Cisco Crosswork Infrastructure 4.4 およびアプリケーション アドミニストレーション ガイド

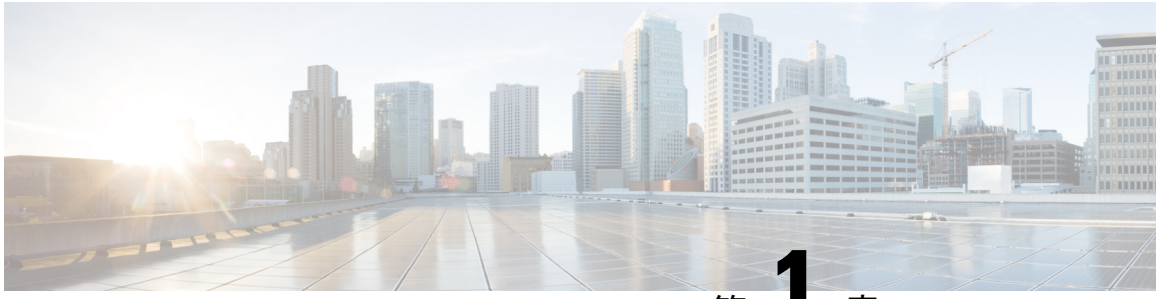
初版：2022 年 10 月 31 日

最終更新：2022 年 11 月 30 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

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

目 次



第 1 章

起動と実行（インストール後）

ここでは、次の内容について説明します。

はじめる前に

Cisco Crosswork アプリケーションの使用を開始する前に、次の基本概念を理解し、計画と情報収集の手順を完了することをお勧めします。

- **ユーザーロール**：シスコでは、ロールベースのアクセス制御を使用して、ユーザーに対してそのユーザーが業務を遂行するために必要なソフトウェア機能のみに限定することをお勧めします。デフォルトでは、作成するすべての新しいユーザーに完全な管理権限が備わります。すべてのユーザに同じ権限を付与する場合を除き、ユーザーロールのシステムを計画し、それらを作成して、作成したユーザープロファイルに割り当てる必要があります。

- **ユーザーアカウント**：ベストプラクティスとして、すべてのユーザーに個別のアカウントを作成し、システム上のユーザーアクティビティの監査レコードを作成することをお勧めします。Crosswork アプリケーションを使用するユーザーのリストを作成します。ユーザー名と予備パスワードを決定し、それらのユーザープロファイルを作成します。Crosswork は、多くの TACACS+ および LDAP サーバーとの統合もサポートしており、ユーザーの役割とアカウントを集中管理できます。詳細については、ユーザー認証の設定（TACACS+ と LDAP） （352 ページ）を参照してください。

- **クレデンシャルプロファイル**：Cisco Crosswork がデバイスにアクセスするか、またはプロバイダと対話するには、クレデンシャルを提示できる必要があります。必要になるたびにクレデンシャルを入力する代わりに、クレデンシャルプロファイルを作成すると、この情報を安全に保存できます。プラットフォームは、アクセスプロトコルのタイプごとに一意のクレデンシャルをサポートし、複数のプロトコルとそれらに対応するクレデンシャルを 1 つのプロファイルにバンドルできます。同じクレデンシャルを使用するデバイスは、クレデンシャルプロファイルを共有できます。たとえば、特定の建物内のすべてのルータが

単一の SSH ユーザー ID とパスワードを共有する場合、Cisco Crosswork がそれらにアクセスして管理できるように単一のクレデンシャルプロファイルを作成できます。

クレデンシャルプロファイルを作成する前に、デバイスをモニターおよび管理するために使用するアクセスクレデンシャルとサポートされているプロトコルを収集する必要があります。デバイスの場合は、ユーザー ID、パスワード、および SNMP v2 の読み取り/書き込みコミュニティ文字列、SNMPv3 認証と権限タイプなどの追加データが含まれます。他のタイプのプロバイダ（NSO、SR-PCE、ストレージ、アラート、およびWAE）の場合、これには常にユーザー ID、パスワード、および接続プロトコルが含まれます。これらを使用してクレデンシャルプロファイルを作成します。

- **タグ**：タグは、デバイスをグループ化するためにデバイスに添付できる単純なテキスト文字列です。Cisco Crosswork には、ネットワークデバイスのグループ化にそのまま使用できるタグの短いリストが付属しています。独自のタグを作成してさまざまな目的でデバイスを識別、検索、およびグループ化することができます。

  システムの設定時に作成するカスタムタグの予備リストを計画しておくことで、最初のオンボーディング時にデバイスをグループ化するために使用できます。最初にタグの完全なリストを用意する必要はありません。後でさらに追加することもできます。ただし、使用する予定のタグはすべて、必要になる前に配置する必要があります。それ以外の場合は、手動で戻って、使用したい場所に追加する必要があります。詳細については、Cisco NSO プロバイダの追加 （157 ページ）を参照してください。

- **プロバイダ**：Cisco Crosswork アプリケーションは、設定変更、セグメントルーティングパスの計算などのさまざまなタスクに関して Cisco Network Services Orchestrator（NSO）や SR-PCE などの外部サービスに依存しています。Crosswork アプリケーション間での情報のアクセスと再利用を管理するには、外部サービスごとにプロバイダ（NSO や SR-PCE など）を設定する必要があります。プロバイダファミリによって、プロバイダが Cisco Crosswork に提供するサービスのタイプと、そのサービスに固有のパラメータが決まります。それらのサービスタイプとパラメータを設定する必要があります。プロバイダの設定に必要なパラメータは、使用する Crosswork アプリケーションによって異なります。プロバイダを設定する前に、各 Crosswork アプリケーションの要件を確認して収集することが重要です。詳細については、「プロバイダファミリについて （153 ページ）」および「プロバイダの依存関係 （153 ページ）」を参照してください。

  - Cisco Network Services Orchestrator（Cisco NSO）は、すべての Cisco Crosswork アプリケーションのインストールで使用されるデフォルトのプロバイダです。そのため、Cisco NSO の IP アドレスまたはホスト名、ポート、およびプロトコル、ならびに通信するために使用するクレデンシャルを収集する必要があります（クレデンシャルプロファイルとし追加する必要があります）。

  - Crosswork 最適化エンジン を使用する場合は、デバイスを検出し、ポリシー設定をデバイスに配布するために、少なくとも Cisco SR-PCE プロバイダを定義する必要があります。使用する自動オンボーディングモードとデバイス クレデンシャル プロファイルを決定する必要があります（デバイスを自動オンボーディングする場合）。詳細については、「Cisco SR-PCE プロバイダの追加 （160 ページ）」を参照してください。

- **デバイス**：UI、CSV ファイル、API、SR-PCE 検出、または ZTP を使用してデバイスをオンボーディングできます。デバイスのオンボーディング方法によって、Crosswork でデバイスを設定するために必要な情報のタイプが決まります。また、Crosswork は NSO にデバイス設定を転送できるため、NSO プロバイダのプロビジョニング方法を変更できます。詳細については、「インベントリへのデバイスの追加（189ページ）」を参照してください。
- **外部データ送信先**：Cisco Crosswork は Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway）のコントローラとして機能します。Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway）に他のデータ送信先にデータを転送させることを計画しているオペレータは、それらの接続先で必要な形式とその他の接続要件を認識しておく必要があります。詳細については、「Cisco Crosswork Data Gateway （27 ページ）」を参照してください。
- **ラベル**：ラベルは、プレイブックを実行できるユーザーを制限するために Crosswork Change Automation で使用されます。たとえば、下位レベルのオペレータがプレイブックのチェックを実行できるようにする一方で、ラベルを使用してネットワークデバイスの設定に変更を加えるようなより複雑なプレイブックまたは影響力のあるプレイブックを実行しないようにします。
- Crosswork Health Insights を使用する場合は、**KPI（主要業績評価指標）プロファイル**を使用してネットワークの正常性をモニターします。ネットワークでのデバイスの使用方法に基づいて、固有のパフォーマンス条件を確立できます。KPI をグループ化して KPI プロファイルを形成することができます。モニターする予定のデータと、Health Insights の設定時に確立するパフォーマンス目標を把握しておくと役立ちます。
- Crosswork Service Health アプリケーションをインストールする場合は、提供されているサンプルを確認して、ネットワーク内のサービスをモニタする方法を決定する必要があります。

デバイス、クレデンシャルプロファイル、タグ、プロバイダリストをスプレッドシート形式でキャプチャし、そのスプレッドシートを CSV 形式に変換してから、使用する Crosswork アプリケーションにインポート機能を使用して一括でアップロードできます。ユーザーインターフェイスで対応する場所にある [インポート（Import）] アイコンをクリックすると、これらのリストそれぞれの CSV テンプレートにアクセスできます。エクスポート先のパスとファイル名を選択するように求められたら、[テンプレートのダウンロード（Download template）] リンクを選択します。

設定のワークフロー

Cisco Crosswork を使用するための最初の手順は、システムを使用できるように準備することです。次の表に、以下の各タスクを実行する際に役立つトピックを示します。

（注） このワークフローは、Cisco Crosswork Data Gateway がすでにインストールされていることを前提としています。インストール手順については、最新バージョンの *Cisco Crosswork Infrastructure 4.4* およびアプリケーション インストール ガイドを参照してください。

「はじめる前に」で説明した推奨される計画手順を実行できた場合は、このワークフローの各手順を完了するために必要なすべての情報が必要です。

表 *1 : Cisco Crosswork* を開始する前に完了すべきタスク

手順	操作
1. デバイスが通信用とテレメトリ用に適切に設定されていることを確認します。	次のガイドラインと設定例を参照してください。 新しいデバイスのテレメトリの前提条件（190ページ） Cisco NSO デバイスの設定例 （191 ページ）
2. （オプション）セットアップが Cisco NSO LSA 展開の場合は、LSA を有効にします。	階層化されたサービスアーキテクチャ（LSA）を有効にする （362 ページ）の手順に従います。
3. クレデンシャルプロファイルを作成します。	クレデンシャルプロファイルの作成 （143ページ）の手順に従います。
4. プロバイダーを追加します。	プロバイダの追加について （154ページ）の手順に従います。
5. プロバイダーとの通信を検証します。	プロバイダの詳細の取得（179ページ）の手順を使用して、プロバイダの到達可能性を確認します。
6. タグをインポートまたは作成します。	タグをインポートするには、タグのインポート （185ページ）の手順を実行します。 タグを作成するには、タグの作成 （184ページ）の手順を実行します。
7. 希望する方法でデバイスをオンボーディングします。	「インベントリへのデバイスの追加 （189ページ）」を参照してください。
8. Crosswork Data Gateway の設定	データを収集するための Crosswork Data Gateway の設定（34 ページ） の手順を実行します。

手順	操作
9. デバイスと Cisco Crosswork の通信を検証します。	[デバイス（Devices）] ウィンドウを確認します（「ネットワーク デバイスの管理（199ページ）」を参照）。オンボーディングしたすべてのデバイスが到達可能である必要があります。 [到達可能性の状態（Reachability State）] が（到達不能）、（低下）、または（不明）としてマークされているデバイスを調査する場合は をクリックします。
10.（オプション）追加のユーザーアカウントとユーザーロールを作成します。	ユーザーの管理（333ページ）とユーザーロールの作成（337ページ）の手順を実行します。
11.（オプション）追加のクレデンシャルプロファイルとプロバイダーをインポートまたは作成します。	プロバイダをインポートするには、プロバイダのインポート（178ページ）の手順を実行します。 プロバイダを作成するには、UI を使用したプロバイダの追加（155ページ）の手順を実行します。
12.（オプション）要件に応じてデバイスを論理的にグループ化します。	デバイスグループの作成と変更（208ページ）の手順を実行します。
13.（オプション）トポロジの表示設定を行います。	マップの表示設定の定義（305ページ）とリンク帯域幅使用率の色分けしきい値の定義（306ページ）の手順を実行します。

ログインとログアウト

Cisco Crosswork のユーザーインターフェイスはブラウザベースです。サポートされているブラウザのバージョンについては、『*Cisco Crosswork Infrastructure 4.4* およびアプリケーション インストールガイド』の最新バージョンを参照してください。

（注） Cisco Crosswork は、ログインプロンプトの失敗が繰り返された後、指定された期間、ユーザーをロックアウトします。待機時間が経過すると、ユーザーは正しいログイン情報でログインを試行することができます。ユーザーは、有効なログイン資格情報を入力するまでロックアウトされたままになります。

ログインの失敗回数とロックアウト時間は、管理者が [ローカルパスワードポリシー（Local Password Policy）] で設定します。詳細については、AAA サーバー設定を設定（356ページ）を参照してください。

ステップ 1 Web ブラウザを開き、次を入力します。

```
https://<Crosswork Management Network Virtual IP (IPv4)>:30603/
```

または

```
https://[<Crosswork Management Network Virtual IP (IPv6)>]:30603/
```

（注） URL の IPv6 アドレスはブラケットで囲む必要があることに注意してください。

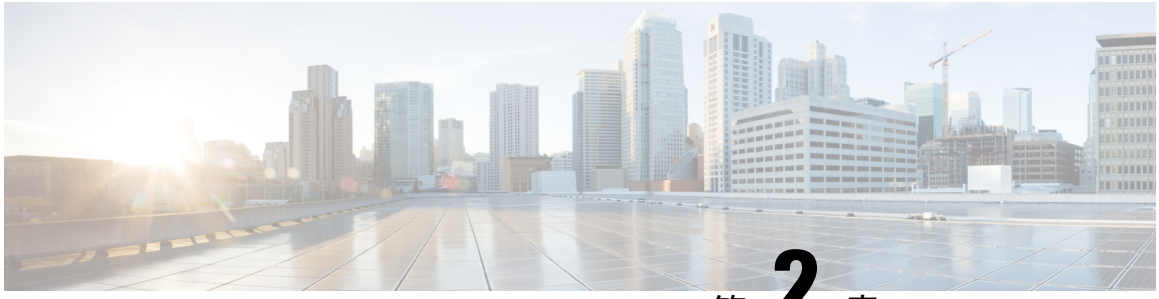
ブラウザから Cisco Crosswork に初めてアクセスした場合、一部のブラウザではサイトが信頼できないという警告が表示されます。この場合は、指示に従ってセキュリティ例外を追加し、サーバーから自己署名証明書をダウンロードします。これを実行すると、ブラウザはその後のすべてのログインで信頼できるサイトとして Cisco Crosswork サーバーを受け入れます。

ステップ 2 Cisco Crosswork のブラウザベースのユーザーインターフェイスにログインウィンドウが表示されます。ユーザー名とパスワードを入力します。

（注） デフォルトの管理者ユーザー名とパスワードは**admin**です。このアカウントは、インストール時に自動的に作成されます（「インストール時に作成された管理ユーザー （334 ページ）」を参照）。このアカウントの初期パスワードは、インストールの検証時に変更する必要があります。シスコでは、デフォルトの管理者クレデンシャルを安全に保管し、通常のログインには使用しないことを強くお勧めしています。代わりに、適切な権限を持つ新しいユーザーロールを作成し、それらのロールに新しいユーザーを割り当てます。作成するユーザーの 1 人以上に「管理者」ロールを割り当てる必要があります。

ステップ 3 [ログイン（Log In）] をクリックします。

ステップ 4 ログアウトするには、メインウィンドウの右上にある をクリックし、[ログアウト（Log out）] を選択します。



第 2 章

Crosswork クラスタの管理

ここでは、次の内容について説明します。

クラスタ管理の概要

Cisco Crosswork プラットフォームはクラスタアーキテクチャを使用します。クラスタは、ノードと呼ばれる仮想マシン（VM）ホストの統合グループにプラットフォームサービスを分散します。基盤となるソフトウェアアーキテクチャは、処理負荷とトラフィック負荷をノード間で自動的かつ動的に分散します。このアーキテクチャにより、Cisco Crosswork はシステムの実際の使用方法に対応し、スケーラブルで可用性の高い拡張可能な方法で実行できます。

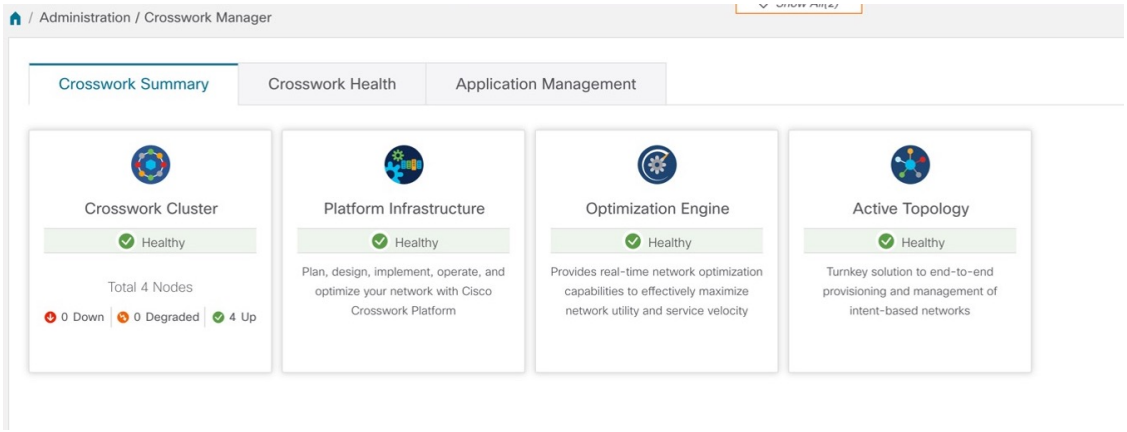
4.1 リリースでは、1 つのクラスタは 3 つ以上のノードで構成され、すべてがハイブリッド設定で動作します。これら 3 つのハイブリッドノードは、すべての Cisco Crosswork の展開に必須です。より厳しいスケール要件がある場合は、最大 3 つのワーカーノードを追加できます。詳細については、新しいクラスタノードの展開 （11 ページ）を参照してください。

管理者ロールに割り当てられたユーザーは、すべてのクラスタ設定およびモニターリング機能にフルアクセスできます。

クラスタの正常性の確認

[Crosswork Manager] ウィンドウを使用して、クラスタの状態を確認します。このウィンドウを表示するには、メインメニューから、**[管理（Administration）]** > **[Crosswork Manager]** を選択します。

図 *1 : [Crosswork Manager]* ウィンドウ

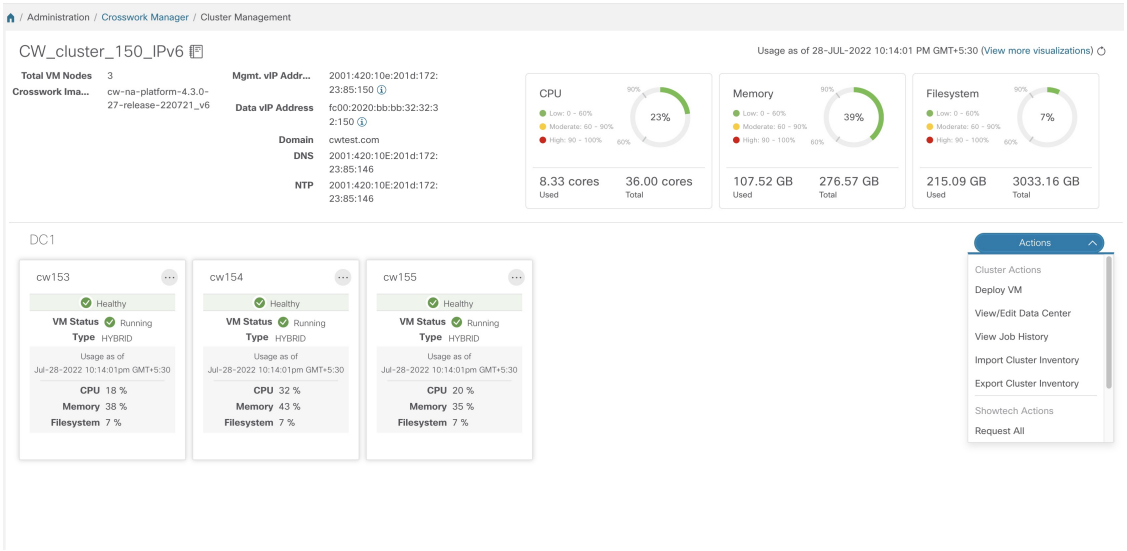


[Crosswork Manager] ウィンドウには、クラスタノードのステータス、プラットフォーム インフラストラクチャ、およびインストールしたアプリケーションに関する概要情報が表示されます。

クラスタの管理

クラスタ内のノードの詳細については、[Crosswork の概要（Crosswork Summary）] タブで、[Crosswork クラスタ（Crosswork Cluster）] タイルをクリックします。Cisco Crosswork には、次の図に示すような [クラスタ管理（Cluster Management）] ウィンドウが表示されます。

図 *2 : [*クラスタ管理（***Cluster Management***）*]* ウィンドウ



注目 手動インストールの場合、クラスタ管理ウィンドウにインベントリの詳細が正しく表示されないことがあります。このような場合、クラスタインベントリのインポート （10 ページ） で説明されているように、クラスタ インベントリ ファイルを手動でインポートする必要があります。

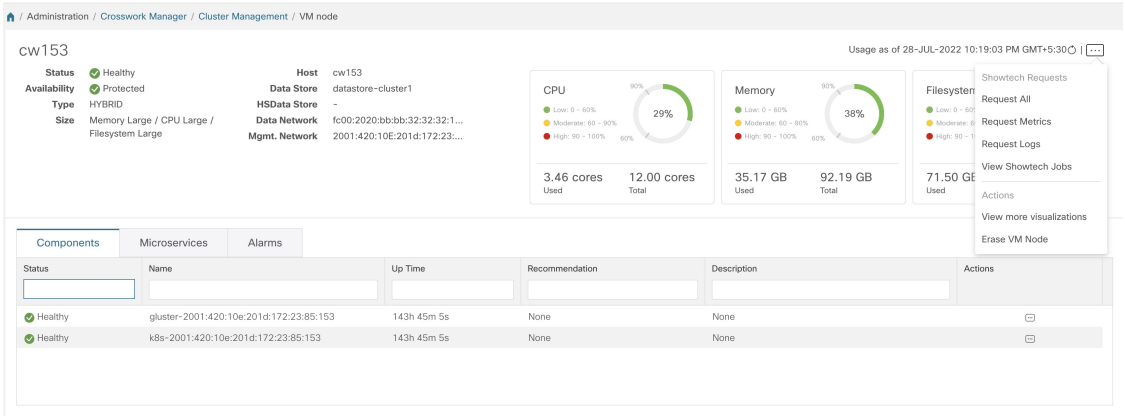
ウィンドウの上部には、クラスタが使用しているリソースの合計が表示されます。下部のセクションには、ノードごとのリソース使用率が表示され、ノードごとに個別の詳細タイルが表示されます。ウィンドウには、使用中の IP アドレス、各ノードがハイブリッドかワーカーかなど、その他の詳細が表示されます。

システム機能をリアルタイムで視覚的にモニター （370 ページ） への [その他の可視化の表示（View more Visualizations）] リンクをクリックします。

VM ノードの詳細

1 つのノードの詳細を表示するには、ノードのタイルで ⋯ をクリックし、[詳細の表示（View Details）] を選択します。[VM ノード（VM Node）] ウィンドウに、ノードの詳細と、ノードで実行されているマイクロサービスのリストが表示されます。

図 *3 : [*クラスタ管理（***Cluster Management***）*]*ウィンドウ



マイクロサービスを再起動するには、[アクション（Action）] で をクリックし、[再起動（Restart）] を選択します。

[Crosswork Health] タブの使用方法については、「プラットフォーム インフラストラクチャとアプリケーション正常性のモニター （368 ページ）」を参照してください。

クラスタインベントリのインポート

vCenter UI を使用して手動でクラスタをインストールした場合（クラスタインストーラツールを使用せずに）、インベントリファイル（.tfvars ファイル）を Cisco Crosswork にインポートして、クラスタの詳細を反映する必要があります。インベントリファイルには、クラスタ内の VM に関する情報と、データセンターのパラメータが含まれています。この操作が完了するまで、Crosswork はクラスタ内の VM ノードを展開または削除できません。

（注） クラスタインベントリファイルを手動でインポートするときは、「*VM_State*」パラメータのコメントを外してください。これを行わないと、VM が機能するようになった後でも、VM のステータスが誤って「初期化中」と表示されます。

ステップ 1 メインメニューから、**[管理（Administration）] > [Crosswork Manager]** を選択します。

ステップ 2 [Crosswork の概要（Crosswork Summary）] タブで、[Crosswork クラスタ（Crosswork Cluster）] タイルをクリックして、[クラスタ管理（Cluster Management）] ウィンドウを表示します。

ステップ 3 **[アクション（Actions）] > [クラスタインベントリのインポート（Import Cluster Inventory）]** を選択して、**[クラスタインベントリのインポート（Import Cluster Inventory）]** ダイアログボックスを表示します。

ステップ 4 （オプション）[サンプルテンプレートファイルのダウンロード（Download sample template file）] をクリックしてテンプレートをダウンロードして編集します。

ステップ 5 **[参照（Browse）]** をクリックし、クラスタ インベントリ ファイルを選択します。

ステップ 6 [インポート（Import）] をクリックして操作を完了します。

新しいクラスタノードの展開

Cisco Crosswork クラスタが形成された後、要件を満たすために追加のノードが必要になる場合があります。次の手順は、新しい VM ノードを展開する方法を示しています。

（注） **Crosswork Summary** ウィンドウと **Cluster Management** ウィンドウには、クラスタに関する情報が表示されます。両方のウィンドウに同じクラスタのステータスが表示されますが、表示がわずかに一致しない場合があります。これは、**Crosswork Summary** ウィンドウに Kubernetes に基づいたノードステータスが表示されるのに対し、**Cluster Management** ウィンドウではデータセンターのノードステータスも考慮されるためです。

この不一致の例は、データセンターのリソースが不足しているために、Crosswork UI でワーカーノードの展開が失敗した場合です。この場合、障害が発生したワーカーノードのステータスは [クラスタ管理（Cluster Management）] ウィンドウに「劣化」と表示され、同じステータスが [Crossworkの概要（Crosswork Summary）] ウィンドウに「ダウン」と表示されます。

始める前に

開始する前に、次のことを確認してください。

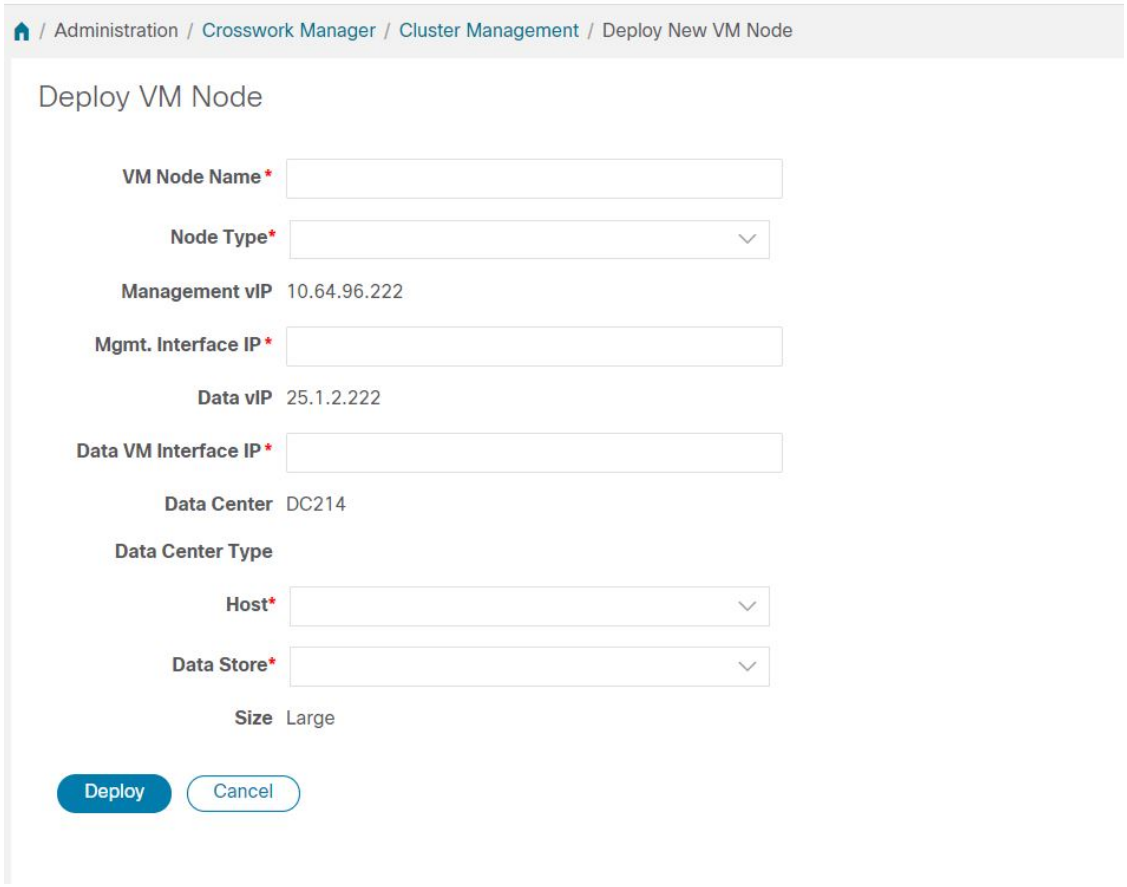
- 管理 IP アドレスなどの Cisco Crosswork ネットワーク設定の詳細。
- データストアやデータ VM インターフェイスの IP アドレスなど、新しいノードを展開する VMware ホストの詳細。
- 追加するノードのタイプ。クラスタには、3つ以上のハイブリッドノードと最大3つのワーカーノードを設定できます。
- クラスタを手動でインストールした場合は、新しいノードを展開する前に、クラスタインベントリ ファイルを Cisco Crosswork にインポートする必要があります。詳細については、クラスタインベントリのインポート（10ページ）を参照してください。[VMの展開（Deploy VM）] オプションは、インポート操作が完了するまで無効になります。

ステップ 1 メインメニューから、**[管理（Administration）]** > **[Crosswork Manager]** を選択します。

ステップ 2 [Crosswork の概要（Crosswork Summary）] タブで、[Crosswork クラスタ（Crosswork Cluster）] タイルをクリックして、[クラスタ管理（Cluster Management）] ウィンドウを表示します。

ステップ 3 **[アクション（Actions）]** > **[VM の展開（Deploy VM）]** を選択して、[新しい VM ノードの展開（Deploy New VM Node）] ウィンドウを表示します。

図 *4 : [VM* ノードの展開（***Deploy VM Node***）*]* ウィンドウ



ステップ 4 表示されたフィールドに関連する値を入力します。

ステップ 5 [展開（Deploy）] をクリックします。システムが VMware の新しいノードのプロビジョニングを開始します。Cisco Crosswork によって、[Crosswork Manager] ウィンドウに新しいノードのタイルが追加されます。タイルには、展開の進行状況が表示されます。

[クラスタ管理（Cluster Management）]>[アクション（Actions）]>[ジョブ履歴の表示（View Job History）] を選択するか、または VMware のユーザーインターフェイスからノードの展開ステータスをモニターできます。

Cisco Crosswork API を使用して VM ノードを追加した場合は、新しく追加された VM ノードタイルで をクリックし、[展開（Deploy）] を選択して操作を完了します。

データセンターのクレデンシャルの表示および編集

このセクションでは、Cisco Crosswork が展開されているデータセンター（VMware vCenter など）のログイン情報を表示および編集する手順について説明します。

ステップ 1 メインメニューから、**[管理（Administration）] > [Crosswork Manager]** を選択します。

ステップ 2 [Crosswork の概要（Crosswork Summary）] タブで、[Crosswork クラスタ（Crosswork Cluster）] タイルをクリックして、[クラスタ管理（Cluster Management）] ウィンドウを表示します。

ステップ 3 **[アクション（Actions）] > [データセンターの表示/編集（View/Edit Data Center）]** を選択して、[データセンターの編集（Edit Data Center）] ウィンドウを表示します。

[データセンターの編集（Edit Data Center）] ウィンドウに、データセンターの詳細が表示されます。

ステップ 4 [データセンターの編集（Edit Data Center）] ウィンドウを使用して、[アクセス（Access）] フィールドに値を入力します（アドレス、ユーザー名、パスワード）。

ステップ 5 [保存（Save）] をクリックして、データセンター クレデンシャルの変更を保存します。

クラスタジョブ履歴の表示

[ジョブ履歴（Job History）] ウィンドウを使用して、VM の展開やクラスタインベントリのインポートなど、クラスタジョブのステータスを追跡します。

ステップ 1 メインメニューから、**[管理（Administration）] > [Crosswork Manager]** を選択します。

ステップ 2 [Crosswork の概要（Crosswork Summary）] タブで、[Crosswork クラスタ（Crosswork Cluster）] タイルをクリックして、[クラスタ管理（Cluster Management）] ウィンドウを表示します。

ステップ 3 **[アクション（Actions）] > [ジョブ履歴の表示（View Job History）]** を選択します。

[ジョブ履歴（Job History）] ウィンドウに、クラスタジョブのリストが表示されます。[ステータス（Status）]、[ジョブ ID（Job ID）]、[VM ID]、[アクション（Action）]、および [ユーザー（Users）] のフィールドを使用して、[ジョブ（Jobs）] リストをフィルタまたはソートできます。

ステップ 4 いずれかのジョブをクリックすると、右側の [ジョブの詳細（Job Details）] パネルに表示されます。

クラスタインベントリのエクスポート

クラスタ インベントリ ファイルを使用して、Cisco Crosswork クラスタをモニターおよび管理します。

ステップ 1 メインメニューから、**[管理（Administration）] > [Crosswork Manager]** を選択します。

ステップ 2 [Crosswork の概要（Crosswork Summary）] タブで、[Crosswork クラスタ（Crosswork Cluster）] タイルをクリックして、[クラスタ管理（Cluster Management）] ウィンドウを表示します。

ステップ 3 **[アクション（Actions）] > [クラスタインベントリのエクスポート（Export Cluster Inventory）]**を選択します。

Cisco Crosswork により、クラスタインベントリ gzip ファイルがローカルディレクトリにダウンロードされます。

クラスタログとメトリックの収集

管理者は、各クラスタコンポーネントの定期的なログとメトリックを収集することで、Cisco Crosswork クラスタのコンポーネントをモニターまたは監査できます。これらのコンポーネントには、クラスタ全体、クラスタ内の個々のノード、および各ノードで実行されているマイクロサービスが含まれます。

Cisco Crosswork は次の showtech オプションを使用してログとメトリックを提供します。

- [すべて要求（Request All）]：ログとメトリックの両方を収集します。
- [メトリックの要求（Request Metrics）]：メトリックのみを収集します。
- [ログの収集（Collect Logs）]：ログのみを収集します。
- [Showtech ジョブの表示（View Showtech Jobs）]：すべての showtech ジョブを表示します。

（注） Showtech ログは、アプリケーションごとに個別に収集する必要があります。

ステップ 1 メインメニューから、**[管理（Administration）] > [Crosswork Manager]** を選択します。

ステップ 2 [Crosswork の概要（Crosswork Summary）] タブで、[Crosswork クラスタ（Crosswork Cluster）] タイルをクリックして、[クラスタ管理（Cluster Management）] ウィンドウを表示します。

ステップ 3 クラスタのログとメトリックを収集するには、[アクション（Actions）] をクリックし、実行する showtech オプションを選択します。

ステップ 4 クラスタ内の任意のノードのログとメトリックを収集するには、次の手順を実行します。

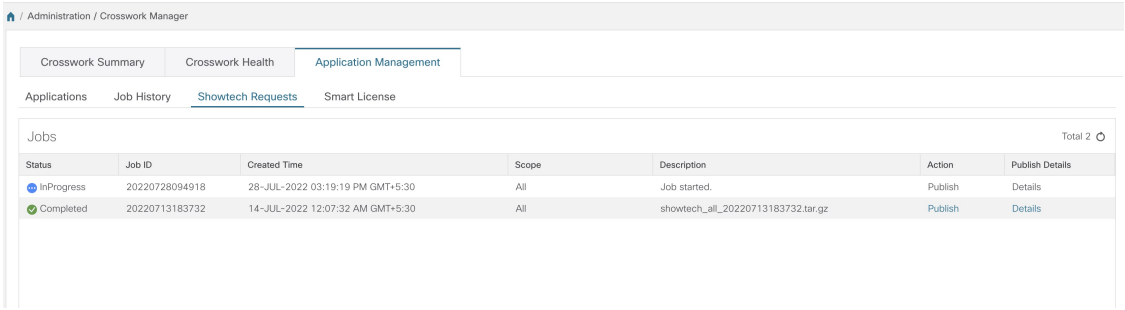
a) ノードタイルをクリックします。

b) [Showtech オプション（Showtech Options）] をクリックし、実行する操作を選択します。

ステップ 5 VM ノードで実行されている個々のマイクロサービスのログとメトリックを収集するには、[アクション（Actions）] 列の下にある をクリックします。次に、実行する showtech オプションを選択します。

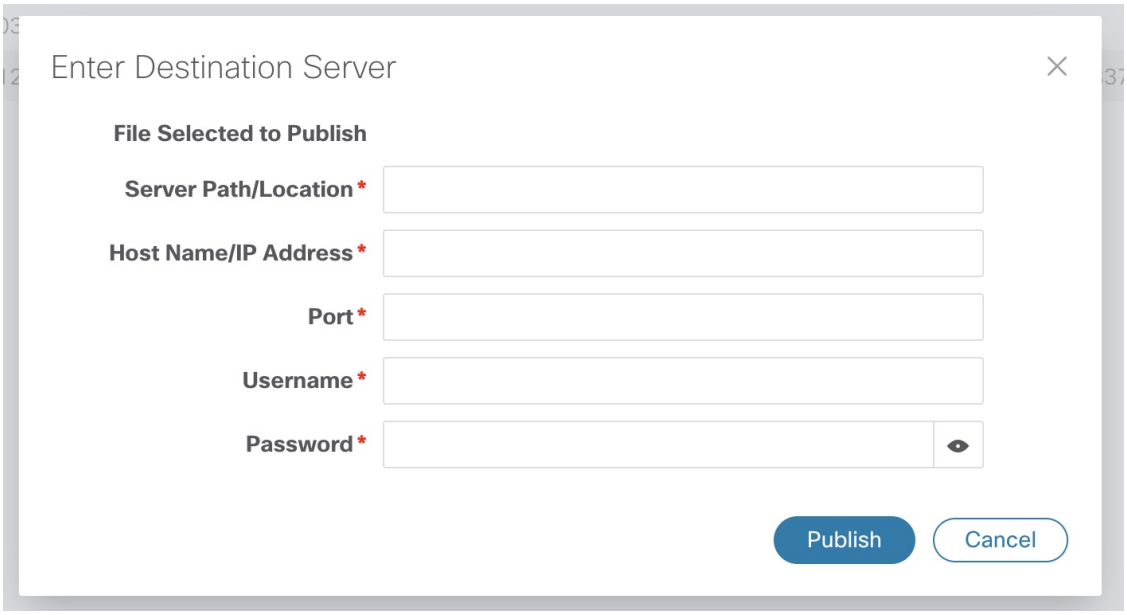
ステップ 6 （オプション）[Showtechジョブの表示（View Showtech Jobs）] をクリックします。[Showtech 要求（Showtech Requests）] ウィンドウに、showtech ジョブの詳細が表示されます。

図 *5 : Showtech* リクエストウィンドウ



ステップ 7 （オプション）[公開（Publish）] をクリックして、showtech ログを公開します。[宛先サーバーの入力（Enter Destination Server）] ダイアログボックスが表示されます。関連する詳細を入力し、[公開（Publish）] をクリックします。

図 *6 : Showtech* リクエストウィンドウ



[詳細（Details）] をクリックして、showtech ログの公開の詳細を表示します。

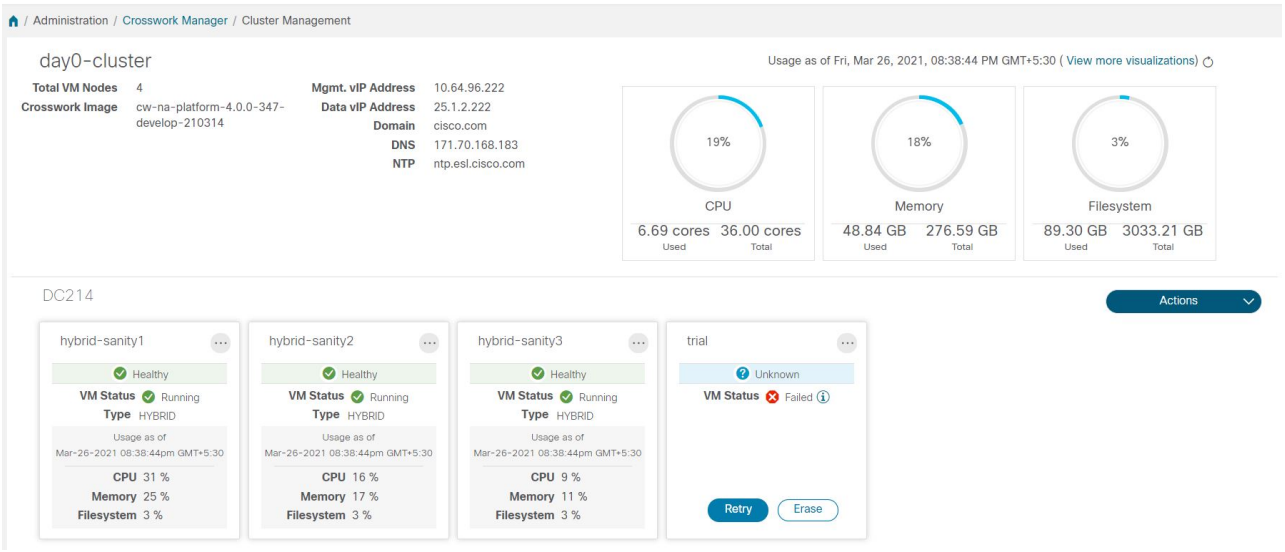
失敗したノードの再試行

情報が正しくないノードの展開は失敗する可能性があります。正しい詳細を入力した後、展開を再試行できます。

ステップ 1 メインメニューから、**[管理（Administration）] > [Crosswork Manager]** を選択します。

ステップ 2 [Crosswork の概要（Crosswork Summary）] タブで、[Crosswork クラスタ（Crosswork Cluster）] タイルをクリックして、[クラスタ管理（Cluster Management）] ウィンドウを表示します。

図 7: [クラスタ管理（*Cluster Management*）] ウィンドウ：*VM* 展開の失敗



ステップ 3 失敗したノードのタイルで [再試行（Retry）] をクリックして、[新しい VM ノードの展開（Deploy New VM Node）] ウィンドウを表示します。

ステップ 4 表示されたフィールドに修正した情報を入力します。

ステップ 5 [展開（Deploy）] をクリックします。

ノードの消去

管理者は、**障害が発生した**ノードまたは**正常な**ノードを Cisco Crosswork クラスタから消去（削除）できます。ノードを消去すると、Cisco Crosswork クラスタからノード参照が削除され、ホスト VM から削除されます。

ノードを消去する手順は、ハイブリッドノードとワーカーノードで同じです。ただし、消去の回数とタイミングはそれぞれ異なります。

- システムは、3 つの動作可能なハイブリッドノードを常に維持する必要があります。3 つのハイブリッドノードの 1 つに障害が発生した場合、システムは機能しますが、可用性の観点からは低下します。このような場合、障害のあるノードは削除され、新しいハイブリッドノードを展開して置き換える必要があります。
- 1 ー 3 つのワーカーノードを設定できます。すべてを問題なく消去できますが、一度に 1 つずつ消去して置換することをお勧めします。

- 1 つ以上のワーカーノードとアプリケーションが存在していて、1 つのハイブリッドノードに障害が発生した場合は、クラスタシステムのリカバリ （19 ページ）で説明している「システムのクリーン再起動」の手順を試行します。

  複数のハイブリッドノードに障害がある場合は、クラスタシステムのリカバリ （19 ページ）で説明している「再展開とリカバリ」の手順に従ってください。

- これらの手順を実行しても問題が解決しない場合は、シスコ カスタマー エクスペリエンス チームにお問い合わせください。

警告

- ノードの消去は中断を伴うアクションであり、アクションが完了するまで一部のプロセスをブロックする可能性があります。中断を最小限に抑えるには、メンテナンス時間帯にのみこのアクティビティを実行してください。
- ワーカーノードとハイブリッドノードを削除すると、残りのノードに余分なワークロードがかかり、システムパフォーマンスに影響する可能性があります。ノードを削除する前に、シスコ カスタマー エクスペリエンス チームにお問い合わせください。
- ハイブリッドノードまたはワーカーノードの削除中に、`cw-ui` ポッドが新しいノードに再配置されるため、Cisco Crosswork UI が 1 ー 2 分間到達不能になることがあります。

（注） 手動のクラスタインストールの場合、Crosswork UI から VM を消去してから、データセンター（vCenter など）から VM を削除する必要があります。

ステップ 1 メインメニューから、**[管理（Administration）]** > **[Crosswork Manager]** を選択します。

ステップ 2 [Crosswork の概要（Crosswork Summary）] タブで、[Crosswork クラスタ（Crosswork Cluster）] タイルをクリックして、[クラスタ管理（Cluster Management）] ウィンドウを表示します。

ステップ 3 削除するノードのタイルで、 … をクリックし、[消去（Erase）] を選択して [VMノードの消去（Erase VM Node）] ダイアログボックスを表示します。

ステップ 4 再度 **[削除（Erase）]** をクリックして、アクションを確認します。

（注） 削除されたノードは、履歴データのみのエントリとして Grafana ダッシュボードに引き続き表示されます。

メンテナンスモード設定の管理

メンテナンスモードは、Crosswork システムを一時的にシャットダウンする手段を提供します。メンテナンスモードを正常にシャットダウンします。Crosswork は、シャットダウン前にすべてのアプリケーションデータを同期します。

システムがメンテナンスモードになり、シャットダウン後に再起動するまでに数分かかることがあります。その間は、他のユーザーはログインしたり、Crosswork アプリケーションを使用しないでください。

始める前に

システムをメンテナンスモードにする予定があることを他のユーザーに通知し、ログアウトの期限を示します。メンテナンスモードの操作は、一度開始するとキャンセルできません。

ステップ 1 Crosswork をメンテナンスモードにするには、次の手順を実行します。

a) メインメニューから、**[管理（Administration）]** > **[設定（Settings）]** > **[システム設定（System Settings）]** > **[メンテナンスモード（Maintenance Mode）]** を選択します。

b) [メンテナンス（Maintenance）] スライダを右または [オン（On）] の位置にドラッグします。

c) シャットダウンを開始しようとしていることが Crosswork によって警告されます。[続行（Continue）] をクリックして選択内容を確認します。

システムがメンテナンスモードになるまでに数分かかる場合があります。その間は、他のユーザーはログインしたり、Crosswork アプリケーションを使用しないでください。

（注） クラスタを再起動する場合は、システムがメンテナンスモードになった後、Cisco Crosswork データベースが同期できるように 5 分間待ってから続行します。

ステップ 2 メンテナンスモードから Crosswork を再起動するには、次の手順を実行します。

a) メインメニューから、**[管理（Administration）]** > **[設定（Settings）]** > **[システム設定（System Settings）]** > **[メンテナンスモード（Maintenance Mode）]** を選択します。

b) [メンテナンス（Maintenance）] スライダを左または [オフ（Off）] の位置にドラッグします。

システムの再起動には数分かかる場合があります。その間は、他のユーザーはログインしたり、Crosswork アプリケーションを使用しないでください。

（注） 以前にシステムをメンテナンスモードにしたときに再起動または復元を実行した場合、システムはメンテナンスモードで起動し、ポップアップウィンドウでメンテナンスモードをオフにするように求められます。プロンプトが表示されない場合（メンテナンスモード中にシステムが再起動した場合でも）、アプリケーションが正常に機能するように、メンテナンスモードのオンとオフを切り替える必要があります。

クラスタシステムのリカバリ

システムリカバリが必要な場合

注意 このトピックで説明されている方法は、3 つのハイブリッド VM ノードのみ（およびワーカーノードなし）で構成されるクラスタプロファイルを使用すると失敗する可能性があります。この障害は、ワーカーノードがないために VM の回復力が不足しているために発生します。

Cisco Crosswork クラスタの通常の操作中に、システム全体を回復する必要がある場合があります。これは、1 つ以上のノードの誤動作、1 つ以上のサービスまたはアプリケーションの誤動作、またはクラスタ全体のホストを破壊する災害の結果である可能性があります。

機能クラスタには、3 つ以上のハイブリッドノードが必要です。これらのハイブリッドノードは、コア Cisco Crosswork の管理、オーケストレーション、およびインフラストラクチャ サービスによって課される処理およびトラフィック負荷を共有します。ハイブリッドノードは可用性が高く、処理負荷をノード間とワーカーノードに自動的に再分散することができます。

クラスタは、1 つのハイブリッドノードの再起動（グレースフルまたはアングレースフル）を許容できます。ハイブリッドノードの再起動中もシステムは機能しますが、可用性の観点からは低下します。システムは、ワーカーノードにかなり多数の障害が発生しても許容できますが、ワーカーノードが復元されるまで、システムの可用性は低下します。

Cisco Crosswork は、ノード、アプリケーション、またはサービスが誤動作するとアラームを生成します。システム障害が発生している場合は、まずアラームを調べます。次に、アラームで識別された個々のノード、アプリケーション、またはサービスの正常性を確認します。クラスタの正常性の確認 （8 ページ）に記載されている機能を使用して、問題の発生源をドリルダウンし、サービス障害であることが判明した場合は、問題のあるサービスを再起動できます。

1 つのハイブリッドノードに障害が発生したことを示すか、または 1 つのハイブリッドノードと 1 つ以上のワーカーノードに障害が発生したことを示すアラームが表示された場合は、障害が発生したノードの再起動または交換（消去してから再度追加）を試します。それでも問題が解決しない場合は、システムのクリーンリブートを実行することを検討してください。

2 つ以上のハイブリッドノードの損失は二重障害になります。障害が発生したハイブリッドノードを交換または再起動しても、システムが正しく回復する保証はありません。また、システム全体が劣化し、思わしくない状態になっている場合もあります。このような状態の場合は、新しいクラスタを展開した後、古いクラスタから取得した最新のバックアップを使用してシステム全体を回復できます。

重要

- Crosswork ネットワーク コントローラー ソリューションを実行している 3 VM クラスタでは、VM のシャットダウンはサポートされていません。VM に障害が発生した場合、残りの 2 つの VM は、障害が発生した VM から移行されるすべてのポッドをサポートできません。VM のシャットダウンを有効にするには、追加のワーカーノードを展開する必要があります。
- いずれかの VM の再起動は、3 VM クラスタでサポートされています。再起動の場合、VM の復元には 5 分（再起動された VM で `orch pod` が実行されていない場合）から最大 25 分（再起動された VM で `orch pod` が実行されている場合）かかることがあります。

次の 2 つの項では、それぞれの場合に実行する手順について説明します。

システムのクリーンリブート（VMware）

システムのクリーンリブートを実行するには、次の手順を実行します。

1. Crosswork をメンテナンスモードにします。詳細については、メンテナンスモード設定の管理 （18 ページ）を参照してください。
2. 各ノードをホストしている VM の電源を切ります。
   1. VMware vSphere Web クライアントにログインします。
   2. [ナビゲータ（Navigator）] ペインで、シャットダウンする VM を右クリックします。
   3. **[電源（Power）] > [電源オフ（Power Off）]** を選択します。
   4. VM のステータスが [オフ（Off）] に変わるまで待ちます。
3. 残りのすべての VM が確実にシャットダウンするまで、手順 2 を各 VM に繰り返します。
4. 最初のハイブリッドノードをホストする VM の電源を入れます。
   1. [ナビゲータ（Navigator）] ペインで、電源をオンにする VM を右クリックします。
   2. **[電源（Power）] > [電源オン（Power Up）]** を選択します。
   3. VM のステータスが [オン（On）] に変わるまで待ち、さらに 30 秒待ってから続行します。
5. 残りの各ハイブリッドノードに対して手順 4 を繰り返し、再起動を 30 秒ずらして続行します。その後、各ワーカーノードで続行し、再起動を 30 秒ずらします。
6. すべての VM の電源がオンになるまでにかかる時間は、ハードウェアのパフォーマンス特性によって異なります。すべての VM の電源を入れたら、数分待ってから Crosswork にログインします。
7. Crosswork をメンテナンスモードから移動します。詳細については、メンテナンスモード設定の管理 （18 ページ）を参照してください。

（注） Crosswork クラスタが正常な状態でない場合、メンテナンスモードを強制しようとすると失敗する可能性があります。試行が成功したにもかかわらず、アプリケーションの同期の問題が引き続き発生する可能性があります。このような場合、失敗したサービスのリストと失敗の理由を示すアラームが生成されます。このシナリオに直面した場合でも、以下で説明する「再展開と復元」の方法を続行できます。

再展開と復元（VMware）

バックアップからシステムを再展開して回復するには、次の手順を実行します。この方法では、リカバリが必要になる前にシステムのバックアップを定期的に実行していることを前提としています。バックアップの実行方法については、「Cisco Crosswork のバックアップと復元の管理 （123 ページ）」を参照してください。

1. 各ノードをホストしている VM の電源を切ります。
   1. VMware vSphere Web クライアントにログインします。
   2. [ナビゲータ（Navigator）] ペインで、シャットダウンする VM を右クリックします。
   3. **[電源（Power）] > [電源オフ（Power Off）]** を選択します。
   4. VM のステータスが [オフ（Off）] に変わるまで待ちます。
   5. 必要に応じて、クラスタ内の残りのノードでこれらの手順を繰り返します。
2. すべての VM の電源がオフになったら、次の手順を実行して削除します。
   1. VMware vSphere Web クライアントの [ナビゲータ（Navigator）] ペインで、削除する VM を右クリックします。
   2. [ディスクから削除（Delete from Disk）] を選択します。
   3. VM のステータスが [削除済み（Deleted）] に変わるまで待ちます。
   4. 必要に応じて、クラスタ内の残りの VM ノードに対してこれらの手順を繰り返します。
3. 『*Cisco Crosswork Infrastructure 4.4 and Applications Installation Guide*』の説明に従って、新しい Cisco Crosswork クラスタを展開します。
4. 災害後に Cisco Crosswork を復元する （126 ページ）の説明に従って、新しく展開したクラスタのシステム状態を回復します。

クラスタリソースの再調整

クラスタ管理の一環として、Crosswork は各クラスタノードのリソース使用率を常にモニタリングしています。いずれかのノードの CPU 使用率が高くなると（デフォルトでは、「高」範

囲は 90 ～ 100% に設定されています）、Crosswork はアクションを実行するように求める通知をトリガーします。その後、[再調整（Rebalance）] 機能を使用して、クラスター内の既存の VM ノード間でリソースを再割り当てできます。

クラスタ内の他のノードも容量いっぱいに近づいている場合は、リソースの再割り当てを容易にするために、[再調整（Rebalance）] オプションを試す前に新しいワーカーノードを展開することをお勧めします。ワーカーノードの追加の詳細については、「新しいクラスタノードの展開 （11 ページ）」を参照してください。

注意 再調整には 15 分から 30 分かかることがあります。その間、Crosswork アプリケーションは使用できません。一旦開始されると、再調整操作はキャンセルできません。

始める前に

- データの整合性を確保するために、再調整する前に Crosswork をメンテナンスモードにする必要があります。
- 再調整中にログインしたユーザーは、セッションを失います。再調整のためにシステムをメンテナンスモードにすることを事前に他のユーザーに通知し、ログアウトする期限を設けてください。

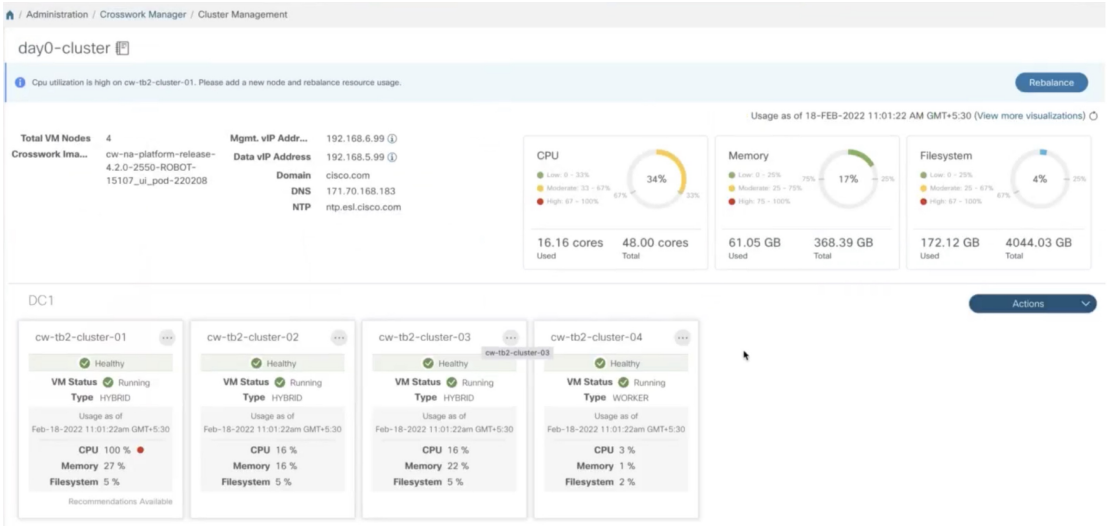
ステップ 1 メインメニューから、**[管理（Administration）] > [Crosswork Manager]** を選択します。

ステップ 2 [Crosswork の概要（Crosswork Summary）] タブで、[Crosswork クラスタ（Crosswork Cluster）] タイルをクリックして、[クラスタ管理（Cluster Management）] ウィンドウを表示します。

この手順では、3 つのハイブリッドノードと 1 つのワーカーノードを持つサンプルクラスタ（**day0-control**）が考慮されています。ハイブリッドノードの 1 つで CPU 使用率が高くなっています（**cw-tb2-cluster-01** で 100%）。詳しくは下の画像をご覧ください。

クラスタ名の下にバナーが表示され、クラスタノードでリソースが過剰に使用されていることを警告し、さらにワーカーノードを追加することを推奨します。

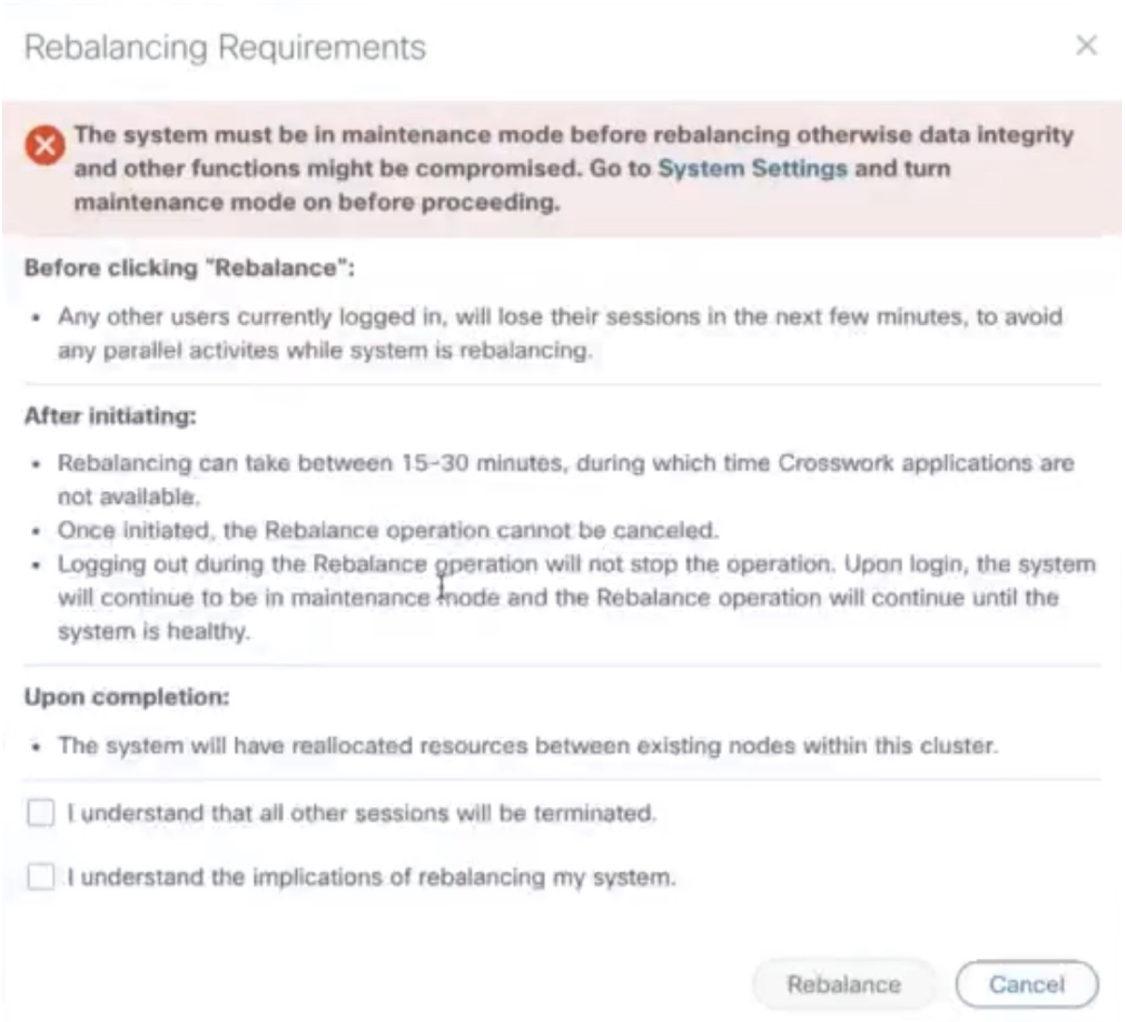
図 *8 :* 再調整通知



ノードのタイルで、 をクリックして [詳細の表示（View Details）] を選択すると、詳細が表示されます。

ステップ 3 [再調整（Rebalance）] をクリックすると、[再調整要件（Rebalance Requirements）] が表示されます。要件を読み、再調整を開始する準備ができたら、2 つのチェックボックスをオンにします。

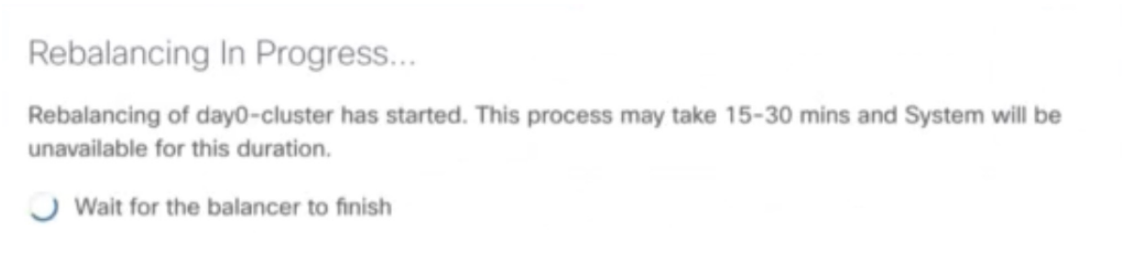
図 *9* : 再調整要件



ステップ 4 [再調整（Rebalance）] をクリックし、プロセスを開始します。Crosswork は、過剰に使用された VM ノードのリソースをクラスタ内の他のノードに再割り当てし始めます。

再調整の状態を示すダイアログボックスが表示されます。プロセスが完了するまでお待ちください。

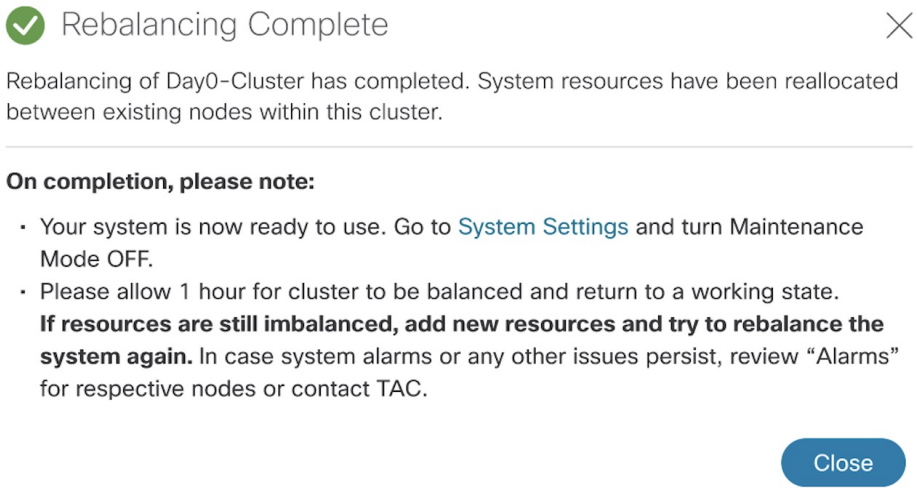
図 *10* : 再調整ステータス



ステップ 5 再調整プロセスが完了すると、次のいずれかの結果シナリオが表示される場合があります。

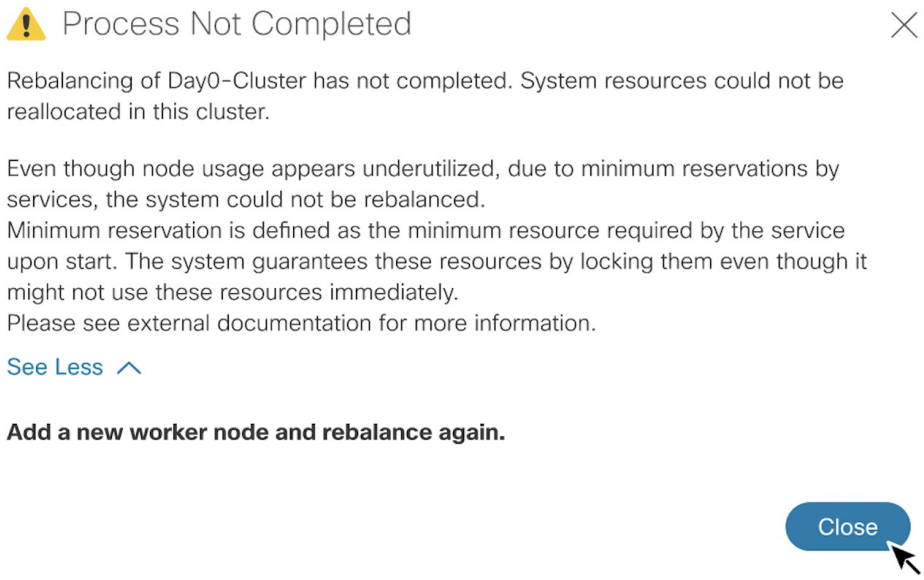
- **成功のシナリオ**：再調整操作が成功したことを示すダイアログボックス。ダイアログボックスの指示に従って続行します。

図 *11*：再調整の結果：成功



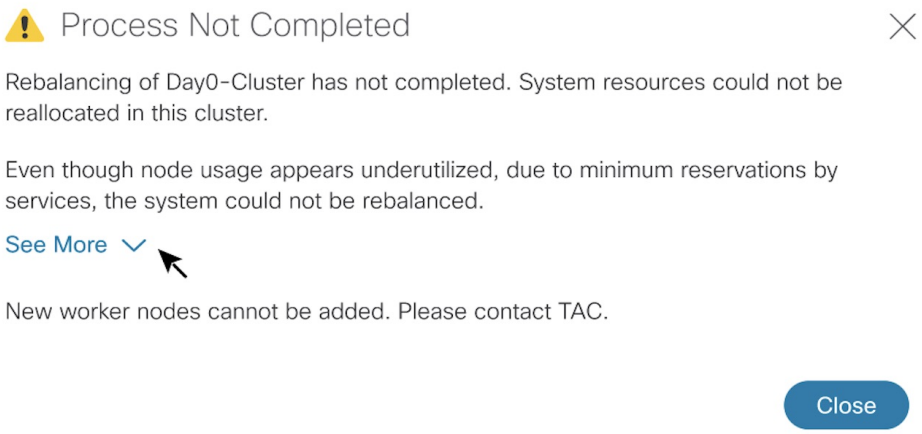
- **障害シナリオ：新しいワーカーノードを追加できるスコープ**：再調整の失敗を示すダイアログボックスが表示されます。この場合、システムは、新しいワーカーノードを追加して再調整プロセスを再試行するように求めます。

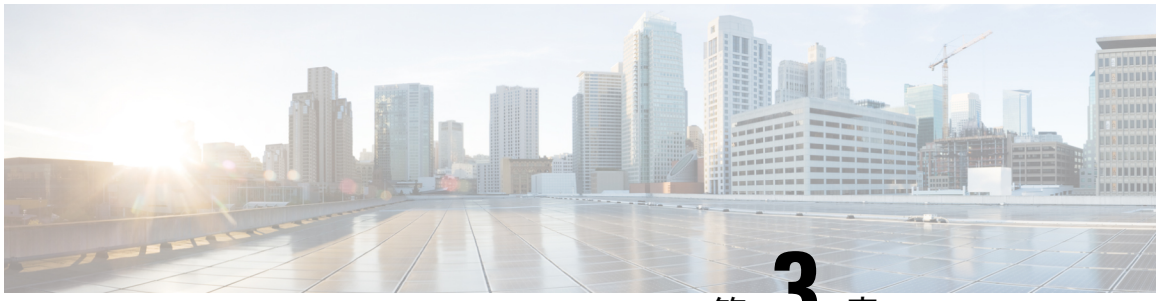
図 *12*：再調整の結果：新しいワーカーノードを追加



- **失敗のシナリオ**：**新しいワーカーノードを追加するスコープがない**：再調整の失敗を示すダイアログボックスが表示されます。この場合、システムは、新しいワーカーノードを追加できないため、TAC に連絡するように求めます。

図 *13*：再調整の結果：新しいワーカーノードを追加





第 3 章

Cisco Crosswork Data Gateway

ここでは、次の内容について説明します。

Cisco Crosswork Data Gateway の概要

Cisco Crosswork Data Gateway は、マルチベンダーデバイスからネットワークデータを収集するためのセキュアな共通の収集プラットフォームです。これは、MDT、SNMP、CLI、gNMI、Syslog、および NETCONF を含む複数のデータ収集プロトコルをサポートするネットワークデバイスの近くに展開される、オンプレミスのアプリケーションです。必要な Cisco Crosswork Data Gateway の数は、サポートされるデバイスの数、処理するデータの量、収集する頻度、およびネットワークアーキテクチャによって異なります。

Crosswork Data Gateway が Cisco Crosswork インフラストラクチャ（このガイドでは Cisco Crosswork とも呼ばれます）とともに展開されている場合、Cisco Crosswork は**コントローラアプリケーション**として機能します。

Crosswork Data Gateway では次の概念を使用します。

- **Crosswork Data Gateway VM**：インストールする Crosswork Data Gateway VM。
- **Crosswork Data Gateway プロファイル**：

  Cisco Crosswork Data Gateway では、オンプレミス展開用に次のプロファイルをサポートされています。各プロファイルの VM の要件については、『*Cisco Crosswork Infrastructure 4.4* およびアプリケーション インストールガイド』の「*Cisco Crosswork* のインストール要件」を参照してください。

  - **On-Premise Standard**：Crosswork Health Insights と Crosswork Service Health（Automated Assurance）を除くすべての Crosswork アプリケーションで使用します。

- **On-Premise Extended**：Crosswork Health Insights と Crosswork Service Health（Automated Assurance）で使用します。

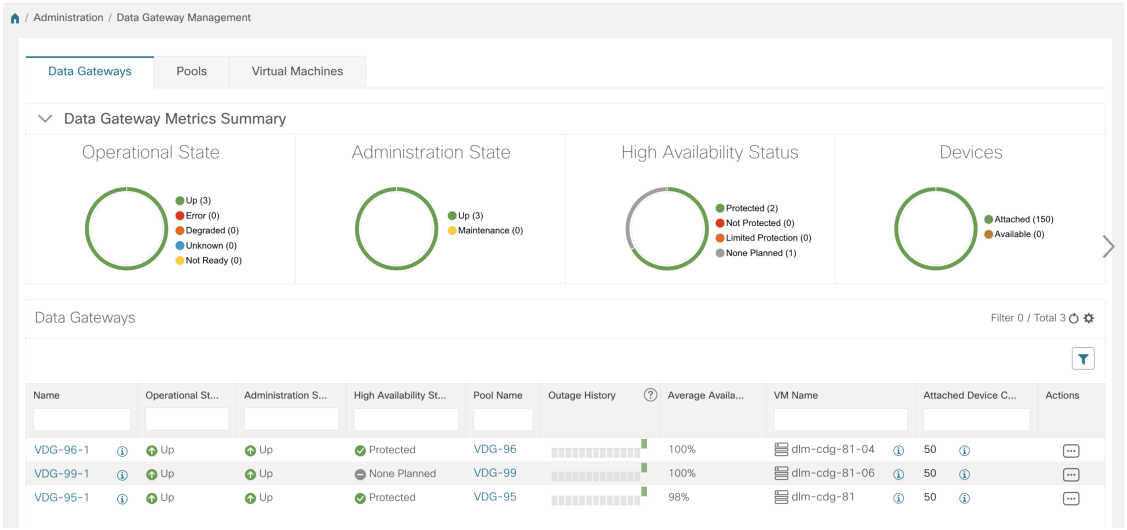
注目 **On-Premise Standard with Extra Resources** プロファイルは、利用制限付きの機能として使用できますが、データセンターに Crosswork Data Gateway を展開している間は使用しないでください。支援が必要な場合は、シスコ カスタマー エクスペリエンス チームにお問い合わせください。

- **Crosswork Data Gateway プール**：高可用性を有効にするオプションを備えた 1 つ以上の Crosswork Data Gateway で構成される論理ユニット。Crosswork Data Gateway VM がダウンすると、Cisco Crosswork は自動的に VM をプールのスペアで置き換えてデバイスを管理し、データ収集の中断を最小限に抑えます。
- **Crosswork Data Gateway**：仮想 IP アドレスが Crosswork Data Gateway プールに追加されたときに割り当てられる Crosswork Data Gateway VM。デバイスの接続または切断、収集ジョブの作成などの操作は、Crosswork Data Gateway で行われます。
- **データ送信先**：Crosswork Data Gateway によって収集されたデータの内部または外部の受信者。デフォルトでは、Cisco Crosswork はデータの接続先として定義されます。その他の接続先（外部ユーザー）は、Cisco Crosswork の UI または API を使用して定義できます。
- **収集ジョブ**：Crosswork Data Gateway がデータを収集するために実行する必要があるタスク。Crosswork アプリケーションは、デバイスの到達可能性を確認し、ネットワークとサービスの正常性を判断するために必要なテレメトリデータを収集する収集ジョブを作成します。Cisco Crosswork の UI と API を使用すると、Crosswork 以外のアプリケーションの収集ジョブを設定できます。
- **カスタム ソフトウェア パッケージ**：デバイスカバレッジを拡張し、現在サポートされていないデバイスからのデータ収集をサポートするためのファイルとデバイスモデルの定義。

（注） この章では、Cisco Crosswork の UI を介してアクセスできる Cisco Crosswork Data Gateway の機能についてのみ説明します。Cisco Crosswork Data Gateway VM のインタラクティブコンソールとその管理方法の詳細については、「**付録 A**：」Crosswork Data Gateway VM の設定 （393 ページ）を参照してください。

Crosswork Data Gateway の UI の概要

Cisco Crosswork Data Gateway の管理ビューを開くには、Cisco Crosswork にログインし、左側のナビゲーションバーから **[管理（Administration）]** > **[Data Gatewayの管理（Data Gateway Management）]** を選択します。



[Data Gateway の管理（Data Gateway Management）] ページには、次の 3 つのタブがあります。

- **Data Gateways**：ネットワーク内の仮想 Cisco Crosswork Data Gateway の詳細を表示します。このタブから Data Gateway にデバイスを接続または切断できます。
- **プール**：Cisco Crosswork Data Gateway プールを管理します。
- **仮想マシン**：物理的な Cisco Crosswork Data Gateway VM を管理します。

次の表では、[Data Gateway の管理（Data Gateway Management）] ページのさまざまなフィールドについて説明します。

表 *2 : Cisco Crosswork Data Gateway の UI*

フィールド	説明
動作状態（**Operational State**）	Cisco Crosswork Data Gateway VM の動作状態。 Crosswork Data Gateway VM の動作状態は次のとおりです。 • [不明（Unknown）]： Crosswork Data Gateway VM の動作状態は、Cisco Crosswork に登録されていますが、まだセッションが確立していないため不明です。 • [低下（Degraded）]： Cisco Crosswork Data Gateway VM は到達可能ですが、1 つ以上のコンポーネントが [OK] 以外の状態です。 • [準備中（Not Ready）]：Cisco Crosswork Data Gateway は Cisco Crosswork に登録されていますが、サウスバウンド仮想 IP アドレスが関連付けられたアクティブなゲートウェイではないため、収集ジョブを受信する準備が整っていません。 • [アップ（Up）]：Cisco Crosswork Data Gateway VM が動作しており、個々のすべてのコンポーネントは「OK」です。 • [エラー（Error）]： Cisco Crosswork Data Gateway VM が到達不能であるか、またはその一部のコンポーネントがエラー状態になっています。

フィールド	説明
管理状態（**Admin State**）	Cisco Crosswork Data Gateway VM の管理状態。 • [アップ（Up）]：VM は管理上、稼働中です。 • [メンテナンス（Maintenance）]：アップグレードやその他のメンテナンスアクティビティ（証明書のアップロードなど）を実行するために、Cisco Crosswork と Cisco Crosswork Data Gateway 間の操作が中断されます。
仮想マシン名（**Virtual Machine Name**）	Cisco Crosswork Data Gateway VM 名前の横にある情報アイコンをクリックすると、各 VM の登録の詳細が表示されます。これには、次が含まれます。 • プール名 • VM 名 • Crosswork Data Gateway のプロファイルを示す VM タイプ。 • 関連する MAC アドレスを持つ管理 IP（eth0） • 関連する MAC アドレスを持つ eth1 IP（ノースバウンド/vNIC1） • MAC アドレスのみを持つ eth2（ノースバウンド/vNIC2） （注） eth2 IP（サウスバウンド IP）は、プールの作成時に Crosswork Data Gateway VM に割り当てられます。したがって、各 VM の登録の詳細の一部としては表示されません。
IPv4 管理 IP アドレス（IPv4 Mgmt.IP Address）	Cisco Crosswork Data Gateway VM の管理 IPv4 アドレス。
IPv6 管理 IP アドレス（IPv6 Mgmt.IP Address）	Cisco Crosswork Data Gateway VM の管理 IPv6 アドレス。

フィールド	説明
ロール（**Role**）	Cisco Crosswork Data Gateway VM のロールを表示します。次のいずれかになります。 • [割り当て済み（Assigned）]：Cisco Crosswork Data Gateway VM がプールに割り当てられている場合。 • [未割り当て（Unassigned）]：どのプールにも Cisco Crosswork Data Gateway VM が割り当てられていない場合。 • [スペア（Spare）]：Cisco Crosswork Data Gateway VM がプールの一部であってもスタンバイモードの場合。 [ロール（Role）] が [未割り当て（Unassigned）] の Cisco Crosswork Data Gateway VM を Crosswork Data Gateway に割り当てる必要があります。
停止履歴（Outage History）	Cisco Crosswork Data Gateway VM の 14 日間の停止履歴。 1 日の状態集約は、[エラー（Error）]、[低下（Degraded）]、[アップ（Up）]、[不明（Unknown）]、[準備中（Not Ready）] の優先順位で実行されます。 たとえば、Crosswork Data Gateway VM が [不明（Unknown）] から [低下（Degraded）] の後、[アップ（Up）] になった場合、当日は [低下（Degraded）] の色（オレンジ）で表示されます。これは、[アップ（Up）] や [不明（不明）] よりも [低下（Degraded）] のほうが優先されるためです。 Crosswork Data Gateway がその日の任意の時点で [エラー（Error）] 状態になった場合、タイルは赤になります。Data Gateway が [エラー（Error）] ではなく、[低下（Degraded）] 状態の場合、そのタイルはオレンジ色になります。DG が [エラー（Error）] または [低下（Degraded）] 状態ではなく、[アップ（Up）] のみであった場合、タイルは緑色です。
プール名（Pool Name）	Crosswork Data Gateway VM が割り当てられている Crosswork Data Gateway のプールの名前。

フィールド	説明
Data Gateway 名（Data Gateway Name）	Crosswork Data Gateway VM をプールに追加するときに自動的に作成される Cisco Crosswork Data Gateway の名前。
高可用性のステータス（High Availability Status）	Crosswork Data Gateway の高可用性のステータスは次のいずれかです。 • [保護（Protected）]：すべての VM が稼働しており、プール内に 1 つ以上のスタンバイがあります。 • [保護なし（Not Protected）]：すべてのスタンバイ VM がダウンしています。 • [限定的な保護（Limited Protection）]：一部のスタンバイ VM がダウンしていますが、1 つ以上のスタンバイ VM が稼働しています。 • [計画なし（None Planned）]：プールの作成時にスタンバイ VM がプールに追加されませんでした。
平均可用性（Average Availability）	Cisco Crosswork Data Gateway VM の正常性を示す値。このパーセンテージは、最初のイベントの開始時刻と最後のイベントの終了時刻の間に、Crosswork Data Gateway が稼働状態であった合計時間（ミリ秒単位）として計算されます。 （注） 最後のイベントの終了時刻は現在のタイムスタンプであるため、最後のイベントの期間は開始時刻と現在のタイムスタンプの間になります。
VM ID	Cisco Crosswork Data Gateway VM の VM ID。
接続デバイス数（Attached Device Count）	Cisco Crosswork Data Gateway のプールに接続されているデバイスの数。
一意の識別子（Unique Identifier）	Cisco Crosswork Data Gateway VM の一意の識別子。

データを収集するための Crosswork Data Gateway の設定

Crosswork Data Gateway では、収集ジョブを実行する前に、まず次の設定タスクを実行する必要があります。

（注） このワークフローは、『*Cisco Crosswork Infrastructure 4.4* およびアプリケーション インストールガイド』で説明されているように、Cisco Crosswork Data Gateway がすでにインストールされていることを前提としています。

次の表の手順 1 から手順 3 までを実行して、Crosswork Data Gateway を設定し、Cisco Crosswork とその他の Crosswork アプリケーションで実行します。手順 4 ー手順 6 はオプションであり、外部のデータ送信先とカスタム収集ジョブを作成してデータを収集および転送する Crosswork Data Gateway の機能を拡張する場合にのみ必要です。

表 *3:* データの収集を目的とした *Cisco Crosswork Data Gateway* の設定を実行するためのタスク

タスク	次の手順を実行します。
1. Crosswork Data Gateway プールを作成します。	Cisco Crosswork Data Gateway プールの作成（36 ページ）
2. デバイスを Crosswork Data Gateway に接続します。	Crosswork Data Gateway へのデバイスの接続（39 ページ）
3. デフォルトの収集ジョブが作成され、正常に実行されていることを確認します。	収集ジョブのモニター （106 ページ）
4. （オプション）デバイスカバレッジを拡張して、現在サポートされていないデバイスまたはサードパーティ製デバイスからデータを収集します。	カスタムデバイスパッケージを管理 （57 ページ）
5. （オプション）データを外部のデータ送信先に転送します。	外部データ送信先の作成と管理 （50 ページ）
6. （オプション）カスタム収集ジョブ（Cisco Crosswork によって作成されたもの以外）を作成します。	Crosswork Data Gateway の収集ジョブの管理（62 ページ）

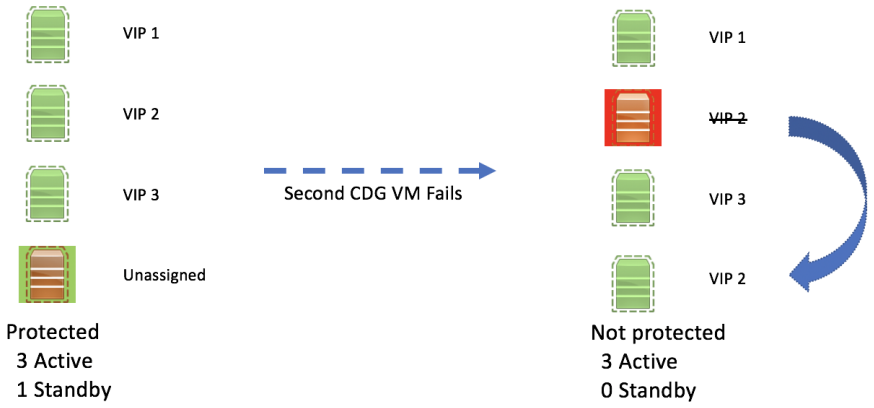
プールによる Crosswork Data Gateway の高可用性

Cisco Crosswork Data Gateway プールによって、デバイスが管理され、最小限の中断で収集が行われます。

プールは、高可用性を有効にするオプションを備えた 1 つ以上の Cisco Crosswork Data Gateway VM で構成できます。

プール内の Crosswork Data Gateway VM がダウンした場合、Cisco Crosswork は自動的にその VM をプール内のスタンバイ VM に置き換えます（フェールオーバー）。[動作状態（Operational state）] が [エラー（Error）] で、[保護されている（Protected）] プールの一部である Crosswork Data Gateway VM は、フェールオーバーに適格です。障害が発生した VM からスタンバイ VM へデバイスと既存の収集ジョブが自動的に割り当てられます。ダウンした VM が動作可能になると、その VM はプール内でスタンバイ VM になります。

図 *14 : Crosswork Data Gateway* の高可用性



（注） プール内の Crosswork Data Gateway の複数の VM に同じサウスバウンド IP アドレスがある場合にスタンバイ Crosswork Data Gateway を再起動すると、そのスタンバイ Crosswork Data Gateway VM の起動後にそのサウスバウンド IP アドレスが失われます。

たとえば、サウスバウンド IP アドレスが IP1 の CDG1（アクティブ）はダウンします。Cisco Crosswork は、CDG1 を新しいアクティブな VM として CDG2（スタンバイ）に置き換え、CDG2 のサウスバウンド IP と同じ IP1 をプログラムします。後で CDG1 が起動し、プール内の新しいスタンバイになりますが、サウスバウンド IP アドレスと同じ IP1 を保持します。これにより、CDG1 と CDG2 の両方がサウスバウンド IP と同じ IP1 になります。

Crosswork Data Gateway のプールには次の状態があります。

- [保護（Protected）]：すべての VM が稼働しており、プール内に 1 つ以上のスタンバイ VM があります。
- [保護なし（Not Protected）]：すべてのスタンバイ VM がダウンしており、使用中の VM を置き換えることができません。
- [限定的な保護（Limited Protection）]：一部のスタンバイ VM がダウンしていますが、1 つ以上のスタンバイ VM が稼働しています。

- [計画なし（None Planned）]：プールの作成時にスタンバイ VM がプールに追加されませんでした。

Datagateway が 3 回連続のバイタルサイクル（30 秒）の間、そのヘルスの報告に失敗した場合、Data Gateway の [動作状態（Operational state）] は [エラー（Error）] であると見なされます。ヘルスレポートの失敗は、次のことが原因である可能性があります。

- Datagateway VM の問題。たとえば、データゲートウェイで正常性を報告するためのリソースが不足しています。
- Cisco Crosswork と Crosswork Data Gateway 間のネットワークの問題。

Crosswork Data Gateway の [動作状態（Operational state）] は 20 秒ごとにチェックされます。アクティブな VM が [エラー（Error）] 状態の場合、フェールオーバーがトリガーされ、プール内のスペア VM がプール内のアクティブな VM になります。

セキュアな Syslog 通信の FQDN を有効にする

Crosswork Data Gateway は、syslog 証明書に Crosswork Data Gateway の仮想 IP アドレスの代わりにホスト名または完全修飾ドメイン名（FQDN）が含まれている必要があるデバイスへの安全な syslog 通信をサポートします。これは、syslog 証明書にホスト名または FQDN を持つことを義務付けるデバイスで有効にできるオプション機能です。有効にすると、Cisco Crosswork は、DNS サーバーから Crosswork Data Gateway の各仮想 IP アドレスのホスト名または FQDN をフェッチします。新しく追加された仮想 IP の FQDN は、プールを保存した後に取得されます。その後、syslog 証明書には、Crosswork Data Gateway の仮想 IP アドレスの代わりに、CN および SAN の FQDN が含まれます。デバイスでセキュア Syslog を設定する方法の詳細については、「デバイスでのセキュア Syslog の設定 （83 ページ）」を参照してください。

（注） Crosswork Data Gateway プールは、FQDN を有効にせずに作成できます。この場合、syslog 証明書には Crosswork Data Gateway の仮想 IP アドレスが含まれます。後でいつでもプールを編集して、FQDN を有効または無効にして、syslog 証明書に FQDN と仮想 IP アドレスを切り替えることができます。

プール内の仮想 IP の FQDN 値を更新するには（FQDN 値が DNS サーバーで更新された場合）、プールの [アクション（Actions）] > [FQDNの更新（Refresh FQDN）] オプションを使用します。

Cisco Crosswork Data Gateway プールの作成

Cisco Crosswork Data Gateway プールを作成する場合は、次のガイドラインに従います。

- 少なくとも 1 つのプールを作成し、Crosswork Data Gateway VM をそのプールに割り当てる必要があります。収集用の Crosswork Data Gateway を設定するには、この手順が必須です。
- プール内のすべての Crosswork Data Gateway VM は、同じ構成（Standard、、または Extended）である必要があります。

- VM を Amazon EC2 に展開した場合、プール内のすべての Crosswork Data Gateway VM は同じ可用性ゾーンからのものである必要があります。

Crosswork Data Gateway プールを作成するには、次の手順を実行します。

始める前に

Cisco Crosswork Data Gateway のプールを作成する前に、次を確認してください。

- プールの高可用性を有効にするかどうかを決定すること。
- プールに追加する Crosswork Data Gateway のすべての VM をインストールしたことを確認する。
- Crosswork Data Gateway VM の動作状態が [準備中（Not Ready）] であることを確認します。
- 仮想 IP アドレス（アクティブなデータゲートウェイごとに 1 つの仮想 IP）、サブネットマスク、ゲートウェイ情報などのネットワーク情報を用意します。

（注） ゲートウェイは、3 つの NIC を使用する場合にのみ必要です。

展開内の vNIC の数に応じて、仮想 IP アドレスは次のようになります。

- 単一の NIC 展開での管理ネットワーク上の追加の IP アドレス。
- 2 NIC 展開用のデータネットワーク上の追加 IP アドレス。
- 3 NIC 展開用のサウスバウンドネットワーク上の IP アドレス。

これらの仮想 IP アドレスは、ネットワーク設計段階で事前に計画する必要があります。

- プール内の仮想 IP アドレスに対して完全修飾ドメイン名（FQDN）を有効にするかどうかを決定します。はいの場合、プールを正常に作成するために、DNS サーバーで仮想 IP の FQDN が設定されていることを確認してください。

ステップ 1 メインメニューから **[管理（Administration）] > [Data Gateway の管理（Data Gateway Management）]** を選択し、[プール（Pools）] タブをクリックします。

ステップ 2 [プール（Pools）] タブで、＋ボタンをクリックしてプールを作成します。

ステップ 3 [プールのパラメータ（Pool Parameters）] ペインで、次のパラメータに値を入力します。

- [プール名（Pool Name）]：ネットワークを適切に説明するプールの名前。
- [説明（Description）]：プールの説明。

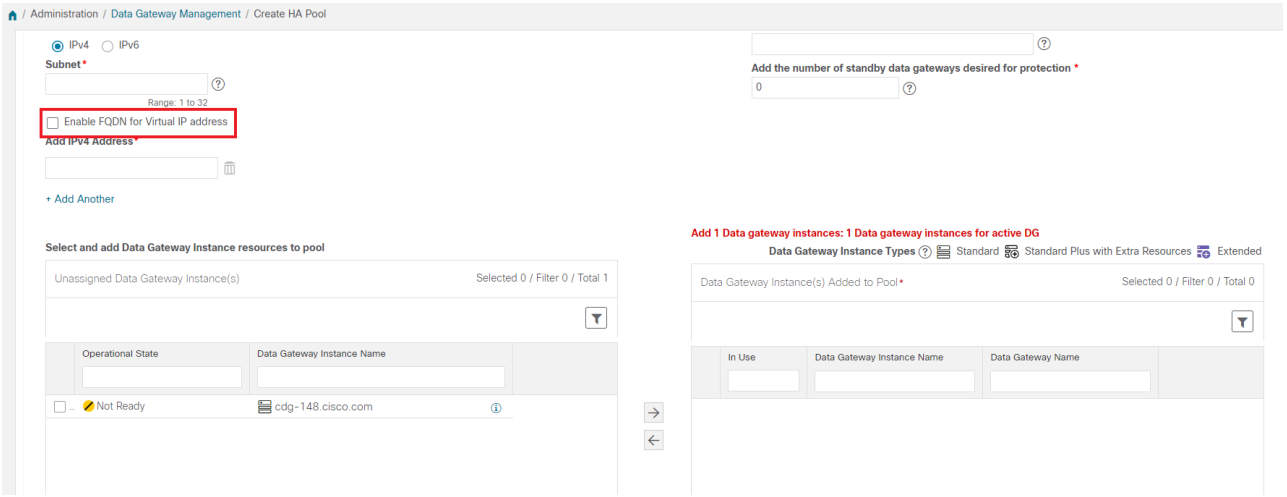
ステップ 4 [プールリソース（Pool Resources）] ペインで、次の詳細を追加します。

- [IPv4] または [IPv6]：仮想 IP の IPv4 または IPv6 アドレスファミリを選択します。

- [サブネットマスク（Subnet Mask）]：各 Cisco Crosswork Data Gatewayのサブネットマスク
- [ゲートウェイ（Gateway）]：デバイスと通信するための Cisco Crosswork Data Gateway それぞれのゲートウェイアドレス。

  （注） Cisco Crosswork Data Gateway VM の vNIC が 3 つ未満の場合、このフィールドは適用されません。

- （オプション）[仮想IPアドレスのFQDNを有効にする]：このオプションを選択して、syslog 証明書の Crosswork Data Gateway の各仮想 IP アドレスにホスト名または完全修飾ドメイン名（FQDN）を使用します。



- [IPv4] の追加または [IPv6] の追加：前に選択したアドレスファミリ（IPv4 または IPv6）に基づいて、すべてのアクティブな Cisco Crosswork Data Gateway VM の仮想 IP アドレスを入力します。
- [保護に必要なスタンバイ データ ゲートウェイの数を追加する（Add the number of standby data gateways desired for protection）]：このフィールドに 0 より大きい値を入力すると、プールの高可用性が有効になります。アクティブなデータゲートウェイがダウンした場合、保護を確保するためにプール内の「スタンバイ」が置き換わります。

  プールに追加する Cisco Crosswork Data Gateway VM の数は、仮想 IP とスタンバイ Cisco Crosswork Data Gateway VM の合計数と同じにする必要があります。たとえば、仮想 IP を 3 つ入力し、2 つのスタンバイ VM が必要な場合は、5 つの Cisco Crosswork Data Gateway VM をプールに追加します。

- [VMリソースを選択してプールに追加する（Select and Add VM Resources to pool）]：左側の [未割り当ての仮想マシン（Unassigned Virtual Machine(s)）] を選択し、右矢印をクリックして VM を [プールに追加されている仮想マシン（Virtual Machine(s) Added to Pool）] に移動します。

ステップ 5 [保存（Save）] をクリックします。

[保存（Save）] をクリックし、仮想 Crosswork Data Gateway が自動的に作成され、[Data Gateway] タブに表示されます。デバイスをこの仮想 Crosswork Data Gateway に接続して収集ジョブを実行します。

（注） DNS サーバーの仮想 IP の FQDN 構成が欠落している場合、プールの作成は失敗します。DNS サーバーの FQDN 構成を確認するか、FQDN オプションを無効にして再試行してください。

Crosswork Data Gateway へのデバイスの接続

Crosswork Data Gateway にデバイスを接続する場合は、次のガイドラインに従います。

- デバイスは 1 つの Crosswork Data Gateway のみに接続できます。
- 最適なパフォーマンスを得るには、300 台以下のデバイスで数回に分けて Crosswork Data Gateway に接続することをお勧めします。

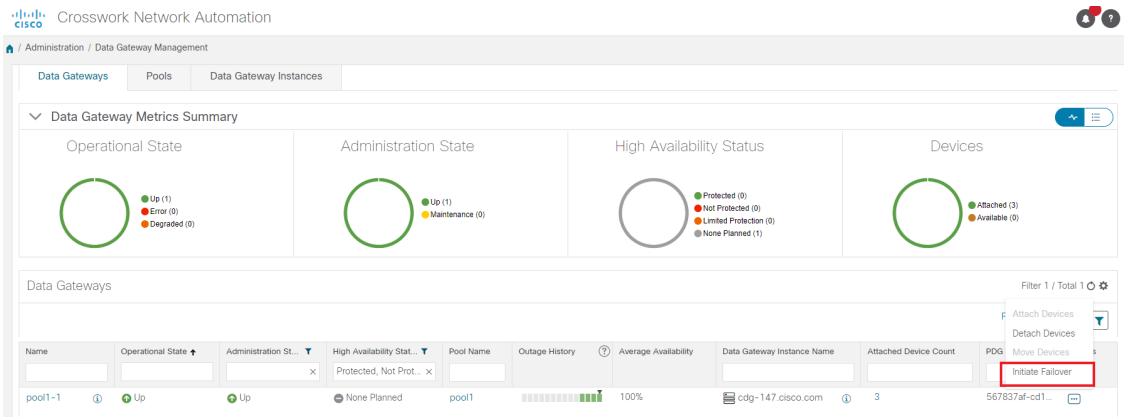
（注） Crosswork Data Gateway では、SSH 接続が失敗する可能性があるため、古い安全でない鍵交換アルゴリズム（KEX）の使用をサポートしていません。

始める前に

デバイスを接続する Crosswork Data Gateway の [管理状態（Admin state）] と [動作状態（Operational state）] が [アップ（Up）] であることを確認します。

ステップ 1 （オプション）既存の Crosswork Data Gateway にデバイスを接続する前に、Crosswork Data Gateway の正常性を確認することをお勧めします。詳細については、「Crosswork Data Gateway 正常性のモニタリング（40 ページ）」を参照してください。

ステップ 2 メインメニューから、[管理（Administration）]>[Data Gateway の管理（Data Gateway Management）]>[データゲートウェイ（Data Gateways）] に移動します。



ステップ 3 デバイスを接続する Crosswork Data Gateway の [アクション（Actions）] 列で、… をクリックして [デバイスの接続（Attach Devices）] を選択します。[デバイスの接続（Attach Devices）] ウィンドウが開き、接続可能なすべてのデバイスが表示されます。

ステップ 4 すべてのデバイスを接続するには、[すべてのデバイスの接続（Attach All Devices）] をクリックします。それ以外の場合は、接続するデバイスを選択し、[選択したデバイスの接続（Attach Selected Devices）] をクリックします。

ステップ 5 [確認：デバイスの接続（Confirm-Attach Devices）] ダイアログで、[接続（Attach）] をクリックします。

[データゲートウェイ（Data Gateways）] ペインの [接続デバイス数（Attached Device Count）] 列を確認して、変更が成功したことを確認します。

Crosswork Data Gateway の正常性をモニターし、Crosswork Data Gateway が新しく接続されたデバイスで正常に機能していることを確認します。「Crosswork Data Gateway 正常性のモニタリング （40 ページ）」を参照してください。

Crosswork Data Gateway の設定後の管理

この項では、Crosswork Data Gateway 内のさまざまなメンテナンスタスクについて説明します。

Crosswork Data Gateway 正常性のモニタリング

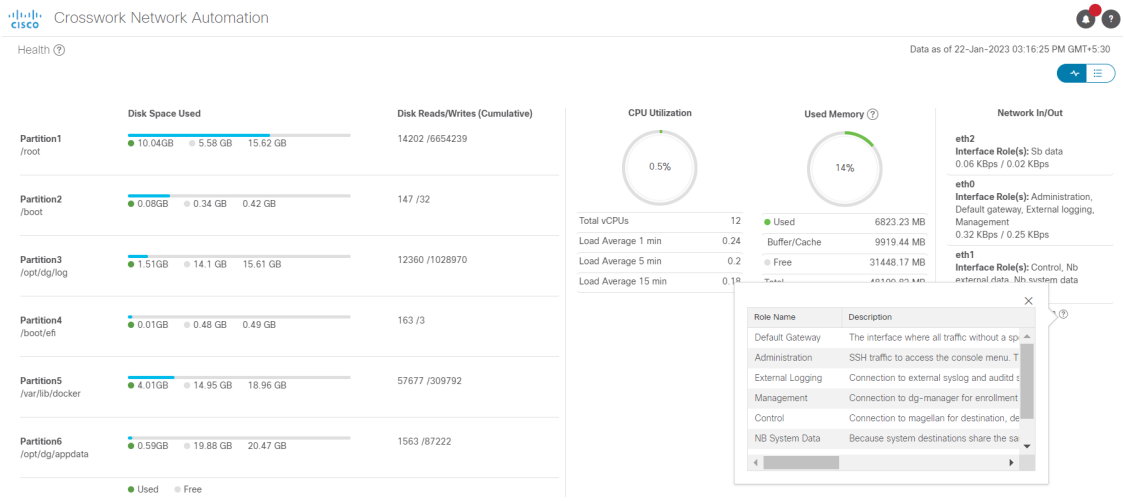
Crosswork Data Gateway の操作とヘルスの概要は、**[管理（Administration）] > [データゲートウェイ管理（Data Gateway Management）] > [データゲートウェイ（Data Gateways）] >（クリック）{Crosswork Data Gateway}** の順にアクセスし、Crosswork Data Gateway 詳細ページから表示できます。このページには、Crosswork Data Gateway で実行されているさまざまなコンテナ化されたサービスの状態の詳細も含まれています。Crosswork Data Gateway の全体的な正常性は、コンテナ化された各サービスの正常性にも依存します。

このページには、次のパラメータが表示されます。

- [一般的なCisco Crosswork Data Gatewayの詳細（General Cisco Crosswork Data Gateway）]：動作状態、高可用性の状態、接続されているデバイスの数、割り当てられたジョブなど、Crosswork Data Gateway の一般的な詳細を表示します。[アクション（Actions）] オプション UI から使用できるさまざまなトラブルシューティングのオプションについて説明します。
- [履歴（History）]：タイムスタンプ、停止時間、クリア時間を含む、14 日間の Cisco Crosswork Data Gateway の停止履歴チャートを表示します。ペインの右上隅のオプション

を使用して、グラフ内の特定の期間の履歴チャートの拡大、縮小、パンを実行したり、SVG と PNG をダウンロードします。

- [イベント（Events）]：過去 14 日間のすべての Cisco Crosswork Data Gateway の遷移状態の変更のリストを表示します。これには、動作状態の変更、ロールの変更、ステータス変更の理由を示すメッセージ、タイムスタンプ、期間を含むイベントの詳細などの情報が含まれます。
- [正常性（Health）]：Cisco Crosswork Data Gateway の正常性情報を示します。右上隅のタイムスタンプは、最後の正常性データが収集されたときのタイムスタンプです。Crosswork Data Gateway が [エラー（Error）] 状態の場合、または何らかの理由でデータが古い場合、タイムスタンプラベルはデータが古いことを示します。Crosswork Data Gateway の [CPU使用率（CPU Utilization）] が 80% を超える場合は、[CPU使用率（CPU Utilization）] がさらに増加して Crosswork Data Gateway の障害につながる前に、是正措置を講じることをお勧めします。



- [サービスステータス（Service Status）]：Crosswork Data Gateway で実行されている個々のコンテナサービスの正常性情報と、個々のサービスを再起動するオプション（[アクション（Action）] > [再起動（Restart）]）を使用したリソース消費が表示されます。[負荷（Load）] 列は、その特定のコレクタ/サービスの処理負荷を示します。コレクタの負荷スコアは、いくつかのメトリックを使用して計算されます。。負荷スコアは、低、中、または高の重大度ゾーンにマップされます。コレクタが常に**高**ゾーンで動作している場合、そのコレクタが特定のCPU/メモリリソースプロファイルのピーク容量に達したことを意味します。負荷スコアの計算方法の詳細については、[負荷スコアの計算（Load Score Calculation）]https://www.cisco.com/c/dam/en/us/td/docs/cloud-systems-management/crosswork-data-gateway/Load_Metrics_Calculation.pdf を参照してください。

（注） コンテナサービスのリストは、標準の Crosswork Data Gateway と拡張 Crosswork Data Gateway で異なります。拡張 Crosswork Data Gatewayには、より多くのコンテナがインストールされています。

表示されるリソース消費データは、docker 統計からのものです。これらの値は、コンテナ化されたサービスによって消費される実際のリソースよりも高くなります。

Service Status

Data as of 22-Jan-2023 03:16:25 PM G

Services	Status	Load	CPU Utilization	Memory Used (MB)	Java Heap Memory Used/Max (MB)	Network In/Out (MB)	Network In/Out Rate (B/Sec)	Disk In/Out (MB)
cli collector	Running	⚠	0.22 %	857.74	325.36 / 460	202 / 50.5	136 / 236	0 / 514
controller gateway	Running	-	0.02 %	13.47	-	482 / 526	1658 / 1305	0 / 191
gnmi collector	Running	⚠	0.12 %	289.41	51.81 / 76	19.6 / 14.7	114 / 169	0 / 205
icon	Running	-	0.13 %	393.43	-	15.1 / 12.3	27 / 41	0 / 172
image manager	Running	-	0.12 %	348.86	99.24 / 147	103 / 125	6 / 13	0.25 / 249
mdt collector	Running	⚠	0.12 %	299.37	48.17 / 80	19.6 / 14.7	129 / 184	0 / 206
netconf collector	Running	⚠	0.15 %	636.8	267.08 / 330	19.6 / 14.7	110 / 158	0 / 242
oam manager	Running	-	0.14 %	445.54	95.56 / 138	391 / 160	1099 / 2167	55.6 / 905
snmp collector	Running	⚠	0.28 %	1215.48	401.32 / 840	56.2 / 29.3	155 / 234	0.02 / 441
syslog collector	Running	⚠	0.11 %	403.6	62.29 / 94	23.2 / 24	144 / 157	0 / 229

ネットワーク内の Crosswork Data Gateway の正常性を定期的に監視して、過負荷を防止し、追加のリソースを追加したり、Crosswork Data Gateway の負荷を適切なタイミングで削減するなどの是正措置を積極的に講じることをお勧めします。

1. Crosswork Data Gateway に障害が発生した場合、またはリソース容量の制限に近づいている場合、アラームは DG-Manager によって生成されます。
2. Crosswork Data Gateway の [CPU使用率（CPU Utilization）] が 80% を超える場合は、デバイスを別の CDG に移動する、他の VM をプールに追加する、または既存の収集ジョブの頻度を増やすことによって、[CPU使用率（CPU Utilization）] を下げるまで、収集ジョブを作成しないことをお勧めします。
3. Crosswork Data Gateway の [CPU使用率（CPU Utilization）] が 90% を超える場合は、[CPU使用率（CPU Utilization）] の低い別の Crosswork Data Gateway にデバイスを移動することをお勧めします。
4. システムアラームを毎週確認することをお勧めします。リソースの問題ではなく、データのドロップが頻繁に発生していないことを確認してください。次に、データの宛先の問題を修正するか、収集ジョブの頻度を増やします。

Crosswork Data Gateway プールの管理

次の手順を実行して Cisco Crosswork Data Gateway プールを編集または削除します。プールを作成するには、「Cisco Crosswork Data Gateway プールの作成 （36 ページ）」を参照してください。

始める前に

プールを編集または削除する前に考慮すべき重要なポイント：

- デバイスが接続されている仮想 IP アドレスは削除できません。
- Crosswork Data Gateway VM は、すべてのデバイスのマッピングが Crosswork Data Gateway から削除された場合にのみプールから削除できます。Crosswork Data Gateway VM をプールから削除すると、同じプールからのスタンバイ VM に自動的に置換されます。
- Crosswork Data Gateway プールを削除する前に、最初に Crosswork Data Gateway からデバイスを切り離すか、デバイスを別の Crosswork Data Gateway に移動します。

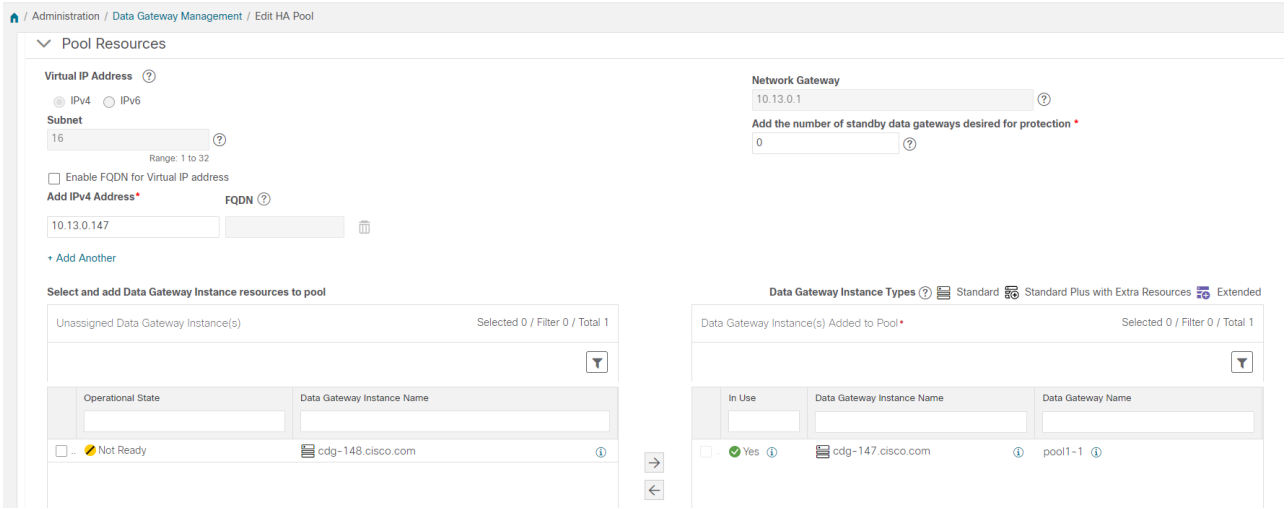
ステップ 1 メインメニューから **[管理（Administration）] > [Data Gateway の管理（Data Gateway Management）]** を選択し、[プール（Pools）] タブをクリックします。

ステップ 2 **Cisco Crosswork Data Gateway プールの編集**：

a) このページに表示されるプールの一覧から編集したいプールを選択し、

b) [高可用性（HA）プールの編集（Edit High Availability (HA) Pool] ページを開くには、✎ ボタンをクリックします。

リソースプールを編集する場合、[プールリソース（Pool Resources）] ペインのパラメータのみを変更できます。[プールパラメータ（Pool Parameters）] ペインでパラメータを編集することはできません。[プールパラメータ（Pool Parameters）] ペインでパラメータを変更するには、必要な値で新しいプールを作成し、Cisco Crosswork Data Gateway VM をそのプールに移動します。



c) [プールリソース（Pool Resources）] ペインでは、次の操作を実行できます。

- 必要なアクティブ データ ゲートウェイごとに仮想 IP アドレスを追加し、削除します。
- スタンバイ Crosswork Data Gateway VM の数を変更します。
- Crosswork Data Gateway VM をプールから追加および削除します。

- プールの FQDN を有効または無効にします。

d) 変更が完了したら、[保存（Save）] をクリックします。

ステップ 3 **Crosswork Data Gateway プールの削除**：

a) 削除するプールを選択し、 をクリックします。

b) [高可用性（HA）プールの削除（Delete High Availability (HA) Pool] ウィンドウで [削除（Delete）] をクリックして、プールを削除します。

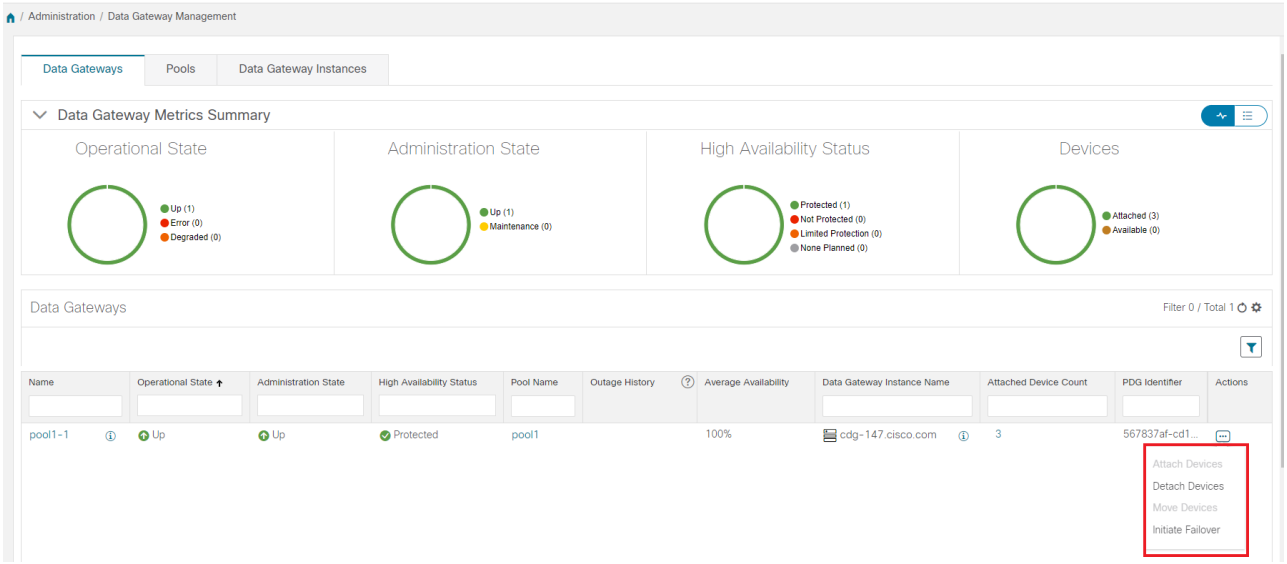
Cisco Crosswork Data Gateway デバイス割り当ての管理

Crosswork Data Gateway からデバイスを移動または切り離す場合は、次のガイドラインに従います。

- デバイスは 1 つの Crosswork Data Gateway のみに接続できます。
- デバイスを異なるプールの Crosswork Data Gateway に移動する場合は、プールのゲートウェイが現在のプールのゲートウェイと同じであることを確認してください。ゲートウェイが一致しない Crosswork Data Gateway にデバイスを移動すると、収集が失敗します。
- Cisco Crosswork Data Gateway からデバイスを切り離すと、そのデバイスに対応するすべての収集ジョブが削除されます。切り離すデバイスに送信された収集ジョブを失いたくない場合は、代わりに別の Cisco Data Gateway にデバイスを移動します。

Crosswork Data Gateway プールからデバイスを移動または切り離すには、次の手順に従います。プールにデバイスを追加するには、「Crosswork Data Gateway へのデバイスの接続 （39 ページ）」を参照してください。

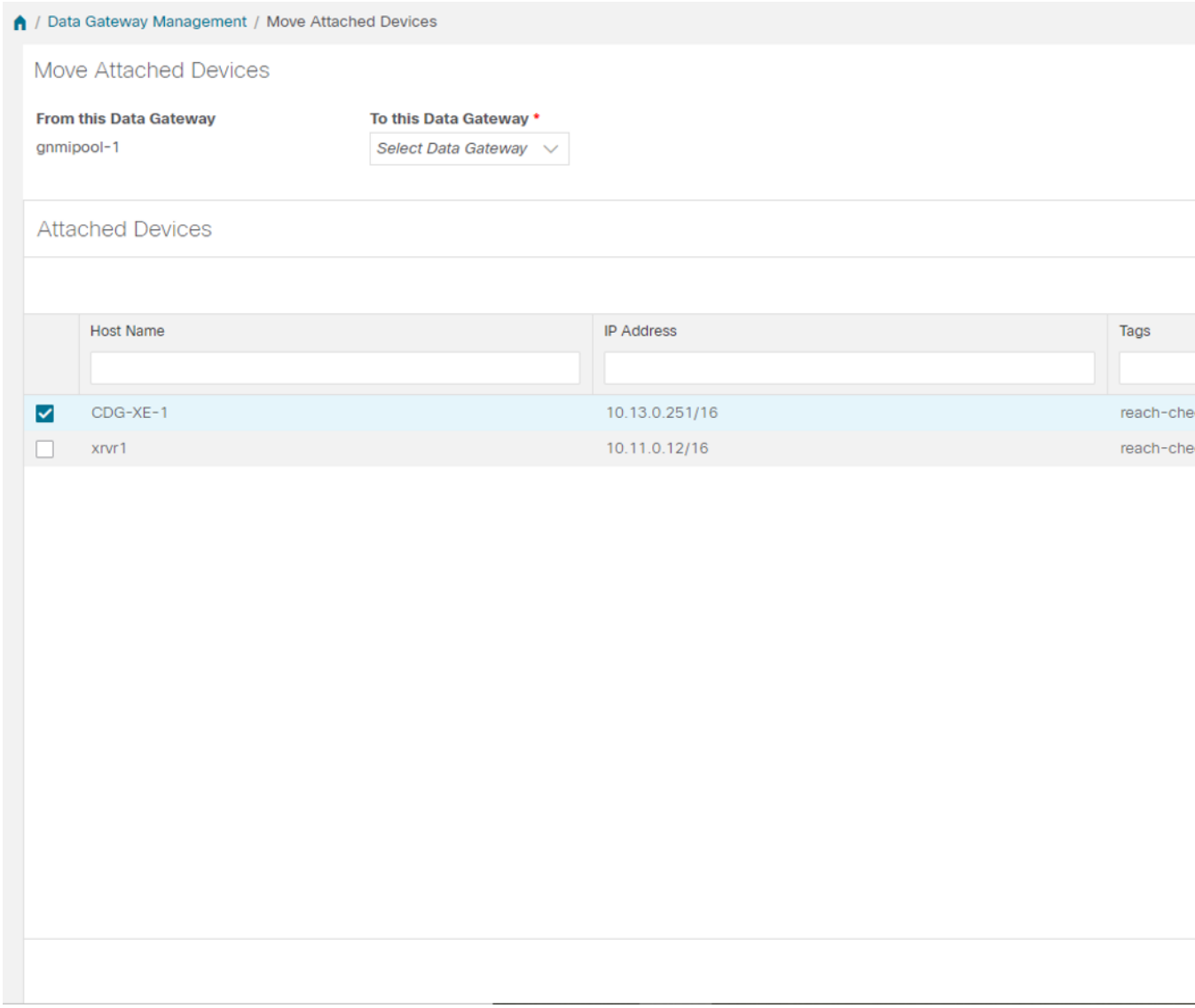
ステップ 1 Cisco Crosswork メインメニューから、[管理（Administration）] > [Data Gateway の管理（Data Gateway Management）] > [データゲートウェイ（Data Gateways）] に移動します。



