Cisco Nexus Dashboard User Guide, Release 2.3.x

Table of Contents

初版: 2023-01-31
最終更新日: 2023-03-09

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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

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

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

Table 1. Latest Updates

リリース	変更	文書化場所
2.3.1	このドキュメントの最初のリリース	—

このドキュメントの最新バージョン

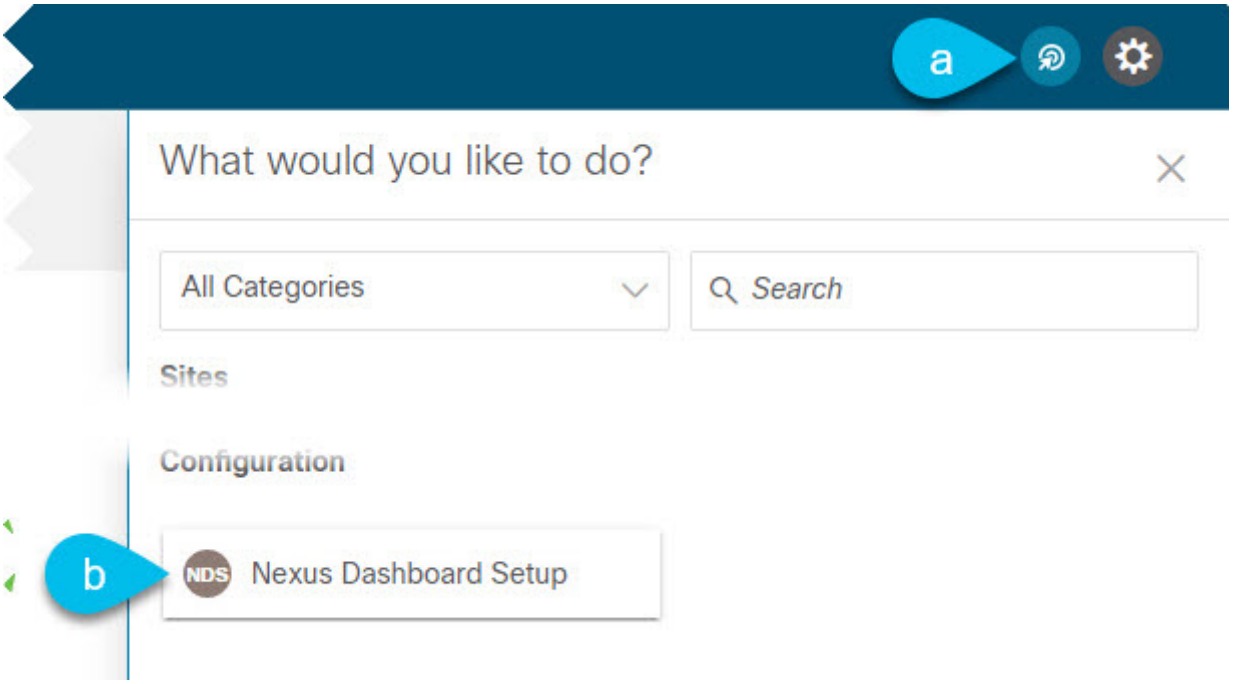
このドキュメントは、Nexus DashboardのGUIおよびインターネット上のwww.cisco.comから入手できます。
このドキュメントの最新バージョンについては、https://www.cisco.com/c/dam/en/us/td/docs/dcn/nd/2x/user-guide/cisco-nexus-dashboard-user-guide-211.pdf にアクセスしてください。 [*Nexus Dashboard User Guide*].

初回セットアップ

新しいNexus
Dashboard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るようになります。

。[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。 。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 Network Controllerで管理される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。

注：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。

。[プロキシ設定（**Proxy Configuration**）] タイルで、[開始（**Begin**）] をクリックします。 。[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。 .. [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。 .. [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。 .. 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。 。（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

始める前に

- 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またはクラウド ネットワーク コントローラ 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、 [Fabric Connectivity] 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 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 接続を構成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構成する必要があります。

    これは通常、初期のクラスタ展開に行なわれます。そして詳細についは、https://www.cisco.com/c/en/us/support/data-center-analytics/nexus-dashboard/products-installation-guides-list.html[*Cisco Nexus Dashboard Deployment Guide*]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。

。[サイトの追加（**Add Sites**）] タイルで、[開始（**Begin**）] をクリックします。 。[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。 。追加するサイトのタイプを選択します。

+ 注：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、https://www.cisco.com/c/dam/en/us/td/docs/Website/datacenter/day2ops/index.html[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の ACI サイト向け * **Cloud Network Controller** — Cisco Cloud Network ControllerCloud ACI によって管理されるクラウド サイト向け * **NDFC** — Cisco NDFC によって管理されるオンプレミスサイト向け

。サイト情報を入力します。 .. 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/IP アドレス（**Host Name/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。

+ 注：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。 （オプション）*ピア証明書を検証 — Nexus ダッシュボードが接続する（例えばサイトコントローラ）ホストの証明書が有効であることと信頼されている 認証局（CA）にサインされていることを検証することを許可します。

  注：このオプションを使用してサイトを追加する前に Nexus ダッシュボードに証明書が既にインポートされていることが必要です。証明書を既に追加していなければ サイトを追加 ウィザードをキャンセルして最初に、[Validating Peer Certificates] に記されている手順に従います。そして、証明書をインポートした後にここに説明されている通りにサイトを追加します。

  有効な証明書をインポートせずに*ピア証明書を検証* オプションを有効にするとサイトの導入準備は機能不全になります。

（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、[Fabric Connectivity] 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。

+ .. クラウド ネットワーク コントローラ 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/IPアドレス* クラウド ネットワークコントローラとの通信に使用されます。

+ 注：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。 （オプション）*ピア証明書を検証 — Nexus ダッシュボードが接続する（例えばサイトコントローラ）ホストの証明書が有効であることと信頼されている 認証局（CA）にサインされていることを検証することを許可します。

  注：このオプションを使用してサイトを追加する前に Nexus ダッシュボードに証明書が既にインポートされていることが必要です。証明書を既に追加していなければ サイトを追加 ウィザードをキャンセルして最初に、[Validating Peer Certificates] に記されている手順に従います。そして、証明書をインポートした後にここに説明されている通りにサイトを追加します。

有効な証明書をインポートせずに*ピア証明書を検証*
オプションを有効にするとサイトの導入準備は機能不全になります。

（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。

+ 注：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、[Configuring Proxy] を参照してください。

a. NDFC 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/IP アドレス* — Cisco NDFC との通信に使用されます。

  これは NDFC のインバンドIPアドレスである必要があります。

  注：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。（オプション）*ピア証明書を検証 — Nexus ダッシュボードが接続する（例えばサイトコントローラ）ホストの証明書が有効であることと信頼されている 認証局（CA）にサインされていることを検証することを許可します。

  注：このオプションを使用してサイトを追加する前に Nexus ダッシュボードに証明書が既にインポートされていることが必要です。証明書を既に追加していなければ サイトを追加 ウィザードをキャンセルして最初に、[Validating Peer Certificates] に記されている手順に従います。そして、証明書をインポートした後にここに説明されている通りにサイトを追加します。
  有効な証明書をインポートせずに*ピア証明書を検証*
  オプションを有効にするとサイトの導入準備は機能不全になります。

- **Sites** — 指定したコントローラに管理されている NDFC ファブリックを選択するためにサイトを選択 をクリックします。 。[追加（**Add**）] をクリックして、サイトの追加を終了します。 。（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。 。(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構成

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。

。ネットワーク スケール*タイルで、*開始 をクリックします。 。セットアップ - ネットワークスケール ページで、必要な情報を入力します。

+
注：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 フィールドに、この Nexus ダッシュボード クラスタが管理する、展開のサイトの目標数を入力します。

   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 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 ドロップダウンメニューから、Nexus ダッシュボード インサイト サービスにおけるターゲットフロー数を選択します。

プラットフォーム概要

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

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

Nexus ダッシュボード クラスタは通常、1 つまたは 3 つの`マスター`ノードで構成されます。また、3 ノード
クラスタの場合、マスターノードで障害が発生した際に簡単にクラスタを回復させられるよう、いくつかの ワーカー ノードをプロビジョニングして、水平スケーリングや スタンバイ ノードを有効化できます。このリリースでサポートされる最大の ワーカー と スタンバイ ノードの数は、https://www.cisco.com/c/en/us/support/data-center-analytics/nexus-dashboard/products-release-notes-list.html[*Cisco Nexus Dashboard Release Notes*] の「検証された拡張性の制限」セクションを参照します。ノードを追加してクラスターを拡張する方法の詳細については、 [Infrastructure Management] 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 ダッシュボード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、https://www.cisco.com/c/en/us/td/docs/dcn/nd/2x/hardware/cisco-nexus-dashboard-hardware-setup-guide-2x.html[*Nexus Dashboard Hardware Setup Guide*] を、展開計画と Nexus ダッシュボードソフトウェアのインストールについては、https://www.cisco.com/c/en/us/support/data-center-analytics/nexus-dashboard/products-installation-and-configuration-guides-list.html[*Nexus Dashboard Deployment Guide*] を参照してください。

サービス

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

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

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

物理的な Nexus ダッシュボードサーバーを購入する場合、Nexus ダッシュボード Insights および Nexus Dashboard Orchestrator サービスを、出荷前にハードウェアに事前インストールすることを選択できます。詳細については、https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/nexus-dashboard/guide-c07-744361.html[*Nexus Dashboard Ordering Guide*]を参照します。Nexus ダッシュボードの仮想またはクラウド フォーム ファクタを展開している場合、クラスタの準備が整った後にサービスを個別に展開する必要があることに注意してください。

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。

注：すべてのサービスがすべてのフォーム
ファクタでサポートされているわけではありません。展開を計画するときは、フォーム
ファクターのためのhttps://www.cisco.com/c/dam/en/us/td/docs/dcn/tools/nd-sizing/index.html[Nexus Dashboard Cluster Sizing] ツールとクラスタ サイズの要件確認します。

- Cisco Nexus ダッシュボード物理アプライアンス（.iso）

  このフォームファクタは、Cisco Nexus Dashboardソフトウェアスタックがプレインストールされた状態で購入した元の物理アプライアンスハードウェアを指します。

  このドキュメントの後半のセクションでは、既存の物理アプライアンスハードウェアでソフトウェアスタックを設定してクラスタを展開する方法について説明します。元の Cisco Nexus ダッシュボードプラットフォーム
  ハードウェアのセットアップについては、https://www.cisco.com/c/en/us/support/data-center-analytics/nexus-dashboard/products-installation-guides-list.html[*Cisco Nexus Dashboard Hardware Setup Guide*] で説明されています。

- 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用に設計されたノード プロファイル
  - アプリ ノード：Nexus Dashboard Orchestrator などの非データ集約型アプリケーション用に設計されたノード プロファイル

- Linux KVM（.qcow2）

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

- Amazon Web Services（.ami）

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

- Microsoft Azure（.arm）

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

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

  リリース2.2(1)以降、既存のRed Hat Enterprise LinuxサーバーでNexus

Dashboardノードを実行できます。

クラスタサイジングのガイドライン

前述のように、Nexus Dashboard クラスタは、最初に 1 つまたは 3 つのマスターノードを使用して展開されます。実行するサービスの種類と数によっては、クラスタに追加の`ワーカー`ノードを展開することが必要な場合があります。クラスタのサイジング情報と、特定の使用例に基づく推奨ノード数については、https://www.cisco.com/c/dam/en/us/td/docs/dcn/tools/nd-sizing/index.html[*Nexus Dashboard Capacity Planning*] ツールを参照してください。

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

クラスタへのワーカーノードの追加については、 [Managing Worker Nodes] 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、 [Managing Standby Nodes] を参照してください。

サポートされるサービス

サポートされるアプリケーションの完全なリストおよび関連する互換性情報については、https://www.cisco.com/c/dam/en/us/td/docs/dcn/tools/dcn-apps/index.html[*Data Center Networking Services Compatibility Matrix*] を参照してください。

要件と注意事項

ネットワーク時間プロトコール（NTP）とドメイン ネーム システム（DNS）

Nexus ダッシュボード ノードでの展開とアップグレードには、常に、有効な DNS サーバーと NTP サーバーが必要です。

有効な DNS 接続がない場合（到達不能またはプレースホルダ IP アドレスを使用している場合など）、システムを正常に展開またはアップグレードできない可能性があります。

注：Nexus ダッシュボードは、DNS クライアントとリゾルバーの両方として機能します。内部サービス向けには、DNS リゾルバーとして機能する内部の Core DNS サーバーを使用します。また、DNS クライアントとしても動作して、イントラネット内またはインターネットの外部ホストに到達できるようにするためには、外部 DNS サーバーを構成する必要があります。+ 加えて、Nexus Dashboard は、ワイルドカード レコードを持つ DNS サーバーをサポートしていません。

Nexus ダッシュボード外部ネットワーク

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

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

データネットワーク	管理ネットワーク
• Nexus ダッシュボード ノードのクラスタリング • アプリケーション間の通信 • 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 ダッシュボード 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 ダッシュボード ファームウェアのアップロード • Cisco DC App Center（AppStore） [Services Management] の説明に従って Nexus ダッシュボード アプリストアからアプリケーションをインストールするには、管理ネットワーク経由でページ https://dcappcenter.cisco.com にアクセスできる必要があります。 • Intersight デバイス コネクタ

2つのネットワークには次の要件があります。

- すべての新しい Nexus ダッシュボード展開では、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 ダッシュボード Insights サービスの場合、データ ネットワークは、各ファブリックおよび APIC のインバンド ネットワークに IP 到達可能性を提供する必要があります。
- Nexus Dashboard Insights と AppDynamics の統合では、データネットワークが AppDynamics コントローラに IP 到達可能性を提供する必要があります。
- Nexus ダッシュボード オーケストレータ サービスの場合、データ ネットワークは、Cisco APIC サイトに対してインバンドおよび/またはアウトオブバンド IP 到達可能性を持ちますが、Cisco NDFC サイトに対してはインバンド到達可能性が必要です。

*データ ネットワーク インターフェイスで、Nexus ダッシュボード トラフィックに使用できる最小 MTU が 1500 である必要があります。

+ 必要に応じて、高いMTUを設定できます。

- 次の表は、管理ネットワークとデータネットワークのサービス固有の要件をまとめたものです。

  注：データ サブネットを変更するには、クラスタを再展開する必要があるため、将来の追加サービスを考慮して、
  ノードとサービスに必要な最低限よりも大きなサブネットを使用することをお勧めします。このセクションに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 とレイヤ 3 接続両方の永続的な IP アドレスの割り当ては、https://www.cisco.com/c/en/us/support/data-center-analytics/nexus-dashboard/products-installation-and-configuration-guides-list.html[Cisco Nexus ダッシュボード ユーザ ガイド] で説明されているように、UI の外部サービス プール設定を使用してクラスタが展開された後に行われます。

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

Nexus ダッシュボード 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 **IP** の総数
Nexus Dashboard Orchestrator	レイヤ 3 隣接	レイヤ 3 隣接	N/A
SFLOW/NetFlow のない Nexus Dashboard Insights（ACI ファブリック）	レイヤ 3 隣接	レイヤ 3 隣接	N/A

Nexus ダッシュボード 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 **IP** の総数
SFLOW/NetFlow（NDFC ファブリック）のない Nexus ダッシュボード インサイツ	レイヤ 3 隣接	レイヤ 2 隣接	IPv4 を使用している場合、データ インターフェイス ネットワーク内の 6 つの IP IPv6 を使用している場合、データ インターフェイス ネットワーク内の 7 つの IP
SFLOW/NetFlow（ACI または NDFCファブリック）を使用した Nexus ダッシュボード インサイツ	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、リリース 12.0（x）

Nexus ダッシュボードサービス	管理インターフェイス	データインターフェイス	永続 **IP** の総数
レイヤ 2 隣接	レイヤ 2 隣接	If ローカルエリアネットワーク（**LAN**）デバイス管理接続*は、管理（デフォルト）に設定されています： *** SNMP/Syslog** および **SCP** サービス用の管理ネットワーク内の **2** つの **IP** **EPL** が有効になっている場合、各ファブリックのデータネットワークに **1** つの追加 **IP** メディア用の IP ファブリック* が有効になっている場合、テレメトリ用の管理ネットワークに 1 つの追加の IP **LAN** デバイス管理の接続性が データ に設定されている場合： * SNMP/Syslog および SCP サービス用のデータネットワーク内の 2 つの IP ***EPL** が有効になっている場合、各ファブリックのデータネットワークに 1 つの追加 IP * メディア用の **IP** ファブリック が有効になっている場合、テレメトリ用のデータネットワークに 1 つの追加の IP Nexus ダッシュボードファブリックコントローラ、リリース 12.1（1）以降	レイヤ 2 またはレイヤ 3 隣接

Nexus ダッシュボード 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 **IP** の総数
レイヤ 2 またはレイヤ 3 隣接	LAN 展開タイプで **LAN** デバイス管理の接続性が 管理（デフォルト）に設定されたレイヤー 2 モードで動作している場合 * SNMP/Syslog および SCP サービス用の管理ネットワーク内の 2 つの IP **EPL*** が有効になっている場合、各ファブリックのデータネットワークに **1** つの追加 **IP** メディア用の IP ファブリック* が有効になっている場合、テレメトリ用の管理ネットワークに 1 つの追加の IP LAN 展開タイプで **LAN** デバイス管理の接続性が データ に設定されたレイヤー 2 モードで動作している場合： * SNMP/Syslog および SCP サービス用のデータネットワーク内の 2 つの IP **EPL*** が有効になっている場合、各ファブリックのデータネットワークに **1** つの追加 **IP *** メディア用の **IP** ファブリック が有効になっている場合、テレメトリ用のデータネットワークに **1** つの追加の **IP** **LAN** 展開タイプのレイヤ **3** モードで動作している場合：	Cisco Nexus ダッシュボード データ ブローカー	レイヤ 3 隣接

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

  注：Nexus　　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	**RTT** の最大値
Nexus Dashboard クラスタ	ノード間	150 ミリ秒
Nexus ダッシュボード オーケストレータ	ノード間	150 ミリ秒
	サイトへ	500 ミリ秒
Nexus ダッシュボード インサイツ	ノード間	50 ミリ秒
	サイトへ	50 ミリ秒 Nexus Dashboard Fabric Controller
ノード間	50 ミリ秒	サイトへ
50 ミリ秒	Cisco Nexus ダッシュボード データ ブローカー	ノード間
150 ミリ秒		サイトへ

Nexus ダッシュボードの内部ネットワーク

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

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

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

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

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

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

注：異なる　　Nexus　　ダッシュボード　　ノードに展開されたコンテナ間の通信は、VXLAN でカプセル化され、送信元と宛先としてデータ　　インターフェイスの　　IP アドレスを使用します。これは、アプリケーション
オーバーレイとサービスオーバーレイのアドレスがデータネットワークの外部に公開されることはなく、これらのサブネット上のトラフィックは内部でルーティングされ、クラスタノード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。+ 同じ理由で、アプリまたはサービスのサブネットには `169.254.0.0/16`（Kubernetes br1 サブネット）を使用しないことをお勧めします。

BGP 構成と永続的な IP

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

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

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

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

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

通信ポート：Nexus ダッシュボード

Nexus Dashboard クラスタには、次のポートが必要です。

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

Table 2. Nexus ダッシュボード通信ポート（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	出力	TACACS サーバー DNS
53	TCP/UDP	出力	DNS サーバー HTTP 80	TCP
出力	インターネット/プロキシ NTP	123 UDP	出力	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	出力	LDAP サーバー	Radius
1812	TCP	出力	Radius サーバー	KMS
9880	TCP	入力/出力	他のクラスタ ノードと ACI ファブリック	インフラサービス

Table 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	出力	スイッチと APIC の帯域内
HTTPS	443	TCP	出力	スイッチと APIC/NDFC の帯域内 VXLAN
4789	TCP	入力/出力	その他のクラスタ ノード	KMS
9880	TCP	入力/出力	他のクラスタ ノードと ACI ファブリック	インフラサービス

