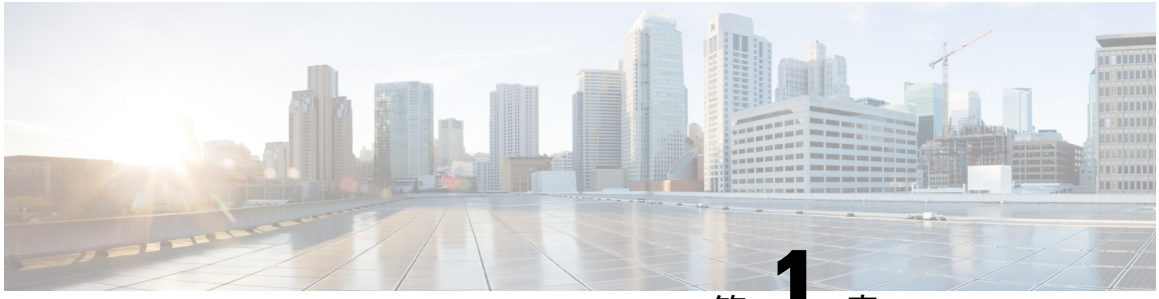
Cisco Crosswork Planning 7.0 収集の設定と管理

最終更新：2025 年 3 月 18 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

概要

本書は、Cisco Crosswork Planning コレクタアプリケーションを起動して実行するために必要な手順を説明することを目的とした、インストール後に使用するドキュメントです。仕様に従ってネットワークモデルを生成するようにコレクタを設定する方法について説明します。

この章は次のトピックで構成されています。

Cisco Crosswork Planning の概要

Cisco Crosswork Planning は、Cisco Crosswork infrastructure 上で実行される、Cisco Crosswork Network Automation 製品スイートの一部です。

Cisco Crosswork Planning は、ネットワークとそのネットワーク上のトラフィックデマンドの継続的なモニタリングと分析を通じて、現在のネットワークのモデルを作成および維持するためのツールを提供します。このネットワークモデルには、トポロジ、設定、トラフィック情報など、特定の時点でのネットワークに関するすべての関連情報が含まれています。この情報は、トラフィック要求、パス、ノードとリンクの障害、ネットワークの最適化、またはその他の変更によるネットワークへの影響を分析するための基礎として使用できます。

Cisco Crosswork Planning の重要な機能の一部を次に示します。

- トラフィックエンジニアリングおよびネットワークの最適化：サービスレベル要件を満たすように TE LSP 設定を計算し、キャパシティ管理を実行し、ローカルまたはグローバルの最適化を実行して、展開されたネットワークリソースの効率を最大化します。
- デマンドエンジニアリング：ネットワーク上のトラフィック需要の追加、削除、または変更がネットワーク トラフィック フローに与える影響を調べます。

- トポロジと予測分析：設計またはネットワーク障害によって引き起こされるネットワークトポロジの変更がネットワークパフォーマンスに与える影響を観察します。
- TE トンネルプログラミング：トンネルパスや予約帯域幅などのトンネルパラメータを変更した場合の影響を調べます。
- サービスクラス（CoS）対応のオンデマンド帯域幅：既存のネットワークトラフィックと需要を調べ、ルータ間で一連のサービスクラス固有の需要を許可します。

Cisco Crosswork Planning は、次のサーバーコンポーネントで構成されます。各コンポーネントは互いに独立して実行され、要件に基づいて有効化または無効化できます。

- **Cisco Crosswork Planning Collector**

  Cisco Crosswork Planning Collector は、ネットワークとそのネットワーク上のトラフィックデマンドの継続的なモニタリングと分析を通じて、現在のネットワークのモデルを作成、維持、およびアーカイブする一連のサービスで構成されます。

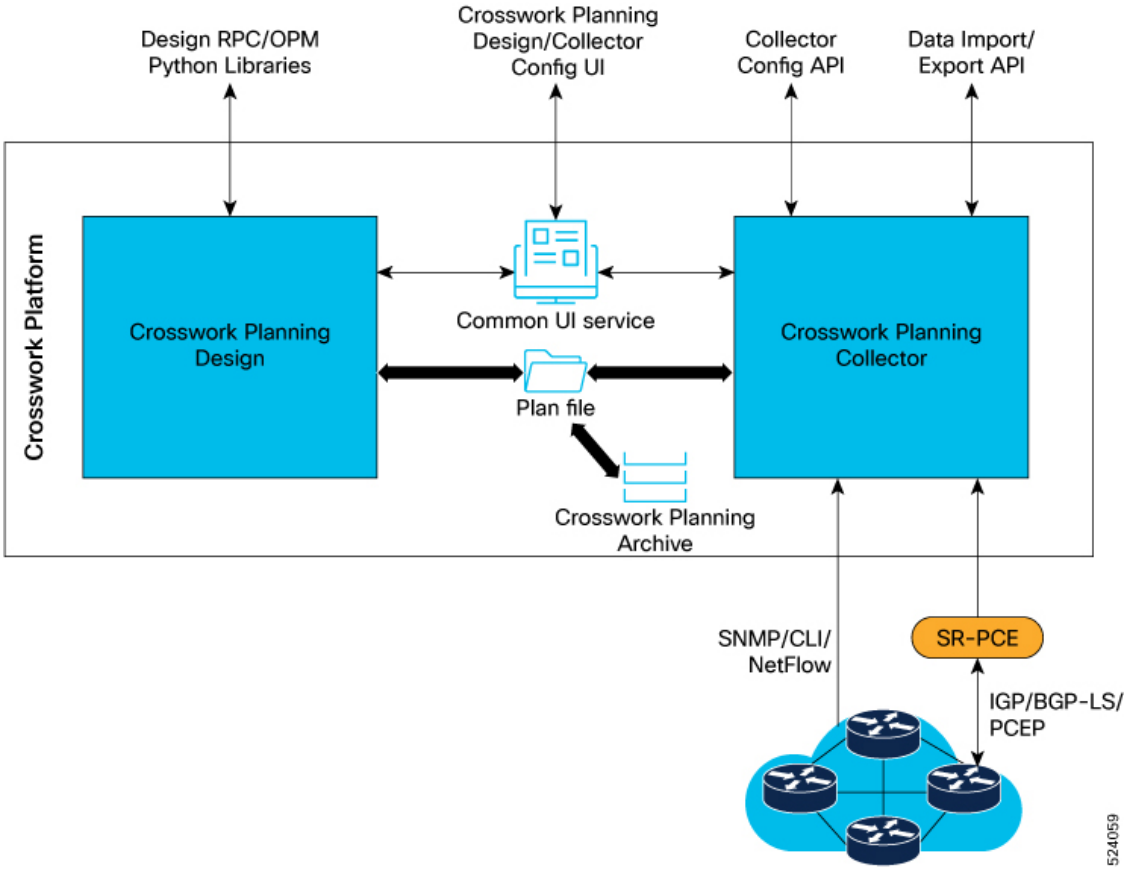
- **Cisco Crosswork Planning Design**

  Cisco Crosswork Planning Design は、ネットワークエンジニアやオペレータがネットワークの成長を予測し、障害をシミュレートし、また、コストを最小限に抑えながらパフォーマンス目標を達成して設計を最適化するのに役立つネットワーク設計および計画ツールです。

システム概要

Cisco Crosswork Planning は Crosswork インフラストラクチャで実行されます。Cisco Crosswork Planning Design アプリケーションと Cisco Crosswork Planning Collector アプリケーションは個別のコンポーネントとしてパッケージ化されており、要件に応じて有効/無効にできます。これら2つのアプリケーションは、互いに独立して実行されます。ネットワークモデルをインポートするための、Cisco Crosswork Planning Design と Cisco Crosswork Planning Collector のアーカイブ間の通信は、明確に定義された API を介して行われます。

図 *1* : システム概要



Cisco Crosswork Planning のコレクタ

コレクタは、抽象ネットワークモデルの一部を作成するパッケージであり、そのためにネットワークにクエリを実行します。ほとんどのコレクタは次のように動作します。

1. 送信元ネットワークモデル（または単に送信元モデル）を読み取ります。
2. 実際のネットワークから取得した情報で送信元モデルを拡張します。
3. 結果のモデルを使用して接続先ネットワークモデル（または単に接続先モデル）を生成します。

Cisco Crosswork Planning には、次のような複数のコレクタが含まれています。

- **トポロジコレクタ**：SNMP クエリおよび SR-PCE によって強化された IGP データベースを検出し、これに基づいたトポロジ情報（ノード、インターフェイス、回路）を使用して、基本的なネットワークモデルを作成します。トポロジコレクタには送信元モデルがありません。

- **LSP コレクタ**：LSP 情報で送信元モデルを強化し、追加情報で接続先モデルを生成します。
- **トラフィックコレクタ**：ネットワークからポーリングされたトラフィック統計で送信元モデルを強化し、追加情報で新しい接続先モデルを生成します。
- **レイアウトコレクタ**：送信元モデルにレイアウトプロパティを追加して、可視化を改善します。追加のレイアウト情報を使用して、新しい接続先モデルを生成します。コレクタはレイアウトプロパティの変更を記録するため、送信元モデルが変更され、接続先モデルが更新されると、それに応じて接続先モデルのレイアウトプロパティが更新されます。

Cisco Crosswork Planning でサポートされるすべてのコレクタを網羅したリストについては、コレクタの説明 （53 ページ）を参照してください。

ネットワークモデルとプランファイル

Cisco Crosswork Planning Collector アプリケーションは、ネットワークモデルを生成します。ネットワークモデルは、さまざまなコレクタからの情報を組み合わせて、実際のネットワークから構築できます。モデル構築チェーンは、必要な情報を備えたネットワークモデルを生成するように編成された収集の配置です。ネットワークモデルはプランファイル（.pln 形式）で保存され、Cisco Crosswork Planning Design アプリケーションからダウンロードまたは表示できます。

コレクタの集約

Cisco Crosswork Planning では、次のアグリゲータを使用して 2 つのレベルのデータ集約（統合）が行われます。

- デルタ集約ルールエンジン（DARE） （4 ページ）
- 単純な集約エンジン（SAgE） （4 ページ）

詳細については、次のトピックを参照してください。

デルタ集約ルールエンジン（DARE）

DARE アグリゲータは、さまざまなコレクタを 1 つにまとめ、それぞれからモデル情報を選択し、その情報を単一のモデルに統合する Cisco Crosswork Planning コンポーネントです。DARE の主な機能は、すべてのトポロジコレクタのデータを統合することです。

単純な集約エンジン（SAgE）

Simple Aggregation Engine（SAgE）は、トラフィック、インベントリ、レイアウト、マルチキャスト、NetFlow、デマンドなどのすべてのネットワーク情報を統合する Cisco Crosswork Planning

コンポーネントです。SAgE により、これらの変更が、DARE ネットワークからのトポロジ変更とともに最終的なネットワークに集約されます。すべてのコレクタからのネットワーク情報がプランファイルに書き込まれます。ネットワークの変更は、SAgEからアーカイブできます。

SAgE アグリゲータを使用すると、トラフィック収集、インベントリ収集、レイアウトなどを並行して実行できます。

デフォルトでは、すべてのコレクタがコレクタの設定時に集約に含まれます。収集のスケジュール時に、任意のコレクタを集約から除外できます。詳細については、集約コレクタの出力（43 ページ）を参照してください。

ネットワークモデルの生成

ネットワークモデルは、集約の各レベルが完了すると生成されます。最初のモデルは、DARE 集約の出力として生成されます（デルタ集約ルールエンジン（DARE）（4 ページ）を参照）。このファイルは、トラフィック、インベントリ、レイアウト、NetFlow、デマンドなどのコンポーネントによってデータソースとして使用されます。SAgE 集約が完了すると（単純な集約エンジン（SAgE）（4 ページ）を参照）、2 番目のファイルである最終ネットワークモデルが生成されます。これは、集約された収集データの最終出力です。

ログインとログアウト

Cisco Crosswork Planning はブラウザベースのアプリケーションです。サポートされているブラウザのバージョンの詳細については、*Cisco Crosswork Planning 7.0* インストールガイドの「サポートされている Web ブラウザ」の項を参照してください。

Cisco Crosswork Planning をインストールすると、次の手順を使用して Cisco Crosswork Planning UI にアクセスできます。

手順

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/
```

ブラウザから Cisco Crosswork Planning 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 Planning サーバーを受け入れます。

ステップ 2 Cisco Crosswork Planning 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。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。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（Login）] 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（Logout）] を選択します。

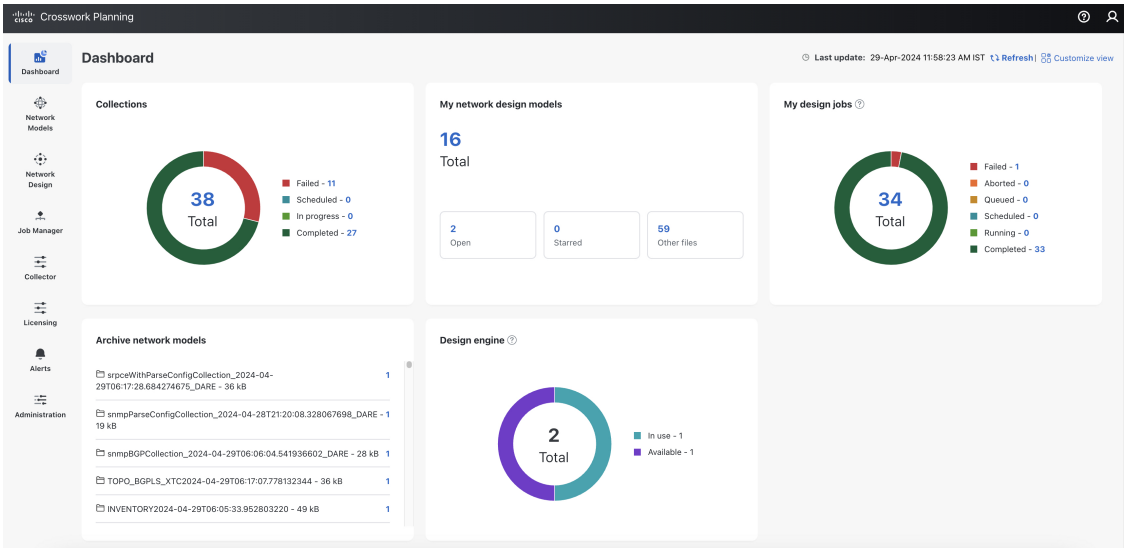
（注）
プランファイルでの作業中にログアウトしても、ファイルは閉じられません。開いたままです。

ダッシュボード

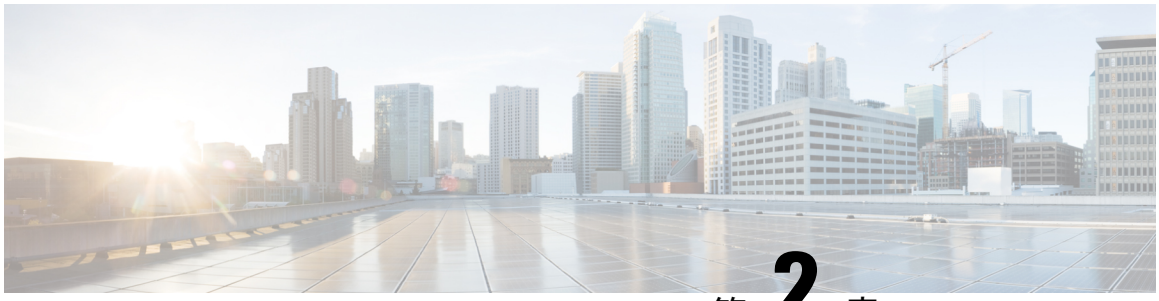
ログインに成功すると、[ダッシュボード（Dashboard）] ページが開きます。[ダッシュボード（Dashboard）] ページでは、Cisco Crosswork Planning の運用概要をすばやく把握できます。ダッシュボードは一連のダッシュレットで構成されています。ダッシュボードに含まれるダッシュレットは、インストールされている Cisco Crosswork Planning アプリケーションによって異なります。たとえば、Cisco Crosswork Planning Collector アプリケーションをインストールした場合にのみ、[収集（Collections）] および [ネットワークモデルのアーカイブ（Archive network models）] ダッシュレットが表示されます。Cisco Crosswork Planning Design アプリケーションをインストールした場合にのみ、[マイネットワーク設計モデル（My network design models）]、[マイ設計ジョブ（My Design Jobs）]、および [設計エンジン（Design engine）] ダッシュレットが表示されます。

各ダッシュレット内のリンクを使用すると、詳細を詳しく調べることができます。このリンクにより、目的のページに簡単に移動できます。

図 *2 : [ダッシュボード（Dashboard）] ビュー*



ダッシュレットの表示方法をカスタマイズするには、右上隅にある [ビューをカスタマイズ（Customize view）] ボタンを使用します。詳細については、*Cisco Crosswork Planning Design 7.0* ユーザーガイドのダッシュボードビューのカスタマイズに関するトピックを参照してください。



第 2 章

ネットワークモデルの設定

ここでは、次の内容について説明します。

ワークフロー：ネットワークモデルの作成

Cisco Crosswork Planning UI は、ネットワークのモデル構築チェーンを作成する複雑さを隠す、使いやすいインターフェイスを提供します。1 つのネットワーク（収集）にある複数のデータコレクタの設定をまとめて、統合されたデータを含む単一のネットワークモデルを生成できます。Cisco Crosswork Planning UI は、デバイスとネットワークのアクセス設定、ネットワークモデルの作成、ユーザー管理、エージェント設定などに使用します。

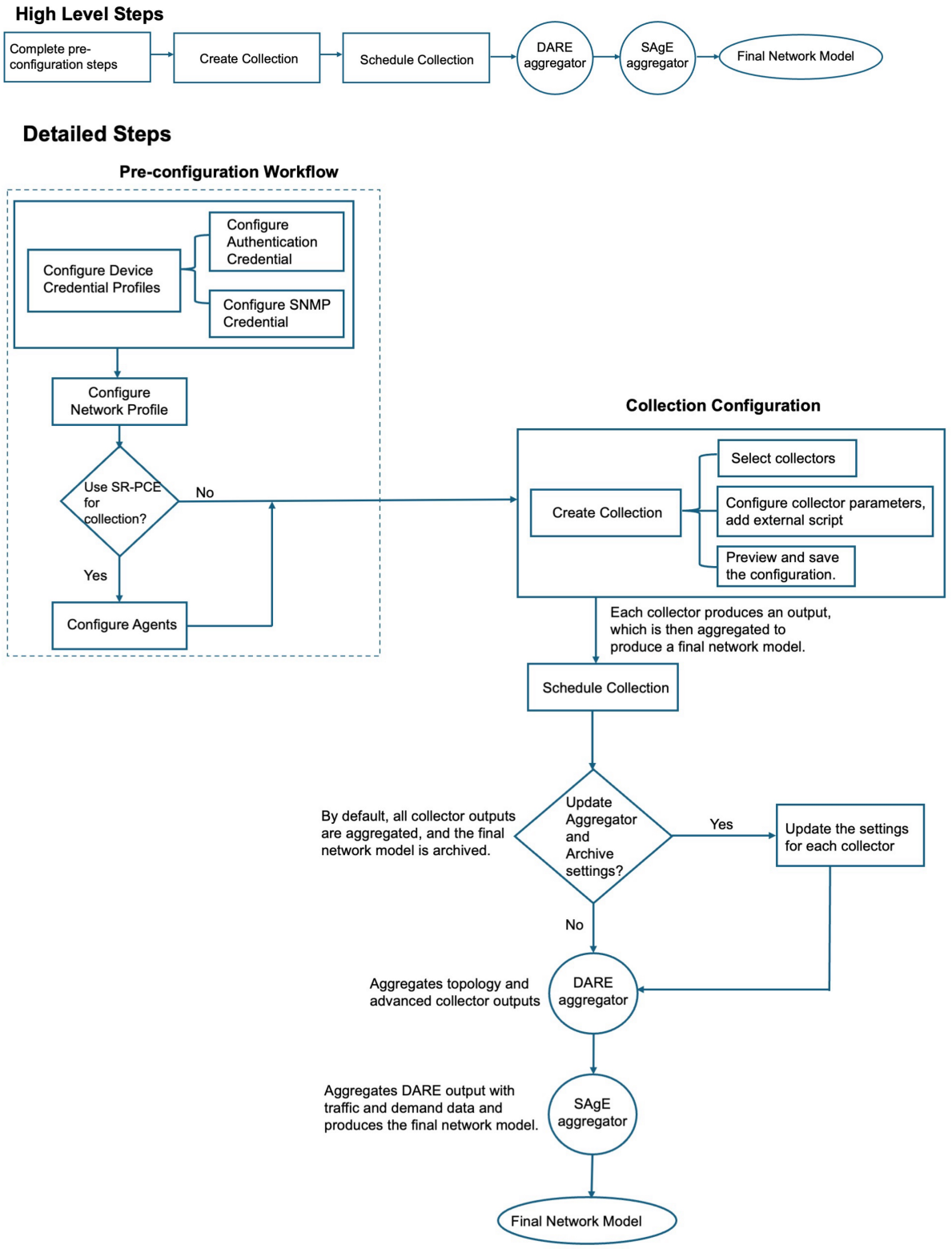
次の表と画像は、個々のネットワークモデルを設定に関するワークフローの概要を示しています。

表 *1*：ネットワークモデル作成ワークフロー

手順	操作
1. デバイス認証グループ、SNMP グループ、およびネットワーク プロファイル アクセスを構成します。	ワークフロー：事前設定手順 （12 ページ）を参照してください。

手順	操作
2.（オプション）エージェントを設定します。このステップは、SR-PCE または NetFlow 情報を収集する場合にのみ必要です。	エージェントの設定 （27 ページ）を参照してください。
3. 収集を設定します（基本設定および詳細設定）。	ワークフロー：収集の設定 （12 ページ）を参照してください。
4. 収集をいつ実行するかをスケジュールします。	スケジュールの追加 （39 ページ）を参照してください。
5.（オプション）要件に応じてネットワークモデルの集約とアーカイブを管理します。	参照先 • 集約コレクタの出力 （43 ページ） • アーカイブの設定 （46 ページ）
6.Cisco Crosswork Planning Design アプリケーションでプランファイルを表示またはダウンロードします。	プランファイルの表示またはダウンロード （48 ページ）を参照してください。

図 *3 :* ネットワークモデル作成ワークフロー



ワークフロー：事前設定手順

次のワークフローでは、ネットワークモデルを作成する前に実行する必要がある手順について説明します。この事前設定ワークフローには、デバイス、デバイスマッピング、およびエージェントにアクセスするためのクレデンシャルプロファイルの作成が含まれます。

表 *2:* 事前設定のワークフロー

手順	操作
1. デバイス クレデンシャル プロファイル（認証プロファイルおよびSNMPプロファイル）を設定します。	クレデンシャルプロファイルの設定（18 ページ）を参照してください。
2. ネットワーク アクセス プロファイルを設定します。	ネットワークプロファイルの設定（22 ページ）を参照してください。
3.（オプション）特定の情報を収集するエージェントを作成します。 このステップは、SR-PCE または NetFlow 情報を収集する場合にのみ必要です。	エージェントの設定（27 ページ）を参照してください。

ワークフロー：収集の設定

ネットワークモデルを作成する最初の手順は、トポロジ収集で新しいネットワーク（収集）を作成することです。[収集（Collections）]ページ（メインメニューから**[コレクタ（Collector）]**>**[収集（Collections）]**を選択）を使用して、さまざまなコレクタを設定します。収集するネットワーク要素を選択できます。SR-PCE が収集に使用されるかどうかを示すこともできます。コレクタの選択に基づいて、コレクタのチェーンが導出されて表示されます。各コレクタが出力を生成します。これらの出力が集約され、最終的なネットワークモデルが生成されます。ページの上部にある番号付きのナビゲーションには、ネットワークモデル設定プロセスの現在位置が表示されます。

収集の設定プロセスに関連するワークフローの概要は次のとおりです。

表 *3:* 収集の設定のワークフロー

ステップ	説明
1. 事前設定ワークフローに記載されているすべての手順を実行します。	ワークフロー：事前設定手順（12 ページ）を参照してください。

ステップ	説明
2. 必要なコレクタを選択します。	1. 最初のステップとして、追加のネットワーク収集のソースとなる [基本トポロジ（Basic Topology）] コレクタを選択します。 2. 要件に応じて、追加のコレクタを選択します。コレクタは、[基本トポロジ（Basic topology）]、[高度なモデリング（Advanced modeling）]、および [トラフィックとデマンド（Traffic and Demands）] の各セクションに分類されます。
3. 収集パラメータを設定します。	前の手順で選択したコレクタに応じて、設定パラメータが異なります。左側のペインには選択したコレクタが表示され、右側のペインには選択したコレクタに関連する設定パラメータが表示されます。必要な詳細情報をすべて入力します。
4. （オプション）収集モデルに対して外部スクリプトを実行します。	既存の Cisco Crosswork Planning コレクタでは提供されない、ネットワークからの特定のデータが必要な場合は、選択したネットワークモデルに対してカスタマイズされたスクリプトを実行できます。詳細については、ネットワークモデルに対する外部スクリプトの実行 （97 ページ） を参照してください。
5. コレクタを設定した順序をプレビューします。	コレクタを設定した順序をプレビューします。設定に問題がない場合は、 収集の作成を続行します。
6. 収集のスケジュールを設定します。	収集ジョブはすぐに実行することも、特定の時刻または間隔で定期的に実行するようにスケジュールを設定することもできます。1つの収集に複数のスケジュールを設定することもできます。詳細については、収集のスケジュール （39 ページ） を参照してください。
7. （オプション）必要に応じて、集約とアーカイブの設定を更新します。	参照先： • 集約コレクタの出力 （43 ページ） • アーカイブの設定 （46 ページ）

コレクタ設定の移行

Cisco Crosswork Planning では、Cisco WAE 7.5.x/7.6.x から、および Cisco Crosswork Planning インスタンスから別のインスタンスにコレクタ設定を移行できます。

（注） ファイルのアップロードオプションがあるコレクタを使用する場合は、コレクタ設定をインポートした後に正しいファイルをアップロードしてください。設定をインポートすると、サーバーでは実際のファイルではなくファイル名のみ復元されるため、この操作が必要です。正しいファイルが使用されていない場合、収集は失敗します。

Cisco WAE からのコレクタ設定の移行

コレクタ設定を Cisco WAE 7.5.x/7.6.x から Cisco Crosswork Planning に移行するには、次の手順に従います。

始める前に

- Cisco Download Software サイトから、アップグレードスクリプトをダウンロードします。

手順

ステップ 1 設定をバックアップしていない場合は、次の手順を使用して設定をバックアップし、Cisco Crosswork Planning と互換性のある設定に移行します。

a) Cisco WAE 7.x がインストールさているマシンにログインします。

b) 次のコマンドを入力します。

```
# ./wae_upgrade --export --install-dir <WAE_7.x_INSTALL_DIR> --cfg-dir
<dir_to_save_exported_config>

Where:
      --install-dir   indicates the directory where 7.x WAE is installed
      --cfg-dir       indicates the folder where the backup of 7.x configuration
                      must reside
```

ステップ 2 バックアップされた設定がすでにある場合は、次の手順を使用して、Cisco Crosswork Planning と互換性のある形式にファイルを変換します。

a) Cisco WAE 7.x の設定がバックアップされているマシンにログインします。

b) 次のコマンドを入力します。

