション メニューから **[サービス（Services）]** を選択します。

   Nexus Dashboard にインストールされているすべてのサービスがここに表示されます。
3. 該当するサービスのタイルの **[(...)]** メニューをクリックし、**[削除（Delete）]** を選択してサービスを削除します。

動作

ファームウェア管理（クラスタアップグレード）

ここでは、さまざまなファームウェアバージョンを管理し、クラスタのアップグレードを実行する方法について説明します。

アップグレードプロセスでは、新しいイメージをアップロードしてから展開します。クラスタファームウェアのダウングレードにも同じワークフローを使用できます。

このリリースの Nexus Dashboard では、ダウングレードがサポートされていません。以前のリリースにダウングレードするには、新しいクラスタを展開してアプリケーションを再インストールする必要があります。

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変更、ガイドライン、および問題については、対象のリリースの *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 Dashboard フォーム ファクタで同じです。

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

- 現在の Nexus Dashboard クラスタが正常であることを確認します。

  Nexus Dashboard GUI の [システム概要（System Overview）] ページでシステムのステータスを確認するか、rescue-user としてノードの 1 つにログインし、acs health コマンドを実行します。

- 「設定のバックアップの作成」の説明に従って、既存の設定をバックアップします。
- アップグレードが進行中は、ワーカーノードやスタンバイノードを追加するなど、クラスタの設定を変更してはいけません。
- このリリースの Nexus Dashboard では、ダウングレードがサポートされていません。

  以前のリリースにダウングレードするには、新しいクラスタを展開してアプリケーションを再インストールする必要があります。

イメージの追加

Nexus Dashboard クラスタをアップグレードする前に、GUI を使用してアップグレードイメージを追加して、使用できるようにする必要があります。

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

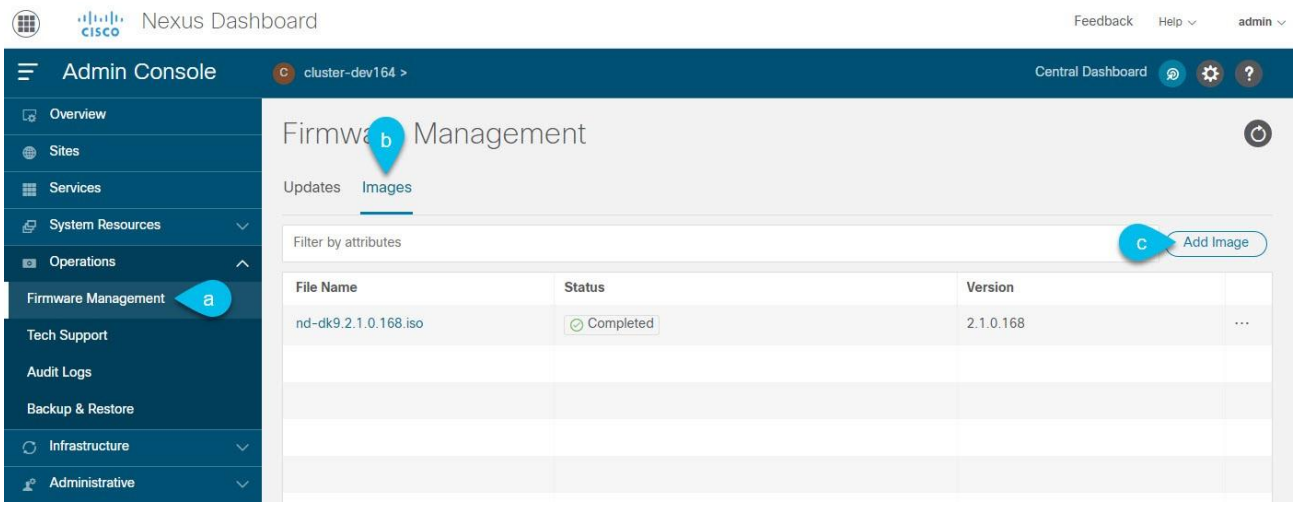
   b. ダウンロードする Nexus Dashboard のバージョンを選択します。
   c. Cisco Nexus Dashboard イメージ(nd-dk9.<version>.iso)をダウンロードします。

最初のクラスタ展開に VMware ESX .ova、Linux KVM .qcow2、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の .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。

2. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
3. イメージを追加します。



a. メイン ナビゲーション メニューから、**[操作（Operations）] > [ファームウェア管理（Firmware Management）]** を選択します。

b. メインペインで、**[イメージ（Images）]** タブを選択します。

ページには、以前に追加されたイメージが一覧表示されます。

c. メインペインの右上で、**[アクション（Actions）]** メニューをクリックし、**[イメージの追加（Add Image）]** をクリックします。

4. **[ファームウェアイメージの追加（Add Firmware Image）]** ウィンドウが表示されたら、イメージをリモートサーバーまたはローカルシステムのどちらに保存するかを選択します。

a. リモートイメージを指定する場合は、イメージの完全な **URL** を指定します。

b. ローカルイメージをアップロードする場合は、**[ファイルの選択（Choose File）]** をクリックし、ローカルシステムからイメージファイルを選択します。

ローカルマシンからアップロードする場合、アップロード速度が遅いとセッションがタイムアウトし、転送が中断される可能性があります。少なくとも 40Mbps のアップロード速度と、セッションタイムアウトを(デフォルトの 1200 から)1800 秒に増やすことをお勧めします。セッションタイムアウトは、Nexus Dashboard GUI の **[管理（Administrative）] > [セキュリティ（Security）]** ページで変更できます。

5. **[アップロード（Upload）]** をクリックして、イメージをアップロードします。

[イメージ（Images）] タブにイメージのアップロードの進行状況が表示されます。完了を待ってから、次のセクションに進みます。

クラスタのアップグレード

はじめる前に

「イメージの追加」の説明に従って、アップグレードイメージが Nexus Dashboard クラスタに追加されている必要があります。

クラスタをアップグレードするには、次の手順を実行します。

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. 更新を開始します。
   a. メイン ナビゲーション メニューから、**[操作（Operations）] > [ファームウェア管理（Firmware Management）]** を選択します。
   b. メインペインで、**[更新（Updates）]** タブを選択します。
   c. **[更新のセットアップ（Set up Update）]** または **[詳細の変更（Modify Details）]** をクリックします。

      クラスタを初めてアップグレードする場合は、ページの中央にある **[更新のセットアップ（Setup Update）]** ボタンをクリックします。

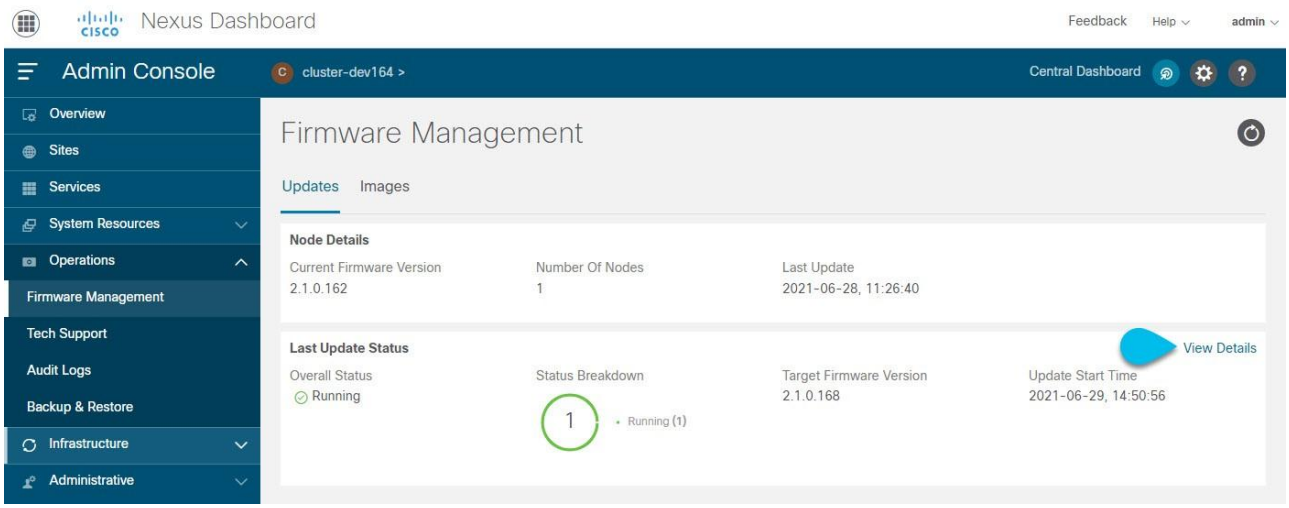
      以前クラスタをアップグレードした場合は、**[更新のセットアップ（Setup Update）]** ボタンではなく、最後のアップグレードの詳細がこのページに表示されます。この場合、画面の右上にある **[詳細の変更（Modify Details）]** ボタンをクリックします。
3. **[セットアップ/バージョンの選択（Setup/Version Selection）]** 画面で、対象バージョンを選択し、**[次へ（Next）]** をクリックして続行します。

   Nexus ダッシュボードに複数の画像をアップロードした場合は、それらがここに表示されます。
4. **[セットアップ/確認（Setup/Confirmation）]** 画面で更新の詳細を確認し、**[インストールの開始（Begin Install）]** をクリックして続行します。

   画面が **[インストール（Install）]** タブに進み、各ノードの進行状況を確認できます。

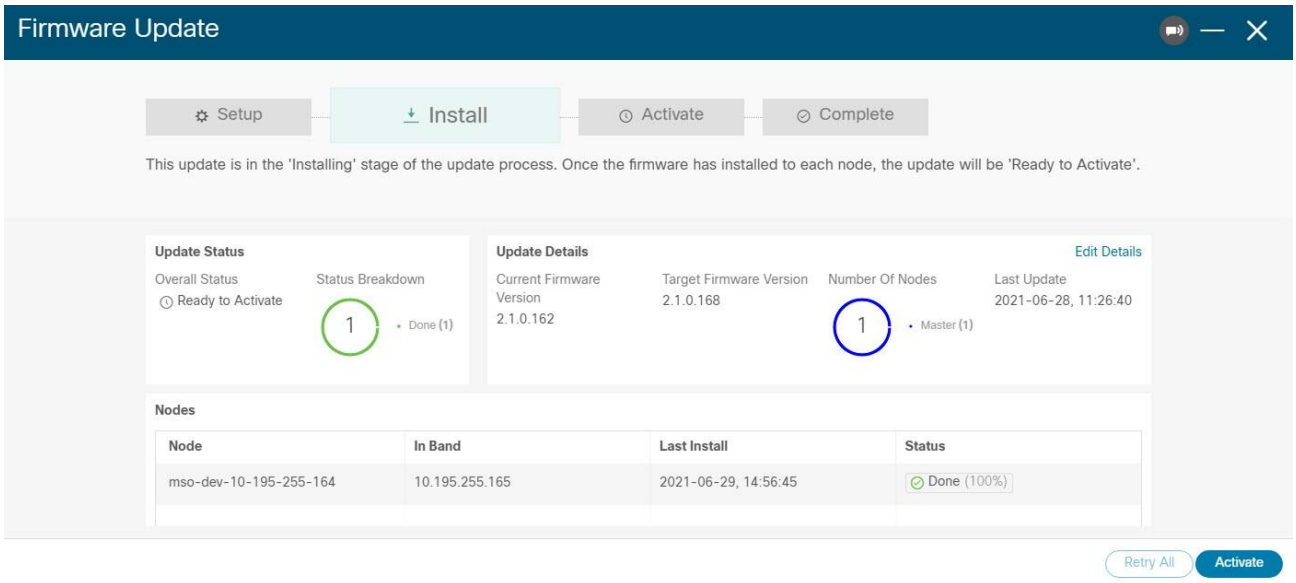
   このプロセスには最長 20 分かかることがあり、その間はこの画面から移動できます。
5. イメージのインストールが完了するまで待ちます。

   インストールステータスを確認するには、**[操作（Operations）] [ファームウェア管理（Firmware Management）]**画面に戻り、**[最終ステータス（Last Status）]**タイルの**[詳細の表示（View Details）]**リンクをクリックします。



6. **[有効化（Activate）]** をクリックします。

   インストール画面から移動した場合は、**[操作（Operations）] > [ファームウェア管理（Firmware Management）]** 画面に戻り、**[最新ステータス（Last Status）]** タイルの **[詳細の表示（View Details）]** リンクをクリックします。



   すべてのクラスタサービスが開始するまでさらに最長 20 分かかる場合があります。このプロセス中は GUI が使用できなくなることがあります。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。以下に示すように、**[アクティブ化（Activate）]** 画面でアクティブ化プロセスを追跡できます。

イメージの削除

Nexus Dashboard では、アップロードしたファームウェアイメージが保持されます。いずれかのイメージを(たとえば、古いアップグレードから)削除する場合は、次の手順を実行できます。

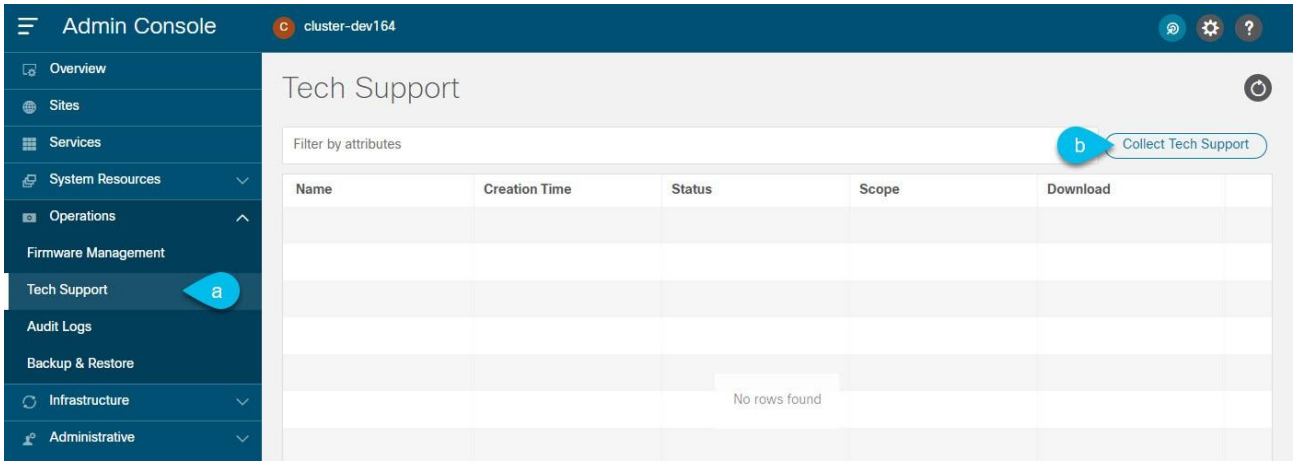
1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. メイン ナビゲーション メニューから、**[操作（Operations）] > [ファームウェア管理（Firmware Management）]** を選択します。
3. メインペインで、**[イメージ（Images）]** タブを選択します。
4. 削除するイメージの横にある **[アクション（Actions）]**（[...]）メニューをクリックし、**[イメージの削除（Delete Image）]** を選択します。
5. メインペインの右上で、**[アクション（Actions）]** メニューをクリックし、**[イメージの削除（Delete Image）]** を選択します。
6. **[削除の確認（Confirm Delete）]** プロンプトで、**[OK]** をクリックして確定します。

テクニカルサポート

テクニカルサポート機能により、ユーザーはシステムのログとアクティビティ情報を収集して Cisco TAC による詳細なトラブルシューティングに備えることができます。Cisco Nexus Dashboard は、ベストエフォートのテクニカルサポート収集機能を備えており、個々のノード、クラスタ全体、またはアプリケーションのテクニカルサポート情報をダウンロードできます。テクニカルサポートファイルは Cisco Nexus Dashboard でホストされており、いつでもダウンロードできます。

テクニカルサポート情報を収集するには、次の手順を実行します。

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. テクニカルサポートを収集します。



a. メイン ナビゲーション メニューから、**[操作（Operations）] > [テクニカルサポート（Tech Support）]** を選択します。

b. メインペインの右上で、**[アクション（Actions）]** メニューをクリックし、**[テクニカルサポートの収集（Collect Tech Support）]** を選択します。

3. **[テクニカルサポートの収集（Collect Tech Support）]** ウィンドウが開いたら、説明を入力します。
4. **[範囲（Scope）]** ドロップダウンから、テクニカルサポート情報を収集するカテゴリを選択します。
   - [システム（System）]は、インフラストラクチャのテクニカルサポート情報を収集します。
   - [App Store] は、App Store のテクニカルサポート情報を収集します。
   - サービス固有の選択は、その特定のサービスのテクニカルサポート情報を収集します。
5. **[収集（Collect）]** をクリックします。

   テクニカルサポートの収集を開始すると、同じ画面で進行状況を確認できます。

   何らかの理由でテクニカルサポートの収集プロセスに失敗した場合は、各ノードに rescue-user としてログインし、acs techsupport collect コマンドのいずれかを実行して、同じ情報を取得することもできます。特定の techsupport collect コマンドオプションの詳細については、「便利なコマンド」を参照してください。

6. テクニカルサポートアーカイブをダウンロードします。

   収集が完了したら、横の **[ダウンロード（Download）]** をクリックしてアーカイブをダウンロードできます。

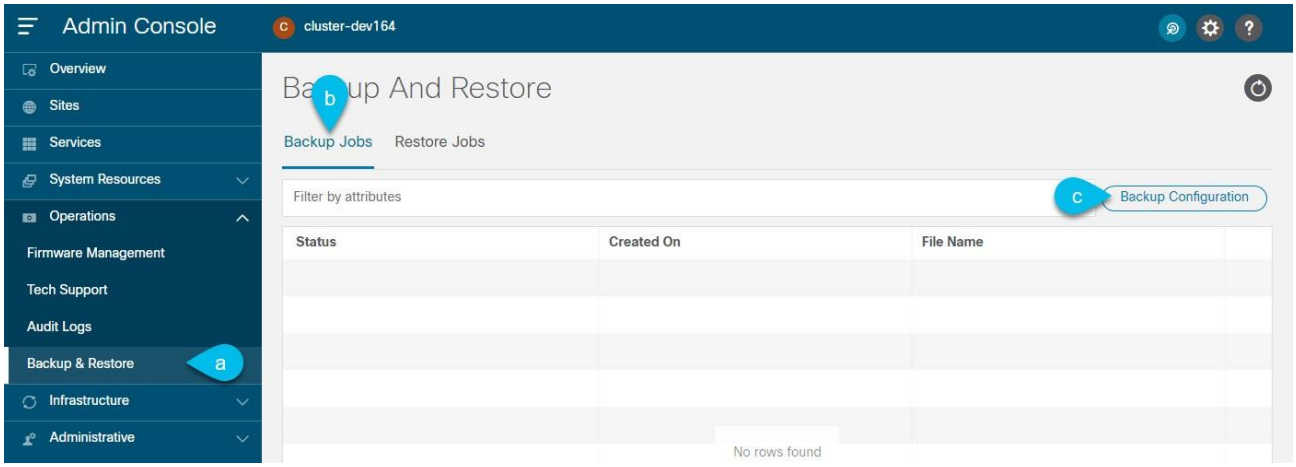
既存のテクニカル サポート パッケージを削除するには、**[テクニカルサポート（Tech Support）]** 画面でパッケージを選択し、**[アクション（Actions）]** メニューから **[テクニカルサポートの削除（Delete Tech Support）]** を選択します。

バックアップと復元

ここでは、Nexus Dashboard クラスタの設定をバックアップまたは復元する方法について説明します。

設定のバックアップの作成

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. バックアップを開始します。



a. メイン ナビゲーション メニューから、**[操作（Operations）] > [バックアップと復元（Backups & Restore）]** を選択します。

b. メインペインで、**[バックアップジョブ（Backup Jobs）]** タブを選択します。

c. メインペインの右上で、**[バックアップ設定（Backup Configuration）]** をクリックします。

3. **[バックアップ設定（Backup Configuration）]** ウィンドウが開いたら、**[暗号化キー（Encryption Key）]** と **[ファイル名（File Name）]** を入力します。

   暗号化キーはアーカイブの暗号化に使用され、8 文字以上にする必要があります。

4. **[ダウンロード（Download）]** をクリックしてバックアップを開始します。

Cisco Nexus Dashboard は設定のバックアップまたは暗号化キーを保存しないため、Nexus Dashboard クラスタ外でそれらをダウンロードして維持する必要があります。

設定の復元

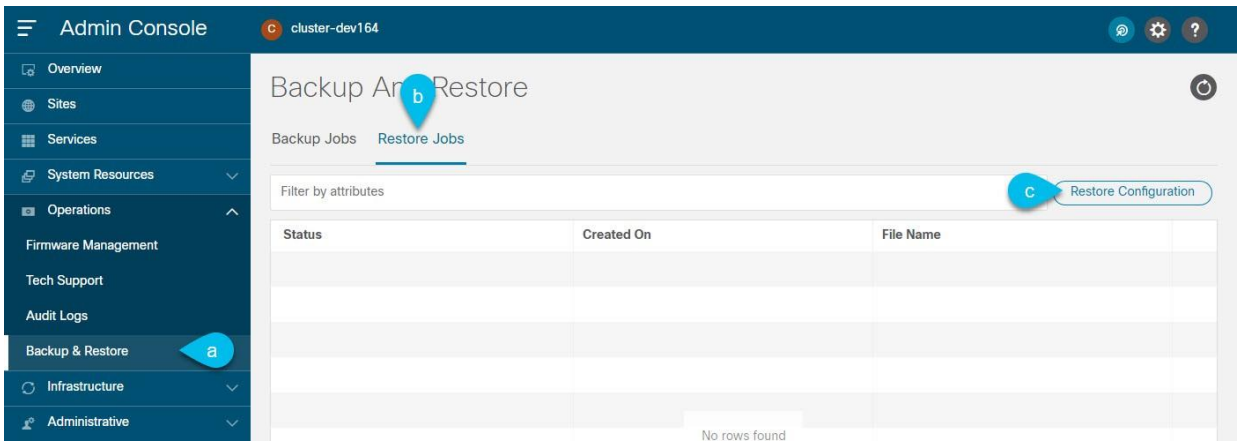
はじめる前に

- バックアップの設定にレイヤ 3 モードの永続 IP が 1 つ以上含まれている場合は、その設定を復元する前に、すべてのクラスタノードに対して BGP を設定していることを確認する必要があります。

  設定のインポート前に BGP が設定されていない場合、インポートは失敗します。

  詳細については、「永続 IP アドレス」を参照してください。

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. 設定の復元を開始します。



a. メイン ナビゲーション メニューから、**[操作（Operations）] > [バックアップと復元（Backups & Restore）]** を選択します。

b. メインペインで、**[復元ジョブ（Restore Jobs）]** タブを選択します。

c. メインペインの右上にある **[設定の復元（Restore Configuration）]** をクリックします。

リストされているバックアップのいずれかを選択する必要はありません。次の画面で、設定のバックアップファイルをアップロードするように求められます。

3. 詳細を入力します。

a. **[暗号化キー（Encryption Key）]** を入力します。

これは、バックアップの作成時に使用したものと同じ暗号化キーである必要があります。

b. **[ファイルの選択（Choose File）]** をクリックし、バックアップファイルを選択します。

Cisco Nexus ダッシュボードには設定のバックアップは保存されないため、復元する前にバックアップファイルをアップロードする必要があります。

このファイルは .tgz または tar.gz 形式である必要があります。

4. **[インポート（Import）]** をクリックして、復元手順を開始します。

イベント分析

[操作（Operations）]カテゴリの**[イベント分析（Event Analytics）]**ページでは、Nexus Dashboard クラスタ内のイベントとアラートのシステム全体のリストを表示できます。

イベント

[イベント（Events）]タブでは、Nexus Dashboard のプラットフォームレベルのイベントと監査ログに簡単にアクセスできます。**[監査ログ（Audit Logs）]** タブには、クラスタ操作中に発生したすべてのイベントが表示されます。Nexus Dashboard GUI でイベントとログを直接表示することに加えて、「クラスタ構成」で説明されているように、イベントを外部の syslog サーバーにストリーミングするようにクラスタを構成することもできます。

[イベント（Events）] タブには、解決と注視が必要な重大度の高いイベントが含まれている可能性があります。

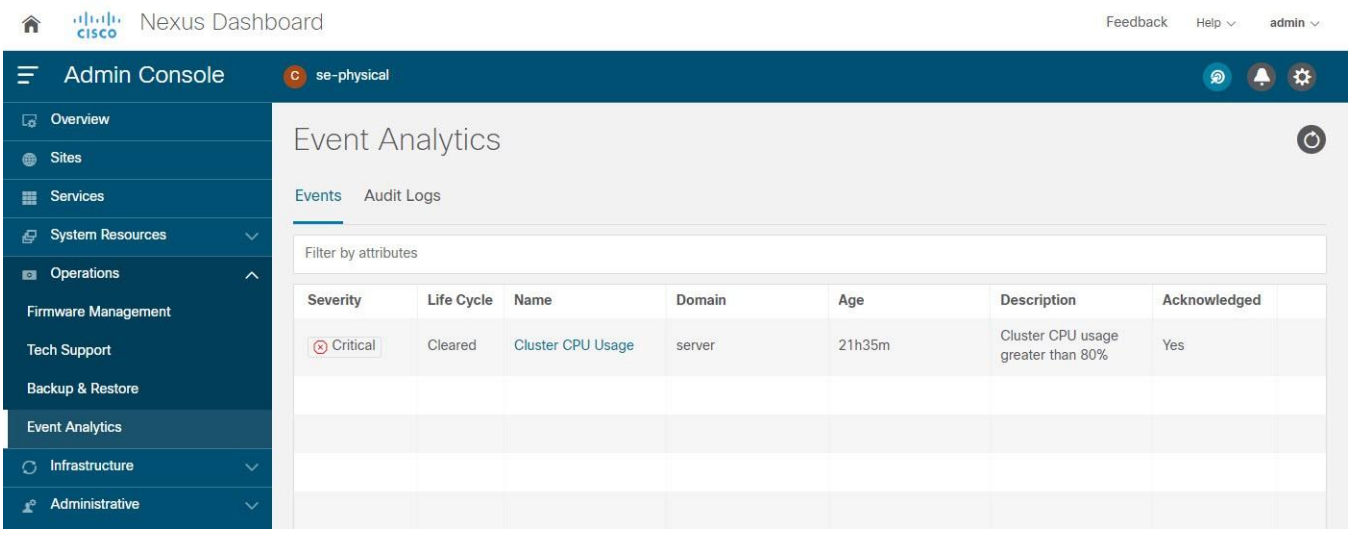


図 9. イベント分析

リスト内の重要なイベントすべての概要を表示したり、特定のイベントをダブルクリックしてそれに関する追加情報を表示したりできます。イベントを表示または解析したら、リスト内のイベントの横にある **[アクション（Actions）]**（**[...]**）メニューをクリックして、イベントの確認とクリアを選択できます。

監査ログ

Nexus Dashboard の監査ログ機能は、クラスタを最初に展開するときに自動的に有効になります。この機能は環境内でユーザーが行った変更をキャプチャします。

メイン ナビゲーション メニューから **[操作（Operations）] > [監査ログ（Audit Logs）]** を選択して、GUI で監査ログを直接表示できます。

ログはデフォルトではソートされないことに注意してください。いずれかの列見出しをクリックすると、リストをソートできます。

[属性でフィルタ（Filter by attributes）] フィールドを使用してリストをフィルタリングし、特定の属性と値のペアを指定することもできます。

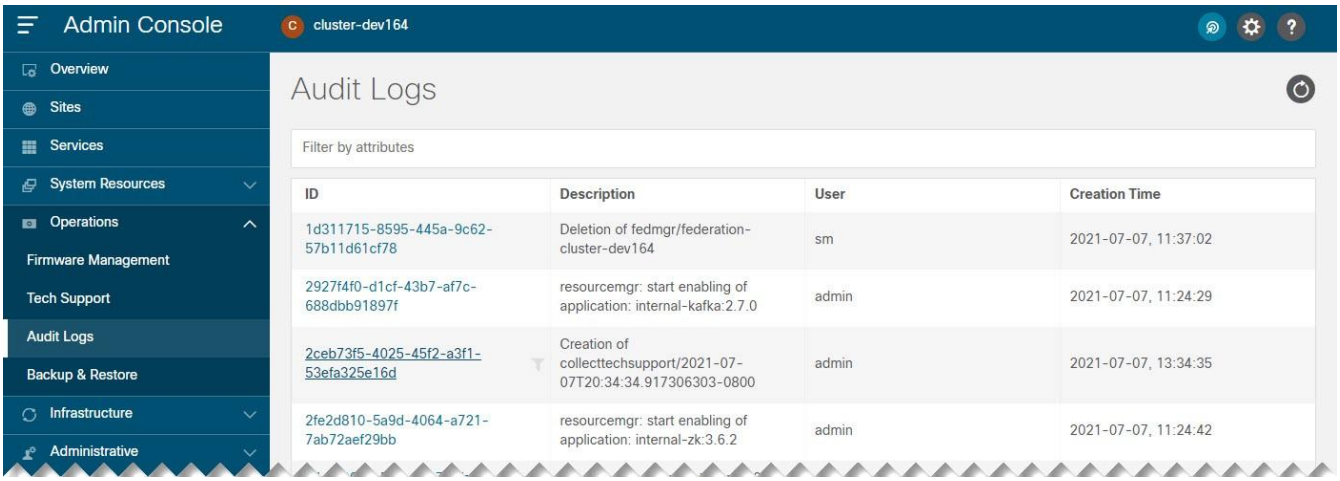


図 10 監査ログ

また、特定のエントリに関する詳細情報を表示するには、リスト内のエントリをクリックして **[詳細（Details）]** タブを開きます。

イベントのエクスポート

Nexus Dashboard は、さまざまなイベント、障害、およびアラートを生成できる 1 つ以上のサービスをホストできます。この情報は、Apache Kafka を使用して公開および保管されます。リリース 2.1(2)では、クラスタレベルのアラートを表示して外部アナライザにエクスポートできましたが、このタイプの情報をすべて外部イベント モニタリング サービスにエクスポートする統一された方法はありませんでした。

