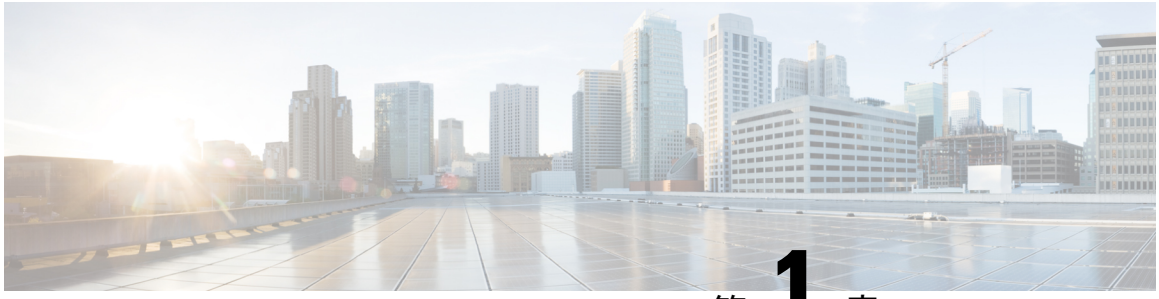
Cisco Crosswork Planning 7.1 コレクションの設定と管理

最終更新：2026 年 1 月 14 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

はじめに

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。

この章の内容は、次のとおりです。

Cisco Crosswork Planning の主な機能

Cisco Crosswork Planning は、ネットワークとそのトラフィック需要を継続的にモニターすることで、既存のネットワークのモデルを作成するツールを提供します。このネットワークモデルには、任意の時点で、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。

主な機能

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。

コンポーネント

Cisco Crosswork Planning は、2 つのプライマリコンポーネントで構成されます：

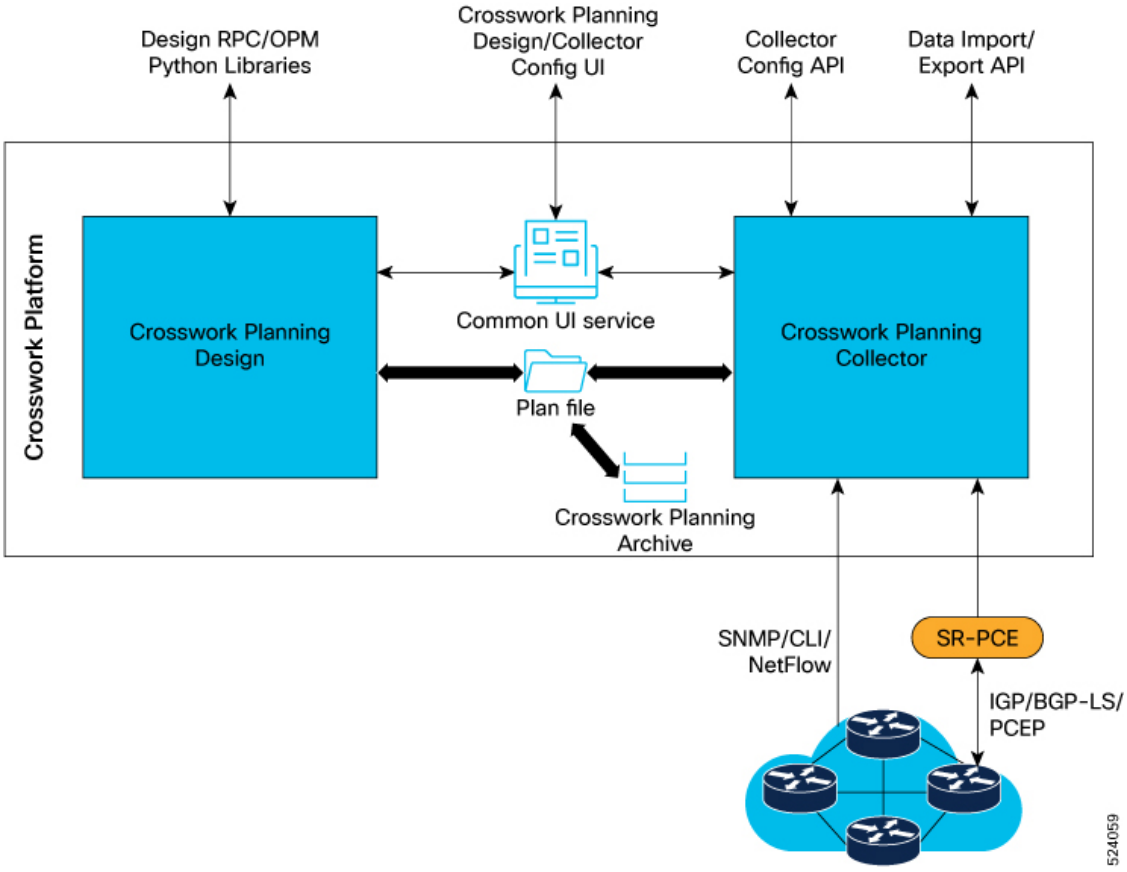
- Cisco Crosswork Planning Collector：このコンポーネントは、現在のネットワークのモデルを作成、維持、およびアーカイブするための一連のサービスを含みます。これは、ネットワークとそのネットワーク上のトラフィックの需要の継続的な監視と分析によって実現されます。
- Cisco Crosswork Planning Design：ネットワークエンジニアやオペレータがネットワークの成長を予測し、障害をシミュレートし、また、コストを最小限に抑えながらネットワーク設計を最適化して、パフォーマンス目標を達成するのに役立ちます。

Cisco Crosswork Planning system

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 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、ニーズに応じて有効/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



コレクタ

コレクタとは、ネットワークをクエリすることで、抽象ネットワークモデルの一部を生成するパッケージです。

通常、コレクタは次の方法で動作します。

1. 送信元モデルとも呼ばれる送信元ネットワークモデルを読み取ります。
2. これは、実際のネットワークから取得した情報で、この送信元を拡張します。
3. 結果のモデルを使用して接続先ネットワークモデルを生成します。これは、接続先モデルとも呼ばれます。

コレクタの種類

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： これらのコレクタは、基本的なネットワークモデルにノード、インターフェイス、回路などのトポロジ情報を入力します。これは、SNMP クエリと SR -PCE

が拡張した、検出されたIGPデータベースに基づいています。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拡張し、追加情報で接続先モデルを生成します。
- Traffic コレクタ：このコレクタは、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拡張し、追加情報で新しい接続先モデルを生成します。
- Layout コレクタ：このコレクタは、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。送信元モデルが変更されると、それに応じてコレクタは接続先モデルのレイアウトプロパティを更新します。

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 （61 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

ネットワークモデルは出力で、

- Cisco Crosswork Planning コレクタアプリケーションによって生成されます。
- さまざまなコレクタからの情報を組み合わせます。
- 実際のネットワークの構成とトポロジを反映します。

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。

システムは、結果のネットワークモデルをプランファイル形式（.pln）で保存します。これは、Cisco Crosswork Planning Design アプリケーションで表示またはダウンロードできます。

集約コンポーネント

集約エンジンは、さまざまなソースから収集されたネットワークデータを統合して、包括的なネットワークモデルを生成します。

ここでは、Cisco Crosswork Planning の Delta Aggregation Rules Engine（DARE）および Simple Aggregation Engine（SAgE）のロールと関数について説明します。

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。これは、主にすべてのトポロジコレクタのデータを統合します。

単純な集約エンジン（SAgE）

SAgE アグリゲータは、トラフィック、一覧、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。

SAgE アグリゲータを使用すると、トラフィックコレクション、一覧収集、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、コレクタ出力の集約（44 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。このファイルは、トラフィック、一覧、レイアウト、NetFlow、デマンドなどのコンポーネントに対しては、データソースとして機能します。SAgE 集約が完了すると、2 番目のファイルとネットワークモデルが生成されます。これは、収集された集約データの最終出力です。

Cisco Crosswork Planning にログインする

このトピックでは、Cisco Crosswork Planning をインストールした後に、UI にアクセスする方法について説明します。

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 7.2* インストールガイド の 「サポートされている *Web* ブラウザ」項を参照してください。

手順

ステップ 1 Web ブラウザを開いて、`https://<Crosswork Management Network Virtual IP (IPv4)>:30603/` と入力します。

ブラウザから Cisco Crosswork Planning に初回アクセスした場合は、サイトが信頼できないという警告が表示される場合があります。これが表示された場合は、プロンプトに従って、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 にログインします。

a) 管理者のユーザー名である **admin** とデフォルトパスワードの **admin** を入力します。
b) [ログイン（Login）] をクリックします。
c) 管理者のデフォルトのパスワードを変更するように求められたら、表示されたフィールドに新しいパスワードを入力し、[OK] をクリックします。

（注）
強力な VM パスワード（大文字と小文字、数字、特殊文字を含む 8 文字以上の長さ）を使用します。ディクショナリの単語や関連する単語に類似したパスワードの使用は避けてください（例：「Pa55w0rd!」）。

[Crosswork Manager] ページが表示されます。

ステップ 3 **[Crossworkの正常性（Crosswork Health）]** タブ、**[Crossworkプラットフォームインフラストラクチャ（Crosswork Platform Infrastructure）]** タブ の順に選択し、Cisco Crosswork Planning で実行されているマイクロサービスの正常性ステータスを表示します。

ステップ 4 （オプション）管理者アカウントに割り当てられた名前を、よりわかりやすい名前に変更します。

ステップ 5 手動インストールの場合：UI にログインした後、VM が正常であることを確認します。Cisco Crosswork Planning UI から一覧のサンプル（.tfvars ファイル）をダウンロードし、data center パラメータを使用して VM 関連情報と一緒に更新します。次に、そのファイルを Cisco Crosswork Planning UI にインポートします。詳細については、インベントリファイルのインポート を参照してください。

Cisco Crosswork Planning へのアクセス権があるため、必要に応じてタスクの計画または管理を開始できます。

次のタスク

ログアウトするには、メインページの右上隅で、[]、**[ログアウト（Logout）]** の順に選択します。

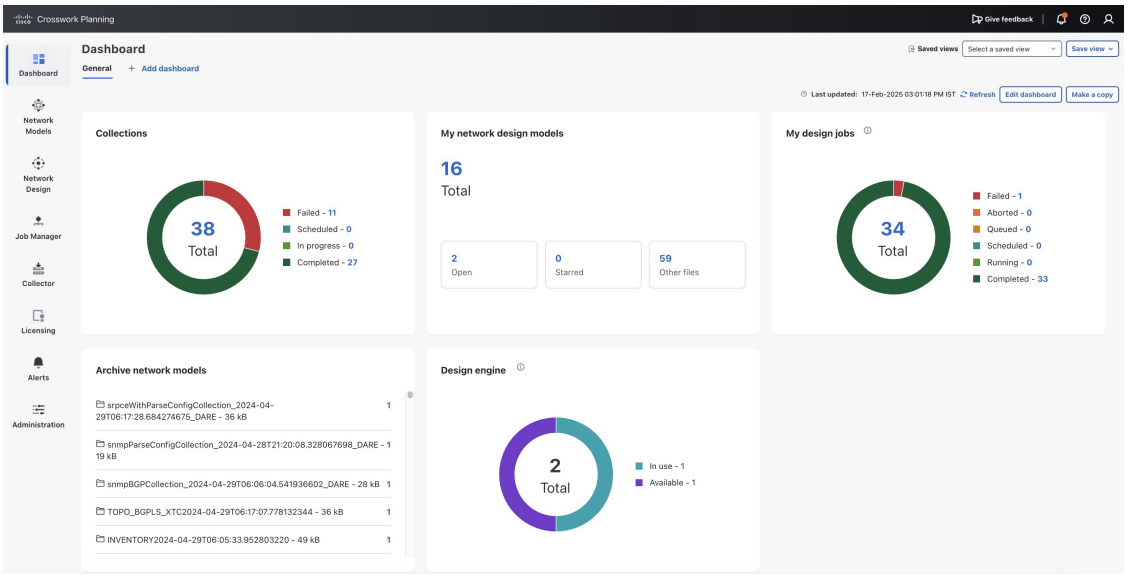
（注） プランファイルでの作業中にログアウトした場合、ファイルは閉じられず、開いたままになります。

ダッシュボード

[ダッシュボード（Dashboard）] ページでは、Cisco Crosswork Planning の動作サマリーを一目で確認できます。このページは、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るさまざまなダッシュレットで構成されます。

たとえば、Cisco Crosswork Planning Collector アプリケーションがインストールされている場合にのみ、**[コレクション（Collections）]** および **[アーカイブネットワークモデル（Archive network models）]** ダッシュレットが表示されます。同様に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。

図 *2:* ダッシュボードの画面

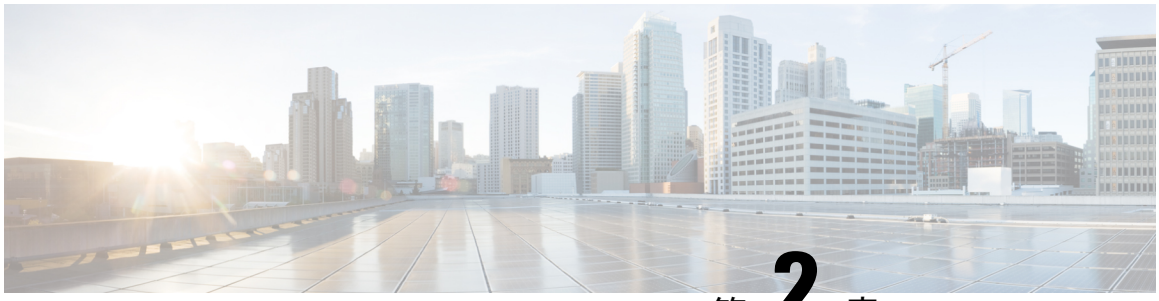


ダッシュレットのナビゲーション

各ダッシュレットのリンクを使用すると、目的のページに簡単に移動できます。

ダッシュレットのカスタマイズ

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 **[ダッシュボードの編集（Edit dashboard）]** ボタンを使用します。詳細については、「*Cisco Crosswork Planning Design 7.2* ユーザーガイド」の「」ダッシュレットをカスタマイズする」を参照してください。



第 2 章

ネットワークモデルの設定

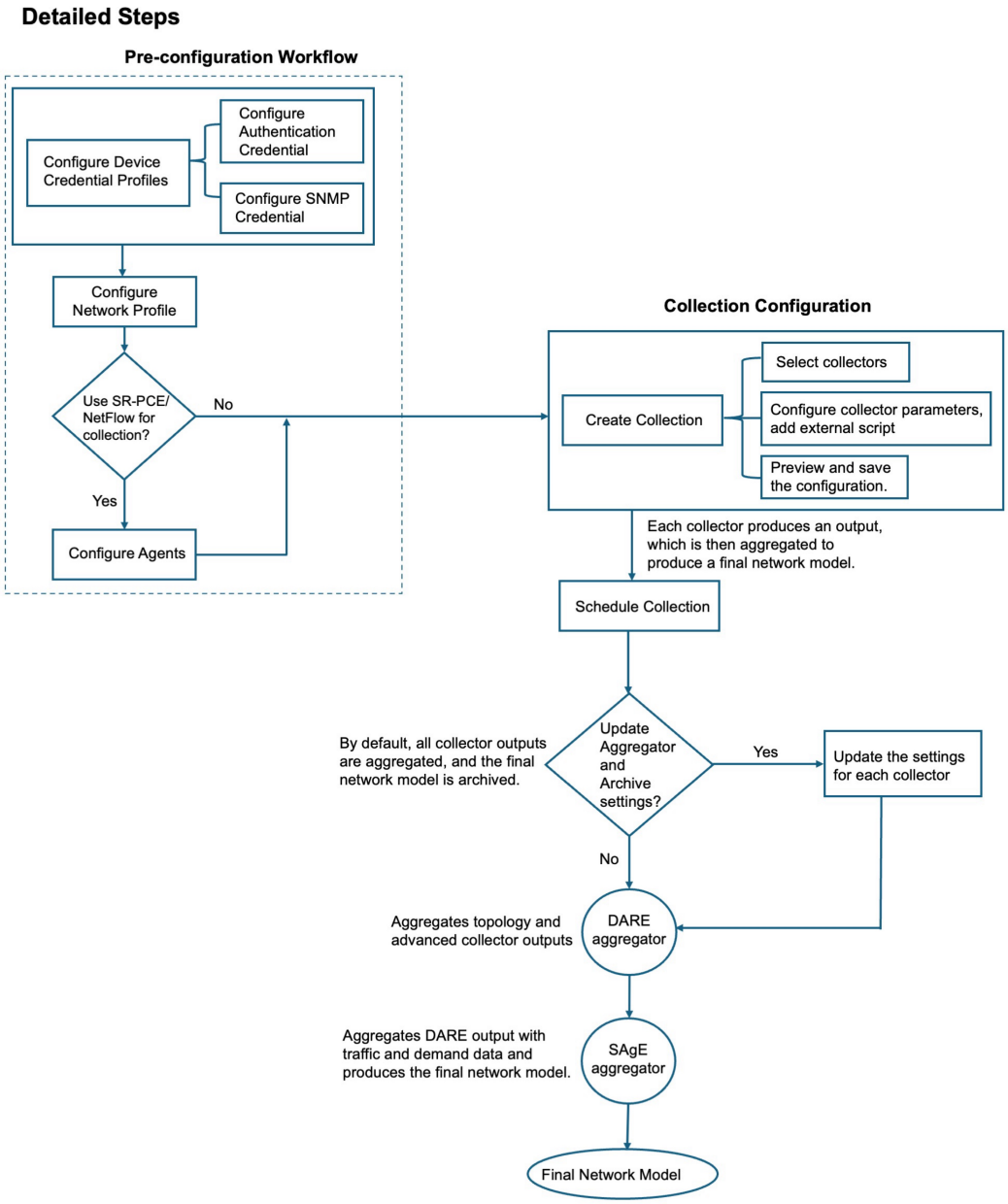
ネットワークモデル作成ワークフロー

process_summary

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 を使用して、デバイス、ネットワークアクセスを構成し、ネットワークモデルを作成し、ユーザーを管理し、エージェントを構成します。

process_workflow

図 *3 :* ネットワークモデル作成ワークフロー



これらが、ネットワークモデル作成の段階です。

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。詳細については、「事前構成ワークフロー （11 ページ）」を参照してください。
2. （オプション）SR-PCE または NetFlow 情報を収集する必要がある場合にのみエージェントを構成します。詳細については、「エージェントの構成 （22 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）。詳細については、「コレクションの設定（28 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。コレクションのスケジュール（36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。詳細については、「コレクタ出力の集約（44 ページ）」および「アーカイブの構成（47 ページ）」を参照してください。
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。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」を参照してください。

事前構成ワークフロー

process_summary

この事前構成ワークフローは、ネットワークモデル作成に必要な準備手順を概説します。これには、ログイン情報プロファイルの設定、デバイスへのアクセス、ネットワークアクセスの構成、必要に応じて、特定の情報を収集するためのエージェントの作成が含まれます。

process_workflow

これらが、事前構成ワークフローの手順です。

1. デバイスログイン情報プロファイル（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、「ログイン情報プロファイルの構成（11 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。詳細については、「ネットワークプロファイルの設定（16 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。詳細については、「エージェントの構成（22 ページ）」を参照してください。