```
# ./wae_upgrade --migrate --cfg-dir <dir_containing_7.x_config>

Where:
      --cfg-dir       indicates the folder where the 7.x configuation is backed up.
                      This configuration will be migrated to Cisco Crosswork Planning
                      compatible configuration.
```

ステップ 3 次の手順を使用して、Cisco Crosswork Planning 互換の設定ファイルを Cisco Crosswork Planning にインポートします。

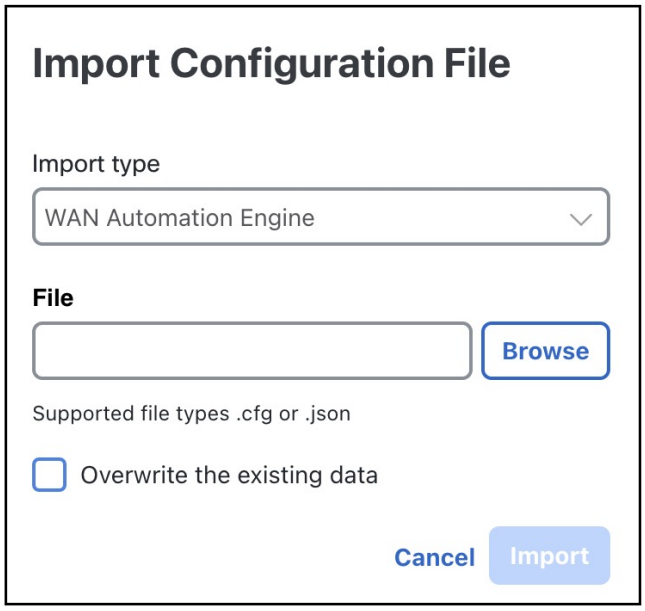
（注）

移行する前に、アップグレードスクリプトを使用して設定がバックアップされていることを確認します。バックアップされていないと、移行は失敗します。

a) Cisco Crosswork Planning UI にログインします。
b) メインメニューから、**[コレクタ（Collector）]** > **[移行（Migration）]** の順に選択します。
c) [アクション（Actions）] をクリックし、[設定の移行（Configuration migration）] を選択します。

[設定ファイルのインポート（Import configuration file）] ウィンドウが表示されます。

図 4 : [設定ファイルのインポート（*Import configuration file*）] ウィンドウ



d) [インポートタイプ（Import Type）] ドロップダウンから、[WAN自動化エンジン（WAN Automation Engine）] を選択します。
e) [参照（Browse）] をクリックし、Cisco Crosswork Planning と互換性のある Cisco WAE コレクタ設定ファイルを選択します。
f) （オプション）既存のコレクタ設定を上書きする場合は、[既存のデータを上書きする（Overwrite the existing data）] チェックボックスをオンにします。
g) [インポート（Import）] をクリックして、コレクタ設定ファイルをインポートします。

[移行（Migration）] ページ（**[コレクタ（Collector）]** > **[移行（Migration）]**）でインポートのステータスをモニターできます。インポートが成功すると、[インポートステータス（Import status）] 列にタスクのステータスが [成功（Success）] と表示されます。

（注） Cisco WAE から Cisco Crosswork Planning に移行すると、Telnet と SSH の設定は保持されません。必要に応じて、各設定を手動で確認および更新する必要があります。

移行中に除外される設定

次の設定は、Cisco WAE から Cisco Crosswork Planning への移行中に移行されません。

- HA、LDAP、およびユーザー管理の設定
- スマートライセンスの設定
- WMD 設定
- オプティカルエージェント、オプティカル NIMO、L1-L3 マッピング、フィージビリティ制限マージン、中央周波数除外リストなど、すべてのオプティカル/L1 関連の設定。これは、 このリリースでは Cisco Crosswork Planning の収集がオプティカル機能をサポートしていないためです。ただし、オプティカル設定はアップグレードスクリプトの一部として収集され、将来使用できます。
- AS NIMO 間の設定
- デマンド推論コレクタのデマンドのコピーステップにおける送信元コレクタの詳細（これらのフィールドは Cisco WAE と Cisco Crosswork Planningで異なるため）。これらの詳細は、移行後に手動で設定する必要があります。
- コンポーザワークフローに含まれないネットワーク
- 外部の実行可能スクリプト設定。これらのスクリプトは、Cisco Crosswork Planning に展開する前にいくつかの変更とテストが必要になる場合があります。
- 設定済みのデバイスログイン情報デフォルトのログイン情報がインポートされるため、ログイン情報を再入力する必要があります。
- 特定のリソースファイル（更新されたネットワークアクセスファイル、sql-capabilities、sql-source-capabilities などの高度なアグリゲータ設定など）。
- NetFlow エージェントの場合の Nodeflow 設定（BGP の詳細）。この設定は、移行後に手動で設定する必要があります。
- ネットワーク レコード プラン ファイル

Cisco Crosswork Planning インスタンス間でのコレクタ設定の移行

（注） お使いの構成で SR-PCE コレクタを使用している場合は、移行後に [SR-PCEホスト（SR-PCE host） フィールド と [SR-PCEホストのバックアップ（Backup SR-PCE host）] フィールドを手動で更新してください。Cisco Crosswork Planning インスタンス間でコレクタ設定を移行するときに、これらのフィールドが更新されないため、この操作が必要です。

次の手順に従って、任意の Cisco Crosswork Planning インスタンス（ソース）から別のインスタンス（ターゲット）にコレクタ設定を移行します。

手順

ステップ 1 設定を移行する元のソースマシンからコレクタ設定ファイルをダウンロードします。

a) 設定の移行元の Cisco Crosswork Planning インスタンスにログインします。
b) メインメニューから、**[コレクタ（Collector）] > [移行（Migration）]** の順に選択します。
c) [アクション（Actions）] をクリックし、[設定のバックアップ（Configuration backup）] を選択します。

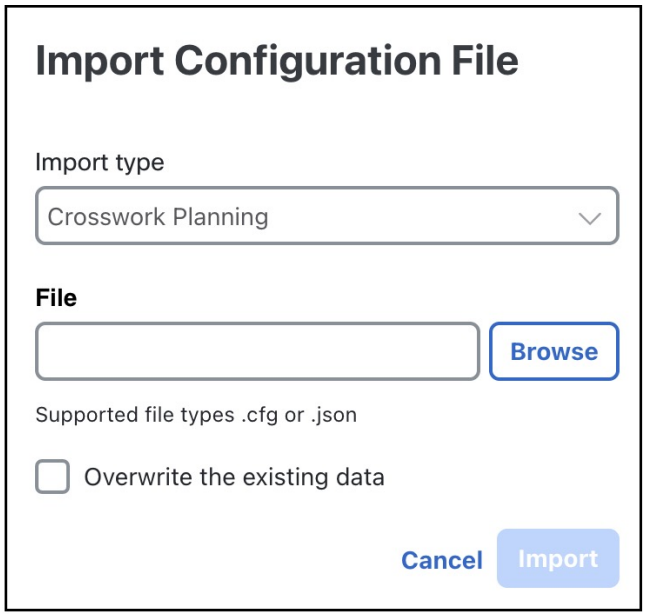
コレクタ設定ファイルがローカルマシンにダウンロードされます。

ステップ 2 コレクタ設定ファイルを、移行先のターゲットマシンにインポートします。

a) 設定の移行先の Cisco Crosswork Planning インスタンスにログインします。
b) メインメニューから、**[コレクタ（Collector）] > [移行（Migration）]** の順に選択します。
c) [アクション（Actions）] をクリックし、[設定の移行（Configuration migration）] を選択します。

[設定ファイルのインポート（Import configuration file）] ウィンドウが表示されます。

図 *5 : [*設定ファイルのインポート（*Import configuration file***）*]* ウィンドウ**

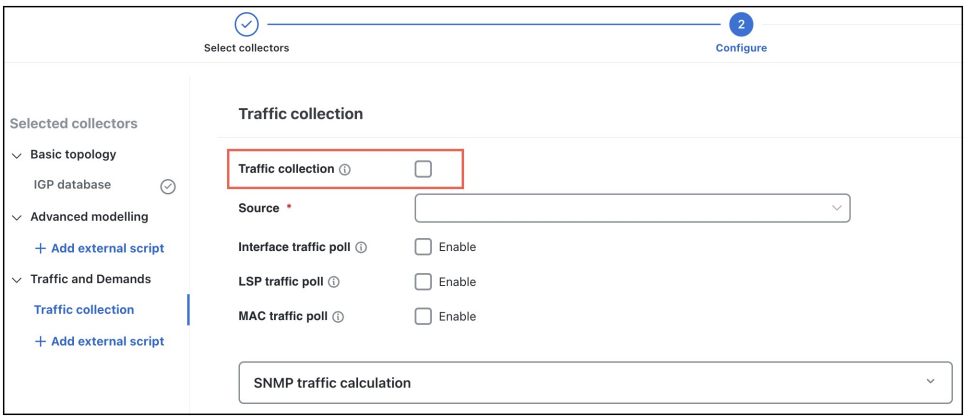


d) [インポートタイプ（Import type）] ドロップダウンから、[Crosswork Planning] を選択します。
e) [参照（Browse）] を選択して、手順 1（c）でダウンロードしたコレクタ設定ファイルを選択します。
f) （オプション）既存のコレクタ設定を上書きする場合は、[既存のデータを上書きする（Overwrite the existing data）] チェックボックスをオンにします。
g) [インポート（Import）] をクリックして、コレクタ設定ファイルをインポートします。

[移行（Migration）] ページ（**[コレクタ（Collector）] > [移行（Migration）]**）でインポートのステータスをモニターできます。インポートが成功すると、[インポートステータス（Import status）] 列にタスクのステータスが [成功（Success）] と表示されます。

（注） トラフィック収集の場合、トラフィック収集が正常に実行されていても、移行後にトラフィック ポーラー エージェントのステータスが [エージェント（Agent）] ページにダウンと表示される場合は、[収集（Collections）]（[コレクタ（Collector）] > [収集（Collections）]）ページで次の手順を実行します。

1. エージェントに対応する収集の [収集の編集（Edit Collection）] を選択します。
2. [トラフィックコレクタの設定（Traffic collection configuration）] ページで、[トラフィック収集（Traffic collection）] チェックボックスをオフにして、設定を保存します。
3. [トラフィック収集（Traffic collection）] チェックボックスを再度有効にして、設定を再度保存します。



[トラフィックとデマンド（Traffic and Demands）] コレクタの設定の詳細については、トラフィック統計情報の収集 （89 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の設定

デバイスにアクセスするには、クレデンシャルプロファイルを定義する必要があります。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、特定の建物にあるすべてのルータで単一の SSH ユーザー ID とパスワードを共有する場合、Cisco Crosswork Planning がそれらの情報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、および接続プロトコルが含まれます。また、SNMPv2 の読み取り/書き込みコミュニティストリング、SNMPv3 認証タイプと権限タイプなどの追加データが必要になります。

次のワークフローでは、クレデンシャルプロファイルを作成する手順について説明します。

表 *4:* クレデンシャルプロファイルの設定ワークフロー

手順	操作
1. デバイスにアクセスするためのデバイス認証情報を設定します。	認証情報の設定 （19 ページ） を参照してください。
2. ネットワークサーバーにアクセスするための SNMP ログイン情報を設定します。	SNMP ログイン情報の設定 （20 ページ） を参照してください。

認証情報の設定

[収集（Collections）] ページ（**[コレクタ（Collector）] > [収集（Collections）]**）に初めてアクセスした場合、[ようこそ（Welcome）] 画面が表示されます。[開始（Get Started）] をクリックして、事前設定手順を確認します。左側のステップを示すペインに、手順の一覧が表示されます。最初のステップでは、認証情報の作成を完了するように指示されます。

または

[コレクタ（Collector）] > [ログイン情報（Credentials）] ページから認証情報を設定するには、次の手順を実行します。

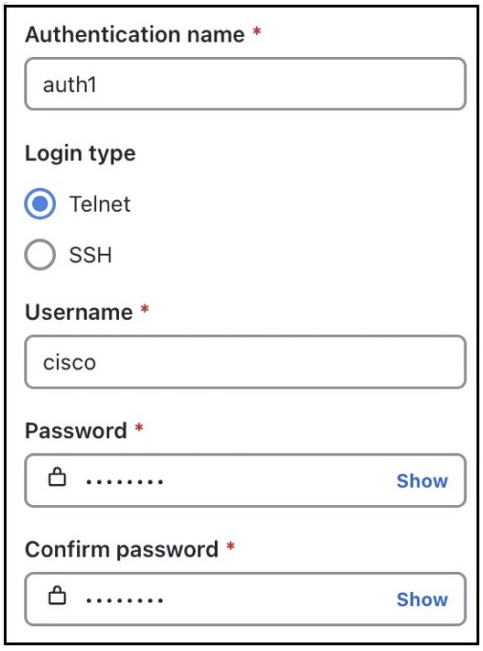
手順

ステップ 1 メインメニューから、**[コレクタ（Collector）] > [ログイン情報（Credentials）]** の順に選択します。

ステップ 2 [認証（Authentication）] タブで、 [+新規作成（+ Create New）] ボタンをクリックします。

（注）
認証情報を初めて作成する場合は、[ログイン情報の設定（Setup credentials）] をクリックします。

図 *6 :* 認証情報の設定



ステップ 3 次のフィールドに値を入力します。

- [認証名（Authentication Name）]：わかりやすい名前を入力します。
- [ログインタイプ（Login type）]：使用するログインプロトコル（[SSH] または [Telnet]）を選択します。SSH プロトコルはより安全です。Telnet プロトコルは、ユーザー名とパスワードを暗号化しません。
- [ログイン情報（Credential）]フィールド：[ユーザー名（Username）]、[パスワード（Password）]、および [パスワードの確認（Confirm Password）] フィールドに値を入力します。

ステップ 4 [保存（Save）] をクリックします。

SNMP ログイン情報の設定

[収集（Collections）] ページ（**[コレクタ（Collector）] > [収集（Collections）]**）に初めてアクセスした場合、[ようこそ（Welcome）] 画面が表示されます。[開始（Get Started）] をクリックして、事前設定手順を確認します。左側のステップを示すペインに、手順の一覧が表示されます。最初のステップを完了したら、2 番目のステップで SNMP ログイン情報の作成を完了します。

または

[コレクタ（Collector）] > [ログイン情報（Credentials）] ページから SNMP ログイン情報を設定するには、次の手順を実行します。

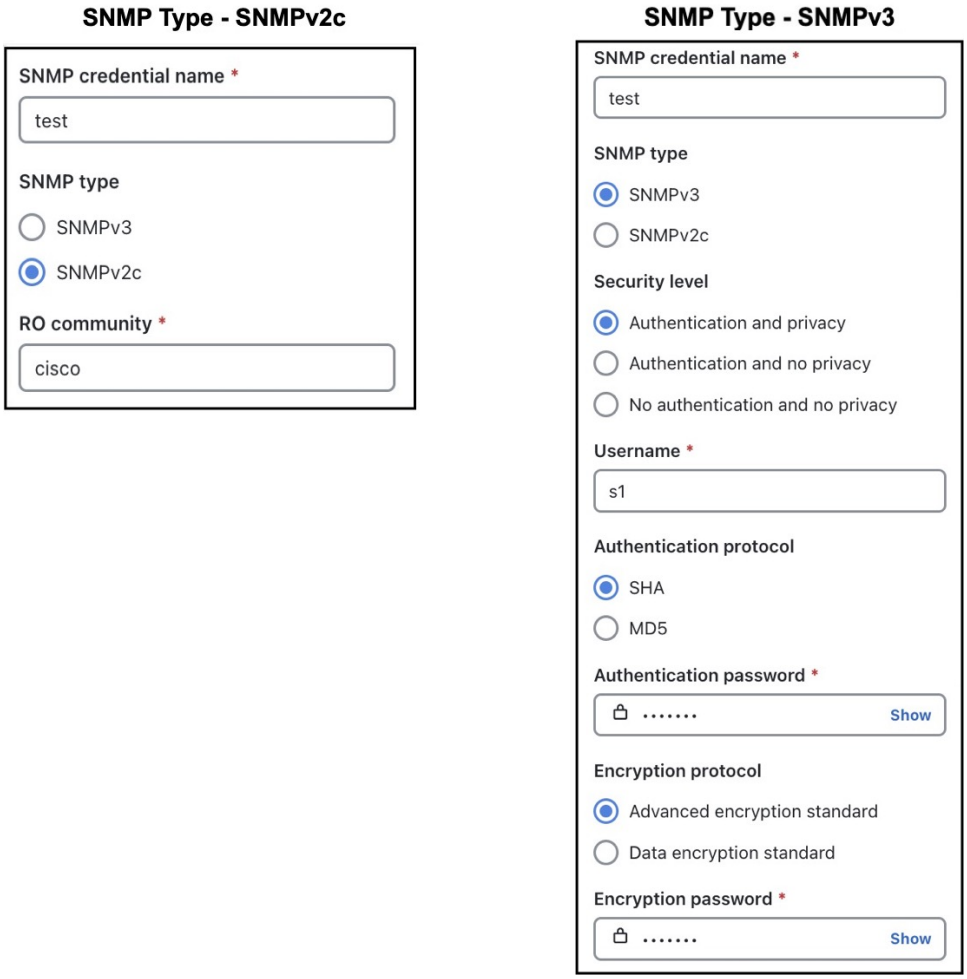
手順

ステップ 1 メインメニューから、**[コレクタ（Collector）] > [ログイン情報（Credentials）]** の順に選択します。

ステップ 2 [SNMP] タブをクリックし、[+新規作成（+ Create New）] ボタンをクリックします。

（注）
認証情報を初めて作成する場合は、[ログイン情報の設定（Setup credentials）] をクリックします。

図 *7 : SNMP* ログイン情報の設定



ステップ 3 [SNMPログイン情報名（SNMP credential name）] フィールドに、SNMP プロファイルのわかりやすい名前を入力します。

ステップ 4 [SNMPタイプ（SNMP type）] で、使用する SNMP プロトコル（[SNMPv2c] または [SNMPv3]）を選択します。

- [SNMPv2c] を選択した場合、パスワードとして機能する SNMP RO コミュニティストリングを入力します。これは、ノードとシードルータの間で送信されるメッセージを認証するために使用されます。

- [SNMPv3] を選択した場合、次のデフォルトのログイン情報を入力します。
  - [セキュリティレベル（Security level）]：次のいずれかを選択します。
    - [認証とプライバシー（Authentication and privacy）]：認証と暗号化の両方が提供されるセキュリティレベル。
    - [認証あり、プライバシーなし（Authentication and no privacy）]：認証は提供されるが、暗号化は提供されないセキュリティレベル。
    - [認証なし、プライバシーなし（No Authentication and no privacy）]：認証も暗号化も提供されないセキュリティレベル。
  - [ユーザー名（Username）]：ユーザー名を入力します。
  - [認証プロトコル（Authentication protocol）]：次のいずれかを選択します。
    - [SHA]：HMAC-SHA-96 認証プロトコル
    - [MD5]：HMAC-MD5-96 認証プロトコル
  - [認証パスワード（Authentication password）]：認証パスワードを入力します。
  - [暗号化プロトコル（Encryption protocol）] および [暗号化パスワード（Encryption password）]：暗号化オプションでは、SNMP セキュリティ暗号化に Data Encryption Standard（DES; データ暗号規格）または 128 ビット Advanced Encryption Standard（AES）暗号化を選択できます。AES-128 トークンは、このプライバシーパスワードが 128 ビット AES キー # の生成用であることを示します。AES 暗号化パスワードは最小で 8 文字で指定できます。パスフレーズをクリア テキストで指定する場合、最大 64 文字を指定できます。ローカライズド キーを使用する場合は、最大 130 文字を指定できます。

ステップ 5 [保存（Save）] をクリックします。

ネットワークプロファイルの設定

ネットワークからデータを収集するためのネットワークプロファイルを定義します。このネットワークプロファイルは、ネットワークノードとそのログイン情報で構成されます。また、フィルタ条件を適用して、検出中にいくつかのノードを含めたり、除外したりできます。

[収集（Collections）] ページ（**[コレクタ（Collector）]** > **[収集（Collections）]**）に初めてアクセスした場合、[ようこそ（Welcome）] 画面が表示されます。[開始（Get Started）] をクリックして、事前設定手順を確認します。左側のステップを示すペインに、手順の一覧が表示されます。最初の 2 つのステップを完了したら、3 番目のステップでネットワークプロファイルの作成を完了します。

または

[コレクタ（Collector）] > **[ネットワークプロファイル（Network Profiles）]** ページから SNMP ログイン情報を設定するには、次の手順を実行します。

始める前に

デバイス クレデンシャル プロファイル（認証プロファイルおよび SNMP プロファイル）を設定します。詳細については、「認証情報の設定 （19 ページ）」および「SNMP ログイン情報の設定 （20 ページ）」を参照してください。

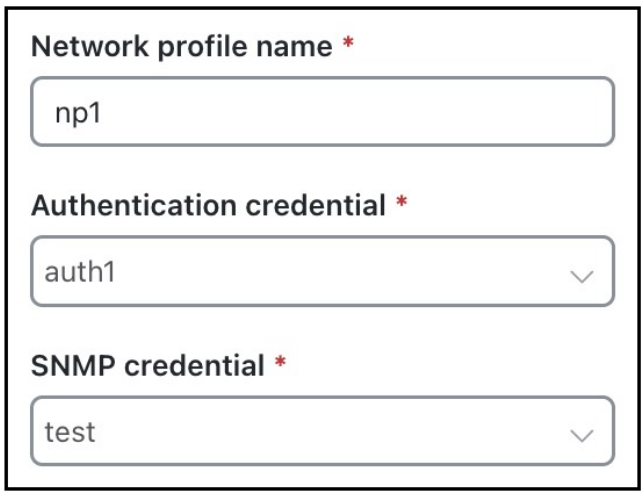
手順

ステップ 1 メインメニューから、**[コレクタ（Collector）]** > **[ネットワークプロファイル（Network Profiles）]** の順に選択します。

ステップ 2 [+新規作成（+ Create New）] ボタンをクリックします。

（注）
ネットワークプロファイルを初めて作成する場合は、[ネットワークプロファイルの設定（Setup Network Profile）] をクリックします。

図 *8* : ネットワークプロファイルの作成



ステップ 3 次の情報を入力します。

- [ネットワークプロファイル名（Network Profile Name）]：ネットワーク アクセス プロファイルの名前を入力します。
- [認証情報（Authentication Credential）]：ドロップダウンリストから該当する認証情報を選択します。認証情報を作成していない場合は、認証情報の設定 （19 ページ）に記載されている手順を使用して作成します。
- [SNMPログイン情報（SNMP Credential）]：ドロップダウンリストから該当する SNMP ログイン情報を選択します。SNMP ログイン情報を作成していない場合は、SNMP ログイン情報の設定 （20 ページ）に記載されている手順を使用して作成します。

ステップ 4 [作成して続行（Create & Proceed）] をクリックします。

ステップ 5 （オプション）ネットワークアクセスのログイン情報に関連付けられたノードを追加または編集する場合は、ノードの追加または編集 （24 ページ）を参照してください。

ステップ 6 （オプション）収集に個々のノードを含めたり、除外したりする場合は、ノードフィルタの設定 （25 ページ）を参照してください。

ステップ 7 [保存（Save）] をクリックします。

ノードの追加または編集

前述のトピックで作成したネットワークアクセスのログイン情報に関連付けられたノードを追加または編集するには、次の手順を実行します。

手順

ステップ 1 メインメニューから、**[コレクタ（Collector）] > [ネットワークプロファイル（Network Profiles）]** の順に選択します。

ステップ 2 必要なネットワークプロファイルを選択し、[保存して続行（Save & Proceed）] をクリックします。

ステップ 3 [ノードリスト（Node List）] で、[ノードの編集（Edit nodes）] ボタンをクリックし、次のいずれかを実行します。

- 初めて手動でノードを追加する場合は、[+ノードの追加（+ Add node）] ボタンをクリックします。[ノードの追加（Add Node）] ウィンドウにノードの詳細を入力し、[保存（Save）] をクリックします。新しく追加されたノードが [ノードリスト（Node List）] ページに表示されます。

  さらにノードを追加する場合は、  をクリックして詳細を入力します。

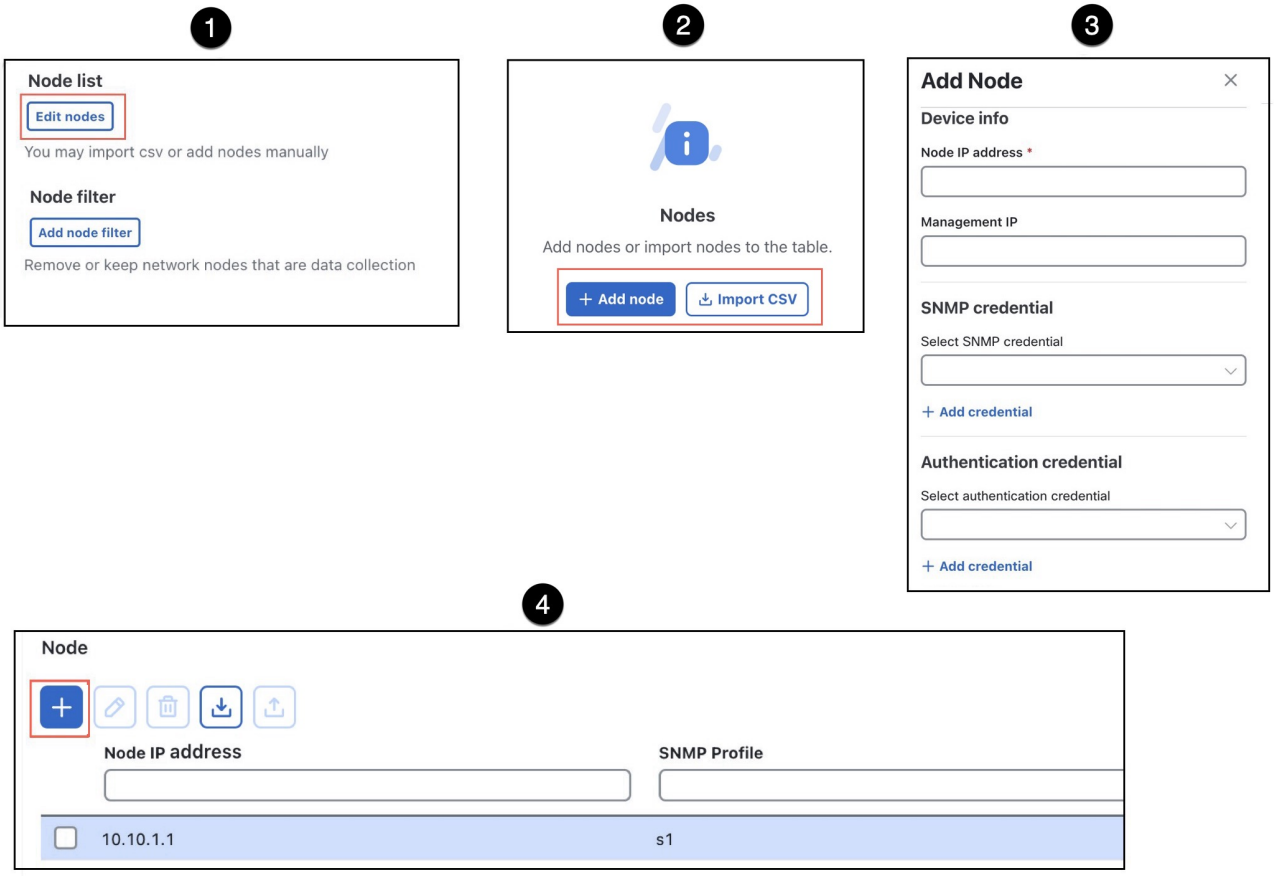
- ノードの追加がない場合にノードリストをインポートする場合は、 

ボタンをクリックします。[参照（Browse）] をクリックして CSV ファイルパスを入力し、[インポート（Import）] をクリックします。新しくインポートされたノードが [ノードリスト（Node List）] ページに表示されます。

  別のノードリストをインポートする場合は、  をクリックして CSV ファイルをインポートします。

  ノードリストを含むサンプルファイルをダウンロードするには、**サンプルファイル**のリンクをクリックします。

図 *9 : [*ノードの追加（***Add Nodes***）*]* ページ



- ノードリストをエクスポートするには、 をクリックします。
- ノードを編集するには、ノードを選択して をクリックし、ノードの詳細を入力します。
- ノードを削除するには、ノードを選択して をクリックします。

ステップ 4 [完了（Done）] をクリックします。

ノードフィルタの設定

Cisco Crosswork Planning を使用すると、個々のノードをデータ収集に含めたり、収集から除外したりできます。

（注）

- ノード/ホスト名またはループバック IP をノードフィルタリストに追加できます。管理 IP はノードフィルタ IP に追加しないでください。
- ノード/ホスト名は IS-IS で機能します。
- OSPF データベースにはノード名がないため、フィルタリングは IP アドレスでのみ機能します。
- ノードフィルタは、セグメントリストのホップをサポートしていません。

手順

ステップ 1 メインメニューから、**[コレクタ（Collector）] > [ネットワークプロファイル（Network Profiles）]** の順に選択します。

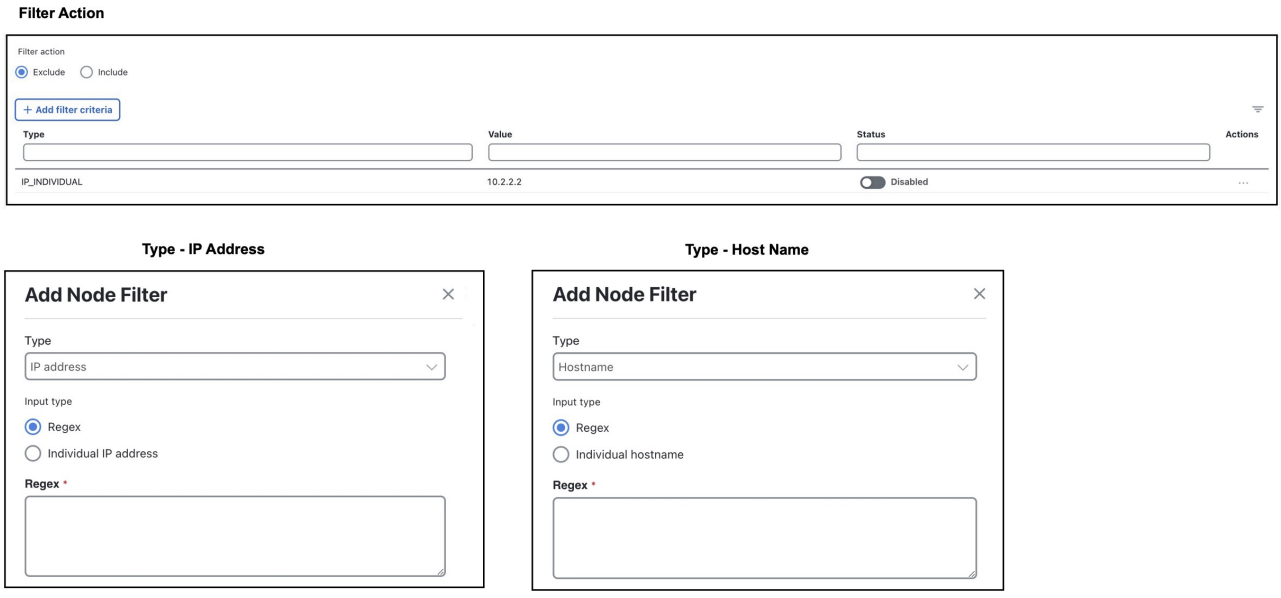
ステップ 2 必要なネットワークプロファイルを選択し、[保存して続行（Save & Proceed）] をクリックします。

ステップ 3 [ノードフィルタの追加（Add Node Filter）] をクリックします。

ステップ 4 [フィルタアクション（Filter Action）] で、個々のノードを除外するか含めるには、それぞれ [除外（Exclude）] または [含める（Include）] を選択します。

ステップ 5 [+フィルタ条件の追加（+ Add Filter Criteria）] をクリックします。[ノードフィルタの追加（Add Node Filter）] ページが表示されます。

図 *10 : [ノードフィルタ（Node Filter）] ページ*



ステップ 6 [タイプ（Type）] ドロップダウンリストから、フィルタ処理に使用するタイプを選択します。オプションは、[IPアドレス（IP Address）] と [ホスト名（Hostname）] です。

ステップ 7 [入力タイプ（Input type）] で必要なオプションを選択します。前のステップで選択したタイプに基づいて、異なるオプションが表示されます。

- [IPアドレス（IP Address）] を選択した場合、オプションは [正規表現（Regex）] と [個別のIPアドレス（Individual IP Address）] です。
- [ホスト名（Hostname）] を選択した場合、オプションは [正規表現（Regex）] と [個別のホスト名（Individual Hostname）] です。

単一の表現に複数のノードを含めたり除外したりする場合は、[正規表現（Regex）]オプションを使用します。[正規表現（Regex）] フィールドに**正規表現**を入力します。

[個別のIPアドレス（Individual IP Address）] オプションを使用して、各ノードの IP アドレスを追加します。[IPアドレス（IP Address）] フィールドに IP アドレスを入力します。

[個別のホスト名（Individual hostname）] オプションを使用して、各ノードのホスト名を追加します。[ホスト名（Hostname）] フィールドにホスト名を入力します。

ステップ 8 [保存（Save）] をクリックします。

ステップ 9 （オプション）ステップ 4 ～ 8 を繰り返して、フィルタ条件を追加します。

ステップ 10 [ステータス（Status）] 列のトグルを [有効（Enabled）] の位置にスライドして、フィルタでこれらのエントリを考慮に入れます。

ステップ 11 [保存（Save）] をクリックします。

ノードを編集または削除するには、[アクション（Actions）]列の下にある ⋯ >[編集（Edit）] または ⋯ > [削除（Delete）] オプションを使用します 。

エージェントの設定

エージェントは情報収集タスクを実行するため、特定のネットワーク収集操作の前に設定する必要があります。このセクションでは、Cisco Crosswork Planning UI を使用して XTC エージェントを設定する方法について説明します。

（注） このタスクは、SR-PCE または NetFlow 情報を収集する場合にのみ必要です。

（注） 収集に**トラフィック収集**コレクタが含まれている場合、[コレクタ（Collector）] > [エージェント（Agents）] ページには、トラフィック ポーラー エージェントの詳細も表示されます。エージェントの名前は、収集の名前と同じです。

[収集（Collections）] ページ（**[コレクタ（Collector）] > [収集（Collections）]**）に初めてアクセスした場合、[ようこそ（Welcome）] 画面が表示されます。[開始（Get Started）] をクリックして、事前設定手順を確認します。左側のステップを示すペインに、手順の一覧が表示されま

す。最初の 3 つのステップを完了したら、4 番目のステップでエージェントの作成を完了します。

または

[コレクタ（Collector）] > **[ネットワークプロファイル（Network Profiles）]** ページから SNMP ログイン情報を設定するには、次の手順を実行します。

手順

ステップ 1 メインメニューから、**[コレクタ（Collector）]** > **[エージェント（Agents）]** の順に選択します。

ステップ 2 [+新規作成（+ Create New）] をクリックします。

（注）
エージェントを初めて作成する場合は、[エージェントの設定（Setup agent）] をクリックします。

ステップ 3 [エージェント名（Agent name）] フィールドにエージェントの名前を入力します。

ステップ 4 必要なコレクタタイプを選択します。オプションは、[SR-PCE] または [NetFlow] です。

- SR-PCE エージェントは、SR-PCE サーバーから定期的に情報を収集し、SR-PCE によって送信されたトポロジ、LSP データ、および通知を処理します。エージェントは、SR-PCE の REST インターフェイスに接続し、PCE トポロジを取得します。

  （注）
  ネットワーク収集を実行する前に、SR-PCE を使用するすべてのネットワークに対して SR-PCE エージェントを設定する必要があります。

- NetFlow コレクタは、フローレコードの受信、処理、および保存を実行します。このデータは、ネットワークのトラフィックパターンと動作を分析し、インサイトを得るのに役立ちます。

ステップ 5 設定オプションは、選択した**コレクタタイプ**によって異なります。

- コレクタタイプとして [SR-PCE] を選択した場合は、表 5 : SR-PCE エージェントの設定オプション（29 ページ）に記載されている該当する設定の詳細を入力します。
- コレクタタイプとして [NetFlow] を選択した場合は、表 6 : NetFlow エージェントの設定オプション（31 ページ）に記載されている該当する設定の詳細を入力します。

ステップ 6 [保存（Save）] をクリックします。

新たに作成されたエージェントが **[コレクタ（Collector）]** > **[エージェント（Agents）]** ページに表示されます。

- 保存後に設定パラメータを編集すると、SR-PCE および NetFlow エージェントが再起動します。
- SR-PCE エージェントは、

- [有効（Enabled）] オプションが選択されている限り、設定後または Cisco Crosswork Planning の起動時にすぐに開始します。
- （a）設定が削除された場合、（b）Cisco Crosswork Planning が停止した場合、あるいは（c）[有効（Enabled）] オプションの選択が解除された場合は停止します。

次のタスク

[収集（Collections）] ページ（**[コレクタ（Collector）] > [収集（Collections）]**）を使用して、ネットワークモデルを構築するためのコレクタを設定します。詳細については、収集の作成（33 ページ）を参照してください。

SR-PCE および NetFlow エージェントの設定オプション

このトピックでは、SR-PCE および NetFlow エージェントを設定するときに使用できるオプションについて説明します。

表 *5 : SR-PCE* エージェントの設定オプション

オプション	説明
有効（Enabled）	SR-PCE エージェントを有効にします。デフォルトでは有効です。
SR-PCEホストIP（SR-PCE host IP）	SR-PCE ルータのホスト IP アドレスを示します。
SR-PCE RESTポート（SR-PCE REST port）	SR-PCE ホストに接続するポート番号を示します。デフォルトは 8080 です。
認証タイプ（Authentication type）	SR-PCE ホストへの接続に使用する認証タイプを示します。次のオプションを使用できます。 • Basic：HTTP Basic 認証（プレーンテキスト）を使用します。 • ダイジェスト（Digest）：HTTP ダイジェスト認証（MD5）を使用します。 • なし（None）：認証を使用しません。これは、古い IOS XR バージョンにのみ適用されます。
ユーザー名（Username）	SR-PCE ホストに接続するためのユーザー名を示します。
パスワード（Password）	SR-PCE ホストに接続するためのパスワードを示します。
接続再試行回数（Connection retry count）	SR-PCE ホストへの接続の最大再試行回数を示します。

オプション	説明
トポロジ収集（Topology collection）	トポロジデータを収集し、ネットワーク変更のサブスクリプションを取得するかどうかを指定します。オプションは、収集のみ（Collection only）、収集とサブスクリプション（Collection and Subscription）、およびオフ（Off）です。デフォルトは収集とサブスクリプション（Collection and Subscription）です。
LSP収集（LSP collection）	LSPデータを収集し、ネットワーク変更のサブスクリプションを取得するかどうかを指定します。オプションは、収集のみ（Collection only）、収集とサブスクリプション（Collection and Subscription）、およびオフ（Off）です。デフォルトは収集とサブスクリプション（Collection and Subscription）です。
接続タイムアウト間隔（Connection timeout interval）	接続タイムアウトを秒単位で指定します。デフォルトは 50 秒です。
プールサイズ（Pool size）	SR-PCE データを並行して処理するスレッドの数を示します。
キープアライブインターバル（Keep alive interval）	キープアライブメッセージを送信する間隔（秒単位）を示します。デフォルトは 10 です。
バッチサイズ（Batch size）	各メッセージで送信するノードの数を示します。デフォルトは 1000 です。
キープアライブしきい値（Keep alive threshold）	欠落したキープアライブメッセージのしきい値を指定します。デフォルトは 2 です。
イベントバッファが有効（Event buffer enabled）	SR-PCE エージェントで通知を処理するためのバッファ時間を追加できます。SR-PCE エージェントは通知を処理し、バッファリングされた時間（[イベントバッファ時間（Events buffer time）] フィールドで指定）の後にのみ、統合通知が SR-PCE および PCEP LSP コレクタに送信されます。この機能は、リンクフラッピングなどの連続通知が多すぎる場合に役立ちます。 SR-PCE エージェントは、[トポロジ収集（Topology collection）] フィールドと [LSP収集（LSP collection）] フィールドを使用して、トポロジ情報または LSP 情報のみを収集するように設定できます。
イベントバッファ時間（Events buffer time）	コレクタに送信する前にSR-PCEイベントをバッファリングする時間を秒単位で示します。
再生イベントの遅延（Playback events delay）	実際のイベントを模倣するSR-PCEイベントの再生の遅延を秒単位で示します（0 = 遅延なし）。
最大LSP履歴（Max LSP history）	送信するLSPエントリの数を示します。デフォルトは0です。

オプション	説明
ネットレコーダーモード（Net recorder mode）	SNMP メッセージを記録します。オフ（Off）、記録（Record）、または再生（Playback）を選択できます。デフォルトはオフです。

表 *6 : NetFlow* エージェントの設定オプション

オプション	説明
BGP	パッシブ BGP ピアリングを有効にします。Cisco Crosswork Planning は、ルータとの BGP セッションのセットアップを試行します。[BGP] チェックボックスの下に表示されているテーブルに BGP の詳細を入力します。
名前（Name）	ノード名を示します。
サンプリングレート（Sampling rate）	ノードからエクスポートされたフローのパケットのサンプリングレートを示します。たとえば、値が 1,024 の場合、1,024 あるパケットから 1 つが決定論的またはランダムな方法で選択されます。
フロー送信元IP（Flow source IP）	フローエクスポートパケットの IPv4 送信元アドレスを示します。
BGP送信元IP（BGP source IP）	iBGP 更新メッセージの IPv4 または IPv6 送信元アドレスを示します。
BGPパスワード（BGP password）	MD5 認証の BGP ピアリングパスワードを示します。
インターバル（Interval）	出力ファイルを書き込む間隔を秒単位で示します。0 よりも大きく、60 の倍数である値を入力します。デフォルトは 900 秒です。

オプション	説明
フローサイズ（Flow size）	ネットワーク全体の集約されたフローエクスポートトラフィック レートに基づいて、フロー収集の展開サイズを示します。値は次のとおりです。 • 小規模（Small）：フロートラフィックレートが 10 Mbps 未満の場合に推奨されます。 • 中規模（Medium）：フロートラフィックレートが 10 ～ 50 Mbps の場合に推奨されます。 • 大規模（Large）：フロートラフィックレートが 50 Mbps を超える場合に推奨されます。 • ラボ（Lab）：お客様用ではありません。 デフォルトは中規模（Medium）です。
追加集約（Extra aggregation）	リストから集約キーを選択できます。

エージェントの操作

作成されたエージェントに対して、次の複数の操作を実行できます。

- [編集（Edit）]：エージェントのパラメータを編集するには、このオプションを使用します。
- [起動（Start）]、[再起動（Restart）]、および [停止（ Stop）]：これらのオプションを使用して、エージェントをそれぞれ起動、再起動、および停止します。
- [接続の確認（Verify connection）]：エージェントのステータスを確認するには、このオプションを使用します。
- [削除（Delete）]：エージェントを削除するには、このオプションを使用します。
- [スケジュールの追加（Add schedule）] および [スケジュールの編集（Edit schedule）]：これらのオプションを使用して、エージェントのデータ更新頻度をそれぞれ設定および編集します。cron 式を使用してスケジュールを入力します。

（注） このオプションは、SR-PCE エージェントでのみ使用できます。スケジュールの追加または編集のみ可能です。[ステータス（Status）]、[時間（Duration）] などのスケジュールの詳細を表示することはできません。

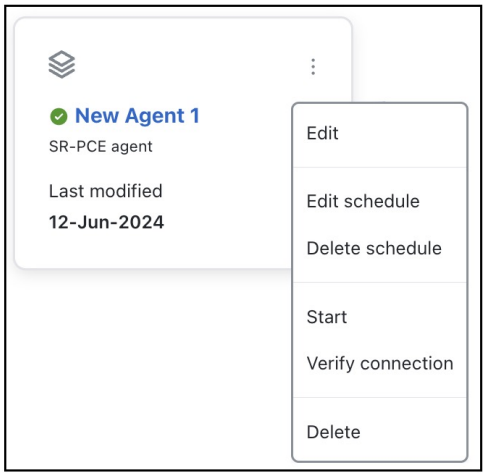
- [スケジュールの削除（Delete schedule）]：エージェントに設定されているデータ更新頻度を削除するには、このオプションを使用します。

（注） このオプションは、SR-PCE エージェントでのみ使用できます。

これらのオプションにアクセスするには、次の手順を実行します。

1. メインメニューから、**[コレクタ（Collector）]** > **[エージェント（Agents）]** の順に選択します。作成済みのエージェントのリストが表示されます。
2. 編集するエージェントの ⋮ をクリックし、関連するオプションを選択します。オプションはエージェントのタイプに応じて異なることに注意してください。

図 *11* : エージェントの操作 - 例



収集の設定