ステップ 2 **デバイスを移動する**には、次の手順を実行します。

a) デバイスを移動する Crosswork Data Gateway の [アクション（Actions）] 列で、[...] をクリックして [デバイスの移動（Move Devices）] を選択します。[接続されているデバイスの移動（Move Attached Devices）] ウィンドウが開き、移動可能なすべてのデバイスが表示されます。

b) [このデータゲートウェイに移動（To this Data Gateway）] ドロップダウンから、デバイスの移動先のデータゲートウェイを選択します。



c) すべてのデバイスを移動するには、[すべてのデバイスの移動（Move All Devices）] をクリックします。それ以外の場合は、移動するデバイスを選択し、[選択したデバイスの移動（Move Selected Devices）] をクリックします。

d) [確認：デバイスの移動（Confirm - Move Devices）] ウィンドウで、[移動（Move）] をクリックします。

ステップ 3 **デバイスを切り離す**には、次の手順を実行します。

a) デバイスを切り離す Crosswork Data Gateway の [アクション（Actions）] 列で、… をクリックして [デバイスの切り離し（Detach Devices）] を選択します。[デバイスの切断（Detach Devices）] ウィンドウが開き、接続されているすべてのデバイスが表示されます。

b) すべてのデバイスを切り離すには、[すべてのデバイスの切断（Detach All Devices）] をクリックします。それ以外の場合は、切り離すデバイスを選択し、[切断（Detach）] をクリックします。

c) [確認：デバイスの切断（Confirm - Detach Devices）] ウィンドウで、[切断（Detach）] をクリックします。

[データゲートウェイ（Data Gateways）] ペインの [接続デバイス数（Attached Device Count）] を確認して、変更が成功したことを確認します。接続デバイス数の横にある[i] アイコンをクリックすると、選択した Crosswork Data Gateway に接続されているすべてのデバイスのリストが表示されます。

Crosswork Data Gateway VM の維持

この項では、Crosswork Data Gateway VM のメンテナンスタスクについて説明します。

- Cisco Crosswork Data Gateway VM の管理状態の変更 （47 ページ）
- Cisco Crosswork からの Cisco Crosswork Data Gateway VM の削除 （48 ページ）
- Crosswork Data Gateway VM の再展開 （49 ページ）

Cisco Crosswork Data Gateway VM の管理状態の変更

Cisco Crosswork プラットフォームと Cisco Crosswork Data Gateway 間での動作を一時停止するために、データセンター内でアップグレードまたはその他のメンテナンスを実行することが必要になる場合があります。これは、Cisco Crosswork Data Gateway を [メンテナンス（Maintenance）] モードにすることで実現できます。ダウンタイム時に、管理者は証明書の更新などの変更を、Cisco Crosswork Data Gateway に加えることができます。

（注） メンテナンスアクティビティが Crosswork と Crosswork Data Gateway の間の通信に影響を与えている場合は収集は中断され、通信が復元されると再開されます。同様に、メンテナンスアクティビティが Crosswork Data Gateway と外部接続先（Kafka/gRPC）間の通信に影響している場合は収集が相互に中断され、通信が復元されると再開されます。

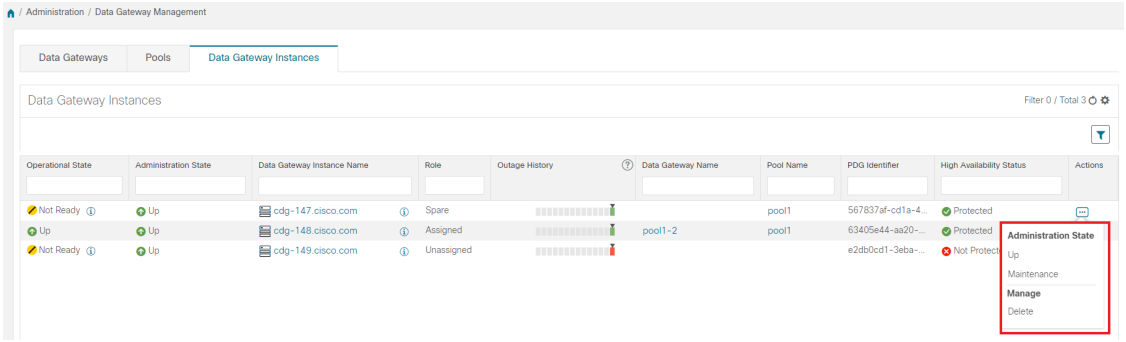
変更が完了すると、管理者は管理状態を [アップ（Up）] に変更できます。Crosswork Data Gateway VM が起動すると、Cisco Crosswork がジョブの送信を再開します。

（注） メンテナンス（ネットワーク上で行われる作業またはネットワークの停止）は、失敗する可能性がありますが、収集を停止しません。[管理状態（Administration state）] が [メンテナンス（Maintenance）] である Crosswork Data Gateway VM の場合、収集は正常に停止し、VM が管理状態を [アップ（Up）] に戻すと再開します。

Crosswork Data Gateway VM の管理状態を変更するには、次の手順を実行します。

ステップ 1 メインメニューから [管理（Administration）] > [Data Gateway の管理（Data Gateway Management）] > [仮想マシン（Virtual Machines）] をクリックします。

ステップ 2 Cisco Crosswork Data Gateway の場合に管理ステータスを変更するには、[アクション（Actions）] 列で ··· をクリックします。



ステップ 3 切り替える管理状態を選択します。

Cisco Crosswork からの Cisco Crosswork Data Gateway VM の削除

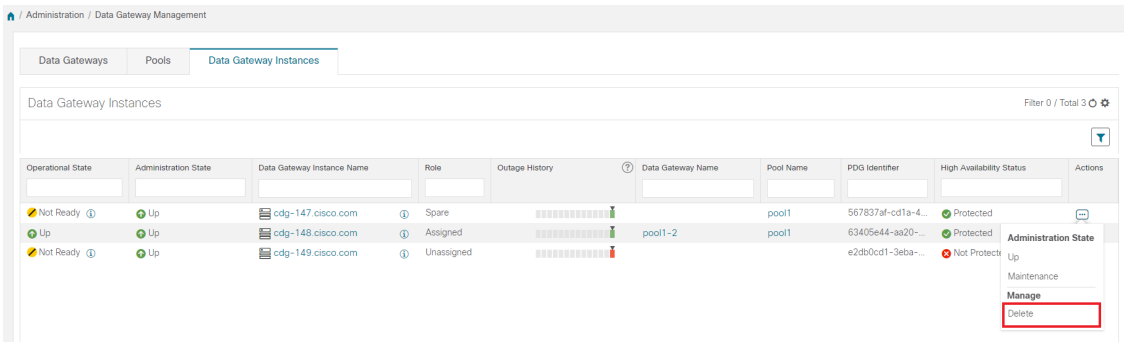
Cisco Crosswork から Cisco Crosswork Data Gateway VMを削除するには、次の手順を実行します。

始める前に

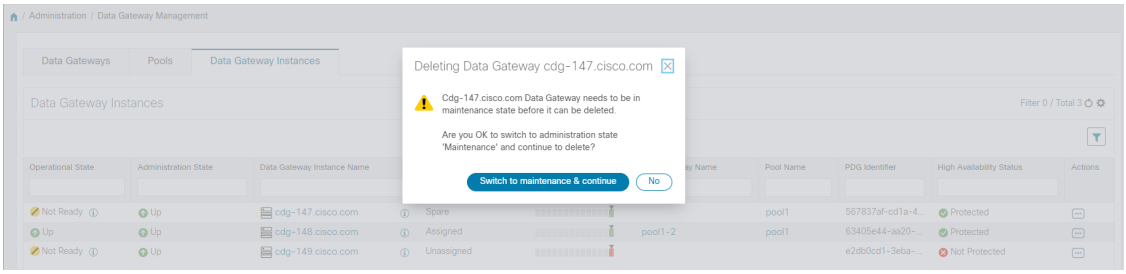
これらのデバイスに対応するジョブが失われないように、接続されているデバイスを別のデータゲートウェイに移動することをお勧めします。Cisco Crosswork Data Gateway VM からデバイスを切り離すと、対応するジョブが削除されます。

ステップ 1 メインメニューから [管理（Administration）] > [Data Gateway の管理（Data Gateway Management）] > [仮想マシン（Virtual Machines）] をクリックします。

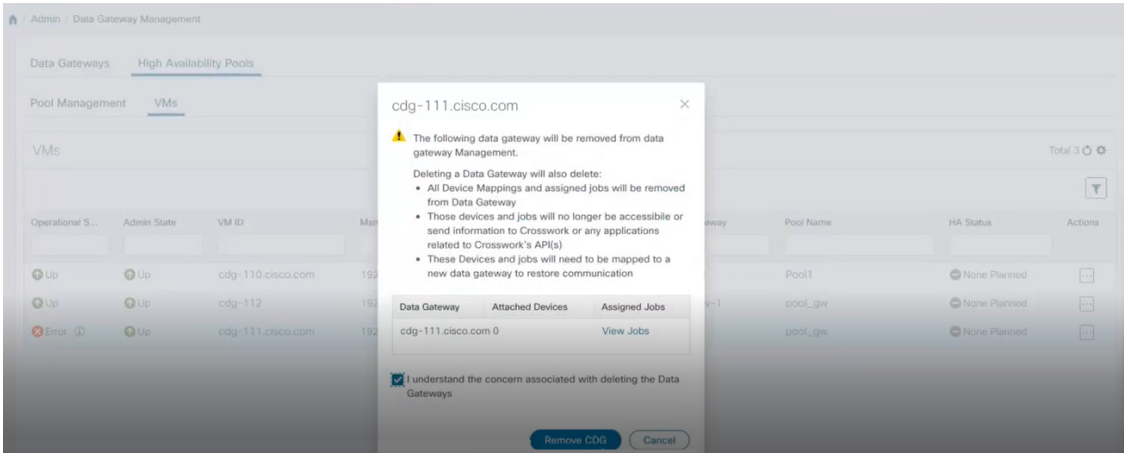
ステップ 2 Crosswork Data Gateway を削除する場合は、[アクション（Actions）] 列の下にある ··· をクリックし、[削除（Delete）] をクリックします。



ステップ 3 削除する Cisco Crosswork Data Gateway VM はメンテナンスモードになっている必要があります。[メンテナンス（Maintenance）] モードに切り替えるように求められたら、[切り替えて続行（Switch & Continue）] をクリックします。



ステップ 4 [データゲートウェイの削除に関連する事項を理解しました（I understand the concern associated with deleting the Data Gateways）] のチェックボックスをオンにします。 [CDG の削除（Remove CDG）] をクリックします。



Crosswork Data Gateway VM の再展開

Crosswork Data Gateway VM を再展開するには、古い VM を削除して新しい VM をインストールします。新しい Crosswork Data Gateway VM のインストール方法の詳細については、『*Cisco Crosswork Infrastructure 4.4* およびアプリケーション インストール ガイド』の「*Cisco Crosswork Data Gateway* のインストール」の項を参照してください。

VM の展開プロファイルを変更するために Crosswork Data Gateway VM を再展開する場合（たとえば、プロファイルを Standard から Extended に変更する場合）、Crosswork Data Gateway VM の再展開を試みる前に、Data Gateway グローバルパラメータの変更を手動でロールバックしてください。

考慮すべき重要な点

1. Crosswork Data Gateway VM がすでに Cisco Crosswork に登録されており、同じ名前で VM を再度インストールした場合は、Crosswork Data Gateway VM の [管理状態（Administration）] を [メンテナンス（Maintenance）] に変更して自動登録を実行します。
2. Crosswork Data Gateway VM がすでに Cisco Crosswork に登録されており、Cisco Crosswork を再度インストールした場合は、既存の Crosswork Data Gateway VM を Cisco Crosswork に再登録します。Crosswork Data Gateway の再登録 （415 ページ） を参照してください。

Crosswork Data Gateway グローバル設定を設定

このセクションでは、Cisco Crosswork Data Gateway のグローバル設定を設定する方法について説明します。これらの設定は次のとおりです。

- 外部データ送信先の作成と管理 （50 ページ）。
- カスタムデバイスパッケージを管理 （57 ページ）。
- Crosswork Data Gateway グローバルパラメータの設定 （59 ページ）。
- Crosswork Data Gateway ダイナミックリソースの割り当て （61 ページ）。

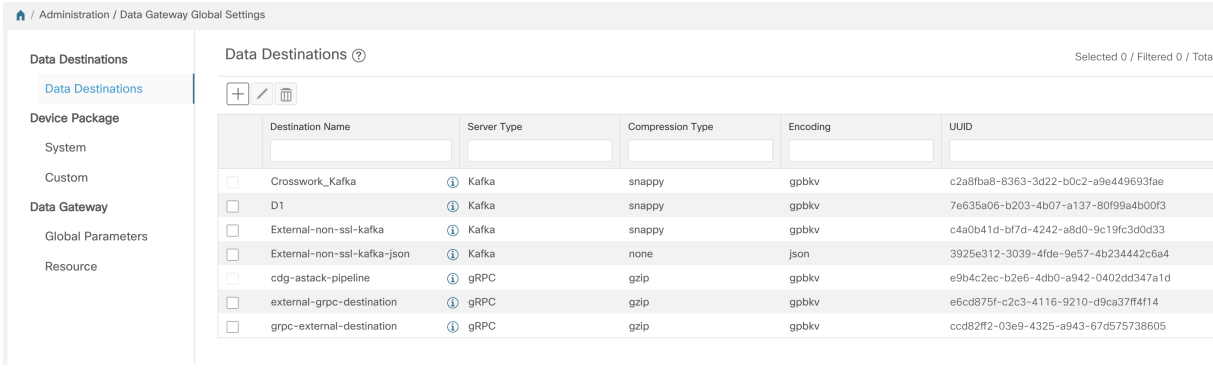
外部データ送信先の作成と管理

Cisco Crosswork では、収集ジョブでデータをデポジットするために使用できる外部データ送信先（Kafka または外部 gRPC）を作成できます。

[管理（Administration）] > [Data Gatewayのグローバル設定（Data Gateway Global Settings）] > [データ送信先（Data Destinations）] に移動してアクセスできます。新しいデータ送信先の追加、既存のデータ送信先の設定の更新、データ送信先の削除を行うことができます。

[データ送信先（Data Destinations）]ページのテーブルには、データをデポジットするために収集ジョブで使用できる承認済みのデータ送信先のリストが表示されます。

（注） **Crosswork_Kafka** と **cd-astack-pipeline** は内部データ送信先であり、更新または削除はできません。



UUID は、データ送信先の一意の識別子です。Cisco Crosswork は外部データ送信先が作成されると、この ID を自動的に生成します。Cisco Crosswork UI を使用して収集ジョブを作成する場合、設定済みの宛先のドロップダウンリストを使用してデータの宛先を選択します。API を介して収集ジョブを作成する場合、収集したデータをコレクタが送信する宛先の UUID を知る必要があります。

データ送信先の詳細を表示するには、[データ送信先（Data Destinations）] ペインで、詳細を表示するデータ送信先名の横にある アイコンをクリックします。

外部収集ジョブのライセンス要件

データを外部のデータ送信先に転送できる収集ジョブを作成できるようにするには、次のライセンス要件を満たしていることを確認します。

1. メインメニューから、[管理（Administration）] > [アプリケーション管理（Application Management）] > [スマートライセンス（Smart License）] に移動します。
2. アプリケーションフィールドで [Crosswork プラットフォームサービス（Crosswork Platform Services）] を選択します。
3. ステータスが次のようになっていることを確認します。
   - [登録ステータス（Registration Status ）] : [登録済み（Registered）]

     Cisco Smart Software Manager（CSSM）に登録済みであり、予約済みライセンス機能の使用が許可されていることを示します。
   - [ライセンス認証ステータス（License Authorization Status）] : [認証済み（Authorized）]（[準拠（In Compliance）]）

     外部収集ジョブのデバイス数を超えていないことを示します。
   - [スマートライセンスの使用状況（Smart Licensing Usage）] で、**CW_EXTERNAL_COLLECT** のステータスが [準拠（In Compliance）] になっています。

評価期間が終了した後、または外部収集ジョブのデバイス数を超えた場合（[ライセンス認証ステータス（License Authorization Status）] が [コンプライアンス違反（Out of Compliance）]）、

Cisco Smart Software Manager（CSSM）に登録しないと、外部収集ジョブを作成できません。ただし、この場合も既存の収集ジョブは表示および削除できます。

データ宛先の追加または編集

新しいデータ送信先を追加するには、次の手順を実行します。その後、このデータ宛先を使用してデータを転送できます。複数のデータ送信先を追加することができます。

外部データの宛先を追加する際の注意点は次のとおりです。

- 既存の外部 Kafka データの送信先を同じ IP アドレスで再インストールする場合は、コレクタを再起動して変更を有効にする必要があります。
- Cisco Crosswork と指定したデータ送信先、つまり Crosswork Kafka または外部 Kafka のいずれかの間の通信チャネルをセキュリティで保護できます。（この手順の**ステップ 6** に進みます）。ただし、セキュリティを有効にすると、パフォーマンスに影響する可能性があります。
- 外部データ送信先で TLS 接続が必要な場合は、公開証明書を準備するか、クライアント認証が必要な場合は、クライアント証明書とキーファイルを準備します。クライアントキーはパスワードで暗号化されている可能性があり、データ送信先のプロビジョニングの一部として設定する必要があります。現在、Crosswork Data Gateway は IP ベースの証明書のみをサポートしています。
- 認証局で証明書を生成する場合は、証明書が PEM でエンコードされ、キーファイルが PKCS＃8 形式であることを確認します。
- Cisco Crosswork にジョブを送信する前に、Kafka トピックを作成してください。外部 Kafka およびその外部 Kafka でのトピックの管理方法によっては、収集したデータをその特定の外部 Kafka/トピックにディスパッチする時点でトピックが存在しない場合、Cisco Crosswork ログに次の例外が表示される場合があります。これは、トピックがまだ作成されていないか、収集ジョブが完了する前にトピックが削除されたことが原因である可能性があります。

```
destinationContext: topicmdt4
org.apache.kafka.common.errors.UnknownTopicOrPartitionException: This server does
not host this topic-partition.
```

- データ宛先のポート接続を確認して検証します。宛先でポートに到達できない場合、収集が失敗します。
- Crosswork Data Gateway では、Kafka 宛先の宛先プロパティでカスタム値を設定できます（この手順のステップ 4 を参照）。

（注） この機能は、gRPC 宛先ではサポートされていません。

[宛先の詳細（Destination Details）] ペインに入力されたグローバルプロパティは必須であり、個々のコレクタレベルでカスタム値が指定されていない限り、デフォルトで Kafka 宛

先に適用されます。コレクタに指定するカスタム値は、そのコレクタにのみ適用されます。

始める前に

データ収集に外部 Kafka サーバーを使用している場合は、次のことを確認します。

- 外部 Kafka サーバーで次のプロパティを設定した。

（注） この説明はこのドキュメントの対象範囲外であるため、これらのプロパティの説明と使用方法については、Kafka のドキュメントを参照してください。

  - `num.io.threads = 8`
  - `num.network.threads = 3`
  - `message.max.bytes= 30000000`

- データ収集に使用する Kafkaトピックを作成している。

ステップ 1 メインメニューから、**[管理（Administration）] > [Data Gatewayのグローバル設定（Data Gateway Global Settings）] > [データ宛先（Data Destinations）]**を選択します。

ステップ 2 [データ送信先（Data Destinations）] ページで、＋ボタンをクリックします。[接続先の追加（Add Destination）] ページが開きます。

既存の接続先を編集する場合は、✎ボタンをクリックして [接続先の編集（Edit Destination）] ページを開き、パラメータを編集します。

（注） データ送信先を更新すると、更新内容に従って Cisco Crosswork Data Gateway がそのデータ送信先とのセッションを再確立するようになります。データ収集は一時停止され、セッションが再確立されると再開されます。

ステップ 3 次のパラメータの値を入力するか、または変更します。

フィールド	値
接続先名（Destination Name）	わかりやすいデータ送信先名を入力します。名前には、最大 128 文字の英数字と、アンダースコア（「_」）、またはハイフン（「-」）を含めることができます。その他の特殊文字は使用できません。 多数のデータ送信先がある場合は、後で識別できるように、できるだけわかりやすい名前にします。
サーバ タイプ（Server Type）	ドロップダウンから、データ送信先のサーバータイプ（Kafka/gRPC）を選択します。

フィールド	値
エンコーディング（Encoding）	ドロップダウンから、エンコーディング（json/gpbkv）を選択します。
圧縮タイプ（Compression Type）	ドロップダウンから、圧縮タイプを選択します。 Kafka でサポートされている圧縮タイプは、snappy、gzip、lz4、zstd、およびnone です。 （注） zstd 圧縮タイプは、Kafka 2.0 以降でのみサポートされています。 gRPC でサポートされている圧縮タイプは、snappy、gzip、および deflate です。
最大メッセージサイズ（バイト）（Maximum Message Size (bytes)）（Kafka のみ）	最大メッセージサイズを入力します（バイト単位）。 • **デフォルト値**：100000000 バイト/30 MB • **最小**：1000000 バイト/1 MB • **最大**：100000000 バイト/30 MB
バッファメモリ（Kafka のみ）	必要なバッファメモリをバイト単位で入力します。 • **デフォルト値**：52428800 バイト • **最小**：52428800 バイト • **最大**：314572800 バイト
バッチサイズ（バイト）（Batch Size (bytes)）（Kafka のみ）	必要なバッチサイズを入力します（バイト単位）。 • **デフォルト値**：6400000 バイト/6.4 MB • **最小**：16384 バイト/16.38 KB • **最大**：6400000 バイト/6.4 MB
リンガー（ミリ秒）（Linger (milliseconds)）（Kafka のみ）	必要なリンガー時間を入力します（ミリ秒単位）。 • **デフォルト値**：5,000 ms • **最小**：0 ms • **最大**：5000 ms

テレメトリベースの収集の場合は、最適な結果を得るために、[バッチサイズ（Batch size）] を 16384 バイト、[リンガー（Linger）] を 500 ミリ秒に設定することをお勧めします。

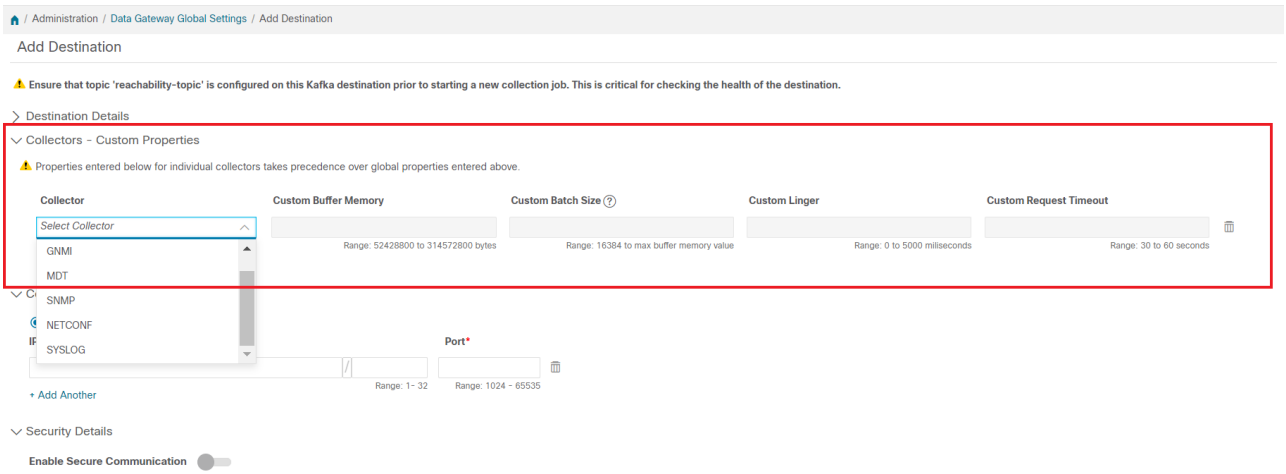
ステップ 4 （オプション）Kafka 宛先のグローバルプロパティとは異なるカスタム値を設定するには、[コレクタ設定のカスタマイズ（Customize Collector Settings）] ウィンドウで、

a) [コレクタ（Collector）] を選択します。
b) 次のフィールドの値を入力します

- **カスタムバッファメモリ**
- **カスタムバッチサイズ**

（注） [カスタムバッチサイズ（Custom Batch Size）] は [カスタムバッファメモリ（Custom Buffer Memory）] の実行時の値を超えることはできません。[カスタムバッファメモリ（Custom Buffer Memory）] フィールドに値を指定しない場合、[カスタムバッチサイズ（Custom Batch Size）] は [バッファメモリ（Buffer Memory）] フィールドの値に対して検証されます。

- [カスタムリンガー（Custom Linger）]
- [カスタム要求タイムアウト（Custom Request Timeout）]



c) [+別を追加（+ Add Another）] をクリックしてこの手順を繰り返し、別のコレクタのカスタム設定を追加します。

（注） ここで入力した個々のコレクタのプロパティは、ステップ 3 で入力したグローバル設定よりも優先されます。ここでフィールドに値を入力しない場合、同じ値はステップ 3 で入力したグローバルプロパティから取得されます。

ステップ 5 [接続の詳細（Connection Details）] オプションから TCP/IP スタックを選択します。IPv4 と IPv6 がサポートされます。

ステップ 6 次の表に従って [接続の詳細（Connection Details）] フィールドに入力します。表示されるフィールドは、選択した接続タイプによって異なります。入力する値は、外部 Kafka または gRPC サーバーで設定されている値と一致する必要があります。

接続タイプ（Connectivity Type）	フィールド
IPv4	必要な [IPv4 アドレス/サブネットマスク（IPv4 Address/Subnet Mask）] と [ポート（Port）] に入力します。[+ もう 1 つ追加する（+ Add Another）] をクリックして、複数の IPv4 アドレスを追加できます。 IPv4 サブネットマスクの範囲は 1 ー 32、ポートの範囲は 1024 ー 65535 です。
IPv6	必要な [IPv6 アドレス/サブネットマスク（IPv6 Address/Subnet Mask）] と [ポート（Port）] に入力します。[+ もう 1 つ追加する（+ Add Another）] をクリックして、複数の IPv6 アドレスを追加できます。 IPv6 サブネットマスクの範囲は 1 ー 128、ポートの範囲は 1024 ー 65535 です。

ステップ 7 （オプション）データ送信先に安全に接続するには、[セキュリティの詳細（Security Details）] で [セキュア通信の有効化（Enable Secure Communication）] オプションを有効にします。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

[セキュア通信の有効化（Enable Secure Communication）] オプションを有効にした場合は、Cisco Crosswork UI（[管理（Administration）] > [証明書の管理（Certificate Management）]）に移動し、新たに追加したデータ送信先に関連する証明書を追加します。この手順は、デバイスとのセキュアな通信を確立するには必須です。詳細については、「証明書の管理（315ページ）」を参照してください。

（注） [セキュア通信の有効化（Enable Secure Communication）] オプションを有効にした後、データ送信先の証明書を追加しなかった場合、Cisco Crosswork はすべての収集ジョブに対して非セキュアモードで接続先に接続します。

データ送信先の削除

データ送信先を削除するには、次の手順を実行します。

始める前に

データ送信先は、どの収集ジョブにも関連付けられていない場合にのみ削除できます。[収集ジョブ（Collection Jobs）] ビューで、データ送信先を使用している収集ジョブがあるかどうかを確認することをお勧めします。

ステップ 1 メインメニューから、**[管理（Administration）] > [Data Gatewayのグローバル設定（Data Gateway Global Settings）] > [データ宛先（Data Destinations）]**を選択します。

ステップ 2 表示された宛先一覧から削除したいデータ宛先を選択し、🗑 ボタンをクリックします。

ステップ 3 [データ送信先の削除（Delete Data Destination(s)）] ポップアップで、[削除（Delete）] をクリックして確認します。

カスタムデバイスパッケージを管理

たとえば、デバイスカバレッジと収集機能をサードパーティ製デバイスに拡張する必要がある場合に、カスタムデバイスパッケージを Cisco Crosswork にアップロードできます。システムデバイスと MIB パッケージは、Crosswork ソフトウェアにバンドルされており、システムインスタンスに自動的にダウンロードされます。システムデバイスと MIB パッケージは変更できません。

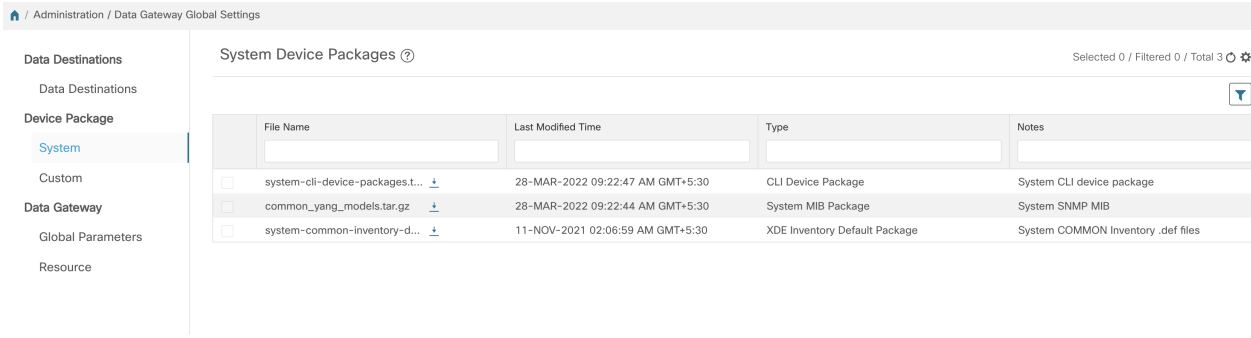
次の 3 つのタイプのカスタムデバイスパッケージを Cisco Crosswork にアップロードできます。

1. **CLI デバイスパッケージ**：CLI ベースの KPI を使用して、サードパーティ製デバイスのデバイス正常性をモニターします。すべてのカスタム CLI デバイスパッケージは、対応する YANG モデルとともにファイル `custom-cli-device-packages.tar.xz` に含まれている必要があります。複数のファイルをサポートできます。
2. **カスタム MIB パッケージ**：カスタム MIB およびデバイスパッケージは、サードパーティ製デバイスに固有であるか、または収集されたデータをフィルタ処理したり、シスコデバイス用に異なる形式にしたりするために使用できます。これらのパッケージは編集できます。すべてのカスタム SNMP MIB パッケージは、YANG モデルとともにファイル `custom-mib-packages.tar.xz` に含める必要があります。複数のファイルをサポートできます。

（注） Cisco Crosswork Data Gateway は、システムにすでに含まれている標準的な MIB のサードパーティ製デバイスで SNMP ポーリングを有効にします。独自の MIB は、収集要求が独自の MIB から MIB テーブル名またはスカラー名を参照する場合にのみ必要です。ただし、要求が OID ベースの場合、MIB は必要ありません。

3. **SNMP デバイスパッケージ**：Cisco Crosswork Data Gateway では、必要な MIB と YANG の説明を追加したカスタム SNMP デバイスパッケージをアップロードすることで、SNMP カバレッジを拡張できます。

[デバイスパッケージ（Device Packages）] ペインには、[管理（Administration）] > [Data Gateway のグローバル設定（Data Gateway Global Settings）] > [デバイスパッケージ（Device Packages] アクセスできます。



デバイスパッケージをダウンロードするには、[ファイル名（File Name）]列の名前の横にある ボタンをクリックします。

カスタムデバイスパッケージを追加

これは、Cisco Crosswork へのデバイスパッケージのアップロードに関するガイドラインです。

1. 1 つのデバイスパッケージ tar.gz ファイルに 1 つ以上の xar ファイルをアップロードできます。
2. Cisco Crosswork では、カスタム MIB パッケージファイルでシステム MIB パッケージファイルを上書きすることはできません。その結果、アップロード試行が失敗します。
3. カスタムデバイスパッケージの TAR ファイルに含まれているのはデバイスパッケージフォルダのみであり、TAR ファイルの一部として親フォルダまたはフォルダの階層が含まれていないことを確認します。正しくインポートされなかった場合、Cisco Crosswork はカスタムデバイスパッケージでジョブを実行すると例外をスローします。
4. Cisco Crosswork は、ファイル拡張子を確認する以外に、アップロードされるファイルを検証しません。

次の手順を実行してカスタム ソフトウェア パッケージをアップロードします。

始める前に

カスタム MIB パッケージの一部として新しい MIB をアップロードする場合は、それらの新しい MIB ファイルを既存のシステム MIB ファイルとともにコレクタ内にアップロードできることを確認します。つまり、ファイル内のすべての依存関係が適切に解決されます。

（注） カスタムデバイスパッケージを実行する収集ジョブのパフォーマンスは、カスタムデバイスパッケージがどの程度最適化されているかによって異なります。Cisco Crosswork にアップロードする前に、デバイスパッケージが展開したい規模に最適化されていることを確認してください。

カスタム MIB と Yang を検証する方法、つまり、それらが Cisco Crosswork にアップロードできるかどうかを確認する方法については、「Use Custom MIBs and Yangs on Cisco DevNet」を参照してください。

ステップ 1 メインメニューから、**[管理（Administration）] > [Data Gateway のグローバル設定（Data Gateway Global Settings）]** を選択します。

ステップ 2 [カスタムデバイスパッケージ（Custom Device Packages）] ウィンドウで、＋をクリックします。

既存のカスタム CLI デバイスパッケージを更新するには、テーブルのファイル名の横にあるアップロードアイコンをクリックします。

ステップ 3 表示される [Add Device Package（デバイスパッケージを追加）] ウィンドウで、インポートするカスタムデバイスパッケージのタイプを [Type（タイプ）] ドロップダウンから選択します。

ステップ 4 [ファイル名（File Name）]の空白フィールドをクリックしてファイルブラウザウィンドウを開き、インポートするデバイスパッケージを選択して [開く（Open）] をクリックします。

ステップ 5 [メモ（Notes）] フィールドにカスタムデバイスパッケージの説明を追加します。多数のパッケージがある場合は、それらを区別できるようにこの手順で説明を加えることをお勧めします。

ステップ 6 [アップロード（Upload）] をクリックします。

次のタスク

影響を受けたすべてのサービスを再起動して、最新のカスタム MIB パッケージの更新を取得します。

カスタムデバイスパッケージを削除

カスタムデバイスパッケージを削除すると、すべての YANG ファイルと XAR ファイルが Cisco Crosswork から削除されます。これは、カスタムデバイスパッケージを使用するすべての収集ジョブに影響します。

カスタムデバイスパッケージを削除するには、次の手順に従います。

ステップ 1 メインメニューから、**[管理（Administration）] > [Data Gatewayのグローバル設定（Data Gateway Global Settings）] > [デバイスパッケージ（Device Packages）] > [カスタム（Custom）]**を選択します。

ステップ 2 [カスタムデバイスパッケージ（Custom Device Packages）] ペインに表示されているリストから、削除するカスタムデバイスパッケージを選択して 🗑 をクリックします。

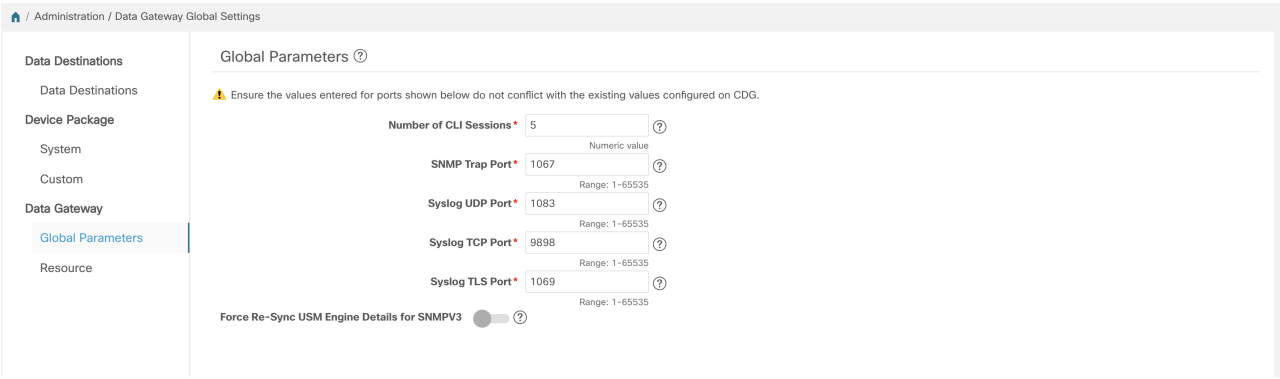
ステップ 3 表示された [カスタムデバイスの削除（Delete Custom Device Package）] ウィンドウで、[削除（Delete）] をクリックして確認します。

Crosswork Data Gateway グローバルパラメータの設定

Crosswork Data Gateway を使用すると、ネットワーク内のすべての Crosswork Data Gateway で次のパラメータを更新できます。

（注） これらの設定には、管理者ユーザーのみがアクセスできます。

ステップ 1 [管理（Administration）] > [データ ゲートウェイ グローバル設定（Data Gateway Global Settings）] > [データ ゲートウェイ（Data Gateway）] > [グローバルパラメータ（Global Parameters）] に移動します。



ステップ 2 次のパラメータの 1 つ以上を変更します。

（注） 更新するポート値が有効なポートであり、既存のポート値と競合しないことを確認してください。デバイス上で同じポート値を設定する必要があります。

パラメータ名	説明
CLI セッションの数	Crosswork Data Gateway とデバイス間の CLI セッションの最大数。デフォルト値は 3 です。 （注） この値は、同じパラメータに設定されている内部構成をオーバーライドします。
SNMP Trap Port	デフォルト値は 1062 です。
Syslog UDP ポート	デフォルト値は 9514 です。
Syslog TCP ポート	デフォルト値は 9898 です。
Syslog TLS ポート	デフォルト値は 6514 です。
NMPV3 の USM エンジンの詳細を強制的に再同期する	USM の詳細は、デバイスが再起動または再イメージ化されるたびに変更されます。SNMPV3 コレクションは、USM の詳細のいずれかが変更されるたびに機能を停止します。 このオプションを有効にすると、最初の収集が失敗した後、変更があるたびに USM の詳細が自動的に同期されます。 デフォルト値は [False] です。

ステップ 3 ポートを更新する場合は、表示される [グローバルパラメータ（Global Parameters）] ウィンドウで [はい（Yes）] を選択して、コレクタを再起動できることを確認します。ポートを更新すると、コレクタは再起動し、実行中の収集ジョブを一時停止します。再起動が完了すると、ジョブは自動的に再開されます。

ステップ 4 [保存（save）] をクリックして変更を適用します。

ネットワーク内の Crosswork Data Gateway でのパラメータの更新が成功したかどうかを示すウィンドウが表示されます。

1. すべての Crosswork Data Gateway が正常に更新された場合、更新が成功したことを示す成功メッセージが UI に表示されます。
2. ネットワーク内の Crosswork Data Gateways のいずれかを更新できなかった場合、UI にエラーウィンドウが表示されます。Crosswork Data Gateway は、復旧中に障害が発生した Crosswork Data Gateway のパラメータを自動的に更新しようとします。一部のコレクタは、リカバリの一環として再始動される場合があります。

（注） Crosswork Data Gateway でグローバルパラメータの更新に失敗する理由の 1 つは、OAM チャネルがダウンしている可能性があります。OAM チャネルが再確立された後、Crosswork Data Gateway はこれらのパラメータを Crosswork Data Gateway に再度送信しようとし（同期していません）、既存の値と比較した後に値を更新します。

次のタスク

いずれかのポートを更新した場合は、[管理（Administration）]>[データゲートウェイ管理（Data Gateway Management）] > [データゲートウェイ（Data Gateways）] タブに移動し、すべての Crosswork Data Gateways の動作状態がアップになっていることを確認します。

Crosswork Data Gateway ダイナミックリソースの割り当て

Crosswork Data Gateway を使用すると、コレクタサービスの実行時にメモリをダイナミックに設定して割り当てることができます。使用頻度の高いコレクタにより多くのメモリを割り当てたり、UI からリソースのバランスを調整したりできます。

（注） これらの設定には、管理者ユーザーのみがアクセスできます。

このページには、コレクタサービス用に現在設定されているメモリと CPU のセットが表示されます。このページでメモリ値に加えた変更は、現在登録されている Crosswork Data Gateway と将来の Crosswork Data Gateway に適用されます。

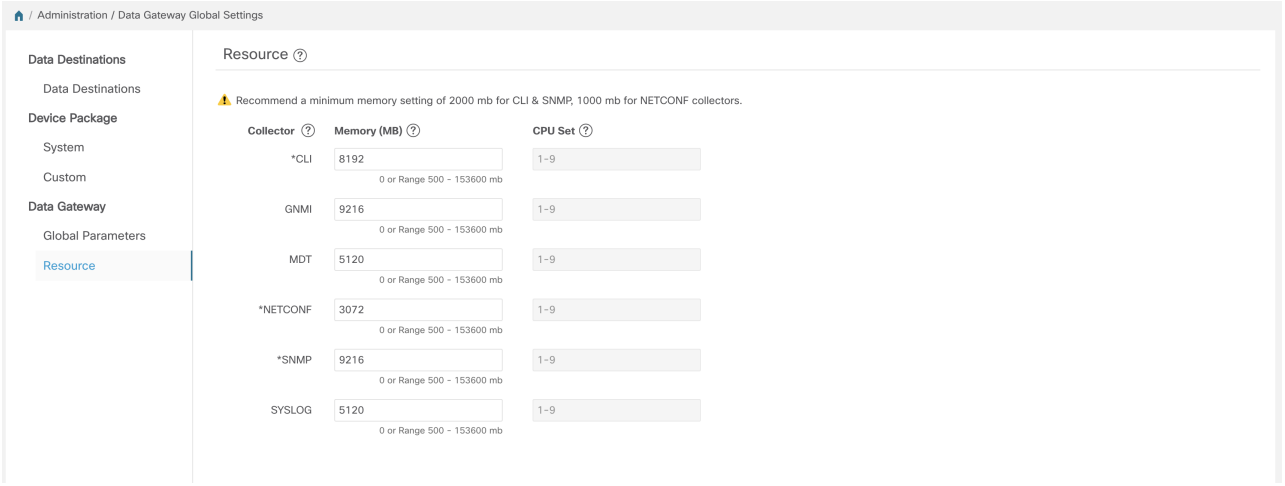
（注） このページに表示されるコレクタのリストは動的です。つまり、展開に固有です。

コレクタのリソース割り当てを更新するには、次の手順を実行します：

（注） Cisco Customer Experience（CX）チームと協力していない限り、これらの設定を変更しないことをお勧めします。

ステップ 1 [管理（Administration）] > [データ ゲートウェイのグローバル設定（Data Gateway Global Settings）] > [データゲートウェイ（Data Gateway）] > [リソース（Resource）] に移動します。

コレクタのリストと、コレクタごとに消費されたリソースがここに表示されます。



ステップ 2 メモリ割り当てを変更するコレクタの [メモリ（Memory）] フィールドに、更新された値を入力します。

ステップ 3 変更が完了したら、[保存（Save）] をクリックします。

コレクタの値を更新すると、コレクタが再起動し、実行中の収集ジョブが一時停止します。再起動が完了すると、ジョブは自動的に再開されます。

Crosswork Data Gateway の収集ジョブの管理

収集ジョブは、Cisco Crosswork Data Gateway が実行することが期待されるタスクである。アプリケーションは、収集ジョブを介してデータ収集を要求します。次に、Cisco Crosswork はこれらの収集ジョブを Cisco Crosswork Data Gateway に割り当てて、要求に対応できるようにします。

Crosswork Data Gateway は、CLI、MDT、SNMP、gNMI（ダイヤルイン）、syslog、NETCONF などの複数のデータ収集プロトコルをサポートしています。サポートされているプロトコルのいずれかを介して転送可能である限り、Crosswork Data Gateway ではどのようなタイプのデータでも収集できます。

Cisco Crosswork には、次の 2 種類のデータ収集要求があります。

1. Cisco Crosswork 内の内部プロセスのデータを転送するためのデータ収集要求。Cisco Crosswork は、この目的のためにシステムジョブを作成します。システムジョブを作成または編集することはできません。
2. 外部データの送信先にデータを転送するためのデータ収集要求。

KPI プロファイルの作成時に外部データ送信先を追加することにより、単一の収集要求で、収集されたデータを外部データ送信先と Cisco Crosswork Health Insights に転送できます。詳細については、『*Cisco Crosswork Change Automation and Health Insights 4.3 User Guide*』の「*Create a New KPI Profile*」の項を参照してください。

（注）
1. Cisco Crosswork Data Gateway は、Cisco Crosswork Data Gateway に対して（リスニング）収集ジョブの要求がない場合は着信トラフィックをドロップします。また、未承認デバイス（つまり、Crosswork Data Gateway に接続されていないデバイス）から受信したデータ、syslog イベント、および SNMP トラップもドロップします。
2. ポーリングされたデータは、Cisco Crosswork Data Gatewayがデータを処理して送信する準備ができるまでデバイスから要求できません。

[収集ジョブ（Collection Jobs）]ページから、Cisco Crosswork に登録されているすべての Crosswork Data Gateway インスタンスで現在アクティブな収集ジョブを表示できます。

Cisco Crosswork の UI の左側のナビゲーションバーで、[管理（Administration）] > [収集ジョブ（Collection Jobs）] を選択します。

[収集ジョブ（Collection Jobs）] ページの左側のペインには、[一括ジョブ（Bulk Jobs）] と [パラメータ化されたジョブ（Parametrized Jobs）] の 2 つのタブがあります。[一括ジョブ（Bulk Jobs）] には、システムによって、またはここの UI および API から作成されたすべての収集ジョブが一覧表示されます。[パラメータ化されたジョブ（Parametrized Jobs）] ペインには、Cisco Crosswork Service Health アプリケーションによって作成されたすべてのアクティブなジョブが一覧表示されます。

（注） [パラメータ化されたジョブ（Parametrized Jobs）] ペインにはデータがなく、Cisco Crosswork Service Health が展開されていない場合は空のままです。

詳細については、収集ジョブのモニター （106 ページ）を参照してください。

収集ジョブのタイプ

Cisco Crosswork の UI（CLI/SNMP のみ）から、または API を使用してデータを要求する収集ジョブの次のリストを作成できます。

• CLI 収集ジョブ （64 ページ）

- SNMP 収集ジョブ （65 ページ）
- MDT 収集ジョブ （74 ページ）
- Syslog 収集ジョブ （76 ページ）
- gNMI 収集ジョブ （87 ページ）
- NETCONF 収集ジョブ （99 ページ）

作成した収集ジョブごとに、Cisco Crosswork Data Gateway は収集要求を実行し、収集したデータを優先データ送信先に転送します。

この章では、Cisco Crosswork の UI から収集ジョブを作成する方法について説明します。API を使用して収集ジョブを作成するには、『Crosswork Data Gateway APIs on Cisco Devnet』を参照してください。

Cisco Crosswork の UI のすべての収集ジョブの初期ステータスは [不明（Unknown）] です。収集ジョブを受信すると、Cisco Crosswork Data Gateway は基本的な検証を実行します。収集ジョブが有効な場合、そのステータスは [成功（Successful）] に変わります。それ以外の場合は [失敗（Failed）] に変わります。

[パターン（Cadence）] の値は秒単位です。この値は、設定されたセンサーデータの収集頻度に応じて、10 ー 2764800 秒（最大 32 日間）の範囲で設定できます。

（注） パターンは 60 秒にすることをお勧めします。

前の実行がまだ進行中であるためにデバイスからの収集がスキップされると、Cisco Crosswork Data Gateway は警告ログを生成します。このシナリオではアラートは生成されません。

CLI 収集ジョブ

Cisco Crosswork Data Gateway は、ネットワークデバイスからの CLI ベースのデータ収集をサポートしています。このタイプの収集ジョブでは、次のコマンドがサポートされています。

- `show` と、短縮バージョンの `sh`
- `traceroute`
- `dir`

CLI 収集を適切に動作させるためには、デバイスにバナー設定を含めないでください。これをオフにする方法については、デバイスのマニュアルを参照してください。

CLI 収集ジョブは、Cisco Crosswork の UI からか、または API を使用して作成できます。詳細については、「Cisco Crosswork の UI からの収集ジョブの作成 （101 ページ）」または Cisco DevNet を参照してください。

次に、Kafka 外部接続先の CLI 収集ジョブのペイロードの例を示します。この例では、特に 2 つの値に注意してください。

1. デバイスは、IP アドレスではなく UUID で識別されます。
2. 宛先も UUID によって参照されます。UI を使用して作成された収集ジョブの場合、Cisco Crosswork は UUID を検索します。独自の収集ジョブを作成するときは、これらの値を調べる必要があります。

```
{
  "collection_job": {
    "application_context": {
      "context_id": "collection-job1",
      "application_id": "APP1"
    },
    "collection_mode": {
      "lifetime_type": "APPLICATION_MANAGED",
      "collector_type": "CLI_COLLECTOR"
    },
    "job_device_set": {
      "device_set": {
        "devices": {
          "device_ids": [
            "658adb03-cc61-448d-972f-4fcec32cbfe8"
          ]
        }
      }
    },
    "sensor_input_configs": [
      {
        "sensor_data": {
          "cli_sensor": {
            "command": "show platform"
          }
        },
        "cadence_in_millisec": "tel:60000"
      }
    ],
    "sensor_output_configs": [
     {
        "sensor_data": {
          "cli_sensor": {
            "command": "show platform"
          }
        },
        "destination": {
          "destination_id": "1e71f2fb-ea65-4242-8efa-e33cec71b369",
          "context_id": "topic1"
        }
      }
    ]
  }
}
```

SNMP 収集ジョブ

Cisco Crosswork Data Gateway では、デバイスでサポートされている OID に基づく SNMP ベースのデータ収集をサポートしています。

SNMP コレクタは、設定プロファイル（収集する MIB オブジェクトのリストと取得先のデバイスのリスト）を取得するためのポーリング要求を Cisco Crosswork に行います。事前にパッケージ化された MIB モジュールのリストまたは MIB モジュールのカスタムリストを検索して、対応する OID を決定します。

（注） Cisco Crosswork Data Gateway は、システムにすでに含まれている標準的な MIB のサードパーティ製デバイスで SNMP ポーリングを有効にします。独自の MIB は、収集要求が独自の MIB から MIB テーブル名またはスカラー名を参照する場合にのみ必要です。ただし、要求が OID ベースの場合、MIB は必要ありません。

OID が解決されると、SNMP コレクタへの入力として提供されます。

カスタムデバイスパッケージを追加 （58 ページ）の説明に従って、Crosswork Data Gateway VM にデバイスパッケージをインポートできます。

データポーリングとトラップでサポートされている SNMP バージョンは次のとおりです。

- ポーリングデータ
  - SNMP V1
  - SNMP V2
  - SNMP V3（no auth nopriv、auth no priv、authpriv）
  - サポートされている認証プロトコル：SHA-1、MD5
  - サポートされている priv プロトコル：DES、3DES、AES128、AES192、AES256、CiscoAES192、CiscoAES256
- トラップ
  - SNMP V1
  - SNMP V2
  - SNMP V3（no auth nopriv、auth no priv、authpriv）

デバイスでの設定例：

次の表に、さまざまな SNMP 機能を有効にするサンプルコマンドを示します。詳細については、プラットフォーム固有のドキュメントを参照してください。

表 *4 :* デバイスで ***SNMP*** を有効にする設定例

バージョン	コマンド	目的
V1	`snmp-server group <group_name> v1` `snmp-server user <user_name> <group_name> v1`	SNMP バージョン、ユーザー/ユーザーグループの詳細を定義します。

	`snmp-server host <host_ip> traps <community_string> udp-port 1062`
	次の例を参考にしてください。
	`snmp-server host a.b.c.d traps test udp-port 1062`
		トラップデータの転送先を定義します。

	`snmp-server traps snmp linkup` `snmp-server traps snmp linkdown`	リンクステータスを通知するトラップを有効にします。
V2c	`snmp-server group <group_name> v2c` `snmp-server user <user_name> <group_name> v2c`	SNMP バージョン、ユーザー/ユーザーグループの詳細を定義します。
	`snmp-server host <host_ip> traps SNMP version <community_string> udp-port 1062` `snmp-server host a.b.c.d traps version 2c v2test udp-port 1062`	トラップデータの転送先を定義します。 （注） ここに記載されている IP アドレスは、Crosswork Data Gateway の仮想IPアドレスである必要があります。
	`snmp-server traps snmp linkup` `snmp-server traps snmp linkdown`	リンクステータスを通知するトラップを有効にします。

バージョン	コマンド	目的
V3 （注） SNMPv3 ユーザーのパスワードは、8 バイト以上にする必要があります。	`snmp-server host <host_IP> traps version 3 priv <user_name> udp-port 1062`	トラップデータの転送先を定義します。 （注） ここに記載されている IP アドレスは、Crosswork Data Gateway の仮想IPアドレスである必要があります。
	`snmp-server user <user_name> <group_name> v3 auth md5 <password> priv aes 128 <password>`	指定した名前付きアクセス リストのメンバに対して認証をイネーブルにするように SNMP サーバ グループを設定します。
	`snmp-server view <user_name> < MIB > included`	何を報告する必要があるかを定義します。
	`snmp-server group <group_name> v3 auth notify <user_name> read <user_name> write <user_name>`	SNMP バージョン、ユーザー/ユーザーグループの詳細を定義します。
	`snmp-serverenabletrapssnmp [authentication] [linkup] [linkdown] [warmstart] [coldstart]`	

バージョン	コマンド	目的
		• オプションのキーワードを一切指定せずに使用した場合、authenticationFailure、linkUp、linkDown、warmStart、および coldStart の各トラップをイネーブルにします。 • キーワード指定で使用した場合は、指定したタイプのトラップのみがイネーブルになります。たとえば、すべてのインターフェイスに対して linkUp と linkDown の SNMP トラップだけをグローバルにイネーブルにするには、このコマンドの **snmp-server enable snmp linkup linkdown** という形式を使用します。

SNMP コレクタは、次の操作をサポートしています。

- スカラー

（注） 1 つの収集で複数のスカラー OID を要求する場合は、デバイスへの 1 つの `getbulkrequestquery` で複数の SNMP GET 要求をパックできます。

- TABLE
- WALK
- COLUMN

これらの操作は、センサー設定で定義されます（以下のペイロード例を参照）。

（注） デバイスの応答時間が 1,500 ミリ秒を超える場合は、オプションの **deviceParams** 属性 **snmpRequestTimeoutMillis**（ペイロード例には表示されていない）を使用する必要があります。デバイスの応答時間が非常に長いことが確実でない限り、**snmpRequestTimeoutMillis** を使用することは推奨されません。

snmpRequestTimeoutMillis の値はミリ秒単位で指定する必要があります。

デフォルトの最小値は 1,500 ミリ秒です。ただし、この属性の最大値に制限はありません。

次に、SNMP 収集ジョブの例を示します。

```
{
  "collection_job": {
    "application_context": {
      "context_id": "collection-job1",
      "application_id": "APP1"
    },
    "collection_mode": {
      "lifetime_type": "APPLICATION_MANAGED",
      "collector_type": "SNMP_COLLECTOR"
    },
    "job_device_set": {
      "device_set": {
        "devices": {
          "device_ids": [
            "c70fc034-0cbd-443f-ad3d-a30d4319f937",
            "8627c130-9127-4ed7-ace5-93d3b4321d5e",
            "c0067069-c8f6-4183-9e67-1f2e9bf56f58"
          ]
        }
      }
    },
    "sensor_input_configs": [
      {
        "sensor_data": {
          "snmp_sensor": {
            "snmp_mib": {
              "oid": "1.3.6.1.2.1.1.3.0",
              "snmp_operation": "SCALAR"
            }
          }
        },
        "cadence_in_millisec": "60000"
      },
      {
        "sensor_data": {
          "snmp_sensor": {
            "snmp_mib": {
              "oid": "1.3.6.1.2.1.31.1.1",
              "snmp_operation": "TABLE"
            }
          }
        },
        "cadence_in_millisec": "60000"
      }
    ],
    "sensor_output_configs": [
      {
        "sensor_data": {
```

```
          "snmp_sensor": {
            "snmp_mib": {
              "oid": "1.3.6.1.2.1.1.3.0",
              "snmp_operation": "SCALAR"
            }
          }
        },
        "destination": {
          "destination_id": "4c2ab662-2670-4b3c-b7d3-b94acba98c56",
          "context_id": "topic1_461cb8aa-a16a-44b8-b79f-c3daf3ea925f"
        }
      },
      {
        "sensor_data": {
          "snmp_sensor": {
            "snmp_mib": {
              "oid": "1.3.6.1.2.1.31.1.1",
              "snmp_operation": "TABLE"
            }
          }
        },
        "destination": {
          "destination_id": "4c2ab662-2670-4b3c-b7d3-b94acba98c56",
          "context_id": "topic2_e7ed6300-fc8c-47ee-8445-70e543057f8a"
        }
      }
    ]
  }
}
```

SNMP トラップ収集ジョブ

SNMP トラップ収集ジョブは、API を介してのみ作成できます。トラップリスナーはポートでリッスンし、（関心のあるトピックに基づいて）受信者にデータをディスパッチします。

Crosswork Data Gateway は UDP ポート 1062 でトラップをリッスンします。

（注） SNMP トラップ収集ジョブを送信する前に、SNMP トラップをデバイス上で正しく設定して、Crosswork Data Gateway の仮想 IP アドレスに送信する必要があります。

SNMP トラップ収集ジョブのワークフロー

SNMP トラップを受信すると、Cisco Crosswork Data Gateway は以下を実行します。

1. デバイスに対して収集ジョブが作成されているかどうかを確認します。
2. トラップバージョンとコミュニティ文字列を確認します。
3. SNMP v3 の場合は、ユーザー認証と priv プロトコルとクレデンシャルも検証します。

（注） SNMPV3 auth-priv トラップは、デバイスまたはルータの engineId に依存して、ローカル USM ユーザーテーブルを維持します。したがって、デバイスまたはルータの engineId が変更されるたびに、トラップの受信が中断されます。トラップの受信を再開するには、それぞれのデバイスを取り外して取り付けてください。

Crosswork Data Gateway は、センサーパスに示されたトラップ OID に基づいてトラップをフィルタ処理し、要求されたトラップのみを送信します。

収集ジョブが無効か、デバイスに設定がないか、またはトラップが受信されない場合、ジョブのステータスは [不明（Unknown）] のままです。サポートされているトラップと MIB のリストについては、「SNMP での収集用に事前にロードしたトラップと MIB のリスト （419 ページ）」を参照してください。

Crosswork Data Gateway は、次の 3 つのタイプの非 YANG/OID ベースのトラップをサポートします。

表 *5:* サポートされている非 *YANG/OID* ベースのトラップのリスト

センサーパス	目的
*	フィルタなしでデバイスからプッシュされたすべてのトラップを取得します。
MIB レベルトラップ	1 つの MIB 通知の OID （例：すべての isis-mib レベルトラップを取得する場合は 1.3.6.1.2.1.138.0）
特定のトラップ	特定のトラップの OID （例：linkUp トラップを取得する場合は 1.3.6.1.6.3.1.1.5.4）

次に、SNMP トラップ収集ジョブの例を示します。

```
{
  "collection_job": {
    "application_context": {
      "context_id": "collection-job1",
      "application_id": "APP1"
    },
    "collection_mode": {
      "lifetime_type": "APPLICATION_MANAGED",
      "collector_type": "TRAP_COLLECTOR"
    },
    "job_device_set": {
      "device_set": {
        "devices": {
          "device_ids": [
            "a9b8f43d-130b-4866-a26a-4d0f9e07562a",
            "8c4431a0-f21d-452d-95a8-84323a19e0d6",
            "eaab2647-2351-40ae-bf94-6e4a3d79af3a"
          ]
        }
      }
    },
    "sensor_input_configs": [
      {
        "sensor_data": {
          "trap_sensor": {
            "path": "1.3.6.1.6.3.1.1.4"
          }
        },
        "cadence_in_millisec": "60000"
      }
```

```
    ],
    "sensor_output_configs": [
      {
        "sensor_data": {
          "trap_sensor": {
            "path": "1.3.6.1.6.3.1.1.4"
          }
        },
        "destination": {
          "destination_id": "4c2ab662-2670-4b3c-b7d3-b94acba98c56",
          "context_id": "topic1_696600ae-80ee-4a02-96cb-3a01a2415324"
        }
      }
    ]
  }
}
```

外部アプリケーションへのトラップ転送の有効化

デバイス上の Crosswork に必要なトラップのみを選択して有効にすることをお勧めします。

接続先で受信したデータのトラップタイプを識別するには、*oid*（OBJECT_IDENTIFIER。`1.3.6.1.6.3.1.1.4.1.0` など）と OidRecords の *oid* に関連付けられている *strValue* を検索します（アプリケーションは対象の OID を照合してトラップの種類を特定できます）。

次に、トラップを外部アプリケーションに転送するための値とペイロードの例を示します。

- リンク アップ

  ```
  1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.4
  ```

- Link Down

  ```
  1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.3
  ```

- Syslog

  ```
  1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.4.1.9.9.41.2.0.1
  ```

- Cold Start

  ```
  1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.1
  ```

```
{
  "nodeIdStr": "BF5-XRV9K1.tr3.es",
  "nodeIdUuid": "C9tZ5lJoSJKf5OZ67+U5JQ==",
  "collectionId": "133",
  "collectionStartTime": "1580931985267",
  "msgTimestamp": "1580931985267",
  "dataGpbkv": [
    {
      "timestamp": "1580931985267",
      "name": "trapsensor.path",
      "snmpTrap": {
        "version": "V2c",
        "pduType": "TRAP",
        "v2v3Data": {
          "agentAddress": "172.70.39.227",
          "oidRecords": [
            {
              "oid": "1.3.6.1.2.1.1.3.0",
              "strValue": "7 days, 2:15:17.02"
```

```
            },
            {
              "oid": "1.3.6.1.6.3.1.1.4.1.0",  // This oid is the Object Identifier.
              "strValue": "1.3.6.1.6.3.1.1.5.3" // This is the value that determines the
 kind of trap.
            },
            {
              "oid": "1.3.6.1.2.1.2.2.1.1.8",
              "strValue": "8"
            },
            {
              "oid": "1.3.6.1.2.1.2.2.1.2.8",
              "strValue": "GigabitEthernet0/0/0/2"
            },
            {
              "oid": "1.3.6.1.2.1.2.2.1.3.8",
              "strValue": "6"
            },
            {
              "oid": "1.3.6.1.4.1.9.9.276.1.1.2.1.3.8",
              "strValue": "down"
            }
          ]
        }
      }
    }
  ],
  "collectionEndTime": "1580931985267",
  "collectorUuid": "YmNjZjEzMTktZjFlOS00NTE5LWI4OTgtY2Y1ZmQxZDFjNWExOlRSQVBfQ09MTEVDVE9S",

  "status": {
    "status": "SUCCESS"
  },
  "modelData": {},
  "sensorData": {
    "trapSensor": {
      "path": "1.3.6.1.6.3.1.1.5.4"
    }
  },
  "applicationContexts": [
    {
      "applicationId": "APP1",
      "contextId": "collection-job-snmp-traps"
    }
  ]
}
```


MDT 収集ジョブ

Crosswork Data Gateway は、モデル駆動型テレメトリ（MDT）を使用してネットワークデバイスからのデータ収集をサポートし、デバイスからのテレメトリストリームを直接消費します（IOS-XR ベースのプラットフォームのみ）。

Crosswork Data Gateway は、次のトランスポートモードのデータ収集をサポートしています。

- MDT TCP ダイヤルアウトモード

Cisco Crosswork は NSO を利用して必要な MDT 設定をデバイスにプッシュし、対応する収集ジョブの設定を Crosswork Data Gateway に送信します。

（注）

- バックアップ操作と復元操作の間に既存の MDT ジョブに何らかの変更（更新）がある場合、Cisco Crosswork はデバイス上で設定更新のジョブを再生しません。これには NSO が関係するためです。NSO/デバイスの設定を復元する必要があります。Cisco Crosswork はデータベース内のジョブのみを復元します。
- YANG モジュールを使用する前に、サポートされているかどうかを確認します。「MDT での収集用に事前にロードした YANG モジュールのリスト （427 ページ）」の項を参照してください。

次に、MDT 収集のペイロードの例を示します。

```
{
 "collection_job": {
  "job_device_set": {
   "device_set": {
    "device_group": "mdt"
   }
  },
  "sensor_output_configs": [{
    "sensor_data": {
     "mdt_sensor": {
      "path":
"Cisco-IOS-XR-infra-statsd-oper:infra-statistics/interfaces/interface/latest/generic-counters"

     }
    },
    "destination": {
     "context_id": "cw.mdt_sensor.cisco-ios-xr-infra-statsd-oper.gpb",
     "destination_id": "c2a8fba8-8363-3d22-b0c2-a9e449693fae"
    }
   },
   {
    "sensor_data": {
     "mdt_sensor": {
      "path":
"Cisco-IOS-XR-infra-statsd-oper:infra-statistics/interfaces/interface/data-rate"
     }
    },
    "destination": {
     "context_id": "cw.mdt_sensor.cisco-ios-xr-infra-statsd-oper.gpb",
     "destination_id": "c2a8fba8-8363-3d22-b0c2-a9e449693fae"
    }
   }
  ],
  "sensor_input_configs": [{
    "sensor_data": {
     "mdt_sensor": {
      "path":
"Cisco-IOS-XR-infra-statsd-oper:infra-statistics/interfaces/interface/data-rate"
     }
    },
    "cadence_in_millisec": "70000"
   }, {
    "sensor_data": {
     "mdt_sensor": {
      "path":
"Cisco-IOS-XR-infra-statsd-oper:infra-statistics/interfaces/interface/latest/generic-counters"
```

```
      }
     },
     "cadence_in_millisec": "70000"
    }
   ],
   "application_context": {
    "context_id": "c4",
    "application_id": "a4-mdt"
   },
   "collection_mode": {
    "lifetime_type": "APPLICATION_MANAGED",
    "collector_type": "MDT_COLLECTOR"
   }
  }
}
```

MDT 収集ジョブのワークフロー

MDT ベースの KPI がデバイスでアクティブ化されると、Cisco Crosswork

1. 構成要求を NSO に送信して、ターゲットデバイスでのデータ収集を有効にします。
2. Crosswork Data Gateway に収集ジョブ作成リクエストを送信します。
3. Crosswork Data Gateway は、収集したデータを指定した宛先に送信するためのディストリビューションを作成します。

Syslog 収集ジョブ

Crosswork Data Gateway は、デバイスからの Syslog ベースのイベント収集をサポートしています。サポートされている Syslog 形式は次のとおりです。

- RFC5424 syslog 形式
- RFC3164 syslog 形式

（注） ネットワーク内のデバイスから syslog データを収集するには、syslog のデータを Crosswork Data Gateway に送信するようにデバイスを設定する必要があります。プラットフォーム固有のマニュアルを参照してください。

デバイスの設定例については、「デバイスでの Syslog（非セキュア）の設定 （82 ページ）」を参照してください。Cisco Crosswork では、デバイスへのセキュアな syslog 通信を設定することもできます。「デバイスでのセキュア Syslog の設定 （83 ページ）」のデバイス設定例を参照してください。

Syslog データの収集

Syslog データは、PRI ベースの SyslogSensor またはフィルタベースの SyslogSensor を指定することでフィルタ処理することができます。ペイロードで指定されたフィルタに一致する syslog イベントのみが、指定された接続先に送信されます。

次に、PRI ベースの SyslogSensor フィルタを使用した Syslog 収集ペイロードの例を示します。

```
{
  "collection_job": {
      "job_device_set": {
      "device_set": {
        "devices": {
          "device_ids": [
            "c6f25a33-92e6-468a-ba0d-15490f1ce787"
          ]
        }
      }
    },
    "sensor_output_configs": [
      {
        "sensor_data": {
          "syslog_sensor": {
            "pris": {
                "facilities": [0, 1, 3, 23,4],
                "severities": [0, 4, 5, 6, 7]
            }
        }
        },
        "destination": {
          "context_id": "syslogtopic",
          "destination_id": "c2a8fba8-8363-3d22-b0c2-a9e449693fae"
        }
      }
    ],
    "sensor_input_configs": [
      {
        "sensor_data": {
          "syslog_sensor": {
            "pris": {
                "facilities": [0,1, 3, 23,4],
                "severities": [0,4, 5, 6, 7]
            }
        }
        },
        "cadence_in_millisec": "60000"
      }
    ],
    "application_context": {
      "context_id": "demomilesstone2syslog",
      "application_id": "SyslogDemo2"
    },
    "collection_mode": {
      "lifetime_type": "APPLICATION_MANAGED",
      "collector_type": "SYSLOG_COLLECTOR"
    }
  }
}
```

フィルタベースの SyslogSensor は、正規表現、PRI、およびシビラティ（重大度） - ファシリティに基づいています。AND または OR を使用して、複数のフィルタ（最大 3 つのフィルタ）を指定および結合できます。デフォルトでは、論理演算子が指定されていない場合は AND 条件が適用されます。次に、フィルタベースの SyslogSensor フィルタを使用した Syslog 収集ペイロードの例を示します。

```
{
      "collection_job": {
      "job_device_set": {
      "device_set": {
      "devices": {
      "device_ids": [
```

```
"ce33ad3c-d6d0-42b7-b24b-67dfa77c6ee8"
          ]
        }
     }
 },
"sensor_output_configs": [{
  "sensor_data": {
    "syslog_sensor": {
      "filters": {
        "filter": [{
          "syslog_filter": {
            "severity_facility": {
                "severity": {
                  "op": "LESSER_THAN",
                   "value": 7
                            },
                   "facility": {
                   "op": "EQUALS",
                   "value": 23
                    }
                 }
              }
          },
          {
            "syslog_filter": {
             "pri_filter": {
              "value": {
                "op": "GREATER_THAN",
                  "value": 180
                             }
                          }
                       }
                    },
                    {
                      "syslog_filter": {
                       "regex_filter": {
                       "pattern": "SSHD\\[\\d+\\]"
                                    }
                                  }
                                }
                                ],
                          "operator": "AND"
                                }
                              }
                            },
       "destination": {
       "context_id": "3filtersand",
        "destination_id": "c2a8fba8-8363-3d22-b0c2-a9e449693fae"
                        }
                      }],
    "sensor_input_configs": [{
    "sensor_data": {
     "syslog_sensor": {
           "filters": {
              "filter": [{
                  "syslog_filter": {
                      "severity_facility": {
                          "severity": {
                              "op": "LESSER_THAN",
                                  "value": 7
                                        },
                              "facility": {
                               "op": "EQUALS",
                                "value": 23
```

```
                                                    }
                                                  }
                                                }
                                              },
                                            {
                                           "syslog_filter": {
                                           "pri_filter": {
                                             "value": {
                                             "op": "GREATER_THAN",
                                             "value": 180
                                                     }
                                                   }
                                                 }
                                               },
                                            {
                                         "syslog_filter": {
                                         "regex_filter": {
                                         "pattern": "SSHD\\[\\d+\\]"
                                             }
                                           }
                                         }
                                       ],
                                  "operator": "AND"
                                      }
                                    }
                                  },
                       "cadence_in_millisec": "60000"
                                 }],
                    "application_context": {
                    "context_id": "AND_syslog.3Filters_oneofeach",
                    "application_id": "testing.postman.syslog.3Filters_oneofeach_AND"
                        },
                   "collection_mode": {
                   "lifetime_type": "APPLICATION_MANAGED",
                   "collector_type": "SYSLOG_COLLECTOR"
                    }
                }
}
```

Syslog 収集ジョブの出力

Cisco Crosswork の UI からデバイスをオンボーディングする場合（[デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）] > [デバイスの詳細（Device Details）]）、[Syslog 形式（Syslog Format）] フィールドで選択した値によって、デバイスから受信した syslog イベントを Syslog コレクタで解析する形式が設定されます。[不明（UNKNOWN）]、[RFC5424]、または [RFC3164] のいずれかを選択できます。

次に、各オプションの出力例を示します。

1. [不明（UNKNOWN）] : Syslog 収集ジョブの出力に、デバイスから受信した syslog イベントが含まれています。

（注） デバイスは RFC5424/RFC3164 形式で syslog イベントを生成するように設定されていても [Syslog 形式（Syslog Format）] フィールドに形式が指定されていない場合、デフォルトでは [不明（UNKNOWN）] と見なされます。

サンプル出力：

```
node_id_str: "xrv9k-VM8"
node_id_uuid: ":i\300\216>\366BM\262\270@\337\225\2723&"
collection_id: 1056
collection_start_time: 1616711596200
msg_timestamp: 1616711596201
data_gpbkv {
  timestamp: 1616711596201
  name: "syslogsensor.path"
  fields {
    name: "RAW"
    string_value: "<6>1 Mar 25 15:34:41.321 PDT - SSHD_ 69570 - - 98949:
RP/0/RP0/CPU0:SSHD_[69570]: %SECURITY-SSHD-6-INFO_SUCCESS : Successfully authenticated
 user \'admin\' from \'40.40.40.116\' on \'vty0\'(cipher \'aes128-ctr\', mac
\'hmac-sha1\') \n"
  }
  fields {
    name: "DEVICE_IP"
    string_value: "40.40.40.30"
  }
}
collection_end_time: 1616711596200
collector_uuid: "17328736-b726-4fe3-b922-231a4a30a54f:SYSLOG_COLLECTOR"
status {
  status: SUCCESS
}
model_data {
}
sensor_data {
  syslog_sensor {
    pris {
      facilities: 0
      facilities: 3
      facilities: 4
      facilities: 23
      severities: 0
      severities: 5
      severities: 6
      severities: 7
    }
  }
}
application_contexts {
  application_id: "SyslogApp-xr-8-job1"
  context_id: "xr-8-job1"
}
version: "1"
```

2. [RFC5424]：デバイスがsyslogイベントをRFC5424形式で生成するように設定され、[Syslog形式（Syslog Format）] フィールドで [RFC5424] 形式が選択されている場合、Syslog収集ジョブ収集の出力には、デバイスから受信したsyslogイベント（RAW）とデバイスからのRFC5424 のベストエフォート解析済みの syslog イベントが含まれます。

（注） Syslog コレクタは、次の Java RegEx パターンに従ってベストエフォートで syslog イベントを解析します。

RFC5424

```
"^<(?<pri>\\d+)>(?<version>\\d{1,3})\\s*(?<date>(([0-9]{4}\\s+)?[a-zA-Z]{3}\\s+\\d+\\s+\\d+:\\d+:\\d+.\\d{3}\\s+[a-zA-Z
9T:.Z-]+))\\s*(?<host>\\S+)\\s*(?<processname>\\S+)\\s*(?<procid>\\S+)\\s*(?<msgid>\\S+)\\s*(?<structureddata>(-|\\[
<message>.+)$";
```

サンプル出力：

```
....
....


collection_start_time: 1596307542398
msg_timestamp: 1596307542405
data_gpbkv {
  timestamp: 1596307542405
  name: "syslogsensor.path"
  fields {
    name: "RAW"
    string_value: "<13>1 2020 Aug  1 12:03:32.461 UTC:  iosxr254node config 65910 -
 - 2782: RP/0/RSP0/CPU0:2020 Aug  1 12:03:32.461 UTC: config[65910]:
%MGBL-SYS-5-CONFIG_I : Configured from console by admin on vty0 (10.24.88.215) \n"
  }
  fields {
    name: "RFC5424"
    string_value: "pri=13,  severity=5,  facility=1,  version=1,
date=2020-08-01T12:03:32.461,  remoteAddress=/172.28.122.254,  host=\'iosxr254node\',
  message=\'2782: RP/0/RSP0/CPU0:2020 Aug  1 12:03:32.461 UTC: config[65910]:
%MGBL-SYS-5-CONFIG_I : Configured from console by admin on vty0 (10.24.88.215) \',
messageId=null, processName=config, structuredDataList=null"
  }
  fields {
    name: "DEVICE_IP"
    string_value: "172.28.122.254"
  }
}
collection_end_time: 1596307542404
collector_uuid: "ac961b09-8f67-4c93-a99a-31eef50f7fa9:SYSLOG_COLLECTOR"
status {
  status: SUCCESS
}
...
...
```

3. [RFC3164]：デバイスが syslog イベントを RFC3164 形式で生成するように設定され、[Syslog 形式（Syslog Format）] フィールドで [RFC3164] 形式が選択されている場合、Syslog ジョブ収集の出力には、RAW（デバイスから受信したもの）syslog イベントとデバイスかの RFC3164 のベストエフォート解析済みの syslog イベントの両方が含まれます。

（注） Syslog コレクタは、次の Java RegEx パターンに従ってベストエフォートで syslog イベントを解析します。

RFC3164

```
"^(<(?<pri>\\d+)>[:]*\\s*)?(?<date>(\\*[a-zA-Z]{3}\\s+\\d+\\s+[0-9]{4}\\s+\\d+:\\d+:\\d+\\.[\\d{3}\\s+]+[[a-zA-Z]{3}[:]*]?\\s+)|([
[a-zA-Z]{3}\\s+\\d+\\s+\\d+:\\d+:\\d+[.]*[\\d{3}\\s+]+[[a-zA-Z]{3}[:]*]*)|([0-9T:.Z-]+))\\s+(?<host>\\S+)?\\s+((?<tag>[^\\[\\s\\]]+
<procid>\\d+)\\])?:)*\\s*(?<message>.+)$";
```

サンプル出力：

```
....
.....
collection_id: 20
collection_start_time: 1596306752737
msg_timestamp: 1596306752743
data_gpbkv {
  timestamp: 1596306752743
  name: "syslogsensor.path"
  fields {
    name: "RAW"
    string_value: "<14>2020 Aug  1 11:50:22.799 UTC:  iosxr254node 2756:
RP/0/RSP0/CPU0:2020 Aug  1 11:50:22.799 UTC: config[65910]: %MGBL-CONFIG-6-DB_COMMIT
 : Configuration committed by user \'admin\'. Use \'show configuration commit changes
 1000000580\' to view the changes. \n"
  }
  fields {
    name: "RFC3164"
    string_value: "pri=14,  severity=6,  facility=1,  version=null,
date=2020-08-01T11:50:22.799,  remoteAddress=/172.28.122.254,  host=\'iosxr254node\',
  message=\'RP/0/RSP0/CPU0:2020 Aug  1 11:50:22.799 UTC: config[65910]:
%MGBL-CONFIG-6-DB_COMMIT : Configuration committed by user \'admin\'. Use \'show
configuration commit changes 1000000580\' to view the changes. \', tag=2756"
  }
  fields {
    name: "DEVICE_IP"
    string_value: "172.28.122.254"
  }
}
collection_end_time: 1596306752742
collector_uuid: "ac961b09-8f67-4c93-a99a-31eef50f7fa9:SYSLOG_COLLECTOR"
status {
  status: SUCCESS
}
....
....
```

Syslog コレクタが [Syslog 形式（Syslog Format）] フィールドで指定された形式に従って syslog イベントを解析できない場合、Syslog 収集ジョブの出力には、デバイスから受信した syslog イベント（RAW）が含まれます。

デバイスでの Syslog（非セキュア）の設定

この項では、デバイスで RFC3164 形式または RFC5424 形式の syslog を設定するための設定例を示します。

RFC3164 Syslog 形式の設定

（注） 次のコードで強調表示されている設定は、解析された出力でのフォーマットの問題を回避するために必要です。

Cisco IOS XR デバイスの場合：

```
logging <CDG IP> port 9514 OR logging <CDG IP> vrf <vrfname> port 9514
logging trap [severity]
logging facility [facility value]
logging suppress duplicates
service timestamps log datetime msec show-timezone year
logging hostnameprefix <some host related prefix e.g.iosxrhost2>
```

Cisco IOS XE デバイスの場合：

```
no logging message-counter syslog
logging trap <serverity>
logging facility <facility>
logging host <CDG IP> transport tcp port 9898 session-id string <sessionidstring> -->
To use TCP channel
OR
logging host <CDG IP> transport udp port 9514 session-id string <sessionidstring> --->
To use UDP channel
OR
logging host <CDG IP> vrf Mgmt-intf transport udp port 9514 session-id string
<sessionidstring> --> To use UDP via vrf
service timestamps log datetime msec year show-timezone
```

RFC5424 Syslog 形式の設定

Cisco IOS XR デバイスの場合：

```
logging <CDG IP> port 9514 OR logging <server 1> vrf <vrfname> port 9514
logging trap [severity]
logging facility [facility value]
logging suppress duplicates
service timestamps log datetime msec show-timezone year
logging hostnameprefix <some host related prefix e.g.iosxrhost2>
logging format rfc5424
```

Cisco IOS XE デバイスの場合：

```
no logging message-counter syslog
logging trap <serverity>
logging facility <facility>
logging host <CDG IP> transport tcp port 9898 session-id string <sessionidstring> -->
To use TCP channel
OR
logging host <CDG IP> transport udp port 9514 session-id string <sessionidstring> --->
To use UDP channel
OR
logging host <CDG IP> vrf Mgmt-intf transport udp port 9514 session-id string
<sessionidstring> --> To use UDP via vrf
service timestamps log datetime msec year show-timezone
logging trap syslog-format 5424 --> if applicable
```

デバイスでのセキュア Syslog の設定

デバイスへのセキュアな syslog 通信を確立するには、次の手順を実行します。

1. Cisco Crosswork の [証明書管理 UI（Certificate Management）] ページから Cisco Crosswork 信頼チェーンをダウンロードします。
2. Cisco Crosswork 信頼チェーンを使用してデバイスを設定します。

Syslog 証明書のダウンロード

1. Cisco Crosswork の UIで、[管理（Administration）] > [証明書管理（Certificate Management）] に移動します。
2. 「**crosswork-device-syslog**」行で [i] をクリックします。
3. [すべてエクスポート（Export All）] をクリックして、証明書をダウンロードします。

   次のファイルがシステムにダウンロードされます。

デバイスでの Cisco Crosswork トラストポイントの設定

TLS を有効にする XR デバイスの設定例

```
RP/0/RSP0/CPU0:ASR9k(config)#crypto ca trustpoint syslog-root
RP/0/RSP0/CPU0:ASR9k(config-trustp)#enrollment terminal
RP/0/RSP0/CPU0:ASR9k(config-trustp)#crl optional
RP/0/RSP0/CPU0:ASR9k(config-trustp)#commit
RP/0/RSP0/CPU0:ASR9k(config-trustp)#end
RP/0/RSP0/CPU0:ASR9k#
RP/0/RSP0/CPU0:ASR9k#crypto ca authenticate syslog-root
Fri Jan 22 11:07:41.880 GMT


Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIGKzCCBBOgAwIBAgIRAKfyU89yjmrXVDRKBWuSGPgwDQYJKoZIhvcNAQELBQAw
bDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAkNBMREwDwYDVQQHEwhTYW4gSm9zZTEa
.....................................................................
.....................................................................
jPQ/UrO8N3sC1gGJX7CIIh5cE+KIJ51ep8i1eKSJ5wHWRTmv342MnG2StgOTtaFF
vrkWHD02o6jRuYXDWEUptDOg8oEritZb+SNPXWUc/2mbYog6ks6EeMC69VjkZPo=
-----END CERTIFICATE-----

Read 1583 bytes as CA certificate
  Serial Number  : A7:F2:53:CF:72:8E:6A:D7:54:34:4A:05:6B:92:18:F8
  Subject:
                CN=Crosswork Device Root CA,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
  Issued By      :
                CN=Crosswork Device Root CA,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
  Validity Start : 02:37:09 UTC Sat Jan 16 2021
  Validity End   : 02:37:09 UTC Thu Jan 15 2026
  SHA1 Fingerprint:
                209B3815271C22ADF78CB906F6A32DD9D97BBDBA
```

```
Fingerprint: 2FF85849EBAAB9B059ACB9F5363D5C9CDo you accept this certificate? [yes/no]:
yes
RP/0/RSP0/CPU0:ASR9k#config
RP/0/RSP0/CPU0:ASR9k(config)#crypto ca trustpoint syslog-inter
RP/0/RSP0/CPU0:ASR9k(config-trustp)#enrollment terminal
RP/0/RSP0/CPU0:ASR9k(config-trustp)#crl optional
RP/0/RSP0/CPU0:ASR9k(config-trustp)#commit
RP/0/RSP0/CPU0:ASR9k#crypto ca authenticate syslog-inter
Fri Jan 22 11:10:30.090 GMT


Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIGFDCCA/ygAwIBAgIRAkhqHQXcJzQzeQK6U2wn8PIwDQYJKoZIhvcNAQELBQAw
bDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAkNBMREwDwYDVQQHEwhTYW4gSm9zZTEa
.............................................................
.............................................................
5lBk617z6cxFER5c+/PmJFhcreisTxXg1aJbFdnB5C8f+0uUIdLghykQ/zaZGuBn
AAB70c9r9OeKGJWzvv1e2U8HH1pdQ/nd
-----END CERTIFICATE-----

Read 1560 bytes as CA certificate
  Serial Number  : 02:48:6A:1D:05:DC:27:34:33:79:02:BA:53:6C:27:F0:F2
  Subject:
                CN=device-syslog,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
  Issued By      :
                CN=Crosswork Device Root CA,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
  Validity Start : 02:37:11 UTC Sat Jan 16 2021
  Validity End   : 02:37:11 UTC Mon Jan 16 2023
  SHA1 Fingerprint:
                B06F2BFDE95413A8D08A01EE3511BC3D42F01E59

CA Certificate validated using issuer certificate.
RP/0/RSP0/CPU0:ASR9k#show crypto ca certificates
Fri Jan 22 15:45:17.196 GMT


Trustpoint       : syslog-root
================================================
CA certificate
  Serial Number  : A7:F2:53:CF:72:8E:6A:D7:54:34:4A:05:6B:92:18:F8
  Subject:
        CN=Crosswork Device Root CA,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
  Issued By      :
        CN=Crosswork Device Root CA,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
  Validity Start : 02:37:09 UTC Sat Jan 16 2021
  Validity End   : 02:37:09 UTC Thu Jan 15 2026
  SHA1 Fingerprint:
         209B3815271C22ADF78CB906F6A32DD9D97BBDBA


Trustpoint       : syslog-inter
================================================
CA certificate
  Serial Number  : 02:48:6A:1D:05:DC:27:34:33:79:02:BA:53:6C:27:F0:F2
  Subject:
        CN=device-syslog,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
  Issued By      :
        CN=Crosswork Device Root CA,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
  Validity Start : 02:37:11 UTC Sat Jan 16 2021
  Validity End   : 02:37:11 UTC Mon Jan 16 2023
```

```
  SHA1 Fingerprint:
         B06F2BFDE95413A8D08A01EE3511BC3D42F01E59
RP/0/RSP0/CPU0:ASR9k(config)#logging tls-server syslog-tb131
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#tls-hostname 10.13.0.159
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#trustpoint syslog-inter
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#severity debugging
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#vrf default
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#commit
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#exit
RP/0/RSP0/CPU0:ASR9k(config)#exit
RP/0/RSP0/CPU0:ASR9k#exit
RP/0/RSP0/CPU0:ASR9k#show running-config logging
Fri Jan 22 11:17:19.385 GMT
logging tls-server syslog-tb131
vrf default
severity debugging
trustpoint syslog-inter
tls-hostname <CDG Southbound IP>
!
logging trap debugging
logging format rfc5424
logging facility user
logging hostnameprefix ASR9k
logging suppress duplicates

RP/0/RSP0/CPU0:ASR9k#
```

TLS を有効にする XE デバイスの設定例

```
csr8kv(config)#crypto pki trustpoint syslog-root
csr8kv(ca-trustpoint)#enrollment terminal
csr8kv(ca-trustpoint)#revocation-check none
csr8kv(ca-trustpoint)#chain-validation stop
csr8kv(ca-trustpoint)#end
csr8kv(config)#crypto pki authenticate syslog-root

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIFPjCCAyYCCQCO6pK5AOGYdjANBgkqhkiG9w0BAQsFADBhMQswCQYDVQQGEwJV
UzELMAkGA1UECAwCQ0ExETAPBgNVBAcMCE1pbHBpdGFzMQ4wDAYDVQQKDAVDaXNj
.....................................................................
.....................................................................
JbimOpXAncoBLo14DXOJLvMVRjn1EULE9AXXCNfnrnBx7jL4CV+qHgEtF6oqclFW
JEA=
-----END CERTIFICATE-----

Certificate has the following attributes:
       Fingerprint MD5: D88D6D8F E53750D4 B36EB498 0A435DA1
      Fingerprint SHA1: 649DE822 1C222C1F 5101BEB8 B29CDF12 5CEE463B

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported


csr8kv(config)#crypto pki trustpoint syslog-intermediate
csr8kv(ca-trustpoint)#enrollment terminal
csr8kv(ca-trustpoint)#revocation-check none
csr8kv(ca-trustpoint)#chain-validation continue syslog-root
csr8kv(ca-trustpoint)#end
csr8kv(config)#crypto pki authenticate syslog-intermediate

Enter the base 64 encoded CA certificate.
```

```
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIFfTCCA2WgAwIBAgICEAAwDQYJKoZIhvcNAQELBQAwXDELMAkGA1UEBhMCVVMx
EzARBgNVBAgMCkNhbGlmb3JuaWExDjAMBgNVBAoMBUNpc2NvMQ4wDAYDVQQLDAVT
.............................................................
.............................................................
Nmz6NQynD7bxdQa9Xq9kyPuY3ZVKXkf312IRH0MEy2yFX/tAen9JqOeZ1g8canmw
TxsWA5TLzy1RmxqQh88f0CM=
-----END CERTIFICATE-----
Trustpoint 'syslog-intermediate' is a subordinate CA.
but certificate is not a CA certificate.
Manual verification required
Certificate has the following attributes:
       Fingerprint MD5: FE27BDBE 9265208A 681670AC F59A2BF1
      Fingerprint SHA1: 03F513BD 4BEB689F A4F4E001 57EC210E 88C7BD19

csr8kv(config)#logging host <CDG Southbound IP> transport tls port 6514
csr8kv(config)#logging trap informational syslog-format rfc5424
csr8kv(config)#logging facility user
csr8kv(config)#service timestamps log datetime msec year show-timezone

csr8kv(config)#logging tls-profile tlsv12
```

FQDN をサポートするための Syslog 構成

サンプルのデバイス構成に加えて次のコマンドを実行して、TLS が FQDN をサポートできるようにします。

1. ドメイン名を設定し、DNS IP をデバイスで設定する必要があります。

```
RP/0/RSP0/CPU0:ASR9k#config
RP/0/RSP0/CPU0:ASR9k(config)#domain name <DNS domain name>
RP/0/RSP0/CPU0:ASR9k(config)#domain name-server <DNS server IP>
```

2. tls-hostname の CDG VIP FQDN を構成する

```
RP/0/RSP0/CPU0:ASR9k(config)#logging tls-server syslog-tb131
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#tls-hostname <CDG VIP FQDN>
```

gNMI 収集ジョブ

Cisco Crosswork は、Cisco Crosswork Data Gateway を介した gRPC ネットワーク管理インターフェイス（gNMI）ベースのテレメトリデータの収集をサポートしています。サブスクリプションに基づく gNMI ダイヤルイン（gRPC ダイヤルイン）ストリーミングのテレメトリデータと、要求した接続先への後続のサブスクリプション応答（通知）のリレーのみをサポートします。

（注） モデルがターゲットのデバイスプラットフォームでサポートされている限り、gNMI 収集はサポートされます。 gNMI 収集ジョブを送信するには、デバイスで gNMI を設定しておく必要があります。プラットフォーム固有のマニュアルを確認します。

デバイスで gNMI を設定するには、「デバイスの設定例：gNMI （94 ページ）」を参照してください。

gNMI では、セキュアモードと非セキュアモードの両方をデバイスで共存させることができます。Cisco Crosswork は、インベントリで渡された情報に基づいて、非セキュアモードよりもセキュアモードを優先します。

デバイスがリロードされると、gNMI コレクタは既存のサブスクリプションがデバイスに再サブスクライブされるようにします。

gNMI 仕様には、メッセージの終わりをマークする方法がありません。したがって、接続先とディスパッチのパターンは gNMI コレクタではサポートされません。

Cisco Crosswork Data Gateway は、gNMI の次のタイプのサブスクライブオプションをサポートしています。

表 *6 : gNMI* のサブスクリプションオプション

タイプ	サブタイプ	説明
[1 回（Once）]		指定したすべてのパスについて、システム設定の現在のスナップショットを 1 回だけ収集して送信します。
Stream	SAMPLE	パターンベースの収集。
	ON_CHANGE	最初の応答には、サブスクライブしているパスのすべての要素の状態が含まれ、その後に、変更リーフ値に対する後続の更新が含まれています。
	TARGET_DEFINED	ルータ/デバイスは、サブスクライブしているパス（つまり、SAMPLE または ON_CHANGE のいずれか）に基づいてリーフ単位でサブスクリプションのモードを選択します。

Crosswork Data Gateway は、デバイスへの単一のサブスクリプションリストで複数のサブスクリプションパスをサブスクライブする機能をサポートしています。たとえば、ON_CHANGE とサブスクリプションモードの ONCE 収集ジョブの組み合わせを指定できます。ON_CHANGE モードは、指定したパスの特定の要素の変更時にのみデータを収集します。一方、サブスクリプションモードの ONCE は、指定したパスの現在のシステムデータを 1 回だけ収集して送信します。

（注）

- Crosswork Data Gateway は、1 つ以上のモードのサポートの宣言をデバイスに依存します。
- デフォルト値の gNMI センサーパスはペイロードに表示されません。これは既知の protobuf の動作です。

  boolean の場合、デフォルト値は false です。enum の場合は、gnmi.proto が指定されます。

  例 1：

```
message GNMIDeviceSetting {
bool suppress_redundant = 1;
bool allow_aggregation = 4;
bool updates_only = 6;
}
```

  例 2：

```
enum SubscriptionMode {
TARGET_DEFINED = 0; //default value will not be printed
ON_CHANGE = 1;
SAMPLE = 2;
}
```

次に、gNMI 収集ペイロードのサンプルを示します。このサンプルでは、デバイスグループ「milpitas」の 2 つの集まりが表示されます。最初は、60 秒ごとに「mode」=「SAMPLE」を使用してインターフェイス統計情報を収集します。2 番目のジョブは、インターフェイスの状態（アップ/ダウン）の変更をキャプチャします。これが検出されると、単に「mode="STREAM"」がコレクタに送信されます。

```
{
    "collection_job": {
        "job_device_set": {
            "device_set": {
                "device_group": "milpitas"
            }
        },
        "sensor_output_configs": [{
            "sensor_data": {
                "gnmi_standard_sensor": {
                    "Subscribe_request": {
                        "subscribe": {
                            "subscription": [{
                                "path": {
                                    "origin": "openconfig-interfaces",
                                    "elem": [{
                                        "name": "interfaces/interface/state/ifindex"
                                    }]
                                },
                                "mode": "SAMPLE",
                                "sample_interval": 10000000000
                            }, {
                                "path": {
                                    "origin": "openconfig-interfaces",
                                    "elem": [{
                                        "name":
"interfaces/interfaces/state/counters/out-octets"
                                    }]
                                },
```

```
                                    "mode": "ON_CHANGE",
                                    "sample_interval": 10000000000
                                }],
                                "mode": "STREAM",
                                "encoding": "JSON"
                            }
                        }
                    }
                },
                "destination": {
                    "context_id": "hukarz",
                    "destination_id": "c2a8fba8-8363-3d22-b0c2-a9e449693fae"
                }
            }],
            "sensor_input_configs": [{
                "sensor_data": {
                    "gnmi_standard_sensor": {
                        "Subscribe_request": {
                            "subscribe": {
                                "subscription": [{
                                    "path": {
                                        "origin": "openconfig-interfaces",
                                        "elem": [{
                                            "name": "interfaces/interface/state/ifindex"
                                        }]
                                    },
                                    "mode": "SAMPLE",
                                    "sample_interval": 10000000000
                                }, {
                                    "path": {
                                        "origin": "openconfig-interfaces",
                                        "elem": [{
                                            "name":
"interfaces/interfaces/state/counters/out-octets"
                                        }]
                                    },
                                    "mode": "ON_CHANGE",
                                    "sample_interval": 10000000000
                                }],
                                "mode": "STREAM",
                                "encoding": "JSON"
                            }
                        }
                    }
                },
                "cadence_in_millisec": "60000"
            }],
            "application_context": {
                "context_id": "testing.group.gnmi.subscription.onchange",
                "application_id": "testing.postman.gnmi.standard.persistent"
            },
            "collection_mode": {
                "lifetime_type": "APPLICATION_MANAGED",
                "collector_type": "GNMI_COLLECTOR"
            }
        }
}
```

デバイスと Crosswork Data Gateway 間でのセキュア gNMI 通信の有効化

Cisco Crosswork は 1 つのルート CA 証明書（自己署名または信頼できるルート CA による署名）のみを使用できます。つまり、すべてのデバイス証明書は同じ CA による署名であることが必要です。

信頼できる別のルート CA によって署名された証明書がある場合は、最初の手順をスキップして手順 2 から開始し、Cisco Crosswork に rootCA 証明書をインポートできます。

Cisco Crosswork とデバイス間でセキュア gNMI を有効にするには、次の手順を実行します。

1. 証明書を生成します。「デバイス証明書の生成 （91 ページ）」を参照してください。

   。
2. Cisco Crosswork の [Crosswork 証明書管理（Crosswork Certificate Management）] の UI に証明書をアップロードします。「gNMI 証明書の設定 （92 ページ）」を参照してください。
3. Cisco Crosswork の UI からセキュア gNMI ポートの詳細を使用してデバイス設定を更新します。Cisco Crosswork からのデバイスのプロトコルの更新 （93 ページ）を参照してください
4. デバイスで gNMI を有効にします。「デバイスの設定例：gNMI （94 ページ）」を参照してください。
5. デバイスで証明書とデバイスキーを設定します。デバイスへの証明書のインポート （97 ページ）。

デバイス証明書の生成

この項では、OpenSSL を使用して証明書を作成する方法について説明します。

証明書を生成する手順は、Open SSL と Microsoft で検証済みです。この手順では、Open SSL を使用してデバイス証明書を生成する手順について説明しました。

（注） Open SSL または Microsoft 以外のユーティリティを使用してデバイス証明書を生成するには、シスコサポートチームにお問い合わせください。

1. **rootCA の作成**

```
# openssl genrsa -out rootCA.key
# openssl req -subj /C=/ST=/L=/O=/CN=CrossworkCA -x509 -new -nodes -key rootCA.key
-sha256 -out rootCA.pem -days 1024
```

   上記のコマンドでは、`days` 属性によって証明書の有効期間が決まります。最小値は 30 日です。つまり、30 日ごとに証明書を更新する必要があります。値を 365 日に設定することをお勧めします。

2. **デバイスキーと証明書の作成**

```
# openssl genrsa -out device.key
# openssl req -subj /C=/ST=/L=/O=/CN=Crosswork -new -key device.key -out device.crs
# openssl x509 -req -extfile <(printf "subjectAltName=IP.0: 10.58.56.18") -in
device.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -sha256 -out device3.crt
 -days 1024
```

   複数のデバイスがある場合、複数のデバイス証明書を作成する代わりに、`subjectAltName` に複数のデバイス IP アドレスをカンマで区切って指定できます。

```
# openssl x509 -req -extfile <(printf "subjectAltName=IP.0: 10.58.56.18, IP.1:
10.58.56.19, IP.2: 10.58.56.20 ..... ") -in device.csr -CA rootCA.pem -CAkey rootCA.key
 -CAcreateserial -sha256 -out device.crt -days 1024
```

gNMI 証明書の設定

Crosswork Data Gateway は gNMI クライアントとして機能し、デバイスは gNMI サーバーとして機能します。Crosswork Data Gateway は、信頼チェーンを使用してデバイスを検証します。すべてのデバイスにグローバルな信頼チェーンがあることが期待されます。信頼チェーンが複数ある場合は、すべてのデバイス信頼チェーン（単一または複数のベンダー）を 1 つの .pem ファイルに追加し、この .pem ファイルを Crosswork 証明書管理の UI にアップロードします。

（注） Crosswork にアップロードできる gNMI 証明書は 1 つのみです。

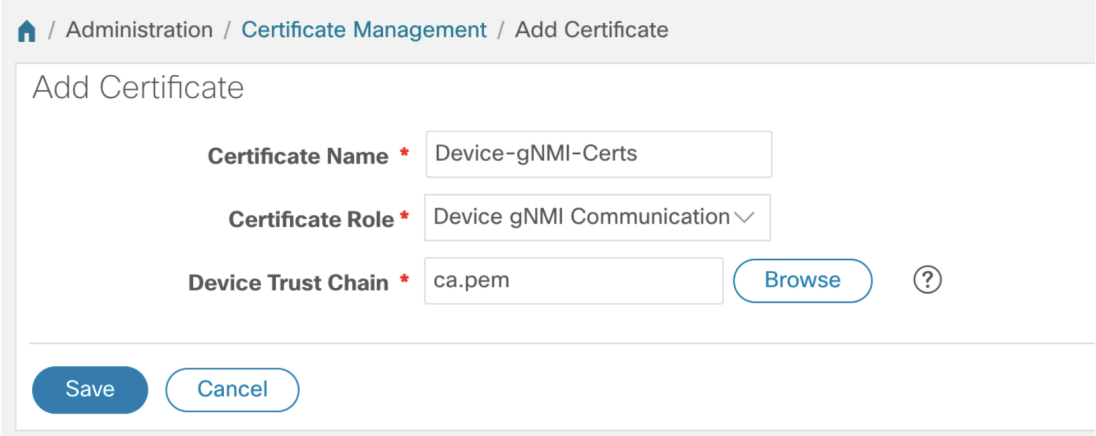
gNMI 証明書を設定するには、次の手順を実行します。

ステップ 1 Cisco Crosswork の UI から、[管理（Administration）] > [証明書管理（Certificate Management）] に移動します。

ステップ 2 [+] アイコンをクリックして証明書を追加します。

ステップ 3 [証明書の追加（Add Certificate）] ウィンドウで、次の詳細情報を入力します。

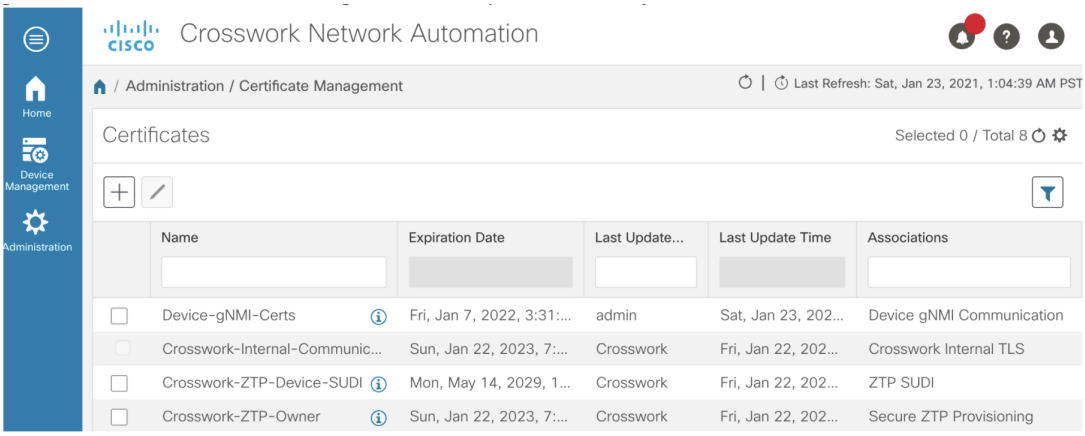
- [デバイス証明書名（Device Certificate Name）]：証明書の名前を入力します。
- [証明書のロール（Certificate Role）]：ドロップダウンリストから [デバイス gNMI 通信（Device gNMI Communication）] を選択します。
- [デバイス信頼チェーン（Device Trust Chain）]：rootCA ファイルの場所までローカルファイルシステムを参照し、そのファイルをアップロードします。



（注） gNMI証明書がすでに設定されている場合で、別の信頼チェーンを使用してデバイスをオンボーディングするときは、既存の .pem ファイルを更新して新しい CA の詳細を含めます。リストから既存の gNMI 証明書を選択し、[編集（Edit）] アイコンをクリックして、新しい .pem ファイルをアップロードします。

ステップ 4 [保存（Save）] をクリックします。

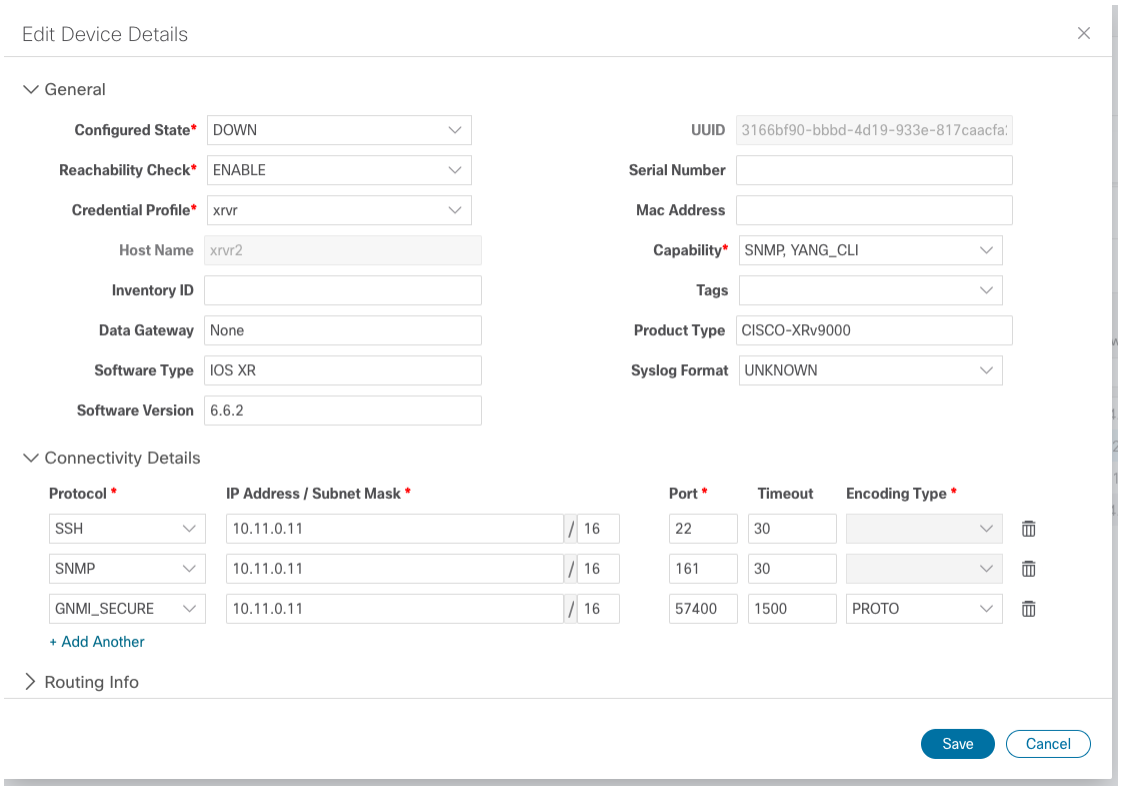
gNMI 証明書が正常に追加されると、設定済みの証明書のリストに表示されます。



Cisco Crosswork からのデバイスのプロトコルの更新

Cisco Crosswork で gNMI 証明書を設定したら、Cisco Crosswork の UI（[デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）]）から、または .csv ファイルでプロトコルの詳細を **GNMI_SECURE** ポートとして指定して、デバイスをセキュアなプロトコルの詳細を使用して更新します。

次の図に、デバイスの更新されたセキュアプロトコルの詳細を示します。



デバイスの設定例：*gNMI*

Cisco IOS XR デバイス

1. HTTP/2 接続で gRPC を有効にします。

```
Router#configure
Router(config)#grpc
Router(config-grpc)#port <port-number>
```

ポート番号の範囲は 57344 ～ 57999 です。ポート番号が使用できない場合は、エラーが表示されます。

2. セッション パラメータを設定します。

```
Router(config)#grpc{ address-family | dscp | max-request-per-user | max-request-total
 | max-streams |
max-streams-per-user | no-tls | service-layer | tls-cipher | tls-mutual |
tls-trustpoint | vrf }
```

値は次のとおりです。

- `address-family`：アドレス ファミリ識別子タイプを設定します
- `dscp`：送信された gRPC で QoS マーキング DSCP を設定します
- `max-request-per-user`：ユーザーあたりの同時要求の最大数を設定します
- `max-request-total`：合計同時要求の最大数を設定します

- `max-streams`：同時gRPC要求の最大数を設定します。サブスクリプションの上限は128要求です。デフォルトは32要求です
- `max-streams-per-user`：ユーザーあたりの同時gRPC要求の最大数を設定します。サブスクリプションの上限は128要求です。デフォルトは32要求です
- `no-tls`：トランスポート レイヤ セキュリティ（TLS）を無効化します。TLSはデフォルトで有効になっています。
- `service-layer`：gRPCサービス レイヤの設定を有効にします
- `tls-cipher`：gRPC TLS暗号スイートを有効にします
- `tls-mutual`：相互認証を設定します
- `tls-trustpoint`：トラストポイントを設定します
- `vrf`：サーバー VRFを有効にします

3. TPA（サードパーティ製アプリケーションのトラフィック保護）を有効にします。

```
tpa
vrf default
  address-family ipv4
   default-route mgmt
   update-source dataports MgmtEth0/RP0/CPU0/0
```

Cisco IOS XE デバイス

次に、gNMIサーバを非セキュア モードで有効にする例を示します。

```
Device# configure terminal
Device(config)# gnmi-yang
Device(config)# gnmi-yang server
Device(config)# gnmi-yang port 50000 <The default port is 50052.>
Device(config)# end
Device
```

次に、gNMIサーバをセキュア モードで有効にする例を示します。

証明書とトラストポイントは、セキュアgNMIサーバにのみ必要です。

```
Device# configure terminal
Device(config)# gnmi-yang server
Device(config)# gnmi-yang secure-server
Device(config)# gnmi-yang secure-trustpoint trustpoint1
Device(config)# gnmi-yang secure-client-auth
Device(config)# gnmi-yang secure-port 50001 <The default port is 50051.>
Device(config)# end
Device
```

デバイスの証明書

証明書とトラストポイントは、セキュアgNMIサーバにのみ必要です。

Linux での OpenSSL を使用した証明書の作成

次に、Linuxマシン上でOpenSSLを使用して証明書を作成する例を示します。

```
# Setting up a CA
openssl genrsa -out rootCA.key 2048
openssl req -subj /C=/ST=/L=/O=/CN=rootCA -x509 -new -nodes -key rootCA.key -sha256 -out
 rootCA.pem

# Setting up device cert and key
openssl genrsa -out device.key 2048
openssl req -subj /C=/ST=/L=/O=/CN=<hostnameFQDN> -new -key device.key -out device.csr
openssl x509 -req -in device.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -out
device.crt -sha256
# Encrpyt device key - needed for input to IOS
openssl rsa -des3 -in device.key -out device.des3.key -passout pass:<password - remember
 this for later>

# Setting up client cert and key
openssl genrsa -out client.key 2048
openssl req -subj /C=/ST=/L=/O=/CN=gnmi_client -new -key client.key -out client.csr
openssl x509 -req -in client.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -out
client.crt -sha256
```

Cisco IOS XR デバイスへの証明書のインストール

Cisco IOS XR に証明書をインストールするには、次のパスのファイルを置き換えます。

1. XR マシンにログインします。
2. 端末プロンプトで run コマンドを入力します。

   ```
   RP/0/RP0/CPU0:xrvr-7.2.1#run
   ```

3. 次のディレクトリに移動します。

   ```
   cd /misc/config/grpc
   ```

4. 次のファイルの内容を置き換えます。
   - ems.pem の内容を device.crt に置き換えます。
   - ems.key の内容を device.key に置き換えます。
   - ca.cert の内容を rootCA.pem に置き換えます。

Cisco IOS XE デバイスへの証明書のインストール

次に、Cisco IOS XE デバイスに証明書をインストールする例を示します。

```
# Send:
Device# configure terminal
Device(config)# crypto pki import trustpoint1 pem terminal password password1

# Receive:
% Enter PEM-formatted CA certificate.
% End with a blank line or "quit" on a line by itself.

# Send:
# Contents of rootCA.pem, followed by newline + 'quit' + newline:
-----BEGIN CERTIFICATE-----
<snip>
-----END CERTIFICATE-----
quit

# Receive:
% Enter PEM-formatted encrypted private General Purpose key.
% End with "quit" on a line by itself.
```

```
# Send:
# Contents of device.des3.key, followed by newline + 'quit' + newline:
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,D954FF9E43F1BA20
<snip>
-----END RSA PRIVATE KEY-----
quit

# Receive:
% Enter PEM-formatted General Purpose certificate.
% End with a blank line or "quit" on a line by itself.

# Send:
# Contents of device.crt, followed by newline + 'quit' + newline:
-----BEGIN CERTIFICATE-----
<snip>
-----END CERTIFICATE-----
quit

# Receive:
% PEM files import succeeded.
Device(config)#

# Send:
Device(config)# crypto pki trustpoint trustpoint1
Device(ca-trustpoint)# revocation-check none
Device(ca-trustpoint)# end
Device#
```


Cisco IOS XR デバイスへの証明書のインストール

Cisco IOS XR デバイスに証明書をインストールするには、次の手順を実行します。

1. rootCA.pem、device.key、および device.crt を /tmp フォルダの下のデバイスにコピーします。
2. IOS XR デバイスにログインします。
3. run コマンドを使用して VM シェルを開始します。

   ```
   RP/0/RP0/CPU0:xrvr-7.2.1#run
   ```
4. 次のディレクトリに移動します。

   ```
   cd /misc/config/grpc
   ```
5. 次のファイルの内容を作成または置換します。

（注） デバイスで TLS が以前に有効になっていた場合は、次のファイルがすでに存在します。その場合、以下で説明するようにこれらのファイルの内容を置き換えます。初めて行う場合は、デバイスで TLS を有効にし、/tmp フォルダからこのフォルダにファイルをコピーします。

- ems.pem with device.crt
- ems.key with device.key

- ca.cert with rootCA.pem

6. 変更を有効にするには、デバイスで TLS を再起動します。これを行うには、「no-tls」コマンドを使用して TLS を無効にし、デバイスで「no no-tls」設定コマンドを使用して再度有効にします。

Cisco IOS XE デバイスへの証明書のインストール

次に、Cisco IOS XE デバイスに証明書をインストールする例を示します。

```
# Send:
Device# configure terminal
Device(config)# crypto pki import trustpoint1 pem terminal password password1

# Receive:
% Enter PEM-formatted CA certificate.
% End with a blank line or "quit" on a line by itself.

# Send:
# Contents of rootCA.pem, followed by newline + 'quit' + newline:
-----BEGIN CERTIFICATE-----
<snip>
-----END CERTIFICATE-----
quit

# Receive:
% Enter PEM-formatted encrypted private General Purpose key.
% End with "quit" on a line by itself.

# Send:
# Contents of device.des3.key, followed by newline + 'quit' + newline:
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,D954FF9E43F1BA20
<snip>
-----END RSA PRIVATE KEY-----
quit

# Receive:
% Enter PEM-formatted General Purpose certificate.
% End with a blank line or "quit" on a line by itself.

# Send:
# Contents of device.crt, followed by newline + 'quit' + newline:
-----BEGIN CERTIFICATE-----
<snip>
-----END CERTIFICATE-----
quit

# Receive:
% PEM files import succeeded.
Device(config)#

# Send:
Device(config)# crypto pki trustpoint trustpoint1
Device(ca-trustpoint)# revocation-check none
Device(ca-trustpoint)# end
Device#
```

NETCONF 収集ジョブ

Crosswork Data Gateway は、ネットワークデバイスからのネットワーク設定プロトコル（NETCONF）ベースのデータ収集をサポートしています。

NETCONF 収集の場合、Crosswork Data Gateway は、CLI 収集ジョブ用にロードされる次のデバイスパッケージを利用します。

- システムデバイスパッケージ：Crosswork Data Gateway の起動後にダウンロードされるシステムデバイスパッケージ。
- カスタムデバイスパッケージ：UI または API からアップロードされたカスタムデバイスパッケージ。

NETCONF コレクタは、次の 2 つのタイプのデータ収集をサポートしています。

- プルベースの収集

  パターンベースの収集とオンデマンド収集をサポートします。

（注） NETCONF コマンドベースの収集はサポートされていません。

- イベントベースの収集

  https://tools.ietf.org/html/rfc5277 のドキュメントに記載されている NETCONF イベント通知をサポートしています。オンデマンド収集はこのタイプの収集ではサポートされておらず、これらの収集ジョブに指定されたパターンは無視されます。

NETCONF 収集ジョブのワークフロー

1. NETCONF 収集ジョブが収集サービス（Helios/Magellan）に送信され要求された収集のパターンまたは数、あるいはイベント通知 RPC を指定します。
2. 収集サービス（Helios / Magellan）は、収集ジョブを Crosswork Data Gateway の NETCONF コレクタに送信します。
3. 収集のタイプ（イベントベースの収集かプルベースの収集か）に応じて、NETCONF コレクタはデバイスから収集を開始します。
4. 収集されたデータは、指定されたデータ送信先（gRPC/Kafka）に転送されます。

サンプル ペイロード：

```
{
  "createUpdateJob": {
    "jobId": {
      "deviceId": "6fa90381-95f3-4a95-ac32-37754e002225",
      "sensorPath": {
        "netconfSensor": {
          "devicePackage": {
            "devicePackageName": "optical_inventory_svo_mne",
            "functionName": "getRawNodeInfo"
          }
```

```
        }
      },
      "collectionType": "PERSISTENT_COLLECTION_TYPE"
    },
    "collectionType": "PERSISTENT_COLLECTION_TYPE",
    "deviceId": "6fa90381-95f3-4a95-ac32-37754e002225",
    "sensorConfig": {
      "sensorPath": {
        "netconfSensor": {
          "devicePackage": {
            "devicePackageName": "optical_inventory_svo_mne",
            "functionName": "getRawNodeInfo"
          }
        }
      },
      "cadenceInMillisec": "60000"
    },
    "destinationSensorConfigs": [
      {
        "jobDestinationId": {
          "destinationId": "6dbc2a4c-e827-438f-9bab-bbeb508c06e2",
          "destinationContextId": "NativeNetconfTopic"
        },
        "destinationId": "6dbc2a4c-e827-438f-9bab-bbeb508c06e2",
        "destinationContextId": "NativeNetconfTopic",
        "sensorConfigHandler": {
          "action": "NORMAL"
        },
        "applicationContext": [
          {
            "applicationId": "EPNM-APP",
            "contextId": "Native-Netconf"
          }
        ]
      }
    ]
  }
}
```

NETCONF コレクタの問題のトラブルシューティング

NETCONF コレクタが継続的に再起動する

次のコマンドを実行して、NETCONF コレクタの docker ログを確認します。

```
docker logs netconf-collector
```

[jarが無効または破損している（invalid or corrupt jar）] というメッセージが表示された場合は、コンテナ用にダウンロードされた Docker イメージが破損していることを意味します。

問題を軽減するための回避策として、次の手順に従います。

1. Crosswork Data Gateway VM にログインします。
2. インタラクティブコンソールから **5 トラブルシューティング**を選択します。
3. **3 すべてのコレクタを削除し、VM を再起動します。**

   これにより、インストール後にダウンロードされたコンテナ（コレクタとオフロード）が削除され、Docker からイメージが削除され、コレクタデータと構成が削除され、VM が再起動され、VM は、インフラストラクチャコンテナのみが実行された初期構成が完了した