サービス	ポート	プロトコル	方向	接続
3379 3380 8989 9090 9969 9979 9989 15233 30002 ～ 30006 30009 ～ 30010 30012 30014 ～ 30015 30018 ～ 30019 30025 30027	TCP	入力/出力	その他のクラスタノード	Kafka
30001	TCP	入力/出力	スイッチと APIC/NDFC の帯域内	インフラサービス
30016 30017	TCP/UDP	入力/出力	その他のクラスタノード	インフラサービス

通信ポート：Nexus ダッシュボード

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

Table 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	スイッチと APIC/NDFC の帯域内
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	その他のクラスタノード
KMS	9989	TCP	入力/出力	他のクラスタノードと 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

Nexus ダッシュボード ファブリック コントローラ通信ポート

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

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

Nexus ダッシュボード ファブリック コントローラ通信ポート

サービス	ポート	プロトコル	方向	接続
SSH	22	TCP	出力	SSH は、デバイスにアクセスするための基本的なメカニズムです。
SCP	22	TCP	出力	NDFC バックアップファイルをリモートサーバーにアーカイブする SCP クライアント。
SMTP	25	TCP	出力 SMTP ポートは、NDFC のサーバー設定メニューから構成できます。+ これはオプションの機能です。	DHCP

サービス	ポート	プロトコル	方向	接続
67	UDP	入力	NDFC ローカル DHCP サーバーがブートストラップ/POAP 用に構成されている場合。+ これは、LAN 展開にのみ適用されます。+ 注：POAP の目的でローカル DHCP サーバーとして NDFC を使用する場合、すべての ND マスターノードの IP を DHCP リレーとして構成する必要があります。ND ノードの管理 IP またはデータ IP が DHCP サーバーにバインドされるかどうかは、NDFC サーバー設定の LAN デバイス管理接続によって決定されます。	DHCP
68 UDP	出力	SNMP		161
TCP/UDP	出力	NDFC からデバイスへの SNMP トラフィック。	HTTPS/HTTP（NX-API）	443/80
TCP	出力 NX-API HTTPS/HTTP クライアントは、構成可能でもあるポート 443/80 でデバイスの NX-API サーバーに接続します。NX-API はオプション機能であり、NDFC 機能の限られたセットで使用されます。+ これは、LAN 展開にのみ適用されます。	HTTPS（vCenter、Kubernetes、Open Stack、Discovery）	443	TCP

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

Table 5. Nexus ダッシュボード ファブリック コントローラ 永続的 *IP* ポート

サービス	ポート	プロトコル	方向	接続
SCP	22	TCP	入力 SCP は、デバイスと NDFC サービス間でファイルを転送するさまざまな機能によって使用されます。NDFC SCP サービスは、ダウンロードとアップロードの両方の SCP サーバーとして機能します。SCP は、POAP 関連ファイルをダウンロードするために、デバイス上の POAP クライアントによっても使用されます。 + NDFC の SCP-POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続的な IP があります。これは、NDFC サーバー設定の [LAN デバイス管理接続（LAN Device Management Connectivity）] 設定によって制御されます。	TFTP（POAP）

サービス	ポート	プロトコル	方向	接続
69	TCP	入力	POAP 経由のデバイス ゼロタッチ プロビジョニングにのみ使用されます。デバイスは、基本的なインベントリ情報を NDFC に送信して（NDFC への制限付きの書き込み専用アクセス） 、セキュアな POAP 通信を開始できます 。NDFC ブートストラップまたは POAP は、TFTP または HTTP/HTTPS 用に構成できます。 + NDFC の SCP- POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた 永続的な IP があります。これは 、NDFC サーバー設定の [LAN デバイス管理接続（ LAN Device Management Connectivity）] 設定によって制御されます。+ これは、LAN 展開にのみ適用されます。	HTTP（POAP） 80

サービス	ポート	プロトコル	方向	接続
TCP	入力	POAP 経由のデバイス ゼロタッチ プロビジョニングにのみ使用されます。デバイスは、基本的なインベントリ情報を NDFC に送信して（NDFC への制限付きの書き込み専用アクセス） 、セキュアな POAP 通信を開始できます。NDFC ブートストラップまたは POAP は、TFTP または HTTP/HTTPS 用に構成できます。 + NDFC の SCP- POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた 永続的な IP があります。これは 、NDFC サーバー設定の [LAN デバイス管理接続（ LAN Device Management Connectivity）] 設定によって制御されます。+ これは、LAN 展開にのみ適用されます。	BGP	179

サービス	ポート	プロトコル	方向	接続
TCP	入力/出力	エンドポイントロケータの場合、有効になっているファブリックごとに、独自の永続的な IP を使用して EPL サービスが生成されます。このサービスは、常に Nexus Dashboard データインターフェイスに関連付けられています。エンドポイント情報を追跡するために必要な BGP アップデートを取得するために、ファブリック上の適切な BGP エンティティ（通常は BGP ルートリフレクタ）と NDFC EPL サービスはピアを行います。+ この機能は、VXLAN BGP EVPN ファブリックの展開にのみ適用されます。+ これは、LAN 展開にのみ適用されます。	HTTPS（POAP）	443

サービス	ポート	プロトコル	方向	接続
TCP	入力	セキュア POAP は、ポート 443 の NDFC HTTPS サーバーを介して実現されます。HTTPS サーバーは SCP-POAP サービスにバインドされ、そのポッドに割り当てられたのと同じ永続的 IP を使用します。+ NDFC の SCP-POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続的な IP があります。これは、NDFC サーバー設定の [LAN デバイス管理接続（LAN Device Management Connectivity）] 設定によって制御されます。+ これは、LAN 展開にのみ適用されます。 Syslog 5.1(4) UDP	入力	NDFC が Syslog サーバーとして構成されている場合、デバイスからの Syslog は、SNMP-Trap/Syslog サービス ポッド + に関連付けられた永続的な IP に向けて送信されます。 NDFC の SNMP-Trap-Syslog サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続的な IP があります。これは、NDFC サーバー設定の [LAN デバイス管理接続（LAN Device Management Connectivity）] 設定によって制御されます。

サービス	ポート	プロトコル	方向	接続
SCP	2022	TCP	出力	NDFC POAP-SCP ポッドの永続的な IP から、Nexus ダッシュボード インサイツ を実行している別の ND クラスタにテクニカル サポート ファイルを転送します。+ NDFC の SCP-POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた 永続的な IP があります。これは、NDFC サーバー設定の LAN デバイス管理接続設定によって制御されます。

サービス	ポート	プロトコル	方向	接続
SNMP トラップ	2162 UDP	入力	デバイスから NDFC への SNMP トラップは、SNMP -Trap/Syslog サービス ポッドに関連付けられた永続的な IP に向けて送信されます。+ NDFC の SNMP-Trap-Syslog サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続的な IP があります。これは、NDFC サーバー設定の [LAN デバイス管理接続（LAN Device Management Connectivity）] 設定によって制御されます。 GRPC（テレメトリ）	33000
TCP	入力	NDFC 永続的 IP に関連付けられた GRPC トランスポートを介して SAN データ (ストレージ、ホスト、フローなど) を受信する SAN Insights Telemetry サーバー。+ これは、SAN 展開でのみ有効です。	GRPC（テレメトリ）	50051

通信ポート：SAN 展開用 Nexus ダッシュボード ファブリック コントローラ

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

Table 6. 単一ノード クラスタでの *SAN* 展開向けの *Nexus* ダッシュボード ファブリック コントローラポート

サービス	ポート	プロトコル	方向	接続
SSH	22	TCP	出力	SSH は、デバイスにアクセスするための基本的なメカニズムです。
SCP	22	TCP	出力	NDFC バックアップファイルをリモートサーバーにアーカイブする SCP クライアント。
SMTP	25	TCP	出力 SMTP ポートは、NDFC のサーバー設定メニューから構成できます。+ これはオプションの機能です。	SNMP
161	TCP/UDP	出力	NDFC からデバイスへの SNMP トラフィック。	HTTPS（vCenter、Kubernetes、Open Stack、Discovery ）

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

Table 7. 単一ノード クラスタでの *SAN* 展開向けの *Nexus* ダッシュボード ファブリック コントローラ 永続的 *IP* ポート

サービス	ポート	プロトコル	方向	接続
SCP	22	TCP	入力 SCP は、デバイスと NDFC サービス間でファイルを転送するさまざまな機能によって使用されます。NDFC SCP サービスは、ダウンロードとアップロードの両方で機能します。 Syslog 5.1(4) UDP	入力

サービス	ポート	プロトコル	方向	接続
NDFC が Syslog サーバーとして構成されている場合、デバイスからの syslog は、SNMP-Trap/Syslog サービス ポッドに関連付けられた永続的 IP に向けて送信されます。+ NDFC の SNMP-Trap-Syslog サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続的な IP があります。これは、NDFC サーバー設定の [LAN デバイス管理接続（LAN Device Management Connectivity）] 設定によって制御されます。	SNMP トラップ	2162 UDP	入力	デバイスから NDFC への SNMP トラップは、SNMP-Trap/Syslog サービス ポッドに関連付けられた永続的な IP に向けて送信されます。+ NDFC の SNMP-Trap-Syslog サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続的な IP があります。 GRPC（テレメトリ）

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

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

物理ノードのケーブル接続

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。

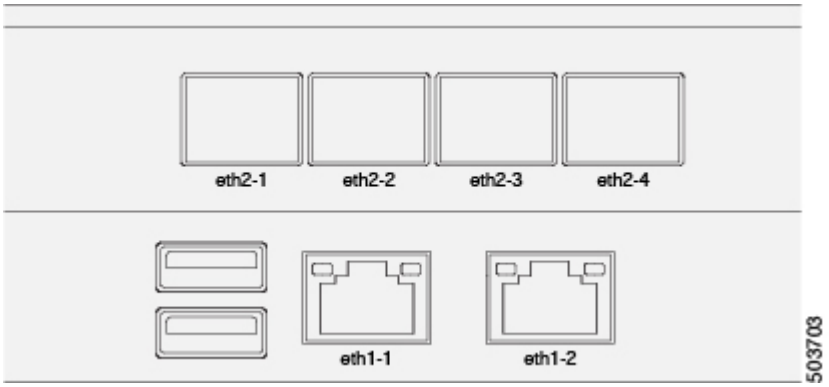


Figure 1. ノードの接続性

インターフェイスは、アクティブ/スタンバイ モードで実行されている、データインターフェイス用と管理インターフェイス用の Linux ボンドとして設定されます。すべてのインターフェイスは個々のホストポートに接続する必要があります。PortChannelおよびvPCはサポートされていません。

Nexus ダッシュボード ノードが Cisco Catalyst スイッチに接続されている場合、VLAN が指定されていない場合、パケットは vlan0 でタグ付けされます。この場合、データ ネットワーク上での到達可能性を確保するために、ノードが接続されているスイッチ インターフェイスに switchport voice vlan dot1p コマンドを追加する必要があります。

外部レイヤ 3 ネットワークを介した接続

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

- Cisco ACI ファブリックのみを管理するために Nexus ダッシュボード オーケストレータを展開する場合は、データ インターフェイスから各サイトの APIC

のインバンドまたはアウトオブバンド（OOB）インターフェイスまたは両方への接続を確立できます。

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

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

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

  ACI ファブリック内に外部接続を構成の詳細は、https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html[*Cisco APIC* レイヤー *3* ネットワーキング構成 *Guide*]にあります。

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

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

- クラスタのセットアップ中にデータ インターフェイスの VLAN ID を指定する場合、その VLAN を許可するトランクとしてホスト ポートを設定する必要があります。

  ただし、ほとんどの一般的な展開では、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。

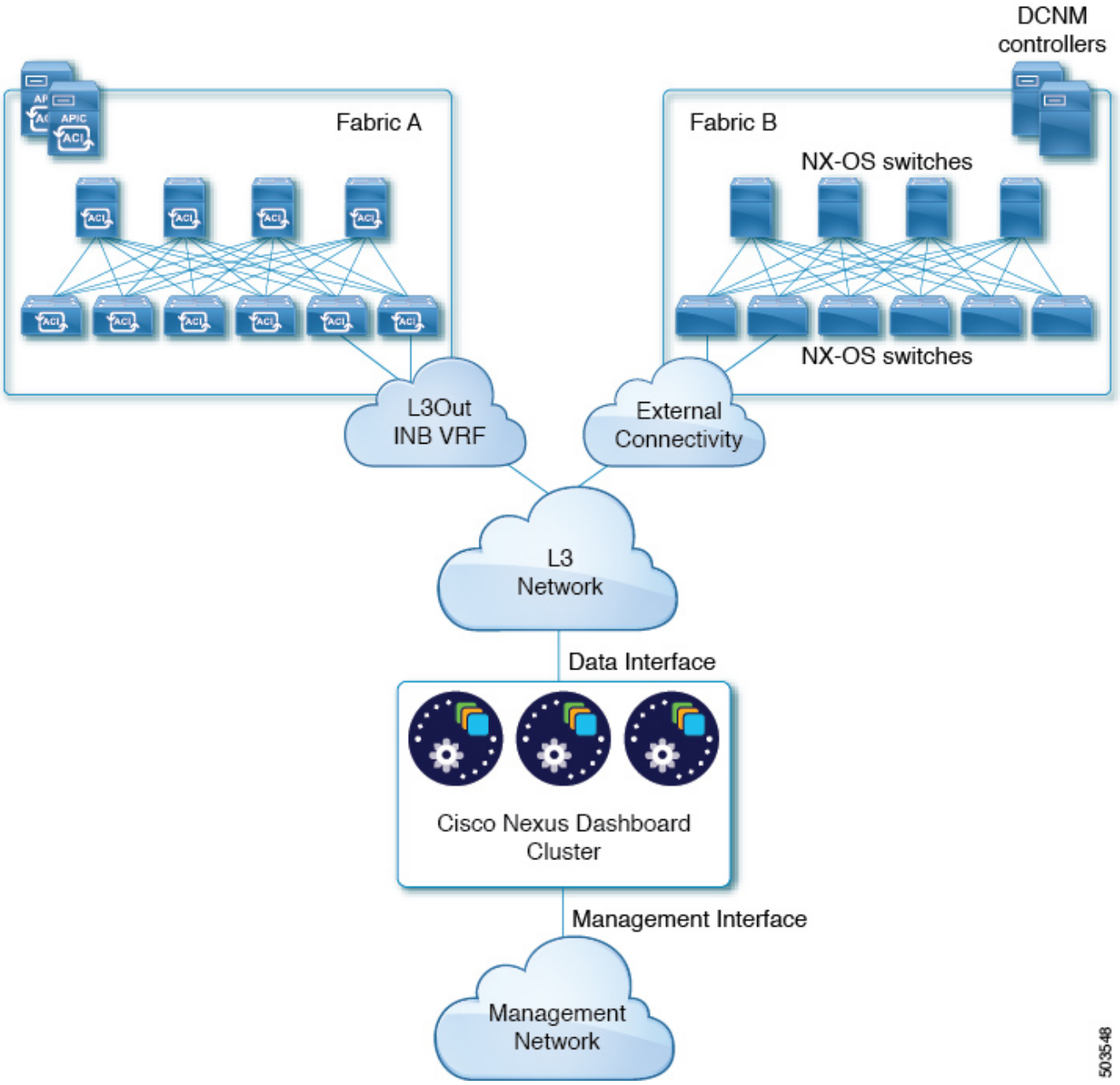


Figure 2. 外部レイヤ *3* ネットワーク経由の接続、*Day-2* 運用サービス

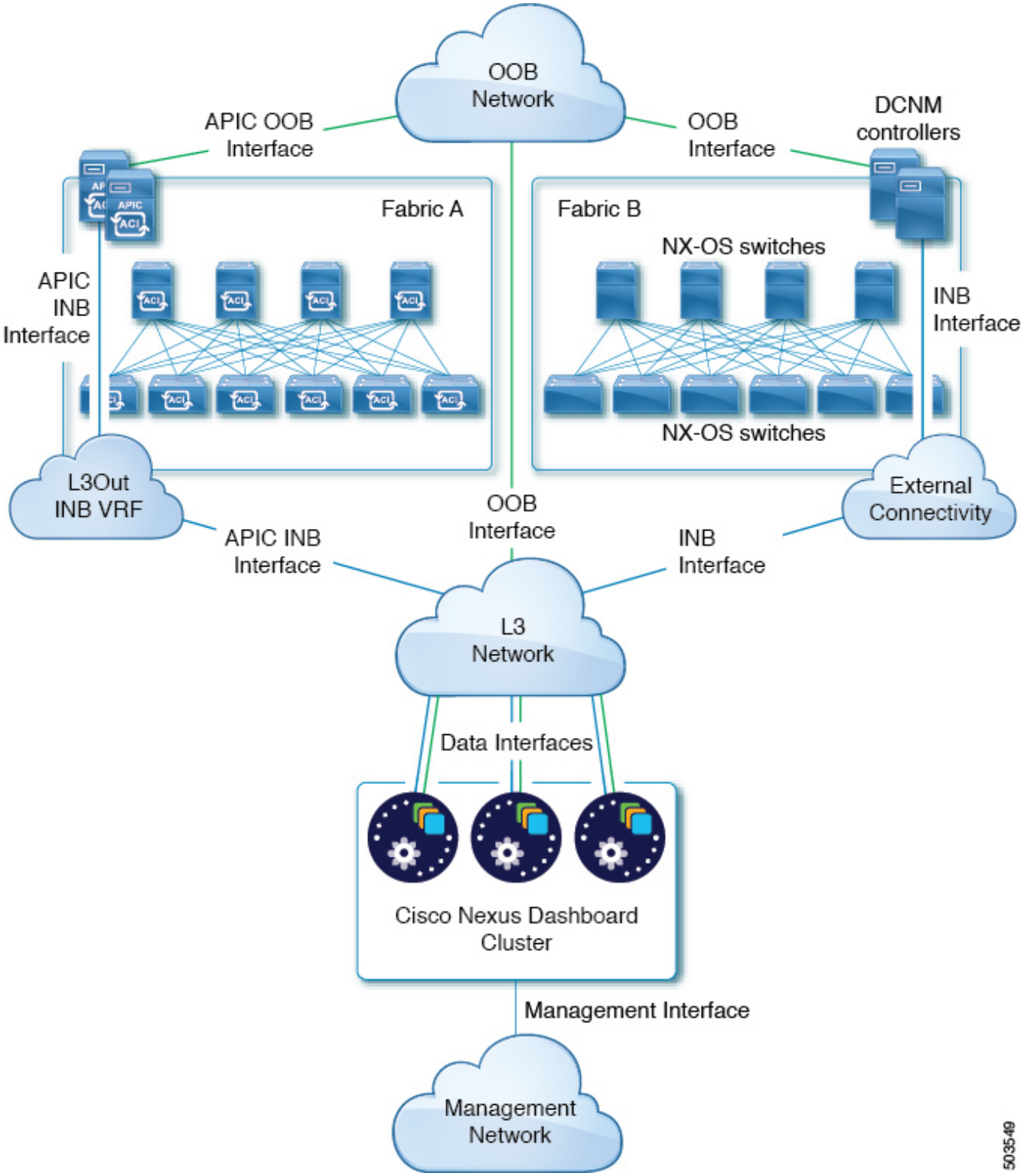


Figure 3. 外部レイヤ *3* ネットワーク経由の接続、*Nexus Dashboard Orchestrator*

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 ダッシュボードオーケストレータを展開する場合は、データ インターフェイスから各サイトのAPICのインバンドまたはアウトオブバンド（OOB）インターフェイス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 ダッシュボードインサイトを展開する場合は、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 を指定する場合は、Nexus ダッシュボード インターフェイスと接続されたネットワークデバイスのポートをトランクとして設定する必要があります。

  ただし、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 ダッシュボード接続用にブリッジドメイン（BD）、サブネット、およびエンドポイント グループ（EPG）を構成することを推奨します。

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

  - ファブリックのインバンド管理 EPG と Cisco Nexus ダッシュボード EPG 間のコントラクトを作成する必要があります。

- 複数のファブリックがサービス エンジンクラスタ上のアプリでモニタリングされている場合、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。