このトピックでは、Cisco Crosswork Planning UI を使用して収集を作成および変更する方法について説明します。

収集の作成

[収集（Collections）] ページには、さまざまなコレクタを使用したネットワークモデルの作成から、収集を実行するためのスケジュールの設定、ネットワークモデルのアーカイブの設定に関する視覚的なワークフローが表示されます。

始める前に

ワークフロー：事前設定手順（12ページ）に示されている手順を完了したことを確認します。

収集を設定するには、次の手順を実行します。

手順

ステップ 1 メインメニューから、**[コレクタ（Collector）] > [収集（Collections）]** の順に選択します。作成済みの収集のリストが表示されます。

ステップ 2 右上隅にある [収集の追加（Add Collection）] をクリックします。[収集の追加（Add Collection）] モーダルウィンドウが開きます。

（注）
初めて収集を作成する場合は、[収集の作成（Create Collection）] ページで [収集の追加（Add Collection）] をクリックします。

ステップ 3 [収集名（Collection Name）] フィールドに、収集の名前を入力します。

ステップ 4 [ノードプロファイル（Node Profile）] ドロップダウンリストから、必要なノードプロファイルを選択します。新しいノードプロファイルを作成する場合は、 [+新規プロファイルの追加（+ Add New Profile）] をクリックします。

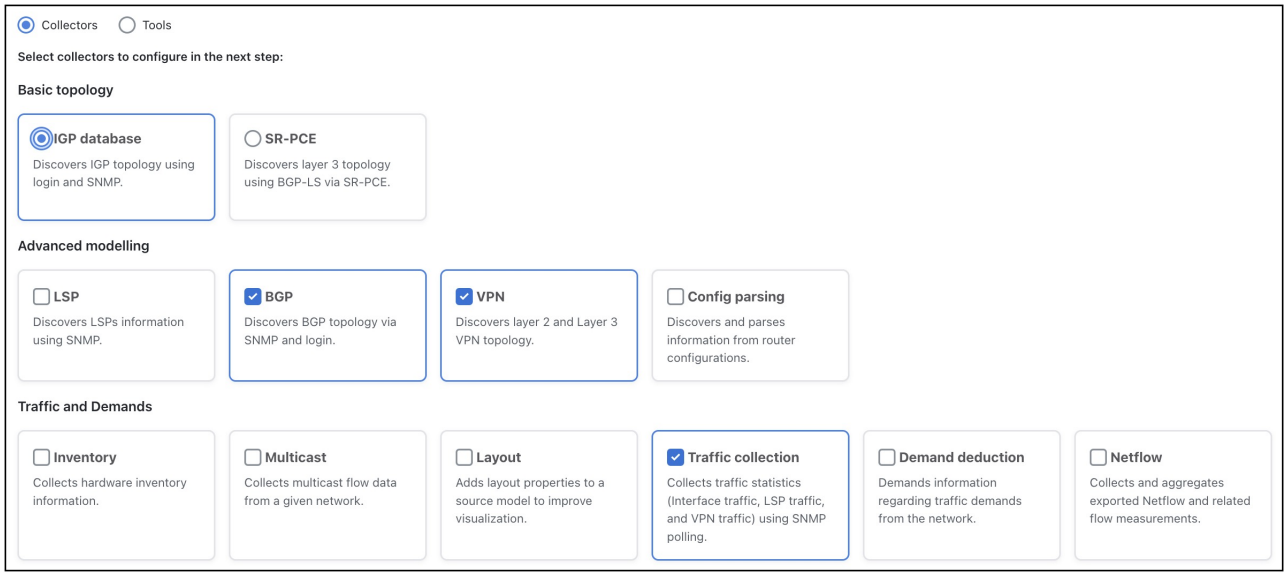
ステップ 5 [続行（Continue）] をクリックします。

上部に番号付きのナビゲーションバーがある [収集設定（Collection Configuration）] ページが表示されます。

ステップ 6 上部の [コレクタ（Collectors）] オプションボタンがクリックされていることを確認します。このオプションは、デフォルトで選択されます。

ステップ 7 必要なコレクタを選択します。ネットワーク収集を開始するには、いずれかの基本トポロジコレクタを選択する必要があります。次に、他のセクションからコレクタを選択します。

図 *12 : [コレクタの選択（Select Collectors）] ページ*



コレクタは、以下のセクションに分類されます。要件に応じて、すべてのセクションからコレクタを選択します。すべてのコレクタの説明については、コレクタの説明 （53 ページ）を参照してください。

- [基本トポロジ（Basic Topology）]：必要な基本トポロジコレクタを選択します。サポートされている基本トポロジコレクタは、IGP データベースと SR-PCE です。選択できるトポロジコレクタは 1 つだけです。
- [高度なモデリング（Advanced Modeling）]：追加のデータ収集を設定するために必要な高度なネットワークデータコレクタを選択します。サポートされている高度なモデリングコレクタは、LSP、BGP、VPN、および構成解析です。複数の高度なコレクタを選択できます。
- [トラフィックとデマンド（Traffic and Demands）]：トラフィック収集に必要なコレクタを選択します。サポートされているトラフィックおよびデマンドコレクタは、インベントリ、マルチキャスト、レイアウト、トラフィック収集、デマンド推論、および NetFlow です。複数のトラフィックコレクタとデマンドコレクタを選択できます。

ステップ 8 設定の 2 番目のステップでは、選択したコレクタの設定パラメータを入力します。次の点に注意してください。

- 左側の [選択されたコレクタ（Selected Collectors）] ペインには、前のステップで選択したコレクタが表示されます。このペインでコレクタ名をクリックして、設定の詳細を入力します。
- [ソース（Source）] ドロップダウンリストから、出力が現在選択されているソース（入力）として機能するコレクタを選択します。
- 特定のコレクタに必要なすべての設定パラメータを入力すると、コレクタ名の横にチェックマークが表示されます。
- 構成プロセス中に選択したコレクタを除外するには、Remove をクリックします。

（注）
選択した各コレクタの設定の詳細を入力する必要があります。入力しないと、[次へ（Next）] ボタンが有効にならず、先に進めません。

図 *13*：収集パラメータの設定

ステップ 9 （オプション）収集モデルに対してカスタマイズされたスクリプトを使用する場合は、[+外部スクリプトの追加（+ Add External Script）] リンクを使用します。詳細については、ネットワークモデルに対する外部スクリプトの実行 （97 ページ） を参照してください。

ステップ 10 すべてのコレクタの設定パラメータを入力したら、[次へ（Next）] をクリックします。

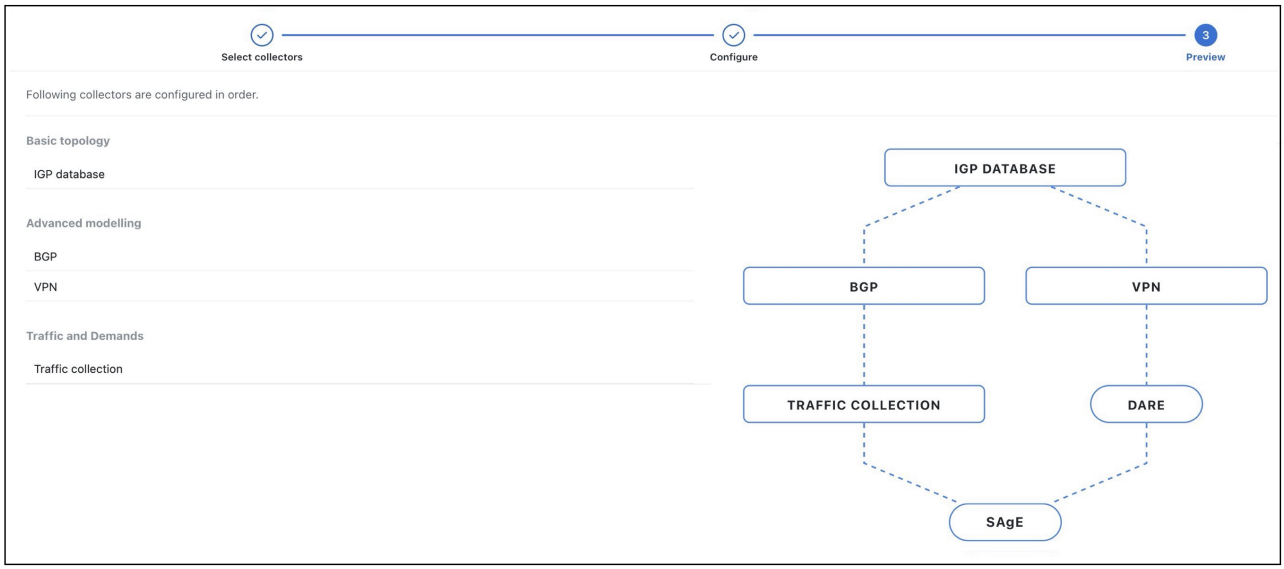
ステップ 11 収集設定の最後の手順は、コレクタが追加された順序をプレビューすることです。プレビュー図では、他のコレクタの入力として使用されているコレクタの出力を確認できます。

設定に問題がない場合は、 [作成（Create）] をクリックして収集の作成を続行します。収集の作成に成功したことを示すメッセージが表示されます。

設定に変更を加える場合は、 [戻る（Back）] をクリックして前のページに戻ります。または、上部にある手順番号をクリックして、必要な設定手順に移動できます。

（注）
- デフォルトでは、すべての変更は変更を加えると自動的に保存されます。[作成（Create）] ボタンをクリックするまで、変更は [ドラフト（Draft）] として保存されます。
- 自動保存は、新しい収集を作成する場合、または収集がドラフト状態の場合にのみ有効になります。既存の収集を編集している場合、変更は自動保存されません。

図 *14* : ページのプレビュー



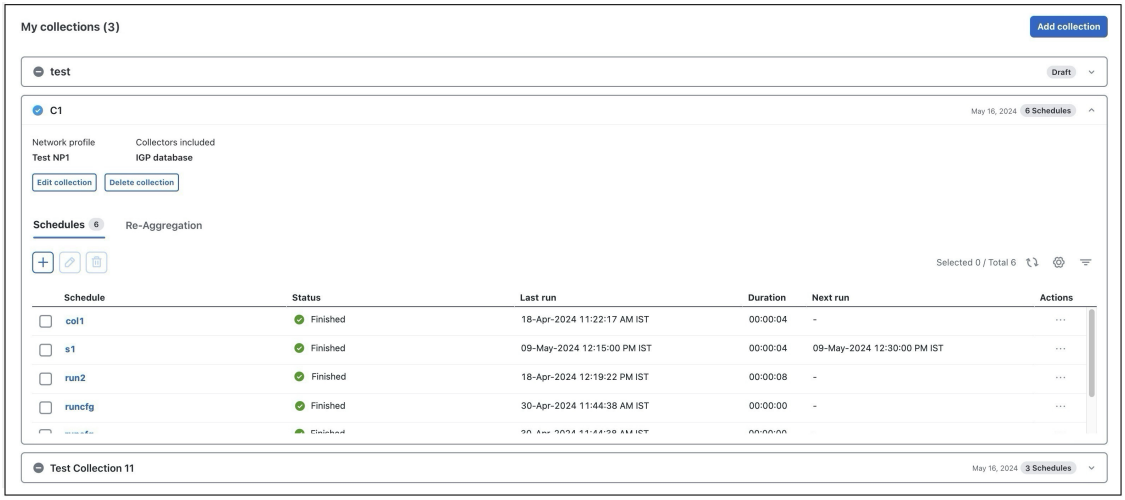
ステップ 12 （オプション）スケジュールをすぐに設定する場合は、ダイアログボックスで [スケジュールの追加（Add Schedule）] をクリックし、スケジュールの設定を続行します。詳細については、スケジュールの追加 （39 ページ） を参照してください。

ステップ 13 成功メッセージボックスで [完了（Done）] をクリックして、収集の作成プロセスを完了します。

新しく追加された収集が **[コレクタ（Collector）] > [収集（Collections）]** ページに表示されます。

次の図は、3 つの収集を含むサンプルの [収集（Collections）] ページを示しています。それぞれの収集パネルを展開して詳細を表示します。

図 *15 :* 使用可能な収集のリスト



次のタスク

収集ジョブのスケジュールを設定します。収集ジョブはすぐに実行するようにスケジュールしたり、特定の間隔で実行するようにスケジュールしたりできます。詳細については、収集のスケジュール （39 ページ） を参照してください。

収集の編集

収集を編集するには、次の手順を実行します。

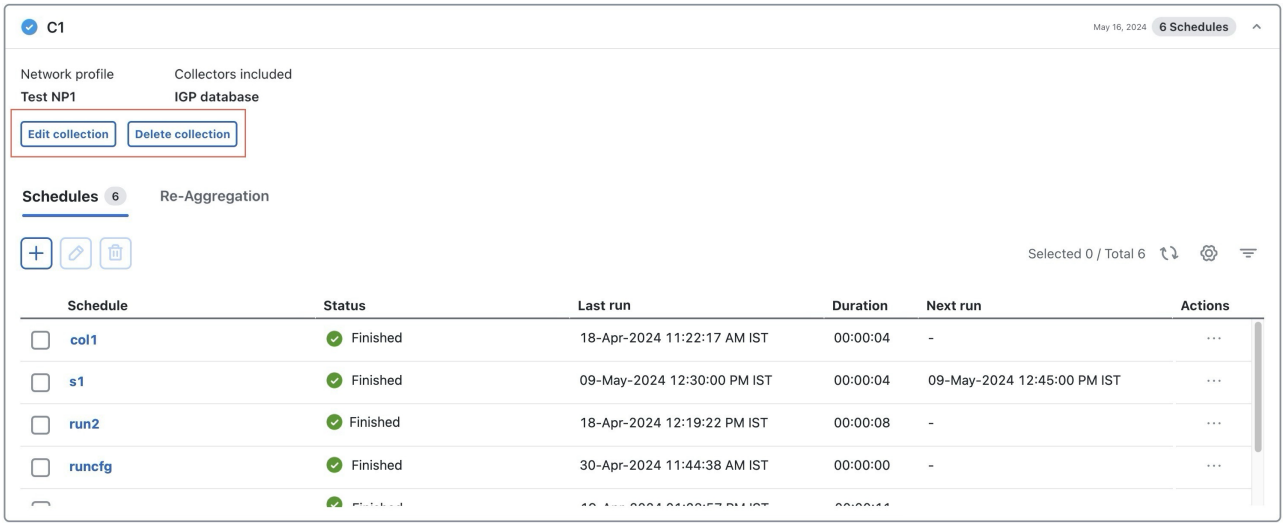
手順

ステップ 1 メインメニューから、**[コレクタ（Collector）]** > **[収集（Collections）]** の順に選択します。作成済みの収集のリストが表示されます（図 15 : 使用可能な収集のリスト （37 ページ）を参照）。

ステップ 2 編集する [収集（Collection）] パネルを展開します。

ステップ 3 [収集の編集（Edit Collection）] をクリックします。

図 *16* : 収集のアクション



ステップ 4 必要に応じて、[コレクタの選択（Select Collectors）] ページと [設定（Configure）] ページで必要な変更を行います。収集の作成 （33 ページ）を参照してください。変更をプレビューし、更新された設定が要件を満たしていることを確認します。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

収集ジョブのスケジュールを設定します。収集ジョブはすぐに実行するようにスケジュールしたり、特定の間隔で実行するようにスケジュールしたりできます。詳細については、スケジュールの追加 （39 ページ）を参照してください。

収集の削除

収集を削除するには、次の手順を実行します。

手順

ステップ 1 メインメニューから、**[コレクタ（Collector）] > [収集（Collections）]** の順に選択します。作成済みの収集のリストが表示されます（図 15 : 使用可能な収集のリスト （37 ページ）を参照）。

ステップ 2 削除する [収集（Collection）] パネルを展開します。

ステップ 3 [収集の削除（Delete collection）] をクリックします（図 16 : 収集のアクション （38 ページ）を参照）。

ステップ 4 確認ダイアログボックスで [はい] をクリックします。

収集の削除に成功したことを示すメッセージが表示されます。

収集のスケジュール

このトピックでは、Cisco Crosswork Planning UI を使用して実行する、さまざまなネットワーク収集のスケジュール方法について説明します。特定の日時に、または定期的に実行するようにジョブをスケジュールできます。また、異なる時間間隔と異なるコレクタ設定を使用して、同じ収集に対して複数のスケジュールを作成できます。

スケジュールの追加

始める前に

- 必要な収集を作成済みであることを確認します。詳細については、収集の作成 （33 ページ） を参照してください。
- cron 式の使用に精通している必要があります。

収集を作成するには、次の手順を実行します。

手順

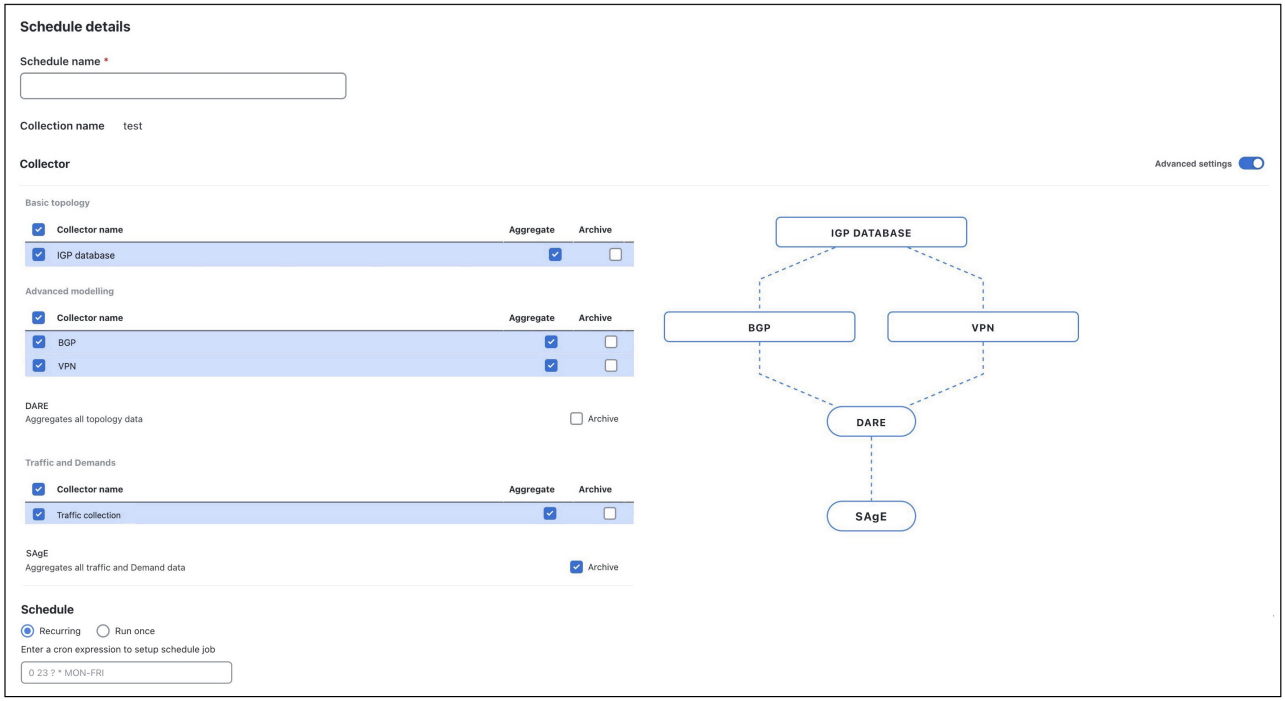
ステップ 1 メインメニューから、**[コレクタ（Collector）]** > **[収集（Collections）]** の順に選択します。作成済みの収集のリストが表示されます（図 15 : 使用可能な収集のリスト （37 ページ）を参照）。

ステップ 2 スケジュールを追加する [収集（Collection）] パネルを展開し、次のいずれかのオプションを使用してスケジュールを作成します。

- 初めてスケジュールを作成する場合は、収集の作成中に、または [収集（Collection）] パネルで [スケジュールの追加（Add Schedule）] ボタンをクリックします。
- 使用可能な他のスケジュールがすでにある場合は、[スケジュール（Schedule）] タブの下にある  アイコンをクリックして、追加のスケジュールを作成します（図 18 : アクションのスケジュール （41 ページ）を参照）。

[スケジュールの詳細（Schedule Details）] ページが表示されます。

図 *17* : スケジュールの詳細



ステップ 3 [スケジュール名（Schedule Name）] フィールドに、スケジューリングジョブの名前を入力します。

ステップ 4 [コレクタ（Collector）] セクションで、次の手順を実行します。

- 収集からコレクタを除外する場合は、そのコレクタ名の横にあるチェックボックスをオフにします。
- コレクタを集約から除外する場合は、対応するコレクタの [集約（Aggregate）] 列の下にあるチェックボックスをオフにします。詳細については、集約コレクタの出力 （43 ページ） を参照してください。
- 収集をアーカイブする場合は、対応するコレクタの [アーカイブ（Archive）] 列の下にあるチェックボックスをオンにします。詳細については、アーカイブの設定 （46 ページ） を参照してください。

ステップ 5 [スケジュール（Schedule）] セクションで、この収集を 1 回だけ実行するか、定期的なジョブとして実行するかを指定します。

- [1回実行（Run Once）] オプションを選択した場合、収集はただちに 1 回だけ実行されます。このオプションを選択すると、下部の [スケジュール（Schedule）] ボタンが [今すぐ実行（Run Now）] に変わるので、クリックして、収集をただちに実行します。
- [繰り返し（Recurring）] オプションを選択した場合は、cron 式を使用して時間間隔を入力します。[繰り返し（Recurring）] オプションは、デフォルトで選択されています。cron 式を入力したら、[スケジュール （Schedule）] をクリックして、指定した時間間隔でジョブを実行します。

設定されたスケジュールは、**[コレクタ （Collector）] > [収集（Collections）]** ページの対応する [収集（Collection）] パネルに表示されます。スケジュールの詳細を表示するには、[スケジュール名（Schedule Name）] 列にあるスケジュールの名前をクリックします。

ステップ 6 （オプション）さらにスケジュールを作成する場合は、ステップ 2 ～ 5 を繰り返します。

スケジュールの編集（Edit Schedules）

スケジュールを編集するには、次の手順を実行します。

手順

ステップ 1 メインメニューから、**[コレクタ（Collector）]** > **[収集（Collections）]** の順に選択します。作成済みの収集のリストが表示されます（図 15 : 使用可能な収集のリスト （37 ページ）を参照）。

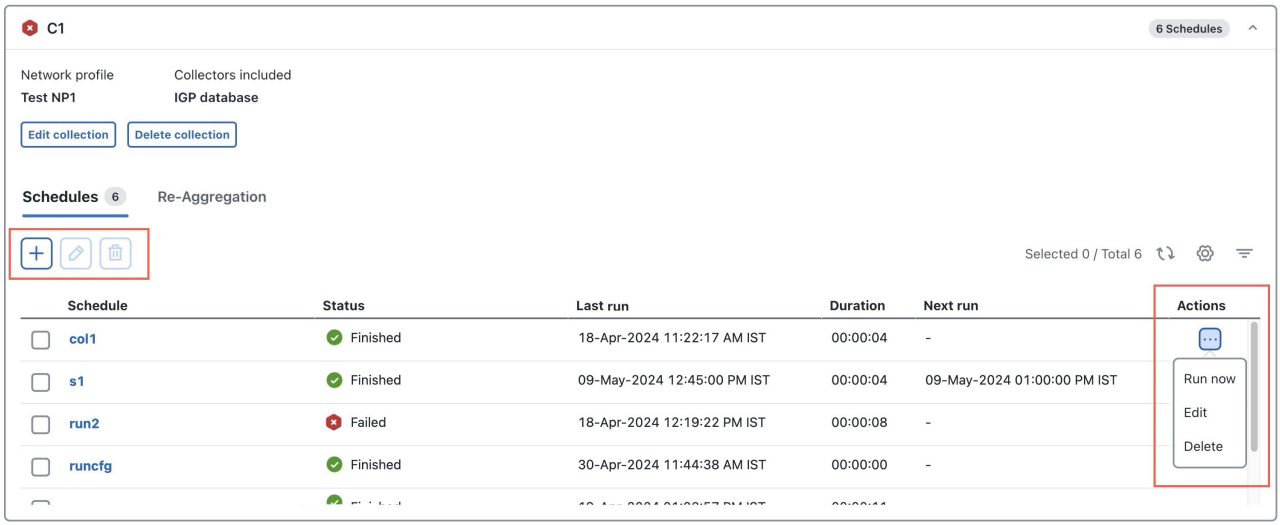
ステップ 2 スケジュールを編集する収集パネルを展開します。

ステップ 3 [スケジュール（Schedules）] タブで、次のいずれかの方法でスケジュールを編集します。

- 編集するスケジュールを選択し、  をクリックします。
- [アクション（Actions）] 列で、編集するスケジュールの ••• > [編集 （Edit）] をクリックします。
- 編集するスケジュールの名前（[スケジュール（Schedule）] 列の下）をクリックし、[編集（Edit）] ボタンをクリックします。

（注）
一度に編集できるスケジュールは 1 つだけです。

図 *18 :* アクションのスケジュール



ステップ 4 [スケジュールの編集（Edit Schedule）] ページで必要な変更を行います。次に、[今すぐ実行（Run Now）] をクリックしてジョブをすぐに実行するか、[スケジュール（Schedule）] をクリックして指定した間隔でジョブを実行します。詳細については、スケジュールの追加 （39 ページ） を参照してください。

スケジュールの削除

スケジュールを削除するには、次の手順を実行します。

手順

ステップ 1 メインメニューから、**[コレクタ（Collector）] > [収集（Collections）]** の順に選択します。作成済みの収集のリストが表示されます（図 15 : 使用可能な収集のリスト （37 ページ）を参照）。

ステップ 2 スケジュールを削除する [収集（Collection）] パネルを展開します。

ステップ 3 [スケジュール（Schedules）] タブで、次のいずれかの方法でスケジュールを削除します（図 18 : アクションのスケジュール （41 ページ）を参照）。

- 削除するスケジュールを選択し、  をクリックします。
- [アクション（Actions）] 列で ··· をクリックし、削除するスケジュールの [削除（Delete）] をクリックします。

（注）
一度に削除できるスケジュールは 1 つだけです。

ステップ 4 確認ダイアログボックスで [はい] をクリックします。

スケジュールが正常に削除されたことを示すメッセージが表示されます。

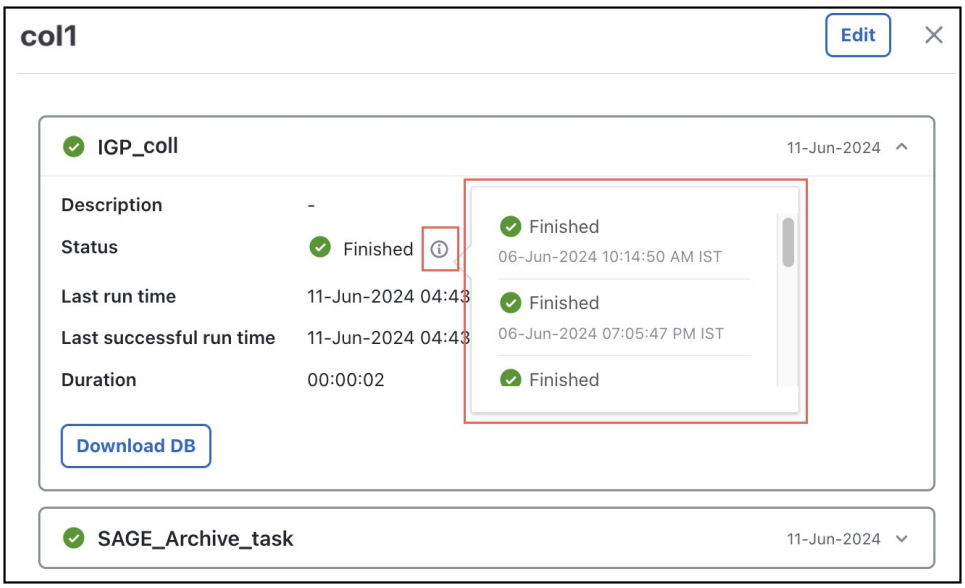
スケジュールタスクのステータスと履歴の表示

収集のスケジュールを設定すると、関連するタスクの現在のステータスと最新の 10 個のステータスを表示できます。

手順は次のとおりです。

1. 収集パネルを展開します。
2. [スケジュール（Schedules）] タブでスケジュールの名前をクリックします。

   開いたページには、スケジュールされた収集に関連するすべてのタスクのステータスが、最近のタスク実行のタイムスタンプ、タスクの期間、および説明（タスクが失敗した場合）とともに表示されます。



3. [ステータス（Status）] フィールドの ⓘ アイコンをクリックすると、最新の 10 個のタスク ステータスが表示されます。

[DBのダウンロード（Download DB）] を クリックして、収集されたデータをコレクタからダウンロードします。

集約コレクタの出力

各コレクタは出力を生成します。これらの出力が集約（統合）されて完全なネットワークモデルが構築されます。Cisco Crosswork Planning は、Delta Aggregation Rules Engine（DARE）を使用して、基本および高度なトポロジコレクタ出力を集約します。Simple Aggregation Engine（SAgE）は、DARE からのトポロジ変更とともにすべてのトラフィックおよびデマンドデータを統合し、最終的なネットワークモデルの作成を支援します。

デフォルトでは、選択したすべてのコレクタがコレクタの設定時に集約に含まれます。収集のスケジュール時に、任意のコレクタを集約から除外できます。除外することで、除外されたコレクタからデータが収集されても、集約されません。

（注） このトピックで説明されている手順は、ネットワークモデルの作成中に実行することを想定しています。詳細については、収集の作成 （33 ページ）を参照してください。

コレクタの出力を集約から除外するには、次の手順を実行します。

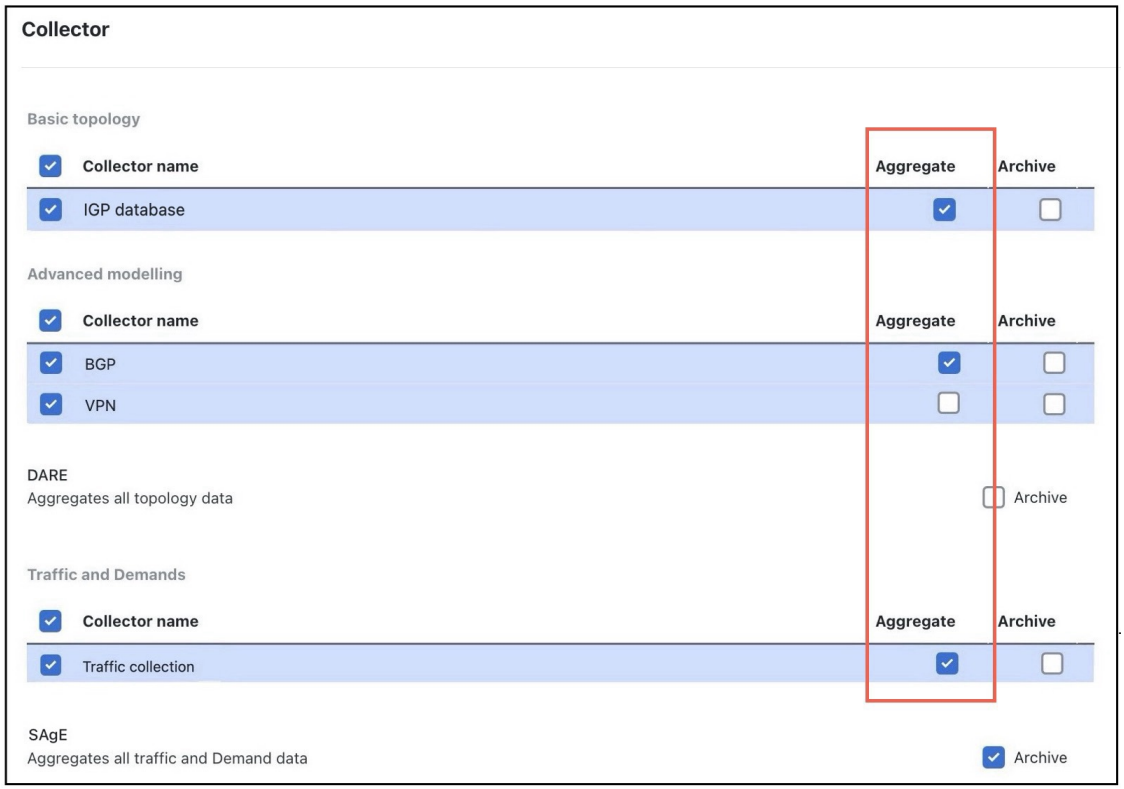
手順

ステップ 1 編集する収集の [スケジュールの追加または編集（Add or Edit Schedules）] ページを開きます。詳細については、スケジュールの追加 （39 ページ）またはスケジュールの編集（Edit Schedules） （41 ページ）を参照してください。

ステップ 2 （オプション）[詳細設定（Advanced Settings）] トグルボタンはデフォルトでオンになってます。オンになっていない場合は、オンにします。

ステップ 3 [コレクタ（Collector）] セクションで、集約から除外するコレクタの [集約（Aggregate）] チェックボックスをオフにします。

図 *19* : 集約設定



ステップ 4 （オプション）スケジュール設定を更新します。詳細については、スケジュールの追加 （39 ページ） を参照してください。

ステップ 5 前のステップで [1回実行（Run Once）] を選択した場合は、[今すぐ実行（Run Now）] をクリックしてジョブをすぐに実行します。[繰り返し（Recurring）] を選択した場合は、[スケジュール（Schedule）] をクリックして、指定した時間間隔でジョブを実行します。

いずれかのコレクタの [集約（Aggregate）] チェックボックスをオフにすると、そのコレクタから収集される後続のデータは集約されません。ただし、オフになっていないコレクタから以前に収集されていたデータは、アグリゲータの出力で引き続き使用できます。

コレクタ出力の再集約

収集プロセス中の任意の時点で、すべてのコレクタの再集約を実行し、DARE および SAgE ネットワークを新たに作成できます。このオプションを使用すると、データ収集は行われませんが、それまでに作成された集約モデルは破棄され、新しい集約プロセスが開始されます。

（注） 収集では、次の点に注意してください。

- 再集約に使用できるスケジューラは 1 つだけです。
- 集約に含まれているコレクタのみが再集約の対象と見なされます。

再集約を実行するには、次の手順を実行します。

手順

ステップ 1 メインメニューから、**[コレクタ（Collector）]** > **[収集（Collections）]** の順に選択します。作成済みの収集のリストが表示されます（図 15 : 使用可能な収集のリスト （37 ページ）を参照）。

ステップ 2 コレクタ出力を再集約する収集パネルを展開します。

ステップ 3 [再集約（Re-Aggregation）] タブをクリックします。

ステップ 4 再集約を初めて実行する場合は、 [スケジュール（Schedule）] または [1回実行（Run once）] ボタンをクリックします。初回ではない場合は、スケジュールを更新するか、次の手順で説明するオプションを使用して集約を再実行します。

- [1回実行（Run Once）] オプションを選択した場合、再集約がただちに 1 回だけ実行されます。
- [スケジュール（Schedule）] オプションを選択した場合、cron 式を使用してデータ更新頻度を入力し、[保存（Save）] をクリックします。データの再同期は、指定した時間間隔で実行されます。

図 *20 :* 収集の再集約

[ネットワーク再集約（Network ReAggregation）] エントリがテーブルに表示され、ジョブのステータスと詳細が示されます。

ステップ 5 必要に応じて、[アクション（Actions）] 列の ••• を使用して、スケジュールを更新するか、再集約をもう一度実行します。前の手順で選択したオプションに応じて、このボタンの下に表示されるオプションは若干異なります。

前の手順で [スケジュール（Schedule）] オプションを選択した場合は、このボタンには [今すぐ実行（Run now）]、[スケジュールの編集（Edit schedule）]、[一時停止（Pause）]、および [削除（Delete）] が表示されます。[1回実行（Run once）] オプションを選択した場合は、[今すぐ実行（Run now）]、[スケジュールの追加（Add schedule）]、および [削除（Delete）] が表示されます。

ステップ 6 （オプション）テーブルの [ネットワーク再集約（Netwok ReAggregation）] リンクをクリックすると、集約の詳細が表示されます。

アーカイブの設定

アーカイブは、プランファイルのリポジトリです。ネットワークモデルを作成し、収集を実行すると、プランファイルを取得して表示できます。プランファイルは、特定の時点でのネットワークに関するすべての関連情報をキャプチャし、トポロジ、トラフィック、ルーティング、および関連情報が含まれます。

同じマシンに Cisco Crosswork Planning Design アプリケーションがインストールされている場合、アーカイブされたネットワークモデルは **[ネットワークモデル（Network Models）] > ローカルアーカイブ（Local Archive）]** に表示されます。

デフォルトでは、最終的なネットワークモデルは、収集の実行後にアーカイブされます。ただし、[スケジュールの追加または編集（Add or Edit Schedules）] ページでは、次のことができます。

- 最終的なネットワークモデルをアーカイブしないことを選択する
- 収集レベルでモデルをアーカイブすることを選択する
- ネットワークモデルのアーカイブをスケジュールする。

（注） このトピックで説明されている手順は、ネットワークモデルの作成中に実行することを想定しています。詳細については、収集の作成 （33 ページ）を参照してください。

手順

ステップ 1 編集する収集の [スケジュールの追加または編集（Add or Edit Schedules）] ページを開きます。詳細については、スケジュールの追加 （39 ページ）またはスケジュールの編集（Edit Schedules） （41 ページ）を参照してください。

ステップ 2 （オプション）[詳細設定（Advanced Settings）] トグルボタンはデフォルトでオンになってます。オンになっていない場合は、オンにします。

ステップ 3 [コレクタ（Collector）] セクションで、次の手順を実行します。

- 収集レベルでネットワークモデルをアーカイブする場合は、対応する収集の [アーカイブ（Archive）] 列の下にあるチェックボックスをオンにします。
- 最終的なネットワークモデルをアーカイブしない場合は、SAgE の横にある [アーカイブ（Archive）] チェックボックスをオフにします。

図 *21* : アーカイブ設定

ステップ 4 （オプション）スケジュール設定を更新します。詳細については、スケジュールの追加 （39 ページ） を参照してください。

ステップ 5 前のステップで [1回実行（Run Once）] を選択した場合は、[今すぐ実行（Run Now）] をクリックしてジョブをすぐに実行します。[繰り返し（Recurring）] を選択した場合は、[スケジュール（Schedule）] をクリックして、指定した時間間隔でジョブを実行します。

最終的なネットワークモデルでは、チェックされていないコレクタから収集されたデータは使用できません。

アーカイブされたネットワークモデルは、[ネットワークモデル（Network Models）] ページの [アーカイブ（Archive）] セクションにプランファイル形式（.pln）で保存されます。

次のタスク

Cisco Crosswork Planning Design アプリケーションからプランファイルにアクセスします。詳細については、プランファイルの表示またはダウンロード （48 ページ）を参照してください。

プランファイルの表示またはダウンロード

アーカイブされたネットワークモデルはプランファイル形式（.pln）で保存され、Cisco Crosswork Planning Design アプリケーションの [ネットワークモデル（Network Models）] ページからダウンロードまたは表示できます。アーカイブの場所は、Cisco Crosswork Planning Design および Collector アプリケーションが同じマシンにインストールされているか、別のマシンにインストールされているかによって異なります。詳細については、以下の項を参照してください。

シナリオ 1：Cisco Crosswork Planning Design アプリケーションと Collector アプリケーションが同じマシンにインストールされている場合

同じマシンに Cisco Crosswork Planning Design および Collector アプリケーションがインストールされている場合、アーカイブされたネットワークモデルは **[ネットワークモデル（Network Models）] > [ローカルアーカイブ（Local archive）]** に表示されます。

ローカルアーカイブからプランファイルを表示またはダウンロードするには、次の手順を実行します。

始める前に

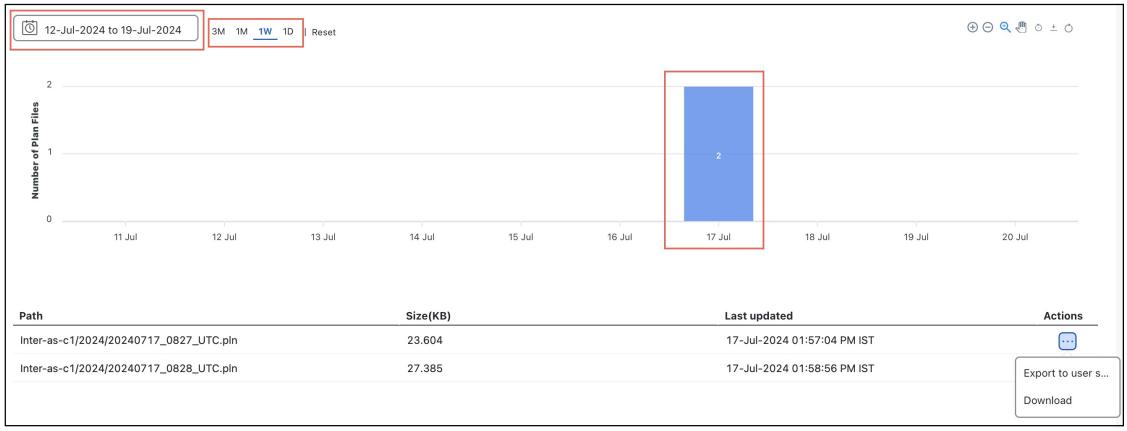
- ネットワークモデルがアーカイブされていることを確認します。詳細については、アーカイブの設定 （46 ページ） を参照してください。

手順

ステップ 1 メインメニューから、[ネットワークモデル（Network Models）] を選択します。

ステップ 2 左ペインの [ローカルアーカイブ（Local archive）] の下に、アーカイブされた収集のリストが表示されます。リストから必要な収集名を選択します。右側のパネルには、さまざまなスケジュールされた時間にこの収集で作成されたプランファイルのリストが表示されます。[最終更新日（Last updated）] 列には、プランファイルが作成された時刻が表示されます。

図 *22*：アーカイブされたプランファイル



プランファイルは、いくつかの方法でフィルタ処理できます。

- 上部の日付範囲選択フィールドを使用して、必要な開始日と終了日を選択します。選択した日付範囲に生成されたプランファイルが下部に表示されます。
- 日付範囲選択フィールドの横にあるリンクを使用して、過去 3 か月（3M）、過去 1 か月（1M）、過去 1 週間（1W）、または前日（1D）に生成された計画ファイルを表示します。
- グラフのバーをクリックすると、特定の日付や時刻に生成されたプランファイルが表示されます。関連するバーセグメントをクリックし続けると、正確なタイムスタンプにドリルダウンします。

ステップ 3 右側のパネルから必要なプランファイルを選択し、[アクション（Actions）]列で ••• をクリックし、[ユーザースペースにエクスポート（Export to user space）] をクリックします。

[プランをユーザースペースにエクスポート（Export plan to User Space）] ウィンドウが表示されます。

（注）
プランファイルをローカルマシンにダウンロードするには、[アクション（Actions）] 列で ••• をクリックし、[ダウンロード（Download）] をクリックします。

ステップ 4 （オプション）[名前を付けて保存（Save as）] フィールドに、プランファイルの新しい名前を入力します。

ステップ 5 （オプション）リストから必要なタグを選択するか（存在する場合）、新しいタグを作成します。

新しいタグを作成するには、[新しいタグの追加（Add new tag）]をクリックし、タグ名を入力して、フィールドの横にある + アイコンをクリックします。

ステップ 6 [保存（Save）] をクリックします。

プランファイルは、[ユーザースペース（User space）] > [マイネットワークモデル（My network models）] ページにインポートされます。

ステップ 7 [ユーザースペース（User space）] > [マイネットワークモデル（My network models）] ページでファイルの名前をクリックして、 [ネットワーク設計（Network Design）] ページでネットワークモデルを可視化します。詳細については、*Cisco Crosswork Planning Design 7.0* ユーザーガイドを参照してください。

シナリオ 2：Cisco Crosswork Planning Design アプリケーションと Collector アプリケーションが異なるマシンにインストールされている場合

Cisco Crosswork Planning Design アプリケーションと Collector アプリケーションが異なるマシンにインストールされている場合、アーカイブされたネットワークモデルは、Cisco Crosswork Planning Design アプリケーションの **[ネットワークモデル（Network Models）] > [リモートアーカイブ（Remote archive）]** に表示されます。

次のワークフローの概要では、外部コレクタからネットワークモデルにアクセスする方法について説明します。

表 7: ワークフロー：外部コレクタからネットワークモデルへのアクセス

手順	操作
1.Cisco Crosswork Planning Collector アプリケーションがインストールされているマシンにネットワークモデルがアーカイブされていることを確認します。	アーカイブの設定 （46 ページ）を参照してください。
2.Cisco Crosswork Planning Collector アプリケーションがインストールされているマシンに接続します（外部コレクタ）。	外部コレクタへの接続 （50 ページ）を参照してください。
3. リモートアーカイブからネットワークモデルにアクセスします。	リモートアーカイブからのプランファイルの表示またはダウンロード （51 ページ） を参照してください。

外部コレクタへの接続

別のマシンの Cisco Crosswork Planning コレクタインスタンス（外部コレクタ）に接続するには、次の手順を実行します。

手順

ステップ 1 Cisco Crosswork Planning Design アプリケーションがインストールされているマシンにログインします。

ステップ 2 メインメニューから、**[管理（Administration）] > [設定（Settings）] > [Designの設定（Design settings）] > [外部コレクタ収集（External collector collection）]** を選択します。

ステップ 3 [ホスト名/IPアドレス（Host name/IP address）] フィールドに、Cisco Crosswork Planning Collector アプリケーションがインストールされているマシン（外部コレクタ）のホスト名または IP アドレスを入力します。

ステップ 4 マシンのポート、ユーザー名、およびパスワードの詳細を入力します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 メインメニューから [ネットワークモデル（Network Models）] を選択し、左側のペインに [リモートアーカイブ（Remote archive）] オプションが表示されていることを確認します。ここには、外部コレクタにアーカイブされた収集が表示されます。

次のタスク

リモートアーカイブから、アーカイブされたネットワークモデルを表示またはダウンロードします。詳細については、リモートアーカイブからのプランファイルの表示またはダウンロード（51 ページ） を参照してください。

リモートアーカイブからのプランファイルの表示またはダウンロード

リモートアーカイブからプランファイルを表示またはダウンロードするには、次の手順を実行します。

手順

ステップ 1 Cisco Crosswork Planning Design アプリケーションがインストールされているマシンにログインします。

ステップ 2 メインメニューから、[ネットワークモデル（Network Models）] を選択します。

ステップ 3 左ペインの [リモートアーカイブ（Remote archive）] の下に、外部コレクタにアーカイブされた収集のリストが表示されます。リストから必要な収集名を選択します。右側のパネルには、さまざまなスケジュールされた時間にこの収集で作成されたプランファイルのリストが表示されます。[最終更新日（Last updated）] 列を使用して、プランファイルが作成された時刻を確認します。

プランファイルは、いくつかの方法でフィルタ処理できます（図 22 : アーカイブされたプランファイル（49 ページ） を参照）。

- 上部の日付範囲選択フィールドを使用して、必要な開始日と終了日を選択します。選択した日付範囲に生成されたプランファイルが下部に表示されます。
- 日付範囲選択フィールドの横にあるリンクを使用して、過去 3 か月（3M）、過去 1 か月（1M）、過去 1 週間（1W）、または前日（1D）に生成された計画ファイルを表示します。

- グラフのバーをクリックすると、特定の日付や時刻に生成されたプランファイルが表示されます。関連するバーセグメントをクリックし続けると、正確なタイムスタンプにドリルダウンします。

ステップ 4 右側のパネルから必要なプランファイルを選択し、[アクション（Actions）] 列で ··· をクリックし、[ユーザースペースにエクスポート（Export to user space）] をクリックします。

[プランをユーザースペースにエクスポート（Export Plan to User Space）] ウィンドウが表示されます。

（注）
プランファイルをローカルマシンにダウンロードするには、[アクション（Actions）] 列で ··· をクリックし、[ダウンロード（Download）] をクリックします。

ステップ 5 （オプション）[名前を付けて保存（Save as）] フィールドに、プランファイルの新しい名前を入力します。

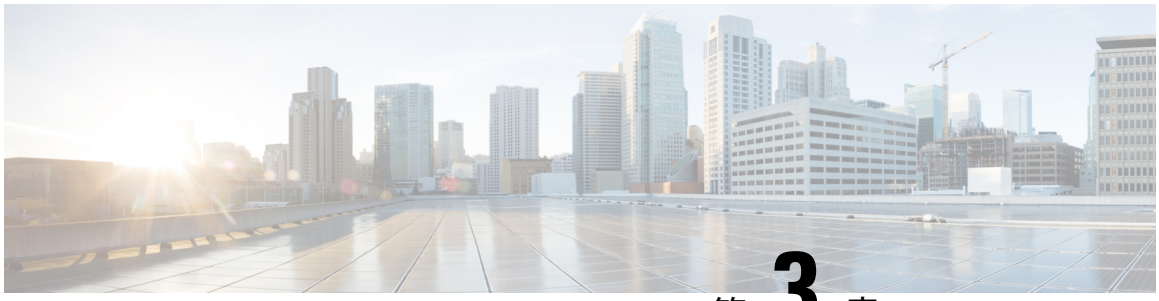
ステップ 6 （オプション）リストから必要なタグを選択するか（存在する場合）、新しいタグを作成します。

新しいタグを作成するには、[新しいタグの追加（Add new tag）] をクリックし、タグ名を入力して、フィールドの横にある + アイコンをクリックします。

ステップ 7 [保存（Save）] をクリックします。

プランファイルは、[ユーザースペース（User space）] > [マイネットワークモデル（My network models）] ページにインポートされます。

ステップ 8 [ユーザースペース（User space）] > [マイネットワークモデル（My network models）] ページでファイルの名前をクリックして、[ネットワーク設計（Network Design）] ページでネットワークモデルを可視化します。詳細については、*Cisco Crosswork Planning Design 7.0* ユーザーガイドを参照してください。



第 3 章

サポートされるコレクタとツール

ここでは、次の内容について説明します。

コレクタの説明

Cisco Crosswork Planning の各コレクタには、収集または展開対象を決定する機能があります。

表 *8*：コレクタの説明

コレクター	説明	前提条件/注意事項	設定手順
基本的なトポロジ収集			

コレクター	説明	前提条件/注意事項	設定手順
IGP データベース	ログインと SNMP を使用して IGP トポロジを検出します。	これは、基本的なトポロジ収集です。結果として得られるネットワークモデルは、他のコレクタの送信元ネットワークとして使用されます。	IGP データベースコレクタを使用したトポロジ情報の収集 （56 ページ）を参照してください。
SR-PCE	SR-PCE 経由で BGP-LS を使用してレイヤ 3 トポロジを検出します。トポロジの送信元として生の SR-PCE データを使用します。ノードおよびインターフェース/ポートのプロパティは、SNMP を使用して検出されます。	• この収集を実行する前に、SR-PCE エージェントを設定する必要があります。詳細については、エージェントの設定 （27 ページ） を参照してください。 • これは、SR-PCE を使用するネットワークの基本的なトポロジ収集です。結果として得られるネットワークモデルは、他のコレクタの送信元ネットワークとして使用されます。	SR-PCE コレクタを使用したトポロジ情報の収集 （58 ページ）を参照してください。
高度なモデリング収集			
LSP	SNMP を使用して LSP 情報を検出します。	• 基本的なトポロジ収集を備えたネットワークモデルが存在する必要があります。 • SR-PCE を使用している場合は、この収集を実行する前に SR-PCE コレクタを使用したトポロジ情報の収集 （58 ページ） を完了する必要があります。	LSP 情報の収集 （62 ページ）を参照してください。