直後の状態に戻ります。Crosswork Data Gateway の再起動後、コンテナは Cisco Infrastructure から再度ダウンロードされます。

Cisco Crosswork の UI からの収集ジョブの作成

収集ジョブを作成するには、次の手順を実行します。

（注） Cisco Crosswork の UI ページを使用して作成した収集ジョブは、1 回のみパブリッシュできます。

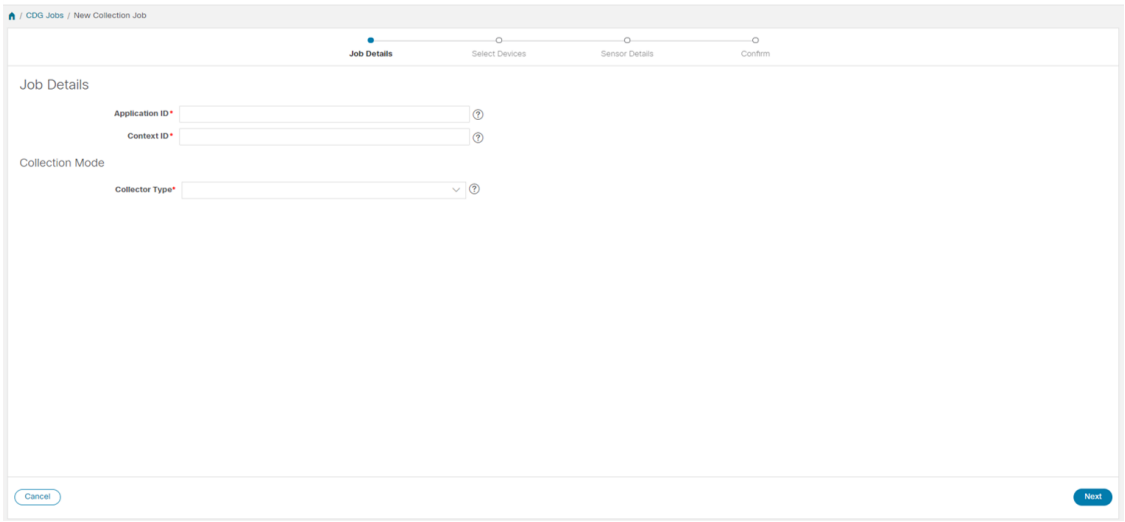
始める前に

収集したデータを保存するためのデータ送信先が作成されている（アクティブになっている）ことを確認します。また、データを収集する予定のセンサーパスと MIB の詳細を確認します。

ステップ 1 メインメニューから、[管理（Administration）] > [収集ジョブ（Collection Jobs）] > [一括ジョブ（Bulk Jobs）] に移動します。

ステップ 2 左側のペインで ⊞ ボタンをクリックします。

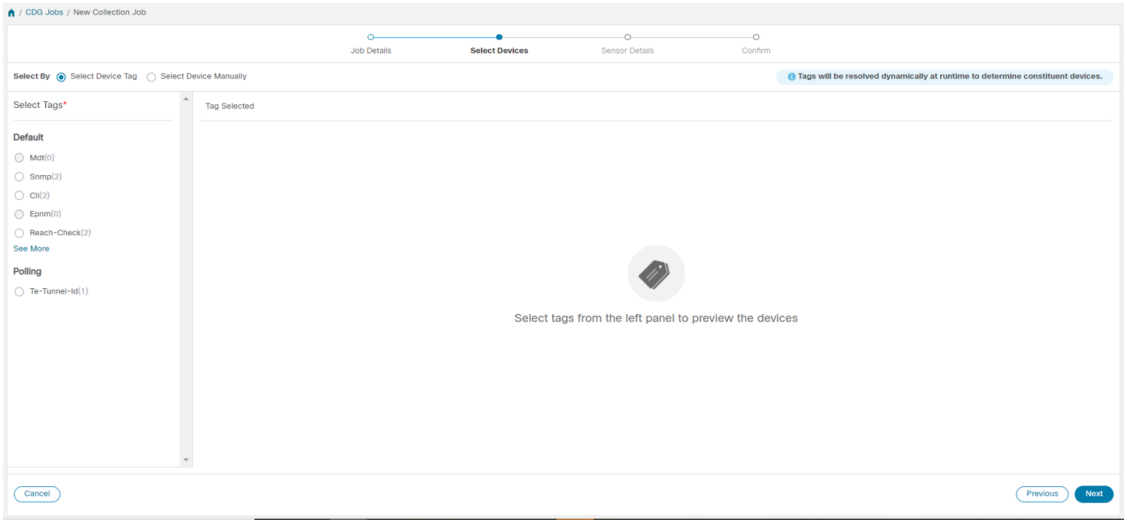
ステップ 3 [ジョブの詳細（Job details）] ページで、次のフィールドに値を入力します。



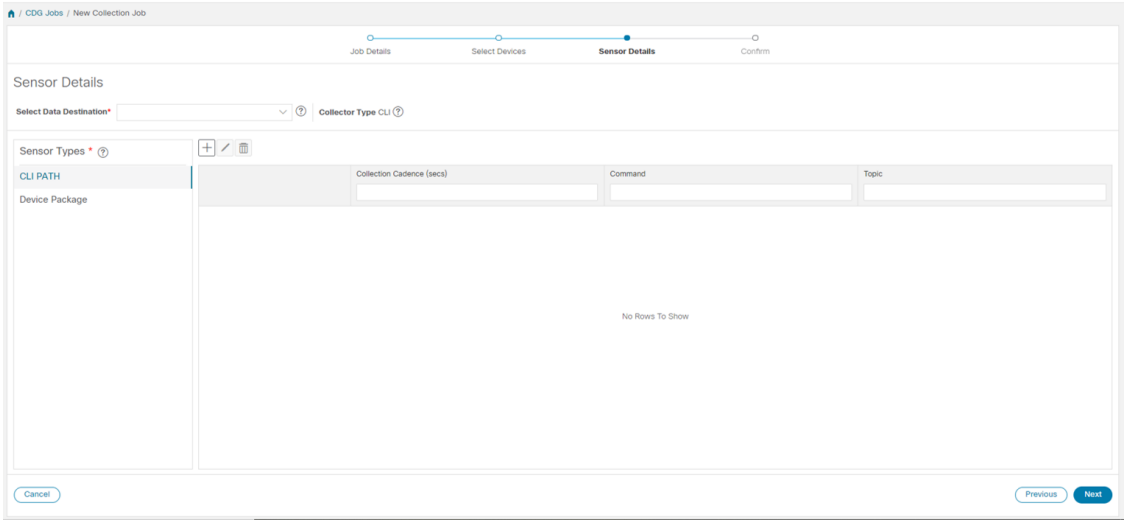
- [アプリケーション ID（Application ID）] : アプリケーションの一意の識別子。
- [コンテキスト（Context）] : すべての収集ジョブでアプリケーションのサブスクリプションを識別するための一意の識別子。
- [コレクタタイプ（Collector Type）] : 収集のタイプ（CLI または SNMP）を選択します。

[次へ（Next）] をクリックします。

ステップ 4 データを収集するデバイスを選択します。デバイスタグに基づいて選択することも、手動で選択することもできます。[次へ（Next）] をクリックします。

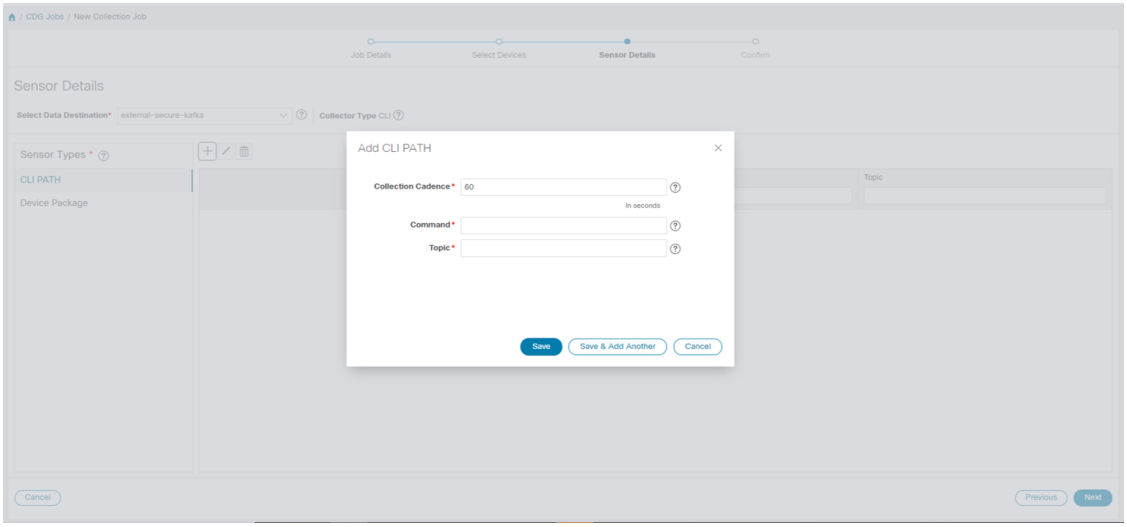


ステップ 5 （CLI での収集の場合にのみ適用）次のセンサーの詳細を入力します。



- [データ送信先の選択（Select Data Destination）] ドロップダウンからデータ送信先を選択します。
- 左側の [センサータイプ（Sensor Types）] ペインからセンサータイプを選択します。

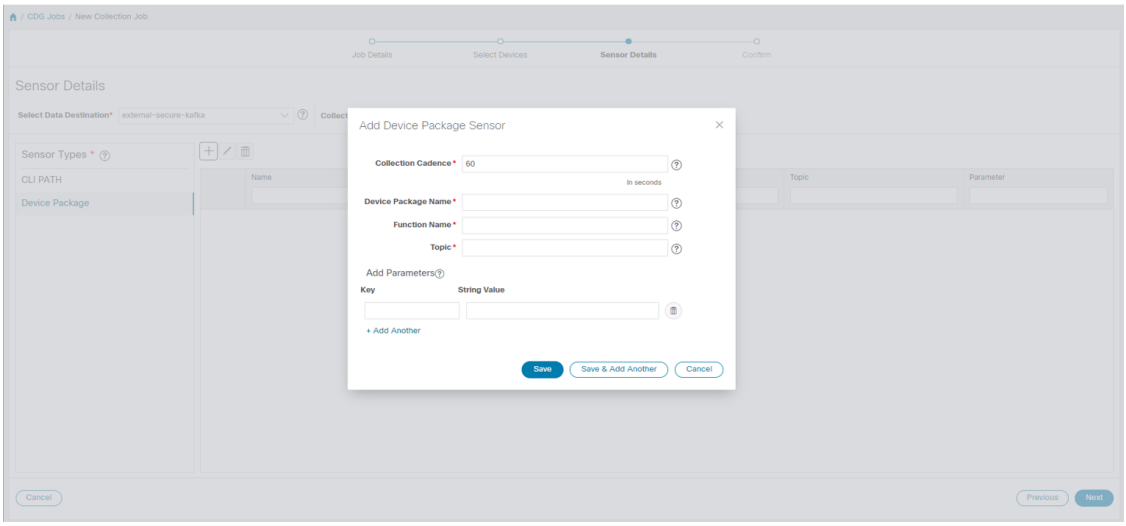
[CLI パス（CLI PATH）] を選択した場合は、＋ボタンをクリックして、[CLI パスの追加（Add CLI Path）] ダイアログボックスに次のパラメータを入力します。



- [収集パターン（Collection Cadence）]：プッシュまたはポーリングパターンを秒単位で指定します。
- [コマンド（Command）]：CLI コマンド
- [トピック（Topic）]：出力先に関連付けられているトピック。

（注）　外部 gRPC サーバーを使用する場合、トピックは任意の文字列にできます。

[デバイスパッケージ（Device Package）] を選択した場合は、[+] ボタンをクリックし、[デバイスパッケージセンサーの追加（Add Device Package Sensor）] ダイアログボックスに次のパラメータの値を入力します。



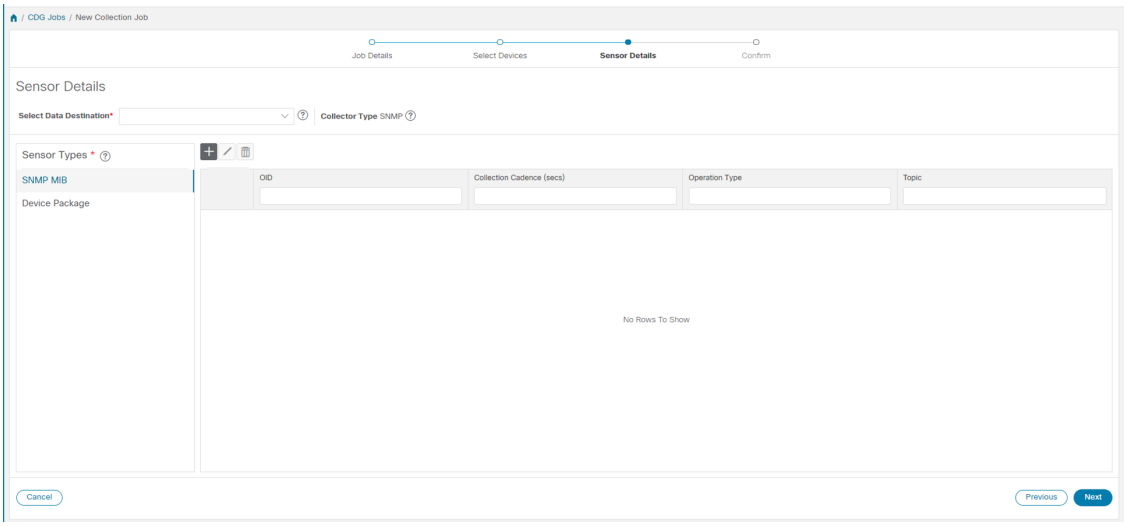
- [収集パターン（Collection Cadence）]：プッシュまたはポーリングパターンを秒単位で指定します。
- [デバイスパッケージ名（Device Package Name）]：デバイスパッケージの作成時に使用するカスタム XDE デバイスパッケージの ID。
- [関数名（Function Name）]：カスタム XDE デバイスパッケージ内の関数名。

- [トピック（Topic）]：出力先に関連付けられているトピック。

パラメータのキーと文字列の値を入力します。

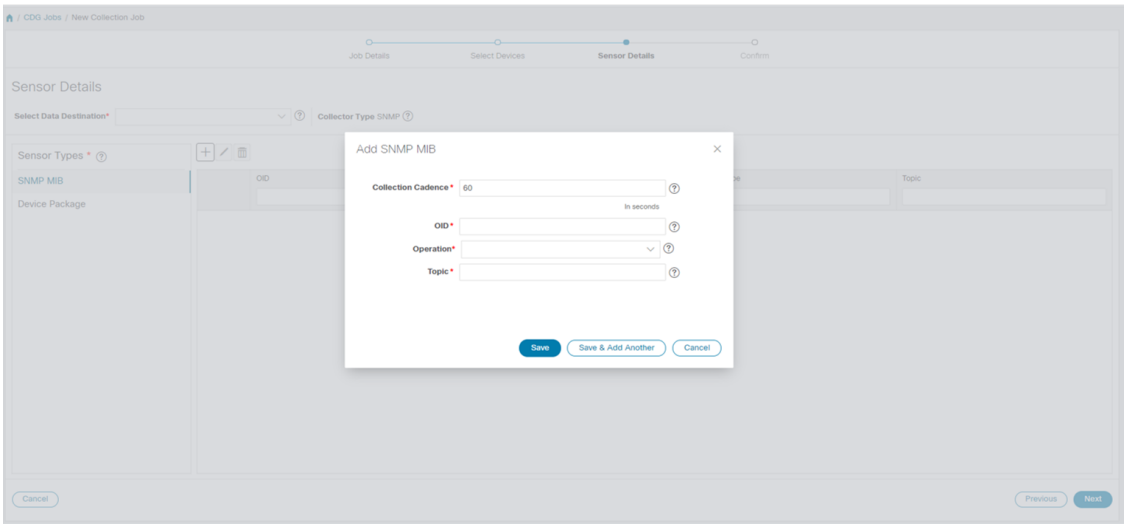
[保存（Save）] をクリックします。

ステップ 6 （SNMP での収集の場合にのみ適用）次のセンサーの詳細を入力します。



- [データ送信先の選択（Select Data Destination）] ドロップダウンからデータ送信先を選択します。
- 左側の [センサータイプ（Sensor Types）] ペインからセンサータイプを選択します。

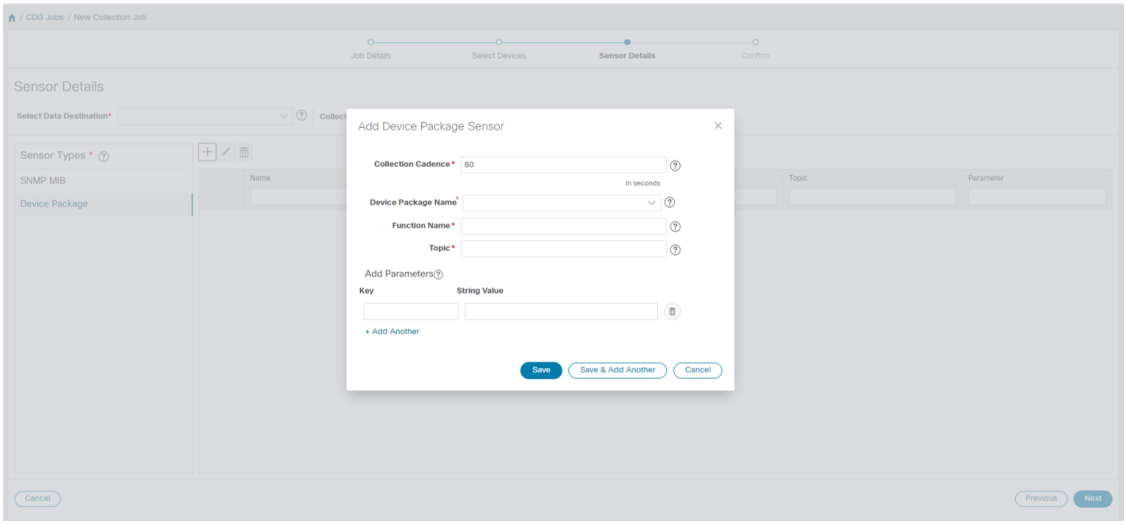
[SNMP MIB] を選択した場合は、⊞ ボタンをクリックして、[SNMP MIB の追加（Add SNMP MIB）] ダイアログボックスに次のパラメータを入力します。



- [収集パターン（Collection Cadence）]：プッシュまたはポーリングパターンを秒単位で指定します。
- OID

- [操作（Operation）]：リストから操作を選択します。
- [トピック（Topic）]：出力先に関連付けられているトピック。

[デバイスパッケージ（Device Package）] を選択した場合は、＋ボタンをクリックし、[デバイスパッケージセンサーの追加（Add Device Package Sensor）] ダイアログボックスに次のパラメータの値を入力します。



- [収集パターン（Collection Cadence）]：プッシュまたはポーリングパターンを秒単位で指定します。
- [デバイスパッケージ名（Device Package Name）]：デバイスパッケージの作成時に使用するカスタムデバイスパッケージの ID。
- [関数名（Function Name）]：カスタムデバイスパッケージ内の関数名。
- [トピック（Topic）]：出力先に関連付けられているトピック。

パラメータのキーと文字列の値を入力します。

[保存（Save）] をクリックします。

ステップ 7 [収集ジョブの作成（Create Collection Job）] をクリックします。

（注） 外部の Kafka 接続先（つまり安全でない Kafka）に対して収集ジョブが送信されると、Kafka へのディスパッチジョブは接続に失敗します。コレクタのログに「`org.apache.kafka.common.errors.TimeoutException: Topic cli-job-kafka-unsecure not present in metadata after 60000 ms`」というエラーが表示されます。Kafka のログには「`SSL authentication error "[2021-01-08 22:17:03,049] INFO [SocketServer brokerId=0] Failed authentication with /80.80.80.108 (SSL handshake failed) (org.apache.kafka.common.network.Selector)`」というエラーが表示されます。

これは、外部の Kafka VM でポートがブロックされているために発生します。次のコマンドを使用して、ポートが Kafka Docker/サーバーポートでリッスンしているかどうかを確認できます。

```
netstat -tulpn
```

Kafka サーバーの問題を修正し、Kafka サーバープロセスを再起動します。

収集ジョブのモニター

[収集ジョブ（Collection Jobs）] ページから、Cisco Crosswork に登録されているすべての Crosswork Data Gateway インスタンスで現在アクティブな収集ジョブのステータスをモニターできます。

Cisco Crosswork の UI の左側のナビゲーションバーで、[管理（Administration）] > [収集ジョブ（Collection Jobs）] を選択します。

この左側のペインには、すべてのアクティブな収集ジョブが、ステータス、アプリ ID、およびコンテキスト ID とともに一覧表示されます。[ジョブの詳細（Job Details）] ペインには、左側ペインの特定のジョブに関連付けられているすべての収集タスクの詳細が表示されます。[収集ジョブ（Collection Jobs）] ペインの収集ジョブの全体的なステータスは、[ジョブの詳細（Jobs Details）] ペインのすべての収集タスクの集約ステータスです。

[収集ジョブ（Collection Jobs）] ペインでジョブを選択すると、[ジョブの詳細（Job Details）] ペインに次の詳細が表示されます。

- 収集ジョブに関連付けられたアプリケーション名とコンテキスト。
- 収集ジョブのステータス。

（注）

- デバイスが Crosswork Data Gateway に接続された後にそのデバイスに関連付けられている収集タスクのステータスは、[不明（Unknown）] になります。
- 次のいずれかの理由で、ジョブのステータスが [不明（Unknown）] になる可能性があります。
  - Crosswork Data Gateway がまだステータスを報告していない。
  - Crosswork Data Gateway と Cisco Crosswork 間の接続が失われた。
  - Crosswork Data Gateway は収集ジョブを受信したが、実際の収集はまだ保留中になっている。たとえば、トラップが Crosswork Data Gateway のサウスバウンド インターフェイスに送信されていない場合やデバイスがテレメトリ更新を送信していない場合などです。
  - 監視している SNMP トラップ収集ジョブのトラップ状態が発生していません。たとえば、リンクアップまたはリンクダウンの遷移を探していて、コレクタが確立されてからリンク状態が変更されていない場合、状態は [不明（Unknown）] として報告されます。したがって、トラップベースのコレクションが機能していることを検証するには、実際にトラップをトリガーする必要があります。
- 収集ジョブが処理された後、処理が成功した場合はステータスが [成功（Successful）] に変わり、それ以外の場合は [失敗（Failed）] に変わります。
- 収集ジョブが低下状態の場合、その原因の 1 つとして、デバイスへの静的ルートが Crosswork Data Gateway から消去されていることが考えられます。
- エラー状態にある宛先へのコレクションは停止しません。宛先状態はバックグラウンドで識別されます。宛先がエラー状態の場合、エラーカウントがインクリメントされます。[ディストリビューション（Distribution）] ステータスに表示されるエラーメッセージをドリルダウンし、それぞれのコレクタログを調べて問題を特定して解決します。
- Cisco Crosswork Health Insights：KPI ジョブは、拡張 Crosswork Data Gateway VM にマッピングされたデバイスでのみ有効にする必要があります。標準の Crosswork Data Gateway VM にマッピングされているデバイスで KPI ジョブを有効にすると、[ジョブの詳細（Jobs Details）] ペインで収集ジョブのステータスが [低下（Degraded）]、収集タスクのステータスが

[失敗（Failed）] として報告されます。

- REST API 要求で渡す収集ジョブのジョブ設定。ジョブの設定を表示するには、[設定の詳細（Config Details）] の横にある アイコンをクリックします。この場合、Cisco Crosswork では、次の 2 つのモードで設定を表示できます。
  - ビュー モード
  - テキストモード
- 収集タイプ
- 収集ジョブの最終変更日時。
- [収集（x）（Collections (x)）] : x は、センサーパスによってデバイスにまたがる要求された収集の入力を指します。対応する [（y）問題（(y) Issues）] は [不明（UNKNOWN）] 状態または [失敗（FAILED）] 状態の入力収集の数です。
- [配布（x）（Distributions (x)）] : x は、センサーパスによってデバイスにまたがる要求された出力収集を指します。対応する [（y）問題（(y) Issues）] は [不明（UNKNOWN）] 状態または [失敗（FAILED）] 状態の出力収集の数です。

Cisco Crosswork は、収集と配布に関する次の詳細も表示します。

フィールド	説明
収集/配布ステータス（Collection/Distribution Status）	収集/配布のステータス。変更ベースで Crosswork Data Gateway 報告されます。詳細については、[収集/配信ステータス（Collection/Distribution Status）] の横にある をクリックします。
ホスト名（Hostname）	収集ジョブが関連付けられているデバイスのホスト名。
デバイス ID（Device Id）	データの収集元のデバイスの一意の識別子。

フィールド	説明
センサーデータ（Sensor Data）	センサーパス 収集/配布の概要を表示するには、 をクリックします。センサーデータの概要ポップアップから [クリップボードにコピー（Copy to Clipboard）] をクリックしてセンサーデータをコピーできます。 収集/配布メトリックの概要を表示するには、 をクリックします。メトリックはパターンベース、つまりデフォルトでは10分 ごとに1回報告されます。収集に関する次のメトリックが表示されます。 • last_collection_time_msec • total_collection_message_count • last_device_latency_msec • last_collection_cadence_msec 収集に関する次のメトリックが表示されます。 • total_output_message_count • last_destination_latency_msec • last_output_cadence_msec • last_output_time_msec • total_output_bytes_count
接続先（Destination）	ジョブのデータ接続先。
最後のステータス変更の報告時刻（Last Status Change Reported Time）	デバイスセンサーペアの最後のステータス変更が Crosswork Data Gateway から報告された日時。

（注）
- `Create Failed` エラーは、N 台のデバイスのうちの一部のデバイスの設定に失敗したことを示します。ただし、収集は正常に設定されたデバイスで行われます。`Control Status` API を使用して、このエラーの原因となっているデバイスを特定できます。
- NSO エラーが原因で特定のデバイスでジョブの作成が失敗した場合は、NSO エラーを修正した後、デバイスの管理状態を手動で最初に [ダウン（Down）] にしてから [アップ（Up）] に変更する必要があります。ただし、これを行うと、デバイス上の収集がリセットされます。

（注）
[作成/削除失敗（Create/Delete failed）] エラーが別の画面ポップアップに表示されます。エラーの詳細を表示するには、ジョブステータスの横にある をクリックします。
- 同じペイロードで PUT 収集ジョブ API を使用してジョブを再作成することもできます。

イベントベースの収集ジョブの収集ステータス

1. データの収集が成功すると、[収集ジョブ（Collection Jobs）] ペインで収集ジョブのステータスが [不明（Unknown）] から [成功（Success）] に変わります。
2. デバイスが Crosswork Data Gateway から切断されると、対応するすべての収集ジョブが削除され、収集ジョブのステータスが [収集ジョブ（Collection Jobs）] ペインに [成功（Success）] と表示されます。[ジョブの詳細（Job Details）] ペインに表示されるデバイスまたは収集タスクはありません。
3. デバイスが Crosswork Data Gateway に接続されると、Crosswork Data Gateway は、ステータスが [不明（Unknown）] に設定されている新しい収集ジョブを受信します。このステータスは、デバイスからイベントを受信した後に [成功（Success）] に変わります。
4. すでに Crosswork Data Gateway に接続されているデバイスでデバイス設定が誤って更新された場合、Crosswork Data Gateway がジョブとイベントを受信しても、[ジョブの詳細（Jobs Details）] ペインの収集タスクのステータスは変わりません。
5. デバイスインベントリが誤ったデバイス IP で更新された場合、[ジョブの詳細（Jobs Details）] ペインの収集タスクのステータスは、予想どおり、[不明（Unknown）] になります。

収集ジョブの削除

システムジョブ（さまざまな Crosswork アプリケーションによって作成されたデフォルトのジョブ）は、問題が発生する可能性があるため削除しないでください。Health Insights によって作成されたジョブは、展開された収集ジョブを削除する KPI プロファイルを無効にすることによってのみ削除する必要があります。[収集ジョブ（Collection Jobs）] ページからは、外部収集ジョブを削除するには、次の手順を使用します。

収集ジョブを削除するには、次の手順を実行します。

ステップ 1 [管理（Administration）] > [収集ジョブ（Collection Jobs）] に移動します。

ステップ 2 [一括ジョブ（Bulk Jobs）] タブまたは [パラメータ化されたジョブ（Parmaterized Jobs）] タブのいずれかを選択します。

ステップ 3 左側の [収集ジョブ（Collection Jobs）] ペインで、削除する収集ジョブを選択します。

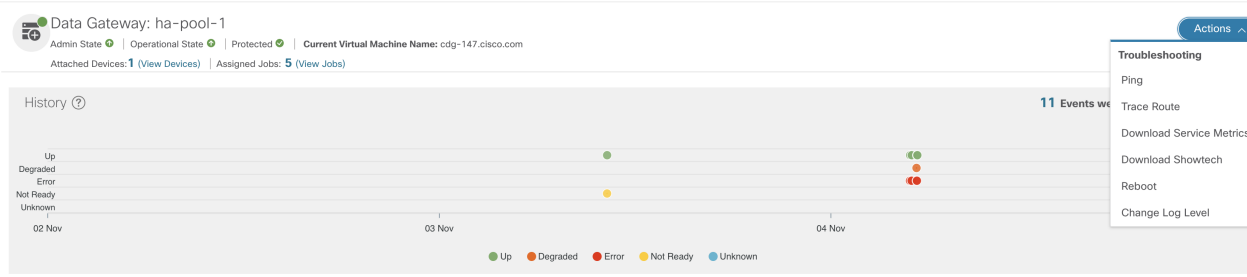
ステップ 4 をクリックします。

ステップ 5 確認を求められたら、[削除（Delete）] をクリックします。

Crosswork Data Gateway のトラブルシューティング

Crosswork Data Gateway は、UI または Crosswork Data Gateway VM のインタラクティブコンソールからトラブルシューティングできます。

この項では、Cisco Crosswork UI から使用できるさまざまなトラブルシューティングのオプションについて説明します。



Crosswork Data Gateway VM のインタラクティブコンソールから使用できるトラブルシューティングオプションの詳細については、「Crosswork Data Gateway VM のトラブルシューティング（410 ページ）」を参照してください。

接続先への接続の確認

Cisco Data Gateway から接続先への接続を確認するには、[トラブルシューティング（Troubleshooting）] メニューの [Ping] オプションと [トレースルート（Traceroute）] オプションを使用します。

（注） 接続先を正常に ping するには、ネットワークで ping トラフィックを有効にする必要があります。

1. [管理（Administration）] > [Data Gateway の管理（Data Gateway Management）] > [データゲートウェイ（Data Gateways）] に移動します。

2. 接続を確認する Cisco Crosswork Data Gateway の名前をクリックします。
3. [Crosswork Data Gateway の詳細（Crosswork Data Gateway details）] ページの右上隅で、[アクション（Actions）] をクリックし、[Ping] または [トレースルート（Traceroute）] を選択します。
   - [Ping] : [パケット数（Number of Packets）] フィールドと [接続先アドレス（Destination Address）] フィールドに詳細を入力し、[Ping] をクリックします。
   - [トレースルート（Traceroute）] : [接続先アドレス（Destination Address）] に入力し、[トレースルート（Traceroute）] をクリックします。
4. 接続先が到達可能な場合、Cisco Crosswork は同じウィンドウに [Ping] または [トレースルート（Traceroute）] のテストの詳細を表示します。

サービスメトリックのダウンロード

Cisco Crosswork の UI から Crosswork Data Gateway のすべての収集ジョブのメトリックをダウンロードするには、次の手順を実行します。

ステップ 1 [管理（Administration）] > [Data Gateway の管理（Data Gateway Management）] > [データゲートウェイ（Data Gateways）] に移動します。

ステップ 2 サービスメトリックをダウンロードする Crosswork Data Gateway の名前をクリックします。

ステップ 3 [Crosswork Data Gateway の詳細（Crosswork Data Gateway details）] ページの右上隅で、[アクション（Actions）] > [サービスメトリックのダウンロード（Download Service Metrics）] をクリックします。

ステップ 4 パスフレーズを入力します。

（注） このパスフレーズを必ずメモしておいてください。このパスフレーズは、後でファイルを復号するために使用します。

ステップ 5 [サービスメトリックのダウンロード（Download Service Metrics）] をクリックします。ファイルは、システムのデフォルトのダウンロードフォルダに暗号化された形式でダウンロードされます。

ステップ 6 ダウンロードが完了したら、次のコマンドを実行して復号します。

（注） ファイルを復号するには、openssl バージョン 1.1.1i を使用する必要があります。`openssl version` コマンドを使用して、システムの openssl バージョンを確認します。

```
openssl enc -d -aes-256-ctr -pbkdf2 -md sha3-512 -iter 100000 -in <service metrics file> -out
<decrypted filename> -pass pass:<encrypt string>
```

showtech ログのダウンロード

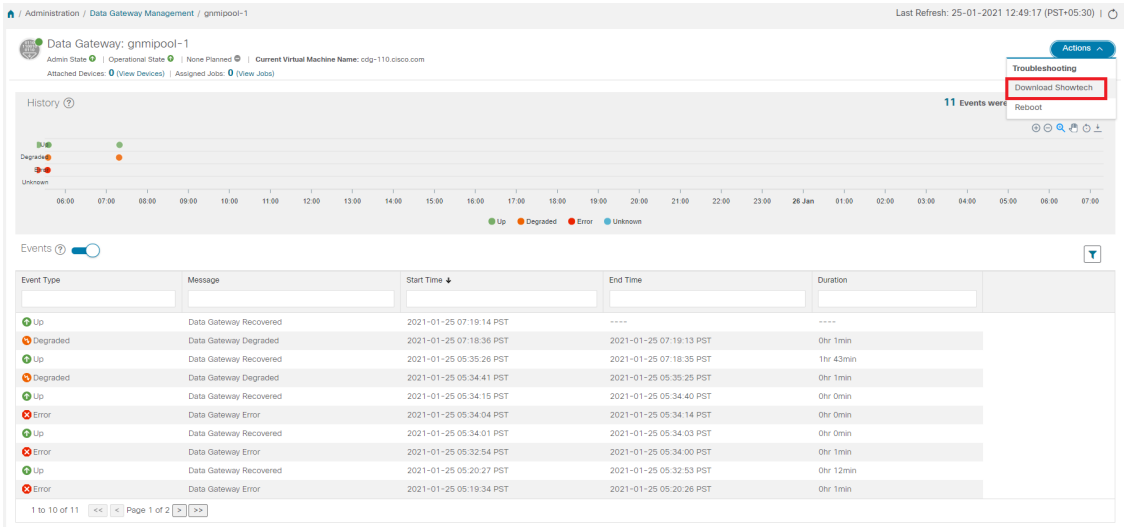
Cisco Crosswork の UI から showtech ログをダウンロードする手順を実行します。

（注） Crosstech Data Gateway が [エラー（ERROR）] 状態の場合、Showtech ログは UI から収集できません。Cisco Crosswork Data Gateway が [低下（DEGRADED）] 状態の場合、OAM-Manager サービスが実行されており、低下していなければ、ログを収集できます。

ステップ 1 [管理（Administration）] > [Data Gateway の管理（Data Gateway Management）] > [データゲートウェイ（Data Gateways）] に移動します。

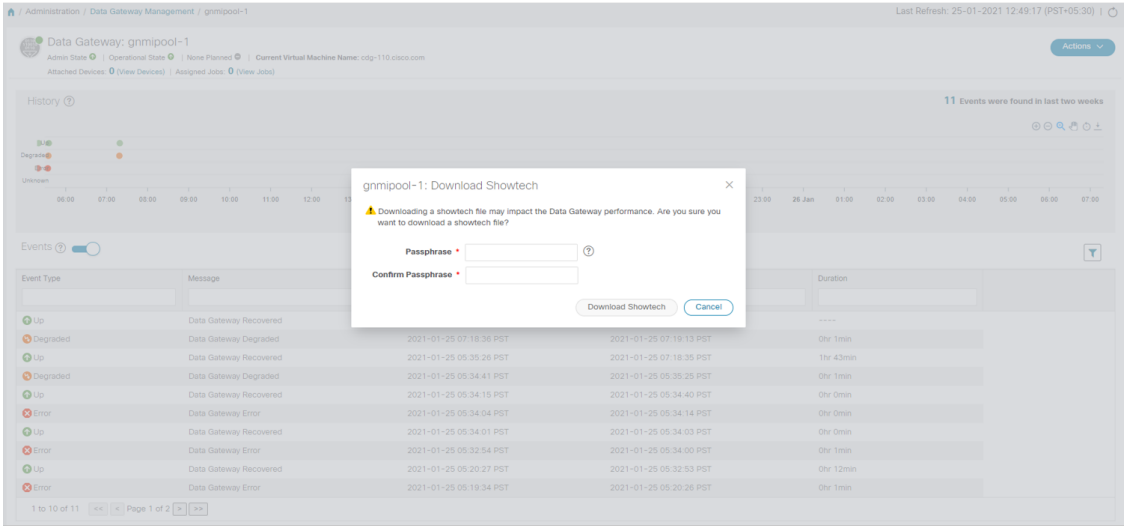
ステップ 2 showtech をダウンロードする Crosswork Data Gateway の名前をクリックします。

ステップ 3 Crosswork Data Gateway の詳細ページの右上隅にある [アクション（Actions）] をクリックし、[Showtech のダウンロード（Download Showtech）] をクリックします。



ステップ 4 パスフレーズを入力します。

（注） このパスフレーズを必ずメモしておいてください。showtech ファイルを復号するには、このパスフレーズを後で入力する必要があります。



ステップ 5 [Showtech のダウンロード（Download Showtech）] をクリックします。showtech ファイルは暗号化された形式でダウンロードされます。

（注） システムの使用時間によっては、showtech ファイルのダウンロードに数分かかる場合があります。

ステップ 6 ダウンロードが完了したら、次のコマンドを実行して復号します。

（注） ファイルを復号するには、OpenSSL バージョン 1.1.1i を使用する必要があります。`openssl version` コマンドを使用して、システムの openssl バージョンを確認します。

MAC でファイルを復号するには、OpenSSL 1.1.1+ をインストールする必要があります。これは、LibreSSL の `openssl` コマンドが OpenSSL の `openssl` コマンドでサポートされているすべてのスイッチはサポートしていないためです。

```
openssl enc -d -aes-256-ctr -pbkdf2 -md sha3-512 -iter 100000 -in <showtech file> -out <decrypted filename> -pass pass:<encrypt string>
```

Cisco Crosswork Data Gateway VM の再起動

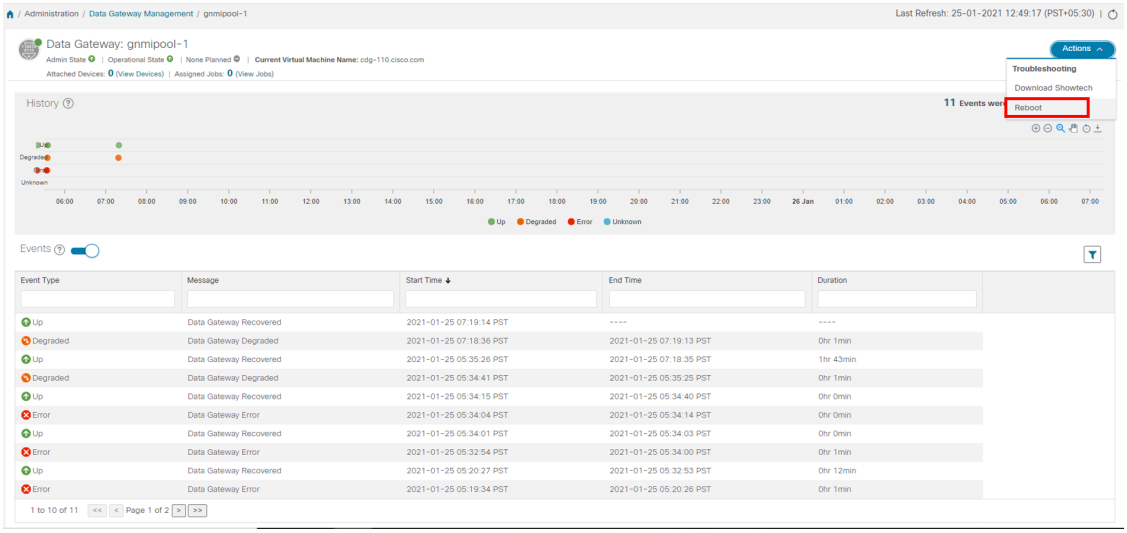
次の手順を実行して、Cisco Crosswork UI から Crosswork Data Gateway を再起動します。

（注） Crosswork Data Gateway を再起動すると、機能が再びアップするまで一時停止します。

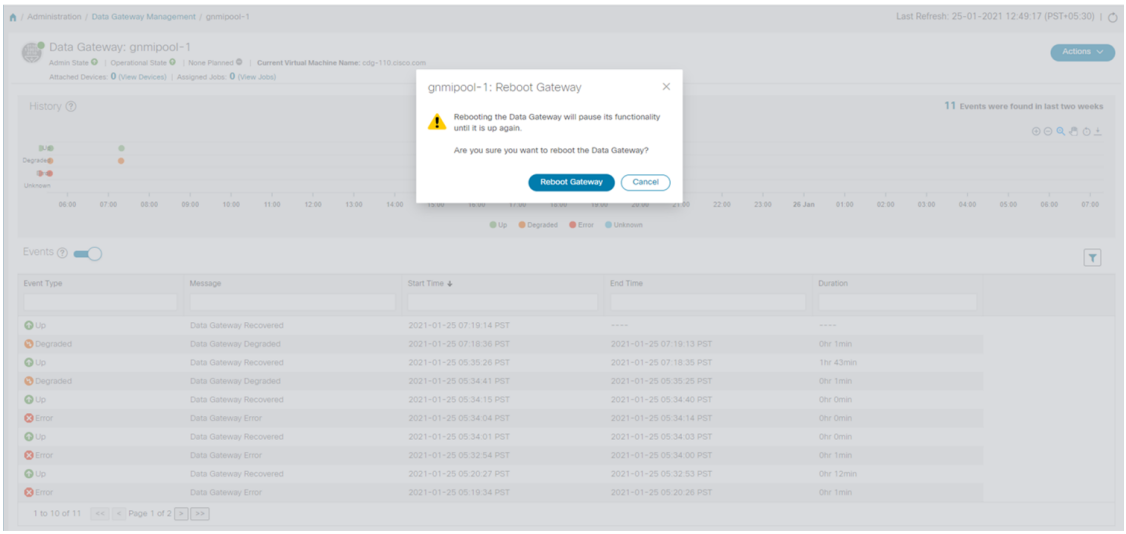
ステップ 1 [管理（Administration）] > [Data Gateway の管理（Data Gateway Management）] > [データゲートウェイ（Data Gateways）] に移動します。

ステップ 2 再起動する Cisco Crosswork Data Gateway の名前をクリックします。

ステップ 3 Crosswork Data Gateway の詳細ページの右上隅にある [アクション（Actions）] をクリックし、[再起動（Reboot）] をクリックします。



ステップ 4 [ゲートウェイの再起動（Reboot Gateway）] をクリックします。



再起動が完了したら、**[管理（Administration）] > [Data Gateway の管理（Data Gateway Management）] > [仮想マシン（Virtual Machines）]** ウィンドウで Cisco Crosswork の動作ステータスを確認します。

Crosswork Data Gateway コンポーネントのログレベルの変更

Cisco Crosswork の UI には、Crosswork Data Gateway のコンポーネント（コレクタ（cli-collector）やインフラサービス（oam-manager）など）のログレベルを変更するオプションがあります。ログレベルの変更は、変更を加える Crosswork Data Gateway にのみ適用されます。

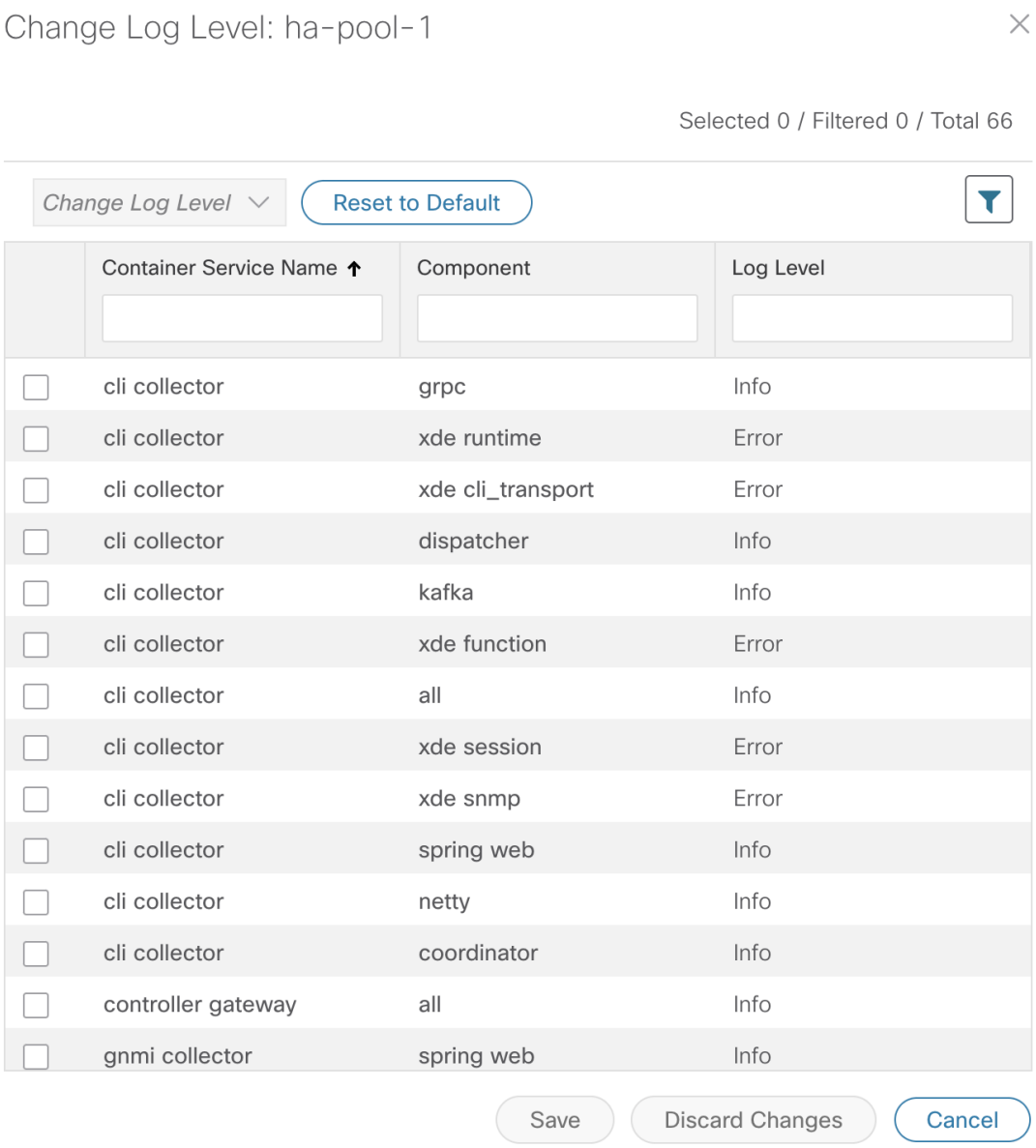
（注） オフロードサービスのログレベルの変更はサポートされていません。

ステップ 1 [管理（Administration）] > [Data Gateway の管理（Data Gateway Management）] > [データゲートウェイ（Data Gateways）] に移動します。

ステップ 2 Crosswork インフラストラクチャ サービスのコレクタのログレベルを変更する Crosswork Data Gateway 名をクリックします。

ステップ 3 [Crosswork Data Gateway の詳細（Crosswork Data Gateway details）] ページの右上隅で、[アクション（Actions）] > [ログレベルの変更（Change Log Level）] をクリックします。

[ログレベルの変更（Change Log Level）] ウィンドウが表示され、各コンテナサービスの現在のログレベルが示されます。



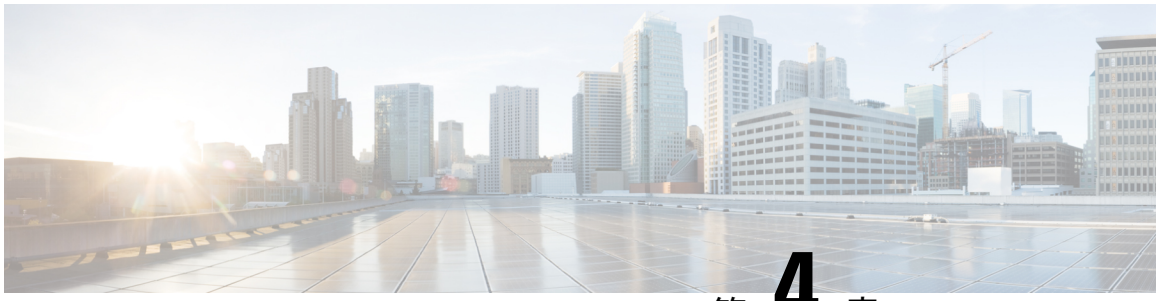
ステップ 4 ログレベルを変更するコンテナサービスのチェックボックスをオンにします。

ステップ 5 テーブルの上部にある [ログレベルの変更（Change Log Level）] ドロップダウンリストから、[デバッグ（Debug）]、[トレース（Trace）]、[警告（Warning）]、[情報（Info）]、および [エラー（Error）] からログレベルを選択します。

（注） すべてのログのログレベルをデフォルトのログレベル（[情報（Info）]）にリセットするには、[デフォルトにリセット（Reset to Default）] をクリックします。

ステップ 6 [保存（Save）] をクリックして変更したログレベルを保存します。

[保存（Save）] をクリックして、コンポーネントのログレベルが正常に変更されたことを示す UI メッセージを表示します。



第 4 章

バックアップの管理

ここでは、次の内容について説明します。

Backup and Restore の概要

Cisco Crosswork のバックアップ機能と復元機能は、データ損失を防ぎ、インストールされているアプリケーションと設定を保持します。

Cisco Crosswork には、データをバックアップおよび復元するための複数のメニューオプションが用意されています。

メインメニューから、**[管理（Administration）]**>**[バックアップと復元（Backup and Restore）]** をクリックして、[バックアップと復元（Backup and Restore）] ウィンドウにアクセスします。

表 *7: Backup and Restore* オプション

メニュー オプション	説明
[アクション（Actions）]>[バックアップ（Actions）] （詳細については、Cisco Crosswork のバックアップと復元の管理（123 ページ）を参照）	Crosswork 構成データベースとアプリケーションファイルを保持します。バックアップファイルは、災害復旧（災害後に Cisco Crosswork を復元する（126 ページ））で使用して、重大な障害から回復することができます。 バックアップオプションの中で、[NSOでバックアップ（Backup with NSO）] することも選択できます。このオプションは、Crosswork 設定とともに Cisco NSO データを保持します。詳細については、「Cisco NSO を使用した Cisco Crosswork のバックアップ（133 ページ）」を参照してください。
[アクション（Actions）]>[データのバックアップ（Data Backup）] （詳細については、Cisco Crosswork のバックアップと復元の管理（123 ページ）を参照）	Crosswork 構成データのみを保持します。 データバックアップオプションは、通常のバックアップよりも高速で、主に、以前の時点にデータを復元するために他の動作しているシステムで使用されます。
[アクション（Actions）]>[災害後の復元（Disaster Restore）] （詳細については、災害後に Cisco Crosswork を復元する（126 ページ） を参照）	自然災害または人為的災害により Cisco Crosswork クラスタが破壊された後、Crosswork 構成データベースとアプリケーションファイルを復元します。 『*Cisco Crosswork Infrastructure 4.4 and Applications Installation Guide*』の手順に従って、最初に新しいクラスタを展開する必要があります。
[アクション（Actions）]>[災害後のデータ復元（Data Disaster Restore）] （詳細については、災害後に Cisco Crosswork を復元する（126 ページ） を参照）	災害復旧操作に似ていますが、Crosswork 構成データのみを復元します。 この操作を実行するには、データバックアップファイル（**[アクション（Actions）]>[データバックアップ（Data Back）]**）が必要です。 新しいクラスタとともに、古い Crosswork クラスタに存在していたアプリケーションの正確なバージョン（データのバックアップを作成したとき）を新しい Crosswork クラスタにインストールする必要があります。アプリケーションのビルドバージョンに不一致があると、データが失われ、復元ジョブが失敗する可能性があります。

メニュー オプション	説明
[アクション（Actions）]>[データ移行（Data Migration）] （詳細については、バックアップと復元を使用してデータを移行する （137 ページ） を参照）	Cisco Crosswork の古いバージョンから新しいバージョンにデータを移行します。

Cisco Crosswork のバックアップと復元の管理

このセクションでは、Cisco Crosswork UI からバックアップおよび復元操作を実行する方法について説明します。

注目

- バックアップ用のターゲットマシンの構築は、このドキュメントの範囲外です。オペレータは、サーバーを配置し、サーバーのログイン情報を把握し、バックアップ用の十分なスペースを備えたターゲットディレクトリを用意する必要があります。
- Crosswork はバックアップを管理しません。オペレータは、ターゲットサーバーから古いバックアップを定期的に削除して、将来のバックアップ用のスペースを確保する必要があります。
- [データバックアップ（Data Backup）] を作成する場合は、クラスタにインストールされているアプリケーションのビルドバージョンを書き留めます。[データの復元（Data Restore）] を実行する前に、それらのアプリケーションの正確なバージョンをインストールして、クラスタで使用できるようにする必要があります。アプリケーションのビルドバージョンに不一致があると、データが失われ、データの復元ジョブが失敗する可能性があります。
- Crosswork バックアッププロセスは、十分な量のストレージスペースを備えたサーバーへの SCP アクセスが必要です。各バックアップに必要なストレージは、クラスタサイズ、クラスタ内のアプリケーション、およびスケール要件によって異なります。
- バックアップまたは復元プロセスにかかる時間は、バックアップのタイプ、クラスタサイズ、クラスタ内のアプリケーションによって異なります。

Cisco Crosswork クラスタのバックアップを作成する場合、またはバックアップからクラスタを復元する場合は、次のガイドラインに従います。

- 最初のログイン時に、バックアップファイルを保存する接続先 SCP サーバーを設定します。この設定は 1 回限りのアクティビティです。このタスクを完了するまで、バックアップを実行したり、復元操作を開始したりできません。

- バックアップ操作または復元操作は、スケジュールされているメンテナンス期間にのみ実行することをお勧めします。これらの操作の実行中、ユーザーは Cisco Crosswork にアクセスしようとしないでください。バックアップではシステムが約 10 分間オフラインになりますが、復元操作に時間がかかることがあります。両方とも、完了するまで他のアプリケーションを一時停止します。これらの一時停止は、データ収集ジョブに影響を与える可能性があります。
- 通常の復元を実行すると、Cisco Crosswork アプリケーションとデータは、バックアップを作成したときと同じバージョンに復元されます。災害後の復元を実行する場合は、バックアップの作成時に使用したものと同じ Cisco Crosswork ソフトウェアイメージを使用する必要があります。異なるバージョンのソフトウェアを使用して作成したバックアップを使用して災害後の復元を実行することはできません。
- ダッシュボードを使用して、プロセスが完了するまで、バックアップまたは復元プロセスの進行状況をモニタします。プロセス中に Cisco Crosswork システムを使用しようとすると、さまざまなサービスが一時停止して頻繁に再起動するため、誤ったコンテンツやエラーが表示されることがあります。
- 一度に実行できるバックアップまたは復元操作は 1 つだけです。
- Cisco Crosswork クラスタと SCP サーバーの両方が同じ IP 環境内に存在する必要があります。たとえば、Cisco Crosswork が IPv6 で通信している場合は、バックアップサーバーも IPv6 で通信している必要があります。
- バックアップサーバーの領域を節約するために、古いバックアップを削除することもできますが、このバージョンのジョブリストには引き続き表示されます。
- より多くの変更を行うオペレータは、より頻繁に（おそらく毎日）バックアップする必要がありますが、他のオペレータは、週に 1 回または主要なシステムのアップグレードの前にバックアップを行うことに慣れているかもしれません。
- デフォルトでは、Crosswork は、正常と見なされないシステムのバックアップを作成することを許可しません。ただし、追加の分析やその他のトラブルシューティング作業のために、シスコとのイメージの共有を容易にするために、この保護をオーバーライドする規定があります。
- 定期的なバックアップまたはデータバックアップを実行するときは、クラスタインベントリ ファイルをエクスポートすることをお勧めします。

始める前に

作業を開始する前に、次を確認してください。

- セキュアな SCP サーバーのホスト名または IP アドレスおよびポート番号。サーバーに十分なストレージがあることを確認してください。
- バックアップファイルの接続先として使用する SCP サーバー上のファイルパス。
- 接続先 SCP サーバーのリモートパスに対するファイルの読み取り/書き込み権限を持つアカウントのユーザークレデンシャル。

- データのバックアップを作成する場合は、インストールされているアプリケーションのビルドバージョンを書き留めます。データの復元を実行する前に、それらのアプリケーションの正確なバージョンをインストールする必要があります。アプリケーションのビルドバージョンに不一致があると、データが失われ、データの復元ジョブが失敗する可能性があります。

ステップ 1　SCP バックアップサーバーを設定します。

a) メインメニューから、**[管理（Administration）]** > **[バックアップと復元（Backup and Restore）]** を選択します。

b) [接続先（Destination）] をクリックして、[接続先の編集（Edit Destination）] ダイアログボックスを表示します。表示されたフィールドに関連するエントリを入力します。

c) [保存（Save）] をクリックして、バックアップサーバーの詳細を確認します。

ステップ 2　バックアップを作成します。

a) メインメニューから、**[管理（Administration）]** > **[バックアップと復元（Backup and Restore）]** を選択します。

b) **[Actions]** > **[Backup]** をクリックして、宛先サーバーの詳細が事前に入力された [Backup] ダイアログボックスを表示します。

（注）　データバックアップを作成するには、**[アクション（Actions）]** > > **[データバックアップ（Data Backup）]** の順にクリックします。ステップ 2 の残りの手順は同じです。

c) [ジョブ名（Job Name）] フィールドに、バックアップに該当する名前を入力します。

d) Cisco Crosswork アプリケーションまたはマイクロサービスの問題があるにもかかわらず、[強制（Force）] チェックボックスをオンにします。

e) バックアップに Cisco NSO のデータを含めない場合は、[Backup NSO] チェックボックスをオフにします。

Cisco Crosswork バックアッププロセスに Cisco NSO データを含める場合は、ここで説明する手順の代わりに、Cisco NSO を使用した Cisco Crosswork のバックアップ （133 ページ） の手順を実行します。

f) 必要に応じて残りのフィールドにも入力します。

別のリモート サーバー アップロード先を指定する場合：事前に入力された [Host Name]、[Port]、[Username]、[Password]、および [Remote Path] フィールドを編集して、別の接続先を指定します。

g) （オプション）[バックアップ準備の確認（Verify Backup Readiness）] をクリックして、Cisco Crosswork にバックアップを完了するのに十分な空きリソースがあることを確認します。確認が成功すると、時間がかかる動作の特性に関する警告が Cisco Crosswork に表示されます。[OK] をクリックして、先へ進みます。

h) [Start Backup] をクリックして、バックアップ操作を開始します。Cisco Crosswork は、対応するバックアップジョブセットを作成し、それをジョブリストに追加します。[Job Details] パネルには、完了した各バックアップステップのステータスが表示されます。

i) バックアップジョブの進行状況を表示するには、[ジョブセットのバックアップ/復元（Backup Restore Job Sets）]テーブルの検索フィールドにジョブの詳細（ステータスやジョブタイプなど）を入力します。次に、目的のジョブセットをクリックします。

[Job Details] パネルに、選択したジョブセットに関する情報（ジョブのステータス、ジョブタイプ、開始時刻など）が表示されます。失敗したジョブがある場合は、[Status] 列の近くにあるアイコンの上にマウスポインタを合わせると、エラーの詳細が表示されます。

j) リモートサーバへのアップロード中にバックアップが失敗した場合：[ジョブの詳細（Job Details）] パネルの [ステータス（Status）] アイコンのすぐ下にある [バックアップのアップロード（Upload backup）] ボタンをクリックして、アップロードを再試行します。

（注） アップロードは、認証情報が正しくない、宛先ディレクトリが無効、サーバーのスペースが不足しているなど、複数の問題が原因で失敗することがあります。[バックアップのアップロード（Upload backup）]ボタンをクリックする前に、問題を調査して修正します（たとえば、古いバックアップをクリーンアップしてスペースを解放するか、[宛先（Destination）] ボタンを使用して別のリモートサーバーとパスを指定します）。

ステップ 3 バックアップファイルから復元するには、次の手順を実行します。

a) メインメニューから、**[管理（Administration）]** > **[バックアップと復元（Backup and Restore）]** を選択します。

b) [バックアップおよび復元ジョブセット（Backup and Restore Job Sets）] テーブルで、復元に使用するバックアップファイルを選択します。[ジョブの詳細（Job Details）] パネルには、選択したバックアップ ファイルに関する情報が表示されます。

c) バックアップファイルを選択した状態で、[ジョブの詳細（Job Details）] パネルに表示されている **[復元（Restore）]** ボタンをクリックして、復元操作を開始します。Cisco Crosswork は対応する復元ジョブセットを作成し、ジョブリストに追加します。

復元操作の進行状況を表示するには、進行状況ダッシュボードへのリンクをクリックします。

（注） データバックアップを復元する手順も同様です。[バックアップと復元のジョブセット（Backup and Restore Job Sets）]テーブルでデータバックアップファイルを選択します。データバックアップファイルを選択した状態で、[ジョブの詳細（Job Details）] パネルに表示されている **[データの復元（Data Restore）]** ボタンをクリックして、データの復元操作を開始します。

災害後に Cisco Crosswork を復元する

ディザスタリカバリは、自然災害または人為的な災害によって Cisco Crosswork クラスタが破壊された後に使用する復元操作です。『*Cisco Crosswork Infrastructure 4.4 and Applications Installation Guide*』の手順に従って、最初に新しいクラスタを展開する必要があります。

クラスタに誤動作しているハイブリッドノードが 1 つあるか、または 1 つ以上の誤作動しているワーカーノードがある場合は、ディザスタリカバリを実行しないでください。代わりに、ク

ラスタ管理機能を使用してこれらのノードを再展開するか、このガイドに記載されている「Crosswork クラスタの管理 （7 ページ）」の章の説明に従って新しいノードに置き換えます。

誤動作しているハイブリッドノードが複数ある場合、システムは機能状態になりません。障害が発生したハイブリッドノードを交換または再起動しても、システムが正しく回復する保証はありません。この場合、新しいクラスタを展開した後、古いクラスタから取得した最新のバックアップを使用するとシステム全体を回復できます。詳細については、このガイドの「Crosswork クラスタの管理 （7 ページ）」の章を参照してください。

ディザスタリカバリを実行する場合は、次の点に注意してください。

- バックアップを復元する新しい Cisco Crosswork クラスタは、バックアップを作成したものと同じ IP アドレスを使用する必要があります。内部証明書は元のクラスタの IP アドレスを使用するため、このガイドラインは重要です。
- 新しいクラスタには、バックアップを作成したクラスタと同じ数とタイプのノードが必要です。
- 新しいクラスタは、バックアップの作成時に使用したものと同じ Cisco Crosswork のソフトウェアイメージを使用する必要があります。異なるバージョンのソフトウェアを使用して作成されたバックアップを使用してクラスタを復元することはできません。
- 完全バックアップの代わりにデータバックアップ（**[アクション（Actions）]>[データバックアップ（Data Backup）]**）を作成している場合は、通常の災害復元の代わりに [災害後のデータ復元] を実行できます。 [災害後のデータ復元（Data Disaster Restore）] を実行する前に、（データバックアップを作成したときに）古い Crosswork クラスタに存在していた正確なバージョンのアプリケーションを新しい Crosswork クラスタにインストールして使用できるようにする必要があります。アプリケーションのビルドバージョンに不一致があると、データが失われ、復元ジョブが失敗する可能性があります。
- 災害が発生する前のシステムの状態を回復できるように、バックアップを最新の状態に保ちます。復元操作では、バックアップが作成されたときにインストールされていたすべてのアプリケーションを復元します。前回のバックアップ以降に追加のアプリケーションやパッチをインストールしてた場合は、別のバックアップを作成します。
- ディザスタリカバリが失敗した場合は、シスコ カスタマー エクスペリエンスにお問い合わせください。
- Crosswork アプリケーションのスマートライセンス登録は、災復元操作中には復元されないため、再度登録する必要があります。

ディザスタリカバリを実行するには、次の手順を実行します。

始める前に

SCP バックアップサーバーから、ディザスタリカバリで使用するバックアップファイルの完全な名前を取得します。このファイルは通常は作成した最新のバックアップファイルです。Cisco Crosswork のバックアップファイル名の形式は次のとおりです。

`backup_JobName_CWVersion_TimeStamp.tar.gz`

ここで、

- *JobName* は、ユーザーが入力したバックアップジョブの名前です。
- *CWVersion* は、バックアップされたシステムの Cisco Crosswork プラットフォームのバージョンです。
- *TimeStamp* は、Cisco Crosswork がバックアップファイルを作成した日時です。

例：`backup_Wednesday_4-0_2021-02-31-12-00.tar.gz`

ステップ 1 新たに展開したクラスタのメインメニューから、**[管理（Administration）]**>**[バックアップと復元（Backup and Restore）]** を選択します。

ステップ 2 **災害後の復元を実行するには、次の手順を実行します。**

[アクション（Actions）] > **[災害後の復元（Disaster Restore）]** をクリックして、リモートサーバーの詳細が事前に入力された [災害後の復元（Disaster Restore）] ダイアログボックスを表示します。

ステップ 3 **災害後の復元を実行するには、次の手順を実行します。**

[アクション（Actions）] > **[災害後のデータ復元（Data Disaster Restore）]** をクリックして、リモートサーバーの詳細が事前に入力された [災害後のデータ復元（Data Disaster Restore）] ダイアログボックスを表示します。

ステップ 4 [バックアップファイル名（Backup File Name）] フィールドに、復元するバックアップのファイル名を入力します。

ステップ 5 [復元の開始（Start Restore）] をクリックして、リカバリ操作を開始します。

操作の進行状況を表示するには、進行状況ダッシュボードへのリンクをクリックします。

Crosswork データゲートウェイのディザスタリカバリシナリオ

このセクションでは、Cisco Crosswork が災害から回復した後に Crosswork Data Gateways を復元するさまざまなシナリオについて説明します。

Cisco Crosswork のディザスタリカバリプロセスは、ネットワーク内の Crosswork Data Gateways を自動的に復元します。次の手順は、Crosswork Data Gateway VM が Cisco Crosswork から削除された場合にのみ必要です。

- ハイアベイラビリティを備えた Crosswork データゲートウェイのディザスタリカバリ（129 ページ）：プール内のすべてのアクティブおよびスタンバイの Crosswork Data Gateway VM は、[動作状態（Operational state）] が [エラー（Error）] になります。

- ハイアベイラビリティなしの Crosswork データゲートウェイのディザスタリカバリ （130 ページ） ：Crosswork Data Gateway VM が 1 つしかないプール、またはスタンバイ VM のない [エラー（Error）] 状態のアクティブな Crosswork Data Gateway VM が複数あるプール。

ハイアベイラビリティを備えた Crosswork データゲートウェイのディザスタリカバリ

次の手順に従って、[エラー（Error）] 状態のアクティブおよびスタンバイの Crosswork Data Gateway VM を含む Crosswork Data Gateway プールを復元します。これらの手順では、1 つのアクティブ VM と 1 つのスタンバイ VM を持つプールを使用します。

始める前に

この手順を続行する前に、Cisco Crosswork ディザスタリカバリ操作が完了していることを確認してください。Crosswork Data Gateway の VM とプールに関するすべての情報は、Crosswork ディザスタリカバリが完了すると、Cisco Crosswork で利用できるようになります。

ステップ 1 災害前のプール内の VM と同じ情報（プロファイル、ホスト名、管理インターフェイス）を持つ新しい Crosswork Data Gateway VM をインストールします。

Cisco Crosswork のディザスタリカバリプロセスが古い VM からデータを復元するため、新しくインストールされた Crosswork Data Gateway VM の動作状態は [エラー（Error）] になります。

ステップ 2 Cisco Crosswork にログインします。

ステップ 3 **[管理（Administration）] > [データゲートウェイ管理（Data Gateway Management）] > [プール（Pools）]** の順に移動します。

ステップ 4 プールを選択して編集し、プールからスタンバイ VM を削除（割り当て解除）します。Crosswork Data Gateway プールの管理 （42 ページ）を参照してください

ステップ 5 スタンバイ VM の [管理状態（Administration State）] を [メンテナンス（Maintenance）] モードに変更します。Cisco Crosswork Data Gateway VM の管理状態の変更 （47 ページ） を参照してください。

約 5 分間待ちます。VM は Cisco Crosswork に自動的に登録します。

（注） データゲートウェイ VM のインタラクティブコンソールから、Cisco Crosswork に VM を手動で再登録することもできます。Crosswork Data Gateway の再登録 （415 ページ） を参照してください。

ステップ 6 プールを再度編集し、スタンバイ VM をプールに追加します。

スタンバイ VM を追加するとフェールオーバーがトリガーされ、新しく追加された VM がプール内のアクティブな VM になります。

ステップ 7 手順 4 から 7 を繰り返して、[動作状態（Operational State）] が [エラー（Error）] になっている（現在の）スタンバイ VM を復元します。

ステップ 8 次のことを確認してください。

- プールには、以前と同様にアクティブ VM とスタンバイ VM があります。
- デバイスは、プール内のアクティブな VM に接続されています。
- 収集ジョブは期待どおりに実行されています。

ハイアベイラビリティなしの Crosswork データゲートウェイのディザスタリカバリ

障害が発生した場合、次の方法を使用して、高可用性なしで Crosswork Data Gateway VM を復元できます。

- 単一の VM を、新しくインストールされた VM（古い VM と同じ情報でインストールされた）で置き換える。
- デバイスを切り離すか、デバイスをネットワーク内の別のデータゲートウェイに移動する。
- スタンバイ VM をプールに追加する（追加の VM をインストールし、プールにスタンバイとして追加する）。

始める前に

この手順を続行する前に、Cisco Crosswork ディザスタリカバリ操作が完了していることを確認してください。Crosswork Data Gateway の VM とプールに関するすべての情報は、Crosswork ディザスタリカバリプロセスが完了すると、Cisco Crosswork で利用できるようになります。

ステップ 1 **古い VM を、古い VM と同じ情報でインストールされた新しくインストールされた VM に置き換える**

a) Cisco Crosswork にログインします。
b) **[管理（Administration）]** > **[データゲートウェイの管理（Data Gateway Management）]** > **[データゲートウェイ（Data Gateways）]**に移動します。
c) 既存のプールを削除します。
d) VM の [管理状態（Administration State）] を [メンテナンス（Maintenance）] モードに変更します。Cisco Crosswork Data Gateway VM の管理状態の変更 （47 ページ） を参照してください。
e) 古い VM と同じ情報を使用して、新しい Crosswork Data Gateway VM をインストールします。
f) VM の [管理状態（Administration State）] を [メンテナンス（Maintenance）] モードの [アップ（Up）] に変更します。

   VM の [動作状態（Operational State）] が [エラー（Error）] から [準備完了（Not Ready）] に変わります。

g) 古いプールと同じ名前で新しいプールを作成し、VM をそのプールに追加します。

Crosswork Data Gateway の [動作状態（Operational State）] が [アップ（Up）] であることを確認します。

h) デバイスをデータゲートウェイに接続します。Crosswork Data Gateway へのデバイスの接続 （39 ページ） を参照してください。

i) 収集ジョブが期待どおりに実行されていることを確認します。

ステップ 2 デバイスを切り離すか、デバイスをネットワーク内の別のデータゲートウェイに移動する

a) Cisco Crosswork にログインします。

b) **[管理（Administration）]>[データゲートウェイの管理（Data Gateway Management）]>[データゲートウェイ（Data Gateways）]**に移動します。

c) VM からデバイスを切り離すか、動作上 [アップ（Up）] している別のデータゲートウェイにデバイスを移動します。Cisco Crosswork Data Gateway デバイス割り当ての管理 （44 ページ） を参照してください。

d) 既存のプールを削除します。

これを行っても、プールから VM の割り当てが解除されることはありません。VM は引き続きプールに割り当てられたものとして表示されます。

e) VM の [管理状態（Administration State）] を [メンテナンス（Maintenance）] モードに変更します。Cisco Crosswork Data Gateway VM の管理状態の変更 （47 ページ） を参照してください。

f) VM を再起動します。これを行うと、プールから VM の割り当てが解除されます。

約 5 分間待ちます。VM は Cisco Crosswork に自動的に登録します。VM が管理上 [アップ（Up）] であり、準備ができていない状態であることを確認します。

（注） データゲートウェイ VM のインタラクティブコンソールから、Cisco Crosswork に VM を手動で再登録することもできます。Crosswork Data Gateway の再登録 （415 ページ） を参照してください。

g) 古いプールと同じ名前で新しいプールを作成し、VM をそのプールに追加します。

h) Crosswork Data Gateway の [動作状態（Operational State）] が [アップ（Up）] になっていることを確認します。

i) デバイスを接続するか、デバイスをこのデータゲートウェイに戻します。Cisco Crosswork Data Gateway デバイス割り当ての管理 （44 ページ） を参照してください。

j) 収集ジョブが期待どおりに実行されていることを確認します。

ステップ 3 スタンバイ VM をプールに追加する（追加の VM をインストールし、プールにスタンバイとして追加する）

（注） 次の手順は、[エラー（Error）] 状態のアクティブな VM が 1 つあるプールを復元する手順を示しています。スタンバイ VM を使用せずに、[エラー（Error）]状態のプール内の複数のアクティブな VM を復元するには、プール内のアクティブな VM ごとに追加の VM を追加してください。

a) 新しい Crosswork Data Gateway VM をインストールします。

b) Cisco Crosswork にログインします。

c) **[管理（Administration）]>[データゲートウェイ管理（Data Gateway Management）]>[プール（Pools）]** の順に移動します。

d) プールを選択して編集し、新しくインストールした VM をプールに追加します。Crosswork Data Gateway プールの管理 （42 ページ）を参照してください

VM を追加するとフェールオーバーがトリガーされ、新しく追加された VM がプール内のアクティブな VM になります。

e) プールを編集し、（現在の）スタンバイ VM をプールから削除します。

f) スタンバイ VM の [管理状態（Administration State）] を [メンテナンス（Maintenance）] モードに変更します。Cisco Crosswork Data Gateway VM の管理状態の変更 （47 ページ） を参照してください。

約 5 分間待ちます。VM は Cisco Crosswork に自動的に登録します。VM が動作可能であり、[準備中（Not Ready）] であることを確認します。

（注） データゲートウェイ VM のインタラクティブコンソールから、Cisco Crosswork に VM を手動で再登録することもできます。Crosswork Data Gateway の再登録 （415 ページ） を参照してください。

g) プールを再度編集し、スタンバイ VM をプールに追加します。

h) Crosswork Data Gateway が動作上 [アップ（Up）] であり、プールにアクティブおよびスタンバイ VM があることを確認します。

i) 次のことを確認してください。

- デバイスは、プール内のアクティブな VM に接続されています。
- 収集ジョブは期待どおりに実行されています。

欠落している SR-TE（SR-MPLS および SRv6）ポリシーと RSVP-TE トンネルの解決

このトピックの情報は、Cisco Crosswork Optimization Engine がインストールされている場合にのみ適用されます。

設定データベースには、Cisco Crosswork が 認識しているすべての SR-TE ポリシーと RSVP-TE トンネルが含まれています。Cisco Crosswork は、SR-TE ポリシーまたは RSVP-TE トンネルをプロビジョニング、変更、または削除するたびに設定データベースを更新します。設定データベースの CLI ツールを使用して、次の操作を実行できます。

- 設定データベースに対する CSV ファイルの読み取りと書き込み。
- 設定データベースから SR-TE ポリシーと RSVP-TE トンネル情報の入力による CSV ファイルの作成。

設定データベース の CLI ツールは、復元操作後に欠落している SR-TE ポリシーと RSVP-TE トンネルを回復する場合に特に役立ちます。たとえば、`-dump-missing` オプションは、欠落している SR-TE ポリシーと RSVP-TE トンネルのリストを表示する CSV ファイルを生成します。

この CSV ファイルを使用して、欠落している SR-TE ポリシーと RSVP-TE トンネルを特定します。次に、`-load`オプションを使用してトポロジにもう一度ロードします。詳細については、CLI ツールのヘルプを参照してください。

ステップ 1 **optima-pce-dispatcher** コンテナを入力します。

```
kubectl exec -it optima-pce-dispatcher-XXXXXXX-XXXX bash
```

ステップ 2 次のコマンドを実行できます。

a) CLI ツールのヘルプテキストを表示します。

```
python3 /opt/optima/pce_dispatcher/config_db/csv_util.py --help
```

b) 設定データベース内のすべての SR-TE ポリシーと RSVP-TE トンネルを CSV ファイルに保存します。

```
python3 /opt/optima/pce_dispatcher/config_db/csv_util.py --dump /<PathToFile>/dump_file.csv
```

c) 生成された CSV ファイルから内容をロードし、設定データベースにポリシーを書き込みます。

```
python3 /opt/optima/pce_dispatcher/config_db/csv_util.py --load /<PathToFile>/load_file.csv
```

（注） このコマンドは、検出された重複する SR-TE ポリシーまたは RSVP-TE トンネルを上書きし、有効な TE トンネルのみを設定データベースに追加します。重複する SR-TE ポリシーには、同じ組み合わせのヘッドエンド、エンドポイント、および色があります。重複する RSVP-TE トンネルには、同じ組み合わせのヘッドエンドとトンネル名があります。

d) CSV のロードが完了したら、次のように、Cisco Crosswork Optimization Engine を再起動してその UI を設定データベースと同期します。

1. メインメニューから、**[管理（Administration）]** > > **[Crosswork Manager]** > **[Crosswork の正常性（Crosswork Health）]** > **[最適化エンジン（Optimization Engine）]** を選択します。
2. **[optima-ui-service]** > > **[アクション（Action）]** > **[再起動（Restart）]** を選択します。再起動には約 5 分かかります。

e) 再起動後、現在トポロジ内にある SR-TE ポリシーと RSVP-TE トンネルを設定データベースの内容と比較します。欠落している SR ポリシーと RSVP-TE トンネルを CSV ファイルに保存します。この CSV ファイルと次のコマンドを使用して、欠落しているポリシーを設定データベースにロードできます。

```
python3 /opt/optima/pce_dispatcher/config_db/csv_util.py -dump-missing /<PathToFile>/dump_file.cs
```

Cisco NSO を使用した Cisco Crosswork のバックアップ

現在、NSO バックアップファイルからの復元は手動プロセスです。

始める前に

始める前に、次のことを確認します。

- セキュア SCP サーバーのホスト名または IP アドレスとポート番号がわかっている。
- バックアップファイルの接続先として使用する SCP サーバーのファイルパスがわかっている。
- 接続先 SCP サーバーのストレージフォルダに対する読み取り権限と書き込み権限を持つアカウントのユーザークレデンシャルがわかっている。

また、NSO プロバイダー、NSO プロバイダーに関連付けられている Cisco Crosswork のクレデンシャルプロファイル、および NSO サーバーが次の前提条件を満たしていることを確認します。

- NSO プロバイダー設定には SSH 接続が含まれます。プロバイダーで SSH を有効にしていない場合、Cisco Crosswork は警告アラームを表示します。Cisco Crosswork は、独自のデータのバックアップを作成しますが、NSO のバックアップは作成しません。
- NSO プロバイダのクレデンシャルプロファイルには、NSO サーバーで `sudo` 権限を持つユーザーのユーザー ID とパスワードが含まれている。
- NSO サーバーには NCT（NSO クラスタツール）がインストールされており、NSO プロバイダのクレデンシャルプロファイルのユーザーは `nct` コマンドを実行できる。
- NSO サーバーには Python バージョン 3.x がインストールされており、NSO プロバイダのクレデンシャルプロファイルのユーザーは `python3` コマンドを実行できる。
- NSO プロバイダのクレデンシャルプロファイルのユーザーは、NSO サーバーのバックアップフォルダとその中のファイルにフルアクセスできる。この要件は通常、NSO サーバーの `/var/opt/ncs/backups/` フォルダに対する完全な読み取り/書き込みアクセスを意味します。

これらの Cisco NSO 要件のいずれかが満たされていない場合、バックアップジョブのすべて、または一部が失敗します。

これらの特別な要件に加えて、Cisco Crosswork のバックアップと復元の管理（123 ページ）で説明されているバックアップの通常のガイドラインは、NSO データを含むバックアップにも適用されます。

ステップ 1 **SCP バックアップサーバーを設定します。**

a) メインメニューから、**[管理（Administration）]** > **[バックアップと復元（Backup and Restore）]** を選択します。

b) [接続先（Destination）] をクリックして、[接続先の編集（Edit Destination）] ダイアログボックスを表示します。表示されたフィールドに関連するエントリを入力します。

c) [保存（Save）] をクリックして、バックアップサーバーの詳細を確認します。

ステップ 2 **Cisco Crosswork と Cisco NSO のバックアップを作成します。**

a) メインメニューから、**[管理（Administration）]** > **[バックアップと復元（Backup and Restore）]** を選択します。

b) **[Actions]** > **[Backup]** をクリックして、宛先サーバーの詳細が事前に入力された [Backup] ダイアログボックスを表示します。

c) [Job Name] フィールドに、バックアップに該当する名前を入力します。

d) Cisco Crosswork アプリケーションまたはマイクロサービスの問題があるにもかかわらず、[強制（Force）] チェックボックスをオンにします。

e) [NSOのバックアップ（Backup NSO）] チェックボックスはオンのままにしてください。

f) 必要に応じて残りのフィールドにも入力します。

別のリモート サーバー アップロード先を指定する場合：事前に入力された [Host Name]、[Port]、[Username]、[Password]、および [Remote Path] フィールドを編集して、別の接続先を指定します。

g) （オプション）[バックアップ準備の確認（Verify Backup Readiness）] をクリックして、Cisco Crosswork にバックアップを完了するのに十分な空きリソースがあることを確認します。確認が成功すると、時間がかかる動作の特性に関する警告が Cisco Crosswork に表示されます。[OK] をクリックして、先へ進みます。

h) [バックアップの開始（Start Backup）] をクリックして、バックアップ操作を開始します。Cisco Crosswork は、対応するバックアップジョブセットを作成し、それをジョブリストに追加し、バックアップの処理を開始します。[ジョブ詳細（Job Details）] パネルには、完了した各バックアップステップのステータスが表示されます。

i) バックアップジョブの進行状況を表示するには、[ジョブセットのバックアップ/復元（Backup Restore Job Sets）] テーブルの検索フィールドにジョブの詳細（ステータスやジョブタイプなど）を入力します。次に、目的のジョブセットをクリックします。

[Job Details] パネルに、選択したジョブセットに関する情報（ジョブのステータス、ジョブタイプ、開始時刻など）が表示されます。失敗したジョブがある場合は、[Status] 列の近くにあるアイコンの上にマウスポインタを合わせると、エラーの詳細が表示されます。

j) リモートサーバへのアップロード中にバックアップが失敗した場合：[ジョブの詳細（Job Details）] パネルの [ステータス（Status）] アイコンのすぐ下にある [バックアップのアップロード（Upload backup）] ボタンをクリックして、アップロードを再試行します。

リモートサーバーの問題が原因でアップロードが失敗した場合は、[バックアップのアップロード（Upload backup）] をクリックする前に、[接続先（Destination）] ボタンを使用して別のリモートサーバーとパスを指定します。

Cisco NSO を使用して Cisco Crosswork を復元する

Cisco Crosswork クラスタとそれに関連する Cisco NSO クラスタをバックアップから復元する場合は、次のガイドラインに従います。

- 復元操作は、スケジュールされているメンテナンス期間にのみ実行することをお勧めします。これらの操作の実行中、ユーザーは Cisco Crosswork や Cisco NSO にアクセスしようとしないでください。Cisco Crosswork の復元操作は時間がかかり、完了するまでは他の Cisco Crosswork アプリケーションが一時停止します。復元中は、Cisco NSO を完全に停止する必要があります。

- Cisco Crosswork と Cisco NSO の両方の復元操作を同時に実行できます。

始める前に

復元するバックアップファイルの完全な名前を SCP サーバーから取得します。このファイルには、Cisco Crosswork と Cisco NSO の両方のバックアップが含まれています。バックアップファイル名の形式は次のとおりです。

`backup_JobName_CWVersion_TimeStamp.tar.gz`

ここで、

- *JobName* は、ユーザーが入力したバックアップジョブの名前です。
- *CWVersion* は、バックアップされたシステムの Cisco Crosswork プラットフォームのバージョンです。
- *TimeStamp* は、Cisco Crosswork がバックアップファイルを作成した日時です。

例：`backup_Wed_4-0_2021-02-31-12-00.tar.gz.`

ステップ 1 リモート SCP バックアップサーバーにログインします（必要な場合）。Linux コマンドラインを使用して、バックアップ先ディレクトリにアクセスし、復元する Cisco NSO 情報を含んでいるバックアップファイルを検索します。次に例を示します。

```
[root@localhost~]# ls -ltr
-rw-rw-r--. 1 root root 8265938605 backup_Wed_4-0_2021-02-31-12-00.tar.gz
```

ステップ 2 `tar-xzvf` を使用して、接続先フォルダの Cisco Crosswork バックアップファイルから Cisco NSO バックアップを抽出します。次に例を示します。

```
[root@localhost~]# tar -xzvf backup_Wed_4-0_2021-02-31-12-00.tar.gz
...
[root@localhost~]# ls -ltr
-rw-rw-r--. 1 root root 8265938605 backup_Wed_4-0_2021-02-31-12-00.tar.gz
-rw-r--r--. 1 root root 8267798605 468c4715-ea09-4c2b-905e-98999d.tar.gz
```

ステップ 3 接続先フォルダの Cisco NSO バックアップファイルを展開します。`/nso/ProviderName/` のフォルダ構造に抽出する Cisco NSO ファイルが表示されます。ここで、`/nso/ProviderName/` は Cisco Crosswork に設定されている Cisco NSO プロバイダの名前です。次の例では、Cisco NSO プロバイダの名前は `nso121` です。

```
tar -xvsf 468c4715-ea09-4c2b-905e-98999d.tar.gz
468c4715-ea09-4c2b-905e-98999d/nso/
468c4715-ea09-4c2b-905e-98999d/nso/nso121/
468c4715-ea09-4c2b-905e-98999d/nso/nso121/log/
468c4715-ea09-4c2b-905e-98999d/nso/nso121/log/nso_backup_result_nso121_Wed.log
468c4715-ea09-4c2b-905e-98999d/nso/nso121/NSO_RESTORE_PATH_nso121
468c4715-ea09-4c2b-905e-98999d/nso/nso121/ncs-5.4.2@backup_Wed_nso121.backup.gz
...
```

ステップ 4 `/nso/ProviderName/` フォルダで拡張子が backup.gz のファイルを見つけます。これが、生成された Cisco NSO バックアップファイルです。前の手順の例では、ファイル名が強調表示されています。

ステップ 5 root 権限を持つユーザーとして Cisco NSO にログインし、コマンドラインにアクセスします。次に、生成された Cisco NSO バックアップファイルを SCP サーバーから Cisco NSO クラスタに指定した復元パスの場所へコピーまたは移動します。次に例を示します。

```
[root@localhost nsol21]# ls
log ncs-5.4.2@backup_Wed_nso121.backup.gz NS0_REST0RE_PATH_nso121
[root@localhost nso121]# more NS0_REST0RE_PATH_nso121
/var/opt/ncs/backups/
[root@localhost nso121]#
...
```

ステップ 6 Cisco NSO の復元操作は、NSO が実行されていないときにのみ実行できます。Cisco NSO クラスタコマンドラインで、次のコマンドを実行して Cisco NSO を停止します。

```
$/etc/init.d/ncs stop
```

ステップ 7 NCS が停止したら、次のコマンドと生成された Cisco NSO バックアップファイルの名前を使用して復元操作を開始します。次に例を示します。

```
#ncs-backup --restore ncs-5.4.2@backup_Wed_nso121.backup.gz
```

このコマンドの実行に問題がある場合は、まず `sudo su` 権限を付与します。

ステップ 8 復元が完了したら、次のコマンドを使用して Cisco NSO を再起動します。このコマンドは完了するまでに数分かかる場合があります。

```
$/etc/init.d/ncs start
```

ステップ 9 Cisco Crosswork クラスタと Cisco NSO クラスタの両方をバックアップから復元したら、Cisco NSO プロバイダを Cisco Crosswork に再度追加します。

バックアップと復元を使用してデータを移行する

データ移行のバックアップと復元を使用することは、Cisco Crosswork インストールを新しいソフトウェアバージョンにアップグレードするとき、または既存のデータを新しいインストールに移動するときの前提条件です。

通常のバックアップと同様に、データ移行バックアップを作成するときは常に次のガイドラインに従ってください。

- データ移行ファイルを格納する宛先 SCP サーバーが設定されていることを確認してください。この設定は 1 回限りのアクティビティです。
- Cisco Crosswork クラスタと SCP サーバーの両方が同じ IP 環境内に存在する必要があります。たとえば、Cisco Crosswork が IPv6 で通信している場合は、バックアップサーバーも IPv6 で通信している必要があります。
- Cisco Crosswork インストールをアップグレードする場合にのみデータ移行バックアップを作成し、スケジュールされたアップグレードウィンドウ中にのみ作成することをお勧めします。データ移行のバックアップまたは復元操作の実行中は、Cisco Crosswork にアクセスしないでください。

始める前に

作業を開始する前に、次を確認してください。

- セキュアな SCP サーバーのホスト名または IP アドレスおよびポート番号。
- データ移行用バックアップファイルの接続先として使用する SCP サーバー上のファイルパス。
- 接続先 SCP サーバーのリモートパスに対するファイルの読み取り/書き込み権限を持つアカウントのユーザークレデンシャル。

ステップ 1　SCP バックアップサーバーを設定します。

a) メインメニューから、**[管理（Administration）] > [バックアップと復元（Backup and Restore）]** を選択します。

b) [接続先（Destination）] をクリックして、[接続先の編集（Edit Destination）] ダイアログボックスを表示します。表示されたフィールドに関連するエントリを入力します。

c) [保存（Save）] をクリックして、バックアップサーバーの詳細を確認します。

ステップ 2　バックアップを作成します。

a) データを別のインストールに移行する Cisco Crosswork インストールに管理者としてログインします。

b) メインメニューから、**[管理（Administration）] > [バックアップと復元（Backup and Restore）]** を選択します。

c) **[Actions] > [Backup]** をクリックして、宛先サーバーの詳細が事前に入力された [Backup] ダイアログボックスを表示します。

d) [Job Name] フィールドに、バックアップに該当する名前を入力します。

e) Cisco Crosswork アプリケーションまたはマイクロサービスの問題があるにもかかわらず、[強制（Force）] チェックボックスをオンにします。

f) 必要に応じて残りのフィールドにも入力します。

別のリモートサーバーアップロード先を指定する場合：事前に入力された [ホスト名（Host Name）]、[ポート（Port）]、[ユーザー名（Username）]、[パスワード（Password）]、および [リモートパス（Remote Path）] フィールドを編集して、別の接続先を指定します。

g) [バックアップの開始（Start Backup）] をクリックして、バックアップ操作を開始します。Cisco Crosswork は、対応するバックアップジョブセットを作成し、それを [バックアップおよび復元ジョブセット（Backup and Restore Job Sets）] テーブルに追加します。[Job Details] パネルには、完了した各バックアップステップのステータスが表示されます。

h) バックアップジョブの進行状況を表示するには、[Backup and Restore Job Sets] テーブルの検索フィールドにジョブの詳細（ステータスやジョブタイプなど）を入力します。次に、目的のジョブセットをクリックします。

[Job Details] パネルに、選択したジョブセットに関する情報（ジョブのステータス、ジョブタイプ、開始時刻など）が表示されます。失敗したジョブがある場合は、[Status] 列の近くにあるアイコンの上にマウスポインタを合わせると、エラーの詳細が表示されます。

i) リモートサーバへのアップロード中にバックアップが失敗した場合：[ジョブの詳細（Job Details）] パネルの [ステータス（Status）] アイコンのすぐ下にある [バックアップのアップロード（Upload backup）] ボタンをクリックして、アップロードを再試行します。

リモートサーバーの問題が原因でアップロードが失敗した場合は、[バックアップのアップロード（Upload backup）] をクリックする前に、[接続先（Destination）] ボタンを使用して別のリモートサーバーとパスを指定します。

ステップ 3 バックアップの新しいインストールへの移行（Migrate the backup to the new installation）

a) バックアップからデータを移行する先の Cisco Crosswork インストールに管理者としてログインします。

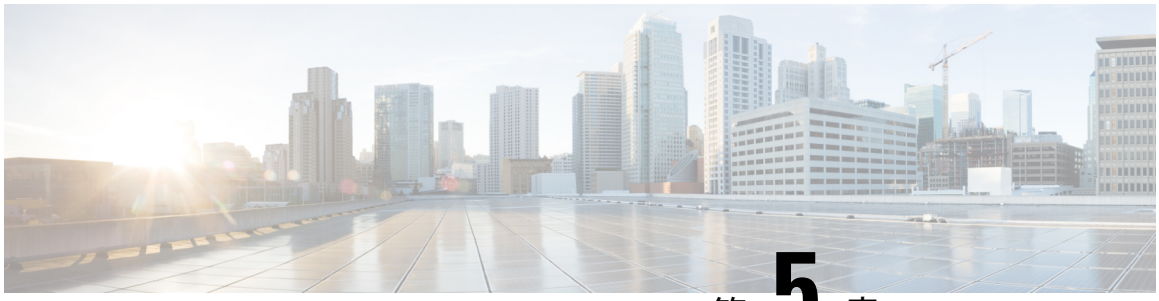
b) メインメニューから、**[管理（Administration）] > [バックアップと復元（Backup and Restore）]** を選択します。

c) **[アクション（Actions）] > [データ移行（Data Migration）]** をクリックして、リモートサーバーの詳細が事前に入力された [Data Migration] ダイアログボックスを表示します。

d) [バックアップファイル名（Backup File Name）] フィールドに、復元するバックアップのファイル名を入力します。

e) [移行を開始（Start Migration）] をクリックして、データ移行操作を開始します。Cisco Crosswork は、対応するデータ移行ジョブセットを作成し、それをジョブリストに追加します。

データ移行操作の進行状況を表示するには、進行状況ダッシュボードへのリンクをクリックします。



第 5 章

デバイス管理のインフラストラクチャの準備

ここでは、次の内容について説明します。

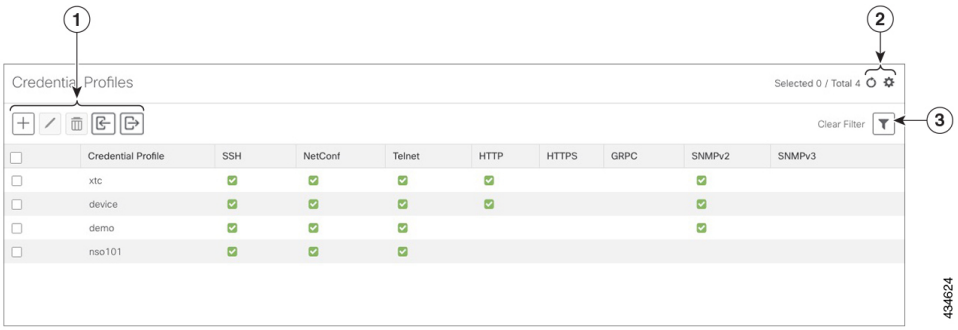
クレデンシャルプロファイルの管理

クレデンシャルプロファイルは、SNMP、Telnet、SSH、HTTP、およびその他のネットワークプロトコルのクレデンシャルの集まりです。1 つのクレデンシャルプロファイルに複数のプロトコルとクレデンシャルを設定できます。

クレデンシャルプロファイルを使用すると、デバイス設定の変更とモニタリングを自動化したり、プロバイダと通信したりできます。デバイスを追加またはインポートする場合、またはプロバイダーを作成する場合は、クレデンシャルプロファイルを指定します。

[クレデンシャルプロファイル（Credential Profiles）] ウィンドウから、新しいクレデンシャルプロファイルを作成したり、既存のプロファイルの設定を更新したり、プロファイルを削除したりできます。このウィンドウを開くには、メインメニューから **[デバイス管理（Device Management）] > [クレデンシャルプロファイル（Credential Profiles）]** を選択します。

図 *15 : [*クレデンシャルプロファイル（***Credentials Profile***）*]* ウィンドウ



項目	説明
1	をクリックして、クレデンシャルプロファイルを追加します。「クレデンシャルプロファイルの作成 （143 ページ）」を参照してください。
	をクリックして、選択したクレデンシャルプロファイルの設定を編集します。「クレデンシャルプロファイルの編集 （148ページ）」を参照してください。
	をクリックして、選択したクレデンシャルプロファイルを削除します。「クレデンシャルプロファイルの削除 （149ページ）」を参照してください。
	クリックして、CSV ファイルから新しいクレデンシャルプロファイルをインポートします。このアイコンをクリックして、CSV ファイルテンプレートをダウンロードすることもできます。テンプレートには、独自の CSV ファイルを作成するためのガイドとして使用できるサンプルデータが含まれています。「クレデンシャルプロファイルのインポート （145ページ）」を参照してください。
	をクリックして、クレデンシャルプロファイルを CSV ファイルにエクスポートします。クレデンシャルプロファイルのエクスポート （149ページ）を参照してください。
2	をクリックして、[クレデンシャルプロファイル（Credential Profiles）] ウィンドウを更新します。
	をクリックして、[クレデンシャルプロファイル（Credential Profiles）] ウィンドウに表示する列をクリックして選択します。

項目	説明
3	をクリックして、[クレデンシャルプロファイル（Credential Profiles）] ウィンドウの 1 つ以上の列にフィルタ条件を設定します。
	設定したフィルタ条件をクリアするには、[フィルタのクリア（Clear Filter）] リンクをクリックします。

クレデンシャルプロファイルの作成

新しいクレデンシャルプロファイルを作成するには、次の手順を実行します。次に、プロファイルを使用し、新しいデバイスまたはプロバイダを追加するときにクレデンシャルを一貫して適用できます。必要な数のプロトコルと対応するクレデンシャルをプロファイルに追加できます。

追加するクレデンシャルプロファイルが多数ある場合は、CSV ファイルに情報を入れてファイルをインポートするほうが効率的です。「クレデンシャルプロファイルのインポート（145 ページ）」を参照してください。

SNMP クレデンシャルを含んでいるデバイスクレデンシャルプロファイルを作成する場合は、デバイスで実際に有効になっている SNMP のバージョンのクレデンシャルと、そのバージョンのみを含めることをお勧めします。たとえば、デバイス設定で SNMPv3 が有効になっていない場合は、そのデバイスのクレデンシャルプロファイルに SNMPv3 クレデンシャルを含めないでください。

インポートおよびエクスポートの機能と CSV ファイルを使用してクレデンシャルプロファイルを一括して作成する場合は、次の点に注意してください。

- CSV ファイルにエクスポートされたすべてのクレデンシャルプロファイルの各パスワードまたはコミュニティ文字列のエントリのすべての文字がアスタリスク（クレデンシャルプロファイルのエクスポート （149 ページ））に置き換えられます。
- CSV ファイルのパスワードとコミュニティ文字列が空白の場合は、クレデンシャルプロファイルをインポートできません（「クレデンシャルプロファイルのインポート（145 ページ）」を参照）。

ネットワークセキュリティを維持するために、インポートする CSV ファイルでは、実際のパスワードとコミュニティ文字列の代わりにアスタリスクを使用することをお勧めします。インポート後、「クレデンシャルプロファイルの編集 （148 ページ）」の手順に従ってアスタリスクを実際のパスワードとコミュニティ文字列に置き換えます。

ステップ 1 メインメニューから **[デバイス管理（Device Management）] > [クレデンシャルプロファイル（Credential Profiles）]** を選択します。

ステップ 2 をクリックします。

ステップ 3 [プロファイル名（Profile Name）] フィールドに、内容がわかるプロファイル名を入力します。名前には、最大 128 文字の英数字と、ドット（.）、アンダースコア（「_」）、またはハイフン（「-」）を含めることができます。その他の特殊文字は使用できません。

クレデンシャルプロファイルが多くなる場合は、[クレデンシャルプロファイル（Credential Profiles）] パネルに情報が表示されるため、可能な限り識別しやすい名前と説明にします。

ステップ 4 [接続タイプ（Connectivity Type）] ドロップダウンからプロトコルを選択します。

ステップ 5 次の表に示されているクレデンシャルフィールドに値を入力します。表示される必須フィールドとオプションフィールドは、選択した接続タイプによって異なります。入力する値は、デバイスに設定されている値と一致している必要があります。

接続タイプ（Connectivity Type）	フィールド
SSH	必須の [ユーザー名（User Name）]、[パスワード（Password）]、[パスワードの確認（Confirm Password）] に入力します。[イネーブルパスワード（Enable Password）] はオプションです。
SNMPv2	必須の SNMPv2 の [読み取りコミュニティ（Read Community）] 文字列を入力します。[書き込みコミュニティ（Write Community）] はオプションです。
NETCONF	必須の [ユーザー名（User Name）]、[パスワード（Password）]、[パスワードの確認（Confirm Password）] に入力します。
TELNET （注） このプロトコルを使用する場合、いくつかのセキュリティ上の制限があります。	必須の [ユーザー名（User Name）]、[パスワード（Password）]、[パスワードの確認（Confirm Password）] に入力します。[イネーブルパスワード（Enable Password）] はオプションです。
HTTP	必須の [ユーザー名（User Name）]、[パスワード（Password）]、[パスワードの確認（Confirm Password）] に入力します。
HTTPS	必須の [ユーザー名（User Name）]、[パスワード（Password）]、[パスワードの確認（Confirm Password）] に入力します。
GRPC	必須の [ユーザー名（User Name）]、[パスワード（Password）]、[パスワードの確認（Confirm Password）] に入力します。
gNMI	必須の [ユーザー名（User Name）]、[パスワード（Password）]、[パスワードの確認（Confirm Password）] に入力します。
TL1	必須の [ユーザー名（User Name）]、[パスワード（Password）]、[パスワードの確認（Confirm Password）] に入力します。

接続タイプ（Connectivity Type）	フィールド
SNMPv3	必須の [セキュリティレベル（Security Level）] を選択し、[ユーザー名（User Name）] に入力します。 AUTH_NO_PRIV または AUTH_PRIV の [セキュリティレベル（Security Level）] に NO_AUTH_NO_PRIV を選択した場合、残りのフィールドはオプションです。 [セキュリティレベル（Security Level）] に AUTH_NO_PRIV を選択した場合は、[認証タイプ（Auth Type）] を選択し、[認証パスワード（Auth Password）] を入力する必要があります。 [セキュリティレベル（Security Level）] に AUTH_PRIV を選択した場合は、[認証タイプ（Auth Type）] と [プライバシータイプ（Priv Type）] を選択し、[認証パスワード（Auth Password）] と [プライバシーパスワード（Priv Password）] を入力する必要があります。 次の SNMPv3 プライバシータイプのみがサポートされています。 • CFB_AES_128 • CBC_DES_56 次のプライバシータイプはサポートされていません。 • AES192 • AES256 • 3DES

ステップ 6 （オプション）このクレデンシャルプロファイルに追加する他のすべてのプロトコルと対応するクレデンシャルに対して、必要に応じて、[+ もう 1 つ追加する（+ Add Another）] をクリックし、上記の手順を繰り返します。

ステップ 7 [保存（Save）] をクリックします。

クレデンシャルプロファイルのインポート

複数のクレデンシャルプロファイルを指定する CSV ファイルを作成し、Cisco Crosswork アプリケーションにインポートするには、次の手順を実行します。

CSVファイルからクレデンシャルプロファイルをインポートすると、まだデータベースに存在しないプロファイルが追加されます。すでに存在するクレデンシャルプロファイルはインポートできません。

以前にエクスポートし、変更したクレデンシャルプロファイル CSV ファイルを再インポートする場合は、エクスポートしたクレデンシャルプロファイルの CSV ファイル内のすべてのパスワードとコミュニティ文字列がアスタリスクに置き換えられることに注意してください。エ

クスポートしたクレデンシャルプロファイルの CSV ファイルのパスワードが空白で設定されている場合は再インポートできません。セキュリティを維持するために、CSV ファイルの実際のパスワードとコミュニティ文字列の代わりにアスタリスクを使用することをお勧めします。インポート後、「クレデンシャルプロファイルの編集（148ページ）」の手順に従ってアスタリスクを実際のパスワードとコミュニティ文字列に置き換えます。

ステップ 1 メインメニューから **[デバイス管理（Device Management）]** > **[クレデンシャルプロファイル（Credential Profiles）]** を選択します。

ステップ 2 をクリックして、ダイアログボックスを開きます。

ステップ 3 インポートするクレデンシャルプロファイルのCSVファイルをまだ作成していない場合は、次の手順を実行します。

a) [「Credential template（*.csv）」サンプルファイルのダウンロード（Download sample 'Credential template (*.csv)' file）] リンクをクリックし、CSV ファイルテンプレートをローカルディスクに保存します。

b) 任意のツールを使用してテンプレートを開きます。ファイルに行を追加し始めます（クレデンシャルファイルごとに 1 行）。

同じフィールド内で複数のエントリを区切るには、セミコロンを使用します。それらのエントリ間に2つのセミコロンをスペースなしで使用することで、フィールドを空白のままにすることを示します。複数のエントリをセミコロンで区切る場合は、各フィールドに値を入力する順序が重要であることに注意してください。たとえば、[接続タイプ（Connectivity Type）] フィールドに **`SSH;NETCONF;TELNET`** と入力し、[ユーザー名（User Name）] フィールドに **`UserTom;UserDick;UserHarry;`** と入力する場合、エントリの順序によって 2 つのフィールド間のマッピングが決定されます。

- SSH：UserTom
- NETCONF：UserDick
- TELNET：UserHarry

次の点にも注意してください。

- デバイスで現在入力されている SNMP コミュニティ文字列情報を正確に入力してください。
- ユーザー ID に関連付けられたパスワードとコミュニティ文字列情報は、作成した CSV ファイルにプレーンテキストで保存されます。これがセキュリティに与える影響に注意し、適切な保護対策を適用してください。

フィールド	エントリ	必須またはオプション
クレデンシャルプロファイル（Credential Profile）	クレデンシャルプロファイルの名前。 例：。	必須
接続タイプ（Connectivity Type）	有効な値：**`SSH`**、**`SNMPv2`**、**`NETCONF`**、**`TELNET`** 、**`HTTP`**、**`HTTPS`**、**`GRPC`**、または **`SNMPv3`**	

フィールド	エントリ	必須またはオプション
ユーザー名（**User Name**）	例：	[接続タイプ（Connectivity Type）] が **SSH**、**NETCONF**、**TELNET**、**HTTP**、**HTTPS**、**SNMPv3**、または **GRPC** の場合は必須です。
パスワード（**Password**）	前述の [ユーザー名（User Name）] のパスワード。	[接続タイプ（Connectivity Type）] が **SSH**、**NETCONF**、**TELNET**、**HTTP**、**HTTPS**、または **GRPC** の場合は必須です。
イネーブルパスワード（**Enable Password**）	イネーブルパスワードを使用します。有効な値は、**ENABLE**、**DISABLE**です。	
イネーブルパスワード値（**Enable Password Value**）	使用するイネーブルパスワードを指定します。	
SNMPV2 読み取りコミュニティ（**SNMPV2 Read Community**）	例：**readprivate**	[接続タイプ（Connectivity Type）] が **SNMPv2** の場合は必須です。
SNMPV2 書き込みコミュニティ（**SNMPV2 Write Community**）	例：**writeprivate**	
SNMPV3 ユーザー名（**SNMPV3 User Name**）	例：**DemoUser**	[接続タイプ（Connectivity Type）] が **SNMPv3** の場合は必須です。
SNMPV3 セキュリティレベル（**SNMPV3 Security Level**）	有効な値は、**noAuthNoPriv**、**AuthNoPriv**、または **AuthPriv** です。	[接続タイプ（Connectivity Type）] が **SNMPv3** の場合は必須です。
SNMPV3 認証タイプ（**SNMPV3 Auth Type**）	有効な値は **HMAC_MD5** または **HMAC_SHA** です。	[接続タイプ（Connectivity Type）] が **SNMPv3** で、[SNMPV3 セキュリティレベル（SnmpV3 Security Level）] が **AuthNoPriv** または **AuthPriv** の場合は必須です。
SNMPV3 認証パスワード（**SNMPV3 Auth Password**）	この認可タイプのパスワード。	[接続タイプ（Connectivity Type）] が **SNMPv3** で、[SNMPV3 セキュリティレベル（SnmpV3 Security Level）] が **AuthNoPriv** または **AuthPriv** の場合は必須です。

フィールド	エントリ	必須またはオプション
SNMPV3 プライバシータイプ（SNMPV3 Priv Type）	有効な値は **CFB_AES_128** または **CBC_DES_56** です。 AES192、AES256、3DES については、 SNMPv3 プライバシータイプはサポートされていません。	[接続タイプ（Connectivity Type）] が **SNMPv3** で、[SNMPV3 セキュリティレベル（SnmpV3 Security Level）] が **AuthPriv** の場合は必須です。
SNMPV3 プライバシーパスワード（SNMPV3 Priv Password）	この権限タイプのパスワード。	[接続タイプ（Connectivity Type）] が **SNMPv3** で、[SNMPV3 セキュリティレベル（SnmpV3 Security Level）] が **AuthPriv** の場合は必須です。

ファイルを保存する前にサンプルデータ行を必ず削除してください。削除しないと、必要なデータとともにインポートされます。インポート中は無視されるため、列ヘッダー行はそのままでかまいません。

c) 完了したら、新しい CSV ファイルを保存します。

ステップ 4 [参照（Browse）] をクリックし、作成した CSV ファイルに移動した後、[開く（Open）] をクリックして選択します。

ステップ 5 CSV ファイルを選択した状態で、[インポート（Import）] をクリックします。

インポートしたクレデンシャルプロファイルが [クレデンシャルプロファイル（Credential Profiles）] ウィンドウに表示されます。

クレデンシャルプロファイルの編集

クレデンシャルプロファイルは、複数のデバイスで（大規模なネットワーク内の何百台ものデバイスでも）共有できます。次の手順を実行し、クレデンシャルプロファイルの設定を変更します。

クレデンシャルプロファイルを編集する前に、変更するプロファイルの CSV バックアップをエクスポートすることをお勧めします（「クレデンシャルプロファイルのエクスポート （149 ページ）」を参照）。

ステップ 1 メインメニューから **[デバイス管理（Device Management）]** > **[クレデンシャル（Credential）]** を選択します。

ステップ 2 [クレデンシャルプロファイル（Credential Profiles）] ウィンドウの左側から、更新するプロファイルを選択し、  をクリックします。
選択したクレデンシャルの [プロファイルの編集（Edit Profile）] ウィンドウが表示されます。

ステップ 3 必要な変更を加えて、[保存（Save）] をクリックします。

クレデンシャルプロファイルのエクスポート

クレデンシャルプロファイルをエクスポートすると、選択したすべてのプロファイルが CSV ファイルに保存されます。これは、クレデンシャルプロファイルのバックアップコピーをすばやく作成する方法です。また、必要に応じて CSV ファイルを編集して再インポートし、新しいプロファイルを追加したり、クレデンシャルプロファイルのデータを変更したりすることもできます。

エクスポートしたクレデンシャルプロファイルの CSV ファイルに、実際のパスワードやコミュニティ文字列は含まれていません。エクスポートした CSV ファイルでは、クレデンシャルプロファイルのパスワードとコミュニティ文字列のエントリのすべての文字がアスタリスクに置き換えられます。エクスポートした CSV ファイルを変更してから再インポートする場合は、実際のパスワードとコミュニティ文字列の代わりにアスタリスクを使用することをお勧めします。インポート後、「クレデンシャルプロファイルの編集（148 ページ）」の手順に従って、アスタリスクを実際のパスワードとコミュニティ文字列に置き換えます。

ステップ 1 メインメニューから **[デバイス管理（Device Management）] > [クレデンシャルプロファイル（Credential Profiles）]** を選択します。

ステップ 2 （オプション）[クレデンシャルプロファイル（Credential Profiles）] ウィンドウで、必要に応じてクレデンシャルプロファイルのリストをフィルタ処理します。

ステップ 3 エクスポートするプロファイルのチェックボックスをオンにします。エクスポートするすべてのプロファイルを選択するには、列の上部にあるチェックボックスをオンにします。

ステップ 4 をクリックします。ブラウザによっては、CSV ファイルを保存するときに使用するパスとファイル名を選択するか、またはすぐに開くよう求められます。

クレデンシャルプロファイルの削除

クレデンシャルプロファイルを削除するには、次の手順を実行します。

（注） 1 つ以上のデバイスまたはプロバイダに関連付けられているクレデンシャルプロファイルは削除できません。

ステップ 1 削除するクレデンシャルプロファイルを含むバックアップ CSV ファイルをエクスポートします（「クレデンシャルプロファイルのエクスポート （149 ページ）」を参照）。

ステップ 2 削除するクレデンシャルプロファイルを使用しているデバイスまたはプロバイダーがあるかどうかを確認します。これは、[デバイス（Devices）] ウィンドウ（**[デバイス管理（Device Management）] > [クレデンシャルプロファイル（Credential Profiles）]** を選択）と [プロバイダ（Provider）] ウィンドウ（**[管理（Administration）] > [プロバイダアクセス管理（Manage Provider Access）]**）の両方で使用可能な [クレデンシャルプロファイル（Credential Profile）] 列でフィルタリングすることで実行できます。

ステップ 3 デバイスまたはプロバイダを別のクレデンシャルプロファイルに再割り当てします（このタスクのヘルプについては、「複数のデバイスのクレデンシャルプロファイルの変更 （150 ページ）」と「プロバイダの編集 （180 ページ）」を参照してください）。

ステップ 4 すべてのデバイスとプロバイダのクレデンシャルプロファイルを再割り当てした後、メインメニューから、**[デバイス管理（Device Management）]** > **[クレデンシャルプロファイル（Credential Profiles）]** を選択します。

ステップ 5 [クレデンシャルプロファイル（Credential Profiles）] ウィンドウで、削除するプロファイルを選択し、🗑をクリックします。

複数のデバイスのクレデンシャルプロファイルの変更

多数のネットワークデバイスのクレデンシャルプロファイルを変更する場合は、デバイスCSVファイルを編集して変更するほうが効率的です。基本的な方法は次のとおりです。

1. クレデンシャルプロファイルを変更するデバイスが含まれている CSV ファイルをエクスポートします（「CSV ファイルへのデバイス情報のエクスポート （199 ページ）」を参照）。
2. CSVファイルを編集し、各デバイスのクレデンシャルプロファイルを変更します（このクレデンシャルプロファイルはすでに存在している必要があります）。編集したファイルを保存します。

変更するクレデンシャルプロファイルがすでに存在していることを確認する必要があります。そのクレデンシャルプロファイルをまだ作成していない場合、CSV のインポートは失敗します。これらのデバイスに関連付けるクレデンシャルプロファイルには、オンボーディング時にこれらのデバイスに設定されたすべてのプロトコルの認証クレデンシャルも必要です。デバイスに設定された特定のプロトコルのクレデンシャルがクレデンシャルプロファイルに存在していないか、または正しくない場合、CSVインポートは成功しますが、これらのデバイスの到達可能性チェックは失敗します。

ステップ 1 メインメニューから **[デバイス管理（Device Management）]** > **[デバイス（Devices）]** を選択します。

ステップ 2 クレデンシャルプロファイルを変更するデバイスを選択します。選択できるオプションは、次のとおりです。

- ⎘をクリックしてすべてのデバイスを含めます。
- [検索（Search）] フィールドにテキストを入力するか、または特定の列をフィルタ処理して、デバイスリストをフィルタ処理します。次に、⎘をクリックし、フィルタ処理したデバイスのリストのみを含めます。
- 変更するデバイスレコードの横にあるチェックボックスをオンにします。次に、⎘をクリックし、オンにしたデバイスのみを含めます。

ステップ 3 任意のツールを使用して、新しい CSV ファイルを編集し、保存します。各デバイスの [クレデンシャルプロファイル（Credential Profile）] フィールドに正しいクレデンシャルプロファイル名を入力してください。

ステップ 4 をクリックします。

ステップ 5 [インポート（Import）] ダイアログボックスで [参照（Browse）] をクリックし、新しい CSV ファイルを参照して [インポート（Import）] をクリックします。

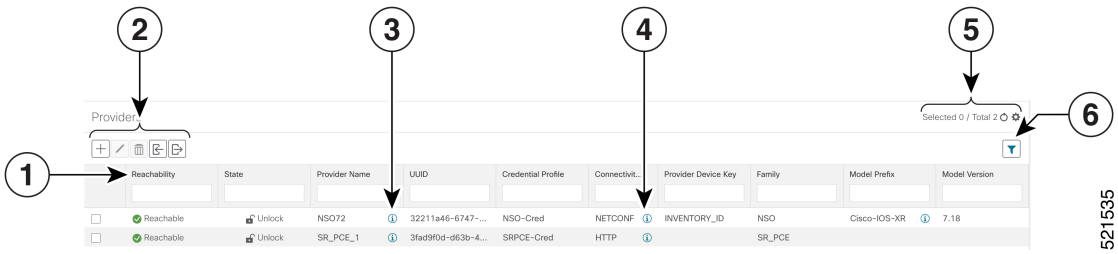
プロバイダの管理

Cisco Crosswork アプリケーションは、外部プロバイダと通信します。Cisco Crosswork はプロバイダ接続の詳細を保存し、その情報をアプリケーションで使用できるようにします。詳細については、「はじめる前に （1 ページ）」を参照してください。

[プロバイダ（Providers）] ウィンドウから、新しいプロバイダの追加、既存のプロバイダ設定の更新、および特定のプロバイダの削除を行うことができます。このウィンドウを開くには、**[管理（Administration）] > [プロバイダアクセスの管理（Manage Provider Access）]** を選択します。

（注） 一連の更新を実行する間にアプリケーションが応答するまで待機します。たとえば、プロバイダーの追加、削除、または再読み込みの間にしばらく待機します。これらのアクションの実行が速すぎると、トポロジサービスがこれらの変更を受信しない可能性があります。ただし、トポロジが同期していない場合は、トポロジサービスを再起動します。

図 *16 : [プロバイダ（Providers）] ウィンドウ*



項目	説明
1	この列のプロバイダの横に表示されるアイコンは、プロバイダの [到達可能性（Reachability）] を示します。デバイスの状態（Device State） （201 ページ）を参照してください。