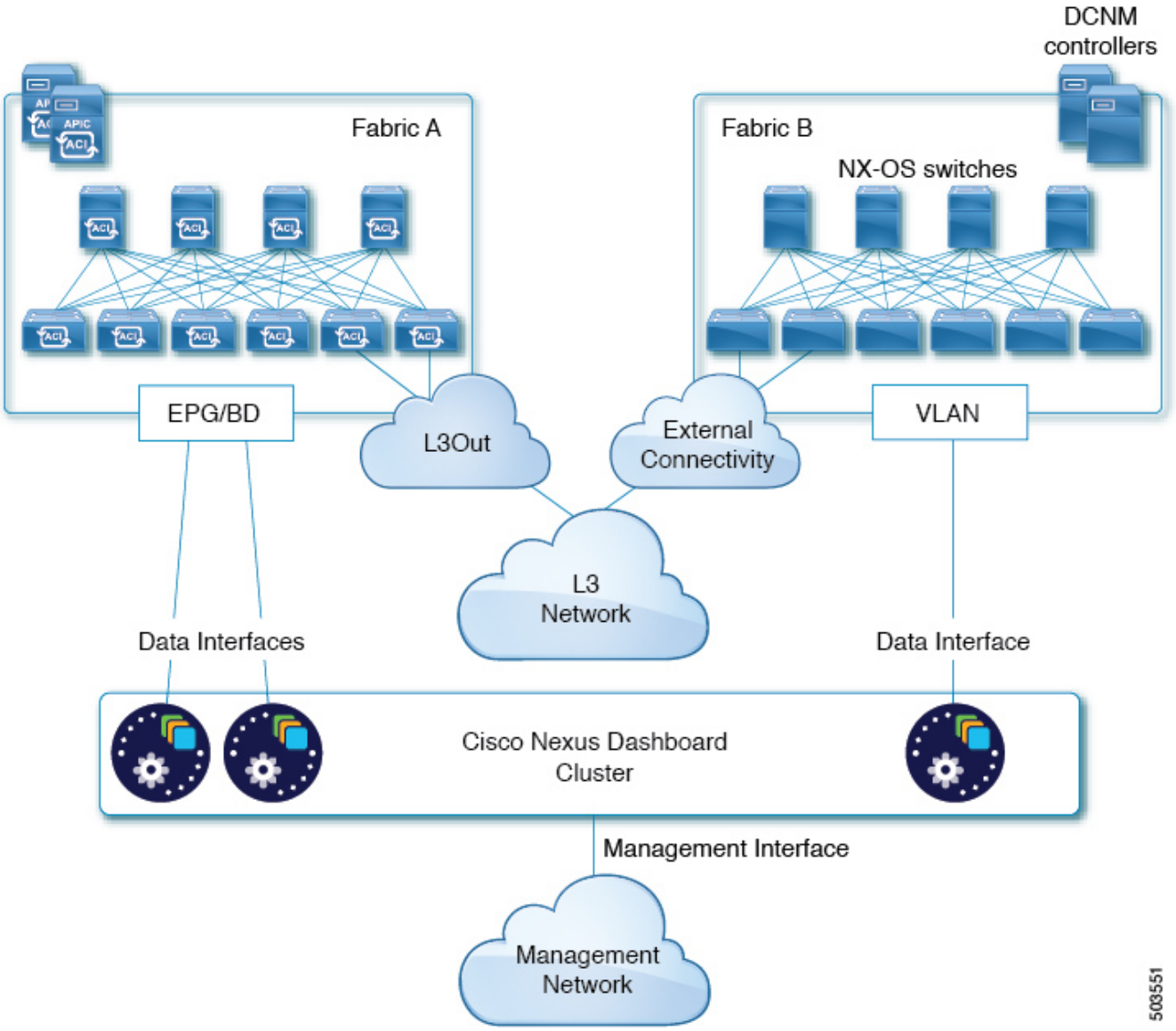


Figure 4. EPG/BD 経由の接続、*Day-2* 運用サービス

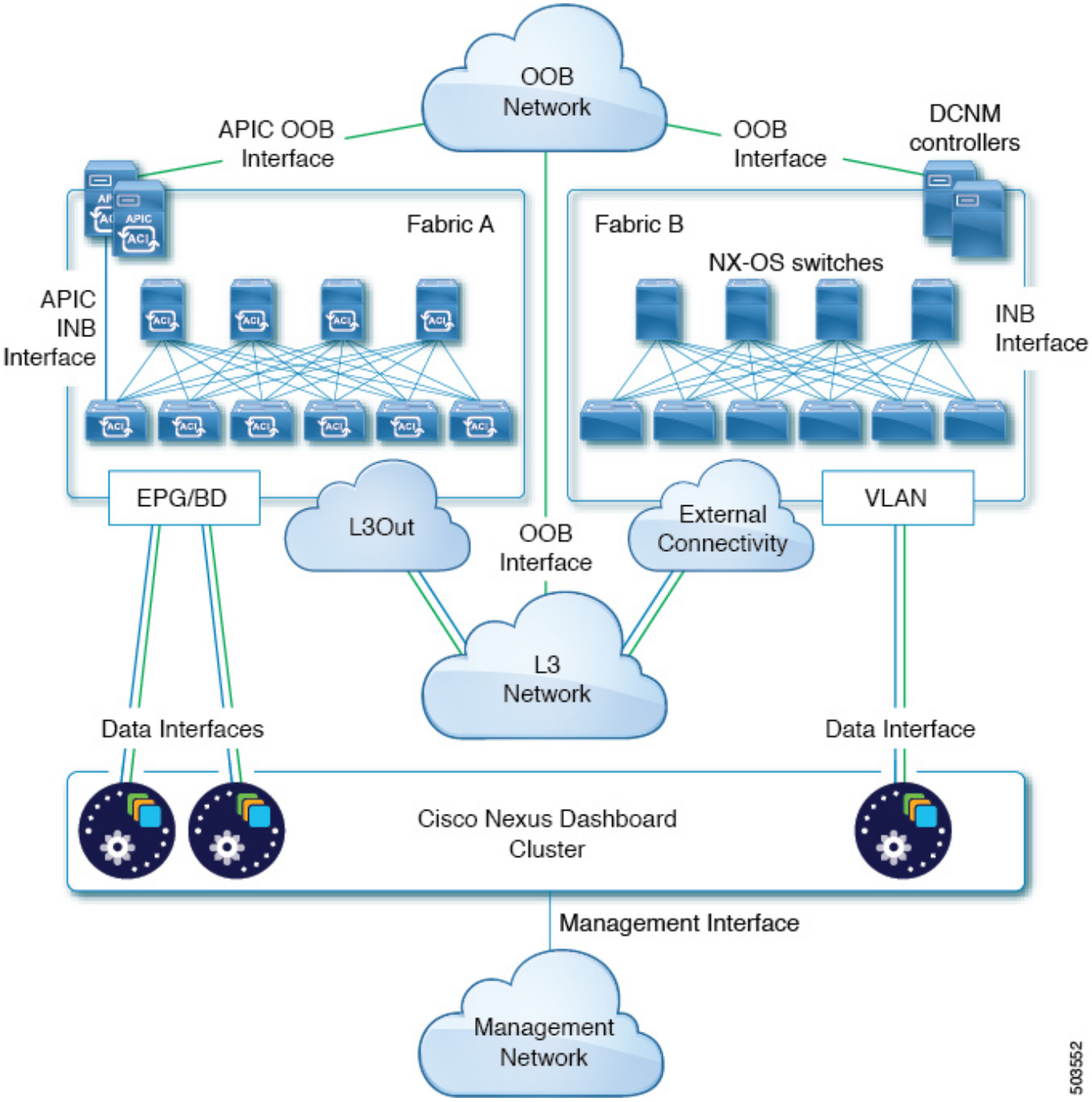


Figure 5. EPG/BD 経由の接続、Nexus Dashboard Orchestrator

GUI の概要

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

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

注：Nexus ダッシュボード GUIにログインしているユーザーの権限に応じて、ユーザー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。ユーザー構成と権限の詳細については、[Users] 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。

ワンビュー 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、およびリソースの使用状況に関する情報が表示されます。

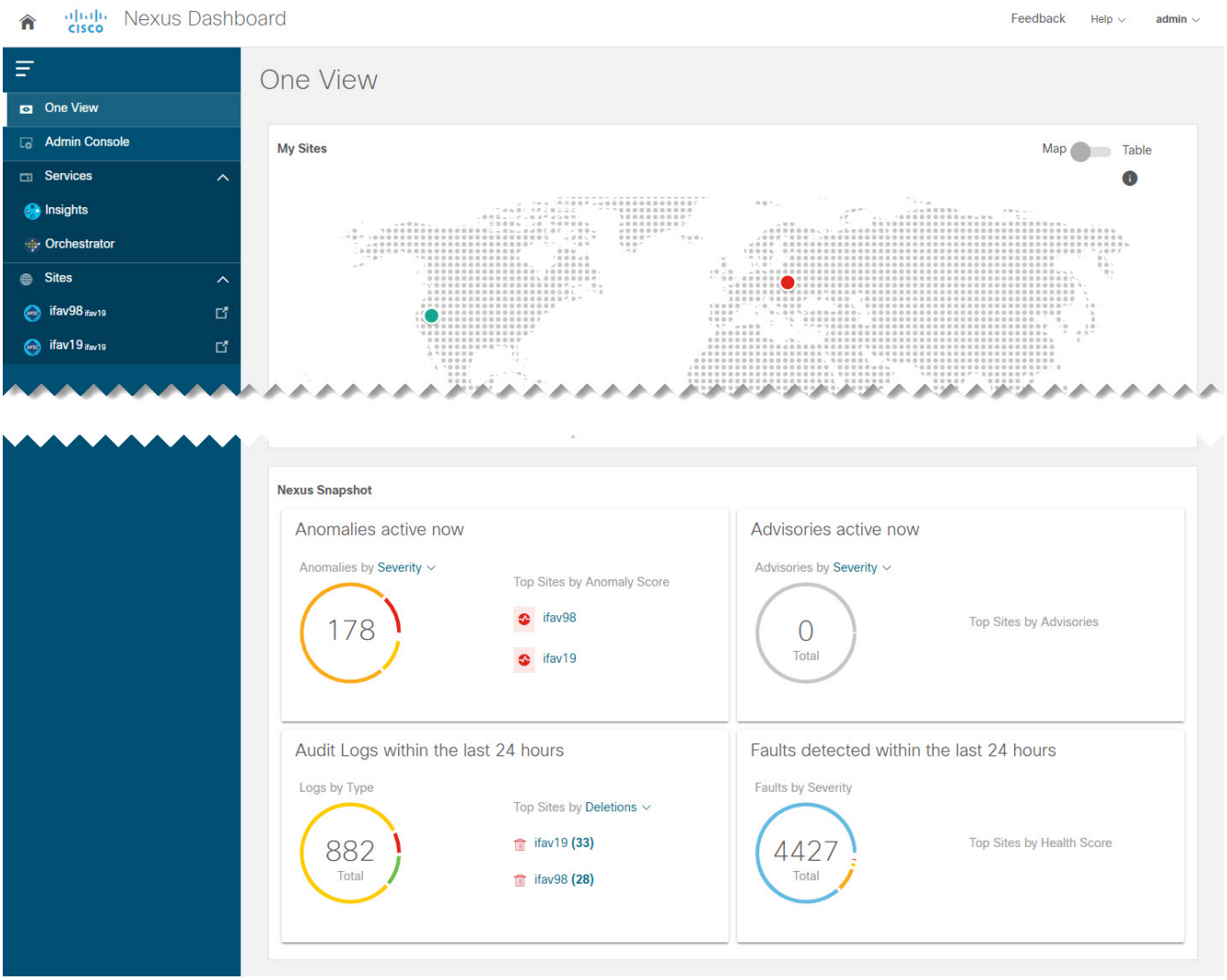


Figure 6. ワン ビュー

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 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。

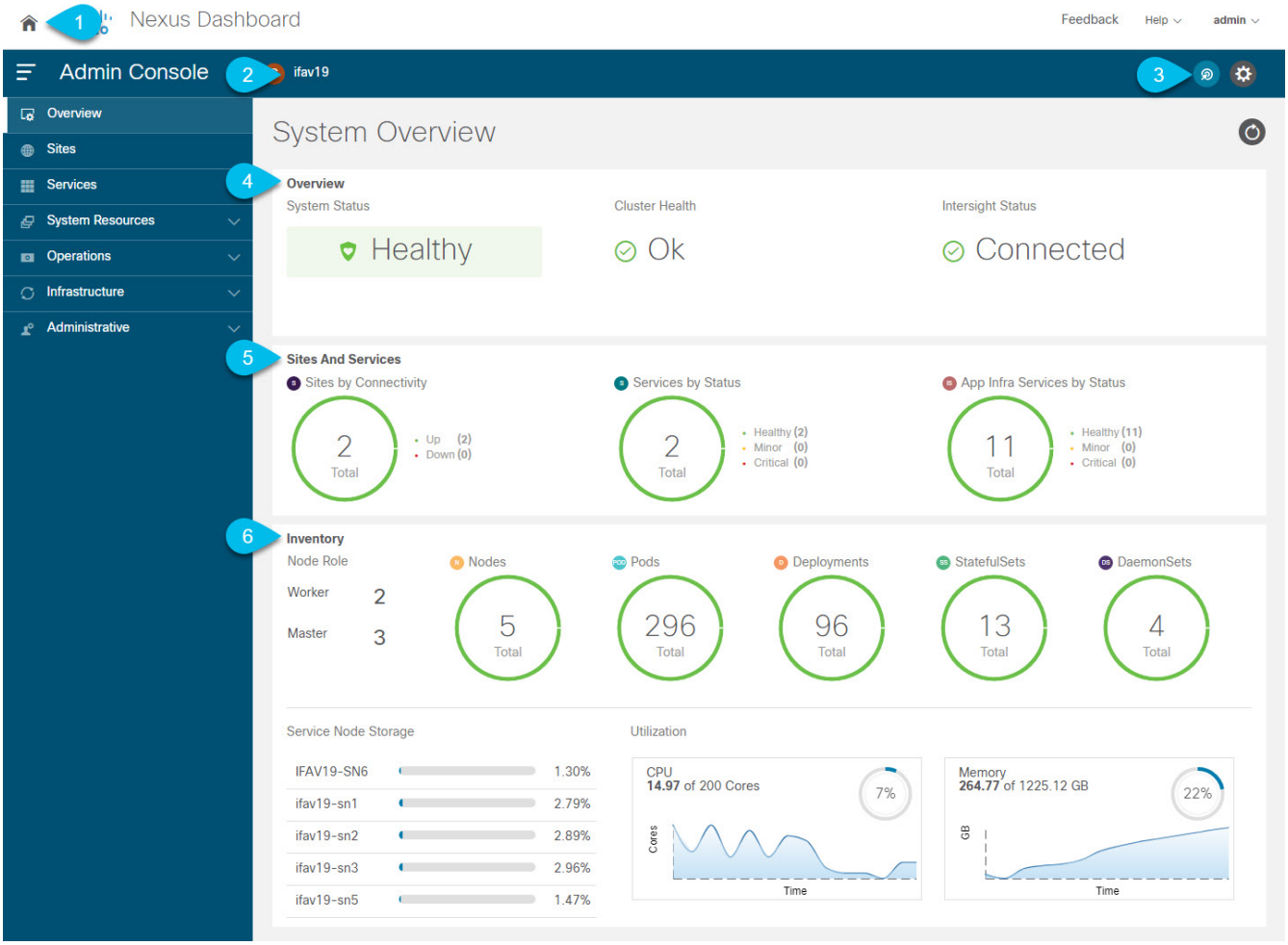


Figure 7. システム概要

。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れるので、さまざまなコンポーネント間を楽に移動できます。 * [ワンビュー（**One View**）] ページ（上で説明）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、[Multi-Cluster Connectivity] 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**）] から、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ます。

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。

。[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。

。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。

。[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。

。[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。

。[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。

注：[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 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。

導入準備サイトの詳細については、 [Site Management] を参照してください。

サービス 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、 [Services Management] を参照してください。

システム リソース 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の変更が必要な場合、新しい設定で新しいポッドが作成され、既存のポッドの設定を変更する代わりに古いポッドが破棄されます。

- [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、クラスタのスケーリングまたはリカバリ中に作成、破棄、または変更される可能性がありますが、サービスの名前は、基になる設定に関係なく、特定のサービスにアクセスする静的な方法を提供します。

- 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した場合、同じ永続識別子を使用して同じ場所に再作成されるため、以前のバージョンと同じストレージボリュームを使用できます。

操作ページ

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 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、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 — [Remote Authentication] の説明に従って、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] で説明されているとおり、ローカルの Nexus ダッシュボード ユーザーを作成および更新したり、Nexus ダッシュボード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 ダッシュボードを使用すると、複数の CiscoACI、Cisco クラウド ネットワーク コントローラ、および Cisco NDFC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帯域内または帯域外の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 Dashboardサービスによって異なり、次のセクションで詳しく説明します。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になっていないため、各サービスの独自のGUIから直接明示的に有効に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 とにログインし、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

始める前に

- 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またはクラウド ネットワーク コントローラ 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、 [Fabric Connectivity] 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 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 接続を構成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構成する必要があります。

    これは通常、初期のクラスタ展開に行なわれます。そして詳細についは、https://www.cisco.com/c/en/us/support/data-center-analytics/nexus-dashboard/products-installation-guides-list.html[*Cisco Nexus Dashboard Deployment Guide*]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。

。Nexus Dashboard の [管理コンソール（**Admin Console**）] に移動します。 。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。 。サイトを追加します。

+ image::503334.jpg[] .. 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。 .. 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。 。追加するサイトのタイプを選択します。

+ 注：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、https://www.cisco.com/c/dam/en/us/td/docs/Website/datacenter/day2ops/index.html[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で管理されるオンプレミス ACI サイト * クラウド ネットワーク コントローラ -- クラウド ネットワーク コントローラで管理されるクラウドサイト向けです。 * **NDFC** — Cisco NDFC によって管理されるオンプレミスサイト向け

。サイト情報を入力します。 .. `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/IP アドレス（**Host Name/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。

+ 注：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。 （オプション）*ピア証明書を検証 — Nexus ダッシュボードが接続する（例えばサイトコントローラ）ホストの証明書が有効であることと信頼されている 認証局（CA）にサインされていることを検証することを許可します。

  注：このオプションを使用してサイトを追加する前に Nexus ダッシュボードに証明書が既にインポートされていることが必要です。証明書を既に追加していなければ サイトを追加 ウィザードをキャンセルして最初に、[Validating Peer Certificates] に記されている手順に従います。そして、証明書をインポートした後にここに説明されている通りにサイトを追加します。
  有効な証明書をインポートせずに*ピア証明書を検証*
  オプションを有効にするとサイトの導入準備は機能不全になります。

（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、[Fabric Connectivity] 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。

+ .. クラウド ネットワーク コントローラ 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/IPアドレス* クラウド ネットワーク コントローラとの通信に使用されます。

+ 注：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。 （オプション）*ピア証明書を検証 — Nexus ダッシュボードが接続する（例えばサイトコントローラ）ホストの証明書が有効であることと信頼されている 認証局（CA）にサインされていることを検証することを許可します。

  注：このオプションを使用してサイトを追加する前に Nexus ダッシュボードに証明書が既にインポートされていることが必要です。証明書を既に追加していなけ

れば　サイトを追加　ウィザードをキャンセルして最初に、[Validating Peer Certificates] に記されている手順に従います。そして、証明書をインポートした後にここに説明されている通りにサイトを追加します。

有効な証明書をインポートせずに*ピア証明書を検証*
オプションを有効にするとサイトの導入準備は機能不全になります。

（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。

+ 注：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。管理ネットワーク経由でプロキシに到達できる場合は、プロキシIPアドレス用のスタティック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、[Cluster Configuration] を参照してください。

a. NDFC 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/IP アドレス* — Cisco NDFC との通信に使用されます。

  これは NDFC のインバンドIPアドレスである必要があります。

  注：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。（オプション）*ピア証明書を検証 — Nexus ダッシュボードが接続する（例えばサイトコントローラ）ホストの証明書が有効であることと信頼されている 認証局（CA）にサインされていることを検証することを許可します。