リリース 2.2(1)以降、すべてのプラットフォームレベル、インフラストラクチャ レベル、およびサービスレベルのイベントを外部の監視および管理システムにエクスポートするようにクラスタを設定できます。Nexus Dashboard で実行される各サービスは、どのサービスレベルのイベントを集約して、エクスポートするクラスタの Kafka サービスに送信するかを正確に定義できます。

イベントストリーミングを設定する場合、次の制限が適用されます。

- このリリースでは、syslog イベントエクスポータのみがサポートされています。
- デフォルトでは、イベントは最大 4 時間保存されます。

イベントのエクスポートを設定するには、次を実行します。

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. メイン ナビゲーション メニューから、**[インフラストラクチャ（Infrastructure）] > [クラスタ設定（Cluster Configuration）]** を選択します。
3. **Syslog** タイルで**[編集（Edit）]**アイコンをクリックします。

   Syslog ダイアログが開いたら、**[+リモート宛先の追加（+ Add Remote Destinations）]** をクリックして新しいサーバーを追加します。次に、サーバーの IP アドレス、プロトコル、およびポート番号を指定し、この時点でこの syslog サーバーへのストリーミングを有効にするかを選択します。

インフラストラクチャ管理

クラスタの設定

クラスタ設定の GUI 画面では、Nexus Dashboard クラスタとそのノード固有の複数のオプションを設定できます。この GUI 画面には、Nexus Dashboard クラスタに存在する可能性のある問題に関する情報も表示されます。

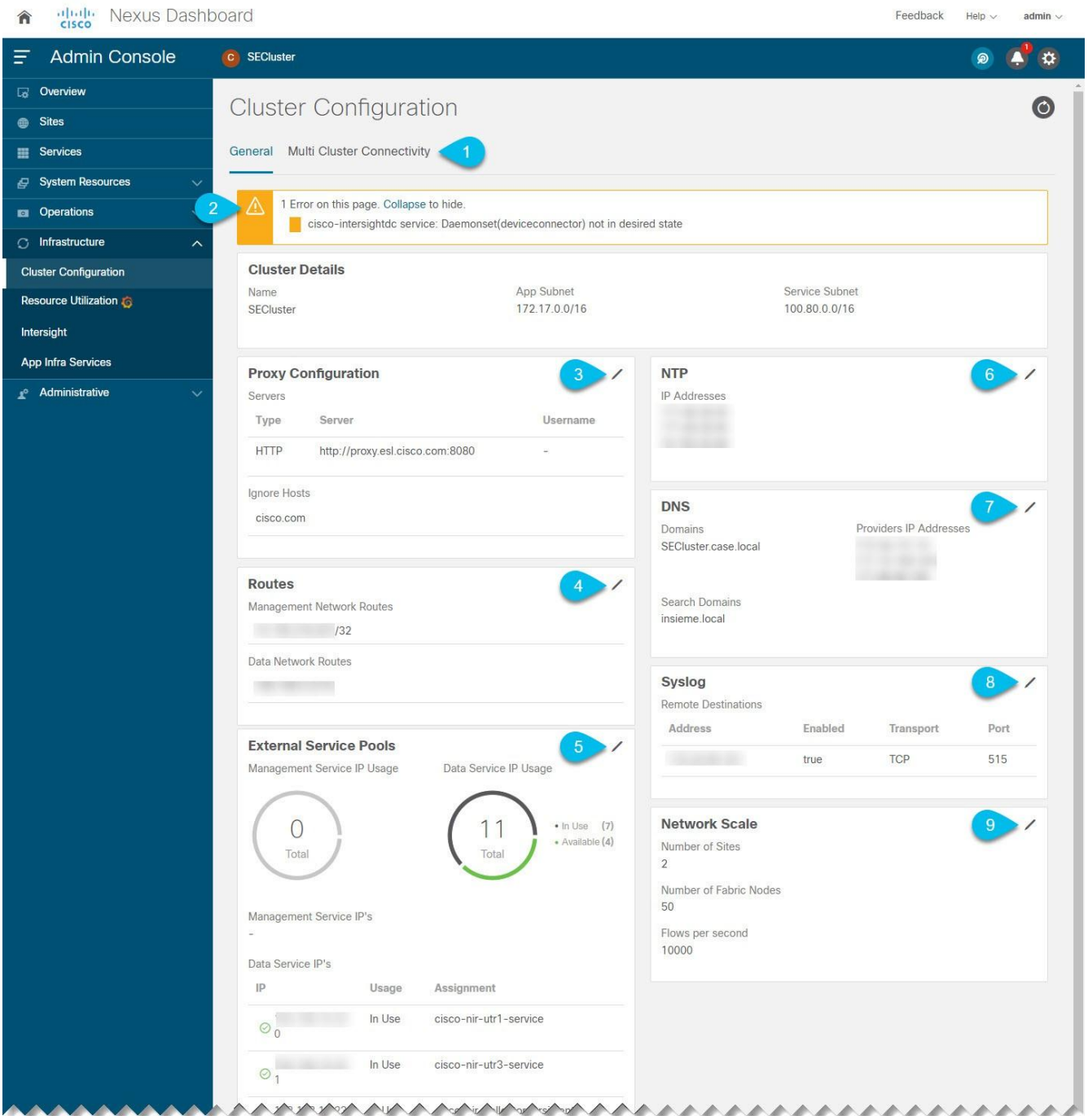


図 11 クラスタの設定

次のクラスタ設定では、IPv4 アドレスのみを IP アドレスとして設定できます。

1. **[マルチクラスタ接続（Multi-cluster Connectivity）]** タブでは、複数のクラスタをまとめて接続し、単一のペインでクラスタとそのサイト、サービス、設定を表示、管理できます。

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. エラーと警告のタイルには、クラスタ内の既存の問題の数が表示されます。**[展開（Expand）]**をクリックすると、特定の問題の完全なリストを表示できます。
3. Nexus Dashboard のプロキシを設定するには、**[プロキシ設定（Proxy Configuration）]** タイルの **[編集（Edit）]** アイコンをクリックします。

   オンプレミスとクラウドサイトの組み合わせや企業ネットワーク内での Nexus Dashboard クラスタの展開など、特定の展開シナリオでは、インターネットとクラウドサイトへのプロキシを介したアクセスが必要な場合があります。

   このリリースでは、単一のプロキシサーバーの追加がサポートされています。

   プロキシサーバーを追加するには、次の手順を実行します。

   a. プロキシ設定ウィンドウで **[+サーバーの追加（+Add Server）]** をクリックします。
   b. **[タイプ（Type）]**ドロップダウンから、プロキシするトラフィックのタイプを選択します。
   c. 必要に応じて、**[サーバー（Server）]** フィールドに、ポートを含むプロキシサーバーの完全なアドレスを入力します。

      たとえば、http://proxy.company.com:80 です。

   d. サーバーにログイン情報が必要な場合は、**ユーザー名**と**パスワード**を入力します。
   e. （任意）**[無視するホストの追加（Add Ignore Host）]** をクリックして、プロキシを無視するホストを指定します。

      クラスタがプロキシをバイパスして直接通信する 1 つ以上のホストを追加できます。

4. 1 つ以上の管理ネットワークまたはデータネットワークルートを追加するには、**[ルート（Routes）]** タイルの**[編集（Edit）]**アイコンをクリックします。

   ここでは、管理インターフェイスまたはデータインターフェイスのスタティックルートを定義できます。たとえば、10.195.216.0/21 をデータネットワークルートとして追加すると、そのサブネット宛てのすべてのトラフィックがデータ ネットワーク インターフェイスから送信されます。

   - 管理ネットワークルートを追加するには、**[管理ネットワークルートの追加（Add Management Network Routes）]** をクリックし、宛先サブネットを指定します。
   - データネットワークルートを追加するには、**[データネットワークルートの追加（Add Data Network Routes）]** をクリックし、宛先サブネットを指定します。

5. 1 つ以上の外部サービスプールを追加するには、**[外部サービスプール（External Service Pools）]** タイルの **[編集（Edit）]** アイコンをクリックします。

   これにより、別の Nexus Dashboard 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に永続 IP アドレスを提供できます。

   詳細情報と設定手順については、「永続 IP アドレス」を参照してください。

6. NTP を設定するには、**[NTP]** タイルの **[編集（Edit）]** アイコンをクリックします。

   デフォルトでは、Nexus Dashboard クラスタの展開時に設定した NTP サーバがここに表示されます。

   [+NTP サーバーの追加（+Add NTP Server）] をクリックして、追加の NTP サーバーを指定できます。

既存の NTP サーバーを削除するには、その横にある **[削除（Delete）]** アイコンをクリックします。少なくとも 1 つの NTP サーバをクラスタに設定する必要があることに注意してください。

7. DNS を設定するには、**[DNS]** タイルの **[編集（Edit）]** アイコンをクリックします。

   デフォルトでは、Nexus Dashboard クラスタの展開時に設定した DNS サーバと検索ドメインがここに表示されます。

   [+プロバイダーの追加（+Add a Provider）] または **[+検索ドメインの追加（+Add a Search Domain）]** をクリックして、追加の DNS サーバーと検索ドメインをそれぞれ指定できます。

   既存の DNS サーバーを削除するには、その横にある **[削除（Delete）]** アイコンをクリックします。

8. イベントログをストリーミングする 1 つ以上の syslog サーバーを指定するには、**[Syslog]** タイルの **[編集（Edit）]** アイコンをクリックします。

   Syslog ダイアログが開いたら、**[+リモート宛先の追加（+ Add Remote Destinations）]** をクリックして新しいサーバーを追加します。次に、サーバーの IP アドレス、プロトコル、およびポート番号を指定し、この時点でこの syslog サーバーへのストリーミングを有効にするかを選択します。

   詳細については、[イベント分析]を参照してください。

9. **ネットワークスケール**を設定するには、**[ネットワークスケール（Network Scale）]**タイルの**[編集（Edit）]**アイコンをクリックします。

   リリース 2.2(1)より前のリリースでは、Nexus Dashboard クラスタにサービスをインストールして有効にした場合、その特定のサービスに必要なクラスタリソース(CPU の数とメモリとストレージの量)を定義するサービス展開プロファイルを選択する必要がありました。

   リリース 2.2(1)以降、リソースプロファイルの選択は、展開のユースケースに直接関連するいくつかのより直感的なパラメータに削減されました。スイッチやフローの数などのこれらのパラメータは、ファブリックのサイズとユースケースの意図を記述し、クラスタがサービスに必要なリソースをインテリジェントに決定できるようにします。パラメータは「ネットワークスケール」として分類されます。

   ネットワークの規模を変更するには、変更を適用するためにサービスを再起動する必要があります。

   a. **[サイトの数（Number of Sites）]**フィールドに、この Nexus Dashboard クラスタが管理する展開のターゲットサイト数を入力します。

   b. **[スイッチの数（Number of Switches）]**フィールドに、展開のスイッチノードのターゲット数を指定します。

   c. **[1 秒あたりのフロー（Flows per second）]**フィールドで、Nexus Dashboard Insights サービスのフローのターゲット数を指定します。

永続 IP アドレス

別の Nexus Dashboard 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に永続 IP アドレスを提供できます。

Nexus Dashboard Insights は、ファブリック内のスイッチからアプリケーションにデータをストリーミン

グするために、サービス(SNMP トラップ、syslog、SAN Insights など)を必要とします。このために、スイッチに IP アドレスが設定されます。通常、サービスの再配置時に IP アドレスが変更された場合、サービスはスイッチの新しい IP アドレスを再設定します。

この IP 再設定の影響がファブリックスイッチに及ぶのを回避するために、サービスはサービスの IP アドレスを保持するように要求できます。その場合、サービスに割り当てることができる一連の IP アドレスを定義してこれに対応する必要があります。

サービスに永続 IP アドレスが必要な場合、以下で説明するように十分な数の IP アドレスが定義されるまで、Nexus Dashboard でそのサービスを有効にすることはできません。

この機能は、NDFC/DCNM ファブリックを使用する Nexus Dashboard Insights でのみサポートされています。さらに、レイヤ 2 機能のみ(管理およびデータサブネットの一部として構成された IP)を使用していて、Nexus Dashboard が VMware ESX に展開されている場合は、https://kb.vmware.com/s/article/1004099 で説明されているように、管理およびデータ ネットワーク インターフェイス ポートグループの両方で無差別モードを有効にする必要があります。

リリース 2.2(1)より前のバージョンでは、この機能は、すべてのノードが同じレイヤ 3 ネットワークの一部であり、永続 IP がノードの管理ネットワークまたはデータネットワークの一部として定義されているクラスタでのみサポートされていました。ここで、アプリケーションは、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 IP をアドバタイズします。

リリース 2.2(1)以降、この機能は、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。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はなりません。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。

永続 IP のガイドラインと制限事項

サービスの永続 IP を設定する場合、次を実行します。

- 次の条件が当てはまる限り、動作するモードを選択できます。
  - レイヤ 2 モードで動作することを選択した場合、ノードは同じデータネットワークおよび管理ネットワークの一部である必要があります。
  - レイヤ 3 モードで動作することを選択した場合、「すべてのノードでの BGP の有効化」で説明されているように、クラスタの展開中または展開後に、すべてのノードに BGP 設定を提供する必要があります。
  - 2 つのモードを切り替えることができます。その場合、特定のモードの既存のサービスを完全に削除する必要があり、新しいモードに対応する新しい永続 IP を設定する必要があります。
- レイヤ 3 モードで 1 つ以上の永続 IP を設定し、クラスタの設定をバックアップする場合、この機能に必要な BGP 設定はバックアップに保存されません。

  そのため、そのクラスタにレイヤ 3 の永続 IP を含むクラスタの設定を復元する前に、すべてのクラスタノードに対して BGP を設定する必要があります。設定のインポート前に BGP が設定されていない場合、インポートは失敗します。

すべてのノードで BGP を有効にする

レイヤ 3 モードで動作する場合は、クラスタ内のすべてのノードに対して BGP を有効にして設定する必要があります。クラスタの展開時に各ノードに BGP を既に設定している場合、または代わりにレイヤ 2 モードで動作する場合は、「永続 IP の設定」に記載されているように、このセクションをスキップして、ノードの管理サブネットとデータサブネットから 1 つ以上の永続 IP を提供するだけです。レイヤ 2 モードでの動作を選択した場合は、すべてのノードが同じレイヤ 3 ネットワークの一部である必要があることに注意してください。レイヤ 3 モードでの動作を選択した場合は、このセクションで説明されているように、IPv4 または IPv6 の永続 IP アドレスをアドバタイズするために、少なくとも 1 つの BGP ピアがすべてのクラスタノードで設定されている必要があります。

はじめる前に

- アップリンクピアルータが、クラスタノードのレイヤ 3 ネットワーク全体でアドバタイズされた永続 IP を交換できることを確認します。
- サービスが永続 IP アドレスを要求すると、サービスが実行されているノード上の BGP を介してデータリンクからアドバタイズされたルートが、サービスのライフサイクル全体を通じて維持されます。

ノードで BGP を設定するには、次を実行します。

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. 左側のナビゲーション メニューから、**[システムリソース（System Resources）] > [ノード（Nodes）]** を選択します。
3. いずれかのノードの横にある**[アクション（Actions）]**(**...**)メニューをクリックし、**[編集（Edit）]**を選択します。
4. **[ノードの編集（Edit Node）]**画面で、**[BGP を有効にする（Enable BGP）]**をオンにします。
5. **[ASN]**フィールドに、ノードの自律システム番号を指定します。
6. **[IPv4 BGP ピアの追加（+Add IPv4 BGP Peer）]**または**[IPv6 BGP ピアの追加（+Add IPv6 BGP Peer）]**をクリックして、ピア IP アドレス情報を提供します。
   a. **[ピアアドレス（Peer Address）]**フィールドに、このノードのピアルータの IPv4 または IPv6 アドレスを指定します。

      マルチホップ BGP ピアリングはサポートされていないため、**ピアアドレス**がノードのデータサブネットの一部であることを確認する必要があります。

   b. **[ピア ASN（Peer ASN）]**フィールドに、ピアルータの自律システム番号を指定します。

      EBGP のみがサポートされているため、ノード ASN とピア ASN が異なることを確認する必要があります。

   c. [保存（Save）] をクリックして変更を保存します。
7. クラスタ内のすべてのノードに対してこれらの手順を繰り返します。

   クラスタ内のすべてのノードで BGP を設定する必要があります。

   すべてのノードに同じ ASN を設定することも、ノードごとに異なる ASN を設定することもできます。

永続 IP の設定

はじめる前に

- すべての永続 IP については、レイヤ 2 またはレイヤ 3 のいずれかのアプローチを使用する必要があります。 2 つのアプローチを組み合わせることはサポートされていません。

  すべてのノードが同じレイヤ 3 ネットワーク内にある場合は、この機能にレイヤ 2 モードまたはレイヤ3モードのいずれかを使用することを選択できます。2つのモードについては、「永続IPアドレス」で説明されています。

ノードが異なるレイヤ 3 ネットワークにいる場合は、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ないように永続 IP を設定する必要があります。

- クラスタ内のノードが異なるレイヤ 3 ネットワークに属している場合は、「すべてのノードでの BGP の有効化」で説明されているように、BGP を有効にして設定する必要があります。
- 永続 IP を使用するサービスが別のノードに再配置されている間、一時的なトラフィックの中断が発生する可能性があります。

  中断時間は、次の要因によって異なります。

  - ノード障害が検出される時間
  - サービスが別のノードに再スケジュールされる時間
  - レイヤ 2 モードの場合、サービスの外部 IP が、GARP(IPv4)経由またはネイバー探索(IPv6)経由で、スケジュールされたノードからアドバタイズされる時間
  - レイヤ 3 モードの場合、サービスの外部 IP が、BGP 経由でスケジュールされたノードからアドバタイズされる時間

1 つ以上の永続 IP アドレスを提供するには、次を実行します。

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. 左側のナビゲーション メニューから、**[インフラストラクチャ（Infrastructure）] > [クラスタ設定（Cluster Configuration）]** を選択します。
3. **[外部サービスプール（External Service Pools）]**タイルで、**[編集（Edit）]**アイコンをクリックします。
4. 表示された**[外部サービスプール（External Service Pools）]**画面で、**[IP アドレスの追加（+Add IP Address）]**をクリックして、管理ネットワークまたはデータネットワーク上で 1 つ以上の IP アドレスを追加します。

   永続 IP を編集するときは、次のルールが適用されます。

   - クラスタ内のすべてのノードが同じレイヤ 3 ネットワークにいる場合、次のいずれかを選択できます。
     - レイヤ 2 モード。この場合、管理サービス用に追加する IP アドレスは管理サブネットの一部である必要があり、データサービスの IP アドレスはデータサブネットの一部である必要があります。
     - レイヤ 3 モード。この場合、追加する IP アドレスは、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することはできません。この場合、" 管理サービス IP" 下の IP の追加はサポートされていないため、GUI の " データサービス IP" カテゴリに IP を追加する必要があります。
   - IPv4 または IPv6 IP アドレスのいずれかを指定する必要があります。両方を指定することはできません。
   - プレフィックスなしで個々の IP アドレスを 1 つずつ追加する必要があります。 IP アドレスの範囲の追加はサポートされていません。
   - 以前に定義された IP は削除できますが、1 つ以上のサービスで現在使用されている IP を削除することはできません。

マルチクラスタ接続

Nexus Dashboard のこのリリースでは、複数の Nexus Dashboard クラスタ間の接続を確立して、単一画面でクラスタを一元管理できます。また、接続されている任意のクラスタで実行中のサイトやサービスにアクセスすることもできます。

2 番目のクラスタを追加すると、クラスタのグループが形成されます。グループの作成元のクラスタは "プライマリ" クラスタとなり、グループ内の他のクラスタには適用されない多くの固有の特性を持ちます。

- すべての追加クラスタを接続するには、プライマリクラスタを使用する必要があります。
- グループからクラスタを削除するには、プライマリクラスタを使用する必要があります。

マルチクラスタ接続を確立しても、グループ内にあるすべてのクラスタの情報が格納された単一データベースは作成されません。すべてのクラスタは独自の設定データベースを保持すると同時に、グループ内の他のすべてのクラスタのプロキシとして機能できます。アクションやリクエストがどのクラスタから送信されたか、またはどのクラスタに送信されるかは関係ありません。

注意事項と制約事項

マルチクラスタ接続を設定する場合は、次のガイドラインが適用されます。

- このリリースでは、物理または仮想（ESX）フォームファクタのみを使用して展開されたクラスタ間のマルチクラスタ接続がサポートされます。つまり、物理的な Nexus Dashboard クラスタを仮想（ESX）クラスタに追加することはできますが、仮想（KVM）またはクラウドクラスタを同じグループに含めることはできません。
- 接続は、マルチクラスタ接続を介して接続されるすべてのクラスタのすべてのノード間で確立する必要があります。
- このリリースでは、最大 4 つのクラスタを接続できます。
- このリリースでは、接続されているすべてのクラスタで最大 12 のサイトがサポートされます。
- マルチクラスタ接続を確立するために使用するプライマリクラスタは、グループ内の他のクラスタと同じまたはそれ以降のリリースの Nexus Dashboard を実行している必要があります。

  つまり、リリース 2.1.1 を実行しているプライマリクラスタから、リリース 2.1.2 を実行している Nexus Dashboard クラスタに接続することはできません。

  相互に接続されている複数のクラスタをアップグレードする場合は、最初に主クラスタをアップグレードする必要があります。

- マルチクラスタ接続と One View は、リモートユーザに対してのみサポートされます。

  複数のクラスタに接続し、いずれかのクラスタにローカル管理者ユーザーとしてログインした場合は、ログイン先のローカルクラスタのみを表示および管理できます。

  グループ内のすべてのクラスタを表示および管理するには、すべてのクラスタで構成されているリモートユーザーとしてログインする必要があります。

- 各クラスタの Nexus ダッシュボード Insights サービスは、グループ内の任意のクラスタにある他の Insights サービスのサイトグループを表示できます。

  ただし、サイトグループを作成する場合、各 Insights サービスでは、サービスのみがインストールされている同じクラスタにオンボードされているサイトを追加できます。

- Nexus Dashboard Orchestrator サービスは、サービスがインストールされている同じクラスタにオンボーディングされているサイトのみをサポートします。

複数のクラスタの接続

はじめる前に

- 「注意事項と制限事項」セクションに記載されている情報をよく理解している必要があります。
- 接続するすべてのクラスタでリモート認証とユーザを設定しておく必要があります。

  マルチクラスタ接続とワンビューはリモートユーザーに対してのみサポートされているため、すべてのクラスタに対して同じリモートユーザーに管理者特権を設定する必要があります。詳細については、「リモート認証」を参照してください。

別のクラスタに接続するには、次の手順を実行します。

1. プライマリとして指定するクラスタの Nexus Dashboard GUI にログインします。
2. 2 番目のクラスタを追加します。

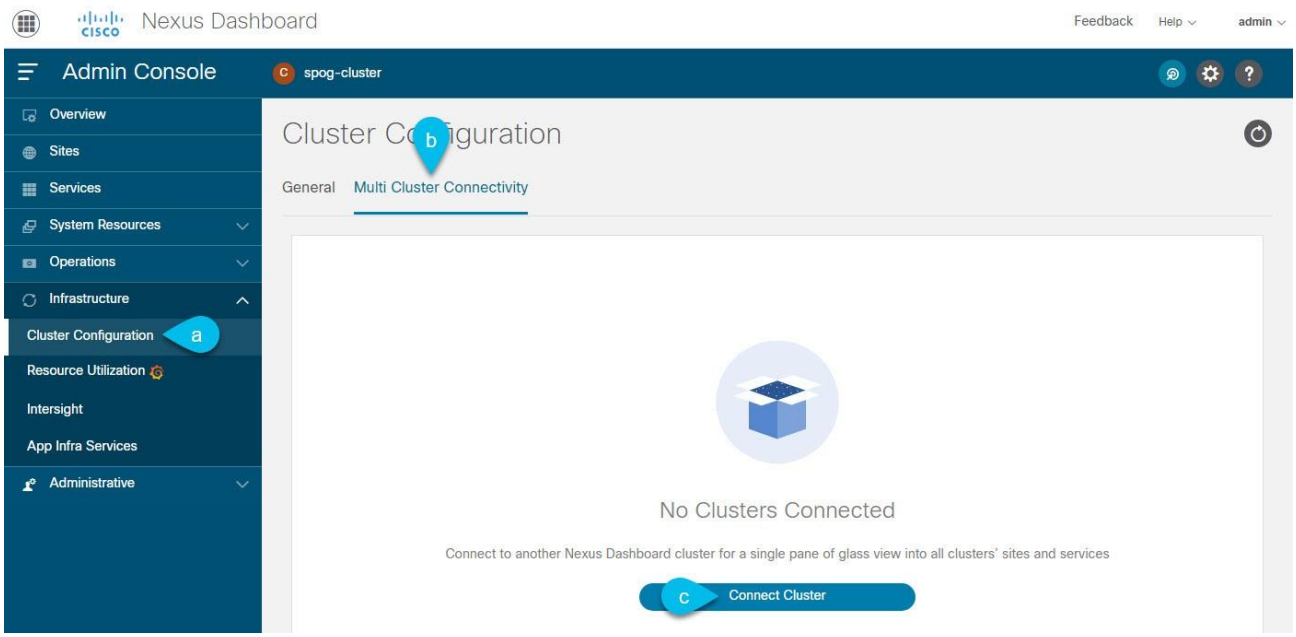


図 12. 2 番目のクラスタの追加

   a. メイン ナビゲーション メニューから、**[インフラストラクチャ（Infrastructure）] > [クラスタ設定（Cluster Configuration）]** を選択します。
   b. メインペインで、**[マルチクラスタ接続（Multi-Cluster Connectivity）]** タブを選択します。
   c. **[クラスタの接続（Connect Cluster）]** をクリックします。
3. クラスタ情報を入力します。

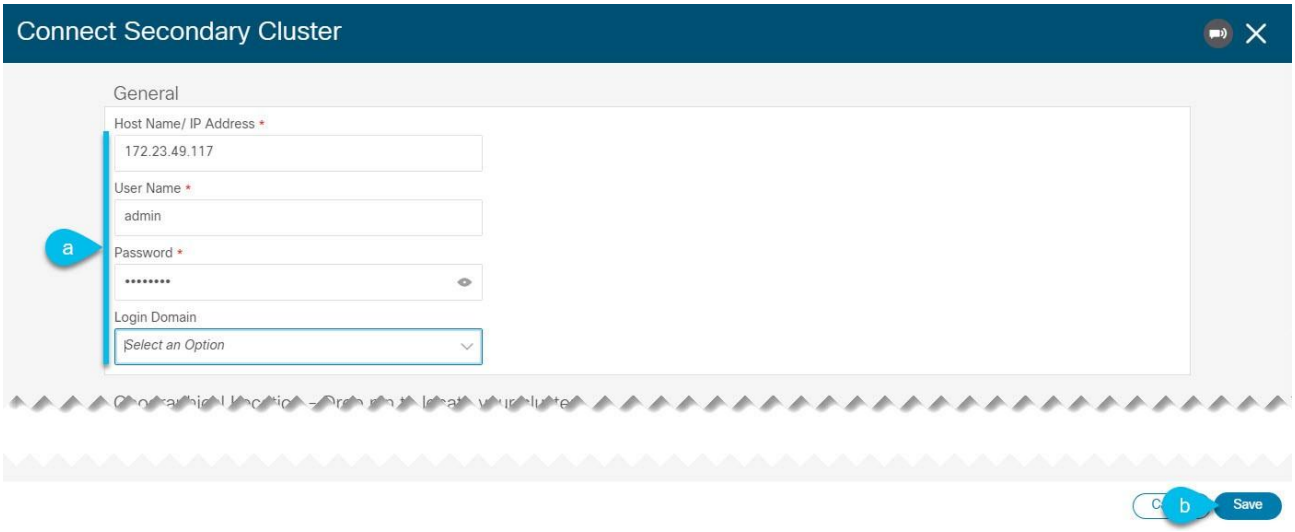


図 13. クラスタ情報の入力

a. 情報フィールドに、追加するクラスタのホスト名または IP アドレスと認証情報を入力します。

   対象クラスタ内にあるいずれか 1 つのノードの管理 IP アドレスのみを指定する必要があります。他のノード情報は、接続の確立後に自動的に同期されます。

b. 次に [**保存（Save）**] をクリックします。

   指定するユーザーには、追加するクラスタの管理者権限が必要です。ユーザーのログイン情報は、追加のクラスタへの接続を最初に確立するときに 1 回使用されます。最初の接続が確立された後、その後のすべての通信は安全なキーを介して行われます。安全なキーは、各クラスタをグループに追加するときにプロビジョニングされます。

   追加するクラスタは、既存のクラスタグループに属していてはなりません。

4. グループに追加する Nexus Dashboard クラスタが他にもあれば、この手順を繰り返します。

   複数のクラスタがグループに追加されると、**[クラスタ設定（Cluster Configuration）] > [マルチクラスタ接続（Multi-Cluster Connectivity）]** ページでステータスを確認できます。

同じマルチクラスタグループの一部である限り、他のクラスタから任意のクラスタを表示および管理できますが、プライマリクラスタを表示している場合はそのグループ内のクラスタの追加と削除のみを実行できます。

[マルチクラスタ接続（Multi-Cluster Connectivity）] ページに、マルチクラスタグループに属するすべてのクラスタが表示されます。**[アクション（Actions）]** ボタンは、プライマリクラスタの表示中にのみ表示されます。クラスタグループを変更するには、「クラスタ間の移動」での説明に従ってプライマリに移動する必要があります。これにより、**[アクション（Actions）]** ボタンが使用可能になります。