ログイン情報プロファイルの構成

process_summary

ログイン情報プロファイルは、ネットワークデバイスにアクセスするために安全にデバイスログイン情報を格納して管理する方法です。

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ログイン情報をサポートし、複数のプロトコルとそれらに対応するログイン情報を 1 つのプロファイルにバンドルできます。同じクレデンシャルを使用するデバイスは、クレデ

ンシャルプロファイルを共有できます。たとえば、特定の建物内のすべてのルータが単一の SSH ユーザー ID とパスワードを共有する場合、Cisco Crosswork Planning がそれらにアクセスして管理できるように単一のログイン情報プロファイルを作成できます。

ログイン情報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必要なアクセスログイン情報とサポートされているプロトコルを収集します。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文字列、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。

process_workflow

これらは、ログイン情報プロファイルの構成の段階です。

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。詳細については、「認証ログイン情報の構成 （12 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。詳細については、「SNMP ログイン情報の設定 （13 ページ）」を参照してください。

認証ログイン情報の構成

この項では、SSH または Telnet を使用してデバイスにアクセスするための認証情報を構成する方法について説明します。

システムで初めてデバイスアクセスを設定する際、または将来のデバイス接続用に新しいログイン情報を追加する際は、認証情報を構成します。これらのログイン情報により、SSH（セキュリティ観点で推奨）または Telnet 経由でネットワークデバイスに安全に接続できます。

初期設定時に、**[コレクタ（Collector）]** > **[コレクション（Collections）]** の順に選択するか、任意の時点で **[ログイン情報（Credentials）]** ページで、認証情報を構成できます。

[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。

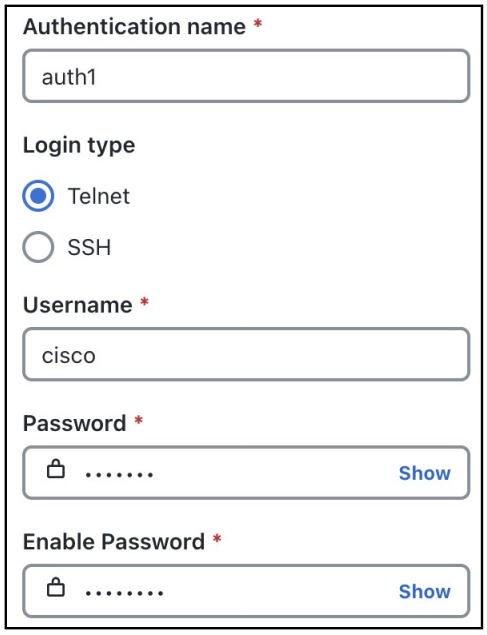
手順

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）]**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 *4* : 認証ログイン情報の構成



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。
- [ログインの種類（Login type）]：要件に応じて、**[SSH]** または **[Telnet]** のいずれかを選択します。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。**[パスワードを有効化（Enable password）]** には、Cisco IOS ルータの有効化モード（特権 EXEC モードとも呼ばれる）へのアクセスに必要なパスワードを指定します。このパスワードは、有効化モードへのアクセスを制御し、ルータでの不正な構成変更を防止します。デバイスが、有効化モードをサポートしていない場合は、**[パスワード（Password）]** フィールドと **[パスワードを有効化（Enable password）]** フィールドの両方で同じパスワードを使用します。

ステップ 4 変更内容を保存します。

システムは、新しい認証情報を保存し、構成に応じて、SSH または Telnet 経由のデバイスアクセスで使用できるようにします。

SNMP ログイン情報の設定

この項では、SNMP ログイン情報を設定してノードとシードルータ間でセキュア通信を有効にする方法について説明します。

SNMP ログイン情報は、ノードとシードルータ間で交換されたメッセージを認証して暗号化するために必要です。初期設定時に、**[コレクタ（Collector）]** > **[コレクション（Collections）]** の順に選択するか、任意の時点で**[ログイン情報（Credentials）]**ページで、SNMP ログイン情報を構成できます。

[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。

Before you begin

SNMPv2c または SNMPv3 のどちらが必要かを事前に決定し、必要な認証または暗号化詳細を収集します。

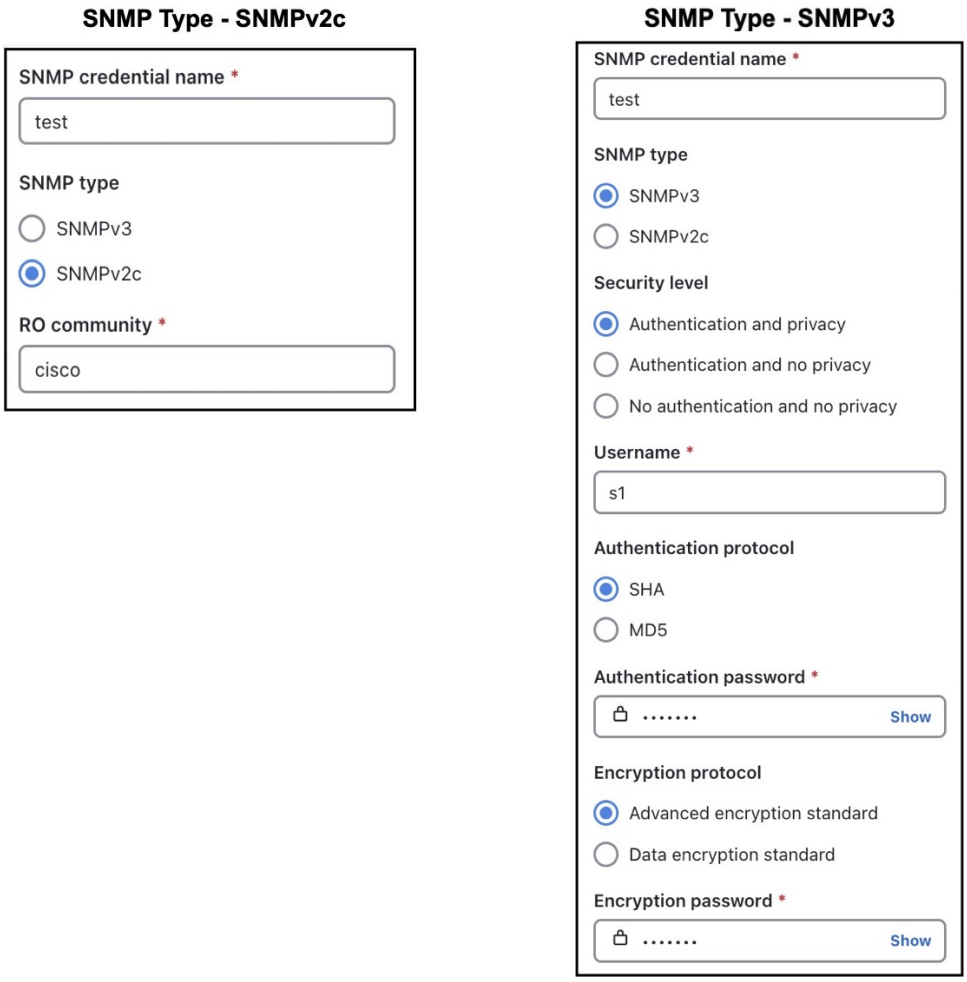
手順

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、**[+新規作成（+ Create New）]** の順に選択します。

（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 *5 : 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 の種類（SNMP type）]** セクションで、使用する SNMP プロトコルを選択します。オプションは、**[SNMPv3]** と **[SNMPv2c]** です。

- [SNMPv2c]：パスワードとして機能する SNMP RO コミュニティ文字列を入力します。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：テーブル 1：SNMPv3 フィールドで言及されているフィールドに値を入力します。

表 *1 : SNMPv3* フィールド

フィールド	アクション（**Action**）
セキュリティレベル	次のいずれかのオプションを選択します。 • [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	ユーザ名を入力します。
認証プロトコル	次のいずれかのオプションを選択します。 • [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	認証パスワードを入力します。
暗号化プロトコルと暗号化パスワード	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。

新しい SNMP ログイン情報は保存され、ノードとシードルータ間の安全なデバイス検出または通信に使用できます。

ネットワークプロファイルの設定

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。この項では、ネットワークからデータを収集するネットワークプロファイルを定義する方法について説明します。

[コレクション（Collections）] ページに初回アクセス時（**[コレクタ（Collector）]、** > **[コレクション（Collections]**の順に選択）、[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。この手順は、左側の [ステッパー（Stepper）] ペインに表示されます。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、次の手順を実行して、**[コレクタ（Collector）]**>**[ネットワークプロファイル（Network Profiles）]** ページで、ネットワークプロファイルを設定します。

Before you begin

デバイスログイン情報プロファイル（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、「認証ログイン情報の構成 （12 ページ）」および「SNMP ログイン情報の設定 （13 ページ）」を参照してください。

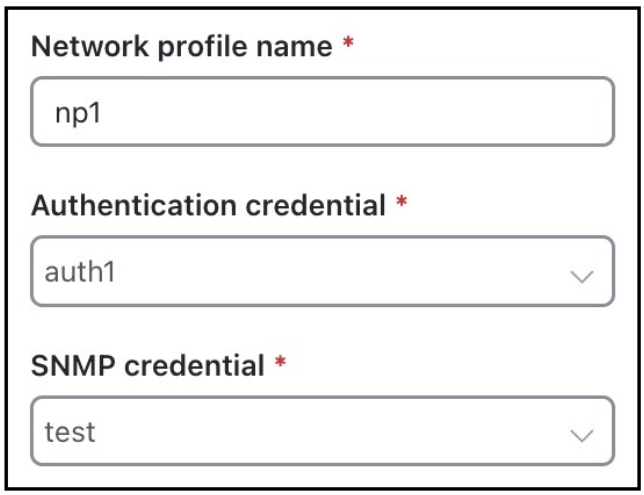
手順

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）] 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 *6*:ネットワークプロファイルの作成



ステップ 3 これらのフィールドに必要な値を入力します。

- [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で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、認証ログイン情報の構成 （12 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で該当する 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 （13 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、ネットワークプロファイルにノードを追加するまたはノードを編集する （18 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（20 ページ）を参照してください。

ステップ 7 変更内容を保存します。

ネットワークプロファイルが正常に作成され、ネットワークからデータを収集する準備が整います。

ネットワークプロファイルにノードを追加するまたはノードを編集する

この項では、ノードを追加または編集して、適切なノード詳細でネットワークプロファイルを更新する方法について説明します。

手順

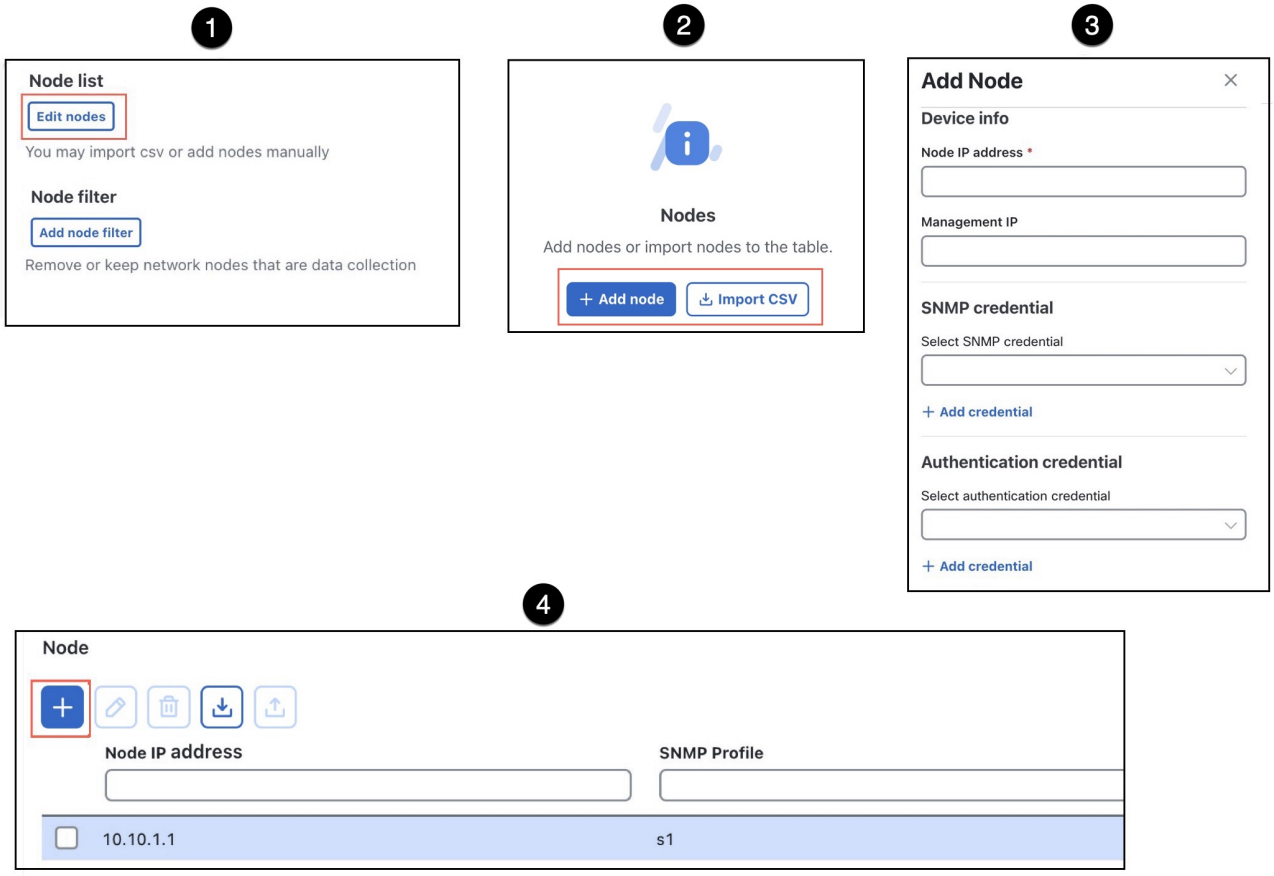
ステップ 1 メインメニューから、**[コレクタ（Collector）] > [ネットワークプロファイル（Network Profiles）]** の順に選択します。

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 **[ノードの一覧（Node list）]** で、**[ノードを編集（Edit nodes）]** をクリックして、ノードの追加方法を決定します。

属性...	以下を実行すると ...	その場合：
ノードがありません	始めてノードを手動で追加する	**1.** **[+ノードを追加（+Add Node）]** をクリックします。 **2.** [ノードを追加（Add Node）] ウィンドウにノードの詳細を入力します。 **3.** [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。
	ノードリストをインポートする	**1.** Import CSV をクリックします。 **2.** **[参照（Browse）]** をクリックして CSV ファイルパスを入力します。 **3.** [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。
ノードが既存する	さらにノードを追加する	[+] をクリックし、詳細を入力します。
	別のノードリストをインポートする	[] をクリックして、CSV ファイルをインポートします。 **[サンプルファイル（sample file）]** リンクをクリックして、ノードリストを含むサンプルファイルをダウンロードします。
	ノードリストをエクスポートする	をクリックします。
	ノードを編集する	**1.** 編集するノードを選択します。 **2.** をクリックします。 **3.** ノードの詳細を入力します。
	ノードを削除する	ノードを選択し、[] をクリックします。

図 *7:* ノードページを編集する



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

この項では、データ収集から具体的なノードを含める/除外する方法について説明します。

ノードフィルタを使用すると、定義された基準に基づいて、データ収集に含めるか、またはデータ収集から除外するノードを制御できます。各ノードに手動でフィルタ処理条件を定義することも、ノードを含む CSV ファイルと各フィルタ処理条件をアップロードすることもできます。

（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。ノードフィルタ IP として管理 IP アドレスを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。

Before you begin

CSV ファイルを使用する場合は、最初の行に、[種類（Type）]、[値（Value）]、[有効（Enabled）] の 3 つの列が含まれている必要があります。

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かを選択します。

ステップ 5 次の手順を実行して、各ノード向けのフィルタ処理条件を手動で指定します。

a) [+フィルタ条件の追加（+ Add Filter Criteria）] をクリックします。

b) フィルタ処理に使用する種類を選択します。オプションは、**[IPアドレス（IP Address）]** と **[ホスト名（Hostname）]** です。

c) **[入力の種類（Input type）]** で必要なオプションを選択して、**[保存（Save）]** をクリックします。前のステップで選択した種類によって、オプションは異なります。

- **[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。

以下を実行すると ...	結果...
単一式を使用して複数ノードを含めるまたは除外する	1. **[正規表現（Regex）]** オプションを選択します。 2. **[正規表現（Regex）]** フィールドに正規表現を入力します。

以下を実行すると ...	結果...
各ノードの IP アドレスを追加する	1. **[個別のIPアドレス（Individual IP address）]** オプションを選択します。 2. [IPアドレス（IP Address）] フィールドに IP アドレスを入力します。
各ノードのホスト名を追加する	1. **[個別のホスト名（Individual hostname）]** オプションを選択します。 2. [ホスト名（Hostname）] フィールドにホスト名を入力します。

d) 必要に応じて、ステップ 5(a) ～ 5(c) を繰り返して、フィルタ条件を追加します。

ステップ 6 次の手順を実行して、CSV ファイルとフィルタ処理するノードリストをインポートします。

a) [Import] をクリックします。
b) ノードとそのフィルタ条件を含む CSV ファイルをアップロードします。ファイルの形式が正しいことを確認したら、サンプル CSV ファイルをダウンロードして、参照します。
c) CSV ファイルをインポートします。
CSV ファイルに一覧されているノードが、[ノードのフィルタ処理（Nodes Filter）] ページに表示されます。

ステップ 7 フィルタのエントリを考慮する場合は、有効にします。**[状態（Status）]** 列にこの情報が表示されます。状態を変更するには、エントリを選択して、**[状態を更新（Update status）]**、希望の状態オプションの順に選択します。

設定に応じて、必要なノードをデータ収集に含めるか、除外します。

次のタスク

ノードを編集、削除またはエクスポートするには、ノードを選択して、**[編集（Edit）]**、**[削除（Delete）]** または **[エクスポート（Export）]** をクリックします。任意の列を使用すると、フィルタやエントリを並べ替えることができます。

エージェントの構成

この項では、Cisco Crosswork Planning でエージェントを構成し、ネットワークコレクション操作を有効にする方法について説明します。

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。

[コレクション（Collections）] ページに初回アクセス時（**[コレクタ（Collector）]** > **[コレクション（Collections]** の順に選択）、[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。この手順は、左側の [ステッパー

（Stepper）] ペインに表示されます。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、次の手順を実行し、**[コレクタ（Collector）]** > **[エージェント（Agents）]** ページの順に選択してエージェントを構成します。

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。

（注）
コレクションに、**Traffic collection** コレクタが含まれている場合は、**[コレクタ（Collector）]**、>**[エージェント（Agents）]** ページに、トラフィック ポーラー エージェント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。

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

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 必要なコレクタの種類を選択します。

- SR-PCE：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）
  ネットワークコレクションを実行する前に、SR-PCEを使用するすべてのネットワークに対してSR-PCEエージェントを構成する必要があります。

- NetFlow：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 構成オプションは、選択したコレクタの種類によって異なります。

- **[SR-PCE]** を選択した場合は、表 2 : SR-PCE エージェントの構成オプション （24 ページ） に記載されている該当する構成詳細を入力します。
- **[NetFlow]** を選択した場合は、表 3 : NetFlow エージェントの構成オプション （26 ページ） に記載されている該当する構成詳細を入力します。