  注：このオプションを使用してサイトを追加する前に Nexus ダッシュボードに証明書が既にインポートされていることが必要です。証明書を既に追加していなければ　サイトを追加　ウィザードをキャンセルして最初に、[Validating Peer Certificates] に記されている手順に従います。そして、証明書をインポートした後にここに説明されている通りにサイトを追加します。

  有効な証明書をインポートせずに*ピア証明書を検証*
  オプションを有効にするとサイトの導入準備は機能不全になります。

- **Sites** — 指定したコントローラに管理されている NDFC ファブリックを選択するためにサイトを選択 をクリックします。

。[追加（**Add**）] をクリックして、サイトの追加を終了します。 。（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。 。(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。

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

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

+ オーケストレータ サービスによって管理される NDFC 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。

+ 注：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。

。[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

始める前に

```
*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。

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

始める前に

- 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、直接管理ネットワークを介して、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、[Cluster Configuration] で説明しています。

- 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、[Installing Services Manually] 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。

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

+ image::503627.jpg[title=App Store からのサービスのインストール] .. 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。 .. メインペインで、[**App Store**] タブを選択します。 .. 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。 。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。[Enabling Services] で説明されている手順に従って、有効にします。

+ 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。

始める前に

- 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。

。サービスのイメージをダウンロードします。 .. Cisco DC App Center にアクセスします。 .. [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。 .. 検索結果ページで、サービスをクリックします。 .. 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。 .. [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。

。Nexus Dashboard の GUI にログインします。 。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。 。サービスイメージをアップロードします。 .. 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。 .. 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。 .. 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。

+ 注：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`

a. [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。

。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。 。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。[Enabling Services] で説明されている手順に従って、有効にします。

+ 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 * [Installing Services Using App Store] または [Installing Services Manually] に記載されているサービスのインストールが完了している必要があります。 * [Cluster Configuration] で説明されているように、ユース
ケースに適したネットワーク拡張パラメータを構成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。

。Nexus Dashboard の [管理コンソール（**Admin Console**）] に移動します。 。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。 。該当するサービスのタイルで、開始をクリックします。

+ 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「ネットワークの拡張」として分類され、サービスを展開する前に [Cluster Configuration] 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 アプリ インフラ サービス 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

サービスを更新するプロセスは、 [Installing Services Using App Store] または [Installing Services Manually]で説明されている最初の展開と同様です。

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。

。 [Installing Services Using App Store] または [Installing Services Manually]の説明に従って、新しいバージョンを展開します。 。Nexus Dashboard GUI の [サービス（**Services**）] 画面に移動します。 。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。 。[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

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

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

始める前に

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。

。Nexus Dashboard の GUI にログインします。 。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。

。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。

操作

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。

注：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、ガイドライン、および問題の変更については、ターゲット リリースのリリースノートを必ずお読みください：https://www.cisco.com/c/en/us/support/data-center-analytics/nexus-dashboard/products-release-notes-list.html[*Release Notes*]。
- クラスタのアップグレードをする前にクラスタ内の全てのサービスを無効化する必要があります。
- アップグレード プロセスは、すべての Nexus ダッシュボード フォーム ファクタで同じです。

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

- 現在の Nexus ダッシュボード クラスタが正常であることを確認します。

  Nexus 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。

- [Creating Configuration Backups] の説明に従って、既存の構成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。

。Nexusダッシュボードイメージをダウンロードします。 .. [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 。ダウンロードするNexusダッシュボードのバージョンを選択します。 .. Cisco Nexus ダッシュボード イメージ（'nd-

dk9<version>.iso`) をダウンロードします。

+ 注：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用の `.iso` イメージをダウンロードする必要があります。

a. （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。

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

+ image::503622.jpg[] .. メイン ナビゲーション メニューから、[操作 > ファームウェア管理（**Operations** > **Firmware Management**）] を選択します。 .. 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。 .. 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。
。[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。 .. 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。 .. 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。

+
注：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 > セキュリティ（**Administrative** > **Security**）] ページで変更できます。

。[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 [Adding Images] の説明に従って、アップグレードイメージが Nexus ダッシュボード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。

。Nexus Dashboard の [管理コンソール（**Admin Console**）] に移動します。 。更新を開始します。 .. メイン ナビゲーション メニューから、[操作 > ファームウェア管理（**Operations** > **Firmware Management**）] を選択します。 .. メインペインで、[更新（**Updates**）] タブを選択します。 .. [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。

。[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。

。検証レポートを確認し、インストール をクリックしてアップグレードを続行します。

+
アップグレードがトリガーされる前に、システムはいくつかの検証チェックを実行し、レポートを表示します。

+ image::504641.jpg[]

。[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。

。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 > ファームウェア管理（**Operations > 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。

+ image::503623.jpg[]

。[**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 > ファームウェア管理（**Operations > 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。

+ image::503624.jpg[]

+ 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。

。Nexus Dashboard の [管理コンソール（**Admin Console**）] に移動します。 。メイン ナビゲーションメニューから、[操作 > ファームウェア管理（**Operations > Firmware Management**）]

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

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

+ image::503628.jpg[] .. メイン ナビゲーション メニューから、[操作 > テクニカル サポート（**Operations > Tech Support**）] を選択します。 .. 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。

。[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。

。[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。 。[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、 [Useful Commands] を参照してください。
。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。

構成のバックアップの作成

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

+ image::503630.jpg[] .. メイン ナビゲーション メニューから、[操作 > バックアップと復元（**Operations > Backups & Restore**）] を選択します。 .. 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。 .. 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。

。[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。 。[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。

+ 注：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

現在の構成に次の設定が　1
つ以上含まれている場合は、バックアップを復元する前にそれらを削除する必要があります。

- [Persistent IP Addresses] で説明されている永続的な IP。
- [Exporting Events] で説明されているストリーミング イベントの Syslog。
- [Cluster Configuration]で説明されている静的ルート。

構成のバックアップを復元する：

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

+ image::503633.jpg[] .. メイン ナビゲーション メニューから、[操作 > バックアップと復元（**Operations > Backups & Restore**）] を選択します。 .. メインペインで、[復元ジョブ（**Restore Jobs**）] タブを選択します。 .. 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。 。詳細を入力します。 .. [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。 .. [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。 。インポートをクリックして、復元手順を開始します。

イベント分析

*操作*カテゴリの*イベント分析*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*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、[Cluster Configuration]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シビラティ（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。

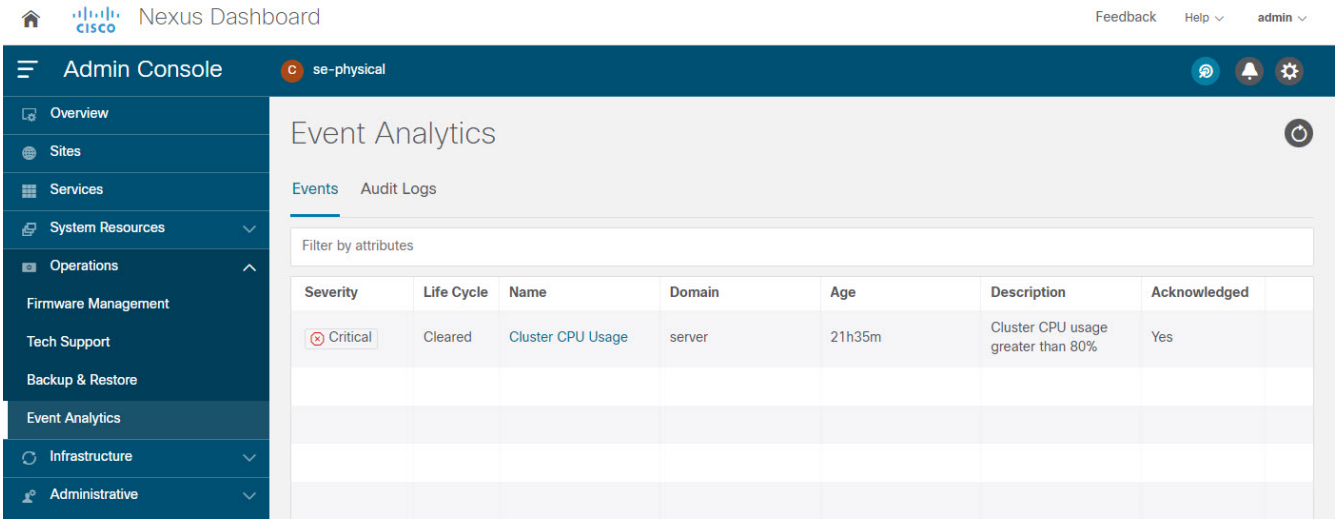


Figure 8. イベント分析

リスト内のすべての重要なイベントの概要を表示するか、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 > 監査ログ（Operations > 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。

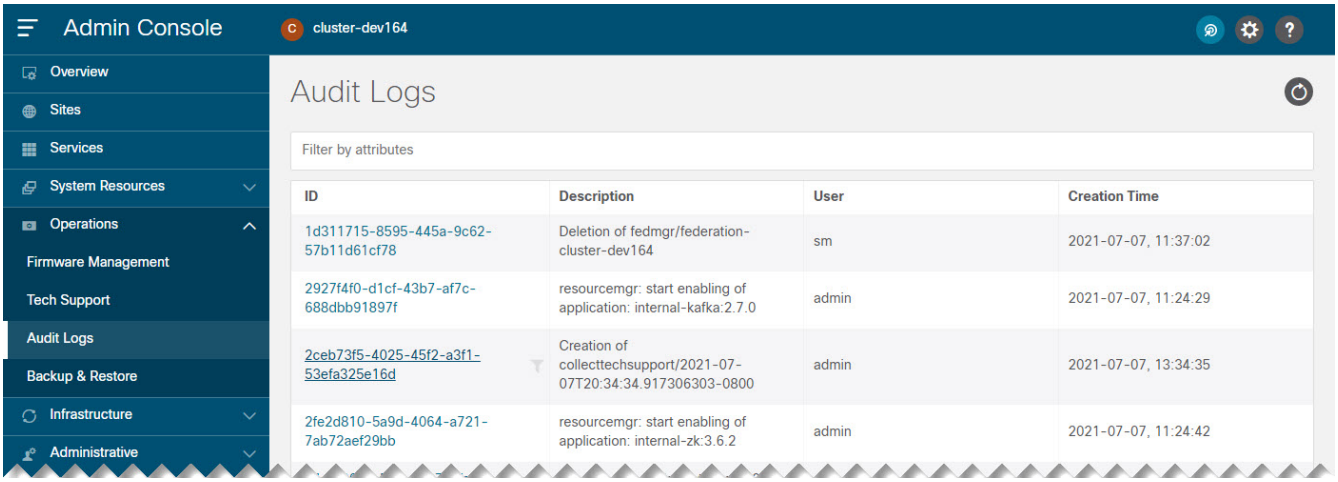


Figure 9. 監査ログ

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。

。Nexus Dashboard の [管理コンソール（**Admin Console**）] に移動します。 。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 > クラスタ設定（**Infrastructure > Cluster Configuration**）] を選択します。 。* Syslog* タイルで * 編集* 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どうかを選択します。

インフラストラクチャ管理

クラスタ設定

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。

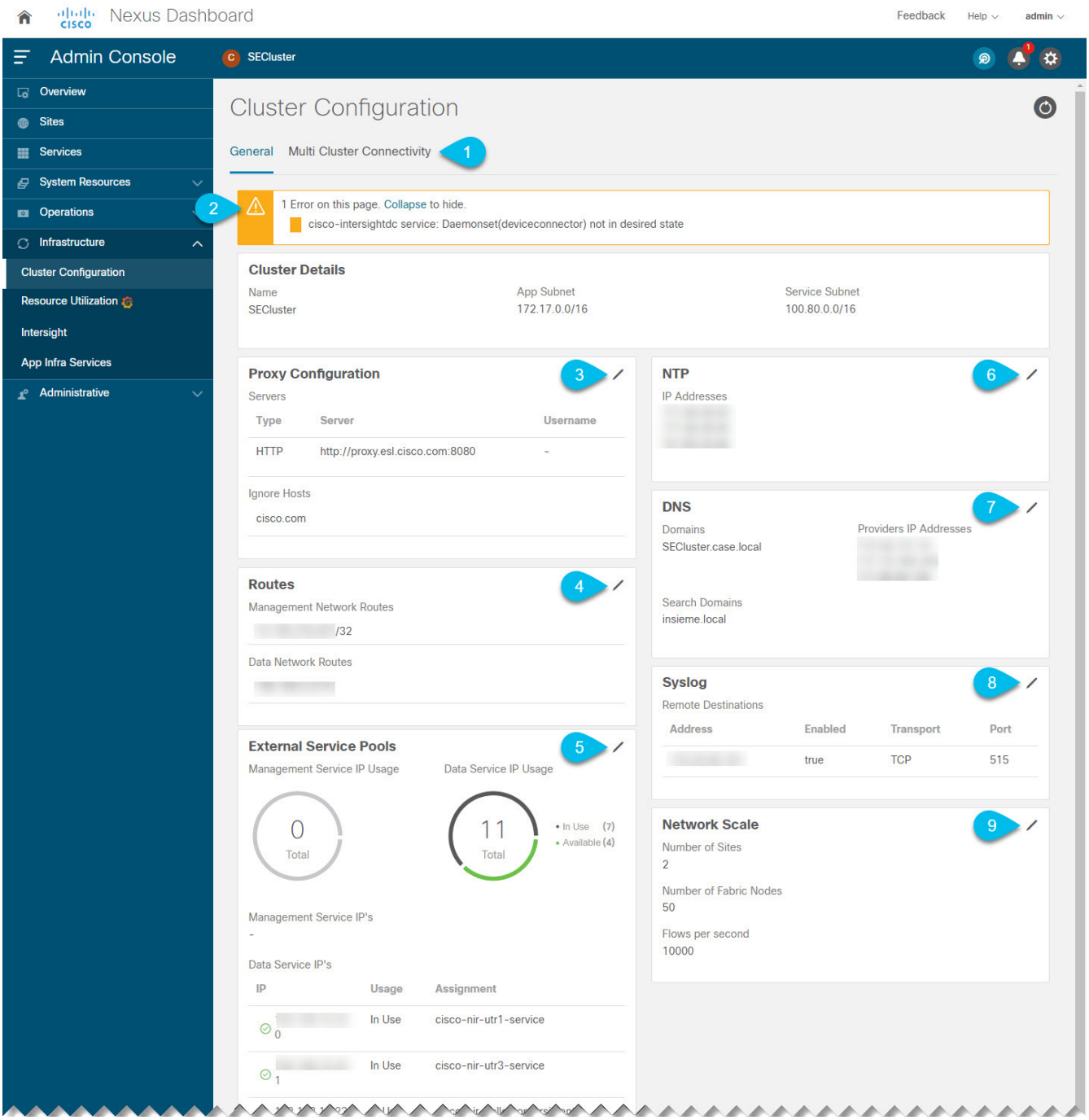


Figure 10. クラスタ設定

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。

。[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、[Multi-Cluster Connectivity] を参照してください。

。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。

。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。

+ 注：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。

+ Nexus ダッシュボードは 2 つのメイン ルート テーブルを使用することに注意してください。1
つは管理ネットワーク用、もう 1 つはデータ ネットワーク用です。デフォルトでは、発信元 IP
アドレスのルーティング テーブルが使用されます。つまり、Nexus
ダッシュボードは、プロキシを使用しようとしている POD/サービスのルーティング
テーブルからプロキシに到達しようとします。

+ たとえば、プロキシを構成し、Nexus
ダッシュボードからインターサイト接続を確立してから、クラスタで実行されているインターサイト
サービスから AppD 統合を構成しようとすると、AppD
ホストに到達できないことを示すエラーが表示される場合があります。これは、プロキシが管理インターフェースからしかアクセスできないために発生します。このような場合、以下の「管理ネットワークまたはデータ ネットワーク ルート」で説明されているように、プロキシ IP アドレスの管理ネットワークルートを追加する必要もあります。

+ 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。

。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。

。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。

+ 詳細情報と構成手順については、[Persistent IP Addresses] を参照してください。

。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。

。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。

。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、[Events Analytics] を参照してください。

。ネットワークスケール　　を構成するには、ネットワークの拡張　　タイルの　　編集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。

+
注：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 フィールドに、この Nexus ダッシュボード クラスタが管理する、展開のサイトの目標数を入力します。
b. スイッチの数 フィールドに、展開するスイッチ ノードの目標数を指定します。
c. **1**秒あたりのフロー フィールドで、Nexus ダッシュボード インサイツ 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 ダッシュボード インサイトは、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トラップと syslog 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。

注：この機能は、NDFC ファブリックを使用するNexus ダッシュボード インサイト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 ダッシュボード 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IPは、"レイヤ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。

- 一部のサービスはこの機能をサポートしていないか、追加のガイドラインが必要であるため、展開する予定のサービスのドキュメントを確認してください。

  現時点では、永続的な IP は、Nexus ダッシュボード インサイトおよび Nexus ダッシュボード ファブリック
  コントローラでサポートされています。サービス固有のドキュメントは、次のリンクで見つけることができます。

  - Nexus Dashboard Fabric Controller
  - Nexus Dashboard Insights

- 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、 [Enabling BGP On All Nodes] 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 構成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 を構成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を構成し、クラスタの構成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 を既に構成している場合、または代わりにレイヤ 2 モードで動作する場合は、[Configuring Persistent IPs] 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。

始める前に * 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。

。Nexus Dashboard の [管理コンソール（**Admin Console**）] に移動します。 。左側のナビゲーションメニューから、システム情報技術 > ノード を選択します。 。いずれかのノードの横にある アクション（**...**）メニューをクリックし、編集 を選択します。 。ノードの編集 画面で、**BGP**を有効にするをオンにします。 。**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。 。**+IPv4 BGP**ピアの追加 または **+IPv6 BGP**ピアの追加 をクリックして、ピア IP アドレス情報を提供します。 .. ピア アドレス 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。 .. ピア**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。 .. [保存（**Save**）] をクリックして、変更内容を保存します。 。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 の構成

始める前に * 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 つのモードは [Persistent IP Addresses] 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、[Enabling BGP On All Nodes] で説明されているように、BGPを有効にして構成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。

- ノード障害を検出する時間
- サービスが別のノードに再スケジュールされる時間
- サービスの外部 IP がスケジュールされたノードから GARP (IPv4) または近隣探索 (IPv6) を介してアドバタイズされる時間レイヤー 2 モード
- レイヤー 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。

。Nexus Dashboard の [管理コンソール（**Admin Console**）] に移動します。 。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 > クラスタ構成 を選択します。 。外部サービス プール タイルで、編集 アイコンをクリックします。 。表示された 外部サービスプール 画面で、* IP

アドレスの追加* 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。
- 一緒に接続できるクラスタの数やすべてのクラスタにわたるサイトの数などのサポートされるスケールの制限については、ご使用のリリースのhttps://www.cisco.com/c/en/us/support/data-center-analytics/nexus-dashboard/products-release-notes-list.html[*Nexus Dashboard Release Notes*]を参照します。
- 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。
- 一緒に接続する予定のクラスターにオンボーディングされたサイトの名前は、それらのクラスタ全体で一意である必要があります。

  異なるクラスタ間でサイト名が重複すると、ドメイン ネーム システム（DNS）解決が失敗する可能性があります。

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 2.3.1 を実行しているプライマリクラスタから、リリース 2.2.1 を実行しているNexus ダッシュボード 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。
- 接続されたクラスタ
  グループ内の任意のクラスターから、他のクラスタが同じまたは以前のバージョンの Nexus ダッシュボードを実行している場合にのみ、他のクラスターを表示できます。

つまり、「cluster1」がリリース 2.3.1 を実行し、「cluster2」がリリース 2.2.1 を実行している場合、「cluster1」から「cluster2」を表示できますが、その逆はできません。

- マルチクラスタ接続と One View は、リモートユーザー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 Dashboard 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 * [Guidelines and Limitations] 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ー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、[Remote Authentication]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。

。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番目のクラスタを追加します。

+ image::503612.jpg[title=2 番目のクラスタの追加] .. 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 > クラスタ設定（**Infrastructure** > **Cluster Configuration**）] を選択します。 .. 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。 .. [クラスタの接続（**Connect Cluster**）] をクリックします。 。クラスタ情報を入力します。

+ image::503613.jpg[title=クラスタ情報の提供] .. 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。 .. 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。

。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。

+ 複数のクラスタをグループに追加した場合、[クラスタ設定 > マルチクラスタ接続（**Configuration > 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、[Navigating Between Clusters] 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、アクションボタンが使用可能になります。

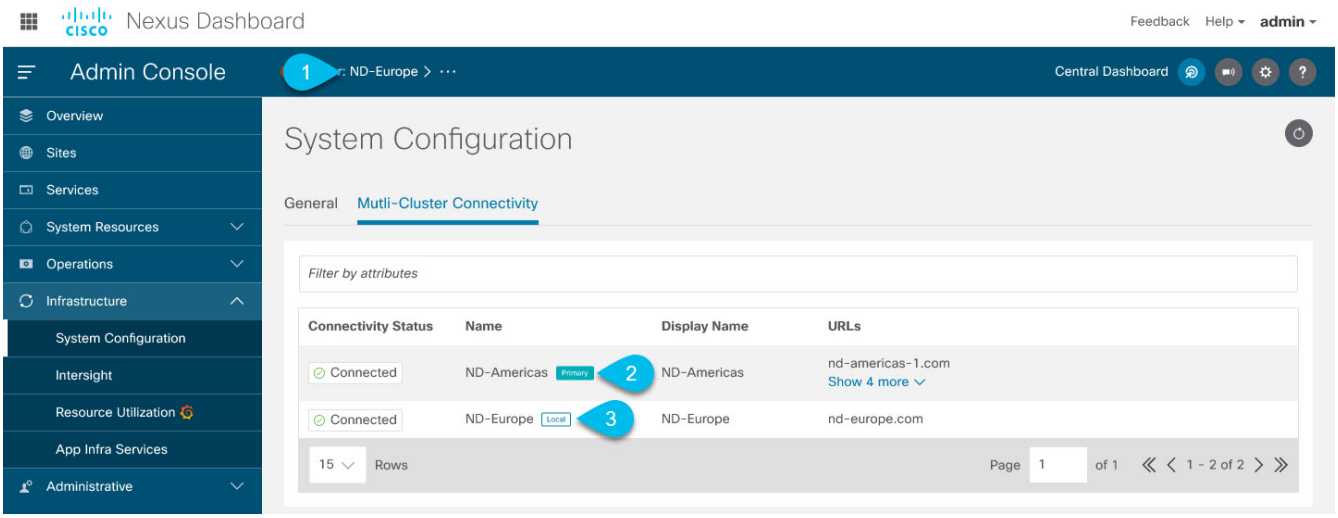


Figure 11. プライマリ クラスタと非プライマリ クラスタ

。*クラスタ：<name>*領域には、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。 。[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。 。[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

複数のクラスタに同時に接続すると、マルチクラスタ接続のUIページを使用できるようになります。このページにアクセスするには、Nexus ダッシュボード UIページの右上にある * 集中ダッシュボード*

をクリックします。他のクラスタに接続されていないクラスタにログインすると、このUIオプションは表示されません。

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。

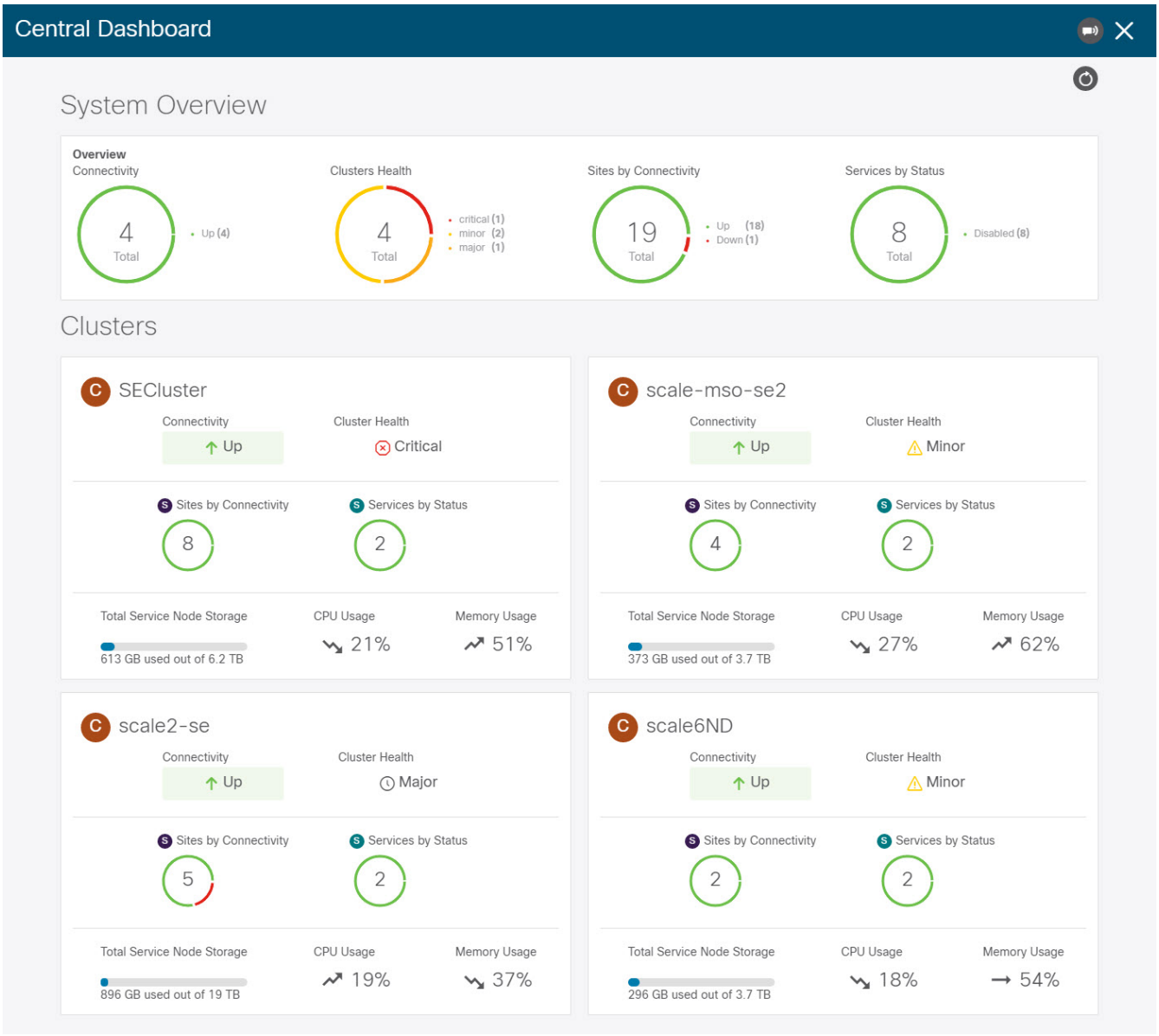


Figure 12. 中央ダッシュボード

注：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。

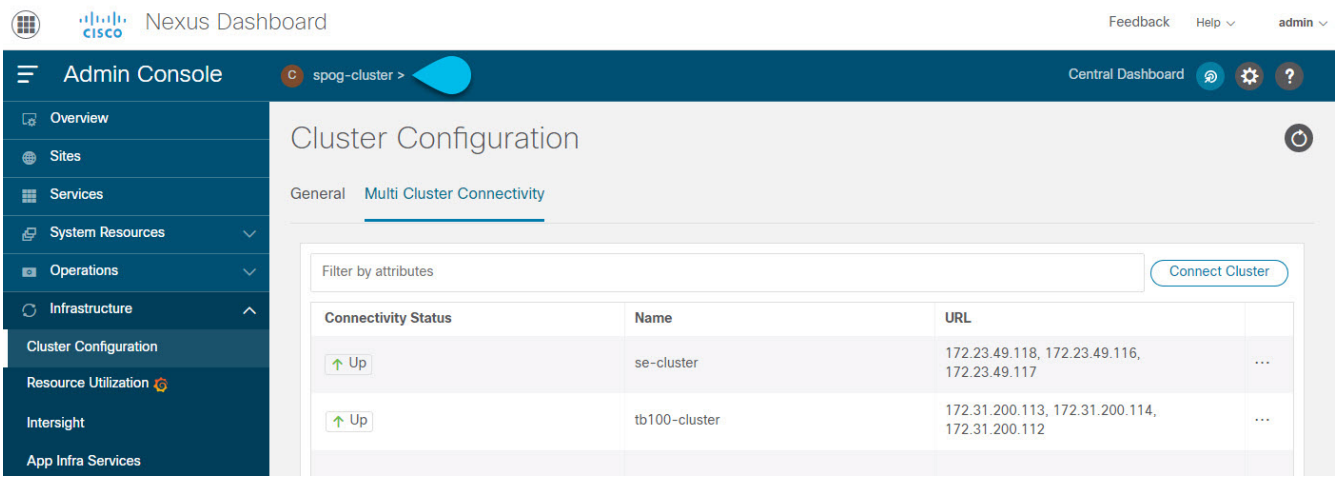


Figure 13. クラスタ間の移動

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。

。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。 。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 > クラスタ設定（**Infrastructure > Cluster Configuration**）] を選択します。 。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。 。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。 。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、https://www.cisco.com/c/en/us/td/docs/dcn/nd/2x/deployment/cisco-nexus-dashboard-deployment-guide-2x.html[*Nexus Nexus Dashboard Deployment Guide*] で説明されています。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。

注：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（例えば、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、[Managing Worker Nodes] を参照します。
- スタンバイ ノードの詳細については、[Managing Standby Nodes] を参照します。

物理ノードの前提条件とガイドライン

- [Platform Overview] 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。
- 展開したサービスの リリース ノート で説明されている追加の追加条件を全てレビューと完了をしたことを確認します。

  一部のサービスには、「ワーカー」ノードと「スタンバイ」ノードに関する追加の警告がある場合があります。サービス固有のドキュメントは、次のリンクで見つけることができます。

  - *Nexus Dashboard Fabric Controller Release Notes*
  - *Nexus Dashboard Insights Release Notes*
  - *Nexus Dashboard Orchestrator Release Notes*
- For maximum number of `worker` and `standby` nodes in a single cluster, see the *Nexus Dashboard Release Notes* for your release.
- サポートされているハードウェアを使用していること、およびサーバーがラックに取り付けられて接続されていることを確認してください。

  物理アプライアンス フォーム ファクタは、UCS-C220-M5 および UCS-C225-M6 の元の Nexus ダッシュボード プラットフォーム
  ハードウェアでのみサポートされます。次の表に、サーバの物理的アプライアンス サーバの PID と仕様を示します。

  Table 8. Supported UCS-C220-M5 Hardware

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 - 256 GB RAM - 4x 25G仮想インターフェイス カード1455 - 4x 2.4TB HDD - 400GB SSD - 1.2TB NVMe ドライブ - 1050W電源

Table 9. Supported UCS-C225-M6 Hardware

PID	ハードウェア
ND-NODE-G4	- UCS C225 M6 シャーシ 2.8GHz AMD CPU - 256 GB RAM - 4x 2.4TB HDD - 960GB SSD - 1.6TB NVME ドライブ - Intel X710T2LG 2x10 GbE（銅） - Intel E810XXVDA2 2x25/10 GbE（光ファイバ） - 1050W電源

注：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 Dashboardノードとして使用できなくなります。

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

  CIMC のサポートおよび推奨される最小バージョンは、Nexus ダッシュボード リリースの *Release Notes* の「互換性」セクションにリストされています。

- 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、[Manual Upgrades] 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、[Re-Imaging Nodes] 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、[Managing Worker Nodes] 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、[Managing Standby Nodes] 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、https://www.cisco.com/c/en/us/td/docs/dcn/nd/2x/deployment/cisco-nexus-dashboard-deployment-guide-2x.html[*Nexus Nexus Dashboard Deployment Guide*] で説明されています。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。

注：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、[Managing Worker Nodes] を参照します。
- スタンバイ ノードの詳細については、[Managing Standby Nodes] を参照します。

ESX ノードの前提条件とガイドライン

- [Platform Overview] 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。
- 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、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用に設計されたノード プロファイル
  - アプリ ノード：Nexus Dashboard Orchestrator などの非データ集約型アプリケーション用に設計されたノード プロファイル

    Table 10. サポートされているハードウェア

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 2.3.1	VMware ESXi 7.0, 7.0.1, 7.0.2, 7.0.3 vCenter を使用して展開する場合、VMware vCenter 7.0.1、7.0.2 各 VM には次のものが必要です。 • 少なくとも 2.2 GHz の物理予約された 32 個の vCPU • 物理予約された 128GB の RAM • データ ボリューム用の 3TB SSD ストレージとシステム ボリューム用の追加の 50GB `データ`ノードは、次の最小パフォーマンス要件を満たすストレージに展開する必要があります： ◦ SSD はデータストアに直接接続するか、RAID ホスト バス アダプター (HBA) を使用する場合は JBOD モードで接続する必要があります ◦ SSD は混合使用/アプリケーション向けに最適化する必要があります (読み取り最適化ではない) ◦ 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 7.0、7.0.1、7.0.2、7.0.3 vCenter を使用して展開する場合、VMware vCenter 7.0.1、7.0.2 各 VM には次のものが必要です。 • 少なくとも 2.2 GHz の物理予約された 16 個の vCPU • 物理予約された 64GB の RAM • データ ボリューム用に 500GB HDD または SSD ストレージ、システム ボリューム用に追加の 50GB 一部のサービスでは、アプリ ノードをより高速な SSD ストレージに展開する必要がありますが、他のサービスでは HDD をサポートしています。https://www.cisco.com/c/dam/en/us/td/docs/dcn/tools/nd-sizing/index.html[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 [Prerequisites and Guidelines for ESX Nodes] 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。

。Cisco Nexus Dashboard OVAイメージを取得します。 .. [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/ .. ダウンロードするNexusダッシュボードのバージョンを選択します。 .. Nexus ダッシュボード 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`）。

。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。

。新しい VM 展開を開始します。

+ image::503090.jpg["OVF テンプレートを展開します"] .. 展開する ESX ホストを右クリックします。 .. [OVFテンプレートの展開...]を選択します。

+ **OVF**テンプレートの展開 ウィザードが表示されます。

。[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。

+ image::503932.jpg["OVF テンプレートを選択します"] .. 画像を提供します。

+ 環境内の Web サーバー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。 .. 作業を継続するために 続行 をクリックします。

。名前とフォルダの選択 画面で、VM の名前と場所を入力します。

+ image::503933.jpg["名前とフォルダを選択します"] 仮想マシンの名前を入力します。 .. 仮想マシンのストレージ場所を選択します。 .. 作業を継続するために 続行 をクリックします

。コンピューティング技術情報の選択 画面で、ESX ホストを選択します。

+ image::503934.jpg["コンピューティング リソースを選択します"] 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。 .. 作業を継続するために 続行 をクリックします

。[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。

。構成 画面で、展開するノード プロファイルを選択します。

+ image::503935.jpg["構成"] .. ユース ケースの要件に基づいて、アプリ または データ ノード プロファイルを選択します。 .. ノード プロファイルの詳細については、[Prerequisites and Guidelines for ESX Nodes] を参照してください。 .. 作業を継続するために 続行 をクリックします

。ストレージの選択 画面で、ストレージ情報を入力します。

+ image::503936.jpg[ストレージを選択します"] .. 仮想ディスク フォーマットの選択 ドロップダウン リストから シック プロビジョニング Lazy Zeroed を選択します。 .. 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。 .. 作業を継続するために 続行 をクリックします

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

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

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

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

。[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。

+ image::503937.jpg["テンプレートをカスタマイズします"] „ ノードのデータディスク容量を指定します。

+ 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。 .. *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。 .. 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。 .. 管理ネットワーク の IP ゲートウェイを入力します。 .. 作業を継続するために 続行 をクリックします。

。[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。

。VMの展開が完了したら、VMの電源をオンにします。

。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、[Managing Worker Nodes] 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、[Managing Standby Nodes] 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 [Prerequisites and Guidelines for ESX Nodes] 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。

。Cisco Nexus Dashboard OVAイメージを取得します。 .. [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/ .. ダウンロードするNexusダッシュボードのバージョンを選択します。 .. Nexus ダッシュボード 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`）。

。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。

。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。 。[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。 。[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。 。[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。 。[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。 。[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。 。[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。 。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]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。
。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。

d. 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...
```