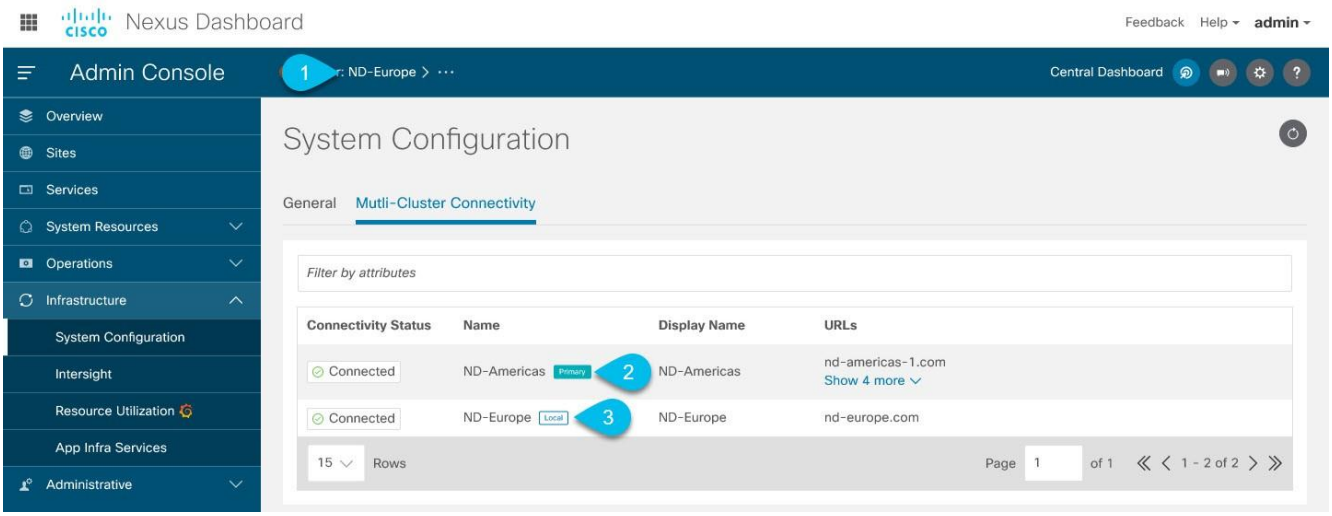


図 14. プライマリクラスタと非プライマリクラスタ

1. **[クラスタ：<name>（Cluster: <name>）]** エリアには、現在表示しているクラスタが表示されます。

   クラスタグループに属するクラスタに初めてログインすると、ここに表示されます。クラスタの名前をクリックすると、同じグループに属するリモートクラスタに移動して管理できます。

2. [プライマリ（Primary）] ラベルは、グループのプライマリクラスタを示します。

   クラスタの追加や削除など、クラスタグループに変更を加えるには、このクラスタを表示する必要があります。

3. [ローカル（Local）] ラベルは、ログインしているクラスタを示します。

   これは、ブラウザの URL フィールドにアドレスが表示されるクラスタです。上記のように別のクラスタに移動しても、ブラウザの URL とローカルラベルは変更されません。

中央ダッシュボード

中央のマルチクラスタ接続ダッシュボード UI ページにアクセスするには、Nexus Dashboard UI ページの右上にある **[中央ダッシュボード（Central Dashboard）]** をクリックします。このページには、作成したクラスタグループ全体にわたるすべてのクラスタ、サイト、およびサービスを含むシステム全体の概要とステータスが表示されるため、クラスタへの接続損失といった明らかな問題をすばやく見つけることができます。

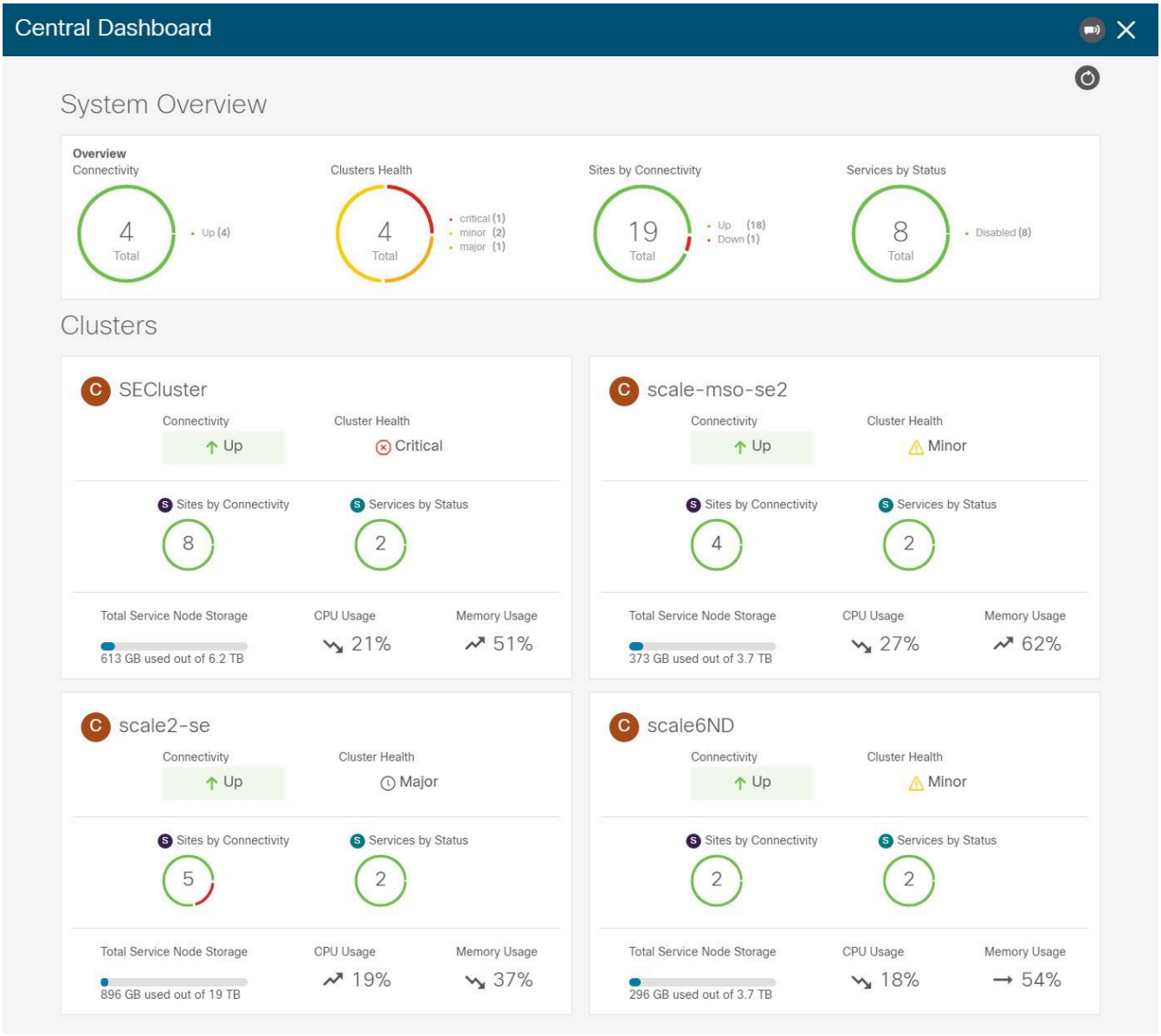


図 15. 中央ダッシュボード

この画面に表示されるクラスタ接続は、各クラスタのプライマリクラスタへの接続のみを示します。グループ内のすべてのクラスタ間のフルメッシュ接続は対象外です。

クラスタ間の移動

2 つ以上のクラスタをまとめて接続すると、既にログインしているクラスタから任意のクラスタとそのサイトやサービスを単一画面に直接表示して一元管理できます。

現在表示されているクラスタを変更するには、いずれかの Nexus Dashboard ページでクラスタ名をクリックします。

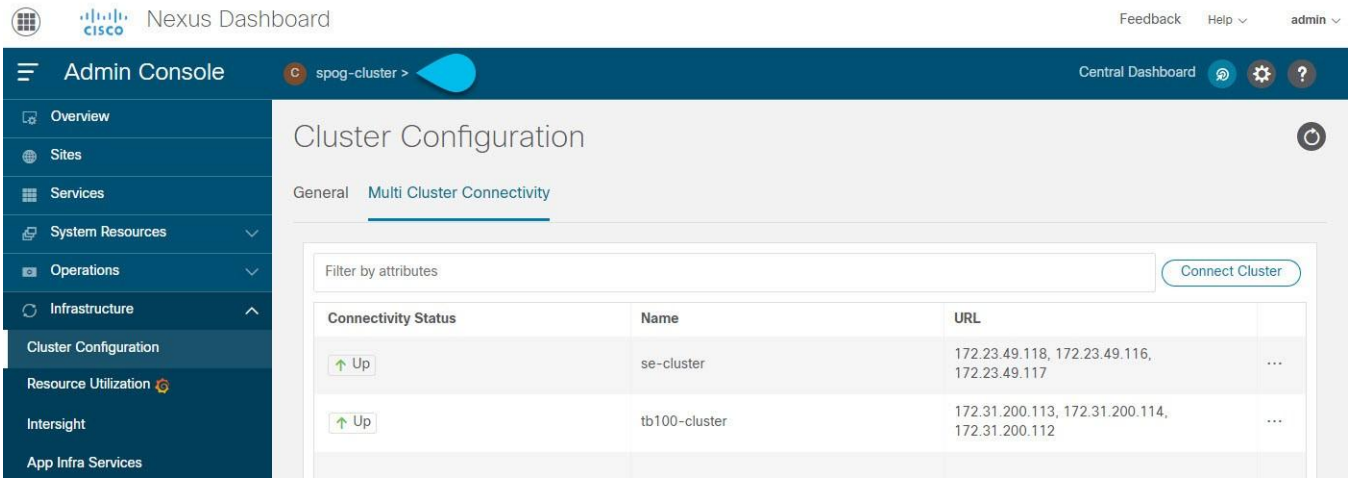


図 16. クラスタ間の移動

現在のクラスタを変更した後、選択したクラスタの情報を表示するには現在のページの右上にある **[更新（Refresh）]** ボタンをクリックする必要がある場合があります。ここからは、そのクラスタに直接ログインした場合と同じように、任意のアクションを実行できます。

クラスタの切断

既存のグループからクラスタを切断するには、次の手順を実行します。

1. プライマリクラスタの Nexus Dashboard GUI にログインします。

   グループに対するクラスタの追加と削除は、プライマリクラスタから実行する必要があります。

2. メイン ナビゲーション メニューから、**[インフラストラクチャ（Infrastructure）] > [クラスタ設定（Cluster Configuration）]** を選択します。
3. メインペインで、**[マルチクラスタ接続（Multi-Cluster Connectivity）]** タブを選択します。
4. 削除するクラスタの **[アクション（Actions）]**（[...]）メニューから、**[クラスタの接続解除（Disconnect Cluster）]** を選択します。
5. 確認ウィンドウで、**[OK]** をクリックします。

追加の物理ノードの展開

クラスタの初期展開については、『*Cisco Nexus Dashboard 展開ガイド*』を参照してください。ここからのセクションでは、ワーカーまたはスタンバイノードとして追加の物理ノードを展開する方法について説明します。

既存のクラスタにノードを追加する場合、追加ノードは、クラスタ内にある残りのノードと同じフォームファクタ(物理または仮想)である必要があります。このリリースは、異なるフォームファクタのノードを持つクラスタには対応していません。

追加ノードを展開した後、そのロールに基づいてそのノードを登録し、クラスタに追加できます。

- ワーカーノードの詳細については、「ワーカーノードの管理」を参照してください。
- スタンバイノードの詳細については、「スタンバイノードの管理」を参照してください。

物理ノードの前提条件とガイドライン

- 「プラットフォームの概要」で説明されている一般的な前提条件、特にネットワークとファブリック接続のセクションを事前に確認し、条件を満たします。
- 単一クラスタ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。
- 次のハードウェアを使用していることを確認してください。

  物理アプライアンスのフォームファクタは、元の Nexus Dashboard ハードウェアでのみサポートされます。次の表に、物理アプライアンスサーバーの PID と仕様を示します。

  表 5. サポート対象ハードウェア

PID	ハードウェア
SE-NODE-G2	- UCS C220 M5 シャーシ - 2x 10 コア 2.2G Intel Xeon Silver CPU - 4 X 25 G 仮想インターフェイスカード 1455 - 2.4TB HDD X 4 - 400 GB SSD - 1.2 TB NVMe ドライブ - 256 GB RAM - 1050 W 電源装置

  上記のハードウェアは、Nexus Dashboard ソフトウェアのみをサポートします。他のオペレーティングシステムがインストールされている場合、そのノードは Nexus ダッシュボード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 4.1(3d)。

  サポートされる最小バージョン：CIMC、リリース 4.0（1a）。

- 『*Nexus Dashboard ハードウェア 設置ガイド*』の説明に従って、物理サーバーをラックに取り付けて接続します。
- ハードウェアが既存のクラスタと同じ Nexus Dashboard リリースを実行していることを確認します。

  新しいノードで以前のリリースを実行している場合は、「手動アップグレード」の説明に従って、現在のリリースに手動でアップグレードする必要があります。

  何らかの理由で手動アップグレードを実行できない場合は、「ノードの再イメージ化」の説明に従って、ソフトウェアを再インストールできます。

物理ノードの展開

上記のすべての前提条件を完了したら、ノードを接続してノード固有の電源をオンにします。

ノードの展開が完了したら、クラスタに追加できます。

- ノードをワーカーノードとして追加するには、「ワーカーノードの管理」を参照してください。
- ノードをスタンバイノードとして追加するには、「スタンバイノードの管理」を参照してください。

VMware ESX での追加の仮想ノードの展開

クラスタの初期展開については、『*Cisco Nexus Dashboard 展開ガイド*』を参照してください。ここからのセクションでは、ワーカーまたはスタンバイノードとして追加のノードを VMware ESX に展開する方法について説明します。

> 既存のクラスタにノードを追加する場合、追加ノードは、クラスタ内にある残りのノードと同じフォームファクタ(物理または仮想)である必要があります。このリリースは、異なるフォームファクタのノードを持つクラスタには対応していません。

追加ノードを展開した後、そのロールに基づいてそのノードを登録し、クラスタに追加できます。

- ワーカーノードの詳細については、「ワーカーノードの管理」を参照してください。
- スタンバイノードの詳細については、「スタンバイノードの管理」を参照してください。

ESX ノードの前提条件とガイドライン

- 「プラットフォームの 概要」で説明されている一般的な前提条件、特にネットワークとファブリックの接続性のセクション事前に確認し、条件を満たします。
- このリリースでは、最大 6 つのワーカーノード（3 つのアプリケーションノードと 3 つのデータノード）と合計 2 つのスタンバイノードを持つ VMware ESX クラスタがサポートされます。
- VMware ESX で展開する場合は、vCenter を使用して展開するか、ESXi ホストに直接展開するかを選択できます。

  詳細については、次のいずれかのセクションを参照してください。

- VMware ESX で展開する場合は、次の 2 種類のノードを展開できます。
  - 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
  - アプリケーションノード - Nexus Dashboard Orchestrator などの非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

    表 6. サポート対象ハードウェア

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 2.2.1	VMware ESXi 6.5、6.7、または 6.7 VMware vCenter 6.x（vCenter を使用して展開する場合） 各 VM には次のものが必要です。 ・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 データノードは、次の最小パフォーマンス要件を満たすストレージに展開する必要があります。 ○ SSD は、データストアに直接接続するか、RAID ホストバスアダプタ（HBA）を使用している場合は JBOD モードで接続する必要があります。 ○ SSD は、混合使用/アプリケーション用に最適化する必要があります（読み取り最適化ではありません） ○ 4K ランダム読み取り IOPS：93000 ○ 4K ランダム書き込み IOPS：31000 各 Nexus Dashboard ノードは、異なる ESXi サーバーに展開することを推奨します。	VMware ESXi 6.5、6.7、または 6.7 VMware vCenter 6.x（vCenter を使用して展開する場合） 各 VM には次のものが必要です。 ・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 Dashboard 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 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。

vCenter を使用した ESX ノードの展開

はじめる前に

「ESX ノードの前提条件と ガイドライン」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。

ここでは、vCenter を使用して VMware ESXi で追加の Cisco Nexus Dashboard ノードを展開する方法について説明します。

1. Cisco Nexus Dashboard OVA イメージを取得します。

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

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

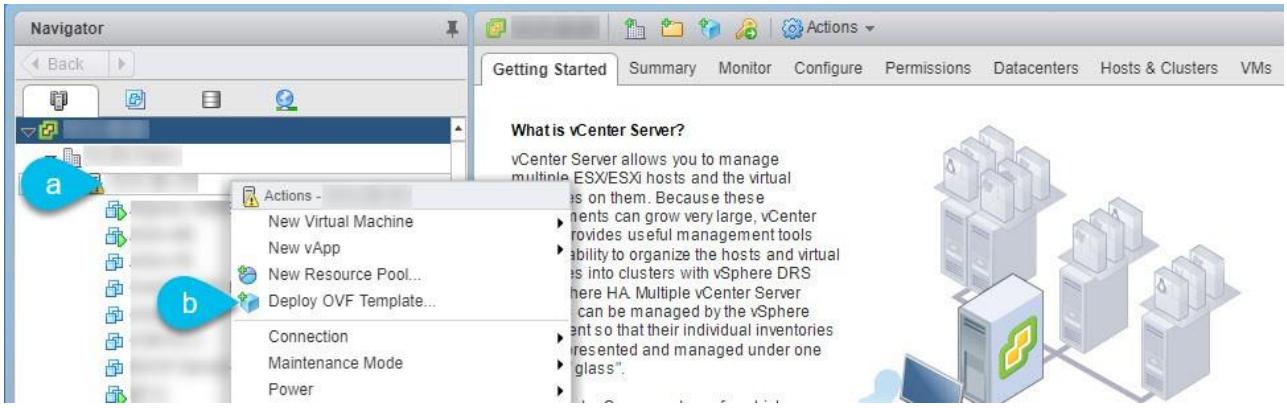
   b. ダウンロードする Nexus Dashboard のバージョンを選択します。

   c. Nexus Dashboard OVA イメージの横にある**ダウンロード**アイコンをクリックします（nd-dk9.<version>.ova）。

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。

3. 新しい VM 展開を開始します。

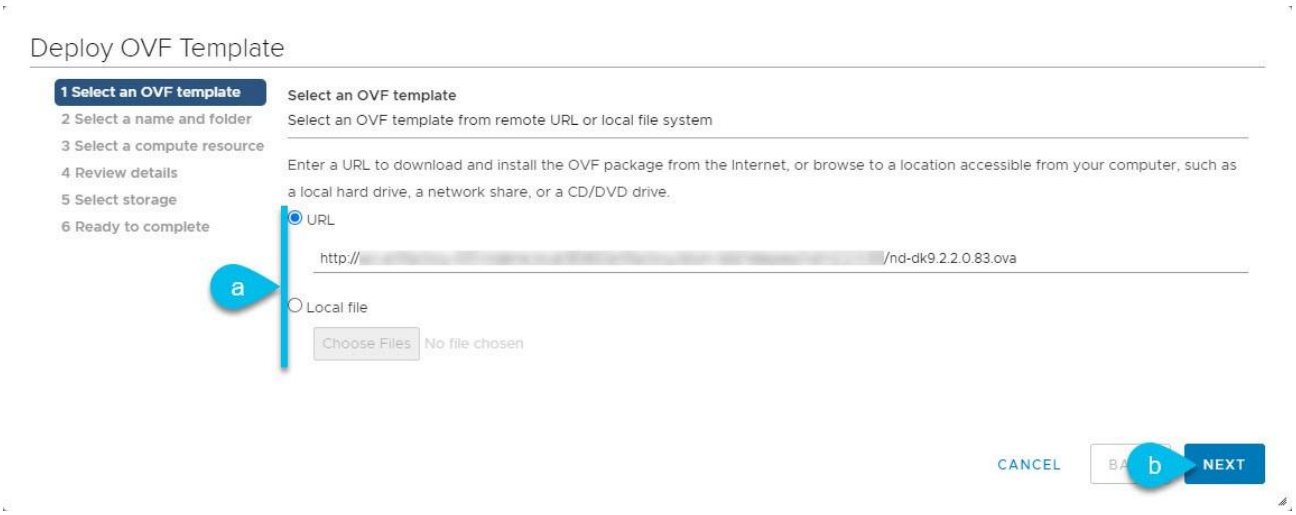


   a. 展開する ESX ホストを右クリックします。

   b. [OVF テンプレートの展開（Deploy OVF Template）] を選択します。

      [OVF テンプレートの展開（Deploy OVF Template）] ウィザードが表示されます。

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、**[次へ（Next）]** をクリックします。



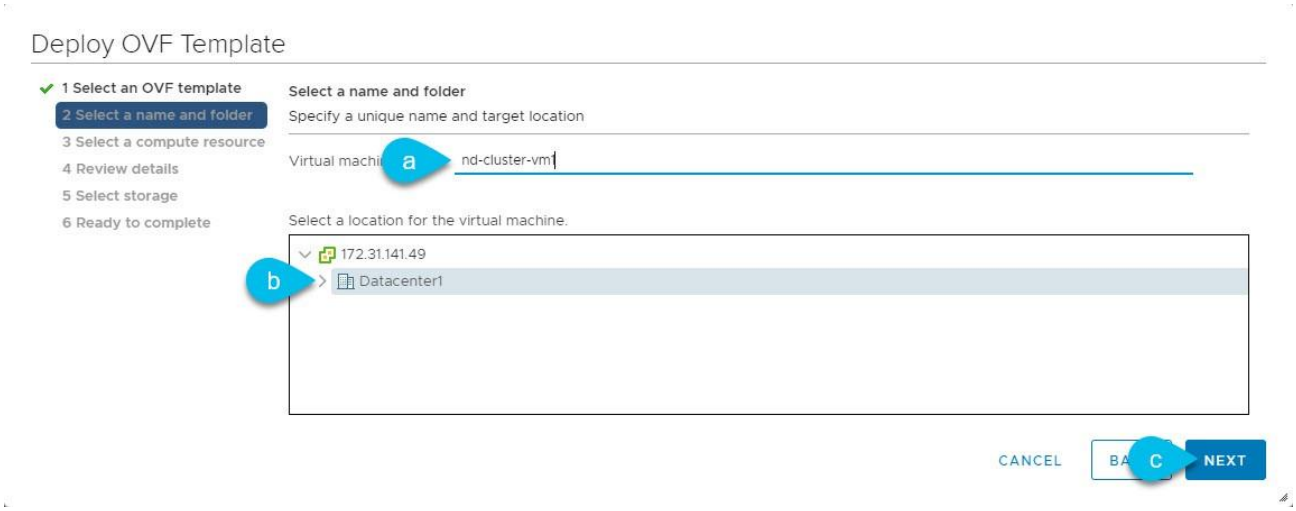
   a. 画像を提供します。

環境内の Web サーバでイメージをホストしている場合は、**[URL]** を選択し、イメージの URL を指定します。

イメージがローカルの場合は、**[ローカルファイル（Local file）]** を選択し、**[ファイルの選択（Choose Files）]** をクリックしてダウンロードした OVA ファイルを選択します。

b. [次へ（Next）] をクリックして次に進みます。

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。

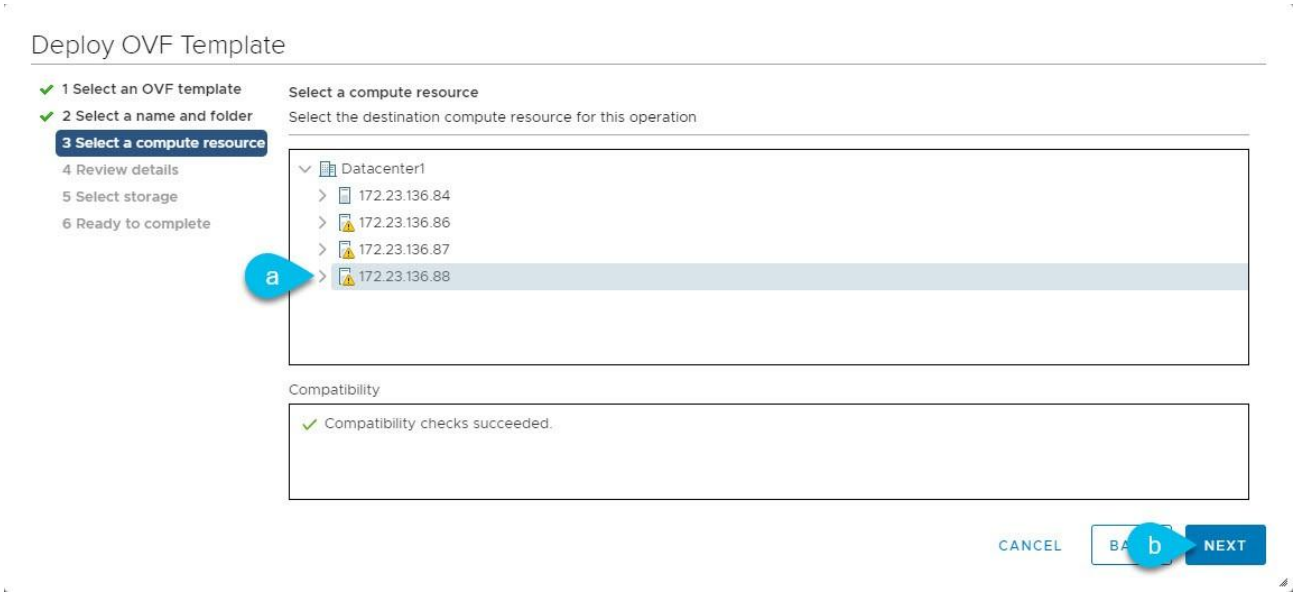


a. 仮想マシンの名前を入力します。

b. 仮想マシンのストレージ場所を選択します。

c. [次へ（Next）] をクリックして次に進みます。

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

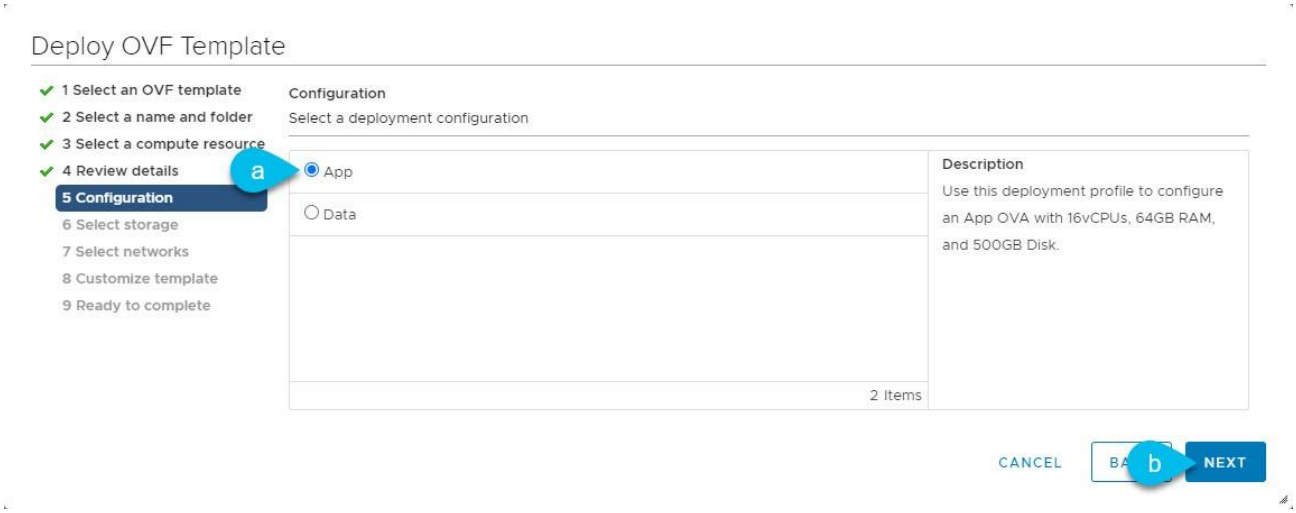


a. 仮想マシンの vCenter データセンターと ESX ホストを選択します。

b. [次へ（Next）] をクリックして次に進みます。

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。

8. **[設定（Configuration）]** 画面で、展開するノードプロファイルを選択します。

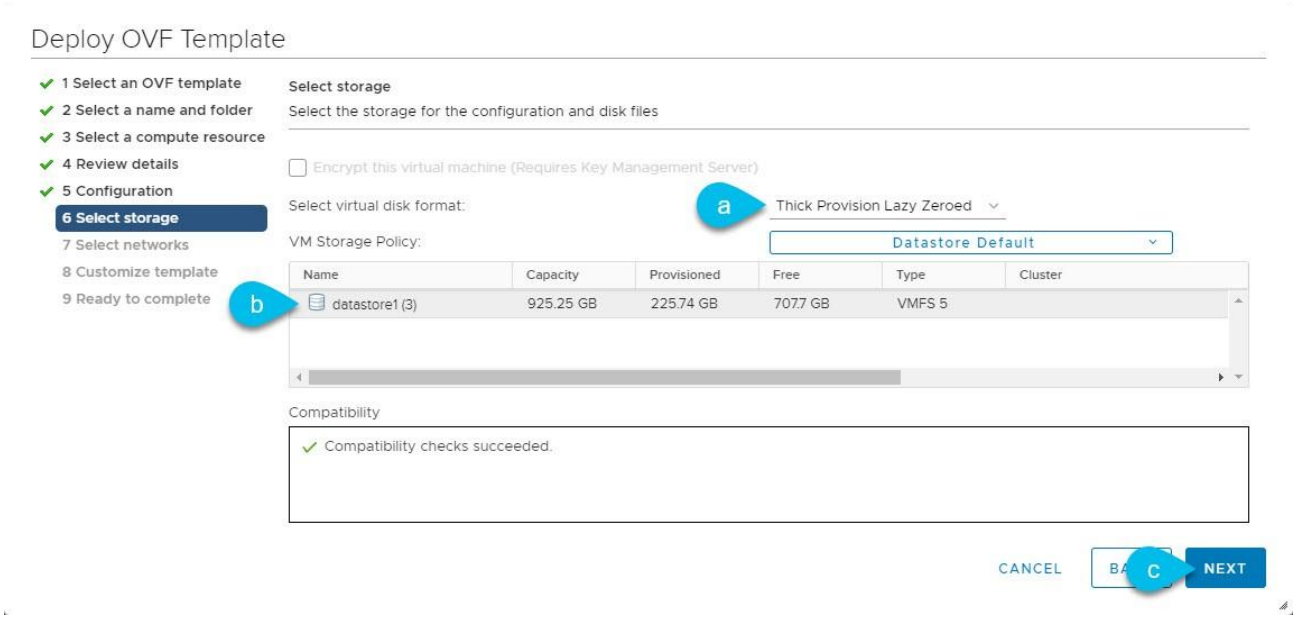


a. ユースケースの要件に基づいて、アプリまたはデータ ノード プロファイルを選択します。

b. ノードプロファイルの詳細については、「ESX ノードの前提条件とガイドライン」を参照してください。

c. [次へ（Next）] をクリックして次に進みます。

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



a. **[仮想ディスク フォーマットの選択（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）] をクリックして次に進みます。