PCEP LSP	（SR-PCE コレクタが基本トポロジコレクタとして選択されている場合にのみアクセス可能）SR-PCE を使用して PCEP LSP を検出します。	収集を実行する前に、SR-PCE コレクタを使用したトポロジ情報の収集 （58 ページ） を完了する必要があります。	SR-PCE を使用した PCEP LSP 情報の収集 （64 ページ）を参照してください。
BGP	ログインと SNMP を使用して BGP ピアリングを検出します。	基本的なトポロジ収集を備えたネットワークモデルが存在する必要があります。	BGP ピアリングの検出 （70 ページ）を参照してください。

コレクター	説明	前提条件/注意事項	設定手順
VPN	レイヤ 2 およびレイヤ 3 VPN トポロジを検出します。	基本的なトポロジ収集を備えたネットワークモデルが存在する必要があります。	VPN トポロジの検出 （73 ページ）を参照してください。
構成解析	ネットワーク内のルータ設定から情報を検出して解析します。	基本的なトポロジ収集を備えたネットワークモデルが存在する必要があります。	構成解析を使用したポート、LSP、SRLG、および VPN 情報の収集 （83 ページ）を参照してください。
トラフィックとデマンドの収集			
インベントリ	ハードウェアインベントリ情報を収集します。	基本的なトポロジ収集を備えたネットワークモデルが存在する必要があります。	ハードウェアインベントリ情報の収集 （75 ページ）を参照してください。
マルチキャスト	特定のネットワークからマルチキャストフローデータを収集します。	基本的なトポロジ収集を備えたネットワークモデルが存在する必要があります。	ネットワークからのマルチキャスト フロー データのコレクタ （66 ページ）を参照してください。
レイアウト（Layout）	送信元モデルにレイアウトプロパティを追加して、視覚化を改善します。	• 集約ネットワークモデル。 • レイアウトコレクタを設定したら、レイアウトのプロパティを含むプランファイルをレイアウトモデルにインポートして戻す必要があります。	ネットワークモデルの可視化の向上 （87 ページ）を参照してください。
トラフィック収集	SNMP ポーリングを使用して、トラフィック統計情報（インターフェイス トラフィック、LSP トラフィック、MAC トラフィック、および VPN トラフィック）を収集します。	• 基本的なトポロジ収集を備えたネットワークモデルが存在する必要があります。 • LSP トラフィックを収集する場合、LSP を備えたネットワークモデルが存在する必要があります。LSP 情報の収集 （62 ページ） を参照してください。 • VPN トラフィックを収集する場合、VPN を備えたネットワークモデルが存在する必要があります。VPN トポロジの検出 （73 ページ）を参照してください。	トラフィック統計情報の収集 （89 ページ）を参照してください

コレクター	説明	前提条件/注意事項	設定手順
デマンド推論	ネットワークからトラフィックデマンドに関する情報を収集します。	トラフィックデータを含む送信元 DARE ネットワークが存在する必要があります。	トラフィックデマンド情報の収集 （92 ページ）を参照してください。
NetFlow	エクスポートされた NetFlow および関連するフロー測定値を収集して集約します。	基本的なトポロジ収集を備えたネットワークモデルが存在する必要があります。	NetFlow 収集を構成する （94 ページ）を参照してください。
カスタム スクリプト			
外部スクリプト	カスタマイズされたスクリプトを実行して、送信元ネットワークモデルに追加データを付加します。	送信元ネットワークモデルとカスタムスクリプトが存在する必要があります。	ネットワークモデルに対する外部スクリプトの実行 （97 ページ）を参照してください

基本的なトポロジ情報の収集

基本的なトポロジ収集から得られるネットワークモデルは、追加のデータ収集のソースネットワークとして使用されます。Cisco Crosswork Planning 内には、この目的で使用される 2 つのコレクタ、**IGP データベース** と **SR-PCE** があります。トポロジ情報を収集するようにこれらのコレクタを設定する方法の詳細については、IGP データベースコレクタを使用したトポロジ情報の収集 （56 ページ）およびSR-PCE コレクタを使用したトポロジ情報の収集 （58 ページ）を参照してください。

IGP データベースコレクタを使用したトポロジ情報の収集

Cisco Crosswork Planning には、IGP データベースと SR-PCE の 2 つのトポロジコレクタがあります。単一の収集では、トポロジに関連する情報を収集するために、いずれかのコレクタを選択できます。両方のコレクタは選択できません。

トポロジ収集に SR-PCE コレクタを使用するには、SR-PCE コレクタを使用したトポロジ情報の収集 （58 ページ）を参照してください。

IGP データベースコレクタは、ノードプロパティの収集、および SNMP を使用したインターフェイスとポートの検出により、IGP データベースを使用してネットワークトポロジを検出します。このコレクタは、必要となる基本的なデータ収集を提供するため、通常、他のコレクタの前に最初に設定されます。このコレクタは、完全なトポロジディスカバリを提供します。OSPF および IS-IS のマルチインスタンスの収集もサポートされています。ルータから収集されたすべてのリンクには、関連付けられた IGP プロセス ID があります。

トポロジディスカバリの結果得られたネットワークモデルは、他のコレクタが使用するコアノード、回路、およびインターフェイス情報を提供するため、追加の収集用の送信元ネットワークとして使用されます。

始める前に

- ワークフロー：事前設定手順 （12 ページ）に記載されている手順を実行します。

IGP データベースコレクタを設定するには、次の手順を実行します。

手順

ステップ 1 新しい収集を作成するか、既存の収集を編集するかを決定します。詳細については、収集の作成 （33 ページ）または収集の編集 （37 ページ）を参照してください。

ステップ 2 [基本トポロジ（Basic topology）] セクションで [IGPデータベース（IGP database）] を選択し、[次へ（Next）] をクリックします。

ステップ 3 [設定（Configure）] ページの [シードルータ（Seed router）] セクションで、次の設定パラメータを入力します。

- [インデックス（Index）]：シードルータのインデックス番号。
- [ルータIP（Router IP）]：シードルータの管理 IP アドレス。
- [プロトコルタイプ（Protocol Type）]：ネットワークで実行されている IGP プロトコルを選択します。オプションは、[OSPF]、[OSPFv3]、[IS-IS]、および [IS-ISv6] です。

  [プロトコルタイプ（Protocol Type）] として [OSPF] または [OSPFv3] を選択した場合は、[詳細（Advanced）] ページの [OSPF] エリアの値を入力します（⚙ をクリック）。OSPF エリアオプションでは、エリアID または すべてを指定します。デフォルトは area 0 です。

  [プロトコルタイプ（Protocol Type）] として [IS-IS] または [IS-ISv6] を選択した場合は、[詳細（Advanced）] ページで [IS-ISレベル（ISIS level）] の値（1、2、または両方）を入力します（⚙ をクリック）。デフォルトのレベルは 2 です。

- [インターフェイスの収集（Collect Interfaces）]：完全なネットワークトポロジを検出するには、このチェックボックスをオンにします。デフォルトで、このオプションは有効になっています。

ステップ 4 （オプション）シードルータを追加するには、[+ルータの追加（+ Add Router）] をクリックし、各シードルータに対してステップ 3 を繰り返します。インデックス番号が各シードルータに対して一意であることを確認します。

ステップ 5 （オプション）ノードから個々の QoS 情報を除外するか含めるには、[詳細設定（Advanced settings）] > [QoSノードフィルタ（QoS Node Filter）] セクションで、[+ノードフィルタの追加（+ Add node filter）] をクリックし、必要に応じて値を入力します。

ステップ 6 （オプション）[詳細設定（Advanced settings）] パネルを展開し、関連するフィールドに詳細を入力します。詳細オプションの説明については、IGP および SR-PCE コレクタの詳細オプション （60 ページ）を参照してください。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 設定をプレビューし、[作成（Create）] をクリックして収集を作成します。

次のタスク

- 収集ジョブのスケジュールを設定します。収集ジョブはすぐに実行するようにスケジュールしたり、特定の間隔で実行するようにスケジュールしたりできます。詳細については、収集のスケジュール （39 ページ） を参照してください。
- この収集を送信元ネットワークとして使用して、追加の収集を設定します。さまざまなコレクタの設定の詳細については、この章の関連トピックを参照してください。収集の編集の詳細については、収集の編集 （37 ページ）を参照してください。

SR-PCE コレクタを使用したトポロジ情報の収集

（注） Cisco Crosswork Planning には、IGP データベースと SR-PCE の 2 つのトポロジコレクタがあります。単一の収集では、トポロジに関連する情報を収集するために、いずれかのコレクタを選択できます。両方のコレクタは選択できません。

トポロジ収集に IGP データベースコレクタを使用するには、「IGP データベースコレクタを使用したトポロジ情報の収集 （56 ページ）」を参照してください。

SR-PCE コレクタは、SR-PCE を使用してレイヤ 3 トポロジを検出します。SR-PCE エージェントは、SR-PCE サーバーに接続し、サーバーから送信されたテレメトリデータを処理する Cisco Crosswork Planning コンポーネントです。SR-PCE エージェントは、SR-PCE との 2 つの異なる REST 接続を使用します。1 つは LSP 用、もう 1 つはトポロジデータ収集用です。トポロジと LSP データの収集後、SR-PCE エージェントは（オプションで）SR-PCE にサブスクライブし、さらなるネットワーク変更イベントをリッスンします。

ノードおよびインターフェース/ポートのプロパティは、SNMP を使用して検出されます。テスト目的では、SNMP アクセスが利用できない場合、SR-PCE のみを使用して（[拡張ディスカバリ（Extended discovery）] フィールドは無効の状態で）SR-PCE トポロジディスカバリを使用することもできます。トポロジディスカバリの結果得られたネットワークモデルは、他のコレクタが使用するコアノード、回路、およびインターフェイス情報を提供するため、追加の収集用の送信元ネットワークとして使用されます。

SR-PCE コレクタにより、IGP メトリック、遅延、およびノードオーバーロードの変更によるネットワーク更新もキャプチャされるようになりました。

このコレクタにより、FlexAlgoAffinities、FlexAlgorithms、SRv6NodeSIDs、SRv6InterfaceSIDs、NodePrefixLoopbacks、および NodeSIDPrefixLoopbacks テーブルにデータが入力されます。SRv6 に関連付けられたループバックアドレスは SR-PCE を使用して取得されないため、SRv6NodeSIDPrefixLoopbacks テーブルにはデータが入力されません。

（注） デフォルトでは、NodePrefixLoopbacks の ISIS レベルは level2 に設定されています。同じ内容が OSPF ネットワークにも入力されます。

Cisco Crosswork Planning は、FlexAlgo 列の非 null から null 値への更新を反映しません。値は、意図的な DARE 再同期の後に反映され始めます。

IPv4 メトリック値は IGP メトリックテーブルに入力され、Ipv6 値は IPv6-IGP メトリックテーブルに入力されます。TE メトリック値も同様に更新されます。

SR-PCE コレクタは、NetIntXtcLinks の LocalDomainIdentifier 列を読み取り、インターフェイステーブルに IGP プロセス ID を入力します。

（注） デュアルスタックサポート（IPv4 と IPv6 の両方を同時に処理する機能）、およびインターフェイス上の OSPF または ISIS の設定は、データ収集の一部として正しく入力されます。ただし、SR-PCE 収集中に、デュアルプロトコル（OSPF および ISIS）がデータ収集用の単一インターフェイスで有効になっている場合、デュアルスタックとそのインターフェイス解決はサポートされません。

始める前に

- ワークフロー：事前設定手順 （12 ページ）に記載されている手順を実行します。
- SR-PCE エージェントが設定され、実行している必要があります。詳細については、エージェントの設定 （27 ページ）を参照してください。

SR-PCE コレクタを設定するには、次の手順を実行します。

手順

ステップ 1 新しい収集を作成するか、既存の収集を編集するかを決定します。詳細については、収集の作成 （33 ページ）または収集の編集 （37 ページ）を参照してください。

ステップ 2 [基本トポロジ（Basic topology）] セクションで [SR-PCE] を選択し、[次へ（Next）] をクリックします。

ステップ 3 [設定（Configure）] ページで、次の設定パラメータを入力します。

- [SR-PCEホスト（SR-PCE host）]：SR-PCE エージェントを選択します。
- [バックアップSR-PCEホスト（Backup SR-PCE host）]：バックアップ SR-PCE エージェントを選択します。バックアップがない場合は、同じ SR-PCE エージェントを入力できます。
- [ASN]：ネットワーク内のすべての自律システムから情報を収集する場合は 0 を入力し、特定の ASN からのみ情報を収集する場合は自律システム番号（ASN）を入力します。たとえば、SR-PCE エージェントが ASN 64010 および ASN 64020 を認識できる場合、64020 と入力すると ASN 64020 からのみ情報を収集します。
- [IGPプロトコル（IGP protocol）]：ネットワークで実行されている IGP プロトコルを選択します。

- [拡張ディスカバリ（Extend discovery）]：完全なネットワークトポロジ（ノードおよびインターフェイス）を検出するには、[有効（Enabled）] チェックボックスをオンにします。
- [リアクティブネットワーク（Reactive Network）]：SR-PCE からの通知を登録し、ノードやリンクの追加を更新するには、[有効（Enabled）] チェックボックスをオンにします。
- [トリガー収集（Trigger collection）]：新しいトポロジの追加（ノードまたはリンク）時にトポロジ収集を収集するには、[有効（Enabled）] チェックボックスをオンにします。

ステップ 4 （オプション）[詳細設定（Advanced settings）] パネルを展開し、関連するフィールドに詳細を入力します。詳細オプションの説明については、IGP および SR-PCE コレクタの詳細オプション （60 ページ）を参照してください。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 設定をプレビューし、[作成（Create）] をクリックして収集を作成します。

次のタスク

- 収集ジョブのスケジュールを設定します。収集ジョブはすぐに実行するようにスケジュールしたり、特定の間隔で実行するようにスケジュールしたりできます。詳細については、収集のスケジュール （39 ページ） を参照してください。
- この収集を送信元ネットワークとして使用して、追加の収集を設定します。さまざまなコレクタの設定の詳細については、この章の関連トピックを参照してください。収集の編集の詳細については、収集の編集 （37 ページ）を参照してください。

IGP および SR-PCE コレクタの詳細オプション

IGP データベースと SR-PCE コレクタを使用する場合は、いくつかの詳細オプションを設定できます。

オプション	説明
IGP と SR-PCE の両方の収集に適用可能なオプション：	
ノード	
ノードパフォーマンスの収集（Node performance collection）	有効になっている場合、ノードパフォーマンスデータを収集します。
ノードサフィックスの削除（Remove node suffix）	ノードに指定されたサフィックスが含まれている場合は、ノード名からノードサフィックスを削除します。たとえば、「company.net」はネットワークのドメイン名を削除します。
QoS キュー（QoS queues）	インターフェイス（ルータで QoS が設定されている）で QoS 情報を表示できるようにします。

オプション	説明
データ収集タイムアウト（Data collection timeout）	データ収集に許可される最大時間を示します（分単位）。データ収集に使用される内部ツールは、指定された制限時間を超えるとタイムアウトになり、終了します。デフォルトは 60 分です。
QoS ノードフィルタ（QoS node filter）	QoS データを取得するノードを決定するためのフィルタを示します。
インターフェイス	
パラレルリンクの検索（Find parallel links）	IGP データベースに存在しないパラレルリンクを検索します（IS-IS TE 拡張機能が有効になっていない場合）。
IP 推測（IP guessing）	トポロジデータベースに存在しないインターフェイスに対して実行する IP アドレス推測のレベルを示します。IS-IS TE 拡張機能が有効になっていない場合に使用されます。 • オフ（OFF）：推測を実行しません。 • セーフ（Safe）：あいまいさのない推測を選択します。 • フル（FULL）：あいまいな場合に最善の判断を下します。
ポート LAG 検出（Port LAG discovery）	ポートメンバーの LAG 検出を有効にします。
LAGポートの照合（LAG port match）	ポート回路でローカルポートとリモートポートを照合する方法を決定します。 • 推測（Guess）：できるだけ多くのポートに一致するポート回路を作成します。 • 正確（Exact）：LACP に基づいて照合します。 • 完全（Complete）：最初に LACP に基づいて照合してから、できるだけ多くの照合を試みます。 • なし（None）：ポート回路を作成しません。
回路のクリーンアップ（Cleanup circuits）	インターフェイスに関連付けられている IP アドレスを持たない回路を削除します。IS-IS アドバタイジングの不整合を修正するために、IS-IS データベースで回路の削除が必要になる場合があります。
説明をコピー（Copy description）	論理インターフェイスが 1 つだけで、その説明が空白の場合は、物理インターフェイスの説明を論理インターフェイスにコピーします。
物理ポート（Physical ports）	シスコの L3 物理ポートを収集します。

オプション	説明
最小 IP 推測（Minimum IP guessing）	最小の IP 推測プレフィックス長を示します。プレフィックス長がそれ以上であるすべてのインターフェイスが考慮されます。
プレフィックスの最小長（Minimum prefix length）	パラレルリンクを検索するときに許可する最小プレフィックス長を示します。プレフィックス長がそれ以上（ただし 32 未満）であるすべてのインターフェイスが考慮されます。
データ収集タイムアウト（Data collection timeout）	データ収集に許可される最大時間を示します（分単位）。データ収集に使用される内部ツールは、指定された制限時間を超えるとタイムアウトになり、終了します。デフォルトは 60 分です。
デバッグ	
冗長（Verbosity）	ログの冗長レベルを示します。このレベルは、ログメッセージに表示される詳細と情報の程度を指します。デフォルトは 30 で、有効な範囲は 1 ～ 60 です。
ネットレコーダー（Net recorder）	SNMP メッセージを記録します。オプションは、オフ（Off）、記録（Record）、および再生（Playback）です。デフォルトはオフ（Off）です。 • 録音（Record）：ライブネットワークとの間で送受信される SNMP メッセージは、検出の実行時に内部で録音され、デバッグに使用されます。 • 再生（Playback）：録音されたメッセージは、ライブネットワークから送信されたかのようにコレクタを介して再生されるため、ネットワーク収集のオフラインデバッグが可能です。 • オフ（Off）：記録や再生は実行されません。
SR-PCE 収集にのみ適用されるオプション：	
シングルエンド eBGP 検出（Single-ended eBGP discovery）	リンクエンドが 1 つしかない（一般的ではない）eBGP リンクを検出します。

LSP 情報の収集

LSP コレクタは、SNMP を使用してネットワーク内の RSVP LSP 情報を収集します。

始める前に

ワークフロー：事前設定手順 （12 ページ）に記載されている手順を実行します。

LSP コレクタを設定するには、次の手順を実行します。

手順

ステップ 1 新しい収集を作成するか、既存の収集を編集するかを決定します。詳細については、収集の作成 （33 ページ）または収集の編集 （37 ページ）を参照してください。

ステップ 2 要件に応じて、いずれかの基本トポロジコレクタを選択します。

ステップ 3 [高度なモデリング（Advanced modeling）] セクションで [LSP] を選択し、[次へ（Next）] をクリックします。

ステップ 4 [設定（Configure）] ページで、左側の [選択されたコレクタ（Selected collectors）] ペインにある [LSP] をクリックします。

（注）
基本トポロジパラメータが自分のニーズに合わせて更新されていることを確認します。必要に応じてパラメータを更新します。

ステップ 5 次の設定パラメータを入力します。

- [ソース（Source）]：出力がこのコレクタの入力として機能するソースコレクタを選択します。
- [FRR LSPの取得（Get FRR LSPs）]：マルチプロトコル ラベル スイッチング（MPLS）高速再ルーティング（FRR）LSP（バックアップおよびバイパス）情報を検出する場合は [有効（Enabled）] チェックボックスをオンにします。

ステップ 6 （オプション）[詳細設定（Advanced settings）] パネルを展開し、関連するフィールドに詳細を入力します。詳細オプションの説明については、LSP 収集の詳細オプション （63 ページ）を参照してください。

ステップ 7 [Next] をクリックします。

ステップ 8 設定をプレビューし、[作成（Create）] をクリックして収集を作成します。

次のタスク

- 収集ジョブのスケジュールを設定します。収集ジョブはすぐに実行するようにスケジュールしたり、特定の間隔で実行するようにスケジュールしたりできます。詳細については、収集のスケジュール （39 ページ） を参照してください。
- この収集を送信元ネットワークとして使用して、追加の収集を設定します。さまざまなコレクタの設定の詳細については、この章の関連トピックを参照してください。収集の編集の詳細については、収集の編集 （37 ページ）を参照してください。

LSP 収集の詳細オプション

LSP コレクタを使用する場合は、いくつかの詳細オプションを設定できます。

オプション	説明
計算されたホップを使用（Use calculated hops）	パスホップを検出するときに、実際のパスホップテーブルの代わりに計算されたパスホップテーブルを使用します。
実際のパスの検索（Find actual path）	LSP の実際のパスを検出します。
追加情報の入手（Get extras）	追加の LSP プロパティを収集します。
シグナル名の使用（Use signaled name）	LSP トンネル名（IOS-XR）の代わりに LSP トンネルのシグナル名を使用します。
自動帯域幅（Auto bandwidth）	自動帯域幅を検出します。
データ収集タイムアウト（Data collection timeout）	データ収集に許可される最大時間を示します（分単位）。データ収集に使用される内部ツールは、指定された制限時間を超えるとタイムアウトになり、終了します。デフォルトは 60 分です。
デバッグ	
冗長（Verbosity）	ログの冗長レベルを示します。このレベルは、ログメッセージに表示される詳細と情報の程度を指します。デフォルトは 30 で、有効な範囲は 1 ～ 60 です。
ネットレコーダー（Net recorder）	SNMP メッセージを記録します。オプションは、オフ（Off）、記録（Record）、および 再生（Playback）です。デフォルトはオフ（Off）です。 • 録音（Record）：ライブネットワークとの間で送受信される SNMP メッセージは、検出の実行時に内部で録音され、デバッグに使用されます。 • 再生（Playback）：録音されたメッセージは、ライブネットワークから送信されたかのようにコレクタを介して再生されるため、ネットワーク収集のオフラインデバッグが可能です。 • オフ（Off）：記録や再生は実行されません。

SR-PCE を使用した PCEP LSP 情報の収集

PCEP LSP コレクタは、SR-PCE コレクタから収集されたデータを使用し、LSP 情報を追加して、新しいネットワークモデルを作成します。

始める前に

- ワークフロー：事前設定手順 （12 ページ）に記載されている手順を実行します。
- SR-PCE（SR-PC コレクタ）を使用した BGP-LS トポロジ収集がネットワークで完了していることを確認します。LSP を収集するための送信元ネットワークとしてこのモデルを使用する必要があります。詳細については、SR-PCE コレクタを使用したトポロジ情報の収集 （58 ページ）を参照してください。

PCEP LSP コレクタを設定するには、次の手順を実行します。

手順

ステップ 1 新しい収集を作成するか、既存の収集を編集するかを決定します。詳細については、収集の作成 （33 ページ）または収集の編集 （37 ページ）を参照してください。

ステップ 2 [基本トポロジ（Basic topology）] セクションで [SR-PCE] を選択します。

ステップ 3 [高度なモデリング（Advanced modeling）] セクションで [PCEP LSP] を選択し、[次へ（Next）] をクリックします。

ステップ 4 [設定（Configure）] ページで、左側の [選択されたコレクタ（Selected collectors）] ペインにある [PCEP LSP] をクリックします。

（注）
基本トポロジパラメータが自分のニーズに合わせて更新されていることを確認します。必要に応じてパラメータを更新します。

ステップ 5 次の設定パラメータを入力します。

- [ソース（Source）]：出力がこのコレクタの入力として機能するソースコレクタを選択します。
- [エージェント（Agents）]：ドロップダウンリストから関連する SR-PCE エージェントを選択します。エージェントの作成の詳細については、エージェントの設定 （27 ページ）を参照してください。
- [リアクティブネットワーク（Reactive Network）]：SR-PCE からの通知を登録し、追加または削除に基づき LSP を更新するには、[有効（Enabled）] チェックボックスをオンにします。このオプションは、デフォルトで有効です。

ステップ 6 （オプション）[詳細設定（Advanced settings）] パネルを展開し、次の情報を入力します。

- [RSVPシグナル名の使用（RSVP use signalled name）]：LSP トンネル名（IOS-XR）の代わりに RSVP LSP トンネルのシグナル名を使用するには、[有効（Enabled）] チェックボックスをオンにします。
- [SRシグナル名の使用（SR use signalled name）]：LSP トンネル名（IOS-XR）の代わりに SR LSP トンネルのシグナル名を使用するには、[有効（Enabled）] チェックボックスをオンにします。
- [SRインデックスの追加（SR add index）]：関連付けられたインターフェイス（IOS-XR）から SR LSP トンネルにインデックスを追加するには、[有効（Enabled）] チェックボックスをオンにします。

- [データ収集タイムアウト（Data Collection Timeout）]：データ収集に許可される最大時間を入力します（分単位）。データ収集に使用される内部ツールは、指定された制限時間を超えるとタイムアウトになり、終了します。デフォルトは 60 分です。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 設定をプレビューし、[作成（Create）] をクリックして収集を作成します。

次のタスク

- 収集ジョブのスケジュールを設定します。収集ジョブはすぐに実行するようにスケジュールしたり、特定の間隔で実行するようにスケジュールしたりできます。詳細については、収集のスケジュール （39 ページ） を参照してください。
- この収集を送信元ネットワークとして使用して、追加の収集を設定します。さまざまなコレクタの設定の詳細については、この章の関連トピックを参照してください。収集の編集の詳細については、収集の編集 （37 ページ）を参照してください。

ネットワークからのマルチキャストフローデータのコレクタ

マルチキャストコレクタは、特定のネットワークからマルチキャストフローデータを収集します。これは、次のコレクタの収集です。

- [ログイン検出マルチキャスト（Login find multicast）]：ルータにログインして、マルチキャストフローデータを取得または解析します。
- [ログインポーリングマルチキャスト（Login poll multicast）]：ルータにログインしてマルチキャスト トラフィックレートを取得します。
- [SNMP検出マルチキャスト（SNMP find multicast）]：SNMP を使用してマルチキャストフローのマルチキャストデータを収集します。
- [SNMPポーリングマルチキャスト（SNMP poll multicast）]：SNMP を使用してマルチキャストフローのトラフィックデータレートを収集します。

始める前に

ワークフロー：事前設定手順 （12 ページ）に記載されている手順を実行します。

マルチキャストを設定するには、次の手順を実行します。

手順

ステップ 1 新しい収集を作成するか、既存の収集を編集するかを決定します。詳細については、収集の作成 （33 ページ）または収集の編集 （37 ページ）を参照してください。

ステップ 2 要件に応じて、いずれかの基本トポロジコレクタを選択します。

ステップ 3 [トラフィックとデマンド（Traffic and Demands）] セクションで [マルチキャスト（Multicast）] を選択し、[次へ（Next）] をクリックします。

ステップ 4 [設定（Configure）] ページで、左側の [選択されたコレクタ（Selected Collectors）] ペインにある [マルチキャスト（Multicast）] をクリックします。

（注）
基本トポロジパラメータが自分のニーズに合わせて更新されていることを確認します。必要に応じてパラメータを更新します。

ステップ 5 次の設定パラメータを入力します。

- [ソース（Source）]：出力がこのコレクタの入力として機能するソースコレクタを選択します。
- [データ収集ソース（Data Collection Source）]：マルチキャストデータの収集に使用するコレクタを選択します。オプションは、[ログイン検出マルチキャスト（Login find multicast）]、[ログインポーリングマルチキャスト（Login poll multicast）]、[SNMP検出マルチキャスト（SNMP find multicast）]、および [SNMPポーリングマルチキャスト（SNMP poll multicast）] です。

ステップ 6 （オプション）[コレクタ設定（Collector Settings）] パネルを展開し、関連するフィールドに詳細を入力します。前のステップで選択したコレクタに基づいて、オプションが異なります。詳細オプションの説明については、マルチキャストコレクタの詳細オプション （67 ページ）を参照してください。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 設定をプレビューし、[作成（Create）] をクリックして収集を作成します。

次のタスク

- 収集ジョブのスケジュールを設定します。収集ジョブはすぐに実行するようにスケジュールしたり、特定の間隔で実行するようにスケジュールしたりできます。詳細については、収集のスケジュール （39 ページ）を参照してください。
- この収集を送信元ネットワークとして使用して、追加の収集を設定します。さまざまなコレクタの設定の詳細については、この章の関連トピックを参照してください。収集の編集の詳細については、収集の編集 （37 ページ）を参照してください。

マルチキャストコレクタの詳細オプション

マルチキャストコレクタを使用する場合は、いくつかの詳細オプションを設定できます。

オプション	説明
ログイン検出マルチキャストの設定	
データ収集タイムアウト（Data collection timeout）	データ収集に許可される最大時間を示します（分単位）。データ収集に使用される内部ツールは、指定された制限時間を超えるとタイムアウトになり、終了します。デフォルトは 30 分です。
既存の設定を使用（Use existing config）	収集された既存のマルチキャスト設定をキャッシュから使用します。
設定の強制更新（Force config update）	マルチキャスト設定ファイルは、データディレクトリに存在する場合でも更新されます。
設定を保存（Save configs）	マルチキャスト設定をキャッシュに保存するか、破棄するかを指定します。
ファイルの上書き（Overwrite files）	既存のファイルを上書きするかどうかを指定します。
ログイン ポーリング マルチキャスト設定	
データ収集タイムアウト（Data collection timeout）	データ収集に許可される最大時間を示します（分単位）。データ収集に使用される内部ツールは、指定された制限時間を超えるとタイムアウトになり、終了します。デフォルトは 30 分です。
サンプル数（No of samples）	取得されるサンプルの数を示します。
ポーリング間隔（Polling interval）	ログインによるレート読み取り間の遅延時間（秒単位）を示します。
トラフィックレベル名（Traffic level name）	トラフィックレベルの名前を示します。
トラフィック フィルタリング（Traffic filtering）	各 S|G グループの複数の送信元からのマルチキャストトラフィックをフィルタ処理する方法を指定します。
既存の設定を使用（Use existing config）	収集された既存のマルチキャスト設定をキャッシュから使用します。
設定の強制更新（Force config update）	マルチキャスト設定ファイルは、データディレクトリに存在する場合でも更新されます。
設定を保存（Save configs）	マルチキャスト設定をキャッシュに保存するか、破棄するかを指定します。
ファイルの上書き（Overwrite files）	既存のファイルを上書きするかどうかを指定します。

オプション	説明
SNMP 検出マルチキャストの設定	
データ収集タイムアウト（Data collection timeout）	データ収集に許可される最大時間を示します（分単位）。データ収集に使用される内部ツールは、指定された制限時間を超えるとタイムアウトになり、終了します。デフォルトは 30 分です。
SNMP ポーリングマルチキャストの設定	
データ収集タイムアウト（Data collection timeout）	データ収集に許可される最大時間を示します（分単位）。データ収集に使用される内部ツールは、指定された制限時間を超えるとタイムアウトになり、終了します。デフォルトは 30 分です。
サンプル数（No of samples）	取得されるサンプルの数を示します。
ポーリング間隔（Polling interval）	ログインによるレート読み取り間の遅延時間（秒単位）を示します。
トラフィックレベル名（Traffic level name）	トラフィックレベルの名前を示します。
トラフィックフィルタリング（Traffic filtering）	各 S|G グループの複数の送信元からのマルチキャストトラフィックをフィルタ処理する方法を指定します。
デバッグ	
冗長（Verbosity）	ログの冗長レベルを示します。このレベルは、ログメッセージに表示される詳細と情報の程度を指します。デフォルトは 30 で、有効な範囲は 1 ～ 60 です。
ネットレコーダー（Net recorder）	SNMP メッセージを記録します。オプションは、オフ（Off）、記録（Record）、および 再生（Playback）です。デフォルトはオフ（Off）です。 • 録音（Record）：ライブネットワークとの間で送受信される SNMP メッセージは、検出の実行時に内部で録音され、デバッグに使用されます。 • 再生（Playback）：録音されたメッセージは、ライブネットワークから送信されたかのようにコレクタを介して再生されるため、ネットワーク収集のオフラインデバッグが可能です。 • オフ（Off）：記録や再生は実行されません。

BGP ピアリングの検出