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。
  - また、（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、「コレクションの設定 （30 ページ）」を参照してください。

SR-PCE および NetFlow エージェントの構成オプション

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

SR-PCE エージェントの構成オプション

このテーブルは、SR-PCE エージェントの構成オプションを示しています。

表 *2 : SR-PCE* エージェントの構成オプション

オプション	説明
有効化	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 ルータのホスト IP アドレス。
SR-PCE REST ポート	SR-PCE ホストに接続するポート番号。デフォルトは 8080 です。
認証タイプ	SR-PCE ホストへの接続に使用する認証タイプ。 • [ベーシック（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）] : 認証は使用されません。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	SR-PCE ホストに接続するためのユーザー名。
パスワード	SR-PCE ホストに接続するためのパスワード。

オプション	説明
接続再試行回数	SR-PCE ホストへの接続の最大再試行回数。
トポロジ収集	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。 以下のオプションがあります。 • コレクションのみ • コレクションとサブスクリプション（デフォルト） • オフ
LSP 収集	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。以下のオプションがあります。 • コレクションのみ • コレクションとサブスクリプション（デフォルト） • オフ
接続タイムアウト間隔	接続タイムアウト（秒）デフォルトは 50 秒です。
プールサイズ	SR-PCE データを並行して処理するスレッドの数。
キープアライブインターバル	キープアライブメッセージを送信する間隔（秒単位）。デフォルトは 10 です。
バッチサイズ	各メッセージで送信するノードの数。デフォルトは1000です。
キープアライブしきい値	欠落したキープアライブメッセージのしきい値。デフォルトは 2 です。
イベントバッファが有効	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	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秒単位の時間。

オプション	説明
再生イベントの遅延	実際のイベントを模倣する SR-PCE イベントの再生の秒単位の遅延（0 = 遅延なし）。
最大 LSP 履歴	送信する LSP エントリ数。デフォルトは 0 です。
ネットレコーダーモード	SNMP メッセージを録音します。[オフ（Off）]、[録音（Record）]、または [再生（Playback）] を選択できます。デフォルトはオフです。

NetFlow エージェントの構成オプション

このテーブルは、NetFlow エージェントの構成オプションを示しています。

表 *3 : NetFlow* エージェントの構成オプション

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。
サンプリングレート	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。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	フローエクスポートパケットの IPv4 送信元アドレス。
BGP 送信元 IP	iBGP 更新メッセージの IPv4 または IPv6 送信元アドレス。
BGP パスワード	MD5 認証の BGP ピアリングパスワード。
インターバル	出力ファイルを書き込む秒単位の間隔。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	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 レートに基づいたフローコレクションデプロイサイズ。 • [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：お客様向けではありません。 デフォルトは [中規模（Medium）] です。
追加集約	リストから集約キーを選択します。

エージェント設定の編集

この項では、パラメータの編集、スケジュールの管理、接続の確認など、エージェントでさまざまな操作を実行する方法について説明します。

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。作成済みのエージェントのリストが表示されます。

ステップ 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。

オプション	説明
編集（Edit）	エージェントのパラメータの変更
• 開始 • 再起動（Restart） • 停止（Stop）	それぞれエージェントを開始、再起動、停止します。
接続の確認	エージェントの状態を確認します。 NetFlow エージェントの詳細な状態を表示するには、**[詳細を表示（More details）]** をクリックします。

オプション	説明
消去	エージェントを削除します。
• スケジュールの追加 • スケジュールを編集	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。 （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。
スケジュールを削除する	エージェントに設定されているデータ更新周波数を削除します。 （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。

ステップ 3 エージェントに対して目的の操作を選択したら、後続の画面上のオプションに進み、タスクを完了します。

コレクションの設定

この項では、コレクタを設定してそのパラメータを構成し、ネットワークモデルを作成する方法について説明します。

process_summary

このプロセスに関与する主要なコンポーネントは次のとおりです。

- [コレクション（Collections）] ページ：さまざまなコレクタを構成し、コレクションタスクを管理するために使用されます。
- [コレクタ（Collectors）]：ネットワークデータを収集するためのツール。スタートアップスクリプト、[基本トポロジ（Basic topology）]、[高度なモデリング（Advanced modeling）]、[トラフィックとデマンド（Traffic and Demands）] で分類されます。
- 構成パラメータ：要件に基づいて調整する必要がある、各コレクタに関連付けられている設定。

[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。選択したコレクタに応じて、コレクタのチェーンが派生し、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。

process_workflow

これらは、コレクションの設定段階です。

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。	事前構成ワークフロー （11 ページ）を参照してください。
2. 必要なコレクタを選択します。	**1.** コレクション構成チェーンの最初の手順として外部スクリプトを使用する場合は、**[スクリプト（Script）]** を選択します。 **2.** [Basic Topologyコレクタ（Basic topology collector）] を選択します。スタートアップスクリプトを使用しない場合、この手順は必須です。最初の手順として、追加のネットワークコレクションのソースとなる Basic Topology コレクタのいずれかを選択します。 **3.** 必要に応じて、追加のコレクタを選択します。コレクタは、**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、構成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 （115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。	構成したコレクタの順序を確認します。構成に問題がない場合は、コレクションの作成を続行します。
6. コレクション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、コレクションのスケジュール （36 ページ） を参照してください。

ステップ	説明
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： • コレクタ出力の集約 （44 ページ） • アーカイブの構成 （47 ページ）

コレクションの設定

このトピックでは、Cisco Crosswork Planning UI を使用してコレクションを作成する方法について説明します。

[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。

重要 Cisco Crosswork Planning でコレクションを構成する際は、コレクションとネットワークデバイスがシステムのキャパシティにどのように影響するかを把握することが重要です。6,000 や 3,000 ノードなどの規模数は、組み合わされたすべてのコレクション全体の合計キャパシティです。たとえば、6,000 ノードの構成を作成する場合、すべてのノードを含む 1 つのコレクションを使用することも、1,000 のノードが各 6 つのコレクションに割り当てられた複数のコレクションを使用することもできます。ただし、システムに定義された規模の制限を超えると、パフォーマンスの問題につながります。例として、コレクタと集約のメモリ不足が挙げられます。すべてのコレクション内のデバイス数またはインターフェイス数が定義された規模制限内に収まっており、最適なシステムパフォーマンスが維持されていることを確認します。規模数の詳細については、「*Cisco Crosswork Planning 7.2* インストールガイド」の「プロファイル仕様」項を参照してください。

Before you begin

事前構成ワークフロー （11 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 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 コレクション作成プロセスを開始します。

a) 右上隅にある **[コレクションを追加（Add Collection）]** をクリックします。[コレクションを追加（Add Collection）] ページが表示されます。

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。

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

c) **[ノードプロファイル（Node Profile）]** ドロップダウンリストで、必要なノードプロファイルを選択します。

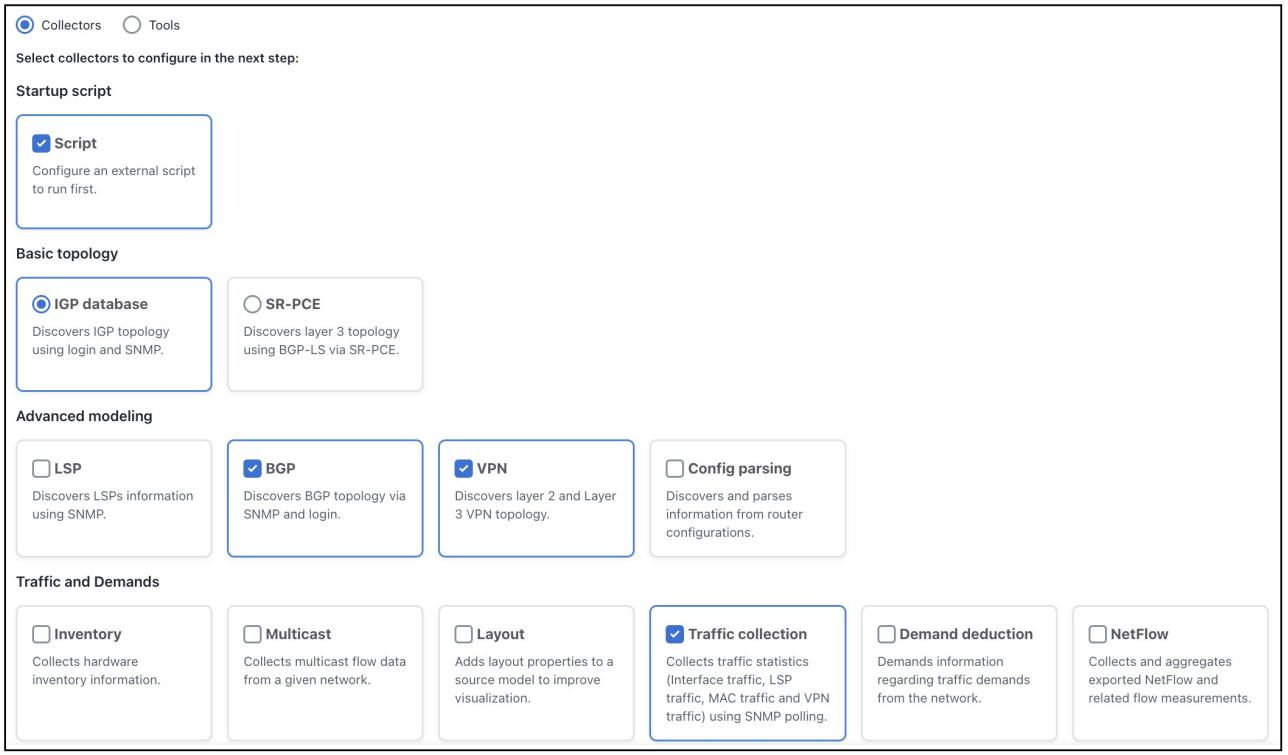
新しいプロファイルを作成するには、**[+新しいプロファイルを追加（+ Add new profile）]** をクリックします。

d) **[続行（Continue）]** をクリックして、[コレクション構成（collection configuration）] ページに進みます。

ステップ 3 必要な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 （61 ページ）を参照してください。

a) 上部で **[コレクタ（Collectors）]** が選択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。

図 *8 : [コレクタ（Collectors）]* ページを選択する



b) コレクション構成チェーンの最初の手順として外部スクリプトを使用する場合は、**[スクリプ（Script）]** を選択します。

コレクションで選択できるスタートアップスクリプトの数は 1 つのみです。

c) ネットワークコレクションを開始するには、いずれかの Basic Topology コレクタを選択する必要があります。サポートされているコレクションとして、IGP データベースと SR-PCE が挙げられます。

選択できるトポロジコレクタは、1 つのみです。

d) 必要に応じて、これらのセクションで追加のコレクタを選択します。

- [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ーを選択します。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。高度なコレクタは、複数選択できます。
- [トラフィックとデマンド（Traffic and Demands）]：トラフィックコレクション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。Traffic コレクタと Demand コレクタは複数選択できます。

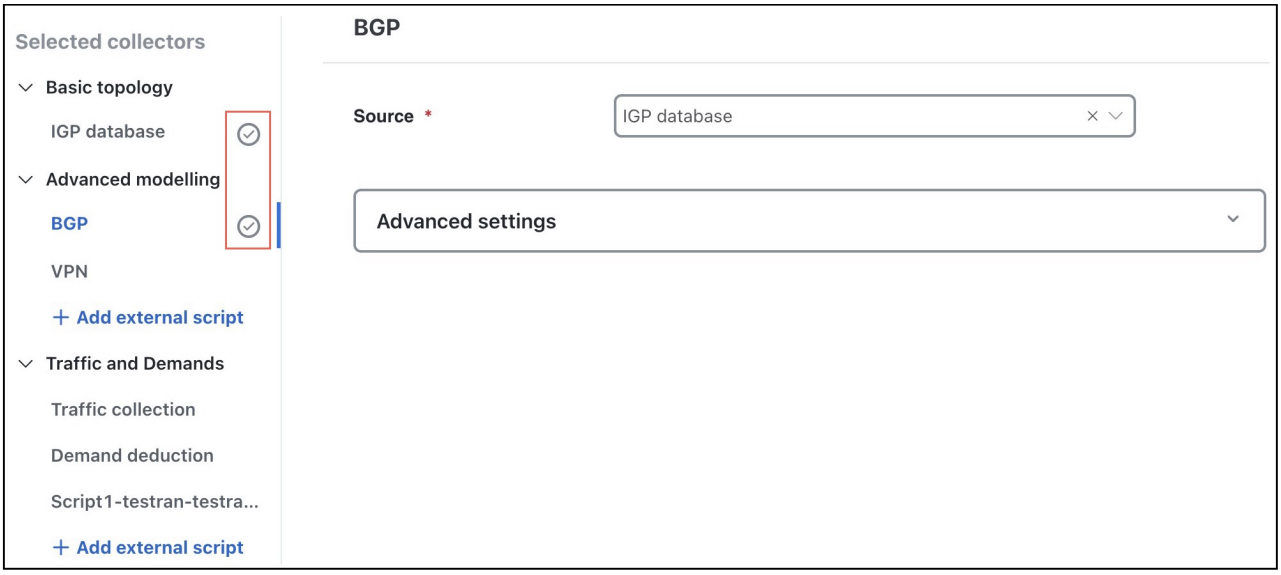
ステップ 4 コレクタを構成します。

a) 選択したコレクタの構成パラメータを入力します。

- 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で、現在選択されているコレクタのソース（入力）として機能する出力があ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）
選択したすべてのコレクタの構成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 *9*：コレクションパラメータの設定



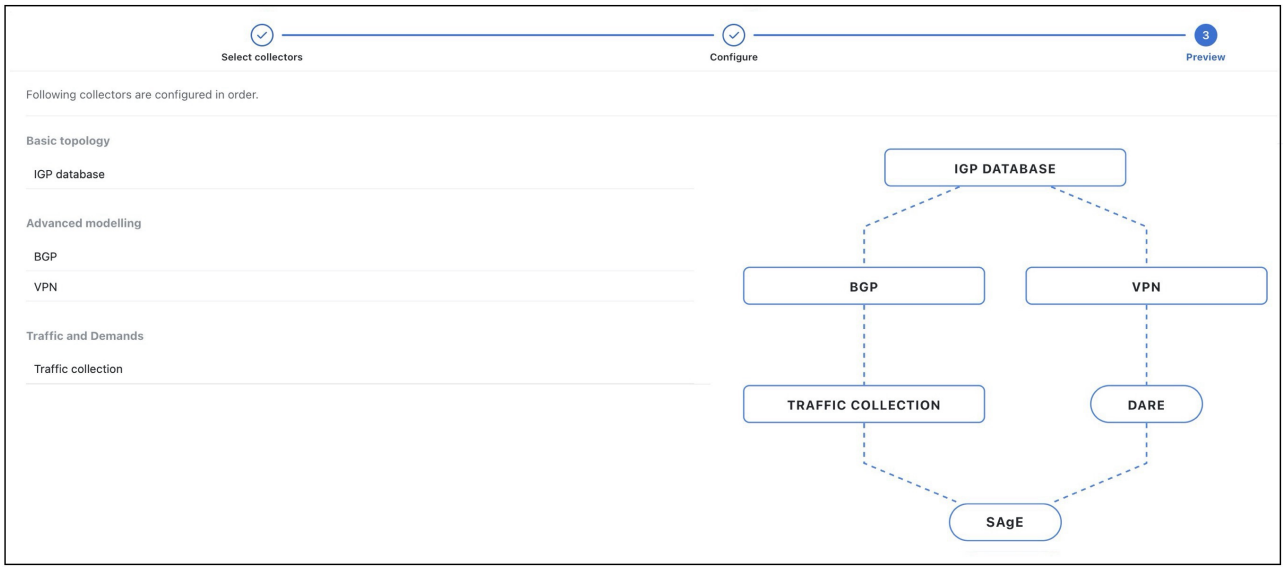
b) （オプション）コレクションモデルに対してカスタマイズされたスクリプトを使用する場合は、**[+外部スクリプトを追加（+ Add External Script）]** リンクを使用します。詳細については、ネットワークモデルに対する外部スクリプトの実行 （115 ページ） を参照してください。

c) 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 5 コレクタが追加された順番とコレクションの作成が完了した順番をプレビューします。

a) プレビュー図で、コレクタが追加された順番を確認します。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。

図 *10 : [プレビュー（Preview）]* ページ



b) 構成に問題がない場合は、**[作成（Create）]** をクリックしてコレクションの作成を続行します。

- コレクションが正常に作成された旨が記載された確認メッセージが表示されます。
- 構成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時に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。

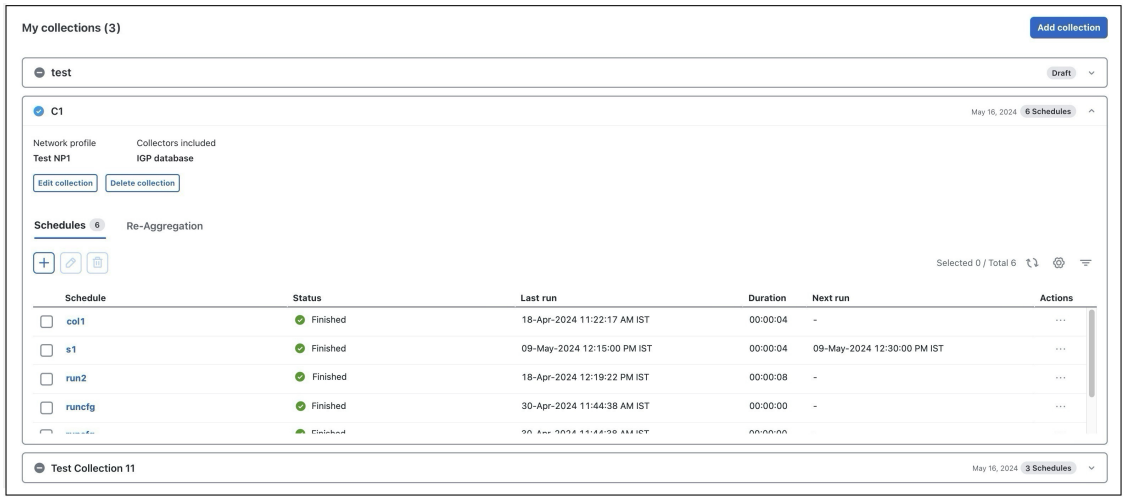
ステップ 6 （オプション）スケジュールをすぐに設定する場合は、ダイアログボックスで[スケジュールの追加（Add Schedule）]をクリックし、スケジュールの設定を続行します。詳細については、コレクションのスケジュール （36 ページ） を参照してください。

ステップ 7 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。各 [収集（Collection）] パネルを展開して詳細を表示します。

この図は、3 つのコレクションを含むサンプルの [コレクション（Collections）] ページを示しています。

図 *11* : 使用可能なコレクションのリスト



次のタスク

コレクション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、「コレクションのスケジュール （36 ページ）」を参照してください。