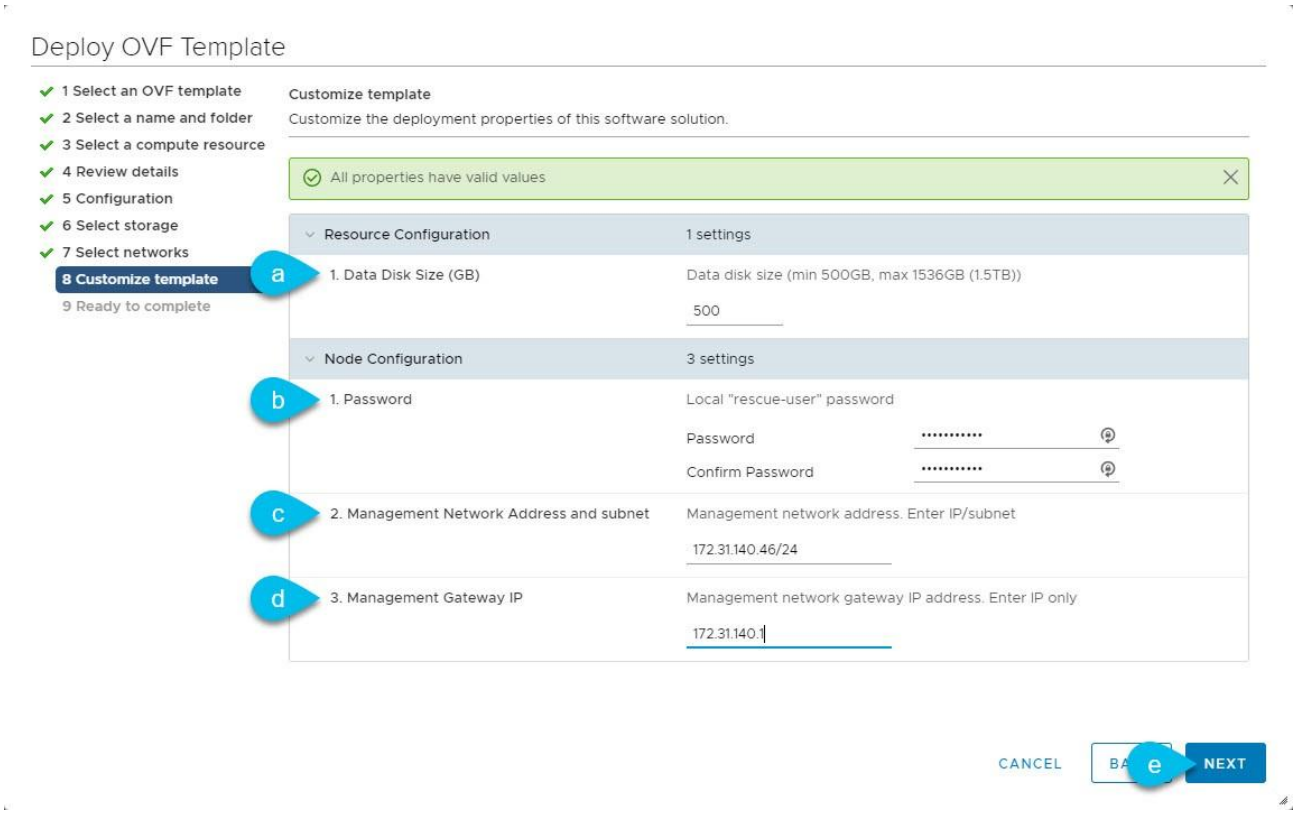
10. **[ネットワークの選択（Select networks）]** 画面で、Nexus Dashboard の管理およびデータ ネットワークの VM ネットワークを選択し、**[次へ（Next）]** をクリックして続行します。

Nexus Dashboard クラスタには 2 つのネットワークが必要です。

- fabric0 は、Nexus Dashboard クラスタのデータ ネットワークに使用されます
- mgmt0 は、Nexus Dashboard クラスタの管理ネットワークに使用されます。

これらのネットワークの詳細については、「ネットワーク接続」を参照してください。

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



a. ノードのデータディスクのサイズを指定します。

   必要なデータ ボリュームにはデフォルト値を使用することを推奨します。

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

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

b. **パスワード**を入力して確認します。

   このパスワードは、各ノードの rescue-user アカウントに使用されます。すべてのノードに同じパスワードを設定することを推奨しますが、2 番目と 3 番目のノードに異なるパスワードを指定することもできます。

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

d. **管理ネットワーク**の IP ゲートウェイを入力します。

e. [次へ（Next）] をクリックして次に進みます。

12. **[完了準備（Ready to complete）]** 画面で、すべての情報が正しいことを確認し、**[終了（Finish）]** をクリックしてノードの展開を開始します。
13. VM の展開が完了したら、VM の電源をオンにします。
14. ノードをマスターまたはスタンバイとして追加します。

    ノードを展開したら、クラスタに追加できます。

    - ノードをワーカーノードとして追加するには、「ワーカーノードの管理」を参照してください。
    - ノードをスタンバイノードとして追加するには、「スタンバイノードの管理」を参照してください。

ESXi での ESX ノードの直接展開

はじめる前に

「ESX ノードの前提条件と ガイドライン」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。

ここでは、vCenter を使用して VMware ESXi で追加の Cisco Nexus Dashboard ノードを展開する方法について説明します。

1. Cisco Nexus Dashboard OVA イメージを取得します。
   a. [ソフトウェア ダウンロード（Software Download）] ページを参照します。

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

   b. ダウンロードする Nexus Dashboard のバージョンを選択します。
   c. Nexus Dashboard OVA イメージの横にある**ダウンロード**アイコンをクリックします（nd-dk9.<version>.ova）。
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。
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。
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。
5. [OVF と VMDK ファイルの選択（Select OVF and VMDK files）] 画面で、仮想マシン名（nd- node-worker1 など）と最初の手順でダウンロードした OVA イメージを入力し、[次へ（Next）] をクリックします。
6. [Select storage] 画面で、VM のデータストアを選択し、[Next] をクリックします。
7. [OVF と VMDK ファイルの選択（Select OVF and VMDK files）] 画面で、仮想マシン名（nd- node-worker1 など）と最初の手順でダウンロードした OVA イメージを入力し、[次へ（Next）] をクリックします。
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。

   ネットワークは 2 つあり、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。
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。
10. VM の展開が終了するまで待ち、VMware ツールの定期的な時刻同期が無効になっていることを確認してから、VM を起動します。

    時刻の同期を無効にするには、次の手順を実行します。
    a. ノードの VM を右クリックして、[設定の編集（Edit Settings）] を選択します。
    b. [設定の編集]ウィンドウで、[VM オプション]タブを選択します。
    c. [VMware ツール]カテゴリを展開し、[ホストとゲスト時刻の同期]オプションのチェックボックスをオフにします。

11. ノードのコンソールを開き、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。

    初回のセットアップ ユーティリティを実行するようにプロンプトが表示されます。

    ```
    [ OK ] Started atomix-boot-setup.
    Starting Initial cloud-init job (pre-networking)...
    Starting logrotate...
    Starting logwatch...
    Starting keyhole...
    [ OK ] Started keyhole.
    [ OK ] Started logrotate.
    [ OK ] Started logwatch.
    Press any key to run first-boot setup on this console...
    ```

    b. admin パスワードを入力し、確認します。

    このパスワードは、レスキューユーザーが SSH ログインする際、およびこのノードをクラスタに追加する際に使用します。

    ```
    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。

    ```
    構成を確認してください
    Management network:
    Gateway: 192.168.9.1
    IP Address/Mask: 192.168.9.172/24
    Re-enter config? (y/N): n
    ```

12. ノードをマスターまたはスタンバイとして追加します。

ノードを展開したら、クラスタに追加できます。

- ノードをワーカーノードとして追加するには、「ワーカーノードの管理」を参照してください。
- ノードをスタンバイノードとして追加するには、「スタンバイノードの管理」を参照してください。

Linux KVM での追加の仮想ノードの展開

クラスタの初期展開については、『*Cisco Nexus Dashboard 展開ガイド*』を参照してください。ここからのセクションでは、ワーカーまたはスタンバイノードとして追加のノードを Linux KVM に展開する方法について説明します。

既存のクラスタにノードを追加する場合、追加ノードは、クラスタ内にある残りのノードと同じフォームファクタ(物理または仮想)である必要があります。このリリースは、異なるフォームファクタのノードを持つクラスタには対応していません。

追加ノードを展開した後、そのロールに基づいてそのノードを登録し、クラスタに追加できます。

- ワーカーノードの詳細については、「ワーカーノードの管理」を参照してください。
- スタンバイノードの詳細については、「スタンバイノードの管理」を参照してください。

KVM ノードの前提条件とガイドライン

- 「プラットフォームの 概要」で説明されている一般的な前提条件、特にネットワークとファブリックの接続性のセクション事前にを確認し、条件を満たします。
- このリリースでは、最大 6 つのワーカーノードと合計 2 つのスタンバイノードを持つ KVM クラスタがサポートされます。
- VM に十分なリソースがあることを確認します。

表 7. サポート対象ハードウェア

Nexus Dashboard バージョン	VM の要件
リリース 2.1.1	- Linux カーネル 3.10.0-957.el7.x86_64 以降、KVM libvirt-4.5.0-23.el7_7.1.x86_64 以降 ノード VM には次が必要です。 - 16 vCPU - 48 GB 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。 # fio --rw=write --ioengine=sync --fdatasync=1 --directory=test-data_with_se --size=22m --bs=2300 --name=mytest And confirm that the 99.00th=[<value>] in the fsync/fdatasync/sync_file_range section is under 20ms. 各 Nexus Dashboard ノードは、異なる KVM サーバーに展開することを推奨します。

KVM ノードの展開

はじめる前に

「KVM ノードの前提条件と ガイドライン」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。

ここでは、Linux KVM で追加の Cisco Nexus Dashboard ノードを展開する方法について説明します。

1. Cisco Nexus Dashboard の qcow2 イメージを取得します。
   a. [ソフトウェア ダウンロード（Software Download）] ページを参照します。

      https://software.cisco.com/download/home/286324815/type

   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 Dashboard のイメージ（nd-dk9.<version>.qcow2）をダウンロードします。
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。

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のディレクトリを作成します。

      次の手順は、/home/nd-node-worker1 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-node-worker1/
      # cd /home/nd-node-worker1
      ```

   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-node-worker1/nd-node-worker1-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 Dashboard 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。

      # quemu-img create -f qcow2 /home/nd-node-worker1/nd-node-worker1-disk2.qcow2 500G

      次の手順に進む前に、/home/nd-node- worker1/ ディレクトリに 2 つのディスクイメージがある必要があります。

      - /home/nd-node-worker1/nd-node-worker1-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-node-worker1/nd-node-worker1-disk2.qcow2 は、作成した新しい 500GB のディスクです。

4. ノードの VM を作成します。

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

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

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

c. **[既存のストレージパスを指定（Provide existing storage path）]**フィールドで **[参照（Browse）]** をクリックし、nd-node-worker1- disk1.qcow2 ファイルを選択します。

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

d. OS タイプとバージョンに[汎用]を選択し、[進む]をクリックします。

e. 48GB のメモリと 16 個の CPU を指定し、[進む]をクリックします。

f. 仮想マシンの名前（例：nd-node-worker1）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。

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（Customize configuration before install）]** 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（VM details）] ウィンドウが開きます。

5. VM の詳細ウィンドウで、NIC のデバイスモデルを変更します。
   a. NIC <mac>を選択します。
   b. [デバイス モデル] で、[e1000] を選択します。
6. VM の詳細ウィンドウで、2 番目の NIC を追加します。
   a. [ハードウェアを追加（Add Hardware）] をクリックします。
   b. **[新しい仮想ハードウェアの追加（Add new virtual hardware）]** 画面で、**[ネットワーク]** を選択します。
   c. **[ネットワークソース（Network Source）]** で、KVM ホストのデバイスを選択します。
   d. デフォルトの MAC アドレス の値のままにします。
   e. **[デバイス モデル]** で、[e1000] を選択します。
7. **[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（Add new virtual hardware）]** 画面で、**[ストレージ（Storage）]** を選択します。
   c. **[カスタムストレージの選択または作成（Select or create custom storage）]** を選択し、**[管理（Manage）]**をクリックして、作成した nd-node-worker1- disk2.qcow2 ファイルを選択します。
   d. **[終了（Finish）]** をクリックして 2 番目のディスクを追加します。
8. 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。
9. VM を起動します。
10. ノードのコンソールを開き、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。

    初回のセットアップ ユーティリティを実行するようにプロンプトが表示されます。

```
[ OK ] Started atomix-boot-setup.
Starting Initial cloud-init job (pre-networking)...
Starting logrotate...
Starting logwatch...
Starting keyhole...
[ OK ] Started keyhole.
[ OK ] Started logrotate.
[ OK ] Started logwatch.
Press any key to run first-boot setup on this console...
```

b. admin パスワードを入力し、確認します。

このパスワードは、レスキューユーザーが SSH ログインする際、およびこのノードをクラスタに追加する際に使用します。

```
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。

```
構成を確認してください
Management network:
Gateway: 192.168.9.1
IP Address/Mask: 192.168.9.172/24
Re-enter config? (y/N): n
```

11. ノードをマスターまたはスタンバイとしてクラスタに追加します。

ブートストラッププロセスが完了したら、クラスタに追加できます。

- ノードをワーカーノードとして追加するには、「ワーカーノードの管理」を参照してください。
- ノードをスタンバイノードとして追加するには、「スタンバイノードの管理」を参照してください。

ワーカーノードの管理

既存の 3 ノードクラスタに複数のワーカーノードを追加して水平方向にスケーリングし、アプリケーションの共同ホスティングを実現できます。

アプリケーションの共同ホスティングとクラスタサイジングの詳細については、このドキュメントの「プラットフォームの概要」セクションを参照してください。

ワーカーノードは、AWS または Azure に展開された Nexus Dashboard クラスタのクラウドフォームファクタではサポートされません。

ワーカー ノードの追加

ここでは、ワーカーノードをクラスタに追加して水平スケーリングを可能にする方法について説明します。

はじめる前に

- 既存のマスターノードとクラスタが正常であることを確認します。
- 「追加の物理ノードの展開」、「VMware ESX での 追加の仮想ノードの展開」、「ESXi での ESX ノードの直接展開」、または「Linux KVM での 追加の仮想ノードの展開」の説明に従って、新しいノードを準備して展開します。
- 追加するノードの電源がオンになっていることを確認します。
- 物理ノードを追加する場合は、新しいノードの CIMC IP アドレスとログイン情報があることを確認します。

  Nexus ダッシュボード GUI を使用して新しいノードを追加するには、CIMC 情報を使用する必要があります。
- 仮想ノードを追加する場合は、ノードの管理 IP アドレスとログイン情報があることを確認します。

ワーカーノードを追加するには、次の手順を実行します。

1. Cisco Nexus Dashboard の GUI にログインします。
2. メイン ナビゲーション メニューから、**[システムリソース（System Resources）] > [ノード（Nodes）]** を選択します。
3. メインペインで、**[ノードの追加（Add Node）]** をクリックします。

   [ノードの追加（Add Node）] 画面が開きます。
4. **[ノードの追加（Add Node）]** 画面で、ノードの情報を入力します。
   a. ノードの **[名前（Name）]** を入力します。
   b. **[タイプ（Type）]** ドロップダウンから [ワーカー（Worker）] を選択します。
   c. ノードの **[クレデンシャル（Credentials）]** 情報を入力し、**[検証（Verify）]** をクリックします。

      物理ノードの場合、これはサーバーの CIMC の IP アドレス、ユーザー名、およびパスワードです。CIMC は、ノードの残りの情報を設定するために使用されます。

      仮想ノードの場合、これは展開時にノードに定義した IP アドレスと rescue-user パスワードです。
   d. **[管理ネットワーク（Management Network）]** 情報を入力します。

仮想ノードの場合、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 アドレスとログイン情報に基づいてノードから取得された情報が事前に入力されます。

物理ノードの場合、ここで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指定する必要があります。

e. **[データネットワーク（Data Network）]** 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。

f. （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。

IPv6 情報を入力する場合は、ノードの追加時に行う必要があります。

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。

5. **[保存（Save）]** をクリックしてノードを追加します。

設定がノードにプッシュされ、ノードが GUI のリストに追加されます。

1. Nexus Dashboard Insights アプリケーションを実行している場合は、アプリケーションを無効にしてから再度有効にします。

新しいワーカーノードを追加した後、サービスを新しいノードに適切に配布するには、アプリケーションを無効にしてから再度有効にする必要があります。

ワーカー ノードの削除

はじめる前に

- マスターノードとクラスタが正常であることを確認します。

既存のワーカーノードを削除するには、次の手順を実行します。

1. Cisco Nexus Dashboard の GUI にログインします。
2. メイン ナビゲーション メニューから、**[システムリソース（System Resources）] > [ノード（Nodes）]** を選択します。
3. 削除するワーカーノードの横にあるチェックボックスをオンにします。
4. **[アクション（Actions）]** メニューから **[削除（Delete）]** を選択してノードを削除します。

スタンバイノードの管理

最大 2 つのスタンバイノードを追加できます。1 つ以上のマスターノードに障害が発生した場合に、障害が発生したマスターノードをスタンバイノードで置き換えることで、クラスタ機能を迅速に復元できます。

展開、初期設定、およびアップグレードに関しては、スタンバイノードはワーカーノードに似ています。ただし、ワーカーノードとは異なり、クラスタはワークロードにスタンバイノードを使用しません。

スタンバイノードは、AWS または Azure に導入された単一ノードのクラスタではサポートされません。

次の 2 つのケースがサポートされます。

- 1 つのマスターノードで障害が発生

  UI を使用して、スタンバイノードを新しいマスターノードに変換できます。

- 2 つのマスターノードで障害が発生

  クラスタ機能を復元するには、いずれかのノードの手動フェールオーバーを実行する必要があります。次に、標準的手順を使用して 2 番目のノードをフェールオーバーします。

スタンバイノードの追加

ここでは、マスターノードに障害が発生した場合にクラスタを簡単に回復できるように、クラスタにスタンバイノードを追加する方法について説明します。

はじめる前に

- 既存のマスターノードとクラスタが正常であることを確認します。
- 「追加の物理ノードの展開」、「VMware ESX での 追加の仮想ノードの展開」、「ESXi での ESX ノードの直接展開」、または「Linux KVM での 追加の仮想ノードの展開」の説明に従って、新しいノードを準備して展開します。

  フェールオーバーできるのは同じタイプのノード間のみであるため、交換が必要になる可能性のあるクラスタ内のノードと同じタイプのノードを展開する必要があります。2 つのノードプロファイル（OVA-app および OVA-data）を持つ VMware ESX に展開された仮想ノードの場合は、同じプロファイルのノード間でもフェールオーバーできます。

- 追加するノードの電源がオンになっていることを確認します。
- 物理ノードを追加する場合は、新しいノードの CIMC IP アドレスとログイン情報があることを確認します。

  Nexus ダッシュボード GUI を使用して新しいノードを追加するには、CIMC 情報を使用する必要があります。

- 仮想ノードを追加する場合は、ノードの管理 IP アドレスとログイン情報があることを確認します。

スタンバイノードを追加するには、次の手順を実行します。

1. Cisco Nexus Dashboard の GUI にログインします。
2. メイン ナビゲーション メニューから、**[システムリソース（System Resources）] > [ノード（Nodes）]** を選択します。
3. メインペインで、**[ノードの追加（Add Node）]** をクリックします。

   [ノードの追加（Add Node）] 画面が開きます。

4. **[ノードの追加（Add Node）]** 画面で、ノードの情報を入力します。
   a. ノードの **[名前（Name）]** を入力します。
   b. **[タイプ（Type）]** ドロップダウンから [スタンバイ（Standby）] を選択します。

c. ノードの **[クレデンシャル（Credentials）]** 情報を入力し、**[検証（Verify）]** をクリックします。

物理ノードの場合、これはサーバーの CIMC の IP アドレス、ユーザー名、およびパスワードです。CIMC は、ノードの残りの情報を設定するために使用されます。

仮想ノードの場合、これは展開時にノードに定義した IP アドレスと rescue-user パスワードです。

d. **[管理ネットワーク（Management Network）]** 情報を入力します。

仮想ノードの場合、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 アドレスとログイン情報に基づいてノードから取得された情報が事前に入力されます。

物理ノードの場合、ここで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指定する必要があります。

e. **[データネットワーク（Data Network）]** 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。

f. （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。

IPv6 情報を入力する場合は、ノードの追加時に行う必要があります。

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。

5. **[保存（Save）]** をクリックしてノードを追加します。

設定がノードにプッシュされ、ノードが GUI のリストに追加されます。

単一のマスターノードとスタンバイノードの置換

ここでは、事前に設定したスタンバイノードを使用したフェールオーバーについて説明します。クラスタにスタンバイノードがない場合は、代わりに「トラブルシューティング」のセクションの 1 つで説明されている手順に従ってください。

はじめる前に

- 少なくとも 2 つのマスターノードが正常であることを確認します。

  2 つのマスターノードを使用できない場合は、「2 つのマスターノードをスタンバイノードに置き換える」の説明に従って、クラスタを手動で復元する必要があります。

- クラスタ内に使用可能なスタンバイノードが少なくとも 1 つあることを確認してください。

  スタンバイノードのセットアップと設定については、「スタンバイノードの追加」で説明されています。

- 置換するマスターノードの電源がオフになっていることを確認します。

フェールオーバーの完了後に、置換するマスターノードをクラスタに再度追加することはできません。置換するマスターノードがまだ機能していて、フェールオーバー後にクラスタに再度追加する場合は、工場出荷時にリセット(acs factory-reset)するか、イメージを再作成して、スタンバイノードまたはマスターノードとしてのみ追加する必要があります。

単一のマスターノードをフェールオーバーするには、次の手順を実行します。

1. Cisco Nexus Dashboard の GUI にログインします。
2. メイン ナビゲーション メニューから、**[システムリソース（System Resources）] > [ノード（Nodes）]** を選択します。
3. 交換する非アクティブなマスターノードの横にある **[アクション（Actions）]**（**[...]**）メニューをクリックします。
4. **[フェールオーバー（Failover）]** を選択します。

   スタンバイノードがすでに構成および追加されている必要があることに注意してください。そうでない場合、**[フェールオーバー（Failover）]** メニューオプションは使用できません。
5. **[フェールオーバー（Fail Over）]** ウィンドウが開いたら、ドロップダウンからスタンバイノードを選択します。
6. **[保存（Save）]** をクリックして、フェールオーバーを完了します。

   障害が発生したマスターノードがリストから削除され、選択したスタンバイノードに置き換えられます。サービスが新しいマスターノードに復元されている間、非アクティブステータスが維持されます。

   すべてのサービスが復元されるまでに最大 10 分かかる場合があり、その時点で新しいマスターノードのステータスがアクティブに変わります。

2 つのマスターノードとスタンバイノードの置換

ここでは、事前に設定したスタンバイノードを使用したフェールオーバーについて説明します。クラスタにスタンバイノードがない場合は、「トラブルシューティング」のいずれかの項に記載されている手順に従ってください。

マスターノードのうち 1 つのみに障害が発生した場合は、「単一マスターノードのスタンバイノードへの置換」の説明に従って、GUI を使用してスタンバイノードに置き換えることができます。

ただし、2 つのマスターノードが使用できない場合、クラスタ全体が読み取り専用モードになります。この場合、UI を含むほとんどの操作が無効になり、クラスタに変更を加えることができません。ここでは、障害が発生したマスターノードの 1 つをスタンバイノードにフェールオーバーしてクラスタを回復させ、通常の操作を復元する方法について説明します。復元した時点で、通常の手順を使用して 2 番目のマスターノードを回復できます。

はじめる前に

- クラスタ内に使用可能なスタンバイノードが少なくとも 1 つあることを確認してください。

  スタンバイノードのセットアップと設定については、「スタンバイノードの追加」で説明されています。
- 交換するマスターノードの電源がオフになっていることを確認します。

フェールオーバーの完了後に、置換するマスターノードをクラスタに再度追加することはできません。置換するマスターノードがまだ機能していて、フェールオーバー後にクラスタに再度追加する場合は、工場出荷時にリセット(acs factory-reset)するか、イメージを再作成して、スタンバイノードまたはマスターノードとしてのみ追加する必要があります。

2 つのマスターノードをフェールオーバーするには、次の手順を実行します。

1. CLI 経由で rescue-user として残りのマスターノードにログインします。
2. failover コマンドを実行します。

   次のコマンドで、<node1-data-ip> と <node2-data-ip> を障害が発生したノードのデータネットワーク IP アドレスに置き換えます。

   ```
   # acs failover --failedIP <node1-data-ip> --failedIP <node2-data-ip>
   ```

   最初のノードだけがフェールオーバーされますが、クラスタを回復するには、指定した 2 番目のノードが内部で必要です。

   デフォルトでは、正常なマスターノードが使用可能なスタンバイノードを自動的に選択し、最初に障害が発生したノード（<node1-data-ip>）をフェールオーバーします。

   特定のスタンバイノードを指定する場合は、<standby-node-data-ip> を上記のコマンドに追加できます。

   ```
   # acs failover --failedIP <node1-data-ip> --failedIP <node2-data-ip> \
     --standbyIP <standby-node1-data-ip>
   ```

3. 操作を続行することを確定します。

   ```
   警告：フェールオーバーは中断を伴う操作になる可能性があるため、2 つのマスターノードがハードウェア障害により動作しなくなった際に障害からクラスタを回復するための最終手段としてのみ実行してください。
   Proceed? (y/n): y
   ```

   マスターノードが設定の状態をスタンバイノードにコピーし、両方のノードが再起動します。ノードが起動してラスタが復元されるまでに最長 30 分かかる場合があります。マスターノードの UI に移動して、進行状況を確認できます。

4. クラスタがバックアップされたら、2 番目に障害が発生したマスターノードをフェールオーバーします。

   ここからは「単一のマスターノードと スタンバイノードの置換」に記載されている標準的な手順を使用できます。

スタンバイノードの削除

はじめる前に

- マスターノードとクラスタが正常であることを確認します。

既存のスタンバイノードを削除するには、次の手順を実行します。

1. Cisco Nexus Dashboard の GUI にログインします。
2. メイン ナビゲーション メニューから、**[システムリソース（System Resources）] > [ノード（Nodes）]** を選択します。
3. 削除するスタンバイノードの横にあるチェックボックスをオンにします。
4. **[アクション（Actions）]** メニューから **[削除（Delete）]** を選択してノードを削除します。

管理

Nexus Dashboard の GUI にログインするユーザーの認証方法を選択できます。今回のリリースでは、ローカル認証に加えて、LDAP、RADIUS、および TACACS リモート認証サーバーもサポートしています。ユーザーのロールと権限についてはこのセクションで、リモート認証の設定については「リモート認証」で、ローカルユーザーの設定については「ユーザー」で説明します。

ロールとアクセス許可

Cisco Nexus Dashboard では、ロールベース アクセス コントロール(RBAC)で定義されているロールに応じて、ユーザーはアクセスが許可されます。ロールはローカル認証と外部認証の両方で使用され、Nexus Dashboard やそこで実行されているサービスに適用されます。すべてのロールに、読み取り専用または書き込み権限を割り当てることができます。読み取り専用アクセスではユーザーはオブジェクトと設定を表示でき、書き込みアクセスではユーザーは変更を加えることができます。

次のセクションに、Nexus Dashboard で使用可能なユーザーロールとプラットフォーム内で関連付けられている権限、および個々のサービスを示します。

Nexus Dashboard Insights および Orchestrator のロール

ユーザロール	ND プラットフォーム	オーケストレータサービス	Insights サービス
管理者	すべての設定、機能、タスクへのフルアクセスが許可されます。 サービスの追加と削除を実行できる唯一のロールです。	フルアクセス。	フルアクセス。
承認者	ダッシュボードのロールと同じです。	テンプレート設定の承認または拒否を実行できます。テンプレートの編集や展開は実行できません。	なし
ダッシュボードユーザー	ダッシュボードビューへのアクセスとアプリケーションの起動を実行できますが、Nexus Dashboard の設定は変更できません。	アクセス権なし。	読み取り専用アクセス権
展開担当者	ダッシュボードのロールと同じです。	テンプレートをサイトに展開できますが、テンプレートの編集や承認は実行できません。	なし

ユーザロール	ND プラットフォーム	オーケストレータサービス	Insights サービス
ポリシー マネージャ	ダッシュボードのロールと同じです。	アクセス権なし。	アクセス権なし。
サイト管理者	サイトのオンボーディングと構成に関連する設定にアクセスできます。	サイトのステータスをマネージドまたはアンマネージドに切り替えられます。	アクセス権なし。
サイトマネージャ	サイト管理者ロールと同じです。	サイト、インフラ、テナント、スキーマ、ポリシーを設定できます。	すべてのファブリックを設定できます。
テナントマネージャ	ダッシュボードのロールと同じです。	インフラ、テナント、スキーマを設定できます。	すべてのファブリックを設定できます。
ユーザーマネージャ	ユーザーの作成、権限の変更、リモート認証プロバイダーの追加などのユーザー設定にアクセスできます。	アクセス権なし。	アクセス権なし。

上記の各ロールは、一連の権限に関連付けられています。これらの権限は、関連する要素を表示し、関連しない要素をユーザーのビューから非表示にするために使用されます。たとえば、次の図は、ユーザーマネージャとサイト管理者の権限を持つユーザーに表示される GUI 画面を示しています。ナビゲーションメニューには使用できる他のカテゴリのメモのみがあります。

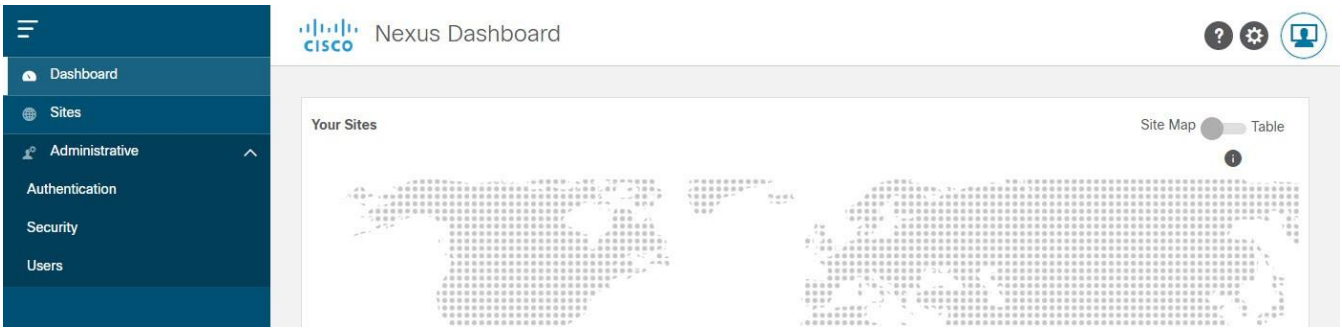


図 17. ロールベースの GUI アクセス

リモート認証サーバーで同じロールを設定し、そのサーバーを使用して Nexus Dashboard ユーザーを認証できます。リモート認証の詳細については、「リモート認証」セクションを参照してください。

Nexus Dashboard Data Broker ロール

Nexus Dashboard Data Broker サービスでは、Insights にリストされている Nexus Dashboard ロールと Orchestrator ロールから任意のものを使用できます。これらはすべて実質的には同じです。いずれかのロールが書き込み権限を持つユーザーに割り当てられている場合、そのユーザーは Data Broker サービスでネットワーク管理者ロールを持ちます。割り当てられているロールが読み取り権限のみのユーザーは、Data Broker サービスのネットワーク オペレータロールを持ちます。

Nexus Dashboard Fabric ファブリック コントローラ ロール

ユーザロール	Nexus ダッシュボード ファブリック コントローラ
NDFC アクセス管理者	NDFC の **インターフェイスマネージャ**画面で、ネットワーク インターフェイスに関連する操作を実行できます。 アクセス管理者は、次のアクションを実行できます。 ・レイヤ 2 ポート チャネル、および vPC を追加、編集、削除、展開します。 ・ホスト vPC、およびイーサネット インターフェイスを編集します。 ・管理インターフェイスからの保存、プレビュー、および展開。 ・LAN クラシックのインターフェイス、およびポリシーに関連付けられていない場合は外部ファブリックを編集します。nve、管理、トンネル、サブインターフェイス、SVI、インターフェイスグループ化、およびループバック インターフェイスを除く ただし、アクセス管理者は次のアクションを実行できません。 ・レイヤ 3 ポートチャネル、ST FEX、AA FEX、ループバック インターフェイス、nve インターフェイス、およびサブインターフェイスは編集できません。 ・レイヤ 3、ST FEX、AA FEX のメンバーインターフェイスおよびポートチャネルは編集できません。 ・アンダーレイとリンクから関連付けられたポリシーを持つインターフェイスは編集できません。 ・ポートチャネルのようなピアは編集できません。 ・管理インターフェイスを編集できません。 ・トンネルを編集できません。
NDFC デバイス アップグレード管理者	NDFC のイメージ管理画面でデバイスのアップグレードに関連する操作を実行できます。
NDFC ネットワーク管理者	完全な管理アクセスを許可します。

ユーザロール	Nexus ダッシュボード ファブリック コントローラ
NDFC ネットワークオペレータ	次の NDFC メニューへの読み取り専用アクセスを許可します。 ・ダッシュボード ・トポロジ ・モニタ（Monitor） ・アプリケーション ネットワークオペレータのユーザーは、以下を表示できます。 ・ファブリックビルダー ・ファブリックの設定 ・設定のプレビュー ・ポリシー ・テンプレート （Templates） ただし、ネットワークオペレータは次の操作を実行できません。 ・ファブリック内のスイッチの予期される構成を変更できません。 ・スイッチに構成を展開できません。 ・ライセンス、追加ユーザーの作成などの管理オプションにアクセスできません。

ユーザロール	Nexus ダッシュボード ファブリック コントローラ
NDFC ネットワークステージャ	構成の変更を行うことができますが、ネットワーク管理者ユーザーがその変更を後で展開する必要があります。 ネットワークステージャのユーザーは、次のアクションを実行できます。 ・インターフェイス構成の編集 ・ポリシーの表示または編集 ・インターフェイスの作成 ・ファブリック設定の変更 ・テンプレートの編集または作成 ただし、ネットワークステージャは次のアクションを実行できません。 ・スイッチに設定を展開できません。 ・DCNM Web UI または REST API から展開関連のアクションを実行できません。 ・ライセンス、追加ユーザーの作成などの管理オプションにアクセスできません。 ・スイッチをメンテナンスモードに入れるか解除するかの切り替えはできません。 ・ファブリックを展開フリーズモードに入れるか解除するかの切り替えはできません。 ・パッチをインストールできません。 ・スイッチをアップグレードできません。 ・ファブリックを作成または削除できません。 ・スイッチをインポートまたは削除できません。 ネットワークステージャは、既存のファブリックのインテントのみを定義できますが、その構成を展開することはできません。ネットワーク ステージャ ロールを持つユーザーがステージングした変更および編集を展開できるのは、ネットワーク管理者です。

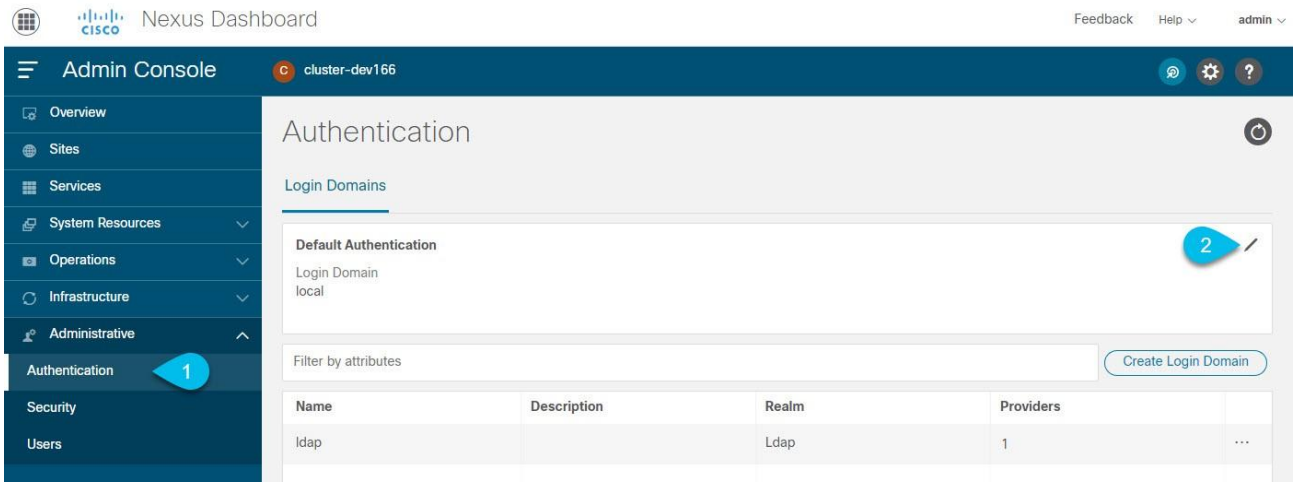
デフォルト認証ドメインの選択

デフォルトでは、ログイン画面でのユーザー認証でローカルドメインが選択されます。ドロップダウンメニューから使用可能なログインドメインのいずれかを選択して、ログイン時にドメインを手動で変更できます。

または、次のように、最も一般的に使用される別のデフォルトログインドメインを設定できます。

デフォルトドメインとして設定できるのは、既存のドメインに限られます。リモート認証ドメインの追加については、「リモート認証」を参照してください。

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. デフォルトのログインドメインを選択します。



   a. メイン ナビゲーション メニューから、**[管理（Administrative）] > [認証（Authentication）]** の順に選択します。

   b. **[デフォルト認証（Default Authentication）]** タイルの右上にある **[編集（Edit）]** アイコンをクリックします。

      [デフォルト認証（Default Authentication）] ウィンドウが開きます。

3. **[デフォルト認証（Default Authentication）]** が開いたら、ドロップダウンから **[ログインドメイン（Login Domain）]** を選択します。

リモート認証

Cisco Nexus Dashboard は、LDAP、TACACS、Radius などの多数のリモート認証プロバイダーをサポートしています。

外部認証サーバーを設定する場合は、次のことに注意してください。

- リモート認証サーバーの各ユーザーごとに設定を行う必要があります。
- すべての LDAP 設定は、大文字と小文字が区別されます。

  たとえば、LDAP サーバーに OU=Cisco Users、Nexus Dashboard に OU=cisco users がある場合、認証は機能しません。

- LDAP 設定のベストプラクティスは、属性文字列として CiscoAVPair を使用することです。何らかの理由でオブジェクト ID 1.3.6.1.4.1.9.22.1 を使用できない場合は、追加のオブジェクト ID 1.3.6.1.4.1.9.2742.1-5 を LDAP サーバーで使用することもできます。

  または、各ユーザーの Cisco AVPair 値を設定する代わりに、Nexus Dashboard で LDAP グループマップを作成できます。

- Nexus Dashboard、サイト、およびアプリケーション間のシングルサインオン(SSO)は、リモートユーザーのみが使用できます。
- SSO を使用して Nexus Dashboard の**[サイト]**ページから APIC サイトにクロス起動する場合、Nexus Dashboard ユーザーに対して定義された AV ペアは、APIC へのログイン時にも使用されます。

  たとえば、Nexus Dashboard クラスタの管理者として定義されたユーザーは、APIC での管理者権限も付与されます。

リモート認証サーバーの設定

Nexus Dashboard ユーザーのリモート認証サーバーを設定する際、ユーザー名とそのユーザーに割り当てられたロールを指定して、カスタム属性値(AV)のペアを追加する必要があります。

ユーザーロールとその権限は、「ロールと権限」で説明されているように、Nexus Dashboard GUI で直接設定するローカルユーザーと同じです。

次の表に、Nexus Dashboard のユーザーロールと、LDAP などのリモート認証サーバーでロールを定義するために使用する AV ペアを示します。

表 8. Nexus Dashboard AV ペア

ユーザロール	AV ペア値
管理者	admin
Approver	approver
ダッシュボードユーザー	app-user
展開担当者	deployer
ポリシー マネージャ	site-policy
サイト管理者	site-admin
サイト マネージャ	config-manager
テナントマネージャ	tenant-policy
ユーザーマネージャ	aaa

表 9. Nexus Dashboard Fabric Controller AV ペア

ユーザロール	AV ペア値
NDFC アクセス管理者	access-admin
NDFC デバイスアップグレード管理者	device-upg-admin
NDFC ネットワーク管理者	ネットワーク管理者
NDFC ネットワークオペレータ	network-operator
NDFC ネットワークステージャ	network-stager

AV ペアの文字列形式は、特定のユーザに読み取り/書き込みロールを設定するか、読み取り専用ロールを設定するか、または読み取り/書き込みロールと読み取り専用ロールの組み合わせを設定するかで異なります。通常の文字列にはドメインが含まれており、その後にスラッシュ（/）で区切って読み取り専用ロールからは切り離された読み取り/書き込みロールが続きます。個々のロールはパイプ（|）で区切られています。