BGP コレクタは、SNMP とログインを介して BGP トポロジを検出します。また、トポロジネットワーク（通常は IGP トポロジコレクタの出力）を送信元ネットワークとして使用して、BGP リンクを外部 ASN ノードに追加します。

始める前に

ワークフロー：事前設定手順 （12 ページ）に記載されている手順を実行します。

BGP コレクタを設定するには、次の手順を実行します。

手順

ステップ 1 新しい収集を作成するか、既存の収集を編集するかを決定します。詳細については、収集の作成 （33 ページ）または収集の編集 （37 ページ）を参照してください。

ステップ 2 要件に応じて、いずれかの基本トポロジコレクタを選択します。

ステップ 3 [高度なモデリング（Advanced Modeling）] セクションで [BGP] を選択し、[次へ（Next）] をクリックします。

ステップ 4 [設定（Configure）] ページで、左側の [選択されたコレクタ（Selected Collectors）] ペインにある [BGP] をクリックします。

（注）
基本トポロジパラメータが自分のニーズに合わせて更新されていることを確認します。必要に応じてパラメータを更新します。

ステップ 5 [ソース（Source）] ドロップダウンリストから、出力がこのコレクタの入力として機能するソースコレクタを選択します。

ステップ 6 （オプション）[詳細設定（Advanced settings）] パネルを展開し、関連するフィールドに詳細を入力します。詳細オプションの説明については、BGP トポロジの詳細オプション （71 ページ）を参照してください。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 設定をプレビューし、[作成（Create）] をクリックして収集を作成します。

次のタスク

- 収集ジョブのスケジュールを設定します。収集ジョブはすぐに実行するようにスケジュールしたり、特定の間隔で実行するようにスケジュールしたりできます。詳細については、収集のスケジュール （39 ページ） を参照してください。

- この収集を送信元ネットワークとして使用して、追加の収集を設定します。さまざまなコレクタの設定の詳細については、この章の関連トピックを参照してください。収集の編集の詳細については、収集の編集 （37 ページ）を参照してください。

BGP トポロジの詳細オプション

BGP コレクタを使用する場合は、いくつかの詳細オプションを設定できます。

オプション	説明
ASNを含める（ASN include）	含める ASN を入力できます。デフォルトでは、すべての ASN が含まれます。
内部ASN（Internal ASNs）	内部 ASN を入力できます。
プロトコル（Protocol）	Internet Protocol（IP）のバージョンを指定します。オプションは IPv4 と IPv6 です。
最小 IPv4 プレフィックス長（Min IPv4 prefix length）	BGP リンクとしてインターフェイスを検出する際の IPv4 サブネット照合の制限を制御するための最小プレフィックス長を示します。
最小 IPv6 プレフィックス長（Min IPv6 prefix length）	BGP リンクとしてインターフェイスを検出する際の IPv6 サブネット照合の制限を制御するための最小 IPv6 プレフィックス長を示します。
ログインマルチホップ（Login multi hop）	マルチホップピアを含む可能性のあるルータにログインするかどうかを示します。
強制ログインプラットフォーム（Force login platform）	プラットフォーム検出をオーバーライドして、指定されたプラットフォームを使用します。有効な値：cisco、juniper、alu、huawei。
フォールバックログインプラットフォーム（Fallback login platform）	プラットフォームの検出が失敗した場合のフォールバックベンダーを示します。有効な値：cisco、juniper、alu、huawei。
enableの送信を試す（Try send enable）	ルータにログインするときに、プラットフォームタイプが検出されない場合、enable password を送信します。
Telnetユーザー名プロンプト（Telnet username prompt）	代替カスタムユーザー名プロンプトを示します。

オプション	説明
Telnetパスワードプロンプト（Telnet password prompt）	代替カスタム パスワード プロンプトを示します。
内部ASNリンクの検索（Find internal ASN links）	2 つ以上の内部 ASN 間のリンクを検索します。通常、IGP がこれらのリンクを検出するため、このアクションは必要ありません。
非IP出口インターフェイスの検索（Find non IP exit interface）	ネクストホップ IP アドレスとしてではなく、インターフェイスとして表現される出口インターフェイスを検索します（これはまれなケースです）。 （注） このアクションにより、BGP 検出に対する SNMP リクエストの量が増加し、パフォーマンスに影響します。
内部出口インターフェイス（Internal exit interface）	内部 ASN への BGP リンクを検出します。
MACアドレスの取得（Get MAC address）	Internet Exchange パブリック ピアリング スイッチに接続されている BGP ピアの送信元 MAC アドレスを収集します。このアクションは、MAC アカウンティングの場合にのみ必要です。
DNSを使用（Use DNS）	DNS を使用して BGP IP アドレスを解決するかどうかを示します。
すべてを強制的にチェック（Force check all）	マルチホップピアの可能性が示されていない場合でも、すべてのルータを確認するかどうかを示します。このアクションは遅い可能性があります。
データ収集タイムアウト（Data collection timeout）	データ収集に許可される最大時間を示します（分単位）。データ収集に使用される内部ツールは、指定された制限時間を超えるとタイムアウトになり、終了します。デフォルトは 60 分です。
デバッグ	
冗長（Verbosity）	ログの冗長レベルを示します。このレベルは、ログメッセージに表示される詳細と情報の程度を指します。デフォルトは 30 で、有効な範囲は 1 ～ 60 です。

オプション	説明
ネットレコーダー（Net recorder）	SNMP メッセージを記録します。オプションは、オフ（Off）、記録（Record）、および 再生（Playback）です。デフォルトはオフ（Off）です。 • 録音（Record）：ライブネットワークとの間で送受信される SNMP メッセージは、検出の実行時に内部で録音され、デバッグに使用されます。 • 再生（Playback）：録音されたメッセージは、ライブネットワークから送信されたかのようにコレクタを介して再生されるため、ネットワーク収集のオフラインデバッグが可能です。 • オフ（Off）：記録や再生は実行されません。
ログイン記録モード（Login record mode）	検出プロセスを記録します。オプションは、オフ（Off）、記録（Record）、および再生（Playback）です。デフォルトはオフ（Off）です。 • 記録（Record）：ライブネットワークとの間で送受信されるメッセージは、ツールの実行時に内部で記録され、デバッグに使用されます。 • 再生（Playback）：記録されたメッセージは、ライブネットワークから送信されたかのようにツールを介して再生されるため、ネットワーク収集のオフラインデバッグが可能です。 • オフ（Off）：記録や再生は実行されません。

VPN トポロジの検出

VPN コレクタは、レイヤ 2 およびレイヤ 3 VPN トポロジを検出します。

（注） 現在、レイヤ 2 VPN では P2P-VPWS xconnect 検出のみがサポートされています。

始める前に

ワークフロー：事前設定手順 （12 ページ）に記載されている手順を実行します。

VPN コレクタを設定するには、次の手順を実行します。

手順

ステップ 1 新しい収集を作成するか、既存の収集を編集するかを決定します。詳細については、収集の作成（33 ページ）または収集の編集 （37 ページ）を参照してください。

ステップ 2 要件に応じて、いずれかの基本トポロジコレクタを選択します。

ステップ 3 [高度なモデリング（Advanced Modeling）] セクションで [VPN] を選択し、[次へ（Next）] をクリックします。

ステップ 4 [設定（Configure）] ページで、左側の [選択されたコレクタ（Selected Collectors）] ペインにある [VPN] をクリックします。

（注）
基本トポロジパラメータが自分のニーズに合わせて更新されていることを確認します。必要に応じてパラメータを更新します。

ステップ 5 次の設定パラメータを入力します。

- [ソース（Source）]：出力がこのコレクタの入力として機能するソースコレクタを選択します。
- [VPNタイプ（VPN type）]：少なくとも 1 つの VPN タイプを選択します。
  - [VPWS]：ネットワークで Virtual Private Wire Service（VPWS）が使用されている場合は、このタイプを追加します。
  - [L3VPN]：ネットワークでレイヤ 3 VPN が使用されている場合は、このタイプを追加します。

ステップ 6 （オプション）[詳細設定（Advanced settings）] パネルを展開し、次の情報を入力します。

- [データ収集タイムアウト（Data Collection Timeout）]：データ収集に許可される最大時間（分単位）。データ収集に使用される内部ツールは、指定された制限時間を超えるとタイムアウトになり、終了します。デフォルトは 60 分です。
- [冗長（Verbosity）]：ログの冗長レベル。このレベルは、ログメッセージに表示される詳細と情報の程度を指します。デフォルトは 30 で、有効な範囲は 1 ～ 60 です。
- [ネットレコーダー（Net Recorder）]：SNMPメッセージを記録します。オプションは、オフ（Off）、記録（Record）、および 再生（Playback）です。デフォルトはオフ（Off）です。[記録（Record）] に設定すると、ライブネットワークとの間で送受信される SNMP メッセージは、検出の実行時に内部で記録され、デバッグに使用されます。[再生（Playback）]に設定すると、記録されたメッセージは、ライブネットワークから送信されたかのようにコレクタを介して再生されるため、ネットワーク収集のオフラインデバッグが可能です。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 設定をプレビューし、[作成（Create）] をクリックして収集を作成します。

次のタスク

- 収集ジョブのスケジュールを設定します。収集ジョブはすぐに実行するようにスケジュールしたり、特定の間隔で実行するようにスケジュールしたりできます。詳細については、収集のスケジュール （39 ページ） を参照してください。
- この収集を送信元ネットワークとして使用して、追加の収集を設定します。さまざまなコレクタの設定の詳細については、この章の関連トピックを参照してください。収集の編集の詳細については、収集の編集 （37 ページ）を参照してください。

ハードウェアインベントリ情報の収集

インベントリコレクタは、ハードウェアインベントリ情報を収集します。

収集されるハードウェア

インベントリコレクタは、ハードウェアタイプに基づいて収集されたハードウェア情報を格納する一連の NetIntHardware* テーブルを作成します。次の各オブジェクトは、ノード IP アドレスと SNMP ID によって定義されます。

- NetIntHardwareChassis：ノード IP アドレスと SNMP ID によって識別されるルータシャーシオブジェクト。
- NetIntHardwareContainer：各エントリは、ルータ内のスロット（現場交換可能ユニット（FRU）タイプのデバイスを取り付けられる任意の機構）を表します。たとえば、シャーシスロット、モジュールスロット、ポートスロットなどです。
- NetIntHardwareModule：他のハードウェアデバイスに取り付けられるハードウェアデバイス通常、これらのデバイスは、ラインカード、モジュール、ルートプロセッサなどのトラフィックを直接サポートするものであり、他の機能固有のハードウェアテーブルのいずれにも分類されません。
- NetIntHardwarePort：ルータ上の物理ポート。

ハードウェア階層

ハードウェアには、オブジェクトがルータ内で存在する場所に基づいて親子関係があります。シャーシには親がなく、ルートオブジェクトと見なされます。シャーシ以外の各オブジェクトには 1 つの親があり、1 つ以上の子オブジェクトを持つことができます。子のないオブジェクトは、リーフオブジェクトと呼ばれます（ポートや空のコンテナなど）。この階層は、通常、ハードウェアオブジェクトが他のオブジェクト内にどのように取り付けられているかを反映しています。たとえば、ラインカードを表すモジュールには、スロットを表すコンテナである親オブジェクトがある場合があります。

親は、NetIntHardware* テーブル内で、ParentTable 列と ParentId 列によって識別できます。これらの 2 つの列を Node（ノード IP アドレス）列とともに使用すると、任意のハードウェアオブジェクトの親オブジェクトを見つけることができます。

例：次の NetIntHardwareContainer エントリは、コンテナ 172.23.123.456 に親としてのシャーシがあることを識別しています。NetIntHardwareChassis には、コンテナの ParentId である 2512347 に一致する SnmpID エントリがあります。

NetIntHardwareContainer							
ノード	SnmpID	ParentID	モデル	名前	NumChildren	ParentTable	SlotNumber
172.23.123.456	2503733	2512347		slot mau 0/0/0/5	0	NetIntHardwareChassis	0

親子関係に基づいて各リーフオブジェクトから対応するルートオブジェクトまで階層をトレースすると、一連のオブジェクトタイプでハードウェア階層が形成されます。このトレースは、インベントリコレクタがハードウェアデバイスの処理方法を決定するために使用されます。これは、HWInventoryTemplatesテーブルにエントリを追加する場合にも使用する必要があるプロセスです。

例：Chassis-Container-Module-Module-Container-Port

インベントリを処理するためのテーブル

インベントリコレクタは、NetIntHardware* テーブルを処理して NetIntNodeInventory テーブルを作成します。コレクタには2つの構成ファイルが必要で、オプションの構成ファイルを追加で使用できます。

- テンプレートファイル（必須）：このファイルには、次のテーブルが含まれています。
  - HWInventoryTemplates：最終的な NetIntNodeInventory テーブル内のデバイスを分類するエントリ、および包含からプルーニングするエントリが含まれます。
  - HWNameFormatRules：ハードウェアオブジェクト名をより使いやすくするためにフォーマットするエントリ、および予期しない SNMP 結果を修正するエントリが含まれます。
- 除外ファイル（必須）：ハードウェアオブジェクトが最終的なNetIntNodeInventoryテーブルに含まれないようにするExcludeHWListテーブルが含まれます。これは、トラフィックを転送または伝送しないハードウェアを除外する場合に役立ちます。
- ハードウェア仕様ファイル（オプション）：SNMPによって返されたスロットが不正確な場合に、指定されたデバイスのスロット数に関して収集されたデータを調整するために使用できる HardwareSpec テーブルが含まれます。

テンプレートを変更するか、ファイルを除外することを選択した場合は、それらの変更がソフトウェアのアップグレード後に維持されるようにします。

ハードウェア テンプレートの設定

[インベントリの構築オプション（Build inventory options）] セクションの [テンプレートファイル（Template file）] オプションは、HWInventoryTemplates テーブルと HWNameFormatRules テーブルの両方を含むファイルを呼び出します。

HWInventoryTemplates テーブル

HWInventoryTemplates テーブルは、NetIntHardware* テーブルによって参照されるハードウェアを解釈する方法をインベントリコレクタに指示します。そのため、インベントリコレクタは、オブジェクトをシャーシ、ラインカード、スロットなどの一般的なベンダーに依存しないハードウェアタイプに分類し、関心のないハードウェアタイプを削除できます。

インベントリハードウェアは、シャーシ、スロット、ラインカード、モジュールスロット、モジュール、ポートスロット、ポート、またはトランシーバとして分類されます。コンテナは、スロット、モジュールスロット、またはポートスロットのいずれかに分類されます。モジュールは、モジュールまたはラインカードとして分類されます。他のすべてのハードウェアオブジェクトは、その名前で分類されます。たとえば、シャーシはシャーシとして分類されます。

インベントリコレクタは、HWInventoryTemplates テーブルの次の列で、NetIntHardware* テーブルとの一致を次の順序で調べます。

- DiscoveredHWHierarchy、Vendor、Model
- DiscoveredHWHierarchy、Vendor、*（*は Model 列のすべてのエントリを意味します）

[テンプレートの推測（Guess Template）] オプションを使用して、検索をさらに強化できます。この場合、最初の 2 つの条件を使用して一致が見つからなかった場合、Cisco Crosswork Planning コレクタは DiscoveredHWHierarchy と Vendor の一致のみを検索し、Model は考慮しません。

一致が見つかった場合、DiscoveredHWHierarchy 以降の列により、インベントリコレクタによるハードウェアの分類方法が決まります。以降の列により、ハードウェア オブジェクト タイプ（シャーシ、スロット、ラインカード、モジュールスロット、モジュール、ポートスロット、ポート、またはトランシーバ）が識別されます。各列エントリには、*Type*、*Identifier*、*Name* の形式があります。

- Type は、検出されたハードウェアタイプ（「コンテナ」など）です。
- Identifier は、（1 つ以上の同じタイプの）どのオブジェクトが参照されているのかを指定します（0、1、...）。
- Name は、NetIntHardware* テーブルの列見出しを指定します。これは、NetIntNodeInventory テーブルで、そのオブジェクトに対して表示される名前です。

例：Module,0,Model （Model は、NetIntHardwareModule テーブルの列見出しです）。

複数の名前ソース列をコロンで指定できます。

例：Container,0,Model:Name

ハードウェアカテゴリが存在しないか、空の場合、インベントリコレクタは最終的な NetIntNodeInventory テーブルにそのカテゴリを含めません。

例：

デフォルトのテンプレートファイルの最初の行を使用して、Cisco Crosswork Planning コレクタは、Cisco ASR9K Chassis-Container-Module-Port-Container-Module のように、Vendor、Model、および DiscoveredHWHierarchy 列に一致するエントリを持つ NetIntHardware* テーブルを検索します。

その後、WAE Collector はハードウェア階層（DiscoveredHWHierarchy 列）の各エントリを分類し、ハードウェアタイプ列でその位置を定義します。

最初の Module エントリはラインカードとして定義され、#0 として識別されます。NetIntNodeInventory テーブルに表示される名前は、NetIntHardwareModule テーブルの Model 列に表示される名前です。2 番目のモジュールはトランシーバオブジェクトとして定義され、#1 として識別されます。同じ名前形式を使用します。

階層には 2 つのコンテナがありますが、Type として定義されるのは 1 つだけです。これは、2 番目のコンテナが NetIntNodeInventory テーブルに表示されないことを意味します。

HWInventoryTemplates エントリの追加

Cisco Crosswork Planning コレクタは、HWInventoryTemplates テーブルにないインベントリデバイスを検出した場合、リーフオブジェクトの SNMP ID やルータの IP アドレスなど、ハードウェア階層の一部を指定して警告を生成します。この情報を使用して、リーフからルートまでオブジェクトを手動でトレースし、HWInventoryTemplates テーブル内の適切なエントリを取得できます。ハードウェア階層のトレースについては、「ハードウェア階層」を参照してください。

1. 参照用に警告メッセージをコピーし、ステップ 2 で使用します。
2. ルータの IP アドレス、リーフオブジェクトの SNMP ID、名前、およびモデルを使用して、NetIntHardwarePort または NetIntHardwareContainer テーブルのいずれかで警告で参照されているリーフオブジェクトを見つけます。
3. リーフオブジェクトの ParentTable 列と ParentId 列を使用して、リーフをその親までトレースします。連続する各親について、NetIntHardwareChassis テーブルのルートオブジェクト（シャーシ）に到達するまで、それぞれの ParentTable 列と ParentId 列を使用します。
4. ハードウェア階層内の各オブジェクトが見つかったら、HWInventoryTemplates テーブルの DiscoveredHWHierarchy 列に追加します。Vendor 列と Model 列に入力します。
5. ハードウェア階層内の各オブジェクト（DiscoveredHWHierarchy 列）について、標準ハードウェアタイプのいずれかに分類します。これは、DiscoveredHWHierarchy 列の後に表示される列です。

HWNameFormatRules テーブル

HWNameFormatRules テーブルは、NetIntNodeInventory テーブルの名前の形式を指定する方法を指定します。これは、長い名前や意味のない名前を、ユーザーにとって読みやすく明確な名前に変換するのに役立ちます。

HWInventoryTemplates テーブルのエントリごとに、一致するベンダー、ハードウェアタイプ（HWType）、名前（PatternMatchExpression）が HWNameFormatRules テーブルで検索されます。次に、HWInventoryTemplates テーブルで指定された名前を使用するのではなく、ReplacementExpression 列で識別された名前で NetIntNodeInventory テーブルが更新されます。

複数の一致が適用される場合は、最初に見つかった一致が使用されます。PatternMatchExpression と ReplacementExpression はどちらも、一重引用符で囲んだリテラル文字列または正規表現として定義できます。

例：

HWNameFormatRules			
ベンダー	HWType	PatternMatchExpression	ReplacementExpression
シスコ	シャーシ	\A4\Z	‘7507’
シスコ	ラインカード	800-20017-.*	‘1X10GE-LR-SC’
Juniper	シャーシ	Juniper (MX960) Internet Backbone Router	$1

テーブルの各エントリは次のように機能します。

- 名前が 4 文字で、A が文字列の先頭、Z が文字列の末尾であるすべての Cisco シャーシ名を 7507 に置き換えます。
- 800-20017-.* に一致するすべての Cisco ラインカード名を 1X10GE-LR-SC に置き換えます。
- 「Juniper (MX960) Internet Backbone Router」という名前のすべての Juniper シャーシを MX960 に置き換えます。

（注） SNMP は、多くのスロット名を整数ではなくテキストとして返します。最適に使用するには、スロット番号からすべてのテキストを削除するのがベストプラクティスです。

モデルまたは名前によるハードウェアの除外

[インベントリの構築オプション（Build Inventory Options）] セクションの [除外ファイル（Exclude File）] オプションは、ExcludeHWList テーブルを含むファイルを呼び出します。このテーブルを使用すると、モデル、名前、またはその両方に基づいて、NetIntNodeInventory テーブルから除外するハードウェアオブジェクトを特定できます。これは、たとえば、管理ポートとルートプロセッサを除外する場合に役立ちます。モデルと名前は、正規表現またはリテラルを使用して指定できます。

例：

ExcludeHWList			
HWTable	Vendor	モデル	名前
NetIntHardwarePort	シスコ		\/CPU0\/129$
NetIntHardwareModule	シスコ	800-12308-02	
NetIntHardwarePort	シスコ		管理

テーブルの各エントリは次のように機能します。

- ベンダーが Cisco で、名前が CPU0/129 で終わる NetIntHardwarePort テーブル内のすべてのオブジェクトを除外します。
- ベンダーが Cisco、モデルが 800-12308-02 である NetIntHardwareModule テーブル内のすべてのオブジェクトを除外します。
- ベンダーが Cisco、名前が Mgmt である NetIntHardwarePort テーブル内のすべてのオブジェクトを除外します。

HardwareSpec

[インベントリの構築オプション（Build Inventory Options）] セクションの [ハードウェア仕様ファイル（Hardware Spec File）] オプションは、HardwareSpec テーブルを含むファイルを呼び出します。このテーブルを使用すると、SNMP から返されるデータを調整できます。スロットの総数（TotSlot）とスロット番号の範囲（SlotNum）の両方を調整できます。たとえば、実際にはルートプロセッサを含めて 9 個のスロットがあるのに、SNMP はシャーシに 7 個のスロットを返すことがあります。

このテーブルでは、スロット、モジュールスロット、またはポートスロットを含むハードウェアのみ検索されるため、ハードウェアタイプ（HWType 列）は、シャーシ、ラインカード、またはモジュールである必要があります。SlotNum はスロット番号の範囲を示します。たとえば、スロット 0 から始まるルータもあれば、スロット 1 から始まるルータもあります。

例：

HardwareSpec				
ベンダー	HWType	モデル	TotSlot	SlotNum
シスコ	シャーシ	7609	9	1-9

次のテーブルエントリは、Cisco 7609 シャーシに合計 9 個のスロットを設定し、スロット番号を 9 から付け始めます。

インベントリ収集の設定

始める前に

ワークフロー：事前設定手順 （12 ページ）に記載されている手順を実行します。

インベントリコレクタを設定するには、次の手順を実行します。

手順

ステップ 1 新しい収集を作成するか、既存の収集を編集するかを決定します。詳細については、収集の作成 （33 ページ）または収集の編集 （37 ページ）を参照してください。

ステップ 2 要件に応じて、いずれかの基本トポロジコレクタを選択します。

ステップ 3 [トラフィックとデマンド（Traffic and Demands）] セクションで [インベントリ（Inventory）] を選択し、[次へ（Next）] をクリックします。

ステップ 4 [設定（Configure）] ページで、左側の [選択されたコレクタ（Selected collectors）] ペインにある [インベントリ（Inventory）] をクリックします。

（注）
基本トポロジパラメータが自分のニーズに合わせて更新されていることを確認します。必要に応じてパラメータを更新します。

ステップ 5 [ソース（Source）] ドロップダウンリストから、出力がこのコレクタの入力として機能するソースコレクタを選択します。

ステップ 6 （オプション）[詳細設定（Advanced settings）] パネルを展開し、関連するフィールドに詳細を入力します。詳細オプションの説明については、インベントリ収集の詳細オプション （81 ページ）を参照してください。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 設定をプレビューし、[作成（Create）] をクリックして収集を作成します。

次のタスク

- 収集ジョブのスケジュールを設定します。収集ジョブはすぐに実行するようにスケジュールしたり、特定の間隔で実行するようにスケジュールしたりできます。詳細については、収集のスケジュール （39 ページ）を参照してください。
- この収集を送信元ネットワークとして使用して、追加の収集を設定します。さまざまなコレクタの設定の詳細については、この章の関連トピックを参照してください。収集の編集の詳細については、収集の編集 （37 ページ）を参照してください。

インベントリ収集の詳細オプション

インベントリコレクタを使用する場合は、いくつかの詳細オプションを設定できます。

オプション	説明
インベントリの取得のオプション	
ログイン許可済み（Login allowed）	ルータにログインしてインベントリデータを収集できるようになります。

オプション	説明
データ収集タイムアウト（Data collection timeout）	データ収集に許可される最大時間を示します（分単位）。データ収集に使用される内部ツールは、指定された制限時間を超えるとタイムアウトになり、終了します。デフォルトは 30 分です。
インベントリの構築のオプション	
除外ファイル（Exclude Files）	出力での除外に対して照合するためのハードウェア特性を定義する ExcludeHWList テーブルを含むファイルを示します。 ExcludeHWList を含むサンプルファイルをダウンロードするには、[サンプルファイルのダウンロード（Download sample file）] リンクをクリックします。
テンプレートの推測（Guess Template）	未加工のインベントリデータを処理するときに検索範囲を拡げるかどうかを示します。
テンプレートファイル（Template File）	HWInvetory テンプレートおよび HWNameFormatRules テーブルを含むハードウェア テンプレート ファイルを示します。 [サンプルファイルのダウンロード（Download sample file）] リンクをクリックしてサンプル テンプレート ファイルをダウンロードします。
ハードウェア仕様ファイル（Hardware spec file）	ルータから返された SNMP データを確認するための、特定のタイプのハードウェアのスロット数を定義する HardwareSpec テーブルを含むファイルを示します。 HardwareSpec を含むサンプルファイルをダウンロードするには、[サンプルファイルのダウンロード（Download sample file）] リンクをクリックします。
デバッグ	
冗長（Verbosity）	ログの冗長レベルを示します。このレベルは、ログメッセージに表示される詳細と情報の程度を指します。デフォルトは 30 で、有効な範囲は 1 ～ 60 です。

オプション	説明
ネットレコーダー（Net recorder）	SNMP メッセージを記録します。オプションは、オフ（Off）、記録（Record）、および 再生（Playback）です。デフォルトはオフ（Off）です。 • 録音（Record）：ライブネットワークとの間で送受信される SNMP メッセージは、検出の実行時に内部で録音され、デバッグに使用されます。 • 再生（Playback）：録音されたメッセージは、ライブネットワークから送信されたかのようにコレクタを介して再生されるため、ネットワーク収集のオフラインデバッグが可能です。 • オフ（Off）：記録や再生は実行されません。

構成解析を使用したポート、LSP、SRLG、および VPN 情報の収集

（注） **構成解析**コレクタは、基本トポロジコレクタではありません。SNMP や SR-PCE など、他の収集方法では含まれない詳細を補うためにのみ使用する必要があります。

始める前に

ワークフロー：事前設定手順 （12 ページ）に記載されている手順を実行します。

構成解析コレクタを設定するには、次の手順を実行します。

手順

ステップ 1 新しい収集を作成するか、既存の収集を編集するかを決定します。詳細については、収集の作成 （33 ページ）または収集の編集 （37 ページ）を参照してください。

ステップ 2 要件に応じて、いずれかの基本トポロジコレクタを選択します。

ステップ 3 [高度なモデリング（Advanced Modeling）] セクションで [構成解析（Config Parsing）] を選択し、[次へ（Next）] をクリックします。

ステップ 4 [設定（Configure）] ページで、左側の [選択されたコレクタ（Selected Collectors）] ペインにある [構成解析（Config Parsing）] をクリックします。

（注）

基本トポロジパラメータが自分のニーズに合わせて更新されていることを確認します。必要に応じてパラメータを更新します。

ステップ 5 [ソース（Source）] ドロップダウンリストから、出力がこのコレクタの入力として機能するソースコレクタを選択します。

ステップ 6 [構成の取得（Get Config）] パネルと[構成の解析（Parse config）] パネルを展開し、関連するフィールドに詳細を入力します。フィールドの説明については、構成解析の詳細オプション （84 ページ）を参照してください。

（注）
- L2VPN 構成解析はサポートされていません。
- 構成解析コレクタで L3VPN 情報を収集する場合、すべての VPN が相互に接続されていると見なされます。
- 構成解析コレクタで VPN 情報を収集していて、VPN コレクタも実行されている場合は、コレクタチェーン内で VPN コレクタが構成解析コレクタの前にあることを確認します。
- 片方の端が欠落しているシングルエンドの SRLG は、SR-PCE を介して収集されます。ただし、SRLGSCircuits テーブルは更新されません。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 設定をプレビューし、[作成（Create）] をクリックして収集を作成します。

次のタスク

- 収集ジョブのスケジュールを設定します。収集ジョブはすぐに実行するようにスケジュールしたり、特定の間隔で実行するようにスケジュールしたりできます。詳細については、収集のスケジュール （39 ページ） を参照してください。
- この収集を送信元ネットワークとして使用して、追加の収集を設定します。さまざまなコレクタの設定の詳細については、この章の関連トピックを参照してください。収集の編集の詳細については、収集の編集 （37 ページ）を参照してください。

構成解析の詳細オプション

構成解析コレクタを使用する場合は、いくつかの詳細オプションを設定できます。

オプション	説明
構成取得のオプション	
構成の収集（Collect configuration）	デバイスまたはルータから構成を収集します。

オプション	説明
強制ログインプラットフォーム（Force login platform）	プラットフォーム検出をオーバーライドして、指定されたプラットフォームを使用します。有効な値：cisco、juniper、alu、huawei。
フォールバック ログイン プラットフォーム（Fallback login platform）	プラットフォームの検出が失敗した場合のフォールバックベンダーを示します。有効な値：cisco、juniper、alu、huawei。
enableの送信を試す（Try send enable）	ルータにログインするときに、プラットフォームタイプが検出されない場合、enable password を送信します。
Telnetユーザー名プロンプト（Telnet username prompt）	代替カスタムユーザー名プロンプトを示します。
Telnetパスワードプロンプト（Telnet password prompt）	代替カスタム パスワード プロンプトを示します。
データ収集タイムアウト（Data collection timeout）	データ収集に許可される最大時間を示します（分単位）。データ収集に使用される内部ツールは、指定された制限時間を超えるとタイムアウトになり、終了します。デフォルトは 60 分です。
構成解析のオプション	
プロトコルタイプ（Protocol type）	ネットワークで実行されている IGP プロトコルを選択できます。オプションは、IS-IS、OSPF、および なし（None） です。デフォルトは **IS-IS** です。
IS-IS レベル（ISIS level）	使用する ISIS レベルを示します。エージェントは、IS-IS レベル 1、レベル 2、またはレベル 1 とレベル 2 の両方のメトリックを読み取れます。両方を選択した場合、エージェントは両方のレベルを 1 つのネットワークに結合します。レベル 2 のメトリックが優先されます。
OSPFエリア（OSPF area）	単一の OSPF エリアを収集するか、すべてのエリアを収集するかを示します。このオプションでは、エリア ID またはすべてを指定します。デフォルトは area 0 です。