項目	説明
2	をクリックして、プロバイダを追加します。「プロバイダの追加について （154 ページ）」を参照してください。
	をクリックして、選択したプロバイダの設定を編集します。「プロバイダの編集 （180 ページ）」を参照してください。
	をクリックして、選択したプロバイダを削除します。「プロバイダの削除 （181 ページ）」を参照してください。
	をクリックして、CSV ファイルから新しいプロバイダをインポートするか、または既存のプロバイダを更新します。このアイコンをクリックして、CSV ファイルテンプレートをダウンロードすることもできます。テンプレートには、独自の CSV ファイルを作成するためのガイドとして使用できるサンプルデータが含まれています。「プロバイダのインポート （178 ページ）」を参照してください。
	をクリックして、プロバイダを CSV ファイルにエクスポートします。「プロバイダのエクスポート （182 ページ）」を参照してください。
3	[プロバイダ名（Provider Name）] 列のプロバイダの横にある をクリックして、プロバイダのスタートアップ セッション キー/値のペアの詳細が表示された [対象のプロパティ（Properties for）] ポップアップウィンドウを開きます。
4	[接続タイプ（Connectivity Type）] 列のプロバイダの横にある をクリックして、プロバイダのプロトコル、IP、およびその他の接続情報が表示された [接続の詳細（Connectivity Details）] ポップアップウィンドウを開きます。
5	をクリックして、[プロバイダ（Providers）] ウィンドウを更新します。
	をクリックして、[プロバイダ（Providers）] ウィンドウに表示する列を選択します（参照）。
6	をクリックして、[プロバイダ（Providers）] ウィンドウの 1 つ以上の列にフィルタ条件を設定します。
	設定したフィルタ条件をクリアするには、[フィルタのクリア（Clear Filter）] リンクをクリックします。

プロバイダファミリについて

Cisco Crossworkは、さまざまなタイプまたはファミリのプロバイダをサポートしています。各プロバイダファミリは独自の組み合わせで特別なサービスを提供し、それぞれに固有の要件とオプションがあります。

次の表に、現在サポートされているプロバイダファミリを示します。

表 *8:* サポートされているプロバイダファミリ

プロバイダファミリ	説明
NSO	ネットワークデバイスの設定に使用する Cisco Network Services Orchestrator のインスタンス（Cisco NSO）。「Cisco NSO プロバイダの追加 （157 ページ）」を参照してください。
SR-PCE	Cisco Crossworkアプリケーションがネットワークと通信し、そのネットワークのセグメントルーティング情報を取得するのに必要な設定情報が含まれている Cisco セグメント ルーティング パス計算要素（Cisco SR-PCE） のインスタンス。「Cisco SR-PCE プロバイダの追加 （160 ページ）」を参照してください。
WAE	Cisco WAN Automation Engine（Cisco WAE）のインスタンスは、ネットワークの変化を評価するために使用する「What-If」分析を提供します。「Cisco WAE プロバイダの追加 （173 ページ）」を参照してください。
Syslog ストレージ	KPI と プレイブック によってデバイスから取得した syslog とその他のデータを保存するストレージサーバ（リモートまたはCisco Crossworkアプリケーション VM 自体）のインスタンス。「Syslog ストレージプロバイダの追加 （174 ページ）」を参照してください。
アラート	KPIモニタリング時に収集されたアラートの転送先となるプロバイダのインスタンス（Cisco Crosswork Situation Manager など）。アラートプロバイダの追加 （176 ページ）を参照してください
プロキシ	プロキシプロバイダーのインスタンス。プロキシプロバイダーを追加 （177 ページ）を参照してください

プロバイダの依存関係

この項では、各 Cisco Crosswork アプリケーションと Cisco Crosswork Network Controller に必要なプロバイダ設定について説明します。

Cisco Crosswork Network Controller は、Cisco Crosswork Active Topology と Cisco Crosswork Optimization Engine を組み合わせた統合ソリューションです。また、オプションで Crosswork Network Controller と Crosswork Change Automation、Crosswork Health Insights、Crosswork Zero Touch Provisioning を統合することもできます。

表 *9:* プロバイダ依存性マトリックス

Cisco Crosswork 製品	**Cisco NSO プロバイダ**	**Cisco SR-PCE プロバイダ**	**Cisco WAE プロバイダ**	**Syslog ストレージプロバイダ**	**アラートプロバイダー**
Crosswork Network Controller	必須 必要なプロトコルは HTTPS です プロバイダプロパティキーの **forward** は *true* に設定する必要があります。	必須 必要なプロトコルは HTTP です。	オプション	オプション	オプション
Crosswork 最適化エンジン	オプション	必須 必要なプロトコルは HTTP です。	オプション	オプション	オプション
Crosswork Change Automation Crosswork Health Insights	必須 必要なプロトコルは HTTPS です。 プロバイダプロパティキーの **forward** は *true* に設定する必要があります。	オプション	オプション	オプション	オプション
Crosswork ゼロタッチプロビジョニング	オプション	オプション	オプション	オプション	オプション

プロバイダの追加について

Cisco Crosswork は、さまざまな機能を実行するためにさまざまなプロバイダに依存しています。たとえば、Cisco Network Services Orchestrator はセグメント ルーティング ポリシーとデバイス情報を提供します。新しいプロバイダに依存する機能が将来追加される可能性があり、単一のプロバイダの複数のインスタンスと通信する必要がある場合があります。各プロバイダのサービスにアクセスするには、プロバイダを Cisco Crosswork アプリケーションのシステム設定に追加する必要があります。

プロバイダを追加するには、次の 2 つの方法があります。

1. **UI によるプロバイダの追加**：この方法については、「UI を使用したプロバイダの追加（155ページ）」を参照してください。この方法は最も時間がかかりますが、多数のプロバイダインスタンスを必要としない展開がほとんどであるため、多くの場合に使用されています。
2. **プロバイダ CSV ファイルからのプロバイダのインポート**：この方法については、「プロバイダのインポート（178ページ）」を参照してください。CSV ファイルのインポートは、一度に追加または更新するプロバイダインスタンスの数が多い場合に便利です。

どちらの方法でも、次が必要です。

- Cisco Crosswork アプリケーションがプロバイダにアクセスできるように、対応するクレデンシャルプロファイルを事前に作成します。ヘルプについては、「クレデンシャルプロファイルの作成（143 ページ）」を参照してください。
- プロバイダーとの接続に必要なプロトコル、IPアドレス、ポート番号、およびその他の情報を把握します。
- セッションの起動時にプロバイダが必要とする可能性がある特別なプロパティを把握しておきます。

UI を使用したプロバイダの追加

新しい外部プロバイダーを追加するには、次の手順を使用します。その後で、プロバイダをデバイスにマッピングできます。

ステップ 1 メインメニューから、**[管理（Administration）]>[プロバイダアクセスの管理（Manage Provider Access）]** を選択します。

ステップ 2 ＋ をクリックします。

ステップ 3 次の表に示すように、プロバイダーの値を入力します。

ステップ 4 すべての必須フィールドに入力が完了したら、[保存（Save）] をクリックして新しいプロバイダを追加します。

ステップ 5 （オプション）プロバイダをさらに追加するには、この手順を繰り返します。

表 *10 : [プロバイダの追加（Add Provider）]* フィールド（*=必須）

フィールド	説明
*** プロバイダ名（Provider Name）**	Cisco Crosswork アプリケーションで参照のために使用するプロバイダの名前。例：**`Linux_Server`**。名前には、最大 128 文字の英数字と、ドット（.）、アンダースコア（「_」）、またはハイフン（「-」）を含めることができます。その他の特殊文字は使用できません。

フィールド	説明
*** クレデンシャルプロファイル（Credential Profile）**	Cisco Crosswork アプリケーションがプロバイダへの接続に使用するクレデンシャルプロファイルの名前を選択します。
*** ファミリ（Family）**	プロバイダーファミリを選択します。選択肢は、**NSO**、**WAE**、**SR-PCE**、**ALERT**、および **SYSLOG_STORAGE** です。
接続タイプ（Connection Type）	
*** プロトコル（Protocol）**	Cisco Crosswork アプリケーションがプロバイダへの接続に使用する主要プロトコルを選択します。オプションには、**HTTP**、**HTTPS**、**SSH**、**SNMP**、**NETCONF**、**TELNET** などがあります。 このプロバイダの接続プロトコルをさらに追加するには、最初の行の最後にある ⊕ をクリックします。入力したプロトコルを削除するには、その行の横にある ⊗ をクリックします。 同じプロトコルを複数セットなど、必要な数の接続の詳細のセットを入力できます。
*** IP アドレス/サブネットマスク（IP Address/Subnet Mask）**	プロバイダのサーバーの IP アドレス（IPv4 または IPv6）とサブネットマスクを入力します。
*** ポート（Port）**	プロバイダのサーバーへの接続に使用するポート番号を入力します。これは、設定するプロトコルに対応するポートです。たとえば、プロバイダサーバーとの通信に使用するプロトコルが SSH の場合、ポート番号は通常 22 です。
タイムアウト（Timeout）	接続がタイムアウトするまで待機する時間を入力します（秒単位）。デフォルトは 30 秒です。
モデルのプレフィックス情報（Model Prefix Info）	
*** モデル（Model）**	Cisco NSO プロバイダを追加する場合にのみ必須：Cisco NSO で使用されている NED CLI に一致するモデルプレフィックスを選択します。有効な値は次のとおりです。 **Cisco-IOS-XR** **Cisco-NX-OS** **Cisco-IOS-XE** テレメトリでは、**Cisco-IOS-XR** のみがサポートされています。 この Cisco NSO プロバイダのモデルプレフィックス情報をさらに追加するには、[モデルプレフィックス情報（Model Prefix Info）] セクションの任意の行の末尾にある ⊕ をクリックします。入力したモデルプレフィックスを削除するには、その行の横にある ⊗ をクリックします。
*** バージョン（Version）**	Cisco NSO プロバイダを追加する場合にのみ必須：NSO サーバーで使用する Cisco NSO NED ドライバのバージョンを入力します。
プロバイダのプロパティ（Provider Properties）	

フィールド	説明
プロパティキー（**Property Key**）	設定する特別なプロバイダプロパティのキーの名前を入力します。 プロバイダプロパティは、Cisco Crosswork アプリケーションがプロバイダと連携する方法を制御します。すべてのプロバイダーが必要とするわけではなく、プロパティの数とタイプはプロバイダーファミリによって異なります。これらのプロパティについては、このガイドの特定のプロバイダの追加に関するトピックを参照してください。ただし、Cisco Crosswork アプリケーションはプロバイダのプロパティを検証しないことに注意してください。入力したプロパティがプロバイダに対して有効であることを確認します。 （注） 2 ネットワーク インターフェイス設定では、Cisco Crosswork アプリケーションはデフォルトで管理ネットワーク インターフェイス（**eth0**）を使用してプロバイダと通信します。この動作は、[プロパティキー（Proverty Key）] と [プロパティ値（Proverty Value）] をそれぞれ **outgoing-interface** と **eth1** として追加することで変更できます。この操作はほとんどの場合、管理インターフェイスが管理ネットワークではなく、データネットワークに存在することがあるため、SR-PCE プロバイダの作成時に必要になります。
プロパティ値（**Proverty Value**）	プロパティキーに割り当てる値を入力します。 このプロバイダの特別なプロパティをさらに追加するには、[プロバイダのプロパティ（Provider Properties）] セクションのキー/値ペアの末尾にある ⊕ をクリックします。入力したキー/値のペアを削除するには、そのペアの横に表示される ⊗ をクリックします。

Cisco NSO プロバイダの追加

Cisco Network Services Orchestrator（Cisco NSO）プロバイダは次の機能を提供します。

- Cisco Crosswork アプリケーションへのネットワークサービスとデバイス設定サービス。
- デバイス管理サービスと設定メンテナンスサービス。

（注） Crosswork は、Cisco NSO Layered Service Architecture（LSA）展開をサポートしています。LSA 展開は、すべてのサービスを含む顧客向けサービス（CFS）NSO として機能する複数の NSO プロバイダーと、デバイスを含むリソース向けサービス（RFS）から構成されます。Crosswork は、NSO プロバイダーを CFS または RFS として自動的に識別します。許可される CFS は 1 つだけです。[マネージャ プロバイダー アクセス（Manager Provider Access）] ページの [タイプ（Type）] 列は、NSO プロバイダーを CFS として識別します。

（注） Cisco NSO 機能パックのサンプルは、Cisco Crosswork Network Controller の VPN サービスプロビジョニング機能の出発点として提供されます。これらのサンプルは、一部の限定されたネットワーク設定では「そのまま」使用できますが、Cisco Crosswork Network Controller の拡張可能な設計を示すことを意図としています。一般的な質問への回答は Cisco Devnet で確認できます。シスコ カスタマー エクスペリエンスの担当者は、サンプルに関する一般的な質問への回答を提供できます。特定のユースケースに合わせたサンプルのカスタマイズについては、シスコアカウントチームを通じてサポートを提供いたします。

始める前に

必要な作業は次のとおりです。

- Cisco NSO プロバイダのクレデンシャルプロファイルを作成します（「クレデンシャルプロファイルの作成 （143 ページ）」を参照）。
- Cisco NSO プロバイダに割り当てる名前を確認します。
- トポロジで使用する Cisco NSO NED デバイスモデルとドライババージョンを確認します。

（注） `version` コマンドを使用して Cisco NSO のバージョンを検索できます。次に例を示します。

```
admin@ncs# show ncs-state version
ncs-state version 5.7.6
```

- Cisco NSO サーバーの IP アドレスとホスト名を確認します。NSO が HA で設定されている場合、IP アドレスは管理 VIP アドレスになります。
- Cisco NSO デバイスの設定を確認します。詳細については、「Cisco NSO デバイスの設定例 （191 ページ）」を参照してください。
- Cisco NSO LSA 展開を有効にするには、階層化されたサービスアーキテクチャ（LSA）を有効にする （362 ページ） の手順に従ってください。

UI から Cisco NSO プロバイダを追加するには、次の手順を実行します。すべてのプロバイダの詳細を含む CSV ファイルを作成して Crosswork にインポートすることで、複数のプロバイダを同時にインポートできることに注意してください（「プロバイダのインポート （178 ページ）」を参照）。

ステップ 1 メインメニューから、**[管理（Administration）]** > **[プロバイダアクセスの管理（Manage Provider Access）]** を選択します。

ステップ 2 ＋をクリックします。

ステップ 3 Cisco NSO プロバイダのフィールドに次の値を入力します。

a) 必須フィールド：

- [プロバイダ名（Provider Name）]：プロバイダの名前を入力します。
- [クレデンシャルプロファイル（Credential Profile）]：以前に作成した Cisco NSO のクレデンシャルプロファイルを選択します。
- [ファミリ（Family）]：[NSO] を選択します。
- [接続タイプ（Connection Type(s)）] の [プロトコル（Protocol）] で、Cisco Crosswork アプリケーションがプロバイダへの接続に使用するプロトコルを選択します。 通常は **HTTPS** が優先されます。詳細については、「プロバイダの依存関係 （153 ページ）」を参照してください。
- [IP アドレス/サブネットマスク（IP Address/Subnet Mask）]：Cisco NSO サーバーの IP アドレスサブネットマスクを入力します。
- [ポート（Port）]：HTTPS の場合、HTTPS を使用して NSO にアクセスするには、etc/ncs/ncs.conf で NSO VM の設定と一致するポートを入力します。NSO ではデフォルトポートとして 8888 を使用します。
- [モデル（Model）]：ドロップダウンリストからモデル（[Cisco-IOS-XR]、[Cisco-NX-OS]、または [Cisco-IOS-XE]）を選択し、関連付けられている NED ドライババージョンを入力します。トポロジで使用するデバイスのタイプごとにモデルを追加します。複数ある場合は、サポートされている別のモデルを追加します。
- [バージョン（Version）]：NSO のデバイスモデルにインストールされている NED ソフトウェアバージョンを入力します。

b) オプション値：

- [タイムアウト（Timeout）]：Cisco NSO サーバーへの接続がタイムアウトするまでの待機時間（秒単位）。デフォルトは 30 秒です。

ステップ 4 [プロバイダプロパティ（Provider Properties）] で、[プロパティキー（Property Key）] に **forward**、[プロパティ値（Property Value）] に **true** と入力します。このプロパティは、Cisco Crosswork ネットワークコントローラ ソリューションを使用して UI 内でプロビジョニング操作をできるようにし、Crosswork API ゲートウェイを介して NSO へのノースバウンド インターフェイスを有効にする場合に必要です。

（注） Cisco Crosswork には、NSO アプリケーションを Crosswork UI から相互起動するオプションがあります（この機能は、読み取り専用権限を持つユーザーロールでは使用できません）。相互起動機能を有効にするには、次のいずれかの設定で Cisco NSO をプロバイダとして追加します。

- **Property Key nso_crosslaunch_url** では、[プロパティーキー（Property Key）] フィールドに有効な URL が入力されています。
- プロトコルは **HTTP** か **HTTPS** で、プロバイダは到達可能です。

上記の設定のいずれかが存在する場合、相互起動アイコン（ ）が [プロバイダ名（Provider Name）]列に表示されます。または、ウィンドウの右上隅にある起動アイコンを使用して、NSO アプリケーションを相互起動することができます。

ステップ 5 すべての必須フィールドに入力したら、[保存（Save）] をクリックしてプロバイダとして Cisco NSO を追加します。

ステップ 6 [プロバイダー（Providers）] ウィンドウで、作成した NSO プロバイダーを選択し、**[アクション（Actions）]> [ポリシーの詳細の編集（Edit Policy Details）]** をクリックします。

選択した NSO プロバイダーの [ポリシーの詳細の編集（Edit Policy Details）] ウィンドウが表示されます。

ステップ 7 環境の要件に合わせて構成フィールドを編集します。[保存（Save）] をクリックして変更を保存します。

Cisco SR-PCE プロバイダの追加

Cisco セグメント ルーティング パス計算要素（Cisco SR-PCE）プロバイダは、デバイス検出、管理、設定メンテナンス、およびルート計算サービスを Cisco Crosswork アプリケーションに提供します。SR ポリシー、レイヤ 3 リンク、およびデバイスを学習および検出するには、少なくとも 1 つの SR-PCE プロバイダが必要です。2 番目の SR-PCE をバックアップとして設定するオプションがあります。 が複数のドメインの管理をサポートしていないため、両方の SR-PCE デバイスを同じネットワークに接続する必要があります。

（注） 管理ドメインの SDN コントローラとして SR-PCE への Cisco Crosswork アプリケーションアクセスを有効にするには、SR-PCE をプロバイダとして追加する必要があります。

Cisco SR-PCE の 1 つ以上のインスタンスを（UI を介して）プロバイダとしての追加するには、次の手順を実行します。

始める前に

必要な作業は次のとおりです。

- SR-PCE として機能するようにデバイスを設定します。特定のデバイスプラットフォームの SR 設定ドキュメントを参照して、SR を有効にし（IS-IS または OSPF プロトコルの場合）、SR-PCE を設定します（例：*Cisco NCS 540* シリーズ ルータのセグメントルーティング設定ガイド）。
- Cisco SR-PCE プロバイダのクレデンシャルプロファイルを作成します（「クレデンシャルプロファイルの作成 （143 ページ）」を参照）。これは、基本的な HTTP テキスト認証クレデンシャルである必要があります（現在、MD5 認証はサポートされていません）。追加する Cisco SR-PCE サーバーが認証を必要としない場合でも、プロバイダのクレデンシャルプロファイルを指定する必要がありますが、HTTP プロトコルを使用しない任意のプロファイルを指定できます。
- Cisco SR-PCE プロバイダに割り当てる名前を確認します。通常、これは Cisco SR-PCE サーバーの DNS ホスト名です。
- Cisco SR-PCE サーバーの IP アドレスを確認します。

- Cisco SR-PCE と Cisco Crosswork アプリケーションサーバー間の通信に使用するインターフェイスを確認します。
- Cisco SR-PCE が検出するデバイスを自動でオンボーディングするかどうか、また、その場合は新しいデバイスの追加時にその管理ステータスを [オフ（off）]、[管理対象（managed）]、または[管理対象外（unmanaged）] にするかどうかを決定します。
- Cisco SR-PCE プロバイダが検出する自動オンボーディングデバイスを予定し、それらをデータベースに追加するときに管理対象の状態に設定する場合は、次の手順を実行します。
  - 新しい管理対象デバイスとの通信用に既存のクレデンシャルプロファイルを割り当てます。
  - クレデンシャルプロファイルは、SNMP プロトコルを使用して設定する必要があります。
- 高可用性を実現するには、一意の名前と IP アドレスを使用し、設定が一致する 2 つの個別の Cisco SR-PCE プロバイダを設定します

ステップ 1 メインメニューから、**[管理（Administration）]**>**[プロバイダアクセスの管理（Manage Provider Access）]** を選択します。

ステップ 2 ＋ をクリックします。

ステップ 3 SR-PCE プロバイダのフィールドに次の値を入力します。

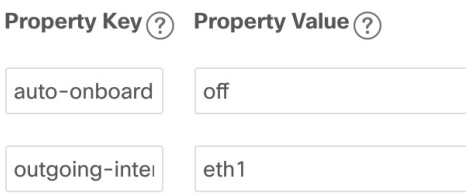
a) 必須フィールド：

- [プロバイダ名（Provider Name）]：SR-PCE プロバイダの名前。
- [クレデンシャルプロファイル（Credential Profile）]：以前に作成した Cisco SR-PCE のクレデンシャルプロファイルを選択します。
- [ファミリ（Family）]：[SR_PCE] を選択します。他のすべてのオプションは無視する必要があります。
- [プロトコル（Protocol）]：[HTTP] を選択します。
- [IP アドレス/サブネットマスク（IP Address/Subnet Mask）]：サーバーの IP アドレス（IPv4 または IPv6）とサブネットマスクを入力します。
- [ポート（Port）]：ポート番号として **8080** を入力します。
- [プロバイダプロパティ（Provider Properties）]：最初のフィールドセットに、次のキー/値ペアのいずれかを入力します。

プロパティキー	値
auto-onboard	**off** （注） すべてのネットワークデバイスを手動で（UI または CSV インポート経由で）入力する場合は、このオプションを使用します。 デバイスが検出されると、デバイスデータは Cisco SR-PCE データベースに記録されますが、Cisco Crosswork インベントリ管理データベースには登録されません。
auto-onboard	**unmanaged** このオプションを有効にすると、Cisco Crosswork が検出するすべてのデバイスが Cisco Crosswork インベントリ管理データベースに登録され、設定済みの状態が **unmanaged** に設定されます。これらのデバイスの SNMP ポーリングが無効になり、管理 IP 情報は含められません。これらのデバイスを後で **managed** の状態にするには、UI を使用してデバイスを編集するか、CSV にエクスポートして変更を加え、更新した CSV をインポートする必要があります。インポート前にデバイス CSV ファイルに追加することによって、クレデンシャルプロファイルを割り当てることもできます（クレデンシャルプロファイルはすでに存在している必要があります）。
auto-onboard	**managed** このオプションは、IPv4 展開でのみ使用できます。このオプションを有効にすると、Cisco SR-PCE が検出するすべてのデバイスが Cisco Crosswork インベントリ管理データベースに登録され、設定済みの状態が **managed** に設定されます。これらのデバイスに対して SNMP ポーリングが有効になり、Cisco SR-PCE は管理 IP アドレス（ルータ ID）も報告します。デバイスは、SR-PCE プロバイダ設定のデバイスプロファイルキーに関連付けられたクレデンシャルプロファイルを使用して追加されます。 （注） IPv6 展開でこのオプションを有効にしても、デバイスはインベントリに [管理対象外（unmanaged）] として登録されます。

プロパティキー	値
device-profile	すべての新しいデバイスの SNMP クレデンシャルが含まれているクレデンシャルプロファイルの名前。 （注） このフィールドは、**auto-onboard** が **managed** または **unmanaged** に設定されている場合にのみ必要です。
outgoing-interface	**eth1** （注） 2 つの NIC 設定を使用する場合に、データ ネットワーク インターフェイスを介して Cisco Crosswork アプリケーションが SR-PCE にアクセスできるようにする場合にのみ、これを設定する必要があります。
topology	**off** または **on**。 これはオプションのプロパティです。指定しない場合、デフォルト値は **on** です。 値を **off** に指定している場合は、SR-PCE プロバイダが L3 トポロジにアクセスできないことを意味します。
pce	**off** または **on**。 これはオプションのプロパティです。指定しない場合、デフォルト値は **on** です。 値を **off** に指定している場合は、SR-PCE プロバイダが LSP とポリシーにアクセスできないことを意味します。

図 *17*: プロバイダープロパティのキーと値の例



（注） [管理対象（managed）] または [管理対象外（unmanaged）] のオプションが設定されていて、後でデバイスを削除する場合は、次のいずれかを実行する必要があります。

- Cisco Crosswork からデバイスを削除する前に、ネットワークからデバイスを再設定して削除します。これにより、Cisco Crosswork がデバイスを再検出して追加しないようにします。
- auto-onboard を **off** に設定してから、デバイスを Cisco Crosswork から削除します。ただし、これを行うと、Cisco Crosswork はネットワーク内の新しいデバイスを検出または自動オンボーディングできなくなります。

b) オプション値：

- [タイムアウト（Timeout）]：SR-PCE サーバーへの接続がタイムアウトするまでの待機時間（秒単位）。デフォルトは 30 秒です。

ステップ 4 すべての必須フィールドに入力したら、[保存（Save）] をクリックして SR-PCE プロバイダを追加します。

ステップ 5 SR-PCE プロバイダにエラーのない緑色の到達可能性ステータスが表示されていることを確認します。[イベント（Events）] ウィンドウ（**[管理（Administration）]** > **[イベント（Events）]**）を表示して、プロバイダが正しく設定されているかどうかを確認することもできます。

ステップ 6 SR-PCE プロバイダごとにこのプロセスを繰り返します。

（注） 一度設定した自動オンボーディングオプションを変更することは推奨されません。これらを変更する必要がある場合は、次の手順を実行します。

1. プロバイダを削除し、[イベント（Events）] ウィンドウに削除の確認が表示されるまで待ちます。
2. 更新した自動オンボーディングオプションでプロバイダを再追加します。
3. [イベント（Events）] ウィンドウで、正しい自動オンボーディングオプションを使用してプロバイダが追加されたことを確認します。

次のタスク

- **`auto-onboard`/`off`** ペアの場合は、**[デバイス管理（Device Management）]** > **[ネットワークデバイス（ Network Devices）]** に移動してデバイスを追加します。
- 自動的にデバイスをオンボーディングする選択をした場合は、**[デバイス管理（Device Management）]** > **[ネットワークデバイス（Network Devices）]** に移動してデバイスリストを表示します。地理的な場所の詳細などのノード情報の詳細を追加するには、デバイスリスト（.csv）をエクスポートし、更新してからインポートします。地理的な場所データが欠落している場合は、論理マップを使用してのみデバイストポロジを表示できます。

Cisco SR-PCE の到達可能性の問題

到達可能性の問題は、[イベント（Events）]テーブルで確認でき、到達可能性ステータスは[プロバイダ（Providers）]ウィンドウで確認できます（「プロバイダの詳細の取得（179ページ）」を参照）。SR-PCE がダウンした場合、SR-PCE は通知の更新を送信できないため、トポロジ内のすべてのリンクは既知であった最後の状態で表示されます。SR-PCE が再度到達可能になると、SR-PCE が再接続され、それに応じてトポロジが更新されることを示すメッセージが[イベント（Events）]テーブル（）に表示されます。SR-PCE が長時間ダウンし、同期されておらず、更新が行われていないことに気づいた場合は、次の UI を使用して SR-PCE を削除し、（接続が戻ったら）もう一度追加します。

1. makecall ディレクトリで、次のコマンドを実行します。

   ```
   # process restart pce_server
   ```

2. UI で、**[管理（Administration）]>[プロバイダアクセスの管理（Manage Provider Access）]** に移動し、SR-PCE プロバイダを削除してから、もう一度追加します。

次の手順を実行して、到達可能性をトラブルシューティングすることもできます。

ステップ 1 デバイスのクレデンシャルを確認します。

ステップ 2 プロバイダホストに ping を実行します。

ステップ 3 プロバイダの接続設定で指定されたプロトコルを使用して接続を試行します。SR-PCE プロバイダの場合、通常は HTTP でポート 8080 です。

ステップ 4 ファイアウォール設定とネットワーク設定を確認します。

ステップ 5 接続できるユーザーを制限する可能性のあるアクセスコントロールリストの設定については、Cisco SR-PCE のホストまたは介入デバイスを確認します。

複数の Cisco SR-PCE HA ペア

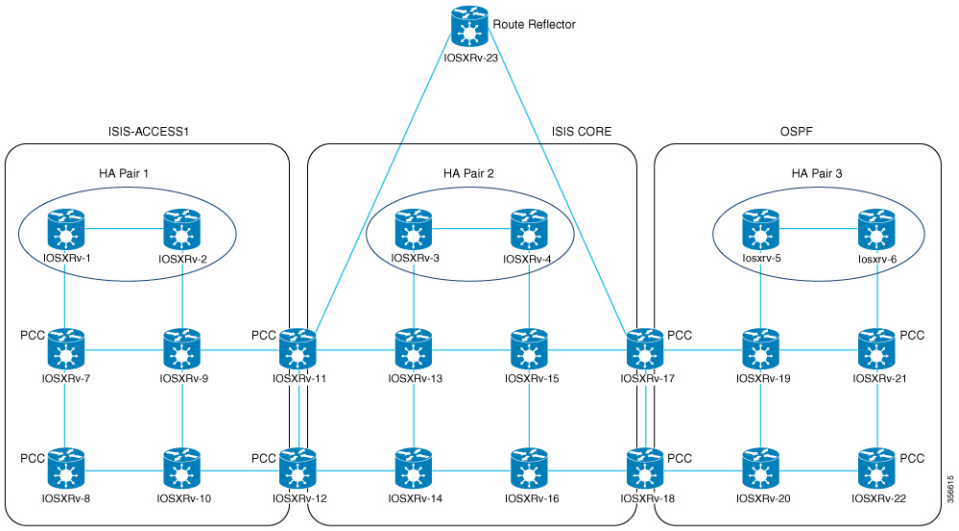
高可用性（HA）を確保するために、最大 8 つの Cisco SR-PCE HA ペア（合計 16 の SR-PCE）を設定できます。Cisco SR-PCE プロバイダの各 HA ペアには、同じネットワークトポロジをサポートしている一致する設定が必要です。HA では、プライマリ SR-PCE が到達不能になった場合に、Cisco Crosswork 最適化エンジンはセカンダリ SR-PCE を使用してネットワークトポロジを検出します。このペアが失敗すると、次の HA ペアが引き継ぎます。ネットワークトポロジは引き続き正しく更新され、[イベント（Events）] テーブル（）で SR-PCE 接続イベントを表示できます。

複数の HA ペア

複数の SR-PCE HA ペアの場合、各 SR-PCE ペアは同じトポロジを認識しますが、パス計算クライアント（PCC）から作成されたトンネルを管理し、それらのみを認識します。次の図に、3 つの SR-PCE HA ペアトポロジの例を示します。次の点に注意してください。

- HA ペア 1：PCE iosxrv-1 と iosxrv-2 は、ヘッドエンドが iosxrv-7 と iosxrv-8 であるトンネルのみをプロビジョニングおよび検出します。iosxrv-9 と iosxrv-10 は PCC ルータではないことに注意してください。
- HA ペア 2：PCE iosxrv-3 と iosxrv-4 は、ヘッドエンドが iosxrv-11、iosxrv-12、iosxrv-17、および iosxrv-18 であるトンネルのみをプロビジョニングおよび検出します。iosxrv-13、iosxrv-14、iosxrv-15、および iosxrv-16 は PCC ルータではないことに注意してください。
- HA ペア 3：PCE iosxrv-5 と iosxrv-6 は、ヘッドエンドが iosxrv-21 と iosxrv-22 であるトンネルについてのみプロビジョニングおよび検出します。iosxrv-19 と iosxrv-20 は PCC ルータではないことに注意してください。

図 *18 : HA* ペアが *3* つの場合のトポロジの例



（注） いずれかの SR-PCE がメインネットワークトポロジのサブセットに含まれている場合、その SR-PCE プロバイダは、[プロパティキー（Property Key）] を **topology**、[プロパティ値（Property Value）] を **off** として追加する必要があります。この値が設定されている場合、この SR-PCE はトポロジの学習に使用されません。

HA の設定

HA Cisco SR-PCE プロバイダの各ペアを Cisco Crosswork 最適化エンジン に追加するには、次の設定を行う必要があります。

（注） HA を有効にするには、両方の SR-PCE 間に復元力のある IPv4 接続が必要です。他の SR-PCE の PCE IP アドレスは、常にピアから到達可能である必要があります。

Cisco SR-PCE デバイスのそれぞれで次のコマンドを発行します。

インターフェイスを有効にします。

```
# interface <interface><slot>/<port>
ipv4 address <sync-link-interface-ip-address> <subnet-mask>
no shut
```

HA を有効にします。

```
# pce rest sibling ipv4 <other-node-pce-address>
```

2 つの SR-PCE 間に同期リンクを確立します。

```
# router static
address-family ipv4 unicast
<other-node-pce-ip-address>/<subnet-mask-length> <remote-sync-link-ip-address>
```

（オプション）`# pce segment-routing traffic-eng peer ipv4 <other-node-pce-ip-address>`

他の PCE ノードではなく、PCC ごとに入力する必要があります。

PCC で次のコマンドを発行します。

SR ポリシーの場合：`# segment-routing traffic-eng pcc redundancy pcc-centric`

RSVP-TE トンネルの場合：`# mpls traffic-eng pce stateful-client redundancy pcc-centric`

兄弟 SR-PCE 設定の確認

SR-PCE から `show tcp brief` コマンドを入力して、HA 内の SR-PCE 間の同期が完全であることを確認します。

```
#show tcp brief | include <remote-SR-PCE-router-id>
```

次の情報が正しいことを確認します。

ローカル アドレス	外部アドレス	状態
<local-SR-PCE-router-id>:8080	*<remote-SR-PCE-router-id>*:*<any-port-id>*	ESTAB
<local-SR-PCE-router-id>:*<any-port-id>*	*<remote-SR-PCE-router-id>*:8080	ESTAB

次に例を示します。

```
RP/0/0/CPU0:iosxrv-1#sh tcp brief | i 192.168.0.2:
Mon Jun 22 18:43:09.044 UTC
0x153af340 0x60000000 0 0 192.168.0.1:47230 192.168.0.2:8080 ESTAB
0x153aaa6c 0x60000000 0 0 192.168.0.1:8080 192.168.0.2:16765 ESTAB
```

この例では、192.168.0.2 がリモート SR-PCE IPです。

SR-PCE 委任

SR-TE ポリシーが作成される場所に応じて、次の SR-PCE 委任が行われます。

- SR-PCE で開始：PCE に設定されたポリシー。SR-TE ポリシーの委任は、送信元 SR-PCE に戻されます。

（注）
- ポリシーは、UI を使用して作成された場合でも PCE で開始できますが、その場合は SR-PCE には明示的に設定されません。
- PCE で RSVP-TE トンネルを直接設定することはできません。

- PCC で開始：デバイスに直接設定された SR-TE ポリシーまたは RSVP-TE トンネル。最も低い優先順位で設定された SR-PCE は、委任された SR-PCE です。優先順位が設定されていない場合、最小の PCE IP アドレスを持つ SR-PCE が委任 SR-PCE になります。次の設定例では、**10.0.0.1** に優先順位値 10 が割り当てられており、これが委任 SR-PCE になることを示しています。

```
segment-routing
  traffic-eng
    pcc
      source-address ipv4 10.0.0.2
      pce address ipv4 10.0.0.1
        precedence 10
       !
      pce address ipv4 10.0.0.8
        precedence 20
       !
       report-all
       redundancy pcc-centric
```

RSVP-TE トンネルの場合：

```
mpls traffic-eng
interface GigabitEthernet0/0/0/0
!
interface GigabitEthernet0/0/0/1
!
interface GigabitEthernet0/0/0/2
!
pce
  peer source ipv4 192.168.0.02
  peer ipv4 192.168.0.9
    precedence 10
  !
  peer ipv4 192.168.0.10
    precedence 20
  !
  stateful-client
   instantiation
   report
   redundancy pcc-centric
   autoroute-announce
  !
!
auto-tunnel pcc
  tunnel-id min 1000 max 5000
```

- Cisco Crosswork SR-PCE で開始：Cisco Crosswork を使用して設定された SR-TE ポリシー。SR-PCE 委任はポリシーごとにランダムです。

（注） Cisco Crosswork 最適化エンジン で変更または削除できるのは、Cisco Crosswork 最適化エンジン によって作成された SR-TE ポリシーまたは RSVP-TE トンネルのみです。

HA の注意事項と制限事項

- すべての PCC が両方の SR-PCE に接続された PCEP であると想定されます。
- SR-PCE が Cisco Crosswork からのみ切断されると、次のようになります。
  - SR-PCE 委任の割り当ては残りますが、切断された SR-PCE は Cisco Crosswork に表示されません。
  - 切断された SR-PCE が委任 PCE の場合、Cisco Crosswork SR-PCE で開始した SR-TE ポリシーを変更することはできません。
- 場合によっては、UI を介して作成した SR-TE ポリシーが Cisco Crosswork Optimization Engineから自動的に削除された場合（意図的であり、予期していた場合）、警告メッセージが表示されません。たとえば、送信元 PCC がリロードされると、UI で作成した SR ポリシーは表示されず、ユーザーには通知されません。
- 1 つの SR-PCE が Cisco Crosswork 最適化エンジン へのアップリンクを除くすべてのリンク（PCC/トポロジデバイスへの）で失敗する極端な場合、Cisco Crosswork 最適化エンジンでトポロジ情報が正確でなくなります。この場合は、接続の問題を修正するか、または [プロバイダ（Provider）]ページから両方の SR-PCE を削除し、到達可能な方をもう一度追加します。

SR-PCE 設定例

次に、HA の場合の複数SR-PCE設定を行うのに役立つ例を示します。適宜変更してください。

冗長 SR-PCE の設定例（Cisco IOS-XR 7.x.x を使用する PCE ）

```
pce
 address ipv4 192.168.0.7
 state-sync ipv4 192.168.0.6
 api
  sibling ipv4 192.168.0.6
```

冗長 SR-PCE の設定例（PCC）

```
segment-routing
 traffic-eng
  pcc
   source-address ipv4 192.0.2.1
   pce address ipv4 192.0.2.6
    precedence 200
   !
   pce address ipv4 192.0.2.7
    precedence 100
   !
```

```
   report-all
   redundancy pcc-centric
```

RSVP-TE の場合の冗長 SR-PCE 設定例（PCC 上）

（注） `Loopback0` は TE ルータ ID を表します。

```
ipv4 unnumbered mpls traffic-eng Loopback0
!
mpls traffic-eng
 pce
  peer source ipv4 209.165.255.1
  peer ipv4 209.165.0.6
   precedence 200
  !
  peer ipv4 209.165.0.7
   precedence 100
  !
  stateful-client
   instantiation
   report
   redundancy pcc-centric
   autoroute-announce
  !
 !
 auto-tunnel pcc
  tunnel-id min 1000 max 1999
 !
!
```

SR-TM の設定例

```
telemetry model-driven
 destination-group crosswork
  address-family ipv4 198.18.1.219 port 9010
   encoding self-describing-gpb
   protocol tcp
  !
 !
 sensor-group SRTM
  sensor-path Cisco-IOS-XR-infra-tc-oper:traffic-collector/afs/af/counters/tunnels
  sensor-path
Cisco-IOS-XR-infra-tc-oper:traffic-collector/vrf-table/default-vrf/afs/af/counters/prefixes

 !
 subscription OE
  sensor-group-id SRTM sample-interval 60000
  destination-id crosswork
  source-interface Loopback0
!
traffic-collector
 interface GigabitEthernet0/0/0/3
 !
 statistics
  history-size 10
```

（注） 接続先アドレスは、Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） VM のサウスバウンド データ インターフェイス（eth1）アドレスを使用します。

プレフィックスとトンネルのカウンタを取得するには、NSO を介してテレメトリ設定でセンサーパスをプッシュする必要があります。トラフィックコレクタがすべてのトラフィック入力インターフェイスで設定されていることを前提としています。この設定は、オンデマンド帯域幅と帯域幅最適化の機能パックを動作させる要求を満たすために必要です。

テレメトリセンサーパス

```
sensor-path Cisco-IOS-XR-infra-tc-oper:traffic-collector/afs/af/counters/tunnels/tunnel
sensor-path
Cisco-IOS-XR-infra-tc-oper:traffic-collector/vrf-table/default-vrf/afs/af/counters/prefixes/prefix
```

NSO 経由ですべてのヘッドエンドルータに Cisco Crosswork 最適化エンジン がプッシュするテレメトリ設定

```
telemetry model-driven
  destination-group CW_43dc8a5ea99529715899b4f5218408a785e40fce
    vrf default
    address-family ipv4 172. 19.68.206 port 31500
      encoding self-describing-gpb
      protocol top
    !
  !
destination-group CW_4b3c69a200668b0a8dc155caff295645c684a8f8
  vrf default
  address-family ipv4 172. 19.68.206 port 31500
    encoding self-describing-gpb
    protocol top
  !
!
sensor-group CW_43dc8a5ea99529715899b4f5218408a785e40fce
  sensor-path Cisco-IOS-XR-infra-tc-oper:traffic-collector/afs/af/counters/tunnels/tunnel
!
sensor-group CW_4b3c69a200668b0a8dc155caff295645c684a8f8
  sensor-path
Cisco-IOS-XR-infra-tc-oper:traffic-collector/vrf-table/default-vrf/afs/af/counters/prefixes/prefix
!
subscription CW_43dc8a5ea99529715899b4f5218408a785e40fce
  sensor-group-id CW_43dc8a5ea99529715899b4f5218408a785e40fce sample-interval 300000
  destination-id CW_43dc8a5ea99529715899b4f5218408a785e40fce
!
subscription CW_4b3c69a200668b0a8dc155caff295645c684a8f8
  sensor-group-id CW_4b3c69a200668b%a8dc155caff295645c684a8f8 sample-interval 300000
  destination-id CW_463c69a200668b0a8dc155caff295645c684a8f8
  !
!
```

トラフィックコレクタの設定（トラフィックコレクタ下に追加するすべての入力トラフィックインターフェイス）

```
RP/0/RSP0/CPU0:PE1-ASR9k#sh running-config traffic-collector
Fri May 22 01:14:35.845 PDT
traffic-collector
  interface GigabitEthernet0/0/0/0
  !
```

```
  statistics
    history-size 1
    collection-interval 1
    history-timeout 1
    history-minute-timeout
  !
!
```

すべてのプレフィックスでの BGP neighbor next-hop-self の追加（TM レートカウンタを表示）。

```
bgp router-id 5.5.5.5
address-family ipv4 unicast
  network 5.5.5.5/32
  redistribute static
!
address-family link-state link-state
!
neighbor 1.1.1.1
  remote-as 65000
  update-source Loopback0
  address-family ipv4 unicast
   next-hop-self
  !
!
```

トラフィック コレクタ トンネルとプレフィックスカウンタ

```
RP/0/RSP0/CPU0:PE1-ASR9k#show traffic-collector ipv4 counters prefix
Fri May 22 01:13:51.458 PDT
Prefix              Label         Base rate         TM rate        State
                                  (Bytes/sec)       (Bytes/sec)
------------------  ------------  ---------------  --------------  -----------------
1.1.1.1/32          650001         3                0              Active
2.2.2.2/32          650002         3                0              Active
3.3.3.3/32          650003         6                0              Active
4.4.4.4/32          650004         1                0              Active
6.6.6.6/32          650200         6326338          6326234        Active
7.7.7.7/32          650007         62763285         62764006       Active
8.8.8.8/32          650008         31129168         31130488       Active
9.9.9.9/32          650009         1                0              Active
10.10.10.10/32      650010         1                0              Active
RP/0/RSP0/CPU0:PE1-ASR9k#stt
RP/0/RSP0/CPU0:PE1-ASR9k#show traffic-collector ipv4 counters tunnel
Fri May 22 01:13:52.169 PDT
RP/0/RSP0/CPU0:PE1-ASR9k#]
```

パス計算クライアント（PCC）サポート

PCC は、SR-PCE への RSVP-TE トンネルと SR ポリシーの両方の委任とレポートをサポートできます。両方を同じ PCC でサポートするには、SR-PCE との 2 つの個別の PCEP 接続を確立する必要があります。各 PCEP 接続には、PCC の個別の送信元 IP アドレス（ループバック）が必要です。

次に、RSVP-TE の場合の PCEP 接続の Cisco IOS-XR 設定例を示します。192.168.0.2 は、SR-PCE に委任され、報告される RSVP-TE トンネルの PCEP セッション送信元 IP です。これは、ルータ上のループバックアドレスです。PCEP セッション用に 2 つの SR-PCE が設定されます。1 つ目は優先順位による RSVP-TE トンネルの委任に優先されます。自動トンネル PCC は、Cisco Crosswork 最適化エンジン で作成されたような PCE によって開始された RSVP-TE トンネルへの割り当てに使用されるトンネル ID の範囲で設定されます。

```
mpls traffic-eng
interface GigabitEthernet0/0/0/2
admin-weight 1
!
interface GigabitEthernet0/0/0/3
admin-weight 1
  pce
    peer source ipv4 192.168.0.2
    peer ipv4 192.168.0.1
      precedence 10
     !
    peer ipv4 192.168.0.8
      precedence 11
     !
    stateful-client
      instantiation
      report
     !
   !
   auto-tunnel pcc
    tunnel-id min 10 max 1000
   !
!
ipv4 unnumbered mpls traffic-eng Loopback0

rsvp
interface GigabitEthernet0/0/0/2
bandwidth 1000000
!
interface GigabitEthernet0/0/0/3
bandwidth 1000000
!
!
```

Cisco WAE プロバイダの追加

Cisco WAN Automation Engine（Cisco WAE）プロバイダは、Cisco Crosswork アプリケーションにトラフィックとトポロジ分析を提供します。基盤となるソフトウェアは Cisco WAE Planning であり、トラフィック、トポロジ、および機器の状態の広範囲に及ぶビューを提供します。障害の影響の「What-If」分析を実行する予測モデルを利用します。

UI を使用しての 1 つ以上の Cisco WAE のインスタンスをプロバイダとして追加するには、次の手順を実行します。CSV ファイルを使用してプロバイダを追加することもできます（「プロバイダのインポート （178 ページ）」を参照）。

始める前に

必要な作業は次のとおりです。

- Cisco WAE プロバイダのクレデンシャルプロファイルを作成します（「クレデンシャルプロファイルの作成 （143 ページ）」を参照）。これは基本的な HTTP/HTTPS テキスト認証クレデンシャルである必要があります（現在、MD5 認証はサポートされていません）。追加する Cisco WAE サーバーが認証を必要としない場合でも、プロバイダのクレデンシャルプロファイルを指定する必要がありますが、HTTP/HTTPS プロトコルを使用しないプロファイルを指定できます。

- プロバイダーに割り当てる名前を確認します。通常、これは Cisco WAE サーバーの DNS ホスト名です。
- Cisco WAE サーバーの IP アドレスとポートを確認します。接続プロトコルは HTTP または HTTPS になります。

ステップ 1 メインメニューから、**[管理（Administration）]** > **[プロバイダアクセスの管理（Manage Provider Access）]** を選択します。

ステップ 2 ＋をクリックします。

ステップ 3 プロバイダのフィールドに次の値を入力します。

a) 必須フィールド：

- [プロバイダ名（Provider Name）]：Cisco WAE プロバイダの名前。
- [クレデンシャルプロファイル（Credential Profile）]：以前に作成したクレデンシャルプロファイルを選択します。
- [ファミリ（Family）]：[WAE] を選択します。
- [プロトコル（Protocol）]：使用しているクレデンシャルプロファイルに従って、それぞれに [HTTP] または [HTTPS] を選択します。
- [IP アドレス/サブネットマスク（IP Address/Subnet Mask）]：サーバーの IP アドレス（IPv4 または IPv6）とサブネットマスクを入力します。
- [ポート（Port）]：ポート番号を入力します（通常、HTTP の場合は **8080**、HTTPS の場合は **8843**）。

b) オプション値：

- [タイムアウト（Timeout）]：サーバーへの接続がタイムアウトするまでの待機時間（秒単位）。デフォルトは 30 秒です。

ステップ 4 すべての必須フィールドに入力したら、[保存（Save）] をクリックしてプロバイダを追加します。

Syslog ストレージプロバイダの追加

ストレージプロバイダーは、プレイブックの実行中に収集されたデータのストレージを提供します。

UI を使用して 1 つ以上のストレージプロバイダを追加するには、次の手順を実行します。CSV ファイルを使用してプロバイダを追加することもできます（「プロバイダのインポート （178 ページ）」を参照）。

始める前に

必要な作業は次のとおりです。

- ストレージプロバイダのクレデンシャルプロファイルを作成します（「クレデンシャルプロファイルの作成（143 ページ）」を参照）。これはSSHクレデンシャルである必要があります。
- ストレージプロバイダーに割り当てる名前を確認します。通常、これはサーバーの DNS ホスト名です。
- ストレージプロバイダのサーバーの IPv4 アドレスとポートを確認します。接続プロトコルは SSH になります。
- ストレージプロバイダのサーバーの接続先ディレクトリを確認します。[プロバイダプロパティ（Provider Properties）] フィールドを使用してこれを指定する必要があります。

ステップ 1 メインメニューから、**[管理（Administration）]**>**[プロバイダアクセスの管理（Manage Provider Access）]** を選択します。

ステップ 2 ＋ をクリックします。

ステップ 3 プロバイダのフィールドに次の値を入力します。

a) 必須フィールド：

- [プロバイダ名（Provider Name）]：ストレージプロバイダの名前。
- [クレデンシャルプロファイル（Credential Profile）]：以前に作成したストレージ クレデンシャル プロファイルを選択します。
- [ファミリ（Family）]：[SYSLOG_STORAGE] を選択します。
- [プロトコル（Protocol）]：Cisco Crosswork アプリケーションがプロバイダへの接続に使用するプロトコルとして [SSH] を選択します。
- [IP アドレス/サブネットマスク（IP Address/Subnet Mask）]：サーバーの IP アドレス（IPv4 または IPv6）とサブネットマスクを入力します。
- [ポート（Port）]：ポート番号を入力します（SSH の場合は通常、**22**）。
- [プロバイダプロパティ（Provider Properties）]：次のキー/値のペアを次のフィールドに入力します。

プロパティキー	プロパティ値
DestinationDirectory	収集されたデータがサーバーに保存される絶対パス。例：**/root/cw-syslogs**

b) オプション値：

- [Timeout（タイムアウト）]：ストレージサーバーへの接続がタイムアウトするまでの待機時間（秒単位）。

ステップ 4 すべての必須フィールドに入力したら、[保存（Save）] をクリックして syslog ストレージプロバイダを追加します。

アラートプロバイダの追加

アラートプロバイダは、KPIモニタリング中に収集されたアラートを転送する接続先です（Cisco Crosswork Situation Manager など）。アラートプロバイダーは、着信アラートパッケージを受信および処理できる必要があります。

UI を使用してアラートプロバイダを追加するには、次の手順を実行します。CSV ファイルをインポートしてアラートプロバイダを追加することもできます（「プロバイダのインポート（178 ページ）」を参照）。

現在、サポートされるアラートプロバイダは 1 つだけです。

始める前に

必要な作業は次のとおりです。

- アラートプロバイダのクレデンシャルプロファイルを作成します（「クレデンシャルプロファイルの作成（143 ページ）」を参照）。これは、基本的な HTTP テキスト認証クレデンシャルである必要があります（現在、MD5 認証はサポートされていません）。プロバイダが認証を必要としない場合でも、プロバイダのクレデンシャルプロファイルを指定する必要がありますが、HTTP プロトコルを使用しない任意のプロファイルを指定できます。
- アラートプロバイダーに割り当てる名前を確認します。通常、これはサーバーの DNS ホスト名です。
- アラートサーバーの IPv4 アドレスとポートを確認します。接続プロトコルは HTTP になります。
- アラート サーバー エンドポイントの URL を確認します。[プロパティ値（Property Value）] フィールドを使用してこれを指定する必要があります。

ステップ 1 メインメニューから、**[管理（Administration）] > [プロバイダアクセスの管理（Manage Provider Access）]** を選択します。

ステップ 2 ＋ をクリックします。

ステップ 3 プロバイダのフィールドに次の値を入力します。

a) 必須フィールド：

- [プロバイダ名（Provider Name）]：アラートプロバイダの名前。

- [クレデンシャルプロファイル（Credential Profile）]：以前に作成したアラートプロバイダのクレデンシャルプロファイルを選択します。
- [ファミリ（Family）]：[アラート（ALERT）] を選択します。
- [プロトコル（Protocol）]：HTTP が事前に選択されています。
- [IP アドレス/サブネットマスク（IP Address/Subnet Mask）]：アラートサーバーの IP アドレス（IPv4 または IPv6）とサブネットマスクを入力します。
- [ポート（Port）]：ポート番号を入力します（通常、HTTP の場合は 80）。
- [プロバイダのプロパティ（Provider Properties）]：**alertEndpointUrl** プロパティキー名が事前に入力されています。[プロパティ値（Property Value）] フィールドに、アラート サーバー エンドポイントのみを入力します。たとえば、エンドポイントへの完全なパスが **http://aws.amazon.com:80/myendpoint/bar1/** の場合、**/myendpoint/bar1/** のみを入力します。

b) オプション値：

- [タイムアウト（Timeout）]：アラートサーバーへの接続がタイムアウトするまで待機する時間（秒単位）。

ステップ 4 すべての必須フィールドに入力したら、[保存（Save）]をクリックしてアラートプロバイダを追加します。

プロキシプロバイダーを追加

UI を使用しての 1 つ以上のプロキシのインスタンスをプロバイダーとして追加するには、次の手順を実行します。CSV ファイルを使用してプロバイダを追加することもできます（「プロバイダのインポート （178 ページ）」を参照）。

始める前に

必要な作業は次のとおりです。

- Proxy プロバイダーのクレデンシャルプロファイルを作成します（「クレデンシャルプロファイルの作成 （143 ページ）」を参照）。これは、基本的な HTTPS テキスト認証資格情報である必要があります。
- プロバイダーに割り当てる名前を確認します。これは通常、プロキシサーバーの DNS ホスト名です。
- プロキシサーバーの IP アドレスとポートを確認します。接続プロトコルは HTTPS になります。

ステップ 1 メインメニューから、**[管理（Admin）]** > **[プロバイダー（Providers）]** を選択します。

ステップ 2 ＋ をクリックします。

ステップ 3 プロバイダのフィールドに次の値を入力します。

a) 必須フィールド：

- [プロバイダー名（Provider Name）]：プロバイダーの名前。
- [クレデンシャルプロファイル（Credential Profile）]：以前に作成したクレデンシャルプロファイルを選択します。
- [ファミリ（Family）]：**プロキシ**を選択します。
- [プロトコル（Protocol）]：[HTTPS] を選択します。
- [IP アドレス/サブネットマスク（IP Address/Subnet Mask）]：サーバーの IP アドレス（IPv4 または IPv6）とサブネットマスクを入力します。
- [ポート（Port）]：ポート番号を入力します（HTTPS の場合、**30603**）。

b) オプション値：

- [タイムアウト（Timeout）]：サーバーへの接続がタイムアウトするまでの待機時間（秒単位）。デフォルトは 30 秒です。

ステップ 4 すべての必須フィールドに入力したら、[保存（Save）] をクリックしてプロバイダを追加します。

プロバイダのインポート

プロバイダを指定する CSV ファイルを作成して Cisco Crosswork アプリケーションにインポートするには、次の手順を実行します。

CSV ファイルからプロバイダをインポートすると、まだデータベースにないプロバイダが追加され、インポートしたプロバイダと同じ名前のプロバイダが更新されます。このため、インポートする前に、現在のすべてのプロバイダのバックアップコピーをエクスポートすることをお勧めします（「プロバイダのエクスポート （182 ページ）」を参照）。

ステップ 1 メインメニューから、**[管理（Administration）]>[プロバイダアクセスの管理（Manage Provider Access）]** を選択します。

ステップ 2 をクリックして、[CSV ファイルのインポート（Import CSV File）] ダイアログボックスを開きます。

ステップ 3 インポートするプロバイダ CSV ファイルをまだ作成していない場合は、次の手順を実行します。

a) [「Provider template（*.csv）」サンプルファイルのダウンロード（Download sample 'Provider template (*.csv)' file）] リンクをクリックし、CSV ファイルテンプレートをローカルストレージリソースに保存します。

b) 任意のツールを使用してテンプレートを開きます。ファイルに行を追加します（プロバイダごとに 1 行）。

同じフィールド内で複数のエントリを区切るには、セミコロンを使用します。それらのエントリ間に 2 つのセミコロンをスペースなしで使用することで、フィールドを空白のままにすることを示します。

エントリをセミコロンで区切る場合は、値を入力する順序が重要です。たとえば、**connectivity_type** フィールドに **SSH;SNMP;NETCONF;TELNET** と入力し、**connectivity_port** フィールドに **22;161;830;23** と入力した場合、エントリの順序によって 2 つのフィールド間のマッピングが決定されます。

- SSH：ポート 22
- SNMP：ポート 161
- NETCONF：ポート 830
- Telnet：ポート 23

ファイルを保存する前にサンプルデータ行を必ず削除してください。削除しないと、必要なデータとともにインポートされます。インポート中は無視されるため、列ヘッダー行はそのままでかまいません。

c) 完了したら、新しい CSV ファイルを保存します。

ステップ 4 [参照（Browse）] をクリックし、作成した CSV ファイルに移動した後、[開く（Open）] をクリックして選択します。

ステップ 5 CSV ファイルを選択した状態で、[インポート（Import）] をクリックします。

インポートしたプロバイダ情報が [プロバイダ（Providers）] ウィンドウに表示されます。

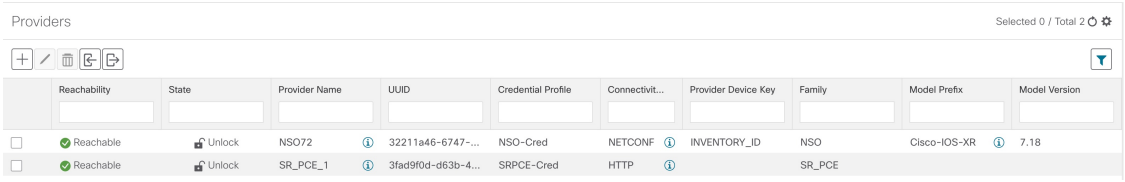
ステップ 6 インポート中に報告されたエラーを解決し、プロバイダの詳細を確認して接続を確定します。

プロバイダの詳細の取得

[プロバイダ（Providers）] ウィンドウを使用して、プロバイダの詳細を取得してそれらの到達可能性を確認します。

ステップ 1 メインメニューから、**[管理（Administration）]** > **[プロバイダアクセスの管理（Manage Provider Access）]** を選択します。
Cisco Crosswork アプリケーションで設定された各プロバイダの [プロバイダ（Providers）] ウィンドウには、次の図に示すように、プロバイダの名前、汎用一意識別子（UUID）、関連するクレデンシャルプロファイルなどの情報が表示されます。

図 *19 : [プロバイダ（Providers）] ウィンドウ*



ステップ 2 [到達可能性（Reachability）] 列のアイコンは、リストされている接続プロトコルを介してプロバイダに到達できるかどうかを示します。詳細については、「デバイスの状態（Device State） （201 ページ）」 を参照してください。

Cisco Crosswork アプリケーションは、プロバイダが追加または変更された直後にプロバイダの到達可能性を確認します。これらのイベント以外は、Cisco Crosswork Change Automation and Health Insights は 5 分ごとに到達可能性を確認し、Crosswork 最適化エンジン は約 10 秒ごとに SR-PCE の到達可能性を確認します。

ステップ 3 次のように、プロバイダの詳細情報をさらに取得します。

a) [プロバイダ名（Provider Name）] 列で、ⓘ をクリックして、プロバイダ固有のキー/値のプロパティを表示します。

b) [接続タイプ（Connectivity Type）] 列で、ⓘ をクリックして、プロバイダ固有のプロトコル、IP 形式、IP アドレス、ポート、タイムアウト情報など、プロバイダの詳細な接続情報を表示します。

c) [モデルプレフィックス（Model Prefix）] 列で、ⓘ をクリックして、Cisco Network Services Orchestrator（Cisco NSO）プロバイダの設定済み NED モデルプレフィックスでサポートされる NED バージョンを表示します。

d) 完了したら、✕ をクリックして詳細ウィンドウを閉じます。

Cisco SR-PCE の到達可能性の問題が発生している場合は、「Cisco SR-PCE の到達可能性の問題 （165 ページ）」を参照してください。HTTP とポート 8080 が設定されていることを確認します。

一般的なプロバイダーの到達可能性の問題については、次のようにトラブルシューティングできます。

1. プロバイダホストに ping を実行します。
2. プロバイダの接続設定で指定されたプロトコルを使用して接続を試行します。。

   次の CLI コマンドを使用して、このチェックを実行できます。

   ```
   curl -v -H "X-Subscribe: stream" "http://<ip-address>:8080/
   bwod/subscribe/json?keepalive-30&priority=5"
   ```

3. ファイアウォール設定とネットワーク設定を確認します。
4. 接続できるユーザーを制限する可能性のあるアクセスコントロールリストの設定については、プロバイダのホストまたは介入デバイスを確認します。

プロバイダの編集

プロバイダ設定を編集する場合は、大規模ネットワーク内に数千台のデバイスがあっても、多数のデバイスにプロバイダがマッピングされる可能性があることに注意してください。

（注）

- プロバイダーの設定を変更する前に、変更の影響を十分に理解しておく必要があります。変更の潜在的なリスクがわからない場合は、シスコサービスにお問い合わせください。
- SR-PCE プロバイダを変更する前に「Cisco SR-PCE プロバイダの追加 （160 ページ）」を参照してください。SR-PCE プロバイダを編集する場合は、追加の手順を実行する必要があります。

。

プロバイダを編集する前に、変更するプロバイダの CSV バックアップをエクスポートすることをお勧めします（「プロバイダのエクスポート （182 ページ）」を参照）。

ステップ 1 メインメニューから、**[管理（Administration）]**>**[プロバイダアクセスの管理（Manage Provider Access）]** を選択します。

ステップ 2 [プロバイダ（Providers）] ウィンドウで、更新するプロバイダを選択して をクリックします。

ステップ 3 必要な変更を加えて、[保存（Save）] をクリックします。

ステップ 4 エラーを解決し、プロバイダーの到達可能性を確認します。

プロバイダの削除

プロバイダを削除するには、次の手順を実行します。

1 つ以上のデバイスまたはクレデンシャルプロファイルに関連付けられているプロバイダを削除しようとすると、アラートが表示されます。

ステップ 1 削除するプロバイダが含まれているバックアップCSVファイルをエクスポートします（「プロバイダのエクスポート （182 ページ）」を参照）。

ステップ 2 （オプション）デバイスがプロバイダにマッピングされているかどうかを確認し、削除する前にプロバイダを変更します。

a) メインメニューから**[デバイス管理（Device Management）]**>**[ネットワークデバイス（Network Devices）]** を選択します。デフォルトでは、[ネットワークデバイス（Network Devices）] タブが表示されます。

b) [ネットワークデバイス（Network Devices）] ウィンドウで、[検索（Search）] フィールドに廃止されたプロバイダ名を入力します。

c) 廃止されたプロバイダにマッピングされているデバイスのチェックボックスをオンにし、をクリックします。

d) [プロバイダ（Provider）] ドロップダウンリストから別のプロバイダを選択します。

e) [保存（Save）] をクリックします。

ステップ 3 次のようにプロバイダーを削除します。

a) メインメニューから、**[管理（Administration）]**>**[プロバイダアクセスの管理（Manage Provider Access）]** を選択します。

b) [プロバイダ（Providers）] ウィンドウで、削除するプロバイダを選択して をクリックします。

c) 確認のダイアログボックスで [削除（Delete）] をクリックします。

プロバイダのエクスポート

プロバイダデータを CSV ファイルにすばやくエクスポートできます。これは、プロバイダー情報のバックアップコピーを保持するための便利な方法です。

（注） CSV ファイルを編集してから再インポートして、既存のプロバイダを更新することはできません。

ステップ 1 メインメニューから、**[管理（Administration）] > [プロバイダアクセスの管理（Manage Provider Access）]** を選択します。

ステップ 2 （オプション）[プロバイダ（Providers）] ウィンドウで、必要に応じてプロバイダリストをフィルタ処理します。

ステップ 3 エクスポートするプロバイダーのチェックボックスをオンにします。エクスポートするすべてのプロバイダーを選択するには、列の上部にあるチェックボックスをオンにします。

ステップ 4 をクリックします。ブラウザによっては、CSV ファイルを保存するときに使用するパスとファイル名を選択するか、またはすぐに開くよう求められます。

タグの管理

[タグ管理（Tag Management）] ウィンドウを使用して、ネットワーク内のデバイスへの割り当てに使用できるタグを管理します。タグは、デバイスの物理的な場所や管理者の電子メール ID などの情報を提供し、デバイスをグループ化するために使用されます。

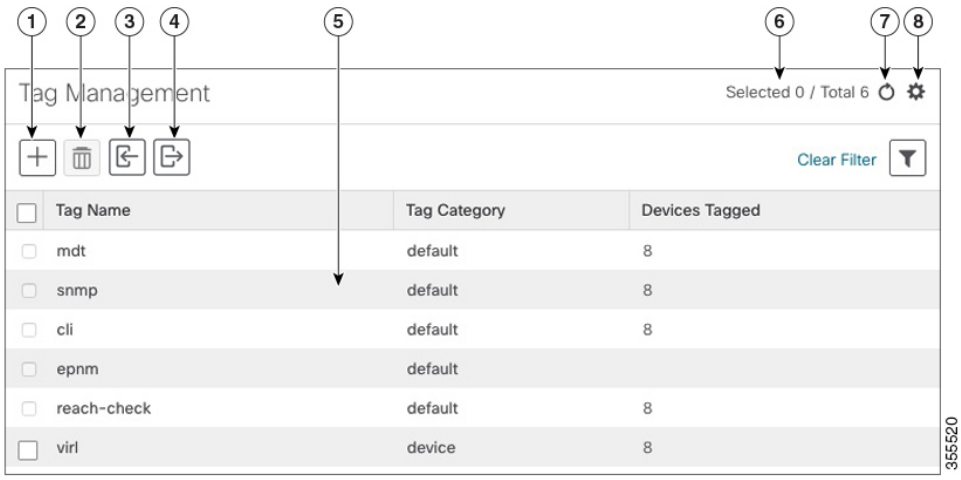
このウィンドウを開くには、**[管理（Administration）] > [タグ（Tags）]** を選択します。

（注） Cisco Crosswork アプリケーションは、タグのデフォルトセットを自動的に作成し、管理するすべてのデバイスに割り当てます。

- cli
- mdt
- reach-check
- snmp
- clock-drift-check

これらのデフォルトタグの選択、編集、削除、または手動によるデバイスとの関連付けは行えません。

図 *20 : [*タグ管理（*Tag Management*）*]* ウィンドウ



項目	説明
1	新しいデバイスタグを作成するには、＋をクリックします。タグの作成（184 ページ）を参照してください。
2	現在選択されているデバイスタグを削除するには、🗑をクリックします。「タグの削除 （187 ページ）」を参照してください。
3	CSV ファイルで定義されたデバイスタグを Cisco Crosswork アプリケーションにインポートするには、をクリックします。「タグのインポート（185ページ）」を参照してください。このアイコンをクリックして、CSV ファイルテンプレートをダウンロードすることもできます。テンプレートには、独自の CSV ファイルを作成するためのガイドとして使用できるサンプルデータが含まれています。
4	現在設定されているタグとその属性がリストされた CSV ファイルをエクスポートするには、をクリックをクリックします。このファイルを更新して Cisco Crosswork アプリケーションにインポートし直すと、複数のタグをすばやく追加または編集できます。「タグのエクスポート（187ページ）」を参照してください。
5	Cisco Crosswork アプリケーションで現在使用可能なタグとその属性を表示します。
6	テーブルで現在選択されているタグの数を示します。
7	[タグ管理（Tag Management）] ウィンドウを更新するには、をクリックします。

項目	説明
8	をクリックし、[タグ管理（Tag Management）] ウィンドウに表示する列を選択します。
	をクリックし、[タグ管理（Tag Management）] ウィンドウの 1 つ以上の列にフィルタ条件を設定します。
	設定したフィルタ条件をクリアするには、[フィルタのクリア（Clear Filter）] リンクをクリックします。

タグの作成

必要な数のタグとタグカテゴリを作成できます。タグが多数ある場合は、各タグを個別に作成するよりも、CSV ファイルにリストしてファイルをインポートするほうが簡単です。「タグのインポート （185 ページ）」を参照してください。

（注）
- タグとタグカテゴリ名は大文字と小文字を区別せず、最大 128 文字の英数字と、ドット（.）、アンダースコア（「_」）、またはハイフン（「-」）を使用できます。その他の特殊文字は使用できません。
- 作成できるタグの最大数は 100 です。

ステップ 1 メインメニューから、**[管理（Administration）] > [タグ（Tags）]** を選択します。[タグ管理（Tag Management）] ウィンドウが開きます。

ステップ 2 をクリックします。[新しいタグの作成（Create New Tags）] ペインが開きます。

ステップ 3 [カテゴリ（Category）] 領域で、次の手順を実行します。

- 新しいタグを既存のカテゴリに関連付けるには、ドロップダウンリストからカテゴリを選択します。
- 新しいタグを新しいカテゴリに関連付けるには、[新しいカテゴリ（New Category）] リンクをクリックし、新しいカテゴリの名前をテキストフィールドに入力し、[保存（Save）] をクリックします。

この手順の後に作成したすべての新しいタグが、選択または作成したカテゴリに割り当てられます。

ステップ 4 [タグ（Tags）] 領域で、作成する新しいタグの名前の入力を開始します。各タグを入力した後、**Return** を押します。

重複するタグを入力しないようにするには、[タグの表示（Show Tags）] リンクをクリックします。[新しいタグの作成（Create New Tags）] ウィンドウには、現在選択されているカテゴリにすでに存在するタグのみが表示されます。

ステップ 5 新しいタグの入力が終了したら、[保存（Save）] をクリックします。

次のタスク

デバイスにタグを追加します。デバイスタグの適用または削除 （186 ページ） を参照してください。

タグのインポート

次の手順を実行して、デバイスに適用するタグがリストされている CSV ファイルを作成し、Cisco Crosswork アプリケーションにインポートします。これは、多数の新しいタグとタグカテゴリをすばやく作成する最も簡単な方法です。

CSV ファイルをインポートすると、データベースにまだ存在していないタグが追加されます。インポートされたタグと同じ名前のタグは上書きされます。このため、インポートする前に、すべての現在のタグのバックアップコピーをエクスポートすることをお勧めします（「タグのエクスポート （187 ページ）」を参照）。

ステップ 1 メインメニューから、**[管理（Admin）] > [タグ（Tags）]** を選択します。

ステップ 2 をクリックして、[CSV ファイルのインポート（Import CSV File）] ダイアログボックスを開きます。

ステップ 3 インポートする CSV ファイルをまだ作成していない場合は、次の手順を実行します。

a) [「Tags template （*.csv）」サンプルファイルのダウンロード（Download sample 'Tags template (*.csv)' file）] リンクをクリックし、CSV ファイルテンプレートをローカルストレージリソースに保存します。

b) 任意のツールを使用してテンプレートを開きます。ファイルに行を追加します（タグごとに 1 行）。行内の各フィールドを区切るには、カンマを使用します。同じフィールド内で複数のエントリを区切るには、セミコロンを使用します。

フィールド	説明	必須またはオプション
タグ名（Tag Name）	タグの名前を入力します。例：**SanFrancisco** または **Spine/Leaf**。	必須
タグカテゴリ（Tag Category）	タグカテゴリを入力します。例：**City** または **Network Role**。	必須

（注） [タグ名（Tag Name）] フィールドと [タグカテゴリ（Tag Category）] フィールドでは大文字と小文字が区別されず、最大 128 文字の英数字と、ドット（.）、アンダースコア（「_」）、またはハイフン（「-」）を使用できます。その他の特殊文字は使用できません。

ファイルを保存する前にサンプルデータ行を必ず削除してください。削除しないと、必要なデータとともにインポートされます。インポート中は無視されるため、列ヘッダー行はそのままでかまいません。

c) 完了したら、新しい CSV ファイルを保存します。

ステップ 4 [参照（Browse）] をクリックし、作成した CSV ファイルに移動した後、[開く（Open）] をクリックして選択します。

ステップ 5 CSV ファイルを選択した状態で、[インポート（Import）] をクリックします。

インポートしたタグとタグカテゴリが [タグ管理（Tag Management）] ウィンドウに表示されます。

次のタスク

デバイスにタグを追加します。デバイスタグの適用または削除（186 ページ）を参照してください。

デバイスタグの適用または削除

タグとそのカテゴリは、デバイスをグループ化するための主要なツールです。一連のデバイスを同じタグでタグ付けすると、それらはグループの一部と見なされ、より簡単に管理できます。

デバイスまたはデバイスグループにタグを適用するためには、タグがすでに存在している必要があります（参照：）。

効率性を高めるため、Cisco Crosswork は、タグ付けされたグループ内のすべてのデバイスのインベントリデータ（トポロジを含む）をインベントリ収集ジョブの単一セットとして自動的に更新します。ただし、タググループのメンバーシップは他の機能では静的であることに注意してください。

1 台のデバイスに最大 15 個のタグを適用できます。

デバイスまたはデバイスのセットにタグを適用するには、次の手順を実行します。

ステップ 1 メインメニューから **[デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）]** を選択します。[ネットワークデバイス（Network Devices）] タブが表示され、デバイスのリストが示されます。

ステップ 2 （オプション）リストが長い場合は、  をクリックして 1 つ以上のフィルタを設定し、タグ付けするデバイスだけにリストを絞り込みます。

ステップ 3 タグ付けするデバイスの横にあるチェックボックスをオンにします。複数のデバイスを選択した場合、変更内容は選択したすべてのデバイスに適用されます。

ステップ 4 ツールバーで  をクリックします。[タグの変更（Modify Tags）] ウィンドウが開き、選択したデバイスに現在適用されているタグが表示されます。

ステップ 5 [オートコンプリートするアイテムの入力（Type to autocomplete item）] をクリックして既存のタグのリストを表示するか、または目的のタグの名前を入力を開始します。

ステップ 6 リスト内の個々のタグをクリックして、デバイスに適用されているタグのリストにそれらを追加します。適用されたタグを削除するには、そのタグの横に表示される [X] アイコンをクリックします。

タグの削除

デバイスタグを削除するには、次の手順を実行します。

（注） タグがデバイスにマッピングされている場合、タグは削除できません。

ステップ 1 削除する予定のタグを含むバックアップCSVファイルをエクスポートします（「タグのエクスポート（187 ページ）」を参照）。

ステップ 2 メインメニューから、**[管理（Administration）]** > **[タグ（Tags）]** を選択します。[タグ管理（Tag Management）] ウィンドウが表示されます。

ステップ 3 削除するタグの横にあるチェックボックスをオンにします。

ステップ 4 ツールバーで をクリックします。

ステップ 5 確認ダイアログボックスに、削除しようとしているタグを現在使用しているデバイスの数が表示されます。[削除（Delete）] をクリックして削除を確認します。

タグのエクスポート

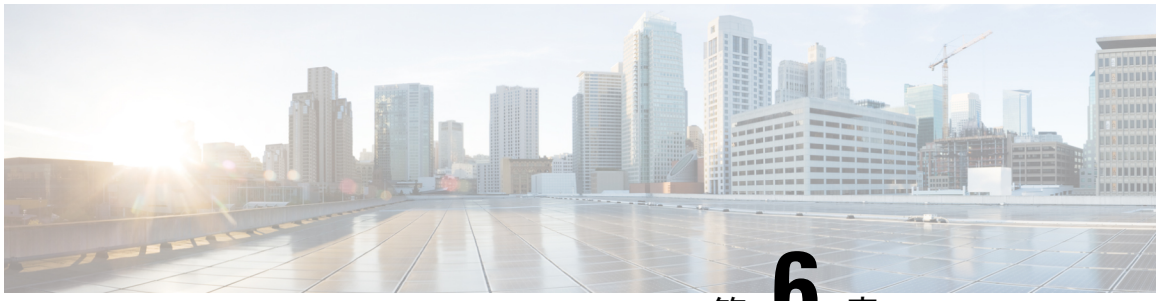
タグとタグカテゴリを CSV ファイルにすばやくエクスポートできます。これにより、タグのバックアップコピーを保持できます。必要に応じてCSVファイルを編集して再インポートし、既存のタグを上書きすることもできます。場合によっては、デバイスとタグを再度関連付ける必要があります。

ステップ 1 メインメニューから、**[管理（Administration）]** > **[タグ（Tags）]** を選択します。

ステップ 2 （オプション）[タグ管理（Tag Management）] ウィンドウで、必要に応じてタグリストをフィルタ処理します。

ステップ 3 エクスポートするタグのチェックボックスをオンにします。エクスポートするすべてのタグを選択するには、列の上部にあるチェックボックスをオンにします。

ステップ 4 をクリックします。ブラウザによっては、CSVファイルを保存するときに使用するパスとファイル名を選択するか、またはすぐに開くよう求められます。



第 6 章

デバイスのオンボーディングと管理

ここでは、次の内容について説明します。

インベントリへのデバイスの追加

Crossworkにデバイスを追加する方法はいくつかあります。それぞれに独自の前提条件があり、デバイスの追加を成功させるために必要です。デバイスが通信用とテレメトリ用に適切に設定されていることを確認します。ガイドラインと設定例については、「新しいデバイスのテレメトリの前提条件 （190ページ）」と「Cisco NSOデバイスの設定例 （191 ページ）」を参照してください。

ほとんどのユーザーの優先順位、メソッド、およびそれらの前提条件は次のとおりです。

1. **Crosswork API を使用したデバイスのインポート**：これはすべての方法の中で最も時間がかからず、効率的ですが、プログラミングスキルと API の知識が必要です。詳細については、『Inventory Management APIs On Cisco Devnet』を参照してください。
2. **デバイスの CSV ファイルからデバイスをインポートする**：この方法は時間がかかる場合があります。この方法を最大限に活かすには、まず次の手順を実行する必要があります。
   - デバイスに関連付けるプロバイダーを作成します。「プロバイダの追加について （154 ページ）」を参照してください。

- CSV ファイルにリストされているすべてのデバイスとプロバイダに対応するクレデンシャルプロファイルを作成します。「クレデンシャルプロファイルの作成 （143 ページ）」を参照してください。
- 新しいデバイスのグループ化に使用するタグを作成します。「タグの作成 （184 ページ）」を参照してください。
- Crosswork から CSV テンプレートファイルをダウンロードし、必要なすべてのデバイスを入力します。

3. **UI を使用したデバイスの追加**：この方法は、入力時にすべてのデータが検証されるため、3 つの方法の中で最もエラーが発生しにくい方法です。また、最も時間のかかる方法であり、一度に追加するデバイスが少ない場合にのみ適しています。適用するプロバイダー、クレデンシャルプロファイル、およびタグは事前に存在している必要があります。詳細については、「UI を使用したデバイスの追加 （192 ページ）」を参照してください。
4. **Cisco SR-PCE プロバイダからの自動オンボーディング**：この方法はかなり自動化されており、比較的簡単です。これらのデバイスに適用するデバイスとプロバイダのクレデンシャルプロファイルとタグは、事前に存在している必要があります。このソースからデバイスをオンボーディングした後、各デバイスを編集して、自動的に検出されないデバイス情報を追加する必要があります。詳細については、「Cisco SR-PCE プロバイダの追加 （160 ページ）」のプロバイダプロパティを参照してください。
5. **ゼロタッチプロビジョニングを使用した自動オンボーディング**：この方法は自動化されていますが、最初にデバイスエントリを作成し、インストールの DHCP サーバーを変更する必要があります。これらのデバイスに適用するデバイスとプロバイダのクレデンシャルプロファイルとタグは、事前に存在している必要があります。この方法を使用してデバイスをプロビジョニングおよびオンボーディングした後、各デバイスを編集して、自動的に提供されない情報を追加する必要があります。詳細については、「ゼロタッチプロビジョニング （213 ページ）」を参照してください。

（注） Cisco Crosswork は、シングルスタック展開モードのみをサポートしています。デバイスは、IPv4 アドレスまたは IPv6 アドレスのいずれか（両方ではない）でオンボーディングできます。

Cisco Crosswork にオンボーディングされているデバイスが Cisco Crosswork Data Gateway インターフェイスと同じサブネット上にある場合、それらは Cisco Crosswork Data Gateway のサウスバウンドネットワーク上にある必要があります。これは、Cisco Crosswork Data Gateway が RPF チェックを実装しており、複数の NIC（2 NIC または 3 NIC）が展開されている、デバイスの送信元アドレスが管理ネットワークまたはノースバウンドネットワーク上にないためです。

新しいデバイスのテレメトリの前提条件

新しいデバイスをオンボーディングする前に、Cisco Crosswork でテレメトリデータを正常に収集および送信するようにデバイスを設定する必要があります。次の項では、SNMP、NETCONF、

SSH、Telnet などのいくつかのテレメトリオプションの設定例を示します。管理する予定のデバイスを設定するためのガイドとして使用します。

（注） SNMPv2 および SNMPv3（Auth/Priv）トラップがサポートされています。

オンボーディング前のデバイス設定

次のコマンドは、正しい SNMPv2 と NETCONF の設定、および SSH と Telnet のレート制限を設定するオンボーディング前のデバイス設定の例を提供します。NETCONF 設定は、デバイスが MDT 対応の場合にのみ必要です。

```
logging console debugging
logging monitor debugging
telnet vrf default ipv4 server max-servers 100
telnet vrf default ipv6 server max-servers 100
crypto key generate rsa
 exec-timeout 0 0
 width 107
 length 37
 absolute-timeout 0
!
snmp-server community public RO
snmp-server community robot-demo2 RO
snmp-server ifindex persist
ntp
 server <NTPServerIPAddress>
!
ssh server v2
ssh server vrf default
ssh server netconf vrf default
ssh server logging
ssh server rate-limit 100
ssh server session-limit 100
!
netconf agent tty
!
netconf-yang agent
 ssh
!
```

SNMPv3 オンボーディング前のデバイス設定

SNMPv3 データ収集を有効にする場合は、前の項の SNMPv2 設定コマンドを繰り返し、次のコマンドを追加します。

```
snmp-server group grpauthpriv v3 priv notify v1default
snmp-server user <user-ID> grpauthpriv v3 auth md5 <password> priv aes 128 <password>
```

Cisco NSO デバイスの設定例

Cisco Network Services Orchestrator（Cisco NSO）をプロバイダとして使用して Cisco Crosswork で管理するデバイスを設定する場合は、Cisco NSO デバイスの設定が次の例のガイドラインに従っていることを確認してください。

この例では、デバイス ID としてホスト名を使用する Cisco NSO 設定を示します。CSV ファイルを使用してデバイスをインポートする場合は、**ROBOT_PROVDEVKEY_HOST_NAME** を provider_node_key フィールドの列挙値として使用します。ここで使用する例のホスト名 **RouterFremont** は、CSV ファイル内のデバイスのホスト名と一致する必要があります。

```
configure
set devices device RouterFremont address 198.18.1.11 port 22
set devices device RouterSFO address 198.18.1.12 port 830
```

次に、リモート名とパスワードが「cisco」の「cisco」という認証グループを作成する例を示します。次に、「Router」で始まる名前のすべてのデバイスを、ned-id「cisco-iosxr-nc-6.6」を使用して「netconf」のデバイスタイプに設定します。最後に、名前が「Router」で始まるすべてのデバイスを「cisco」認証グループに割り当てます。環境に合うように次の設定を編集します。

```
set devices authgroups group cisco default-map remote-name cisco remote-password cisco
set devices device Router* device-type netconf ned-id cisco-iosxr-nc-6.6
set devices device Router* authgroup cisco
```

次の CLI コマンドは、SSH キーのロックを解除してすべてのデバイスから取得します。Cisco NSOは、各デバイスの現在の設定をアップロードして現在の設定を保存することでデバイスと同期します。次のコマンドを使用してデバイス、Cisco NSO、および Cisco Crosswork アプリケーションが共通の設定から開始されていることを確認することが重要です。

```
set devices device Router* state admin-state unlocked
request devices device Router* ssh fetch-host-keys
request devices device Router* sync-from
commit
```

UI を使用したデバイスの追加

UI を使用してデバイスを 1 つずつ追加するには、次の手順に従います。通常の状況では、いくつかのデバイスを追加する場合にのみこの方法を使用します。

ステップ 1 メインメニューから **[デバイス管理（Device Management）]** > **[ネットワークデバイス（Network Devices）]** を選択します。

ステップ 2 ＋ をクリックします。

ステップ 3 次の表に示すように、新しいデバイスの値を入力します。

ステップ 4 [保存（Save）] をクリックします。すべての必須フィールドに入力するまで、[保存（Save）] ボタンは無効になります。

ステップ 5 （オプション）デバイスをさらに追加するには、この手順を繰り返します。

表 *11 : [*新しいデバイスの追加（***Add New Device***）*]* ウィンドウ（** =*必須）

フィールド	説明
*** 管理状態（Administration State）**	デバイスの管理状態。オプションは、次のとおりです。 • [管理対象外（UNMANAGED）] : Crosswork はデバイスをモニターしていません。 • [ダウン（DOWN）] : デバイスは管理されており、ダウンしています。 • [アップ（UP）] : デバイスは管理されており、稼働しています。
*** 到達可能性チェック（Reachability Check）**	Crosswork がデバイスの到達可能性チェックを実行するかどうかを決定します。オプションは、次のとおりです。 • [有効（ENABLE）]（CSV では **`REACH_CHECK_ENABLE`**）：到達可能性を確認して UI の到達可能性状態を自動的に更新します。 • [無効（DISABLE）]（CSV では **`REACH_CHECK_DISABLE`**）：デバイスの到達可能性チェックは無効です。 常に [有効（ENABLE）] に設定することをお勧めします。[設定済みの状態（Configured State）] が [管理対象外（UNMANAGED）] とマークされている場合、このフィールドはオプションです。
*** クレデンシャルプロファイル（Credential Profile）**	データ収集や設定変更のためにデバイスへのアクセスに使用するクレデンシャルプロファイルの名前。例：**`nso23`** または **`srpce123`**。 [設定済みの状態（Configured State）] が [管理対象外（UNMANAGED）] とマークされている場合、このフィールドはオプションです。
ホスト名（Host Name）	デバイスのホスト名。
インベントリ ID（Inventory ID）	デバイスのインベントリ ID 値。値には最大 128 文字の英数字を使用でき、ドット（.）、アンダースコア（「_」）、コロン（「:」）、またはハイフン（「-」）を含めることができます。その他の特殊文字は使用できません。 デバイスのホスト名か、またはインベントリ ID の簡単に識別できる名前を選択します。これは、デバイス名として使用されるインベントリ ID とデバイスを Crosswork に同期するために使用されます。
[ソフトウェア タイプ（Software Type）]	デバイスのソフトウェアタイプ。
ソフトウェア バージョン（Software Version）	デバイスのソフトウェア バージョン。
UUID	デバイスの汎用一意識別子（UUID）。

フィールド	説明
シリアル番号（Serial Number）	デバイスのシリアル番号。
MAC アドレス（MAC Address）	デバイスの MAC アドレス。
*** 機能（Capability）**	デバイスデータの収集を可能にし、デバイスに設定される機能。これは必須の機能であるため、少なくとも **SNMP** を選択する必要があります。**SNMP** が設定されていない場合、デバイスはオンボーディングされません。その他のオプションは、**YANG_MDT**、**YANG_CLI**、**TL1**、および **GNMI** です。選択する機能は、デバイスのソフトウェアタイプとバージョンによって異なります。 （注） MDT 機能を備えたデバイスの場合、この段階では YANG_MDT を選択しないでください。
タグ（Tag）	識別およびグループ化のためにデバイスに割り当てるために使用できるタグ。 デバイスタグを使用して、モニタリングのためにデバイスをグループ化し、デバイスの物理的な場所や管理者の電子メール ID など、他のユーザーにとって重要な可能性がある追加情報を提供します。
製品のタイプ（Product Type）	デバイスの製品タイプ。
Syslog 形式（Syslog Format）	デバイスから受信した syslog イベントの形式は、Syslog コレクタで解析する必要があります。次のオプションがあります。 • [不明（UNKNOWN）]：Syslog コレクタによる解析を行わない場合は、このオプションを選択します。Syslog 収集ジョブの出力には、デバイスから受信した syslog イベントが含まれます。 • [RFC5424]：デバイスから受信した syslog イベントを RFC5424 形式で解析するには、このオプションを選択します。 • [RFC3164]：デバイスから受信した syslog イベントを RFC3164 形式で解析するには、このオプションを選択します。 詳細については、「Syslog 収集ジョブの出力 （79 ページ）」の項を参照してください。
接続の詳細（Connectivity Details）	

フィールド	説明
プロトコル（**Protocol**）	デバイスで使用する接続プロトコル。選択肢は、**SNMP**、**NETCONF**、**TELNET**、**HTTP**、**HTTPS**、**GNMI**、**TL1**、および **GRPC** です。 （注） [セキュア接続（Secure Connection）] スライダを切り替えて、選択した GNMI プロトコルを保護します。 このデバイスの接続プロトコルをさらに追加するには、[接続の詳細（Connectivity Details）] パネルの最初の行の末尾にある ＋ をクリックします。入力したプロトコルを削除するには、パネル内の該当する行の横にある × をクリックします。 同じプロトコルを複数セットなど、必要な数の接続の詳細のセットを入力できます。少なくとも **SSH** と **SNMP** の詳細は入力する必要があります。**SNMP** を設定しない場合、デバイスは追加されません。デバイスを管理する場合（または XR デバイスを管理している場合）、**NETCONF** の詳細を入力する必要があります。**TELNET** 接続はオプションです。
***IP アドレス/サブネットマスク（IP Address/Subnet Mask**）	デバイスの IP アドレス（IPv4 または IPv6）とサブネットマスクを入力します。 （注） 予期しない接続の問題が発生する可能性があるため、IP ネットワークに選択したサブネット（デバイスと接続先を含む）に重複するアドレス空間（サブネット/スーパーネット）がないことを確認してください。 （注） 同じ IP アドレスとサブネットマスクを持つ複数のプロトコルがある場合は、他のフィールドに詳細を自動入力するよう Crosswork に指示できます。
***ポート（Port**）	この接続プロトコルに使用するポート。各プロトコルはポートにマッピングされるため、選択したプロトコルに対応するポート番号を入力してください。各プロトコルの標準的なポート割り当ては次のとおりです。 • SSH：22 • SNMP：161 • NETCONF：830 • TELNET：23 • HTTP：80 • HTTPS：443 GNMI と GNMI_SECURE：ポート値は 57344 ー 57999 です。ここで入力するポート番号が、デバイスで設定されているポート番号と一致していることを確認します。
タイムアウト（**Timeout**）	このプロトコルを使用した通信試行がタイムアウトするまでの経過時間（秒単位）。デフォルト値は 30 秒です。 NETCONF を使用する XE デバイスの場合、推奨される最小タイムアウト値は 90 秒です。その他のすべてのデバイスとプロトコルの場合、推奨される最小タイムアウト値は 60 秒です。

フィールド	説明
エンコード タイプ（Encoding Type）	このフィールドは、**GNMI** プロトコルと **GNMI_SECURE** プロトコルにのみ適用されます。オプションは、**PROTO** と **JSON IETF** です。 デバイスの機能に基づいて、デバイスで一度にサポートされるエンコーディング形式は1つだけです。
ルーティング情報（Routing Info）	
ISIS システム ID（ISIS System ID）	デバイスの IS-IS システムの ID。これは、IS-IS トポロジ内のルータを識別する ID で、SR-PCE 統合に必要です。
OSPF ルータ ID（OSPF Router ID）	デバイスの OSPF ルータ の ID。これは、OSPF トポロジ内のルータを識別する ID で、SR-PCE 統合に必要です。
* TE ルータ ID（TE Router ID）	各 IGP のトラフィック エンジニアリング ルータ の ID。 （注） トポロジ内の L3 リンクを可視化するには、[TE ルータ ID（TE Router ID）] フィールドを入力して、デバイスを Cisco Crosswork にオンボーディングする必要があります。
IPv6 ルータ ID	デバイスの IPv6 ルータ ID。このフィールドは構成可能なパラメータであり、Crosswork によって自動検出されることはありません。
ストリーミングテレメトリの設定（Streaming Telemetry Config）	
Vrf	モデル駆動形テレメトリ（MDT）トラフィックがルーティングされる VRF の名前。
送信元インターフェイス（Source Interface）	デバイスタイプのループバックの範囲。このフィールドは任意です。 （注） このフィールドは、デバイスが [ダウン（DOWN）] または [管理対象外（UNMANAGED）] の状態の場合にのみ編集できます。
MDT 設定の解除	このチェックボックスを有効にすると、Crosswork が NSO 経由でテレメトリ構成をデバイスにプッシュするのをスキップします。この設定はデフォルトでは無効な状態になっています（Crosswork からデバイスに NSO を介してテレメトリ設定がプッシュされます）。 この設定を切り替えるには、デバイスが ADMIN DOWN 状態でなければなりません。設定を有効から無効に切り替える前に、アウトオブバンドの設定のセットアップをクリアする必要があります。
所在地（Location） ネットワークトポロジの地理的ビューに必要な [経度（Longitude）] と [緯度（Latitude）] を除き、ロケーションのすべてのフィールドはオプションです。	
経度（Longitude）、緯度（Latitude）	経度と緯度の値は、地理的マップがデバイスの正しい地理的位置と他のデバイスへのリンクを表示できるようにするために必要です。経度と緯度を 10 進数（DD）形式で入力します。
高度（Altitude）	デバイスが設置されている高度（フィートまたはメートル）。たとえば、**123** です。

フィールド	説明
プロバイダとアクセス（Providers and Access） このデバイスにプロバイダを追加するには、[プロバイダとアクセス（Providers and Access）] パネルの最初の行の末尾にある + をクリックします。入力したプロバイダを削除するには、パネル内のその行の横にある × をクリックします。	
プロバイダファミリ（Provider Family）	トポロジの計算に使用するプロバイダタイプ。リストからプロバイダを選択します。
プロバイダー名（Provider Name）	トポロジ計算に使用されるプロバイダタイプ。リストからプロバイダを選択します。 （注） Cisco NSO LSA 展開の場合、ユーザーは、デバイスを割り当てるリソースに面するサービス（RFS）ノードを選択できます。
クレデンシャル（Credential）	プロバイダに使用するクレデンシャルプロファイル。このフィールドは読み取り専用で、選択したプロバイダーに基づいて自動的に入力されます。

CSV ファイルからのインポートによるデバイスの追加

複数のデバイスを指定する CSV ファイルを作成し、Crosswork にインポートするには、次の手順を実行します。

CSV ファイルからデバイスをインポートすると、まだデータベースにないデバイスが追加され、デバイスレコード内のデータが、インポートされたデバイスのものと一致する [インベントリキータイプ（Inventory Key Type）] フィールド値で上書きされます（これは、システムによって設定され、インポートの影響を受けない UUID を除外します）。このため、インポートする前に、すべての現在のデバイスのバックアップコピーをエクスポートすることをお勧めします。

（注）
- CSV ファイルを使用して多数のデバイスをインポートしている間に、[TE ルータ ID（TE Router ID）] フィールドの値を入力する必要があります。
- Firefox ブラウザを使用して誤った CSV 値を持つ多数のデバイスをインポートすると、ウィンドウが使用できなくなることがあります。この場合は、新しいタブまたはウィンドウで Cisco Crosswork にログインし、正しい CSV 値でデバイスをオンボーディングします。

ステップ 1 メインメニューから **[デバイス管理（Device Management）]** > **[ネットワークデバイス（Network Devices）]** を選択します。デフォルトでは、[ネットワークデバイス（Network Devices）] タブが表示されます。

ステップ 2 ⎘ をクリックして、[CSV ファイルのインポート（Import CSV File）] ダイアログボックスを開きます。

ステップ 3 インポートするデバイス CSV ファイルをまだ作成していない場合：

a) [「Device Management template（*.csv）」サンプルファイルのダウンロード（Download sample 'Device Management template (* .csv)' file）] リンクをクリックし、CSV ファイルテンプレートをローカルストレージリソースに保存します。

b) 任意のツールを使用してテンプレートを開きます。ファイルに行を追加します（デバイスごとに 1 行）。

（注）
- 各デバイスの TE ルータ ID 値が入力されていることを確認します。この値は、SR-PCE から学習したトポロジ内のデバイスを一意に識別するために使用されます。各デバイスの有効な TE ルータ ID がない場合、トポロジは表示されません。
- デバイスのインポート後またはデバイスのオンボーディング後は、TE ルータ ID を変更しないでください。インポート後にデバイスの TE ルータ ID を変更する必要がある場合は、次の手順を実行します。
  1. デバイスを Crosswork から削除する必要があります。
  2. すべての SR-PCE プロバイダを削除する必要があります。
  3. 新しい TE ルータ ID を使用してデバイスを再度オンボーディングします。
  4. SR-PCE プロバイダを再度追加します。

同じフィールド内で複数のエントリを区切るには、セミコロンを使用します。それらのエントリ間に 2 つのセミコロンをスペースなしで使用することで、フィールドを空白のままにすることを示します。複数のエントリをセミコロンで区切る場合は、各フィールドに値を入力する順序が重要であることに注意してください。たとえば、[接続タイプ（Connectivity Type）] フィールドに **SSH;SNMP;NETCONF** と入力し、[接続ポート（Connectivity Port）] フィールドに **`22;161;830`** と入力した場合、エントリの順序によって 2 つのフィールド間のマッピングが決定されます。

- SSH：ポート 22
- SNMP：ポート 161
- NETCONF：ポート 830

入力する必要があるフィールドと必須値のリストについては、UI を使用したデバイスの追加（192 ページ）の [新しいデバイスの追加（Add New Device）] フィールドのテーブルを参照してください。

ファイルを保存する前にサンプルデータ行を必ず削除してください。削除しないと、必要なデータとともにインポートされます。インポート中は無視されるため、列ヘッダー行はそのままでかまいません。

c) 完了したら、新しい CSV ファイルを保存します。

ステップ 4 [参照（Browse）] をクリックし、作成した CSV ファイルに移動した後、[開く（Open）] をクリックして選択します。

ステップ 5 CSV ファイルを選択した状態で、[インポート（Import）] をクリックします。

（注） CSV ファイルを使用して UI 経由でデバイスまたはプロバイダをインポートする場合、ユーザーは操作が完了するまで待機する必要があります。操作の進行中に [インポート（Import）] ボタンをクリックすると、各デバイスまたはプロバイダのエントリの重複が発生します。

ステップ 6 エラーを解決し、デバイスの到達可能性を確認します。

デバイスが最初にインポートされたときに、そのデバイスが到達不能または動作不能として表示されるのは正常です。ただし、30 分後に到達不能または動作不能と表示される場合は、調査が必要な問題がある可能性があります。調査するには、**[デバイス管理（Device Management）] > [ジョブ履歴（Job History）]** を選択し、[ステータス（Status）] 列に表示されるエラーアイコンをクリックします。一般的な問題として、関連付けられたクレデンシャルプロファイルに正しいクレデンシャルが含まれていないことが挙げられます。これをテストするには、サーバーで端末ウィンドウを開き、関連付けられているクレデンシャルプロファイルで指定されたプロトコルとクレデンシャルを使用してデバイスにアクセスします。

ステップ 7 デバイスを正常にオンボーディングしたら、Cisco Crosswork Data Gateway インスタンスにそれらをマッピングする必要があります。

CSV ファイルへのデバイス情報のエクスポート

デバイスリストをエクスポートすると、すべてのデバイス情報が CSV ファイルにエクスポートされます。デバイスリストのエクスポートは、システム内のすべてのデバイスのレコードを一度に保持するのに便利です。必要に応じて CSV ファイルを編集して再インポートし、既存のデバイスデータを上書きすることもできます。

エクスポートしたデバイス CSV ファイルには、各デバイスのクレデンシャルプロファイルの名前のみが含まれ、クレデンシャル自体は含まれません。

ステップ 1 メインメニューから **[デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）]** を選択します。デフォルトでは、[ネットワークデバイス（Network Devices）] タブが表示されます。

ステップ 2 （オプション）必要に応じてデバイスリストをフィルタ処理します。

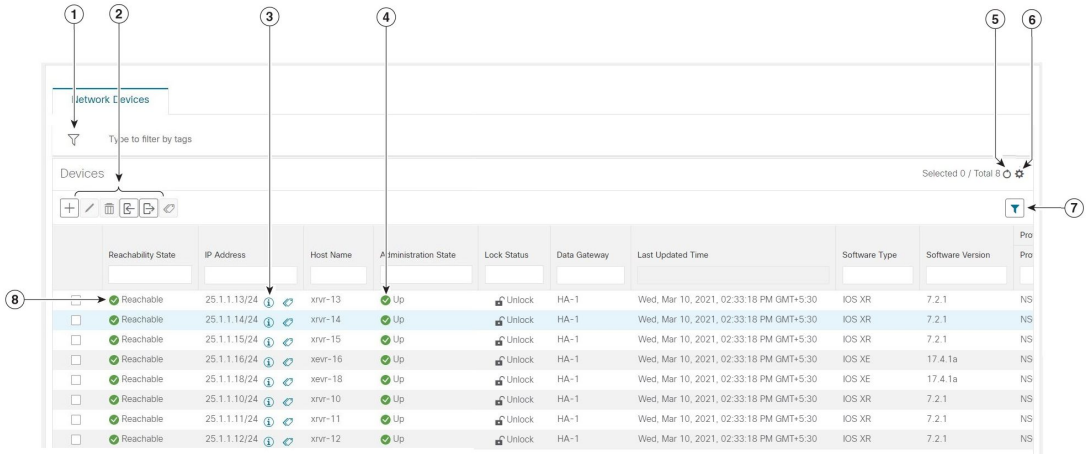
ステップ 3 エクスポートするデバイスのチェックボックスをオンにします。すべてのデバイスをエクスポートするように選択するには、列の上部にあるチェックボックスをオンにします。

ステップ 4 をクリックします。CSV ファイルを保存する際に使用するパスとファイル名を選択するか、またはすぐに開くかを確認するプロンプトがブラウザに表示されます。

ネットワーク デバイスの管理

Cisco Crosswork の [ネットワークデバイス（Network Devices）] ウィンドウには、すべてのデバイスとそのステータスが統合されたリストが表示されます。[ネットワークデバイス（Network Devices）] ウィンドウを表示するには、**[デバイス管理（Device Management] > [ネットワークデバイス（Network Devices）]** を選択します。デフォルトでは、[ネットワークデバイス（Network Devices）] タブが表示されます。

図 *21 : [*ネットワークデバイス（***Network Devices***）*]* ウィンドウ



項目	説明
1	[タグによるフィルタ処理（Filter by tags）] フィールドでは、デバイスに適用されているタグでそれらのデバイスをフィルタ処理できます。検索しようとしているデバイスに適用されているタグの名前を入力します。
2	新しいデバイスをデバイスインベントリに追加するには、＋をクリックします。
	現在選択されているデバイスの情報を編集するには、✎をクリックします。。
	現在選択されているデバイスを削除するには、🗑をクリックします。
	CSV ファイルを使用して、新しいデバイスをインポートし、既存のデバイスを更新するには、⎘をクリックします。このアイコンをクリックして、CSV ファイルテンプレートをダウンロードすることもできます。テンプレートには、独自の CSV ファイルを作成するためのガイドとして使用できるサンプルデータが含まれています。
	選択したデバイスの情報を CSV ファイルにエクスポートするには、⎘をクリックします。
	選択したデバイスに適用されているタグを変更するには、🏷をクリックします。を参照してください。
3	ⓘをクリックすると、[デバイスの詳細（Device Details）] ポップアップウィンドウが開き、選択したデバイスの重要な情報を表示できます。
4	[管理状態（Administration State）] 列のアイコンは、デバイスが動作しているかどうかを示します。
5	デバイスリストを更新するには、↻をクリックします。

項目	説明
6	デバイスリストに表示する列を選択するには、⚙をクリックします。
7	デバイスリストの 1 つ以上の列にフィルタ条件を設定するには、▼をクリックします。
	設定したフィルタ条件をクリアするには、[フィルタのクリア（Clear Filter）] リンクをクリックします。
8	[到達可能性状態（Reachability State）] 列のアイコンは、デバイスが到達可能かどうかを示します。

デバイスの状態（Device State）

Cisco Crosswork は、使用するプロバイダーと管理対象デバイスの到達可能性状態、および到達可能な管理対象デバイスの動作状態および NSO 状態を計算します。次の表のアイコンを使用してこれらの状態を示します。

表 *12*：デバイス状態アイコン

アイコン	意味
[到達可能性状態（Reachability State）] アイコンは、デバイスまたはプロバイダが到達可能かどうかを	
✓	[到達可能（Reachable）]：設定されているすべてのプロトコルによってデバイ
～	[到達可能性低下（Reachability Degraded）]：少なくとも 1 つのプロトコルでデバイスまたはプロバイダに設定されている他の 1 つ以上のプロトコルでは到達でき
✕	[到達不能（Unreachable）]：デバイスまたはプロバイダは、そのプロトコルに
?	[到達可能性不明（Reachability Unknown）]：Cisco Crosswork は、デバイスが到断できません。デバイスが Cisco Crosswork データゲートウェイ（Cisco Crosswo態になる可能性があります。
[動作状態（Operational State）] アイコンは、デバイスが動作しているかどうかを示します。	
↑	デバイスは動作中であり、管理下にあります。すべての個別のプロトコルは「
↓	デバイスが動作していません（「ダウン」）。デバイスがオペレータによってンが使用されます。
?	デバイスの動作状態または設定状態が不明です。
～	デバイスの動作状態または設定状態が低下しています。

アイコン	意味
	デバイスの動作状態または設定状態がエラー状態です。到達して動作状態を計算しプしていないか、または到達不能です。アイコンの横に表示される円内の数字は、リストを表示するには、その数字をクリックします（エラーのアイコンバッジは、できません）。
	デバイスの動作状態は現在確認中です。
	デバイスは削除中です。
	デバイスは管理対象外です。
[NSO状態（NSO State）] アイコンは、デバイスが Cisco NSO と同期されているかどうかを示します。 （注） デバイスのオンボーディング後の Cisco Crosswork と NSO 間の最初の同期では、デバイスの NSC がポリシーに基づいてデバイスを NSO と同期する必要があるかどうかを判断しておらず、初期生します。	
	デバイスは Cisco NSO と同期しています。
	デバイスが Cisco NSO と同期していません。

デバイスの到達可能性状態は次のように計算されます。

1. デバイスの設定状態（ユーザーによる設定）が [アップ（UP）] である限り、到達可能性は常にデバイスごとに計算されます。デバイスが管理上 [ダウン（DOWN）] または [管理対象外（UNMANAGED）] の場合は計算されません。
2. 到達可能性の状態は常に [到達可能（REACHABLE）]、[到達不能（UNREACHABLE）]、または [不明（UNKNOWN）] のいずれかです。
   - 少なくとも 1 つのプロトコルを介してデバイスへのルートが 1 つ以上あり、かつ、デバイスが検出可能な場合、到達可能性状態は [到達可能（REACHABLE）] です。
   - 1 つのプロトコルを介したデバイスへのルートがない場合、またはデバイスが応答しない場合、到達可能性状態は [到達不能（UNREACHABLE）] です。
   - デバイスが [管理対象外（UNMANAGED）] の場合、到達可能性状態は [不明（UNKNOWN）] です。

デバイスの動作状態は次のように計算されます。

1. （ユーザーが設定した）デバイスの動作状態が [アップ（UP）] である限り、動作状態は常に各デバイスに対して計算されます。デバイスが管理上 [ダウン（DOWN）] または [管理対象外（UNMANAGED）] の場合は計算されません。
2. 動作状態は常に [OK] または [エラー（ERROR）] です。

3. デバイスを管理上 OK の状態にするには、デバイスが到達可能で検出可能である必要があります。その他の到達可能性状態は [エラー（ERROR）] です。
4. XR デバイスまたは XE デバイスの場合のみ、管理上 OK の状態では、Crosswork ホストとデバイスクロック間のクロックドリフトの差がデフォルトの値（現在は 2 分）よりも小さいことも必要です。

（注） 一部のタイムゾーン設定では、実際にクロックドリフトが存在しない場合にクロックドリフトエラーが発生することがわかっています。この問題を回避するには、UTC 時間を使用するようにデバイスを設定します。

タグによるネットワークデバイスのフィルタ処理

タグを作成して特定のデバイスに割り当てることで、デバイスの物理的な位置やその管理者の電子メール ID など、他のユーザーにとって重要な可能性のある追加情報を簡単に提供できます。また、タグを使用して、デバイスを一覧表示する任意のウィンドウで同じか、または類似するタグを持つデバイスを検索してグループ化することもできます。

タグでデバイスをフィルタ処理するには、次の手順を実行します。

ステップ 1 メインメニューから **[デバイス管理（Device Management）]** > **[ネットワークデバイス（Network Devices）]** を選択します。

ステップ 2 ユーザーインターフェイスの上部にある [入力してタグでフィルタ処理（Type to filter by tag）] バーに、タグ名のすべてまたは一部を入力します。

[入力してタグでフィルタ処理（Type to filter by Tags）] バーには、先行入力機能があります。入力を開始すると、これまでに入力したすべての文字に一致するタグのドロップダウンリストが表示されます。使用可能なすべてのタグをドロップダウンリストに表示するには、***** を入力します。

ステップ 3 フィルタに追加するタグの名前を選択します。[入力してタグでフィルタ処理（Type to filter by tags）] フィルタバーにフィルタが表示されます。テーブルまたはマップには、そのタグを持つデバイスのみが表示されます。

ステップ 4 複数のタグでフィルタリングする場合は次の手順を実行します。

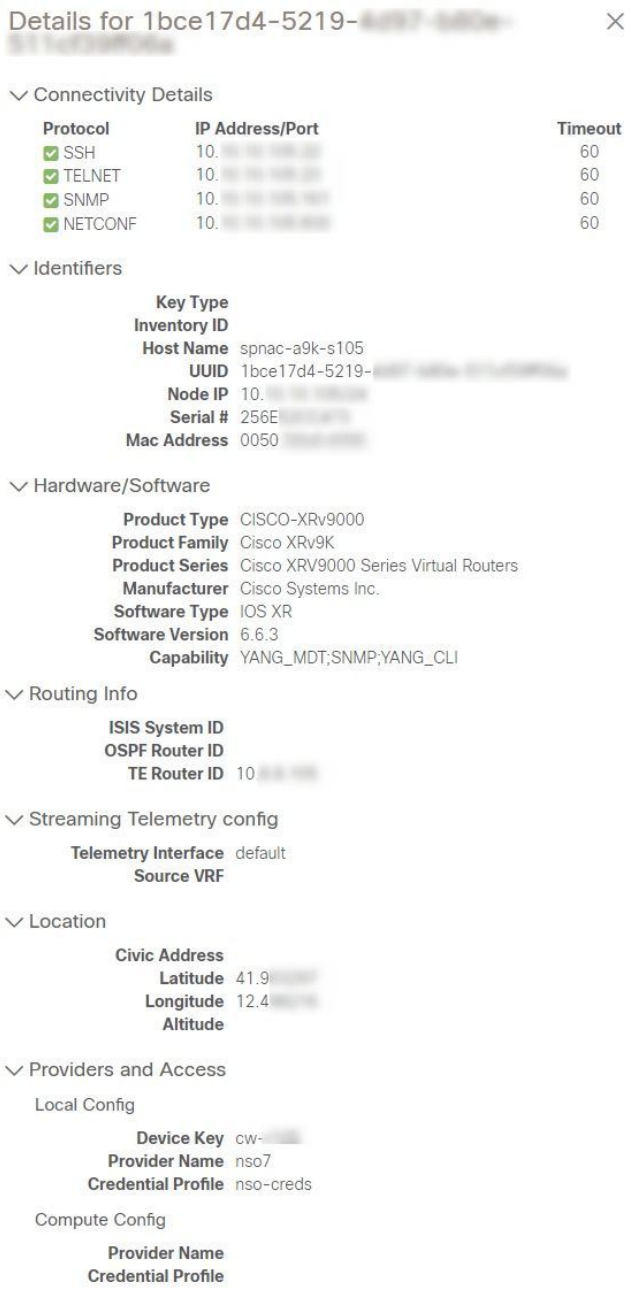
a) フィルタの一部として設定する追加タグごとに、手順 2 と 3 を繰り返します。
b) 必要なすべてのタグを選択したら、[フィルタの適用（Apply Filters）] をクリックします。テーブルまたはマップには、フィルタ内の**すべて**のタグに一致するタグを持つデバイスのみが表示されます。

ステップ 5 すべてのタグフィルタをクリアするには、[フィルタのクリア（Clear Filters）] リンクをクリックします。複数のタグを含むフィルタからタグを削除するには、フィルタ内のそのタグの名前の横にある [X] アイコンをクリックします。

デバイスの詳細情報の取得

[デバイス管理（Device Management）] > **[ネットワークデバイス（Network Devices）]** を選択し、[ネットワークデバイス（Network Devices）] タブにデバイスのリストを表示するたびに、リストされているデバイスの横にある をクリックすると、そのデバイスに関する詳細情報を取得できます。このアイコンをクリックすると、[デバイス名の詳細（Details for DeviceName）] ポップアップウィンドウが開きます。次に例を示します。

図 *22 : [*デバイス名の詳細（***Details for DeviceName***）*]* ウィンドウ



ポップアップウィンドウの上部にある [接続の詳細（Connectivity Details）] 領域を展開します（まだ展開していない場合）。この領域には、すべてのトランスポートタイプの到達可能性ステータスが表示されます。

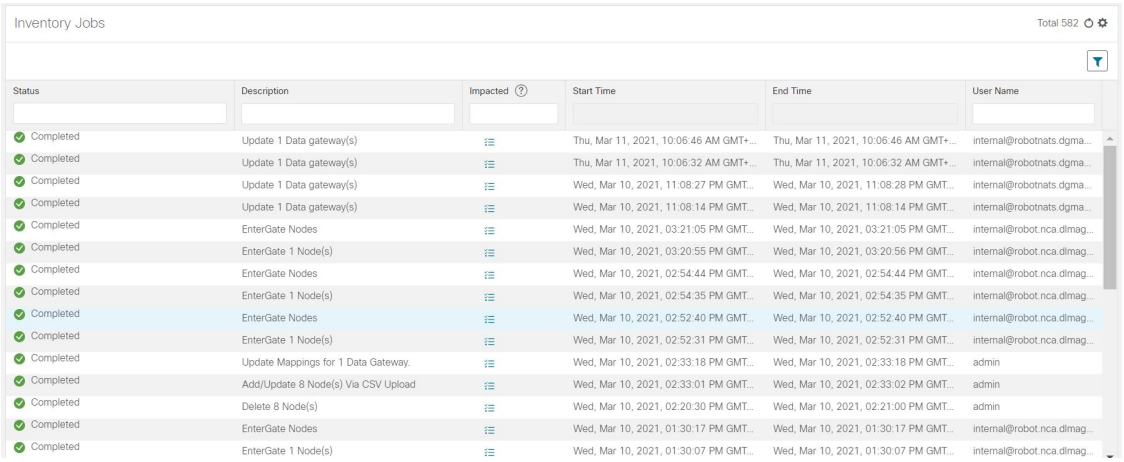
必要に応じて、ポップアップウィンドウの他の領域を展開したり、折りたたんだりします。× をクリックしてウィンドウを閉じます。

デバイスのジョブ履歴の表示

Cisco Crossworkは、デバイス関連のジョブに関する情報を収集して保存します。作成、更新、および削除のすべてのアクティビティを追跡するには、次の手順を実行します。

ステップ1 メインメニューから **[デバイス管理（Device Management）] > [インベントリジョブ（Inventory Jobs）]** を選択します。[インベントリジョブ（Inventory Jobs）] ウィンドウが開き、次のようなデバイス関連のすべてのジョブのログが表示されます。

図 *23 : [インベントリジョブ（Inventory Jobs）] ウィンドウ*



ジョブは作成時刻の降順に表示されます。最新のジョブが最初に表示されます。テーブル内のデータをソートするには、列の見出しをクリックします。もう一度列の見出しをクリックすると、ソートの昇順と降順が切り替わります。

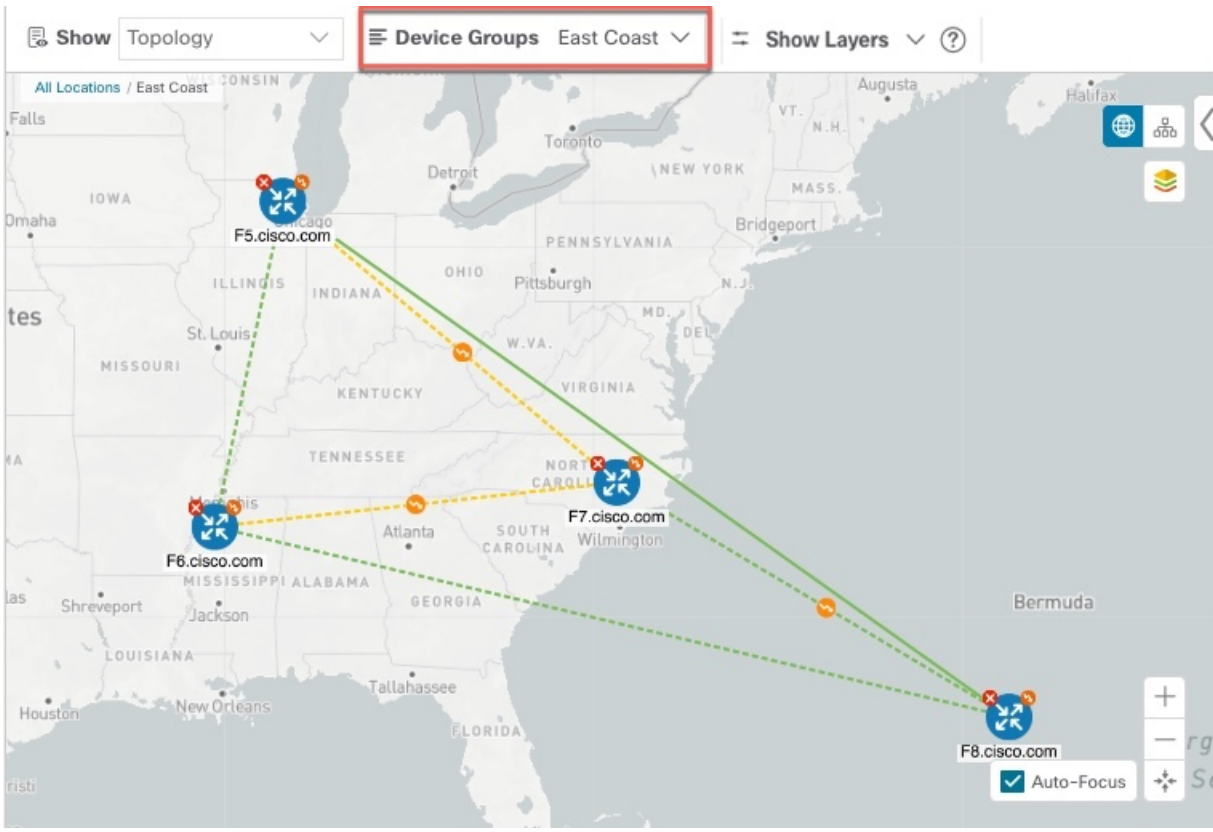
ステップ2 [ステータス（Status）]列には、完了、失敗、実行中、部分的、および警告の状態タイプが表示されます。失敗したジョブまたは部分的なジョブの場合に詳細を確認するには、エラーの横にある をクリックします。