コレクションの編集

このトピックでは、既存のコレクションを編集する方法について説明します。

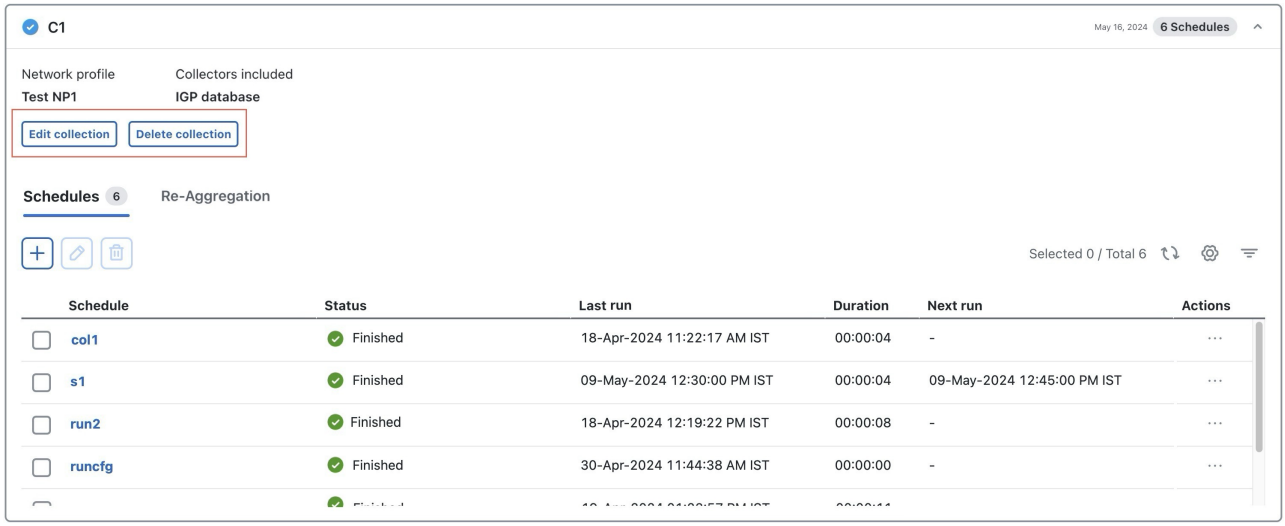
手順

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。既存のコレクションの一覧が表示されます。

ステップ 2 編集する [コレクション（Collection）] 領域を展開します。

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

図 *12 :* コレクションのアクション



ステップ 4 **[コレクタを選択（Select Collectors）]** ページと **[構成（Configure）]** ページで必要な変更を行います。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。詳細については、「コレクションの設定 （30 ページ）」を参照してください。

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、「コレクションのスケジュール （36 ページ）」を参照してください。

コレクションの削除

このトピックでは、既存のコレクションを削除する方法について説明します。

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。既存のコレクションの一覧が表示されます。

ステップ 2 削除する [コレクション（Collection）] 領域を展開します。

ステップ 3 [収集の削除（Delete collection）] をクリックします（図 12 : コレクションのアクション （35 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。

コレクション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。

コレクションのスケジュール

このトピックでは、Cisco Crosswork Planning UI でコレクションをスケジュールしてデータ収集を自動化する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、同じコレクションに対して複数のスケジュールを作成できます。

Before you begin

- 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、コレクションの設定（30 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。

手順

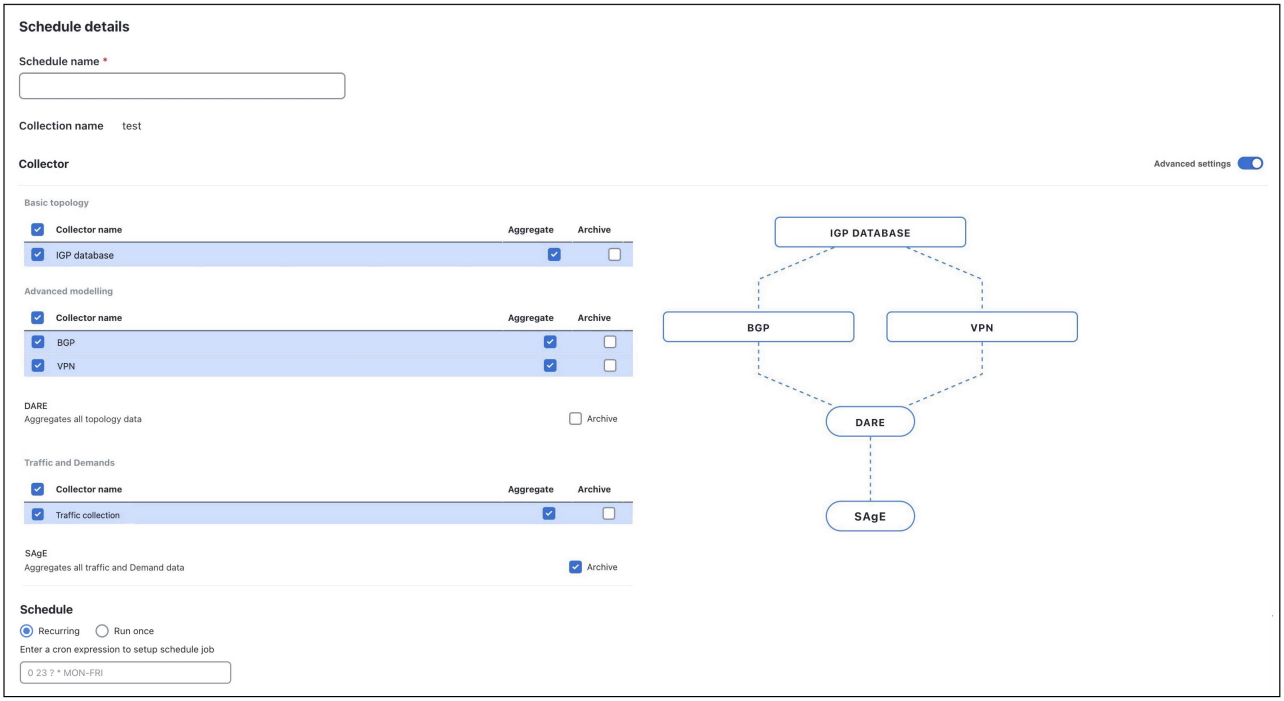
ステップ 1 メインメニューから、**[コレクタ（Collector）] > [収集（Collections）]** の順に選択します。作成済みの収集のリストが表示されます（参考資料については、図 11 : 使用可能なコレクションのリスト （34 ページ）を参照してください）。

ステップ 2 スケジュールを追加する [コレクション（Collection）] パネルを展開します。これら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 14 : スケジュールの作業 （39 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 *13* : 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、スケジュール名を入力します。

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。

- データ収集からコレクタを除外するには、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、コレクタ出力の集約 （44 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、アーカイブの構成 （47 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）]** オプションを選択すると、コレクションはただちに 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）]** オプションを選択する場合は、cron 式を使用して時間間隔を指定します。[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。

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。

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。**[スケジュール名（Schedule name）]** 列でスケジュール名をクリックすると、その詳細が表示されます。

スケジュールの編集

このトピックでは、コレクション内の既存のスケジュールの実行タイミングとパラメータを変更する方法について説明します。

このタスクを使用して、システム内のコレクションで関連するスケジュールを更新します。スケジュールを編集すると、コレクションの実行時を制御でき、運用要件やメンテナンス期間を調整できます。

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。既存のコレクションの一覧が表示されます。

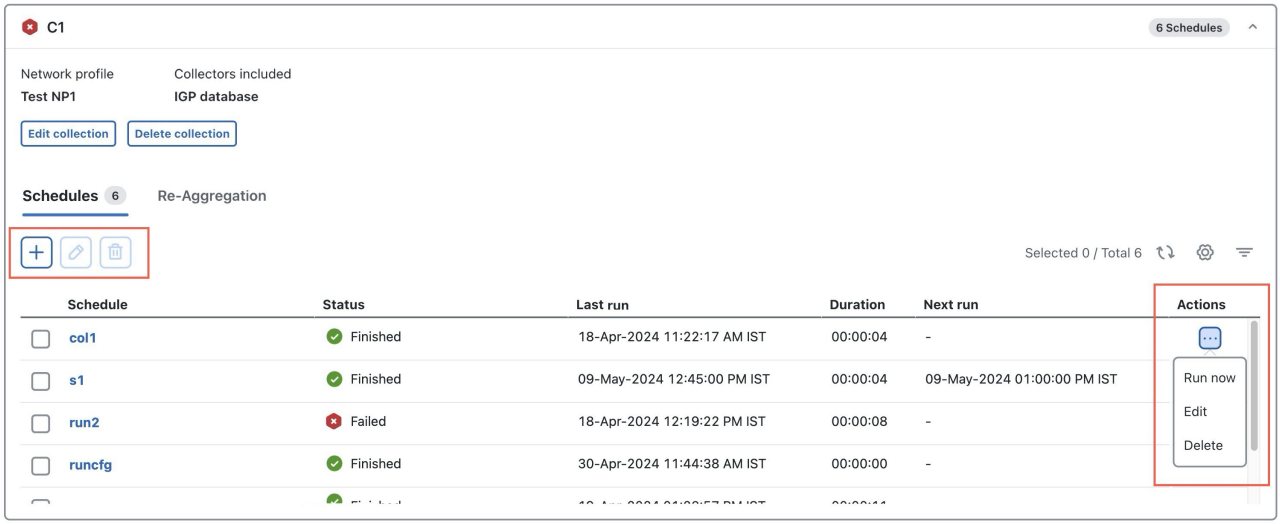
ステップ 2 編集するスケジュールを含む [コレクション（Collection）] パネルを展開します。

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）]** の順に選択します
- 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 *14* : スケジュールの作業



ステップ 4 **[スケジュールを編集（Edit Schedule）]** ページで必要な変更を行います。

ステップ 5 **[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、「コレクションのスケジュール （36 ページ）」を参照してください。

選択したスケジュールが更新されます。コレクションは、選択したオプションに応じて、即時に実行されるか、新しく指定した間隔で実行されます。

スケジュールを削除する

このトピックでは、システムからコレクションスケジュールを削除する方法について説明します。

スケジュールされたデータ収集のアクティビティをクリーンアップして、関連するスケジュールのみをお使いの環境でアクティブにするには、このタスクを使用します。

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。既存のコレクションの一覧が表示されます。

ステップ 2 削除するスケジュールを含む [コレクション（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、次のいずれかのオプションを使用してスケジュールを削除します。

- 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）]** の順に選択します。

（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。

選択したスケジュールがコレクションから削除され、削除が成功したことを示す確認メッセージが表示されます。

スケジュールタスクの状態と履歴の表示

このトピックでは、コレクション用にスケジュールされたタスクの状態と最近の履歴を表示する方法について説明します。

コレクションのスケジュールを構成すると、関連するタスクの現在の状態と最新の 10 の状態を表示できます。これにより、実行結果の追跡、障害のトラブルシュート、収集されたデータのダウンロード（必要な場合）を行うことができます。

Before you begin

コレクションのスケジュールが構成されていることを確認します。

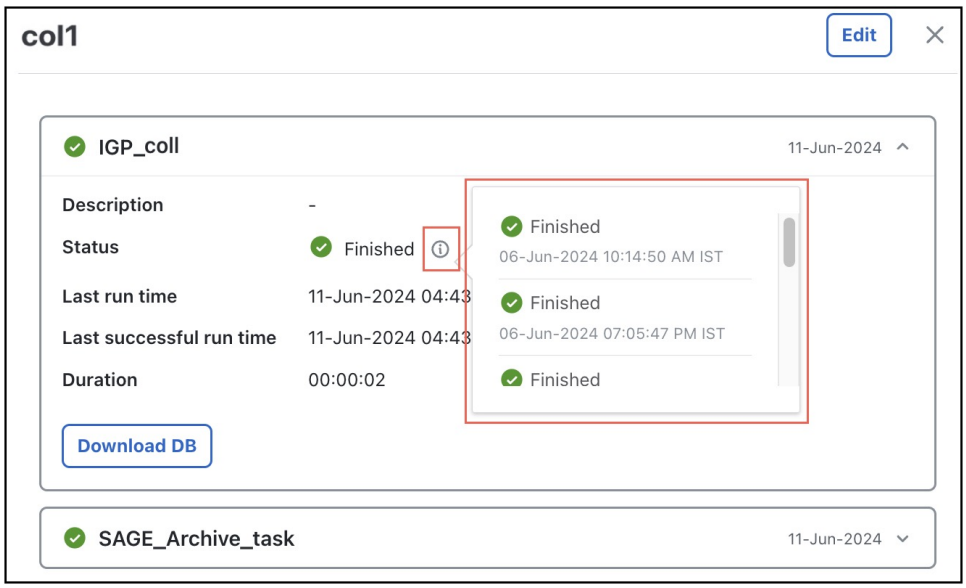
手順

ステップ 1 目的の [コレクション（Collection）] パネルを展開します。

ステップ 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、スケジュールされたコレクションに関連するすべてのタスクの状態が表示されます。これには、以下が含まれます。

- 最近のタスク実行のタイムスタンプ
- 各タスクの期間
- タスクが失敗した場合の説明。



ステップ 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。

失敗したタスクを特定した場合は、提供されている説明を確認し、必要に応じて詳細なトラブルシューティングや修正措置を実施します。

次のタスク

収集されたデータ、ログ、またはレコードファイルをダウンロードするには、「データ、ログ、レコードファイルのダウンロード （41 ページ）」を参照してください。

データ、ログ、レコードファイルのダウンロード

このトピックでは、特定のコレクタが生成したデータベース、ログ、およびレコードファイルをダウンロードする方法について説明します。これらのファイルは、問題のトラブルシューティングやデータの分析に役立ちます。

Before you begin

- コレクタが正常に実行されたことを確認します。
- 注：ログ、データベース、およびレコードファイルのダウンロードに関する制限事項（42 ページ） の制限事項を確認します。

手順

ステップ 1 目的の [コレクション（Collection）] パネルを展開します。

ステップ 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、スケジュールされたコレクションに関連するすべてのタスクの状態が表示されます。

ステップ 3 **[ダウンロード（Download）]** をクリックして、データをダウンロードするオプションのいずれかを選択します。

- **DB**：収集されたネットワークモデルを .db ファイルとしてローカルマシンにダウンロードします。
- **ログ**：コレクタの一部として実行される CLI ツールが生成する 1 つ以上のログを含む .tar ファイルとしてログファイルをダウンロードします。通常、これには sysout CLI ツールのログと関連するデータベースが含まれます。
- **レコードファイル**：コレクタの一部として実行される CLI ツールから収集されたネットワークデータを含むすべてのレコードファイルを含む .tar ファイルをダウンロードします。

  （注）
  Traffic コレクタでは、ポーラーは継続的に実行されます。その結果、ポーラーが実行されている限り、データはレコードファイルに追加されます。レコードファイルをダウンロードするには、まずコレクタの設定でポーラーを無効にして変更を保存して、ポーラーを停止する必要があります。これにより、レコードファイルをダウンロードできるようになります。

- **デバッグファイル**：デバッグに必要なファイルをダウンロードします。このオプションは、NetFlow コレクションでのみ使用できます。デフォルトでは、**missing-flows.txt** および **interas-file.txt** ファイルが含まれます。NetFlow コレクションの設定中に **[マイクロフローをバックトラック（Back Track microflows）]** オプションを有効にすると、デバッグファイルに追加のファイルが含まれます。NetFlow データ コレクションの詳細については、「NetFlow データ収集 （110 ページ）」を参照してください。

選択したデータベースファイル、ログ、またはレコードファイルが、ローカルマシンにダウンロードされます。

次のタスク

標準のアーカイブ ツールを使用してデータを抽出して確認します。

注：ログ、データベース、およびレコードファイルのダウンロードに関する制限事項

ログ、データベース、およびレコードファイルをダウンロードする前に、次の制限事項を考慮します。

- 特定の時点において、前回の実行以降のログ、データベース、およびレコードファイルのセットは、1 セットのみです。
- トラフィックコレクション中、トラフィックポーラーは継続的に実行され、そのログがロールバックされるため、ダウンロードされた .tar ファイルにはロールバックされたすべてのログが含まれます。
- ログファイルまたはレコードファイルを持たないコレクタでは、ログファイルとレコードファイルをダウンロードするオプションは無効になっているか、非表示になっています。

ログファイルとレコードファイルのダウンロードをサポートしているコレクタのリストについては、「ログおよびレコードファイルのダウンロードをサポートするコレクタおよびツール （43 ページ）」を参照してください。

- ダウンロードされたログには、Cisco Crosswork Planning サービスログは含まれていません。
- カスタムスクリプトに情報を記録する場合は、標準出力を使用します。標準出力（コンソール）に書き込まれたログは、スクリプトログとして収集され、ダウンロードできます。指定したファイルに書き込まれたログはダウンロードできません。

ログおよびレコードファイルのダウンロードをサポートするコレクタおよびツール

次の表に、ログまたはレコードファイルをダウンロードできるコレクタとツールを示します。

表 *4:* ログおよびレコードファイルのダウンロードをサポートするコレクタまたはツール

コレクタまたはツール	ダウンロードログ	レコードファイルのダウンロード
IGP データベース	✓	✓
SR-PCE	✓	✓
BGP	✓	✓
LSP	✓	✓
PCEP LSP	✗	✗
VPN	✓	✓
構成解析	✓	✓
インベントリ	✓	✓
マルチキャスト	✗	✗
Multicast コレクタ： • ログイン検出マルチキャスト • ログイン ポーリング マルチキャスト • SNMP 検出マルチキャスト • SNMP ポーリングマルチキャスト	✓	✓

コレクタまたはツール	ダウンロードログ	レコードファイルのダウンロード
レイアウト	✓	✗
トラフィック収集	✓	✓
デマンド推論	✗	✗
デマンド推論ツール： • LSP のデマンド • P2MP LSP のデマンド • デマンド推論 • コピーデマンド • デマンドメッシュクリエータ	✓	✗
NetFlow	✗	✗
外部スクリプト	✓	✗
DARE 集約	✗	✗
SAgE 集約	✗	✗
AS のマージ	✗	✗
代表プランの作成	✓	✗

コレクタ出力の集約

このトピックでは、ネットワークモデル集約プロセスから特定のコレクタ出力を除外する方法について説明します。

各コレクタは、完全なネットワークモデルを構築するために集約（統合）された出力を生成します。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の出力を集約します。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。コレクタ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、コレクションの設定 （30 ページ）を参照してください。