ASN	収集する自律システム番号（ASN）を示します。ASN はデフォルトで無視されます。ただし、複数の BGP ASN にまたがるネットワークでは、このオプションを使用して、ASN 内の複数の IGP プロセス ID またはインスタンス ID から情報を読み取ります。

オプション	説明
オブジェクトを含める（Include objects）	解析する構成オブジェクトを選択できます。使用可能なオプションは、LAG、SRLG、RSVP、VPN、FRR、SR LSPS、LMP、および SR ポリシーです。
回路の一致（Circuit match）	回路を形成するために使用する条件を示します。
LAGポートの照合（LAG port match）	ポート回路でローカルポートとリモートポートを照合する方法を決定します。 • 推測（Guess）：できるだけ多くのポートに一致するポート回路を作成します。 • なし（None）：ポート回路を作成しません。
OSPF プロセス ID（OSPF process ID）	複数の OSPF プロセスがある場合に使用する OSPF プロセス ID を示します。
IS-IS インスタンス ID（IS-IS instance ID）	複数の IS-IS インスタンスがある場合に使用する IS-IS インスタンス ID を示します。
ループバック インターフェイス（Loopback interface）	ルータ IP に使用するループバック インターフェイス番号を示します。
参照を解決（Resolve references）	有効になっている場合、IP アドレス参照を解決します。
マルチスレッディング（Multithreading）	マルチスレッディングを使用するかどうかを示します。
showコマンドのフィルタ処理（Filter showcommands）	複数の show コマンドをフィルタ処理します。
トポロジの構築（Build topology）	構成の解析後、ネットワークトポロジを構築します。
共有メディア（Shared media）	共有メディアの疑似ノードを作成します。
データ収集タイムアウト（Data collection timeout）	データ収集に許可される最大時間を示します（分単位）。データ収集に使用される内部ツールは、指定された制限時間を超えるとタイムアウトになり、終了します。デフォルトは 60 分です。
デバッグ	
冗長（Verbosity）	ログの冗長レベルを示します。このレベルは、ログメッセージに表示される詳細と情報の程度を指します。デフォルトは 30 で、有効な範囲は 1 ～ 60 です。

オプション	説明
ネットレコーダー（Net recorder）	SNMP メッセージを記録します。オプションは、オフ（Off）、記録（Record）、および再生（Playback）です。デフォルトはオフ（Off）です。 • 録音（Record）：ライブネットワークとの間で送受信される SNMP メッセージは、検出の実行時に内部で録音され、デバッグに使用されます。 • 再生（Playback）：録音されたメッセージは、ライブネットワークから送信されたかのようにコレクタを介して再生されるため、ネットワーク収集のオフラインデバッグが可能です。 • オフ（Off）：記録や再生は実行されません。

ネットワークモデルの可視化の向上

レイアウトコレクタは、送信元ネットワークモデルにレイアウトプロパティを追加して、Cisco Crosswork Planning にプランファイルをインポートするときの可視化を改善します。このコレクタは、レイアウトプロパティへの変更を自動的に記録します。送信元ネットワークモデルが変更されると、接続先モデルのレイアウトが更新されます。

接続先ネットワークのレイアウトは、送信元ネットワークに適用されるテンプレートとして機能します。得られるネットワークは、新しい接続先ネットワークとして保存されます。送信元レイアウトにレイアウト情報が含まれていない場合、接続先ネットワークのレイアウトが送信元ネットワークに追加されます。送信元ネットワークにレイアウト情報が含まれている場合、そのレイアウトは、接続先ネットワークのレイアウトと競合がない限り維持されます。競合が存在する場合、接続先ネットワークのレイアウト情報が送信元ネットワークの情報よりも優先されます。

（注） レイアウトコレクタは、ノードとサイトのマッピングのみを保存します。ノードの座標は保存されません。

始める前に

ワークフロー：事前設定手順 （12 ページ）に記載されている手順を実行します。

レイアウトコレクタを設定するには、次の手順を実行します。

手順

ステップ 1 新しい収集を作成するか、既存の収集を編集するかを決定します。詳細については、収集の作成 （33 ページ）または収集の編集 （37 ページ）を参照してください。

ステップ 2 要件に応じて、いずれかの基本トポロジコレクタを選択します。

ステップ 3 [トラフィックとデマンド（Traffic and Demands）] セクションで [レイアウト（Layout）] を選択し、[次へ（Next）] をクリックします。

ステップ 4 [設定（Configure）] ページで、左側の [選択されたコレクタ（Selected Collectors）] ペインにある [レイアウト（Layout）] をクリックします。

（注）
基本トポロジパラメータが自分のニーズに合わせて更新されていることを確認します。必要に応じてパラメータを更新します。

ステップ 5 次の設定パラメータを入力します。

- [ソース（Source）]：出力がこのコレクタの入力として機能するソースコレクタを選択します。
- [テンプレートファイル（Template File）]：レイアウトの詳細のコピー元となるテンプレートプランファイルのパスを入力します。

（注）
Cisco WAE または別の Cisco Crosswork Planning インスタンスからコレクタ設定を移行する場合は、コレクタ設定のインポート後に [テンプレートファイル（Template File）] フィールドが正しいファイルで更新されていることを確認します。設定をインポートすると、サーバーでは実際のファイルではなくファイル名のみ復元されるため、この操作が必要です。フィールドが正しいファイルで更新されていない場合、収集は失敗します。

ステップ 6 （オプション）[詳細設定（Advanced settings）] パネルを展開し、次の情報を入力します。

- [タイムアウト（Timeout）]：データ収集に許可される最大時間（分単位）。データ収集に使用される内部ツールは、指定された制限時間を超えるとタイムアウトになり、終了します。デフォルトは 60 分です。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 設定をプレビューし、[作成（Create）] をクリックして収集を作成します。

次のタスク

- 収集ジョブのスケジュールを設定します。収集ジョブはすぐに実行するようにスケジュールしたり、特定の間隔で実行するようにスケジュールしたりできます。詳細については、収集のスケジュール （39 ページ） を参照してください。

- この収集を送信元ネットワークとして使用して、追加の収集を設定します。さまざまなコレクタの設定の詳細については、この章の関連トピックを参照してください。収集の編集の詳細については、収集の編集 （37 ページ）を参照してください。

トラフィック統計情報の収集

トラフィック収集コレクタは、SNMP ポーリングを使用して、トラフィック統計情報（インターフェイス トラフィック、LSP トラフィック、MAC トラフィック、および VPN トラフィック）を収集します。

（注） **トラフィック収集**コレクタを設定すると、[コレクタ（Collector）]>[エージェント（Agents）] ページでトラフィック ポーラー エージェントの詳細を確認できます。エージェントの名前は、収集の名前と同じです。

始める前に

- ワークフロー：事前設定手順 （12 ページ）に記載されている手順を実行します。
- VPN トラフィックを収集する場合、VPN ネットワークモデルが存在する必要があります。VPN トポロジの検出 （73 ページ） を参照してください。
- LSP トラフィックを収集する場合、LSP ネットワークモデルが存在する必要があります。LSP 情報の収集 （62 ページ） を参照してください。

トラフィック収集コレクタを設定するには、次の手順を実行します。

手順

ステップ 1 新しい収集を作成するか、既存の収集を編集するかを決定します。詳細については、収集の作成 （33 ページ）または収集の編集 （37 ページ）を参照してください。

ステップ 2 要件に応じて、いずれかの基本トポロジコレクタを選択します。

ステップ 3 [トラフィックとデマンド（Traffic and Demands）] セクションで [トラフィック収集（Traffic collection）] を選択し、[次へ（Next）] をクリックします。

ステップ 4 [設定（Configure）] ページで、左側の [選択されたコレクタ（Selected collectors）] ペインにある [トラフィック収集（Traffic collection）] をクリックします。

（注）
基本トポロジパラメータが自分のニーズに合わせて更新されていることを確認します。必要に応じてパラメータを更新します。

ステップ 5 トラフィックポーラーを有効にするには、[トラフィック収集（Traffic collection）] チェックボックスをオンにします。

ステップ 6 [ソース（Source）] ドロップダウンリストから、出力がこのコレクタの入力として機能するソースコレクタを選択します。

ステップ 7 インターフェイスの継続的なトラフィック収集を実行するには、[インターフェイストラフィックポーリング（Interface traffic poll）] を有効にして、次のように入力します。

- [ポーリング期間（Polling Period）]：ポーリング期間を秒単位で入力します。60 秒から始めることをお勧めします。
- [QoS]：キューのトラフィック収集を有効にする場合は、[有効化（Enable）] チェックボックスをオンにします。
- [VPN]：VPN トラフィック収集を有効にする場合は、[有効化（Enable）] チェックボックスをオンにします。有効にする場合は、送信元ネットワークモデルで VPN が有効になっていることを確認します。

ステップ 8 LSP の継続的なトラフィック収集を実行するには、[LSP トラフィックポーリング（LSP traffic poll）] を有効にして、次のように入力します。

- [ポーリング期間（Polling Period）]：ポーリング期間を秒単位で入力します。60 秒から始めることをお勧めします。

ステップ 9 MAC アカウンティングの継続的なトラフィック収集を実行するには、[MAC トラフィックポーリング（MAC traffic poll）] を有効にして、次のように入力します。

- [ポーリング期間（Polling Period）]：ポーリング期間を秒単位で入力します。60 秒から始めることをお勧めします。

（注）
[MAC トラフィックポーリング（MAC traffic poll）] が有効になっている場合は、送信元ネットワークモデルに MAC アドレスがあることを確認してください。

ステップ 10 （オプション）[SNMP トラフィック計算（SNMP traffic computation）] パネルを展開し、関連するフィールドに詳細を入力します。フィールドの説明については、トラフィック収集の詳細オプション （91 ページ） を参照してください。

ステップ 11 [Next] をクリックします。

ステップ 12 設定をプレビューし、[作成（Create）] をクリックして収集を作成します。

収集されたトラフィックデータをプランファイルに入力するスケジュールを設定する必要があります。トラフィックの詳細は、スケジュールされたジョブの実行時にのみプランファイルで更新されます。ジョブが実行されない場合、トラフィックデータはプランファイルで更新されません。

次のタスク

- 収集ジョブのスケジュールを設定します。収集ジョブはすぐに実行するようにスケジュールしたり、特定の間隔で実行するようにスケジュールしたりできます。詳細については、収集のスケジュール （39 ページ） を参照してください。

- この収集を送信元ネットワークとして使用して、追加の収集を設定します。さまざまなコレクタの設定の詳細については、この章の関連トピックを参照してください。収集の編集の詳細については、収集の編集 （37 ページ）を参照してください。

トラフィック収集の詳細オプション

トラフィック収集を使用する場合は、いくつかの詳細オプションを設定できます。

オプション	説明
最小ウィンドウ長（Minimum window length）	トラフィック計算の最小ウィンドウ長（秒単位）を示します。デフォルトは 300 秒です。
最大ウィンドウ長（Maximum window length）	トラフィック計算の最大ウィンドウ長（秒単位）を示します。デフォルトは 450 秒です。
rawカウンタTTL（Raw counter TTL）	raw カウンタを保持する期間（分単位）を示します。デフォルトは 15 分です。
キャパシティを超える分を破棄（Discard over capacity）	キャパシティよりも高いトラフィックレートを破棄します。
ネットレコーダーファイルの最大サイズ（Net recorder file max size）	ネットレコードファイルの最大サイズを示します。
データ収集タイムアウト（Data collection timeout）	データ収集に許可される最大時間を示します（分単位）。データ収集に使用される内部ツールは、指定された制限時間を超えるとタイムアウトになり、終了します。デフォルトは 60 分です。
デバッグ	
冗長（Verbosity）	ログの冗長レベルを示します。このレベルは、ログメッセージに表示される詳細と情報の程度を指します。デフォルトは 30 で、有効な範囲は 1 ～ 60 です。

オプション	説明
ネットレコーダー（Net recorder）	SNMP メッセージを記録します。オプションは、オフ（Off）、記録（Record）、および 再生（Playback）です。デフォルトはオフ（Off）です。 • 録音（Record）：ライブネットワークとの間で送受信される SNMP メッセージは、検出の実行時に内部で録音され、デバッグに使用されます。 • 再生（Playback）：録音されたメッセージは、ライブネットワークから送信されたかのようにコレクタを介して再生されるため、ネットワーク収集のオフラインデバッグが可能です。 • オフ（Off）：記録や再生は実行されません。

トラフィックデマンド情報の収集

デマンド推論コレクタは、ネットワークからトラフィックデマンドに関する情報を収集します。

始める前に

ワークフロー：事前設定手順 （12 ページ）に記載されている手順を実行します。

デマンド推論コレクタを設定するには、次の手順を実行します。

手順

ステップ 1 新しい収集を作成するか、既存の収集を編集するかを決定します。詳細については、収集の作成 （33 ページ）または収集の編集 （37 ページ）を参照してください。

ステップ 2 要件に応じて、いずれかの基本トポロジコレクタを選択します。

ステップ 3 [トラフィックとデマンド（Traffic and Demands）] セクションで [デマンド推論（Demand deduction）] を選択し、[次へ（Next）] をクリックします。

ステップ 4 [設定（Configure）] ページで、左側の [選択されたコレクタ（Selected collectors）] ペインにある [デマンド推論（Demand deduction）] をクリックします。

（注）
基本トポロジパラメータが自分のニーズに合わせて更新されていることを確認します。必要に応じてパラメータを更新します。

ステップ 5 [ソース（Source）] ドロップダウンリストから、出力モデルがこのコレクタの入力として機能するソースコレクタを選択します。

ステップ 6 [デマンドメッシュステップ（Demand mesh steps）]で、[+ステップの追加（+ Add step）] をクリックしてステップを 追加します。[メッシュステップの追加（Add Mess Step）] ウィンドウで、次の詳細情報を入力します。

a) [名前（Name）] フィールドに、ステップの名前を入力します。
b) [ステップ番号（Step number）] フィールドに、このステップを実行する順序を入力します。
c) [ツール（Tool）] ドロップダウンリストから必要なツールを選択します。使用可能なツールは、P2MP LSP のデマンド、デマンド推論、外部実行可能スクリプト、デマンドのコピー、LSP のデマンド、およびデマンドメッシュクリエータです。
d) 選択したツールを実行するには、[有効（Enable）] チェックボックスをオンにします。
e) [ツール設定（Tool Configuration）]セクションで詳細を更新または入力します。選択したツールに基づいて、このセクションのオプションは異なります。
f) （オプション）[詳細設定（Advanced Settings）] パネルを展開し、詳細を入力します。
g) [続行（Continue）] をクリックします。

設定にさらにステップを追加するには、このステップを繰り返します。

追加したステップを削除するには、ステップを選択し、[メッシュステップ（Mesh Step）] ウィンドウで[削除（Delete）] ボタンをクリックします。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 設定をプレビューし、[作成（Create）] をクリックして収集を作成します。

次のタスク

- 収集ジョブのスケジュールを設定します。収集ジョブはすぐに実行するようにスケジュールしたり、特定の間隔で実行するようにスケジュールしたりできます。詳細については、収集のスケジュール （39 ページ） を参照してください。
- この収集を送信元ネットワークとして使用して、追加の収集を設定します。さまざまなコレクタの設定の詳細については、この章の関連トピックを参照してください。収集の編集の詳細については、収集の編集 （37 ページ）を参照してください。

NetFlow データ収集

Cisco Crosswork Planning は、エクスポートされた NetFlow および関連するフロー測定値を収集して集約できます。これらの測定値を使用して、Cisco Crosswork Planning Design 用の正確なデマンドトラフィックデータを構築できます。フロー収集は、デマンド推論を使用したインターフェイス、LSP、およびその他の統計からのデマンドトラフィックの推定に代わる手段を提供します。NetFlow は、トラフィックフローに関する情報を収集し、トラフィックとデマンドのマトリックスを構築するのに役立ちます。フロー測定値のインポートは、ネットワークのエッジルータのフローカバレッジが完全またはほぼ完全な場合に特に役立ちます。さらに、外部の自律システム（AS）間の個々のデマンドの精度が重要な場合にも役立ちます。

トポロジ、BGP ネイバー、インターフェイス統計など、コレクタによって個別に収集されたネットワークデータは、フロー測定値と組み合わされてフローをスケーリングし、外部の自律システムと内部のノードの両方の間で完全なデマンドメッシュを提供します。

Cisco Crosswork Planning は、次のタイプのデータを収集して、フローとそのトラフィック測定値を時間の経過とともに集約したネットワークモデルを構築します。

- NetFlow、JFlow、CFlowd、IPFIX、および Netstream フローを使用したフロートラフィック
- SNMP 経由のインターフェイス トラフィックと BGP ピア
- ピアリングセッション上の BGP パス属性

NetFlow 収集の構成

フロー収集プロセスは、入力方向のルータによってキャプチャおよびエクスポートされる IPv4 および IPv6 フローをサポートしています。また、IPv4 および IPv6 iBGP ピアリングもサポートしています。

ルータは、フローをフロー収集サーバーにエクスポートし、フロー収集サーバーとの BGP ピアリングを確立するように構成する必要があります。次の推奨事項に留意してください。

- NetFlow v5、v9、および IPFIX データグラムは、フロー収集サーバーの UDP ポート番号にエクスポートされます。デフォルト設定は 2100 です。IPv6 フローのエクスポートには、NetFlow v9 または IPFIX が必要です。
- フローコレクタサーバーの iBGP ルートリフレクタ クライアントとして設定されたルータで BGP セッションを定義します。ルータ自体でこれを設定できない場合は、関連するすべてのルーティングテーブルの完全なビューを備えた BGP ルートリフレクタ サーバーを代わりに使用できます。
- フロー エクスポート データグラムの送信元 IPv4 アドレスが iBGP メッセージの送信元 IPv4 アドレスと同じネットワークアドレス空間にある場合は、同じアドレスになるように構成します。
- BGP ルータ ID を明示的に構成します。
- BGP ルートを受信する場合、BGP の `AS path` 属性の最大長は 3 ホップに制限されます。その理由は、単一の IP プレフィックスに付加された BGP 属性（`AS path` を含む）の合計長が非常に大きくなる（最大 64 KB）可能性があることを考慮して、過度のサーバーメモリ消費を防ぐためです。

NetFlow 収集を構成する

始める前に

- ワークフロー：事前設定手順 （12 ページ）に記載されている手順を実行します。
- シングルモードで動作するように NetFlow エージェントを設定します。

NetFlow コレクタを設定するには、次の手順を実行します。

手順

ステップ 1 新しい収集を作成するか、既存の収集を編集するかを決定します。詳細については、収集の作成 （33 ページ）または収集の編集 （37 ページ）を参照してください。

ステップ 2 要件に応じて、いずれかの基本トポロジコレクタを選択します。

ステップ 3 [トラフィックとデマンド（Traffic and Demands）] セクションで [NetFlow] を選択し、[次へ（Next）] をクリックします。

ステップ 4 [設定（Configure）] ページで、左側の [選択されたコレクタ（Selected collectors）] ペインにある [NetFlow] をクリックします。

（注）
基本トポロジパラメータが自分のニーズに合わせて更新されていることを確認します。必要に応じてパラメータを更新します。

ステップ 5 次の設定パラメータを入力します。

- [ソース（Source）]：出力がこのコレクタの入力として機能するソースコレクタを選択します。
- [エージェント（Agents）]：ドロップダウンリストから該当するエージェントを選択します。

ステップ 6 [共通設定（Common config）] セクションの [入力時のASフローの分割（Split AS flows on ingress）] ドロップダウンリストから、外部 ASN のトラフィック集約方法を選択します。

（オプション）他のフィールドに情報を入力します。フィールドの説明については、NetFlow 収集の詳細オプション （96 ページ）を参照してください。

ステップ 7 （オプション）[IASフロー（IAS flows）] パネルと [デマンド（Demands）] パネルを展開し、関連するフィールドに詳細を入力します。各オプションの説明については、NetFlow 収集の詳細オプション （96 ページ）を参照してください。

ステップ 8 [次へ（Next）] をクリックします。

ステップ 9 設定をプレビューし、[作成（Create）] をクリックして収集を作成します。

次のタスク

- 収集ジョブのスケジュールを設定します。収集ジョブはすぐに実行するようにスケジュールしたり、特定の間隔で実行するようにスケジュールしたりできます。詳細については、収集のスケジュール （39 ページ）を参照してください。
- この収集を送信元ネットワークとして使用して、追加の収集を設定します。さまざまなコレクタの設定の詳細については、この章の関連トピックを参照してください。収集の編集の詳細については、収集の編集 （37 ページ）を参照してください。

NetFlow 収集の詳細オプション

NetFlow コレクタを使用する場合は、いくつかの詳細オプションを設定できます。

オプション	説明
共通設定の設定	
入力時の AS フローの分割（Split AS flows on ingress）	外部 ASN のトラフィック集約方法を示します。
ASN	ネットワーク内の内部 AS の ASN を示します。
アドレスファミリ（Address family）	IAS のフローおよびデマンドの計算に含めるプロトコルバージョンを示します。
外部ノードタグ（Ext node tags）	1 つ以上のノードタグを入力できます。[+] をクリックして、1 つ以上のノードタグのリストを入力します。
出力時の AS フローの分割（Split AS flows on egress）	出力 AS に接続しているすべてのインターフェイスを介して、出力で AS 間フローを分割します。
追加集約（Extra aggregation）	ドロップダウンリストから集約キーのリストを選択できます。
ログ レベル（Log level）	ツールのログレベルを示します。オプションは、オフ（Off）、致命的（Fatal）、エラー（Error）、警告（Warn）、通知（Notice）、情報（Info）、デバッグ（Debug）、およびトレース（Trace）です。
スレッド数（Number of threads）	並列計算で使用するスレッドの最大数を示します。
IAS フロー設定	
AS間フローのトリム（Trim inter AS flows）	トラフィックの AS 間フローが厳密に破棄されない下限値をメガビット/秒単位で示します。
BGP外部情報の照合（Match BGP external info）	BGP ピア関係の出力 IP アドレスを照合するかどうかを示します。
入力インターフェイスフィルタ（Ingress interface filter）	ノードとインターフェイスのフィルタを Node:InterfaceName の形式で示します。これは、フローマトリックスを読み取り、対象の入力インターフェイスのみをフィルタ処理する際に適用されます。
出力インターフェイスフィルタ（Egress interface filter）	ノードとインターフェイスのフィルタを Node:InterfaceName の形式で示します。これは、フローマトリックスを読み取り、対象の出力インターフェイスのみをフィルタ処理する際に適用されます。

オプション	説明
マイクロフローのバックトラック（Back track micro flows）	入力ファイルからのマイクロフローと、マイクロフローのデマンドまたはマイクロフローを集約する inter-as-flow との関係を示すファイルを生成するかどうかを示します。
フローインポートID（Flow import IDs）	データのインポート元のフロー ID をカンマで区切って入力できます。
IAS計算タイムアウト（AS computation timeout）	IAS フロー計算のタイムアウトを示します（分単位）。有効な範囲は 1 ～ 1,440 です。デフォルトは 60 分です。
デマンド設定	
デマンド名（Demand name）	新しいデマンドの名前を示します。
デマンドタグ（Demand tag）	新しいデマンドのタグ、または既存のデマンドに追加するタグを示します。
デマンドのトリム（Trim demands）	デマンドが厳密に破棄されない下限値をメガビット/秒単位で示します。
デマンドサービスクラス（Demand service class）	デマンドサービスクラスを示します。
デマンドトラフィックレベル（Demand traffic level）	デマンドトラフィックレベルを示します。
欠落しているフロー（Missing flows）	フローが欠落しているインターフェイスを含むファイルが生成されるパスを示します。

ネットワークモデルに対する外部スクリプトの実行

外部スクリプトを使用すると、選択したネットワークモデルに対してカスタマイズされたスクリプトを実行できます。既存の Cisco Crosswork Planning コレクタで提供されないネットワークからの特定のデータが必要な場合、この手順を実行する必要がある場合があります。この場合、Cisco Crosswork Planning で作成された既存の収集モデルを取得し、カスタムスクリプトからの情報を追加して、必要なデータを含む最終ネットワークモデルを作成します。

始める前に

- ワークフロー：事前設定手順 （12 ページ）に記載されている手順を実行します。
- カスタムスクリプトが使用可能である必要があります。

ネットワークモデルに対して外部手順を実行するには、次の手順を実行します。

手順

ステップ 1 新しい収集を作成するか、既存の収集を編集するかを決定します。詳細については、「収集の作成 （33 ページ）」および「収集の編集 （37 ページ）」を参照してください。

ステップ 2 要件に応じて、いずれかの基本トポロジコレクタを選択します。

ステップ 3 [設定（Configure）]ページで、[高度なモデリング（Advanced Modeling）] または [トラフィックとデマンド（Traffic and Demands）] セクションの [+外部スクリプトの追加（+ Add external script）] をクリックします。

ステップ 4 次の詳細を入力します。

- [コレクタ名（Collector name）]：この収集の名前を入力します。
- [送信元はプランファイルか（Is source a plan file?）]：プランファイルでスクリプトを実行する場合は、このチェックボックスをオンにします。このオプションを選択した場合は、[プランファイルの入力（Input plan file）] フィールドにプランファイルの詳細を入力します。
- [送信元（Source）]：外部スクリプトを実行するコレクタを選択します。たとえば、[送信元（Source）] として BGP を選択した場合、カスタムスクリプトは BGP コレクタで実行されます。BGP 収集からの出力モデルは、カスタムスクリプトで指定された仕様に基づいて更新されます。
- [入力ファイル（Input File）]：カスタムスクリプトを正常に実行するために必要なサポートファイルをアップロードします。
- [実行可能スクリプト（Executable Script）]：カスタムスクリプトの詳細を入力します。
- [スクリプト言語（Script Language）]：カスタムスクリプトの言語を選択します。有効なスクリプト言語は、Python、Shell、および Perl です。
- [アグリゲータプロパティ（Aggregator Properties）]：集約するテーブルや列を指定する場合は .properties ファイルで指定し、このフィールドを使用してファイルをアップロードします。デフォルトでは、すべての列とテーブルが集約されます。
- [タイムアウト（Timeout）]：アクションのタイムアウトを指定します。デフォルトは 30 分です。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 設定をプレビューし、[作成（Create）] をクリックして収集を作成します。

次のタスク

収集ジョブのスケジュールを設定します。収集ジョブはすぐに実行するようにスケジュールしたり、特定の間隔で実行するようにスケジュールしたりできます。詳細については、収集のスケジュール （39 ページ） を参照してください。

AS プランファイルのマージ

[ASのマージ（Merge AS）] ツールは、異なる自律システム（AS）からのプランファイルをマージするのに役立ちます。[ASのマージ（Merge AS）] ツールは、プランファイル間の競合を解決します。ネイティブ形式の計画ファイルもサポートされています。

各 AS は、異なる Cisco Crosswork Planning サーバー上に配置できます。

（注）

- 自律システム（AS）、回路、ノード、インターフェイス、外部エンドポイント、仮想ノードおよび未解決のインターフェイスを持つ外部エンドポイントメンバーのみが解決されます。
- 次のデマンドが解決されます。
  - 実ノードで解決される仮想ノードに関連付けられた送信元または宛先。
  - 特定の形式でインターフェイスに関連付けられた送信元または宛先。
  - 外部エンドポイントに関連付けられた送信元または宛先。
- 次のデマンドは解決されていません。
  - ASN 番号のみに関連付けられた送信元または宛先。
- 特定のプランファイルについては、他のプランファイルが外部 AS 番号として認識するものと内部 AS 番号が一致する必要があり、マージされるすべての自律システムは、すべてのプランファイルで検出される必要があります。

始める前に

- さまざまな自律システム（AS）のトポロジとトラフィック情報を収集します。
- 異なる AS からのプランファイルは、同じ Cisco Crosswork Planning サーバーに存在する必要があり、プランファイルへのパスを指定する必要があります。
- ワークフロー：事前設定手順 （12 ページ）に記載されている手順を実行します。

手順

ステップ 1 新しい収集を作成するか、既存の収集を編集するかを決定します。詳細については、収集の作成 （33 ページ）または収集の編集 （37 ページ）を参照してください。

ステップ 2 上部の [ツール（Tools）] オプションボタンをクリックします。

ステップ 3 [ツール（Tools）] セクションで [ASのマージ（Merge AS）] を選択し、[次へ（Next）] をクリックします。

ステップ 4 次の設定パラメータを入力します。

- [デマンドを保持（Retain demands）]：デマンドをマージするには、[有効（Enabled）] チェックボックスをオンにします。
- [タグ名（Tag name）]：.pln ファイル内の更新された行の識別に役立つタグ名を入力します。.pln ファイルのタグ列は、変更された行のタグ名で更新されます。

ステップ 5 [ソースコレクタ（Source Collector）] セクションで、[+ソースコレクタの追加（+ Add source collector）] をクリックし、関連する収集とコレクタ名を選択します。

ステップ 6 [ソースDB（Source DB）] セクションで、[+ソースDBの追加（+ Add source DB）] をクリックし、[参照（Browse）] をクリックしてシステムに存在するソースプランファイルを選択します。

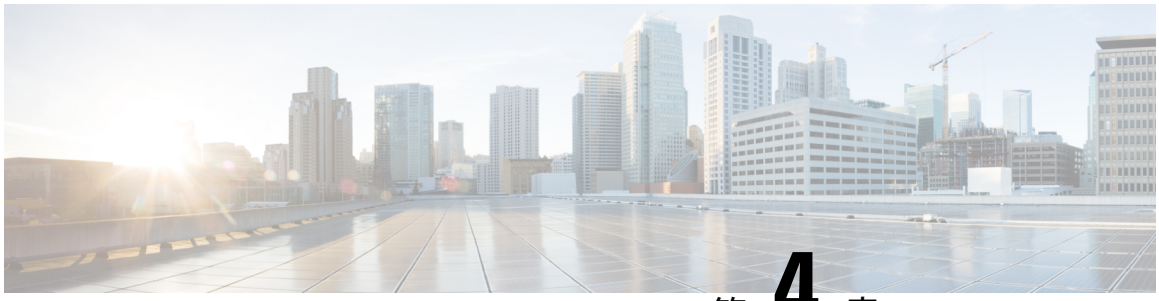
（注）
Cisco WAE または別の Cisco Crosswork Planning インスタンスから設定を移行する場合は、設定のインポート後に [DBファイル（DB File）] フィールドが正しいファイルで更新されていることを確認します。設定をインポートすると、サーバーでは実際のファイルではなくファイル名のみ復元されるため、この操作が必要です。フィールドが正しいファイルで更新されていない場合、収集は失敗します。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 設定をプレビューし、[作成（Create）] をクリックして収集を作成します。

次のタスク

- 収集ジョブのスケジュールを設定します。収集ジョブはすぐに実行するようにスケジュールしたり、特定の間隔で実行するようにスケジュールしたりできます。詳細については、収集のスケジュール （39 ページ） を参照してください。
- この収集を送信元ネットワークとして使用して、追加の収集を設定します。さまざまなコレクタの設定の詳細については、この章の関連トピックを参照してください。収集の編集の詳細については、収集の編集 （37 ページ）を参照してください。



第 4 章

ライセンスの管理

Cisco Crosswork Planning は、シスコ スマート ライセンスをサポートしています。Cisco Crosswork Planning のすべての機能を使用するには、ライセンスが必要です。ライセンスの取得について質問がある場合は、シスコのサポート担当者またはシステム管理者にお問い合わせください。

この章は次のトピックで構成されています。

シスコ スマートライセンシングの概要

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。

ワークフロー：スマートライセンシングの設定

Cisco Smart Licensing の設定手順の概要は次のとおりです。

表 *9:* スマートライセンシング設定のワークフロー

手順	操作
1. Cisco Software Central（software.cisco.com）でスマートアカウントを設定します。	「Smart Account Request」に移動し、Web サイトの指示に従います。
2.（オプション）転送設定を構成します。	Cisco Crosswork Planning とCSSM 間のトランスポートモードの設定 （102 ページ）。
3.Cisco Crosswork Planning を Cisco Smart Software Manager（CSSM）に登録します。	参照先： • トークンを介した Cisco Crosswork Planning の登録 （104 ページ） • オフライン予約による Cisco Crosswork Planning の登録 （108 ページ）

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。

Cisco Crosswork Planning UI のメインメニューから、[ライセンス（Licensing）] を選択します。[スマートライセンス（Smart License）] ページが開きます。このページで、Cisco Crosswork Planning 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。

Cisco Crosswork Planning とCSSM 間のトランスポートモードの設定

トランスポート設定を構成して、Cisco Crosswork Planning の CSSM との通信方法を決定できます。

- [直接（Direct）]：Cisco Crosswork Planning はCSSM に直接接続します。