（注） デバイスに到達できない場合でも、ステータスが [成功（Successful）] と表示される場合があります。表示されているジョブのステータスが正しいことを確認するには、デバイスのステータスも調べます（[デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）]）。

デバイスグループを使用したトポロジビューのフィルタ処理

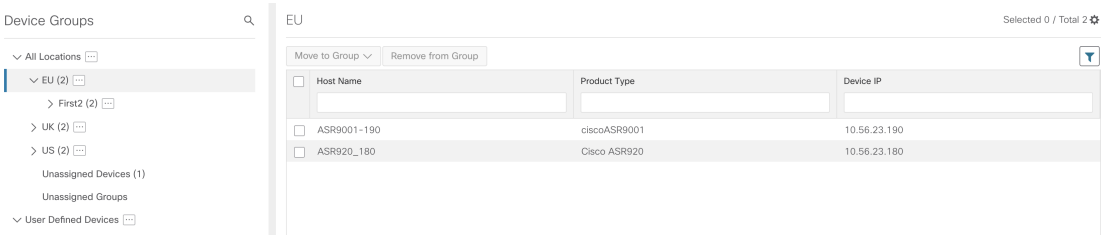
さまざまな目的でデバイスを識別、検索、およびグループ化するためにデバイスグループを作成できます。デバイスグループでは、そのデバイスグループに固有のデータを視覚化して拡大できます。これにより、画面上の乱雑さが軽減され、最も重要なデータに集中できます。たとえば、次の図では、東海岸のデバイスグループが選択されており、トポロジマップに拡大表示されています。また、[デバイス（Devices）]テーブルには、東海岸のデバイスグループに属するデバイスのみが表示されていることに注意してください。

図 *24*：トポロジマップでのデバイスグループの選択



[デバイスグループ（Device Groups）] ウィンドウ（**[デバイス管理（Device Management）]** > **[グループ（Groups）]**）では、デバイスグループを作成および管理できます。デフォルトでは、すべてのデバイスが最初は [未割り当てデバイス（Unassigned Devices）] グループに表示されます。

図 *25 :* デバイスグループセレクタ



デバイスグループの作成と変更

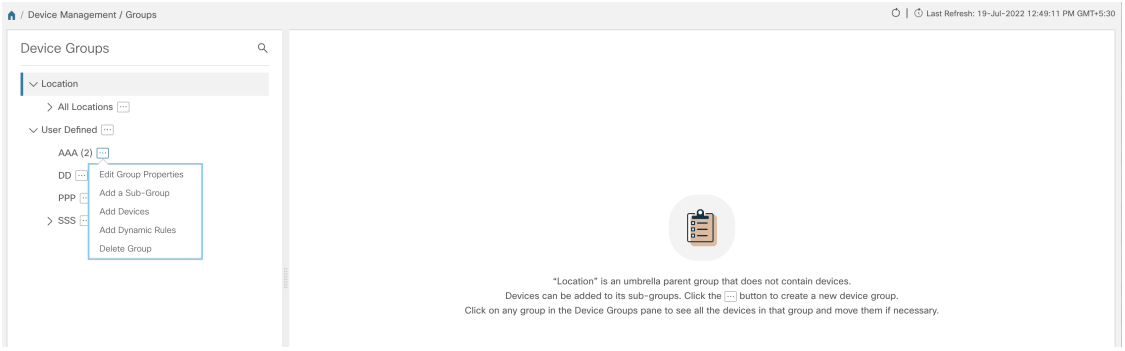
デバイスグループ、およびグループへのデバイスの割り当ては、手動（この項で説明）または自動（次の項で説明）で実行できます。

ステップ 1 メインメニューから **[デバイス管理（Device Management）] > [グループ（Groups）]** を選択します。

ステップ 2 新しいサブグループを追加するには、[すべての場所（All Locations）] の横にある をクリックします。[すべての場所（All Locations）] の下に新しいサブグループが追加されます。

ステップ 3 デバイスをグループに追加するには、右ペインの [未割り当てのデバイス（Unassigned Devices）] でデバイスを選択し、[グループに移動（Move to Group）] ドロップダウンから適切なグループを選択します。

ステップ 4 既存グループの下で、サブグループを編集、削除、または追加するには、[デバイスグループ（Device Groups）] ツリーでグループの横にある をクリックします。



ステップ 5 グループの追加、削除、または編集（名前の変更または移動）を選択します。グループを削除すると、そのグループに属しているすべてのデバイスが [未割り当てデバイス（Unassigned Devices）] グループに移動します。また、グループを削除すると、そのグループのサブグループがすべて削除されます。

（注） デバイスは、1 つのデバイスグループにのみ属することができます。

ステップ 6 [保存（Save）] をクリックします。

ダイナミック デバイス グループの有効化

デバイスホスト名で正規表現（regex）を使用して、デバイスグループを動的に作成し、未割り当てのデバイスをこれらのグループに自動的に追加するルールを作成できます。ルールに一致する新たに追加または検出されたデバイスは、適切なグループに配置されます。

（注） ダイナミックルールは、すでにグループに属しているデバイスには適用されません。ルールで考慮されるようにするデバイスは、[未割り当てデバイス（Unassigned Devices）] に移動する必要があります。

始める前に

[ダイナミックグループ（Dynamic Groups）] ダイアログに示されている例に従うこともできますが、正規表現に精通していると有利です。

ステップ 1 メインメニューから **[デバイス管理（Device Management）] > [グループ（Groups）]** を選択します。

ステップ 2 [すべての場所（All Locations）] > [動的グループ化ルールの管理（Manage Dynamic Grouping Rule）] の横にある をクリックします。

ステップ 3 [他の詳細と例の表示（Show more details and examples）] をクリックして、必要な [ホスト名（Host Name）] フィールドと [グループ名（Group Name）] フィールドに入力します。

ステップ 4 [未割り当てデバイス（Unassigned Devices）] グループに既存のデバイスがある場合は、[ルールのテスト（Test Rule）] をクリックして、作成されるグループ名のタイプのサンプリングを表示します。

ステップ 5 [ルールの有効化（Enable Rule）] トグルをオンにして、ルールを有効にします。ルールが有効になると、システムは未割り当てのデバイスを 1 分おきに確認し、ルールに基づいてそれらを適切なグループに割り当てます。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 この方法で作成されたグループは、最初は [未割り当てグループ（Unassigned Groups）] の下に表示されます（ルールが初めて有効になったときに作成されます）。新たに作成したグループを必要なグループ階層に移動します。

ステップ 8 新しく作成した未割り当てグループを適切なグループに移動するには、次の手順を実行します。

a) すべてのロケーションの横にある をクリックし、[サブグループを追加（Add a Sub-Group）] をクリックします。
b) 新しいグループに詳細を入力して [作成（Create）] をクリックします。
c) 左ペインから未割り当てのデバイスをクリックします。
d) 右側のペインから、移動するデバイスを選択し、[グループに移動（Move to Group）] をクリックして適切なグループに移動します。

デバイスの編集

デバイスの情報を更新するには、次の手順を実行します。

デバイスを編集する前に、変更するデバイスの CSV バックアップをエクスポートしておくことをお勧めします。

ステップ 1 メインメニューから **[デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）]** を選択します。

ステップ 2 （オプション）特定の列をフィルタ処理してデバイスのリストをフィルタ処理します。

ステップ 3 変更するデバイスのチェックボックスをオンにし、✎ をクリックします。

ステップ 4 必要に応じて、デバイスに設定されている値を編集します。

（注） 既存のフィールドに加えて、選択したデバイスに設定されているデータゲートウェイを表示することもできます。このフィールドは読み取り専用です。

ステップ 5 [保存（Save）] をクリックします。[保存（Save）] ボタンは、すべての必須フィールドの入力が完了するまではグレー表示されます。

ステップ 6 エラーを解決し、デバイスの到達可能性を確認します。

デバイスの削除

次の手順を実行して、デバイスを削除します。

始める前に

- SR-PCE プロバイダーの [auto-onboard] プロパティを [管理（managed）] または [管理対象外（unmanaged）] オプションに設定した場合は、1 つ以上の SR-PCE の [自動オンボード（auto-onboard）] を [オフ（off）] に設定します。
- デバイスを削除する前に、デバイスが切断され、電源がオフになっていることを確認します。
- デバイス が MDT 機能を備えた Cisco NSO にマッピングされ、テレメトリ設定がプッシュされると、それらの設定はデバイスから削除されます。
- [自動オンボード（auto-onboard）] が [オフ（off）] に設定されていないためにまだ機能しており、ネットワークに接続されている場合、デバイスは削除時に管理対象外として再検出されます。

ステップ 1 削除するデバイスを含んでいるバックアップ CSV ファイルをエクスポートします。

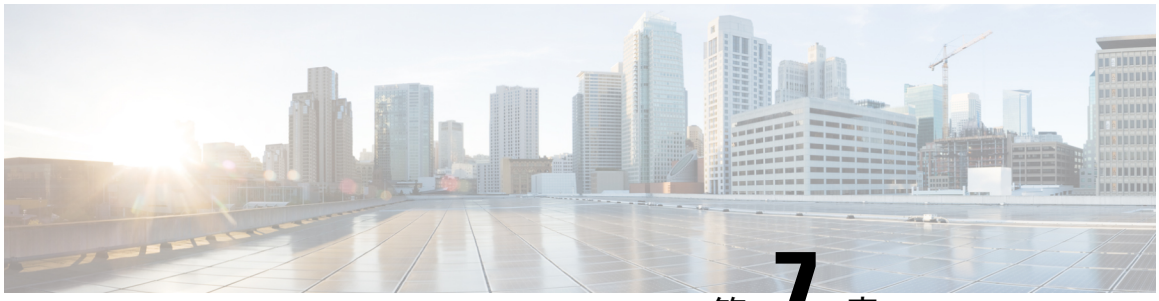
ステップ 2 メインメニューから **[デバイス管理（Device Management）]** > **[ネットワークデバイス（Network Devices）]** を選択します。

ステップ 3 （オプション）[デバイス（Devices）] ウィンドウで、[検索（Search）] フィールドにテキストを入力するか、または特定の列をフィルタ処理して、デバイスのリストをフィルタ処理します。

ステップ 4 削除するデバイスのチェックボックスをオンにします。

ステップ 5 をクリックします。

ステップ 6 確認のダイアログボックスで [削除（Delete）] をクリックします。



第 7 章

ゼロタッチ プロビジョニング

ここでは、次の内容について説明します。

ゼロタッチプロビジョニングの概念

Cisco Crosswork Zero Touch Provisioning（ZTP）アプリケーションでは、工場出荷時の状態のデバイスをブランチオフィスまたはリモートの場所に出荷し、物理的に設置した後でプロビジョニングすることができます。ローカルオペレータは、イメージをインストールしたり、設定したりすることなく、これらのデバイスをネットワークにケーブル接続できます。ZTP を使用するには、まずDHCP サーバーと ZTP アプリケーションで各デバイスのエントリを確立します。その後、デバイスをネットワークに接続して電源を投入するか、リロードすることで、ZTP 処理をアクティブ化できます。デバイスは自動的にソフトウェアイメージと設定をダウンロードし、デバイスに適用します（設定のみを適用することもできます）。設定が完了すると、ZTP は新しいデバイスを Cisco Crosswork デバイスインベントリにオンボーディングします。その後、他の Cisco Crosswork アプリケーションを使用して、デバイスをモニターおよび管理できます。

Cisco Crosswork ZTP では、次の基本用語と概念を使用します。

- **クラシック ZTP**：ソフトウェアと設定ファイルをダウンロードしてデバイスに適用するプロセス。iPXE ファームウェアと HTTP を使用してデバイスを起動し、ダウンロードを実行します。パブリックネットワークでの使用には適していません。
- **セキュア ZTP**：ソフトウェアイメージと設定ファイルをダウンロードしてデバイスに適用するセキュアなプロセス。セキュアなトランスポートプロトコルと証明書を使用してデバイスを検証し、ダウンロードを実行します。
- **PnP ZTP**：ソフトウェアイメージと設定ファイルをダウンロードし、シスコデバイスに適用するセキュアなプロセス。Cisco Plug and Play（Cisco PnP）を使用してデバイスを検証し、セキュアで暗号化されたチャネルを介してダウンロードを実行します。

- **評価ライセンスのカウントダウン**：ZTP を使用して、デバイスをライセンスなしで 90 日間オンボーディングできます。この評価期間が終了すると、ZTP を使用して以前にオンボーディングしたすべてのデバイスと、予定している今後のニーズをカバーするのに十分なキャパシティを備えたライセンスバンドルを購入してインストールするまでは、ZTP を使用して新しいデバイスをオンボーディングすることはできません。

- **イメージファイル**：デバイスにネットワーク オペレーティング システムをインストールするために使用するバイナリ ソフトウェアイメージファイル。シスコのデバイスの場合、これらのファイルはCisco IOSイメージのサポートされているバージョンです。ソフトウェアイメージのインストールは、ZTP処理ではオプションの部分となります。インストールするように設定されている場合、ZTP プロセスは Cisco Crosswork からデバイスにイメージをダウンロードします。デバイスによってそのインストールが行われます。SMU もインストールする必要がある場合、ZTP はクラシック ZTP とセキュア ZTP の設定処理の一部としてそれらをインストールできます（SMU は PnP ZTP ではサポートされていません）。

- **Cisco Plug and Play（Cisco PnP）**：シスコ独自のゼロタッチ プロビジョニング ソリューションで、ほとんどのIOS ソフトウェアイメージにバンドルされています。Cisco PnP は、ソフトウェア PnP エージェントと PnP サーバーを使用して、デバイスにイメージと設定を配布します。通信の安全を確保するために、サーバーとエージェントは HTTPS を使用して通信します。

- **設定ファイル**：新しくイメージ化されたデバイスや再イメージ化されたデバイスの動作パラメータを設定するために使用するファイル。使用する予定のZTPモードに応じて、ファイルはPython スクリプト、Linux シェルスクリプト、またはASCIIテキストとして保存された一連の Cisco IOS CLI コマンドになります（これらのすべてがすべての ZTP モードでサポートされているわけではありません）。ZTPプロセスは、新しくイメージ化されたデバイスに設定ファイルをダウンロードし、実行します。ZTP処理には設定ファイルが必要です。セキュア ZTP は、最大 3 つの異なる設定ファイルもサポートします。これらの設定ファイルは、事前設定、Day 0、および設定後の順序でオンボーディング中に適用されます。

- **設定の処理方法**：セキュア ZTP ユーザーオプション。新しい設定を既存のデバイス設定にマージするか、または上書きするかを指定できます。セキュア ZTP を実装している場合にのみ使用できます。

- **クレデンシャルプロファイル**：SNMP、SSH、HTTP、およびその他のネットワークプロトコルを介してデバイスにアクセスするために使用するパスワードとコミュニティ文字列の集まり。Cisco Crossworkは、クレデンシャルプロファイルを使用してデバイスにアクセスし、デバイスアクセスを自動化します。すべてのクレデンシャルプロファイルは、パスワードとコミュニティ文字列を暗号化形式で保存します。

- **ブートファイル名**：ZTP リポジトリに保存されているソフトウェアイメージの明示的なパスと名前。ZTP を使用してオンボーディングする予定のデバイスごとに、DHCP のデバイス設定の一部としてブートファイル名を指定します。

- **HTTPS/TLS**：Hypertext Transport Protocol Secure（HTTPS）は、HTTP プロトコルのセキュアな形式です。暗号化したレイヤで HTTP をラップします。このレイヤは Transport Layer Security（TLS）（以前の Secure Sockets Layer、つまり SSL）です。
- **iPXE**：オープンソース ブート ファームウェア iPXE は、ブート前実行環境（PXE）クライアントファームウェアとブートローダの一般的な実装です。 iPXE を使用すると、組み込み PXE サポートのないデバイスをネットワークから起動できます。iPXE ブートプロセスは、従来の ZTP 処理の通常部分にすぎません。
- **所有者証明書**：組織の認証局（CA）署名入りエンドエンティティ証明書。公開キーを組織にバインドします。所有者証明書は、セキュア ZTP 処理の一部としてデバイスにインストールします。
- **所有権バウチャー**：所有権バウチャーは、デバイスに保存されている所有者証明書を検証することにより、デバイスの所有者を識別するために使用されます。シスコは、組織からの要求に応じて所有権バウチャーを提供します。
- **Cisco PnP エージェント**：Cisco IOS-XE デバイスに組み込まれたソフトウェアエージェント。PnP エージェントをサポートするデバイスは、スタートアップ設定ファイルなしで初めて電源が投入されるたびに、Cisco PnP サーバーを検索しようとします。このエージェントは、DHCP や DNS など、さまざまな方法でサーバーの IP アドレスを検出できます。
- **Cisco PnP サーバー**：ソフトウェアイメージおよび設定の管理と Cisco PnP 対応デバイスへの配布を行う中央サーバー。Cisco Crosswork ZTP には、HTTPS を使用して PnP エージェントと通信するように設定された PnP サーバーが組み込まれています。
- **SUDI**：セキュアな一意のデバイス識別子（SUDI）は、関連付けられたキーペアを持つ証明書です。SUDI には、デバイスの製品識別子とシリアル番号が含まれています。シスコは製造時に SUDI とキーペアをデバイスハードウェアのトラストアンカーモジュール（TAm）に挿入し、デバイスにイミュータブル ID を付与します。セキュア ZTP 処理時に、バックエンドシステムはデバイスにアイデンティティの検証を要求します。ルータは SUDI ベースのアイデンティティを使用して応答します。このやり取りと TAm 暗号化サービスにより、バックエンドシステムは暗号化されたイメージと設定ファイルを提供できます。これらの暗号化されたファイルを開くことができるのは、検証済みのルータだけです。これにより、パブリックネットワーク上での転送の機密性が確保されます。
- **SUDI ルート CA 証明書**：認証局（CA）によって発行および署名され、下位の SUDI 証明書を認証するために使用する SUDI のルート認証証明書。
- **UUID**：汎用一意識別子（UUID）は、Cisco Crosswork にアップロードしたイメージファイルを一意に識別します。クラシック ZTP とセキュア ZTP では、DHCP ブートファイル URL のソフトウェアイメージファイルの UUID を使用します。
- **ZTP アセット**：ZTP では、新しいデバイスをオンボーディングするために、いくつかのタイプのファイルと情報にアクセスする必要があります。これらのファイルと情報を総称して「ZTP アセット」と呼びます。ZTP 処理を開始する前に、ZTP 設定の一部としてこれらのアセットをロードします。

- **ZTP プロファイル**：（通常は）1 つのイメージと 1 つの設定を 1 つのユニットに結合する Cisco Crosswork ストレージ構成。Cisco Crosswork は、ZTP プロファイルを使用して、イメージ化プロセスと設定プロセスを自動化します。ZTP プロファイルの使用は任意ですが、推奨されています。これらは、デバイスファミリ、クラス、およびロールに関する ZTP イメージと設定の整理を簡単にし、ZTP の使用に一貫性を持たせるのに役立ちます。
- **ZTP リポジトリ**：Cisco Crosswork がイメージと設定ファイルを保存する場所。

ZTP でのプラットフォームサポート

このトピックでは、シスコ製とサードパーティ製のソフトウェアおよびデバイスに対する Cisco Crosswork Zero Touch Provisioning のサポートについて詳しく説明します。

クラシック ZTP でのプラットフォームサポート

次のプラットフォームは、クラシック ZTP をサポートしています。

- **ソフトウェア**：Cisco IOS-XR バージョン 6.6.3、7.0.1、7.0.2、7.0.12、7.3.1 以降。
- **ハードウェア**：
  - Cisco Network Convergence Systems（NCS）520 および 540 シリーズ ルータ
  - Cisco NCS 1000-1004 シリーズ ルータ
  - Cisco NCS 5500 シリーズ ルータ
  - Cisco NCS 8000 および 8800 シリーズ ルータ（Spitfire 固定モード）

クラシック ZTP は、サードパーティ製のデバイスまたはソフトウェアをサポートしていません。

セキュア ZTP でのプラットフォームサポート

次のプラットフォームでセキュア ZTP がサポートされています。

- **ソフトウェア**：Cisco IOS-XR バージョン 7.3.1 以降（ただし、このリリースではサポートされていないリリース 7.3.2 と 7.4.1 を除く）。

  単一イメージのインストールとして、IOS-XR 6.6.3 から 7.3.1 にアップグレードできます。
- **ハードウェア**：
  - Cisco Network Convergence Systems（NCS）540 シリーズ
  - Cisco NCS 1000 ～ 1004 シリーズ
  - Cisco NCS 5500 シリーズ
  - Cisco NCS 8000 シリーズと 8800 シリーズ（Spitfire 固定モード）

セキュア ZTP は、サードパーティ製デバイスのプロビジョニングをサポートしています。

- Secure ZTP RFC 8572（https://tools.ietf.org/html/rfc8572）に 100% 準拠していること。
- デバイス証明書と所有権バウチャーのシリアル番号がシスコ形式のガイドラインと一致していること。詳細については、次のセクション「Secure ZTP：サードパーティ製デバイス証明書および所有権バウチャーのガイドライン」を参照してください。

PnP ZTP でのプラットフォームサポート

次のプラットフォームで PnP ZTP がサポートされています。

- **ソフトウェア**：Cisco IOS-XE バージョン 16.12、17.4.1、17.5.1. お客様に推奨されるバージョンは、バージョン 16.12.5 です。
- **ハードウェア**：
  - Cisco Network Convergence Systems（NCS）520 シリーズ ルータ
  - Cisco アグリゲーション サービス ルータ（ASR）903
  - Cisco ASR 907
  - Cisco ASR 920

PnP ZTP は、サードパーティ製デバイスまたはソフトウェアをサポートしていません。

PnP ZTP を使用する場合は、ZTP 処理をトリガーする**前**に、各 IOS-XE デバイスの最小ライセンスブートレベルが **metroipaccess** または **advancedmetroipaccess** に設定されていることを確認します。ブートレベルが正しく設定されている場合、デバイスの IOS-XE `#sh run | sec license` CLI コマンドの出力に、2 つのライセンスレベル、`license boot level advancedmetroipaccess` または `license boot level metroipaccess` のいずれかを示すステートメントが含まれている必要があります。コマンド出力に他のライセンスレベル、特にこれらのライセンスレベルより低いライセンスレベルが示されている場合は、Cisco PnP の暗号化機能が有効になりません。これにより、証明書のインストールが失敗して PnP ZTP デバイスのプロビジョニングが失敗します。

セキュア ZTP：サードパーティ製デバイス証明書および所有権バウチャーのガイドライン

デバイスのセキュア ZTP 処理は、デバイスと Cisco Crosswork 間の正常な HTTPS/TLS ハンドシェイクから始まります。ハンドシェイク後、セキュア ZTP はデバイス証明書からシリアル番号を抽出する必要があります。セキュア ZTP は、抽出したシリアル番号を内部のシリアル番号の「許可」リストと照合して検証します。許可リストを作成するには、デバイスのシリアル番号を Cisco Crosswork にアップロードします。所有権バウチャーを使用してダウンロードを検証する場合も、同様のシリアル番号検証手順が後で実行されます。

Cisco IOS-XR デバイスとは異なり、サードパーティベンダーのデバイス証明書のシリアル番号の形式はベンダー間で標準化されていません。通常、サードパーティベンダーのデバイス証明書には、`Subject` フィールドまたはセクションがあります。`Subject` には、ベンダーが決定する複数のキーと値のペアが含まれます。通常、キーと値のペアの 1 つは `serialNumber` キーです。このキーの値には、実際のデバイスのシリアル番号が文字列として含まれます。その前には、

文字列 SN: が付きます。たとえば、サードパーティのデバイス証明書の Subject セクションに serialNumber = PID:NCS-5501 SN:FOC2331R0CW というキーと値が含まれているとします。セキュア ZTP は SN: 文字列の後の値を取得し、その値を許可リスト内のシリアル番号の 1 つと照合します。

サードパーティベンダーのデバイス証明書の形式が異なると、検証エラーが発生する可能性があります。障害の程度は、差異の程度によって異なります。ベンダー証明書がこの形式とまったく一致しない場合があります。証明書の Subject フィールドに、SN: 文字列を含む値を持つ serialNumber キーを含めることはできません。この場合、セキュア ZTP の処理は、デバイスのシリアル番号として serialNumber キーの文字列値全体（存在する場合）を使用するようにフォールバックします。次に、その値をシリアル番号の許可リストの1つと照合します。この2つの方法（文字列照合とフォールバック）は、セキュア ZTP がサードパーティ製デバイスのシリアル番号を判別するための唯一の手段です。ベンダー証明書がこの想定と大幅に異なる場合、セキュア ZTP はデバイスをまったく検証できない可能性があります。

セキュア ZTP では、所有権バウチャーに対して同様の形式が想定されます。シスコのツールは、*SerialNumber*.vcj 形式のファイル名で所有権バウチャーを生成します。ここで、*SerialNumber* はデバイスのシリアル番号です。セキュア ZTP は、ファイル名からシリアル番号を抽出し、許可リスト内のいずれかの番号との照合を試みます。マルチベンダーサポートでは、サードパーティベンダーのツールが同じ形式のファイル名で OV ファイルを生成すると想定しています。この想定が満たされない場合は、検証が失敗する可能性があります。

ZTP の実装の決定

ベストプラクティスとして、使用するデバイスに最も安全な実装を常に選択してください。ただし、ZTP には実装のさまざまな選択肢があり、コスト対メリットのトレードオフを事前に検討に値します。

- **クラシック ZTP を使用する場合**：クラシック ZTP はセキュア ZTP よりも簡単に実装できます。PDC、所有者証明書、または所有権バウチャーは必要ありません。デバイスとサーバーの検証が厳密ではなくなり、設定も複雑でないため、処理エラーの影響を受けにくくなります。セキュア ZTP と PnP ZTP ではサポートされていないため、シスコのデバイスが 7.3.1 より前の IOS-XR バージョンを実行している場合は、これが唯一の選択肢となります。クラシック ZTP にはデバイスのシリアル番号チェックが含まれていますが、トランスポート層では安全ではありません。リモートデバイスへのルートがメトロネットワークまたはその他のセキュアでないネットワークを通過する場合は推奨されません。

- **セキュア ZTP を使用する場合**：パブリックネットワークを通過する必要があり、セキュア ZTP をサポートするデバイスがある場合は、セキュア ZTP を使用します。この ZTP が提供する追加のセキュリティには、クラシック ZTP よりも複雑な設定が必要です。設定タスクを初めて使用する場合、この複雑さが原因で処理エラーが発生しやすくなります。セキュア ZTP の設定には、デバイスの製造元からの証明書と所有権バウチャーも必要です。クラシック ZTP はサードパーティ製ハードウェアをサポートしていないため、サードパーティ製のデバイスを使用している場合に使用します。サードパーティ製デバイスとそのソフトウェアは、RFC 8572 と 8366 に 100% に準拠している必要があります。サードパーティ製のデバイスのデバイス証明書には、デバイスのシリアル番号が含まれている必要があります。サードパーティ所有権バウチャーは、デバイスのシリアル番号をファイル

名として使用する形式である必要があります。シスコは、すべてのサードパーティ製デバイスとのセキュア ZTP 互換性を保証することはできません。サードパーティ製デバイスのサポートの詳細については、「ZTP でのプラットフォームサポート（216 ページ）」を参照してください。

- **PnP ZTP を使用する場合**：Cisco PnP プロトコルをサポートする Cisco IOS-XE デバイスのセキュアプロビジョニングの設定が必要な場合は、PnP ZTP を使用します。設定はセキュア ZTP よりも簡単ですが、クラシック ZTP よりは若干複雑です。そのため、ネットワークデバイスがこれらの基本要件を満たしている場合に最適です。
- **イメージデバイスで ZTP を使用**：ZTP モードのいずれかを使用する場合、ソフトウェアイメージを指定する必要はありません。この機能を使用すると、ソフトウェアイメージがすでにインストールされている 1 台以上のデバイスをリモートの場所に出荷できます。その後、これらのデバイスに接続し、リモートで ZTP 処理をトリガーできます。設定方法に応じて、次を適用できます。
  - 設定のみ
  - 複数の設定を持つ 1 つ以上のイメージまたは SMU。

  セキュア ZTP は、事前設定、Day 0、および設定後のスクリプト実行機能を提供するため、事前にイメージ化されたデバイスにより高い柔軟性が実現します。クラシック ZTP モードとセキュア ZTP モードの両方で設定ファイルをチェーンできますが、追加のスクリプトを実行するクラシック ZTP の機能は、特定のデバイスで許可されるスクリプトの実行のサポートに制限されます。PnP ZTP は CLI コマンドのみを実行でき、スクリプトを実行することはできません。

  いずれの場合も、結果としてデバイスがオンボーディングされます。Cisco Crosswork にオンボーディングされた後は、ZTP を使用してデバイスを再設定することは避けてください（詳細については、「オンボーディング済み ZTP デバイスの再設定（285 ページ）」を参照してください）。
- **設定の整理**：デバイス間で可能な限り一貫した設定を維持します。一貫性により、問題の解決が容易になります。新しいデバイスをオンラインにするために実行する必要がある追加設定の量を最小限に抑えます。また、デバイスを再設定またはアップグレードする際に留意すべき「特別な」事項の数を減らします。最初に、同じデバイスファミリの同じロールを持つすべてのデバイスの基本設定が同じか、または類似していることを確認します。

  デバイスが果たす役割の定義方法は、組織、その運用方法、およびネットワーク環境の複雑さによって異なります。たとえば、組織が金融サービス企業であるとします。路上の ATM、標準的な営業時間中に開いている小売店、民間のトレーディングオフィスの 3 つのタイプのブランチがあります。各タイプのブランチのすべてのデバイスを対象とする 3 つのセットの基本プロファイルを定義できます。これらプロファイルのそれぞれに設定ファイルをマッピングできます。

  一貫性を強化するもう 1 つの方法は、同様のタイプのデバイス用に基本的なスクリプト設定を作成し、スクリプトロジックを使用して、特別なロールを持つデバイス用の他のスクリプトを呼び出す（チェーンする）ことです。Classic ZTP を使用している場合、スクリプトは指定した設定ファイルにあります。この例を拡張すると、そのスクリプトは共通の設

定を適用し、ブランチタイプに応じて他のスクリプトをダウンロードして適用します。セキュア ZTP を使用する場合は、Day 0 設定スクリプトに加えて、事前設定および設定後のスクリプトを指定できるため、柔軟性が高まります。

ZTP の処理ロジック

Cisco Crosswork ZTP の処理は、クラシック ZTP、セキュア ZTP、または PnP ZTP のいずれを実装するかによって異なります。このトピックの次のセクションでは、各 ZTP モードの ZTP 処理の各ステップについて詳しく説明します。

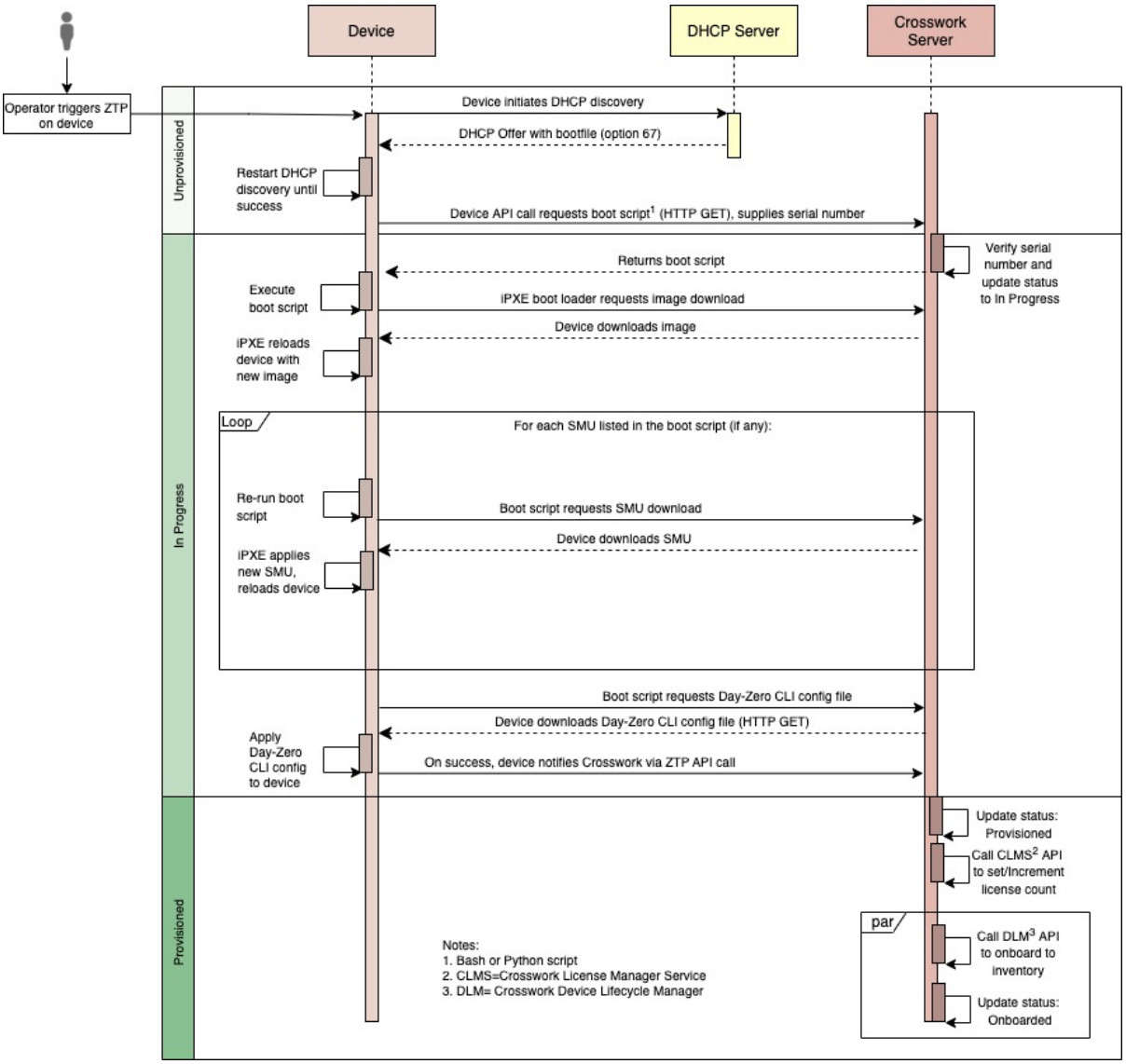
デバイスのリセットまたはリロードによって開始されると、ZTP プロセスは自動的に進行します。また、Cisco Crosswork は、[ゼロタッチデバイス（Zero Touch Devices）] ウィンドウを更新し、各デバイスで処理が完了したときに示すステータスメッセージも表示します。各セクションの図は、これらの状態遷移を、各図の左側にある緑の陰影のブロックで示しています。導入準備状態に到達するのは ZTP 処理の最後にのみ発生するため、導入完了状態への遷移は表示されません。

図で示されているように、ZTP で使用する構成スクリプトは、Cisco Crosswork API コールを使用して、デバイスの状態変化を Cisco Crosswork に報告する必要があります。構成がこれに失敗した場合、Crosswork は発生した状態の変更を登録できず、ZTP のプロビジョニングとオンボーディングに失敗します。これらのコールの例を確認するには、**[デバイス管理（Device Management）] > [ZTP 設定ファイル（ZTP Configuration Files）]** を選択し、[サンプルスクリプトのダウンロード（Download Sample Script）] をクリックします。

クラシック ZTP の処理

次の図に、クラシック ZTP がデバイスのプロビジョニングとオンボーディングに使用する処理ロジックを示します。

図 *26* : クラシック *ZTP* の処理

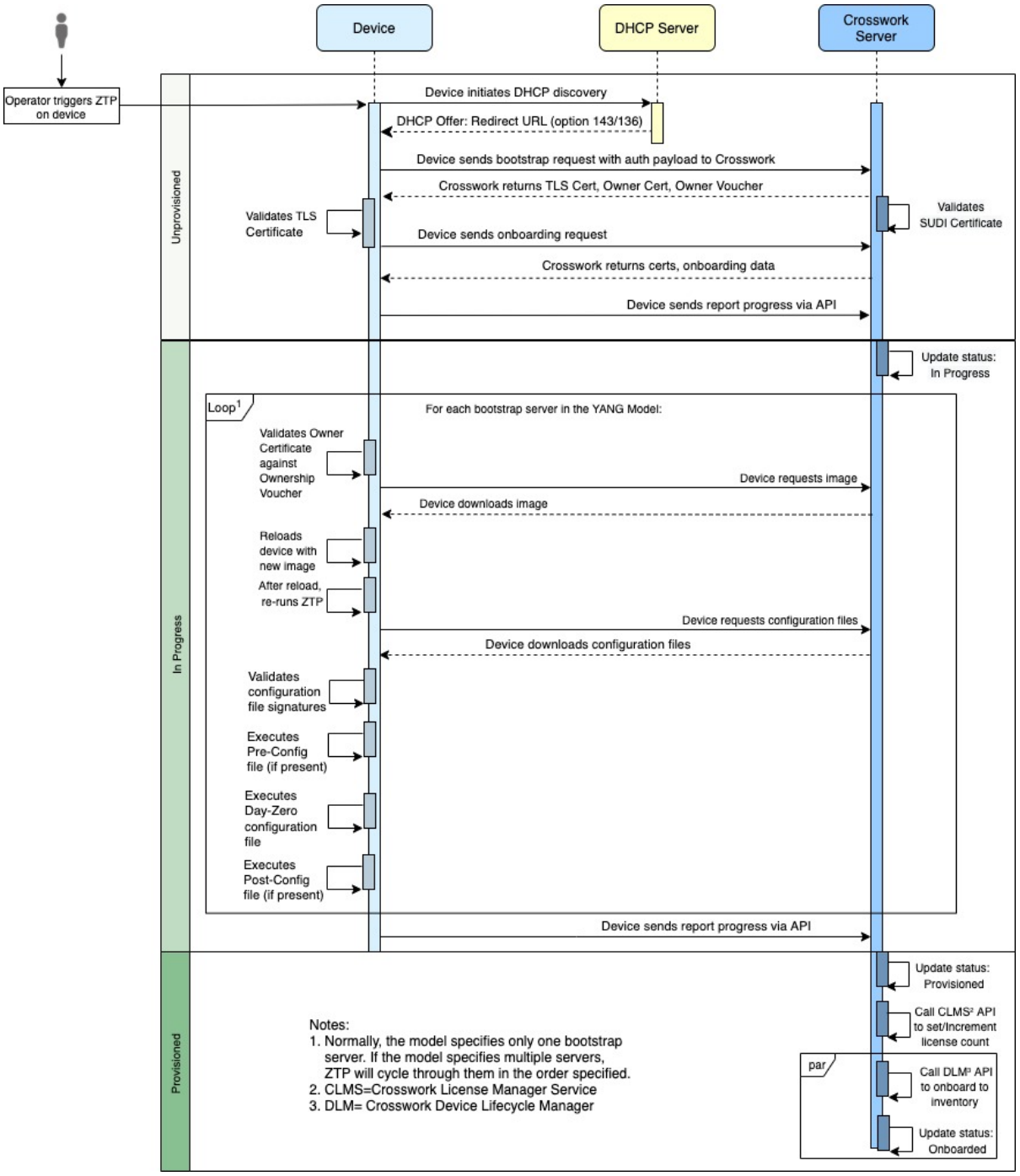


DHCPサーバーは、デバイスのシリアル番号に基づいてデバイスのアイデンティティを確認してから、ブートファイルとイメージのダウンロードを提供します。ZTPがデバイスをイメージ化すると、デバイスは設定ファイルをダウンロードし、実行します。

セキュア ZTP の処理

次の図に、セキュア ZTP がデバイスのプロビジョニングとオンボーディングに使用するプロセスロジックを示します。

図 *27 :* セキュア *ZTP* の処理



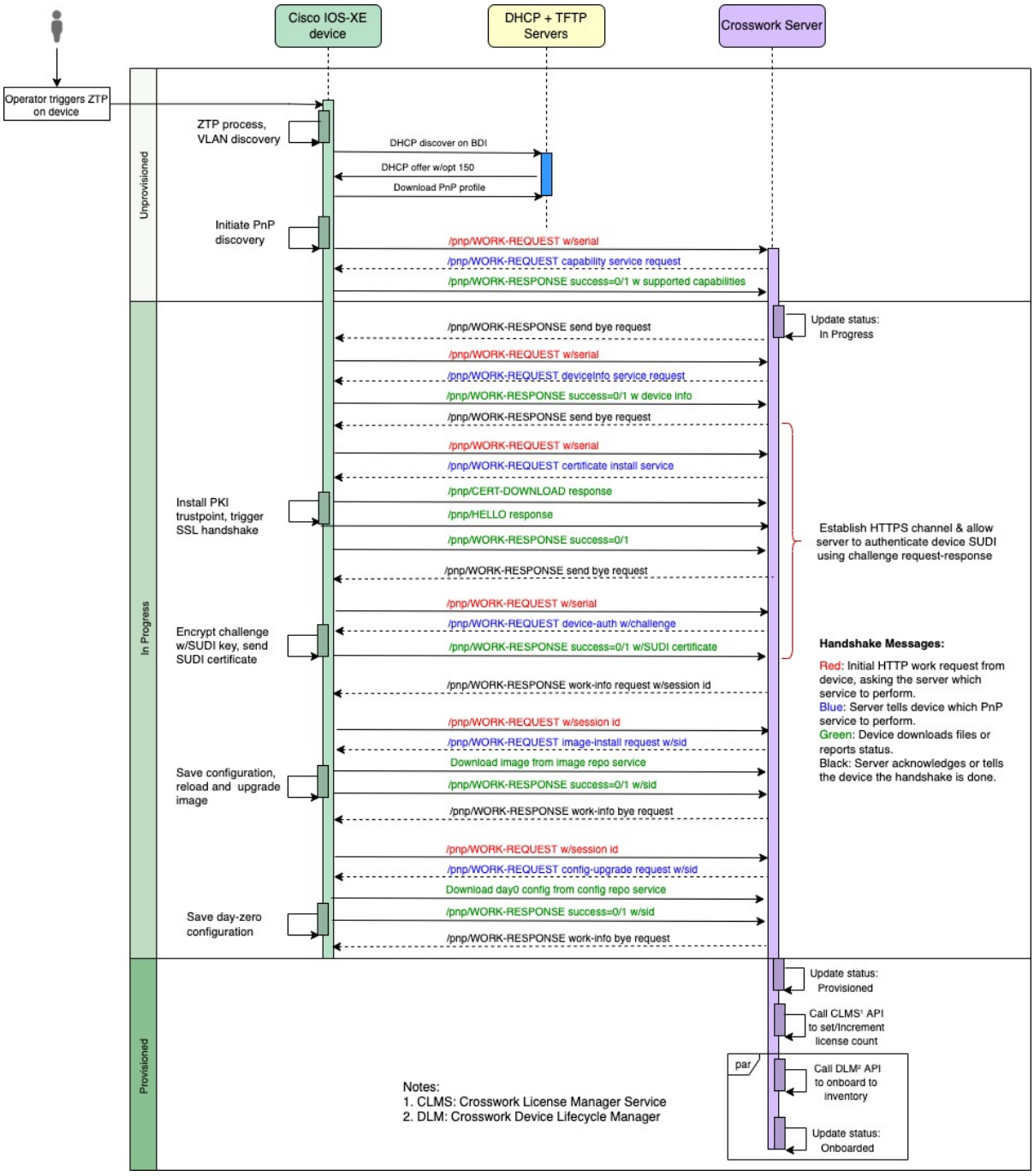
デバイスと ZTP ブートストラップサーバーは TLS/HTTPS を介してデバイスとサーバー証明書でセキュアな一意のデバイス識別子（SUDI）を使用し、相互に認証します。セキュアな HTTPS チャネルを介して、ブートストラップサーバーはデバイスに署名付きイメージと設定アーティファクトをダウンロードさせます。これらのアーティファクトは、RFC 8572 YANG スキーマ（https://tools.ietf.org/html/rfc8572#section-6.3）に準拠する必要があります。デバイスは新しい

イメージ（存在する場合）をインストールしてリロードすると、設定スクリプトをダウンロードして実行します。

PnP ZTP の処理

次の図に、PnP ZTP がデバイスのプロビジョニングとオンボーディングに使用するプロセスロジックを示します。

図 *28 : PnP ZTP* の処理



オペレータが PnP ZTP 処理をトリガーすると、デバイスは VLAN 検出を実行し、DHCP 検出が開始される BDI インターフェイスを作成します。DHCP 検出の一部として、デバイスは DHCP オプション 150 設定を使用して外部 TFTP サーバーの IP アドレスも取得します。デバイスは、認証なしで TFTP サーバーから PnP プロファイルをダウンロードし、デバイスの実行コンフィギュレーションにコピーします。PnP プロファイルは CLI テキストファイルです。プロファイ

ルは、デバイスの PnP エージェントをアクティブにし、ポート 30620 上で組み込み Crosswork PnP サーバーに作業要求を HTTP 経由で送信します。次に、PnP サーバーはデバイスのシリアル番号を Crosswork のシリアル番号の「許可」リスト（以前に Crosswork にアップロードしたもの）と照合して検証し、PnP 機能サービス要求を開始します。デバイスからの PnP 作業応答が成功すると、デバイスのプロビジョニングステータスが [プロビジョニングなし（Unprovisioned）] から [進行中（In Progress）] に変更されます。その後、PnP サーバーは、デバイス情報、証明書のインストール、イメージのインストール、設定のアップグレードなどの要求を含む一連のサービス要求を開始します。これらの各サービス要求には、PnP サーバーと PnP エージェント間の 4 ウェイハンドシェイクが含まれます。証明書インストール要求の一部として、Crosswork PnP サーバーはその証明書をデバイスと共有します。デバイスにこのトラストポイントを正常にインストールすると、PnP プロファイル設定が変更され、Crosswork で HTTPS とポート 30603 の使用が開始されます。後続のイメージと設定のダウンロード要求は、HTTPS を使用してトランザクションを保護します。現在、デバイスでは SUDI 証明書認証はサポートされていません。デバイスが新しいイメージ（存在する場合）をダウンロードしてインストールし、リロードすると、PnP プロセスは引き続き CLI 設定ファイルをダウンロードし、デバイスの実行コンフィギュレーションに適用します。デバイスのステータスが [プロビジョニング済み（Provisioned）] に設定され、ライセンス数が Crosswork で更新されます。デバイスのステータスは [オンボーディング済み（Onboarded）] に設定され、デバイスは PnP サーバーとの通信を停止します。

ZTP と評価ライセンス

すべての Cisco Crosswork アプリケーションは、ライセンスなしで 90 日間使用できます。ユーザーがシステムにログインするたびに、Crosswork はトライアル期間の残りの日数を示すバナーを表示します。トライアルが期限切れになると、バナーにその旨が表示されます。その時点で、それ以上のデバイスでは ZTP オンボーディングプロセスを完了できなくなります。ZTP ライセンスは、ブロック単位で販売されるライセンスによる消費ベースモデルに従います。ZTP を使用してデバイスをオンボーディングする機能を取り戻すには、トライアル期間中にオンボーディングしたデバイスの数と、今後 ZTP でオンボーディングする予定の新しいデバイスの数の両方をカバーするライセンスブロックをインストールする必要があります。たとえば、トライアル中に 10 台のデバイスをオンボーディングしてから、91 日目に10 台のデバイスのライセンスバンドルをインストールした場合、使用できるライセンスは残りません。別のデバイスをオンボーディングする前に、少なくとも 1 つのライセンスブロックをインストールする必要があります。必要に応じて、ライセンスブロックを追加できます。オペレータは、ライセンスの消費をモニターして、予期せぬライセンス不足を回避する必要があります。使用済みのライセンスの数と、まだ使用可能なライセンスの数を確認するには、Cisco Smart Licensing のサイトを確認します。

オンボーディング済みの ZTP デバイスは、常に次のいずれかに関連付けられます。

- シリアル番号、または
- Option 82 ロケーション ID 属性の値（リモート ID と回線 ID）。

シリアル番号とロケーション ID によって「許可」リストが形成されます。ZTP は、デバイスをオンボーディングしてライセンスを割り当てることを決定するときに、このリストを使用し

ます。オンボーディング済みの ZTP デバイスをインベントリから削除し、後で再度オンボーディングする場合は、同じシリアル番号またはロケーション ID を使用します。別のシリアル番号やロケーション ID を使用すると、ライセンスが余分に消費される場合があります。現在のリリースでは、このシナリオの回避策は提供されていません。いずれの場合も、同じシリアル番号またはロケーション ID を持つ 2 つの異なる ZTP デバイスを同時にアクティブにすることはできません。

ZTP 設定のワークフロー

ゼロタッチプロビジョニングでは、ZTP ブートと設定をトリガーする前に、次の設定タスクを最初に実行しておく必要があります。

1. 環境が、セキュリティ、プロバイダ設定、およびデバイス接続に関する ZTP の前提条件を満たしていることを確認します。ZTP の前提条件を満たす （226 ページ）を参照してください
2. ZTP が処理に必要とするアセットのタイプを組み立てて Crosswork に読み込ませます。使用したい ZTP モードやオンボーディングするデバイスによっては、最低 3 種類から最高 8 種類のアセットを用意する必要があります。ZTP アセットの組み立てと読み込み （227 ページ）を参照してください
3. オプション：ZTP プロファイルを作成します。これは、オンボーディングプロセス中にデバイスのイメージングと構成を簡素化および標準化するのに役立ちます。ZTP プロファイルの作成 （250 ページ）を参照してください
4. ZTP デバイスエントリを作成します。ZTP は、デバイスを Cisco Crosswork デバイスインベントリにオンボーディングするときに、これらのデバイスエントリをデータベースの「アンカー」として使用します。オンボーディングするデバイスが多数ある場合は、CSV ファイル（「ZTP デバイスエントリのアップロード （259 ページ）」を参照）をインポートしてエントリを一括で作成します。オンボーディングするデバイスが少数の場合は、Cisco Crosswork の UI（「単一 ZTP デバイスエントリの作成 （258 ページ）」を参照） を使用してこれらのエントリを 1 つずつ作成するほうが便利です。Crosswork API を使用してデバイスをオンボードすることもできます（Cisco Crosswork DevNet ページの ZTP API リファレンスを参照）。

このセクションの残りのトピックでは、これらの各タスクを実行する方法について説明します。

ZTP の前提条件を満たす

ZTP との互換性を確保するために、Cisco Crosswork のインストールは次の前提条件を満たしている必要があります。

- ZTP にデバイスを Cisco NSO へオンボーディングさせる場合は、NSO を Cisco Crosswork プロバイダとして 設定します。必ず NSO プロバイダのプロパティキーを `forward` に、プロパティ値を `true` に設定してください。

- Cisco Crosswork クラスタノードはデバイスから、ノードはデバイスから、アウトオブバンド管理ネットワークまたはインバウンド データ ネットワークのいずれかを介して到達可能である必要があります。これらの要件の範囲の一般的な表示については、『*Cisco Crosswork Infrastructure and Applications Installation Guide*』の「Network Requirements」の項にあるネットワーク図を参照してください。このタイプのアクセスを有効にするには、ファイアウォール設定変更が必要な場合があります。
- Crosswork ZTP を使用してオンボーディングする Crosswork クラスタノードとデバイスがまったく異なるサブネットにある場合は、Crosswork ノードからデバイスサブネットへの 1 つ以上の静的ルートを設定する必要があります。メインメニューからこれを行うには、**[管理（Administration）]** > **[設定（Settings）]** > **[静的ルート（Static Routes）]** を選択します。[+] をクリックし、接続先サブネットの IP アドレスとマスク（スラッシュ表記）を入力して、[追加（Add）] をクリックします。
- PnP ZTP の使用を計画している場合は、TFTP サーバーを Cisco Crosswork プロバイダーとして追加する必要があります。TFTP サーバーは、次のような汎用プロファイルを使用して設定できます。

```
pnp profile test-profile
    transport http ipv4 192.168.100.205 port 30620
```

ZTP アセットの組み立てと読み込み

「ZTP アセット」という用語は、次のチェックリストに示されているソフトウェアと構成ファイル、ログイン情報、証明書、およびその他のアセットを指します。準備して Crosswork に読み込ませる必要があるアセットの数は、使用する ZTP モードに必要かどうか、デバイスのオンボーディングを開始したときのデバイスの状態、およびその他の要因によって異なります。

便宜上、これらのアセットをチェックリストに示されている順序で準備して読み込むことをお勧めします。ソフトウェアイメージなどのオプションのアセットを含む各アセットを準備して読み込む方法の詳細については、チェックリストの最後の列にあるリンクされたトピックを参照してください。

多くの組織は、シリアル番号や構成ファイルなどの ZTP アセットのライブラリを維持しています。組織にこのようなライブラリがある場合は、デスクトップから簡単にアクセスできるようにしてください。これにより、ZTP の設定を簡単に実行できます。

IOS-XR デバイスでセキュア ZTP を使用する背景については、『*System Setup and Software Installation Guide for Cisco NCS 540 Series Routers, IOS XR Release 7.3.x*』の「Securely Provision Your Network Devices」の章を参照してください。

Cisco Crosswork は、IOS-XR デバイス用に、Cisco Crosswork を認証局として独自の TLS 証明書を提供しています。IOS-XR デバイスは Crosswork TLS サーバー証明書で X.509 検証を実行しないため、独自の TLS CA 証明書チェーンを提供またはアップロードする必要はありません。

表 *13 : ZTP* 資産チェックリスト

順序	アセット	クラシック ZTP	セキュア ZTP	PnP ZTP	詳細については、次を参照してください。
1	ソフトウェア イメージ	オプション	オプション	オプション	デバイスにソフトウェアイメージがインストールされていない場合は、ソフトウェアイメージが必要です。ソフトウェアイメージの検索と読み込み（229 ページ）
2	設定	**必須**	**必須作業です**。複数の設定をサポートしています。	**必須**	構成ファイルと読み込み（230 ページ）
3	ソフトウェア メンテナンス アップグレード（SMU）	オプション	オプション	サポート対象外	SMU の検索と読み込み（242 ページ）
4	デバイスのクレデンシャル	**必須**	**必須**	**必須**	ZTP でのクレデンシャル プロファイルの作成（242 ページ）
5	シリアル番号	**必須**	**必須**	**必須**	デバイスのシリアル番号の検索と読み込み（244 ページ）
6	ピン留めされたドメイン証明書（PDC）、所有者証明書（OC）、および所有者キー	未使用	**必須**	未使用	PDC、所有者証明書、および所有者キーを更新する（245 ページ）。
7	所有権バウチャー	未使用	**必須**	未使用	所有権バウチャーのリクエストと読み込み（248 ページ）。

順序	アセット	クラシック ZTP	セキュア ZTP	PnP ZTP	詳細については、次を参照してください。
8	SUDI ルート証明書	未使用	必須	IOS-XE デバイスのみに必要	SUDI ルート証明書の準備と読み込み（249 ページ）

ソフトウェアイメージの検索と読み込み

ソフトウェアイメージは、ネットワークデバイスの機能を可能にする、インストール可能なネットワーク オペレーティング システム ソフトウェア（Cisco IOS-XR、または PnP ZTP の場合は Cisco IOS-XE など）を含むファイルです。

ソフトウェアイメージの読み込みは、すべてのZTPモードでオプションですが、オンボーディングしているデバイスにソフトウェアイメージがインストールされていない場合は必須です。すでにイメージ化されているデバイスにソフトウェアイメージを適用する必要はありません。イメージを読み込まずに、構成ファイルをデバイスに適用することもできます。イメージの読み込みは、オンボードするデバイスにイメージがインストールされていない場合、またはデバイスのオンボードと同時にネットワーク OS をアップグレードする場合にのみ必要です。

シスコは、IOS-XR イメージを TAR、ISO、BIN、または RPM ファイルとして配布しています。シスコでは、IOS-XE イメージを BIN ファイルとして配布しています。各シスコイメージファイルは、特定のデバイスプラットフォームまたはファミリの特定のネットワーク OS の単一リリースを表します。

[シスコサポート & ダウンロード（Cisco Support & Downloads）]https://www.cisco.com/c/en/us/support/index.html ページからソフトウェア イメージ ファイルをダウンロードします。ダウンロード中に、イメージの MD5 チェックサムを記録します。アップロードするイメージの独自の MD5 チェックサムを生成することもできます。Cisco Crosswork は MD5 チェックサムを使用してソフトウェア イメージ ファイルの整合性を検証します。

ソフトウェア イメージ ファイルを一度に 1 つずつ Cisco Crosswork に読み込ませ、読み込み中に各ソフトウェア イメージ ファイルの MD5 チェックサムを入力します。

ソフトウェアイメージを Cisco Crosswork に読み込ませるには、次の手順を実行します。

1. Cisco Crosswork を起動します。
2. メインメニューから、**[デバイス管理（Device Management）]** > **[ソフトウェアイメージ（Software Images）]**を選択します。
3. をクリックします。 
4. 入力するか、または**[参照（Browse）]**をクリックし、アップグレードするコンポーネントのソフトウェア イメージ ファイルを選択しますプロンプトが表示されたら、ファイルの MD5 チェックサムを入力します。
5. **[追加（Add）]** をクリックして、ソフトウェア イメージ ファイルの追加を終了します。

6. 計画された ZTP 実行で使用されるすべてのソフトウェア イメージ ファイルを読み込むまで、必要に応じて繰り返します。

構成ファイルと読み込み

構成ファイルは、特定のデバイスにインストールされているソフトウェアイメージの機能を構成するスクリプトファイルです。これらはすべての ZTP モードに必要です。

クラシック ZTP とセキュア ZTP モードで使用される構成ファイルは、Linux シェルスクリプト（SH）、Python スクリプト（PY）、または ASCII テキストファイル（TXT）に保存されたデバイスのオペレーティングシステムの CLI コマンドです。Cisco IOS-XR デバイスで、クラシック ZTP とセキュア ZTP のみを使用する場合は、構成ファイルを使用して、SMU を使用してインストールされているネットワーク OS ソフトウェアバージョンをアップグレードすることもできます（「SMU の検索と読み込み （242 ページ）」を参照）。

従来の ZTP は、デバイスごとに 1 つの day-zero 構成ファイルのみをサポートします。セキュア ZTP では、オンボーディング時に最大 3 つの構成ファイルを適用できます。1 つは事前設定の準備用、2 つ目は Day 0 設定またはメイン設定、3 つ目は Day 0 設定後に適用される設定後ファイルです。Day 0 設定のみが必須です。アプリケーションの順序は固定されています。

Cisco PnP ZTP は、Cisco ASR 900 デバイスと Cisco NCS 520 デバイスでは Day 0 設定 TXT ファイルのみをサポートします。PnP ZTP 設定ファイルでは、IOS-XE CLI コマンドを使用する必要があります。PnP ZTP は、Linux シェル（SH）または Python（PY）スクリプトファイルをサポートしていません。

Cisco Crosswork に設定ファイルを 1 つずつアップロードします。

組織またはコンサルタントが構成ファイルを作成します。次のセクションでは、ZTP モードのいずれかを使用してデバイスをオンボーディングするときに使用する構成ファイルを準備するためのガイドラインと、これらのファイルを Cisco Crosswork に読み込む方法について説明します。

設定例ファイルのダウンロード

構成スクリプトファイルの内容は、使用するデバイスと組織での使用方法によって大きく異なります。したがって、このドキュメントでは使用可能なすべてのオプションを完全には説明していません。

覚えておくべき主なガイドラインは次のとおりです。

1. カスタム設定コードは、デフォルトとカスタムの両方の置換可能（または「プレースホルダ」）パラメータを使用できます。これにより、デバイスエントリを一括でインポートするとき、または一度に 1 つずつ作成するときに、[設定属性（Configuration Attributes）] フィールドを使用してランタイム時に値を挿入できます。

2. 必要に応じて、新しいカスタム置換可能パラメータを作成できます。既定のパラメータと同じ名前を使用せず、このトピックで説明する変数の命名規則に従っていれば、任意の名前を付けることができます。デフォルトの置き換え可能なパラメータを使用する場合、デバイスエントリの [構成属性（Configuration Attributes）] フィールドで設定した値の代わり

に、このトピックの「設定ファイルでデフォルトの置き換え可能なパラメータを使用する」セクションで説明されているソースからランタイム値が挿入されます。

3. 置換可能パラメータの名前は大文字と小文字が区別され、中カッコとドル記号を含める必要があります。スペースを含めることはできません（代わりにアンダースコアを使用）。
4. すべてのカスタム置換可能パラメータのランタイム値が[設定属性（Configuration Attributes）]フィールドに指定されていることを確認します。ランタイム値を指定しなかったカスタム置換可能パラメータが 1 つでもある場合は、デバイス設定プロセスが失敗します。
5. セキュア ZTP を使用している場合は、Day 0 設定にのみカスタム置換可能パラメータを使用できます。カスタム置換可能パラメータは、事前設定ファイルと設定後ファイルではサポートされていません。
6. 一部のタスクを実行するには、Cisco Crosswork の API コールを使用する必要があります。特に、デバイスが 1 つの ZTP 状態から別の状態に移行したときに、コードで API コールを使用して Cisco Crosswork サーバーに通知する必要があります。。
7. どの設定ファイルでも別の設定ファイルをコールして実行できますが（デバイスに正常にダウンロードできる場合）、セキュア ZTP でのみ、初期のセキュアなダウンロードの一環として個別の事前設定ファイル、設定後ファイル、および Day 0 設定ファイルを指定できます。
8. 設定ファイル名に複数のピリオドを含めることはできず、また、スペースの代わりにアンダースコアを使用する必要があります。その他のファイルの制限は、以下で説明する設定例ファイルに記載されています。

置き換え可能なパラメータと API コールの使用方法の例については、Cisco Crosswork ZTP アプリケーションに付属の Cisco IOS-XR デバイスの ZTP 構成ファイルを参照してください。Cisco Crosswork から ZTP 設定例ファイルをダウンロードするには、**[デバイス管理（Device Management）] > [ZTP 設定ファイル（ZTP Configuration Files）]** を選択し、[サンプルスクリプトのダウンロード（XR）（Download Sample Script (XR)）] をクリックします。サンプル構成スクリプトにはコメントが付けられており、より一般的に使用される API 呼び出しと置き換え可能なパラメータの例が示されています。

置換可能なパラメータの詳細については、以下のセクション「構成ファイルでのデフォルトの置換可能パラメータの使用」および「構成ファイルでのカスタムの置換可能パラメータの使用」を参照してください。

Crosswork API コールの詳細については、Cisco Crosswork の Cisco Developer Network（DevNet）サイトで利用可能な「Crosswork API References」メニューの ZTP デバイスと設定 API に関する項を参照してください。

次のセクション「サンプル ZTP 構成スクリプト」では、置き換え可能なパラメータと API の使用方法の例を示します。

設定ファイルのプレビュー

以前に Cisco Crosswork にアップロードされた設定ファイルの内容をプレビューするには、**[デバイス管理（Device Management）] > [ZTP 設定ファイル（ZTP Configuration Files）]** を選択

し、設定ファイル名をクリックします。ポップアッププレビューには、次の表に示すように、重要なコード機能のコードシンタックスのスタイルが含まれています。

表 *14 : ZTP* 設定ファイルプレビューのコードシンタックスの色

対象のコード機能	表示色
句読点、演算子、エンティティ、URL、変数、クラス名、定数	黒色
コメント	グレー
プロパティ、タグ、ブール値、関数名、シンボル	オレンジ
セレクタ、属性名、文字、組み込み、挿入	深緑
機能	パープル
キーワード、属性値	青
正規表現、重要	茶
文字列	緑
番号、イーサネットアドレス、MACアドレス	マゼンタ

設定ファイルでのデフォルトの置換可能パラメータの使用

次の表に、カスタム設定ファイルで使用できるデフォルトの置換可能パラメータを示します。実行時に、これらの各プレースホルダを Cisco Crosswork は各デバイスの適切な値に置き換えます。これらのプレースホルダの使用例については、Cisco Crosswork から設定スクリプトの例をダウンロードしてください（**[デバイス管理（Device Management）] > [ZTP 設定ファイル（ZTP Configuration Files）] > [サンプルスクリプトのダウンロード（XR）（Download Sample Script (XR)）]**）。これらのデフォルトの置き換え可能なパラメータの使用方法を示す例については、このトピックの後半のセクション「サンプル ZTP 構成スクリプト」を参照してください。

表 *15 : ZTP* 設定ファイルのデフォルトパラメータ

Cisco Crosswork が置換するプレースホルダ	使用される値
{$HOSTNAME}	ZTP デバイスエントリで指定されているデバイスのホスト名。
{$IP_ADDRESS}	ZTP デバイスエントリで指定されているデバイスの IP アドレス。
{$SSH_USERNAME}	クレデンシャルプロファイルの [ユーザー名（User Name）] フィールドの値（[接続タイプ（Connectivity Type）] が [SSH] の場合）。

Cisco Crosswork が置換するプレースホルダ	使用される値
{$SSH_PASSWORD}	クレデンシャルプロファイルの [パスワード（Password）] フィールドの値（[接続タイプ（Connectivity Type）] が [SSH] の場合）。
{$SSH_ENPASSWORD}	クレデンシャルプロファイルの [イネーブルパスワード（Enable Password）] フィールドの値（[接続タイプ（Connectivity Type）] が [SSH] の場合）。
{$SNMP_READ_COM}	クレデンシャルプロファイルの [読み取りコミュニティ（Read Community）] フィールドの値（[接続タイプ（Connectivity Type）] が [SNMPv2] の場合）。
{$SNMP_WRITE_COM}	クレデンシャルプロファイルの [書き込みコミュニティ（Write Community）] フィールドの値（[接続タイプ（Connectivity Type）] が [SNMPv2] の場合）。
{$SNMP_SEC_LEVEL}	クレデンシャルプロファイルの [セキュリティレベル（Security Level）] フィールドの値（[接続タイプ（Connectivity Type）] が [SNMPv3] の場合）。
{$SNMP_USERNAME}	クレデンシャルプロファイルの [ユーザー名（User Name）] フィールドの値（[接続タイプ（Connectivity Type）] が [SNMPv2] または [SNMPv3] の場合）。
{$SNMP_AUTH_TYPE}	クレデンシャルプロファイルの [ユーザー名（User Name）] フィールドの値（[接続タイプ（Connectivity Type）] が [SNMPv3] で [セキュリティレベル（Security Level）] が [AUTH_NO_PRIV] または [AUTH_PRIV] の場合）。
{$SNMP_AUTH_PASS}	クレデンシャルプロファイルの [ユーザー名（User Name）] フィールドの値（[接続タイプ（Connectivity Type）] が [SNMPv3] で [セキュリティレベル（Security Level）] が [AUTH_NO_PRIV] または [AUTH_PRIV] の場合）。
{$SNMP_PRIV_TYPE}	クレデンシャルプロファイルの [ユーザー名（User Name）] フィールドの値（[接続タイプ（Connectivity Type）] が [SNMPv3] で [セキュリティレベル（Security Level）] が [AUTH_PRIV] の場合）。
{$SNMP_PRIV_PASS}	クレデンシャルプロファイルの [プライバシーパスワード（Priv Password）] フィールドの値（[接続タイプ（Connectivity Type）] が [SNMPv3] で [セキュリティレベル（Security Level）] が [AUTH_PRIV] の場合）。

設定ファイルでのカスタム置換可能パラメータの使用

次の例に示すように、独自のカスタム置換可能パラメータを設定ファイルに作成できます。この例に示すように、同じ設定ファイル内でカスタムとデフォルトの置換可能パラメータを使用できます。

次の条件を満たしている限り、任意の名前をカスタム置換可能パラメータに割り当てることができます。

- 指定された変数定義形式（{$MyParm} など）に従う。
- パラメータ名のスペースをアンダーライン文字に置き換える。
- デフォルトの置換可能パラメータと同じ名前や大文字を再使用しない。
- デバイスエントリファイルの [設定属性（Configuration Attributes）] フィールドに、各カスタムパラメータの値を入力する。次の CLI 設定のサンプルファイルとそのカスタムパラメータを ZTP デバイスエントリファイルで使用するには、ZTP デバイスエントリファイルの各デバイスの [設定属性（Configuration Attributes）] フィールドで **{$LOOPBACK0_IP}** カスタムパラメータの値を指定する必要があります。カスタムパラメータの値を指定し忘れた場合は、設定が失敗します。

セキュア ZTP を使用している場合は、Day 0 設定ファイルのみでカスタム置換可能パラメータがサポートされます。

このスクリプトの例の最初の行は、IOS-XR デバイスの CLI スクリプトで必要です。これにより、ZTP はファイルが CLI スクリプトか bash/Python スクリプトかを確認できます。必要に応じてバージョン番号を更新してください。IOS-XE デバイスの場合、このような行は必要ありません。

図 *29 :* 置換可能パラメータが混在する *IOS-XR CLI* 設定スクリプトの例

```
!! IOS XR Configuration 7.3.1
!
hostname {$HOSTNAME}
username {$SSH_USERNAME}
 group root-lr
 group cisco-support
 password 0 {$SSH_PASSWORD}
!
cdp
!
line console
exec-timeout 0 0
!
line default
exec-timeout 0 0
session-timeout 120
!

call-home
 service active
 contact smart-licensing
 profile CiscoTAC-1
  active
  destination transport-method http
 !
!
```

```
interface Loopback0
 ipv4 address {$LOOPBACK0_IP} 255.255.255.255
!
interface MgmtEth0/RP0/CPU0/0
 description OOB Management ZTP
 ipv4 address {$IP_ADDRESS}
!
end
```

ZTP 設定スクリプトの例

このセクションでは、ZTP の構成スクリプトの例を示します。

図 *30 : IOS XR* デバイスのクラシック *ZTP Day 0* 構成スクリプト

```
#!/bin/bash

################################################################################
#
# ztpSampleScriptFile.sh
#
# Purpose: This sample script is required to notify Crosswork of the status of
# ZTP processing on an IOS XR device, and to update the device's IP address and
# hostname in Crosswork. It is also used to download a day0 config file from
# Crosswork config repository and apply this initial configuration to the device.
#
# To use: Modify the sample script as needed, following the comment guidance.
# Then upload the modified script to the Crosswork config repository.
# Next, copy the URL of this file from the repository and set that
# value in the DHCP server boot filename for ZTP config download. When ZTP is
# triggered on the device, it will download and run the script, then notify
# Crosswork.
#
# Replace the following variables with valid values & upload to Crosswork config
# repository. Sample values are provided for reference.
# - XRZTP_INTERFACE_NAME: e.g., MgmtEth0/RP0/CPU0/0 interface where ZTP triggered
# - CW_HOST_IP: Crosswork VM management or data network IP address
# - CW_PORT: 30604 for HTTP & 30603 only for HTTPS download of config file
# - CW_CONFIG_UUID: Replace with UUID of day0 config file from Crosswork repo,
#   assuming user has already uploaded device day-0 config file.
#
# This script has been tested and is known to work on Cisco NCS5501, NCS540l,
# ASR9901, and 8800 routers.
#
################################################################################


export LOGFILE=/disk0:/ztp/customer/user-script.log

XRZTP_INTERFACE_NAME="MgmtEth0/RP0/CPU0/0"
# ZTP helper library is assumed to be installed in IOS-XR linux shell
source /pkg/bin/ztp_helper.sh
interfacedata=$(xrcmd "show interface ${XRZTP_INTERFACE_NAME}")

CW_HOST_IP="<EnterIPv4AddressHere>"
CW_PORT="30604"
CW_CONFIG_UUID="e04661f8-0169-4ad3-82b8-a7c26c4f2565"

# Send logging information to log file on device disk0:/ztp/user-script.log
function ztp_log() {

    echo "$(date +"%b %d %H:%M:%S") "$1 >> $LOGFILE
}
```

```
#
# Get chassis serial number of the device, required by ZTP process.
# This works on Cisco NCS5501, NCS540l, 8800 series routers.
#
function get_serialkey(){

    local sn=$(dmidecode | grep -m 1 "Serial Number:" | awk '{print $NF}');
    if [ "$sn" != "Not found" ]; then
           ztp_log "Serial $sn found.";
           # The value of $sn from dmidecode should be same as serial number
           # of XR device chassis.
           DEVNAME=$sn;
           return 0
    else
        ztp_log "Serial $sn not found.";
        return 1
    fi
}

#
# Get chassis serial number of the device, required by ZTP process.
# This is tested and works on Cisco ASR 9901, but not other devices.
#
function get_serialkey_asr9901(){

     udi=$(xrcmd "show license udi")
     sn="$(cut -d':' -f4 <<<"$udi")"
     pid="$(cut -d':' -f3 <<<"$udi")"
     pid="$(cut -d',' -f1 <<<"$pid")"
     echo "Serial Number $sn"
     echo "product id $pid"
}

#
# Get IP address and subnet mask from device. IP address is assigned from DHCP
# server on interface where ZTP was triggered.
#
function get_ipaddress(){

    local ipvar=($(echo $interfacedata | awk -F "Internet address is " '{sub(/
.*/,"",$2);print $2}'));
    local ipv4addr=$(xrcmd "sh run interface ${XRZTP_INTERFACE_NAME} | i ipv4 address"
| awk '{print $3}')
    local ipv6addr=$(xrcmd "sh run interface ${XRZTP_INTERFACE_NAME} | i ipv6 address"
| awk '{print $3}')
    local ipaddress=($(echo $ipvar | awk -F "/" '{sub(/ .*/,"",$1);print $1}'));
    local mask=($(echo $ipvar | awk -F "/" '{sub(/ .*/,"",$2);print $2}'));
    local maskv6=($(echo $ipv6addr | awk -F "/" '{sub(/ .*/,"",$2);print $2}'));

    ztp_log "### Value of interfacedata => $interfacedata ###"
    ztp_log "### Value of ipvar => $ipvar ###"
    ztp_log "#####IPv4 address $ipaddress and mask $mask found. #####";

    IPADDR=$ipaddress
    MASK=$mask
    MASKV6=$maskv6

    return 0
}

#
# Fetch hostname from device configuration.
#
```

```
function get_hostname(){

    hostnamedata=$(xrcmd "show running-config hostname")
    local hostname=($(echo $hostnamedata | awk -F "hostname " '{sub(/ .*/,"",$2);print
$2}'));

    ztp_log "#####hostname $hostname found.";
    HOSTNAME=$hostname;
    return 0;
}

#
# Download day-0 config file from Crosswork config repository using values
# set for CW_HOST_IP, CW_PORT and CW_CONFIG_UUID.
# The MESSAGE variable is optional, can be used to display a suitable message
# based on the ZTP success/failure log.
#
function download_config(){

    ztp_log "### Downloading system configuration ::: ${DEVNAME} ###";
    ztp_log "### ip address passed value ::: ${IPADDR} ###";
    ip netns exec global-vrf /usr/bin/curl -k --connect-timeout 60 -L -v --max-filesize
 104857600
http://${CW_HOST_IP}:${CW_PORT}/crosswork/configsvc/v1/configs/device/files/${CW_CONFIG_UUID}
 -H X-cisco-serial*:${DEVNAME} -H X-cisco-arch*:x86_64 -H X-cisco-uuid*: -H
X-cisco-oper*:exr-config -o /disk0:/ztp/customer/downloaded-config 2>&1

    if [[ "$?" != 0 ]]; then
        STATUS="ProvisioningError"
        ztp_log "### status::: ${STATUS} ###"
        ztp_log "### Error downloading system configuration, please review the log ###"
        MESSAGE="Error downloading system configuration"
    else
        STATUS="Provisioned"
        ztp_log "### status::: ${STATUS} ###"
        ztp_log "### Downloading system configuration complete ###"
        MESSAGE="Downloading system configuration complete"
    fi
}

#
# Apply downloaded configuration to the device and derive ZTP status based on
# success/failure of ZTP process. The MESSAGE variable is optional, can be used
# to display a suitable message based on the ZTP success/failure log.
#
function apply_config(){
    ztp_log "### Applying initial system configuration ###";
   xrapply_with_reason "Initial ZTP configuration" /disk0:/ztp/customer/downloaded-config
 2>&1 >> $LOGFILE;
    ztp_log "### Checking for errors ###";
    local config_status=$(xrcmd "show configuration failed");
    if [[ $config_status ]]; then
        echo $config_status  >> $LOGFILE
        STATUS="ProvisioningError"
        ztp_log "### status::: ${STATUS} ###"
        ztp_log "!!! Error encountered applying configuration file, please review the
log !!!!";
        MESSAGE="Error encountered applying configuration file, ZTP process failed"
    else
       STATUS="Provisioned"
       ztp_log "### status::: ${STATUS} ###"
       ztp_log "### Applying system configuration complete ###";
       MESSAGE="Applying system configuration complete, ZTP process completed"
   fi
```

```
}

#
# Call Crosswork ZTP API to update device ZTP status, IP address, hostname.
# Without this function, device status will remain in "In Progress" and not
# be updated in Crosswork.
#
# Using this API, device SSH/SNMP connectivity details can also be updated.
# Values for connectivity details values can be added as part of
# "connectivityDetails" array in below curl command. Sample snippet provided:
#
#   "connectivityDetails": [{
#     "protocol": "SSH",
#     "inetAddr": [{
#       "inetAddressFamily": "IPV4/IPV6",
#       "ipaddrs": "<ssh/snmp ipaddress>",
#       "mask": <ipaddress mask(Integer).>,
#       "type": "CONNECTIVITYINFO"
#     }],
#     "port": <ssh/snmp port(Integer)>,
#     "timeout": <ssh/snmp timeout(Integer). default to 60sec>
#   }]
#
function update_device_status() {

     echo "'"$IPADDR"'"
     echo "'"$MASK"'"
     echo "'"$DEVNAME"'"
     echo "'"$STATUS"'"
     echo "'"$HOSTNAME"'"
     echo "'"$MESSAGE"'"


    curl -d '{
       "ipAddress":{
            "inetAddressFamily": "IPV4",
            "ipaddrs": "'"$IPADDR"'",
            "mask":  '$MASK'
        },
       "serialNumber":"'"$DEVNAME"'",
       "status":"'"$STATUS"'",
       "hostName":"'"$HOSTNAME"'",
       "message":"'"$MESSAGE"'"
   }' -H "Content-Type: application/json" -X PATCH
http://${CW_HOST_IP}:${CW_PORT}/crosswork/ztp/v1/deviceinfo/status
}


# ==== Script entry point ====
STATUS="InProgress"
get_serialkey;
#get_serialkey_asr9901; // For Cisco ASR9901, replace get_serialkey with
get_serialkey_asr9901.
ztp_log "Hello from ${DEVNAME} !!!";
get_ipaddress;
ztp_log "Starting autoprovision process...";
download_config;
apply_config;
get_hostname;
update_device_status;

ztp_log "Autoprovision complete...";
exit 0
```

図 *31 :* セキュア *ZTP*：シンプルな *Day-Zero* 構成スクリプト

```
!! IOS XR
!
hostname ztpdevice1
!
interface MgmtEth0/RP0/CPU0/0
 ipv4 address dhcp
!
```

図 *32 :* セキュア *ZTP*：置き換え可能なパラメータを使用した *Day-Zero* 構成スクリプト

```
!! IOS XR
!
hostname {$hname}
!
interface MgmtEth0/RP0/CPU0/0
 ipv4 address {$mgmt_ipaddr} {$mgmt_subnet_mask}
!
```

図 *33 :* セキュア *ZTP*：構成後スクリプト

```
#!/bin/bash

################################################################################
#
#SZTP post script to update hostname and ipaddress for the device
# input -  serial key and crosswork host and port
#
################################################################################


export LOGFILE=/disk0:/ztp/customer/user-script.log

XRZTP_INTERFACE_NAME="MgmtEth0/RP0/CPU0/0"
# ZTP helper library is assumed to be installed in IOS-XR linux shell
source /pkg/bin/ztp_helper.sh
interfacedata=$(xrcmd "show interface ${XRZTP_INTERFACE_NAME}")

CW_HOST_IP="<EnterIPv4AddressHere>"   #update from the post script prepare code
CW_PORT="30603"           #update from the post script prepare code


# Send logging information to log file on device disk0:/ztp/user-script.log
function ztp_log() {

    echo "$(date +"%b %d %H:%M:%S") "$1 >> $LOGFILE
}


#
# Get IP address and subnet mask from device. IP address is assigned from DHCP
# server on interface where ZTP was triggered.
#
function get_ipaddress(){

    local ipvar=($(echo $interfacedata | awk -F "Internet address is " '{sub(/
.*/,"",$2);print $2}'));
    local ipv4addr=$(xrcmd "sh run interface ${XRZTP_INTERFACE_NAME} | i ipv4 address"
| awk '{print $3}')
    local ipv6addr=$(xrcmd "sh run interface ${XRZTP_INTERFACE_NAME} | i ipv6 address"
| awk '{print $3}')
    local ipaddress=($(echo $ipvar | awk -F "/" '{sub(/ .*/,"",$1);print $1}'));
    local mask=($(echo $ipvar | awk -F "/" '{sub(/ .*/,"",$2);print $2}'));
    local maskv6=($(echo $ipv6addr | awk -F "/" '{sub(/ .*/,"",$2);print $2}'));
```

```
    ztp_log "### Value of interfacedata => $interfacedata ###"
    ztp_log "### Value of ipvar => $ipvar ###"
    ztp_log "#####IPv4 address $ipaddress and mask $mask found. #####";

    IPADDR=$ipaddress
    MASK=$mask
    MASKV6=$maskv6

    return 0
}

#
# Fetch hostname from device configuration.
#
function get_hostname(){

    hostnamedata=$(xrcmd "show running-config hostname")
    local hostname=($(echo $hostnamedata | awk -F "hostname " '{sub(/ .*/,"",$2);print
$2}'));

    ztp_log "#####hostname $hostname found.";
    HOSTNAME=$hostname;
    return 0;
}



#
# Call Crosswork ZTP API to update device ZTP status, IP address, hostname.
# Without this function, device status will remain in "In Progress" and not
# be updated in Crosswork.
#
# Using this API, device SSH/SNMP connectivity details can also be updated.
# Values for connectivity details values can be added as part of
# "connectivityDetails" array in below curl command. Sample snippet provided:
#
#   "connectivityDetails": [{
#     "protocol": "SSH",
#     "inetAddr": [{
#       "inetAddressFamily": "IPV4/IPV6",
#       "ipaddrs": "<ssh/snmp ipaddress>",
#       "mask": <ipaddress mask(Integer).>,
#       "type": "CONNECTIVITYINFO"
#     }],
#     "port": <ssh/snmp port(Integer)>,
#     "timeout": <ssh/snmp timeout(Integer). default to 60sec>
#   }]
#
function update_device_status() {

     echo "'"$IPADDR"'"
     echo "'"$MASK"'"
     echo "'"$SERIAL_KEY"'"
     echo "'"$HOSTNAME"'"


    curl -d '{
       "ipAddress":{
            "inetAddressFamily": "IPV4",
            "ipaddrs": "'"$IPADDR"'",
            "mask":  '$MASK'
        },
       "serialNumber":"'"$SERIAL_KEY"'",
```

```
       "hostName":"'"$HOSTNAME"'",
       "message":"Post config script updated succssfully"
   }' -H "Content-Type: application/json" -X PATCH
http://${CW_HOST_IP}:${CW_PORT}/crosswork/ztp/v1/deviceinfo/status
}

function get_sudi_serial() {
   local rp_card_num=`ip netns exec xrnns /pkg/bin/show_platform_sysdb | grep Active  |
 cut -d ' ' -f 1`
   echo $rp_card_num
   xrcmd "show platform security tam all location $rp_card_num" > tamfile.txt
   local sudi_serial=$(sed -n -e '/Device Serial Number/ s/.*\- *//p' tamfile.txt)
   echo $sudi_serial
   SERIAL_KEY=$sudi_serial
   return 0
}

function ztp_disable()
{
 xrcmd "ztp disable noprompt"
}

function ztp_enable()
{
 xrcmd "ztp enable noprompt"
}

# ==== Script entry point ====
get_sudi_serial;
ztp_log "Hello from ${SERIAL_KEY} !!!";
get_ipaddress;
get_hostname;
update_device_status;

ztp_log "Autoprovision complete...";
ztp_log "Disabling secure mod"
ztp_disable;
exit 0
```

構成ファイルの読み込み

構成ファイルを Cisco Crosswork に読み込むには、次の手順を実行します。

1. Cisco Crosswork を起動します。
2. メインメニューから、**[デバイス管理（Device Management）]** > **[ZTP構成ファイル（ZTP Configuration Files）]** を選択ます。
3. をクリックします。 ＋
4. [参照（Browse）] をクリックして設定ファイルを選択します。
5. 必要な構成情報を入力します。

   セキュア ZTP を実装する場合は、[タイプ（Type）] ドロップダウンを使用して、追加する構成ファイルが [事前設定（Pre-config）] か、[Day 0設定（Day0 config）] か、または [設定後（Post-config）] かを指定します。

   クラシック ZTP と PnP ZTP の場合は、常に [Day 0設定（Day0-config）] [タイプ（Type）] ドロップダウンを選択します。

6. [追加（Add）] をクリックして、構成ファイルの追加を終了します。
7. 計画された ZTP 実行で使用されるすべての構成ファイルをロードするまで、必要に応じて繰り返します。

SMU の検索と読み込み

ソフトウェア メンテナンス アップデート（SMU）は、シスコ ネットワーク オペレーティング システム ソフトウェア イメージの特定のリリースにおける重大な問題のポイントフィックスを提供するシスコ ソフトウェア パッケージ ファイルです。シスコは、SMU に関連する問題を説明する readme.txt ファイルを使用してブート不可形式の SMU を配布しています。シスコは、ソフトウェアイメージの次のメンテナンスリリースに SMU のコンテンツを展開します。

ZTP オンボーディング中にデバイスに SMU を適用することは、クラシック ZTP およびセキュア ZTP でのみサポートされ、その後は構成ファイルの適用中にのみサポートされます（「構成ファイルと読み込み（230 ページ）」を参照）。SMU は、Cisco IOS-XE デバイスまたは PnP ZTP ではサポートされていません。

ソフトウェアイメージと同様に、[Cisco Support & Downloads（シスコサポート & ダウンロード）]https://www.cisco.com/c/en/us/support/index.html ページから SMU ファイルをダウンロードします。ダウンロード中に、SMU ファイルの MD5 チェックサムを記録します。Cisco Crosswork は MD5 チェックサムを使用して SMU ファイルの整合性を検証します。一度に 1 つずつ SMU を Cisco Crosswork に読み込ませ、読み込み中に各 SMU ファイルの MD5 チェックサムを入力します。

SMU を Cisco Crosswork に読み込ませるには、次の手順を実行します：

1. Cisco Crosswork を起動します。
2. メインメニューから、**[デバイス管理（Device Management）]** > **[ソフトウェアイメージ（Software Images）]**を選択します。
3. をクリックします。 
4. 入力するか、または**[参照（Browse）]**をクリックし、アップグレードするコンポーネントの SMU ファイルを選択しますプロンプトが表示されたら、ファイルの MD5 チェックサムを入力します。
5. **[追加（Add）]** をクリックして、SMU の追加を終了します。
6. 計画された ZTP 実行で使用されるすべての SMU ファイルを読み込むまで、必要に応じて繰り返します。

ZTP でのクレデンシャルプロファイルの作成

Cisco Crosswork ZTP では、デバイスにアクセスして設定するのにクレデンシャルプロファイルが必要です。次に、CSV ファイルを使用して一括でクレデンシャルプロファイルを追加する方法を示します。

クレデンシャルプロファイルを 1 つずつ追加することもできます。これを行うには、**[デバイス管理（Device Management）] > [クレデンシャルプロファイル（Credential Profiles）]**を選択し、＋をクリックします。

クレデンシャルプロファイルを使用すると、デバイスがサポートするプロトコルごとに異なるクレデンシャルを指定できます。SNMP クレデンシャルを含んでいるデバイス クレデンシャル プロファイルを作成する場合は、プロファイルにはデバイスで実際に有効になっている SNMP のバージョンのクレデンシャルと、そのバージョンのみを含めることをお勧めします。たとえば、デバイス設定で SNMPv3 が有効になっていない場合は、そのデバイスのクレデンシャル プロファイルに SNMPv3 クレデンシャルを含めないでください。

ステップ 1 メインメニューから **[デバイス管理（Device Management）] > [クレデンシャルプロファイル（Credential Profiles）]** を選択します。

ステップ 2 ⎘をクリックします。

ステップ 3 [「Credential template（*.csv）」サンプルファイルのダウンロード（Download sample 'Credential template (*.csv)' file）] リンクをクリックし、CSV ファイルテンプレートをローカルに保存します。

ステップ 4 任意のエディタを使用して CSV テンプレートを開きます。作成するクレデンシャルプロファイルごとに 1 行ずつファイルに行を追加します。

これを行う場合は、次のガイドラインに従います。

- クレデンシャルプロファイルの [パスワード（Password）] 列が空白の場合、CSV ファイルをインポートできません。必要に応じて、これらのフィールドに実際のパスワードを入力できます。Cisco Crosswork は暗号化された形式でこれらのパスワードを保存します。この方法を選択した場合は、アップロード後すぐに CSV ファイルを破棄してください。CSV ファイルの [パスワード（Password）] 列にアスタリスクを入力してインポートすることをお勧めします。インポートが成功したら、Cisco Crosswork の GUI を使用して各プロファイルを編集し、次の手順で説明するように実際のパスワードを入力できます。
- 同じフィールド内で複数のエントリを区切るには、セミコロンを使用します。
- 複数のエントリをセミコロンで区切る場合は、各フィールドに値を入力する順序が重要であることに注意してください。1 つの列の最初のエントリは次の列の最初のエントリにマッピングされます。例：[パスワードタイプ（Password Type）] に、パスワードタイプのリスト、**`ROBOT_USERPASS_SSH;ROBOT_USERPASS_TELNET;ROBOT_USERPASS_NETCONF`** を入力します。次に、[ユーザー名（User Name）] 列に **`Tom;Dick;Harry;`**、[パスワード（Password）] 列に **`root;MyPass;Turtledove;`** と入力します。これらの列に入力する順序によって、入力した 3 つのパスワードタイプ、3 つ のユーザー名、および 3 つのパスワードの間に次のマッピングが設定されます。
  - ROBOT_USERPASS_SSH; Tom ; root
  - ROBOT_USERPASS_NETCONF; Dick ; MyPass
  - ROBOT_USERPASS_TELNET; Harry; Turtledove
- ファイルを保存する前に、サンプルデータ行を必ず削除してください。列ヘッダー行は無視できます。

ステップ 5 完了したら、CSV ファイルを新しい名前で保存します。

ステップ 6 必要に応じて、**[デバイス管理（Device Management）]>[クレデンシャルプロファイル（Credential Profiles）]** を再度選択し、 をクリックします。

ステップ 7 [参照（Browse）] をクリックして CSV ファイルまで移動し選択します。

ステップ 8 CSV ファイルを選択した状態で、[インポート（Import）] をクリックします。

ステップ 9 インポートが完了したら、次の手順を実行します。

a) [クレデンシャルプロファイル（Credential Profiles）] ウィンドウの左側から、更新するプロファイルを選択し、 をクリックします。

b) クレデンシャルプロファイルのパスワードとコミュニティ文字列を入力し、[保存（Save）] をクリックします。

c) すべてのパスワードとコミュニティ文字列を入力するまで、必要に応じてこれらの手順を繰り返します。

デバイスのシリアル番号の検索と読み込み

デバイスのシリアル番号は、すべての ZTP モードで必要です。

ほとんどの組織は、非販売在庫レコードの一部としてネットワークデバイスのシリアル番号のデータベースを維持しています。ネットワークに新しいデバイスを追加する場合、通常、購入時に新しいデバイスのシリアル番号を同じデータベースに追加します。これは、ZTP を使用してオンボードする予定のデバイスのシリアル番号を探す最初の場所です。

新しく購入したデバイスのシリアル番号を取得するには、シスコサポートに連絡することもできます。

最後の手段として、すでにイメージが作成されている Cisco IOS デバイスの場合は、デバイスコンソールにログインして、`show inventory CLI` コマンドを実行します。コマンド出力で、次の図に示すようなデバイス名と説明のセクションを探します。（この例に示すように）ラインカードまたはその他のオプションを備えたデバイスの場合、シャーシとカードの両方のシリアル番号を読み込む必要があります。

```
RP/0/RP0/CPU0:ios#sh inv
Wed May 18 13:33:53.674 UTC
NAME: "0/RP0", DESCR: "NC5501 w/o TCAM Route Processor Card"
PID: NCS-5501          , VID: V01, SN: FOC23297HGS

NAME: "Rack 0", DESCR: "NCS5501 w/o TCAM 1RU Chassis"
PID: NCS-5501          , VID: V01, SN: FOC2332R014
...
```

デバイスのシリアル番号を Cisco Crosswork に読み込ませるには、次の手順を実行します。

1. Cisco Crosswork を起動します。
2. メインメニューから、**[デバイス管理（Device Management）]>[シリアル番号とバウチャー（Serial Number and Voucher）]** を選択します。
3. [シリアル番号を追加（Use Serial Number）] をクリックします。

4. [CSVのアップロード（Upload CSV）] をクリックし、**serialnumber.csv** リンクをクリックして `sampleSerialnumber.csv` テンプレートファイルをダウンロードします。
5. 選択した CSV ファイルエディタを使用して、ZTP を使用してオンボーディングする予定のすべてのデバイスのシリアル番号をテンプレートに入力します。更新したCSVファイルテンプレートを新しい名前で保存します。
6. [シリアル番号の追加（Add Serial Number）] を再度選択します。
7. [参照（Browse）] をクリックして、更新された CSV ファイルを選択します。
8. [シリアル番号の追加（Add Serial Number）] をクリックして、シリアル番号をインポートします。

PDC、所有者証明書、および所有者キーを更新する

ピン留めされたドメイン証明書、所有者証明書、および所有者キーは、セキュア ZTP にのみ必要です。これらは、Classic ZTP および PnP ZTP では使用されません。

テスト環境では、ZTP が最初にインストールされたときに Cisco Crosswork が生成するデフォルトのピン留めドメイン証明書（PDC）、所有者証明書（OC）、および所有者キーを使用できます。これらの資格情報は、認証局（CA）としてシスコに依存しており、製品テストの便宜のためにのみ提供されています。シスコは、これらのデフォルトのログイン情報を使用している場合、ネットワークをセキュリティリスクにさらさない保護された「サンドボックス」環境で Cisco Crosswork をテストしていると想定しています。

本番環境で使用する場合は、ドメイン証明書をピン留めし、中間 OC を生成し、所有者キーに署名する必要があります。その後、次のセクション「デフォルトの PDC、OC、および所有者キーを更新する」の手順を使用して、これらのログイン情報のデフォルトバージョンを更新できます。

独自の証明書管理スタッフと手順を持つ組織は、選択した CA を使用して PDC、OC、および所有者キーを生成する方法に精通しています。これらのタスクでさらに支援が必要な組織は、このトピックの後半のセクション「ドメイン証明書のピン留め、所有者証明書の生成、所有者キーの署名」の例とアドバイスを参照してください。

デフォルトの PDC、OC、および所有者キーを更新する

デフォルトのピン留めドメイン証明書（PDC）、所有者証明書（OC）、および所有者キーを更新するには、次の手順を実行します。

1. Crosswork を起動します。
2. メインメニューから、**[管理（Administration）]>[証明書管理（Certificate Management）]** を選択します。
3. [証明書（Certificates）] で、[Crosswork ZTP 所有者（Crosswork-ZTP-Owner）] の横にある ⋯ をクリックし、[証明書の更新（Update Certificate）] をクリックします。
4. [参照（Browse）] をクリックして、固定ドメイン証明書（PEM ファイルまたは CRT ファイル）を選択します。ファイルを選択した状態で、[保存（Save）] をクリックします。

5. [参照（Browse）] をクリックして、所有者証明書（PEM ファイルまたは CRT ファイル）を選択します。ファイルを選択した状態で、[保存（Save）] をクリックします。
6. [参照（Browse）] をクリックして、所有者キー（PEM ファイル、KEY ファイル、CRT ファイル）を選択します。ファイルを選択した状態で、[保存（Save）] をクリックします。
7. [保存（Save）] をクリックして、デフォルトの証明書とキーを更新します。

ドメイン証明書をピン留めし、所有者証明書を生成し、所有者キーに署名します

次の手順では、OpenSSL と Linux Bash シェルを使用して、独自の認証局を使用して PDC、OC、および署名された所有者キーを生成する方法を示す一連の例を示します。このプロセスの追加の説明と例は、次の公開リソースで見つけることができます：OpenSSL Certificate Authority（認証局）。これらのログイン情報を生成したら、前のセクション「既定の PDC、OC、および所有者キーを更新する」の手順に従います。

1. 使用または生成する証明書とその他のファイルを管理するための一連のディレクトリを作成します。次に例を示します。

```
#!/bin/sh
mkdir ./ca
mkdir ./ca/certs
mkdir ./ca/crl
mkdir ./ca/newcerts
mkdir ./ca/private
chmod 700 ./ca/private
touch ./ca/index.txt
echo 1000 > ./ca/serial
mkdir ./ca/intermediate
mkdir ./ca/intermediate/certs
mkdir ./ca/intermediate/crl
mkdir ./ca/intermediate/csr
mkdir ./ca/intermediate/newcerts
mkdir ./ca/intermediate/private
chmod 700 ./ca/intermediate/private
touch ./ca/intermediate/index.txt
echo 1000 > ./ca/intermediate/serial
echo 1000 > ./ca/intermediate/crlnumber
```

2. ルートキーを生成します。次に例を示します。

```
#!/bin/bash
cd ca
openssl genrsa -aes256 -out private/ca.key.pem 4096
chmod 400 ./private/ca.key.pem
```

3. ルート証明書を生成します。次に例を示します。

```
#!/bin/bash
cd ca
##-subj "/C=us/ST=nc/L=rtp/O=cisco/OU=cx/CN=cisco.com" \
openssl req -config openssl.cnf -key ./private/ca.key.pem -new -x509 -days 7300
-sha256 -subj "/C=us/ST=nc/L=rtp/O=cisco/OU=cx/CN=cisco.com" -extensions v3_ca -out
 certs/ca.cert.pem
chmod 444 ./certs/ca.cert.pem
```

4. ルート証明書を確認します。次に例を示します。

```
#!/bin/bash
cd ca
openssl x509 -noout -text -in certs/ca.cert.pem
```

5. 中間キーを生成します。次に例を示します。

```
#!/bin/bash
cd ca
openssl genrsa -aes256 -out intermediate/private/intermediate.key.pem 4096
chmod 400 ./intermediate/private/intermediate.key.pem
```

6. 中間証明書を生成します。次に例を示します。

```
#!/bin/bash
cd ca
##-subj "/C=us/ST=nc/L=rtp/O=cisco/OU=cx/CN=cisco.com" \
openssl req -config intermediate/openssl.cnf -new -sha256 \
      -key intermediate/private/intermediate.key.pem \
      -out intermediate/csr/intermediate.csr.pem \
      -subj "/C=us/ST=nc/L=rtp/O=cisco/OU=cx/CN=intermediate.cisco.com"
chmod 444 ./certs/ca.cert.pem
© 2022 GitHub, Inc.
```

7. 中間鍵に署名します。次に例を示します。

```
#!/bin/bash
cd ca
openssl ca -config openssl.cnf -extensions v3_intermediate_ca \
      -days 3650 -notext -md sha256 \
      -in intermediate/csr/intermediate.csr.pem \
      -out intermediate/certs/intermediate.cert.pem
chmod 444 ./intermediate/certs/intermediate.cert.pem
```

8. 中間証明書を確認します。次に例を示します。

```
#!/bin/bash
cd ca
openssl x509 -noout -text -in intermediate/certs/intermediate.cert.pem
```

9. 証明書チェーンを作成します。次に例を示します。

```
#!/bin/bash
cd ca
cat intermediate/certs/intermediate.cert.pem \
      certs/ca.cert.pem > intermediate/certs/ca-chain.cert.pem
chmod 444 intermediate/certs/ca-chain.cert.pem
```

10. 証明書失効リスト（CRL）に署名します。次に例を示します。

```
#!/bin/bash
mycsr=$1
myip=$2
export SAN="IP:${myip}"
echo $SAN
cd ca
openssl ca -config intermediate/openssl.cnf \
      -extensions usrSrv_cert -days 750 -notext -md sha256 \
      -in intermediate/csr/${mycsr}.csr.pem \
      -out intermediate/certs/${mycsr}.cert.pem
chmod 444 intermediate/certs/${mycsr}.cert.pem
```

所有権バウチャーのリクエストと読み込み

所有権証明書（OV）は、セキュア ZTP にのみ必要です。提供方法に応じて、一度に 1 つずつ読み込むことも、まとめて読み込むこともできます。

シスコは、要求に応じて OV を VCJ または TAR ファイルの形式で提供します。

Secure ZTP を使用してサードパーティのデバイスをオンボードする場合は、サードパーティの製造元に VCJ ファイルを要求する必要があります。製造元が提供する VCJ ファイルは命名規則 *serial.vcj* に従う必要があります。ここで、*serial* は対応するデバイスのシリアル番号です。Cisco Crosswork では、所有権バウチャーをデバイスにマッピングするために、このファイル命名規則が必要です。サードパーティメーカーのバウチャーに関する制限の背景については、「#unique_151 unique_151_Connect_42_SecureZTPGuidelinesThird （217 ページ）」を参照してください。

シスコからの所有権バウチャーのリクエスト

Secure ZTP を使用してオンボードする予定のシスコデバイスの OV を要求するには、[シスコサポートにお問い合わせください（Contact Cisco Support）]https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html。OV を要求するときは、以下を提供する必要があります。

- [ピン留めされたドメイン証明書（Pinned Domain Certificate）]：認証局（CA）によって発行され、ユーザーがピン留めした信頼できるデジタル証明書。PDC のピン留めの詳細については、「PDC、所有者証明書、および所有者キーを更新する （245 ページ）」を参照してください。
- Secure ZTP を使用してオンボードする予定の各デバイスのシリアル番号（「デバイスのシリアル番号の検索と読み込み （244 ページ）」を参照）。

単一のデバイスに対するリクエストの例を次に示します。

```
{
    "expires-on": "2016-10-21T19:31:42Z",
    "assertion": "verified",
    "serial-number": "JADA123456789",
    "idevid-issuer": "base64encodedvalue==",
    "pinned-domain-cert": "base64endvalue==",
    "last-renewal-date": "2017-10-07T19:31:42Z"
 }
```

シスコサポートは、VCJ ファイルを送信することにより、OV 要求に応答します。複数のデバイスの OV をリクエストした場合、単一の VCJ ファイルではなく、TAR ファイルで複数の VCJ を受け取ります。シスコサポートと合意した安全な方法を使用して、VCJ または TAR ファイル交換を実行することをお勧めします。

個々の VCJ ファイルには、送信元が何であれ、ファイル名としてデバイスのシリアル番号が必要であることに注意してください。ステップ 1 で指定された要求例に従って、シスコは次の名前のファイルを返します：JADA123456789.VCJ。

所有権バウチャーの読み込み

所有権バウチャーの読み込むには、次の手順を実行します。

1. Cisco Crosswork を起動します。
2. メインメニューから、**[デバイス管理（Device Management）]**>**[シリアル番号とバウチャー（Serial Number and Voucher）]** を選択します。
3. [バウチャーの追加（Add Voucher）] をクリックします。
4. アップロードする VCJ または TAR ファイルの名前を入力するか、参照します。
5. [アップロード（Upload）] をクリックして、OV のアップロードを完了します。

デフォルトの所有権バウチャー証明書の更新

デフォルトの所有権バウチャー証明書を更新するには、次を実行します。

1. メインメニューから、**[管理（Administration）]**>**[証明書管理（Certificate Management）]** を選択します。
2. [証明書の更新（Update Certificate）] をクリックします。
3. [参照（Browse）] をクリックして、デフォルトの所有権バウチャーの更新に使用する TAR ファイルまたは VCJ ファイルを選択します。
4. [証明書の更新（Update Certificate）] をクリックします。
5. **[保存（Save）]** をクリックします。

SUDI ルート証明書の準備と読み込み

SUDI ルート証明書は、IOS-XE デバイスのオンボーディング時にセキュア e ZTP および PnP ZTP に必要です。Classic ZTP には使用されません。

「SUDI 証明書」には次の 2 種類があります。

- デバイスの **SUDI 証明書**（トラストアンカー証明書とも呼ばれます）。すべての Cisco IOS-XR および IOS-XE デバイスには、SUDI 証明書がデバイスに保存されています。デバイスの SUDI 証明書は変更できません。
- **SUDI ルート証明書**。これは、各デバイスで SUDI 証明書を有効にするルート認証局です。

SUDI ルート証明書を Crosswork にアップロードすると、セキュア ZTP プロセス（および IOS-XE デバイスの場合は PnP ZTP プロセス）が、SUDI ルート証明書をデバイスに保存されている SUDI 証明書と比較することによって、各デバイスを認証できるようになります。これは、PnP ZTP または Secure ZTP プロセスがデバイスにブートストラップ情報を提供する前に必要です。

SUDI ルート証明書を準備して Cisco Crosswork にアップロードするには、次の手順を実行します。

1. 「Cisco Root CA 2048」および「Cisco Root CA 2099」ファイルを PEM 形式で、Cisco PKI：ポリシー、証明書、およびドキュメント（https://www.cisco.com/security/pki/policies/index.html）からダウンロードします。

2. 次の例のように、ASCIIテキストエディタを使用して、ダウンロードした2つのPEMファイルを1つのPEMファイルに結合します。

```
-----BEGIN CERTIFICATE-----
MIIDQzCCAiugAwIBAgIQX/h7KCtU3I1CoxW1aMmt/zANBgkqhkiG9w0BAQUFADA1
....
kxpUnwVwwEpxYB5DC2Ae/qPOgRnhCzU=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDITCCAgmgAwIBAgIJAZozWHjOFsHBMA0GCSqGSIb3DQEBCwUAMC0xDjAMBgNV
...
PKkmBlNQ9hQcNM3CSzVvEAK0CCEo/NJ/xzZ6WX1/f8Df1eXbFg==
-----END CERTIFICATE-----
```

3. Cisco Crosswork を起動します。
4. メインメニューから、**[管理（Administration）]**>**[証明書管理（Certificate Administration）]** を選択します。
5. ＋をクリックして、次のようにフィールドに入力します。

   [証明書名（Certificate Name）]：Crosswork-ZTP-Device-SUDI

   [証明書の役割（Certificate Role）]：ZTP SUDI

   [Cisco M2 CA証明書（Cisco M2 CA Certificate）]：アップロードする PEM ファイルの名前を入力するか、参照します。
6. [保存（Save）] をクリックします。Crosswork は SUDI ルート証明書を保存します。

ZTP プロファイルの作成

Cisco Crossworkは、ZTPプロファイルを使用して、イメージ化プロセスと設定プロセスを自動化します。ZTPプロファイルはオプションですが、作成することを強くお勧めします。ZTPイメージ化と設定プロセスを簡素化するのに役立ちます。ZTPプロファイルを使用すると、特定のクラスのまたはデバイスファミリ内のデバイスに適用できる、定義済みのイメージファイルと設定ファイルのセットを整理できます。

クラシック ZTP を実装する場合、各 ZTP プロファイルには 1 つのイメージファイルと、1 つの設定ファイルのみを関連付けることができます。セキュア ZTP では、事前設定ファイル、設定後ファイル、および Day 0 設定ファイルを指定できます。

ZTP プロファイルでは、イメージファイルを指定する必要はありません。

ZTPプロファイルはいくつでも作成できます。デバイスファミリごと、ユースケースごと、またはネットワークロールごとに1つのZTPプロファイルのみを作成することをお勧めします。

ステップ 1 メインメニューから **[デバイス管理（Device Management）]** > **[ゼロタッチプロファイル（Zero Touch Profiles）]** を選択します。

ステップ 2 [+ 新しいプロファイル（+ New Profile）] をクリックします。

ステップ 3 新しいZTPプロファイルに必要な値を入力します。プロファイルのソフトウェアイメージを指定する必要はありません。

ステップ 4 セキュア ZTP を実装する場合は、[セキュア ZTP（Secure ZTP）] のスライダを [有効（Enabled）] に移動します。次に、事前設定ファイルと設定後ファイルの名前を入力します。

OS バージョンとして IOS-XE を選択した場合、セキュア ZTP は使用できません。

ステップ 5 [保存（Save）] をクリックして新しい ZTP プロファイルを作成します。

ZTP デバイスエントリファイルの作成

Cisco Crosswork は、ZTP デバイスエントリを使用して、プロビジョニングするデバイスの IP アドレス、プロトコル、およびその他の情報を事前に指定できます。Cisco Crosswork は、ZTP 処理が正常に完了すると、これらのインポートされたエントリに詳細情報を入力します。

複数の ZTP デバイスエントリを作成する最も簡単な方法は、デバイスエントリの CSV ファイルを使用して、それらをまとめてインポートすることです。慣れるまでは、デバイスエントリの CSV ファイル形式を試すことをお勧めします。テンプレートのコピーに 1 つまたは 2 つのデバイスエントリのみを追加し、インポートします。その後で、必要な結果を取得する方法を確認できます。

次のトピックでは、デバイスエントリの CSV ファイルをダウンロードして使用し、適切な形式の ZTP デバイスエントリを一括で作成する方法について説明します。

また、単一ZTPデバイスエントリの作成（258ページ）で説明するように、Cisco Crosswork の UI を使用して、ZTP デバイスエントリを 1 つずつ作成することもできます。

ZTP デバイスエントリ CSV テンプレートのダウンロードと編集

1. メインメニューから **[デバイス管理（Device Management）]** > **[デバイス（Devices）]** を選択します。
2. [ゼロタッチデバイス（Zero Touch Devices）] タブをクリックします。
3. をクリックします。
4. [「devices import」テンプレート（.csv）のダウンロード（Download 'devices import' template (.csv)）] リンクをクリックし、[保存（Save）] をクリックしてローカルストレージリソースに保存します。[キャンセル（Cancel）] をクリックしてダイアログボックスをクリアします。
5. 選択したアプリケーションで CSV テンプレートを開き、新しい名前で保存します。各行で、ZTP を使用してオンボーディングする予定の各デバイスのエントリを作成します。各列に入力する値については、次のトピックの項を参照してください。

ZTP デバイスエントリの CSV テンプレートリファレンス

次の表で、テンプレート内の列の使用方法について説明します。エントリを必要とする列については、列名の横にアスタリスク（*）を付けて示しています。

4 つの [接続（Connectivity）] 列では複数のエントリが許可されているため、1 台のデバイスに複数の接続プロトコルを指定できます。このオプションを使用する場合は、エントリ間にセミコロンを使用し、次の 3 つの列に同じ順序で値を入力します。たとえば、[接続プロトコル（Connectivity Protocol）] 列に **SSH;NETCONF;** と入力するとします。[接続ポート（Connectivity Port）] 列に **23;830;** と入力した場合、2 つの列のエントリは次のようにマッピングされます。

- SSH：22
- NETCONF：830

表 *16 : ZTP* デバイス エントリ テンプレートの列リファレンス

テンプレートの列	使用方法
シリアル番号（Serial Number）*	デバイスのシリアル番号を入力します。同じデバイスに対して最大 3 つのシリアル番号を入力できます。これらは、以前に Cisco Crosswork にロードした各デバイスのシリアル番号と同じである必要があります。 ZTP では、通常のすべての展開にシリアル番号のエントリが必要です。DHCP Option 82 を使用してリレーエージェントを実装する場合は、このフィールドを空白のままにすることもできますが、デバイスを識別するためにリモート ID と回線 ID は指定する必要があります。
ロケーションが有効（Location Enabled）	ロケーション ID を使用してデバイスを識別する場合は、TRUE と入力します。シリアル番号で識別する場合は、FALSE と入力します。TRUE と入力した場合は、対応する列にリモート ID と回線 ID を入力します。FALSE と入力した場合は、対応する列にシリアル番号を入力します。
リモート ID（Remote ID）*	セキュア ZTP を実装し、Option 82 を使用する場合：ブートストラップサーバーとして機能するリモートホストの名前を識別します。 DHCP Option 82 を使用してリレーエージェントを実装する場合は、このエントリは必須です。デバイスのリモート ID と回線 ID の組み合わせを入力する必要があります。 Option 82 を使用しない場合は、このフィールドを空白のままにできますが、デバイスのシリアル番号は指定する必要があります。
回線 ID（Circuit ID）*	セキュア ZTP を実装し、Option 82 を使用する場合：ブートストラップサーバーが要求を受信するインターフェイスまたは VLAN を識別します。 DHCP Option 82 を使用してリレーエージェントを実装する場合は、このエントリは必須です。デバイスのリモート ID と回線 ID の組み合わせを入力する必要があります。 Option 82 を使用しない場合は、このフィールドを空白のままにできますが、デバイスのシリアル番号は指定する必要があります。

テンプレートの列	使用方法
ホスト名（Host Name）*	デバイスに割り当てるホスト名を入力します。
クレデンシャルプロファイル（Credential Profile）*	Cisco Crosswork がデバイスにアクセスして設定するために使用するクレデンシャルプロファイルの名前を入力します。入力する名前は、Cisco Crossworkで指定されているクレデンシャルプロファイルの名前と一致する必要があります。
OS プラットフォーム（OS Platform）*	デバイスの OS プラットフォームを入力します。たとえば、IOS XR などです。Cisco IOS プラットフォーム名は、ハイフンではなくスペースを使用して入力する必要があることに注意してください。
バージョン（Version）*	デバイス プラットフォーム イメージの OS プラットフォームのバージョンを入力します。プラットフォームのバージョンは、プロビジョニングに使用するイメージファイルと設定ファイルに指定されているものと同じバージョンである必要があります。 [プロファイル名（Profile Name）] 列に ZTP プロファイルを指定しない場合にのみ必要です。
デバイスファミリ（Device Family）*	デバイスのデバイスファミリを入力します。デバイスファミリは、ZTP がプロビジョニングに使用するイメージファイルと設定ファイルのデバイスファミリと一致する必要があります。 [プロファイル名（Profile Name）] 列に ZTP プロファイルを指定しない場合にのみ必要です。
設定 ID（Config ID）*	デバイスの設定時に使用する設定ファイルの Cisco Crosswork によって割り当てられた ID を入力します。Cisco Crosswork は、アップロード時にすべての設定ファイルに一意の ID を割り当てます。 [プロファイル名（Profile Name）] 列に ZTP プロファイルを指定しない場合にのみ必要です。
[プロファイル名（Profile Name）] *	このデバイスのプロビジョニングに使用する ZTP プロファイルの名前を入力します。 ZTP プロファイルを使用して設定 ID、イメージ ID、OS プラットフォームなどを指定する場合にのみ必要です。
[製品 ID（Product ID）] *	デバイスハードウェアにコード化された、シスコによって割り当てられた PID（製品 ID）を入力します。PID は、工場出荷時にすべてのシスコ ネットワーキング デバイスに貼付されているラベルに印刷された UDI（一意のデバイス識別子）情報から取得できます。 このリリースでは、PID の検証は行われないことに注意してください。将来の要件に備えて、正しい PID を指定することをお勧めします。

テンプレートの列	使用方法
UUID	オンボーディング時にデバイスに割り当てる汎用一意識別子（UUID）を生成して指定することができます。このオプションを選択した場合は、この列に 128 ビット UUID を入力します。それ以外の場合は、このフィールドを空白のままにしておくと、Cisco Crosswork はデバイスのオンボーディング時にランダムな UUID を割り当てます。
[MACアドレス（MAC Address）]	デバイスの MAC アドレスを入力します。
[IPアドレス（IP Address）]	デバイスの IP アドレス（IPv4 または IPv6）と、そのサブネットマスクをスラッシュ表記で入力します。
[設定属性（Configuration Attributes）]	デバイスの設定ファイルのカスタムの置換可能パラメータに Cisco Crosswork で使用する値を入力します。デフォルトの置換可能パラメータのみを使用する場合は、このフィールドを空白のままにします。セキュア ZTP を使用している場合、カスタムの置換可能なパラメータは、Day 0 設定ファイルのパラメータにのみ使用できます。これらのパラメータの使用方法については、次を参照してください。
接続プロトコル（Connectivity Protocol）	デバイスをモニターするため、または Cisco Crosswork アプリケーションと機能をサポートするために必要な接続プロトコル。選択できるプロトコルは、**SSH**、**SNMPv2**、**NETCONF**、**TELNET**、**HTTP**、**HTTPS**、**GRPC**、および **SNMPv3** です。プロトコルの正しい組み合わせを選択するには、次のセクション「Crosswork 接続プロトコルの要件」の表を参照してください。
[接続 IP アドレス（Connectivity IP Address）]	接続プロトコルの IP アドレス（IPv4 または IPv6）とサブネットマスクを入力します。接続プロトコルの設定を選択した場合にのみ必要です。

テンプレートの列	使用方法
[接続ポート（Connectivity Port）]	この接続プロトコルに使用するポートを入力します。各プロトコルがポートにマッピングされます。選択したプロトコルにマッピングされるポート番号を必ず入力してください。 次の場合を除き、すべてのデバイスに1つ以上のポートとプロトコルを指定します。 • オンボーディングしたデバイスのステータスを管理対象外またはダウンとして設定します。 • オンボーディングしたデバイスの Cisco Crosswork 到達可能性チェックを無効にします。 デバイスごとに複数のプロトコルとポートを指定する必要がある場合があります。指定するプロトコルとポートの数は、Cisco Crosswork の設定方法と使用している Crosswork アプリケーションによって異なります。プロトコルの正しい組み合わせを選択するには、次のセクション「Crosswork 接続プロトコルの要件」の表を参照してください。
接続タイムアウト（Connectivity Timeout）	このプロトコルを使用した通信試行がタイムアウトするまでの経過時間を入力します（秒単位）。デフォルト値は 30 秒、推奨されるタイムアウト値は 60 秒です。
プロバイダー名（Provider Name）	新しい ZTP デバイスをオンボーディングするプロバイダの名前を入力します。入力する名前は、Cisco Crosswork で指定されているデバイス管理プロバイダの名前と正確に一致する必要があります。
インベントリ ID（Inventory ID）	デバイスに割り当てるインベントリ ID を入力します。
セキュア ZTP が有効（Secure ZTP Enabled）	セキュア ZTP を使用してデバイスをプロビジョニングする場合は TRUE、そうでない場合は FALSE と入力します。
[セキュア ZTP が暗号化済み（Secure ZTP Encrypted）]	現在サポートされていません。FALSE と入力します。
[イメージ ID（Image ID）]	Cisco Crosswork は、アップロード時にすべてのソフトウェア イメージ ファイルに一意の ID を割り当てます。 デバイスにインストールするソフトウェアイメージファイルの Cisco Crosswork によって割り当てられた ID を入力します。 オンボーディング時にソフトウェアイメージのインストールを含める必要があり、[プロファイル名（Profile Name）] 列にこのソフトウェアイメージを含む ZTP プロファイルを指定しなかった場合にのみ必要です。