e. admin のパスワードを入力して確認します。

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:
```

f. 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
```

g. 入力した譲歩をレビューし、確認します。

入力した情報を変更するかどうかを尋ねられます。すべてのフィールドが正しい場合は、n を選択して続行します。

入力した情報を変更する場合は、y を入力して基本設定スクリプトを再起動します。

```
Please review the config
Management network:
ゲートウェイ：192.168.9.1
IP アドレス/マスク：192.168.9.172/24
構成を再入力しますか？(y/N): n
```

。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、[Managing Worker Nodes] 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、[Managing Standby Nodes] を参照してください。

Linux KVMでの追加の仮想ノードの展開

クラスタの初期導入については、https://www.cisco.com/c/en/us/support/data-center-analytics/nexus-dashboard/products-installation-guides-list.html[*Nexus* *Nexus* ダッシュボード導入ガイド] で説明されています 。ここからのセクションでは、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。

注：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。

追加のノードを展開したら、[Managing Standby Nodes] で説明されているように、スタンバイ ノードとしてクラスタに追加できます。

KVMノードの前提条件とガイドライン

- [Platform Overview] 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。
- VMに十分なリソースがあることを確認します。

  Table 11. 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 2.2.x	• サポートされている Linux 流通： ◦ Nexus ダッシュボードオーケストレータの場合、CentOS Linux に展開する必要があります ◦ Nexus ダッシュボード ファブリックコントローラの場合、CentOS または Red Hat 企業 Linux に展開する必要があります。 • カーネルと KVM のサポートされているバージョン： ◦ Kernel `3.10.0-957.el7.x86_64` または、それ以降 ◦ KVM `libvirt-4.5.0-23.el7_7.1.x86_64` または、それ以降 • 16 vCPU • 64 GB の RAM • 500 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` また、`fsync/fdatasync/sync_file_range` セクションの `99.00th=[<value>]` が 20 ミリ秒未満であることを確認します。 • 各Nexus ダッシュボードノードは、異なるKVMサーバ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 [Prerequisites and Guidelines for KVM Nodes] 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。

。Cisco Nexus Dashboardイメージをダウンロードします。 .. ソフトウェア ダウンロードページを参照します。

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

左側のサイドバーから、ダウンロードする Nexus ダッシュボードのバージョンを選択します。 .. Linux KVM (nd-dk9 の Cisco Nexus ダッシュボード イメージをダウンロードします.<version>.qcow2).