- [トランスポートゲートウェイ（Transport Gateway）]：Cisco Crosswork Planning は、トランスポートゲートウェイ、またはクラウドベースとユーザーエクスペリエンスが同じながらもオンプレミスに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。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。

（注） Cisco Crosswork Planning は SmartTransport URL のみをサポートします。URL の形式は http://<*SSM-ONPREM-IP*>/SmartTransport です。

- [HTTP/HTTPSプロキシ（HTTP/HTTPS Proxy）]：Cisco Crosswork Planning は、プロキシが設定されている場合、設定されたプロキシを介してダイレクトモードエンドポイントと通信します。

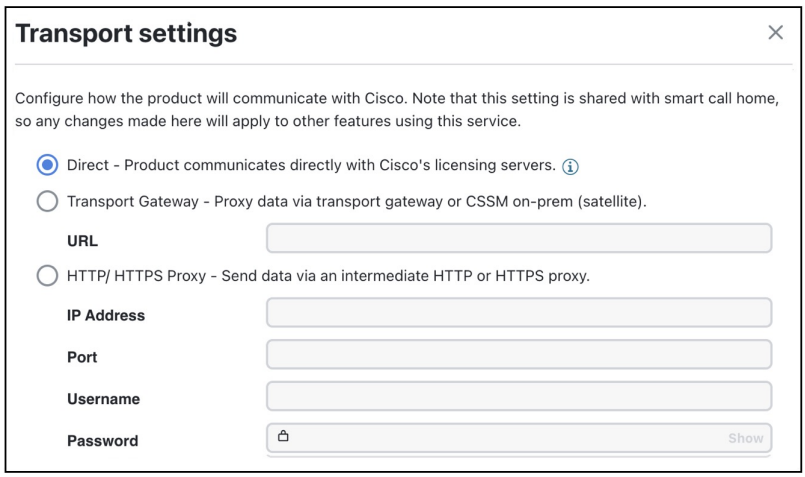
（注） トランスポート設定は、Cisco Crosswork Planning 製品が登録済みモードになっている間は変更できません。変更するには登録を解除する必要があります。

手順

ステップ 1 メインメニューから、[ライセンス（Licensing）] を選択します。[スマートライセンス（Smart License）] ページが開きます。

ステップ 2 [トランスポート設定（Transport settings）] フィールドに、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。

図 *23 : [トランスポート設定（Transport Settings）]* ダイアログボックス



ステップ 3 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 4 [保存（Save）] をクリックします。

トークンを介した Cisco Crosswork Planning 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 Planning 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、Cisco Software Central 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。

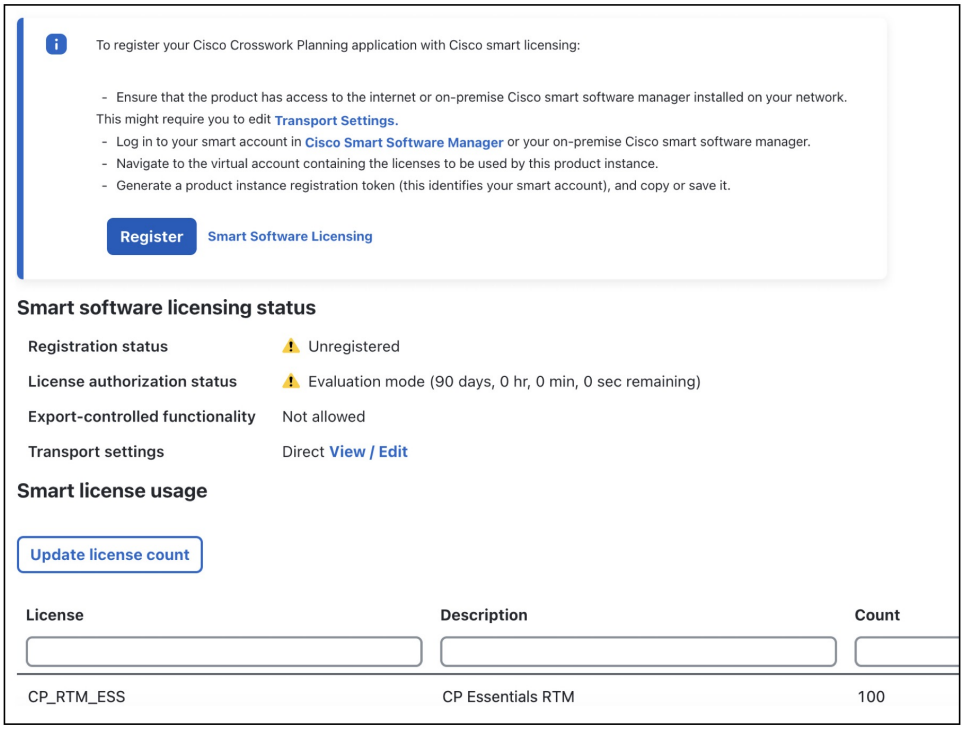
始める前に

スマートアカウントがあることを確認します。ない場合、「Smart Account Request」に移動し、Web サイトの指示に従います。

手順

ステップ 1 メインメニューから、[ライセンス（Licensing）] を選択します。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 [未登録（Unregistered）] と [評価（Evaluation）] モードになります。

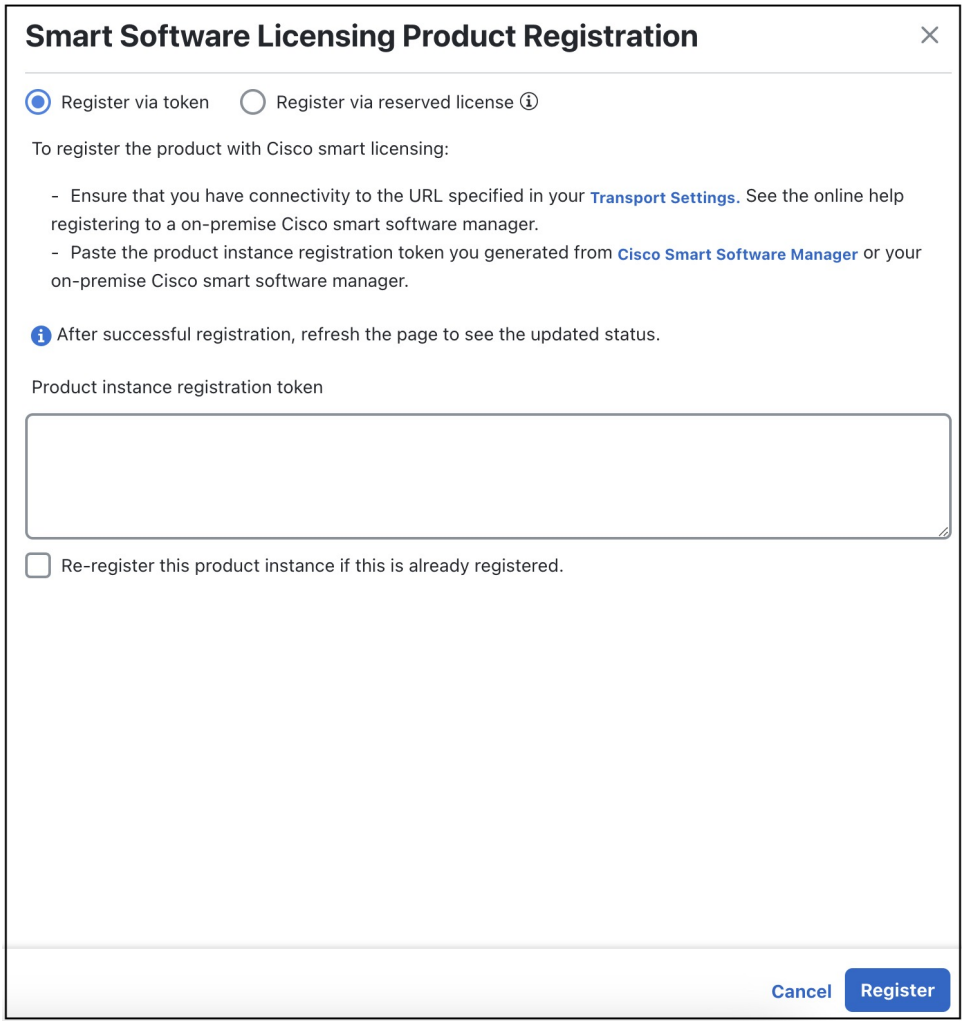
図 *24* : スマート ソフトウェア ライセンスの未登録の例



ステップ 2 上部の [スマート ソフトウェア ライセンシング（Smart Software Licensing）] 情報ボックスで、[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。

図 *25 : [*スマートソフトウェアライセンシング製品登録（***Smart Software Licensing Product Registration***）*]* ダイアログボックス



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ます。

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。

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）

- 要求が成功するまでに少なくとも 20 秒かかります。最初の 20 秒以内にバックエンドから正しい応答が得られない場合、UI は最大 5 分間、10 秒ごとにチェックを続けます。5 分経過しても応答が得られない場合は、一般的なエラーメッセージが表示されます。

- 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。
- 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 Planning に対して、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。

始める前に

アプリケーションが登録済みモードであることを確認します。

手順

ステップ 1 メインメニューから、[ライセンス（Licensing）] を選択します。[スマートライセンス（Smart License）] ページが表示されます。

ステップ 2 [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 （113 ページ）を参照してください。

オフライン予約による Cisco Crosswork Planning の登録

スマートライセンスが使用されている場合、Cisco Crosswork Planning は使用状況情報を CSSM と定期的に共有します。CSSM に定期的に接続したくない場合は、Cisco Smart Licensing にオフライン予約のオプションが用意されています。

始める前に

スマートアカウントがあることを確認します。ない場合、「Smart Account Request」に移動し、Web サイトの指示に従います。

手順

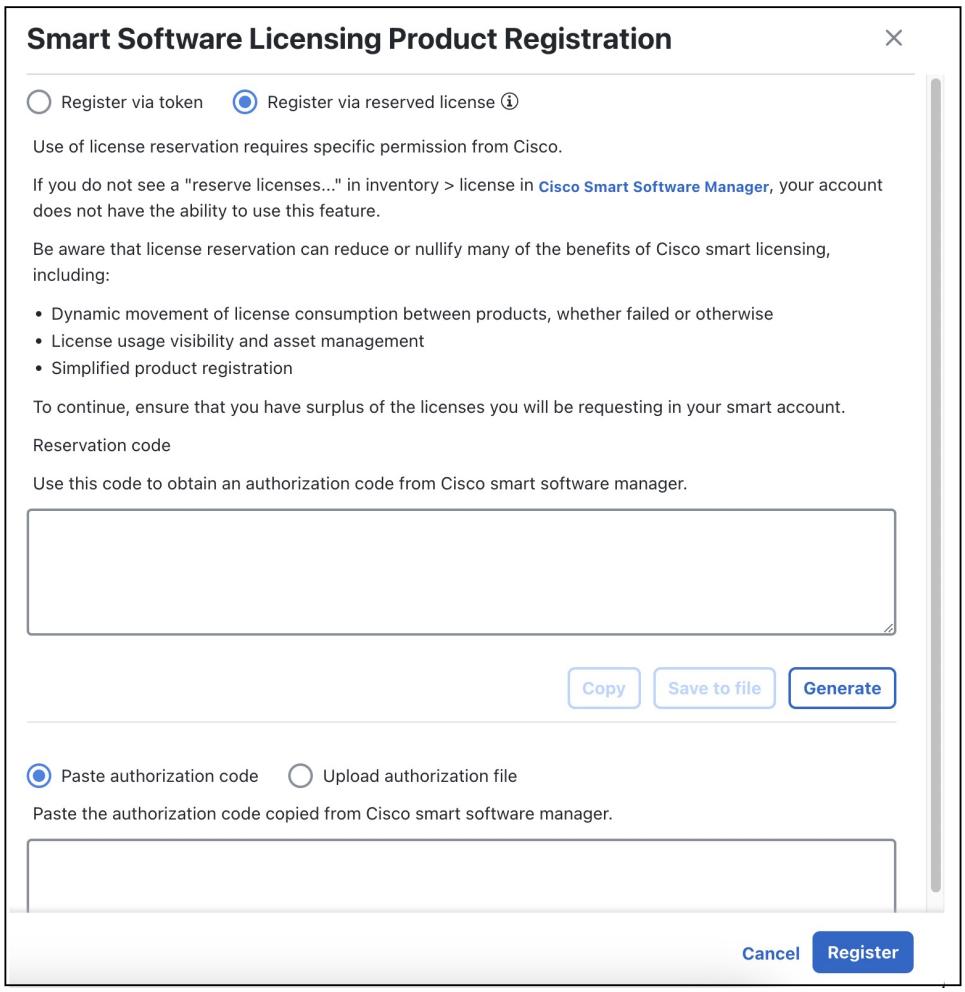
ステップ 1 メインメニューから、[ライセンス（Licensing）] を選択します。

ステップ 2 上部の [スマート ソフトウェア ライセンシング（Smart Software Licensing）] 情報ボックスで、[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 [予約済みライセンスで登録（Register via reserved license）] オプションを選択します。

図 *26 : [*スマートソフトウェアライセンシング製品登録（***Smart Software Licensing Product Registration***）*]* ダイアログボックス



ステップ 4 [予約コード（Reservation code）] セクションの下にある [生成（Generate）] ボタンをクリックします。予約要求コードが生成され、テキストフィールドに入力されます。[コピー（Copy）] ボタンを使用してこのコードをコピーします。

ステップ 5 CSSM に移動し、適切なバーチャルアカウントを選択します。

ステップ 6 [ライセンス（Licenses）] タブをクリックし、[ライセンス予約（License Reservation）] をクリックします。手順 3 で生成した予約要求コードを貼り付けて、[次へ（Next）] をクリックします。

ステップ 7 [ライセンスの選択（Select Licenses）] ページで、必要な予約のタイプを選択します。次に、[Next] をクリックします。

ステップ 8 [レビューと確認（Review and Confirm）] ページで [認証コードの生成（Generate Authorization Code）] をクリックします。[クリップボードにコピー（Copy to Clipboard）] ボタンを使用してコードをコピーします。

ステップ 9 Cisco Crosswork Planning UI の [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）] ページに戻ります。[認証コードを貼り付ける（Paste authorisation code）] オプションボタンを選択して、テキストフィールドに承認コードを貼り付けます。

ステップ 10 [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。

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。

オフライン予約の更新

[予約の更新（Update Reservation）] オプションを使用して、オフライン予約で予約されたライセンス数を更新します。

手順

ステップ 1 メインメニューから、[ライセンス（Licensing）] を選択します。製品インスタンス名を書き留めます（[スマートソフトウェアライセンシングのステータス（Smart Software Licensing Status）] セクションにあります）。

ステップ 2 CSSM に移動し、適切なバーチャルアカウントを選択します。

ステップ 3 [製品インスタンス名（Product Instance Name）] に一致する製品インスタンスの名前をクリックします。

ステップ 4 この製品インスタンスに対応する [アクション（Actions）] ドロップダウンボタンをクリックし、[予約の更新（Update Reservation）] を選択します。

ステップ 5 [ライセンスの選択（Select Licenses）] 画面で、[特定のライセンス予約（Reserve a Specific License）] オプションボタンを選択し、リストから必要なライセンスの数を更新して、[次へ（Next）] をクリックします。

ステップ 6 [レビューと確認（Review and Confirm）] ページで [認証コードの生成（Generate Authorization Code）] をクリックします。[クリップボードにコピー（Copy to Clipboard）] ボタンを使用してコードをコピーします。

ステップ 7 Cisco Crosswork Planning UI の [スマートライセンス（Smart License）] ページに戻ります。[アクション（Actions）] ドロップダウンボタンをクリックし、[予約の更新（Update Reservation）] を選択します。前の手順で生成した認証コードを貼り付け、[更新（Update）] をクリックします。

確認コードが生成されます。[スマートソフトウェアライセンシングのステータス（Smart Software Licensing Status）] セクションで確認できます。このコードをコピーします。

ステップ 8 CSSM に戻ります。必要な製品インスタンス名をクリックします。

ステップ 9 [アクション（Actions）] ドロップダウンボタンをクリックし、[確認コードの入力（Enter Confirmation Code）] を選択します。

ステップ 10 手順 7 で生成された予約確認コードを入力/貼り付けて、[OK] をクリックします。

ライセンス数は、Cisco Crosswork Planning UI の [スマートライセンス（Smart License）] ページで更新されます。

オフライン予約の無効化

[予約の返却（Return Reservation）] オプションを使用して、予約済みのライセンスをリリースします。ライセンスがリリースされると、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 （113 ページ）を参照してください。

手順

ステップ 1 メインメニューから、[ライセンス（Licensing）] を選択します。製品インスタンス名を書き留めます（[スマートソフトウェアライセンシングのステータス（Smart Software Licensing Status）] セクションにあります）。

ステップ 2 [アクション（Actions）] ドロップダウンボタンをクリックし、[予約の返却（Return Reservation）] を選択します。

ステップ 3 [予約の返却の確認（Confirm Return Reservation）] ウィンドウで、[確認（Confirm）] をクリックします。

リリースコード（予約リターンコード）が生成されます。[コピー（Copy）] ボタンを使用してこのコードをコピーします。

ステップ 4 CSSM に移動し、適切なバーチャルアカウントを選択します。

ステップ 5 [製品インスタンス名（Product Instance Name）] に一致する製品インスタンスの名前をクリックします。

ステップ 6 この製品インスタンスに対応する [アクション（Actions）] ドロップダウンボタンをクリックし、[削除（Remove）] を選択します。

ステップ 7 [予約の削除（Remove Reservation）] ポップアップで、手順 3 で生成した予約リターンコードを貼り付け、[予約の削除（Remove Reservation）] をクリックします。

Cisco Crosswork Planning UI の [スマートライセンス（Smart License）] ページで、登録ステータスが [未登録（Unregistered）] に更新されます。

ステップ 8 Cisco Crosswork Planning UI で [スマートライセンス（Smart License）] ページに戻ります。[アクション（Actions）] ドロップダウンボタンをクリックし、[ライセンス予約の無効化（Disable License Reservation）] を選択します。

ライセンス数の更新

Cisco Crosswork Planning では、要件に応じて使用するライセンスの数を入力できます。バーチャルアカウントに十分な数のライセンスがあることを確認します。ライセンス数が不足していると、コンプライアンス違反となります。

Cisco Crosswork Planning Design アプリケーションの各ツールが正しく機能するには、適切な数のライセンスが必要です。ライセンス数を更新するには、次の手順を実行します。

手順

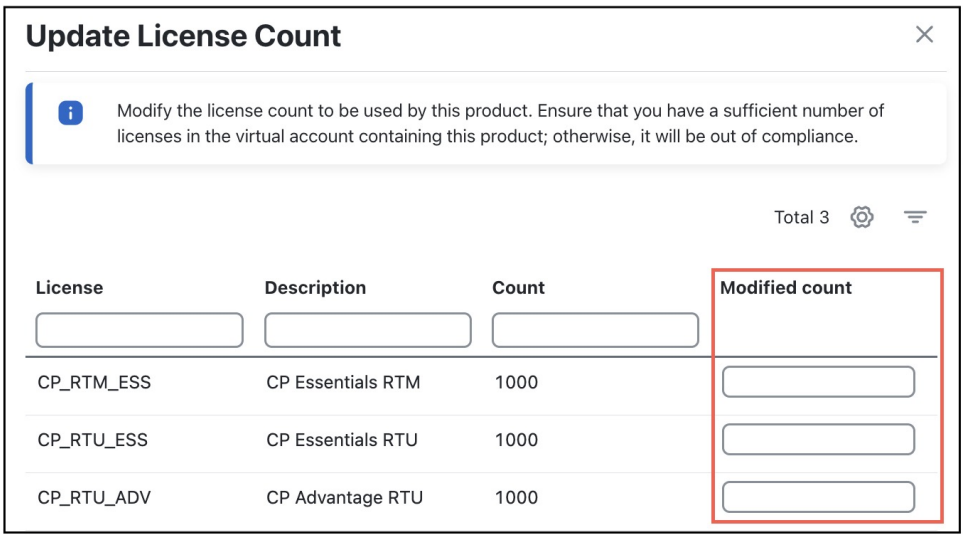
ステップ 1 メインメニューから、[ライセンス（Licensing）] を選択します。

ステップ 2 [ライセンスの使用状況（License usage）] セクションで、[ライセンス数の更新（Update license count）] をクリックします。

[ライセンス数の更新（Update License Count）] ウィンドウが表示されます。

ステップ 3 [変更後の数（Modified count）] 列に必要なライセンス数を入力します。

図 *27* : ライセンス数の更新



Cisco Crosswork Planning には、3 種類のライセンスがあります。

- CP_RTM_ESS：1 つのライセンスを使用するか、ネットワーク内のノード数と同じ数のライセンスを使用するかを選択できます。Cisco Crosswork Planning Collector アプリケーションは、使用可能なライセンスが 1 つしかない場合でも機能します。ただし、Cisco Crosswork Planning Design アプリケーションの場合、カウントはネットワーク内のノード数と一致する必要があります。これは、ツールとイニシャライザが正しく機能するために必要です。
- CP_RTU_ESS：カウントを 1 にして、Cisco Crosswork Planning Collector と Design の両方のアプリケーションを正しく機能させることができます。
- CP_RTU_ADV：カウントを 1 にして、Cisco Crosswork Planning Collector と Design の両方のアプリケーションを正しく機能させることができます。

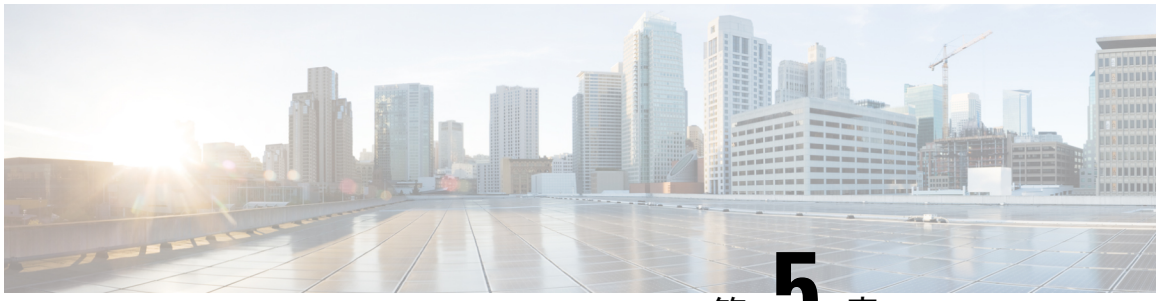
ステップ 4 [保存（Save）] をクリックします。

ライセンス認証ステータス

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 *10 :* 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。



第 5 章

管理タスクの管理

この章は次のトピックで構成されています。

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

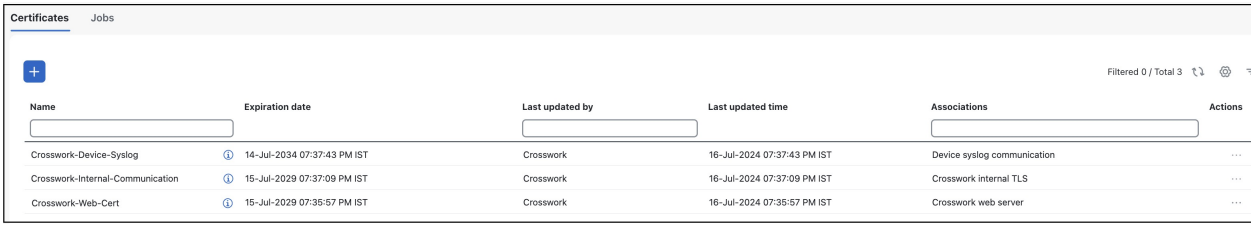
明書の秘密キーから開始し、信頼チェーン内の各証明書の秘密キーは、最終エンティティ証明書に最終的に署名するまで、チェーン内の次の証明書に署名して発行します。エンドエンティティ証明書は、チェーン内の最後の証明書であり、クライアント証明書またはサーバー証明書として使用されます。

Cisco Crosswork Planningでの証明書の使用方法

Cisco Crosswork とデバイス間の通信やさまざまなCisco 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。

証明書管理ウィンドウ（**[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 Planning が提供するデフォルトの証明書を示します。

図 *28 :* 証明書管理ウィンドウ



証明書のタイプと使用方法

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 内部 TLS	Crosswork-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。 • 相互認証とサーバー認証を許可します。	Crosswork	Crosswork	ダウンロード	5 年	—
Crosswork Web サーバー	Crosswork Web証明書（Crosswork-Web-Cert） 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。	Crosswork 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
Crosswork デバイス Syslog	Crosswork-Device-Syslog	• Crosswork によって生成および提供されます。 • サーバー認証を許可します。		Device	ダウンロード	5 年	—

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。

- [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 （133 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。

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 （116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。

手順

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。

（注）
Cisco Crosswork Planning 7.0 には、[セキュアLDAP通信（Secure LDAP communication）] オプションのみを適用できます。

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 [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。

手順

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）
Crosswork 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

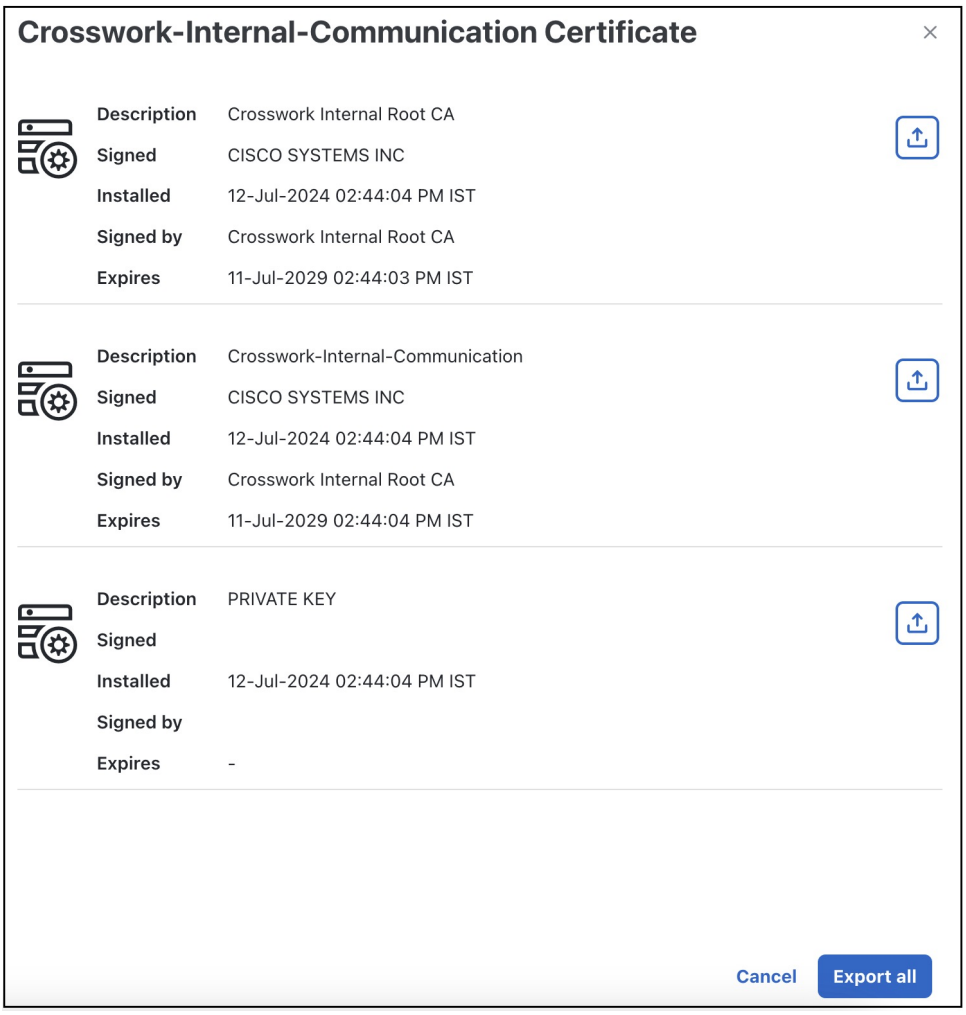
証明書をエクスポートするには、次の手順を実行します。

手順

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 *29 :* 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。

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 Planning 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 （124 ページ）」を参照）。

手順

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。詳細については、監査ログの表示 （149 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、Cisco Crosswork Planning 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、API の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データのみを表示する必要があるユーザーのロールには、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 *11* : 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	アクティブなネットワーク管理者	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	Cisco Crosswork Planning Design および Collector	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。

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 （121 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、RADIUS および LDAP 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。

手順

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 [グローバルAPI権限（Global API Permissions）] 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化が表示されます。

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 ユーザロールの権限設定を定義するには、[グローバルAPI権限（Global API Permissions）] タブを選択し、次の手順を実行します。

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 （125 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 （121 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 （125 ページ）」を参照）。

ユーザーロールを複製するには、次の手順を実行します。

手順

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。

ユーザーロールを編集するには、次の手順を実行します。

手順

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 左側の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 [グローバルAPI権限（Global API Permissions）] タブに、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。

ユーザーロールを削除するには、次の手順を実行します。

手順

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。

グローバル API 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。

次の表は、Cisco Crosswork Planning のさまざまな**グローバル API 権限**の概要です。

表 *12* : グローバル *API* 権限のカテゴリ

カテゴリ	グローバル API 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	Cisco Crosswork Planning 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 Cisco Crosswork Planning 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）」、「パスワードポリシーの更新」、「パスワードのツールチップヘルプテキストの取得」、「アクティブなセッションの取得」などが含まれます。 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。
管理操作（Administrative Operations）	診断情報 API	
アラームおよびイベント	アラームおよびイベント API	システムアラームを管理できます。 （注） Cisco Crosswork Planning アプリケーションに関連付けられているアラームとイベントは、Cisco Crosswork Planning 7.0 ではサポートされていません。
Crosswork Planning		

カテゴリ	グローバル API 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、Cisco Crosswork Planning 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 • ノード情報の管理（ログインバナーの設定、マイクロサービスの再起動など） • 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。
	API を見る	Cisco Crosswork Planning Design でのビューの管理。 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。

アクティブセッションの管理

管理者は、Cisco Crosswork Planning 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

注目

- 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。

手順

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）]** タブを選択します。

[アクティブセッション（Active sessions）] タブには、Cisco Crosswork Planning 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。

（注）
[送信元IP（Source IP）] 列は、[監査のために送信元IPを有効にします（Enable source IP for auditing）] チェックボックスをオンにして、Cisco Crosswork Planning に再ログインした場合にのみ表示されます。このオプションは、**[管理（Administration）] > [AAA] > [設定（Settings）]** ページの [送信元IP（Source IP）] セクションにあります。

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、[終了（Terminate）] 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。

注目
- 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。
- セッションが終了したユーザーには、次のエラーメッセージが表示されます。「セッションが終了しました。もう一度ログインし直してください（`Your session has ended. Log into the system again to continue`）」。

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、「監査ログの表示 （149 ページ）」を参照してください。

ユーザー認証の設定（TACACS+、LDAP および RADIUS）

Cisco Crosswork Planning は、ローカルユーザーのサポートに加えて、TACACS+、LDAP、および RADIUS サーバーとの統合により、TACACS+、LDAP、および RADIUS 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+、LDAP、および RADIUS サーバーを設定します。
- TACACS+、LDAP、および RADIUS 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。
- TACACS+、LDAP、および RADIUS ユーザーの認証にシングルサインオン（SSO）を有効にすることもできます。詳細については、シングルサインオン（SSO）の有効化（138 ページ）を参照してください。

（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（124 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。

注意 この項の手順に従って操作を行うと、Cisco Crosswork Planning 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、すべての外部サーバーの認証の変更を 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。

TACACS+ サーバーの管理

Cisco Crosswork Planning 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。

Crosswork をスタンドアロンサーバー（(open TACACS+）、または 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。

始める前に

- Cisco Crosswork Planning で AAA サーバーを設定する前に、TACACS+ サーバー（スタンドアロンまたはCisco ISE）で関連パラメータ（ユーザーロール、デバイスアクセスグループ属性、共有秘密形式、共有秘密値）を設定します。Cisco ISE での手順の詳細については、最新バージョンの『Cisco Identity Services Engine Administrator Guide』を参照してください。

手順

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、新しい TACACS+ サーバーの追加、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。

表 *13 : TACACS+* フィールドの説明

フィールド	説明
[認証順序（Authentication order）]	一意の優先順位値を指定して認証要求に優先順位を割り当てます。順序は 10 ～ 99 の間の任意の数値です。10 未満はシステムで予約済みです。 デフォルトでは 10 が選択されます。
IP アドレス	TACACS+ サーバーの IP アドレスを入力します（IP アドレスが選択されている場合）。
DNS 名	DNS 名を入力します（DNS 名を選択した場合）。IPv4 DNS 名のみがサポートされています。
Port	デフォルトの TACACS+ ポート番号は 49 です。
[共有秘密形式（Shared secret format）]	アクティブな TACACS+ サーバーの共有秘密。ASCII または 16 進数を選択します。
[共有秘密（Shared secret）]/[共有秘密の確認（Confirm shared secret）]	アクティブな TACACS+ サーバーのプレーンテキストの共有秘密。入力したテキストの形式は、選択した形式（ASCII または 16 進数）と一致する必要があります。 Crosswork が外部認証サーバーと通信するには、この画面で入力する [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。

フィールド	説明
サービス	アクセスしようとしているサービスの値を入力します。たとえば、「raccess」です。 このフィールドは、スタンドアロンTACACS+の場合にのみ検証されます。Cisco ISE の場合は、ジャンク値を入力できます。フィールドを空白のままにしないでください。
ポリシー ID	TACACS+ サーバーで作成したユーザーロールを入力します。 （注） 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 Planning 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 Cisco Crosswork Planning にログインし直します。
[再送信タイムアウト（Retransmit timeout）]	タイムアウトの値を入力します。最大タイムアウトは 30 秒です。
Retries	許可される認証の再試行回数を指定します。
認証タイプ	TACACS+ の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。

詳細については、このトピックの最後にある例を参照してください。

c) 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。
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、確定します。

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。Cisco Crosswork Planning は、ユーザーを認証するための LDAP サーバー（OpenLDAP、Active Directory、およびセキュア LDAP）の使用をサポートします。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（118 ページ） を参照してください。

始める前に

- Cisco Crosswork Planning で AAA サーバーを設定する前に、LDAP サーバーで関連パラメータ（バインド DN、ポリシーベース DN、ポリシー ID など）を設定します。

手順

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、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。

表 *14 : LDAP* フィールドの説明

フィールド	説明
[認証順序（Authentication order）]	一意の優先順位値を指定して認証要求に優先順位を割り当てます。順序は 10 ～ 99 の間の任意の数値です。10 未満はシステムで予約済みです。 デフォルトでは 10 が選択されます。
名前	LDAP ハンドラの名前。

フィールド	説明
[IPアドレス/ホスト名（IP address/ Host name）]	LDAP サーバーの IP アドレスまたはホスト名
セキュア接続	SSL 通信を介して LDAP サーバーに接続する場合は、[セキュア接続（Secure Connection）] トグルボタンをオンにします。オンにする場合は、[証明書（Certificate）] ドロップダウンリストからセキュア LDAP 証明書を選択します。 （注） セキュア LDAP サーバーを設定する前に、[証明書の管理（Certificate Management）] 画面にセキュア LDAP 証明書を追加する必要があります。 このフィールドは、デフォルトでは無効です。
ポート	デフォルトの LDAP ポート番号は 389 です。セキュア接続 SSL が有効になっている場合は、デフォルトの LDAP ポート番号は 636 です。
バインド DN（Bind DN）	データベースへのログインアクセスの詳細を入力します。バインド DN により、ユーザーは LDAP サーバーにログインできます。
[バインドログイン情報（Bind credential）]/[バインドログイン情報の確認（Confirm bind credential）]	LDAP サーバーにログインするためのユーザー名とパスワード。
ベース DN（Base DN）	ベース DN は、LDAP サーバーがディレクトリ内のユーザー認証を検索するために使用する開始点です。
[ユーザーフィルタ（User filter）]	ユーザー検索のフィルタ。
[DNの形式（DN Format）]	ベース DN でユーザーを識別するために使用される形式。
[プリンシパル l ID（Principal l ID）]	この値は、特定のユーザー名が編成されている LDAP サーバー ユーザー プロファイル内の UID 属性を表します。
[ポリシーベースDN（Policy BaseDN）]	この値は、ディレクトリ内のユーザーロールのロールマッピングを表します。
[ポリシーマップ属性（Policy map attribute）]	これは、ポリシーベース DN でユーザーを識別するのに役立ちます。 この値は、LDAP サーバー属性の `userFilter` パラメータにマッピングされます。

フィールド	説明
