Cisco Nexus Dashboard オペレーション、リリース 3.1.x

目次

ファームウェア管理

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。

次の項では、ファームウェア アップグレードの参考情報を提供します。パラメータの最新のアップグレード プロセスに関する情報は、オンライン版の *Nexus Dashboard Deployment Guide* を参照してください。

前提条件とガイドライン

既存のNexusダッシュボードクラスタをアップグレードする前に、次の手順を実行します。

- アップグレードに影響する可能性のある動作変更、ガイドライン、および問題については、対象のリリースの*リリースノート*を必ずお読みください。

  アップグレード プロセスは、すべての Nexus Dashboard フォーム ファクタで同じです。ただし、既存のクラスタが物理サーバー、VMware ESX、Linux KVM、Azure、または AWS を使用して展開されている場合は、ターゲット リリースの ISO イメージ（nd-dk9.<version> .iso）アップグレードします。既存のクラスターが Red Hat Enterprise Linux に展開されている場合は、RHEL 固有のイメージ（nd-rhel-）。
  <version>.tar）。

- 既存のクラスタで実行している任意のサービス、およびターゲットリリースで実行を計画している任意のサービスのリリースノートとアップグレードガイドで、アップグレードに影響する可能性がある動作、ガイドライン、問題に関するサービス固有の変更を確認します。

  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 ファブリック コントローラ、リリース ノート*
  - *Nexus Dashboard ファブリック コントローラ、アップグレード ガイド*
  - *Nexus Dashboard Insights リリース ノート*
  - *Nexus Dashboard Insights アップグレード ガイド*
  - *Nexus Dashboard Orchestrator リリース ノート*
  - *Nexus Dashboard Orchestrator アップグレード ガイド*

- 物理的な Nexus Dashboard クラスタをアップグレードしている場合は、ノードにターゲットの Nexus Dashboard リリースでサポートされている最小の CIMC バージョンがあることを確認してください。

  サポートされている CIMC バージョンは、ターゲット リリースの Nexus Dashboard *リリース ノート* にリストされています。CIMC のアップグレードについては、「CIMC のアップグレード」を参照してください。

- アップグレードを続行する前に、データを保護し、潜在的なリスクを最小限に抑えるために、アップグレードの前に Nexus ダッシュボードとサービスの構成バックアップを実行する必要があります。

- クラスタで実行されているすべてのサービスを無効にする必要があります。
- 有効な DNS および NTP サーバーが構成され、すべてのクラスター ノードから到達可能である必要があります。
- 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 の管理コンソール（**Admin Console**）の **[概要（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 コマンドを実行して All components are healthy が返ってくることを確認します。

- アップグレードが進行中にワーカーまたはスタンバイ ノードを追加するなど、設定変更がクラスタに対して行われていないことを確認します。
- このリリースにアップグレードした後、すべてのサービスをこのリリースによりサポートされている最新バージョンにアップグレードすることをお勧めします。Nexus ダッシュボードとサービスの相互運用性サポートの完全なリストについては、「*Nexus ダッシュボードとサービスの互換性マトリクス*」を参照してください。
- Nexus Dashboard ではプラットフォームのダウングレードは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サービスを再インストールする必要があります。

イメージの追加

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

1. Nexusダッシュボードイメージをダウンロードします。
   a. ソフトウェア ダウンロード ページを参照してください。

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

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

      

      初期クラスタ展開に
      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でisoイメージをダウンロードする必要があります。

   d. （オプション）環境内のWebサーバでイメージをホストします。

      イメージをNexusダッシュボードクラスタにアップロードする場合、イメージに直接URLを指定するオプションがあります。

2. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
3. イメージを追加します。
   a. メイン メニューで、**[管理（Admin）] > [ソフトウェア管理（Software Management）]** を選択します。
   b. メインペインで、**[イメージ（Images）]** タブを選択します。

      ページには、以前に追加されたイメージが一覧表示されます。

c. メインペインで、[イメージの追加（**Add Image**）] をクリックします。

4. [ソフトウェア イメージの追加（Add Software Image）] ウィンドウが表示されたら、イメージをリモート サーバーまたはローカル システムのどちらに保存するかを選択します。
   a. リモートイメージを指定する場合は、イメージの完全な **URL** を指定します。
   b. ローカルイメージをアップロードする場合は、[ファイルの選択（**Choose File**）] をクリックし、ローカルシステムからイメージファイルを選択します。