。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。

+
たとえば、クラスタを最初に展開するときに、イメージを既にコピーしている場合は、同じ基本イメージを使用して、この手順をスキップできます。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。

+ scp を使用してイメージをコピーできます。次に例を示します。

+

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

。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 ルート ユーザとしてログインします。

b. ノードのスナップショット用のディレクトリを作成します。

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

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

c. スナップショットを作成します。

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

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

   次の手順では、nd-node4 を追加することを前提としています。

d. ノードの追加ディスクイメージを作成します。

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

   ```
   # quemu-img create -f qcow2 /home/nd-node1/nd-node4-disk2.qcow2 500G
   ```

   次の手順に進む前に、次の準備が必要です。

- /home/nd-node4/nd-node4-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-node4/nd-node4-disk2.qcow2 は、作成した新しい 500GB のディスクです。

。最初のノードの VM を作成します。

+ CLI または KVM GUI を使用して、次の構成で VM を作成できます：

+ * 16 vCPU * 64GB の RAM * オペレーティング システムの種類を linux2020 に設定 virtio に設定されたネットワーク デバイス モデル * バス 0x00 とスロット 0x03 にマップされた管理インターフェイスと、バス 0x00 とスロット 0x04 にマップされたデータ インターフェイス

+ 注：Nexus ダッシュボードは、管理インターフェイスがバス 0x00 とスロット 0x03 に接続され、データ インターフェイスがバス 0x00 とスロット`0x04` に接続されることを想定しています。そうでない場合、クラスタはネットワークに接続できません。

+ たとえば、CLI を使用して VM を作成するには：

```
# virt-install --name <node-name> \
--vcpus 16 --ram 64000 --osinfo linux2020 \
--disk path=/home/nd-node4/nd-node4-disk1.qcow2 \
--disk path=/home/nd-node4/nd-node4-disk2.qcow2 \
--network bridge:br-
oob,model=virtio,address.type=pci,address.domain=0,address.bus=0,address.slot=3 \
--network bridge:br-
vnd,model=virtio,address.type=pci,address.domain=0,address.bus=0,address.slot=4 \
--noautoconsole --import
```

。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。 ..
いずれかのキーを押して、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...
```

a. admin パスワードを入力し、確認します。

このパスワードは、rescue-user SSH ログインおよび初期 GUI パスワードに使用されます。

```
Admin Password:
Reenter Admin Password:
```

b. 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
```

c. ノードが「クラスタ リーダー」かどうかを尋ねられたら、「いいえ」を選択します。

「ワーカー」または「スタンバイ」ノードを追加しているため、クラスタ
リーダーとして指定しないでください。

```
Is cluster leader?: n
```

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`
を入力して続行します。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
Cluster leader: no
```

。初期ブートストラップ処理が完了するまで待ちます。

+ 管理ネットワーク情報を提供して確認したら、最初の ブートストラップ
プロセスが完了するまで待ちます。

+

```
システムが起動するまでお待ちください：[##########################] 100%
システムが稼働しています。UI がオンラインになるまでお待ちください。

システム UI オンライン。続行するには https://192.168.9.172 にログインしてください。
```

。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、[Managing Worker Nodes] 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、[Managing Standby Nodes] 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 [Platform Overview] セクションを参照してください。

注：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。

始める前に

- 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。 [Deploying Additional Physical Nodes]、[Deploying Additional Virtual Nodes in VMware ESX]、[Deploying ESX Node Directly in ESXi] または [Deploying Additional Virtual Nodes in Linux KVM] 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。

。Cisco Nexus DashboardのGUIにログインします。

。メイン ナビゲーション メニューから、[システムリソース > ノード（System Resources > Nodes）] を選択します。 。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。 。[ノードの追加（**Add Node**）] 画面で、ノードの情報を入力します。 .. ノードの [名前（**Name**）] を入力します。 .. [タイプ（**Type**）] ドロップダウンから [ワーカー（**Worker**）] を選択します。 .. 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を使用して、ノードの残りの情報が設定されます。

+ 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。 .. [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。 .. [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。 .. （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。 。[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。

。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

始める前に

*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。

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。

。Cisco Nexus DashboardのGUIにログインします。 。メイン ナビゲーション メニューから、[システムリソース > ノード（System Resources > Nodes）] を選択します。 。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。 。[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。

注：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。

始める前に

- 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。 [Deploying Additional Physical Nodes]、[Deploying Additional Virtual Nodes in VMware ESX]、[Deploying ESX Node Directly in ESXi] または [Deploying Additional Virtual Nodes in Linux KVM] 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（物理または仮想）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。

。Cisco Nexus DashboardのGUIにログインします。

。メイン ナビゲーション メニューから、[システムリソース > ノード（System Resources > Nodes）] を選択します。 。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。 。[ノードの追加（**Add Node**）] 画面で、ノードの情報を入力します。 .. ノードの [名前（**Name**）] を入力します。 .. [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。 .. 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を使用して、ノードの残りの情報が設定されます。

+ 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。 .. [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。 .. [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。 .. （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。 。[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 [Troubleshooting] 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。

始める前に

- 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、[Replacing Two Master Nodes with Standby Nodes] 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構成については、 [Adding Standby Nodes] 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。

  注：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。

。Cisco Nexus DashboardのGUIにログインします。 。メイン ナビゲーション メニューから、[システムリソース > ノード（System Resources > Nodes）] を選択します。 。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。 。[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。 。[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。 。[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、[Troubleshooting] 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、 [Replacing Single Master Node with Standby Node] 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、クラスタがオフラインになります。この場合、UIを含むほとんどの操作が無効になり、クラスタに構成に変更を加えることができません。「rescue-user」として残りのマスター ノードに引き続き SSH で接続できます。これは、機能不全になったマスター ノードの 1 つをスタンバイ ノードに手動でフェイル オーバーすることにより、クラスタを回復するために使用されます。2 つの「マスター」ノードが再び使用可能になると、クラスタは通常の操作を再開できます。その時点で、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。

始める前に

- 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構成については、 [Adding Standby Nodes] 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。

  注：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。

。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。 。
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>

+ 注：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>

。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。

。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 [Replacing Single Master Node with Standby Node] 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

始める前に

*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。

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。

。Cisco Nexus DashboardのGUIにログインします。 。メイン ナビゲーション メニューから、[システムリソース > ノード（System Resources > Nodes）] を選択します。 。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。 。[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 [Remote Authentication] で、ローカルユーザーの構成については [Users] で説明します。

ロールと権限

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。

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、 [Remote Authentication] セクションを参照してください。

Nexus ダッシュボード、インサイト、およびオーケストレーター ロール

ユーザー ロール	**ND** プラットフォーム	オーケストレータ サービス	インサイト 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。	N/A
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。	アクセスなし。	読み取り専用アクセス権。
展開者	`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。	N/A
ポリシー マネージャ	「ダッシュボード」ロールと同じ。	アクセスなし。	アクセスなし。

ユーザー ロール	ND プラットフォーム	オーケストレータ サービス	インサイト サービス
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。管理された と `管理されていない` の間でサイトステータス、ファブリック リソーステンプレート、ファブリック ポリシー テンプレート、およびモニタリングテンプレート（アクセスSPAN）を変更できるようにします。	アクセスなし。	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、テナントポリシー、スキーマ、およびモニタリングテンプレート（テナントSPAN）の構成を許可します。	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`ロールと同じです。	インフラ、テナント、テナントポリシー、スキーマ、およびモニタリングテンプレート（テナントSPAN）の構成を許可します。	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

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、ナビゲーション メニューで利用できない他のカテゴリのみの`ユーザー管理者` と サイト管理者 権限の持つユーザーに GUI 画面が表示されます。

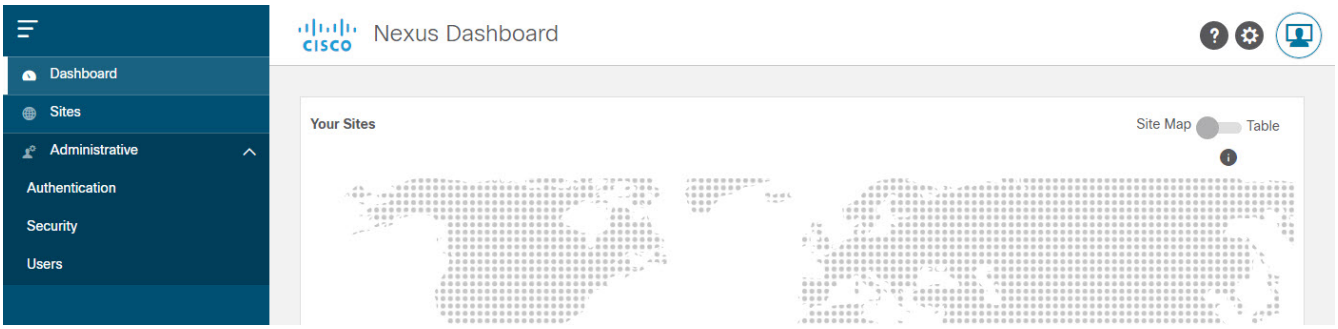


Figure 14. ロールベースの *GUI* アクセス

Nexus Dashboard Data Broker ロール

Nexus Dashboard Data Brokerサービスの場合、xref:_nd_core_rolesにリストされているNexus Dashboardロール (Nexus Dashboard、Insights、およびOrchestratorロール) のいずれかを使用できます。これらはすべて実質的に同じです。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

ユーザー ロール	**Nexus Dashboard Fabric** ファブリック コントローラ ロール
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、および展開を行います。 • 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。 • ピア リンク ポート チャネルを編集できません。 • 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。

ユーザー ロール	**Nexus Dashboard Fabric** ファブリック コントローラ ロール
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 • アプリケーション `ネットワーク オペレータ`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 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。

ユーザー ロール	**Nexus Dashboard Fabric** ファブリック コントローラ ロール
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 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。 • メンテナンス モードの切り替えはできません。 • 展開フリーズ モードでファブリックを移動したり、展開モードから解放したりすることはできません。 • 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。 注：`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。

デフォルトの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。

注：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、 [Remote Authentication] を参照してください。

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

+ image::503618.jpg[] .. メイン ナビゲーション メニューから、[管理 > 認証（**Administrative > Authentication**）] の順に選択します。 .. [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。 。[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 ダッシュボードの*サイト*ページからAPICサイトにクロス起動する場合、Nexus ダッシュボード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 ダッシュボード 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、[Roles and Permissions] で説明されているように、Nexus ダッシュボード GUIで直接構成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。

Table 12. Nexus Dashboard AVペア

ユーザー ロール	**AV** ペア値
管理者	`admin`
承認者	`approver`
ダッシュボード ユーザー	`app-user`
展開者	`deployer`
ポリシー マネージャ	`config-manager`

ユーザー ロール	AV ペア値
サイト管理者	site-admin
サイト マネージャ	site-policy
テナントマネージャ	tenant-policy
ユーザー マネージャ	aaa

Table 13. Nexus Dashboard Fabric Controller AVペア

ユーザー 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	network-admin
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>
```

注：このリリースでは、all 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
```

読み取り専用の権限のみ、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もスラッシュ（/）文字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。

- Read-only: shell:domains=all//site-admin
- Read-write: 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 * [Configuring Remote Authentication Server] 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。

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

+ image::503619.jpg[] .. メイン ナビゲーション メニューから、[管理 > 認証（**Administrative > Authentication**）] の順に選択します。 .. 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。 。[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。 .. [名前（**Name**）] にドメインの名前を入力します。 .. （任意）[説明（**Description**）] にドメインの説明を入力します。 .. [レルム（**Realm**）] ドロップダウンから `Ldap` を選択します。 .. 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。
。リモート認証サーバーの詳細を入力します。 .. 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。 .. （任意）サーバーの説明を [説明（**Description**）] に入力します。 .. 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。 .. 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。 .. 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。 .. 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。 .. [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、次の手順で説明します。 **..** （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。 .. （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。 .. [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。 .. [保存（**Save**）] をクリックしてプロバイダー設定を完了します。 .. 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。

。（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。

+ .. [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。 .. [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。 .. グループの [グループDN（**Group DN**）] を指定します。 .. LDAP グループの [ロール（**Roles**）] を 1 つ以上選択します。 .. [保存（**Save**）] をクリックしてグループ設定を保存します。 .. 追加の LDAPグループがあれば、この手順を繰り返します。 。[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 * [Configuring Remote Authentication Server] 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構成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。

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

+ image::503619.jpg[] .. メイン ナビゲーション メニューから、[管理 > 認証（**Administrative > Authentication**）] の順に選択します。 .. 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。 。[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。 .. [名前（**Name**）] にドメインの名前を入力します。 .. （任意）[説明（**Description**）] にドメインの説明を入力します。 .. [レルム（**Realm**）] ドロップダウンから `Radius` または `Tacacs` を選択します。 .. 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。 。リモート認証サーバーの詳細を入力します。 .. 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。 .. （任意）サーバーの説明を [説明（**Description**）] に入力します。 .. 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。 .. 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。 .. 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。 .. （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。 .. [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。 .. [保存（**Save**）] をクリックしてプロバイダー設定を完了します。 .. 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。 。[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。

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

+ image::503652.jpg[] .. メイン ナビゲーション メニューから、[管理 > 認証（**Administrative > Authentication**）] の順に選択します。 .. 特定のドメインをクリックします。 .. 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。 。[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。 。[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。

。Nexus Dashboard の [管理コンソール（**Admin Console**）] に移動します。 。メイン ナビゲーション メニューから、[管理 > 認証（**Administrative > Authentication**）] の順に選択します。 。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。

+ image::503617.jpg[]

+ 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

。Nexus Dashboard の [管理コンソール（**Admin Console**）] に移動します。 。メイン ナビゲーション メニューから、[管理 > 認証（**Administrative** > **Authentication**）] の順に選択します。 。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。

+ image::503617.jpg[]

。[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、ユーザーログインに多要素認証(MFA)を使用するようにNexus Dashboardを設定できます。

多要素認証を設定する場合、次を実行します。

- [Configuring Okta Account as MFA Provider] 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。

- [Configuring MFA Client] 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。

- [Adding Okta as Remote Authentication Provider] 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。

。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。

。新しいアプリ統合を作成します。 .. 左側のナビゲーションメニューから、[アプリケーション > アプリケーション（**Application > Application**）] を選択します。 .. [アプリケーション統合の作成（**Create App Integration**）] をクリックします。 .. [サインイン方法（**Sign-in method**）] は、[OIDC - OpenID接続（`OIDC - OpenID Connect`）] を選択します。 .. [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。 .. **[Next]** をクリックします。 .. [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。 .. サインインリダイレクト**URI** 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。 .. [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。 .. 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。

。必要な属性をデフォルトユーザーに追加します。 .. 左側のナビゲーションメニューから、[ディレクトリ > プロファイルエディタ（**Directory > Profile Editor**）] を選択します。 .. [Okta ユーザー（**Okta**

User（デフォルト））] のプロファイルをクリックします。 .. [+属性の追加（**+Add Attribute**）] をクリックします。 .. [データ型（**Data type**）] では、文字列（`string`）を選択します。 .. [表示名（**Display name**）]、[変数名（**Variable name**）]、および [説明（**Description**）] に、`CiscoAVPair` と入力します。 .. [属性が必要（**Attribute required**）] がオフ（`unchecked`）になっていることを確認します。 .. 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。 .. [データ型（**Data type**）] では、文字列（`string`）を選択します。 .. [表示名（**Display name**）]、[変数名（**Variable name**）]、および [説明（**Description**）] に、`nduser` と入力します。 .. [属性が必要（**Attribute required**）] がオフ（`unchecked`）になっていることを確認します。 .. 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。

。作成した `nd-mfa` ユーザーに必要な属性を追加します。 .. 左側のナビゲーションメニューから、[ディレクトリ > プロファイルエディタ（**Directory > Profile Editor**）] を選択します。 .. nd-mfa ユーザー（**nd-mfa User**（デフォルト）） のプロファイルをクリックします。 .. [+属性の追加（**+Add Attribute**）] をクリックします。 .. [データ型（**Data type**）] では、文字列（`string`）を選択します。 .. [表示名（**Display name**）]、[変数名（**Variable name**）]、および [説明（**Description**）] に、`CiscoAVPair` と入力します。 .. [属性が必要（**Attribute required**）] にチェックが入っている（`checked`）ことを確認します。 .. 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。 .. [データ型（**Data type**）] では、文字列（`string`）を選択します。 .. [表示名（**Display name**）]、[変数名（**Variable name**）]、および [説明（**Description**）] に、`nduser` と入力します。 .. [属性が必要（**Attribute required**）] にチェックが入っている（`checked`）ことを確認します。 .. 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。 。属性をマッピングします。 .. 左側のナビゲーションメニューから、[ディレクトリ > プロファイルエディタ（**Directory > Profile Editor**）] を選択します。 .. nd-mfa ユーザー（**nd-mfa User**）のプロファイルをクリックします。 .. 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。

+ image::503662.jpg[] [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。 .. [`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。 .. [`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。 .. [マッピングの保存（**Save Mappings**）] をクリックします。 .. [今すぐ更新を適用（**Apply Update now**）]をクリックします。

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

。ユーザーをアプリに割り当てます。 .. 左側のナビゲーションメニューから、[アプリケーション > アプリケーション（**Application > Application**）] を選択します。 .. 作成したアプリケーション（`nd-mfa`）をクリックします。 .. [課題（**Assignments**）] タブを選択します。 .. [割り当て > ユーザーに割り当て（**Assign > 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。 ..

[ユーザーへのnd-mfaの割り当て（**Assign nd-mfa to People**）] 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。 .. 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、[Configuring Remote Authentication Server] 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。 .. [保存して戻る（**Save and Go Back**）] をクリックします。 .. 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。

。アプリの [要求（**Claims**）] を設定します。 .. 左のナビゲーションメニューから [セキュリティ > API（**Security > API**）] を選択します。 .. デフォルト*の名前をクリックします。 .. **[要求（*Claims**）] タブを選択します。 .. [+要求の追加（**+Add Claim**）] をクリックして、`CiscoAVPair` 要求を追加します。 .. [名前（**Name**）] フィールドに、`CiscoAVPair` と入力します。 .. [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0ン（`Access Token`）] もサポートされています。 .. [値（**Value**）] フィールドに、`appuser.CiscoAVPair` と入力します。 .. **[Save]** をクリックします。 .. [+要求の追加（**+Add Claim**）] をクリックして、`nduser` の要求を追加します。 .. [名前（**Name**）] フィールドに、`nduser` と入力します。 .. [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。 .. [値（`Value`）] フィールドに、`appuser.nduser` と入力します。 .. **[Save]** をクリックします。

。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。 .. 左のナビゲーションメニューから [セキュリティ > API（**Security > API**）] を選択します。 .. デフォルト*の名前をクリックします。 .. **[発行者（*Issuer**）] の値を書き留めます。

+ image::503663.jpg[] 左側のナビゲーションメニューから、[アプリケーション > アプリケーション（**Application > Application**）] を選択します。 .. 作成したアプリケーション（`nd-mfa`）をクリックします。 .. [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。

+ image::503664.jpg[]

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。

。Oktaアカウントにログインします。 。DUOをMFAタイプとして追加します。 .. 左のナビゲーションメニューから [セキュリティ> 多要素（**Security** > **Multifactor**）] を選択します。 .. [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。 .. [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（**Duo Username Format**）] が [電子メール（`Email`）] に設定されていることを確認します。 .. **[Save]** をクリックします。

。Duo ルールを作成します。 .. 左側のナビゲーションメニューから、[アプリケーション > アプリケーション（**Application** > **Application**）] を選択します。 .. 作成したアプリケーション（`nd-mfa`）をクリックします。 .. [サインオン（**Sign On**）] タブを選択します。 .. [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。 .. ルールの名前を入力します。 .. [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。 .. 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。 .. **[Save]** をクリックします。

。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。

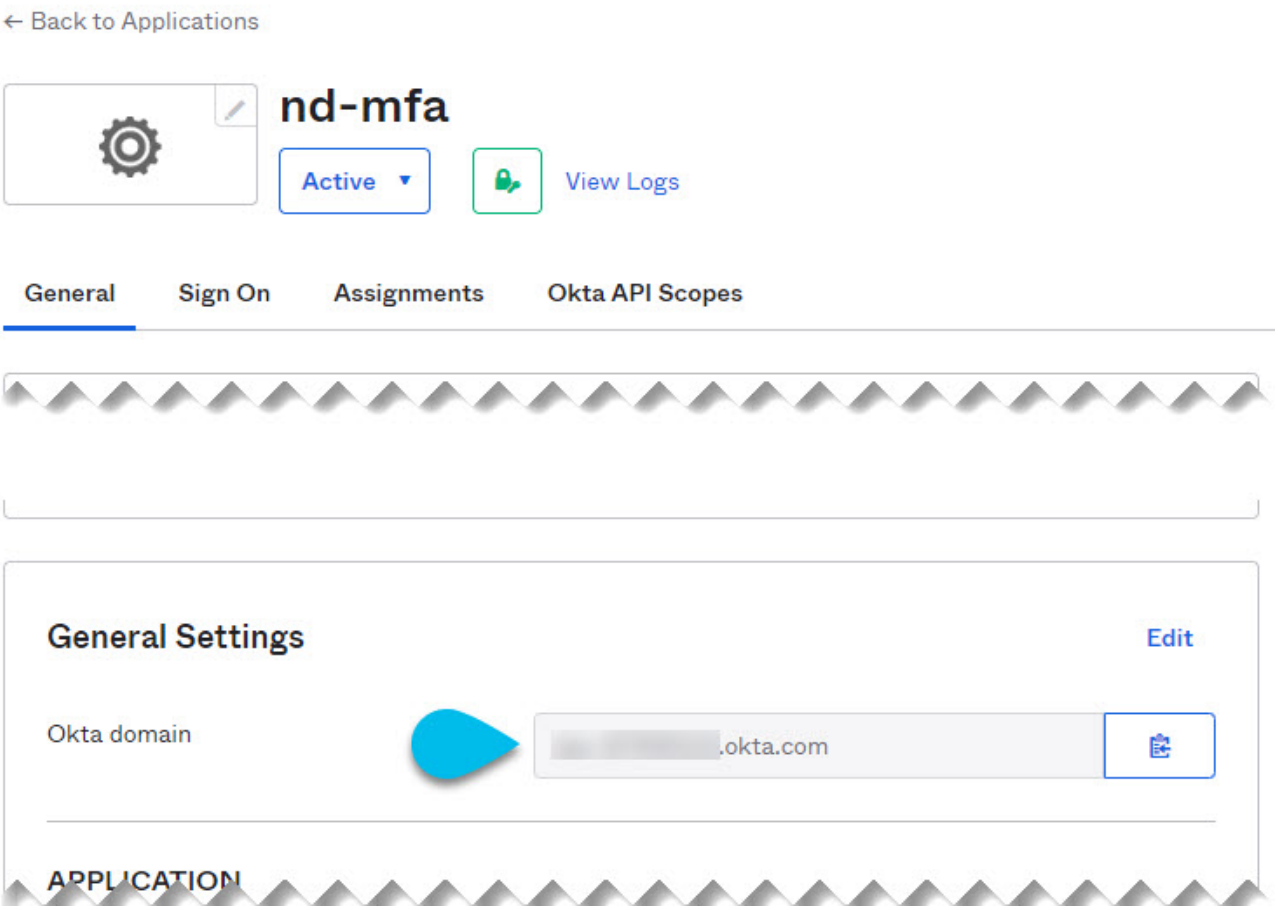
+ Duoダッシュボードでユーザーを設定するには、次を実行します。

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 Use*r）] 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。

e. [Configuring Okta Account as MFA Provider] 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 > アプリケーション（**Application** > **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（**Okta domain**）] の URL をコピーします。



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。

f. [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 * [Configuring Okta Account as MFA Provider] 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、[Configuring Okta Account as MFA Provider] 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、[Cluster Configuration] 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。

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

。認証ドメインを追加します。

+ image::503619.jpg[] メイン ナビゲーション メニューから、[管理 > 認証（**Administrative > Authentication**）] の順に選択します。 .. 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。

。[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。 .. [名前（**Name**）] にドメインの名前を入力します。 .. （任意）[説明（**Description**）] にドメインの説明を入力します。 .. [レルム（**Realm**）] ドロップダウンから、[OIDC] を選択します。 .. [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。 .. [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。 .. [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。 .. （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。 .. [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。 。[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

。通常どおり、Nexus DashboardのIPの1つに移動します。 。*ログイン ドメイン* ドロップダウンから、[Adding Okta as Remote Authentication Provider] 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。 。**[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。 。[Configuring Okta Account as MFA Provider] 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。 。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 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 タブには、 [Remote Authentication] 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構成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構成の詳細については、[Remote Authentication] を参照してください。

ローカル ユーザーの追加

。Nexus Dashboard の [管理コンソール（**Admin Console**）] に移動します。 。新しいローカルユーザを作成します。 .. メイン ナビゲーション メニューから、[管理 > ユーザー（**Administrative > Users**）] を選択します。 .. 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。 。[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。 .. ログインに使用する*ユーザー ID* を入力します。 .. 最初の*パスワード*を入力して確認します。 .. ユーザーの*名*、姓、 *電子メールアドレス*を入力します。 .. 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、 [Roles and Permissions] 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。 **.. [**作成（***Create**）] をクリックしてユーザーを保存します。

ローカル ユーザーの編集

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

+ image::503350.jpg[] .. メイン ナビゲーション メニューから、[管理 > ユーザー（**Administrative > Users**）] を選択します。 .. メインペインで、ユーザーの名前をクリックします。 .. 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。 。 <***user-name***> 画面で、編集アイコンをクリックします。 。[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 > セキュリティの設定（**Administrative > 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。

始める前に * 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。

- 秘密鍵（`nd.key`）
- 認証局（CA）の公開証明書（`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、 [Generating Private Key and Self-Signed Certificate] 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、 [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。

。Nexus Dashboard の [管理コンソール（**Admin Console**）] に移動します。 。セキュリティの設定を編集します。 .. メイン ナビゲーション メニューから、[管理 > セキュリティ（**Administrative > Security**）] を選択します。 .. 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。 .. 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。 。セキュリティの構成 画面で、必要に応じて 1 つ以上フィールドのを更新します。

+
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. **SSL** 暗号 フィールドをクリックして、有効にする追加の暗号スイートをドロップダウンから選択するか、既存の暗号スイートの **x** アイコンをクリックして削除します。

暗号スイートは、ネットワーク接続を保護するために使用されるアルゴリズム（キー交換、一括暗号化、メッセージ認証コードなど）を定義します。　このフィールドを使用すると、Nexus ダッシュボード
クラスタがネットワーク通信に使用する暗号スイートをカスタマイズし、安全性の低い TLS1.2 や TLS1.3 などの望ましくないスイートを無効にすることができます。

e. [キー（**Key**）] フィールドで、秘密キーを指定します。

f. [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。

g. [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。

h. （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。

i. [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設定に対して、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。制限付きのセキュリティドメインのユーザーは、別のグループの物理環境に不注意により影響を与える可能性があることを心配することなく、そのドメイン内で幅広いレベルの権限が付与されます。

セキュリティドメインを作成するには、次を実行します。

。Nexus Dashboard の [管理コンソール（**Admin Console**）] に移動します。 。新しいセキュリティドメインを作成します。 .. メイン ナビゲーション メニューから、[管理 > セキュリティ（**Administrative > Security**）] を選択します。 .. 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。 .. 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。 。[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。 .. [名前（**Name**）] にドメインの名前を入力します。 .. （任意）ドメインの説明を入力します。 .. [作成（**Create**）] をクリックしてドメインを保存します。

ピア証明書の検証

リリース 2.3.1 以降、サイト コントローラの認証局（CA）ルート証明書チェーンを Nexus ダッシュボードにインポートできます。これにより、Nexus ダッシュボードが接続するホスト（サイト コントローラなど）の証明書が有効であり、サイトを追加するときに信頼できる認証局（CA）によって署名されていることを確認できます。

Cisco APIC からの証明書チェーンのエクスポート

。Cisco APIC にログインします。 。管理アクセスに使用されているキー リングを確認します。

+ image::503127.jpg[]

a. 上部のナビゲーション バーで、ファブリック > ファブリック ポリシー を選択します。
b. 左側のナビゲーション メニューで、ポリシー > ポッド > 管理アクセス を選択します。
c. メイン ペインで、**Admin KeyRing** フィールドの名前を書き留めます。

   上記の例では、`default` キー リングが使用されています。ただし、カスタム証明書チェーンを使用してカスタム キー リングを作成した場合は、そのキー リングの名前が **Admin KeyRing** フィールドにリストされます。

   Cisco APIC のカスタム セキュリティ構成については、ご使用のリリース用のhttps://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html[*Cisco APIC Security Configuration Guide*] で詳しく説明されています。

。キー リングで使用される証明書をエクスポートします。

+ image::503967.jpg[]

a. 上部のナビゲーション バーで、**Admin** > **AAA** を選択します。
b. 左側のナビゲーションメニューで、テナント をクリックします。
c. メイン ペインで、キー リング タブを選択します。
d. 前の手順で見つけたキー リングの名前をクリックし、証明書 をコピーします。

   上記の例は、前のステップの「デフォルト」キーリングを示しています。ただし、カスタム キー リングが構成されている場合は、キー リングの作成に使用された CA 証明書チェーンを選択します。

   コピーするテキストには、`-----BEGIN CERTIFICATE-----` と `-----END CERTIFICATE-----` を含める必要があります。次に例を示します：