ポリシー ID	[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。 （注） 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 Planning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、Cisco Crosswork Planning 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。
接続タイムアウト	タイムアウトの値を入力します。最大タイムアウトは 30 秒です。

詳細については、このトピックの最後にある例を参照してください。

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 サーバーを選択して、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 サーバーを選択して、をクリックします。
b) [削除（Delete）] をクリックして確認します。

RADIUS サーバーの管理

Crosswork は、RADIUS（Remote Authentication Dial-In User Service）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。Crosswork を Cisco ISE（Identity Service Engine）などのアプリケーションと統合して、RADIUS プロトコルを使用して認証することもできます。

始める前に

- TACACS+ サーバーと同様に、Cisco Crosswork Planning で AAA サーバーを設定する前に、RADIUS サーバーで関連パラメータ（ユーザーロール、デバイスアクセスグループ属性、共有秘密形式、共有秘密値）を設定する必要があります。Cisco ISE での手順の詳細については、最新バージョンの『Cisco Identity Services Engine Administrator Guide』を参照してください。

手順

ステップ 1 メインメニューから、[管理（Administration）] > [AAA] > [サーバー（Servers）] > [RADIUS] タブを選択します。このウィンドウからは、新しい RADIUS サーバーの追加、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 RADIUS サーバーを追加するには：**

a) ＋アイコンをクリックします。

b) 必要な RADIUS サーバー情報を入力します。

表 *15 : RADIUS* フィールドの説明

フィールド	説明
[認証順序（Authentication order）]	一意の優先順位値を指定して認証要求に優先順位を割り当てます。順序は 10 ～ 99 の間の任意の数値です。10 未満はシステムで予約済みです。 デフォルトでは 10 が選択されます。
IP アドレス	TACACS+ サーバーの IP アドレスを入力します（IP アドレスが選択されている場合）。
DNS 名	IPv4 DNS名のみがサポートされています（DNS名が選択されている場合）。
ポート	デフォルトの RADIUS ポート番号は 1645 です。
[共有秘密形式（Shared secret format）]	アクティブな RADIUS サーバーの共有秘密。ASCII または 16 進数を選択します。
[共有秘密（Shared secret）]/[共有秘密の確認（Confirm shared secret）]	アクティブな RADIUS サーバーのプレーンテキストの共有秘密。入力したテキストの形式は、選択した形式（ASCII または 16 進数）と一致する必要があります。 Cisco Crosswork Planning が外部認証サーバーと通信するには、この画面で入力する [共有秘密（Shared Secret）] パラメータが、RADIUS 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。
サービス	アクセスしようとしているサービスの値を入力します。たとえば、「raccess」です。

フィールド	説明
ポリシー ID	[ポリシーID（Policy Id）] フィールドは、 RADIUS サーバーで作成したユーザーロールに対応します。 （注） 必要なユーザーロールを作成する前に RADIUS ユーザーとして Cisco Crosswork Planning 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、RADIUS サーバーで不足しているユーザーロールを作成し、RADIUS ユーザーログイン情報を使用して Cisco Crosswork Planning にログインし直します。
[再送信タイムアウト（Retransmit timeout）]	タイムアウトの値を入力します。最大タイムアウトは 30 秒です。
Retries	許可される認証の再試行回数を指定します。
認証タイプ	RADIUS の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。

RADIUS の設定は TACACS+ と非常によく似ているため、詳細については、 TACACS+ サーバーの管理 （130 ページ）の詳細な例を参照してください。

c) 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。
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、確定します。

ステップ 3　RADIUS サーバーを編集するには：

a) RADIUS 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　RADIUS サーバーを削除するには：

a) RADIUS 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。

シングルサインオン（SSO）の有効化

シングルサインオン（SSO）は、単一の ID とパスワードを使用して、関連するが独立したソフトウェアシステムのいずれかにログインできる認証方法です。これにより、一度ログインすると、認証要素を再入力することなくサービスにアクセスできます。Cisco Crosswork はアイデンティティ プロバイダー（IDP）として機能し、信頼するサービスプロバイダーに認証サポートを提供します。TACACS+、LDAP、および RADIUS ユーザーの認証に SSO を有効にすることもできます。

注目

- Cisco Crosswork Planning を再インストールするときは、Cisco Crosswork Planning からの最新の IDP メタデータが、サービス プロバイダー アプリケーションに対して更新されていることを確認する必要があります。これを行わないと、メタデータ情報が一致しないため、認証が失敗します。
- 初めてログインするユーザーは、パスワードを強制的に変更する前に別のユーザー名の使用に切り替えることはできません。唯一の回避策は、管理者がセッションを終了することです。

（注） Central Authentication Service（CAS）ポッドが再起動中または実行されていない場合、Cisco Crosswork Planning ログインページは表示されません。

始める前に

[管理（Administration）] > [AAA] > [設定（Settings）] ページで [監査のために送信元IPを有効にします（Enable source IP for auditing）] チェックボックスがオンになっていることを確認します。

手順

ステップ 1 メインメニューから、**[管理（Administration）] > [AAA] > [SSO]** の順に選択します。このウィンドウを使用して、サービスプロバイダーの追加、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 **新しいサービスプロバイダーを追加するには**、次のことを行います。

a) ＋アイコンをクリックします。

b) [アイデンティティ プロバイダー（Identity Provider）] ウィンドウで、次のフィールドに値を入力します。

- [名前（Name）]：サービスプロバイダーの名前を入力します。

- [評価順序（Evaluation Order）]：サービス定義が考慮される順序を示す一意の番号を入力します。
- [メタデータ（Metadata）]：フィールドをクリックするか、[参照（Browse）] をクリックして、SAML クライアントの展開を説明するメタデータ XML ドキュメントに移動します。

ステップ 3 [追加（Add）] をクリックして、サービスプロバイダーの追加を終了します。

ステップ 4 [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、確定します。

設定を保存した後、統合サービス プロバイダー アプリケーションに初めてログインすると、アプリケーションは Cisco Crosswork サーバーにリダイレクトされます。Crosswork 認証情報を提供すると、サービスプロバイダー アプリケーションは自動的にログインします。以降のすべてのアプリケーションログインでは、認証の詳細を入力する必要はありません。

ステップ 5 **サービスプロバイダーを編集するには**、次のことを行います。

a) サービスプロバイダ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。必要に応じて、[評価順序（Evaluation Order）] と [メタデータ（Metadata）] の値を更新できます。

b) 変更を加えた後、[更新（Update）] をクリックします。

ステップ 6 **サービスプロバイダーを削除するには**、次のことを行います。

a) サービスプロバイダ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。

手順

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、Cisco Crosswork Planning 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ー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 [並列セッションの数（Number of parallel sessions）] フィールドと [ユーザー1人当たりの並列セッションの数（Number of Parallel sessions per user）] フィールドに関連する値を入力します。

（注）
Cisco Crosswork Planning は、次の数の並列セッションをサポートします。

- 同時ユーザーに対して 5 ～ 400 の並列セッション。並列セッション数を超えると、Cisco Crosswork Planning へのログイン時にエラーが表示されます。
- ユーザー 1 人当たりの同時セッションに対して、1 ～ 400 の並列セッション。

ステップ 5 監査とアカウンティングのためにユーザーの IP アドレス（送信元 IP）をログに記録するには、[監査のために送信元IPを有効にします（Enable source IP for auditing）] チェックボックスをオンにします。デフォルトでは、このチェックボックスは無効になっています。このオプションを有効にしてCisco Crosswork Planningに再ログインすると、[監査ログ（Audit Log）] ページと [アクティブセッション（Active Sessions）] ページに [送信元IP（Source IP）] 列が表示されます。

ステップ 6 [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 Planning 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。

システムとアプリケーションの正常性のモニター

Cisco 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 [管理（Administration）] > [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、このウィンドウでは、Cisco Crosswork、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

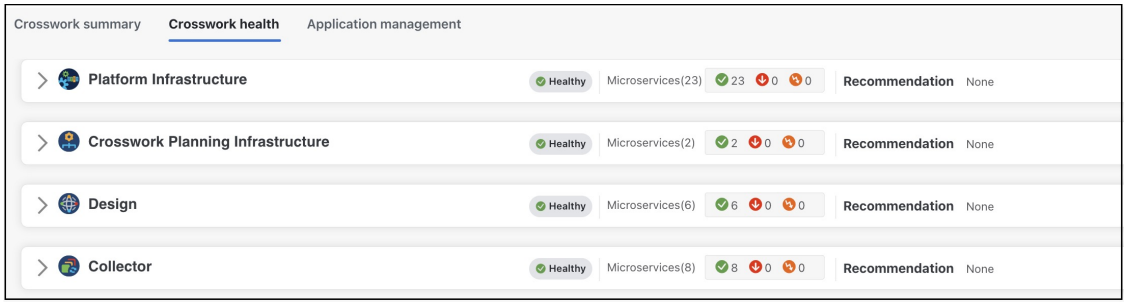
特定、診断、および修正するために使用できるツールと情報が、シスコ カスタマー エクスペリエンス アカウント チームからのサポートとガイダンスとともに提供されます。

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。

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

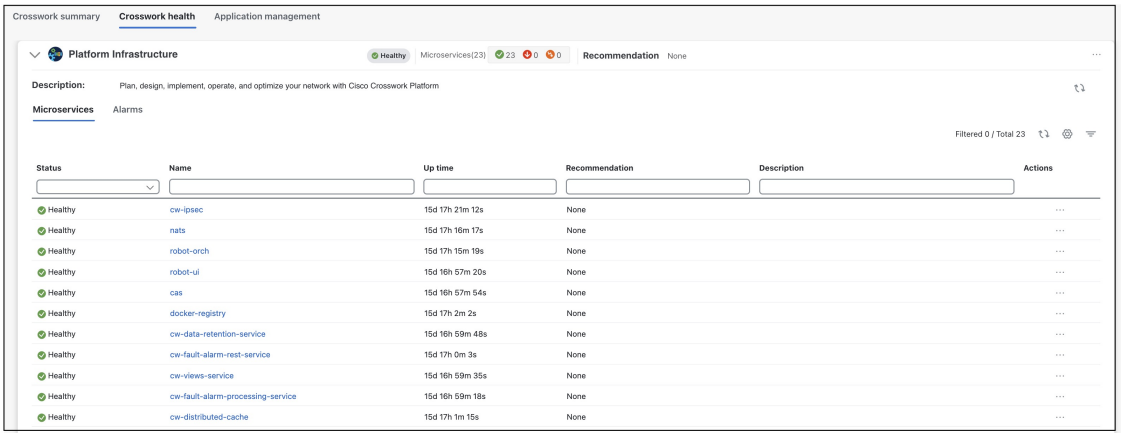
[Crossworkの正常性（Crosswork Health）] ウィンドウ（**[管理（Administration）]** > **[Crosswork Manager]** > **[Crossworkの正常性（Crosswork Health）]** タブ）には、Cisco Crosswork プラットフォーム インフラストラクチャとインストールされているアプリケーションの正常性の概要と、マイクロサービスステータスの詳細が表示されます。

図 *30 : [Crossworkの正常性（Crosswork Health）] タブ*



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。

図 *31 : [マイクロサービス（Microservices）] タブ*



[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、次の操作を実行できます。

- 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。
- アラームのステータスを変更します（確認、未確認、クリア）。アラームを選択し、[ステータスの変更（Change status）] ドロップダウンから必要なステータスを選択します。
- アラームへメモを追加します。アラームを選択し、[メモ（Notes）]ボタンをクリックします。

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。上部にある ••• > [アプリケーションの詳細の表示（View application details）] 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。

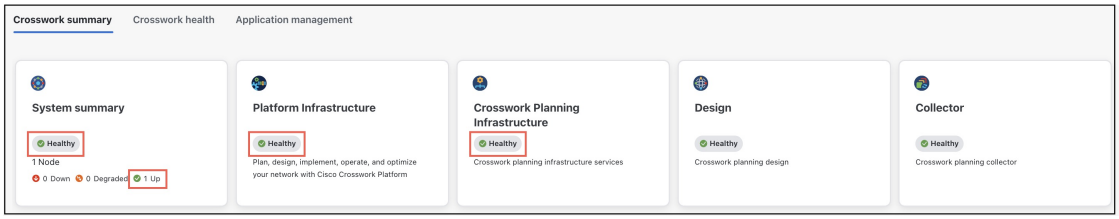
手順

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、[システム概要（System Summary）]、[プラットフォーム インフラストラクチャ（Platform Infrastructure）]、および [Crosswork Planningインフラストラクチャ（Crosswork Planning Infrastructure）] が正常であることを確認します。

図 *32 : [Crosswork* の概要（*Crosswork Summary*）*]*

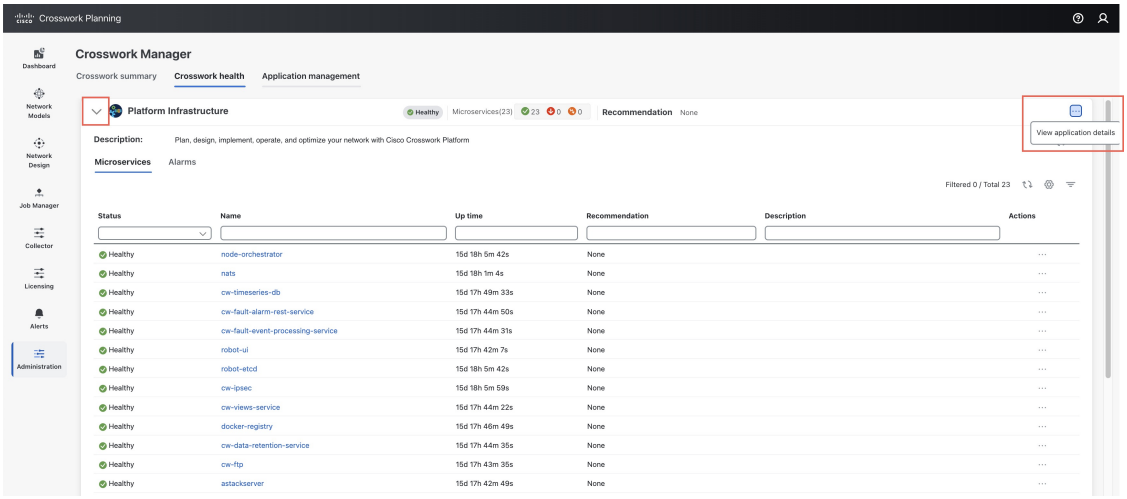


ステップ 2 Crosswork プラットフォーム インフラストラクチャの一部として実行されているマイクロサービスに関する詳細情報を確認および表示します。

a) [Crosswork の正常性（Crosswork Health）] タブをクリックします。

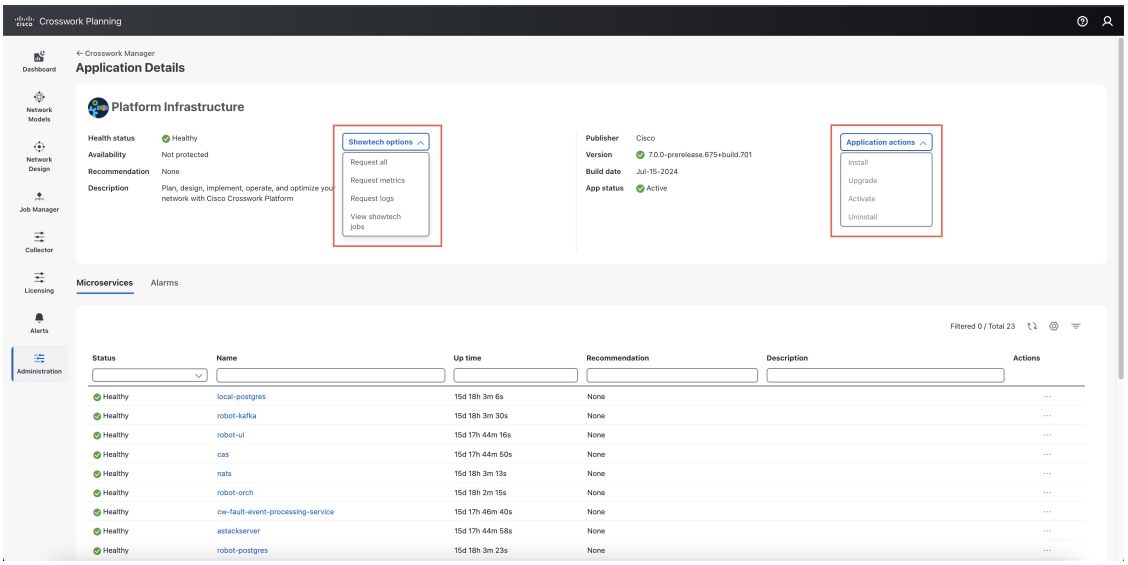
b) [Crossworkプラットフォームインフラストラクチャ（Crosswork Platform Infrastructure）] の行を展開し、 をクリックして [アプリケーション詳細を表示（View application details）] を選択します。

図 *33 : [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。

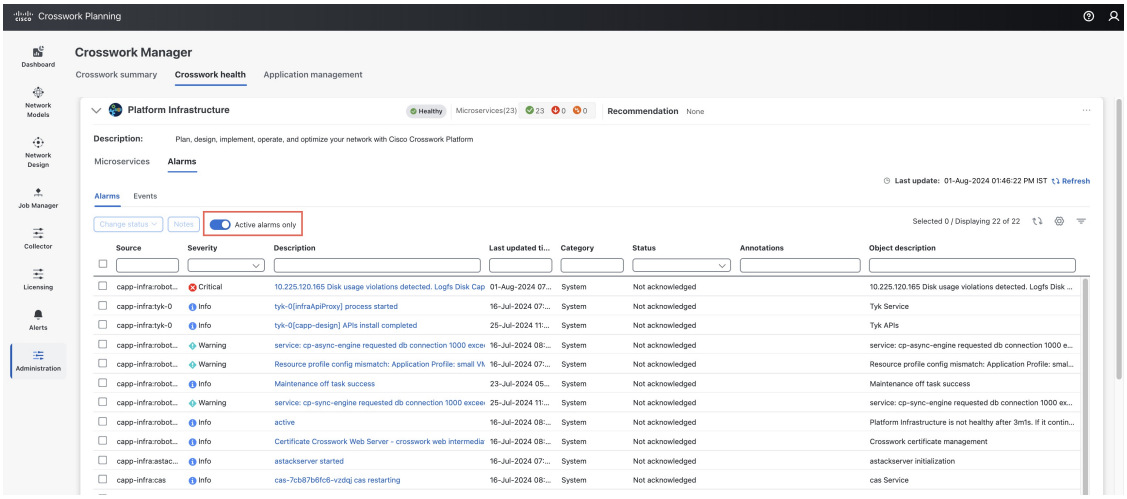
図 *34 :* アプリケーションの詳細（*Application Details*）



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。

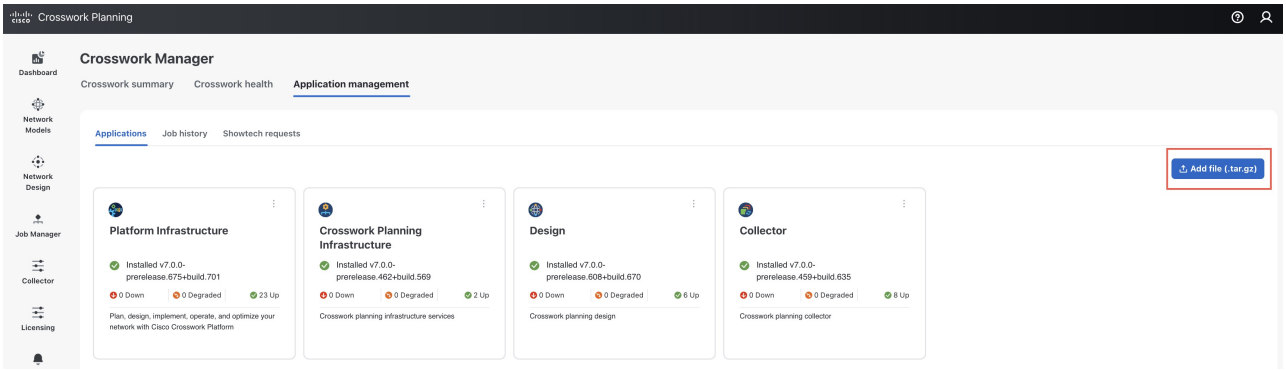
図 *35 : アラーム*



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。

図 *36 : [アプリケーション管理（Application Management）] ウィンドウ*



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。

バックアップの管理

Backup and Restore の概要

Cisco Crosswork Planning 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 Planning 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 *16 : 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）]>[データのバックアップ（Data backup）] （詳細については、Cisco Crosswork Planning バックアップと復元の管理 （146 ページ） を参照）	Cisco Crosswork Planning 構成データを保持します。バックアップファイルは、データの災害復旧（災害後の Cisco Crosswork Planning の復元（148 ページ）） で使用して、重大な機能停止から回復することができます。
[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、災害後の Cisco Crosswork Planning の復元（148 ページ） を参照）	自然災害または人為的災害により Cisco Crosswork Planning サーバーの再構築が必要になった後に、Cisco Crosswork Planning 構成データを復元します。
[アクション（Actions）] > [データ移行（Data migration）] （注） このオプションは、Cisco Crosswork Planning 7.0 ではサポートされていません。	

Cisco Crosswork Planning バックアップと復元の管理

このセクションでは、Cisco Crosswork Planning UI からデータ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。
- バックアッププロセスには、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、Cisco Crosswork Planning サーバー内のアプリケーション、およびスケールの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、および Cisco Crosswork Planning サーバー内のアプリケーションによって異なります。

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。
- 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メモしている。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。

手順

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、[接続先の追加（Add 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) **[アクション（Actions）]** > **[データのバックアップ（Data 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 [データのバックアップ（Data Backup）] ダイアログボックスを表示します。

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) マイクロサービスの問題があってもバックアップを作成する場合は、[強制（Force）] チェックボックスをオンにします。

e) 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。

f) （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 Planning 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 Planning に表示されます。[OK] をクリックして、先へ進みます。

g) [バックアップ（Backup）] をクリックして、バックアップ操作を開始します。Cisco Crosswork Planning 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。

h) バックアップジョブの進行状況を表示するには、[バックアップおよび復元ジョブセット（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。

[ジョブの詳細（Job Details）] パネルに、選択したジョブセットに関する情報（ジョブステータス、ジョブ名、ジョブタイプなど）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。

（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）。

災害後の Cisco Crosswork Planning の復元

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 Planning サーバーが破壊された後に使用する復元操作です。*Cisco Crosswork Planning 7.0* インストールガイドの手順に従って、最初に新しいサーバーを展開する必要があります。

データの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。

- [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 Cisco Crosswork Planning サーバー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 Cisco Crosswork Planning サーバー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。
- 新しい Cisco Crosswork Planning サーバーは、バックアップの作成時に使用したものと同じ Cisco Crosswork Planning 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サーバーを復元することはできません。
- 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 Planning 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 Planning プラットフォームのバージョンです。
- *TimeStamp* は、Cisco Crosswork Planning 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`

手順

ステップ 1 新たに展開したCisco Crosswork Planningサーバー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 **[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 3 [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 4 [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。

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。

- メインメニューから **[アラート（Alerts）]** > **[アラームとイベント（Alarms and Events）]** 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）] タブから、次の操作を実行できます。

  - 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。
  - アラームのステータスを変更します（確認、未確認、クリア）。アラームを選択し、[ステータスの変更（Change status）] ドロップダウンから必要なステータスを選択します。
  - アラームへメモを追加します。アラームを選択し、[メモ（Notes）]ボタンをクリックします。

監査ログの表示

[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。
- [送信元IP（Source IP）]：アクションが実行されたマシンのIPアドレス。この列は、[監査のために送信元IPを有効にします（Enable source IP for auditing）]チェックボックスをオンにして、Cisco Crosswork Planningに再ログインした場合にのみ表示されます。このチェックボックスは、**[管理（Administration）]** > **[AAA]** > **[設定（Settings）]** ページの [送信元IP（Source IP）] セクションにあります。
- 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。

手順

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。

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。Cisco Crosswork Planning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。

手順

ステップ1 メインメニューから、**[管理（Administration）]** > **[設定（Settings]** の順に選択します。

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（Enable）] 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）ユーザーがログインする前に免責事項に同意するようにユーザーに求めるには、[ユーザーの同意が必要（Require user consent）] の下の [有効（Enable）] チェックボックスをオンにします。
d) （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、行った変更が Cisco Crosswork Planning ログインプロンプトの前にどのように表示されるのかを確認できます。

[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。

[デフォルトにリセット（Reset to default）] 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。

e) 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）] > [ログイン前の免責事項（Pre-Login Disclaimer）]** を選択し、[有効（Enable）] チェックボックスをオフにします。

メンテナンスモード設定の管理

メンテナンスモードでは、Cisco Crosswork Planning システムを一時的にシャットダウンする手段が提供されます。Cisco Crosswork Planning 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るまでに数分かかる場合があります。メンテナンスモードをオフにすると、再起動します。その間は、ログインしたり、Cisco Crosswork Planning アプリケーションを使用したりできません。

⚠

注意

- メンテナンスモードを有効にする前に、Cisco Crosswork Planning システムのバックアップを作成してください。
- 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。

手順

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) [メンテナンスのオン/オフ（Turn on/off maintenance）] スライダを右、すなわちオンの位置にドラッグします。

c) システムがメンテナンスモードに移行しようとしていることを示す警告メッセージが表示されます。[続行（Continue）] をクリックして選択内容を確認します。

（注）
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) [メンテナンスのオン/オフ（Turn on/off maintenance）] スライダを左、すなわちオフの位置にドラッグします。

（注）
システムをメンテナンスモードにした状態で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。

ネットワークアクセス設定の更新

[ネットワークアクセス設定（Network access configuration）] セクションでは、SNMP、ログイン、および SAM インターフェイスを介したネットワークアクセスに使用されるパラメータを指定します。これらのパラメータは、特定の要件に合うように変更できます。たとえば、必要に応じて SNMP タイムアウト値を更新できます。

⚠

注意 編集する前に、変更はグローバルに適用され、すべての収集、ジョブ、およびプランファイルに影響することに留意してください。

ネットワークアクセス設定を編集するには、次の手順を実行します。

手順

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）] > [収集の設定（Collection settings）] > [ネットワークアクセス設定（Network access configuration）]** を選択します。

ステップ 2 [Edit] ボタンをクリックします。必要なサービスを無効にするように設定を変更すると収集が失敗することを通知する、アラートウィンドウが表示されます。タイムアウトとその他のパラメータのみを変更する場合は、[確認（Confirm）] をクリックします。

ページが編集可能になります。

ステップ 3 要件に応じてファイルを編集します。

ステップ 4 [保存（Save）] をクリックして、変更内容を保存します。

ネットワークアクセス設定ファイルのダウンロード：

ネットワークアクセス設定ファイルをローカルマシンにダウンロードするには、  をクリックします。

コレクタ機能の更新

各コレクタのデータソースと、コレクタによってデータが入力されているテーブル/列は、[コレクタ機能（Collector capability）]ページに表示されます。Cisco Crosswork Planningでは、要件に応じてこれらの設定を更新できます。

注意 更新する前に、変更はグローバルに適用され、すべての収集、ジョブ、およびプランファイルに影響することに留意してください。

コレクタのテーブルと列の詳細は、次の形式を使用して設定されます。

Collector.table.table-name=ALL/Column list

ここで、ALLは、コレクタによってそのテーブルのすべての列にデータが入力されることを示します。コレクタによって列のサブセットのみが入力される場合は、カンマで区切られた列名のリストとして指定されます。

デフォルト設定を更新するには、次の手順を実行します。

手順

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）] > [収集の設定（Collection settings）] > [コレクタ機能（Collector capability）]** を選択します。

ステップ 2 [Edit] ボタンをクリックします。

ページが編集可能になります。

ステップ 3 要件に応じて .txt ファイルを編集します。

ステップ 4 [保存（Save）] をクリックして、変更内容を保存します。

コレクタ機能設定のダウンロード

コレクタ機能の設定をローカルマシンにダウンロードするには、  をクリックします。

デフォルト設定にリセット

設定をデフォルト値にリセットするには、右上の [デフォルト設定のリセット（Reset default config）] ボタンをクリックします。

エージングの構成

デフォルトでは、回路、ポート、ノード、またはリンクがネットワークから消失すると、永久に削除され、再検出する必要があります。消失したこれらの要素がネットワークから完全に削除されるまでCisco Crosswork Planningがこれらの要素を保持する期間を設定するには、次の手順を実行します。

⚠

注意 設定する前に、変更はグローバルに適用され、すべての収集、ジョブ、およびプランファイルに影響することに留意してください。

手順

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）] > [収集の設定（Collection Settings）] > [パージ遅延（Purge delay）]** を選択します。

ステップ 2 **[有効（Enable）]** チェックボックスをオンにして、エージングを有効にします。

ステップ 3 該当するフィールドに値を入力します。

- [L3ポート（L3 port）] : L3 ポートが非アクティブになった後に、ネットワーク内で保持する必要がある期間を入力します。
- [L3ノード（L3 node）] : L3 ノードが非アクティブになった後に、ネットワーク内で保持する必要がある期間を入力します。
- [L3回路（L3 circuit）] : L3 回路が非アクティブになった後に、ネットワーク内で保持する必要がある期間を入力します。

（注）
[L3ノード（L3 node）] の値は [L3ポート（L3 port）] の値以上である必要があります。すなわち、[L3ポート（L3 port）] の値は [L3回路（L3 circuit）] の値以上である必要があります。

アーカイブされたプランファイルの消去の設定

アーカイブされたプランファイルは、ストレージ容量を節約するためにCisco Crosswork Planningで定期的に削除されます。デフォルトでは、ファイルは 30 日間保持されます。

要件に応じて保持期間（日数）を設定するには、次の手順を実行します。

手順

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）]** > **[収集の設定（Collection settings）]** > **[アーカイブ消去（Archive purge）]** を選択します。

ステップ 2 [アーカイブ保持（Archive retention）] フィールドに、ファイルが削除されるまでの日数を入力します。

たとえば、このフィールドに 40 と入力すると、40 日よりも古いプランファイルが削除されます。

ステップ 3 [保存（Save）] をクリックして、変更内容を保存します。

（注） アーカイブされたプランファイルの消去を無効にするには、[有効（Enable）] チェックボックスをオフにします。無効にすると、最終的にストレージ容量を使い切ってしまうことに注意してください。

スタティックルートの設定

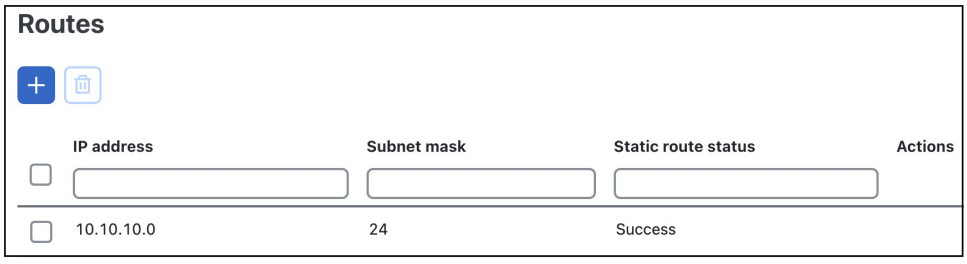
スタティックルートは、異なるサブセット内のデバイスに到達するために使用されます。

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。

手順

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）]** > **[デバイス接続管理（Device connectivity management）]** > **[ルート（Routes）]** を選択します。



ステップ 2 + をクリックします。[ルートIPの追加（Add Route IP）] ウィンドウが表示されます。

ステップ 3 有効な IPv4 または IPv6 サブネットを CIDR 形式で入力します。

ステップ 4 [追加（Add）] 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。

手順

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）] > [デバイス接続管理（Device connectivity management）] > [ルート（Routes）]** を選択します。

ステップ 2 削除するスタティックルートを選択し、  をクリックします。

ステップ 3 確認ウィンドウで、[削除（Delete）] をクリックします。

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。