テンプレートの列	使用方法
[事前設定 ID（PreConfig ID）]	Cisco Crossworkは、アップロード時にすべての設定ファイルに一意のIDを割り当てます。 [設定 ID（Config ID）] 列に指定した設定ファイルを実行する前に、実行する設定スクリプトの Cisco Crosswork ID を入力します。 オンボーディング時に事前設定ファイルを実行する場合にのみ必要です。
[設定後 ID（PostConfig ID）]	Cisco Crossworkは、アップロード時にすべての設定ファイルに一意のIDを割り当てます。 [設定 ID（Config ID）] 列に指定した設定ファイルを実行した直後に実行する設定スクリプトの Cisco Crosswork ID を入力します。 オンボーディング時に設定後ファイルを実行する場合にのみ必要です。
[SZTP 設定モード（SZTP Config Mode）]	セキュア ZTP で、[設定 ID（Config ID）] 列、[事前設定 ID（PreConfig ID）] 列、および [設定後 ID（PostConfig ID）] 列で指定した設定ファイルをデバイス上の既存の設定とマージする場合は、**`merge`** と入力します。指定した設定ファイルの内容で既存の設定を上書きする場合は、この列を空白のままにします（この列を空白のままにすることで、上書きがデフォルトになります）。
バージョン ID（Version ID）	設定のバージョン ID。 オンボーディング時に実行する事前設定ファイルと設定後ファイルを指定した場合にのみ必要です。
routingInfo.globalospfrouterid	デバイスに OSPF を実装する場合は、デバイスの OSPF ルータ ID を入力します。これ以外の場合は、このフィールドは空白のままにしておきます。
routingInfo.globalisissystemid	デバイスに IS-IS を実装する場合は、デバイスの IS-IS システム ID を入力します。これ以外の場合は、このフィールドは空白のままにしておきます。
routingInfo.teRouterid	デバイスにトラフィック エンジニアリングを実装する場合は、デバイスの TE ルータ ID を入力します。これ以外の場合は、このフィールドは空白のままにしておきます。

Crosswork 接続プロトコルの要件

Cisco Crossworkアプリケーションでは、デバイスごとにさまざまな接続プロトコルを有効にする必要があります。次の表に、サポートされる各接続プロトコルのこれらの要件を示します。この表に示されているアプリケーションを使用する場合は、デバイスでこれらのプロトコルを有効にしてください。オンボーディングするには、各デバイスでこれらのプロトコルの少なく

とも 1 つを有効にする必要があります。これらのプロトコルが 1 つもなければ、デバイスをオンボーディングできません。

表 *17 :* アプリケーションと機能の接続プロトコルの要件

プロトコル	ポート	**Crosswork** アプリケーション	アプリケーション機能
GRPC	9090	• Cisco Crosswork Network Controller • Cisco Crosswork Change Automation and Health Insights • Cisco Crosswork Optimization Engine	Cisco Crosswork API 通信
HTTP	80	• Cisco Crosswork Network Controller • Cisco Crosswork Change Automation and Health Insights • Cisco Crosswork Optimization Engine	Cisco Network Services Orchestrator へのデバイスのオンボーディング
HTTPS	443	• Cisco Crosswork Network Controller	Cisco Network Services Orchestrator へのデバイスのオンボーディング
NETCONF	830	• Cisco Crosswork Network Controller • Cisco Crosswork Change Automation and Health Insights • Cisco Crosswork Optimization Engine	Cisco Network Services Orchestrator へのデバイスのオンボーディング
SNMPv2	161	• Cisco Crosswork Network Controller • Cisco Crosswork Change Automation and Health Insights • Cisco Crosswork Optimization Engine	SNMPv2 でのデータ収集

プロトコル	ポート	Crosswork アプリケーション	アプリケーション機能
SNMPv3	161	• Cisco Crosswork Network Controller • Cisco Crosswork Change Automation and Health Insights • Cisco Crosswork Optimization Engine	SNMPv3 でのデータ収集
SSH	22	• Cisco Crosswork Network Controller • Cisco Crosswork Change Automation and Health Insights • Cisco Crosswork Optimization Engine	• CLI でのデータ収集 • デバイスへの SSH アクセス

単一 ZTP デバイスエントリの作成

ZTP を使用してオンボーディングするデバイスが少数の場合は、デバイスエントリを 1 つずつ作成するほうが簡単な場合があります。単一の ZTP デバイスエントリを作成するには、ZTP ユーザーインターフェイスで次の手順を実行します。

ステップ 1 メインメニューから **[デバイス管理（Device Management）] > [デバイス（Devices）]** を選択します。

ステップ 2 [ゼロタッチデバイス（Zero Touch Devices）] タブをクリックします。

ステップ 3 ＋をクリックします。

ステップ 4 新しい ZTP デバイスエントリの値を入力します。

各デバイスエントリに必要な情報については、「ZTP デバイスエントリファイルの作成 （251 ページ）」のテンプレートリファレンスを参照してください。

ZTP でデバイスをオンボーディングすると、Cisco Crosswork はデバイスの地理的位置など、デバイスに関する詳細情報を要求するフィールドを表示します。「オンボーディング済み ZTP デバイス情報の入力 （283 ページ）」の説明に従って、デバイスのインベントリレコードを編集して、この追加情報を提供する必要があります。

ステップ 5 [保存（Save）] をクリックします。

ZTP プロビジョニングのワークフロー

ZTP の設定が完了したら、次のようにデバイスをプロビジョニングして維持できます。

1. ZTP 処理をトリガーした後、Cisco Crosswork がイメージと設定ソフトウェアを安全にダウンロードできるように DHCP を設定します。
2. 作成した ZTP デバイスエントリの CSV ファイルを Cisco Crosswork にアップロードします。ファイルをインポートすると、オンボーディング時に ZTP が入力するデバイスエントリが作成されます。少数の ZTP デバイスのみをオンボーディングする場合は、代わりに ZTP ユーザーインターフェイスを使用してデバイスエントリを作成します。
3. 各デバイスの電源の再投入または CLI の再起動の実行によって ZTP 処理をトリガーします。
4. オンボーディングされるデバイスの情報を入力します。それらを編集し、（たとえば）プロビジョニング時に ZTP が検出できなかった地理的位置情報を入力します。

このコアワークフローを完了すると、次のトピックのアドバイスと方法を使用して、ZTP デバイスの継続的なメンテナンスを実行できます。

- 追加情報で ZTP デバイスを更新します。
- オンボーディング後、他のアプリケーションを使用するか、デバイスを削除して再オンボーディングした後、ZTP デバイスを再設定します。
- デバイスライセンスを消費することなく、ZTP デバイスを廃止または交換します。
- デバイスのオンボーディングに使用した ZTP アセットでハウスキーピングを実行します。
- ZTP 処理およびデバイスの問題をトラブルシューティングします。

この項の残りのトピックでは、これらの各タスクの実行方法について説明します。

ZTP デバイスエントリのアップロード

次に、事前に作成した ZTP デバイスエントリ CSV ファイルをインポートして、複数の ZTP デバイスエントリを作成する手順を示します。

インポートした ZTP デバイスエントリは、[ゼロタッチデバイス（Zero Touch Devices）] タブに常に [ステータスが（Status）] が [プロビジョニングなし（Unprovisioned）] に設定された状態で表示されます。これらは、ZTP 処理をトリガーするまで [プロビジョニングなし（Unprovisioned）] のままになります。

ステップ 1 メインメニューから **[デバイス管理（Device Management）]** > **[ネットワークデバイス（Network Devices）]** を選択します。

ステップ 2 [ゼロタッチデバイス（Zero Touch Devices）] タブをクリックします。

ステップ 3 をクリックします。

ステップ 4 [参照（Browse）] をクリックし、作成した ZTP デバイスエントリ CSV ファイルに移動してそのファイルを選択します。

ステップ 5 CSV ファイルを選択した状態で、[インポート（Import）] をクリックします。

Crosswork ZTP での DHCP の設定

ZTP 処理をトリガーする前に、Cisco Crosswork がデバイスと通信してダウンロード要求に応答できるように、DHCP（および PnP ZTP の場合は TFTP）サーバー設定を更新する必要があります。

次のトピックでは、この要件を満たすようにサーバー設定を更新する例を示します。次の手順と例は、使用する ZTP モードによって異なります。

- クラシック ZTP については、「クラシック ZTP での DHCP の設定 （260 ページ）」を参照してください。
- セキュア ZTP については、「セキュア ZTP での DHCP の設定 （264 ページ）」を参照してください。
- PnP ZTP については、「PnP ZTP での DHCP と TFTP の設定 （266 ページ）」を参照してください。
- クラシック ZTP と Cisco PNR の設定スクリプトのセットについては、「Cisco Prime Network Registrar（CPNR）でのクラシック ZTP DHCP の設定スクリプト （266 ページ）」を参照してください。

クラシック ZTP での DHCP の設定

ZTP 処理をトリガーする前に、ZTP デバイスとそれらに適用するソフトウェアを特定する情報を使用して DHCP 設定ファイルを更新します。この情報により、Cisco Crosswork と DHCP は ZTP デバイスを識別し、ネットワーク接続とファイルのダウンロードの要求に応答できるようになります。

以降のトピックでは、この要件を満たすように DHCP サーバー設定を更新する例を示します。これらのトピックの例では、次の図に示す DHCP コンテキスト設定を前提としています。図は、Internet Systems Consortium DHCP サーバーの設定例を示しています。

図 *34 :* クラシック *ZTP DHCP* コンテキスト

```
#
authoritative;

default-lease-time 7200;
max-lease-time 7200;

subnet 192.168.100.0 netmask 255.255.255.0 {
  option routers 192.168.100.1;
  option domain-name "cisco.com";
  option domain-name-servers 171.70.168.183;
```

```
  option subnet-mask 255.255.255.0;
  range 192.168.100.105 192.168.100.195;
}
```

例：クラシック ZTP の DHCP 設定

セキュア ネットワーク ドメインのみを介してデバイスをプロビジョニングする場合は、クラシック ZTP を使用することを強くお勧めします。

クラシック ZTP でサポートされているシスコのデバイスでは、HTTP 経由でのみ iPXE ソフトウェアイメージをダウンロードできます。これらの同じデバイスは、HTTP または HTTPS を介した設定ファイルのダウンロードをサポートしています。これらのオプションでは、組織の DHCP サーバー設定に DHCP ブートファイル URL のエントリが必要です。

イメージと設定ファイルのダウンロードの両方に HTTP を使用する場合は、これらの URL で HTTP プロトコルとポート 30604 を指定する必要があります。詳細については、図 1 と 2 の例を参照してください。

設定ファイルのダウンロードのみに HTTPS を使用する場合は、URL で HTTPS プロトコルとポート 30603 を指定する必要があります。URL の HTTPS プロトコルの前に -k オプションを指定します。ヘルプについては、図 3 および 4 の例を参照してください。

ZTP では、設定のダウンロードに DHCP Option 82 を使用できます。Option 82（DHCP リレーエージェント情報オプションとも呼ばれる）は、IP スプーフィングや MAC スプーフィング、または DHCP アドレス枯渇を使用した攻撃からデバイスを保護します。Option 82 を使用すると、オンボーディングしりデバイスとデバイス要求を解決する DHCP サーバー間に配置された中間ルータまたは中継ルータを指定できます。このオプションを使用するには、ロケーション ID を指定します。ロケーション ID は、回線 ID（インターフェイスまたは VLAN ID）とリモート ID（ホスト名）で構成されます。図 2 および 4 の例に示すように、これらの値を設定ダウンロード URL のパラメータとして指定します。Option 82 の詳細については、RFC 3046（http://tools.ietf.org/html/rfc3046）を参照してください。

次の例に従う場合：

- <*CW_HOST_IP*> を Cisco Crosswork クラスタの IP アドレスに必ず置き換えてください。
- <*IMAGE_UUID*> を ZTP リポジトリのソフトウェアイメージファイルの UUID に置き換えます。ブートファイル名と UUID の使用に関するヘルプについては、このトピックの後のセクション「DHCP セットアップ用のブートファイル名と UUID のコピー」を参照してください。
- 設定ファイルには UUID は必要ありません。

図 *35 : HTTP* を使用したクラシック *ZTP DHCP* の設定

```
host cztp1 {
 hardware ethernet 00:a7:42:86:54:f1;
  if exists user-class and option user-class = "iPXE" {
     filename =
"http://<CW_HOST_IP>:30604/crosswork/imagesvc/v1/device/files/<IMAGE_UUID>";
  } else if exists user-class and option user-class ="exr-config" {
     filename = "http://<CW_HOST_IP>:30604/crosswork/configsvc/v1/file";
  }
}
```

図 *36 : HTTP* と *Option 82* を使用したクラシック *ZTP DHCP* の設定

```
host cztp2 {
 hardware ethernet 00:a7:42:86:54:f2;
  if exists user-class and option user-class = "iPXE" {
     filename =
"http://<CW_HOST_IP>:30604/crosswork/imagesvc/v1/device/files/<IMAGE_UUID>";
  } else if exists user-class and option user-class ="exr-config" {
     filename =
"http://<CW_HOST_IP>:30604/crosswork/configsvc/v1/file?circuitid=Gig001&remoteid=MAR1";
  }
}
```

図 *37 : HTTPS* を使用したクラシック *ZTP DHCP* の設定

```
host cztp3 {
 hardware ethernet 00:a7:42:86:54:f3;
  if exists user-class and option user-class = "iPXE" {
     filename =
"http://<CW_HOST_IP>:30604/crosswork/imagesvc/v1/device/files/<IMAGE_UUID>";
  } else if exists user-class and option user-class ="exr-config" {
     filename = "-k https://<CW_HOST_IP>:30603/crosswork/configsvc/v1/file";
  }
}
```

図 *38 : HTTPS* と *Option 82* を使用したクラシック *ZTP DHCP* の設定

```
host cztp4 {
 hardware ethernet 00:a7:42:86:54:f4;
  if exists user-class and option user-class = "iPXE" {
     filename =
"http://<CW_HOST_IP>:30604/crosswork/imagesvc/v1/device/files/<IMAGE_UUID>";
  } else if exists user-class and option user-class ="exr-config" {
     filename = "-k
https://<CW_HOST_IP>:30603/crosswork/configsvc/v1/file?circuitid=Gig001&remoteid=MAR1";
  }
}
```

例：クラシック ZTP での Generic Internet Systems Consortium（ISC）DHCP の設定

次の図に、Internet Systems Consortium（ISC）DHCP サーバーの `/etc/dhcp/dhcp.conf` 設定ファイルでクラシック ZTP に対して作成するホストエントリのタイプの例を示します。

他のサードパーティ製DHCPサーバーは全体的な実装が異なりますが、多くの場合はこれらのISC の例と同様のオプションと形式を使用します。

これらの新しいエントリの作成が完了したら、ISC DHCP サーバーを必ずリロードするか、または再起動します。

図 *39 :* クラシック *ZTP ISC IPv4 DHCP* の設定例

```
host NCS5k-1
{
    option dhcp-client-identifier "FOC2302R09H";
    hardware ethernet 00:cc:fc:bb:be:6a;
    fixed-address 105.1.1.16;
    if exists user-class and option user-class = "iPXE" {
        filename = "http://<CW_HOST_IP>:30604/crosswork/imagesvc/v1/device/files/
           <IMAGE_UUID>
    } else if exists user-class and option user-class = "exr-config" {
        filename = "http://<CW_HOST_IP>:30604/crosswork/configsvc/v1/file";
```

```
    }
}
```

図 *40 :* クラシック *ZTP ISC IPv6 DHCP*の設定例

```
host 5501
{
    host-identifier option dhcp6.client-id
00:02:00:00:00:09:46:4f:43:32:33:30:38:52:30:53:33:00;
    fixed-address6 fc00:15:2::36;
    if exists dhcp6.user-class and substring(option dhcp6.user-class, 2, 4) = "iPXE" {
      option dhcp6.bootfile-url
"http://<CW_HOST_IP>:30604/crosswork/imagesvc/v1/device/files/
        <IMAGE_UUID>";
    } else {if exists dhcp6.user-class and substring(option dhcp6.user-class, 0, 10) =
"exr-config" {
      option dhcp6.bootfile-url
"http://<CW_HOST_IP>:30604/crosswork/crosswork/configsvc/vl/file";
    }
}
```

次の表に、IPv4 ISC DHCP デバイスエントリの例内の各行と、使用される値のソースを示します。IPv6 の例のエントリの説明は同じですが、IPv6 のアドレッシング方式に適合させています。

表 *18 : ISC IPv4 DHCP* 設定のホストエントリと値（クラシック *ZTP*）

IPv4 エントリ	説明
`host NCS5k-1`	デバイスエントリのホスト名。ホスト名は、実際に割り当てられたホスト名と同じにすることができますが、同じである必要はありません。
`option dhcp-client-identifier`	デバイスエントリの一意の ID。IPv4 の例に示されている値「`FOC2302R09H`」は、デバイスのシリアル番号です。シリアル番号はデバイスのシャーシで確認できます。デバイスに物理的にアクセスできない場合は、IOS-XR の `show inventory` コマンドでシリアル番号が表示されます。
`hardware ethernet 00:cc:fc:bb:be:6a`	デバイスのイーサネット NIC ポートの MAC アドレス。このアドレスは、ZTP プロセスをトリガーするアドレスです。Cisco Crosswork から到達可能なアドレスであれば、管理ポートまたはデータポートを指定できます。
`fixed-address 105.1.1.16`	設定時にデバイスに割り当てられる IP アドレス。この例は静的 IP の場合ですが、標準の DHCP IP のプール割り当てコマンドを使用することもできます。

IPv4 エントリ	説明
`option user-class = "iPXE"` and `filename =`	この行は、着信 ZTP 要求に「`iPXE`」オプションが含まれていることを確認します。クラシック ZTP では、このオプションを使用してデバイスをイメージ化します。要求にこのオプションが含まれている場合、デバイスは、`filename =` パラメータで指定された UUID とパスに一致するイメージファイルをダウンロードします。
`option user-class = "exr-config"` and `ffl filename =`	この行は、着信 ZTP 要求に「`exr-config`」オプションが含まれていることを確認します。ZTP はこのオプションを使用してデバイスを設定します。要求にこのオプションが含まれている場合、デバイスは `filename =` パラメータで指定されたパスに一致する設定ファイルをダウンロードします。

DHCP 設定用のブートファイル名と UUID のコピー

DHCPサーバーの設定ファイルを変更する場合は、各ソフトウェアイメージのブートファイル名と UUID を指定します。すでに Cisco Crosswork にアップロードしたソフトウェアイメージのリストから、両方をクリップボードに直接コピーできます。設定ファイルにはUUIDは必要ありません。

ソフトウェアイメージのブートファイル名と UUID をコピーするには、次の手順を実行します。

1. メインメニューから **[デバイス管理（Device Management）]** > **[ソフトウェアイメージ（Software Images）]** を選択します。
2. コピーする場合は、次の手順を実行します。
   - ソフトウェアイメージのブートファイル名と UUID：[イメージ/SMU 名（Image/SMU Name）] 列の をクリックします。
   - ソフトウェアイメージの UUID のみ：[イメージの UUID（Image UUID）] 列の をクリックします。

   Cisco Crosswork によってブートファイル名と UUID がクリップボードにコピーされます。これを DHCP ホストエントリに貼り付けることができます。

   コピーしたファイルパスを使用して DHCP ホストエントリを作成する場合は、*IP* 変数を Cisco Crosswork サーバーの IP アドレスとポートに置き換えます。

セキュア ZTP での DHCP の設定

セキュア ZTP 処理をトリガーする前に、ZTP デバイスとそれらに適用するソフトウェアを特定する情報を使用して DHCP 構成ファイルを更新します。この情報により、Cisco Crosswork と DHCP は ZTP デバイスを識別し、ネットワーク接続とファイルのダウンロードの要求に応答できるようになります。

次に、この要件を満たすようにDHCPサーバー構成ファイルを更新する方法を示す例を示します。この例では、インターネット システム コンソーシアム（ICS）DHCP サーバーを使用していることを前提としています。セキュア ZTP には、`sztp-redirect` オプションを有効にする行が必要です。

デバイスはオプション 143 とともにユーザークラスオプション `xr-config` を送信するため、これはホストブロックの一部として示されているように設定する必要があることに注意してください。

図 *41* : セキュア *ZTP DHCP* 構成ファイル

```
# dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#
# Attention: If /etc/ltsp/dhcpd.conf exists, it will be used as the
# configuration file instead of this file.
#

# option definitions common to all supported networks...
option domain-name "cisco.com";
option domain-name-servers 192.168.100.101, 171.70.168.183;
option sztp-redirect code 143 = text;
option subnet-mask 255.255.255.0;
default-lease-time 600;
max-lease-time 7200;
INTERFACES="ens192";

# The ddns-updates-style parameter controls whether or not the server will
# attempt to do a DNS update when a lease is confirmed. We default to the
# behavior of the version 2 packages ('none'), since DHCP v2 does not
# have support for DDNS.
#ddns-update-style none;

# If this DHCP server is the official DHCP server for the local
# network, uncomment the "authoritative" directive below.
#authoritative;

# Use this to send dhcp log messages to a different log file (you also
# have to hack syslog.conf to complete the redirection).
#log-facility local7;

# No service will be given on this subnet, but declaring it helps the
# DHCP server to understand the network topology.

subnet 192.168.100.0 netmask 255.255.255.0 {
 option routers 192.168.100.100;
 range 192.168.100.105 192.168.100.150;
}

host sztpdevice {
 hardware ethernet 08:4f:a9:0e:43:c8;
 fixed-address 192.168.100.153;
  if exists user-class and option user-class ="xr-config" {
# If you want to use a remote circuit ID to identify a remote host
# comment out the first option line and uncomment the second.
     option sztp-redirect
"https://<CrossworkHostIP>:30617/restconf/operations/ietf-sztp-bootstrap-server:get-bootstrap-data";

     #option sztp-redirect
"https://<CrossworkHostIP>:30617/restconf/operations/ietf-sztp-bootstrap-server:get-bootstrap-data?remoteid=MAR1&circuitid=Gig001";
```

```
  }
}
```

PnP ZTP での DHCP と TFTP の設定

PnP ZTP 処理をトリガーする前に、次の手順を実行する必要があります。

1. ASR 900 デバイスと NCS 520 デバイスから到達可能な外部 TFTP サーバーを設定します。
2. PnP プロファイルを外部 TFTP サーバーにアップロードします。
3. Cisco Crosswork PnP サーバーの場所を示す情報で DHCP 設定ファイルを更新します。

この情報により、Cisco Crosswork が許可されます。

以降のトピックでは、これらの各タスクを実行する例を示します。

外部 TFTP サーバーの設定

サポートされているすべての Cisco ASR 900 シリーズと NCS 520 シリーズのルータには、外部 TFTP サーバが必要です。サーバーはポート 69 UDP でアクティブである必要があります。

TFTP への PnP プロファイルのアップロード

PnPプロファイルは、単純な汎用設定ファイルです。TFTPリポジトリの設定サービスへのPnPプロファイルのアップロードは、1 回限りのアクティビティです。

プロファイルの内容で、Crosswork クラスタの仮想データポートの使用を指定する必要があります。この例では、IP アドレス 192.168.100.211 は組み込み Cisco Crosswork PnP サーバーのデータ VIP であり、30620 は PnP サーバーの外部ポートです。

図 *42 :* 例：汎用 *PnP* プロファイル

```
pnp profile cwpnp-data
transport http ipv4 192.168.100.211 port 30620
```

DHCP サーバーの設定

DCHCP エントリは、デバイス上の PnP エージェントから外部 TFTP サーバーの IP アドレスにトラフィックをリダイレクトします。

図 *43 : PnP ZTP DHCP* の設定例

```
option tftp code 150 = text;
host cztp1 {
 hardware ethernet 00:a7:42:86:54:f1;
  option tftp150 "192.168.100.205":
   }
```

Cisco Prime Network Registrar（CPNR）でのクラシック ZTP DHCP の設定スクリプト

次に示すのは、クラシックZTPデバイス、イメージ、および設定ファイルのエントリをCPNR DHCP サーバーの設定ファイルに追加できるスクリプトの 2 セットです。IPv4 用に 3 つのスクリプトが 1 セット、IPv6 用に 5 つのスクリプトがもう 1 セットあります。

（注） 次のスクリプトは、クラシック ZTP 専用です。セキュア ZTP または PnP ZTP では使用できません。

これらのスクリプトを使用するには、次の手順を実行します。

1. スクリプトの内容をコピーして、ここに示す名前のローカルテキストファイルに貼り付けます。
2. スクリプトのコメントで説明されているように、`ztp-v4-setup-vi-nrcmd.txt` スクリプトまたは `ztp-v6-setup-vi-nrcmd.txt` スクリプトのデバイス、イメージ、および設定エントリを必要に応じて変更します。
3. 使用するスクリプトファイルをローカル CPNR サーバーのルートフォルダにコピーします。
4. 次のコマンドを使用して、CPNR サーバーでスクリプトを実行します。

   ```
   [root@cpnr-local ~]#/opt/nwreg2/local/usrbin/nrcmd -N username -P password
   <ztp-IPVersion-setup-via-nrcmd.txt
   ```

   ここで、

   - *username* は、CPNR サーバーで管理者権限を持つユーザー ID の名前です。
   - *password* は、対応する CPNR 管理者のユーザー ID のパスワードです。
   - *IPVersion* は IPv4 バージョンのスクリプトの場合は `v4`、IPv6 バージョンのスクリプトの場合は `v6` です。

図 *44 : IPv4* スクリプト *1/3* : *ztp-v4-setup-vi-nrcmd.txt*

```
#
# Create the scope
#
scope ztp-ncs-5501-mgmt create 192.0.20.0/24

# Add the dynamic range
scope ztp-ncs-5501-mgmt addrange 200 225

# Default the routers option. Note: No need to do subnet-mask. It is automatically
provided.
scope-policy ztp-ncs-5501-mgmt setoption routers 10.10.10.1

# Set the lease time for clients on this scope
scope-policy ztp-ncs-5501-mgmt setoption dhcp-lease-time 216000
#
# Load the option 43 definitions
import option-set ztp-v4-option-set.txt
#
# Set the client classing expression and enable use of client-class
dhcp set client-class-lookup-id=@ztp-v4-client-class-expr.txt
dhcp enable client-class
#
# Load the client classes - these are used to lookup the correct client details
# depending on whether an iso or script is requested by the client.
```

```
client-class ztp-iso create
client-class ztp-iso set client-lookup-id="(or (try (concat (as-string
    (request get option 61)) \"-iso\")) (request macaddress-string))"
#
client-class ztp-script create
client-class ztp-script set client-lookup-id="(or (try (concat (as-string
    (request get option 61)) \"-script\")) (request macaddress-string))"
#
# Clients that are not ztp will fall into the ztp-none class
# and should not be offered service so they are excluded.
#
client-class ztp-none create
client-class ztp-none set action=exclude
#
# Create a default client that will prevent service to unknown clients.
client default create
client default set action=exclude
#
# Create some ZTP clients
#
# For each ZTP client we create two clients based on their serial number.
# (See above for the client-lookup-id expressions.)
# One has "-iso" added to the end that will be used when the client's
# request includes "iPXE" in option 77.
# The other has "-script" added to the end that will be used when the
# client's request includes "exr-config" in option 77.
#

### Device-1 Settings ####
client <device-1-serial-num>-iso create
client-policy <device-1-serial-num>-iso set packet-file-name=

"http://<cw-ipv4-address>:30604/crosswork/imagesvc/v1/device/files/cw-image-uuid-d3930e13-b081-4905-b2e5-051249d9b0db"


client <device-1-serial-num>-script create
client-policy <device-1-serial-num>-script set packet-file-name=

"http://<cw-ipv4-address>:30604/crosswork/configsvc/v1/configs/device/files/d1d7b441-3a27-47d1-aef0-39c3087d34c1"
client-policy <device-1-serial-num>-script setvendoroption 43 Cisco-ZTP "(1 exr-config)(2
 0)"

### Device-2 Settings ####
client <device-2-serial-num>--iso create
client-policy <device-2-serial-num>-iso set packet-file-name=

"http://<cw-ipv4-address>:30604/crosswork/imagesvc/v1/device/files/cw-image-uuid-d3930e13-b081-4905-b2e5-051249d9b0db"


client <device-2-serial-num>-script create
client-policy <device-2-serial-num>-script set packet-file-name=

"http://<cw-ipv4-address>:30604/crosswork/configsvc/v1/configs/device/files/d1640deb-8252-47b6-aab1-a843c0c7757b"
client-policy <device-2-serial-num>-script setvendoroption 43 Cisco-ZTP "(1 exr-config)(2
 0)"

#
# Create more as needed using the above as models.
# Note: For those that need option 67 (boot file), you can use:
#   client-policy <name> setoption boot-file "<file-url>"
#
# The next line is optional. Uncomment it if you want to log what the script is doing.
# dhcp set log-settings=+incoming-packet-detail,outgoing-packet-detail,client-detail
```

```
# Assure that the server is up-to-date with this configuration
dhcp reload
```

図 *45 : IPv4* スクリプト *2/3* : *ztp-v4-setup-vi-nrcmd.txt*

```
#
# Create the scope
#
scope ztp-ncs-5501-mgmt create 192.0.20.0/24

# Add the dynamic range
scope ztp-ncs-5501-mgmt addrange 200 225

# Default the routers option. Note: No need to do subnet-mask. It is automatically
provided.
scope-policy ztp-ncs-5501-mgmt setoption routers 10.10.10.1

# Set the lease time for clients on this scope
scope-policy ztp-ncs-5501-mgmt setoption dhcp-lease-time 216000
#
# Load the option 43 definitions
import option-set ztp-v4-option-set.txt
#
# Set the client classing expression and enable use of client-class
dhcp set client-class-lookup-id=@ztp-v4-client-class-expr.txt
dhcp enable client-class
#
# Load the client classes - these are used to lookup the correct client details
# depending on whether an iso or script is requested by the client.
client-class ztp-iso create
client-class ztp-iso set client-lookup-id="(or (try (concat (as-string
    (request get option 61)) \"-iso\")) (request macaddress-string))"
#
client-class ztp-script create
client-class ztp-script set client-lookup-id="(or (try (concat (as-string
    (request get option 61)) \"-script\")) (request macaddress-string))"
#
# Clients that are not ztp will fall into the ztp-none class
# and should not be offered service so they are excluded.
#
client-class ztp-none create
client-class ztp-none set action=exclude
#
# Create a default client that will prevent service to unknown clients.
client default create
client default set action=exclude
#
# Create some ZTP clients
#
# For each ZTP client we create two clients based on their serial number.
# (See above for the client-lookup-id expressions.)
# One has "-iso" added to the end that will be used when the client's
# request includes "iPXE" in option 77.
# The other has "-script" added to the end that will be used when the
# client's request includes "exr-config" in option 77.
#

### Device-1 Settings ####
client <device-1-serial-num>-iso create
client-policy <device-1-serial-num>-iso set packet-file-name=

"http://<cw-ipv4-address>:30604/crosswork/imagesvc/v1/device/files/cw-image-uuid-d3930e13-b081-4905-b2e5-051249d9b0cb"


client <device-1-serial-num>-script create
```

```
client-policy <device-1-serial-num>-script set packet-file-name=

"http://<cw-ipv4-address>:30604/crosswork/configsvc/v1/configs/device/files/d1d7b441-3a27-47d1-aef0-39c3087d34c1"
client-policy <device-1-serial-num>-script setvendoroption 43 Cisco-ZTP "(1 exr-config)(2
 0)"

### Device-2 Settings ####
client <device-2-serial-num>--iso create
client-policy <device-2-serial-num>-iso set packet-file-name=

"http://<cw-ipv4-address>:30604/crosswork/imagesvc/v1/device/files/cw-image-uuid-d3930e13-b081-4905-b2e5-051249d9b0db"


client <device-2-serial-num>-script create
client-policy <device-2-serial-num>-script set packet-file-name=

"http://<cw-ipv4-address>:30604/crosswork/configsvc/v1/configs/device/files/d1640deb-8252-47b6-aab1-a843c0c7757b"
client-policy <device-2-serial-num>-script setvendoroption 43 Cisco-ZTP "(1 exr-config)(2
 0)"

#
# Create more as needed using the above as models.
# Note: For those that need option 67 (boot file), you can use:
#   client-policy <name> setoption boot-file "<file-url>"
#
# The next line is optional. Uncomment it if you want to log what the script is doing.
# dhcp set log-settings=+incoming-packet-detail,outgoing-packet-detail,client-detail

# Assure that the server is up-to-date with this configuration
dhcp reload
```

図 *46 : IPv4* スクリプト *3/3* : *ztp-v4-client-class-expr.txt*

```
(or
   (if (equal (as-string (request get-blob option 77)) "iPXE") "ztp-iso")
   (if (equal (as-string (request get-blob option 77)) "exr-config") "ztp-script")
   "ztp-none"
)
```

図 *47 : IPv6* スクリプト *1/5* : *ztp-v6-setup-vi-nrcmd.txt*

```
#
# create prefix for mgmt
prefix prefix-for-mgmt create 2001:DB8:10e:201a::/64
#
# Set the client classing expression and enable use
# of client-class
#
dhcp set v6-client-class-lookup-id=@ztp-v6-client-class-expr.txt
dhcp enable client-class
#
# Load the client classes - these are used to lookup the correct
# client details depending on whether an iso or script is requested
# by the client.
#
client-class ztp-iso create
client-class ztp-iso set v6-client-lookup-id=@ztp-v6-iso-lookup-expr.txt
#
client-class ztp-script create
client-class ztp-script set v6-client-lookup-id=@ztp-v6-script-lookup-expr.txt
client-class-policy ztp-script set v6-reply-options=17
#
# Delete option set (may not exist and ok if fails)
```

```
#
option-set dhcp6-cisco-custom delete
#
import option-set ztp-v6-options.txt
#
# Clients that are not ztp will fall into the ztp-none class
# and should not be offered service so they are excluded.
#
client-class ztp-none create action=exclude
#
# Create a default client that will prevent service to
# unknown clients.
#
client default create
client default set action=exclude
#
# Create some ZTP clients
#
# For each ZTP client we create two clients based on their mac-address.
# One has "-iso" added to the end that will be used when the client's
# request does not include the "exr-config" in option 77.
# The other has "-script" added to the end that will be used when the
# client's request does include "exr-config" in option 77.
#
client <device-serial-no>-iso create
# Set the vendor options using blob format as option definitions are for different data
client-policy <device-serial-no>-iso setV6VendorOption 17 dhcp6-cisco-custom "(1
exr-config)(2 0)"
# Escape the [ and ] as nrcmd (which uses tcl interpreter) will otherwise fail command
client-policy <device-serial-no>-iso setv6option bootfile-url

"http://\[cw-ipv6-address\]:30604/crosswork/imagesvc/v1/device/files/cw-image-uuid-aec596

      a1-7847-4254-966a-2456aa5"
#
client <device-serial-no>-script create
# Set the vendor options using blob format as option definitions are for different data
client-policy <device-serial-no>-script setV6VendorOption 17 dhcp6-cisco-custom "(1
exr-config)(2 0)"
# Escape the [ and ] as nrcmd (which uses tcl interpreter) will otherwise fail command
client-policy <device-serial-no>-script setv6option bootfile-url
   "http://\[cw-ipv6-address\]:30604/crosswork/configsvc/v1/configs/device/files/8eb6b7e1

      -bd54-40bb-84e0-89f11a60128b"
#

# Assure the server is up-to-date with this configuration
dhcp reload
```

図 *48 : IPv6* スクリプト *2/5* : *ztp-v6-client-class-expr.txt*

```
(or (try (if (equal (as-string (request get option 15)) "exr-config") "ztp-script"))
    (try (if (equal (as-string (request get option 15)) "iPXE") "ztp-iso"))
   "ztp-none"
)
```

図 *49 : IPv6* スクリプト *3/5* : *ztp-v6-iso-lookup-expr.txt*

```
(let (id)
  (setq id (request get option 1))
  (or
# First try extracting the serial number from DUID
```

```
      (try (if (equali (substring id 0 6) 00:02:00:00:00:09)
                (concat (as-string (substring id 6 128)) "-script")
           )
      )
# If that fails, use normal client-id (DUID) lookup
     (concat (to-string id) "-iso")

  )
)
```

図 *50 : IPv6* スクリプト *4/5* : ***ztp-v6-script-lookup-expr.txt***

```
(let (id)
  (setq id (request get option 1))
  (or
# First try extracting the serial number from DUID
      (try (if (equali (substring id 0 6) 00:02:00:00:00:09)
                (concat (as-string (substring id 6 128)) "-script")
           )
      )
# If that fails, use normal client-id (DUID) lookup
     (concat (to-string id) "-script")
  )
)
```

図 *51 : IPv6* スクリプト *5/5* : ***ztp-v6-options.txt***

```
# Option Definition Set Export/Import Utility
# Version: 1
#
{
  ( name = dhcp6-cisco-custom )
  ( desc = Cisco Systems, Inc. )
  ( vendor-option-enterprise-id = 9 )
  ( id-range = 2 )
  ( option-list = [
    {
      ( name = cisco-17 )
      ( id = 17 )
      ( base-type = AT_VENDOR_OPTS )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
      ( option-list = [
        {
          ( name = clientID )
          ( id = 1 )
          ( base-type = AT_NSTRING )
          ( sepstr = , )
          ( desc = ZTP - clientID )
        }
        {
          ( name = authCode )
          ( id = 2 )
          ( base-type = AT_INT8 )
          ( sepstr = , )
          ( desc = ZTP - authCode )
        }
        {
          ( id = 3 )
          ( name = md5sum )
          ( base-type = AT_NSTRING )
          ( desc = ZTP - md5sum )
        }
```

```
{
  ( name = cnr-leasequery )
  ( id = 13 )
  ( base-type = AT_BLOB )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
  ( option-list = [
    {
      ( name = oro )
      ( id = 1 )
      ( base-type = AT_SHORT )
      ( flags = AF_IMMUTABLE )
      ( repeat = ZERO_OR_MORE )
      ( sepstr = , )
    }
    {
      ( name = dhcp-state )
      ( id = 2 )
      ( base-type = AT_INT8 )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = data-source )
      ( id = 3 )
      ( base-type = AT_INT8 )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = start-time-of-state )
      ( id = 4 )
      ( base-type = AT_TIME )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = base-time )
      ( id = 5 )
      ( base-type = AT_DATE )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = query-start-time )
      ( id = 6 )
      ( base-type = AT_DATE )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = query-end-time )
      ( id = 7 )
      ( base-type = AT_DATE )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = client-class-name )
      ( id = 8 )
      ( base-type = AT_NSTRING )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
```

```
{
  ( name = partner-last-transaction-time )
  ( id = 9 )
  ( base-type = AT_TIME )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = client-creation-time )
  ( id = 10 )
  ( base-type = AT_TIME )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = limitation-id )
  ( id = 11 )
  ( base-type = AT_BLOB )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = binding-start-time )
  ( id = 12 )
  ( base-type = AT_TIME )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = binding-end-time )
  ( id = 13 )
  ( base-type = AT_STIME )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = fwd-dns-config-name )
  ( id = 14 )
  ( base-type = AT_NSTRING )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = rev-dns-config-name )
  ( id = 15 )
  ( base-type = AT_NSTRING )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = lookup-key )
  ( id = 16 )
  ( base-type = AT_BLOB )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = user-defined-data )
  ( id = 17 )
  ( base-type = AT_NSTRING )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
```

```
      ( name = prefix-name )
      ( id = 18 )
      ( base-type = AT_NSTRING )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = failover-state-serial-number )
      ( id = 19 )
      ( base-type = AT_INT )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = reservation-key )
      ( id = 20 )
      ( base-type = AT_BLOB )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = failover-partner-lifetime )
      ( id = 21 )
      ( base-type = AT_STIME )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = failover-next-partner-lifetime )
      ( id = 22 )
      ( base-type = AT_STIME )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = failover-expiration-time )
      ( id = 23 )
      ( base-type = AT_STIME )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = client-oro )
      ( id = 24 )
      ( base-type = AT_SHORT )
      ( flags = AF_IMMUTABLE )
      ( repeat = ZERO_OR_MORE )
      ( sepstr = , )
    }
  ] )
}
{
  ( name = failover )
  ( id = 21 )
  ( base-type = AT_BLOB )
  ( flags = AF_NO_CONFIG_OPTION,AF_SUPPORTS_ENCAP_OPTION,AF_IMMUTABLE )
  ( sepstr = , )
  ( option-list = [
    {
      ( name = server-state )
      ( id = 1 )
      ( base-type = AT_INT8 )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
```

```
}
{
  ( name = server-flags )
  ( id = 2 )
  ( base-type = AT_INT8 )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = binding-status )
  ( id = 3 )
  ( base-type = AT_INT8 )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = binding-flags )
  ( id = 4 )
  ( base-type = AT_INT8 )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = start-time-of-state )
  ( id = 5 )
  ( base-type = AT_DATE )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = state-expiration-time )
  ( id = 6 )
  ( base-type = AT_DATE )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = failover-expiration-time )
  ( id = 7 )
  ( base-type = AT_DATE )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = bndupd-serial )
  ( id = 8 )
  ( base-type = AT_INT )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = bndack-serial )
  ( id = 9 )
  ( base-type = AT_INT )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = client-flags )
  ( id = 10 )
  ( base-type = AT_INT )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
```

```
{
  ( name = vpn-id )
  ( id = 11 )
  ( base-type = AT_INT )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = lookup-key )
  ( id = 12 )
  ( base-type = AT_BLOB )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
  ( option-list = [
    {
      ( name = type )
      ( id = 0 )
      ( base-type = AT_INT8 )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = data )
      ( id = 0 )
      ( base-type = AT_BLOB )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
  ] )
}
{
  ( name = user-defined-data )
  ( id = 13 )
  ( base-type = AT_BLOB )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = reconfigure-data )
  ( id = 14 )
  ( base-type = AT_BLOB )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
  ( option-list = [
    {
      ( name = time )
      ( id = 0 )
      ( base-type = AT_DATE )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = key )
      ( id = 0 )
      ( base-type = AT_BLOB )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
  ] )
}
{
  ( name = requested-fqdn )
  ( id = 15 )
  ( base-type = AT_BLOB )
```

```
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
  ( option-list = [
    {
      ( name = flags )
      ( id = 0 )
      ( base-type = AT_INT8 )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = domain-name )
      ( id = 0 )
      ( base-type = AT_DNSNAME )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
  ] )
}
{
  ( name = forward-dnsupdate )
  ( id = 16 )
  ( base-type = AT_NSTRING )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = reverse-dnsupdate )
  ( id = 17 )
  ( base-type = AT_NSTRING )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = partner-raw-cltt )
  ( id = 18 )
  ( base-type = AT_DATE )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = client-class )
  ( id = 19 )
  ( base-type = AT_NSTRING )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = status-code )
  ( id = 20 )
  ( base-type = AT_BLOB )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
  ( option-list = [
    {
      ( name = status-code )
      ( id = 0 )
      ( base-type = AT_SHORT )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = status-message )
      ( id = 0 )
```

```
      ( base-type = AT_NSTRING )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
  ] )
}
{
  ( name = dns-info )
  ( id = 21 )
  ( base-type = AT_BLOB )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
  ( option-list = [
    {
      ( name = flags )
      ( id = 0 )
      ( base-type = AT_SHORT )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = host-label-count )
      ( id = 0 )
      ( base-type = AT_INT8 )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = name-number )
      ( id = 0 )
      ( base-type = AT_INT8 )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
  ] )
}
{
  ( name = base-time )
  ( id = 22 )
  ( base-type = AT_DATE )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = relationship-name )
  ( id = 23 )
  ( base-type = AT_NSTRING )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = protocol-version )
  ( id = 24 )
  ( base-type = AT_INT )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = mclt )
  ( id = 25 )
  ( base-type = AT_INT )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
```

```
{
  ( name = dns-removal-info )
  ( id = 26 )
  ( base-type = AT_BLOB )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
  ( option-list = [
    {
      ( name = host-name )
      ( id = 1 )
      ( base-type = AT_RDNSNAME )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = zone-name )
      ( id = 2 )
      ( base-type = AT_DNSNAME )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = flags )
      ( id = 3 )
      ( base-type = AT_SHORT )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = forward-dnsupdate )
      ( id = 4 )
      ( base-type = AT_NSTRING )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = reverse-dnsupdate )
      ( id = 5 )
      ( base-type = AT_NSTRING )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
  ] )
}
{
  ( name = max-unacked-bndupd )
  ( id = 27 )
  ( base-type = AT_INT )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = receive-timer )
  ( id = 28 )
  ( base-type = AT_INT )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = hash-bucket-assignment )
  ( id = 29 )
  ( base-type = AT_BLOB )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
```

```
        }
        {
          ( name = partner-down-time )
          ( id = 30 )
          ( base-type = AT_DATE )
          ( flags = AF_IMMUTABLE )
          ( sepstr = , )
        }
        {
          ( name = next-partner-lifetime )
          ( id = 31 )
          ( base-type = AT_DATE )
          ( flags = AF_IMMUTABLE )
          ( sepstr = , )
        }
        {
          ( name = next-partner-lifetime-sent )
          ( id = 32 )
          ( base-type = AT_DATE )
          ( flags = AF_IMMUTABLE )
          ( sepstr = , )
        }
        {
          ( name = client-oro )
          ( id = 33 )
          ( base-type = AT_SHORT )
          ( flags = AF_IMMUTABLE )
          ( repeat = ZERO_OR_MORE )
          ( sepstr = , )
        }
        {
          ( name = requested-prefix-length )
          ( id = 34 )
          ( base-type = AT_INT8 )
          ( flags = AF_IMMUTABLE )
          ( sepstr = , )
        }
      ] )
    }
  ] )
}
```

ZTP デバイスブートストラップのトリガー

Cisco Crosswork にインポートされたデバイスエントリと DHCP が設定されている場合は、各デバイスを再起動することで ZTP 処理を開始できます。

始める前に

いずれかのデバイスで ZTP ブートストラップをトリガーする前に、次の作業が完了していることを確認します。

- 「ZTP 設定のワークフロー（226 ページ）」で説明されているすべての予備設定タスク。
- ZTP デバイスエントリファイルの作成（251 ページ）または 単一 ZTP デバイスエントリの作成（258 ページ）の説明に従ったブートストラップするデバイスの ZTP デバイスエントリの作成。

- Crosswork ZTP での DHCP の設定 （260 ページ） の説明に従った ZTP モードとサーバーの選択に適した DHCP の設定

セキュア ZTP を使用している場合：

1. オンボードする各デバイスのコンソールに Telnet で接続します：`telnet <device IP><userID><password>`。
2. デバイスで Secure ZTP が有効になっているかどうかを確認します。
   1. IOS-XR バージョン 7.5.2 以前の場合：Bash 実行モードに入り、次のコマンドを発行します：`[xr-vm_node:~]$pyztp2 --ztp-mode ZTP モード：セキュア`
   2. 7.5.2 以降の IOS-XR バージョンの場合：IOS CLI コマンドプロンプトに移動し、次のコマンド `show ztp information` を入力します。
3. ログと構成を消去するには、次のコマンドを発行します。

```
ios#ztp clean

ios#config terminal

ios(config)#commit 置換

ios(config)#end
```

PnP ZTP を使用する場合は、ZTP 処理をトリガーする**前に**、各 IOS-XE デバイスの最小ライセンスブートレベルが **metroipaccess** または **advancedmetroipaccess** に設定されていることを確認します。ブートレベルが正しく設定されている場合、デバイスの IOS-XE `#sh run | sec license` CLI コマンドの出力に、2 つのライセンスレベル、`license boot level advancedmetroipaccess` または `license boot level metroipaccess` のいずれかを示すステートメントが含まれている必要があります。コマンド出力にこれらの 2 つより低い他のライセンスレベルが表示された場合、Cisco PnP 暗号化機能が有効になりません。これにより、証明書のインストールが失敗して PnP ZTP デバイスのプロビジョニングが失敗します。

ステップ 1 使用している ZTP モードに適した ZTP 処理を開始します。

- クラシック ZTP の場合は、次のいずれかのオプションを使用します。
  - デバイスの電源を再投入して再起動します。
  - ピンを使用して、デバイスの背面にあるシャーシリセットボタンを押します。15 秒間、またはデバイスの電源ライトが点滅し始めるまで押します。
  - 以前にイメージ化したデバイスの場合は、Telnet 経由でデバイスコンソールに接続し、**ztp initiator** コマンドを発行します。
- セキュア ZTP の場合は、次のいずれかのオプションを使用します。
  - デバイスの電源を再投入して再起動します。

- ピンを使用して、デバイスの背面にあるシャーシリセットボタンを押します。15 秒間、またはデバイスの電源ライトが点滅し始めるまで押します。
- 以前にイメージ化されたデバイスの場合：Telnet 経由でデバイスコンソールに接続し、次のコマンドを発行します（ここで指定された `ztp initiate interface` 値により、デバイス管理ポートでセキュア ZTP が開始されます）：

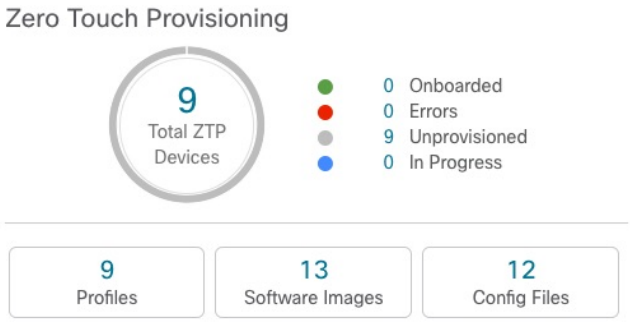
```
ztp enable noprompt

ztp initiate debug verbose interface MgmtEth 0/RP0/CPU0/0
```

- PnP ZTP の場合は、デバイスに適したオプションを使用します。
  - Cisco ASR 903、ASR 907、および NCS 520デバイスの場合は、Telnet 経由で接続し、**write erase** コマンドを発行してから、**reload** コマンドを実行します。
  - Cisco ASR 920 デバイスの場合は、シャーシの ZTP ボタンを 8 秒間押します。

このセッション中にプロビジョニングする予定のデバイスごとに、必要に応じてこの手順を繰り返します。1 回のセッションの間に、すべてのデバイスまたは必要な数のデバイスを再起動できます。

ステップ 2 次の図に示すように、[ゼロタッチプロビジョニング（Zero Touch Provisioning）] ステータスタイルを使用して、ZTP 処理の進行状況をモニターします。タイルを表示するには、メインメニューの [ホーム（Home）] アイコンをクリックします。



タイルには、現在の ZTP 処理ステータスの概要ビューが表示されます。現在使用中のすべての ZTP プロファイル、イメージ、および設定ファイルの数を示します。また、タイルには、可能性がある ZTP 処理状態ごとのデバイスの数も表示されます。

オンボーディング済み ZTP デバイス情報の入力

ZTP デバイスは、オンボーディングされると、自動的に Cisco Crosswork の共有デバイスインベントリに組み込まれます。他のデバイスと同様に編集できます。次の手順では、ZTP を使用してオンボーディングされたデバイスに情報を追加する 2 つの方法について説明します。

デバイスを編集する前に、変更するデバイスの CSV バックアップをエクスポートすることをお勧めします。これは、手順 2 で説明するエクスポート機能を使用して実行できます。

始める前に

完全なデバイス インベントリ レコードに必要な一部の情報が不要であるか、または自動化によって利用できません。たとえば、地理的データで、デバイスが建物内の特定の住所またはGPS座標のセットにあることを示すデータなどです。このようなロケーションデータは、アクティブなネットワークを持つほとんどの組織の要件であり、人間のオペレータによってのみ追加できます。

その他の種類のインベントリ情報は、他のアプリケーションを使用してネットワークを管理する場合に役立ちます。たとえば、Cisco Crosswork タグを使用すると、Cisco Crosswork Health Insights の b KPI を特定のデバイスに簡単に適用できます。同様に、SRE ポリシーをデバイスに関連付けると、Cisco Crosswork Network Controller または Cisco Crosswork Optimization Engine をより簡単に使用できるようになります。Cisco NSO などの一部の Cisco Crosswork プロバイダは、この種の拡張デバイス情報に基づいて便利な機能を提供します。すべては人間による更新が必要です。

他の Cisco Crosswork アプリケーションとプロバイダの機能を使用して、このような情報を追加できます。このトピックの詳細については、アプリケーションのユーザーズマニュアルを参照してください。Cisco Crosswork ZTP を使用して、情報の多くを追加することもできます。

ステップ 1 ZTP デバイスのインベントリレコードを更新するには、次の手順を実行します。

a) メインメニューから **[デバイス管理（Device Management）]** > **[ネットワークデバイス（Network Devices）]** を選択します。
b) [ZTP デバイス（ZTP Devices）] タブをクリックします。
c) 変更するデバイスを選択し、 をクリックします。
d) [ステータス（Status）] フィールドの値を [プロビジョニングなし（Unprovisioned）] に変更します。
e) 必要に応じて、デバイスに設定されている他の値を編集します。
f) [保存（Save）] をクリックします。

ステップ 2 ZTP を使用してオンボーディングされたデバイスを含め、デバイスのインベントリレコードを一括で更新するには、次の手順を実行します。

a) メインメニューから **[デバイス管理（Device Management）]** > **[デバイス（Devices）]** を選択します。
b) をクリックします。CSV ファイルを保存します。
c) 選択したアプリケーションで CSV テンプレートを開き、追加または更新するデバイス情報を編集します。更新しないデバイスの行を削除することをお勧めします。
d) 完了したら、編集した CSV ファイルを保存します。
e) 必要に応じて、**[デバイス管理（Device Management）]** > **[デバイス（Devices）]** を選択し、[ゼロタッチデバイス（Zero Touch Devices）] タブをクリックします。
f) をクリックします。
g) [参照（Browse）] をクリックし、作成した CSV ファイルに移動してそのファイルを選択します。
h) CSV ファイルを選択した状態で、[インポート（Import）] をクリックします。

オンボーディング済み ZTP デバイスの再設定

Cisco Crosswork ZTP の目的は、新しいデバイスのエキスパートを現場に配置することなく、新しいデバイスを迅速かつ簡単にオンボーディングすることです。ZTP は、そのタスクの一部としてイメージ化と設定を実行し、デバイス設定の一部としてスクリプトを実行します。ただし、汎用のデバイス設定ユーティリティとして設計されていないため、このような使い方はしないでください。

ZTP を使用してオンボーディングしたデバイスを再設定する必要がある場合は、次を使用します。

- Cisco Crosswork Change Automation Playbook。オンデマンドでデバイスに設定変更を展開できます。
- Cisco Network Services Orchestrator（Cisco NSO）または使用している Cisco Crosswork の他のプロバイダの設定変更機能。
- デバイスとデバイスの OS コマンド ライン インターフェイスへの直接接続。

これらの方法のいずれも使用できない場合は、デバイスを削除するのが最善の方法です。正しい設定を使用すれば、デバイスを再度オンボーディングできます。

ZTP デバイスを削除するには、**[デバイス管理（Device Management）] > [デバイス（Devices）] > [ゼロタッチデバイス（Zero Touch Devices）]** を選択し、テーブル内のデバイスを選択して をクリックします。

ZTP を使用してオンボーディングしたデバイスの廃止と交換

ZTP を使用してオンボーディングされたシスコのデバイスの廃止が必要な場合があります。デバイスライセンスは、オンボーディング時に入力したデバイスのシリアル番号に関連付けられます。ZTP では、1 台のデバイスを最大 3 つの異なるシリアル番号に関連付けることができます。この事実を使用して、ネットワークと Cisco Crosswork インベントリから障害が発生したデバイスまたは古いデバイスを削除できます。追加のライセンスを消費することなく、後で置き換えることができます。

このルールは、シャーシを備えたデバイスだけでなく、ラインカードやその他の着脱可能なデバイスモジュールにも適用されます。これらの各モジュールには、独自のシリアル番号があります。モジュールの RMA が必要な場合は、古いライセンスを新しいモジュールのシリアル番号に関連付けます。ただし、次の手順に従って、インベントリから古いラインカードとそのシリアル番号を削除します。

1. **[デバイス管理（Device Management）] > [デバイス（Devices）] > [ゼロタッチデバイス（Zero Touch Devices）]** を選択します。
2. テーブルで古いデバイスを見つけ、そのシリアル番号を記録します。
3. デバイスを選択し、 をクリックして削除します。

デバイスを削除した後も、Cisco Crossworkはこのシリアル番号に関連付けられたライセンスを消費済みとしてカウントします。新しいデバイスまたはRMA交換デバイスの購入の一部としてこのライセンスを追跡し、アクティブな使用のために古いデバイスのライセンスを戻すことができます。

Cisco Crossworkでは、同じライセンスを持つアクティブなデバイスを2台設定することはできません。新しいデバイスまたは交換用デバイスをオンボーディングする前に、古いデバイスを削除する必要があります。

4. 新しいデバイスをオンボーディングする場合は、次の手順を実行します。
    1. 新しいデバイスのZTPデバイスエントリを作成する場合は、新しいシリアル番号と古いシリアル番号の両方を入力します。
    2. セキュアZTPを使用している場合は、新しいデバイスの所有権バウチャー要求とともに、古いデバイスと新しいデバイスの両方のシリアル番号を送信します。シスコは、再生成された所有権バウチャーの使用中のライセンスに、古いシリアル番号と新しいシリアル番号を関連付けます。
    3. 他のZTPデバイスと同様に、新しいデバイスをオンボーディングします。古いデバイスライセンスのみが使用されます。

ZTP アセットのハウスキーピング

ZTPによるデバイスのオンボーディングが完了したら、アセンブルしたZTPアセットの一部のオフラインコピーを削除できます。組織のポリシーとベストプラクティスに応じて、他のユーザーを保持します。推奨事項：

- [ZTPプロファイル（ZTP profiles）]：通常は、オンボーディングの完了後にZTPプロファイルを削除しても安全です。ZTPプロファイルを削除するには、**[デバイス管理（Device Management）]** > **[ゼロタッチプロファイル（Zero Touch Profiles）]** を選択します。削除するZTPプロファイルを表すタイルで、⋯をクリックし、ドロップダウンメニューから[削除（Delete）]を選択します。
- [ZTPデバイスエントリCSVファイル（ZTP device entry CSV file）]：このファイルのオフラインコピーを保持してテンプレートとして使用することができます。このファイルは、同じネットワークアーキテクチャとデバイスタイプを共有するブランチオフィスが多数ある場合に便利です。それ以外の場合は、ファイルシステムから削除できます。CSVファイルテンプレートはいつでもダウンロードできます。オンボーディング後に入力したデータを含む、ZTPデバイスのすべてのデータが含まれているバックアップCSVファイルをエクスポートすると便利な場合があります。CSVデバイスのバックアップをエクスポートするには、**[デバイス管理（Device Management Devices）]** > **[デバイス（Devices）]** > **[ゼロタッチデバイス（Zero Touch Devices）]** を選択します。次に、⎘をクリックしてCSVファイルを保存します。
- [ソフトウェアイメージとSMU（Software images and SMUs）]：これらのファイルの実稼働バージョンをオフラインで保存し、組織のポリシーに従って古いバージョンを削除しま

す。同じファミリの複数のデバイスをイメージ化するために使用する場合は、アップロードしたイメージファイルを Cisco Crosswork から削除しないでください。古いイメージを削除するには、**[デバイス管理（Device Management）]**>**[ソフトウェアイメージ（Software Images）]** を選択し、テーブル内のファイルを選択して、 をクリックします。

- [設定ファイル（Configuration files）]：すでに Cisco Crosswork にアップロードしている設定を保持する必要はありませんが、組織のポリシーが異なる場合があります。ZTP を使用して同じファミリのデバイスをさらに設定する場合は、アップロードした設定ファイルを削除しないでください。設定が変更された場合は、保存されているバージョンを簡単に更新できます。新しい設定ファイルまたはスクリプトを作成し、**[デバイス管理（Device Management）]**>**[設定ファイル（Configuration Files）]** を選択し、テーブル内のファイルを選択して、 をクリックします。次に、作成した新しいスクリプトファイルを参照し、新しい設定をコピーして貼り付けることができます。設定が古くなった場合は削除します。**[デバイス管理（Device Management）]** > **[設定ファイル（Configuration Files）]** を選択し、テーブル内のファイルを選択して、 をクリックします。
- [クレデンシャルプロファイル（Credential profiles）]：インポートしたクレデンシャルプロファイルの CSV ファイルはすぐに削除できます。アップロードされているクレデンシャルプロファイルは削除しないでください。ユーザー名とパスワードを変更した場合は、クレデンシャルプロファイルを更新します。**[デバイス管理（Device Management）]** > **[クレデンシャル（Credentials）]** を選択し、テーブル内のクレデンシャルプロファイルを選択して、 をクリックします。

ZTP の問題のトラブルシューティング

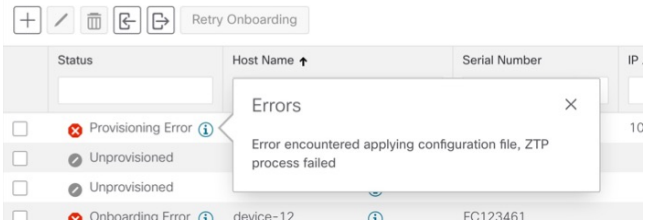
通常、Cisco Crosswork ZTP のプロビジョニングとオンボーディングは迅速かつ自動的に行われます。問題はときどき発生するため、次のトピックでは、一般的な問題と ZTP モードに固有の問題の両方を含む、問題を診断および修正する方法について説明します。

Cisco Crosswork ZTP を使用してオンボーディングできるサードパーティ製デバイスは、セキュア ZTP RFC に 100% 準拠しているサードパーティ製デバイスのみです。

ステータス列を使用して ZTP の問題を診断する

[ゼロタッチデバイス（Zero Touch Devices）] ウィンドウの [ステータス（Status）] 列には、ZTP 処理が [プロビジョニングエラー（Provisioning Error）]、[オンボーディングエラー（Onboarding Error）]、または（セキュア ZTP の場合のみ）[ZTP エラー（ZTP Error）] で終了したすべてのデバイスエントリの横に が表示されます。 をクリックすると、エラーに関する情報を示すポップアップウィンドウが表示されます。次に例を示します。ポップアップウィンドウの表示が終了したら、 をクリックして閉じます。

図 *52 : [*プロビジョニングエラー（*Provisioning Error*）*]* ポップアップウィンドウ



次の 2 つのセクションで説明するように、ZTP エラーログを使用して問題を診断することもできます。

エラーログを使用して ZTP の問題を診断する

Crosswork を実行している 1 つ以上の仮想マシンと、その VM で実行されている Crosswork ZTP サービス Kubernetes ポッドのインスタンスの 1 つに SSH ログインすることにより、ZTP エラーログ ファイルに直接アクセスできます。手順は次のとおりです。

1. 次のような Secure Shell コマンドを使用して VM にログインします。

```
ssh admin@VMIP
```

それぞれの説明は次のとおりです。

- `admin` は Crosswork 管理者 ID です。例：cw-admin。
- `VMIP` は、Crosswork を実行している仮想マシンの IP アドレスです。例：192.168.100.102。

2. 次のようなコマンドを使用して、cw-ztp-service Kubernetes ポッドにアクセスします。

```
# kubectl exec -it PodID# bash
```

`PodID#` は、cw-ztp-service Kubernetes ポッドの ID です。アクセスするポッドの番号と一致するように、必要に応じてポッド ID 番号を変更します（ポッド 0 が常に最初です）。例：`cw-ztp-service-0`、`cw-ztp-service-1`、`cw-ztp-service-2` 等

次のようなコマンドでログフォルダに移動します：`cd /var/log/robot/`。その後、フォルダ内の次の ZTP 固有のファイルのいずれかを開くことができます。

- `cw-image-service_stdout.log`
- `cw-image-service_stderr.log`
- `cw-config-service_stdout.log`
- `cw-config-service_stderr.log`

ZTP エラーログの要求

Crosswork ユーザーインターフェイスを使用して、ZTP エラーログファイルのコピーを要求できます。手順は次のとおりです。

1. 管理者権限を持つ ID を使用して、Crosswork ユーザーインターフェイスにログインします。

2.**[管理（Administration）] > [Crosswork Manager]**を選択します。

3. [Crossworkの概要（Crosswork Summary）] ページが表示されたら、[ゼロタッチプロビジョニング（Zero Touch Provisioning）] タイルをクリックします。Crosswork は、ZTP アプリケーションの詳細を表示します。

4. アプリケーションの詳細が表示されたら、**[Showtechのオプション（Showtech Options）] > [リクエストロゴ（Request Logs）]**の順に選択します。次に、**[Showtechリクエスト（Showtech Requests）]** を選択します。 リクエストが完了すると、ダッシュボードからログファイルを取得できます。

（注） 処理のオンボーディングフェーズで問題が発生した場合は、ZTP のログに加えて、Crosswork インベントリ マネージャ アプリケーション（dlminvmgr）のログを要求することができます。上記の手順 3 で、[ゼロタッチプロビジョニング（Zero Touch Provisioning）] の代わりに **[プラットフォームインフラストラクチャ（Platform Infrastructure）]** を選択することで、これを行うことができます。

共通の ZTP 問題のトラブルシューティング

以下は、ZTP モードのいずれかで発生する可能性のある一般的な問題の解決策を示しています。

表 *19 :* 一般的な *ZTP* の問題と修正

フェーズ	問題	症状	Remedy
[設定（Setup）]	イメージ、構成、または SMU ファイルのアップロードが失敗する	アップロード中にユーザーインターフェイスに表示されるエラーメッセージ	ファイルの MD5 チェックサムが正しいことを確認します。ファイル情報が正しい場合でも、ネットワーク接続が遅いためにイメージのアップロードが失敗する可能性があります。この問題が発生している場合は、アップロードを再試行します。
	ZTP デバイスエントリまたは ZTP プロファイルの作成時に、アップロードされたファイルがドロップダウンメニューに表示されない	ドロップダウンリストにないファイル	ドロップダウンメニューでは、デバイスエントリまたは ZTP プロファイルで指定したデバイスファミリと IOS リリース番号に基づいてファイルを選択します。ファイル情報が、作成しているデバイスエントリまたはプロファイルの情報と一致していることを確認します。
	デバイスエントリの CSV ファイルのインポート中にエラーが発生しました	異なります。エラーログを参照	インベントリ内のデバイスにインポートするデバイスと同じシリアル番号がある場合は、インポートする前にデバイスが [プロビジョニングなし（Unprovisioned）] 状態であることを確認します。CSV ファイルを使用してインポートしたすべてのデバイスのステータスは、インポート時に [プロビジョニングなし（Unprovisioned）] に設定されます。 インポートする前に、CSV ファイルに記載されている設定、イメージ、および ZTP プロファイルが存在することを確認します。デバイスの CSV ファイルをエクスポートし、変更を加えて再インポートすることで、デバイスイメージファイルと設定ファイルを編集できます。この編集方法を使用する場合は、インポート前に CSV ファイルに正しい UUID があることを確認します。
プロビジョニングされていない	DHCP が応答しないか、オファーの実行に失敗する	ZTP 処理の停止	ping および同様のツールを使用して、Cisco Crosswork サーバーから DHCP サーバーへのアクセスをテストします。

フェーズ	問題	症状	Remedy
進行中（In Progress）	イメージまたは SMU ファイルのダウンロードに失敗した	ZTP 処理の停止	Cisco Crosswork とデバイス間にネットワーク接続があることを確認します。デバイスが IP アドレスを DHCP サーバーから取得していることを確認します。DHCP サーバーの設定ファイルで指定されたソフトウェアイメージの UUID が正しいことを確認します。 設定ファイルで指定されたイメージ UUID を修正する必要がある場合は、ZTP 処理を再度開始する前に DHCP サーバーを再起動してください。
	設定ファイルのダウンロードに失敗した	ログに記録されたエラー	Cisco Crosswork とデバイス間にネットワーク接続があることを確認します。デバイスが IP アドレスを DHCP サーバーから取得していることを確認します。DHCP サーバーの設定ファイルで指定されたソフトウェアイメージの UUID が正しいことを確認します。DHCP 設定ファイルで指定されたイメージ UUID を修正する必要がある場合は、ZTP 処理を再度開始する前に DHCP サーバーを再起動してください。デバイスのシリアル番号がデバイスのシャーシのシリアル番号と一致していることを確認します。 ZTP 処理を開始する前に、デバイスのステータスが [プロビジョニングなし（Unprovisioned）] か、または [進行中（In Progress）] であることを確認します。デバイスが他の状態である限り、設定のダウンロードは失敗し続けます。

フェーズ	問題	症状	Remedy
オンボード済み	デバイスの状態が [オンボーディング済み（Onboarded）] と表示され、[プロビジョニング済み（Provisioned）] と表示されない	ステータス列に**プロビジョニング済み**が表示されませんでした	[プロビジョニング済み（Provisioned）] は、ZTP 処理の中間状態です。デバイスの状態が [プロビジョニング済み（Provisioned）] に変わると、Cisco Crosswork はすぐにデバイスのオンボーディングを試みます。ステータスが [オンボーディング済み（Onboarded）] か、または [オンボーディングエラー（Onboarding Error）] に変わります。
	オンボーディングエラー	ステータス列に**オンボーディングエラー**が表示される	デバイスを一意に識別するためのデフォルトの Cisco Crosswork デバイスライフサイクル管理（DLM）ポリシーは、IP アドレスです。既存のデバイスと一致する IP アドレスを持つ新しいデバイスをインポートすると、デバイスのステータスが [プロビジョニング済み（Provisioned）] に変わり、その後、[オンボーディングエラー（Onboarding Error）] に変わります。新しいデバイスの IP アドレスが空白の場合、同じ結果が得られます。インストールで OSPF ID、ISIS ID、またはその他の DLM ポリシーを使用してデバイス ID を決定する場合も、同じ問題が発生します。オンボーディングは、すべての DLM ポリシーフィールドに一意の空白以外の値を入力した場合にのみ成功します。オンボーディングが失敗した場合は、ポップアップエラーメッセージを調べて、対応するフィールドを更新し、オンボーディングを再試行します。

クラシック ZTP の問題のトラブルシューティング

次の表は、Classic ZTP 処理で発生する可能性のある問題の解決策を示しています。

表 *20* : クラシック *ZTP* の問題と修正

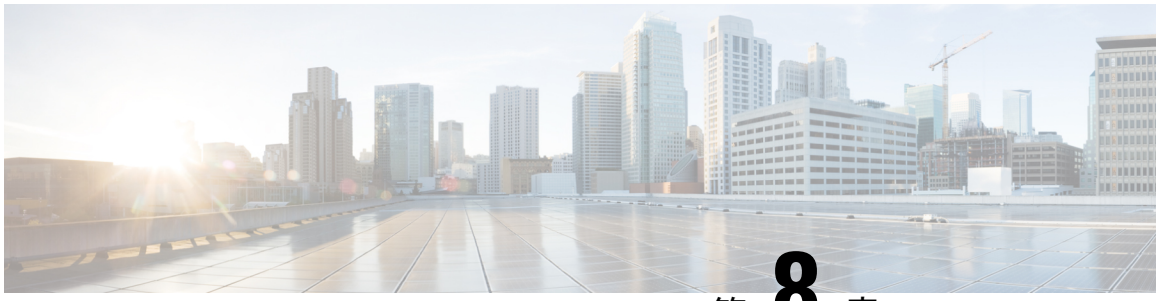
フェーズ	問題	症状	Remedy
プロビジョニングされていない	Crossworkはデバイスのシリアル番号を確認できません	ステータス列に「進行中」と表示されない	ZTP は、追加するデバイスの数に関係なく、複数のシリアル番号の追加をサポートします。デバイスエントリを作成するときは、正しいシリアル番号を割り当ててください。ZTP はシリアル番号に基づいて開始され、接続されたデバイスエントリはそれに基づいて状態の変化を表示し始めます。
進行中（In Progress）	ブートスクリプトの実行に失敗する	処理が停止します。エラーログを参照してください。	ブートスクリプトにエラーがないか調べて修正し、再試行してください。
	iPXEのリロードが失敗する	処理が停止します。エラーログを参照してください。	これは、デバイスの一時的な問題が原因である可能性があります。再度お試しください。プロセスが繰り返し失敗する場合は、シスコデバイスサポートチームに連絡してください。
プロビジョニングされていない、進行中	デバイス進捗レポートAPI 呼び出しが失敗する	処理が停止します。エラーログを参照してください。	API 呼び出しの形式が正しく、値が正しいことを確認してください。それらを修正して、再試行してください。ネットワークの問題が原因で一時的に接続が失われた結果である可能性もあります。

PnP ZTP の問題のトラブルシューティング

次の表は、PnP ZTP 処理で発生する可能性がある問題の解決策を示しています。処理の各段階でのアクティビティの詳細については、[ZTP処理のトピックへのリンク（Link to ZTP Processing topic）] を参照してください。

表 *21 : PnP ZTP* の問題と修正

フェーズ	問題	症状	Remedy
プロビジョニングされていない	PnP プロファイルのダウンロードが失敗する	デバイスがプロビジョニングされていない状態のままになる	パケットのドロップまたは同様のネットワークトラフィックの問題により、ダウンロードが失敗した可能性があります。まず、PnP プロファイルに正しいファイル名、プロトコル、IP アドレス、およびポートが指定されていることを確認します。TFTP サーバーが稼働していて到達可能であることを確認します。次に、デバイスから ZTP を再度トリガーしてみてください。
プロビジョニングされていない、進行中	機能サービスリクエストが失敗する	ZTP デバイスエントリは、「サービス機能チェックに失敗しました」というメッセージとともにエラー状態に移行します。理由：デバイスが最低限必要な機能をサポートしていません。	PnP ZTP が機能するには、プロビジョニングされる XE デバイスが次の最小機能をサポートしている必要があります。 • device-info • 証明書のインストール • image-install • config-upgrade • バックオフ この要件に問題がある場合は、シスコデバイスサポートチームにお問い合わせください。
進行中（In Progress）	証明書インストールに失敗しました	ZTP デバイスがエラー状態になり、「証明書のインストールサービスに失敗しました」というメッセージが表示されます。	まず、XEデバイスにログインし、トラストポイント「CrossworkPnP」がすでに存在する場合はクリーンアップします。次に、Crosswork GUI からデバイスを UnProvisioned 状態に戻し、ZTP を最初から再トリガーします。



第 8 章

マップの設定

ここでは、次の内容について説明します。

ダッシュボードでのクイックビューの取得

ホームページにはカスタマイズ可能な一連のダッシュレットが表示され、デバイスの到達可能性や動作ステータスなど、管理対象ネットワークの運用の概要がひと目でわかります。ダッシュボードは一連のダッシュレットで構成され、各ダッシュレットは同じカテゴリに属するさまざまなタイプのデータを表します。

図 *53 : Crosswork* のホームページ

引き出し線番号	説明
1	**メインメニュー**：メインメニューでは、インストールされている Cisco Crosswork アプリケーションと、デバイス管理および管理のタスクに移動できます。メニューオプションは、インストールされている Cisco Crosswork アプリケーションによって若干異なる場合があります。

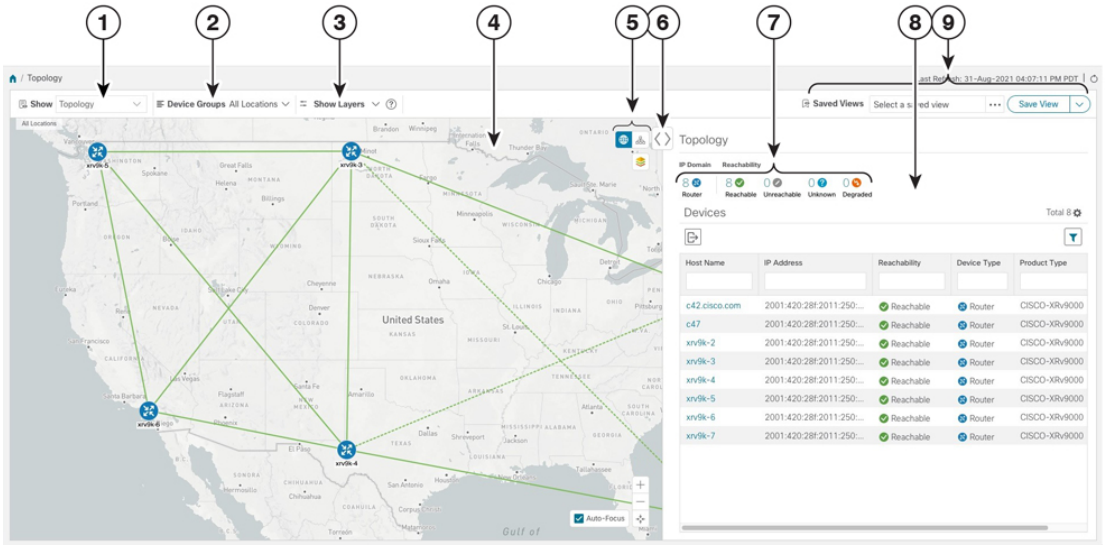
引き出し線番号	説明
2	**ダッシュレット**：情報は、インストールされている Cisco Crosswork アプリケーションによって異なります。 • ダッシュレット内の詳細情報をドリルダウンするには、値をクリックします。クリックしたフィルタ処理済みデータのみを表示するウィンドウが表示されます。 • ダッシュレットのレイアウトを追加または変更するには、[ビューのカスタマイズ（Customize View）] をクリックします。ダッシュレットを目的のレイアウトに移動し、[保存（Save）] をクリックします。
3	設定のアイコン： [アラート（Alerts）] アイコンは、注意が必要なシステム操作に関連する現在のエラー状態を通知し、それらの状態に関する詳細情報へのリンクを提供します。 [イベント（Events）] アイコンは、システム操作に関連する新しいイベントを通知し、すべてのシステムイベントの履歴にアクセスできるようにします。 [バージョン情報（About）] アイコンには、Cisco Crosswork 製品の現在のバージョンが表示されます。 [ユーザーアカウント（User Account）] アイコンを使用すると、ユーザー名の表示、パスワードの変更、ログアウトを行えます。

トポロジマップでのデバイスとリンクの表示

ネットワークトポロジマップを表示するには、メインメニューから [トポロジ（Topology）] を選択します。

詳細については、「デバイスとリンクの詳細の表示 （301 ページ）」を参照してください。

図 *54 : Cisco Crosswork UI* とトポロジマップ



引き出し線番号	説明
1	[トポロジマップビュー（Topology Map View）]：[表示（Show）] ドロップダウンリストから、マップに表示するデータを表示するオプションをクリックします。 [トポロジ（Topology）] を選択すると、ネットワーク内のデバイスとリンクが表示されます。
2	[デバイスグループ（Device Groups）]：ドロップダウンリストから、マップに表示するデバイスのグループをクリックします。他のすべてのデバイスグループは非表示になります。
3	[表示/非表示（Show/Hide）]：ドロップダウンリストから、マップに表示するネットワークレイヤをクリックします。選択したレイヤに属するすべてのデバイスとリンクが表示されます。デフォルトでは、すべてのレイヤが表示されます。

引き出し線番号	説明
4	[トポロジマップ（Topology Map）]：ネットワークトポロジは、論理マップまたは地理的マップに表示できます。ここでは、デバイスとリンクが地理的コンテキストで表示されます。マップでドリルダウンすると、デバイスとリンクに関する詳細を確認できます。 [デバイス（Device）]： • デバイス設定の概要を表示するには、マウスカーソルをデバイスアイコンの上に合わせます。ホスト名、状態、ノードID、およびデバイスタイプを表示するポップアップウィンドウが表示されます。 • デバイスの詳細を表示するには、デバイスアイコンをクリックします。 • デバイスが物理的に近接している場合、地理的なマップはそれらをクラスタとして表示します。青色の円内の番号（  ）は、クラスタ内のデバイスの数を示します。この方法でデバイスを表示すると、マップ上での重複や混乱を防ぐことができます。 [リンク（Link）]： • 実線は、2 つのデバイス間の単一リンクを示します。2 つのデバイス間、またはデバイスとデバイスのクラスタの間に複数のリンクがある場合は、代わりに線は点線で表示されます。破線は、複数のリンクを表す集約リンクか、または同じ物理リンクでの複数のプロトコル（IPv4 や IPv6 など）の使用を示します。 • A と Z はそれぞれヘッドエンドとエンドポイントを示します。 • リンク情報の詳細を表示するには、リンクをクリックします。 （注）　デュアルスタックリンクは、集約されていても 1 本の線で表示されます。
5	 ：論理マップは、自動レイアウトアルゴリズムに従って配置されたデバイスとそれらのリンクを示し、地理的な位置は無視されます。レイアウトアルゴリズムを変更できます。  ：地理的マップは、単一のデバイス、デバイスクラスタ、リンク、およびトンネルを世界地図に重ねて表示します。マップ上の各デバイスの位置は、デバイスインベントリで定義されているデバイスの GPS 座標（経度と緯度）を反映します。  ：[表示設定（Display Preferences）] ウィンドウでは、デバイス、リンク、の表示設定を変更できます。

引き出し線番号	説明
6	[サイドパネルの展開/折りたたみ/非表示（Expand/Collapse/Hide Side Panel）]：サイドパネルの内容を展開するか、または折りたたみます。トポロジマップを拡大表示するには、サイドパネルを閉じます。
7	[ミニダッシュボード（Mini Dashboard）] には、IP ドメインとデバイスの到達可能性ステータスの概要が表示されます。フィルタが適用されると、[ミニダッシュボード（Mini Dashboard）] が更新され、[デバイス（Devices）] テーブルに表示される内容が反映されます。 （注） アラームステータス機能が有効になっている場合は、ここにアラーム情報も表示されます。アラームステータスを表示するには、EMS サービスアプリケーションをインストールし、アラームを表示するデバイスで Syslog および SNMP トラップのホスト情報を設定する必要があります。アラームステータス機能は、一部のライセンスパッケージで利用できます。
8	このウィンドウの内容は、インストールしているアプリケーションの種類、トポロジマップの [表示（Show）] に設定されている内容、の詳細情報を表示することを選択しているかによって異なります。。
9	[保存済みカスタムマップビュー（Saved Custom Map Views）]：現在のマップの設定とレイアウト、保存済みビューに保存されているテーブルの設定を使用して名前付きカスタムビューを作成したり、以前に作成したカスタムビューを表示できます。

Topo-svc リンクディスカバリー

リンク タイプ	検出	Link State
L3 リンク（ISIS、OSPF）	PCE 経由	PCE はリンク動作状態に基づいて UP または DOWN に設定します

リンク タイプ	検出	Link State
L2 リンク（CDP、LLDP、LAG）	SNMP mib 経由：CDP、LLDP、LAG	リンク状態は、2 つのリンクエンドインターフェイスの動作状態（IF mib 経由）に基づいています。 • 最初に検出されたときのリンク状態は UP です。 • リンクエンドインターフェイスの動作状態の 1 つが DOWN になると、リンク状態は DOWN に設定されます。 • リンク側インターフェースの動作状態が両方とも UP の場合、リンク状態は UP に設定されます。

リンク状態の定義

Link State	説明
アップ	リンクは両方向の PCE トポロジに存在します。
デグレード	リンクは、PCE トポロジで一方向のみで報告されます。
Down	リンクは両方向でダウンしていると報告されています。

トポロジ要素に使用されるそれぞれのサウスバウンド インターフェイス/プロトコルを次の表に示します。

プロトコル/方法	内容	ユースケース
IGP/BGP-LS（SR-PCE 経由	リアルタイムトポロジ（ノード、リンク、リンクメトリックなど）	オプティマエンジン（OE）モデル構築 • L3 トポロジビジュアライザ
PCE（SR-PCE 経由	リアルタイム LSP ステータス、PCE-int LSP の CRUD	• SR/SRv6、RSVP-TE LSP 可視化 • PCE-int LSP 作成/更新/削除

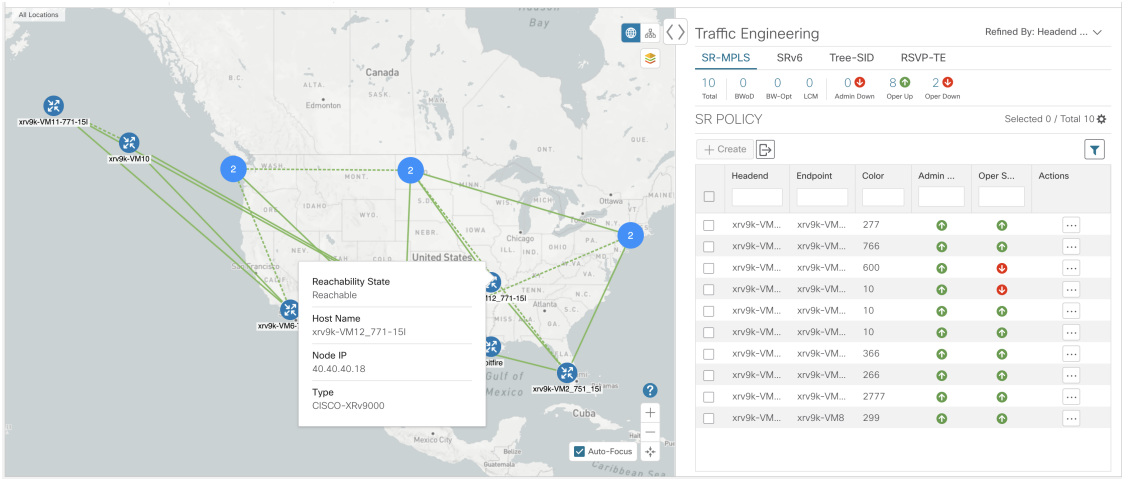
プロトコル/方法	内容	ユースケース
SNMP（SNMPv2-MIB、IP-MIB、IF-MIB、LLDP-MIB、CISCO CDB-MIB）（CDG 経由）	システム情報、インターフェイステーブル（インターフェースおよび SR-TE/RSVP-TE トラフィック使用率） IP アドレステーブル、L2 隣接情報	デバイス管理：デバイス詳細 オプティマエンジン（OE）モデル構築 • L2/L3 トポロジ • インターフェイス名、管理/操作ステータス • インターフェイス & SR ポリシー/RSVP-TE の利用 OE モデルシミュレーション • IGP/LSP パスシミュレーション • 帯域幅の使用例（BwOD/BwOpt/LCM）
CLI（CDG 経由）：「show clock」	Clock Drift	KPI モニタリングでデバイスとシステムが同期されていることを確認する必要がある CAHI によって使用されます。
CLI（CDG 経由）：「show mpls	TE ルータ ID	SR-PCE を介して学習した同じ TE ルータ ID と DLM モードを一致させるため。

デバイスとリンクの詳細の表示

次に、トポロジマップを使用してデバイスとリンクの詳細（Link Aggregation Group（LAG）の詳細を含む（ステップ 6 参照））を表示する例を示します。

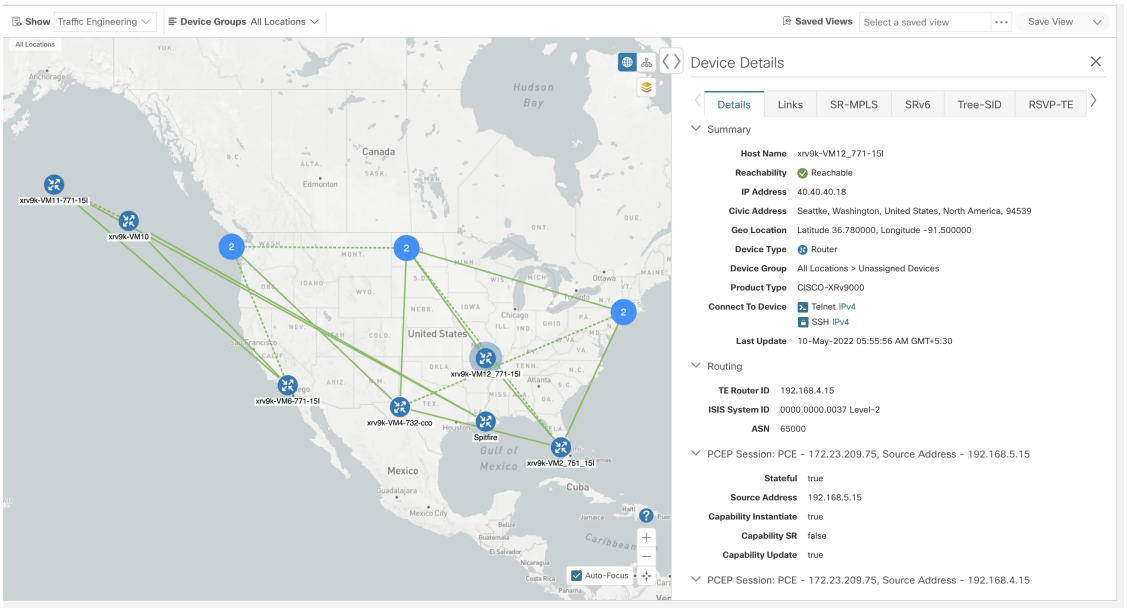
ステップ 1 メインメニューから、[トポロジ（Topology）] を選択します。

ステップ 2 デバイスのホスト名、到達可能性の状態、IP アドレス、およびタイプをすばやく表示するには、デバイスアイコン上にマウスを合わせます。



ステップ 3 デバイスの詳細をさらに表示するには、デバイスアイコンをクリックします。

a) 次の例は、トポロジマップのデバイスの詳細を示しています。



（注） アラームステータス機能が有効になっている場合は、ここにアラーム情報も表示されます。アラームステータスを表示するには、Common EMS サービスアプリケーションをインストールし、アラームを表示するデバイスで Syslog および SNMP トラップのホスト情報を設定する必要があります。アラームステータス機能は、一部のライセンスパッケージで利用できます。

複数の IGP のセットアップでは、ルーティングの詳細ですべての IGP、IS-IS、および OSPF プロセスを表示することもできます。次の例を参照してください。

図 *55* : 複数の *IGP* : *OSPF* プロセス

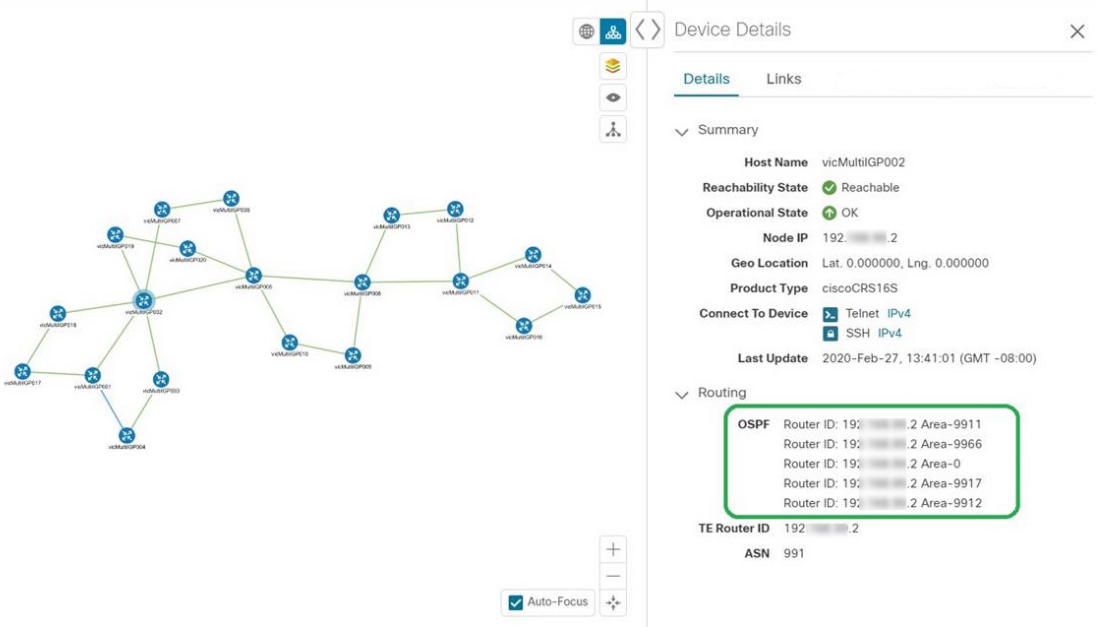


図 *56* : 複数の *IGP* : *ISIS* プロセス

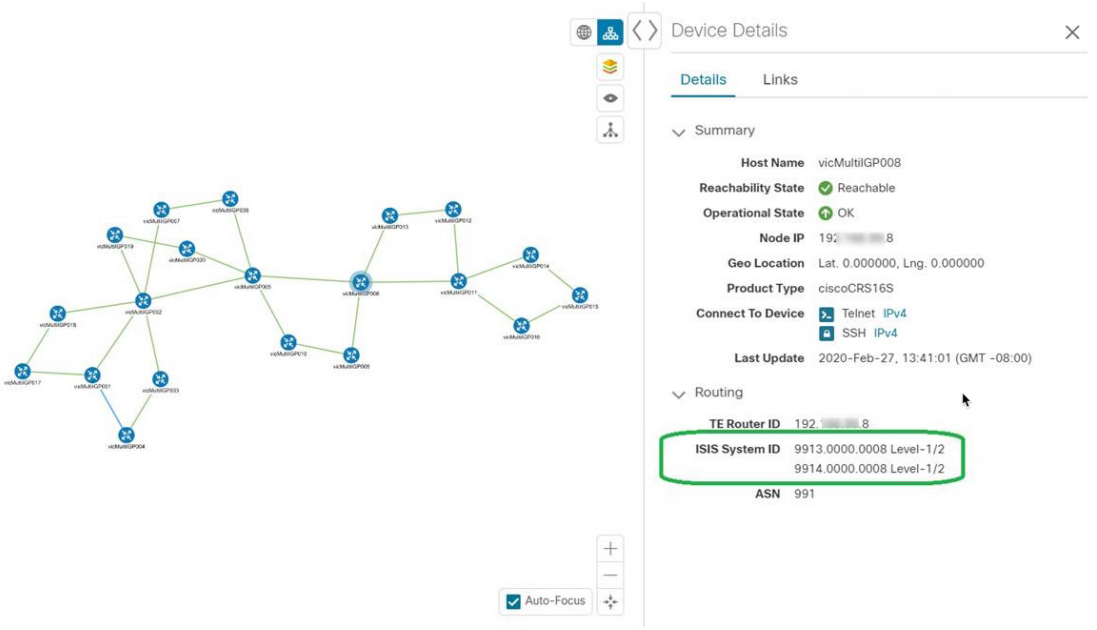
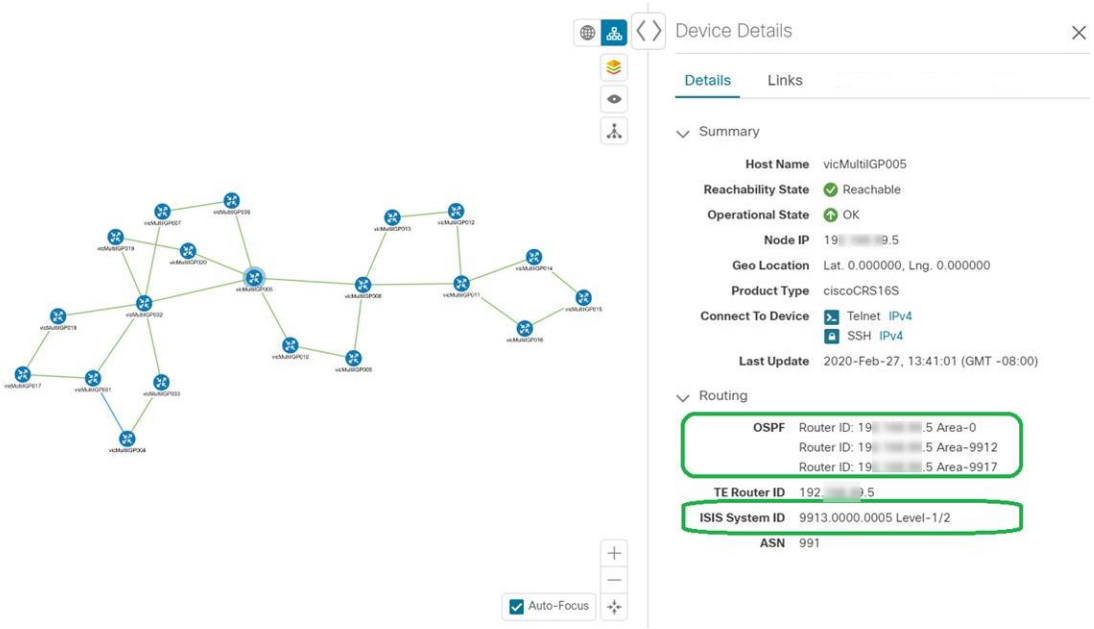
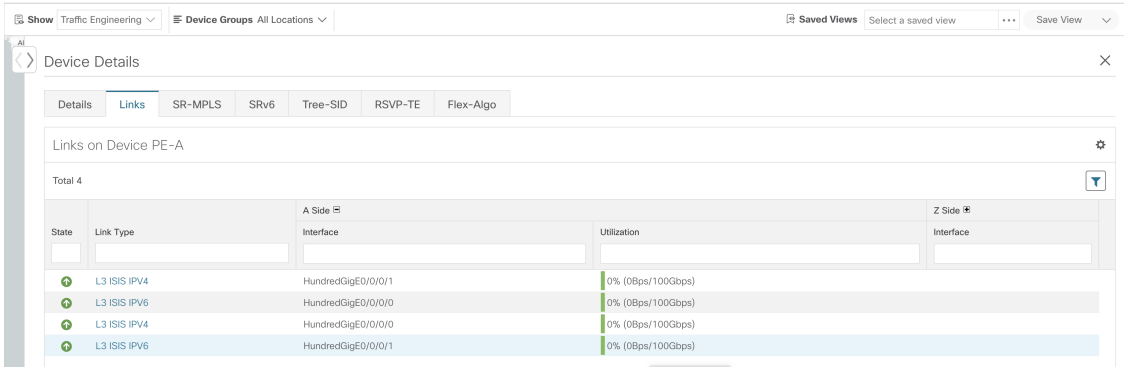


図 *57* : 複数の *IGP* : *OSPF* および *ISIS* プロセス



ステップ 4 デバイスのリンクを表示するには、[リンク（Links）] タブをクリックし、右側のパネルを展開してすべてのリンクの詳細を表示します。



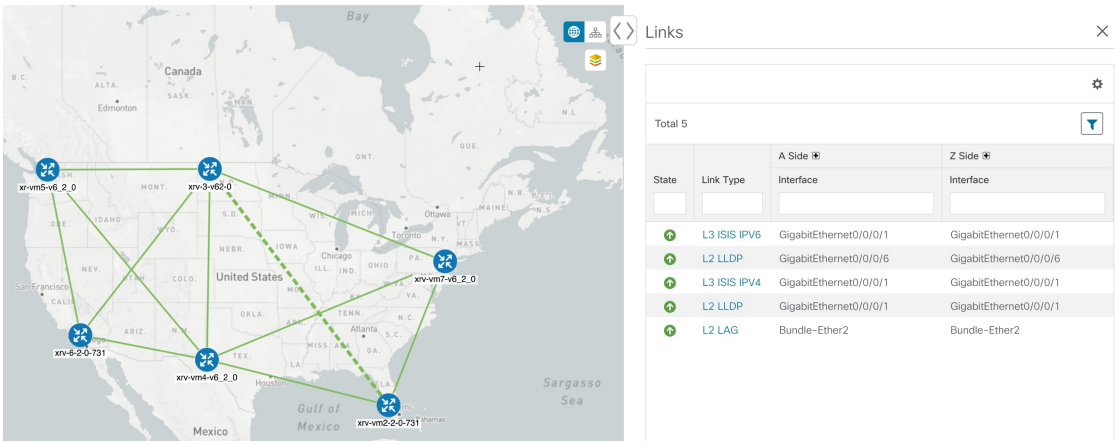
ステップ 5 使用率を表示するには、[A側（A side）] または [Z側（Z side）] を展開します。

ipv4 および ipv6 リンクに表示される使用率は、各アドレスファミリに固有ではなく、インターフェイスまたはサブインターフェイスの集約トラフィックを表します。サブインターフェイス リンクに表示される使用率は、サブインターフェイスのトラフィックのメインインターフェイスでの帯域幅使用率を表します。

ステップ 6 サイドパネルを折りたたんで、[デバイスの詳細（Device Details）] ウィンドウを閉じます。

ステップ 7 破線をクリックします。破線は、複数のリンクを表す集約リンクを示します。

（注） デュアルスタックリンク（集約）は、1 本の線で表示されます。



マップの表示設定の定義

ネットワークトポロジは、論理マップまたは地理的マップ（Geoマップ）に表示できます。ここでは、デバイスとリンクが地理的コンテキストで表示されます。論理マップは、自動レイアウトアルゴリズムに従って配置されたデバイスとそれらのリンクを示し、地理的な位置は無視されます。Geoマップは、単一のデバイス、デバイスクラスタ、リンク、およびトンネルを世界地図に重ねて表示します。マップ上の各デバイスの位置は、デバイスの GPS 座標（経度と緯度）を反映します。

論理マップは、介入を必要とせずに自動的にレンダリングされます。地理的マップは、外部マッププロバイダー（Mapbox）からのマップタイルを使用してデフォルトでレンダリングされます。外部マッププロバイダーを使用する場合は、インターネットアクセスが必要です。インターネットにアクセスできない場合は、Cisco.comからマップファイルをダウンロードして、それらをシステムにアップロードすることができます。これらのマップファイルは、Geoマップをレンダリングするために内部的にアクセスされます。「地理的マップを表示するための内部マップのオフライン使用 （305 ページ）」を参照してください。

マップを設定する場合、管理者は表示設定（リンク帯域幅使用率の変化を表す色など）も定義できます。

マップを設定し、表示設定を定義するには、次を参照してください。

- 地理的マップを表示するための内部マップのオフライン使用 （305 ページ）
- リンク帯域幅使用率の色分けしきい値の定義 （306 ページ）

地理的マップを表示するための内部マップのオフライン使用

このシステムは、デフォルトでは、直接インターネット接続を介して特定のMapbox URLからGeo マップタイルを取得するように設定されています。インターネットに接続していないため、システムが外部マッププロバイダにアクセスして地理的なマップタイルを取得できない場

合は、ネットワークに必要な世界の地域を表す内部マップファイルをアップロードすることができます。これらのマップファイルは、Cisco.comからダウンロードしてシステムにアップロードする必要があります。マップファイルの名前は、**africa-geomaps-1.0.0-for-Crosswork-4.1.0-signed.tar.gz** のように、マップファイルに含まれている世界の地域を示しています。世界の特定の地域でネットワークを管理する場合は、関連するマップファイルのみをアップロードします。使用可能なすべてのマップファイルをアップロードする必要はありません。

（注） 内部マップを使用してオフラインで作業し、マップファイルをアップロードしない場合、地理的なマップには、街や通りなどの詳細を含まない一般的な世界地図が表示されます。

内部マップを使用して地理的マップを表示するには、次の手順を実行します。

始める前に

Cisco.com から必要なマップファイルをダウンロードし、アクセス可能なサーバーに配置します。サーバーは、ファイル転送用の SCP プロトコルをサポートしている必要があります。

ステップ 1 メインメニューから、**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択します。

ステップ 2 [トポロジ（Topology）] で、[マップ（Map）] オプションをクリックします。

ステップ 3 [内部マップを使用してオフラインで作業する（Work offline with internal Maps）] オプションボタンを選択し、[管理（Manage）] をクリックします。

ステップ 4 [内部マップの管理（Manage Internal Maps）] ダイアログで、をクリックして新しいマップファイルをアップロードします。一度にアップロードできるファイルは 1 つです。

ステップ 5 [マップファイルのアップロード（Upload Map File）] ダイアログで、システムがファイルにアクセスできるように、ダウンロードしたマップファイルの場所を参照します。

ステップ 6 [アップロード（Upload）] をクリックします。
指定した場所からマップがアップロードされます。アップロードプロセスには時間がかかることがあります。ブラウザを閉じたり、[キャンセル（Cancel）] をクリックして中断したりしないでください。プロセスが完了すると、新しいマップが [内部マップの管理（Manage Internal Maps）] ダイアログの [アップロード済みのマップ（Uploaded Maps）] に表示されます。

ステップ 7 必要に応じて、追加のマップをアップロードします。

リンク帯域幅使用率の色分けしきい値の定義

リンク帯域幅の使用率は、論理マップと地理的マップで視覚化およびモニターできます。リンクは、リンクでの現在使用されている総帯域幅のパーセンテージに基づいて色分けされます。次に、デフォルトの帯域幅使用率しきい値（パーセンテージ範囲）と対応する色インジケータのセットを示します。これらの色のしきい値は、管理者がカスタマイズできます。

- 緑：使用率 0 ー 25%
- 黄色：使用率 25 ー 50%
- オレンジ：使用率 50 ー 75%
- 赤：使用率 75 ー 100%

リンクの帯域幅使用率の色のしきい値を定義するには、次の手順を実行します。

ステップ 1 メインメニューから、**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択します。

ステップ 2 [トポロジ（Topology）] で、[帯域幅使用率（Bandwidth Utilization）] オプションをクリックします。

ステップ 3 [リンクの色分けのしきい値（Link Coloring Thresholds）] 領域で、リンクを色分けする基準を定義します。各行で、色とその色が表す帯域幅のパーセンテージ範囲を定義します。次の点に注意してください。

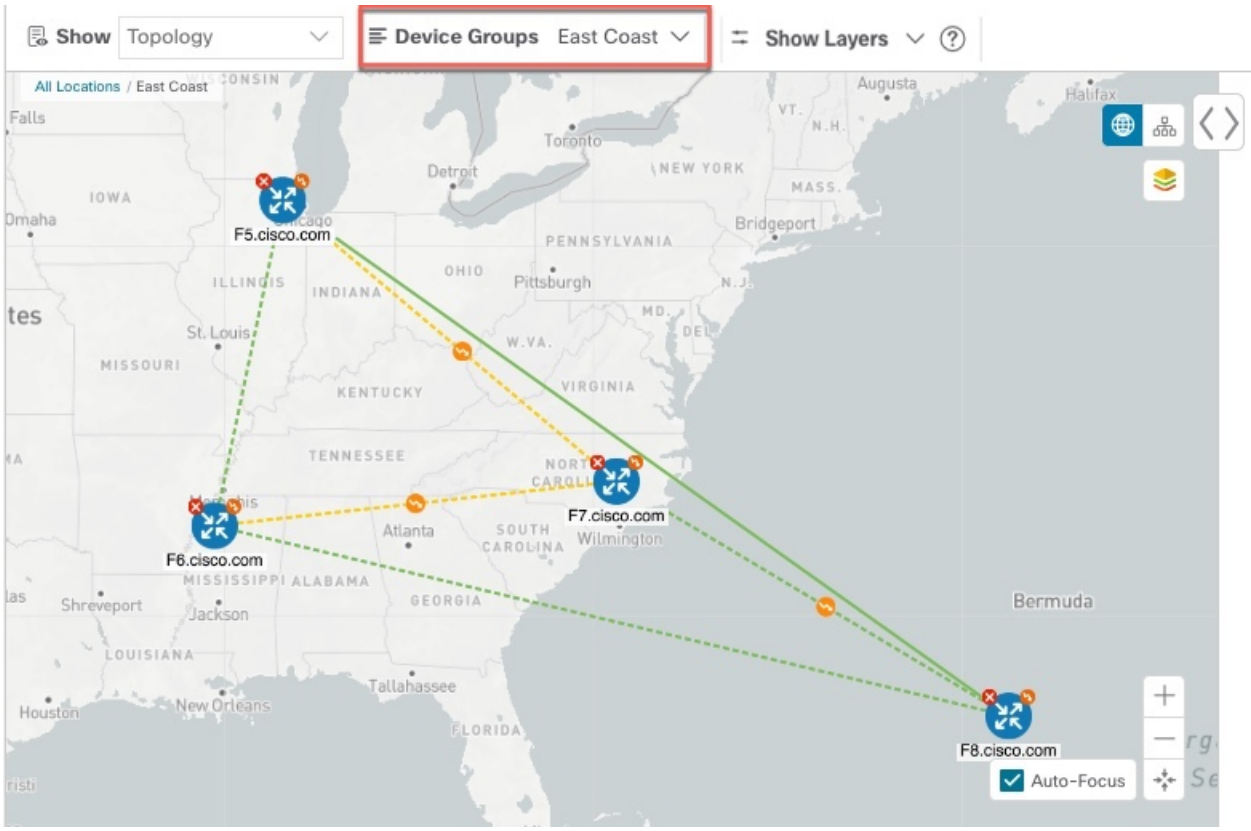
- [変更後（To）] フィールドにのみ値を入力できます。各行は、前の行の範囲の末尾から自動的に始まります。
- しきい値は連続している必要があります。つまり、各行の範囲は前の行の範囲の次から始める必要があります。たとえば、最初の行の範囲が 0 ー 25% の場合、2 番目の行の範囲は 25 よりも大きい値で終わる必要があります。
- 複数のしきい値に同じ色を使用することはできません。たとえば、最初の行と 2 番目の行の両方に [緑（Green）] を選択することはできません。

ステップ 4 [保存（Save）] をクリックします。

デバイスグループを使用したトポロジビューのフィルタ処理

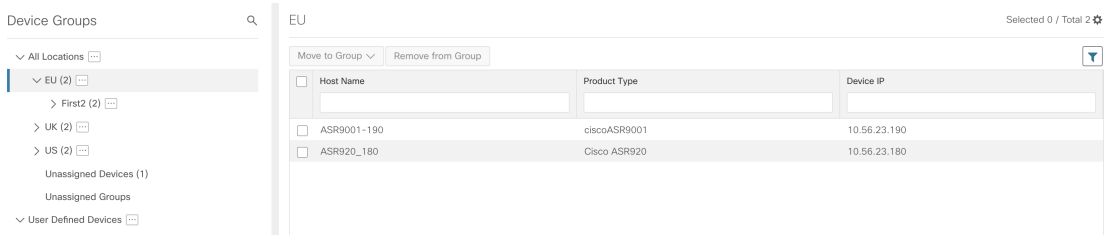
さまざまな目的でデバイスを識別、検索、およびグループ化するためにデバイスグループを作成できます。デバイスグループでは、そのデバイスグループに固有のデータを視覚化して拡大できます。これにより、画面上の乱雑さが軽減され、最も重要なデータに集中できます。たとえば、次の図では、東海岸のデバイスグループが選択されており、トポロジマップに拡大表示されています。また、[デバイス（Devices）]テーブルには、東海岸のデバイスグループに属するデバイスのみが表示されていることに注意してください。

図 *58 :* トポロジマップでのデバイスグループの選択



[デバイスグループ（Device Groups）] ウィンドウ（**[デバイス管理（Device Management）]** > **[グループ（Groups）]**）では、デバイスグループを作成および管理できます。デフォルトでは、すべてのデバイスが最初は [未割り当てデバイス（Unassigned Devices）] グループに表示されます。

図 *59 :* デバイスグループセレクタ



デバイスグループの作成と変更

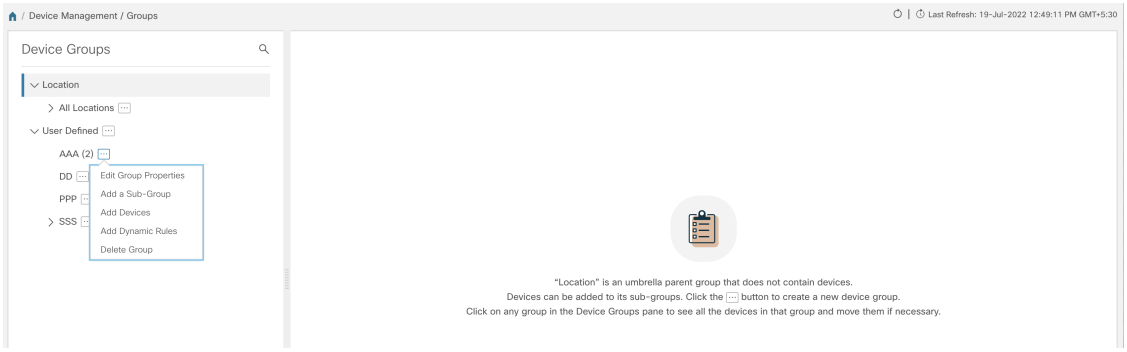
デバイスグループ、およびグループへのデバイスの割り当ては、手動（この項で説明）または自動（次の項で説明）で実行できます。

ステップ 1 メインメニューから **[デバイス管理（Device Management）]** > **[グループ（Groups）]** を選択します。

ステップ 2 新しいサブグループを追加するには、[すべての場所（All Locations）]の横にある をクリックします。[すべての場所（All Locations）] の下に新しいサブグループが追加されます。

ステップ 3 デバイスをグループに追加するには、右ペインの [未割り当てのデバイス（Unassigned Devices）] でデバイスを選択し、[グループに移動（Move to Group）] ドロップダウンから適切なグループを選択します。

ステップ 4 既存グループの下で、サブグループを編集、削除、または追加するには、[デバイスグループ（Device Groups）] ツリーでグループの横にある をクリックします。



ステップ 5 グループの追加、削除、または編集（名前の変更または移動）を選択します。グループを削除すると、そのグループに属しているすべてのデバイスが [未割り当てデバイス（Unassigned Devices）] グループに移動します。また、グループを削除すると、そのグループのサブグループがすべて削除されます。

（注） デバイスは、1 つのデバイスグループにのみ属することができます。

ステップ 6 [保存（Save）] をクリックします。

ダイナミック デバイス グループの有効化

デバイスホスト名で正規表現（regex）を使用して、デバイスグループを動的に作成し、未割り当てのデバイスをこれらのグループに自動的に追加するルールを作成できます。ルールに一致する新たに追加または検出されたデバイスは、適切なグループに配置されます。

（注） ダイナミックルールは、すでにグループに属しているデバイスには適用されません。ルールで考慮されるようにするデバイスは、[未割り当てデバイス（Unassigned Devices）] に移動する必要があります。

始める前に

[ダイナミックグループ（Dynamic Groups）] ダイアログに示されている例に従うこともできますが、正規表現に精通していると有利です。

ステップ 1 メインメニューから **[デバイス管理（Device Management）] > [グループ（Groups）]** を選択します。

ステップ 2 [すべての場所（All Locations）] > [動的グループ化ルールの管理（Manage Dynamic Grouping Rule）] の横にある をクリックします。

ステップ 3 [他の詳細と例の表示（Show more details and examples）] をクリックして、必要な [ホスト名（Host Name）] フィールドと [グループ名（Group Name）] フィールドに入力します。

ステップ 4 [未割り当てデバイス（Unassigned Devices）] グループに既存のデバイスがある場合は、[ルールのテスト（Test Rule）] をクリックして、作成されるグループ名のタイプのサンプリングを表示します。

ステップ 5 [ルールの有効化（Enable Rule）] トグルをオンにして、ルールを有効にします。ルールが有効になると、システムは未割り当てのデバイスを 1 分おきに確認し、ルールに基づいてそれらを適切なグループに割り当てます。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 この方法で作成されたグループは、最初は [未割り当てグループ（Unassigned Groups）] の下に表示されます（ルールが初めて有効になったときに作成されます）。新たに作成したグループを必要なグループ階層に移動します。

ステップ 8 新しく作成した未割り当てグループを適切なグループに移動するには、次の手順を実行します。

a) すべてのロケーションの横にある をクリックし、[サブグループを追加（Add a Sub-Group）] をクリックします。
b) 新しいグループに詳細を入力して [作成（Create）] をクリックします。
c) 左ペインから未割り当てのデバイスをクリックします。
d) 右側のペインから、移動するデバイスを選択し、[グループに移動（Move to Group）] をクリックして適切なグループに移動します。

マップ表示設定のカスタマイズ

ニーズと設定に基づいて、トポロジマップを視覚的な設定を行うことができます。次を実行できます。

- リンクとデバイスの表示のカスタマイズ （310 ページ）

リンクとデバイスの表示のカスタマイズ

デバイスとリンクマップの表示設定を設定するには、[トポロジ（Topology）] を選択し、トポロジマップの をクリックします。

- 集約リンク、およびリンクの状態と使用状況を簡単に確認できるようにするリンクの色付け方法を表示するには、[リンク（Links）] をクリックします。デフォルトでは、集約リンクはマップ上で単一リンクと区別され、リンクはリンク使用率のしきい値に基づいて色付けされます。管理者は、使用率のしきい値と対応する色を変更できます。

- デバイスの状態とデバイスのラベル付けを表示するには、[デバイス（Devices）] をクリックします。デフォルトでは、デバイスの状態はマップに表示され、ホスト名はデバイスのラベル付けに使用されます。

TE タイムアウトの設定

SR-TE ポリシー、RSVP-TE トンネル、オンデマンド帯域幅、および IGP パスのデータのプロビジョニングと取得のタイムアウト設定を行うには、**[管理（Administration）] > [システム設定（System Settings）] > [トラフィック エンジニアリング（Traffic Engineering）] > [全般（General Settings）]** タブを選択します。タイムアウト期間のオプションを入力します。詳細については、?をクリックしてください。

（注） SR-PCE の応答が遅い場合、タイムアウトの設定で各アクションの応答時間を変更します。大規模トポロジの設定を変更したり、遅延や負荷による SR-PCE 応答の遅延に対処したりできます。

トポロジリンク検出の有効化または無効化

システム設定を調整して、LLDP、CDP、および LAG プロトコルの L2 トポロジリンクの検出を有効または無効にすることができます。デフォルトでは、トポロジ検出オプションは無効になっています。無効にすると、選択したプロトコルのリンク（以前に検出されたリンクを含む）はマップに表示されません。

トポロジ検出を有効にするには、次の手順を実行します。

始める前に

- 設定を変更する前に、すべてのポッドが正常であることを確認します。

ステップ 1 メインメニューから、**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択します。

ステップ 2 [トポロジ（Topology）] で、[検出（Discovery）] オプションをクリックします。

ステップ 3 検出を有効にするプロトコルのチェックボックスをオンにします。

ステップ 4 [保存（Save）] をクリックして変更を保存します。

選択したプロトコルの横に「プロトコルを有効にしています（Enabling Protocol）」というメッセージが表示されます。システムが検出操作を完了するまで待ちます。