```
-----BEGIN CERTIFICATE-----
MIIDQzCCAiugAwIBAgIUWrvhVTKdEKTbLc7vB+oiqXQz3HcwDQYJKoZIhvcNAQEN
[...]
-----END CERTIFICATE-----
```

Cisco NDFC からの証明書チェーンのエクスポート

。サービスをホストしている Nexus ダッシュボードにログインします。

+ NDFC の場合、サービスとは別の証明書がないため、Nexus ダッシュボード ホストの証明書を使用します。 。証明書をエクスポートします。

+ image::503129.jpg[]

a. メイン ナビゲーション メニューから、管理 > セキュリティ を選択します。
b. メインペインで、セキュリティの設定 タブを選択します

c. セキュリティ構成 ページで、編集 アイコンをクリックします。

d. ルート証明書 をコピーします。

注：コピーする文字列にスペースや改行文字（`\n`）が含まれていないことを確認するために、セキュリティ構成 ページから直接ではなく、編集 ページから証明書チェーンをコピーすることをお勧めします。

コピーするテキストには、`-----BEGIN CERTIFICATE-----` と `-----END CERTIFICATE-----` を含める必要があります。次に例を示します：

```
-----BEGIN CERTIFICATE-----
MIIDhTCCAm2gAwIBAgIIOqlnNF7g9e8wDQYJKoZIhvcNAQELBQAwSzELMAkGA1UE
[...]
-----END CERTIFICATE-----
```

Cisco DCNM からの証明書チェーンのエクスポート

。「sysadmin」ユーザーとして Cisco DCNM に SSH で接続します。

+ 他のサイト コントローラとは異なり、DCNM 証明書は UI では使用できないため、CLI を使用する必要があります。

+

```
# ssh -l sysadmin <dcnm-ip-address>
```

+ DCNM での証明書管理の詳細については、「https://www.cisco.com/c/en/us/td/docs/dcn/dcnm/1151/installation/lanfabric/cisco-dcnm-lanfabric-install- and-upgrade-guide-1151/certificates.html[Certificate Management]」の_Cisco DCNM Installation and Upgrade Guide for LAN Fabric Deployment_の章を参照します。

。`/var/lib/dcnm/afw/apigateway/` ディレクトリへ変更します。

+ 証明書（`dcnmweb.crt`）ファイルはこのディレクトリにあります。

+

```
dcnm# cd /var/lib/dcnm/afw/apigateway/
dcnm# ls -ltr /* View the contents of the folder
total 128
-rw------- 1 root root 1844 Nov 18 13:14 dcnmweb.key.2019-11-20T132939-08:00
-rw-r--r-- 1 root root 1532 Nov 18 13:14 dcnmweb.crt.2019-11-20T132939-08:00
-rw------- 1 root root 1844 Nov 20 10:15 dcnmweb.key.2019-11-20T132950-08:00
-rw-r--r-- 1 root root 1532 Nov 20 10:15 dcnmweb.crt.2019-11-20T132950-08:00
-rw------- 1 root root 1844 Dec 22 13:59 dcnmweb.key
-rw-r--r-- 1 root root 1532 Dec 22 13:59 dcnmweb.crt
```

。ルート証明書をチェックします。

+ 証明書の署名に使用した認証局によっては、ルート証明書が「dcnmweb.crt」ファイルに含まれている場合と、別のファイルとして提供されている場合があります。

+ ルート証明書が含まれているかどうかを確認するには：

+ `dcnm# openssl x509 -text -noout -in dcnmweb.crt`

+
ファイルにルート証明書が含まれている場合は、それをコピーします。それ以外の場合は、証明書に署名するときに取得する必要があるルート証明書ファイルを使用します。

Cisco クラウド ネットワーク コントローラからの証明書チェーンのエクスポート

。Cisco クラウド ネットワーク コントローラにログインします。 。証明書をエクスポートします。

+ image::503128.jpg[]

a. メイン ナビゲーション メニューから、管理 > セキュリティ を選択します。
b. メイン ペインで、キー リング タブを選択します。
c. Nexus ダッシュボードにインポートする証明書の名前をクリックし、認証局（**CA**）をコピーします。

   上記の例は、`default` キー リングを示しています。ただし、カスタム キー リングが構成されている場合は、キー リングの作成に使用された CA 証明書チェーンを選択します。

   コピーするテキストには、`-----BEGIN CERTIFICATE-----` と `-----END CERTIFICATE-----` を含める必要があります。次に例を示します：

```
-----BEGIN CERTIFICATE-----
MIIDvTCCAqWgAwIBAgIJAI6W9R8DXDgLMA0GCSqGSIb3DQEBDQUAMEAxCzAJBgNV
[...]
-----END CERTIFICATE-----
```

Nexus ダッシュボードへの証明書のインポート

。サイトを導入準備する予定の Nexus ダッシュボードにログインします。 。証明書を Nexus ダッシュボードにインポートします。 .. サイトを導入準備する Nexus ダッシュボードにログインします。 .. 左側のナビゲーション メニューで、管理 > セキュリティ を選択します。 .. メインペインで、**CA** 証明書タブを選択します。 .. **CA** 証明書を追加をクリックし、証明書の一意の名前を指定して、サイトのコントローラからコピーした証明書チェーンを貼り付けます。

。通常どおりサイトの追加を続行しますが、ピア証明書の検証 オプションを有効にします。

+ 有効な証明書をインポートせずに ピア証明書を検証 オプションを有効にするとサイトの導入準備は機能不全になることに注意してください。

+ サイトの追加については [Adding Sites] で説明しています。

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に加えて、Nexus Dashboardをはじめとする他の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。詳細な*自動更新*オプションについては、<<Configuring Device Connector Settings> >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。

注：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、[Cluster Configuration] 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 ポータルに接続します。これによって、接続されたデバイスが情報を送信し、Cisco Intersight ポータルから制御命令を受信するための安全な方法が から提供されます。

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。

。Nexus Dashboard の [管理コンソール（**Admin Console**）] に移動します。 。メインメニューから [インフラストラクチャ > Intersight（**Infrastructure > Intersight**）] を選択します。 。メインペインの右上の [設定（**Settings**）] をクリックします。 。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。 .. 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。

a. [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。

b. 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。

。[保存（**Save**）] をクリックして、変更内容を保存します。

。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 [Configuring Device Connector Settings] の説明に従って、Intersight デバイスコネクタを構成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。

。Nexus Dashboard の [管理コンソール（**Admin Console**）] に移動します。 。メインメニューから [インフラストラクチャ > Intersight（**Infrastructure > Intersight**）] を選択します。
。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 [Cluster Configuration] 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。

。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、[Configuring Device Connector Settings] で説明されています。

+ 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。

。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。

+ image::503388.jpg[]

。Cisco Intersight クラウドサイト（https://www.Intersight.com）にログインします。

。Intersight マニュアルの、
https://www.intersight.com/help/getting_started#target_claim[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。

+ 注：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。

。Nexus Dashboard の [管理コンソール（**Admin Console**）] に移動します。 。メインメニューから [インフラストラクチャ > Intersight（**Infrastructure > Intersight**）] を選択します。 。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 表示 クラスタ` — クラスタ構成を表示。
- `acs 表示 ノード` — クラスタ内のすべてのノードに関する情報を表示します。
- `acs 表示 マスター` — クラスタ内の `マスター` ノードに関する情報を表示します。
- `acs 表示 ワーカー` — クラスタ内の `ワーカー` ノードに関する情報を表示します。
- `acs 表示 スタンバイ` — クラスタ内の `スタンバイ` ノードに関する情報を表示します。
- `acs ntp show` — NTP 情報を表示します。
- `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。
- `kubectl` コマンドは、読み取り専用 Kubernetes コマンドをサポートします。

  たとえば、これを使用して、システムで実行されているすべてのポッドのリストを取得できます：

  ```
  $ kubectl get pods -A
  NAMESPACE  NAME  READY  STATUS  RESTARTS  AGE
  aaamgr  aaamgr-54494fdbc8-q8rc4  2/2  実行中  0  3d3h
  authy-oidc  authy-oidc-75fdf44b57-x48xr  1/1  実行中  3 (3d3h ago) 3d4h
  authy  authy-857fbb7fdc-7cwgg  3/3  実行中  0  3d4h
  cisco-appcenter  apiserver-686655896d-kmqhq  1/1  実行中  0  3d3h
  [...]
  ```

- `acs elasticsearch` コマンドは、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。

```
$ acs elasticsearch --name cisco-ndfc-controller-elasticsearch health
{
"cluster_name" : "cisco-ndfc-controller-elasticsearch",
"status" : "green",
"timed_out" : false,
"number_of_nodes" : 3,
"number_of_data_nodes" : 3,
"discovered_master" : true,
"active_primary_shards" : 10,
"active_shards" : 21,
"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
}
```

次の例のように、kubectl コマンドを使用して、サービス固有のポッド名のリストを取得できます：