```
shell:domains=<domain>/<writeRole1>|<writeRole2>/<readRole1>|<readRole2>
```

このリリースでは、全ドメインがサポートされています。シングルサインオン（SSO）機能をサポートするために APIC AV ペア形式との整合性を維持するためです。

たとえば次の文字列を使用すると、テナントマネージャロールとポリシーマネージャロールがユーザーに割り当てられると同時に、ユーザーマネージャユーザーに表示されるオブジェクトを参照できます。

```
shell:domains=all/tenant-policy|site-policy/aaa
```

読み取り専用権限のみ、または読み取り/書き込み権限のみをユーザーに設定する場合にも、スラッシュ（/）を含める必要があります。次の例は、サイト管理者ロールで使用可能なオブジェクトへの読み取り/書き込みアクセス権または読み取り専用アクセス権のみを設定する方法を示しています。

- 読み取り専用：shell:domains=all//site-admin
- 読み取り/書き込み：shell:domains=all/site-admin/

リモート認証プロバイダーとしての LDAP の追加

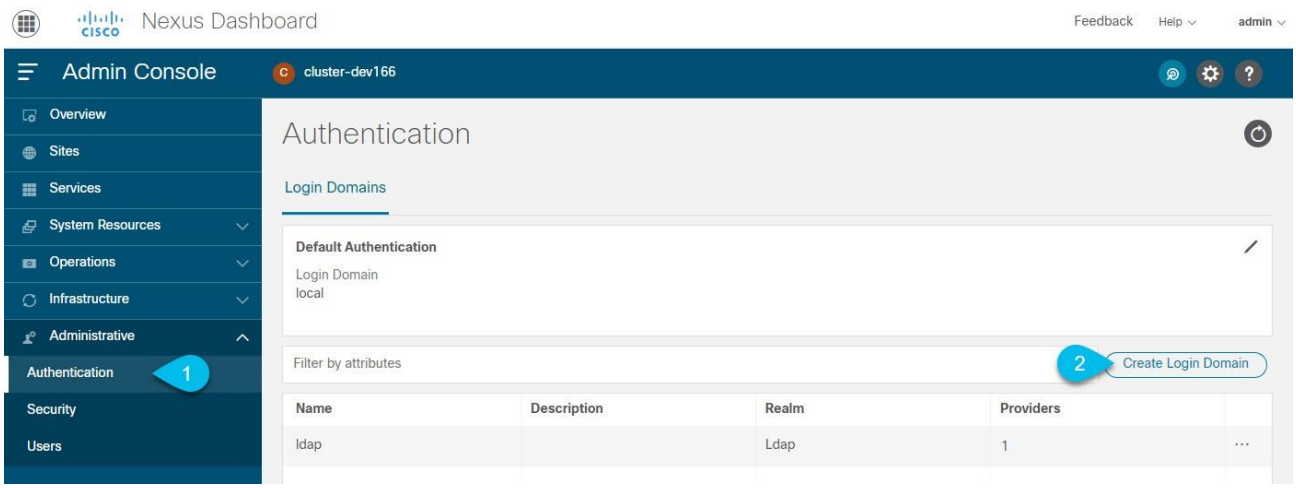
はじめる前に

- 「リモート認証サーバーの設定」の説明に従って、LDAP サーバーに 1 人以上のユーザーを設定しておく必要があります。

  LDAP 設定のエンドツーエンドの検証には、既存のユーザーを使用する必要があります。

LDAP リモート認証プロバイダーを追加するには、次の手順を実行します。

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. 認証ドメインを追加します。



   a. メイン ナビゲーション メニューから、**[管理（Administrative）] > [認証（Authentication）]** の順に選択します。

   b. メインペインの右上で、**[アクション（Actions）]** メニューをクリックし、**[ログインドメインの作成（Create Login Domain）]** を選択します。

3. **[ログインドメインの作成（Create Login Domain）]** 画面が開いたら、ドメインの詳細を入力します。

   a. **[名前（Name）]** にドメインの名前を入力します。

   b. （任意）**[説明（Description）]** にドメインの説明を入力します。

   c. **[レルム（Realm）]** ドロップダウンから [Ldap] を選択します。

   d. 次に、**[+プロバイダーの追加（+Add Provider）]** をクリックして、リモート認証サーバーを追加します。

      [プロバイダーの追加（Add Provider）] ウィンドウが開きます。

4. リモート認証サーバーの詳細を入力します。
   a. サーバーのホスト名を **[ホスト名（Hostname）]** に入力するか、IP アドレスを **[IP アドレス（IP Address）]** に入力します。
   b. （任意）サーバーの説明を **[説明（Description）]** に入力します。
   c. ポート番号を **[ポート（Port）]** に入力します。

      LDAP のデフォルトのポートは 389 です。

   d. ベース DN を **[ベース DN（Base DN）]** に、バインド DN を **[バインド DN（Bind DN）]** に入力します。

      ベース DN とバインド DN は、LDAP サーバーがどのように設定されているかによって異なります。LDAP サーバーで作成されたユーザーの識別名から、ベース DN とバインド DN の値を取得できます。

      ベース DN は、サーバーがユーザーを検索するポイントです。たとえば、DC=nd,DC=local です。

      バインド DN は、サーバに対する認証に使用されるクレデンシャルです。たとえば、CN=admin, CN=Users,DC=nd,DC=local のようになります。

   e. キーを **[キー（Key）]** に入力して確認します。

      これは、バインド DN ユーザーのパスワードです。匿名バインドはサポートされていないため、フィールドに有効な値を入力する必要があります。

   f. 認証サーバーに接続する際のタイムアウトを **[タイムアウト（Timeout）]** に、再試行回数を **[試行回数（Retries）]** に指定します。
   g. **[LDAP 属性（LDAP Attribute）]** フィールドに入力して、グループメンバーシップとロールを指定します。

      次の 2 つのオプションがサポートされています。

      - ciscoAVPair（デフォルト） - ユーザーロールの Cisco AVPair 属性で設定した LDAP サーバーに使用されます。
      - memberOf - LDAP グループマップで設定した LDAP サーバーに使用されます。グループマップの追加については、次のステップで説明します。

   h. （任意）LDAP 通信の場合は **[SSL]** を有効にします。

      SSL を有効にする場合は、**[SSL 証明書（SSL Certificate）]** と **[SSL 証明書検証タイプ（SSL Certificate Validation）]** も指定する必要があります。

      - [許可（Permissive）]：任意の認証局（CA）によって署名された証明書を受け入れ、暗号化に使用します。
      - [厳格（Strict）]：使用する前に証明書チェーン全体を確認します。

   i. （任意）**[サーバーのモニタリング（Server Monitoring）]** を有効にします。

      モニタリングを有効にする場合は、**[ユーザー名（Username）]** と **[パスワード（Password）]** も指定する必要があります。

   j. **[検証（Validation）]** フィールドに、追加する LDAP サーバーですでに設定されているユーザーの **[ユーザー名（Username）]**と **[パスワード（Password）]** を入力します。

      Nexus Dashboard はこのユーザー情報に基づいてエンドツーエンドの認証を検証し、入力した設定が妥当であるかを確認します。

k. **[保存（Save）]** をクリックしてプロバイダー設定を完了します。

l. このドメインで使用する LDAP 認証サーバーが他にもあれば、この手順を繰り返します。

5. （任意）**[LDAP グループマップルール（LDAP Group Map Rules）]** を有効にして設定します。

   Cisco AV ペア文字列を使用して LDAP ユーザーを認証する場合は、この手順をスキップしてください。

   a. **[LDAP 認証の選択（LDAP Auth Choice）]** で、[LDAP グループマップルール（LDAP Group Map Rules）] を選択します。

   b. **[LDAP グループ マップ ルールの追加（Add LDAP Group Map Rule）]** をクリックします。

      [LDAP グループマップルールの追加（Add LDAP Group Map Rule）] ウィンドウが開きます。

   c. グループの **[グループ DN（Group DN）]** を指定します。

   d. LDAP グループの **[ロール（Roles）]** を 1 つ以上選択します。

   e. **[保存（Save）]** をクリックしてグループ設定を保存します。

   f. 追加の LDAP グループがあれば、この手順を繰り返します。

6. **[作成（Create）]** をクリックして、ドメインの追加を終了します。

リモート認証プロバイダーとしての RADIUS または TACACS の追加

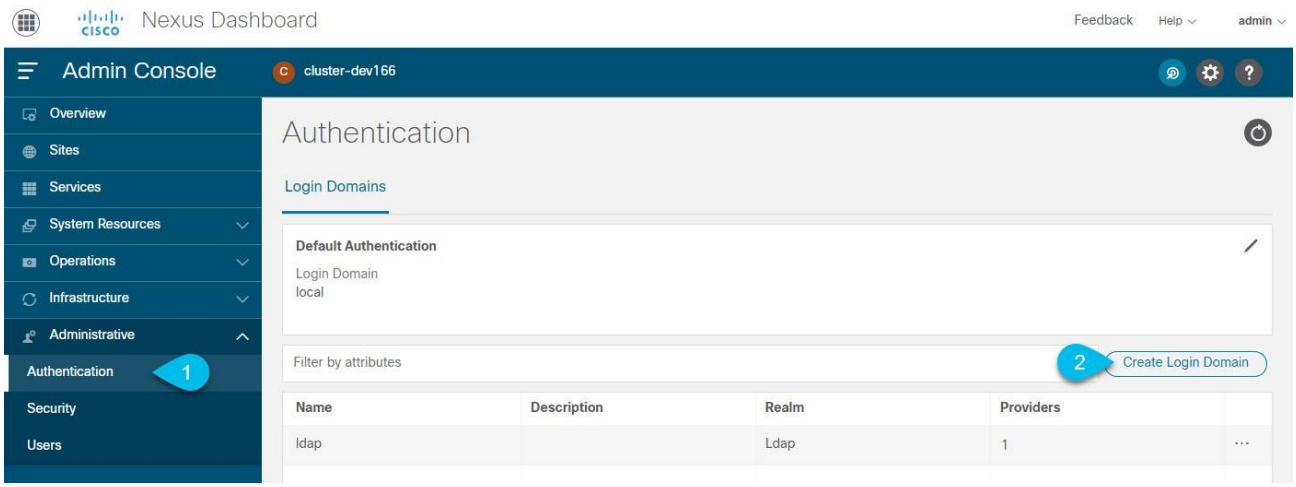
はじめる前に

- 「リモート認証サーバーの設定」の説明に従って、リモート認証サーバーに 1 人以上のユーザーを設定しておく必要があります。

  プロバイダー設定のエンドツーエンドの検証には、既存のユーザーを使用する必要があります。

Radius または TACACS リモート認証プロバイダーを追加するには、次の手順を実行します。

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. 認証ドメインを追加します。



   a. メイン ナビゲーション メニューから、**[管理（Administrative）] > [認証（Authentication）]** の順に選択します。

   b. メインペインの右上で、**[アクション（Actions）]** メニューをクリックし、**[ログインドメインの作成（Create Login Domain）]** を選択します。

3. **[ログインドメインの作成（Create Login Domain）]** 画面が開いたら、ドメインの詳細を入力します。
   a. **[名前（Name）]** にドメインの名前を入力します。
   b. （任意）**[説明（Description）]** にドメインの説明を入力します。
   c. **[レルム（Realm）]** ドロップダウンから [Radius] または [Tacacs] を選択します。
   d. 次に、**[+プロバイダーの追加（+Add Provider）]** をクリックして、リモート認証サーバーを追加します。

      [プロバイダーの追加（Add Provider）] ウィンドウが開きます。

4. リモート認証サーバーの詳細を入力します。
   a. サーバーのホスト名を **[ホスト名（Hostname）]** に入力するか、IP アドレスを **[IP アドレス（IP Address）]** に入力します。
   b. （任意）サーバーの説明を **[説明（Description）]** に入力します。
   c. サーバーが使用する**認証プロトコル**を選択します。

      [PAP]、[CHAP]、または [MS-CHAP] から選択します。

   d. ポート番号を **[ポート（Port）]** に入力します。

      デフォルトのポートは RADIUS に対して 1812、TACACS に対して 49 です。

   e. キーを **[キー（Key）]** に入力して確認します。

      これはプロバイダーサーバーへの接続で使用するパスワードです。

   f. （任意）**[サーバーのモニタリング（Server Monitoring）]** を有効にするかを選択します。

      モニタリングを有効にする場合は、**[ユーザー名（Username）]** と **[パスワード（Password）]** も指定する必要があります。

   g. **[検証（Validation）]** フィールドに、追加するリモートサーバーですでに設定されているユーザーの **[ユーザー名（Username）]** と **[パスワード（Password）]** を入力します。

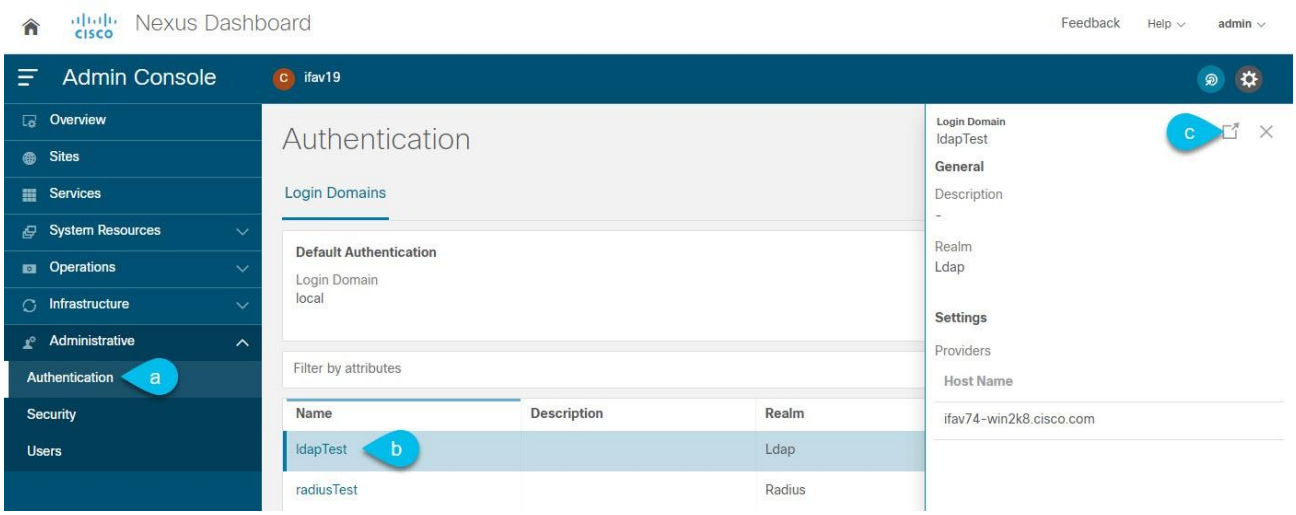
      Nexus Dashboard はこのユーザー情報に基づいてエンドツーエンドの認証を検証し、入力した設定が妥当であるかを確認します。

   h. **[保存（Save）]** をクリックしてプロバイダー設定を完了します。
   i. 追加のリモート認証サーバーがあれば、この手順を繰り返します。
5. **[作成（Create）]** をクリックして、ドメインの追加を終了します。

リモートユーザーログインの検証

Nexus Dashboard では、特定のユーザーのクレデンシャルを使用してログインを試行することで、リモート認証プロバイダーの到達可能性を検証できます。

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. テストするドメインに移動します。



a. メイン ナビゲーション メニューから、**[管理（Administrative）] > [認証（Authentication）]** の順に選択します。

b. 特定のドメインをクリックします。

c. 右側のプロパティサイドバーで、詳細アイコンをクリックします。

ドメインの **[概要（Overview）]** ページが開きます。

3. **[概要（Overview）]** ページで、テストするプロバイダーの横にある **[検証（Validate）]** をクリックします。

4. **[プロバイダーの検証（Validate Provider）]** ウィンドウで、この認証プロバイダーで定義されているユーザーの **[ユーザー名（Username）]** と **[パスワード（Password）]** を入力し、**[検証（Validate）]** をクリックします。

認証が成功したかどうかを示すメッセージが表示されます。

認証失敗メッセージが表示された場合は、認証プロバイダーのサーバーに到達可能であること、およびテストに使用したユーザーのクレデンシャルが有効になっており、プロバイダーで設定されていることを確認してください。

リモート認証ドメインの編集

作成したドメインに変更を加える場合は、次の手順を実行します。

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. メイン ナビゲーション メニューから、**[管理（Administrative）] > [認証（Authentication）]** の順に選択します。
3. ドメインの **[アクション（Actions）]** メニューから、**[ログインドメインの編集（Edit Login Domain）]** を選択します。

認証ドメインの名前とタイプは変更できませんが、説明とプロバイダー設定は変更できます。

単に説明を更新するなど、ログインドメインに変更を加えた場合は、既存のすべてのプロバイダーに対してキーを再入力する必要があります。

リモート認証ドメインの削除

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. メイン ナビゲーション メニューから、**[管理（Administrative）] > [認証（Authentication）]** の順に選択します。
3. ドメインの **[アクション（Actions）]** メニューから、**[ログインドメインの削除（Delete Login Domain）]** を選択します。

4. **[削除の確認（Confirm Delete）]** プロンプトで、**[OK]** をクリックして確定します。

多要素認証

リリース 2.1.2 以降、Nexus Dashboard でユーザーログインに多要素認証（MFA）を使用する設定が可能になりました。

多要素認証を設定する場合、次を実行します。

- 「MFA プロバイダーとしての Okta アカウントの構成」で説明されているように、MFA プロバイダーの各ユーザーを構成します。

  このリリースでは、MFA プロバイダーとして Okta のみがサポートされています。

- 「MFA クライアントの構成」で説明されているように、MFA プロバイダーとクライアントの統合を確立します。

  このリリースでは、MFA クライアントとして Duo のみがサポートされています。

- 「Okta をリモート認証プロバイダーとして追加する」で説明されているように、MFA プロバイダーを Nexus Dashboard の外部認証ドメインとして追加します。

MFA プロバイダーとしての Okta アカウントの構成

次の手順では、Okta をプロバイダーとして使用して Nexus Dashboard の MFA を有効にするために必要な基本設定を示します。詳細な Okta 設定は、このドキュメントの範囲外です。使用可能なすべてのオプションについては、Okta のドキュメントを参照してください。

Nexus Dashboard MFA 用に Okta を設定するには、次を実行します。

1. Okta アカウントにログインします。

   アカウントを作成するには、https://developer.okta.com にアクセスします。

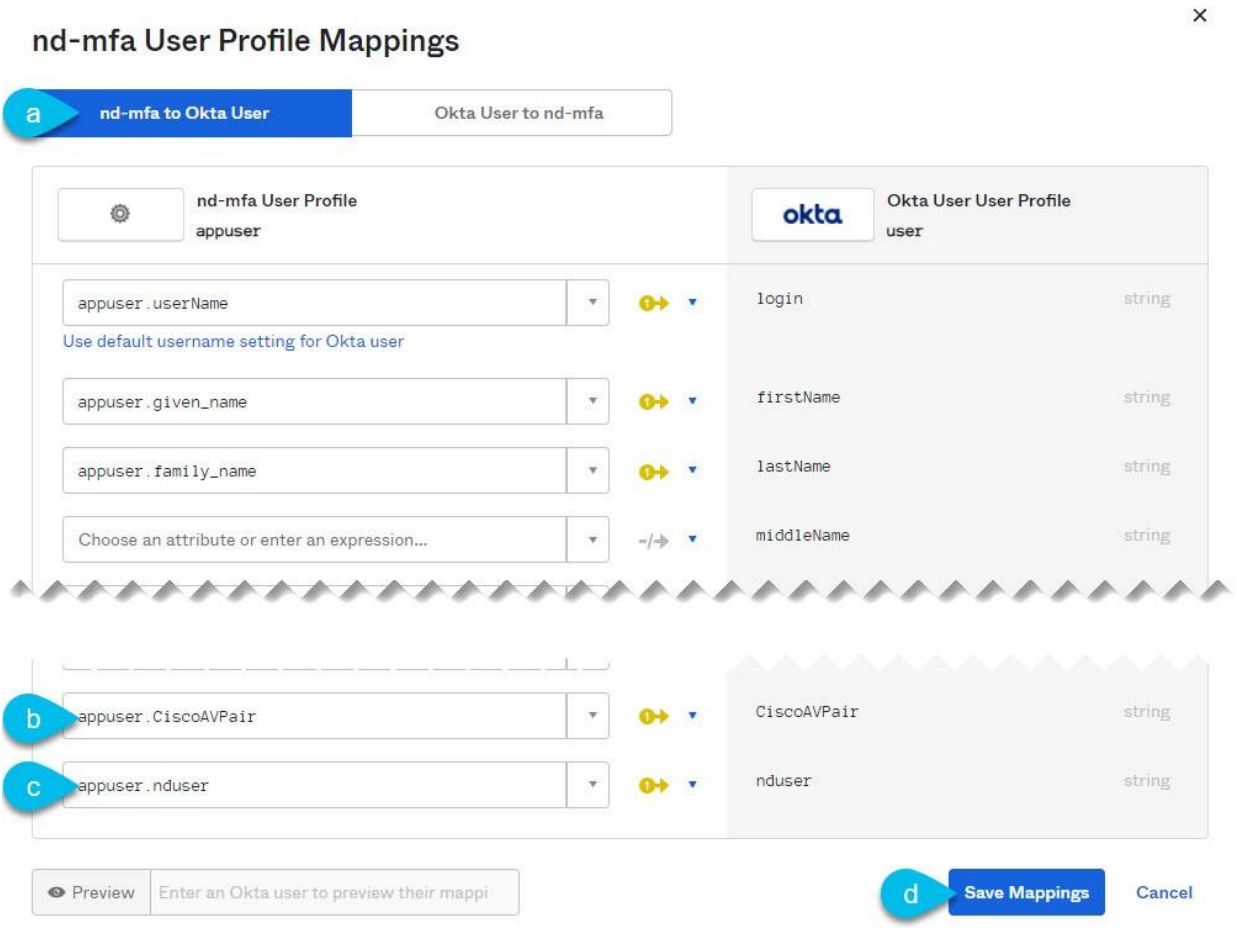
2. 新しいアプリ統合を作成します。
   a. 左側のナビゲーションメニューから、**[アプリケーション（Application）] > [アプリケーション（Application）]** を選択します。
   b. **[アプリケーション統合の作成（Create App Integration）]** をクリックします。
   c. **[サインイン方法（Sign-in method）]** は、[OIDC - OpenID 接続（OIDC - OpenID Connect）] を選択します。
   d. **[アプリケーションタイプ（Application Type）]** は、[Web アプリケーション（Web Application）] を選択します。
   e. [次へ（Next）] をクリックします。
   f. **[アプリケーション統合名（App integration name）]** を指定します。たとえば nd-mfa です。

      次の手順では、アプリ統合名として nd-mfa を使用していることを前提としています。別の名前を選択する場合は、必要に応じて nd-mfa を置き換えます。
   g. **[サインインリダイレクト URI（Sign-in redirect URIs）]** には、*https://<nd-node1-ip>/oidccallback* を入力します。

      次に、**[+URI の追加（+Add URI）]** をクリックして、クラスタ内のすべてのノードの URI を指定します。
   h. **[制御されたアクセス（Controlled Access）]** で、[今はグループの割り当てをスキップ（Skip group assignment for now）] を選択します。
   i. その他のフィールドはデフォルト値のままにして、**[保存（Save）]** をクリックします。
3. 必要な属性をデフォルトユーザーに追加します。
   a. 左側のナビゲーションメニューから、**[ディレクトリ（Directory）] > [プロファイル エディタ（Profile Editor）]** を選択します。
   b. **Okta ユーザー（デフォルト）** のプロファイルをクリックします。
   c. **[+属性の追加（+Add Attribute）]** をクリックします。
   d. **[データ型（Data type）]** では、文字列を選択します。
   e. **[表示名（Display name）]**、**[変数名（Variable name）]**、および **[説明（Description）]** に、CiscoAVPair と入力します。
   f. **[属性が必要（Attribute required）]** がオフになっていることを確認します。
   g. 他のフィールドはデフォルト値のままにして、**[保存してさらに追加（Save and Add Another）]** をクリックします。
   h. **[データ型（Data type）]** では、文字列を選択します。
   i. **[表示名（Display name）]**、**[変数名（Variable name）]**、および **[説明（Description）]** に、nduser と入力します。
   j. **[属性が必要（Attribute required）]** がオフになっていることを確認します。
   k. その他のフィールドはデフォルト値のままにして、**[保存（Save）]** をクリックします。
4. 作成した nd-mfa ユーザーに必要な属性を追加します。
   a. 左側のナビゲーションメニューから、**[ディレクトリ（Directory）] > [プロファイル エディタ（Profile Editor）]** を選択します。
   b. **nd-mfa ユーザー（デフォルト）** のプロファイルをクリックします。
   c. **[+属性の追加（+Add Attribute）]** をクリックします。
   d. **[データ型（Data type）]** では、文字列を選択します。
   e. **[表示名（Display name）]**、**[変数名（Variable name）]**、および **[説明（Description）]** に、CiscoAVPair と入力します。
   f. **[属性が必要（Attribute required）]** にチェックが入っていることを確認します。
   g. 他のフィールドはデフォルト値のままにして、**[保存してさらに追加（Save and Add Another）]** をクリックします。

h. **[データ型（Data type）]** では、文字列を選択します。
i. **[表示名（Display name）]**、**[変数名（Variable name）]**、および **[説明（Description）]** に、nduser と入力します。
j. **[属性が必要（Attribute required）]** にチェックが入っていることを確認します。
k. その他のフィールドはデフォルト値のままにして、**[保存（Save）]** をクリックします。

5. 属性をマッピングします。
   a. 左側のナビゲーションメニューから、**[ディレクトリ（Directory）] > [プロファイルエディタ（Profile Editor）]** を選択します。
   b. **nd-mfa ユーザー**のプロファイルをクリックします。
   c. メインウィンドウの **[属性（Attributes）]** 領域で、**[マッピング（Mappings）]** をクリックします。
   [nd-mfa ユーザー プロファイル マッピング（nd-mfa User Profile Mappings）] ウィンドウが開きます。



   d. **[nd-mfa ユーザー プロファイル マッピング（nd-mfa User Profile Mappings）]** ウィンドウの上部で、**[nd-mfa を Okta ユーザーに（nd-mfa to Okta User）]** をクリックします。
   e. [CiscoAVPair] の横にあるドロップダウンメニューから app.CiscoAVPair を選択します。
   f. [nduser] の横にあるドロップダウンメニューから app.nduser を選択します。
   g. **[マッピングの保存（Save Mappings）]** をクリックします。
   h. **[今すぐ更新を適用（Apply Update now）]**をクリックします。

6. ユーザを作成します。
   a. 左側のナビゲーションメニューから、**[ディレクトリ（Directory）] > [ユーザー（People）]** を選択します。
   b. **[+ユーザーの追加（+Add person）]** をクリックします。

c. ユーザー情報を入力します。

d. **[保存してさらに追加（Save and Add Another）]** をクリックして別のユーザーを追加するか、**[保存（Save）]** をクリックして終了します。

Nexus Dashboar にログインできるようにするすべてのユーザーを追加する必要があります。

7. ユーザーをアプリに割り当てます。

a. 左側のナビゲーションメニューから、**[アプリケーション（Application）] > [アプリケーション（Application）]** を選択します。

b. 作成したアプリケーション（nd-mfa）をクリックします。

c. **[課題（Assignments）]** タブを選択します。

d. **[割り当て（Assign）] > [ユーザーに割り当て（Assign to People）]** を選択します。

[ユーザーへの nd-mfa の割り当て（Assign nd-mfa to People）] ウィンドウが開きます。

e. **[ユーザーへの nd-mfa の割り当て]** ウィンドウで、ユーザーの横にある **[割り当て（Assign）]** をクリックし、ユーザーが Nexus Dashboard にログインできるようにします。

f. ユーザーの詳細ウィンドウが開いたら、**[CiscoAVPair]** および **[nduser]** フィールドに値を入力します。

CiscoAVPair の値は、「リモート認証サーバーの設定」で説明されています（例：shell:domains=all/admin/）。

nduser の値は、Nexus Dashboard にログインするときにこのユーザーのユーザー名として使用されます。

g. **[保存して戻る（Save and Go Back）]** をクリックします。

h. 別のユーザーを割り当てるか、**[完了（Done）]** をクリックして終了します。

前の手順で作成したすべてのユーザーを追加する必要があります。

8. アプリの **[要求（Claims）]** を設定します。

a. 左のナビゲーションメニューから **[セキュリティ（Security）] > [API]** を選択します。

b. **デフォルト**の名前をクリックします。

c. **[要求（Claims）]** タブを選択します。

d. **[+要求の追加（+Add Claim）]** をクリックして、CiscoAVPair 要求を追加します。

e. **[名前（Name）]** フィールドに、CiscoAVPair と入力します。

f. **[トークンタイプに含める（Include in token type）]** ドロップダウンから、[ID トークン（ID Token）] を選択します。

[ID トークン（ID Token）] の使用をお勧めしますが、[アクセストークン（Access Token）] もサポートされています。

g. **[値（Value）]** フィールドに、appuser.CiscoAVPair と入力します。

h. [**保存（Save）**] をクリックします。

i. **[+要求の追加（+Add Claim）]** をクリックして、nduser の要求を追加します。

j. **[名前（Name）]** フィールドに、nduser と入力します。

k. **[トークンタイプに含める（Include in token type）]** ドロップダウンから、[ID トークン（ID Token）] を選択します。

両方の要求を同じトークンで作成する必要があります。ID トークンとアクセストークンの混在はサポートされていません。

l. **[値（Value）]** フィールドに、appuser.nduser と入力します。

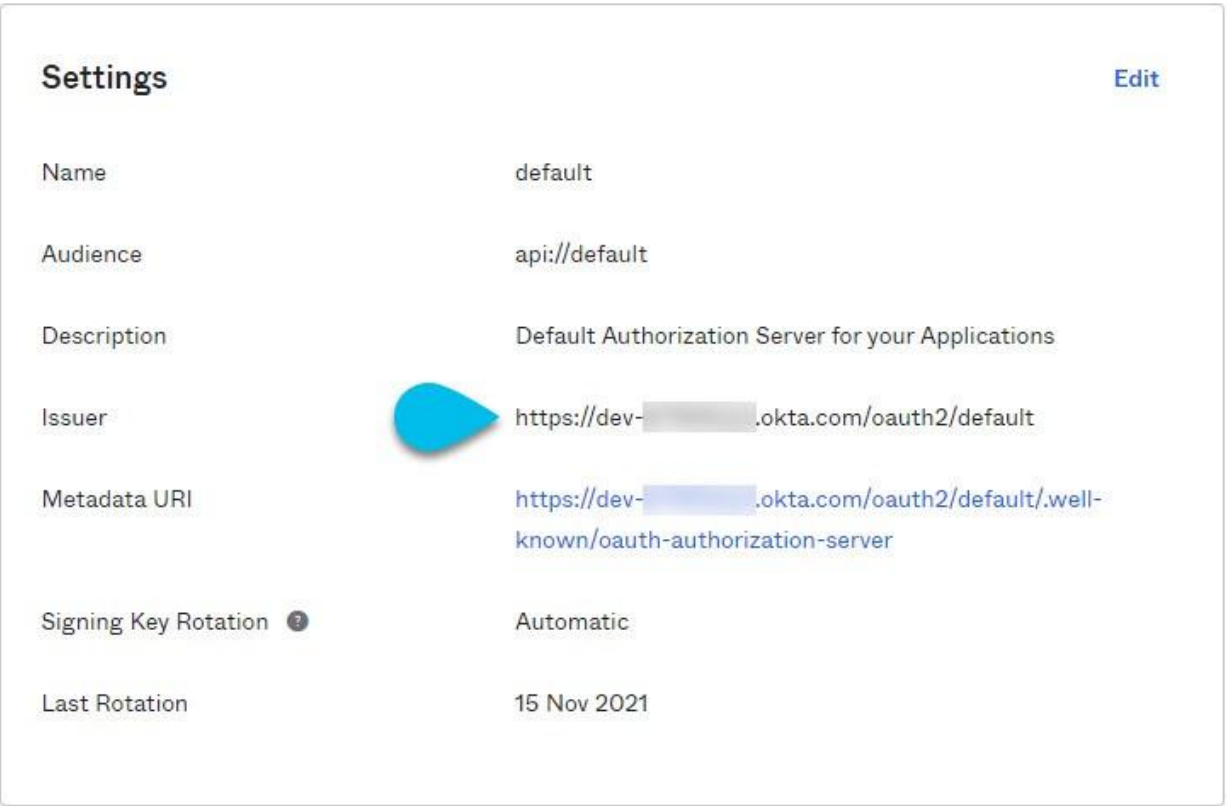
m. [**保存（Save）**] をクリックします。

9. Nexus Dashboard の認証プロバイダーとして追加するために必要な Okta アカウント情報を収集します。

a. 左のナビゲーションメニューから **[セキュリティ（Security）] > [API]** を選択します。

b. **デフォルト**の名前をクリックします。

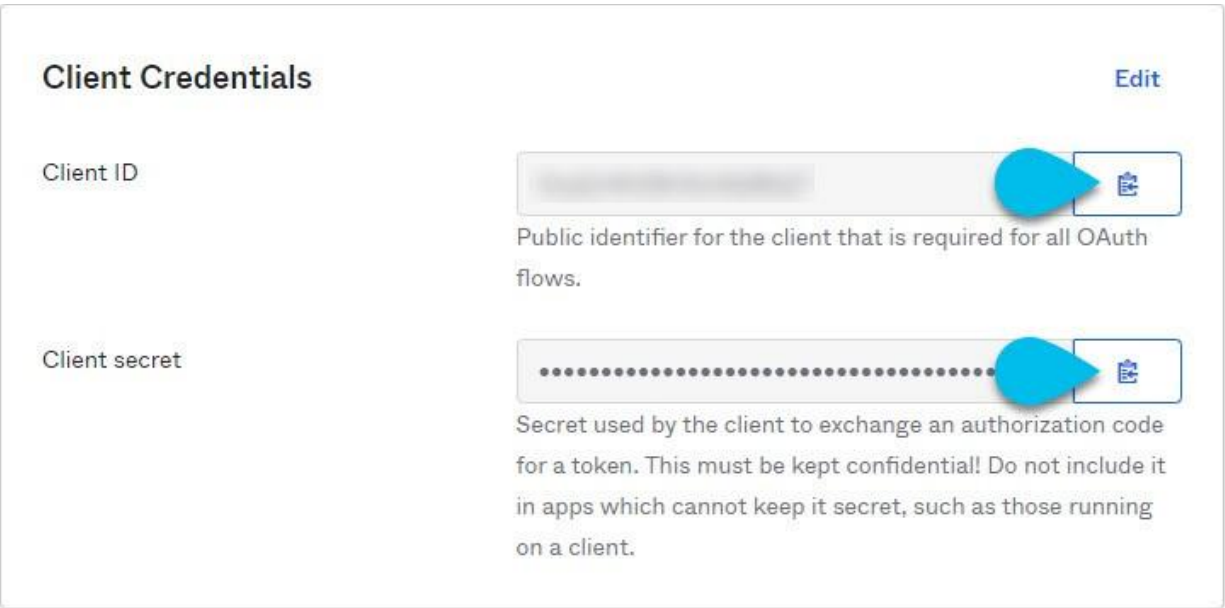
c. **[発行者（Issuer）]** の値を書き留めます。



d. 左側のナビゲーションメニューから、**[アプリケーション（Application）] > [アプリケーション（Application）]** を選択します。

e. 作成したアプリケーション（nd-mfa）をクリックします。

f. **[クライアント ID（Client ID）]** と **[クライアントシークレット（Client Secret）]** の値を書き留めます。



MFA クライアントの設定

このリリースでは、MFA クライアントとして Cisco Duo のみがサポートされています。

次の手順では、Cisco Duo for Nexus Dashboard MFA を使用できるようにするために必要な基本設定を提供します。詳細な Duo 設定は、このドキュメントの範囲外です。使用可能なすべてのオプションについては、Cisco Duo のドキュメントを参照してください。

Duo を設定するには、次を実行します。

1. Okta アカウントにログインします。
2. DUO を MFA タイプとして追加します。
    a. 左のナビゲーションメニューから **[セキュリティ（Security）] > [多要素（Multifactor）]** を選択します。
    b. **[要素タイプ（Factor Types）]** タブで、[Duo セキュリティ（Duo Security）] を選択します。

        Duo Security オプションがない場合は、https://support.okta.com/help/s/opencase から Okta でサポートケースを開く必要があります。
    c. **[Duo セキュリティ（Duo Security）]** ウィンドウで、必要な情報を入力します。

        統合キー、秘密キー、API ホスト名を取得する方法の詳細については、https://duo.com/docs/okta を参照してください。

        Duo ユーザー名の形式が電子メールに設定されていることを確認します。
    d. [**保存（Save）**] をクリックします。
3. Duo ルールを作成します。
    a. 左側のナビゲーションメニューから、**[アプリケーション（Application）] > [アプリケーション（Application）]** を選択します。
    b. 作成したアプリケーション（nd-mfa）をクリックします。
    c. **[サインオン（Sign On）]** タブを選択します。
    d. **[サインオンポリシー（Sign On Policy）]** 領域で、**[+ルールの追加（+Add Rule）]** をクリックします。
    e. ルールの名前を入力します。
    f. **[アクセス（Access）]** 領域で **[要素のプロンプト（Prompt for factor）]** を有効にして、**[すべてのサインオン（Every sign on）]** を選択します。
    g. ユースケースの必要に応じて、他のオプションを指定します。
    h. [**保存（Save）**] をクリックします。
4. Okta と Duo の統合を構成します。