検出を有効にすると、収集ジョブが作成されます。次の表に、各プロトコル設定で作成される収集ジョブとセンサーパスを示します。

表 *22*：各設定の収集ジョブ

L2 設定	Helios 収集ジョブ ID	コンテキスト ID	収集された MIB	センサーパス
なし（デフォルト）	cw.topo_svc	cw.toposvc.snmp cw.toposvc.snmptraps	IF-MIB, IP-MIB, IF-MIB:notification	IF-MIB:IF-MIB/ifTable/ifEntry IP-MIB:IP-MIB/ipAddressTable/ipAddressEntry IF-MIB:notifications
CDP	cw.topo_svc	cw.toposvc.cdp	IF-MIB, CDP-MIB	IF-MIB:IF-MIB/ifTable/ifEntry CISCO-CDP-MIB:CISCO-CDP-MIB/cdpCacheTable/cdpCacheEntry CISCO-CDP-MIB:CISCO-CDP-MIB/cdpInterfaceTable/cdpInterfaceEntry
LLDP	cw.topo_svc	cw.toposvc.lldp	IF-MIB, LLDP-MIB	IF-MIB:IF-MIB/ifTable/ifEntry LLDP-MIB:LLDP-MIB/lldpLocPortTable/lldpLocPortEntry LLDP-MIB:LLDP-MIB/lldpRemTable/lldpRemEntry
LAG	cw.topo_svc	cw.toposvc.lag	IF-MIB, LAG-MIB	IF-MIB:IF-MIB/ifTable/ifEntry IEEE8023-LAG-MIB:IEEE8023-LAG-MIB/dot3adAggTable/dot3adAggEntry IEEE8023-LAG-MIB:IEEE8023-LAG-MIB/dot3adAggPortTable/dot3adAggPortEntry

次の表に、トポロジ検出を有効または無効にする際の一般的なエラーを示します。

表 *23*：一般的なエラーのシナリオ

考えられるエラーのシナリオ	原因	原因と推奨処置
無効にすると、無効なリンクの一部がマップに表示される。	これは、プロトコルを有効にした後すぐに無効にしようとすると発生します。そのため、SNMP プロセッサが完了する前に、以前の有効化ジョブ用に作成された収集ジョブが強制終了される可能性があります。タイミングの問題により、無効なリンクは引き続き表示されます。	間に十分な待機時間を指定してプロトコルを再度有効または無効にするか、または toposvc を再起動します。

考えられるエラーのシナリオ	原因	原因と推奨処置
検出を有効にしようとすると、heliosジョブが失敗し、それ以降の編集で設定が無効になる。	これは、heliosポッドが正常でない場合に発生する可能性があります。これは、Crossworkが収集ジョブの作成中にユーザーによる編集を無効にするため、失敗状態のままになることがあります。	ポッドが正常であることを確認した後、間に十分な待機時間を指定してプロトコルを有効または無効にするか、または`toposvc`を再起動します。
検出設定を変更すると、TopoUI または TopoSvc がクラッシュし、予測不能なステータスが発生する。	収集ジョブの作成中または削除中にユーザーがそれ以降は編集できないようにするメカニズムは、ETCD 経由で通信するポッドに依存しています。この間にポッドがクラッシュすると、ETCD キーが正しく設定されません。	

簡易アクセスのトポロジビューの保存

マップ上のデバイスとリンクを再配置すると、通常、変更は保存されません。便利なマップレイアウトに簡単にアクセスするには、名前付きカスタムビューとして保存すると、毎回マップを再配置することなくすばやく取得できます。これは、多数のデバイスを含む大規模なネットワークを管理する場合に特に役立ちます。

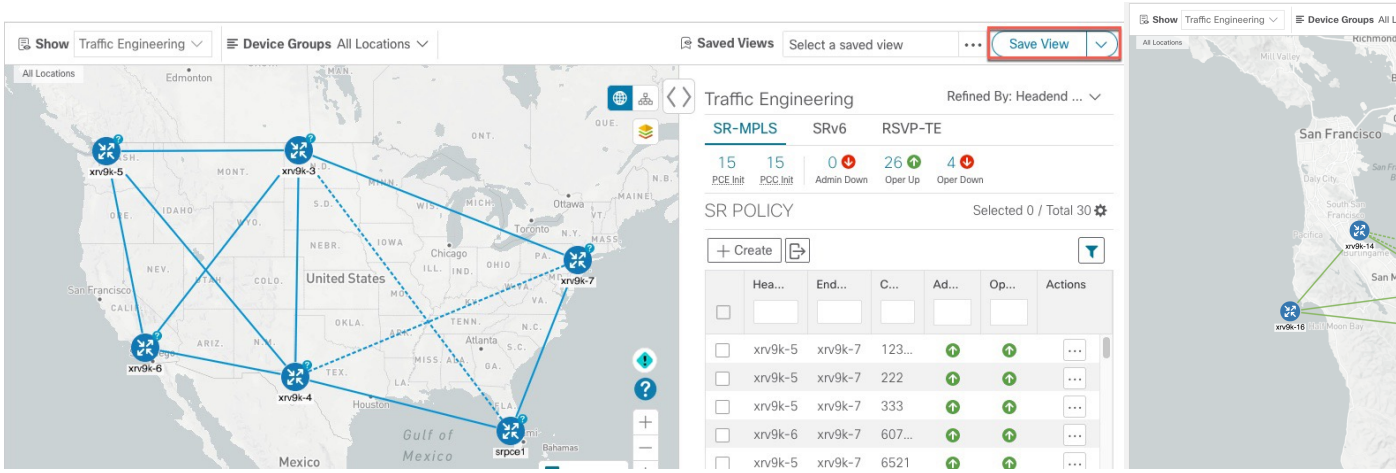
カスタムビューを保存すると、次の設定が保存されます。

- 地理的マップか論理マップか。
- 論理マップのレイアウト内のデバイスの位置。
- デバイスとリンクの表示設定。

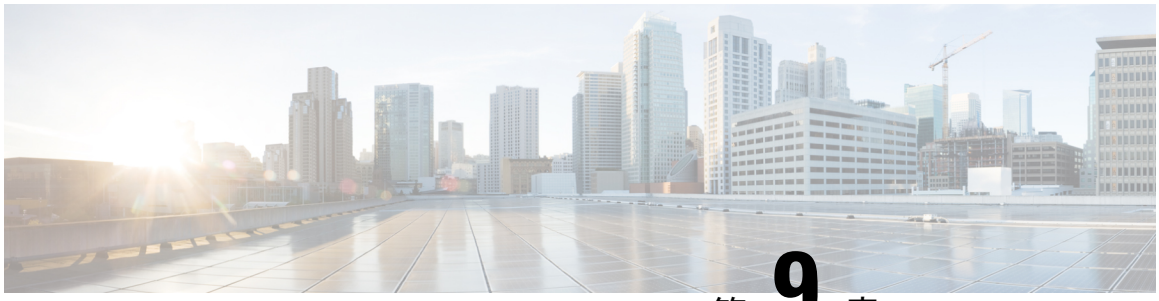
（注） すべてのカスタムビューは、すべてのユーザーに表示されます。ただし、ビューを変更できるのは管理者ロールを持つユーザーまたはカスタムビューを作成したユーザーのみです。

ステップ 1 必要な情報のみが含まれ、レイアウトがニーズを満たすまで、現在のマップビューをカスタマイズします。

ステップ 2 思いどおりになったら、[ビューの保存（Save View）] をクリックします。



ステップ 3 新しいカスタムビューの一意の名前を入力し、[保存（Save）]をクリックします。後でビューを変更（[Select a saved view] をクリック）し、トポロジの編集、名前の変更、またはビューの削除を選択できます。



第 9 章

システムアクセスとセキュリティの管理

ここでは、次の内容について説明します。

証明書の管理

証明書とは

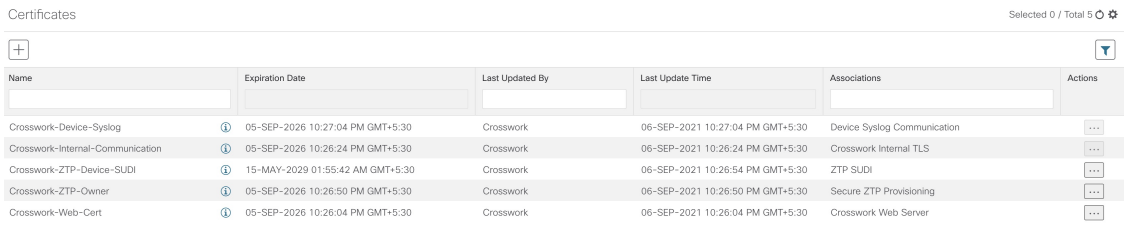
証明書は、個人、サーバー、会社、または別のエンティティを識別し、そのエンティティを公開キーに関連付ける電子文書です。公開キーを使用して証明書を作成すると、一致する秘密キーも生成されます。TLS では、公開キーはエンティティに送信されるデータの暗号化に使用され、秘密キーは復号に使用されます。証明書は、発行者または「親」証明書（認証局）によって、つまり、親の秘密キーによって署名されます。証明書は自己署名することもできます。TLS の交換では、証明書の発行者の有効性を確認するために証明書の階層が使用されます。この階層は信頼チェーンと呼ばれ、ルート CA 証明書（自己署名）、場合によっては複数レベルの中間 CA 証明書、およびサーバー（またはクライアント）証明書（エンドエンティティ）の 3 つのタイプで構成されます。中間証明書は、サーバー証明書を CA のルート証明書にリンクし、追加のセキュリティ層を提供する「信頼のリンク」として機能します。ルート証明書の秘密キーから開始し、信頼チェーン内の各証明書の秘密キーは、最終エンティティ証明書に最終的に署名するまで、チェーン内の次の証明書に署名して発行します。エンドエンティティ証明書は、チェーン内の最後の証明書であり、クライアント証明書またはサーバー証明書として使用されます。これらのプロトコルの詳細については、「X.509 証明書 （357 ページ）」と「HTTPS （357 ページ）」を参照してください。

Crosswork での証明書の使用方法

Crosswork アプリケーションとデバイス間の通信やさまざまな Crosswork コンポーネント間の通信は、TLS プロトコルを使用して保護されます。TLS は X.509 証明書を使用して安全にデバイスを認証し、データを暗号化して送信元から接続先までその整合性を確保します。Crosswork は、生成された証明書とクライアントがアップロードした証明書を組み合わせて使用します。アップロードされた証明書は、認証局（CA）から購入するか、自己署名することができます。たとえば、Cisco Crosswork VM がホストする Web サーバーとクライアントブラウザベースのユーザーインターフェイスは、TLS 経由で交換される Crosswork によって生成された X.509 証明書を使用して相互に通信します。

Crosswork Cert Manager は、分散フレームワーク内の複数のマイクロサービスおよびサービスのプロキシであり、すべての Crosswork 証明書を管理します。証明書管理 の UI（**[管理（Administration）] > [証明書管理（Certificate Management）]**）を使用すると、証明書を表示、アップロード、および変更できます。次の図に、Cisco Crosswork が提供するデフォルトの証明書を示します。

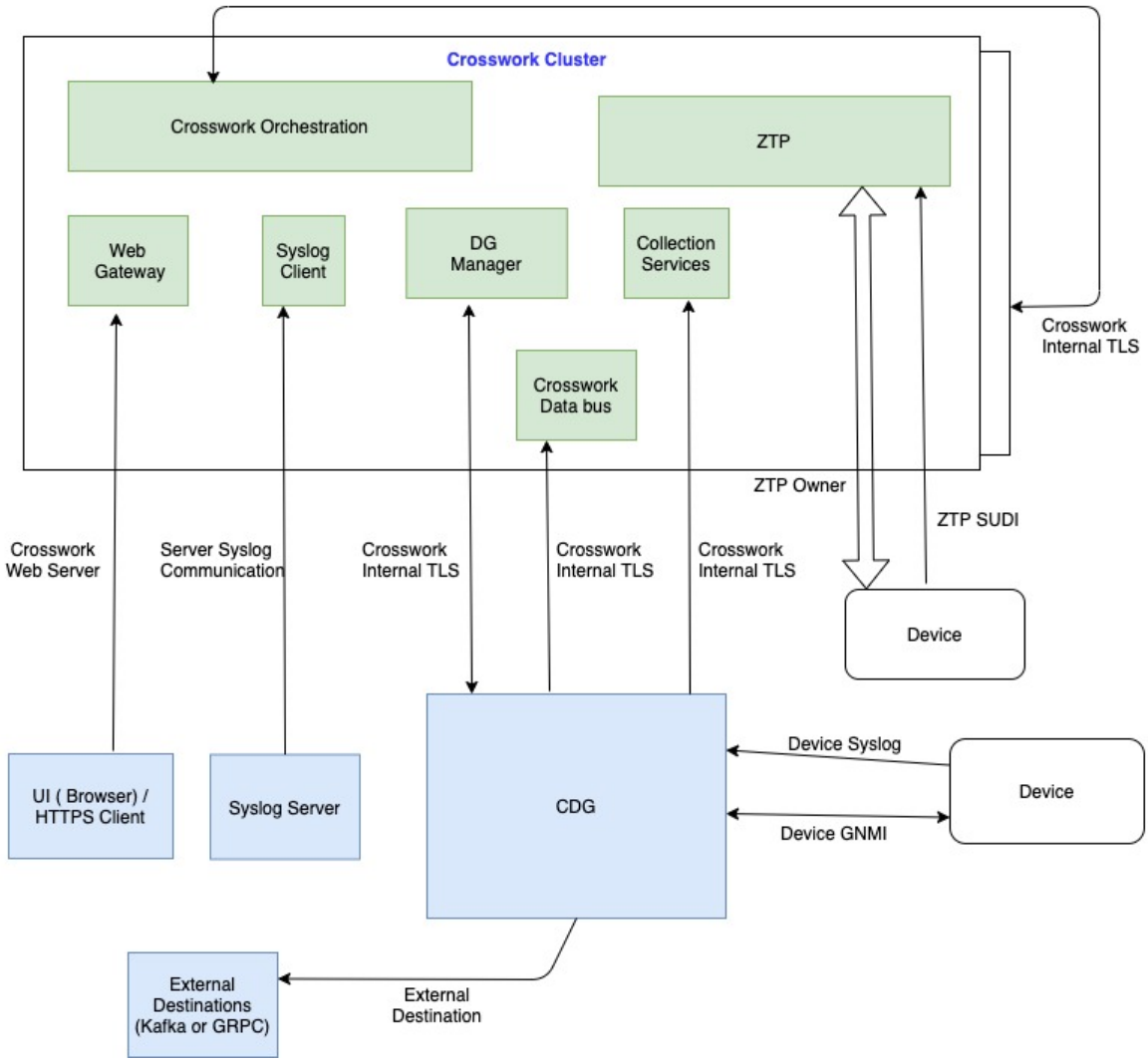
図 *60 :* 証明書管理の *UI*



証明書のタイプと使用方法

次の図に、Crosswork がさまざまな通信チャネルで証明書を使用する方法を示します。

図 *61 : Cisco Crosswork* の証明書



これらの証明書は、次の表に示すように、使用例に応じて異なるプロパティを持つさまざまなロールに分類されます。

ロール	UI 名	説明	サーバー	クライアント	許可される操作	デフォルトの有効期限	許可される有効期限
Crosswork（CW）内部 TLS	CW 内部通信（CW- Internal-Communication）	• Crosswork によって生成および提供されます。 • この信頼チェーンは、UI（サーバーとクライアントリーフ証明書を含む）で使用でき、初期化時に Crosswork によって作成されます。これらは、Crosswork と CDG 間のプロセス間通信と内部 Crosswork コンポーネント間の通信に使用されます。 • 相互認証とサーバー認証を許可します。	CW	• CDG • CW	ダウンロード	5 年	—
CW Web サーバー	CW Web 証明書（CW-Web-Certificate） サーバー認証	• Crosswork によって生成および提供されます。 • ユーザーブラウザと Crosswork 間の通信を提供します。 • サーバー認証を許可します。	CW Web サーバー	ユーザーブラウザまたは API クライアント	• アップロード • ダウンロード	5 年	30 日 ～ 5 年

ロール	UI 名	説明	サーバー	クライアント	許可される操作	デフォルトの有効期限	許可される有効期限
ZTP SUDI	CW ZTP デバイスの SUDI（CW-ZTP-Device-SUDI）	• Crosswork の一部として提供される公開シスコ証明書。 • ZTP アプリケーションとデバイス間の ZTP プロトコル通信チャネルを提供します。 • サーバー認証を許可します。	CW ZTP	Device	• アップロード • ダウンロード	100 日	30 日 ～ ユーザー定義
セキュア ZTP プロビジョニング	CW ZTP 所有者（CW-ZTP-Owner）	• Crosswork によって生成および提供されます。 • ZTP によってデバイスに転送され、暗号化の第 2 層に使用されます。	CW ZTP	Device	• アップロード • ダウンロード	5	30 日 ～ ユーザー定義
デバイスの Syslog	CW デバイスの Syslog（CW-Device-Syslog）	• Crosswork によって生成および提供されます。 • デバイスと CDG 間の Syslog テレメトリ通信を提供します。 • サーバー認証を許可します。	CDG	Device	ダウンロード	5 年	—

ロール	UI 名	説明	サーバー	クライアント	許可される操作	デフォルトの有効期限	許可される有効期限
デバイス gNMI 通信	—	デバイスと CDG 間の GNMI テレメトリ通信を提供します。	CDG	Device	• アップロード • ダウンロード	N/A	30 日 ～ ユーザー定義
サーバーの Syslog	N/A	• Crosswork から外部 Syslog サーバーへの syslog イベントとログを許可します。 • サーバー認証を許可します。	外部 Syslog サーバー	Crosswork	• アップロード （注） 異なるサーバーに関連付けられた複数の証明書をアップロードできます。 • ダウンロード	—	30 ～ ユーザー定義

ロール	UI 名	説明	サーバー	クライアント	許可される操作	デフォルトの有効期限	許可される有効期限
外部接続先	—	CDG から外部接続先（Kafka または GRPC）にテレメトリデータをエクスポートします。	外部接続先（Kafka または GRPC）	CDG	• アップロード （注） • ダウンロード	— 異なる接続先に関連付けられた複数の証明書をアップロードできます。	30 ～ ユーザー定義

Crosswork には 2 つのカテゴリロールがあります。

- 信頼チェーンのみをアップロードまたはダウンロードできるロール
- 信頼チェーンと中間証明書およびキーの両方のアップロードまたはダウンロードを許可するロール

新しい証明書の追加

次のロールの証明書を追加できます。

- [外部接続先（External Destination）]：このロール用にアップロードした証明書は、CDG と外部接続先（Kafka サーバーなど）間の通信を保護するために使用されます。相互認証を有効にするには、CDG と外部サーバーの両方に共通する **CA 証明書信頼チェーン**をアップロードします。この信頼チェーンには、ルート CA 証明書と任意の数のオプションの中間 CA 証明書が含まれています。チェーンの最後の中間証明書とそれに対応する秘密キーは、**中間キー**、**中間証明書**、およびオプションで**パスフレーズ**（中間キーの生成に使用した場合）を使用して UI に個別にアップロードされます。Crosswork は、外部接続先に接続する CDG のこの中間キーを使用して、クライアント証明書を内部的に作成します。接続先（Kafka など）のサーバー証明書の信頼は、同じルート CA 証明書から取得する必要があります。
- [Syslogサーバー通信（Syslog Server Communication）]：ユーザーは Syslog サーバー証明書の信頼チェーンをアップロードします。この信頼チェーンは、Syslog サーバーを認証するために Crosswork で使用されます。この信頼チェーンがアップロードされ、Crosswork 内に伝達されると、ユーザーは syslog サーバーを追加して（**[管理（Administration）]** > **[設定（Settings）]** > **[Syslog サーバー設定（Syslog Server Configuration）]**）、証明書を関連付けて TLS を有効にできます。詳細については、「Syslog サーバーの設定 （361 ページ）」を参照してください。
- [デバイスgNMI通信（Devices gNMI communication）]：ユーザーは、接続しているデバイスを認証するために CDG で使用される信頼チェーンのバンドルをアップロードします。この信頼チェーンとデバイス gNMI 証明書もデバイスで設定する必要があります。アップロードする信頼チェーンファイルには、ネットワーク内のすべてのデバイスが接続できるように、必要に応じて信頼証明書の階層を複数含めることができます。詳細については、「gNMI 証明書の設定 （92 ページ）」を参照してください。
- [セキュアLDAP通信（Secure LDAP Communication）]：ユーザーは、セキュア LDAP 証明書の信頼チェーンをアップロードします。この信頼チェーンは、LDAP サーバーを認証するために Crosswork で使用されます。この信頼チェーンがアップロードされて Crosswork 内に伝播されると、ユーザーは LDAP サーバーを追加し（LDAP サーバーの管理 （354 ページ） を参照）、証明書を関連付けることができます。

（注） Cisco Crosswork は、Web 証明書を直接受信しません。中間 CA と中間キーを受け入れて新しい Web 証明書を作成し、Web ゲートウェイに適用します。

（Cisco Crosswork 内で提供されるデフォルトの証明書を使用する代わりに）独自の ZTP（ゼロタッチプロビジョニングの概念 （213 ページ））と Web 証明書をアップロードする場合は、[編集（Edit）] 機能を使用します（「証明書の編集」を参照）。

始める前に

- 証明書のタイプと使用方法については、「証明書のタイプと使用方法 （316 ページ）」を参照してください。
- アップロードするすべての証明書がプライバシー強化メール（PEM）形式である必要があります。簡単に移動できるように、これらの証明書がシステム内のどこにあるかに注意してください。
- アップロードする信頼チェーンファイルには同じファイル内の階層全体（ルート CA と中間証明書）が含まれている場合があります。場合によっては、同じファイルで複数のチェーンを使用することもできます。
- 中間キーは、PKCS1 形式または PKCS8 形式である必要があります。
- 外部接続先の新しい証明書を追加する前に、データ送信先を設定する必要があります。詳細については、「データ宛先の追加または編集 （52 ページ）」を参照してください。

ステップ 1 メインメニューから **[管理（Administration）] > [証明書管理（Certificate Management）]** を選択し、＋をクリックします。

ステップ 2 署名書の一意の名前を入力します。

ステップ 3 [証明書のロール（Certificate Role）] ドロップダウンメニューから、証明書を使用する目的を選択します。詳細については、「証明書の管理 （315 ページ）」を参照してください。

ステップ 4 [参照（Browse）] をクリックして証明書の信頼チェーンに移動します。

ステップ 5 外部接続先証明書の場合は、1 つ以上の接続先を選択し、CA 証明書の信頼チェーン、中間証明書、および中間キーを指定する必要があります。パスフレーズフィールドはオプションで、中間キーの作成に使用されます（該当する場合）。

ステップ 6 [保存（Save）] をクリックします。

（注） アップロードされると、Crosswork 証明書マネージャはサーバー証明書を受け入れ、検証し、生成します。検証が成功すると、アラーム（「Crosswork Web サーバーの再起動（Crosswork Web Server Restart）」）によって証明書が適用されようとしていることが示されます。証明書管理 UI は自動的にログアウトし、証明書を Web ゲートウェイに適用します。新しい証明書を確認するには、https://<crosswork_ip>:30603 の横にあるロック <Not Secure>/<secure> アイコンをクリックします。

証明書の編集

証明書を編集して、接続先を追加または削除したり、期限切れまたは誤って設定された証明書をアップロードおよび置換したりできます。ユーザー指定の証明書と、ZTP および Web 証明書を編集できます。Cisco Crosswork が提供するその他のシステム証明書は変更できず、選択できません。

また、この手順に従って証明書を「削除」して証明書を置き換えるか、または割り当てられた接続先のセキュリティを無効にする（[セキュアな通信を有効にする（Enable Secure Communication）]オプションを無効にする）こともできます（「データ宛先の追加または編集（52 ページ）」を参照）。Cisco Crosswork システムからの証明書の永続的な削除はサポートされていません。

（注） ZTP 証明書については、「ZTP アセットの組み立てと読み込み（227 ページ）」を参照してください。

ステップ 1 メインメニューから、**[管理（Administration）]** > **[証明書管理（Certificate Management）]** を選択し、変更する証明書を確認します。

ステップ 2 変更する証明書で … をクリックし、[証明書の更新（Update Certificate）] を選択します。

ステップ 3 必要なオプションを更新します。

（注） CW Web サーバー証明書の更新時に、次のフィールドに関連する値を入力します。

- [Crosswork Web CA]：ルート CA 証明書と中間証明書を 1 つ以上含むか、まったく含んでいない信頼チェーンファイル（PEM 形式）。
- [Crosswork Web 中間（Crosswork Web Intermediate）]：ルート CA 証明書で署名された中間 CA 証明書。
- [Crosswork Web 中間キー（Crosswork Web Intermediate Key）]：中間 CA 証明書に関連付けられているキー。
- [Crosswork Web パスフレーズ（Crosswork Web Passphrase）]：これはオプションのフィールドです。

検証が成功すると、証明書管理 UI が自動的にログアウトし、Web ゲートウェイに証明書を適用します。

ステップ 4 [保存（Save）] をクリックします。

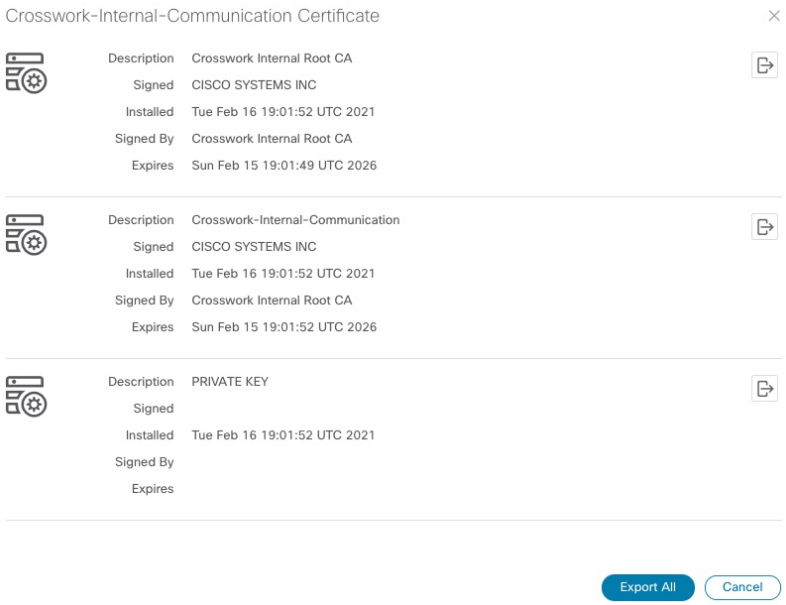
証明書のダウンロード

証明書をエクスポートするには、次の手順を実行します。

ステップ 1 メインメニューから **[管理（Administration）]** > **[証明書管理（Certificate Management）]** を選択します。

ステップ 2 ダウンロードする証明書の ⓘ をクリックします。

図 *62 :* 証明書のエクスポート



ステップ 3 ルート証明書、中間証明書、および秘密キーを個別にダウンロードするには、をクリックします。証明書と秘密キーすべてを一度にダウンロードするには、[すべてエクスポート（Export All）] をクリックします。

証明書の更新

証明書は、有効期限が切れるまで1年間有効です。以下の手順は、クラスタ内の各ノード（ハイブリッドとワーカー）で順番に実行する必要があります。1 つのノードで証明書を更新したら、次のノードに進む前にポッドが正常であることを確認します。

（注） 有効期限が切れる前に証明書を更新する場合は、クラスタが動作状態にあるため、メンテナンスウィンドウ中にこのアクティビティを実行することをお勧めします。

証明書を更新するには、次の手順を実行します。

ステップ 1 ノードで、コマンドを実行して root ユーザーに移動します。

```
sudo -i
```

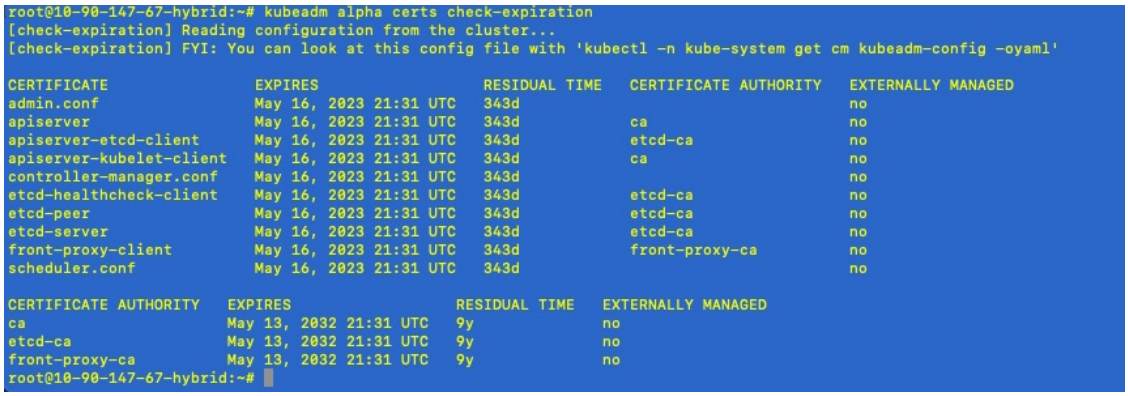
パスワードを入力するように求められます。`cw-admin` ユーザーパスワード。

ステップ 2 証明書の日付が期限切れになっているかどうかを確認します。

```
kubeadm alpha certs check-expiration
```

次の画像は、出力のサンプルです。

図 *63* : 証明書の有効期限のサンプル出力



ステップ 3 証明書と conf ファイルのバックアップを作成します。

```
mkdir $HOME/Old-K8-Certs
mkdir $HOME/Old-K8-Certs/pki
cp -p /etc/kubernetes/pki/*.* $HOME/Old-K8-Certs/pki
cp -p /etc/kubernetes/*.conf $HOME/Old-K8-Certs
~#
```

ステップ 4 コマンドを実行して証明書を更新します。

```
kubeadm alpha certs renew all
```

ステップ 5 手順 2 を繰り返して、新しい証明書の作成を確認します。

ステップ 6 コマンドを実行して kubelet を再起動します。

```
systemctl stop kubelet
```

（注） 再起動はすべてのノードで発生し、更新された証明書は kubelet と kube-apiserver が再起動されるまで有効になりません。再起動時にアプリケーションからの操作を停止することをお勧めします。

kubelet を停止した後、次のプロセスを見つけます（ps -eaf | grep を使用）<process name>）：

```
kube-apiserver
controller-manager
kube-scheduler
```

それらを中止（kill -9 <pid> を使用）します。上記のプロセスを強制終了した後、以下を実行して kubelet を再起動します。

```
systemctl daemon-reload
systemctl start kubelet
```

ノードは最初に劣化状態に移行し、次にダウン状態に移行します。

（注） ノードがダウン状態に移行した後でも、syslog には引き続きトラフィックが表示される場合があります。

```
10-90-147-67-hybrid kernel: [1897091.695393] ll header: 00000000: ff ff ff ff ff ff fa
51 56 a2 9c 7c 08 0
10-90-147-67-hybrid kernel: [1897091.695414] IPv4: martian source 169.254.1.1 from
10.244.215.17, on dev calieff0340c649
10-90-147-67-hybrid kernel: [1897091.695416] ll header: 00000000: ff ff ff ff ff ff 72
e8 75 10 bb 64 08 06
```

ステップ 7 すべてのポッドが正常で実行されていることを確認します。

```
kubectl get pods -A -o wide
```

また、再起動したハイブリッドノードで実行中のポッドも検証します。

ステップ 8 証明書が更新されているかどうかを確認します。

ステップ 9 問題が引き続き発生する場合は、conf ファイルを変更します。

```
sudo kubeadm alpha kubeconfig user --org system:nodes --client-name system:node:$(hostname) >
/etc/kubernetes/kubelet.conf
```

クラスター内のノードごとに上記の手順を繰り返します。

ライセンスの管理

シスコ スマート ライセンシングは、シスコ ポートフォリオ全体および組織全体でソフトウェアをより簡単かつ迅速に一貫して購入および管理できる柔軟なライセンスモデルです。また、これは安全です。ユーザーがアクセスできるものを制御できます。スマートライセンスを使用すると、次のことが可能になります。

- **簡単なアクティベーション**：スマートライセンスは、組織全体で使用できるソフトウェアライセンスのプールを確立します。PAK（製品アクティベーションキー）は不要です。
- **管理の統合**：My Cisco Entitlements（MCE）は、使いやすいポータルですべてのシスコ製品とサービスの完全なビューを提供するので、取得したもの、使用しているものを常に把握できます。
- **ライセンスの柔軟性**：ソフトウェアはハードウェアにノードロックされていないため、必要に応じてライセンスを簡単に使用および転送できます。

スマートライセンスを使用するには、まず Cisco Software Central でスマートアカウントを設定する必要があります（software.cisco.com）。**Cisco スマートアカウント**は、スマート対応製品のリポジトリを提供し、シスコライセンスの有効化、ライセンスの使用状況の監視、およびシスコ製品購入の追跡を可能にします。**Cisco Smart Software Manage（CSSM）**を使用すると、一元化された 1 つの Web サイトから Cisco スマートソフトウェアのすべてのライセンスを管理できます。Cisco Smart Software Manager では、ライセンスを管理するためにスマートアカウント内で複数のバーチャルアカウントを作成および管理できます。シスコライセンスの詳細については、cisco.com/go/licensingguide を参照してください。

メインメニューから **[管理（Administration）]** > **[スマートライセンスの登録（Smart Licensing Registration）]** を選択し、[スマート ソフトウェア ライセンス（Smart Software Licensing）] ウィンドウを表示します。このウィンドウを使用して、Cisco Crosswork アプリケーションの登録、トランスポート設定の編集、ライセンスの更新、アプリケーションの登録解除を行うことができます。

スマートライセンスの登録の前提条件

次が必要です。

- Cisco スマートアカウント。
- Cisco Crosswork アプリケーションの購入済みライセンス。

転送設定

トランスポート設定を構成して、Cisco Crosswork とシスコのサーバーとの通信方法を決定します。

- [直接（Direct）]：アプリケーションは Cisco Smart Software Manager（CSSM）に直接接続します。
- [トランスポートゲートウェイ（Transport Gateway）]：アプリケーションは、トランスポートゲートウェイ、またはクラウドベースのユーザーエクスペリエンスを複製してもオンプレミスのすべての通信を保持する CSSM オンプレミスオプションを介して通信します。

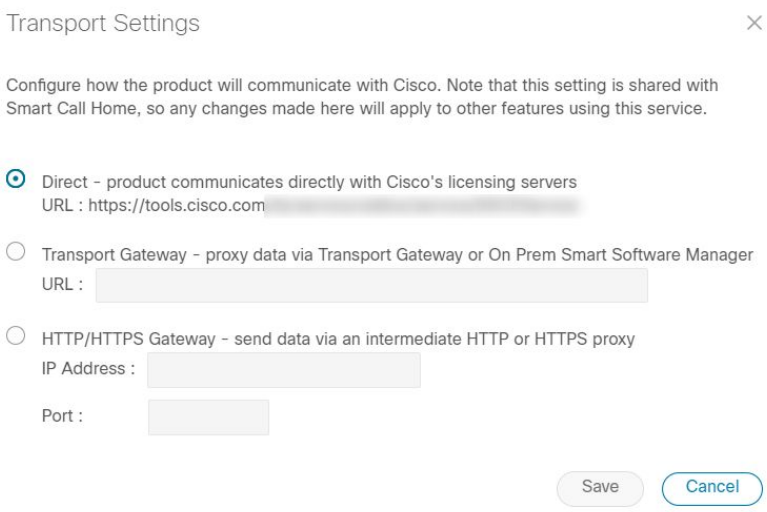
（注） CSSM オンプレミスオプションの詳細については、『Smart Software Manager guide』を参照してください。

- [HTTP/HTTPS ゲートウェイ（HTTP/HTTPS Gateway）]：アプリケーションは中間プロキシサーバーを介して接続します。これは、直接モードにのみ適用されます。

（注） トランスポート設定は、Cisco Crosswork が登録モードになっている間は変更できません。変更するには登録を解除する必要があります。

ステップ 1 [スマート ソフトウェア ライセンス（Smart Software Licensing）] ウィンドウの [トランスポート設定（Transport Settings）] に、現在選択されているトランスポートモードが表示されます。変更するには、[表示/編集（View/Edit）] をクリックします。

[トランスポート設定（Transport Settings）] ダイアログボックスが表示されます。



ステップ 2 関連するトランスポートモードを選択し、表示されたフィールドに関連するエントリを入力します。

ステップ 3 [保存（Save）] をクリックします。

Cisco Crosswork アプリケーションの登録

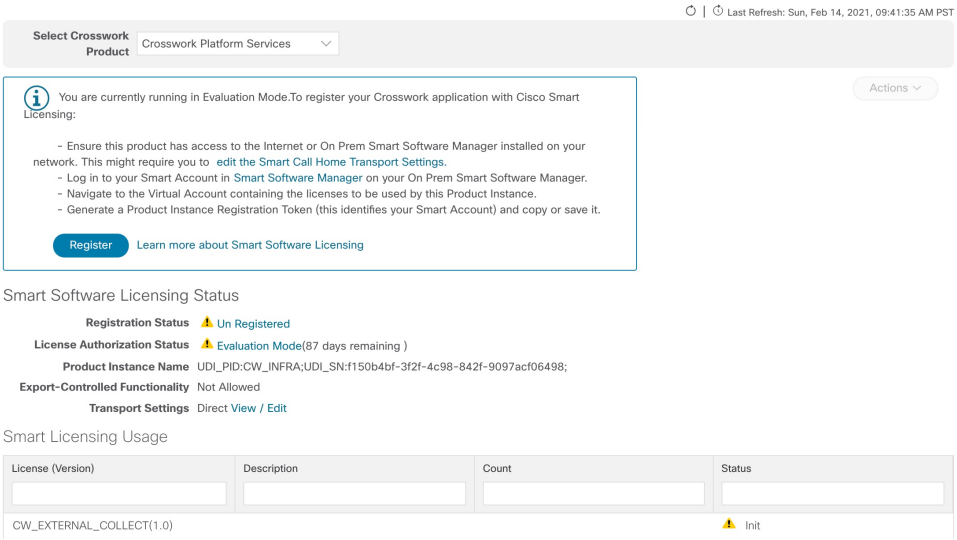
ライセンス機能を有効にするには、登録 ID トークンを使用して Cisco Crosswork アプリケーションを CSSM に登録する必要があります。登録されると、ID 証明書はスマートアカウントに安全に保存され、進行中のすべての通信に使用されます。証明書は 1 年間有効で、6 ヵ月後に自動的に更新されて継続的な運用が保証されます。

（注） 登録トークンの生成については、Smart Software Manager の Web ページで提供されているサポートリソースを参照してください。

ステップ 1 メインメニューから **[管理（Administration）]** > **[スマートライセンスの登録（Smart Licensing Registration）]** を選択し、[スマート ソフトウェア ライセンス（Smart Software Licensing）] ウィンドウを表示します。登録ステータス

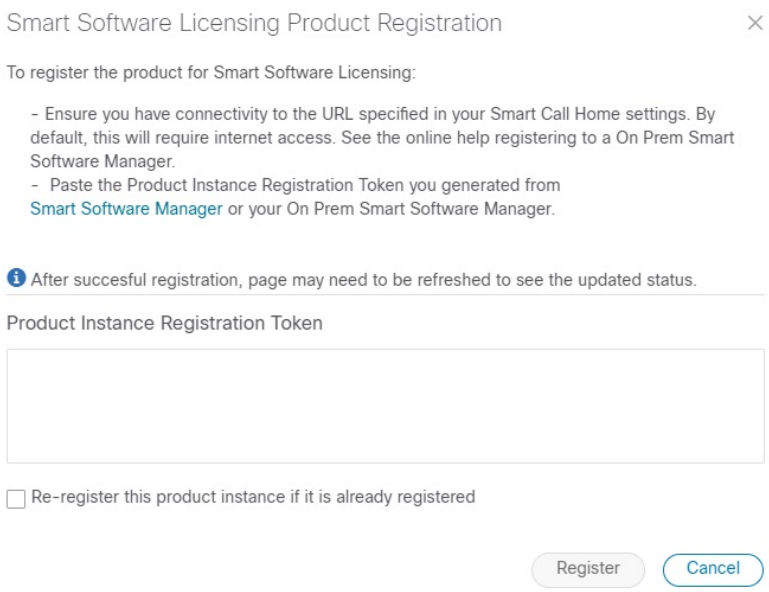
登録ステータスとライセンス認証ステータスは、それぞれ [未登録（Unregistered）] と [評価（Evaluation）] モードになります。

図 *64* : スマート ソフトウェア ライセンスの未登録の例



ステップ 2 [スマート ソフトウェア ライセンス（Smart Software Licensing）] ウィンドウで、[登録（Register）] をクリックします。

[スマート ソフトウェア ライセンス製品の登録（Smart Software Licensing Product Registration）] ダイアログボックスが表示されます。



ステップ 3 **[製品インスタンス登録トークン（Product Instance Registration Token）]** フィールドに、スマートアカウントから生成された登録トークンを入力します。トークン ID が正確で、有効期間内であることを確認してます。詳細については、「https://www.cisco.com/c/en_in/products/software/smart-accounts/software-licensing.html」を参照してください。

ステップ 4 （オプション）アプリケーションを再登録する場合は、[すでに登録されている場合はこの製品を再登録します（Re-register this product registration if is already registered）] チェックボックスをオンにします。

（注） バックアップ復元または災害後の復元操作の後、Cisco Crosswork VM を CSSM に手動で再登録する必要があります。これは、復元操作で使用されるバックアップの取得中にすでに登録されている Cisco Crosswork VM の場合に適用されます。

ステップ 5 [登録（Register）] をクリックします。登録の処理には数分かかる場合があります。成功すると、「製品登録が正常に完了しました（Product Registration completed successfully）」というメッセージが表示されます。

登録ステータスとライセンス認証ステータスは、それぞれ [登録済み（Registered）] と [承認済み（Authorized）] に更新されます。

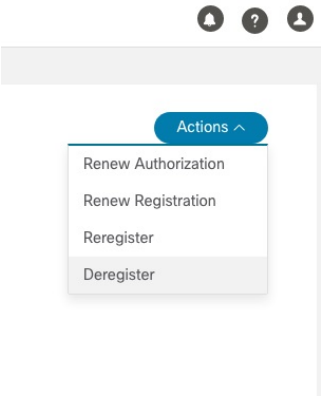
（注）
- 登録エラー（「通信送信エラー」や「ライセンスクラウドからの無効な応答」など）が発生した場合は、しばらく待ってから登録を再試行してください。複数回試行してもエラーが続く場合は、シスコ カスタマー エクスペリエンス チームにお問い合わせください。
- 登録中に通信タイムアウトエラーが発生した場合は、エラーダイアログボックスで [OK] をクリックすると、アプリケーションが登録を再試行します。
- 場合によっては、登録が成功した後に更新されたステータスを表示するには、ページを手動で更新する必要があります。

ライセンスアクションの手動での実行

Cisco Crosswork の場合、登録および認証の更新はデフォルトで自動的に有効になっています。ただし、アプリケーションとシスコサーバー間の通信障害が発生した場合は、これらのアクションを手動で開始できます。[アクション（Actions）] ドロップダウンボタンを使用して、アプリケーションを手動で更新、再登録、および登録解除できます。

（注） Cisco Optimization Engine スマートライセンスの場合、ノードカウントは、デバイスの最初のオンボーディング中、およびライセンスの登録と資格付与中に追跡されます。ノード数の変更は、GMT の 24 時間ごとにスマートライセンスサーバーと同期されます。待機しない場合は、アプリケーションライセンスを再登録して、ノード数をすぐに更新できます。

ステップ 1 [スマートライセンス（Smart License）] ウィンドウで、[アクション（Actions）] ドロップダウンボタンをクリックし、次のクイックアクションに関連するオプションを選択します。



a) **[アクション（Actions）] > [認証の更新（Renew Authorization）]**：30 日の終わりに自動更新サービスが失敗した場合に手動で認証を更新します。

b) **[アクション（Actions）]>[登録の更新（Renew Registration）]**：6 か月の終わりに自動更新サービスが失敗した場合に手動で登録を更新します。

c) **[アクション（Actions）] > [再登録（Re-register）]**：登録トークンの期限切れなどの理由で、アプリケーションを再登録します。

d) **[アクション（Actions）] > [登録解除（De-register）]**：トランスポート設定を変更する必要があるなどの場合に、アプリケーションの登録を解除します。

（注） 登録が解除されると、アプリケーションは [評価（Evaluation）] モード（評価期間がある場合）または [評価期限切れ（Evaluation Expired）] モードに移行します。詳細については、ライセンス認証ステータス （332 ページ）を参照してください。

ステップ 2 選択したアクションが正常に実行されます。

ライセンス認証ステータス

Cisco Crosswork アプリケーションの登録ステータスに基づいて、次のライセンス認証ステータスが表示されます。

表 *24 :* ライセンス認証ステータス

登録ステータス	ライセンス認証ステータス	説明
未登録	評価モード（Evaluation mode）	アプリケーションのライセンス機能を自由に使用できる 90 日の評価期間。この状態は、アプリケーションを初めて使用するときに開始されます。
	評価期限切れ（Evaluation Expired）	評価期間の終了時にアプリケーションが正常に登録されませんでした。この状態の間、アプリケーション機能は無効になります。アプリケーションを使用し続けるには、登録する必要があります。
	登録期限切れ（Registered Expires）	アプリケーションは、アイデンティティ証明書の有効期限が切れる前に CSSM に接続できず、未登録状態に戻りました。残りの評価期間がある場合、アプリケーションは再開します。この段階では、アプリケーションを再登録するために新しい登録 ID トークンが必要です。
登録済み	承認済み（準拠）（Authorized (In Compliance)）	アプリケーションは、予約済みのライセンス機能の使用を完全に許可されています。認証は 30 日ごとに自動的に更新されます。
	コンプライアンス違反（Out of Compliance）	アプリケーションの現在の機能を使用するために予約できる十分なライセンスが関連付けられたバーチャルアカウントにありません。アプリケーションを引き続き使用するには、トークンに登録されている権限/使用制限を更新する必要があります。
	認証が期限切れ（Authorization Expired）	アプリケーションが 90 日以上 CSSM と通信できず、認証の有効期限が切れています。

ユーザーの管理

ベストプラクティスとして、管理者はすべてのユーザーに対して個別のアカウントを作成する必要があります。Cisco Crosswork を使用するユーザーのリストを準備します。ユーザー名と予備パスワードを決定し、それらのユーザープロファイルを作成します。ユーザーアカウントの作成時に、ユーザーがアクセスできる機能を決定するためのユーザーロールを割り当てます。「admin」以外のユーザーロールを使用する場合は、ユーザーを追加する前にユーザーロールを作成します（「ユーザーロールの作成 （337 ページ）」を参照）。

ステップ 1 メインメニューから、**[管理（Administration）] > [ユーザーとロール（Users and Roles）] > [ユーザー（Users）]** タブを選択します。このウィンドウから、新しいユーザーの追加、既存のユーザーの設定の編集、およびユーザーの削除を行うことができます。

ステップ 2 新しいユーザーを追加するには、次の手順を実行します

a) ⊞ をクリックして必要なユーザーの詳細を入力します。

b) [保存（Save）] をクリックします。

ステップ 3 ユーザーを編集するには、次の手順を実行します。

a) ユーザーの横にあるチェックボックスをクリックし、✎ をクリックします。

b) 変更を加えたら、[保存（Save）] をクリックします。

ステップ 4 ユーザーを削除するには、次の手順を実行します。

a) ユーザーの横にあるチェックボックスをクリックし、🗑 をクリックします。

b) [削除の確認（Confirm Deletion）] ウィンドウで、[削除（Delete）] をクリックします。

ステップ 5 ユーザーの監査ログを表示するには、次の手順を実行します：

a) [アクション（Actions）] 列の下の ⋯ アイコンをクリックし、[監査ログ（Audit Log）] を選択します。

選択したユーザー名の [監査ログ（Audit Log）] 画面が表示されます。監査ログの詳細については、「View Audit Log （392 ページ）」を参照してください。

インストール時に作成された管理ユーザー

インストール時に、Crosswork は 2 つの特別な管理 ID を作成します。

1. ユーザー名が **cw-admin** で、デフォルトのパスワードが **admin** の**仮想マシン管理者**。データセンター管理者はこの ID を使用してログインし、Crosswork サーバーをホストしている VM をトラブルシューティングします。
2. ユーザー名が **admin** でデフォルトのパスワードが **admin** の **Cisco Crosswork 管理者**。製品管理者は、この ID を使用してログインし、ユーザーインターフェイスを設定し、新しいユーザー ID の作成などの特別な操作を実行します。

両方の管理ユーザー ID のデフォルトパスワードは、最初に使用するときに変更する必要があります。次の方法を使用して、Cisco Crosswork 管理者パスワードを変更することもできます。

- 管理者ユーザーとしてログインし、管理者ユーザーパスワードを編集します。
- `admin(config)# username admin <password>` と入力します。

ユーザーロール、機能カテゴリ、および権限

[ロール（Roles）] ウィンドウでは、適切な権限を持つユーザーがカスタムユーザーロールを定義できます。デフォルトの *admin* ロールと同様に、カスタムユーザーロールは次の要素で構成されます。

- 「Operator」や「admin」などの一意の名前。
- 選択した、名前付きの 1 つ以上の機能カテゴリ。そのロールを持つユーザーが、API によって制御されている特定の Cisco Crosswork 機能を実行するために必要なその API にアクセスできるかどうかを制御します。
- 選択した 1 つ以上の権限。そのロールを持つユーザーが機能カテゴリ内で実行できる操作の範囲を制御します。

ユーザーロールが機能カテゴリにアクセスできるようにするには、そのカテゴリとその基盤となる API が選択済みであることがそのロールの [ロール（Roles）] ページに表示されている必要があります。機能カテゴリが未選択としてユーザーロールに表示されている場合、このロールが割り当てられているユーザーは、その機能領域にアクセスすることはできません。

一部の機能カテゴリは、1 つのカテゴリ名で複数の API をグループ化します。たとえば、「AAA」カテゴリは、パスワードの変更、リモート認証サーバーの統合、およびユーザーとロールの管理の API へのアクセスを制御します。このタイプのカテゴリでは、一部の API を選択しないままにして、それら API へのアクセスを拒否する一方で、他の API を選択してカテゴリ内のそれらの API へのアクセスを提供することができます。たとえば、自身のパスワードを変更できても、リモート AAA サーバーのインストールを統合するための設定を表示または変更できない、または新しいユーザーとロールを作成できない「オペレータ」ロールを作成する場合は、「AAA」というカテゴリ名を設定し、[リモート認証サーバー統合 API（Remote Authentication Server Integration API）] チェックボックスと [ユーザーおよびロール管理 API（Users and Role Management API）] チェックボックスをオフにします。

選択したカテゴリの各ロールについて、[ロール（Roles）] ページでは、基盤となる各機能 API に対する権限を定義することもできます。

- [読み取り（Read）] 権限では、ユーザーはその API によって制御されているオブジェクトを表示および操作できますが、オブジェクトの変更や削除はできません。
- [書き込み（Write）] 権限では、ユーザーはその API によって制御されているオブジェクトを表示および変更できますが、削除はできません。
- [削除（Delete）] 権限では、その API によって制御されているオブジェクトに対する削除権限がユーザーロールに付与されます。削除権限は、Crosswork プラットフォームとそのアプリケーションによって設定された基本的な制限を上書きしないことに注意してください。

必要に応じて権限を混在させることもできます。

- ユーザーアクセス用の API を選択する場合は、その API に少なくとも「読み取り」権限を付与する必要があります。

- ユーザーアクセス用の API を選択すると、Cisco Crosswork はそのユーザーがその API に対するすべての権限を持つことを想定し、自動的に 3 つの権限すべてを選択します。
- [読み取り（Read）] を含むすべての権限をオフにすると、Cisco Crosswork は API へのアクセスを拒否すると想定し、選択が解除されます。

ベスト プラクティス：

カスタムユーザーロールを作成する場合は、次のベストプラクティスに従うことをお勧めします。

- Crosswork の展開全体のメンテナンスと管理のための管理を明示的に担当する管理者ユーザーのロールでの [削除（Delete）] 権限を制限します。
- すべての Cisco Crosswork API を使用する開発者のロールには、管理者ユーザーと同じ権限が必要です。
- Cisco Crosswork を使用してネットワークの管理に積極的に関与しているユーザーには、少なくとも [読み取り（Read）] 権限と [書き込み（Write）] 権限をロールに適用します。
- システムアーキテクトまたはプランナーとしての業務に役立つ Cisco Crosswork データのみを表示する必要があるユーザーには、ロールへの読み取り専用アクセス権を付与します。

次の表に、作成を検討する必要があるカスタムユーザーロールの例を示します。

表 *25 :* カスタムユーザーロールの例

ロール	説明	カテゴリ/API	権限
オペレータ	アクティブネットワーク マネージャ。KPIアラートに応じてプレイブックをトリガーします。	すべて	読み取り、書き込み
モニター	アラートのみをモニターします	Health Insights、インベントリ、トポロジ	読み取り専用
API インテグレータ	すべて	すべて	すべて

（注） 管理者ロールには読み取り、書き込み、および削除の権限を含める必要があり、読み取り/書き込みロールには読み取りと書き込みの両方の権限を含める必要があります。ゼロタッチプロビジョニング機能を使用するには、すべての ZTP API にアクセスする必要があります。

ユーザーロールの作成

管理者権限を持つローカルユーザーは、必要に応じて新しいユーザーを作成できます（「ユーザーの管理 （333 ページ）」を参照）。

この方法で作成されたユーザーは、割り当てたユーザーロールに関連付けられている機能またはタスクのみを実行できます。

ローカル **admin** ロールは、すべての機能へのアクセスを可能にします。インストール時に作成され、変更または削除することはできません。ただし、その権限は新しいローカルユーザーに割り当てることができます。ローカルユーザーのみがユーザーロールを作成または更新できます。 TACACS ユーザーはそれらの操作を実行できません。

新しいユーザーロールを作成するには、次の手順を実行します。

ステップ 1 メインメニューから、**[管理（Administration）]**>**[ユーザーとロール（Users and Roles）]**>**[ロール（Roles）]** タブを選択します。

[ロール（Roles）] ウィンドウの左側には [ロール（Roles）] テーブル、右側には対応する [管理（admin）] テーブルがあり、選択したロールのユーザー権限のグループが表示されます。

ステップ 2 [ロール（Roles）] テーブルで、＋をクリックしてテーブルに新しいロールエントリを表示します。

ステップ 3 新しいロールに一意の名前を入力します。

ステップ 4 ユーザーロールの権限設定を定義します。

a) このロールを持つユーザーがアクセスできるすべての API のチェックボックスをオンにします。API は、対応するアプリケーションに基づいて論理的にグループ化されます。

b) API ごとに、適切なチェックボックスをオンにして、ユーザーロールに [読み取り（Read）]、[書き込み（Write）]、および [削除（Delete）] の権限があるかどうかを定義します。API グループ全体（AAA など）を選択することもできます。グループ内のすべての API が選択され、これらの API には [読み取り（Read）]、[書き込み（Write）]、および [削除（Delete）] の権限が事前に選択されています。

ステップ 5 [保存 (Save)] をクリックして、新しいロールを作成します。

新しいユーザーロールを 1 つ以上のユーザー ID に割り当てるには、ユーザー ID の [ロール（Role）] の設定を編集します（「ユーザーロールの編集 （338 ページ）」を参照）。

ユーザーロールの複製

既存のユーザーロールの複製は、新しいユーザーロールの作成と同じですが、権限を設定する必要はありません。必要に応じて、複製されたユーザーロールに元のユーザーロールのすべての権限を継承させることができます。

ユーザーロールの複製は、多数の新しいユーザーロールをすばやく作成して割り当てるための便利な方法です。次の手順に従って、既存のロールを複数回複製できます。複製されたユーザーロールの権限の定義はオプションの手順です。複製されたロールに新しい名前を付ける必要があるだけです。必要に応じて、ユーザーグループに実行するロールを示す名前を割り当て

ることができます。次に、そのユーザーグループのユーザー ID を編集して、新しいロールを割り当てます（「ユーザーの管理（333ページ）」を参照）。後で、ロール自体を編集してユーザーに必要な権限を付与できます（「ユーザーロールの編集（338 ページ）」を参照）。

ステップ 1 メインメニューから、**[管理（Administration）]>[ユーザーとロール（Users and Roles）]>[ロール（Roles）]** タブを選択します。

ステップ 2 既存のロールをクリックします。

ステップ 3 をクリックして、元のロールのすべての権限を持つ新しい重複エントリを [ロール（Roles）] テーブルに作成します。

ステップ 4 複製したロールに一意の名前を入力します。

ステップ 5 （オプション）ロールの設定を定義します。

a) 複製したロールがアクセスできるすべての API のチェックボックスをオンにします。

b) 各 API について、適切なチェックボックスをオンにして、クローンロールに [読み取り（Read）]、[書き込み（Write）]、および [削除（Delete）] の権限があるかどうかを定義します。API グループ全体（AAA など）を選択することもできます。グループ内のすべての API が選択され、これらの API には [読み取り（Read）]、[書き込み（Write）]、および [削除（Delete）] の権限が事前に選択されています。

ステップ 6 [保存 (Save)] をクリックして、新たに複製したロールを作成します。

ユーザーロールの編集

管理者権限を持つユーザーは、デフォルトの **admin** ロール以外のユーザーロールの権限をすばやく変更できます。

ステップ 1 メインメニューから、**[管理（Administration）]>[ユーザーとロール（Users and Roles）]>[ロール（Roles）]** タブを選択します。

ステップ 2 [ロール（Roles）] テーブルで、既存のロールをクリックして選択します。右側の [管理者（Admin）] テーブルに、選択したロールの権限設定が表示されます。

ステップ 3 ロールの設定を定義します。

a) ロールがアクセスできるすべての API のチェックボックスをオンにします。

b) API ごとに、適切なチェックボックスをオンにして、ロールに [読み取り（Read）]、[書き込み（Write）]、および [削除（Delete）] の権限があるかどうかを定義します。API グループ全体（AAA など）を選択することもできます。グループ内のすべての API が選択され、これらの API には [読み取り（Read）]、[書き込み（Write）]、および [削除（Delete）] の権限が事前に選択されています。

ステップ 4 完了したら、[保存（Save）] をクリックします。

ユーザーロールの削除

管理者権限を持つユーザーは、デフォルトの**admin**ユーザーロールではないユーザーロール、または現在ユーザー ID に割り当てられていないユーザーロールを削除できます。1 つ以上のユーザー ID に現在割り当てられているロールを削除する場合は、それらのユーザー ID を編集して別のユーザーロールに割り当てる必要があります。

ステップ 1 メインメニューから、**[管理（Administration）]**>**[ユーザーとロール（Users and Roles）]**>**[ロール（Roles）]** タブを選択します。

ステップ 2 削除するロールをクリックします。

ステップ 3 をクリックします。

ステップ 4 [削除（Delete）] をクリックして、ユーザーロールの削除を確定します。

ロール権限のカテゴリ

[ロール（Roles）] ウィンドウでは、適切な権限を持つユーザーがカスタムユーザーロールを定義できます。

次の表は、Cisco Crosswork のさまざまなロール権限カテゴリの概要です。

表 *26 :* ロール権限のカテゴリ

カテゴリ	ロール権限	説明
AAA	パスワード変更 API	パスワードを管理する権限を提供します。読み取りおよび書き込みアクセス許可は、デフォルトで自動的に有効になります。削除アクセス許可は、パスワード変更操作には適用されません（パスワードは削除できません。変更のみが可能です）。
	リモート認証サーバー統合 API	Crossworkでリモート認証サーバー構成を管理する権限を提供します。構成を表示/読み取るには読み取りアクセス許可が必要です。また、外部認証サーバー（LDAP、TACACS など）の構成を Crossworkに追加/更新するには、書き込みアクセス許可が必要です。削除アクセス許可は、これらの API には適用されません。
	ユーザーとロールの管理 API	ユーザー、ロール、セッション、およびパスワードポリシーを管理する権限を提供します。サポートされている操作には、「新しいユーザー/ロールの作成」、「ユーザー/ロールの更新」、「ユーザー/ロールの削除」、「ユーザー/ロールのタスク詳細の更新」、「セッション管理（アイドル タイムアウト、最大セッション..）」が含まれます。 "、"パスワード ポリシーの更新"、"パスワード ツールチップのヘルプ テキストの取得"、"アクティブなセッションの取得" など。 読み取りアクセス許可ではコンテンツを表示でき、書き込みアクセス許可では作成と更新ができ、削除アクセス許可ではユーザーまたはロールを削除できます。
アラーム	アラーム API	アラームを管理できます。 読み取りアクセス許可により、要求基準に従ってイベント/アラームを取得し、Syslog 宛先のリストを取得し、トラップ宛先のリストを取得できます。 書き込みアクセス許可により、アラームが発生または確認されたときの応答の設定、イベントの作成/発生、イベント情報マニフェストの更新、およびアラームへのメモの追加を行うことができます。 削除アクセス許可により、REST宛先、Syslog宛先、およびトラップ宛先を削除できます。

カテゴリ	ロール権限	説明
自動保証 DSS インスタンス	データストアサービスの管理者設定	管理者は、データストアストレージ情報（読み取りアクセス許可）を表示し、外部ストレージ（書き込みアクセス許可）の診断テストを実行できます。
	データストアサービス API	長期保存のために外部ストレージを使用したり、サービスメトリクスデータをアーカイブするために Service Assurance が使用する外部データストアを管理したりできます。 読み取りアクセス許可により、ストレージプロバイダー情報の取得、ストレージ統計の確認などを行うことができます。 書き込みアクセス許可により、ローカル CW データストアを外部ストレージと同期し、診断を実行できます。 削除アクセス許可により、外部ストレージプロバイダーを削除できます。

カテゴリ	ロール権限	説明
Crosswork Network Controller	CAT FP 展開マネージャ API	関数パックのアップロードと展開を管理できます。 読み取りアクセス許可により、パッケージ、ファイル、および展開情報のリストを取得できます。 書き込みアクセス許可により、パッケージ/関数パック/ファイルをアップロード/展開/展開解除できます。 削除アクセス許可は、これらの API には適用されません。
	CAT インベントリ RESTCONF API	North Bound Interface（NBI）CAT サービスインベントリデータ用の RESTCONF インターフェイス（CAT から外部コンシューマーへ）。 読み取りアクセス許可では CAT からサービス情報を取得でき、書き込みアクセス許可ではオペレーション API を呼び出して CAT からサービス情報を取得できます。削除アクセス許可は、これらの API には適用されません。
	CAT ISTP REST API	システム使用のみ。 CAT UI/ISTP が機能するには、読み取り/書き込みアクセス許可が必須です。削除アクセス許可は、これらの API には適用されません。
	CAT サービスオーバーレイ API	主にオーバーレイの問題を調査するために使用されます。読み取りアクセス許可のみが適用されます。
	CAT UI API	CAT UI がすべての NSO サービスとリソースを取得できるようにする必須の API。 読み取りアクセス許可を使用すると、すべてのサービス情報を取得して表示できます。書き込みアクセス許可を使用すると、サービス保証情報をコミットできます。削除アクセス許可は、これらの API には適用されません。
	NSO コネクタ API	サービスの再同期、完全な再同期、ログレベルの変更、およびサービスの HA ステータスを返すことができます。 読み取りアクセス許可ではサービスのステータスを確認できますが、他のすべての操作には書き込みアクセス許可が必要です。削除アクセス許可は、これらの API には適用されません。
	OAM サービス API	N/A

カテゴリ	ロール権限	説明
変更自動化	管理 API	ジョブスケジューリングの管理、ログイン情報の上書きの管理、および Playbook 実行のためのユーザーロールの構成を行うための管理制御を提供します。 読み取りアクセス許可ではステータスを確認して情報を取得でき、書き込みアクセス許可では変更を行うことができます。削除アクセス許可は、これらの API には適用されません。
	アプリケーション API	変更自動化タスクを管理できます（たとえば、Playbook 実行のスケジュール、Playbook の実行、Playbook ジョブの更新、Playbook 実行ステータスの確認、Playbook ジョブセットの詳細の確認、サポートされている YANG モジュールの一覧表示など）。 読み取りアクセス許可では、該当する情報を表示できます（たとえば、ジョブステータスの確認、ジョブの詳細の取得など）。一方、書き込みアクセス許可は、Playbook ジョブのスケジューリング/実行に必要です。削除アクセス許可は、これらの API には適用されません。
	プレイブック API	プレイブックを管理できます。 読み取りアクセス許可により、プレイブック、パラメータ、およびポリシー仕様を取得できます。 書き込みアクセス許可により、プレイブックのインポート/エクスポート、および生成が可能になります。 削除アクセス許可により、プレイブックを削除できます。
	Play API	プレイを管理できます。 読み取りアクセス許可ではプレイを取得または表示でき、書き込みアクセス許可ではプレイを作成、更新、またはインポートできます。削除アクセス許可により、プレイを削除できます。

カテゴリ	ロール権限	説明
コレクションインフラ	コレクション API	収集ジョブを管理するための API のアクセス許可。 読み取り/書き込み/削除アクセス許可に基づいて、収集ジョブの表示、新しい収集ジョブ（外部）の作成/更新、または既存の収集ジョブの削除を行うことができます。システム収集ジョブ（Crosswork 消費のために内部で設定されたデータ収集）は、これらのアクセス許可に関係なく変更できません（管理者のみに許可されます）。ただし、読み取りアクセス許可を持つユーザーは、システム収集ジョブを含むすべての収集ジョブの詳細を表示できます。 ほとんどのユーザーにとって、デバイス/センサーパスレベルごとの収集ジョブの詳細（要求とステータス）と実際のデータ収集ステータス/メトリックを表示できるため、読み取り専用のアクセス許可で十分です。
	データ ゲートウェイ マネージャ API	宛先、データゲートウェイ、カスタムパッケージなどでCRUD操作を実行するアクセス許可。 読み取りアクセス許可ではデータを表示でき、書き込みアクセス許可ではデータの追加/更新/削除ができます。
Crosswork 最適化エンジン	OPTIMA 分析 API	Crosswork Optimization Engine で分析を管理できます。 読み取りアクセス許可では履歴データを表示/エクスポートでき、書き込みアクセス許可では Traffic Engineering Dashboard の設定を変更できます。
	最適化エンジン UI API	SR ポリシー、RSVP トンネル、LCM、BWoPT、BWoD、およびプレビューポリシーを管理できます。 読み取りアクセス許可により、展開されたポリシー、設定、ルート、LCM ドメイン構成/データ、サービスオーバーレイデータ、パスクエリ、ダッシュボードメトリックなどを表示できます。 書き込みアクセス許可により、LCM、BWoD、BWoptの設定、ポリシーの展開、CNC/COE管理ポリシーのプレビューなどを行うことができます。 削除アクセス許可により、SR ポリシー、RSVP トンネルの削除、アフィニティマッピングの削除、LCM ドメインの削除を行うことができます。

カテゴリ	ロール権限	説明
Crosswork Optimization Engine v2	最適化エンジン RESTCONF API v2	Crosswork Optimization Engine で RESTCONF インターフェイスのアクセス許可をカスタマイズできます。 読み取りアクセス許可により、L2およびL3トポロジの詳細、およびセグメントルーティングポリシーの詳細を取得できま 書き込みアクセス許可により、ポリシールートのフェッチ、SR ポリシーのプロビジョニング/変更/削除/プレビュー、および LCM 構成の管理を行うことができます。 削除アクセス許可は、これらの API には適用されません。
データゲートウェイのグローバル設定	データ ゲートウェイ グローバル パラメータ API	CDG には特定のパラメータがあり、展開内のすべての CDG でグローバルに変更できます。 読み取りアクセス許可ではデータを表示できますが、データをリセット/更新するには書き込みアクセス許可が必要です。
	Data Gateway グローバルリソースリセット API	グローバルパラメータに対して行われた更新をリセットできます。 読み取りアクセス許可ではデータを表示できますが、書き込みアクセス許可はデータをリセット/更新します。
	Data Gateway グローバルリソース更新 API	グローバルパラメータを更新できます。 読み取りアクセス許可ではデータを表示できますが、書き込みアクセス許可はデータを更新します。
データゲートウェイのトラブルシューティング	データ ゲートウェイ再起動 API	Crosswork Data Gateway（CDG）を再起動します。 書き込みアクセス許可では、CDG を再起動できます。
	データゲートウェイ Showtech API	CDG の showtech ログを生成してダウンロードします 読み取りアクセス許可により showtech を表示でき、書き込みアクセス許可により showtech が生成されます。 書き込みアクセス許可により、showtech を生成できます
Health Insights	Health Insights API	Heath Insights の KPI を管理できます。 書き込みアクセス許可では、すべての KPI、KPI プロファイル、ジョブの詳細、アラートなどを表示できます。 書き込みアクセス許可により、KPI および KPI プロファイルの作成または更新、KPI プロファイルの有効化/無効化、KPI とプレイブックのリンクなどを行うことができます。 削除アクセス許可により、カスタム KPI および KPI プロファイルを削除できます。

カテゴリ	ロール権限	説明
アイコンサーバー	ICON サーバー API	トポロジおよび最適化のユースケースを対象としたインターフェイス/IP データ収集の収集設定を更新できます。
インベントリ	インベントリ API	インベントリ管理ができます。 読み取りアクセス許可により、次のことができます。 • ノードのリスト、ノードのログイン情報、およびデータベース内のノードの数を取得します。 • HA プール、DG 登録、仮想データゲートウェイ、およびインベントリジョブ情報のリストを取得します。 • ポリシー、プロバイダー、およびタグのリストを取得します。 書き込みアクセス許可では、次のことができます。 • 仮想データゲートウェイプールへのデバイスマッピングを更新します。 • 要求されたノードをロック/ロック解除します。 • ノードからタグの関連付けを削除します。部分的な割り当て解除はサポートしていません。 • 一連のデバイスへの入力データを更新します。 • プロバイダーのオンボーディングの API エンドポイントを設定します。 削除アクセス許可により、次のことができます。 • ログイン情報プロファイルとノードの一括削除を実行します。 • 削除操作用の CSV をアップロードします。 • HA プール、データゲートウェイの登録、および仮想データゲートウェイを削除します。 • ポリシー、プロバイダー、およびタグを削除します。

カテゴリ	ロール権限	説明
プラットフォーム	プラットフォーム API	読み取りアクセス許可により、サーバーステータス、クラスタノード情報、アプリケーション ヘルス ステータス、収集ジョブステータス、証明書情報、バックアップおよび復元ジョブステータスなどを取得できます。 書き込みアクセス許可では、次のことができます。 • xFTP サーバーのイネーブル化/ディセーブル化 • クラスタの管理（ログインバナーの設定、マイクロサービスの再起動など） • クラスタリソースの再調整 • ノードの管理（クラスタインベントリのエクスポート、VM の追加、VM 構成の適用、クラスタからの VM の削除など） • 証明書の管理（トラストストアと中間キーストアのエクスポート、証明書の作成または更新、Web サーバーの構成など） • 通常/データのみのバックアップおよび復元操作を実行します。 • アプリケーションの管理（アクティブ化、非アクティブ化、アンインストール、パッケージの追加など） 削除アクセス許可により、VM（ID で識別される）を削除したり、ソフトウェアリポジトリからアプリケーションを削除したりできます。
	分散キャッシュ API	読み取りアクセス許可により、トラブルシューティングのためにキャッシュ統計を取得できます。
	API のグループ化	グループ化管理とトポロジグループの選択ツリー。 読み取りアクセス許可ではトポロジUIを表示でき、書き込みアクセス許可ではグループの作成/更新ができます。グループ管理ページからグループを削除するには、削除アクセス許可が必要です。
	API を見る	トポロジーでのビュー管理。 読み取りアクセス許可ではビューを表示でき、書き込みアクセス許可ではビューを作成/更新でき、削除アクセス許可では削除機能が有効になります。

カテゴリ	ロール権限	説明
トポロジ	地理 API	オフラインマップの地理サービスを提供します。 読み取りアクセス許可はオフラインモードで Geo Map を使用でき、書き込みアクセス許可では Geo Map ファイルをアップロードでき、削除アクセス許可は設定で地図ファイルを削除できます。
	トポロジ API	トポロジページ、設定、またはトポロジ視覚化フレームワークを使用するその他のページを管理できます。 トポロジの視覚化には、読み取りアクセス許可が必須です。書き込みアクセス許可ではトポロジ設定を更新でき、削除アクセス許可ではトポロジリンクがダウンした場合に削除できます。
プロキシ	Crosswork プロキシ API	NSO Restconf NBI の CNC プロキシ API を管理するアクセス許可。 読み取りアクセス許可は NSO REST conf NBI のすべての GET 要求を許可し、書き込みアクセス許可は POST/PUT/PATCH 操作を許可し、削除アクセス許可はすべての削除 API を有効にします。
SWIM	SWIM NB API	SWIM リポジトリにイメージをアップロードし、デバイスに配布してインストールできます。 読み取りアクセス許可を使用すると、SWIM リポジトリからすべてのイメージを一覧表示したり、デバイスからのイメージ情報を表示したり、SWIM ジョブの詳細を確認したりできます。書き込みアクセス許可により、インストール関連のすべての操作をアップロード/配布し、実行することができます。削除アクセス許可により、コピーした画像をデバイスから削除できます。 変更自動化でソフトウェアのインストール/アンインストール Playbook を実行するには、書き込み/削除アクセス許可が必要です。

カテゴリ	ロール権限	説明
Service Health	アーカイバ API	読み取りアクセス許可により、次のことができます。 • 特定のサービスに履歴データが存在するかどうかを確認します。 • 特定のサービスの履歴タイムラインシリーズを取得します。 • 選択したサービスのタイムスタンプのサービスグラフを取得します。 • サービスメトリックデータを取得する 書き込み/削除アクセス許可は、これらの API には適用されません。
	保証グラフマネージャ API	読み取りアクセス許可により、次のことができます。 • サービスの詳細を取得します。 • 影響を受けるサービスのリストを取得します。 • 一致するサブサービス（トランスポートまたはデバイスのみ）のリストを取得します。 書き込み/削除アクセス許可は、これらの API には適用されません。
	ヒューリスティック パッケージ マネージャ API	ヒューリスティック パッケージ管理のアクセス許可と、サービスアシュアランスのプラグインと構成プロファイルを管理するためのアクセス許可。 読み込みアクセス許可により、ヒューリスティック パッケージのエクスポート、ヒューリスティック パッケージの詳細（ルール、プロファイル、サブサービス、メトリクス、プラグイン）のクエリ、および保証オプションのクエリが可能になります。 書き込みアクセス許可により、ヒューリスティック パッケージをインポートし、すべての作成/更新操作を実行できます。 削減アクセス許可により、削除操作を実行できます（たとえば、RuleClass、MetricClass などを削除します）。

カテゴリ	ロール権限	説明
ゼロタッチ プロビジョニング	CW コンフィギュレーション サービス API	読み取りアクセス許可により、次のことができます。 • ZTP 構成リポジトリに保存されているすべての day-0 構成ファイルを一覧表示します。 • ZTP 構成リポジトリに保存されている 0 日目の構成ファイルの数を取得します。 • ZTP 構成リポジトリから day-0 構成ファイルをダウンロードします。 • CW ZTP リポジトリに保存されている Day-0 構成ファイルに関連付けられた情報に基づいて、すべてのデバイスファミリ/デバイスバージョンとデバイスプラットフォームを一覧表示します。 書き込みアクセス許可では、次のことができます。 • 0 日目の構成ファイルまたはスクリプトを ZTP 構成リポジトリにアップロードします。 • ZTP 設定リポジトリに保存されている特定の 0 日目の設定ファイルに関連するメタデータを一覧表示/更新します 削除アクセス許可により、ZTP 構成リポジトリにアップロードされた構成ファイルとスクリプトを削除できます。
	CW イメージ サービス API	読み取りアクセス許可により、次のことができます。 • ZTP イメージリポジトリに保存されているすべてのデバイスイメージファイルを一覧表示します。 • CW ZTP リポジトリに保存されているイメージファイルに関連付けられているすべてのデバイスプラットフォーム/ファミリ名を一覧表示します。 • ID でデバイスイメージファイルをダウンロードします。 書き込みアクセス許可により、ZTP イメージリポジトリに保存されている特定のイメージファイルに関連付けられた関連メタデータを更新できます。 削除アクセス許可により、ZTP イメージリポジトリにアップロードされたイメージファイルを削除できます。
	CW ZTP サービス API	

カテゴリ	ロール権限	説明
		ZTP デバイスとプロファイルを管理できます。Crosswork に追加/更新/削除します。 読み取りアクセス許可により、ZTP デバイス、シリアル番号/OV、プロファイル、サンプルデータ CSV を取得し、ZTP デバイス、プロファイルを一覧表示し、ZTP デバイスとメタデータをエクスポートできます。 削除アクセス許可により、ZTPデバイス、シリアル番号/OV、プロファイルを追加し、ZTP デバイスの属性を追加/更新できます。 削除アクセス許可により、ZTP デバイス、プロファイル、シリアル番号/所有権証明書を削除できます。
CW-CLMS	共通ライセンス管理サービス（CLMS）API	Crosswork でライセンス登録を管理するための API のアクセス許可。 読み取りアクセス許可により、スマートライセンス設定、登録ステータス、およびライセンス使用状況を表示できますが、書き込みアクセス許可は、ライセンスの登録、再登録、登録解除、更新などのスマートライセンス設定を変更するために必要です。

アクティブセッションの管理

管理者は、Cisco Crosswork UI でアクティブなセッションを監視および管理し、次のアクションを実行できます。

- ユーザーセッションの終了
- 監査ログの表示

（注）
- 終了するアクセス許可を持つ管理者以外のユーザーは、自分のセッションを終了できます。
- 読み取りアクセス許可を持つ管理者以外のユーザーは、セッションの監査ログのみを収集できます。
- 読み取りアクセス許可がない管理者以外のユーザーは、[アクティブセッション（Active Sessions）] ウィンドウを表示できません。

ステップ 1 メインメニューから、**[管理（Administration）] > [ユーザーとロール（Users and Roles）] > [アクティブセッション（Active Sessions）]**の順に選択します。

[アクティブセッション（Active Sessions）] タブには、Cisco Crosswork のすべてのアクティブセッションが、ユーザー名、ログイン時間、ログイン方法などの詳細とともに表示されます。

ステップ 2 ユーザーセッションを終了するには、[アクション（Actions）] 列の下の アイコンをクリックし、[セッションの終了（Terminate Session）] を選択します。アクションを確認するためのダイアログボックスが表示されます。[終了（Terminate）] を選択し、セッションを終了します。

（注） セッションを終了するときは注意することをお勧めします。セッションが終了したユーザーは、事前に警告を受け取ることはなく、保存されていない作業は失われます。

ステップ 3 ユーザーの監査ログを表示するには、[アクション（Actions）] 列の下にある アイコンをクリックし、[監査ログ（Audit Log）] を選択します。

選択したユーザー名の [監査ログ（Audit Log）] 画面が表示されます。監査ログの詳細については、「View Audit Log （392 ページ）」を参照してください。

ユーザー認証の設定（TACACS+ と LDAP）

Cisco Crosswork は、ローカルユーザーのサポートに加えて、TACACS+ サーバーと LDAP サーバーとの統合により TACACS+ と LDAP のユーザーをサポートします。統合プロセスには次の手順があります。

- TACACS+ と LDAP サーバーを設定します。
- TACACS+ と LDAP のユーザーが参照するロールを作成します。
- AAA 設定を設定します。

（注）

- AAA サーバーページは、すべてのサーバーが 1 回の要求で更新される一括更新モードで動作します。サーバーの削除に関連するアクセス許可を持つユーザーのみに「リモート認証サーバーの統合 API」の書き込みアクセス許可を付与することをお勧めします。
- 読み取りと書き込みのアクセス許可のみを持つ（「削除」アクセス許可のない）ユーザーは、削除操作が「書き込み」アクセス許可の一部であるため、Cisco Crosswork から AAA サーバーの詳細を削除できます。詳細については、ユーザーロールの作成（337 ページ）を参照してください。
- AAA サーバーに変更を加えるとき（作成/編集/削除）、変更するたびに数分間待つことをお勧めします。十分な間隔を空けて頻繁に AAA を変更すると、外部ログインが失敗する可能性があります。
- Cisco Crosswork は、最大 5 台の外部サーバーの構成をサポートします。

TACACS+ サーバーの管理

Crosswork は、TACACS+ サーバーを使用してユーザーを認証することをサポートしています。

注意 この項の手順に従って操作を行うと、Crosswork のユーザーインターフェイスへのすべての新しいログインに影響することに注意してください。セッションの中断を最小限に抑えるために、すべての TACACS+ の変更を 1 回のセッションで実行し、送信することをお勧めします。

始める前に

Cisco Crosswork と同じものを設定する前に、TACACS+ サーバーで必要なユーザーロールを作成する必要があります。Crosswork を Cisco ISE（Identity Service Engine）などのアプリケーションと統合して、TACACS+ プロトコルを使用して認証することができます。このサービスを利用するには、Cisco ISE で Crosswork をクライアントとして設定する必要があります。詳細については、『Cisco Identity Services Engine Administrator Guide』を参照してください。
https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/admin_guide/b_ISE_admin_3_0/b_ISE_admin_30_device_admin.html

ステップ 1 メインメニューから、**[管理（Administration）]** > **[AAA]** > **[サーバー（Servers）]** > **[TACACS+]** タブを選択します。このウィンドウからは、新し TACACS+ サーバーの追加、設定の編集、および削除を行うことができます。

ステップ 2 **新しい TACACS+ サーバーを追加するには、次の手順を実行します：**

a) ＋アイコンをクリックします。

b) 必要な TACACS+ サーバー情報を入力します。

（注）
- 一意の優先順位値を指定し、認証要求に優先順位を割り当てることができます。
- Crossworkが外部認証サーバーと通信するには、このページで入力する[共有秘密（Shared Secret）]パラメータが、TACACS+サーバーで設定されている共有秘密の値と一致する必要があります。

c) 認証タイプを選択します。
- PAP：パスワードベースの認証は、2つのエンティティが1つのパスワードを事前に共有し、そのパスワードを認証の基準に使用するプロトコルです。
- CHAP：チャレンジハンドシェイク認証プロトコルでは、クライアントとサーバーの両方がプレーンテキストの秘密キーを認識しており、その秘密キーは絶対にネットワーク上に送信されないことが必要になります。CHAPは、パスワード認証プロトコル（PAP）より優れたセキュリティを提供します。

d) 関連するすべての詳細を入力したら、[追加（Add）]をクリックします。

（注） [ポリシーID（Policy ID）]フィールドは、TACACS+サーバーで作成したユーザーロールに対応します。必要なユーザーロールを作成する前にTACACS+ユーザーとしてCisco Crossworkにログインしようとすると、「キーが認証されていません。一致するポリシーがありません（Key not authorized: no matching policy）」というエラーメッセージが表示されます。この場合は、ブラウザを閉じます。ローカル管理者ユーザーとしてログインし、TACACS+サーバーで不足しているユーザーロールを作成し、TACACS+ユーザーログイン情報を使用してCrossworkにログインし直します。

e) [すべての変更を保存（Save All Changes）]をクリックします。変更を更新するためのサーバーの再起動に関する警告メッセージが表示されます。[変更の保存（Save Changes）]をクリックして確認します。

ステップ3 TACACS+ サーバーを編集するには、次の手順を実行します：

a) TACACS+ サーバーの横にあるチェックボックスをクリックし、をクリックします。
b) 変更を加えた後、[更新（Update）]をクリックします。

ステップ4 TACACS+ サーバーを削除するには、次の手順を実行します：

a) TACACS+ サーバーの横にあるチェックボックスをクリックし、  をクリックします。[サーバー IP アドレスの削除（Delete server-IP-address）]ダイアログボックスが開きます。
b) [削除（Delete）]をクリックして確認します。

LDAP サーバーの管理

Lightweight Directory Access Protocol（LDAP）は、ディレクトリ情報にアクセスして管理するために使用されるサーバープロトコルです。Crossworkは、LDAPサーバー（OpenLDAP、Active Directory、およびセキュアLDAP）を使用してユーザーを認証することをサポートしています。

IP ネットワーク経由でディレクトリを管理し、データ転送用の単純な文字列形式を使用して TCP/IP 上で直接実行します。

セキュア LDAP プロトコルを使用するには、LDAP サーバーを追加する前にセキュア LDAP 通信証明書を追加する必要があります。証明書の追加の詳細については、新しい証明書の追加（322 ページ） を参照してください。

注意 この項の手順に従って操作を行うと、Crosswork のユーザーインターフェイスへのすべての新しいログインに影響することに注意してください。セッションの中断を最小限に抑えるために、すべての LDAP サーバーの変更を 1 回のセッションで実行し、送信することをお勧めします。

ステップ 1 メインメニューから、**[管理（Administration）] > [AAA] > [サーバー（Servers）] > [LDAP]** タブを選択します。このウィンドウを使用して、新しい LDAP サーバーの追加、設定の編集、および削除を行うことができます。

ステップ 2 **新しい LDAP サーバーを追加するには、次の手順を実行します：**

a) ＋アイコンをクリックします。

b) 必要な LDAP サーバーの詳細を入力します。

（注）
- TACACS+ サーバーと同様に、一意の優先順位値を指定し、認証要求に優先順位を割り当てることができます。
- セキュア LDAP サーバーを追加するには、[セキュア接続（Secure Connection）] トグルボタンを有効にして、関連するセキュア LDAP 証明書を [証明書（Certificate）] ドロップダウンリストから選択します。
- [ポリシーID（Policy ID）] フィールドは、 LDAP サーバーで作成したユーザーロールに対応します。必要なユーザーロールを作成する前に LDAP ユーザーとして Cisco Crosswork にログインしようとすると、「ログインに失敗しました。ポリシーが見つかりません。ネットワーク管理者にお問い合わせください。」というエラーメッセージが表示されます。このエラーを回避するには、Crosswork で新しい LDAP サーバーを設定する前に、LDAP サーバーで関連するユーザーロールを作成してください。

c) [Add] をクリックします。

d) [すべての変更を保存（Save All Changes）] をクリックします。変更を更新するためのサーバーの再起動に関する警告メッセージが表示されます。[変更の保存（Save Changes）] をクリックして確認します。

ステップ 3 **LDAP サーバーを編集するには、次の手順を実行します：**

a) LDAP サーバーの横にあるチェックボックスをクリックし、✎をクリックします。

b) 変更を加えた後、[更新（Update）] をクリックします。

ステップ 4 **LDAP サーバーを削除するには、次の手順を実行します：**

a) LDAP サーバーの横にあるチェックボックスをクリックし、 をクリックします。
b) [削除（Delete）] をクリックして確認します。

AAA サーバー設定を設定

関連する AAA アクセス許可を持つユーザーは、AAA 設定を設定できます。

ステップ 1 メインメニューから、**[管理（Administration）] > [AAA] > [設定（Settings]** の順に選択します。

ステップ 2 [ローカルへのフォールバック（Fallback to Local）] に関連する設定を選択します。デフォルトでは、Crosswork はローカルデータベース認証よりも外部認証サーバーを優先します。

（注） 管理者ユーザーは常にローカルで認証されます。

ステップ 3 [アイドル状態のユーザをすべてログアウトする間隔（Logout All Idle Users After）] フィールドの関連する値を選択します。 指定された制限を超えてアイドル状態のままになっているユーザーは、自動的にログアウトされます。

（注） デフォルトのタイムアウト値は30分です。タイムアウト値を調整すると、ページが更新されて変更が適用されます。

ステップ 4 [並列セッション数（Number of Parallel Sessions）] に関連する値を入力します。

（注） Crosswork は、同時使用ユーザーに対して 5 ～ 200 の並列セッションセッションをサポートします。並列セッション数を超えると、Crosswork へのログイン時にエラーが表示されます。

ステップ 5 [ローカルパスワードポリシー（Local Password Policy）] に関連する設定を選択します。特定のパスワード設定はデフォルトで有効になっており、無効にすることはできません（たとえば、最初のログイン時にパスワードを変更する）。

（注） パスワードポリシーの変更は、ユーザーが次にパスワードを変更したときにのみ適用されます。ログイン時に、既存のパスワードのコンプライアンスはチェックされません。

（注） [ローカルパスワードポリシー（Local Password Policy）] を使用すると、管理者は、ユーザーが Cisco Crosswork からロックアウトされるまでのログイン試行の失敗回数とロックアウト期間を設定できます。待機時間が経過すると、ユーザーは正しいログイン情報でログインを試行することができます。

セキュリティ強化の概要

セキュリティを強化するには、次のコンポーネントがセキュリティメカニズムを最適化できるように調整する必要があります。

- Cisco Crosswork インフラストラクチャ
- Cisco Crosswork ストレージ システム（ローカルまたは外部）

Cisco Crosswork セキュリティを強化するには、次のタスクを実行する必要があります。

- 非セキュア ポートと未使用ポートのシャットダウン
- ネットワーク ファイアウォールの設定
- 必要に応じた Cisco Crosswork インフラストラクチャの強化

主な情報源として、シスコの担当者が各展開環境に固有のサーバー強化ガイダンスをご提供しますが、この項に示す手順に従って Cisco Crosswork を保護することもできます。

認証スロットリング

Cisco Crosswork は、パスワードの推測やその他の関連する不正使用のシナリオを回避するために、ログイン試行の失敗後にログイン試行を抑制します。ユーザー名のログイン試行が失敗すると、そのユーザー名のすべての認証試行が 3 秒間ブロックされます。スロットリングは、TACACS、LDAP、デフォルトのローカル認証など、サポートされているすべての認証方式に適用できます。

主要なセキュリティ概念

Cisco Crosswork 製品のセキュリティの最適化を目指す管理者は、次のセキュリティ概念をよく理解しておく必要があります。

HTTPS

Hypertext Transfer Protocol Secure（HTTPS）では、チャネルを介して送信されるデータの暗号化に、セキュア ソケット レイヤ（SSL） またはその後続の標準規格である Transport Layer Security（TLS）が使用されます。SSL で複数の脆弱性が見つかったため、Cisco Crosswork では現在 TLS のみがサポートされています。

（注） TLS は大まかに SSL と呼ばれることが多いため、本ガイドでもこの表記に従います。

SSL は、プライバシー、認証、およびデータ整合性を組み合わせることで、クライアントとサーバーの間のデータ転送を保護します。これらのセキュリティメカニズムを有効にするために、SSL は証明書、秘密キー/公開キー交換ペア、および Diffie-Hellman 鍵共有パラメータを使用します。

X.509 証明書

X.509 証明書と秘密キー/公開キーの ペアは、ユーザー認証と通信パートナーのアイデンティティ検証に使用されるデジタル識別の一種です。VeriSign や Thawte などの認証局（CA）は、

エンティティ（サーバーまたはクライアント）を識別するための証明書を発行します。クライアントまたはサーバー証明書には、発行認証局の名前とデジタル署名、シリアル番号、証明書が発行されたクライアントまたはサーバーの名前、公開キー、および証明書の有効期限が含まれます。CA は、1 つ以上の署名証明書を使用して SSL 証明書を作成します。各署名証明書には、CA 署名の作成に使用される照合秘密キーがあります。CA は署名付き証明書（公開キーが埋め込まている）を簡単に入手できるようにしているため、誰でもその証明書を使用して、SSL 証明書が実際に特定の CA によって署名されたことを確認できます。

一般に、ハイ アベイラビリティ（HA）と非 HA の両方の環境で証明書を設定するには、次の手順が必要です。

1. サーバーの ID 証明書を生成する。
2. サーバーに ID 証明書をインストールする。
3. 対応するルート証明書をクライアントまたはブラウザにインストールする。

実行する必要がある具体的なタスクは、ご利用の環境によって異なります。

次の点に注意してください。

- サーバーの開始/停止シーケンシングは、HA 環境で慎重に行う必要があります。
- 仮想 IP アドレスが設定されている非 HA 環境では、より複雑な証明書要求プロセスを完了する必要があります。

1 方向 SSL 認証

これは、クライアントが適切なサーバー（中間サーバーではなく）に接続していることを保証する必要がある場合に使用される認証方法で、オンライン バンキングの Web サイトなどのパブリック リソースに適しています。認証は、クライアントがサーバー上のリソースへのアクセスを要求したときに開始されます。リソースが存在するサーバーは、そのアイデンティティを証明するために、サーバー証明書（別名 SSL 証明書または x.509 証明書）をクライアントに送信します。クライアントは受信したサーバー証明書を、クライアントまたはブラウザにインストールする必要がある別の信頼できるオブジェクト（サーバー ルート証明書）と照合して検証します。サーバーの検証後、暗号化された（つまりセキュアな）通信チャネルが確立されます。ここで、Cisco Crosswork サーバーによって HTML 形式の有効なユーザー名とパスワードの入力が求められます。SSL 接続が確立された後にユーザー クレデンシャルを入力すると、未認証の第三者による傍受を防ぐことができます。最終的に、ユーザー名とパスワードが受け入れられた後、サーバー上に存在するリソースへのアクセスが許可されます。

（注） クライアントは複数のサーバーとやり取りするために、複数のサーバー証明書を格納する必要がある場合があります。

クライアントにルート証明書をインストールする必要があるかどうかを判断するには、ブラウザの URL フィールドでロック アイコンを探します。通常このアイコンが表示される場合は、必要なルート証明書がすでにインストール済みであることを示します。多くの場合、これはより大きいいずれかの認証局（CA）によって署名されたサーバー証明書に該当します。一般的なブラウザではこれらの CA からのルート証明書が含まれているからです。

クライアントがサーバー証明書に署名した CA を認識しない場合は、接続がセキュリティで保護されていないことを意味します。これは必ずしも大きな問題ではなく、接続するサーバーの ID が検証されていないことを示しているだけです。この時点で、次の 2 つの操作のいずれかを実行できます。1 つは必要なルート証明書をクライアントまたはブラウザにインストールできます。ブラウザの URL フィールドにロック アイコンが表示された場合は、証明書が正常にインストールされたことを意味します。もう 1 つは、クライアントに自己署名証明書をインストールできることです。信頼できる CA によって署名されたルート証明書とは異なり、自己署名証明書は作成者である個人またはエンティティによって署名されます。自己署名証明書を使用して暗号化チャネルを作成できますが、接続するサーバーの ID が検証されていないため、固有のリスクが伴うことを理解しておいてください。

非セキュアなポートおよびサービスの無効化

一般的なポリシーとして、不要なポートを無効にする必要があります。まず、どのポートが有効になっているかを確認した後、Cisco Crosswork の通常の機能を妨げることなく安全に無効化できるポートを判別する必要があります。これを行うには、開いているポートのリストを表示し、Cisco Crosswork で必要なポートのリストと比較します。

開いているすべてのリスニングポートのリストを表示するには、次の手順を実行します。

ステップ 1 Linux CLI 管理者ユーザーとしてログインし、**netstat -aln** コマンドを入力します。
netstat -aln コマンドは、現在開いている（有効化されている）サーバーの TCP/UDP ポート、システムで使用している他のサービスのステータス、およびその他のセキュリティ関連の設定情報を表示します。このコマンドは、次のような出力を返します。

```
[root@vm ~]# netstat -aln
Active Internet connections (servers and established)
Proto  Recv-Q   Send-Q   Local Address            Foreign Address         State
```

```
tcp    0      0      0.0.0.0:111             0.0.0.0:*               LISTEN
tcp    0      0      127.0.0.1:8080          0.0.0.0:*               LISTEN
tcp    0      0      0.0.0.0:22              0.0.0.0:*               LISTEN
tcp    0      0      127.0.0.1:25            0.0.0.0:*               LISTEN
tcp    0      0      127.0.0.1:10248         0.0.0.0:*               LISTEN
tcp    0      0      127.0.0.1:10249         0.0.0.0:*               LISTEN
tcp    0      0      192.168.125.114:40764   192.168.125.114:2379    ESTABLISHED
tcp    0      0      192.168.125.114:48714   192.168.125.114:10250   CLOSE_WAIT
tcp    0      0      192.168.125.114:40798   192.168.125.114:2379    ESTABLISHED
tcp    0      0      127.0.0.1:33392         127.0.0.1:8080          TIME_WAIT
tcp    0      0      192.168.125.114:40814   192.168.125.114:2379    ESTABLISHED
tcp    0      0      192.168.125.114:40780   192.168.125.114:2379    ESTABLISHED
tcp    0      0      127.0.0.1:8080          127.0.0.1:44276         ESTABLISHED
tcp    0      0      192.168.125.114:40836   192.168.125.114:2379    ESTABLISHED
tcp    0      0      192.168.125.114:40768   192.168.125.114:2379    ESTABLISHED
tcp    0      0      127.0.0.1:59434         127.0.0.1:8080          ESTABLISHED
tcp    0      0      192.168.125.114:40818   192.168.125.114:2379    ESTABLISHED
tcp    0      0      192.168.125.114:22      192.168.125.1:45837     ESTABLISHED
tcp    0      0      127.0.0.1:8080          127.0.0.1:48174         ESTABLISHED
tcp    0      0      127.0.0.1:49150         127.0.0.1:8080          ESTABLISHED
tcp    0      0      192.168.125.114:40816   192.168.125.114:2379    ESTABLISHED
tcp    0      0      192.168.125.114:55444   192.168.125.114:2379    ESTABLISHED
```

ステップ 2 ※ Cisco Crosswork で使用されているポートのテーブルを確認し、ポートがそのテーブルにリストされているかどうかを確認します。この表を参考にすると、どのサービスがポートを使用しているか、およびどのサービスが不要で、安全に無効化できるかを判別できます。この場合の「安全」とは、製品に悪影響を及ぼさずにポートを安全に無効化できることを意味します。

（注） ポートまたはサービスを無効化する必要があるかどうかが不明の場合は、Cisco の担当者にお問い合わせください。

ステップ 3 ネットワーク内にファイアウォールがある場合、Cisco Crosswork の動作に必要なトラフィックのみを許可するようにファイアウォールを設定します。

ストレージの強化

データベース、バックアップ サーバーなど、Cisco Crosswork のインストールに含めるすべてのストレージ要素を保護することをお勧めします。

- 外部ストレージを使用している場合は、ストレージのベンダーとシスコの担当者にお問い合わせください。
- 内部ストレージを使用している場合は、シスコの担当者にお問い合わせください。
- Cisco Crosswork をアンインストールまたは削除する場合は、センシティブ データを含む可能性があるすべての VM 関連ファイルがデジタルで破棄（単に削除されるのではなく）されていることを確認してください。詳細については、シスコの担当者にお問い合わせください。

システム設定の構成

管理者ユーザーは、次のシステム設定を構成できます。

Syslog サーバーの設定

Crosswork では、外部 syslog コンシューマは次を行うことができます。

- Crosswork に登録し、システムイベントを syslog として受信する。
- syslog として転送するイベントの種類をコンシューマごとに定義およびフィルタ処理する。
- syslog がコンシューマに転送されるレートを定義する。

（注） Syslog TLS サーバー証明書が追加されたら、5 分から 10 分待ってから、syslog サーバーを構成します。

始める前に

Syslog TLS サーバー証明書をアップロードしたことを確認してください。詳細については、新しい証明書の追加 （322 ページ）を参照してください。

ステップ 1 メインメニューから、**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** タブを選択します。

ステップ 2 [サーバー（Server）] で、[Syslog 設定（Syslog Configuration）] オプションをクリックします。

ステップ 3 ＋ をクリックします。

ステップ 4 Syslog 設定の詳細を入力します。詳細については、各オプションの横にある ⓘ をクリックしてください。

[条件（Criteria）] オプションを使用して、syslog として転送するイベントの種類と範囲を定義します。例：**(EventSeverity<2 or EventSeverity>=5) and OriginAppId=capp-infra and EventCategory=1**

この式では、イベントがインフラストラクチャ プラットフォームから発信され、カテゴリがシステムで、シビラティ（重大度）が 2 未満または 5 以上の場合にのみイベントが syslog として送信されます。

注意 式は自由形式であり、検証されません。

ステップ 5 [保存（Save）] をクリックします。

トラップサーバーを設定

[設定（Settings）] ウィンドウからトラップサーバーを管理するには、以下の手順に従います。

ステップ 1 メインメニューから、**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** タブを選択します。

ステップ 2 [サーバー（Server）] で、[サーバーのトラップ（Trap servers）] オプションをクリックします。

ステップ 3 ＋ をクリックします。

ステップ 4 トラップサーバーの詳細を入力します。詳細については、各オプションの横にある ⓘ をクリックしてください。

[条件（Criteria）] オプションを使用して、トラップとして転送するイベントの種類と範囲を定義します。

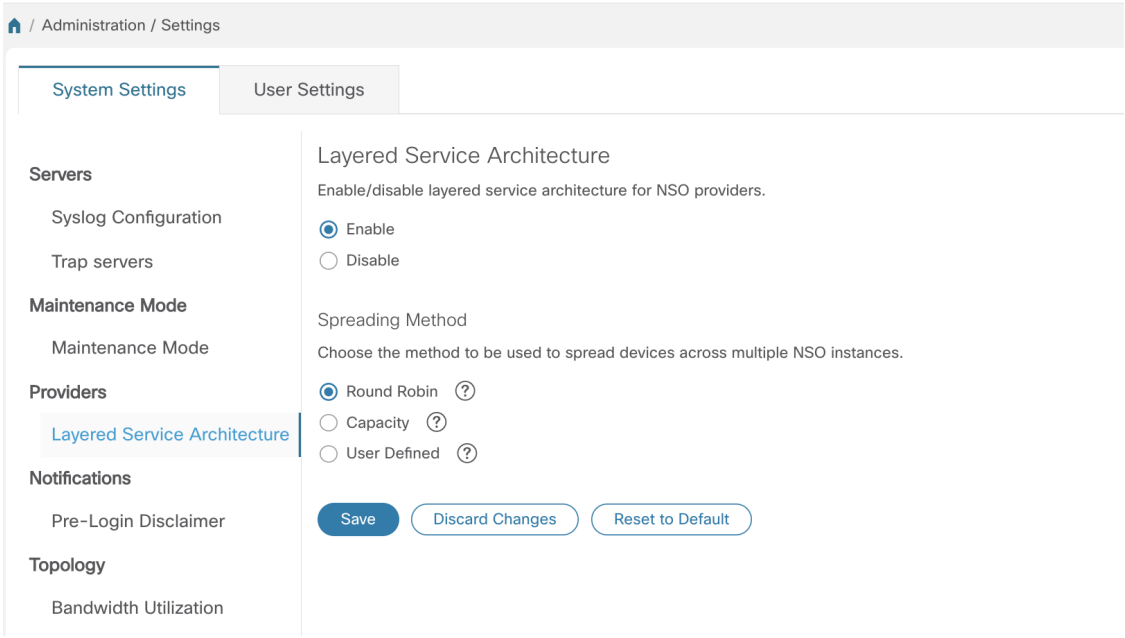
イベントの発生に使用される属性の詳細については、[イベントとアラームの例（Events and Alarms examples）] をクリックしてください。

ステップ 5 関連するすべての情報を入力したら、[追加（Add）] をクリックします。

階層化されたサービスアーキテクチャ（LSA）を有効にする

この手順は、Cisco NSO LSA 展開を選択して、メモリとプロビジョニング スループットを向上させるために任意の多くのデバイスノードを追加することを選択した場合にのみ適用されます。

ステップ 1 メインメニューから、**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [階層化されたサービスアーキテクチャ（Layered Service Architecture）]** を選択します。



ステップ 2 [有効（Enable）] を選択します。

ステップ 3 複数の NSO インスタンスにデバイスを分散する方法を選択します。

- [ラウンドロビン（Round Robin）]：デバイスを周期的に RFS ノードに均等に配布します（たとえば、デバイス 1 から RFS1、デバイス 2 から RFS2 など）。
- [容量（Capacity）]：デバイスの数は、その合計容量に基づいて各 RFS インスタンスに割り当てられます。
- [ユーザー定義（User Defined）]：デバイスは、デバイス設定でデバイスに指定された NSO プロバイダーに割り当てられます。詳細については、UI を使用したデバイスの追加 （192 ページ）を参照してください。

ステップ 4 [保存（Save）] をクリックします。

（注） 設定を保存すると、すべての NSO プロバイダーを削除せずに設定を無効にすることはできません。

ログイン前の免責事項の設定

多くの組織では、ユーザーがログインする前に、システムが免責事項メッセージをバナーに表示することを求めています。システムを使用する際に承認済みのユーザーには義務をバナーで通知したり、未承認のユーザーには警告をバナーに表示することがあります。Crosswork ユーザーに対してこのようなバナーを有効にし、必要に応じて免責事項メッセージをカスタマイズできます。

ステップ 1 メインメニューから、**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** タブを選択します。

ステップ 2 [通知（Notifications）] で、[ログイン前の免責事項（Pre-Login Disclaimer）] オプションをクリックします。

ステップ 3 免責事項を有効にし、バナーをカスタマイズするには、次の手順を実行します。

a) [有効（Enabled）] チェックボックスをオンにします。

b) 必要に応じて、バナーの [タイトル（Title）]、[アイコン（Icon）]、および [免責事項のテキスト（Disclaimer Text）] をカスタマイズします。

c) オプション：免責事項の編集中に、次のことを実行できます。

[プレビュー（Preview）] をクリックすると、Crosswork ログインプロンプトの前に表示される変更を確認できます。

[変更の破棄（Discard Changes）] をクリックすると、最後に保存したバージョンのバナーに戻ります。

[リセット（Reset）] をクリックすると、バナーが元のデフォルトのバージョンに戻ります。

d) 変更が完了したら、[保存（Save）] をクリックして変更を保存し、すべてのユーザーにカスタム免責事項を表示できるようにします。

ステップ 4 免責事項の表示をオフにするには、**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [ログイン前の免責事項（Pre-Login Disclaimer）]** を選択し、[有効（Enabled）] チェックボックスをオフにします。

ファイルサーバー設定の管理

Cisco Crosswork は、セキュアなファイル転送サービスを必要とする Crosswork アプリケーションにそれらのサービス（FTP と SFTP）を提供します。デフォルトでは無効です。

（注） この機能は現在、EPNM アプリケーションでのみサポートされています。有効化のシナリオの詳細については、EPNM のユーザーマニュアルを参照してください。

ステップ 1 FTP サーバーを有効化するには、次の手順を実行します。

a) メインメニューから、**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [ファイルサーバー（File Servers）]** を選択します。

b) [FTP] で、[有効化（Enable）] オプションボタンを選択します。

c) [保存（Save）] をクリックして設定を保存します。

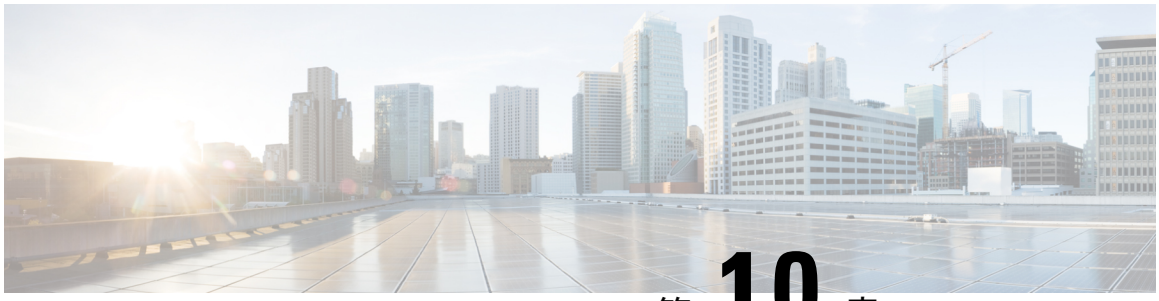
ステップ 2 SFTP サーバーを有効にするには、次の手順を実行します。

a) メインメニューから、**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [ファイルサーバー（File Servers）]** を選択します。

b) [サーバーアップロードの有効化（Enable Server Upload）] スライダを [オン（On）] の位置にドラッグします。

注意 SFTP は、外部から Cisco Crosswork ストレージへの書き込みアクセスを許可するアップロードオプションをサポートしています。アップロードを有効にする際は注意が必要です。また、不要になったらすぐに無効にする必要があります。

c) [保存（Save）] をクリックして設定を保存します。



第 10 章

システム正常性の管理

ここでは、次の内容について説明します。

システムとアプリケーションの正常性のモニター

Crosswork プラットフォームは、マイクロサービスで構成されるアーキテクチャ上に構築されます。これらのマイクロサービスの性質上、Crosswork システム内のさまざまなサービスには依存関係があります。すべてのサービスが稼働している場合、システムとアプリケーションは正常と見なされます。1 つ以上のサービスがダウンしている場合、正常性は [Degraded（低下）] と見なされます。すべてのサービスがダウンしている場合、正常性のステータスは [ダウン（Down）] です。

メインメニューから [Crosswork Manager] を選択して、[Crosswork の概要（Crosswork Summary）] ウィンドウと [Crosswork の正常性（Crosswork Health）] ウィンドウにアクセスします。各ウィンドウには、システムとアプリケーションの正常性をモニターするためのさまざまなビューがあります。また、このウィンドウには、Cisco Crosswork クラスタ、プラットフォーム インフラストラクチャ、およびインストールされているアプリケーションの問題を特定、診断、および修正するために使用できるツールと情報が、シスコ カスタマー エクスペリエンス アカウント チームからのサポートとガイダンスとともに表示されます。

両方のウィンドウで同じタイプの情報にアクセスできますが、各サマリーとビューの目的は異なります。

クラスタの正常性のモニター

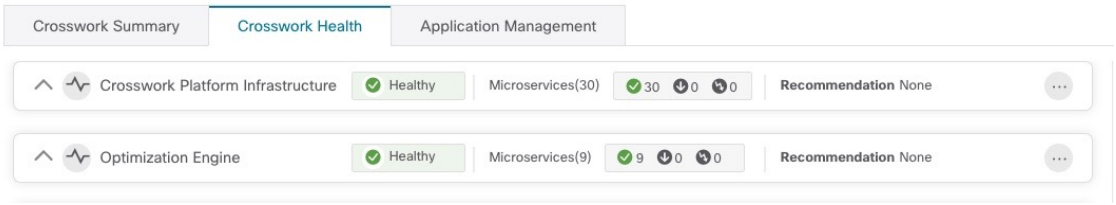
[Crosswork の概要（Crosswork Summary）] ウィンドウ（**[Crosswork Manager]** > **[Crosswork の概要（Crosswork Summary）]**）には、システム全体の正常性の概要が表示されます。[Crosswork の概要（Crosswork Summary）] ウィンドウの主な目的は、ハードウェアリソースと VM の観点から Crosswork クラスタの正常性を表示することです。たとえば、アプリケーションをインストールまたはアップグレードする前に、ハードウェアリソースが正常であり、VM が正常に動

作しているかどうかを確認できます。[Crosswork クラスタ（Crosswork Cluster）] タイルをクリックすると、リソース使用率を視覚的に確認し、VM をドリルダウンして、VM またはクラスタ関連のアクティビティを実行できます。また、サービスが低下したり、ハードウェアリソースが過剰に使用されたりすることもあります。その時点で、ハードウェアの観点から、システム内の VM の数が不足していることがわかり、システムを拡張するためにさらに VM を追加するように求められることがあります。詳細については、「クラスタの正常性の確認 （8 ページ）」を参照してください。

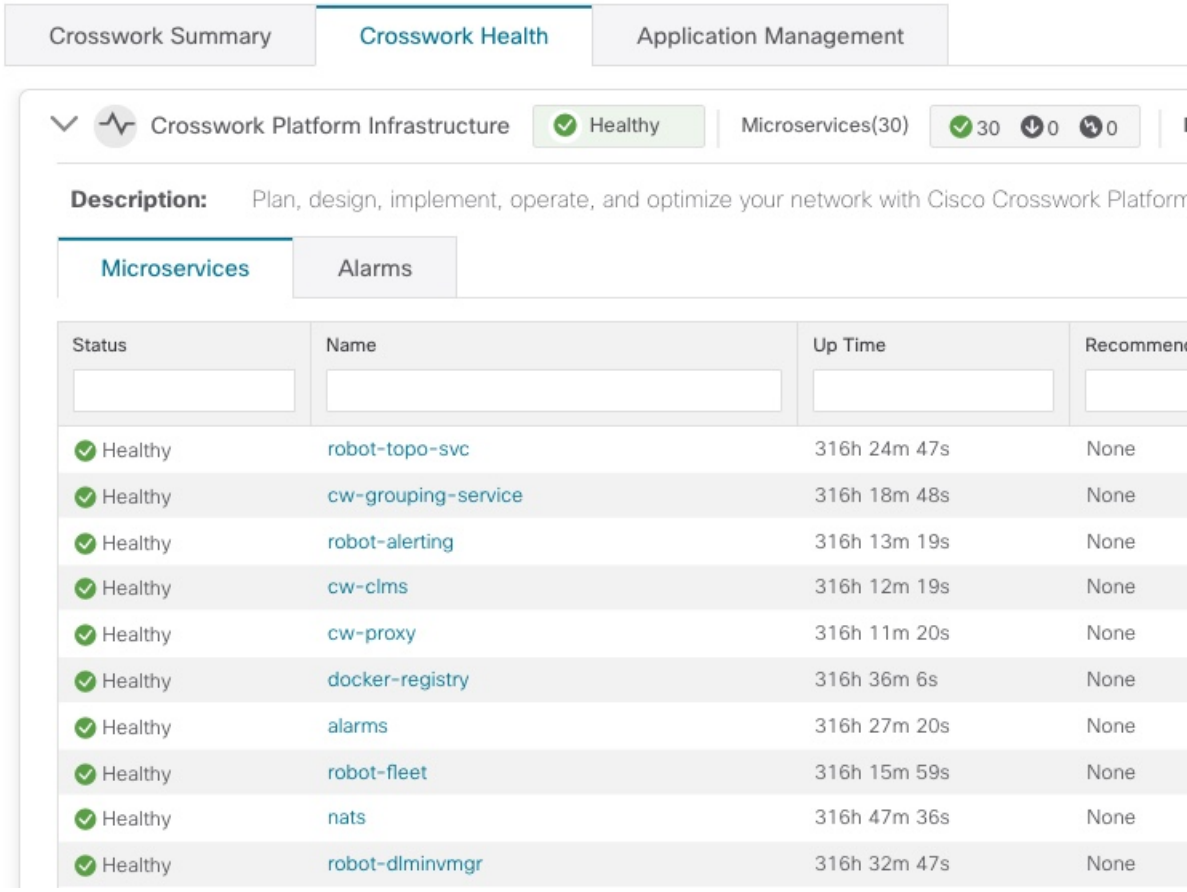
Crosswork クラスタの正常性を表示するだけでなく、[Cisco Crosswork プラットフォーム インフラストラクチャ（Cisco Crosswork Platform Infrastructure）] タイルとアプリケーションタイルをクリックして、マイクロサービスやアラームなどの詳細を表示することもできます。

プラットフォームインフラストラクチャとアプリケーション正常性のモニター

[Crosswork の正常性（Crosswork Health）] ウィンドウ（**[Crosswork Manager]** > **[Crosswork の正常性（Crosswork Health）]** タブ）には、Cisco Crosswork プラットフォーム インフラストラクチャとインストールされているアプリケーションの正常性の概要と、マイクロサービスステータスの詳細が表示されます。



このウィンドウ内で、アプリケーションの行を展開して、マイクロサービスとアラームの情報を表示します。



[マイクロサービス（Microservices）] タブで、次の手順を実行します。

- マイクロサービス名をクリックして、マイクロサービスのリストと、該当する場合は関連付けられているマイクロサービスのリストを表示します。
- ⋯ をクリックして再起動するか、マイクロサービスごとに Showtech データとログを取得します。

（注） Showtech ログは、アプリケーションごとに個別に収集する必要があります。

[アラーム（Alarms）] タブから、次の手順を実行します。

- アラームの詳細をドリルダウンするには、アラームの説明をクリックします。
- 確認し、ステータスを変更し、アラームにメモを追加します。

また、Cisco Crosswork アプリケーションまたは Cisco Crosswork Platform Showtech サービスログをすべてダウンロードし、[アプリケーションの詳細（Application Details）] ウィンドウから

インストール関連の操作を実行することもできます。 をクリックして、[アプリケーションの詳細（Application Details）] ウィンドウを開きます。

システム機能をリアルタイムで視覚的にモニター

[Crosswork Manager] ウィンドウからアクセスできる一連のモニタリングダッシュボードを使用すると、Cisco Crosswork の正常性とその機能をリアルタイムでモニターできます。

Cisco Crosswork は Grafana を使用してこれらのダッシュボードを作成します。データベースで収集されたメトリックを使用して、製品のインフラストラクチャをグラフィカルに表示します。これらのダッシュボードを使用して、個々の Cisco Crosswork アプリケーションまたはその基盤となっているサービスで発生する可能性がある問題を診断できます。

複数のモニターダッシュボードがあり、モニターする機能のタイプとそれらが提供するメトリックによって分類されます。次の表に、インストールされている Cisco Crosswork アプリケーションに応じて使用可能なカテゴリを示します。

表 *27*：モニタリング ダッシュボードのカテゴリ

このダッシュボードカテゴリ...	モニターの対象
Change Automation	プレイブックの機能。メトリックには、実行された MOP ジョブの数、応答遅延、API コール、データベースアクティビティなどが含まれます。
Optima	機能パック、トラフィック、および SR-PCE ディスパッチャ機能。
収集 - マネージャ（Collection - Manager）	デバイスデータ収集機能。メトリックには、テレメトリ収集遅延、収集操作合計、テレメトリに関連するメモリおよびデータベースアクティビティ、遅延収集などが含まれます。
Health Insights	重要業績評価指標。メトリックには、KPI アラート、API コールなどの数が含まれます。
Infra	システムインフラストラクチャメッセージングとデータベースアクティビティ。
インベントリ（Inventory）	インベントリマネージャ機能。これらのメトリックには、インベントリ変更アクティビティの合計数が含まれます。
プラットフォーム（Platform）	システムハードウェアおよび通信の使用状況とパフォーマンス。メトリックには、ディスクと CPU の使用率、データベースサイズ、ネットワークとディスクの動作、およびクライアント/サーバー通信が含まれます。
ZTP	ゼロタッチプロビジョニング機能。