次の手順を実行して、集約からのコレクタ出力を除外します。

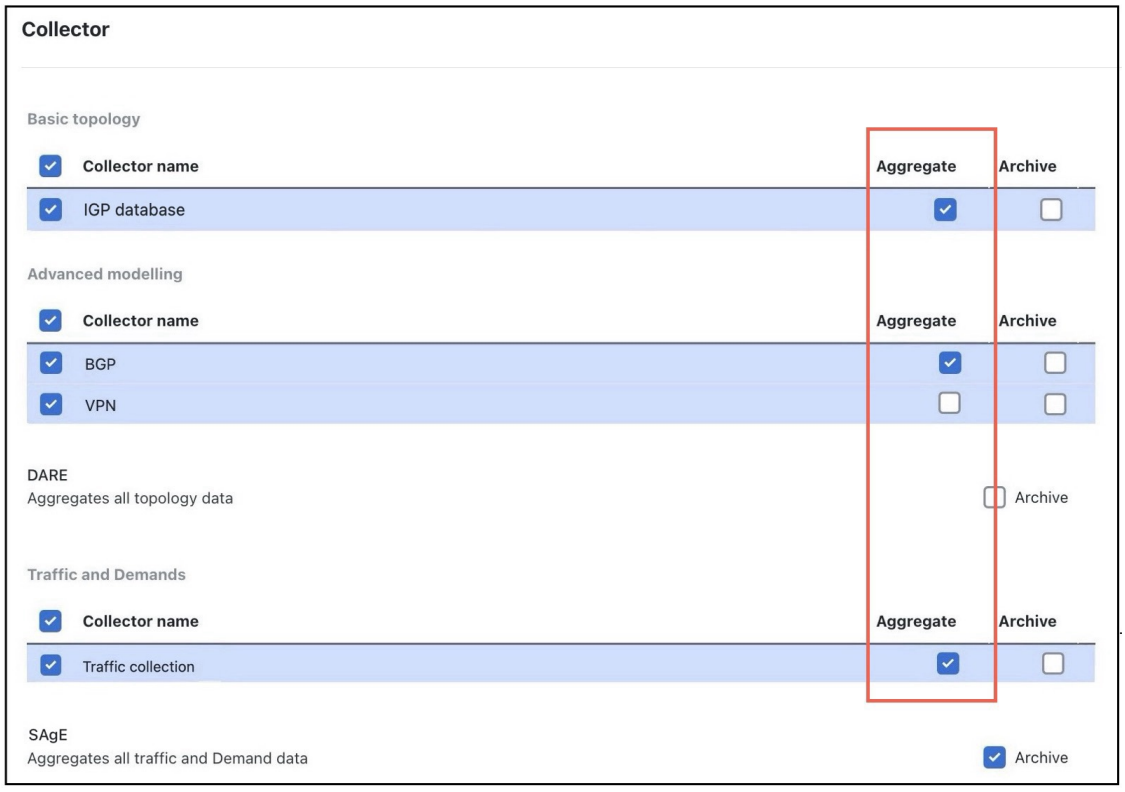
手順

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、コレクションのスケジュール （36 ページ）またはスケジュールの編集 （38 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。オフになっている場合は、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 *15 :* 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、コレクションのスケジュール（36 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。

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。

除外されたコレクタからのデータは集約に含まれなくなり、選択したコレクタ出力のみが最終ネットワークモデルに反映されます。

コレクタ出力の再集約

このトピックでは、コレクタ出力を再集約する方法について説明します。

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。このプロセスは新しいデータ収集をトリガーませんが、以前の集約結果を削除し、新しい集約を開始します。

（注） コレクションで、

- 再集約に使用できるスケジューラーは 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。

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。既存のコレクションの一覧が表示されます。

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 初めて再集約する場合は、**[スケジュール]** または **[1回実行（Run once）]** をクリックします。

- **[1回実行（Run Once）]** をクリックすると、再集約が即座に 1 回だけ実行されます。
- **[スケジュール（Schedule）]** をクリックすると、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。

[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。

図 *16* : コレクションの再集約

ステップ 5 スケジュールを更新するか、再集約を再度実行するには、**[アクション（Actions）]** 列で [•••] をクリックします。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。

- **[スケジュール]**を選択すると、[今すぐ実行（Run Now）]、[スケジュールを編集（Edit schedule）]、[一時停止（Pause）]、および [削除（Delete）] のオプションが表示されます。
- **[1回実行（Run once）]** を選択すると、[今すぐ実行（Run now）]、[スケジュールを追加（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。

システムは以前の集約を破棄し、選択されたコレクタの新しい集約プロセスを開始します。

アーカイブの構成

このトピックでは、コレクションでアーカイブ設定を構成する方法について説明します。

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。アーカイブは、プランファイルのリポジトリです。

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。

Before you begin

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、コレクションの設定 （30 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、コレクションのスケジュール （36 ページ）またはスケジュールの編集 （38 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）]** トグルボタンが、デフォルトでオンになっていることを確認します。有効な場合は、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。

- コレクションレベルでネットワークモデルをアーカイブするには、対応するコレクションの**[アーカイブ（Archive）]** 列のチェックボックスをオンにします。
- 最後の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 *17*：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、コレクションのスケジュール （36 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」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）で保存されます。これらには、Cisco Crosswork Planning Design アプリケーションの**[ネットワークモデル（Network Models）]**ページでアクセスできます。

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。

アプリケーションのインストール時に...	次に、アーカイブされたネットワークモデル...
同じマシン上で	**[ネットワークモデル（Network Models）]** > **[ローカルアーカイブ（Local archive）]**の順に選択すると表示されます。
異なるマシン上で	Cisco Crosswork Planning Design アプリケーションで、**[ネットワークモデル（Network Models）]** > **[リモートアーカイブ（Remote archive）]**の順に選択すると表示されます。

詳細については、「ローカルアーカイブからプランファイルを表示するかダウンロードする（49 ページ）」および「リモートアーカイブからのプランファイルへのアクセス（51 ページ）」を参照してください。

ローカルアーカイブからプランファイルを表示するかダウンロードする

このトピックでは、ローカルアーカイブからプランファイルを表示、ダウンロードする方法にについて説明します。

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、**[ネットワークモデル（Network Models）]** > **[ローカルアーカイブ（Local archive）]** の順に選択すると、アーカイブされたネットワークモデルが表示されます。

Before you begin

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、アーカイブの構成 （47 ページ） を参照してください。

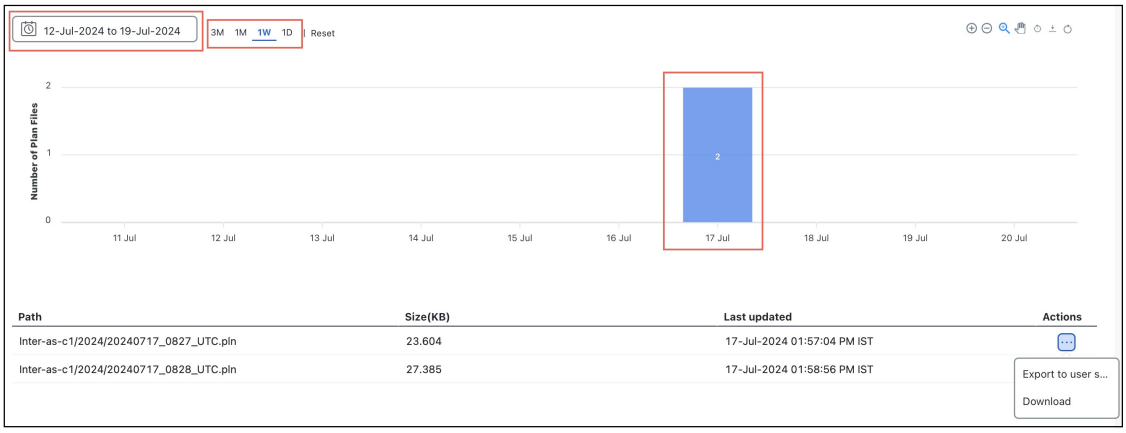
手順

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）]**で、アーカイブされたコレクションのリストから目的のコレクション名を選択します。

右側のパネルには、さまざまな時間にスケジュールされたコレクションで作成されたプランファイルの一覧が表示されます。**[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。

図 *18 :* 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。選択した日付範囲で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（date range selection）] 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）に生成されたプロファイルを表示します。
- グラフバーセグメントをクリックすると、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 [⋯]、**[ユーザースペースにエクスポート（Export to user space）]** の順に選択します。

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

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。

[ユーザースペース（User space）] > [マイユーザースペース（My user space）] ページの順に選択すると、プロファイルが表示されます。

ステップ 7 （オプション）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、[･･･]、**[ダウンロード（Download）]** の順に選択します。

プランファイルが、ユーザースペースにエクスポートされるか、ローカルマシンにダウンロードされます。これで、必要に応じてプランファイルを使用、分析、または視覚化できるようになります。

次のタスク

ネットワークモデルを視覚化するには、**[ユーザースペース（User space）] > [マイネットワークモデル（My network models）]**、ファイル名の順に選択します。**[ネットワーク設計（Network Design）]**ページでネットワークモデルが開きます。詳細については、「*Cisco Crosswork Planning Design 7.2* ユーザーガイド」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へのアクセス

process_summary

Cisco Crosswork Planning Design および Collector アプリケーションを別のマシンにインストールする場合、Cisco Crosswork Planning Design アプリケーションで、**[ネットワークモデル（Network Models）] > [リモートアーカイブ（Remote archive）]** の順に選択すると、アーカイブされたネットワークモデルが表示されます。

process_workflow

次の段階では、リモートアーカイブからプランファイルにアクセスする方法について説明します。

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。詳細については、「アーカイブの構成 （47 ページ）」を参照してください。
2. Cisco Crosswork Planning Design アプリケーションから、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）。詳細については、「外部コレクタへの接続 （52 ページ）」を参照してください。

3. Cisco Crosswork Planning Design アプリケーションの [リモートアーカイブ（Remote archive）] セクションからネットワークモデルにアクセスします。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 （52 ページ）」を参照してください。

外部コレクタへの接続

このトピックでは、別のマシンで、Cisco Crosswork Planning コレクタインスタンス（外部コレクタ）に接続する方法について説明します。

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 外部コレクタマシンのポート、ユーザー名、およびパスワードを入力します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 メインメニューで、**[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。

Cisco Crosswork Planning Design アプリケーションが外部コレクタに接続されます。

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 （52 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

このトピックでは、リモートアーカイブからプランファイルを表示、ダウンロードする方法にについて説明します。

Procedure

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）]**で、アーカイブされたコレクションのリストから目的のコレクション名を選択します。

右側のパネルには、さまざまな時間にスケジュールされたコレクションで作成されたプランファイルの一覧が表示されます。**[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 18 : アーカイブされたプランファイル, on page 50」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。選択した日付範囲で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（date range selection）] 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）に生成されたプロファイルを表示します。
- グラフバーセグメントをクリックすると、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 [⋯]、**[ユーザースペースにエクスポート（Export to user space）]** の順に選択します。

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

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、**[新しいタグを追加（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。

[ユーザースペース（User space）][マイユーザースペース（My user space）] ページの順に選択すると、プロファイルが表示されます。

ステップ 8 （オプション）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、[⋯]、**[ダウンロード（Download）]** の順に選択します。

プランファイルが、ユーザースペースにエクスポートされるか、ローカルマシンにダウンロードされます。これで、必要に応じてプランファイルを使用、分析、または視覚化できるようになります。

What to do next

ネットワークモデルを視覚化するには、**[ユーザースペース（User space）] > [マイネットワークモデル（My network models）]**、ファイル名の順に選択します。**[ネットワーク設計（Network Design）]**ページでネットワークモデルが開きます。詳細については、「*Cisco Crosswork Planning Design 7.2* ユーザーガイド」を参照してください。

コレクタ構成の移行

コレクタ構成の移行とは、次のプロセスを指します。

- コレクタ構成を Cisco WAE 7.5.x/7.6.x または異なる Cisco Crosswork Planning インスタンス間に転送します。
- 既存のコレクタ構成を保持します。
- 対象のプラットフォームで、継続した操作を促進します。

（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。構成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。正しいファイルを使用しないと、コレクションは機能不全になります。

Cisco WAE からのコレクタ構成の移行

この項では、コレクタ構成を Cisco WAE 7.5.x/7.6.x から Cisco Crosswork Planning に移行する方法について説明します。

（注） Layout コレクタを使用する場合は、コレクタ構成をインポートした後に、**[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。

Before you begin

- 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 構成をバックアップしていない場合は、次の手順を実行してバックアップし、Cisco Crosswork Planning と互換性のある構成に移行します。

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) 以下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. The migrated configurations are saved as
                wae_networks.cfg in the provided directory.
```

ステップ 2 構成をすでにバックアップしている場合は、次の手順を実行して、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) 以下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. The migrated configurations are saved as
                  wae_networks.cfg in the provided directory.
```

ステップ 3 次の手順を実行して、移行した構成（**wae_networks.cfg**）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。

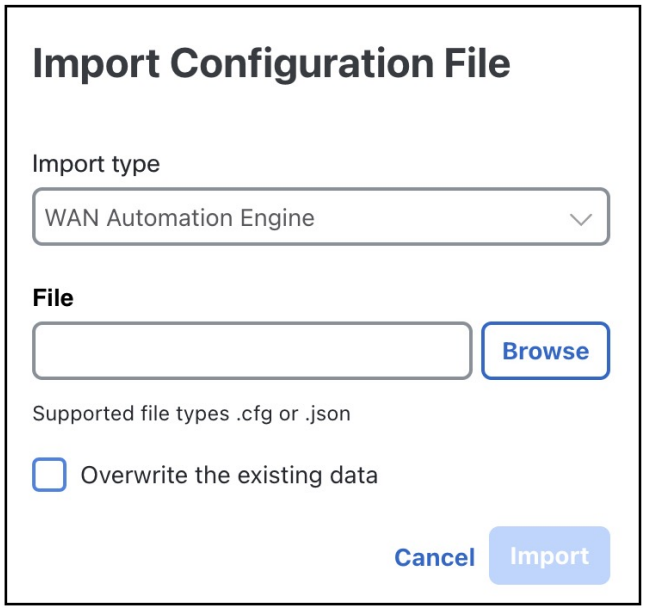
a) Cisco Crosswork Planning UI にログインします。

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、**[構成のバックアップ（Configuration Backup）]** を選択します。

[構成ファイルをインポート（Import Configuration File）] ページが表示されます。

図 *19 :* 構成*[*構成ファイルをインポート（*Import Configuration File*）*]* ページファイルをインポートページ



d) **[インポートタイプ（Import Type）]** ドロップダウンリストで、**[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、**wae_networks.cfg** ファイルを選択します。
f) （オプション）既存のコレクタ構成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) [Import] をクリックします。

システムが、構成を使用してインポートします。[移行（Migration）] ページ（**[コレクタ（Collector）]** > **[移行（Migration）]**）で、進捗を監視できます。インポートが成功すると、**[インポートの状態（Import Status）]** 列にタスクの状態が **[成功（Success）]** と表示されます。

次のタスク

（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構成

次の構成は、Cisco WAE から Cisco Crosswork Planning への移行中に移行されません。

コアシステムとログイン情報の構成

- HA、LDAP、およびユーザー管理の構成
- スマートライセンスの設定
- WMD 設定
- コンポーザワークフローに含まれないネットワーク
- 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。
- ネットワーク レコード プラン ファイル

機能固有の構成

- 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 関連の構成。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、オプティカル構成はアップグレードスクリプトの一部として収集され、今後使用できます。
- 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。
- 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。
- 特定のリソースファイル。たとえば、sql-capabilities、sql-source-capabilities など、更新されたネットワークアクセスファイル、高度な Aggregator 構成。
- 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。

Cisco Crosswork Planning インスタンス間でコレクタ構成を移行する

この項では、ある Cisco Crosswork Planning インスタンス（送信元）から別のインスタンス（ターゲット）にコレクタ構成を移行する方法について説明します。

（注）
- 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ます。これらのフィールドは、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更新されないため、この操作が必要です。
- Layout コレクタを使用する場合は、コレクタ構成をインポートした後に、**[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。

手順

ステップ 1 送信元マシンからコレクタ構成ファイルをダウンロードします。

a) 構成を移行する 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、**[構成のバックアップ（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。

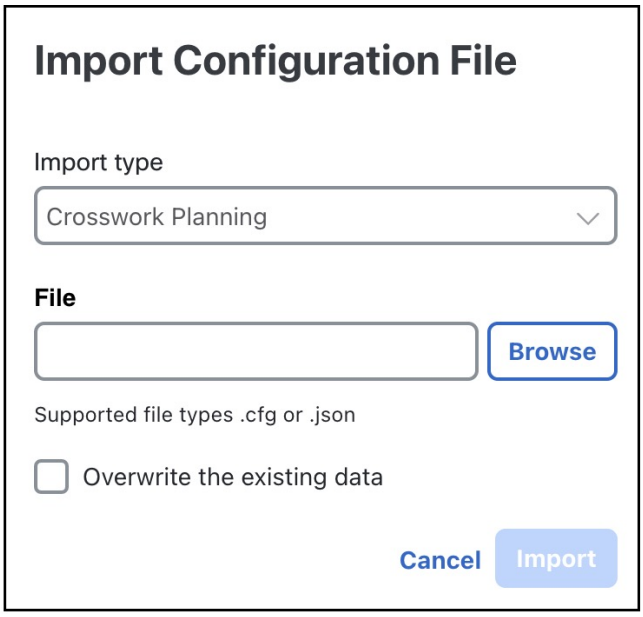
ステップ 2 コレクタ構成ファイルをターゲットマシンにインポートします。

a) 構成を移行する 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、**[構成のバックアップ（Configuration Backup）]** を選択します。

[構成ファイルをインポート（Import Configuration File）] ページが表示されます。

図 *20* : 構成/構成ファイルをインポート（*Import Configuration File*）] ページファイルをインポートページ



d) **[インポートタイプ（Import Type）]** ドロップダウンで、**[Crosswork 計画作成（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構成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。

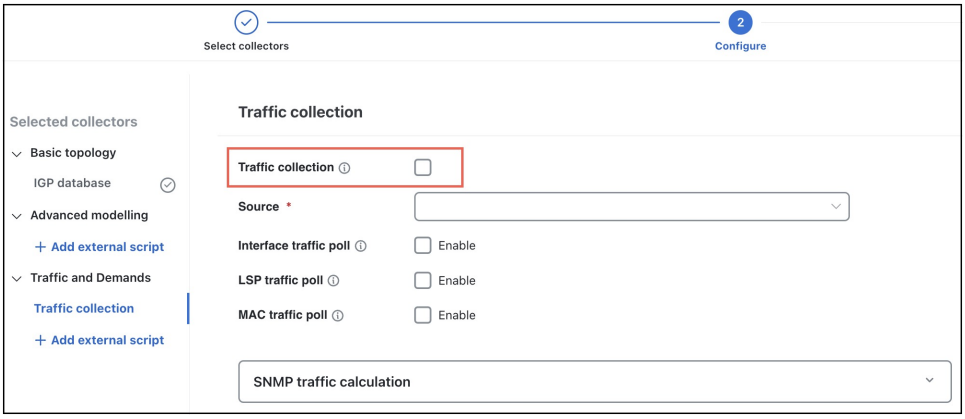
g) [インポート（Import）] をクリックして、コレクタ構成ファイルをインポートします。

システムが、構成を使用してインポートします。[移行（Migration）] ページ（**[コレクタ（Collector）]** > **[移行（Migration）]**）で、進捗を監視できます。インポートが成功すると、**[インポートの状態（Import Status）]** 列にタスクの状態が **[成功（Success）]** と表示されます。

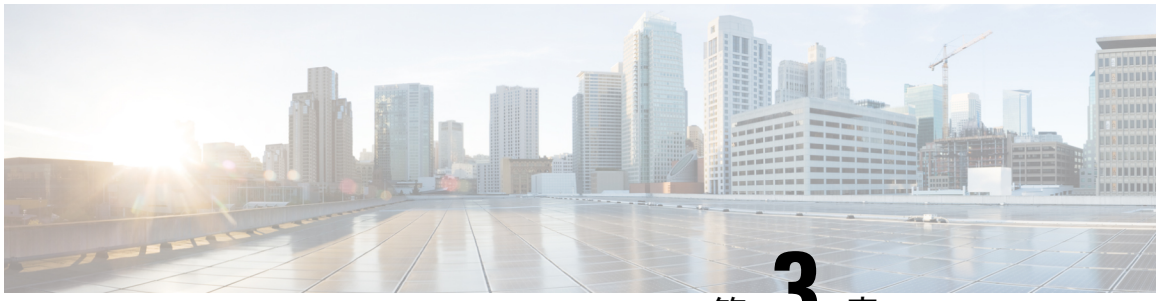
次のタスク

（注） トラフィックコレクションの場合、トラフィックコレクション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 エージェントの状態が [エージェント（Agent）] ページで、停止と表示される場合は、次の手順を実行します。