```
$ kubectl get pods -A | grep elasticsearch
cisco-ndfc-controller-elasticsearch  es-data-0  2/2  実行中  0  109m
cisco-ndfc-controller-elasticsearch  es-data-1  2/2  実行中  0  163m
cisco-ndfc-controller-elasticsearch  es-data-2  2/2  実行中  0  104m
```

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。

CIMC のアップグレード

Cisco Nexus Dashboard ソフトウェアをアップグレードする場合、Nexus Dashboard ノードで実行されている Cisco Integrated Management Controller (CIMC) のバージョンもアップグレードする必要がある場合があります。

サポートされている CIMC ソフトウェア バージョンのリストについては、https://www.cisco.com/c/en/us/support/data-center-analytics/nexus-dashboard/products-release-notes-list.html[リリース ノート] を確認することをお勧めします。

次の手順では、Cisco ホスト アップグレード ユーティリティ (HUU) を使用して Nexus Dashbaord CIMC をアップグレードする方法について説明します。Host Upgrade Utility の詳細については、https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/lomug/4_0/b_huu_4_0_2.html[HUU を使用する Cisco UCS C シリーズ サーバーでのファームウェアのアップグレード]。

注：古いファームウェアを実行している1つ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、クラスタのすべてのノードではなく、そのノードでのみ次の手順を実行します。

始める前に * Cisco Nexus ダッシュボード リリース ノートで提供される情報を確認し、どの CIMC ソフトウェア イメージが Nexus ダッシュボード リリースと互換性があるかを確認します。Cisco Nexus Dashboard のリリース ノートは、Nexus Dashboard のドキュメント ページで入手できます。 * アップグレードに適切な時間を確保します。

+ CIMC バージョンのアップグレード プロセスに必要な時間は、ローカル マシンと UCS-C シャーシ間のリンクの速度と、送信元/ターゲット ソフトウェア イメージ、およびその他の内部コンポーネント バージョンによって異なります。 * CIMC を更新するには、CIMC のアップグレードに使用される vKVM を実行するために、ブラウザおよび/または Java ソフトウェア バージョンを更新する必要がある場合もあります。

注：CIMC バージョンをアップグレードしても、Nexus Dashboard ノードがトラフィックのデータパスに含まれていないため、実稼働ネットワークには影響しません。

Nexus Dashboard CIMC ソフトウェアをアップグレードするには、次の手順を実行します。

。CIMC クレデンシャルを使用して CIMC にログインします。

+ CIMC クレデンシャルは、Nexus Dashboard GUI クレデンシャルとは異なる場合があることに注意してください。 。サーバー > 概要 で BIOS バージョンの最初の部分を見つけて、Cisco Nexus ダッシュボードの UCS プラットフォームのモデルを判別します。

+ image::ServerSummary1.jpg[] . https://software.cisco.com/download で適切な HUU ISO イメージを見つけます。 .. https://software.cisco.com/download の検索ウィンドウに、前の手順で見つけた Cisco Nexus ダッシュボードの UCS プラットフォーム モデルを、ダッシュを使用せずに入力します。 .. 検索結果のリンクをクリックすると、UCS プラットフォームで使用可能なソフトウェアが表示されます。 .. お使いのサーバで使用可能なソフトウェアのリストで、ファームウェアエントリを見つけます。これは、Unified Computing System (UCS) Server Firmware のように表示されています。ファームウェアのリンクをクリックします。 .. CISCO UCS Host Upgrade Utility.iso イメージのリンクを見つけて、このイメージのリリース情報をメモしておきます。

+ image::SoftwareDownload3.jpg[]

。https://software.cisco.com/download サイトから適切な HUU.iso イメージをダウンロードします。
。CIMC GUI から KVM コンソールを起動します。

+ image::LaunchKVM2.jpg[]

+ 注：KVM コンソールを開くことができない場合は、Java バージョンを更新する必要がある可能性があります。 。KVM コンソールで、仮想メディア > 仮想手バイスのアクティブ化 *をクリックし、セッションを受け入れます。 。*仮想メディア > **CD/DVD** のマッピング をクリックし、PC でダウンロードしたイメージに移動します。 。ダウンロードした HUU.iso イメージを選択し、マップ ドライブ をクリックして、ダウンロードした ISO を PC にマッピングします。

+ image::MapDrive.jpg[] . 障害とログ > システム イベント ログ をクリックして、ログを確認します。ログがいっぱいの場合は、ログをクリア を選択してクリックしてログをクリアします。 。電源 > 電源周期システム をクリックして、コールドリブートを実行します。 。**F6** を押してブート メニューを表示し、マップされた DVD を選択してブートできるようにします。
。プロンプトが表示されたら、パスワードを入力します。デフォルトのパスワードは パスワード です。

+ image::SelectBootDevice.jpg[] ブート デバイスを選択するように求められたら、次の図に示すように、**Cisco vKVM-Mapped vDVD** オプションを選択します。
。プロセスが完了するのを待ち、プロンプトが表示されたら、利用規約に同意します。同意する をクリックし、更新してアクティブ化 をクリックします。

+ image::Accept.jpg[]

+ image::UpdateAndActivate1.jpg[] アップグレードが正常に完了したことを確認するには、GUI を使用するか、または CIMC HUU を起動し、最後の更新の確認 を選択して、すべてのコンポーネントがアップグレードをパスしたことを確かめます。
。アップグレードが完了したら、トラステッド プラットフォーム モジュール状態（TPM）が有効になっているかどうかを確認します。 有効になっていない場合は、**BIOS** > **BIOS** を構成 > セキュリティ に移動し、トラステッド プラットフォーム モジュール状態オプションを有効にして、保存 をクリックします。

手動アップグレード

クラスタのアップグレードには、[Firmware Management (Cluster Upgrades)] 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（クラスタに新しいノードを追加しているが、ノードが古いファームウェアを実行している場合）またはクラスタ全体（GUIアップグレードが成功しなかった場合）の手動アップグレードを実行する場合は、代わりに、次の手順を使用することができます。

注：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。

。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。

。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。

。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

。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。

+ 注：次の手順に進む前に、すべてのノードがアップグレードの完了を待つ必要があります。

+ Update succeeded, reboot your host

。1つのノードをリブートします。

+
前のステップで表記されているようにいずれかのノードをリブードする前に、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

。ノードが正常であることを確認します。

+ # acs health All components are healthy

。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 1 つずつにリブートします。

+ 注：次のノードを再起動する前に、`acs` 正常性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。

。すべてのノードが新しいバージョンを起動し、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

。アップグレード後のタスクが完了するまで待ちます。

+ この段階では、UI に進行状況が表示されます。これは、最初のクラスタ展開に似ています。アップグレード後のプロセスが完了すると、通常どおりノードにログインできるようになります。

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構成するだけの場合は、このセクションをスキップして、[Managing Worker Nodes] または、 [Managing Standby Nodes] 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　　[Manual Upgrades] 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。

注：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。

始める前に

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。 サポートされているバージョンの Cisco Integrated Management Controller（CIMC）を実行していることを確認してください。　　推奨バージョン:　**CIMC**、リリース **4.1(3b)**。 サポートされる最小バージョン：CIMC、リリース 4.0(1a)。

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。

。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ダッシュボードのバージョンを選択します。
d. Cisco Nexus ダッシュボード イメージ（ nd-dk9.<version>.iso).
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。

。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。

```
<F2> 設定、<F6> ブート メニュー、<F7> 診断、 <F8> Cisco IMC 構成、<F12>
ネットワーク ブートを押します。
```

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 'ネットワークインターフェースの構成'
ネットワーク インターフェイスの構成
+ echo 'type static, dhcp, bash for a shell to configure networking, or url to re-
enter the url: '
ネットワーキングを構成するには static または dhcp、shell として bash
を入力します。または、url を再入力する場合は、url と入力します。
+ read -p '? ' ntype
? static ①
+ case $ntype in
+ configure_static
+ echo 'Available interfaces'
利用可能なインターフェイス
+ ls -l /sys/class/net
total 0
lrwxrwxrwx. 1 root root 0 Apr 26 01:21 eno1 ->
../../devices/pci0000:3a/0000:3a:00.0/0000:3b:00.0/net/eno1
lrwxrwxrwx. 1 root root 0 Apr 26 01:21 eno1 ->
../../devices/pci0000:3a/0000:3a:00.0/0000:3b:00.0/net/eno1
lrwxrwxrwx. 1 root root 0 Apr 26 01:21 eno5 ->
../../devices/pci0000:5d/0000:5d:00.0/0000:5e:00.0/0000:5f:01.0/0000:61:00.0/0000:6
2:00.0/0000:63:00.0/net/eno5
lrwxrwxrwx. 1 root root 0 Apr 26 01:21 eno6 ->
../../devices/pci0000:5d/0000:5d:00.0/0000:5e:00.0/0000:5f:01.0/0000:61:00.0/0000:6
2:00.0/0000:63:00.1/net/eno6
lrwxrwxrwx. 1 root root 0 Apr 26 01:21 lo -> ../../devices/virtual/net/lo
+ read -p '構成するインターフェース: ' interface
構成するインターフェース: eno1  ②
+ read -p 'address: ' addr
アドレス: 172.23.53.59/21  ③
+ read -p 'ゲートウェイ: ' gw
ゲートウェイ: 172.23.48.1  ④
+ ip addr add 172.23.53.59/23 dev eno1
+ ip link set eno1 up
+ ip route add default via 172.23.48.1
RTNETLINK answers: Network is unreachable
++ seq 1 2
+ for count in '$(seq 1 2)'
+ ping -c 1 172.31.131.47
```

① 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。

② 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。

③ `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。

④ `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。

。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、[Managing Worker Nodes] または [Managing Standby Nodes]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 > AppStore（**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。

解決法

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ないことです。

。解像度　　クラスタの構成　　> **Syslog**
の外部サーバーの構成が正しいことを確認してください。詳細については、[Cluster　　Configuration]
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。

解決法 *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
```

注：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、https://www.cisco.com/c/en/us/td/docs/dcn/nd/2x/deployment/cisco-nexus-dashboard-deployment-guide-211.html[*Cisco Nexus Dashboard Deployment Guide*] 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　ノードのデータ　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。

シングル　　ノード　　クラスタを稼働している場合、クラスタを再作成しない限り、管理　　IP アドレスの変更もサポートされません。

マルチノード　　クラスタを稼働している場合は、次のように　　1　　つ以上のノードの管理　　IP アドレスを変更できます。

。Nexus Dashboard の [管理コンソール（**Admin Console**）] に移動します。 。メイン ナビゲーションメニューから、[システムリソース　>　ノード（System　Resources　>　Nodes）]　を選択します。 。ノードの隣にある（**...**）メニューから、[ノードの編集（**Edit Node**）] を選択します。

+ 現在ログインしていないノードの IP アドレスのみを変更できることに注意してください。現行ノードの IP　　を変更するには、別のノードの管理　　IP アドレスに移動してログインし、最後のノードまでこの手順を繰り返します。　　。ノードの [管理ネットワーク　アドレス（**Management　Network　Address**）]　と　[管理ネットワークゲートウェイ（**Management Network Gateway**）] を更新します。

+ たとえば、それぞれ `172.31.140.58/24` と `172.31.140.1` です。 。**[Save]** をクリックします。

+ 変更はすぐに有効になり、新しい IP アドレスを使用してノードにアクセスできます。

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、多数の `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。

解決法

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。

解決法

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。

[Troubleshooting] のセクションで説明されている一般的な Nexus ダッシュボードのトラブルシューティング コマンドを実行するには、最初に Nexus ダッシュボード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。

。インストール時に YAML 構成ファイルで指定した Nexus ダッシュボードユーザーを使用して、RHEL システムにログインします。 。`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 ダッシュボード環境にアクセスすると、このガイドの [Troubleshooting] のセクションで説明されているすべての一般的な Nexus ダッシュボードコマンドを使用できます。

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、API C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。

解決法

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。

。Nexus Dashboardクラスタにログインします。 。[管理コンソール > サイト（**Admin Console > Sites**）] に移動します。 。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。 。[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。 。**[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、[Replacing Single Master Node with Standby Node] 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 [Adding Standby Nodes] 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 [Replacing Single Physical Master Node without Standby Node] 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。

。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

+ 。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。。[システムリソース > ノード（**System Resources** > **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。 。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。 。[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。

。残りのノード情報が正確であることを確認します。 。[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。

。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。

。新しいNexus Dashboardノードを起動します。

+ VMware ESX での追加ノードの起動については、 [Deploying Additional Virtual Nodes in VMware ESX] で説明されています。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 での追加ノードの起動については、 [Deploying Additional Virtual Nodes in Linux KVM] で説明されています。

+ 注：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。

。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。

。Nexus Dashboardの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。

。ノードを置換します。 .. 左側のナビゲーション ペインから、[システム リソース > ノード（**System Resources > Nodes**）] を選択します。

+ 交換するノードが [非アクティブ（`Inactive`）] としてリスト化されます。

a. 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。

b. 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、接続性を確認します。

c. [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、 [Re-Adding Same Master Node to Physical Cluster] 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 ノードが構成されている場合は、 [Replacing Single Master Node with Standby Node] の手順に従うことを推奨します。

始める前に

- 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、[Replacing Two Master Nodes with Standby Nodes] 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。
- [Deploying Additional Physical Nodes] 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に設定していたのと同じ 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。

。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。。メイン ナビゲーション メニューから、[システムリソース > ノード（System Resources > Nodes）] を選択します。 。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。

+

。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。 。[アクション（**Actions**）] メニューから [置換（**Replace**）] を選択します。 。[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。

始める前に

- 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。

。Nexus Dashboard の [管理コンソール（**Admin Console**）] に移動します。 。メイン ナビゲーション メニューから、[システムリソース > ノード（System Resources > Nodes）] を選択します。 。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。 。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。　　。[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。 。[Managing Worker Nodes] または、[Managing Standby Nodes]　　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。

+ 古いノードを設定したときと同じ設定パラメーターを使用します。

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すことができます。

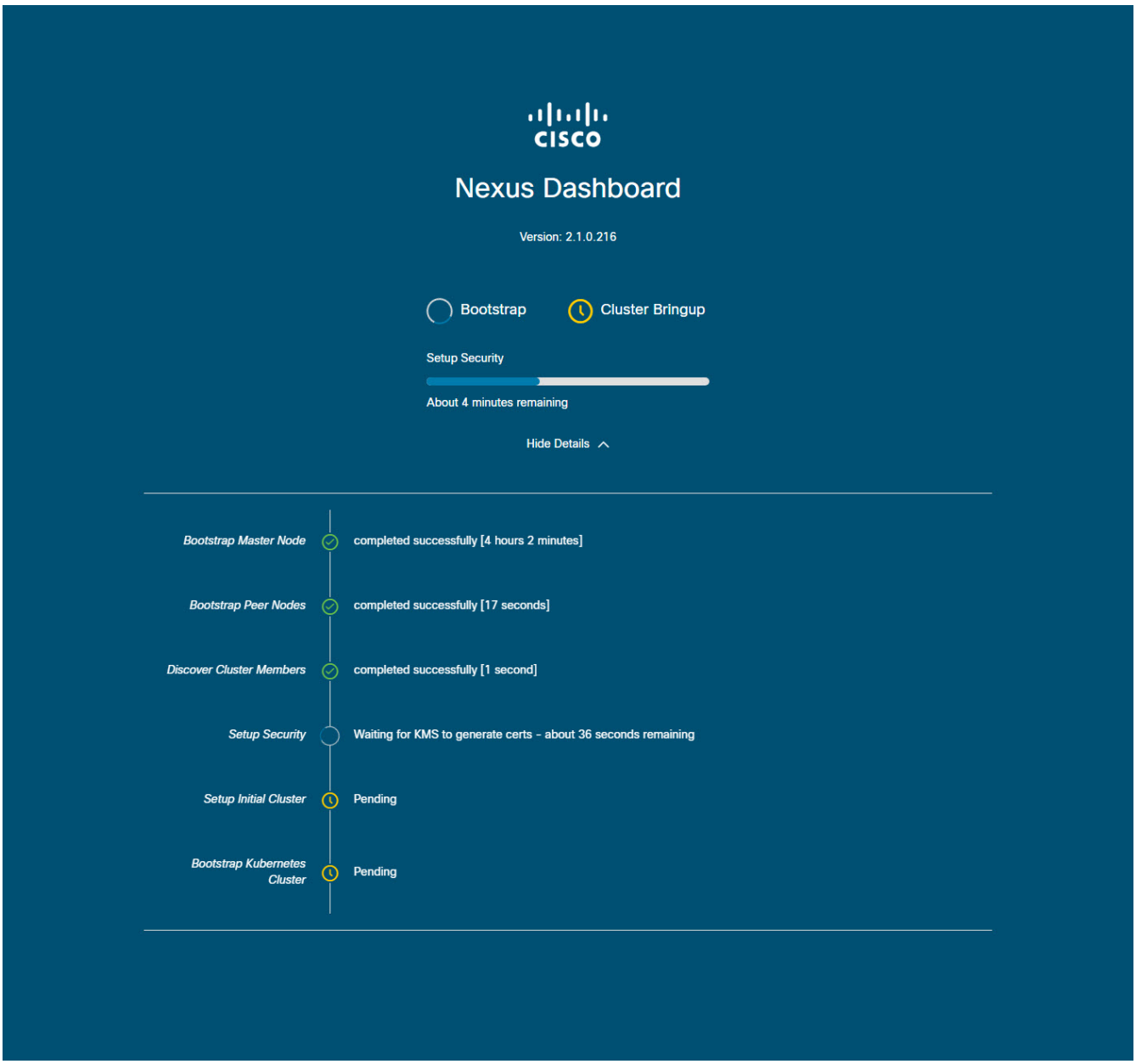


Figure 15. ブートストラップの進行状況

- 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。Then check the specific service's logs in /logs/k8_infra/<service>

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、 [Multi-Cluster Connectivity] 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。

。プライマリクラスタにログインします。 。グループから再展開したクラスタを削除します。

+ < <Disconnecting Clusters>> で説明します。 。クラスタをグループに再度追加します。

+ < <Connecting Multiple Clusters>> で説明します。

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。

。`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。 。グループから再展開したクラスタを削除します。

+ < <Disconnecting Clusters>> で説明します。 。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。

秘密キーの生成、証明書署名要求の作成、およびCA署名付き証明書の取得

このセクションでは、秘密キーの生成、証明書署名要求 (CSR) の作成、および認証局 (CA) によって署名された証明書の取得方法の例を示します。これらはNexusダッシュボードクラスタで使用します。

秘密キーと自己署名証明書の両方を生成する場合は、このセクションをスキップし、代わりに [Generating Private Key and Self-Signed Certificate] で説明されている手順に従ってください。

Nexus ダッシュボード GUI でキーと証明書を追加するために必要な設定手順は、[Security] の章で説明されています。

。秘密キーを生成します。

+ 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
```

。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。

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
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
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
```

。CA署名付き証明書を取得します。

+ 実稼働環境では、前ステップで作成した証明書署名要求（ca.csr）をIdenTrustやDigiCertなどのパブリックCAに送り、CA署名付き証明書（ca.crt）を取得します。

。署名済み証明書を確認します。

+ 次のコマンドは、生成した秘密キーと同じフォルダにCA 署名付き証明書（ca.crt）をコピーしたことを前提としています。

+

```
[rescue-user@localhost ~]$ openssl verify -verbose -CAfile ca.crt nd.crt
nd.crt: OK
```

。生成されたファイルの内容をNexus DashboardのGUIに追加します。

+ [Security Configuration] 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`）

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
。

CA署名付き証明書を使用する場合は、このセクションをスキップして、 Creating CSR, and Obtaining CA-Signed Certificate で説明されている手順に従ってください。

Nexus ダッシュボード GUI でキーと証明書を追加するために必要な設定手順は、[Security]
の章で説明されています。

。秘密キーを生成します。

+ 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
```

。認証局(CA)キーを生成します。

+ ラボやテストの目的などで自己署名CAを生成するには、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
```

。CAのCSRを生成します。

+

```
[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
```

。自己署名ルート証明書を作成します。

+

```
[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
```

。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。

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
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
```

。生成した証明書に自己署名します。

+

```
[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
```

。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
```

。生成されたファイルの内容をNexus DashboardのGUIに追加します。

+ [Security Configuration] 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`）

NDFC によって管理されるスイッチ デバイスを交換した後の NDO 構成の更新

Nexus ダッシュボード ファブリック コントローラ（NDFC）ファブリックが Nexus ダッシュボード オーケストレータ（NDO）によって管理されており、NDFC によって管理される 1 つ以上のデバイスを交換する場合は、NDO が新しいスイッチのシリアル番号を認識していることを確認する必要があります。

次のセクションでは、新しいファブリック デバイスの情報を NDO と同期するために必要な手順の概要を示します。

コアまたはルート サーバー（RS）デバイスの交換

。NDFC にログインします。 。NDFC 簡単ファブリック モードを使用しているときにファブリック内の物理スイッチを交換するには、https://www.cisco.com/c/en/us/td/docs/dcn/ndfc/121x/configuration/fabric-controller/cisco-ndfc-fabric-controller-configuration-guide-121x/lan-switches.html#concept_fwc_lmk_1rb[Cisco NDFC Fabric Controller Configuration Guide]。 。NDOにログインします。 。インフラストラクチャ > サイト接続 に移動します。 。RS/コアが存在する 全般設定 ページの コントロール プレーン構成 で 更新 をクリックします。 。展開 をクリックします。

リーフ スイッチの交換

。NDFC にログインします。 。NDFC 簡単ファブリック モードを使用しているときにファブリック内の物理スイッチを交換するには、https://www.cisco.com/c/en/us/td/docs/dcn/ndfc/121x/configuration/fabric-controller/cisco-ndfc-fabric-controller-configuration-guide-121x/lan-switches.html#concept_fwc_lmk_1rb[Cisco NDFC Fabric Controller Configuration Guide]。 。NDOにログインします。 。アプリケーション管理 > スキーマ に移動し、そのサイト/デバイスのスキーマ/テンプレートをクリックします。 。デバイスに存在していた VRF/ネットワークを再インポートします。 .. 概要を表示 ドロップダウン リストで、テンプレートを選択します。 .. テンプレートのプロパティ セクションで、**VRF** ボックスから VRF /ネットワークをクリックします。 .. インポート*ドロップダウン リストからサイトを選択します。 .. ***VRF** をクリックした後、VRF を選択します。 .. インポート をクリックします。

ボーダー ゲートウェイ（BGW）デバイスの交換

。NDFC にログインします。 。NDFC 簡単ファブリック モードを使用しているときにファブリック内の物理スイッチを交換するには、https://www.cisco.com/c/en/us/td/docs/dcn/ndfc/121x/configuration/fabric-controller/cisco-ndfc-fabric-controller-configuration-guide-121x/lan-switches.html#concept_fwc_lmk_1rb[Cisco NDFC Fabric Controller Configuration Guide]。 。NDOにログインします。 。インフラストラクチャ > サイト接続 に移動します。 。BGW が存在するサイトで 更新 をクリックし、展開 をクリックします。 。アプリケーション管理 > スキーマ に移動し、そのサイト/デバイスのスキーマ /テンプレートをクリックします。 。デバイスに存在していた VRF/ネットワークを再インポートします。 .. 概要を表示 ドロップダウン リストで、テンプレートを選択します。 .. テンプレートのプロパティ セクションで、**VRF** ボックスから VRF /ネットワークをクリックします。 .. インポート*ドロップダウン

リストからサイトを選択します。 .. ***VRF** をクリックした後、VRF を選択します。 .. インポートをクリックします。