ディスク容量を節約するために、Cisco Crosswork は最大 24 時間の収集されたメトリックデータを保持します。

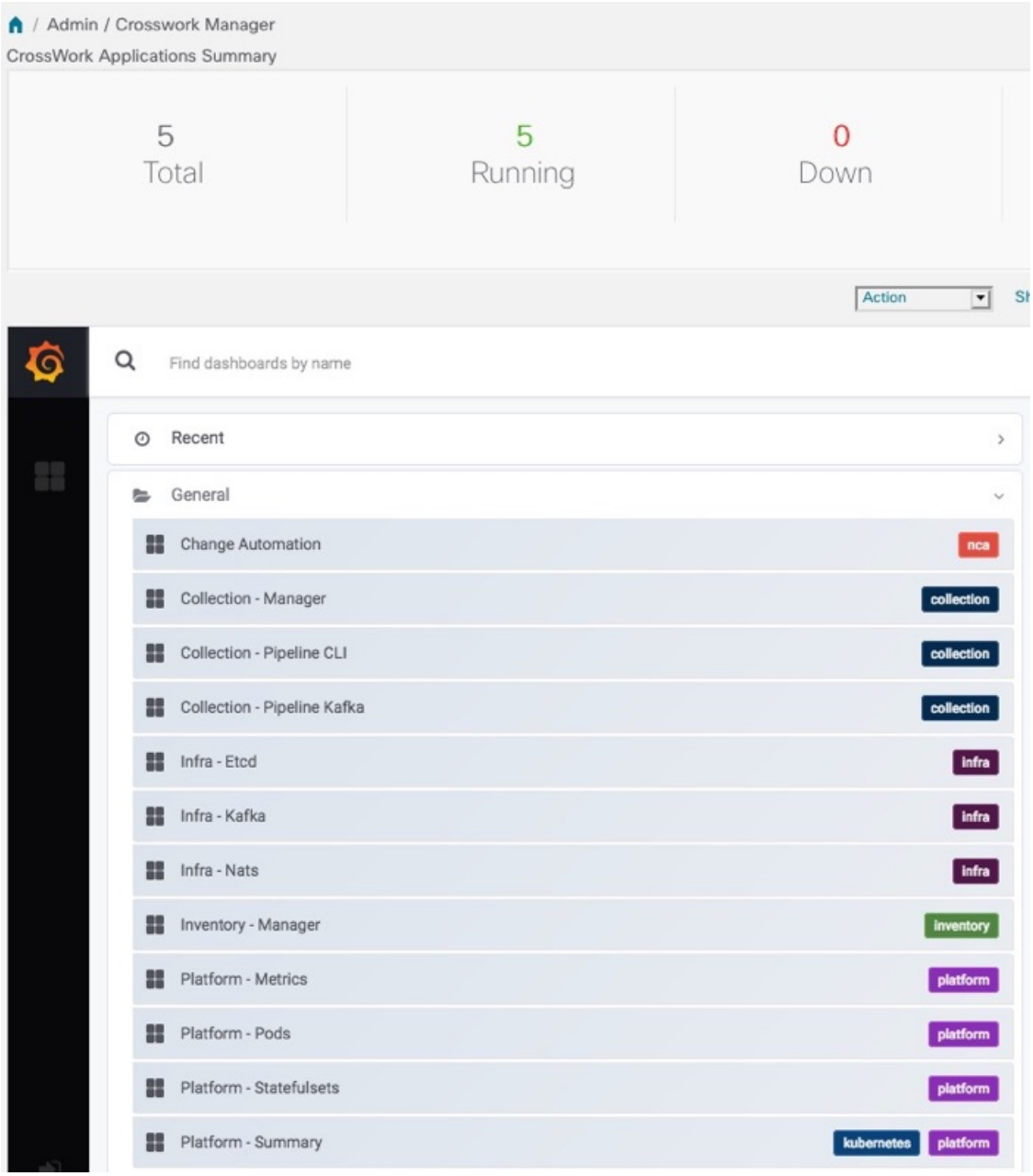
Grafana は、オープンソースの可視化ツールです。次に、Grafana の Cisco Crosswork 実装の使用方法に関する一般的な情報を示します。Grafana 自体の詳細については、https://grafana.com と http://docs.grafana.org を参照してください

ステップ 1 メインメニューから、**[管理（Administration）]** > **[Crosswork Manager]** > **[Crosswork クラスタ（Crosswork Cluster）]** を選択します。

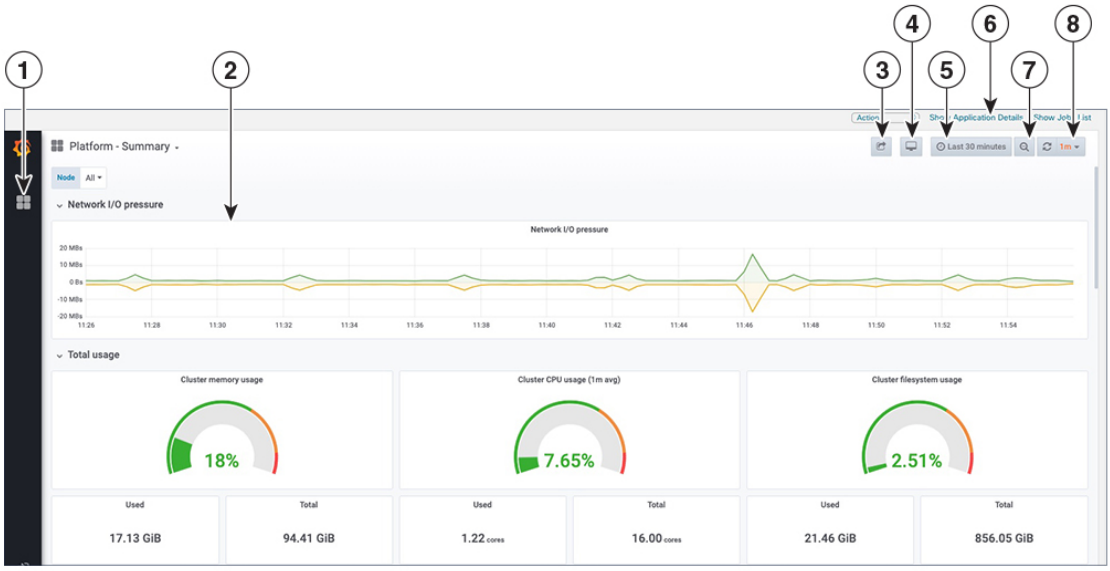
ステップ 2 右上にある [その他の可視化の表示（View more Visualizations）] をクリックします。

Grafana のユーザーインターフェイスが表示されます。

ステップ 3 Grafana のユーザーインターフェイスで、[ホーム（Home）] をクリックします。Grafana には、次の例に示すように、モニタリングダッシュボードとそのカテゴリのリストが表示されます。



ステップ 4 表示するダッシュボードをクリックします。たとえば、[プラットフォーム：概要（Platform - Summary）] ダッシュボードをクリックすると、次の図のいずれかのようなビューが表示されます。



ステップ 5 必要に応じてダッシュボードをスクロールし、ダッシュボードが提供するすべてのメトリックを表示するか、または次の表に示す機能のいずれかを選択します。

項目	説明
1	[ダッシュボード（Dashboard）] アイコン：アイコンをクリックしてダッシュボードリストを再表示し、別のダッシュボードを選択します。
2	[時系列グラフのズーム（Time Series Graph Zoom）]：次のように、時系列データのグラフ内の特定の期間を拡大できます。 **1.** グラフの線で期間の開始点をクリックし、マウスを押したままにします。 **2.** カーソルを終了点にドラッグします。選択しているブロックにライトグレーの網掛けが表示されます。終了点に到達したら、マウスを離します。 ズームした時系列グラフをデフォルトにリセットするには、[ズームアウト（Zoom Out）] アイコンをクリックします。

項目	説明
3	[ダッシュボードの共有（Share Dashboard）]アイコン：表示されているダッシュボードを他のユーザーと共有できるようにするには、このアイコンをクリックします。このアイコンをクリックすると、次のいずれかの必要な形式でダッシュボードを共有するためのタブとオプションを含むポップアップウィンドウが表示されます。 • **URL リンク**：[リンク（Link）] タブをクリックし、[コピー（Copy）] をクリックして、ダッシュボードの URL をクリップボードにコピーします。現在の時刻とテンプレートの設定を URL とともに保持するかどうかも選択できます。 • **ローカル スナップショット ファイル**：[スナップショット（Snapshot）] タブをクリックし、[ローカルスナップショット（Local Snapshot）] をクリックします。Grafana は、サーバー上にダッシュボードのローカルスナップショットを作成します。スナップショットの準備が整ったら、[リンクのコピー（Copy Link）] をクリックして、スナップショットの URL をクリップボードにコピーします。 • **JSON ファイルへのエクスポート**：[エクスポート（Export）] タブをクリックし、[ファイルに保存（Save to file）] をクリックします。エクスポートされた JSON ファイルを保存するか、開くかを尋ねられます。[ファイルに保存（Save to file）] をクリックする前に、[外部で共有するためにエクスポート（Export for Sharing for Externally）] チェックボックスをオンにして、ファイル内のデータソース名をテンプレートにすることもできます。 • **JSON ファイルの表示とクリップボードにコピー**：[エクスポート（Export）] タブをクリックし、[JSON の表示（View JSON）] をクリックします（[JSON の表示（View JSON）] をクリックする前に、[外部で共有するためにエクスポート（Export for sharing externally）] チェックボックスをオンにしてデータソース名をテンプレート化できます）。Grafana は、エクスポートされた JSON コードをポップアップウィンドウに表示します。[クリップボードにコピー（Copy to Clipboard）] をクリックし、クリップボードにファイルをコピーします。
4	[ビューモードのサイクル（Cycle View Mode）] アイコン：デフォルトの Grafana **TV** ビューモードと [キオスク（Kiosk）] モードを切り替えるには、このアイコンをクリックします。[キオスク（Kiosk）] ビューでは、Grafana メニューのほとんどが非表示になります。[キオスク（Kiosk）] ビューを終了するには、[**Esc**] キーを押します。

項目	説明
5	[時間/更新セレクタ（Time/Refresh Selector）]：ダッシュボードに表示されるメトリックの期間と、メトリックが更新される頻度を示します。セレクタをクリックして、別の時間範囲と更新レートを選択します。 時間範囲の開始点と終了点のカスタムペアを指定することも、[今日まで（Today so far）] または [過去 3 時間（Last three hours）] など、いくつかの定義済み範囲のいずれかを選択することもできます。 [オフ（Off）] から [2 日（2 Days）] までの事前定義された更新レートを選択できます。 変更を終えたら、[適用（Apply）] をクリックします。 選択する際は、24 時間分のデータのみが保存されることを覚えておいてください。時間範囲を選択するか、その制限を超える更新レートを選択すると、ダッシュボードが空白になることがあります。
6	[ズームアウト（Zoom Out）] アイコン：このアイコンをクリックすると、ズームした時系列グラフがズーム前の状態にリセットされます。
7	[更新（Refresh）] アイコン：表示されるデータをすぐに更新するか、または更新する時間間隔を選択します。

システム正常性の確認の例

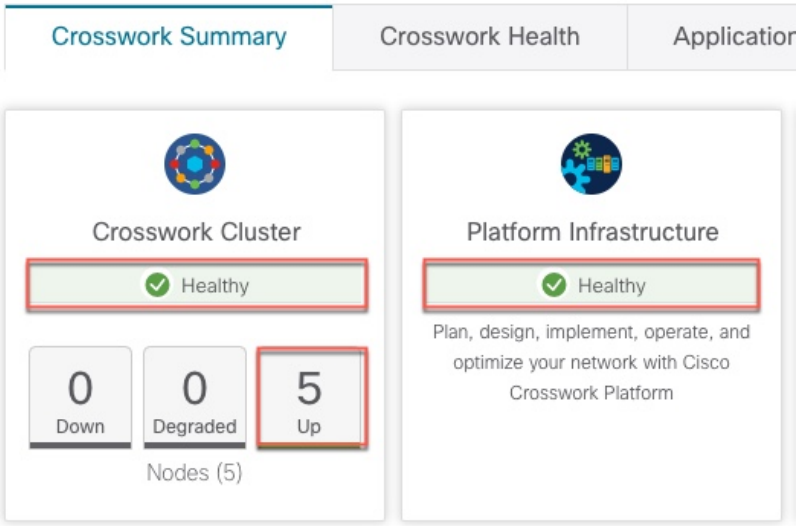
この例では、さまざまなウィンドウや、正常な Crosswork システムで確認すべき領域を検討します。

ステップ 1 システム全体の正常性を確認します。

a) メインメニューから、**[管理（Administration）]** > **[Crosswork Manager]** > **[Crosswork の概要（Crosswork Summary）]** タブを選択します。

b) すべてのノードが動作状態（[アップ（Up）]）であり、Crosswork クラスタとプラットフォーム インフラストラクチャが正常であることを確認します。

図 *65 : [Crosswork* の概要（*Crosswork Summary*）*]*

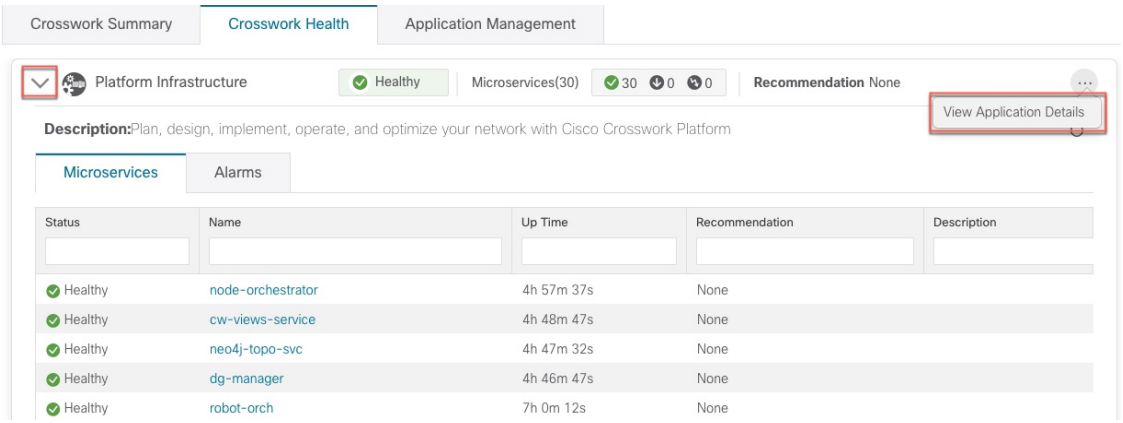


ステップ 2 Crosswork プラットフォーム インフラストラクチャの一部として実行されているマイクロサービスに関する詳細情報を確認および表示します。

a) [Crosswork の正常性（Crosswork Health）] タブをクリックします。

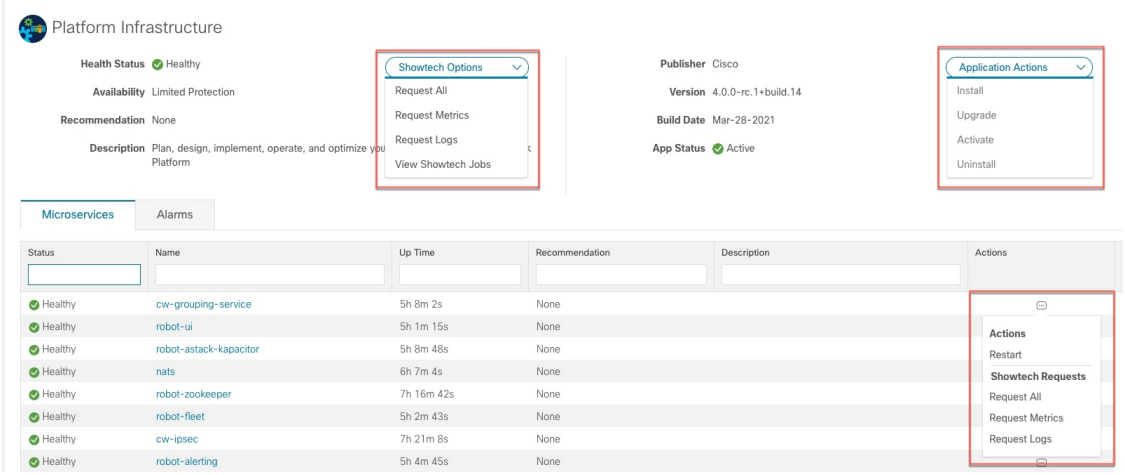
b) [Crosswork プラットフォーム インフラストラクチャ（Crosswork Platform Infrastructure）] の行を展開し、⋯ をクリックして [アプリケーションの詳細（Application Details）] を選択します。

図 *66 : [Crosswork* の正常性（*Crosswork Health*）*]*



c) [アプリケーションの詳細（Application Details）] ウィンドウから、マイクロサービスの詳細をチェックおよび確認し、マイクロサービスを再起動し、showtech 情報を収集できます。このウィンドウからインストール関連のタスクを実行することもできます。

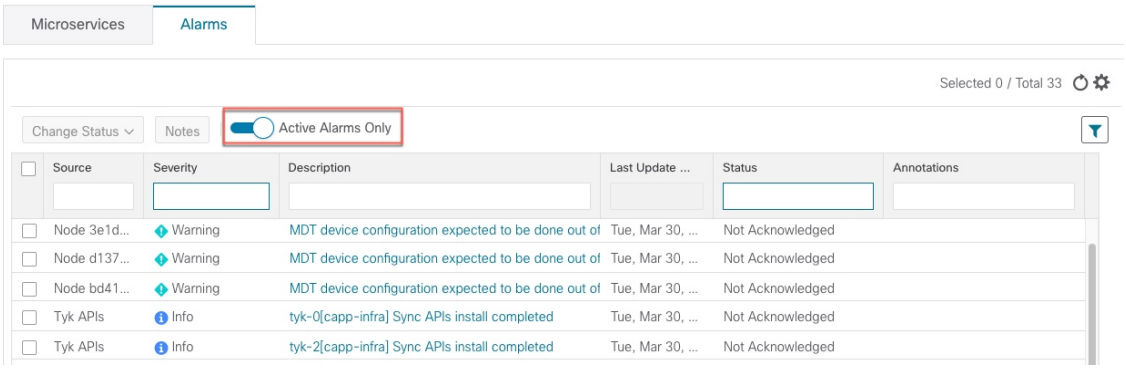
図 *67 :* アプリケーションの詳細（***Application Details***）



ステップ 3 マイクロサービスに関連するアラームを確認および表示します。

a) [アラーム（Alarms）] タブをクリックします。リストには、Crosswork Platform Infrastructure のアラームのみが表示されます。アクティブなアラームのみを表示することで、リストをさらにフィルタ処理できます。

図 *68 :* アラーム



ステップ 4 インストールされている Crosswork アプリケーションを表示します。

a) メインメニューから、**[管理（Administration）] > [Crosswork Manager] > [アプリケーション管理（Application Management）]** タブを選択し、[アプリケーション（Applications）] をクリックします。このウィンドウには、インストールされているすべてのアプリケーションが表示されます。[ファイル（.tar.gz）の追加（Add File (.tar.gz)] をクリックして、さらにアプリケーションをインストールすることもできます。

ステップ 5 ジョブのステータスを表示します。

a) [ジョブ履歴（Job History）] タブをクリックします。このウィンドウには、ジョブのステータスと、ジョブプロセスの一部として実行された一連のイベントに関する情報が表示されます。

システムおよびネットワークアラームの表示

アラームを表示するには、次のいずれかに移動します。

- メインの [Crosswork] ウィンドウで、 をクリックします。
- メインメニューから、**[管理（Administration）] > [アラーム（Alarms）]** を選択します。
- アプリケーション固有のアラームの場合は、**[管理（Administration）] > [Crosswork Manager] > [Crosswork の正常性（Crosswork Health）]** タブを選択します。いずれかのアプリケーションを展開し、[アラーム（Alarms）] タブを選択します。

[アラーム（Alarms）] ウィンドウから次の手順を実行します。

- アラームの詳細をドリルダウンするには、アラームの説明をクリックします。
- 確認し、ステータスを変更し、アラームにメモを追加します。

システム イベント

オペレータが問題をトラブルシューティングできるように、Crosswork インフラストラクチャには、システム関連のイベントを外部サーバに転送する Syslog 機能があります（「Syslog サーバーの設定 （361 ページ）」を参照）。Crosswork プラットフォームに関連するすべてのイベントは、3 つのカテゴリ（Day 0、Day 1、Day 2）に大きく分類されます。次の表に、イベントカテゴリと、そのカテゴリ内のイベントまたはアクションの例を示します。

表 *28 :* イベント分類

イベント分類	イベントとアクションの例
Day 0：Crosswork インフラストラクチャのインストールのみに関連するイベント。	• クラスタのステータスの確認 • ワーカーノードの追加 • ディスクの問題または遅延の問題

イベント分類	イベントとアクションの例
Day 1：Crosswork アプリケーションのインストールに関連するイベント。	• マイクロサービスの再起動 • マイクロサービスの再起動に失敗 • アプリケーションの正常なインストール • アプリケーションの正常なアクティブ化 • アプリケーションがアクティブ化から 3 分以内に正常な状態にならない • ノードのドレインの失敗 • アプリケーションのアクティブ化の失敗 • ワーカーノードの削除
Day 2：システムの運用とメンテナンスに関連するイベント。	• ノード削除 • ノード削除によるクリーンアップの失敗 • アプリケーションの非アクティブ化の失敗 • アプリケーションのアンインストールの失敗 • ディスクまたはネットワークの速度の低下 • ノードの削除 • ノードの挿入 • ノードのドレインの失敗 • k8s ETCD のクリーンアップ • ノードの削除の失敗 • ノードの削除の失敗 • アプリケーションの正常な非アクティブ化 • アプリケーションの正常なアンインストール

Day 0、Day 1、Day 2 のイベント例

次の表に、機能システムでの Day 0、Day 1、Day 2 のさまざまなイベントに関連する情報を示します。

Day 0 イベント

これらのチェックは、システムが正常かどうかを判断するのに役立ちます。

表 *29* : ワーカー ノードの追加

シビラティ（重大度）	[メジャー（Major）]
説明	VM ノードが追加されました。このイベントは、K8 クラスタがノードを検出したときに発生します。
アラームの例	なし
syslog メッセージの例	*<time_stamp> <hosting_hybrid_node> <time_stamp> <crosswork_VIP>* `orchestrator-capp-infra - b54ec903-9e0f-49b8-aaf3-1d72cf644c28 vm4wkr-0 'Successfully added new VM into Inventory: vm4wkr'`
推奨	VM ノードをモニターし、正常なことを示すステータスで UI に表示されていることを確認します。

表 *30* : ネットワークでの低速ディスクまたは遅延の問題

シビラティ（重大度）	[クリティカル（Critical）]
説明	このイベントは、インフラストラクチャ Capp の展開に 1.5 分以上かかった場合か、または Docker プッシュの完了に 2 分以上かかった場合に発生します。 このメッセージは、firstboot.log ファイルで確認できます。
アラームの例	N/A
syslog メッセージの例	N/A

推奨	この問題は、システムでさらに操作を行う前に対処する必要があります。次の手順を実行します。 • ディスクストレージとネットワークのSLA要件が満たされていることを確認します。 • 確認した帯域幅が、ノード間でプロビジョニングされた帯域幅と同じであることを確認します。 • RAID を使用している場合は、RAID 0 であることを確認します。

Day 1 イベント

表 *31 :* ワーカーノードの削除

シビラティ（重大度）	[メジャー（Major）]
説明	このイベントは、VMノードが消去されると発生します。
アラームの例	なし
syslog メッセージの例	*<time_stamp> <hosting_hybrid_node>* *<time_stamp> <crosswork_VIP>* CLUSTER-CLUSTER - 33a5ce0d-6cd0-4e4d-8438-85cfa8fb4ae9 CLUSTER-99 'user=admin,policyId=admin,backend=local,loginTime=2021-02-28T01:38:48Z,Category=VM Manager,RequestId=vm4wkr [Erase VM []]'
推奨	VM ノードをモニターし、UI に表示されなくなっていることを確認します。消去操作が失敗した場合は、ノードの消去を再試行します。

表 *32 :* アプリケーションの追加：成功

シビラティ（重大度）	情報
説明	このイベントは、アプリケーションが正常に追加されると発生します。

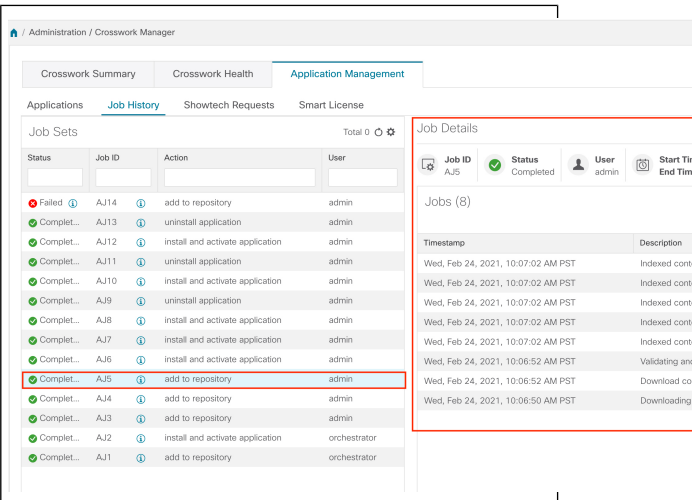
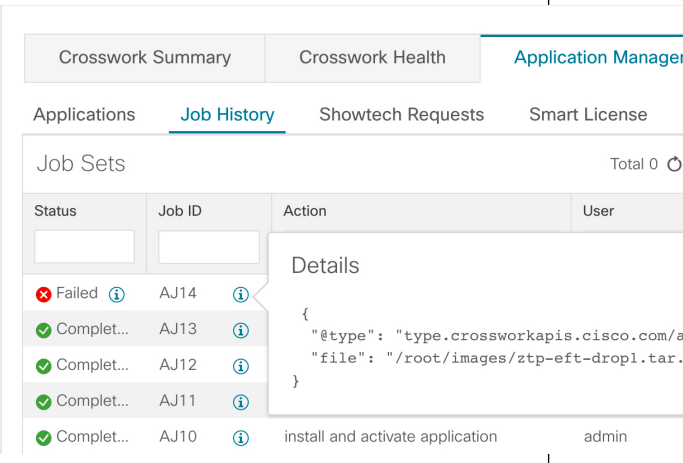
アラーム	
syslog メッセージ	*<time_stamp> <hosting_hybrid_node>* *<time_stamp> <crosswork_VIP>* CLUSTER-CLUSTER - 627b2140-a906-4a96-b59b-1af22f2af9f6 CLUSTER-99 'job_type=INSTALL_AND_ACTIVATE_APPLICATION,manager=app_manager: ,user=admin,policyId=admin,backend=local,loginTime=2021-02- 28T09:34:54Z,payload={"package_identifier":{"id":"cappztp"," version":"1.1.0-prerelease.259+build.260"}} [accepted]'
推奨	なし

表 *33*：アプリケーションの追加：失敗

シビラティ（重大度）	情報
説明	このイベントは、アプリケーションを追加できない場合に発生します。
アラームの例	
syslog メッセージの例	なし

推奨	エラーを修正した後、アプリケーションの追加を再試行します。

表 *34*：アプリケーションのアクティブ化：成功

シビラティ（重大度）	情報
説明	このイベントは、アプリケーションが正常にアクティブ化された後に発生します。
アラームの例	なし
syslog メッセージ	*<time_stamp> <hosting_hybrid_node>* *<time_stamp> <crosswork_VIP>* orchestrator-Crosswork Health Manager - 010689d1-8842-43c2-8ebd-5d91ded9d2d7 cw-ztp-service-0-0 ' cw-ztp-service-0 is healthy.'
推奨	アプリケーションとライセンスをアクティブ化します。

表 *35*：アプリケーションのアクティブ化：失敗

シビラティ（重大度）	[クリティカル（Critical）]
説明	このイベントは、アプリケーションをアクティブ化できない場合に発生します。マイクロサービスまたはポッドが時間内に起動しないため、アクティブ化が失敗する可能性があります。
アラームの例	なし
syslog メッセージ	なし
推奨	次の手順を実行します。 • ジョブ履歴を確認し、アクティブ化プロセスのどこで失敗したかを特定します。起動するポッドのいずれかの開始時に失敗した場合は、ポッドを再起動します。 • アプリケーションをアンインストールしてから、アプリケーションのインストールを再試行してください。

表 *36*：アプリケーションが *3* 分経過しても正常な状態を維持しない

シビラティ（重大度）	[メジャー（Major）]

説明	このイベントは、アプリケーションが正常にアクティブ化されたが、アプリケーションがアクティブになってから 3 分経過してもコンポーネントが正常な状態を維持しない場合に発生します。
アラームの例	なし
syslog メッセージの例	なし
推奨	しばらく待ち、正常な状態になった場合はアラームをクリアします。しばらく経っても正常な状態にならない場合は、Cisco TAC にお問い合わせください。

Day 2 イベント

表 *37:* ノードドレイン：クリーンアップ

シビラティ（重大度）	情報
説明	ノードのドレインは、VM ノードを消去するか、またはノードが 5 分以上応答しない場合に発生します。ドレイン操作時に、ノードで実行されているポッドが移動されます（クラスタ化されたポッドは移動または保留状態になることがあり、単一インスタンスポッドは別のノードに移動します）。
アラームの例	• ノードのドレインの失敗 • ノードの削除時の k8s ETCD のクリーンアップの失敗 • ノードの削除
syslog メッセージ	*<time_stamp> <hosting_hybrid_node>* *<time_stamp> <crosswork_VIP>* orchestrator-Crosswork Health Manager - b062232f-54dc-49b2-8283-506b7bf672a6 astackserver-0-0 ' astackserver-0 health is degraded.'
推奨	操作をモニターします。ドレインが削除の結果である場合は、それぞれのノードを消去し、新しいノードを挿入します。

表 *38 :* ノードのドレイン：失敗

シビラティ（重大度）	[メジャー（Major）]
説明	ノードのドレインは、VM ノードを消去するか、またはノードが 5 分以上応答しない場合に発生します。このイベントは、ノードのドレイン操作が失敗した場合に発生します。
アラームの例	なし
syslog メッセージの例	*<time_stamp> <hosting_hybrid_node>* *<time_stamp> <crosswork_VIP>* orchestrator-Crosswork Health Manager - b062232f-54dc-49b2-8283-506b7bf672a6 astackserver-0-0 ' astackserver-0 health is degraded.'
推奨	ノードを再度消去します。

表 *39 :* ノードの削除：失敗

シビラティ（重大度）	[クリティカル（Critical）]
説明	このシナリオでは、ハイブリッドノードの 1 つに障害が発生したと想定しています。 このイベントは、ノードが5分以上ダウンし、自動的にサービス停止になった場合に発生します。 このイベントは、誰かが Cisco Crosswork を使用せずに VM を停止または削除した場合か、またはそのノードへのネットワークの停止が発生した場合にトリガーされることがあります。k8sはそのノードでポッドの削除を自動的に開始します（ドレイン削除操作）。正常にクリーンアップされている間、VM ノードはダウンとマークされます。
アラームの例	• ノード削除によるクリーンアップの失敗 • ノードの削除時の K8S ETCD のクリーンアップの失敗
syslog メッセージ	なし
推奨	障害が発生したノードを消去し、新しい VM を挿入します。

表 *40 :* ノードの削除：クリーンアップの失敗

シビラティ（重大度）	[クリティカル（Critical）]
説明	このイベントは、ドレイン削除が失敗すると発生します。ノードが 5 分以上ダウンしていると、k8sはそのノードのポッドの削除を自動的に開始します。
アラームの例	なし
syslog メッセージの例	なし
推奨	ノードを消去し、別のクリーンアップ操作を試行します。

表 *41 :* リソースのフットプリントの不足

シビラティ（重大度）	[クリティカル（Critical）]
説明	このイベントは、クラスタノードリソースの使用率が高く、リソースフットプリントが不足している場合に発生します。
アラームの例	なし
syslog メッセージの例	なし
推奨	新しいワーカーノードを追加します。

表 *42 :* アプリケーションの非アクティブ化：成功

シビラティ（重大度）	[マイナー（Minor）]
説明	このイベントは、アプリケーションが非アクティブ化されると発生します。
アラームの例	なし
syslog メッセージの例	*<time_stamp> <hosting_hybrid_node>* *<time_stamp> <crosswork_VIP>* CLUSTER-CLUSTER - ade982ea-7f60-4d6b-b7e0-ebafc789edee CLUSTER-99 © 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential - DRAFT version 1 'user=admin,policyId=admin,backend=local,loginTime=2021-02-28T09:34:54Z,job_type=UNINSTALL_APPLICATION,manager=app_manager:,payload={"application_id":"capp-ztp"} [accepted]'
推奨	なし

表 *43 :* アプリケーションの非アクティブ化：失敗

シビラティ（重大度）	[クリティカル（Critical）]
説明	このイベントは、アプリケーションを非アクティブ化できない場合に発生します。これは、マイクロサービスまたはポッドがまだ実行中の場合に発生する可能性があります。
アラームの例	なし
syslog メッセージ	なし
推奨	次の手順を実行します。 • ジョブ履歴を確認し、アクティブ化プロセスのどこで失敗したかを特定します。起動するポッドのいずれかの開始時に失敗した場合は、ポッドを再起動します。 • アプリケーションをアンインストールしてから、アプリケーションのインストールを再試行してください。

表 *44 :* ネットワークでの低速ディスクまたは遅延の問題

シビラティ（重大度）	[クリティカル（Critical）]
説明	このイベントは、インフラストラクチャ Capp の展開に 1.5 分以上かかった場合か、または Docker プッシュの完了に 2 分以上かかった場合に発生します。 このメッセージは、firstboot.log ファイルで確認できます。
アラームの例	N/A
syslog メッセージの例	N/A

推奨	この問題は、システムでさらに操作を行う前に対処する必要があります。次の手順を実行します。 • ディスクストレージとネットワークのSLA要件が満たされていることを確認します。 • 確認した帯域幅が、ノード間でプロビジョニングされた帯域幅と同じであることを確認します。 • RAID を使用している場合は、RAID 0 であることを確認します。

表 *45 : ETCD* のクリーンアップ

シビラティ（重大度）	情報
説明	このイベントは、誰かがVMノードを消去し、ETCDクリーンメンバーシップのクリーンアップ操作が開始された場合に発生します。
アラームの例	ETCD のクリーンアップが失敗した場合： • ノードの削除時の K8S ETCD のクリーンアップの失敗 • アラームノードの削除
syslog メッセージ	なし
推奨	モニター操作。

表 *46 :* ノードの削除時の *K8S ETCD* のクリーンアップの失敗

シビラティ（重大度）	[メジャー（Major）]
説明	このイベントは、ETCD クリーンアップ操作が失敗した場合に発生します。
アラームの例	なし
syslog メッセージの例	なし
推奨	ノードを再度消去します。

表 *47 :* マイクロサービスの再起動：失敗

シビラティ（重大度）	警告（Warning）

説明	このイベントは、誰かがマイクロサービスまたはポッドを再起動し、操作が失敗したときに発生します。
アラームの例	なし
syslog メッセージの例	なし
推奨	マイクロサービスまたはポッドを再起動します。回復するかどうかを確認するために、これを数回行う必要がある場合があります。

監査情報の収集

監査ログは、システムで実行されたすべての重要なユーザーアクションにユーザー情報をマッピングします。アプリケーションの Showtech ログを表示するには、「プラットフォーム インフラストラクチャとアプリケーション正常性のモニター（368ページ）」を参照してください。

監査ログには、次の操作に関連するユーザーアクションが含まれます。

- デバイスのオンボーディング
- ユーザーの作成、削除、および設定の更新
- Crosswork Data Gateway の管理操作
- 収集ジョブの作成
- 管理タスク（show-tech の実行、トポロジの更新、NSO 関連のアクション）
- Cisco Crosswork Change Automation and Health Insights：
  - プレイブック（インポート、エクスポート、または削除）とプレイブックの実行の管理

（注） プレイブックの実行要求が送信されると、Change Automation は監査ログを出力します。監査ログには、プレイブック名、ユーザー情報、セッションの詳細、ジョブの実行 ID などの詳細が含まれます。Change Automation がプレイブックのメンテナンスタスクを実行すると、監査ログも出力します。メンテナンス監査ログには、実行 ID などの詳細が含まれています。NSO でコミットを実行する場合、メンテナンス監査ログの詳細にはコミットラベルも含まれます。監査ログを使用して、実行 ID に関連付けられたすべてのコミットラベルを特定できます。コミットラベルを使用して、NCS CLI でルックアップを実行します。ルックアップには、Change Automation がデバイスにプッシュした設定変更がそのまま表示されます。

- KPI、KPI プロファイル、アラートグループの作成、削除、設定の更新
- KPI プロファイルの有効化と無効化

- Cisco Crosswork 最適化エンジン：
  - SR-TE ポリシーおよび RSVP TE トンネルの作成、削除、および設定の更新
  - アフィニティマッピングの設定
  - オンデマンド帯域幅および帯域幅最適化機能と設定の更新
  - RESTCONF API の作成、削除、および設定の更新

Cisco Crosswork Change Automation and Health Insights 監査ログエントリの例

次に、ローカル管理者ユーザーがプレイブックを実行したときに作成される監査ログエントリの例を示します。

```
time="2020-06-09 21:24:31.103312" level=info msg="playbook scheduled for execution"
backend=local execution_id=1591737871096-a6699d03-8264-4ea8-8f6f-03e8a58f32a3
latency=11.330355ms loginTime="2020-06-09T20:27:11Z" method=POST
playbook="router_config_traffic_steering" policyId=admin
set_id=5405fdb1-6b37-41cb-94a3-32b180d3b773 set_name=static-acl-b180d3b773
tag="ROBOT_manager-nca-7689b-fdn8g" user=admin
```

Cisco Crosswork 最適化エンジン 監査ログエントリの例

Crosswork 最適化エンジン UI 監査ログエントリの例

```
2020-06-12 02:48:07,990 INFO c.c.s.o.e.AuditLogger [http-nio-8080-exec-3] time=2020-06-12
 02:48:07.000990 message=SR Policy created successfully. user=admin policyId=admin
backend=local loginTime=1591929794
{data={"headEnd":"192.168.0.2","endPoint":"192.168.0.6","color":"999","description":"","profileId":"","bindingSid":"333",
 "path":{"type":"dynamic","pathName":"Automation_validating_sr","metric":"IGP",
"affinity":[{"constraintType":"EXCLUDE_ANY","affinity":[31]}],"disjointness":{"disjointType":"",
 "associationGroup":"","subId":""}, "protectedSegment":"SEG_PROTECTED"}}}
```

Crosswork 最適化エンジン RESTCONF API 監査ログエントリの例

```
time="2020-06-06 13:49:06,308"
message="action=/operations/cisco-crosswork-optimization-engine-sr-policy-operations:sr-policy-delete,
 input={\"input\": {\"sr-policies\": [{\"head-end\": \"192.168.0.2\", \"end-point\":
\"192.168.0.3\", \"color\": 301}]}},
output={\"cisco-crosswork-optimization-engine-sr-policy-operations:output\":{\"results\":
 [{\"head-end\":\"192.168.0.2\",\"end-point\":\"192.168.0.3\",\"color\":301,
\"message\":\"SR policy  not found in Config DB\",\"state\":\"failure\"}]}}" user=admin
 policyId=admin backend=local loginTime=1591451346 method=POST
url=/operations/cisco-crosswork-optimization-engine-sr-policy-operations:sr-policy-delete
```

表 *48 :* 監査ログの共通入力フィールド

フィールド	説明
time	Crosswork がこの監査ログを作成した時刻。

フィールド	説明
message	アプリケーション間で送信されるメッセージ。
msg	アプリケーション間で送信されるメッセージ。
user	ユーザー名。
policyId	ユーザーのロールまたは権限（ローカルデータベース、TACACS、または LDAP サーバーから取得）。
backend	ユーザーを認証するサーバー（ローカルデータベース、TACACS、または LDAP）。
loginTime	ユーザーがログインした epoch 時間。epoch 時間は日付型よりも期間が短く、タイムゾーンに依存しないため、意図的に選択されます。
その他のフィールド	個々のアプリケーションは、そのアプリケーションに固有のフィールドをより多く使用します。次に例を示します。 • Cisco Crosswork Change Automation and Health Insights の監査ログエントリの例では、[プレイブック（playbook）] フィールドは、Change Automation が実行したプレイブックを参照します。 • Crosswork 最適化エンジン の UI 監査ログエントリでは、[データ（data）] は SR-TE ポリシーとその属性の作成の詳細を参照するフィールドです。

監査ログの場所

Crosswork は、監査ログをそれぞれのアプリケーションポッドの下の `/var/log/audit/audit.log` に保存します。次に例を示します。

- 変更自動化 監査ログの例は、ポッドの下の `<robot-nca>` データディレクトリにあります。
- Crosswork 最適化エンジン UI 監査ログの例は、`optima-uiservice` ポッドにあります。RESTCONF API 監査ログは `optima-restconf` ポッドの下にあります。

個々のアプリケーション監査ログに加えて、Cisco Crosswork はすべての監査ログファイルを 1 時間に 1 回収集します。Crosswork は、これらのファイルを gzip で圧縮された個別の tar ファイルとして `/mnt/robot_datafs/<app-name>/<instance>/auditlogs/auditlogs.tar.gz` データディレクトリに保存します。

Crosswork は、アプリケーションごとに指定された最大サイズとバックアップ数に基づいて監査ログファイルを収集します。例：**`MaxSize:20 megabytes`** と **`MaxBackups: 5`**.

View Audit Log

[監査ログ（Audit Log）] ウィンドウは、次の AAA 関連のイベントを追跡します。

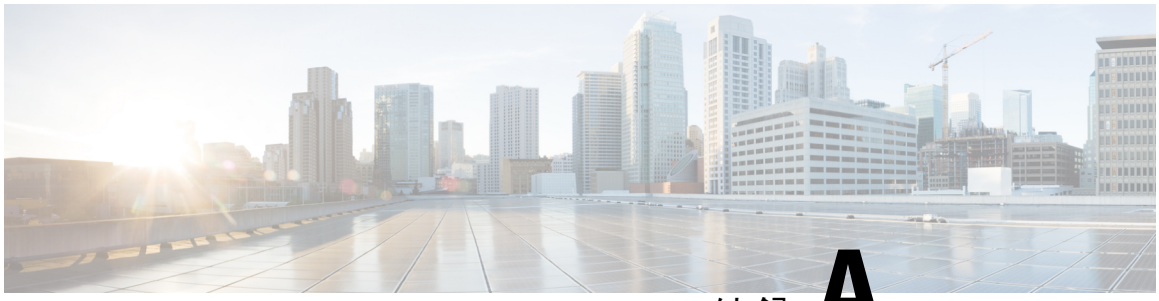
- ユーザーの作成、削除、更新
- ロールの作成、削除、更新
- ユーザー ログイン アクティビティ：ログイン、ログアウト、アクティブセッション最大制限によるログイン失敗、ログイン試行失敗によるアカウントロック。
- ユーザーによるパスワード変更

監査ログを表示するには、次の手順を実行します。

ステップ 1 メインメニューから、**[管理（Administration）] > [監査ログ（Audit Log）]** を選択します。

[監査ログ（Audit Log）] ウィンドウが表示されます。

ステップ 2 をクリックして、クエリに基づいて結果をフィルタリングします。



付録 A

Crosswork Data Gateway VM の設定

Cisco Crosswork Data Gateway インスタンスは、スタンドアロン VM として作成されており、コントローラ アプリケーションとは別の場所に配置することができます（コントローラ アプリケーションは、Cisco Crosswork インフラストラクチャ または Crosswork Cloud です）。この VM は、ネットワークからのデータ収集を可能にするコントローラ アプリケーションに接続できます。

この章は次のトピックで構成されています。

インタラクティブなコンソールの使用

Cisco Crosswork Data Gateway は、ログインに成功するとインタラクティブコンソールを起動します。次の図に示すように、インタラクティブコンソールにメインメニューが表示されます。

（注） ここに示すメインメニューは、**dg-admin** ユーザに対応しています。オペレータには管理者と同じ権限はないため、**dg-oper** ユーザーの場合とは異なります。表 49 : 各ロールの権限 （395 ページ） を参照してください。

メインメニューには、次のオプションが表示されます。

1. 登録パッケージのエクスポート

2. システム設定の表示

3. 現在のシステム設定の変更

4. バイタル

5. トラブルシューティング

p. パスフレーズの変更

l. ログアウト

Crosswork Data Gateway ユーザーの管理

ここでは、次の内容について説明します。

サポートされるユーザ ロール

Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） は次のユーザロールを持つ 2 ユーザのみをサポートしています。

- **管理者**：Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） が初めて起動されたときに、管理者ロールを持つ 1 人のデフォルトの **dg-admin** ユーザが作成されます。このユーザーは削除できず、Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） の VM の起動やシャットダウン、アプリケーションの登録、認証証明書の適用、サーバー設定の構成、カーネルアップグレードの実行などの読み取りと書き込みの両方の権限が設定されています。
- **オペレータ**：VM の最初の起動時に、デフォルトで **dg-oper** ユーザも作成されます。このユーザーは、Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） の正常性を確認し、エラーログを取得し、エラー通知を受信し、Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） インスタンスと出力の接続先間との接続テストを実行できます。

（注）
- ユーザークレデンシャルは、Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） のインストール時に両方のユーザーアカウントに設定されます。
- ユーザはローカル認証されています。

次の表に、各ロールで使用できる権限を示します。

表 *49 :* 各ロールの権限

権限	管理者	オペレータ
登録パッケージのエクスポート	✓	✓
システム設定の表示		
vNIC アドレス NTP DNS プロキシ UUID Syslog 証明書 ファースト ブート プロビジョニング ログ タイムゾーン	✓	✓
現在のシステム設定の変更		
NTP の設定 DNS の設定 制御プロキシの設定 スタティックルートの設定 Syslog の設定 新しい SSH キーの作成 証明書のインポート vNIC2 MTU の設定 タイムゾーンの設定 パスワード要件の設定 同時ログイン数の制限の設定 アイドルタイムアウトの設定	✓	×
バイタル		

権限	管理者	オペレータ
Docker コンテナ Docker イメージ コントローラの到達可能性 NTP の到達可能性 ルート テーブル ARP テーブル ネットワーク接続 ディスク領域使用率 Linux サービス NTP ステータス システム稼動時間	✓	✓
トラブルシューティング		
診断コマンドの実行 show-tech の実行 すべてのコレクタの削除と VM の再起動 VM のリブート auditd ログのエクスポート Data Gateway の再登録 TAC シェルアクセスの有効化	✓ ✓ ✓ ✓ ✓ ✓ ✓	✓ ✓ × × ✓ ✓ ×
パスフレーズの変更	✓	✓

パスワードの変更

管理者ユーザとオペレータユーザの両方が自分のパスフレーズを変更できますが、相互に変更を行うことはできません。

自分のパスフレーズを変更するには、次の手順を実行します。

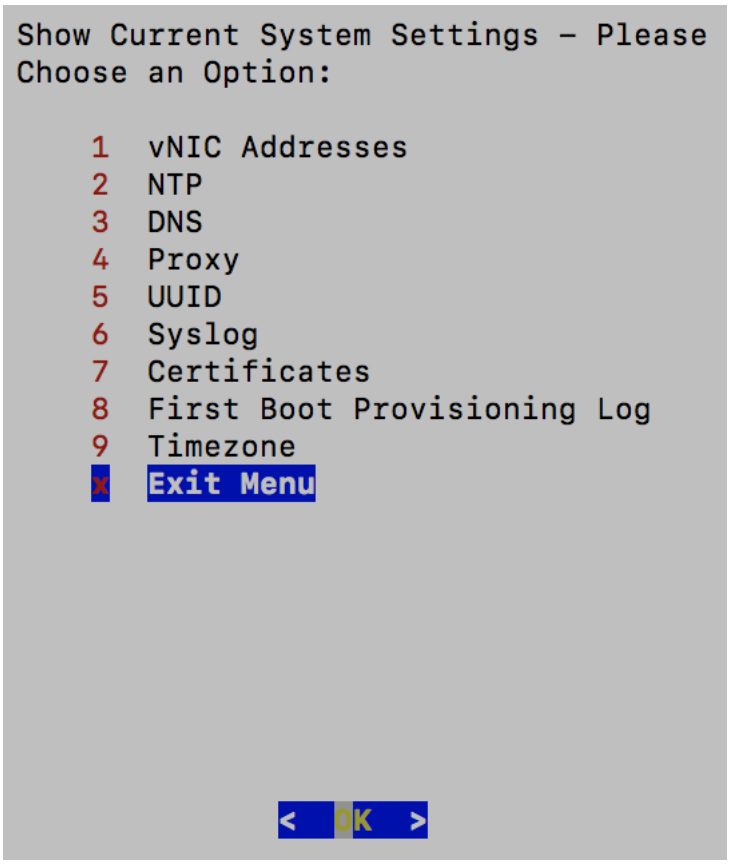
ステップ 1 メインメニューから、[パスフレーズの変更（Change Passphrase）] を選択し、[OK] をクリックします。

ステップ 2 現在のパスワードを入力し、[Enter] キーを押します。

ステップ 3 新しいパスワードを入力し、[Enter] キーを押します。パスワードをもう一度入力して、[Enter] キーを押します。

現在のシステム設定の表示

Crosswork Data Gateway では、次の設定を表示できます。



現在のシステム設定を表示するには、次の手順を実行します。

ステップ 1 次の図に示すように、メインメニューから [2 システム設定の表示（2 Show System Settings）] を選択します。

ステップ 2 [OK] をクリックします。[現在のシステム設定の表示（Show Current System Settings）] メニューが開きます。

ステップ 3 表示する設定を選択します。

設定オプション	説明
[1 vNICアドレス（1 vNIC Addresses）]	アドレス情報を含む、vNIC 設定を表示します。

設定オプション	説明
[2 NTP]	現在設定されている NTP サーバの詳細を表示します。
[3 DNS]	DNS サーバの詳細を表示します。
[4 プロキシ（4 Proxy）]	プロキシサーバの詳細を表示します（設定されている場合）。
[5 UUID]	システム UUID を表示します。
[6 Syslog]	Syslog の転送設定を表示します。Syslog の転送が設定されていない場合は、画面に「# Forwarding configuration follows」と表示されます。
[7 証明書（7 Certificates）]	次の証明書ファイルを表示するオプションがあります。 • Crosswork Data Gateway 署名証明書ファイル • コントローラ署名証明書ファイル • コントローラの SSL/TLS 証明書ファイル • Syslog 証明書ファイル • コレクタ証明書ファイル
[8 ファーストブートプロビジョニングログ（8 First Boot Provisioning Log）]	最初のブートログファイルの内容を表示します。
[9 タイムゾーン（9 Timezone）]	現在の時間帯設定を表示します。

現在のシステム設定の変更

Crosswork Data Gateway では、次の設定を行います。

- NTP。
- DNS 用です。
- 制御プロキシ。
- スタティック ルート
- Syslog。
- SSH キー。

- 証明書。
- vNIC2 MTU。
- タイムゾーン。
- パスワード要件。
- 同時ログイン制限。
- Idle timeout.
- auditd を設定します。

（注）
- Crosswork Data Gateway システム設定は管理者のみが設定できます。
- SCP を使用する必要がある設定オプションで、SCP デフォルトの SCP ポート 22 を使用しない場合は、SCP コマンドの一部としてポートを指定できます。次の例を参考にしてください。

  ```
  -P55 user@host:path/to/file
  ```

  55 はカスタムポートです。

NTP の設定

NTP 時刻は、コントローラ アプリケーションおよびそのCrosswork Data Gatewayインスタンスと同期することが重要です。同期しないと、セッションハンドシェイクが行われず、機能イメージはダウンロードされません。その場合、「clock time not match and sync failed」というエラーメッセージが controller-gateway.log に記録されます。ログファイルにアクセスするには、show-tech の実行 （413 ページ） を参照してください。メインメニューの [バイタル（Vitals）] から [コントローラの到達可能性（Controller Reachability）] および [NTP到達可能性（NTP Reachability）] オプションを使用して、Crosswork Data Gateway と同様にコントローラ アプリケーションの NTP の到達可能性を確認できます。（「Crosswork Data Gateway のバイタルの表示 （407 ページ）」を参照）。NTP が正しく設定されていないと、「Session not established」というエラーが表示されます。

キーファイルによる認証を使用するように Crosswork Data Gateway を設定する場合、chrony.keys ファイルはhttps://chrony.tuxfamily.org/doc/3.5/chrony.conf.html#keyfile に記載されている特定の方法でフォーマットする必要があります。ntpd を使用しており、ntp.keys ファイルを使用するように設定されているサイトでは、ツール https://github.com/mlichvar/ntp2chrony/blob/master/ntp2chrony/ntp2chrony.py を使用して、ntp.keys から chrony.keys に変換できます。ツールは ntpd 設定を chrony 互換形式に変換しますが、キーファイルのみをCrosswork Data Gatewayにインポートする必要があります。

NTP 設定を構成するには、次の手順に従ってください。

ステップ 1 [現在のシステム設定の変更（Change Current System Settings）] メニューから、[1 NTPの設定（1 Configure NTP）] を選択します。

ステップ 2 次のように新しい NTP サーバの詳細を入力します。

- サーバリスト、スペース区切り
- NTP 認証を使用するかどうか
- キーリスト、スペース区切り。サーバリストと数が一致する必要がある
- VM への SCP へのキーファイル URI
- VM への SCP へのキーファイルパスフレーズ

ステップ 3 設定を保存するには [**OK**] をクリックします。

DNS の設定

ステップ 1 [現在のシステム設定の変更（Change Current System Settings）] メニューから、[2 DNSの設定（2 Configure DNS）] を選択し、[OK] をクリックします。

ステップ 2 新しい DNS サーバアドレスとドメインを入力します。

ステップ 3 設定を保存するには [**OK**] をクリックします。

制御プロキシの設定

インストール時にプロキシサーバを設定していない場合は、このオプションを使用してプロキシサーバを設定します。

ステップ 1 [現在のシステム設定の変更（Change Current System Settings）] メニューから、[3 制御プロキシの設定（3 Configure Control Proxy）] を選択し、[OK] をクリックします。

ステップ 2 続行する場合は、次のダイアログで [はい（Yes）] をクリックします。続行しない場合は、[キャンセル（Cancel）] をクリックします。

ステップ 3 次のように新しいプロキシサーバの詳細を入力します。

- サーバ URL
- バイパスアドレス
- プロキシ ユーザ名
- プロキシパスフレーズ

ステップ 4 設定を保存するには [**OK**] をクリックします。

スタティックルートの設定

スタティックルートは、Crosswork Data Gateway がコレクタから追加/削除要求を受信したときに設定されます。メインメニューの [スタティックルートの設定（Configure Static Routes）] オプションは、トラブルシューティングに使用できます。

（注） このオプションを使用して設定されたスタティックルートは、Crosswork Data Gateway のリブート時に失われます。

スタティック ルートの追加

スタティックルートを追加するには、次の手順を実行します。

ステップ 1 [現在のシステム設定の変更（Change Current System Settings）] メニューから、[4 スタティックルートの設定（4 Configure Static Routes）] を選択します。
ステップ 2 スタティックルートを追加するには、[追加（Add）] を選択します。
ステップ 3 スタティックルートを追加するインターフェイスを選択します。
ステップ 4 IP バージョンを選択します。
ステップ 5 プロンプトが表示されたら、CIDR 形式で IPv4 または IPv6 サブネットを入力します。
ステップ 6 設定を保存するには [**OK**] をクリックします。

スタティック ルートの削除

スタティックルートを削除するには、次の手順を実行します。

ステップ 1 [現在のシステム設定の変更（Change Current System Settings）] メニューから、[4 スタティックルートの設定（4 Configure Static Routes）] を選択します。
ステップ 2 スタティックルートを削除するには、[削除（Delete）] を選択します。
ステップ 3 スタティックルートを削除するインターフェイスを選択します。
ステップ 4 IP バージョンを選択します。
ステップ 5 CIDR 形式で IPv4 または IPv6 サブネットを入力します。
ステップ 6 設定を保存するには [**OK**] をクリックします。

Syslog の設定

（注） 複数の Linux ディストリビューションで IPv4 または IPv6 をサポートするように Syslog サーバーを設定する場合は、システム管理者ガイドおよび設定ガイドを参照してください。

次の手順に従い、Syslog を設定します。

ステップ 1 [現在のシステム設定の変更（Change Current System Settings）] メニューから、[5 Syslogの設定（5 Configure Syslog）] を選択します。

ステップ 2 次の syslog 属性の新しい値を入力します。

- [サーバアドレス（Server address）]：管理インターフェイスからアクセス可能な syslog サーバの IPv4 または IPv6 アドレス。IPv6 アドレスを使用している場合は、角カッコ（[1 :: 1]）で囲む必要があります。
- [ポート（Port）]：syslog サーバのポート番号。
- [プロトコル（Protocol）]：syslog の送信時に UDP、TCP、または RELP を使用します。
- [TLS経由のSyslogを使用する?（Use Syslog over TLS?）]：TLS を使用して syslog トラフィックを暗号化します。
- [TLSピア名（TLS Peer Name）]：サーバ証明書の SubjectAltName またはサブジェクト共通名に入力されたとおりの Syslog サーバのホスト名。
- [Syslogルート証明書ファイルURI（Syslog Root Certificate File URI）]：SCP を使用して取得した Syslog サーバの PEM 形式のルート証明書。
- [Syslog証明書ファイルのパスフレーズ（Syslog Certificate File Passphrase）]：Syslog 証明書チェーンを取得する SCP ユーザのパスワード。

ステップ 3 設定を保存するには [**OK**] をクリックします。

新しい SSH キーの作成

新しい SSH キーを作成すると、現在のキーが削除されます。

次の手順に従って、新しい SSH キーを作成します。

ステップ 1 [現在のシステム設定の変更（Change Current System Settings）] メニューから、[6 新しいSSHキーの作成（6 Create new SSH keys）] を選択します。

ステップ 2 [OK] をクリックします。Crosswork Data Gateway は、新しい SSH キーを生成する自動設定プロセスを開始します。

証明書のインポート

コントローラ署名証明書以外の証明書を更新すると、コレクタが再起動します。

Crosswork Data Gateway では、次の証明書をインポートすることができます。

- コントローラ署名証明書ファイル
- コントローラの SSL/TLS 証明書ファイル
- Syslog 証明書ファイル
- プロキシ証明書ファイル

ステップ 1 [現在のシステム設定の変更（Change Current System Settings）] メニューから、[7 証明書のインポート（7 Import Certificate）] を選択します。

ステップ 2 インポートする証明書を選択します。

ステップ 3 選択した証明書ファイルの SCP URI を入力します。

ステップ 4 SCP URI のパスフレーズを入力し、[OK] をクリックします。

vNIC2 MTU の設定

3 つの NIC を使用している場合にのみ、vNIC2 MTU を変更できます。

インターフェイスがジャンボフレームをサポートしている場合、MTU 値の範囲は 60 ー 9000 です。ジャンボフレームをサポートしないインターフェイスの場合、有効な範囲は 60 ー 1500 です。無効な MTU を設定すると、Crosswork Data Gateway は変更を現在設定されている値に戻します。有効な範囲を確認するには、ハードウェアのマニュアルを参照してください。エラーは、showtech の実行後に表示される MTU 変更エラーの kern.log に記録されます。

ステップ 1 [現在のシステム設定の変更（Change Current System Settings）] メニューから、[8 vNIC1 MTUの設定（8 Configure vNIC1 MTU）] を選択します。

ステップ 2 vNIC2 MTU 値を入力します。

ステップ 3 設定を保存するには [**OK**] をクリックします。

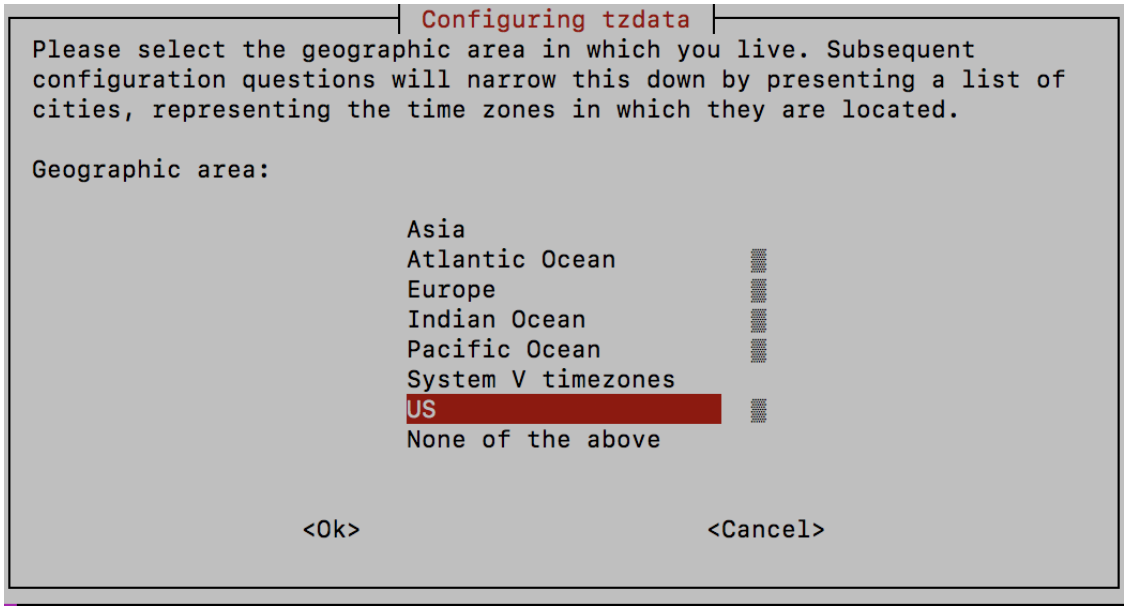
Crosswork Data Gateway VM のタイムゾーンの設定

Crosswork Data Gateway VM は、最初にデフォルトのタイムゾーン（UTC）で起動します。すべての Crosswork Data Gateway プロセス（showtech ログを含む）が、選択した場所に対応したタイムスタンプを反映するように、所在地に合わせてタイムゾーンを更新します。

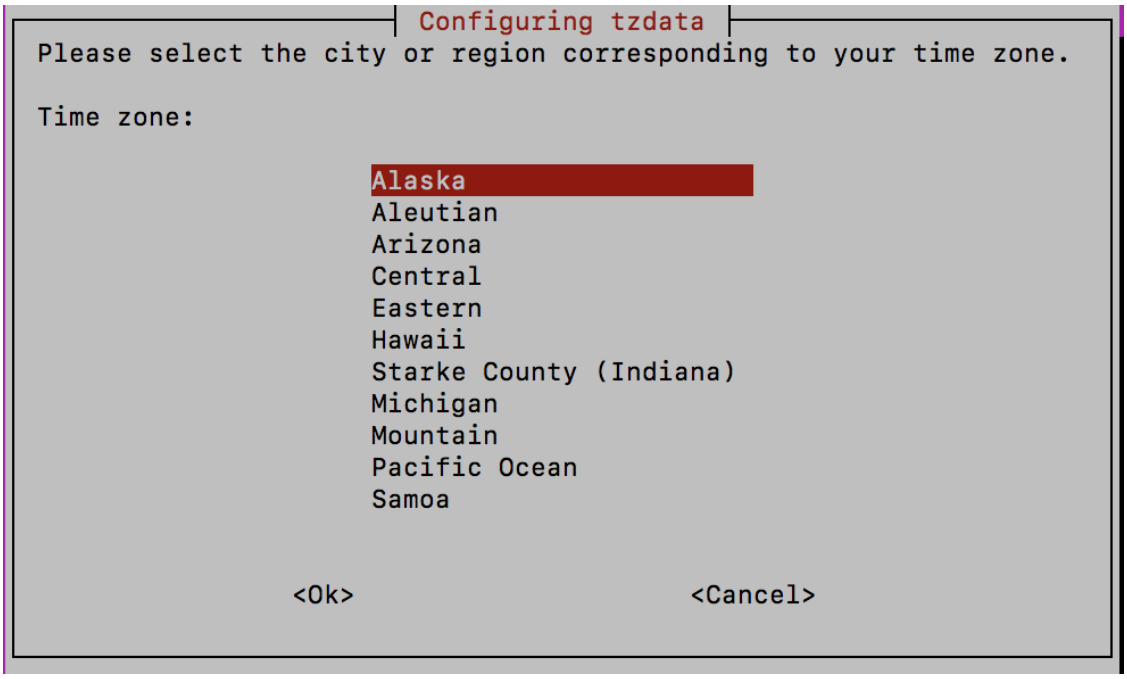
ステップ 1 Crosswork Data GatewayVM のインタラクティブメニューで、[Change Current System Settings] を選択します。

ステップ 2 [9 Timezone] を選択します。

ステップ 3 居住地域を選択します。



ステップ 4 タイムゾーンに対応する都市または地域を選択します。



ステップ 5 [OK] を選択して設定を保存します。

ステップ 6 Crosswork Data GatewayVM をリブートして、すべてのプロセスで新しいタイムゾーンが選択されるようにします。

ステップ 7 Crosswork Data Gateway VM からログアウトします。

パスワード要件の設定

次のパスワード要件を設定できます。

- パスワードの強度
- パスワード履歴
- パスワードの有効期限
- ログインエラー

ステップ 1 [現在のシステム設定の変更（Change Current System Settings）] メニューから、[0 パスワード要件の設定（0 Configure Password Requirements）] を選択します。

ステップ 2 変更するパスワード要件を選択します。

変更するオプションを設定します。

- **[パスワードの強度（Password Strength）]**
  - [クラスの最小数（Min Number of Classes）]

- [最小長（Min Length）]
- [最小変更文字数（Min Changed Characters）]
- [クレジットの最大桁数（Max Digit Credit）]
- [クレジットの最大大文字数（Max Upper Case Letter Credit）]
- [クレジットの最大小文字数（Max Lower Case Letter Credit）]
- [クレジットのその他の文字の最大文字数（Max Other Character Credit）]
- [最大単調シーケンス（Max Monotonic Sequence）]
- [連続する最大文字数（Max Same Consecutive Characters）]
- [同じクラスの最大連続文字数（Max Same Class Consecutive Characters）]

- **[パスワード履歴（Password History）]**
  - [変更の再試行（Change Retries）]
  - [履歴数（History Depth）]

- [パスワードの有効期限（Password expiration）]
  - [最小日数（Min Days）]
  - [最大日数（Min Days）]
  - [警告日（Warn Days）]

- **[ログインエラー（Login Failures）]**
  - [ログインエラー（Login Failures）]
  - [初期ブロック時間（秒）（Initial Block Time (sec)）]
  - [アドレスキャッシュタイム（秒）（Address Cache Time (sec)）]

ステップ 3 設定を保存するには [**OK**] をクリックします。

同時ログイン数の制限の設定

デフォルトでは、Crosswork Data Gateway は、各 VM の **dg-admin** および **dg-oper** ユーザーに対して 10 の同時セッションをサポートします。これを変更するには、次の手順を実行します。

ステップ 1 [現在のシステム設定の変更（Change Current System Settings）] メニューから、[同時ログイン数の制限の設定（Configure Simultaneous Login Limits）] を選択します。

ステップ 2 表示されるウィンドウで、**dg-admin** および **dg-oper** ユーザーの同時セッション数を入力します。

ステップ 3 [OK] を選択して変更内容を保存します。

アイドルタイムアウトの設定

ステップ 1 [現在のシステム設定の変更（Change Current System Settings）] メニューから、[b アイドルタイムアウトの設定（b Configure Idle Timeout）] を選択します。

ステップ 2 表示されるウィンドウに、アイドルタイムアウトの新しい値を入力します。

ステップ 3 **Ok** と入力して、変更を保存します。

リモート監査サーバーの設定

この手順を使用して、リモートサーバーへの auditd daemon のエクスポートを設定します。

ステップ 1 [現在のシステム設定の変更（Change Current System Settings）] メニューから、[c auditdを設定（c Configure auditd）] を選択します。

ステップ 2 次の詳細を入力します。

- リモート Auditd サーバーアドレス。
- リモート auditd サーバーポート。

ステップ 3 [OK] を選択して変更内容を保存します。

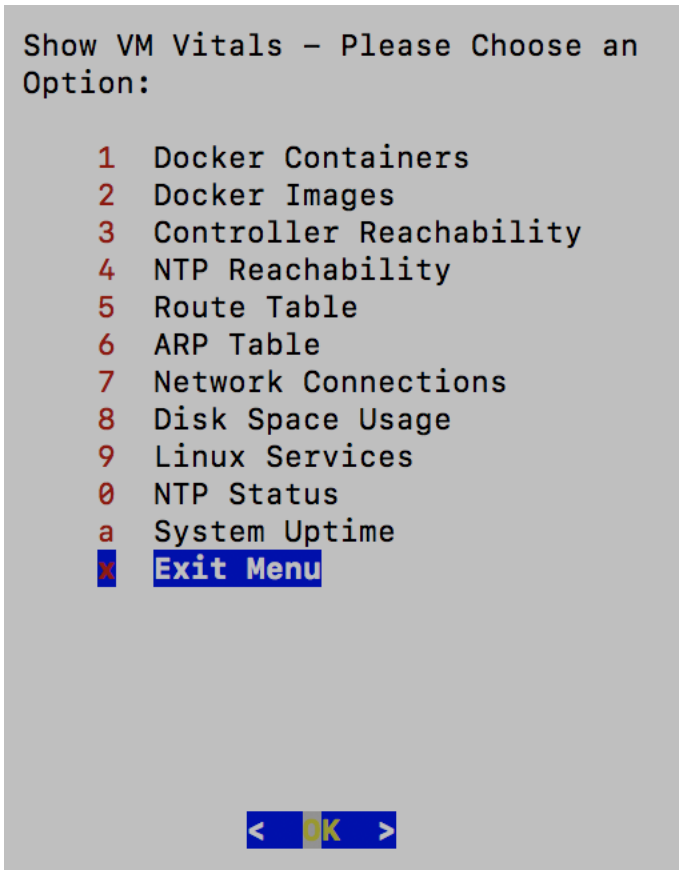
Crosswork Data Gateway のバイタルの表示

以下の手順に従って、Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） のバイタルを表示します。

ステップ 1 メインメニューで、**バイタルを 4 つ**選択します。

ステップ 2 [VMのバイタルの表示（Show VM Vitals）] メニューから、表示するバイタルを選択します。

Crosswork Data Gateway VM の設定



バイタル	説明
Docker コンテナ（Docker Containers）	システムで現在インスタンス化されている Docker コンテナの次のバイタルを表示します。 コンテナ ID（Container ID） イメージ画像（Image） 名前（Name） コマンド（Command） 作成時刻（Created Time） ステータス（Status） ポート（Port）

バイタル	説明
Docker イメージ（Docker Images）	システムで現在保存されている Docker イメージの次の詳細を表示します。 リポジトリ（Repository） イメージ ID（Image ID） 作成時刻（Created Time） サイズ（Size） タグ（Tag）
コントローラの到達可能性（Controller Reachability）	コントローラの到達可能性テストの実行結果を表示します。 デフォルト IPv4 ゲートウェイ（Default IPv4 gateway） デフォルト IPv6 ゲートウェイ（Default IPv6 gateway） DNS サーバ（DNS server） コントローラ（Controller） コントローラセッションのステータス（Controller session status）
NTP の到達可能性（NTP Reachability）	NTP 到達可能性テストの結果を表示します。 NTP サーバの解決（NTP server resolution） Ping NTP ステータス（NTP Status） 現在のシステム時間（Current system time）
ルート テーブル（Route Table）	IPv4 および IPv6 ルーティングテーブルを表示します。
ARP テーブル（ARP Table）	ARP テーブルを表示します。
ネットワーク接続（Network Connections）	現在のネットワーク接続とリスニングポートを表示します。
ディスク領域使用率（Disk Space Usage）	すべてのパーティションの現在のディスク容量の使用状況を表示します。

バイタル	説明
Linux サービス（Linux Services）	次の Linux サービスのステータスを表示します。 • NTP • SSH • Syslog • Docker • Cisco Crosswork データゲートウェイ（Cisco Crosswork Data Gateway） インフラストラクチャ コンテナ
NTP ステータスの確認	NTP サーバーのステータスを表示します。
システム稼働時間の確認	システム稼働時間を表示します。

Crosswork Data Gateway VM のトラブルシューティング

[トラブルシューティング（Troubleshooting）] メニューにアクセスするには、メインメニューから [5 トラブルシューティング（5 Troubleshooting）] を選択します。

（注） 画像は、**dg-admin** ユーザーに対応する [トラブルシューティング（Troubleshooting）] メニューを示しています。**dg-oper** ユーザはこれらのオプションの一部を使用できません。表 49：各ロールの権限 （395 ページ） を参照してください。

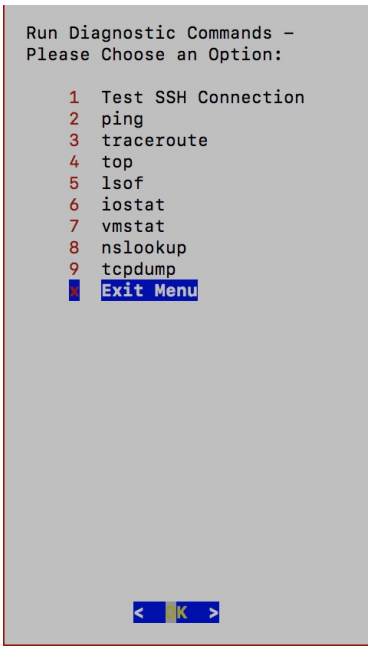
[トラブルシューティング（Troubleshooting）] メニューには、次のオプションがあります。

• 診断コマンドの実行 （411 ページ）
• show-tech の実行 （413 ページ）
• Crosswork Data Gateway VM の再起動 （414 ページ）
• Crosswork Data Gateway VM のシャットダウン （414 ページ）
• auditd ログのエクスポート （414 ページ）
• TAC シェルアクセスの有効化 （415 ページ）

診断コマンドの実行

[診断の実行（Run Diagnostics）] メニューでは、コンソールに次のオプションが表示されます。

図 *69 : [*診断の実行（***Run Diagnostics***）*] メニュー*



ホストへの Ping

Crosswork Data Gateway は、任意の IP アドレスへの到達可能性を確認するために使用できる ping ユーティリティを提供します。

ステップ 1 [診断の実行（Run Diagnostics）] メニューから [2 ping] を選択します。

ステップ 2 次の情報を入力します。

- Ping 回数
- 宛て先ホスト名または IP
- 送信元ポート（UDP、TCP、TCP 接続）
- 宛て先ポート（UDP、TCP、TCP 接続）

ステップ 3 [OK] をクリックします。

ホストに対するトレースルート

Crosswork Data Gateway には遅延の問題のトラブルシューティングに役立つ [トレースルート（traceroute）] オプションが用意されています。このオプションを使用すると、Crosswork Data Gateway が接続先に到達するまでの大まかな時間を予測できます。

ステップ 1 [診断の実行（Run Diagnostics）] メニューから、[3 トレースルート（3 traceroute）] を選択します。

ステップ 2 トレースルート先を入力します。

ステップ 3 [OK] をクリックします。

トラブルシューティングのためのコマンドオプション

Crosswork Data Gateway には、トラブルシューティング用のコマンドがいくつか用意されています。

ステップ 1 [5 トラブルシューティング（5 Troubleshooting）] > [1 診断の実行（1 Run Diagnostics）] に移動します。

ステップ 2 コマンドと各コマンドの他のオプションまたはフィルタを選択します。

- **4 top**
- **5 lsof**
- **6 iostat**
- **7 vmstat**
- **8 nsolookup**

ステップ 3 [OK] をクリックします。

すべてのオプションを選択すると、Crosswork Data Gateway は画面をクリアし、指定したオプションを使用してコマンドを実行します。

tcpdump のダウンロード

Crosswork Data Gateway には、ネットワークトラフィックのキャプチャと分析を可能にする tcpdump オプションがあります。

（注） このタスクは、**dg-admin** ユーザーのみが実行できます。

ステップ 1 [5 トラブルシューティング（5 Troubleshooting）] > [診断の実行（Run Diagnostics）] > [9 tcpdump] に移動します。

ステップ 2 tcpdump ユーティリティを実行するインターフェイスを選択します。すべてのインターフェイスに対して実行するには、[すべて（All）] オプションを選択します。

ステップ 3 適切なチェックボックスをオンにして、画面にパケット情報を表示するか、またはキャプチャしたパケットをファイルに保存します。

ステップ 4 次の詳細を入力して、[OK] をクリックします。

- パケット数の制限（Packet count limit）
- 収集時間の制限（Collection time limit）
- フルサイズの制限（File size limit）
- フィルタ式

選択したオプションに応じて、Crosswork Data Gateway はパケットキャプチャ情報を画面に表示するか、またはファイルに保存します。tcpdumpユーティリティが指定した制限に達すると、Crosswork Data Gatewayはファイルを圧縮し、ファイルをリモートホストに転送するための SCP クレデンシャルを要求します。転送が完了するか、または完了前にファイル転送をキャンセルする場合、圧縮したファイルは削除されます。

show-tech の実行

Crosswork Data Gateway は、ログファイルをユーザ定義の SCP の宛先にエクスポートするオプション **show_tech** を提供します。

次のようなデータが収集されます。

- Docker コンテナで実行されているすべての Data Gateway コンポーネントのログ
- VM バイタル

実行場所のディレクトリに tarball を作成します。出力は `DG-<CDG version>-<CDG host name>-year-month-day--hour-minute-second.tar.xz.enc` という名前の tarball です。

Crosswork Data Gateway の状態によって、このコマンドの実行に数分かかる場合があります。

ステップ 1 [トラブルシューティング（Troubleshooting）] メニューから [5 Show-tech] を選択し、[OK] をクリックします。

ステップ 2 ログとバイタルを含む tarball の保存先を入力します。

ステップ 3 SCP パスフレーズを入力し、[OK] をクリックします。

showtech ファイルは暗号化された形式でダウンロードされます。

（注） システムの使用時間によっては、showtech ファイルのダウンロードに数分かかる場合があります。

ステップ 4 ダウンロードが完了したら、次のコマンドを実行して復号します。

（注） ファイルを復号するには、OpenSSL バージョン 1.1.1i を使用する必要があります。システムの openssl バージョンを確認するには、`openssl version` コマンドを使用します。

MAC でファイルを復号するには、OpenSSL 1.1.1+ をインストールする必要があります。これは、LibreSSL の `openssl` コマンドが OpenSSL の `openssl` コマンドでサポートされているすべてのスイッチはサポートしていないためです。

```
openssl enc -d -AES-256-CBC -pbkdf2 -md sha512 -iter 100000 -in <showtech file> -out <decrypted
filename> -pass pass:<password>
```

Crosswork Data Gateway VM の再起動

（注） このタスクは、**dg-admin** ユーザのみが実行できます。

Crosswork Data Gateway には、VM を再起動するための 2 つのオプションがあります。

- [すべてのコレクタを削除してVMを再起動する（Remove all Collectors and Reboot VM）]：インストール後にダウンロードされたコンテナ（コレクタとオフロード）を停止して、Docker からイメージを削除し、コレクタデータと構成を削除して VM を再起動する場合は、[トラブルシューティング（Troubleshooting）] メニューからこのオプションを選択します。これにより、初期設定が完了した直後の、インフラストラクチャコンテナのみが実行されている状態に VM が戻ります。
- [VMの再起動（Reboot VM）]：通常の再起動の場合は、[トラブルシューティング（Troubleshooting）] メニューからこのオプションを選択します。

Crosswork Data Gateway VM のシャットダウン

[トラブルシューティング（Troubleshooting）] メニューから [5 VM のシャットダウン（5 Shutdown VM）] を選択して、Crosswork Data Gateway VM の電源をオフにします。

auditd ログのエクスポート

auditd ログをエクスポートするには、次の手順を実行します。

ステップ 1 [トラブルシューティング（Troubleshooting）] で、[9 監査ログのエクスポート（9 Export audit Logs）] を選択します。

ステップ 2 auditd ログの tarball 暗号化用のパスフレーズを入力します。

ステップ 3 [OK] をクリックします。

Crosswork Data Gateway の再登録

次の手順に従って Crosswork Data Gateway を再登録します。

始める前に

既存の Crosswork Data Gateway の登録は、再登録する前にコントローラから削除する必要があります。

ステップ 1 [トラブルシューティング（Troubleshooting）] メニューから、[7 Data Gatewayの再登録（7 Re-enroll Data Gateway）] を選択します。

ステップ 2 次のダイアログ ボックスで [Yes] をクリックします。

ローテーションされたログファイルの削除

この手順を使用して、`/var/log` および `/opt/dg/log` フォルダ内のローテーションされたすべてのログファイル（*.gz または *.xz）を削除します。

ステップ 1 [トラブルシューティング（Troubleshooting）] メニューから、[8ローテーションログファイルの削除（8 Remove Rotated Log files）] を選択します。

ステップ 2 表示されるダイアログで [はい（Yes）] を選択して、変更を保存します。

TAC シェルアクセスの有効化

TAC シェルアクセス機能を使用すると、シスコのエンジニアは、**dg-tac** という名前の予約済みのユーザを使用して、多要素認証によって Ubuntu シェルに直接ログインできます。

最初は、ユーザがシェルプロンプトを取得しないように**dg-tac**ユーザアカウントがロックされていて、パスワードが期限切れになっています。有効にすると、dg-tac ユーザは次の暦日の 12:00 a.m UTC（午前 0 時 UTC）までアクティブになります。これは 24 時間未満です。

dg-tac ユーザを有効にする手順は、次のとおりです。

（注） このアクセスを有効にするには、シスコのエンジニアに連絡する必要があります。

始める前に

シスコの担当エンジニアが SWIMS Aberto ツールにアクセスできることを確認してください。

ステップ 1 **dg-admin** ユーザとして Data Gateway VM にログインします。

ステップ 2 メインメニューから、[5 トラブルシューティング（5 Troubleshooting）] を選択します。

ステップ 3 [トラブルシューティング（Troubleshooting）] メニューから、[TACシェルアクセスの有効化（Enable TAC Shell Access）] を選択します。

dg-tac ユーザのログインには設定済みのパスワードと TAC からチャレンジトークンへの応答が必要であることを警告するダイアログが表示されます。この時点で有効化プロセスを停止するには [いいえ（No）] を、続行するには [はい（Yes）] を選択します。

ステップ 4 続行すると、使用する新しいパスワードの入力が求められ、アカウントが無効になる日が表示されます。

ステップ 5 コンソールメニューでアカウントのロックを解除するためのパスワードを入力します。

ステップ 6 Crosswork Data Gateway からログアウトします。

ステップ 7 シスコのエンジニアが Crosswork Data Gateway の VM に直接アクセスできる場合は、次の手順を実行します。それ以外の場合は、**手順 8** に進みます。

a) **dg-tac** ユーザーの手順 5 で設定したパスワードを、担当のシスコエンジニアと共有します。

b) 設定したパスワードを使用してシスコのエンジニアが **dg-tac** ユーザーとして SSH 経由でログインします。

パスワードを入力すると、チャレンジトークンが表示されます。シスコのエンジニアは、SWIMS Aberto ツールを使用してチャレンジトークンに署名し、署名済みの応答を Crosswork Data Gateway の VM でチャレンジトークンに貼り付けます。

c) シスコのエンジニアは **dg-tac** ユーザーとして正常にログインし、トラブルシューティングを実行します。

dg-tac ユーザのアイドルタイムアウト時間は 15 分間です。ログアウトした場合、シスコのエンジニアは、再度ログインするために新しいチャレンジに署名する必要があります。

d) トラブルシューティングが完了したら、シスコのエンジニアは TAC シェルからログアウトします。

ステップ 8 シスコのエンジニアが Crosswork Data Gateway の VM に直接アクセスできない場合は、デスクトップ共有を有効にしてシスコのエンジニアとのミーティングを開始します。

a) 次のコマンドを使用して、**dg-tac** ユーザとして SSH 経由でログインします。

```
ssh dg-tac @<DG hostname or IP>
```

b) **dg-tac** ユーザに設定したパスワードを入力します。

パスワードを入力すると、チャレンジトークンが表示されます。このトークンをシスコのエンジニアと共有します。そのシスコのエンジニアは SWIMS Aberto ツールを使用してトークンに署名し、応答を共有します。

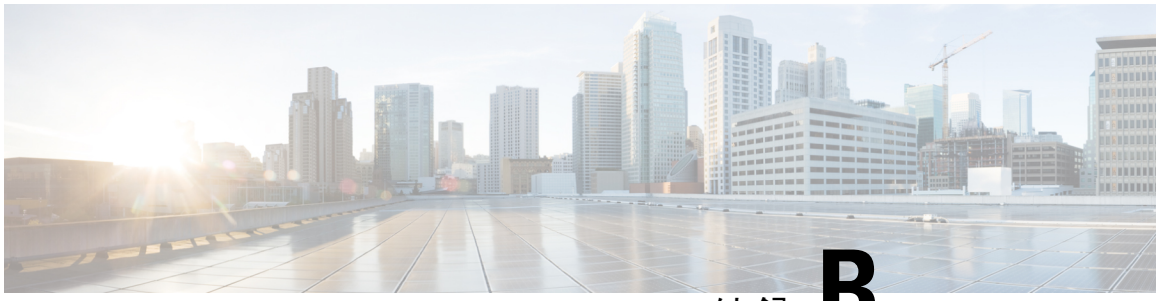
c) チャレンジトークンに対する署名付き応答を Crosswork Data Gateway VM に貼り付けます。Enter キーを押すとシェルプロンプトが表示されます。

d) トラブルシューティングを行うには、デスクトップを共有するか、またはシスコのエンジニアの指示に従います。

dg-tac ユーザのアイドルタイムアウト時間は 15 分間です。ログアウトした場合、シスコのエンジニアは、再度ログインするために新しいチャレンジに署名する必要があります。

e) トラブルシューティングが完了したら、TAC シェルからログアウトします。

Crosswork Data Gateway VM の設定



付録 B

SNMP での収集用に事前にロードしたトラップと MIB のリスト

この項では、Cisco Crosswork Data Gateway が SNMP 収集でサポートしているトラップと MIB を示します。

（注） このリストは、Crosswork がターゲットアプリケーションの場合にのみ適用され、ターゲットが外部アプリケーションの場合は制限されません。

次の制約事項に注意してください。

- システムは、概念テーブルの OID からインデックス値を抽出できません。概念テーブルのインデックスを定義する列のいずれかが入力されていない場合、インデックス値はデータプレーンで行のインスタンス識別子（oid サフィックス）に置き換えられます。
- システムは、**AUGMENT** キーワードを含む概念テーブルからインデックス値を抽出したり、他のテーブルのインデックスを参照したりすることはできません。
- （整数構文を使用した）名前付き数の列挙は、数値を使用して回線上で送信されます。

表 *50*：サポートされている トラップ

トラップ	OID
linkDown	1.3.6.1.6.3.1.1.5.3
linkUp	1.3.6.1.6.3.1.1.5.4
coldStart	1.3.6.1.6.3.1.1.5.1
isisAdjacencyChange	1.3.6.1.2.1.138.0.17

ADSL-LINE-MIB.mib	CISCO-LWAPP-INTERFACE-MIB.mib	IANA-ITU-ALARM-TC-MIB.mib

SNMP での収集用に事前にロードしたトラップと MIB のリスト

ADSL-TC-MIB.mib	CISCO-LWAPP- IPS-MIB.mib	IANA-LANGUAGE-MIB.mib
AGENTX-MIB.mib	CISCO-LWAPP-LINKTEST-MIB.mib	IANA-RTPROTO- MIB.mib
ALARM-MIB.mib	CISCO-LWAPP-LOCAL-AUTH-MIB.mib	IANAifType-MIB.mib
APS-MIB.mib	CISCO-LWAPP- MDNS-MIB.mib	IEEE8021-CFM-MIB.mib
ATM-FORUM-MIB.mib	CISCO-LWAPP-MESH-BATTERY-MIB.mib	IEEE8021-PAE-MIB.mib
ATM-FORUM- TC-MIB.mib	CISCO-LWAPP-MESH-LINKTEST-MIB.mib	IEEE8021-TC-MIB.mib
ATM-MIB.mib	CISCO-LWAPP-MOBILITY-EXT-MIB.mib	IEEE802171-CFM- MIB.mib
ATM-TC-MIB.mib	CISCO-LWAPP-MOBILITY-MIB.mib	IEEE8023-LAG-MIB.mib
ATM2-MIB.mib	CISCO-LWAPP-NETFLOW-MIB.mib	IEEE802dot11-MIB.mib
BGP4-MIB.mib	CISCO-LWAPP- REAP-MIB.mib	IF-INVERTED-STACK-MIB.mib
BRIDGE-MIB.mib	CISCO-LWAPP- RF-MIB.mib	IF-MIB.mib
CISCO-AAA- SERVER-MIB.mib	CISCO-LWAPP- SI-MIB.mib	IGMP-STD-MIB.mib
CISCO-AAA- SESSION-MIB.mib	CISCO-LWAPP- TC-MIB.mib	INET-ADDRESS-MIB.mib
CISCO-AAL5-MIB.mib	CISCO-LWAPP-TRUSTSEC-MIB.mib	INT-SERV-MIB.mib
CISCO-ACCESS-ENVMON-MIB.mib	CISCO-LWAPP- TSM-MIB.mib	INTEGRATED-SERVICES -MIB.mib
CISCO-ATM-EXT -MIB.mib	CISCO-LWAPP- WLAN-MIB.mib	IP-FORWARD-MIB.mib
CISCO-ATM-PVCTRAP-EXTN-MIB.mib	CISCO-LWAPP-WLAN -SECURITY-MIB.mib	IP-MIB.mib
CISCO-ATM- QOS-MIB.mib	CISCO-MEDIA-GATEWAY-MIB.mib	IPMCAST-MIB.mib
CISCO-AUTH-FRAMEWORK-MIB.mib	CISCO-MOTION-MIB.mib	IPMROUTE-MIB.mib
CISCO-BGP-POLICY -ACCOUNTING-MIB.mib	CISCO-MPLS-LSR -EXT-STD-MIB.mib	IPMROUTE-STD -MIB.mib
CISCO-BGP4-MIB.mib	CISCO-MPLS-TC -EXT-STD-MIB.mib	IPV6-FLOW-LABEL -MIB.mib
CISCO-BULK-FILE -MIB.mib	CISCO-MPLS-TE-STD -EXT-MIB.mib	IPV6-ICMP-MIB.mib

SNMP での収集用に事前にロードしたトラップと MIB のリスト

CISCO-CBP-TARGET -MIB.mib	CISCO-NAC-TC -MIB.mib	IPV6-MIB.mib
CISCO-CBP-TARGET -TC-MIB.mib	CISCO-NBAR-PROTOCOL -DISCOVERY-MIB.mib	IPV6-MLD-MIB.mib
CISCO-CBP-TC-MIB.mib	CISCO-NETSYNC -MIB.mib	IPV6-TC.mib
CISCO-CCME-MIB.mib	CISCO-NTP-MIB.mib	IPV6-TCP-MIB.mib
CISCO-CDP-MIB.mib	CISCO-OSPF- MIB.mib	IPV6-UDP-MIB.mib
CISCO-CEF-MIB.mib	CISCO-OSPF- TRAP-MIB.mib	ISDN-MIB.mib
CISCO-CEF-TC.mib	CISCO-OTN-IF-MIB.mib	ISIS-MIB.mib
CISCO-CLASS-BASED -QOS-MIB.mib	CISCO-PAE-MIB.mib	ITU-ALARM-MIB.mib
CISCO-CONFIG- COPY-MIB.mib	CISCO-PAGP-MIB.mib	ITU-ALARM-TC- MIB.mib
CISCO-CONFIG- MAN-MIB.mib	CISCO-PIM-MIB.mib	L2TP-MIB.mib
CISCO-CONTENT-ENGINE-MIB.mib	CISCO-PING-MIB.mib	LANGTAG-TC-MIB.mib
CISCO-CONTEXT-MAPPING-MIB.mib	CISCO-POLICY-GROUP -MIB.mib	LLDP-EXT-DOT1 -MIB.mib
CISCO-DATA -COLLECTION-MIB.mib	CISCO-POWER-ETHERNET-EXT-MIB.mib	LLDP-EXT-DOT3 -MIB.mib
CISCO-DEVICE-EXCEPTION -REPORTING-MIB.mib	CISCO-PRIVATE -VLAN-MIB.mib	LLDP-MIB.mib
CISCO-DIAL-CONTROL-MIB.mib	CISCO-PROCESS-MIB.mib	MAU-MIB.mib
CISCO-DOT11-ASSOCIATION-MIB.mib	CISCO-PRODUCTS- MIB.mib	MGMD-STD-MIB.mib
CISCO-DOT11-HT- PHY-MIB.mib	CISCO-PTP-MIB.mib	MPLS-FTN-STD- MIB.mib
CISCO-DOT11-IF-MIB.mib	CISCO-RADIUS- EXT-MIB.mib	MPLS-L3VPN-STD-MIB.mib
CISCO-DOT11-SSID-SECURITY-MIB.mib	CISCO-RF-MIB.mib	MPLS-LDP-ATM-STD-MIB.mib
CISCO-DOT3- OAM-MIB.mib	CISCO-RF-SUPPLEMENTAL -MIB.mib	MPLS-LDP-FRAME -RELAY-STD-MIB.mib
CISCO-DS3-MIB.mib	CISCO-RTTMON-TC -MIB.mib	MPLS-LDP-GENERIC-STD-MIB.mib
CISCO-DYNAMIC-TEMPLATE-MIB.mib	CISCO-SELECTIVE-VRF-DOWNLOAD-MIB.mib	MPLS-LDP-MIB.mib
CISCO-DYNAMIC -TEMPLATE-TC-MIB.mib	CISCO-SESS-BORDER-CTRLR -CALL-STATS-MIB.mib	MPLS-LDP-STD-MIB.mib
CISCO-EIGRP-MIB.mib	CISCO-SESS-BORDER-CTRLR-EVENT-MIB.mib	MPLS-LSR-MIB.mib

SNMP での収集用に事前にロードしたトラップと MIB のリスト

CISCO-EMBEDDED-EVENT-MGR-MIB.mib	CISCO-SESS-BORDER-CTRLR-STATS-MIB.mib	MPLS-LSR-STD-MIB.mib
CISCO-ENHANCED-IMAGE-MIB.mib	CISCO-SMI.mib	MPLS-TC-MIB.mib
CISCO-ENHANCED-MEMPOOL-MIB.mib	CISCO-SONET-MIB.mib	MPLS-TC-STD-MIB.mib
CISCO-ENTITY-ASSET -MIB.mib	CISCO-ST-TC.mib	MPLS-TE-MIB.mib
CISCO-ENTITY-EXT -MIB.mib	CISCO-STACKWISE- MIB.mib	MPLS-TE-STD-MIB.mib
CISCO-ENTITY-FRU-CONTROL-MIB.mib	CISCO-STP-EXTENSIONS -MIB.mib	MPLS-VPN-MIB.mib
CISCO-ENTITY- QFP-MIB.mib	CISCO-SUBSCRIBER -IDENTITY-TC-MIB.mib	MSDP-MIB.mib
CISCO-ENTITY-REDUNDANCY-MIB.mib	CISCO-SUBSCRIBER-SESSION-MIB.mib	NET-SNMP-AGENT -MIB.mib
CISCO-ENTITY-REDUNDANCY-TC-MIB.mib	CISCO-SUBSCRIBER-SESSION-TC-MIB.mib	NET-SNMP-EXAMPLES -MIB.mib
CISCO-ENTITY-SENSOR-MIB.mib	CISCO-SYSLOG-MIB.mib	NET-SNMP-MIB.mib
CISCO-ENTITY-VENDORTYPE-OID-MIB.mib	CISCO-SYSTEM-EXT- MIB.mib	NET-SNMP-TC.mib
CISCO-ENVMON-MIB.mib	CISCO-SYSTEM-MIB.mib	NHRP-MIB.mib
CISCO-EPM-NOTIFICATION-MIB.mib	CISCO-TAP2-MIB.mib	NOTIFICATION-LOG-MIB.mib
CISCO-ETHER-CFM- MIB.mib	CISCO-TC.mib	OLD-CISCO-CHASSIS-MIB.mib
CISCO-ETHERLIKE- EXT-MIB.mib	CISCO-TCP-MIB.mib	OLD-CISCO-INTERFACES -MIB.mib
CISCO-FABRIC- C12K-MIB.mib	CISCO-TEMP-LWAPP -DHCP-MIB.mib	OLD-CISCO-SYS- MIB.mib
CISCO-FIREWALL -TC.mib	CISCO-TRUSTSEC -SXP-MIB.mib	OLD-CISCO-SYSTEM -MIB.mib
CISCO-FLASH-MIB.mib	CISCO-TRUSTSEC -TC-MIB.mib	OPT-IF-MIB.mib
CISCO-FRAME- RELAY-MIB.mib	CISCO-UBE-MIB.mib	OSPF-MIB.mib
CISCO-FTP-CLIENT -MIB.mib	CISCO-UNIFIED-COMPUTING-ADAPTOR -MIB.mib	OSPF-TRAP-MIB.mib
CISCO-HSRP-EXT -MIB.mib	CISCO-UNIFIED-COMPUTING-COMPUTE -MIB.mib	OSPFV3-MIB.mib

SNMP での収集用に事前にロードしたトラップと MIB のリスト

CISCO-HSRP-MIB.mib	CISCO-UNIFIED-COMPUTING-ETHER -MIB.mib	P-BRIDGE-MIB.mib
CISCO-IETF-ATM2 -PVCTRAP-MIB.mib	CISCO-UNIFIED-COMPUTING-FC- MIB.mib	PIM-MIB.mib
CISCO-IETF-BFD -MIB.mib	CISCO-UNIFIED-COMPUTING-MEMORY -MIB.mib	PIM-STD-MIB.mib
CISCO-IETF-FRR -MIB.mib	CISCO-UNIFIED- COMPUTING -MIB.mib	POWER-ETHERNET -MIB.mib
CISCO-IETF-IPMROUTE -MIB.mib	CISCO-UNIFIED-COMPUTING-NETWORK -MIB.mib	PPP-IP-NCP-MIB.mib
CISCO-IETF-ISIS -MIB.mib	CISCO-UNIFIED-COMPUTING-PROCESSOR -MIB.mib	PPP-LCP-MIB.mib
CISCO-IETF-MPLS-ID -STD-03-MIB.mib	CISCO-UNIFIED-COMPUTING-TC- MIB.mib	PPVPN-TC-MIB.mib
CISCO-IETF-MPLS-TE-EXT-STD-03- MIB.mib	CISCO-VLAN-IFTABLE-RELATIONSHIP -MIB.mib	PTOPO-MIB.mib
CISCO-IETF-MPLS-TE-P2MP-STD-MIB.mib	CISCO-VLAN-MEMBERSHIP-MIB.mib	PerfHist-TC-MIB.mib
CISCO-IETF-MSDP -MIB.mib	CISCO-VOICE-COMMON -DIAL-CONTROL-MIB.mib	Q-BRIDGE-MIB.mib
CISCO-IETF-PIM-EXT -MIB.mib	CISCO-VOICE-DIAL -CONTROL-MIB.mib	RADIUS-ACC-CLIENT -MIB.mib
CISCO-IETF-PIM -MIB.mib	CISCO-VOICE-DNIS -MIB.mib	RADIUS-AUTH-CLIENT -MIB.mib
CISCO-IETF-PW- ATM-MIB.mib	CISCO-VPDN-MGMT -MIB.mib	RFC-1212.mib
CISCO-IETF-PW- ENET-MIB.mib	CISCO-VTP-MIB.mib	RFC-1215.mib
CISCO-IETF-PW-MIB.mib	CISCO-WIRELESS-NOTIFICATION-MIB.mib	RFC1155-SMI.mib
CISCO-IETF-PW- MPLS-MIB.mib	CISCOSB-DEVICEPARAMS -MIB.mib	RFC1213-MIB.mib
CISCO-IETF-PW -TC-MIB.mib	CISCOSB-HWENVIROMENT.mib	RFC1315-MIB.mib
CISCO-IETF-PW -TDM-MIB.mib	CISCOSB-MIB.mib	RFC1398-MIB.mib
CISCO-IETF-VPLS -BGP-EXT-MIB.mib	CISCOSB-Physicaldescription -MIB.mib	RIPv2-MIB.mib
CISCO-IETF-VPLS -GENERIC-MIB.mib	DIAL-CONTROL-MIB.mib	RMON-MIB.mib

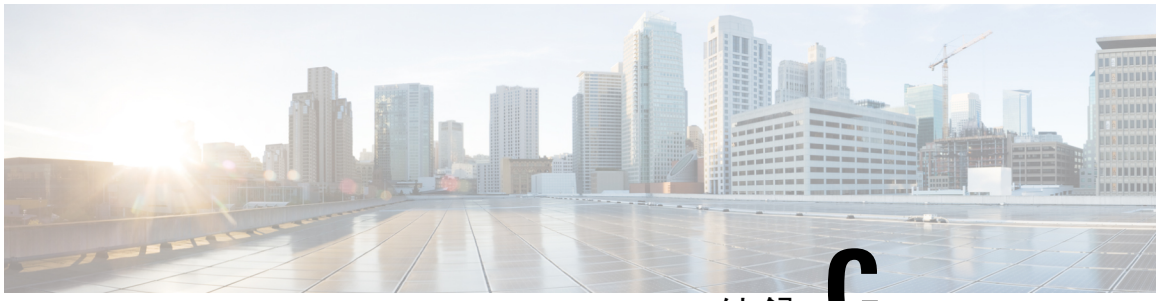
SNMP での収集用に事前にロードしたトラップと MIB のリスト

CISCO-IETF-VPLS- LDP-MIB.mib	DIFFSERV-DSCP-TC.mib	RMON2-MIB.mib
CISCO-IF-EXTENSION -MIB.mib	DIFFSERV-MIB.mib	RSTP-MIB.mib
CISCO-IGMP-FILTER -MIB.mib	DISMAN-NSLOOKUP -MIB.mib	RSVP-MIB.mib
CISCO-IMAGE-LICENSE -MGMT-MIB.mib	DISMAN-PING-MIB.mib	SMON-MIB.mib
CISCO-IMAGE-MIB.mib	DISMAN-SCHEDULE -MIB.mib	SNA-SDLC-MIB.mib
CISCO-IMAGE-TC.mib	DISMAN-SCRIPT-MIB.mib	SNMP-COMMUNITY -MIB.mib
CISCO-IP-LOCAL-POOL-MIB.mib	DISMAN-TRACEROUTE -MIB.mib	SNMP-FRAMEWORK -MIB.mib
CISCO-IP-TAP-MIB.mib	DOT3-OAM-MIB.mib	SNMP-MPD-MIB.mib
CISCO-IP-URPF-MIB.mib	DRAFT-MSDP-MIB.mib	SNMP-NOTIFICATION -MIB.mib
CISCO-IPMROUTE- MIB.mib	DS0-MIB.mib	SNMP-PROXY-MIB.mib
CISCO-IPSEC-FLOW -MONITOR-MIB.mib	DS1-MIB.mib	SNMP-REPEATER -MIB.mib
CISCO-IPSEC-MIB.mib	DS3-MIB.mib	SNMP-TARGET-MIB.mib
CISCO-IPSEC-POLICY -MAP-MIB.mib	ENTITY-MIB.mib	SNMP-USER-BASED -SM-MIB.mib
CISCO-IPSLA-AUTOMEASURE-MIB.mib	ENTITY-SENSOR-MIB.mib	SNMP-USM-AES -MIB.mib
CISCO-IPSLA- ECHO-MIB.mib	ENTITY-STATE-MIB.mib	SNMP-USM-DH-OBJECTS-MIB.mib
CISCO-IPSLA- JITTER-MIB.mib	ENTITY-STATE- TC-MIB.mib	SNMP-VIEW-BASED-ACM-MIB.mib
CISCO-IPSLA- TC-MIB.mib	ESO-CONSORTIUM -MIB.mib	SNMPv2-CONF.mib
CISCO-ISDN-MIB.mib	ETHER-WIS.mib	SNMPv2-MIB.mib
CISCO-LICENSE-MGMT-MIB.mib	EtherLike-MIB.mib	SNMPv2-SMI.mib
CISCO-LOCAL-AUTH-USER-MIB.mib	FDDI-SMT73-MIB.mib	SNMPv2-TC-v1.mib
CISCO-LWAPP- AAA-MIB.mib	FR-MFR-MIB.mib	SNMPv2-TC.mib
CISCO-LWAPP- AP-MIB.mib	FRAME-RELAY -DTE-MIB.mib	SNMPv2-TM.mib
CISCO-LWAPP-CCX-RM-MIB.mib	FRNETSERV- MIB.mib	SONET-MIB.mib
CISCO-LWAPP- CDP-MIB.mib	GMPLS-LSR- STD-MIB.mib	SYSAPPL-MIB.mib
CISCO-LWAPP-CLIENT -ROAMING-CAPABILITY.mib	GMPLS-TC-STD- MIB.mib	TCP-MIB.mib

SNMP での収集用に事前にロードしたトラップと MIB のリスト

CISCO-LWAPP-CLIENT -ROAMING-MIB.mib	GMPLS-TE-STD-MIB.mib	TOKEN-RING-RMON -MIB.mib
CISCO-LWAPP-DHCP -MIB.mib	HC-PerfHist-TC-MIB.mib	TOKENRING-MIB.mib
CISCO-LWAPP-DOT11-CLIENT-CALIB-MIB.mib	HC-RMON-MIB.mib	TRANSPORT-ADDRESS -MIB.mib
CISCO-LWAPP-DOT11-CLIENT-CCX-TC-MIB.mib	HCNUM-TC.mib	TUNNEL-MIB.mib
CISCO-LWAPP-DOT11 -LDAP-MIB.mib	HOST-RESOURCES -MIB.mib	UDP-MIB.mib
CISCO-LWAPP- DOT11-MIB.mib	HOST-RESOURCES -TYPES.mib	VPN-TC-STD-MIB.mib
CISCO-LWAPP -DOWNLOAD-MIB.mib	IANA-ADDRESS-FAMILY-NUMBERS-MIB.mib	VRRP-MIB.mib
CISCO-LWAPP- IDS-MIB.mib	IANA-GMPLS-TC-MIB.mib	

SNMP での収集用に事前にロードしたトラップと MIB のリスト



付録 C

MDTでの収集用に事前にロードしたYANGモジュールのリスト

ここでは、Cisco Crosswork Data Gateway が Cisco IOS XR デバイスの MDT による収集をサポートする YANG モジュールのリストを示します。

cli_xr_bgp_oper.yang	Cisco-IOS-XR-ip-bfd-oper.yang
Cisco-IOS-XR-ipv4-bgp-oper.yang	Cisco-IOS-XR-asr9k-xbar-oper.yang
Cisco-IOS-XR-ipv4-acl-oper.yang	Cisco-IOS-XR-snmp-sensormib-oper.yang
Cisco-IOS-XR-shellutil-filesystem-oper.yang	Cisco-IOS-XR-config-cfgmgr-oper.yang
Cisco-IOS-XR-infra-alarm-logger-oper.yang	Cisco-IOS-XR-infra-fti-oper.yang
Cisco-IOS-XR-icpe-infra-oper.yang	Cisco-IOS-XR-dot1x-oper.yang
Cisco-IOS-XR-fretta-bcm-dpa-stats-oper.yang	Cisco-IOS-XR-sdr-invmgr-diag-oper.yang
Cisco-IOS-XR-cofo-infra-oper.yang	Cisco-IOS-XR-wanphy-ui-oper.yang
Cisco-IOS-XR-man-ems-oper.yang	Cisco-IOS-XR-bundlemgr-oper.yang
Cisco-IOS-XR-mpls-lsd-oper.yang	Cisco-IOS-XR-l2vpn-oper.yang
Cisco-IOS-XR-show-fpd-loc-ng-oper.yang	Cisco-IOS-XR-asr9k-qos-oper.yang
Cisco-IOS-XR-telemetry-model-driven-oper.yang	Cisco-IOS-XR-segment-routing-ms-oper.yang
Cisco-IOS-XR-shellutil-oper.yang	Cisco-IOS-XR-pfi-im-cmd-oper.yang
Cisco-IOS-XR-ip-iep-oper.yang	Cisco-IOS-XR-asic-errors-oper.yang
Cisco-IOS-XR-cdp-oper.yang	Cisco-IOS-XR-lib-keychain-oper.yang
Cisco-IOS-XR-ip-sbfd-oper.yang	Cisco-IOS-XR-sdr-invmgr-oper.yang
Cisco-IOS-XR-tty-management-cmd-oper.yang	Cisco-IOS-XR-ipv4-ospf-oper.yang
Cisco-IOS-XR-upgrade-fpd-oper.yang	Cisco-IOS-XR-pfm-oper.yang
Cisco-IOS-XR-crypto-macsec-secy-oper.yang	Cisco-IOS-XR-config-valid-ccv-oper.yang
Cisco-IOS-XR-ip-iarm-v6-oper.yang	Cisco-IOS-XR-ip-iarm-v4-oper.yang
Cisco-IOS-XR-ipv4-autorp-oper.yang	Cisco-IOS-XR-infra-statsd-oper.yang

MDT での収集用に事前にロードした YANG モジュールのリスト

Cisco-IOS-XR-pbr-vservice-ea-oper.yang	Cisco-IOS-XR-ipv4-vrrp-oper.yang
Cisco-IOS-XR-ip-domain-oper.yang	Cisco-IOS-XR-cmproxy-oper.yang
Cisco-IOS-XR-ipv4-io-oper.yang	Cisco-IOS-XR-crypto-ssh-oper.yang
Cisco-IOS-XR-ipv4-hsrp-oper.yang	Cisco-IOS-XR-controller-optics-oper.yang
Cisco-IOS-XR-freqsync-oper.yang	Cisco-IOS-XR-atm-vcm-oper.yang
Cisco-IOS-XR-aaa-diameter-oper.yang	Cisco-IOS-XR-dnx-driver-fabric-plane-oper.yang
Cisco-IOS-XR-ip-tcp-oper.yang	Cisco-IOS-XR-asr9k-lc-fca-oper.yang
Cisco-IOS-XR-drivers-media-eth-oper.yang	Cisco-IOS-XR-mpls-vpn-oper.yang
Cisco-IOS-XR-infra-policymgr-oper.yang	Cisco-IOS-XR-asr9k-sc-envmon-oper.yang
Cisco-IOS-XR-fretta-bcm-dpa-hw-resources-oper.yang	Cisco-IOS-XR-es-acl-oper.yang
Cisco-IOS-XR-subscriber-ipsub-oper.yang	Cisco-IOS-XR-evpn-oper.yang
Cisco-IOS-XR-infra-rsi-oper.yang	Cisco-IOS-XR-rptiming-tmg-oper.yang
Cisco-IOS-XR-prm-server-oper.yang	Cisco-IOS-XR-ethernet-lldp-oper.yang
Cisco-IOS-XR-l2rib-oper.yang	Cisco-IOS-XR-ip-ntp-oper.yang
Cisco-IOS-XR-subscriber-pppoe-ma-oper.yang	Cisco-IOS-XR-mediasvr-linux-oper.yang
Cisco-IOS-XR-ocni-local-routing-oper.yang	Cisco-IOS-XR-ipv6-ma-oper.yang
Cisco-IOS-XR-reboot-history-oper.yang	Cisco-IOS-XR-infra-rmf-oper.yang
Cisco-IOS-XR-asr9k-lpts-oper.yang	Cisco-IOS-XR-infra-correlator-oper.yang
Cisco-IOS-XR-infra-serg-oper.yang	Cisco-IOS-XR-mpls-static-oper.yang
Cisco-IOS-XR-rgmgr-oper.yang	Cisco-IOS-XR-snmp-entitymib-oper.yang
Cisco-IOS-XR-ncs1k-mxp-headless-oper.yang	Cisco-IOS-XR-pbr-vservice-mgr-oper.yang
Cisco-IOS-XR-aaa-nacm-oper.yang	Cisco-IOS-XR-pfi-im-cmd-ctrlr-oper.yang
Cisco-IOS-XR-infra-rcmd-oper.yang	Cisco-IOS-XR-fretta-bcm-dpa-resources-oper.yang
Cisco-IOS-XR-crypto-macsec-mka-oper.yang	Cisco-IOS-XR-macsec-ctrlr-oper.yang
Cisco-IOS-XR-tunnel-vpdn-oper.yang	Cisco-IOS-XR-ipv6-nd-oper.yang
Cisco-IOS-XR-ipv4-dhcpd-oper.yang	Cisco-IOS-XR-tunnel-l2tun-oper.yang
Cisco-IOS-XR-ip-rip-oper.yang	Cisco-IOS-XR-infra-dumper-exception-oper.yang
Cisco-IOS-XR-ncs1001-otdr-oper.yang	Cisco-IOS-XR-syncc-oper.yang
Cisco-IOS-XR-asr9k-asic-errors-oper.yang	Cisco-IOS-XR-dnx-driver-oper.yang
Cisco-IOS-XR-pmengine-oper.yang	Cisco-IOS-XR-ncs1k-macsec-ea-oper.yang
Cisco-IOS-XR-linux-os-reboot-history-oper.yang	Cisco-IOS-XR-fretta-bcm-dpa-drop-stats-oper.yang
Cisco-IOS-XR-ppp-ea-oper.yang	Cisco-IOS-XR-infra-sla-oper.yang
Cisco-IOS-XR-asr9k-ptp-pd-oper.yang	Cisco-IOS-XR-ncs1001-ots-oper.yang

MDT での収集用に事前にロードした YANG モジュールのリスト

Cisco-IOS-XR-ipv4-igmp-oper.yang	Cisco-IOS-XR-nto-misc-shmem-oper.yang
Cisco-IOS-XR-ipv4-bgp-oc-oper.yang	Cisco-IOS-XR-ip-rib-ipv4-oper.yang
Cisco-IOS-XR-ip-pfilter-oper.yang	Cisco-IOS-XR-ipv4-pim-oper.yang
Cisco-IOS-XR-lpts-pre-ifib-oper.yang	Cisco-IOS-XR-pppoe-ea-oper.yang
Cisco-IOS-XR-ipv6-ospfv3-oper.yang	Cisco-IOS-XR-infra-syslog-oper.yang
Cisco-IOS-XR-asr9k-netflow-oper.yang	Cisco-IOS-XR-crypto-sam-oper.yang
Cisco-IOS-XR-infra-xtc-oper.yang	Cisco-IOS-XR-Ethernet-SPAN-oper.yang
Cisco-IOS-XR-sysdb-oper.yang	Cisco-IOS-XR-lpts-ifib-oper.yang
Cisco-IOS-XR-lib-mpp-oper.yang	Cisco-IOS-XR-ethernet-link-oam-oper.yang
Cisco-IOS-XR-infra-xtc-agent-oper.yang	Cisco-IOS-XR-mpls-ldp-oper.yang
Cisco-IOS-XR-ip-rib-ipv6-oper.yang	Cisco-IOS-XR-tty-management-oper.yang
Cisco-IOS-XR-rptiming-dti-oper.yang	Cisco-IOS-XR-lmp-oper.yang
Cisco-IOS-XR-wd-oper.yang	Cisco-IOS-XR-nto-misc-shprocmem-oper.yang
Cisco-IOS-XR-man-xml-ttyagent-oper.yang	Cisco-IOS-XR-procmem-oper.yang
Cisco-IOS-XR-ip-daps-oper.yang	Cisco-IOS-XR-Subscriber-infra-subdb-oper.yang
Cisco-IOS-XR-spirit-install-instmgr-oper.yang	Cisco-IOS-XR-asr9k-np-oper.yang
Cisco-IOS-XR-fretta-grid-svr-oper.yang	Cisco-IOS-XR-ptp-oper.yang
Cisco-IOS-XR-clns-isis-oper.yang	Cisco-IOS-XR-tunnel-nve-oper.yang
Cisco-IOS-XR-ipv4-bgp-oper.yang	Cisco-IOS-XR-ocni-oper.yang
Cisco-IOS-XR-ipv4-ma-oper.yang	Cisco-IOS-XR-ncs6k-acl-oper.yang
Cisco-IOS-XR-l2-eth-infra-oper.yang	Cisco-IOS-XR-manageability-object-tracking-oper.yang
Cisco-IOS-XR-plat-chas-invmgr-oper.yang	Cisco-IOS-XR-ocni-intfbase-oper.yang
Cisco-IOS-XR-dwdm-ui-oper.yang	Cisco-IOS-XR-infra-tc-oper.yang
Cisco-IOS-XR-policy-repository-oper.yang	Cisco-IOS-XR-subscriber-session-mon-oper.yang
Cisco-IOS-XR-ipv6-new-dhcpv6d-oper.yang	Cisco-IOS-XR-ip-udp-oper.yang
Cisco-IOS-XR-subscriber-srg-oper.yang	Cisco-IOS-XR-ipv6-acl-oper.yang
Cisco-IOS-XR-manageability-perfmgmt-oper.yang	Cisco-IOS-XR-crypto-macsec-pl-oper.yang
Cisco-IOS-XR-dnx-port-mapper-oper.yang	Cisco-IOS-XR-aaa-tacacs-oper.yang
Cisco-IOS-XR-mpls-te-oper.yang	Cisco-IOS-XR-man-ipsla-oper.yang
Cisco-IOS-XR-nto-misc-oper.yang	Cisco-IOS-XR-invmgr-oper.yang
Cisco-IOS-XR-ppp-ma-oper.yang	Cisco-IOS-XR-ipv4-arp-oper.yang
Cisco-IOS-XR-config-cfgmgr-exec-oper.yang	Cisco-IOS-XR-aaa-locald-oper.yang
Cisco-IOS-XR-perf-meas-oper.yang	Cisco-IOS-XR-ha-eem-policy-oper.yang

MDT での収集用に事前にロードした YANG モジュールのリスト

Cisco-IOS-XR-snmp-agent-oper.yang	Cisco-IOS-XR-ascii-ltrace-oper.yang
Cisco-IOS-XR-asr9k-lc-ethctrl-oper.yang	Cisco-IOS-XR-skp-qos-oper.yang
Cisco-IOS-XR-ifmgr-oper.yang	Cisco-IOS-XR-flowspec-oper.yang
Cisco-IOS-XR-iedge4710-oper.yang	Cisco-IOS-XR-icpe-sdacp-oper.yang
Cisco-IOS-XR-controller-otu-oper.yang	Cisco-IOS-XR-fretta-bcm-dpa-npu-stats-oper.yang
Cisco-IOS-XR-subscriber-accounting-oper.yang	Cisco-IOS-XR-alarmgr-server-oper.yang
Cisco-IOS-XR-ncs5500-qos-oper.yang	Cisco-IOS-XR-fia-internal-tcam-oper.yang
Cisco-IOS-XR-skywarp-netflow-oper.yang	Cisco-IOS-XR-tty-server-oper.yang
Cisco-IOS-XR-ncs1k-mxp-lldp-oper.yang	Cisco-IOS-XR-qos-ma-oper.yang
Cisco-IOS-XR-fib-common-oper.yang	Cisco-IOS-XR-aaa-protocol-radius-oper.yang
Cisco-IOS-XR-dnx-netflow-oper.yang	Cisco-IOS-XR-platform-pifib-oper.yang
Cisco-IOS-XR-lpts-pa-oper.yang	Cisco-IOS-XR-asr9k-fsi-oper.yang
Cisco-IOS-XR-ncs1k-mxp-oper.yang	Cisco-IOS-XR-ncs5500-coherent-node-oper.yang
Cisco-IOS-XR-asr9k-sc-invmgr-oper.yang	Cisco-IOS-XR-snmp-ifmib-oper.yang
Cisco-IOS-XR-ptp-pd-oper.yang	Cisco-IOS-XR-ip-mobileip-oper.yang
Cisco-IOS-XR-ethernet-cfm-oper.yang	Cisco-IOS-XR-wdsysmon-fd-oper.yang
Cisco-IOS-XR-pbr-oper.yang	Cisco-IOS-XR-infra-objmgr-oper.yang
Cisco-IOS-XR-ip-rsvp-oper.yang	Cisco-IOS-XR-ipv6-io-oper.yang
Cisco-IOS-XR-terminal-device-oper.yang	Cisco-IOS-XR-plat-chas-invmgr-ng-oper.yang
Cisco-IOS-XR-mpls-oam-oper.yang	Cisco-IOS-XR-ncs5500-coherent-portmode-oper.yang
Cisco-IOS-XR-sse-span-oper.yang	Cisco-IOS-XR-infra-dumper-oper.yang
Cisco-IOS-XR-asr9k-sc-diag-oper.yang	Cisco-IOS-XR-mpls-io-oper.yang

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