1. [コレクション（Collections）] ページで、対応するエージェントのコレクションに対して、**[コレクションを編集（Edit collection）]** をクリックします。
2. [トラフィックコレクションの構成（Traffic Collection Configuration）] ページで、**[トラフィックコレクション（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. **[トラフィックコレクション（Traffic Collection）]** チェックボックスを再度有効にして、構成を再度保存します。



[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 （102 ページ）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

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。

このテーブルは、コレクタとその関数について説明しています。

表 5: コレクタの説明

コレクタ（Collector）	説明	前提条件と注意事項	設定手順
Basic Topology Collection			
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 database コレクタを使用したトポロジ情報の収集 （67 ページ）を参照してください。
SR-PCE	• SR-PCE 経由でレイヤ 3 トポロジを検出します。 • トポロジの送信元として未処理の SR-PCE データを使用します。 • ノード、インターフェースおよびポートのプロパティは、SNMP を使用して検出されます。	• このコレクションを実行する前に、SR-PCE エージェントを構成します。詳細については、エージェントの構成 （22 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 コレクタを構成して、ストア登録情報情報を収集する （70 ページ）を参照してください。
Advanced Modeling Collection			
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 を使用する場合は、SR-PCE コレクタを使用してトポロジ情報を収集してから、このコレクションを実行します。詳細については、「SR-PCE コレクタを構成して、ストア登録情報情報を収集する （70 ページ）」を参照してください。	LSP 情報の収集 （74 ページ） を参照してください。

コレクタ（Collector）	説明	前提条件と注意事項	設定手順
PCEP LSP	SR-PCE を使用して PCEP LSP を検出します。 （注） SR-PCE コレクタを Basic Topology コレクタとして選択すると、このコレクタのみにアクセスできます。	SR-PCE コレクタを使用してトポロジ情報を収集してから、このコレクションを実行します。詳細については、「SR-PCE コレクタを構成して、ストア登録情報情報を収集する （70 ページ）」を参照してください。	SR-PCE を使用した PCEP LSP 情報の収集 （76 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 （82 ページ）を参照してください。
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 （85 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 （95 ページ）を参照してください。
Traffic and Demands Collection			
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。	ハードウェア一覧情報の収集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。	ネットワークからマルチキャストフローデータを収集する （78 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。 • Layout コレクタを構成したら、レイアウトのプロパティを含むプランファイルを Layout モデルにインポートする必要があります。	ネットワークモデルの可視性を向上させるために Layout コレクタを構成する （101 ページ）を参照してください。

コレクタ（Collector）	説明	前提条件と注意事項	設定手順
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 （74 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 （85 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（102 ページ）」を参照してください。
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 （109 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 コレクションの設定（112 ページ）を参照してください。
Custom Scripts			
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（115 ページ）」を参照してください。

外部スクリプトをスタートアップスクリプトとして実行する

このトピックでは、コレクション設定チェーンの最初のステップとして外部スクリプトを実行する方法について説明します。

データ収集チェーンの最初のステップとして外部スクリプトを指定します。有効にすると、スタートアップスクリプトはチェーン内の他のどのコレクタよりも先に実行されます。この機能により、コレクション中にデータを収集および処理する方法がより柔軟になります。

スタートアップスクリプトが最初のステップとして使用される場合、IGP データベースまたは SR-PCE コレクタはオプションになります。その [構成（configuration）] セクションの [送信元（Source）] ドロップダウンリストが有効になります。このソースは、データ収集の基本的なトポロジコレクタでは使用されません。これは、基本トポロジでのスタートアップスクリプトおよびその他の外部スクリプトの後に、これらのコレクタが実行される順序を決定するために使用されます。

Before you begin

- 事前構成ワークフロー （11 ページ）に記載されている手順を実行します。
- カスタム スタートアップ スクリプトに関する重要事項 （66 ページ）を確認してください。
- カスタムスクリプトおよびサポートファイルを、指定されたファイル形式または圧縮アーカイブのいずれかで用意します。

手順

ステップ 1 新しいコレクションを作成するか、既存のコレクションを編集するかを決定します。詳細については、コレクションの設定 （30 ページ）またはコレクションの編集 （34 ページ）を参照してください。

ステップ 2 **[スタートアップスクリプト（Startup script）]** セクションで、**[スクリプト（Script）]** を選択します。

ステップ 3 （オプション）スタートアップスクリプトを選択した場合は、Basic Topology コレクタをスキップするか、スタートアップスクリプトをソースとして設定できます。必要に応じて、追加のコレクタを選択します。

ステップ 4 [構成（Configure）]ページで、スクリプトの詳細を入力します。スタートアップスクリプトの構成は、ソースが不要であることを除いて、他の外部スクリプトの構成と同様です。

オプション	説明
コレクタ名	コレクションの名前を指定します。
送信元はプランファイルか？	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、**[プランファイルを入力（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。
入力ファイル	カスタムスクリプトと、その正常な実行に必要なサポートファイルをアップロードします。複数のファイルが必要な場合は、アップロードする前に、それらを 1 つのアーカイブに圧縮します。有効なフォーマットは、.py、.sh、.pl、.zip、.tar、.gz および .tar.gz です。 （注） ファイルがアップロードされるたびに、入力ファイルオプションが上書きされます。

オプション	説明
実行可能スクリプト	スクリプト実行プロセスを開始するファイル名を入力します。これは、**[入力ファイル（Input file）]** フィールドにアップロードされたファイルの 1 つです。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 （115 ページ） を参照してください。
スクリプト言語	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	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 （オプション）ステップ 3 で他のコレクタを選択した場合は、必要に応じてそれらのパラメータを設定します。

スタートアップスクリプトをコレクタのソースとして使用するには、コレクタのパラメータを設定する際に、**[送信元（Source）]** ドロップダウンリストでスタートアップスクリプト名を選択します。

ステップ 6 [次へ（Next）] をクリックします。

ステップ 7 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。

ステップ 8 収集ジョブのスケジュールを設定します。コレクション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、「コレクションのスケジュール （36 ページ）」を参照してください。

カスタムスクリプトは、コレクション構成チェーンの最初のステップとして実行します。

カスタム スタートアップ スクリプトに関する重要事項

コレクションでカスタム スタートアップ スクリプトを使用する場合は、次の点を確認します。

- コレクションチェーンごとに許可されるスタートアップスクリプトは 1 つだけです。
- スタートアップスクリプトによって生成されるデータベースファイルの集約は、コレクタ構成で設定されたアグリゲータのプロパティによって異なります。
- スタートアップスクリプトをソースとして使用するようにコレクタを構成し、そのスクリプトが有効なデータベースファイルを生成しない場合、コレクタの実行は失敗します。
- 以前のリリースから構成を移行または復元する場合は、必要なすべてのスタートアップ スクリプト オプションが使用可能で、適切に入力されていることを確認します。
- Cisco WAE でスクリプトを使用していて、それを Cisco Crosswork Planning で使用する場合は、修正を加えないと期待通りに動作しない場合があります。これは、さまざまなファイルの参照方法を含む Cisco WAE と Cisco Crosswork Planning のアーキテクチャの違いによ

るものです。Cisco Crosswork Planning で使用するには、適切にスクリプトを調整する必要があります。

基本的なトポロジ情報の収集

process_summary

基本のトポロジ情報の収集には、Basic Topology コレクタの選択と構成が含まれ、これによって構築される初期ネットワークモデルが、Cisco Crosswork Planning での今後のデータ収集の基盤となります。適切なトポロジコレクタを選択すると、どのデータソースを含めるかが決まります。

このプロセスに関与する主要なコレクタは次のとおりです。

- **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。
- **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。

トポロジ情報を収集するために選択できるコレクタは、コレクションごとに 1 つだけです。両方のコレクタを同時に選択することはできません。

process_workflow

基本トポロジ情報を収集する段階は次のとおりです。

1. **IGPデータベース**または **SR -PCE** コレクタのいずれかを選択し、指定されたコレクションのトポロジ情報を収集します。
2. 要件に基づいて、選択したコレクタを設定します。
3. 収集されたデータからネットワークモデルを生成します。これは追加のデータ収集の基盤になります。

IGP データベースと **SR-PCE** コレクタの構成の詳細な手順については、「IGP database コレクタを使用したトポロジ情報の収集 （67 ページ）」および「SR-PCE コレクタを構成して、ストア登録情報情報を収集する （70 ページ）」を参照してください。

IGP database コレクタを使用したトポロジ情報の収集

このトピックでは、**IGP database** コレクタを構成して、IGP database を使用して完全なネットワークトポロジを検出する方法について説明します。

IGP database 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。これは、他のコレクタが必要とする基本的なネットワークデータを提供するため、一般的に最初に構成するコレクタです。複数の OSPF と IS-IS インスタンスをサポートします。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。結果として取得さえるネットワークモデルは、追加のコレクションに対して送信元ネットワークとし

て使用されます。これは、他のコレクタが使用するコアノード、回路、インターフェイス情報を提供するためです。

IGP database コレクタを使用したトポロジ情報の収集

Before you begin

- 事前構成ワークフロー （11 ページ）に記載されている手順を実行します。
- シードルータとして使用するルータのネットワークログイン情報とアクセス権を保持している必要があります。

手順

ステップ 1 新しいコレクションを作成するか、既存のコレクションを編集するかを決定します。詳細については、コレクションの設定 （30 ページ）またはコレクションの編集 （34 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 database]** 、**[次へ（Next）]** の順に選択します。

ステップ 3 [構成（Configure）] ページの **[シードルータ（Seed Router）]** で、次の構成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を入力します。
- **[ルータ IP（Router IP）]**：シードルータの管理 IP アドレスを入力します。
- **[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。

以下を選択した場合 ...	結果...
ospf または **ospfv3**	**[詳細（Advanced）]** ページの **[OSPF領域（OSPF area）]** で値を入力します（[⚙] をクリック）。 OSPF エリアオプションでは、[エリアID（area ID）] または [すべて（all）] を指定します。デフォルトは area 0 です。
isis または **isisv6**	**[詳細（Advanced）]** ページで **[ISIS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。

- **[インターフェイスを収集（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。このオプションは、デフォルトで有効です。

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。すべてのシードルータに一意のインデックス番号を割り当てます。

ステップ 5 （オプション）具体的な QoS ノード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）]** の順に選択し、**[+ノードフィルタを追加（+ Add Node Filter）]** をクリックして、必要な値を入力します。

ステップ 6 （オプション）**[詳細設定（Advanced settings）]** パネルを展開して、必要に応じて、その他の関連する高度なフィールドを構成します。詳細オプションの説明については、IGP および SR-PCE コレクションの詳細オプション （72 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。

ステップ 9 収集ジョブのスケジュールを設定します。コレクション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、「コレクションのスケジュール （36 ページ）」を参照してください。

IGP database コレクタは、トポロジ検出プロセスを開始し、具体的なシードルータと高度な構成オプションを使用してネットワークモデルを構築します。

次のタスク

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、コレクションの編集 （34 ページ）を参照してください。

SR- PCE エージェントとコレクタ

SR-PCE エージェントと SR-PCE コレクタは、SR-PCE サーバーとネットワーク間の通信およびテレメトリ データ コレクションを可能にする Cisco Crosswork Planning コンポーネントです。

SR-PCE agent

SR-PCE エージェントは Cisco Crosswork Planning コンポーネントであり、

- 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し、
- LSP データ収集向けとトポロジ データ コレクション向けの 2 つの異なる REST 接続を SR-PCE を併用します。
- 必要に応じて、SR-PCE をサブスクライブして、トポロジと LSP データを収集した後に、さらなるネットワーク変更イベントをリッスンします。

SR-PCE collector

SR-PCE コレクタは、Cisco Crosswork Planning コンポーネントで、

- IGP メトリック、遅延、およびノードオーバーロードの変更へのネットワーク更新をキャプチャします。
- FlexAlgoAffinities、FlexAlgorithms、SRv6NodeSIDs、SRv6InterfaceSIDs、NodePrefixLoopbacks、NodeSIDPrefixLoopbacks テーブルにデータが入力されます。
- 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。

SR-PCE は、SRv6NodeSIDPrefixLoopbacks テーブルに関連付けられません。これは、SRv6 に関連付けられているループバックアドレスが、SR-PCE を使用して取得されないためです。SRv6NodeSIDPrefixLoopbacks 詳細を入力するには、コレクタの構成中に外部スクリプトを追加します。それ以外の場合、SRv6NodeSID から NodePrefixLoopbacks へのクロステーブルフィルタは Cisco Crosswork Planning Design アプリケーションに結果を表示しません。外部スクリプトの実行の詳細については、「ネットワークモデルに対する外部スクリプトの実行 （115 ページ）」を参照してください。

トポロジディスカバリのメソッド

このトポロジディスカバリから得られるネットワークモデルは、追加のコレクションの送信元ネットワークとして使用されます。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します。

トポロジとインターフェイスまたはポートのプロパティは、2 つの方法で検出できます。

- SNMP の使用：詳細なノード、インターフェイス、またはポートのプロパティを取得するため、ネットワーク検出に推奨されます。
- SR-PCE のみを使用（[拡張ディスカバリ（Extended discovery）] フィールドを無効）：テスト、または SNMP が利用できない場合に役立ちます。

SR-PCE トポロジコレクションに関する重要な注意事項

- デフォルトでは、NodePrefixLoopbacks の ISIS レベルは [level2] に設定されています。OSPF ネットワークは同じ値を使用します。
- Cisco Crosswork Planning は、[FlexAlgo] 列の null 以外の値から null 値への更新を反映しません。更新された値の反映は、DARE 再同期後に開始されます。
- データ収集中、デュアルスタックサポート（IPv4 と IPv6 の両方を同時処理する機能）およびインターフェイスの OSPF または ISIS 構成は、正確に入力されます。ただし、OSPF と ISIS の両方は、データ収集の単一インターフェイスで有効になり、デュアルスタックとそのインターフェイス解決は、SR-PCE コレクション中にサポートされません。
- 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 メトリック値も同じ方法で更新されます。
- SR-PCE コレクタは、インターフェイスのアプリケーション固有リンク属性（ASLA）遅延情報を収集でき、通常はリアルタイムで、この情報を更新します。ただし、コレクタが 1 分以内に SR-PCE から複数の連続したトポロジ更新イベントを受信した場合、次のコレクション中にのみ変更を記録する場合があります。まれに、SR-PCE エージェントを手動で再起動した後にのみ更新が有効になることがあります。

SR-PCE コレクタを構成して、ストア登録情報情報を収集する

このトピックでは、**SR-PCE** コレクタを構成して、SR-PCE を使用してレイヤ 3 トポロジ情報を収集する方法について説明します。

SR-PCE コレクタを設定するには、次の手順を実行します。

Before you begin

- 事前構成ワークフロー （11 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、実行されていることを確認します。エージェント設定の詳細については、「エージェントの構成 （22 ページ）」を参照してください。

手順

ステップ 1 新しいコレクションを作成するか、既存のコレクションを編集するかを決定します。詳細については、コレクションの設定 （30 ページ）またはコレクションの編集 （34 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]** 、**[次へ（Next）]** の順に選択します。

ステップ 3 [構成（Configure）] ページで、次の構成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。
- **[SR-PCEホストをバックアップ（Backup SR-PCE host）]**：バックアップ SR-PCE エージェントを選択します。バックアップが無い場合は、このフィールドを空欄にします。同じ SR-PCE エージェントを **SR-PCE ホスト** および **Backup SR-PCE ホスト**の両方に使用しないようにします。
- **[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。
- **[コレクションをトリガー（Trigger Collection）]**：新しいトポロジの追加（ノードまたはリンク）時にトポロジコレクションを収集するには、**[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）]** パネルを展開して、必要に応じて、その他の関連する高度なフィールドを構成します。詳細オプションの説明については、IGP および SR-PCE コレクションの詳細オプション （72 ページ）を参照してください。

ステップ 5 **[次へ（Next）]** をクリックして続行します。

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。

ステップ 7 収集ジョブのスケジュールを設定します。コレクション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、「コレクションのスケジュール （36 ページ）」を参照してください。

SR-PCE コレクタは、トポロジディスカバリを開始し、レイヤ 3 トポロジ情報を収集し、収集したデータを使用してネットワークモデルを更新します。

次のタスク

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、コレクションの編集 （34 ページ）を参照してください。

IGP および SR-PCE コレクションの詳細オプション

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。

表 *6 : IGP* および *SR-PCE* コレクションの詳細オプション

オプション	説明
Options applicable for both IGP and SR-PCE collection:	
ノード	
ノードパフォーマンスの収集	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	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	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。
データ収集タイムアウト	データ収集に許可される最大時間を分単位で設定します。指定された制限を超える場合は、データ収集に使用する内部ツールがタイムアウトとなり、終了します。デフォルトは 60 分です。
QoS ノードフィルタ	フィルタを定義して、QoS データが収集されるノードを決定します。
インターフェイス	
パラレルリンクの検索	IS-IS TE 拡張機能が有効になっていない場合、IGP データベースに存在しない並列リンクを検索します。

オプション	説明
IP 推測	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。この設定は、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。 • OFF：推論は実行されません。 • Safe：あいまいさが無い場合のみ推論を行います。 • FULL：あいまいさがあっても最善の推論行います。
ポート LAG 検出	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	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。 • 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。 • Exact：LACP に基づいた照合。 • 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。 • None：ポート回路を作成しません。
回路のクリーンアップ	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	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	シスコデバイスに関する L3 物理ポートを収集します。
最小 IP 推測	IP 推論の最小プレフィックス長を指定します。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	並列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	データ収集に許可される最大時間を分単位で設定します。指定された制限を超える場合は、データ収集に使用する内部ツールがタイムアウトとなり、終了します。デフォルトは 60 分です。
デバッグ	

オプション	説明
冗長	ログメッセージの詳細レベルを設定します。デフォルト値は30で、有効な範囲は 1 ～ 60 です。
ネットレコーダー	SNMP メッセージを録音します。オプションは、[オフ（Off）]、[録音（Record）]、および [再生（Playback）] です。デフォルトはオフです。 • [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ます。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、ネットワークコレクションのオフラインデバッグが可能です。 • [オフ（Off）]：録音や再生は実行されません。
Option applicable only for SR-PCE collection:	
シングルエンド eBGP 検出	リンクエンドが 1 つしかない eBGP リンクを検出します。このようなシナリオは一般的ではありません。

LSP 情報の収集

このトピックでは、**LSP** コレクタを構成して、SNMP を使用してネットワーク内の RSVP LSP 情報を収集する方法について説明します。

Before you begin

事前構成ワークフロー （11 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 新しいコレクションを作成するか、既存のコレクションを編集するかを決定します。詳細については、コレクションの設定 （30 ページ）またはコレクションの編集 （34 ページ）を参照してください。