    Okta で構成したユーザーが MFA 用の Duo アプリを使用できるようにする方法は 2 つあります。Duo 管理者に Duo ダッシュボードと同じユーザーをすべて追加してもらうか、個々のユーザーが Okta にログインして自分で登録するかです。

    Duo ダッシュボードでユーザーを設定するには、次を実行します。

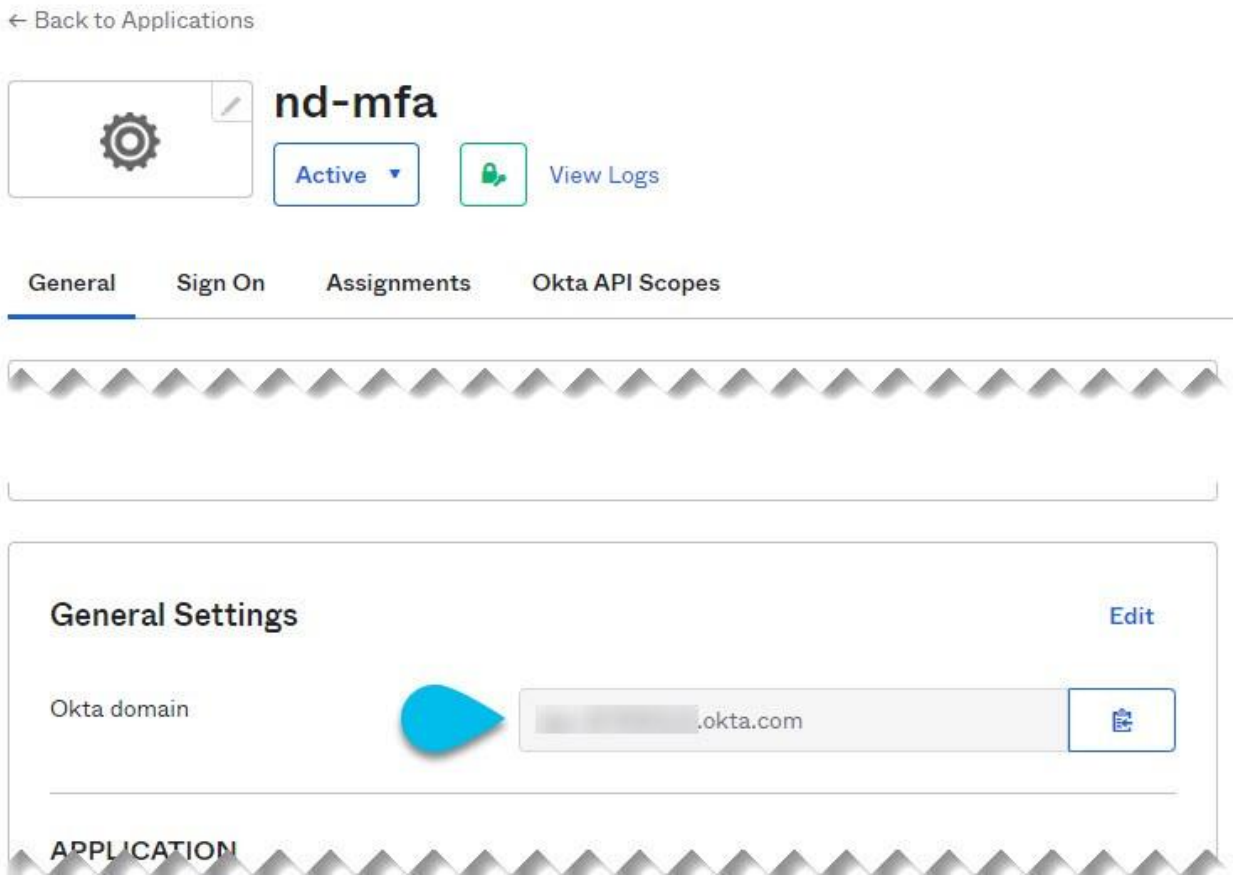
    a. 管理者ユーザーとして Duo ダッシュボードにログインします。
    b. 左のナビゲーションメニューから **ユーザー（Users）]** を選択します。
    c. **[ユーザーの追加（Add User）]** をクリックし、Okta のユーザー情報と一致する詳細情報を入力します。

d. Okta に追加したすべてのユーザーについて、この手順を繰り返します。

自己登録するには、次を実行します。

a. 「MFA プロバイダーとしての Okta アカウントの構成」で作成したすべてのユーザーに、特定の Okta ドメインを使用して自分で Okta にログインするように指示します。

使用する Okta ドメインを決定するには、**[アプリケーション（Application）] > [アプリケーション（Application）]** に移動し、作成した nd-mfa アプリケーションをクリックして、**Okta ドメイン**の URL をコピーします。



b. ログインすると、右上のユーザーメニューから **[設定（Settings）]** ページに移動できます。

c. **[Duo セキュリティ設定（Duo Security Setup）]** を選択し、画面の指示に従います。

リモート認証プロバイダーとしての Okta の追加

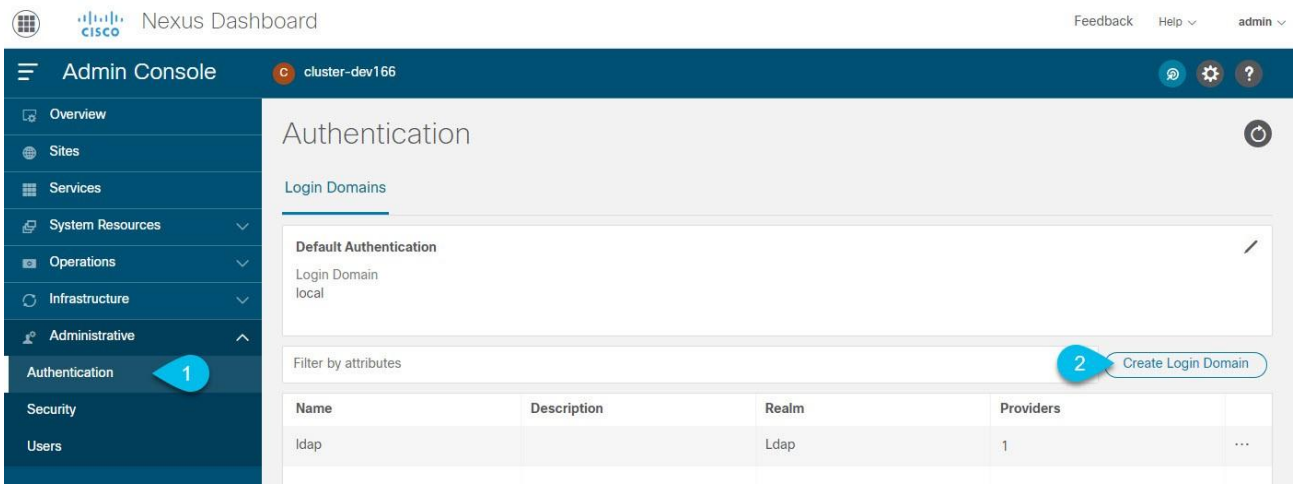
はじめる前に

- 「Okta アカウントの MFA プロバイダーとしての構成」で説明されているように、Okta は 1 人以上のユーザーで構成されている必要があります。
- Okta アカウントからの**クライアント ID**、**クライアントシークレット**、**発行者**情報が手元にある必要があります。これについては、「MFA プロバイダーとしての Okta アカウントの構成」の最後の手順で説明されています。
- プロキシを使用して Okta アカウントに接続する場合は、「クラスタ構成」で説明されているように、プロキシが構成済みである必要があります。

Okta をリモート認証プロバイダーとして追加するには、次を実行します。

1. 管理者ユーザーとして Nexus Dashboard にログインします。
2. **[管理コンソール（Admin Console）]** に移動します。

3. 認証ドメインを追加します。



   a. メイン ナビゲーション メニューから、**[管理（Administrative）] > [認証（Authentication）]** の順に選択します。

   b. メインペインの右上で、**[アクション（Actions）]** メニューをクリックし、**[ログインドメインの作成（Create Login Domain）]** を選択します。

4. **[ログインドメインの作成（Create Login Domain）]** 画面が開いたら、ドメインの詳細を入力します。

   a. **[名前（Name）]** にドメインの名前を入力します。

   b. （任意）**[説明（Description）]** にドメインの説明を入力します。

   c. **[レルム（Realm）]** ドロップダウンから、[OIDC] を選択します。

   d. **[クライアント ID（Client ID）]** フィールドに、Okta アカウントから取得したクライアント ID を入力します。

   e. **[クライアントシークレット（Client Secret）]** フィールドに、Okta アカウントから取得したクライアントシークレットを入力します。

   f. **[発行者（Issuer）]** フィールドに、Okta アカウントから取得した URI を入力します。

   g. （任意）プロキシ経由で Okta に接続する場合は、**[ユーザープロキシ（User Proxy）]** オプションをオンにします。

   h. **[範囲（Scopes）]** オプションはオフのままにします。

      このリリースでは、openid の範囲のみがサポートされています。

5. **[作成（Create）]** をクリックして、ドメインの追加を終了します。

MFA を使用した Nexus Dashboard へのログイン

1. 通常どおり、Nexus Dashboard の IP の 1 つに移動します。
2. **[ログインドメイン（Login Domain）]** ドロップダウンから、「リモート認証プロバイダーとしての Okta の追加」で作成した OIDC ドメインを選択します。

   ユーザー名と**パスワード**のフィールドは表示されません。

3. **[ログイン（Login）] をクリックします。**

   Okta ログインページに移動します。

4. 「MFA プロバイダーとしての Okta アカウントの構成」の説明に従って、Okta で構成されたユーザーを使用してログインします。

   Duo クライアントにプッシュ通知が送信されます。

5. Duo を使用してログインを承認します。

   Nexus Dashboard UI にリダイレクトされ、Okta ユーザーを使用してログインします。

ユーザー

[ユーザー（Users）] の GUI ページでは、Nexus Dashboard にアクセスできるすべてのユーザーを表示および管理できます。

[ローカル（Local）] タブにはすべてのローカルユーザーが表示され、**[リモート（Remote）]** タブには、「リモート認証」セクションの説明に従って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が表示されます。

Nexus Dashboard、サイト、およびアプリケーション間のシングルサインオン(SSO)は、リモートユーザーのみが使用できることに注意してください。リモートユーザーの設定の詳細については、「リモート認証」を参照してください。

ローカル ユーザの追加

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. 新しいローカルユーザを作成します。
   a. メイン ナビゲーション メニューから、**[管理（Administrative）] > [ユーザー（Users）]** を選択します。
   b. メインペインの右上で、**[ローカルユーザーの作成（Create Local User）]** をクリックします。
3. **[ローカルユーザーの作成（Create Local User）]** 画面が開いたら、ユーザーの詳細を入力します。
   a. ログインに使用する**ユーザー ID** を入力します。
   b. 最初の**パスワード**を入力して確認します。
   c. ユーザーの**名**、**姓**、**電子メールアドレス**を入力します。
   d. ユーザーの**ロール**と**権限**を選択します。

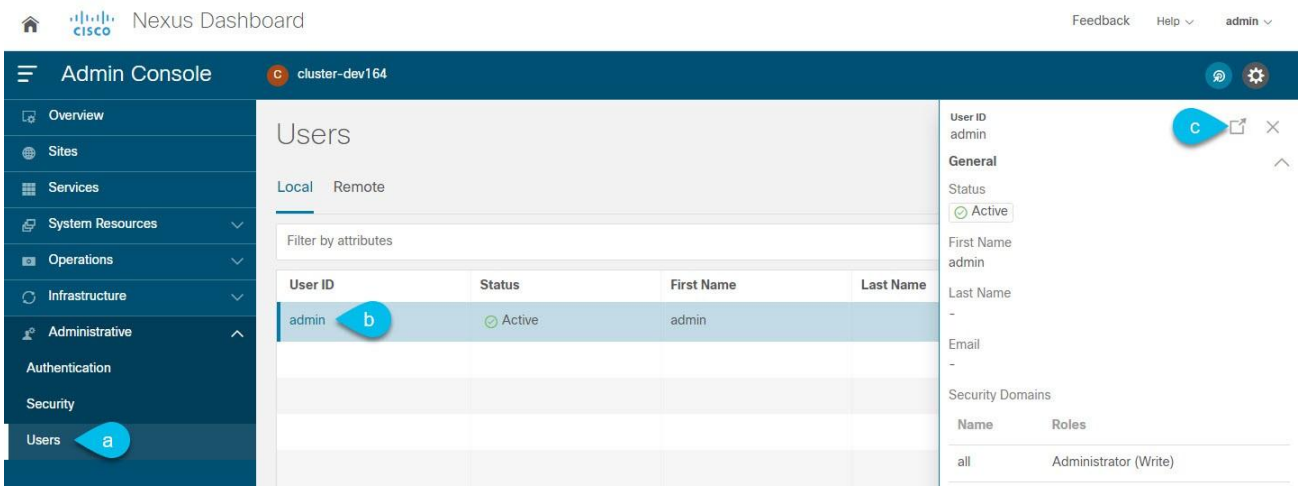
      各ユーザーに対して 1 つ以上のロールを選択できます。使用可能なロールとその権限については、「ロールと権限」を参照してください。

      選択したすべてのユーザーロールに対して、読み取り専用アクセスと読み取り/書き込みアクセスのどちらを有効にするかを選択できます。読み取り専用アクセスの場合、ユーザーは自分のユーザー**ロール**で許可されたオブジェクトと設定を表示できますが、変更することはできません。

   e. **[作成（Create）]** をクリックしてユーザーを保存します。

ローカル ユーザの編集

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. ユーザの詳細画面を開きます。



a. メイン ナビゲーション メニューから、**[管理（Administrative）] > [ユーザー（Users）]** を選択します。

b. メインペインで、ユーザーの名前をクリックします。

c. 詳細ペインが開いたら、**[詳細（Details）]** アイコンをクリックします。

3. ***<user-name>*** の詳細画面が開いたら、**[編集（Edit）]** アイコンをクリックします。

4. **[ユーザーの編集（Edit User）]** 画面で、必要に応じて設定を更新します。

セキュリティ

[セキュリティ（Security）] の GUI ページでは、Nexus Dashboard で使用される証明書を表示および管理できます。

セキュリティ設定

[管理（Administrative）] > [セキュリティの設定（Security Configuration）] ページでは、Nexus Dashboard クラスタで使用される認証セッションのタイムアウトとセキュリティ証明書を設定できます。

はじめる前に

- Nexus Dashboard で使用する予定のキーと証明書がすでに生成されている必要があります。

  通常、これには次のファイルが含まれます。

  - 秘密キー（nd.key）
  - 認証局（CA）パブリック証明書（ca.crt）
  - CA 署名付き証明書（nd.crt）

  自己署名証明書用の上記ファイルの生成については、「秘密キーと自己署名証明書の 生成」で説明されています。

- セキュリティの設定を変更する前に、Nexus Dashboard クラスタの構成バックアップを作成することをお勧めします。

  バックアップの詳細については、[バックアップと復元（Backup and Restore）] を参照してください。

セキュリティの設定を編集するには、次を実行します。

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. セキュリティの設定を編集します。

a. メイン ナビゲーション メニューから、**[管理（Administrative）] > [セキュリティ（Security）]** を選択します。

b. メインペインで、**[セキュリティの設定（Security Configuration）]** タブを選択します。

c. メインペインの右上にある **[編集（Edit）]** アイコンをクリックします。

3. **[セキュリティの設定（Security Configuration）]** 画面で、必要に応じて詳細を更新します。

キーと証明書ファイルのアップロードはサポートされていないため、次のフィールドに情報を貼り付ける必要があることに注意してください。

a. **[セッションタイムアウト（Session Timeout）]** を更新します。

このフィールドは、API トークンの持続時間を定義します。デフォルトは 20 分に設定されています。

b. **[アイドルタイムアウト（Idle Timeout）]** を更新します。

このフィールドは、UI セッションの持続時間を定義します。

c. **[ドメイン名（Domain Name）]** フィールドで、ドメインを指定します。

d. **[キー（Key）]** フィールドで、秘密キーを指定します。

e. **[RSA 証明書（RSA Certificate）]** フィールドに、CA 署名または自己署名の証明書を指定します。

f. **[ルート証明書（Root Certificate）]** フィールドに、CA のパブリック証明書を指定します。

g. （任意）CA が中間証明書を提供している場合は、それを **[中間証明書（Intermediate Certificate）]** フィールドに入力します。

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

変更を保存すると、新しい設定を使用して GUI がリロードされます。

セキュリティ ドメイン

制限付きセキュリティドメインを使用すると、管理者は、両方のグループのユーザーに同じ特権が割り当てられている場合でさえ、別のセキュリティドメインのユーザーグループによって作成されたオブジェクトを表示または変更できないようにすることができます。

たとえば、制限付きセキュリティドメイン（domain1）の管理者は、別のセキュリティドメイン（domain2）のサイト、サービス、クラスタ、ユーザー構成を閲覧できません。

ユーザーは、ユーザーが適切な権限を持っているシステムで作成された構成に対して、常に読み取り専用の可視性を持つことに注意してください。制限付きセキュリティドメインのユーザーには、そのドメイン内で幅広いレベルの特権を与えることができます。ユーザーが別のグループの物理環境に不注意で影響を与える心配はありません。

セキュリティ ドメインを作成する手順：

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. 新しいセキュリティドメインを作成します。

a. メイン ナビゲーション メニューから、**[管理（Administrative）] > [セキュリティ（Security）]** を選択します。

b. メインペインで、**[セキュリティドメイン（Security Domain）]** タブを選択します。

c. メインペインの右上で、**[セキュリティドメインの作成（Create Security Domain）]** をクリックします。

3. **[セキュリティドメインの作成（Create Security Domain）]** 画面が開いたら、ドメインの詳細を入力します。
   a. **[名前（Name）]** にドメインの名前を入力します。
   b. （任意）ドメインの説明を入力します。
   c. **[作成（Create）]** をクリックしてドメインを保存します。

Cisco Intersight

Cisco Intersight は、他のインテリジェントシステムによって拡張される Software-as-a-Service（SaaS）インフラストラクチャ管理プラットフォームです。Cisco Unified Computing System（Cisco UCS）および Cisco HyperFlex ハイパーコンバージド インフラストラクチャ、Cisco APIC、および Nexus Dashboard などといったプラットフォームをグローバルに管理できます。

Cisco Nexus Dashboard Insights などのデータセンターアプリケーションは、各システム(この場合は Nexus Dashboard プラットフォーム)の管理コントローラに組み込まれているデバイスコネクタを介して Cisco Intersight ポータルに接続します。デバイスコネクタは、接続されているデバイスに対して、セキュリティで保護されたインターネット接続を使用して情報を送信し、Cisco Intersight ポータルから制御命令を受信できる安全な方法を提供します。

Intersight 対応のデバイスやアプリケーションが起動すると、デフォルトではブート時にデバイスコネクタが起動し、クラウドサービスに接続しようとします。**[自動更新（Auto Update）]** オプションが有効になっている場合、Cisco Intersight に接続するときに、Intersight サービスによる更新を介してデバイスコネクタが自動的に最新バージョンに更新されます。**[自動更新（Auto Update）]** オプションの詳細については、「デバイスコネクタの設定」を参照してください。

Cisco Intersight のさらに詳細な情報については、https://www.intersight.com/help/getting_started を参照してください。

Application Services Engine からアップグレードした際に、Intersight デバイスコネクタでプロキシの設定に関する要求があった場合は、**[クラスタの設定（Cluster Configuration）]** 画面でプロキシを再設定する必要があります。詳細については、「クラスタの 設定」を参照してください。

デバイスコネクタの設定

デバイスはデバイスコネクタを介して Cisco Intersight ポータルに接続されます。これによって、接続されているデバイスは安全な方法で情報を送信し、Cisco Intersight ポータルから制御命令を受信できます。

すべてのデバイスコネクタは、svc.intersight.com を適切に解決でき、かつポート 443 のアウトバウンドで開始される HTTPS 接続を許可する必要があります。HTTPS 接続にプロキシが必要な場合は、Nexus Dashboard でプロキシを設定する必要があります。

ここでは、基本的なデバイスコネクタの設定方法について説明します。

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. メイン ナビゲーション メニューから、**[インフラストラクチャ（Infrastructure）] > [Intersight]** を選択します。
3. メインペインの右上の **[設定（Settings）]** をクリックします。
4. 基本オプションを設定するには、**[全般（General）]** タブをクリックします。
    a. デバイスコネクタを有効または無効にするには、**[デバイスコネクタ（Device Connector）]** ノブを使用します。

        これにより、デバイスを要求して Intersight の機能を活用できるようになります。無効になっている場合、Cisco Intersight への通信は許可されません。

    b. **[アクセスモード（Access Mode）]** 領域で、このデバイスに変更を加える機能を Intersight に許可するかどうかを決定します。

- [制御の許可（Allow Control）]（デフォルト） - Cisco Intersight で使用可能な機能に基づいて、クラウドから完全な読み取りまたは書き込み操作を実行できます。
- [読み取り専用（Read-only）] – Cisco Intersight から、このデバイスに変更が加えられていないことを確認します。

  たとえば、ファームウェアのアップグレードやプロファイルの展開などのアクションは、読み取り専用モードでは許可されません。ただし、アクションは特定のシステムで使用可能な機能によって異なります。

c. Device Connector の自動更新を有効にするには、**[自動更新（Auto Update）]** ノブを使用します。

   デバイスコネクタのソフトウェアが自動的に更新されるように、自動更新を有効にすることを推奨します。有効にすると、Intersight からアップグレードがプッシュされるたびに、デバイスコネクタがそのイメージを自動的にアップグレードします。

   自動更新を無効にした場合、新しいリリースが利用可能になると、ソフトウェアを手動で更新するように求められます。旧型のデバイスコネクタでは、Cisco Intersight に接続できない可能性があるので注意してください。

5. **[保存 (Save)]** をクリックして、変更内容を保存します。
6. 追加の証明書をインポートするには、**[証明書マネージャ（Certificate Manager）]** タブをクリックします。

   デフォルトでは、デバイスコネクタが信頼するのは、組み込まれている証明書のみです。デバイスコネクタが TLS 接続を確立する際に、サーバーから送られてきた証明書が組み込み証明書と一致しない場合、デバイスコネクタはそのサーバーが信頼できるデバイスかどうかを判断できないため、TLS 接続を終了します。

   この画面で **[インポート（Import）]** ボタンをクリックすると、追加の証明書をアップロードできます。インポートされた証明書は.pem（base64 エンコード）形式である必要があります。証明書が正常にインポートされると、**[信頼できる証明書（Trusted Certificates）]** のリストに記載され、その証明書が正しければ **[使用中（In-Use）]** 列に表示されます。

   証明書の行の末尾にある **[表示（View）]** アイコンをクリックすると、名前、発行日、有効期限などの詳細を表示できます。

ターゲット要求

ここでは、Cisco Intersight のデバイスとして Nexus Dashboard プラットフォームを要求する方法について説明します。

はじめる前に

「デバイスコネクタ 設定」の説明に従って、Intersight デバイスコネクタを設定しておく必要があります。

デバイスを要求するには、次の手順を実行します。

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. メイン ナビゲーション メニューから、**[インフラストラクチャ（Infrastructure）] > [Intersight]** を選択します。
3. デバイスコネクタがすでに設定されているかどうかを確認します。

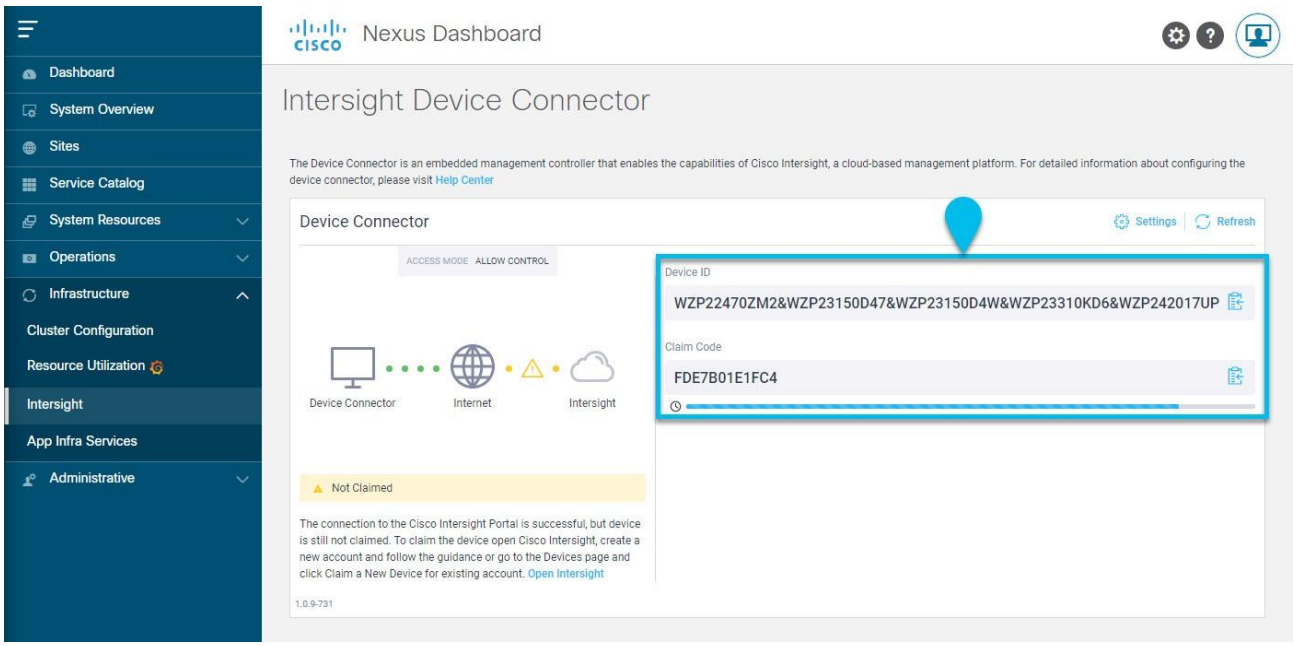
- **[デバイスコネクタ（Device Connector）]** ページで、**インターネット**と **Intersight** が緑色の点線で結ばれ、**[要求済み（Claimed）]** というテキストが表示されている場合、Intersight デバイスコネクタの設定、Intersight クラウドサービスへの接続、およびデバイスの要求は完了しています。この場合、このセクションの残りの部分はスキップできます。
- **[デバイスコネクタ（Device Connector）]** ページで、**インターネット**との接続を示す赤い点線が表示されている場合は、このセクションの残りの部分に進む前に「クラスタの設定」の説明に従って、Nexus Dashboard クラスタがインターネットにアクセスできるようプロキシを設定する必要があります。
- **[デバイスコネクタ（Device Connector）]** ページに、**インターネット**と **Intersight** を結ぶ黄色の点線と注意アイコン、および **[要求が未完了（Not Claimed）]** というテキストが表示されている場合、Intersight デバイスコネクタの設定、Intersight サービスへの接続、およびデバイスの要求は完了していません。次の手順に従って、Intersight デバイスコネクタの設定、Intersight クラウドサービスへの接続、およびデバイスの要求を行います。この場合、デバイスを設定するために残りの手順に進みます。

4. 必要に応じて、デバイスコネクタのソフトウェアを更新します。

   使用可能な新しいデバイスコネクタのソフトウェアバージョンがあり、**[自動更新（Auto Update）]** オプションが有効になっていない場合は、デバイスコネクタに重要な更新プログラムがあることを通知するメッセージが画面の上部に表示されます。自動更新機能の有効化については、「デバイスコネクタの設定」を参照してください。

   デバイスコネクタを手動で更新するには、**[今すぐ更新（Update Now）]** リンクをクリックします。

5. Nexus Dashboard の **[Intersight]** ページに表示されているデバイス ID と要求コードをメモします。



6. Cisco Intersight クラウドサイト（https://www.Intersight.com）にログインします。
7. Intersight マニュアルの「ターゲットの要求」セクションに記載されている手順に従って、デバイスを要求します。

   Intersight でデバイスを要求した後は、Nexus Dashboard の **[デバイスコネクタ（Device Connector）]** ページで **[インターネット（Internet）]** と **[Intersight]** が緑色の点線で結ばれており、**[要求済み（Claimed）]** というテキストが表示されている必要があります。

   最新の状態に更新するには、ページの右上にある **[更新（Refresh）]** をクリックする必要があります。

デバイスの要求解除

Intersight から Nexus Dashboard をデバイスとして要求するのを解除するには、次の手順を実行します。

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. メイン ナビゲーション メニューから、**[インフラストラクチャ（Infrastructure）] > [Intersight]** を選択します。
3. メインペインで、**[要求解除（Unclaim）]** をクリックします。

トラブルシューティング

便利なコマンド

システムデータへのアクセスが制限されている場合、rescue-user として任意のクラスタノードにログインできます。次のコマンドを使用して、Cisco Nexus Dashboard でさまざまな操作を実行できます。

クラスタのトラブルシューティング:

- acs health – クラスタの正常性情報と既存の問題を表示します。
- acs cluster config – クラスタの設定を表示します。
- acs cluster masters – マスターノードの設定を表示します。
- acs cluster workers – ワーカーノードの設定を表示します。
- acs cluster standbys – スタンバイノードの設定を表示します。
- acs techsupport collect -s system – インフラストラクチャのテクニカルサポート情報を収集します。
- acs techsupport collect -s cisco-mso – Nexus Dashboard Orchestrator サービスのテクニカルサポート情報を収集します。
- acs techsupport collect -s cisco-nir – Nexus Dashboard Insights サービスのテクニカルサポート情報を収集します。
- acs techsupport collect -s cisco-appcenter – App Store のテクニカルサポート情報を収集します。
- acs version – Nexus Dashboard のバージョンを返します。

デバイスのリセット:

- acs reboot – すべてのサービスと設定をそのまま使用してノードをリブートします。
- acs reboot clean – Nexus Dashboard とアプリケーションの全データを削除しますが、Nexus Dashboard のブートストラップ設定とポッドイメージは保持します。

  Nexus Dashboard クラスタを初めて起動すると、初期展開プロセスで必要なすべてのポッドイメージがインストールされます。ポッドイメージを保持すると、リブート後のクラスタの起動が高速化されます。

  クラスタ内のすべてのノードを再インストールする場合は、最初にサイトおよびアプリケーション情報をクリーンアップする必要があります。この場合、サイトがすべてのアプリケーションで無効になっており、ND クラスタから削除されていることを確認してください。

- acs reboot clean-wipe – Nexus Dashboard およびアプリケーションイメージを含むアプリケーションの全データを削除しますが、Nexus Dashboard のブートストラップ設定は保持します。

  クラスタが再起動すると、ポッドイメージが再インストールされます。

  クラスタ内のすべてのノードを再インストールする場合は、最初にサイトおよびアプリケーション情報をクリーンアップする必要があります。この場合、サイトがすべてのアプリケーションで無効になっており、ND クラスタから削除されていることを確認してください。

- acs reboot factory-reset – クラスタブートストラップ設定を含む Nexus Dashboard とアプリケーションの全データを削除しますが、アプリケーションイメージは保持します。

  Nexus Dashboard クラスタを初めて起動すると、初期展開プロセスで必要なすべてのポッドイメージがインストールされます。ポッドイメージを保持すると、クラスタの起動が高速化されます。

クラスタ内のすべてのノードを再インストールする場合は、最初にサイトおよびアプリケーション情報をクリーンアップする必要があります。この場合、サイトがすべてのアプリケーションで無効になっており、ND クラスタから削除されていることを確認してください。

- acs reboot factory-wipe - アプリケーションイメージとクラスタブートストラップ設定を含む、Nexus Dashboard とアプリケーションの全データを削除します。

  クラスタが再起動すると、ポッドイメージが再インストールされます。

  クラスタ内のすべてのノードを再インストールする場合は、最初にサイトおよびアプリケーション情報をクリーンアップする必要があります。この場合、サイトがすべてのアプリケーションで無効になっており、ND クラスタから削除されていることを確認してください。

システムと接続に関するトラブルシューティング:

- /logs ディレクトリは rescue-user コンテナにマウントされ、標準ツールで検査できます。
- ping コマンドは、ほとんどのオプションでサポートされています。
- ip コマンドは、ip addr show および ip route show を含む、コマンドの読み取り専用サブセットをサポートします。
- kubelctl コマンドは、読み取り専用の kubectl コマンドをサポートするために使用できます。
- esctl コマンドは、Elasticsearch サービスに関するデバッグ情報を取得できるカスタムユーティリティを呼び出します。

  次の引数がサポートされています。

  - esctl help - 以下で説明する使用情報と使用可能な引数を返します。
  - esctl get nodes - Elasticsearch クラスタのノード情報を返します。

    ```
    $ esctl get nodes
    ip              heap.percent ram.percent [...] node.role master name
    172.17.251.227  24           41          [...] mdi       *      es-data-1
    172.17.251.243  21           39          [...] mdi       -      es-data-2
    172.17.251.154  22           35          [...] mdi       -      es-data-0
    ```

  - esctl get health - Elasticsearch クラスタの正常性情報を返します。