ローカルマシンからアップロードする場合、アップロード速度が遅いとセッションがタイムアウトし、転送が中断される可能性があります。 少なくとも 40Mbps のアップロード速度と、セッション タイムアウトを1800 秒（デフォルトの 1200 から）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。

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

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

クラスタのアップグレード

はじめる前に

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

クラスタをアップグレードするには、次の手順を実行します。

1. Nexus Dashboard の [管理コンソール（**Admin Console**）] に移動します。
2. 更新を開始します。
   a. メイン メニューで、[管理（**Admin**）] > [ソフトウェア管理（**Software Management**）] を選択します。
   b. メイン ペインで、[更新（**Updates**）] タブを選択します。
   c. [更新のセットアップ（**Set up Update**）] または [詳細の変更（**Modify Details**）] をクリックします。

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

      以前クラスタをアップグレードした場合は、[更新のセットアップ（**Setup Update**）] ボタンではなく、最後のアップグレードの詳細がこのページに表示されます。この場合、画面の右上にある [詳細の変更（**Modify Details**）] ボタンをクリックします。

3. [セットアップ/バージョンの選択（**Setup/Version Selection**）] 画面で、対象バージョンを選択し、[次へ（**Next**）] をクリックして続行します。Nexusダッシュボードに複数の画像をアップロードした場合は、それらがここに表示されます。

4. 検証レポートを確認し、[インストール（**Install**）] 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確認検査を実行し、レポートを表示します。

5. **[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。

6. インストールのインストールが完了するまで待ちます。

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

7. **[有効化（Activate）]** をクリックします。

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

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

イメージの削除

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

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

テクニカルサポート

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

テクニカルサポート情報を収集するには、次の手順を実行します。

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. テクニカルサポートを収集します。
   a. メイン ナビゲーション メニューから、**[アナライザ（Analyzer）] > [テクニカルサポート（Tech Support）]** を選択します。
   b. メインペインで、**[テクニカル サポートの収集（Collect Tech Support）]** をクリックします。
3. **[テクニカルサポートの収集（Collect Tech Support）]** ウィンドウが開いたら、説明を入力します。
4. **[範囲（Scope）]** ドロップダウンから、テクニカル サポート情報を収集するカテゴリを選択します。
   - [システム（System）]は、インフラストラクチャのテクニカルサポート情報を収集します。
   - [App Store] は、App Store のテクニカルサポート情報を収集します。
   - サービス固有の選択は、その特定のサービスのテクニカルサポート情報を収集します。
5. **[収集（Collect）]** をクリックします。

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

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

6. テクニカルサポートアーカイブをダウンロードします。

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

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

バックアップと復元

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

設定のバックアップの作成

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. バックアップを開始します。
   a. 左のナビゲーション メニューから **[管理者（Admin）] > [バックアップおよび復元（Backups & Restore）]** を選択します。
   b. メイン ペインで、**[バックアップ ジョブ（Backup Jobs）]** タブを選択します。
   c. メイン ペインで、**[バックアップ設定（Backup Configuration）]** をクリックします。
3. **[バックアップ設定（Backup Configuration）]** ウィンドウが開いたら、**[暗号化キー（Encryption Key）]** と **[ファイル名（File Name）]** を入力します。暗号化キーはアーカイブの暗号化に使用され、8文字以上にする必要があります。
4. **[ダウンロード（Download）]** をクリックしてバックアップを開始します。

Cisco Nexus Dashboard は設定のバックアップや暗号化キーを保存しないので、Nexus Dashboardクラスタがあり 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。

- 「永続的 IP アドレス」で説明されている永続的な IP。
- 「イベントのエクスポート」で説明されているストリーミング イベントの Syslog。
- スタティック ルート（「クラスタ構成」で説明）。構成のバッ

クアップを復元する：

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. 設定の復元を開始します。
   a. 左のナビゲーション メニューから **[管理（Admin）] > [バックアップおよび復元（Backups & Restore）]** を選択します。
   b. メイン ペインで、**[復元ジョブ（Restore Jobs）]** タブを選択します。
   c. メイン ペインの右上にある 復元設定（**Restore Configuration**）] をクリックします。

      リストされているバックアップのいずれかを選択する必要はありません。次の画面で、設定のバックアップファイルをアップロードするように求められます。
3. 詳細を入力します。
   a. **[暗号化キー（Encryption Key）]** を入力します。

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

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

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

このファイルは .tgz または tar.gz 形式である必要があります。

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

履歴とログ

[管理（**Admin**）] > [履歴とログ（**History and Logs**）] ページでは、Nexus Dashboard クラスタ内のイベントとアラートのシステム全体のリストを表示できます。