ステップ 2 コレクション構成チェーンの最初の手順として外部スクリプトを使用する場合は、[スタートアップスクリプト（Startup Script）] オプションを選択します。（オプション）スタートアップスクリプトを選択した場合は、Basic Topology コレクタをスキップするか、スタートアップスクリプトをソースとして構成します。スタートアップスクリプトを使用しない場合は、必要に応じて、いずれかの Basic Topology コレクタを選択する必要があります。

ステップ 3 **[高度なモデリング（Advanced Modeling）]** セクションで、**[LSP]**、**[次へ（Next）]** の順に選択します。

ステップ 4 [構成（Configure）] ページの左側にある **[選択されたコレクタ（Selected Collectors）]** ペインで **[LSP]** をクリックします。

（注）
basic topology 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 次の構成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を取得（Get FRR LSPs）]**：MPLS Fast Reroute (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 コレクションの詳細オプション （75 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。

ステップ 9 収集ジョブのスケジュールを設定します。コレクション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、「コレクションのスケジュール （36 ページ）」を参照してください。

LSP コレクタが設定され、構成に基づいてスケジュールされます。

次のタスク

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、コレクションの編集 （34 ページ）を参照してください。

LSP コレクションの詳細オプション

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。

表 *7: LSP* コレクションの詳細オプション

オプション	説明
計算されたホップを使用	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	LSP の実際のパスを検出します。
追加情報の入手	追加の LSP プロパティを収集します。

オプション	説明
シグナル名の使用	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。 （注） Config parsing と LSP コレクタの併用時に、シグナル名を取得するには、かならず LSP コレクタを実行してから、Config parsing コレクタを実行します。この順序を守らないと、Config parsing が収集した LSP トンネル名が、LSP コレクタが収集したシグナル名値で置き換えられます。
自動帯域幅	自動帯域幅を検出します。
データ収集タイムアウト	データ収集に許可される最大時間を分単位で設定します。指定された制限を超える場合は、データ収集に使用する内部ツールがタイムアウトとなり、終了します。デフォルトは 60 分です。
デバッグ	
冗長	ログメッセージの詳細レベルを設定します。デフォルト値は30で、有効な範囲は 1 ～ 60 です。
ネットレコーダー	SNMP メッセージを録音します。オプションは、[オフ（Off）]、[録音（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ます。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、ネットワークコレクションのオフラインデバッグが可能です。 • [オフ（Off）] : 録音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

このトピックでは、**PCEP LSP** コレクタの構成方法について説明します。

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、新しく強化されたネットワークモデルを作成します。

始める前に

- 事前構成ワークフロー （11 ページ）に記載されている手順を実行します。

- SR-PCE コレクタを使用してネットワークの BGP-LS トポロジコレクションを完了します。LSP 情報収集用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 コレクタを構成して、ストア登録情報情報を収集する （70 ページ）を参照してください。

手順

ステップ 1 新しいコレクションを作成するか、既存のコレクションを編集するかを決定します。詳細については、コレクションの設定 （30 ページ）またはコレクションの編集 （34 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]**、**[次へ（Next）]** の順に選択します。

ステップ 4 [構成（Configure）] ページの左側にある **[選択されたコレクタ（Selected Collectors）]** ペインで **[PCEP LSP]** をクリックします。

（注）
basic topology 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 次の構成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で 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、エージェントの構成 （22 ページ）を参照してください。

  （注）
  複数の SR-PCE エージェントを使用する場合は、コレクタが各エージェントに対して処理するデータ量に応じて、追加の各エージェントが、実行時間全体を延長する場合があるのでご注意ください。この点を考慮して、複数のエージェントの選択時に最適なパフォーマンスを確保します。

- **[リアクティブネットワーク（Reactive Network）]**：**[有効（Enabled）]** チェックボックスをオンにすると、リアルタイム LSP 更新に関する SR-PCE から通知をサブスクライブできます。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使用シグナル名（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使用シグナル名（RSVP 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追加インデックス（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（分単位）。指定された制限を超える場合は、データ収集に使用する内部ツールがタイムアウトとなり、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。

ステップ 9 収集ジョブのスケジュールを設定します。コレクション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、「コレクションのスケジュール （36 ページ）」を参照してください。

PCEP LSP 情報が収集され、既存の SR-PCE トポロジに追加され、詳細な LSP データを含む更新されたネットワークモデルが生成されます。

次のタスク

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、コレクションの編集 （34 ページ）を参照してください。

ネットワークからマルチキャストフローデータを収集する

このトピックでは、**Multicast** コレクタを構成してネットワークからマルチキャストフローデータを収集する方法について説明します。

Multicast コレクタには、次のコレクタが含まれます：

- [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情報を収集します。
- [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レートデータを収集します。

始める前に

事前構成ワークフロー （11 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 新しいコレクションを作成するか、既存のコレクションを編集するかを決定します。詳細については、コレクションの設定 （30 ページ）またはコレクションの編集 （34 ページ）を参照してください。

ステップ 2 コレクション構成チェーンの最初の手順として外部スクリプトを使用する場合は、[スタートアップスクリプ（Startup Script）] オプションを選択します。（オプション）スタートアップスクリプトを選択した場合は、Basic Topology コレクタをスキップするか、スタートアップスクリプトをソースとして構成します。スタートアップスクリプトを使用しない場合は、必要に応じて、いずれかの Basic Topology コレクタを選択する必要があります。

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）]**、**[次へ（Next）]** の順に選択します。

ステップ 4 [構成（Configure）] ページの左側の **[選択したコレクタ（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）
basic topology 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 次の構成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。
- **データ収集送信元**：使用するコレクタを選択してマルチキャストデータを収集します。オプションには、[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）] があります。

ステップ 6 （オプション）***[コレクタ（Collector）]***、**[設定（Settings）]** パネルに順に展開し、関連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よって、オプションは異なります。詳細オプションの説明については、Multicast コレクションの詳細オプション （80 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。

ステップ 9 収集ジョブのスケジュールを設定します。コレクション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、「コレクションのスケジュール （36 ページ）」を参照してください。

Multicast コレクタが構成されます。指定に従ってネットワークからマルチキャストフローデータの収集を開始します。

次のタスク

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、コレクションの編集 （34 ページ）を参照してください。

Multicast コレクションの詳細オプション

Multicast 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。

表 *8 : Multicast* コレクションの詳細オプション

オプション	説明
ログイン検出設定	
データ収集タイムアウト	データ収集に許可される最大時間を分単位で設定します。指定された制限を超える場合は、データ収集に使用する内部ツールがタイムアウトとなり、終了します。デフォルトは 30 分です。
既存の設定を使用	キャッシュに保管されている既存のマルチキャスト構成データを使用します。
設定の強制更新	マルチキャスト構成ファイルがキャッシュにある場合でも、更新します。
設定の保存	キャッシュにマルチキャスト構成を保存するか、未選択の場合は、破棄します。
ファイルの上書き	既存の構成ファイルを上書きします。
ログインポーリング設定	
データ収集タイムアウト	データ収集に許可される最大時間を分単位で設定します。指定された制限を超える場合は、データ収集に使用する内部ツールがタイムアウトとなり、終了します。デフォルトは 30 分です。
サンプル数	ポーリング中に収集するデータサンプルの数を設定します。
ポーリング間隔	秒単位でログインレート読み込みの間隔を設定します。
トラフィックレベル名	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	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定義します。
既存の設定を使用	キャッシュに保管されている既存のマルチキャスト構成データを使用します。

オプション	説明
設定の強制更新	マルチキャスト構成ファイルがキャッシュにある場合でも、更新します。
設定の保存	キャッシュにマルチキャスト構成を保存するか、未選択の場合は、破棄します。
ファイルの上書き	既存の構成ファイルを上書きします。
SNMP 検出設定	
データ収集タイムアウト	データ収集に許可される最大時間を分単位で設定します。指定された制限を超える場合は、データ収集に使用する内部ツールがタイムアウトとなり、終了します。デフォルトは 30 分です。
SNMP ポーリング設定	
データ収集タイムアウト	データ収集に許可される最大時間を分単位で設定します。指定された制限を超える場合は、データ収集に使用する内部ツールがタイムアウトとなり、終了します。デフォルトは 30 分です。
サンプル数	ポーリング中に収集するデータサンプルの数を設定します。
ポーリング間隔	秒単位でログインレート読み込みの間隔を設定します。
トラフィックレベル名	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	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定義します。
デバッグ	
冗長	ログメッセージの詳細レベルを設定します。デフォルト値は30で、有効な範囲は 1 ～ 60 です。
ネットレコーダー	SNMP メッセージを録音します。オプションは、[オフ（Off）]、[録音（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ます。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、ネットワークコレクションのオフラインデバッグが可能です。 • [オフ（Off）] : 録音や再生は実行されません。

BGP ピアリングの検出

このトピックでは、**BGP** コレクタを構成して、SNMP と ログインを使用する BGP トポロジを検出する方法について説明します。

BGPコレクタは、送信元ネットワークとしてトポロジネットワーク（一般的には、IGPコレクタ出力）を使用し、BGP リンクを外部 ASN ノードに追加します。

Before you begin

事前構成ワークフロー （11 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 新しいコレクションを作成するか、既存のコレクションを編集するかを決定します。詳細については、コレクションの設定 （30 ページ）またはコレクションの編集 （34 ページ）を参照してください。

ステップ 2 コレクション構成チェーンの最初の手順として外部スクリプトを使用する場合は、[スタートアップスクリプ（Startup Script）] オプションを選択します。（オプション）スタートアップスクリプトを選択した場合は、Basic Topology コレクタをスキップするか、スタートアップスクリプトをソースとして構成します。スタートアップスクリプトを使用しない場合は、必要に応じて、いずれかの Basic Topology コレクタを選択する必要があります。

ステップ 3 **[高度なモデリング（Advanced Modeling）]** セクションで、**[BGP][次へ（Next）]** の順に選択します。

ステップ 4 [構成（Configure）] ページの左側にある **[選択されたコレクタ（Selected Collectors）]** ペインで **[BGP]** をクリックします。

（注）
basic topology 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 **[送信元（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送信元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）]** パネルを展開して、必要に応じて、その他の関連する高度なフィールドを構成します。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 （83 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。

ステップ 9 収集ジョブのスケジュールを設定します。コレクション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、「コレクションのスケジュール （36 ページ）」を参照してください。

これで、BGP コレクタが構成され、SNMP と ログインを使用する BGP トポロジを検出できるようになります。

次のタスク

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、コレクションの編集 （34 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。

表 *9 : BGP* トポロジコレクションの詳細オプション

オプション	説明
ASN を含める	含める ASN を指定します。デフォルトでは、すべての ASN が含まれます。
内部 ASN	内部 ASN を指定します。
プロトコル	Internet Protocol（IP）のバージョンを指定します。IPv4またはIPv6を選択できます。
最小 IPv4 プレフィックス長	BGP リンクとしてインターフェイスを検出する際に、サブネットの一致をどの程度厳密に制御するかを指定する IPv4 最小プレフィックス長を指定します。
最小 IPv6 プレフィックス長	BGP リンクとしてインターフェイスを検出する際に、サブネットの一致をどの程度厳密に制御するかを指定する IPv6 最小プレフィックス長を指定します。
ログインマルチホップ	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指定します。
強制ログインプラットフォーム	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。有効な値は、cisco、juniper、alu、huawei です。
フォールバック ログイン プラットフォーム	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設定します。有効な値は、cisco、juniper、alu、huawei です。
enable の送信を試す	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。これにより、セカンダリ「有効化パスワード」を必要とするデバイスで構成を取得または修正するために必要な上位レベルのアクセス権が付与されます。
Telnet ユーザー名プロンプト	Telnet の代替ユーザー名プロンプトを指定します。

オプション	説明
Telnet パスワードプロンプト	Telnet の代替パスワードプロンプトを指定します。
内部 ASN リンクの検索	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	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	内部 ASN への BGP リンクを検出します。
MAC アドレスの取得	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	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	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	データ収集に許可される最大時間を分単位で設定します。指定された制限を超える場合は、データ収集に使用する内部ツールがタイムアウトとなり、終了します。デフォルトは 60 分です。
デバッグ	
冗長	ログメッセージの詳細レベルを設定します。デフォルト値は 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	SNMP メッセージを録音します。オプションは、[オフ（Off）]、[録音（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ます。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、ネットワークコレクションのオフラインデバッグが可能です。 • [オフ（Off）]：録音や再生は実行されません。
ログインレコードモード	検出プロセスを記録します。オプションは、[オフ（Off）]、[録音（Record）]、および [再生（Playback）] です。デフォルトはオフです。 • [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、ツール実行時に内部で録音されます。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ツールを介して再生されるため、ネットワークコレクションのオフラインデバッグが可能です。 • [オフ（Off）]：録音や再生は実行されません。

VPN トポロジの検出

このトピックでは、**VPN** コレクタを構成して、レイヤ 2 およびレイヤ 3 VPN トポロジを検出する方法について説明します。

（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

事前構成ワークフロー （11 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 新しいコレクションを作成するか、既存のコレクションを編集するかを決定します。詳細については、コレクションの設定 （30 ページ）またはコレクションの編集 （34 ページ）を参照してください。

ステップ 2 コレクション構成チェーンの最初の手順として外部スクリプトを使用する場合は、[スタートアップスクリプ（Startup Script）] オプションを選択します。（オプション）スタートアップスクリプトを選択した場合は、Basic Topology コレクタをスキップするか、スタートアップスクリプトをソースとして構成します。スタートアップスクリプトを使用しない場合は、必要に応じて、いずれかの Basic Topology コレクタを選択する必要があります。

ステップ 3 **[高度なモデリング（Advanced Modeling）]** セクションで、**[VPN]**、**[次へ（Next）]** の順に選択します。

ステップ 4 [構成（Configure）] ページの左側にある **[選択されたコレクタ（Selected Collectors）]** ペインで **[VPN]** をクリックします。

（注）
basic topology 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 次の構成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）]** パネルを展開して、必要に応じて、その他の関連する高度なフィールドを構成します。

表 *10 : LSP* コレクションの詳細オプション

オプション	説明
データ収集タイムアウト	データ収集に許可される最大時間を分単位で設定します。指定された制限を超える場合は、データ収集に使用する内部ツールがタイムアウトとなり、終了します。デフォルトは 60 分です。
冗長	ログメッセージの詳細レベルを設定します。デフォルト値は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	SNMP メッセージを録音します。オプションは、[オフ（Off）]、[録音（Record）]、および [再生（Playback）] です。デフォルトはオフです。 • [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ます。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、ネットワークコレクションのオフラインデバッグが可能です。 • [オフ（Off）]：録音や再生は実行されません。

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。

ステップ 9 収集ジョブのスケジュールを設定します。コレクション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、「コレクションのスケジュール （36 ページ）」を参照してください。

これで、VPN コレクタが構成されます。

次のタスク

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、コレクションの編集 （34 ページ）を参照してください。

インベントリコレクタとハードウェアテーブル

Inventory コレクタは、Cisco Crosswork Planning コンポーネントで、

- ハードウェア一覧情報をネットワークデバイスから収集します。
- ハードウェアの種類に基づいて構造化されたテーブル（NetIntHardware*）で収集されたデータを保管します。

これらの項では、一覧コレクタを使用して、ハードウェア一覧情報を収集して整理するためのプロセス、コンポーネント、構成テーブル、ベストプラクティスについて説明します。

NetIntHardware テーブル

NetIntHardware* テーブルは、ハードウェアの種類に基づいて収集されたハードウェア情報を格納します。

NetIntHardware テーブルの例をいくつか示します。

- NetIntHardwareChassis：ノード IP アドレスと SNMP ID が特定したルータシャーシオブジェクトを格納します。
- NetIntHardwareContainer：ルータのスロットエントリを格納します（Field Replaceable Unit（FRU）タイプのデバイスをインストールできるあらゆるもの）。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：別のハードウェアデバイスにインストールできるハードウェアデバイスの情報を格納します。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：ルータの物理的なポートを格納します。

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。シャーシを除き、すべてのオブジェクトには 1 つの親オブジェクトがあり、複数の子オブジェクトを持つことができます。ポートや空のコンテナなど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。ハードウェア階層は通常、ハードウェアオブジェクトが別のオブジェクトにインストールされる方法を反映します。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 [ノード（Node）]（ノード IP アドレス）列と併用すると、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：

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（Node）	**SnmpID**	**ParentID**	**モデル（Model）**	**[名前（Name）]**	**NumChildren**	**ParentTable**	**SlotNumber**
172.23.123.456	2503733	2512347		slot mau 0/0/0/5	0	NetIntHardware シャーシ	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。一覧コレクタは、このトレースを使用してハードウェアデバイスの処理方法を判断します。このプロセスは、エントリを HWInventoryTemplates テーブルに追加する際に使用する必要があります。

NetIntNodeInventory 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 テーブルのデバイスを分類するエントリを含み、含まれた状態からプルーニングします。
  - 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。

HWInventoryTemplates テーブルと HWNameFormatRules テーブル

[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。

一覧コレクタは、HWInventoryTemplates テーブルのこれらの列を NetIntHardware* との一致を確認するために、以下の順序で参照します。

- 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。

1. Type は、検出されたハードウェアタイプ（「コンテナ」など）です。
2. 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、...）。
3. 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 テーブルの列の見出しです。

複数の [名前送信元（name source）] 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、一覧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の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。

1. 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。
2. 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。

3. 「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

[一覧構築オプション（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	**ベンダー**	**モデル（Model）**	**[名前（Name）]**
NetIntHardwarePort	シスコ		\/CPU0\/129$
NetIntHardwareModule	シスコ	800-12308-02	
NetIntHardwarePort	シスコ		管理

テーブルエントリ関数は、次のとおりです。

- 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

[一覧の構築オプション（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（Model）**	**TotSlot**	**SlotNum**
シスコ	シャーシ	7609	9	1–9

インベントリコレクションの設定

このトピックでは、**Inventory** コレクタの構成方法について説明します。

始める前に

事前構成ワークフロー （11 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 新しいコレクションを作成するか、既存のコレクションを編集するかを決定します。詳細については、コレクションの設定 （30 ページ）またはコレクションの編集 （34 ページ）を参照してください。

ステップ 2 コレクション構成チェーンの最初の手順として外部スクリプトを使用する場合は、[スタートアップスクリプト（Startup Script）] オプションを選択します。（オプション）スタートアップスクリプトを選択した場合は、Basic Topology コレクタをスキップするか、スタートアップスクリプトをソースとして構成します。スタートアップスクリプトを使用しない場合は、必要に応じて、いずれかの Basic Topology コレクタを選択する必要があります。

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）]**、**[次へ（Next）]** の順に選択します。

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）
basic topology 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 **[送信元（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送信元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）]** パネルを展開して、必要に応じて、その他の関連する高度なフィールドを構成します。詳細オプションの説明については、一覧コレクションの高度なオプション （94 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。

ステップ 9 収集ジョブのスケジュールを設定します。コレクション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、「コレクションのスケジュール （36 ページ）」を参照してください。

Inventory コレクタが設定に基づいて構成されます。

次のタスク

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、コレクションの編集 （34 ページ）を参照してください。