```
$ esctl get health
{
  "cluster_name" : "elasticsearch",
  "status" : "green",
  "timed_out" : false,
  "number_of_nodes" : 3,
  "number_of_data_nodes" : 3,
  "active_primary_shards" : 169,
  "active_shards" : 498,
  "relocating_shards" : 0,
  "initializing_shards" : 0,
  "unassigned_shards" : 0,
  "delayed_unassigned_shards" : 0,
  "number_of_pending_tasks" : 0,
  "number_of_in_flight_fetch" : 0,
  "task_max_waiting_in_queue_millis" : 0,
  "active_shards_percent_as_number" : 100.0
}
```

- esctl get indices - クラスタ内に存在するインデックス、内部のドキュメントと削除されたドキュメントの数、およびインデックスストアの容量に関する情報を返します。

```
$ esctl get indices
health status index                                        ...
green open   cisco_nir-enrich_appdynamicsdb-2021.03.26     ...
green open   cisco_nir-svcstatsdb                          ...
green open   cisco_nir-operdb                              ...
...
```

- esctl get allocexplain - クラスタ内のシャード割り当ておよび任意の対応する障害について説明を返します。
- esctl get shards - シャードとそのシャードが属するノードに関する情報を返します。

Nexus Dashboard で実行できる Elasticsearch サービスのインスタンスは 2 つあります。

- elasticsearch - Nexus Dashboard で実行されているほとんどのアプリケーションで使用される Elasticsearch。

  これは、esctl コマンドがデフォルトで情報を提供するサービスです。

- elasticsearch-nir - Network Insights アプリケーションで特に使用される Elasticsearch。このサービスは、Network Insights アプリケーションを有効にすると開始されます。

  --name=elasticsearch-nir 引数を使用して、esctl コマンドにこのインスタンスに関する情報を表示させることができます。次に例を示します。

```
$ esctl --name=elasticsearch-nir get health
```

アプリケーション情報：

- acs apps instances コマンドは、クラスタで実行されているすべてのアプリケーションを表示します。
- acs apps actions コマンドは、インストール、アップグレード、削除など、アプリケーションで実行された操作履歴を表示します。

手動アップグレード

クラスタのアップグレードには、「ファームウェア管理（クラスタのアップグレード）」セクションで説明されている手順を使用することを推奨します。

ただし、単一ノードの手動アップグレードを実行する場合（クラスタに新しいノードを追加しようとしているが、そのノードで古いファームウェアが実行している場合）またはクラスタ全体（GUI アップグレードに失敗した場合）は、代わりに次の手順を使用します。

古いファームウェアを実行している単一のノードをアップグレードして既存のクラスタに追加する場合は、クラスタ全体ではなく、そのノードでのみ次の手順を実行します。

1. アップグレードするノードに rescue-user としてログインします。
2. アップグレード ISO のイメージファイルを各ノードの /tmp ディレクトリにコピーします。
3. すべてのノードでアップグレードを開始します。

   すべてのノードを並行してアップグレードできます。

   ```
   # acs installer update -f /tmp/nd-dk9.2.1.1a.iso
   Warning: This command will initiate node update to new version.
   Proceed? (y/n): y
   Update in Progress ... Do not press Ctrl^C
   ```

4. ファームウェアのアップグレードが完了するまでお待ちください。

   次の手順に進む前に、すべてのノードがアップグレードされるのを待つ必要があります。

   ```
   Update succeeded, reboot your host
   ```

5. 1 つのノードをリブートします。

   いずれかのノードをリブートする前に、すべてのノードでアップグレードが完了していることを確認してください。

   ```
   # acs reboot
   This command will restart this device, Proceed? (y/n): y
   ```

6. ノードが正常であることを確認します。

```
# acs health
All components are healthy
```

7. 最初のノードが正常にアップグレードされ、正常になったら、他の 2 つのノードを順番にリブートします。

使用できないノードは常に 1 つだけであるため、次のノードを再起動する前に、acs health コマンドを使用してリブートしたノードが起動し、ノードが正常であることを確認する必要があります。

8. すべてのノードが新しいバージョンで起動し、正常になったら、アップグレード後のタスクを実行します。

すべてのノードで次のコマンドを並行して実行できます。

```
# acs installer post-update
Warning: This command will run the post-update scripts. Proceed? (y/n): y
Update in Progress ... Do not press Ctrl^C
Post-update succeeded
```

ノードの再イメージ化

Nexus Dashboard の物理ハードウェアが手元に届いた時点で、ソフトウェアイメージはあらかじめロードされています。既存のソフトウェアを設定するだけの場合は、このセクションをスキップして、「ワーカーノードの管理」または「スタンバイノードの管理」に進みます。

手動でノードを最新のソフトウェアバージョンにアップグレードする場合は、代わりに「手動アップグレード」の手順に従ってください。

ここでは、Nexus Dashboard ハードウェアにソフトウェアスタックを再展開する方法について説明します。サーバーのオペレーティングシステムや GUI にアクセスできなくなるほどの致命的な障害が発生した場合や、既存のバージョンからの直接アップグレードやダウングレードがサポートされていない別のリリースを展開する場合は、次の手順を使用する必要があります。

既存の Nexus Dashboard クラスタを再インストールする場合は、最初にサイトおよびアプリケーション情報をクリーンアップする必要があります。この場合、クラスタを停止する前に、サイトがすべてのアプリケーションで無効になっており、ND クラスタから削除されていることを確認してください。

はじめる前に

- サーバーの CIMC への接続には Serial over LAN（SoL）ポートを使用する必要があります。サーバーの CIMC IP アドレスと SSH クライアントがあることを確認してください。

  CIMC 設定に関する詳細情報は、https://www.cisco.com/c/en/us/ support/servers-unified-computing/ucs-c-series-integrated-management-controller/products-installation-and-configuration-guides-list.html で入手できます。

- Cisco Integrated Management Controller (CIMC)のサポート対象バージョンを実行していることを確認します。
  - 推奨バージョン: CIMC、リリース 4.1(3b)。
  - サポート対象の最小バージョン: CIMC、リリース 4.0(1a)。

Nexus Dashboard ソフトウェアを再インストールするには、次の手順を実行します。

1. Cisco Nexus Dashboard イメージをダウンロードします。
   a. Nexus Dashboard ページに移動して、イメージをダウンロードします。

      https://www.cisco.com/c/ja_jp/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. Cisco Nexus Dashboard イメージ(nd-dk9.<version>.iso)をダウンロードします。
   e. 環境内の Web サーバーでイメージをホスティングします。

      イメージをマウントするときに http URL を指定する必要があります。

2. ISO をサーバに展開します。

   この手順では、サーバーの CIMC に接続する必要があります。CIMC 設定に関する詳細情報は、https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c-series-integrated-management-controller/products-installation-and-configuration-guides-list.html で入手できます。

   a. サーバーの CIMC に SSH 接続します。
   b. 仮想メディアに接続します。

      ```
      C220-WZP21510DHS# scope vmedia
      C220-WZP21510DHS /vmedia #
      ```

   c. CIMC-Mapped vDVD にダウンロードした Nexus Dashboard イメージをマッピングします。

      ```
      C220-WZP21510DHS /vmedia # map-www image http://<ip-address>/<path>
      <image>
      ```

      次に例を示します。

      ```
      C220-WZP21510DHS /vmedia # map-www image http://172.31.131.47/images nd-dk9.2.0.1.iso
      ```

   d. イメージがマウントされていることを確認します。