イベント

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

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

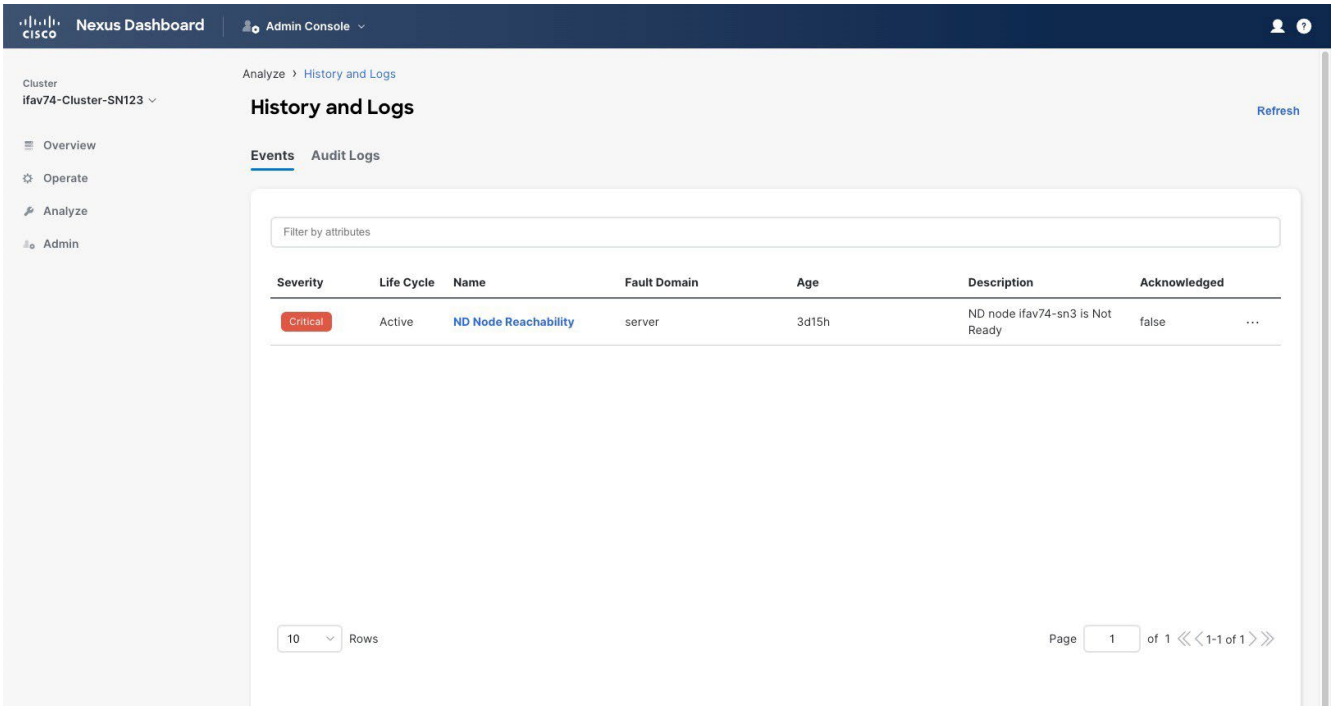

図 1. イベント

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

監査ログ

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

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

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

[属性でフィルタ（**Filter by attributes**）] フィールドを使用してリストをフィルタリングし、特定の属性

と値のペアを指定することもできます。

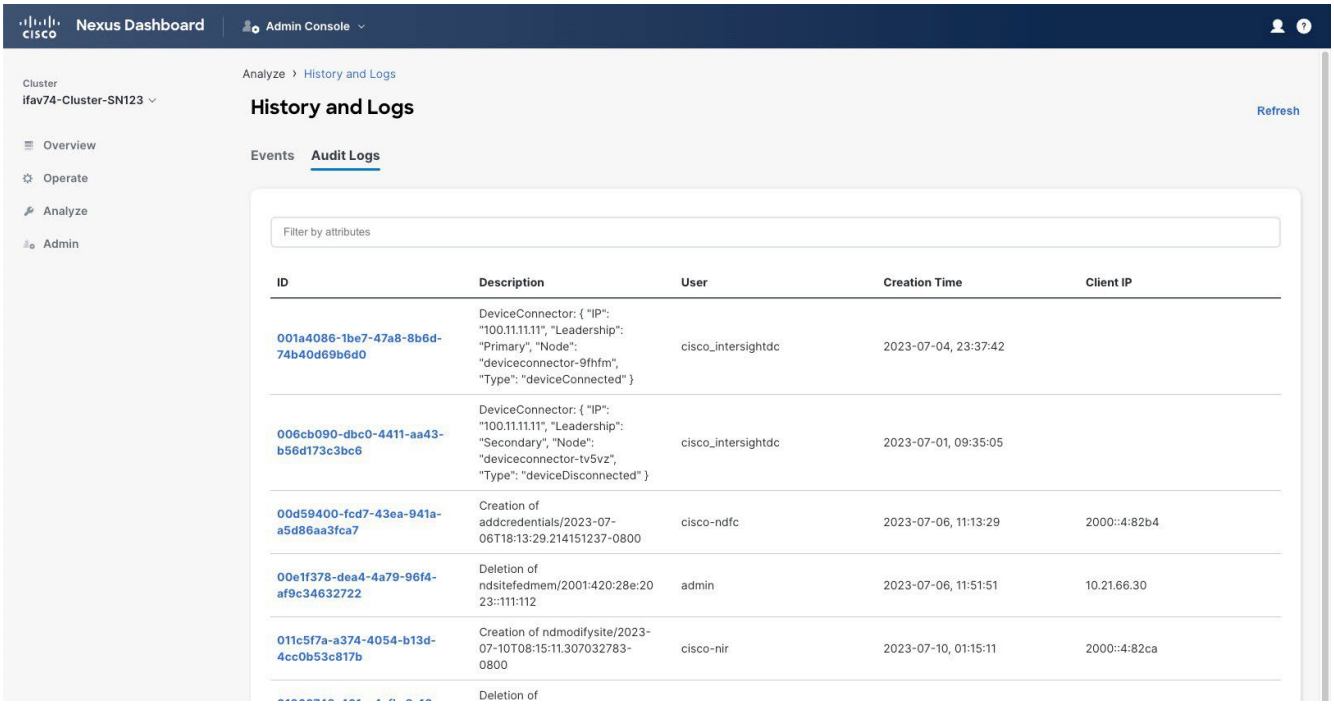

図 2 監査ログ

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。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。
- 次のフロー イベントがエクスポートされます。
  - ノード CPU 超過しきい値
  - ノード ストレージのしきい値超過
  - ノード メモリのしきい値超過
  - クラスタ ノードに到達できません
  - クラスタ ノードが再起動される
  - すべての監査イベント
  - 同期済みでない NTP
  - BGP ピアに到達できないイベ

ントのエクスポートを設定するには、

次の手順を実行します。

1. Nexus Dashboard の **[**管理コンソール（**Admin Console**）**]** に移動します。
2. 左のナビゲーション メニューから **[**管理 **(Admin)] > [**システム 設定 **(System Settings)]** を選択します。
3. **Syslog** タイルで **[**編集（**Edit**）**]** アイコンをクリックします。

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

Cisco Intersight

デバイスの要求解除

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

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

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

Cisco Intersight の詳細については、「https://www.intersight.com/help/saas/ getting_started/overview」を参照してください。

ヒ

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、クラスタの構成 画面でプロキシを再設定する必要があります。詳細については、「クラスタ構成」を参照してください。

デバイスコネクタの設定

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

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

ここでは、基本的なデバイスコネクタの設定方法について説明します。

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

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

    b. **[**アクセス モード（**Access Mode**）**]** 領域で、

このデバイスに変更を加える機能を Intersight に許可するかどうかを決定します。

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

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

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

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

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

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

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

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

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

ターゲット要求

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

はじめる前に

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。

1. Nexus Dashboard の **[管理コンソール（Admin Console）]** に移動します。
2. 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。
3. デバイスコネクタがすでに設定されているかどうかを確認します。

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

4. 必要に応じて、デバイスコネクタのソフトウェアを更新します。

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

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

5. Nexus Dashboard の **[Intersight]** ページに表示されているデバイス ID と要求コードをメモします。
6. Cisco Intersight クラウドサイト（https://www.Intersight.com）にログインします。
7. Intersight マニュアルの「 ターゲットの要求」セクションに記載されている手順に従って、デバイスを要求します。

   デバイスが Intersight で要求されると、Nexus Dashboard のデバイス コネクタ ページに、インターネットと **Intersight** を接続する緑色の点線と「要求済み」というテキストが表示されます。

   > ヒ 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。

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

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

商標

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

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

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

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

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

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

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

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

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