```
C220-WZP21510DHS /vmedia # show mappings
Volume Map-Status Drive-Type Remote-Share Remote-File          Mount-Type
------- ---------- ---------- ------------- ---------------- --------
image OK          CD         [<ip>/<path>] nd-dk9.2.0.1.iso www
```

e. サーバを再起動し、コンソールに接続します。

```
C220-WZP23150D4C /vmedia # exit
C220-WZP23150D4C# scope chassis
C220-WZP23150D4C /chassis # power cycle
C220-WZP23150D4C /chassis # exit
C220-WZP23150D4C# connect host
CISCO Serial Over LAN:
Press Ctrl+x to Exit the session
```

f. ブートデバイスを選択します。

次のメッセージが表示されるまで、ブートプロセスを監視します。

```
Press <F2> Setup, <F6> Boot Menu, <F7> Diagnostics, <F8> Cisco IMC
Configuration, <F12> Network Boot
```

F6 を押して、イメージ（Cisco CIMC-Mapped vDVD1）をマウントした仮想メディアデバイスを選択します。

```
/--------------------------------\
| Please select boot device: |
|--------------------------------|
| (Bus 05 Dev 00)PCI RAID Adapter |
| UNIGEN PHF16H0CM1-DTE PMAP |
| Cisco vKVM-Mapped vHDD1.22 |
| Cisco CIMC-Mapped vHDD1.22 |
| Cisco vKVM-Mapped vDVD1.22 |
| Cisco CIMC-Mapped vDVD1.22 |
| Cisco vKVM-Mapped vFDD1.22 |
| UEFI: Built-in EFI Shell |
| IBA GE Slot 0100 v1585 |
| IBA GE Slot 0101 v1585 |
| Enter Setup |
|--------------------------------|
| ^ and v to move selection |
| ENTER to select boot device |
| ESC to boot using defaults |
\--------------------------------/
```

g. ネットワークを設定します。

サーバーの初回起動時に、次の出力が表示されます。

```
+ '[' -z http://172.31.131.47/nd-dk9.2.0.1.iso ']'
++ awk -F '/|:' '{print $4}'
+ urlip=172.31.131.47
+ '[' -z 172.31.131.47 ']'
+ break
+ '[' -n http://172.31.131.47/nd-dk9.2.0.1.iso ']'
+ set +e
+ configured=0
+ '[' 0 -eq 0 ']'
+ echo 'Configuring network interface'
Configuring network interface
+ echo 'type static, dhcp, bash for a shell to configure networking, or url to re-enter the url: '
type static, dhcp, bash for a shell to configure networking, or url to re-enter the url:
+ read -p '? ' ntype
? static ①
+ case $ntype in
+ configure_static
+ echo 'Available interfaces'
```

```
Available interfaces
+ ls -l /sys/class/net
total 0
lrwxrwxrwx. 1 root root 0 Apr 26 01:21 eno1 ->
../../devices/pci0000:3a/0000:3a:00.0/0000:3b:00.0/net/eno1
lrwxrwxrwx. 1 root root 0 Apr 26 01:21 eno2 ->
../../devices/pci0000:3a/0000:3a:00.0/0000:3b:00.1/net/eno2
lrwxrwxrwx. 1 root root 0 Apr 26 01:21 eno5 ->
../../devices/pci0000:5d/0000:5d:00.0/0000:5e:00.0/0000:5f:01.0/0000:61:00.0/000
0:62:00.0/0000:63:00.0/net/eno5
lrwxrwxrwx. 1 root root 0 Apr 26 01:21 eno6 ->
../../devices/pci0000:5d/0000:5d:00.0/0000:5e:00.0/0000:5f:01.0/0000:61:00.0/000
0:62:00.0/0000:63:00.1/net/eno6
lrwxrwxrwx. 1 root root 0 Apr 26 01:21 lo -> ../../devices/virtual/net/lo
+ read -p 'Interface to configure: ' interface
Interface to configure: eno1 ②
+ read -p 'address: ' addr
address: 172.23.53.59/21 ③
+ read -p 'gateway: ' gw
gateway: 172.23.48.1 ④
+ ip addr add 172.23.53.59/23 dev eno1
+ ip link set eno1 up
+ ip route add default via 172.23.48.1
RTNETLINK answers: Network is unreachable
++ seq 1 2
+ for count in '$(seq 1 2)'
+ ping -c 1 172.31.131.47
```

- IP アドレスについては、環境内に DHCP サーバーがある場合は dchp、そうでない場合は static と入力します。
- インターフェイスには、最初の管理ポート（eno1）を入力します。
- static を選択した場合は、接続で使用する IP アドレスを指定します。
- static を選択した場合は、接続で使用するゲートウェイを指定します。

3. 指定したイメージからサーバーが起動したら、使用可能な唯一のインストールオプションを選択します。

   インストールプロセスが完了するまでに最長 20 分かかる場合があります。

   イメージが展開されたら、「ワーカーノード の管理」または「スタンバイノードの管理」の説明に従って、クラスタにノードを追加できます。

AppStore エラー

Nexus Dashboard の GUI で、**[サービス（Services）] > [AppStore]** タブにアクセスしようとすると、次のエラーが発生する場合があります。

```
{
  " error" : " There was a problem proxying the request"
}
```

原因

アプリストアサービスが実行されているマスターノードに障害が発生すると、アプリストアサービスが別のマスターノードに再配置されるまでに最長 5 分かかる場合があります。

解決策

サービスが回復してページが更新されるまで待ちます。

イベントのエクスポート

Syslog イベントが、目的の外部イベント監視サービスに到達していません。

原因

この問題の最も一般的な原因は、Syslog 宛先サーバーが設定されていないか、正しく設定されていません。

解決策

[クラスタの設定] > [Syslog]の外部サーバーの設定が正しいことを確認してください。詳細については、「クラスタの設定」を参照してください。

原因 2

リモートサーバーは特定の IP アドレスのセットからのトラフィックのみを許可しており、Nexus Dashboard ノードの IP アドレスからのトラフィックは許可されていません。

解決策 2

外部サーバーの設定を更新して、Nexus Dashboard クラスタノードからのトラフィックを許可します。

工場出荷時の状態へのリセット

各ノードで次のコマンドを実行して、物理クラスタ全体をリセットできます。

```
# acs reboot factory-reset
```

これを行うと、すべてのクラスタ設定とアプリケーションが失われるため、クラスタを再構築する必要があります。

仮想またはクラウド型の Nexus Dashboard クラスタをご使用の場合は、『*Cisco Nexus Dashboard 導入ガイド*』で説明されているように、すべてのノードをリセットするのではなく、既存の VM を削除してクラスタ全体を再展開することをお勧めします。

ノード IP アドレスの変更

データまたは管理ネットワークの IP アドレスの変更はサポートされていません。クラスタノードの IP アドレスを変更する場合は、クラスタを再作成する必要があります。

クラスタ構成エラー

Nexus Dashboard でプロキシサーバーを設定または変更すると、**[クラスタ構成（Cluster Configuration）]** ページに、いくつかの cisco-mso service: Replicaset() not in desired state エラーが表示される場合があります。

原因

エラーはサービスの再起動中に表示され、30～60 秒以内に自動的に解決されます。

解決策

サービスが回復してページが更新されるまで待ちます。

ログイン情報の入力を求めない二要素認証（2FA）

2 要素認証を使用した最初のログイン後、その後のログイン試行ではユーザー名とパスワードの情報は要求されず、代わりに空白のページが表示されます。

原因

OIDC アプリケーションに設定されている Cookie のタイムアウトが、Nexus Dashboard で設定されている認証トークンのタイムアウトよりも長くなっています。

解決策

ブラウザのキャッシュをクリアすると、認証プロセスが期待どおりに機能します。

Red Hat Enterprise Linux(RHEL)の展開

RHEL システムにログインして/logs/ndlinux/ ディレクトリを確認すると、インストールログを表示できます。

「トラブルシューティング」のセクションで説明されている一般的な Nexus Dashboard のトラブルシューティング コマンドを実行するには、最初に Nexus Dashboard 環境にアクセスする必要があります。

RHEL システムから Nexus Dashboard 環境にアクセスするには、次を実行します。

1. インストール時に YAML 構成ファイルで指定した Nexus Dashboard ユーザーを使用して、RHEL システムにログインします。
2. attach-nd コマンドを実行して Nexus Dashboard 環境にアクセスします。

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

   Nexus Dashboard 環境にアクセスすると、このガイドの「トラブルシューティング」のセクションで説明されているすべての一般的な Nexus Dashboard コマンドを使用できます。

APIC 設定のインポート後にサイトに接続できない

Cisco APIC サイトを Nexus Dashboard にオンボーディングすると、オンボーディングを反映するように APIC 設定が更新されます。その後、APIC で以前の設定をインポートすると、サイトが Nexus Dashboard またはサービスで使用不可として表示される場合があります。

原因

以前のサイト設定には、オンボードされている Nexus Dashboard クラスタに固有の情報は含まれていません。

解決策

サイトが Nexus Dashboard にオンボーディングされた後、今後の設定の復元のために APIC 設定をエクスポートすることをお勧めします。

発生後に問題を解決するには、Nexus Dashboard GUI でサイトを再登録します。

1. Nexus Dashboard クラスタにログインします。
2. **[管理コンソール（Admin Console）] > [サイト（Sites）]** に移動します。
3. サイトの横の **[アクション（Actions）]**（**[...]**）メニューから、**[サイトの編集（Edit Site）]** を選択します。
4. **[サイト編集（Site Edit）]** 画面で、[サイトの再登録（Re-register Site）] チェックボックスをオンにして、サイトの詳細を再度入力します。
5. [**保存（Save）**] をクリックします。

物理クラスタへの同じマスターノードの再追加

このセクションでは、マスターノードを物理クラスタに再追加する方法について説明します。このシナリオは、設定のリセット（acs reboot factory-reset など）または vMedia の再インストールによって、ノードが誤ってまたは意図的に削除された場合に発生する可能性があります。

クラスタにスタンバイノードがある場合は、「単一マスターノードとスタンバイノードの置換」の説明に従ってスタンバイノードをマスターノードに置き換えて、次に「スタンバイノードの追加」の説明に従って古いマスターノードを新しいスタンバイノードとして追加します。

ハードウェア障害のためにマスターノードを完全に置換（RMA）する必要があるが、使用可能なスタンバイノードがない場合は、代わりに「スタンバイノードのない 単一の物理マスターノードの置換」で説明されている手順に従ってください。

マスターノードを同じクラスタに再度追加するには、次の手順を実行します。

1. ノードが工場出荷時の設定にリセットされていることを確認します。

   ノードが不良状態の場合は、rescue-user としてノードにログインし、次のコマンドを使用してノードをリセットします。

   ```
   # acs reboot factory-reset
   ```

2. 正常なノードのいずれかの管理 IP アドレスを使用して Nexus ダッシュボード GUI にログインします。

3. **[システムリソース（System Resources）] > [ノード（Nodes）]** の順に移動します。

   交換するノードが [非アクティブ（Inactive）] として UI に表示されます。

4. ノードのアクション（**[...]**）メニューから、**[登録（Register）]** を選択します。

   [ノードの登録（Register Node）] ページが開きます。

5. **[ノードの登録（Register Node）]** ページで必要な情報を入力し、**[検証（Validate）]** をクリックします。

   物理ノードの場合は、CIMC IP アドレスとログイン情報を指定する必要があります。

   仮想ノードの場合、管理 IP アドレスは保持されるため、rescue-user のパスワードのみを入力する必要があります。

6. 残りのノード情報が正確であることを確認します。
7. **[登録（Register）]** をクリックしてノードを再登録し、マスターノードをクラスタに再度追加します。

   ノードのブートストラップ、設定、および再追加には最大 20 分かかります。完了すると、ノードは UI にアクティブなマスターノードとして表示されます。

仮想クラスタ内の単一マスターノードの交換

ここでは、VMware ESX または Linux KVM 仮想 Nexus Dashboard クラスタでマスターノードの障害から回復する方法について説明します。この手順では、置換するノードと同じフォームファクタを使用してまったく新しい Nexus Dashboard ノードを展開し、残りのクラスタにマスターノードとして加えます。

1. 障害が発生したノードの VM の電源がオフになっていることを確認します。
2. 新しい Nexus Dashboard ノードを起動します。

   VMware ESX で追加のノードを起動する方法については、「VMware ESX における 追加の仮想ノードの展開」を参照してください。交換するノードと同じタイプ（OVA-App または OVA-Data）のノードを起動する必要があることに注意してください。

   Linux KVM で追加のノードを起動する方法については、「Linux KVM における 追加の仮想ノードの展開」を参照してください。

   障害が発生したノードとまったく同じネットワーク設定を使用していることを確認します。

3. 新しいノードの VM の電源をオンにして、起動するまで待ちます。
4. Nexus Dashboard 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。

5. ノードを置換します。
   a. 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。

      置換するノードが [非アクティブ（Inactive）] としてリスト化されます。

b. 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。

c. 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。

クラスタはそのノードの管理 IP アドレスに接続して接続性を確認します。

d. **[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。

スタンバイノードのない単一の物理マスターノードの交換

ここでは、スタンバイノードのない Nexus Dashboard 物理クラスタで単一のマスターノードの障害から回復する方法について説明します。この手順は、物理的に置換する必要があるハードウェアの問題を対象としていますノードのソフトウェア状態が不良の場合は、代わりに acs reboot clean コマンドを使用し、「物理クラスタへの 同じマスターノードの再追加」の説明に従って、同じノードをクラスタに再追加できます。

クラスタにスタンバイノードが設定されている場合は、「単一マスターノードと スタンバイノードの置換」の手順に従うことを推奨します。

はじめる前に

- 少なくとも 2 つのマスターノードが正常であることを確認します。

  2 つのマスターノードを使用できない場合は、「2 つのマスターノードをスタンバイノードに置き換える」の説明に従って、クラスタを手動で復元する必要があります。

- 置換するマスターノードの電源がオフになっていることを確認します。
- 「追加の物理ノードの展開」の説明に従って、新しいノードを準備して展開します。
- 障害が発生したノードと同じ CIMC IP アドレスとログイン情報が新しいノードに設定されていることを確認します。

  残りのマスターノードは CIMC 情報を使用して、新しいノードで設定を復元します。

- 新しいノードの電源がオンになっていることを確認し、シリアル番号をメモします。

障害が発生した単一のマスターノードを置換するには、次の手順を実行します。

1. 他のいずれかのマスターノードの管理 IP を使用して Nexus Dashboard GUI にログインします。
2. メイン ナビゲーション メニューから、**[システムリソース（System Resources）] > [ノード（Nodes）]** を選択します。
3. ノードリストで、置換するノードの**シリアル**番号を見つけ、ノードの**ステータス**が [非アクティブ（Inactive）] と表示されていることを確認します。
4. Nexus Dashboard の **[ノード（Nodes）]** 画面で、非アクティブなノードの横にあるチェックボックスをオンにして選択します。
5. **[アクション（Actions）]** メニューから **[置換（Replace）]** を選択します。

6. **[新しいシリアル番号（New Serial Number）]** フィールドに新しいノードのシリアル番号を入力し、**[置換（Replace）]** をクリックします。

   プロセスが完了すると、古いノードのシリアル番号が新しいノードのシリアル番号に更新され、新しいマスターノードがクラスタに正常に参加すると、ステータスが [アクティブ（Active）] に変わります。

ワーカーノードまたはスタンバイノードの交換

障害が発生したワーカーノードを置換する場合は、通常のように GUI から非アクティブノードを削除して、まったく新しいワーカーノードを展開します。

はじめる前に

- 置換するワーカーノードの電源がオフになっていることを確認します。

障害が発生したワーカーノードを置換するには、次の手順を実行します。

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. メイン ナビゲーション メニューから、**[システムリソース（System Resources）] > [ノード（Nodes）]** を選択します。
3. ノードリストで、置換するノードの**シリアル**番号を見つけ、ノードの**ステータス**が [非アクティブ（Inactive）] と表示されていることを確認します。
4. 横にあるチェックボックスをクリックして、非アクティブなノードを選択します。
5. **[アクション（Actions）]** メニューから **[削除（Delete）]** を選択します。

   これにより、リストからノードが削除されます。

6. 「ワーカーノードの管理」または「スタンバイノードの管理」の説明に従い、新しいノードの電源をオンにして、新しいワーカーノードまたはスタンバイノードとしてクラスタに追加します。

   古いノードの設定に使用したものと同じ設定パラメータを使用します。

初期クラスタブートストラップの問題

ここでは、初期クラスタ ブートストラップ プロセスのさまざまな段階について説明し、Nexus Dashboard クラスタを最初に展開する際に発生する可能性のあるいくつかの一般的な問題についてまとめます。

ノードを起動して GUI のセットアップ時に各ノードの情報を入力すると、初期ブートストラッププロセスはいくつかの段階を経て、ノードの起動、必要な情報の設定、およびクラスタの作成を実行します。ブートストラップ画面では、進行状況を追跡し、発生する可能性のある問題を示します。

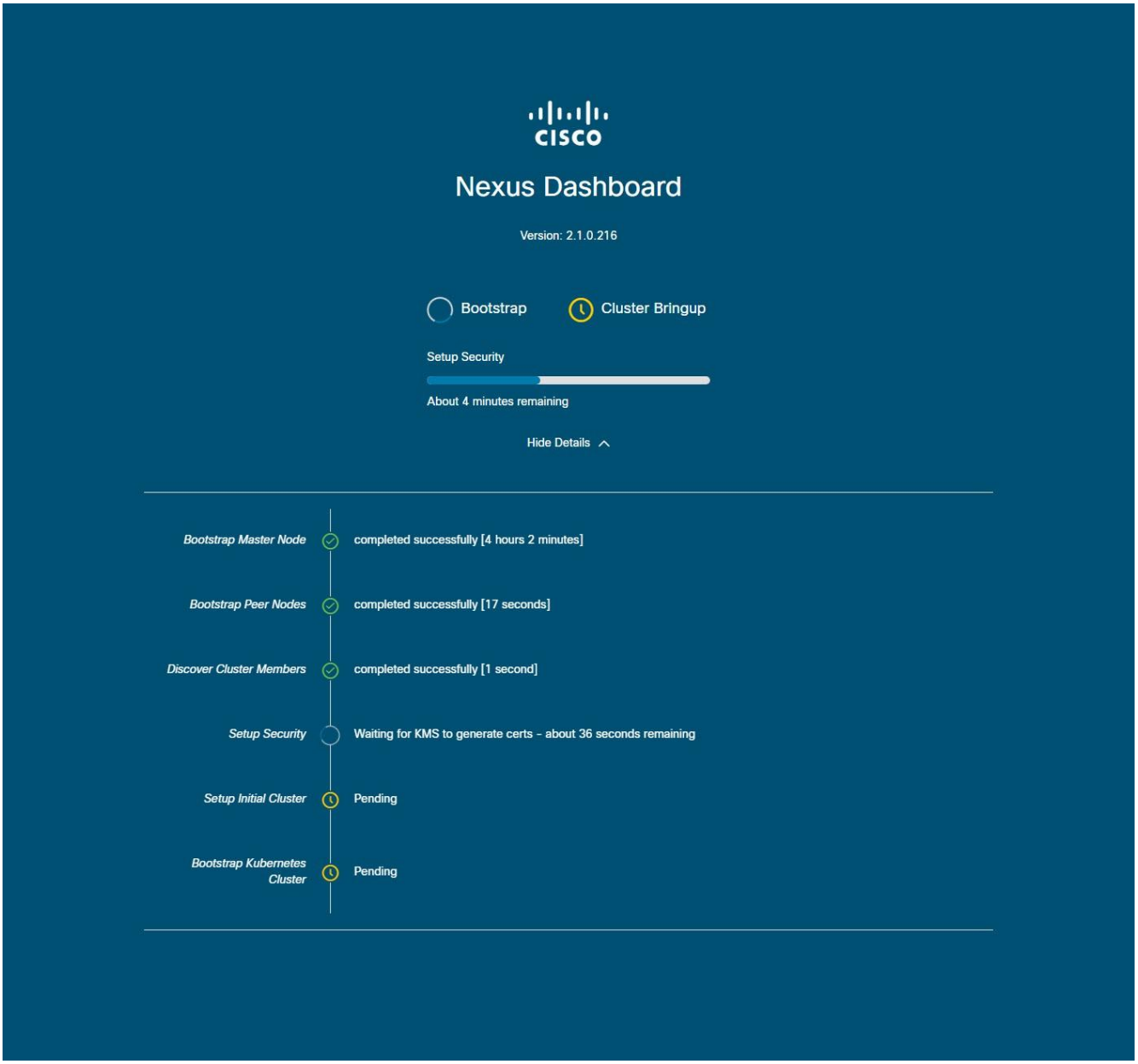


図 18 ブートストラップの進行状況

- ブートストラップ マスターノードとブートストラップピアノード - ユーザーが指定した管理ネットワークとデータネットワークの IP アドレスを使用して、最初のマスターノードを起動します。次に、2 番目と 3 番目のマスターノードをそれぞれの IP を使用して起動します。

  これらの段階のいずれかでプロセスが失敗した場合は、各ノードのコンソールに接続して、入力したすべての情報が正しいことを確認します。acs system-config コマンドを使用すると、設定内容を表示できます。

  ブートストラップログ（/logs/k8/install.log）で詳細を確認することもできます。

  通常、acs reboot factory-reset を使用してノードをリセットし、セットアッププロセスを再起動することで、設定不備が原因で発生した問題を解決できます。

- クラスタメンバーの発見 - データネットワークを介してクラスタ内のすべてのマスターノード間の接続を確立します。

  この段階の障害は通常、データネットワーク IP アドレスの設定ミスと、ノードが他の 2 つのピアに到達できないことを示しています。

任意のノードで acs cluster masters コマンドを使用して、指定したデータ IP を確認できます。

コマンドが情報を返さない場合は、ip addr を使用してデータインターフェイス（bond0br）の IP アドレスを確認し、すべてのノードの IP が他のノードから到達可能であることを確認します。

```
$ ip addr
[..]
6: bond0br: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state
UP group default qlen 1000
    link/ether 52:54:00:e1:93:06 brd ff:ff:ff:ff:ff:ff
    inet 10.195.255.165/24 brd 10.195.255.255 scope global bond0br
       valid_lft forever preferred_lft forever
    inet6 fe80::5054:ff:fee1:9306/64 scope link
       valid_lft forever preferred_lft forever
[..]
```

- セキュリティの設定 - キー管理サービス（KMS）を設定して、ノード間のデータ暗号化を有効にします。

  acs cluster masters コマンドが ca cert not found エラーを返す場合、KMS の問題であることを示しています。詳細については、/logs/kms ログを確認してください。

- 初期クラスタとブートストラップ Kubernetes クラスタのセットアップ - こうした段階での障害は、通常、Kubernetes の問題であることを示しています。

  各ノードの /logs/k8 ログから追加の詳細情報を取得できます。

- **ブートストラップ**の段階が完了すると、プロセスは**クラスタの立ち上げ**の段階に進みます。

  システムの初期化からインフラサービスの準備完了待ちまでの各段階で、残りのサービスを起動してクラスタの作成を完了します。

  この段階で、いずれかのノードで acs health コマンドを使用して、正しく起動していないサービスを確認できます。次に、/logs/k8_infra/*<service>* で特定のサービスのログを確認します。

マルチクラスタ接続の問題

次のセクションでは、マルチクラスタ接続に関する一般的な問題について説明します。

複数のクラスタをまとめて接続する方法の詳細については、「マルチクラスタ接続」を参照してください。

非プライマリクラスタが再接続できない

マルチクラスタ接続グループに属していたクラスタをクリーンリブートして再展開すると、グループのプライマリクラスタはそれを認識できないため、クラスタが到達不能のままになります。

この問題を解決するには、クラスタを接続解除して再接続します。

1. プライマリクラスタにログインします。
2. 再展開したクラスタをグループから削除します。

   これについては、「クラスタの切断」を参照してください。

3. グループにクラスタを再度追加します。

   これについては、「複数のクラスタの接続」を参照してください。

古いバージョンで再展開された非プライマリクラスタ

何らかの理由で、この機能をサポートしていないバージョンの Nexus Dashboard を使用して、グループ内の非プライマリクラスタの 1 つを再展開した場合、プライマリクラスタは引き続きそのクラスタに接続できますが、取得することはできません。 情報と UI は空白のままになります。

この問題を解決するには、そのクラスタをグループから削除します。

1. 管理ユーザーとしてプライマリクラスタにログインします。

   すべてのクラスタで共有されているリモートユーザーでログインすると、UI ページは空白のままになります。

2. 再展開したクラスタをグループから削除します。

   これについては、「クラスタの切断」を参照してください。

3. ログアウトして、マルチクラスタ接続の管理に使用するリモートユーザーを使用して再度ログインし、UI が正しく読み込まれることを確認します。

秘密キーと自己署名証明書の生成

このセクションでは、Nexus Dashboard クラスタで秘密キーとカスタム証明書を使用する場合にそれらを生成する方法の例を示します。Nexus Dashboard GUI でキーと証明書を追加するために必要な設定手順は、「セキュリティ」の章で説明されています。

1. 秘密キーの生成

   OpenSSL がインストールされている任意のプラットフォームで秘密キーを生成するか、rescue-user として Nexus Dashboard ノードの 1 つに SSH で接続し、そこでこの手順を実行します。

```
[rescue-user@localhost ~]$ openssl genrsa -out nd.key 2048
Generating RSA private key, 2048 bit long modulus
.....................
.............
e is 65537 (0x10001)
[rescue-user@localhost ~]$ ls
nd.key
```

2. 認証局(CA)キーを生成します。

   実稼働環境では、通常、IdenTrust や DigiCert などの公開 CA を使用し、それらから CA 署名付き証明書を受け取るため、この手順をスキップできます。

   ラボやテストの目的などで自己署名 CA を生成する場合は、次のコマンドを実行します。

```
[rescue-user@localhost ~]$ openssl genrsa -out ca.key 2048
Generating RSA private key, 2048 bit long modulus
.....................
.............
e is 65537 (0x10001)
[rescue-user@localhost ~]$ ls
ca.key nd.key
```

3. CA の CSR を生成します。

   実稼働展開の場合は、この手順をスキップしてください。

```
[rescue-user@localhost ~]$ openssl req -new -key ca.key -subj
" /CN=Self/C=US/O=Private/ST=Texas"  -out ca.csr
[rescue-user@localhost ~]$ ls
ca.csr ca.key nd.key
```

   次のコマンドを使用して、生成した CSR を確認できます。

```
[rescue-user@localhost ~]$ openssl req -in ca.csr -text -noout
```

4. 自己署名ルート証明書を作成します。

   実稼働展開の場合は、この手順をスキップしてください。

```
[rescue-user@localhost ~]$ openssl x509 -req -in ca.csr -signkey ca.key
-CAcreateserial -out ca.crt -days 3650
Signature ok
subject=/CN=Self/C=US/O=Private/ST=Texas
Getting Private key
[rescue-user@localhost ~]$ ls
ca.crt ca.csr ca.key nd.key
```

   次のコマンドを使用して、生成したルート証明書を確認できます。

```
[rescue-user@localhost ~]$ openssl x509 -in ca.crt -text -noout
```

5. 最初のステップで生成した秘密キーで署名された CSR を生成します。

実稼働展開の場合は、この手順をスキップしてください。

a. 必要な情報を含む CSR 構成ファイル（csr.cfg）を作成します。

構成ファイルの例を以下に示します。

```
[req]
default_bits = 2048
distinguished_name = req_distinguished_name
req_extensions = req_ext
prompt = no
[req_distinguished_name]
countryName = US
stateOrProvinceName = Texas
localityName = Plano
organizationName = CSS
organizationalUnitName = DC
commonName = nd.dc.css
emailAddress = no-reply@mydomain.com
[req_ext]
subjectAltName = @alt_names
[alt_names]
DNS.1 = *.dc.css
IP.1 = 10.0.0.96
IP.2 = 10.0.0.97
```

b. CSR を作成します。

```
[rescue-user@localhost ~]$ openssl req -new -key nd.key -out nd.csr -config
csr.cfg
[rescue-user@localhost ~]$ ls
ca.crt ca.csr ca.key csr.cfg nd.csr nd.key
```

次のコマンドを使用して、生成した CSR を確認できます。

```
[rescue-user@localhost ~]$ openssl req -in nd.csr -text -noout
```

6. 署名された証明書を取得または自己署名します。

実稼働環境では、IdenTrust や DigiCert などの公開 CA から署名付き証明書を取得します

証明書に自己署名するには、次を実行します。

```
[rescue-user@localhost ~]$ openssl x509 -req -in nd.csr -CA ca.crt -CAkey ca.key
-CAcreateserial -out nd.crt -days 3600
Signature ok
subject=/C=US/ST=Texas/L=Plano/O=CSS/OU=DC/CN=nd.dc.css/emailAddress=no-
reply@mydomain.com
Getting CA Private Key
[rescue-user@localhost ~]$ ls
ca.crt ca.csr ca.key ca.srl csr.cfg nd.crt nd.csr nd.key
```

7. 署名済み証明書を確認します。

```
[rescue-user@localhost ~]$ openssl verify -verbose -CAfile ca.crt nd.crt
nd.crt: OK
```

8. 生成されたファイルの内容を Nexus Dashboard の GUI に追加します。

   「セキュリティの設定」で説明されている手順に従って、前の手順で生成した次の 3 つのファイルの内容を入力する必要があります。

   - 秘密キー（nd.key）
   - 認証局（CA）パブリック証明書（ca.crt）
   - CA 署名付き証明書（nd.crt）