一覧コレクションの高度なオプション

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。

表 *11*：一覧コレクションの高度なオプション

オプション	説明
Get inventory options	
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。
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分単位で設定します。指定された制限を超える場合は、データ収集に使用する内部ツールがタイムアウトとなり、終了します。デフォルトは30分です。
Build inventory options	
除外ファイル（Exclude Files）	ExcludeHWList テーブルを含むファイルを選択できます。このテーブルは、出力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、**[サンプルファイルをダウンロード（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）	未加工の一覧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。

オプション	説明
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 ファイルを選択できるようにします。 [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）	HardwareSpec テーブルを含むファイルを選択できるようにします。このテーブルは、具体的なハードウェアの種類のスロット数を定義し、ルータから返された SNMP データを検証します。 HardwareSpec を含むサンプルファイルをダウンロードするには、**[サンプルファイルをダウンロード（Download sample file）]** リンクをクリックします。
デバッグ	
冗長	ログメッセージの詳細レベルを設定します。デフォルト値は 30 で、有効な範囲は 1 ～ 60 です。
ネットレコーダー	SNMP メッセージを録音します。オプションは、[オフ（Off）]、[録音（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ます。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、ネットワークコレクションのオフラインデバッグが可能です。 • [オフ（Off）]：録音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

このトピックでは、**Config parsing** コレクタを構成して、ポート、LSP、SRLG、および VPN 情報を収集する方法について説明します。

（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、他のコレクション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

事前構成ワークフロー （11 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 新しいコレクションを作成するか、既存のコレクションを編集するかを決定します。詳細については、コレクションの設定 （30 ページ）またはコレクションの編集 （34 ページ）を参照してください。

ステップ 2 コレクション構成チェーンの最初の手順として外部スクリプトを使用する場合は、[スタートアップスクリプ（Startup Script）] オプションを選択します。（オプション）スタートアップスクリプトを選択した場合は、Basic Topology コレクタをスキップするか、スタートアップスクリプトをソースとして構成します。スタートアップスクリプトを使用しない場合は、必要に応じて、いずれかの Basic Topology コレクタを選択する必要があります。

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）]**、**[次へ（Next）]** の順に選択します。

ステップ 4 [構成（Configure）] ページの左側にある **[選択されたコレクタ（Selected Collectors）]** ペインで **[構成解析（Config Parsing）]** をクリックします。

（注）
basic topology 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 **[送信元（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送信元コレクタを選択します。

ステップ 6 **[構成を取得（Get config）]**、**[構成を解析（Parse config）]** パネルの順に展開します。該当するフィールドに、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 （97 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。
- Config Parsing 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。
- Config Parsing コレクタと VPN コレクタの両方が VPN 情報を収集する場合は、コレクタチェーン内で、VPN コレクタが Config Parsing コレクタの前で実行されてい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 テーブルでは、これらのエントリは更新されません。

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。

ステップ 9 収集ジョブのスケジュールを設定します。コレクション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、「コレクションのスケジュール （36 ページ）」を参照してください。

次のタスク

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、コレクションの編集 （34 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。

表 *12 :* 構成解析の詳細オプション

オプション	説明
Get config options	
収集の構成	デバイスまたはルータから構成詳細を取得します。
強制ログインプラットフォーム	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。有効な値は、cisco、juniper、alu、huawei です。
フォールバック ログイン プラットフォーム	プラットフォームの検出が失敗した場合、フォールバックベンダーを設定します。有効な値は、cisco、juniper、alu、huawei です。
enable の送信を試す	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。これにより、セカンダリ「有効化パスワード」を必要とするデバイスで構成を取得または修正するために必要な上位レベルのアクセス権が付与されます。
Telnet ユーザー名プロンプト	Telnet の代替ユーザー名プロンプトを指定します。
Telnet パスワードプロンプト	Telnet の代替パスワードプロンプトを指定します。
データ収集タイムアウト	データ収集に許可される最大時間を分単位で設定します。指定された制限を超える場合は、データ収集に使用する内部ツールがタイムアウトとなり、終了します。デフォルトは 60 分です。
Parse config options	

オプション	説明
プロトコル タイプ	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るようにします。オプションは、isis、ospfおよびNoneです。デフォルトは [IS-IS] です。
IS-IS レベル	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、またはその両方を読み取れます。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統合し、レベル 2 を優先させます。
OSPF エリア	1 つの OSPF エリアを収集するか、すべてのエリアを収集するかを指定します。[エリアID（area ID）] または [すべて（all）] を指定します。デフォルトは area 0 です。
ASN	収集する ASN を指定します。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。
オブジェクトを含める	解析する設定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、CS RSVP、VPN、FRR、SR LSPS、LMP、および SR ポリシーです。
回路の一致	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	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制御します。 • 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。 • None：ポート回路を作成しません。
OSPF プロセス 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 を指定します。
IS-IS インスタンス 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 を指定します。
ループバック インターフェイス	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	解析中に IP アドレスリファレンスの解決を有効にします。
マルチスレッディング	構成ファイルのマルチスレッディング プロセスを有効化し、解析を高速化します。

オプション	説明
show コマンドのフィルタ処理	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	構成を解析後、ネットワークトポロジを構築します。
共有メディア	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	データ収集に許可される最大時間を分単位で設定します。指定された制限を超える場合は、データ収集に使用する内部ツールがタイムアウトとなり、終了します。デフォルトは60分です。
デバッグ	
冗長	ログメッセージの詳細レベルを設定します。デフォルト値は30で、有効な範囲は 1 ～ 60 です。
ネットレコーダー	SNMPメッセージを録音します。オプションは、[オフ（Off）]、[録音（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ます。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、ネットワークコレクションのオフラインデバッグが可能です。 • [オフ（Off）]：録音や再生は実行されません。

回路型 RSVP- TE 情報の収集

このトピックでは、ネットワークデバイスから回路型 RSVP（CS-RSVP）LSP 情報を収集する方法について説明します。

回路型 RSVP（CS-RSVP）LSP は、同じエンドポイントを持つ 2 つの単方向 RSVP LSP をバンドルして双方向 RSVP LSP を形成する論理エンティティです。これにより、トラフィックはエンドポイント間で常に両方向に移動できます。

CS RSVP- TE データを収集するには、**LSP** および **Config parsing** コレクタを構成する必要があります。Config parsing コレクタは、ネットワーク内の各デバイスから構成データを収集し、そこから CS-RSVP データを解析するために必要です。収集が正常に実行されると、集約プランファイルにはデバイスから収集された CS-RSVP LSP の詳細が含まれます。

始める前に

- 事前構成ワークフロー （11 ページ）に記載されている手順を実行します。
- デバイスで次の構成を確認します。
  - **双方向** が有効になっている RSVP 構成。
  - **双方向**構成には、両方向で同じ **association id**、**source-address**、**global-id** が含まれます。
  - **双方向**構成は、**co-routed** として **association type** が指定されます。

手順

ステップ 1 新しいコレクションを作成するか、既存のコレクションを編集するかを決定します。詳細については、コレクションの設定 （30 ページ）またはコレクションの編集 （34 ページ）を参照してください。

ステップ 2 コレクション構成チェーンの最初の手順として外部スクリプトを使用する場合は、[スタートアップスクリプ（Startup Script）] オプションを選択します。（オプション）スタートアップスクリプトを選択した場合は、Basic Topology コレクタをスキップするか、スタートアップスクリプトをソースとして構成します。スタートアップスクリプトを使用しない場合は、必要に応じて、いずれかの Basic Topology コレクタを選択する必要があります。

ステップ 3 **[高度なモデリング（Advanced modeling）]** セクションで、**LSP** および **Config parsing** コレクタを選択します。次に、[Next] をクリックします。

ステップ 4 **LSP** と **Config parsing** の両方のコレクタを構成します。**[オブジェクトを含める（Include objects）]** ドロップダウンリストで **[RSVP] と [CS RSVP]** オプションを選択していることを確認します。このオプションは、**[構成解析（Config parsing）]** ページの **[構成を解析（Parse config）]** セクションで使用できます。

その他の LSP および Config parsing オプションの詳細については、「LSP 情報の収集 （74 ページ）」および「構成解析を使用したポート、LSP、SRLG、および VPN 情報の収集 （95 ページ）」を参照してください。

（注）
シグナル名を取得するには、かならず LSP コレクタを実行してから、Config parsing コレクタを実行します。この順序を守らないと、Config parsing が収集した LSP トンネル名が、LSP コレクタが収集したシグナル名値で置き換えられます。

ステップ 5 （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を構成します。詳細オプションの説明については、LSP コレクションの詳細オプション （75 ページ）を参照してください。

ステップ 6 [Next] をクリックします。

ステップ 7 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。

ステップ 8 収集ジョブのスケジュールを設定します。コレクション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、「コレクションのスケジュール （36 ページ）」を参照してください。

生成されるネットワークモデルには、CS-RSVP LSP の詳細が含まれます。

次のタスク

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、コレクションの編集 （34 ページ）を参照してください。

ネットワークモデルの可視性を向上させるために Layout コレクタを構成する

このトピックでは、**Layout** コレクタの構成方法について説明します。

Layout コレクタは、レイアウトプロパティを送信元ネットワークモデルに追加します。これにより、プロファイルを Cisco Crosswork Planning にインポートした際の可視性が向上します。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。

Before you begin

事前構成ワークフロー （11 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 新しいコレクションを作成するか、既存のコレクションを編集するかを決定します。詳細については、コレクションの設定 （30 ページ）またはコレクションの編集 （34 ページ）を参照してください。

ステップ 2 コレクション構成チェーンの最初の手順として外部スクリプトを使用する場合は、[スタートアップスクリプト（Startup Script）] オプションを選択します。（オプション）スタートアップスクリプトを選択した場合は、Basic Topology コレクタをスキップするか、スタートアップスクリプトをソースとして構成します。スタートアップスクリプトを使用しない場合は、必要に応じて、いずれかの Basic Topology コレクタを選択する必要があります。

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）]**、**[次へ（Next）]**の順に選択します。

ステップ 4 [構成（Configure）] ページの左側にある **[選択されたコレクタ（Selected Collectors）]** ペインで **[レイアウト（Layout）]** をクリックします。

（注）
basic topology 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 次の構成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）。指定された制限を超える場合は、データ収集に使用する内部ツールがタイムアウトとなり、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。

ステップ 9 収集ジョブのスケジュールを設定します。コレクション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、「コレクションのスケジュール （36 ページ）」を参照してください。

Layout コレクタが構成されます。

次のタスク

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、コレクションの編集 （34 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

このトピックでは、**Traffic collection** コレクタを構成する方法について説明します。

Traffic collection 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。**Traffic collection** コレクタを構成し、**[コレクタ（Collector）]** > **[エージェント（Agents）]** の順に選択すると、トラフィック ポーラー エージェントを表示できます。エージェント名とコレクション名は一致します。

（注） トラフィックコレクションの実行中、トラフィック詳細を計算するための十分なデータがないため、トラフィックデータは、プロファイルに入力されません。2 回目または 3 回目の実行開始時に、スケジュール期間、最短期間長、最長期間長に応じて、トラフィックデータがプロファイルに入力され始めます。

始める前に

- 事前構成ワークフロー （11 ページ）に記載されている手順を実行します。
- VPN トラフィックを取集するには、VPN ネットワークモデルが必要です。詳細については、「VPN トポロジの検出 （85 ページ）」を参照してください。
- LSP トラフィックを収集するには、LSP ネットワークモデルが必要です。詳細については、「LSP 情報の収集 （74 ページ）」を参照してください。

手順

ステップ 1 新しいコレクションを作成するか、既存のコレクションを編集するかを決定します。詳細については、コレクションの設定 （30 ページ）またはコレクションの編集 （34 ページ）を参照してください。

ステップ 2 コレクション構成チェーンの最初の手順として外部スクリプトを使用する場合は、[スタートアップスクリプ（Startup Script）] オプションを選択します。（オプション）スタートアップスクリプトを選択した場合は、Basic Topology コレクタをスキップするか、スタートアップスクリプトをソースとして構成します。スタートアップスクリプトを使用しない場合は、必要に応じて、いずれかの Basic Topology コレクタを選択する必要があります。

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、**[トラフィックコレクション（Traffic collection）]**、**[次へ（Next）]** の順に選択します。

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）
basic topology 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。

a) 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。
b) **[送信元（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送信元コレクタを選択します。

c) 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コレクション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 トラフィックコレクション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。

d) 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。

（注）
[LSP トラフィックポーリング（LSP 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すべての LSP 詳細があることを確認します。

e) 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。

f) （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、トラフィックコレクションの詳細オプション （105 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。

ステップ 7 収集ジョブのスケジュールを設定します。コレクション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、「コレクションのスケジュール （36 ページ）」を参照してください。

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。

トラフィック統計情報は、後続のスケジュールジョブ実行時に、生成されるプロファイルで収集、表示されます。

次のタスク

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、コレクションの編集 （34 ページ）を参照してください。

トラフィックコレクションの詳細オプション

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。

表 *13*: トラフィックコレクションの詳細オプション

オプション	説明
最短期間長	トラフィック計算の最短期間長を秒単位で指定します。デフォルトは 300 秒です。
最長期間長	トラフィック計算の最長期間長を秒単位で指定します。デフォルトは 450 秒です。
raw カウンタ TTL	生のカウンターデータが保持される期間を分単位で決定します。デフォルトは 15 分です。
キャパシティを超える分を破棄	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	ネットレコードファイルの最大サイズを指定します。
データ収集タイムアウト	データ収集に許可される最大時間を分単位で設定します。指定された制限を超える場合は、データ収集に使用する内部ツールがタイムアウトとなり、終了します。デフォルトは 60 分です。
デバッグ	
冗長	ログメッセージの詳細レベルを設定します。デフォルト値は 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	SNMP メッセージを録音します。オプションは、[オフ（Off）]、[録音（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ます。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、ネットワークコレクションのオフラインデバッグが可能です。 • [オフ（Off）] : 録音や再生は実行されません。

トラフィックポーラー設定の調整

このトピックでは、トラフィックポーリングを効率的に実行する方法について説明します。

トラフィックポーラーは、ネットワークから未処理のトラフィックカウンタを収集します。収集時間は、ネットワークサイズ、ネットワーク遅延、および個々のノードからの応答時間によって異なります。

手順

ステップ 1 **[トラフィックコレクション（Traffic collection）]** 構成ページで、トラフィックポーラーの冗長性を 40 に設定します。

ステップ 2 デフォルトのオプションで開始し、数時間連続収集を実行します。デフォルト値は次のとおりです。

```
Interface traffic poll > Polling period = 60
LSP traffic poll > Polling period = 60
Minimum window length = 300
Maximum window length = 450
Raw counter TTL = 15
```

ステップ 3 トラフィック コレクション スケジューラーを 300 秒ごとに実行するように設定する。

ステップ 4 showtech オプションを使用して、`continuous_poller_out.log` ファイルをダウンロードします。

a) メインメニューで、**[管理（Administration）]** > **[Crosswork Manager]** > **[Crosswork正常性（Crosswork Health）]** > **[コレクタ（Collector）]** の順に選択します。
b) **[マイクロサービス（Microservices）]** タブをクリックします。
c) **collection-service** で、[⋯]、**[ログを要求（Request logs）]** の順に選択します。
d) 生成された tar ファイルをダウンロードして、ログファイルを表示します。

ステップ 5 実際の収集時間を検索します。

例：

```
Info [40]: LSP Traffic Poller: Collection complete. Duration: 43.3 sec
Info [40]: Interface Traffic Poller: Collection complete. Duration: 42.7 sec
```

上記の例では、ポーラーがネットワークをポーリングできる最速のペースは約40～50秒です。この値は、インターフェイス トラフィック ポーリングと LSP トラフィック ポーリングの両方の最短ポーリング期間を表します。トラフィックポーラーはインターフェイスと LSP の両方のトラフィックを同時に入力するため、両方の値を同じ値に設定することをお勧めします。

トラフィックポーラーは、未処理のトラフィックカウンタ c1、c2 などを収集してトラフィックを計算します。トラフィックを計算するには、少なくとも 2 つのカウンタが必要です。

```
(c2.counter - c1.counter)/(c2.timestamp - c1.timestamp)
```

ポーラー構成のベストプラクティス

ポーラー構成を最適化し、信頼性の高いトラフィック データ コレクションを確保するには、次のベストプラクティスに従います。

- ポーラーには少なくとも 2 つのカウンタが必要なため、**[最短期間長（Minimum window length）]** を少なくとも [**2 * polling period**] に設定します。ネットワークのバリエーションに対応するには、期間長を 25% 以上増やします。

  最短期間長は、2 つのカウンタのサンプルに使用するスライディングウィンドウです。最も遠い2つのカウンタ、すなわち指定された期間の最新カウンタと最古カウンタを探します。この期間の平均トラフィックが計算されます。ポーラーには少なくとも2つのカウンタが必要であるため、最小値は少なくともポーリング期間の2倍である必要があります。

- **[最長期間長（Maximum window length）]** を、少なくとも [**2 * polling period**] に設定します。ネットワークのバリエーションに対応するには、期間長を 50% 以上増やします。応答しないノードの場合は、100% 以上で増やします。

  ネットワーク遅延またはノードの応答時間の増加により、最短期間長で、指定期間でカウンタが見つからなかった場合、ポーラーはN/Aとして報告されます。トラフィックデータが空になるのを避けるには、**[最長期間長（Maximum window length）]** と呼ばれる保険期間を使用します。

- **[未処理カウンタTTL（Raw counter TTL）]** を **[最長期間長（Maximum window length）]** 以上に設定します。

  トラフィックポーラーは、RAM 領域を使用するトラフィック計算のためにメモリに未処理のカウンタを保存します。トラフィックポーラーは、メモリに保存されている古いカウンタを定期的にクリーンアップします。システムは、未処理カウンタTTL（分）よりも古いカウンタデータを削除します。

- ポーラーメモリ使用率と、トラフィックの投入にかかった時間を監視します。トラフィックポーラーへのトラフィック投入とは、ネットワーク内のトラフィック計算プロセスとプランファイル更新プロセスです。所要時間はネットワークのサイズによって異なります。システムは、snmp-traffic-poller-service.log ファイルでトラフィック投入に用事田実際の時間をログに記録します。

サンプルログファイルからの行：

```
TrafficCalculatorRfs Did-52-Worker-46: - Traffic calculation took (ms) 379976
TrafficCalculatorRfs Did-52-Worker-46: - Traffic calculation took (ms) 391953
TrafficCalculatorRfs Did-52-Worker-46: - Traffic calculation took (ms) 388853
```

この例では、トラフィックを投入できる（他のツールによって消費される）最速のレートは約 400 秒です。

- snmp-traffic-poller-service.log ファイルに「無効なカウンタ」という警告が表示された場合、たとえば、c1.counter が c2.counter よりも大きいために負のトラフィックが発生する場合は、カウンタがリセットまたはオーバーフローした可能性があることに注意してください。この問題は 32 ビットのカウンタでよく発生します。このエラーが頻発する場合は、スライディングウィンドウのサイズを大きくしてより多くのカウンタを処理し、エラーの可能性を減らします。
- ただし、トラフィックを投入するよりも速いレートでネットワークをポーリングしないでください。上記の例では、最も積極的なポーリング設定は 50 秒ですが、トラフィック投入には約 400 秒かかります。これにより、8 つのネットワークポーリングが無駄になります。これを解決するには、トラフィックポーリング期間、スライディングウィンドウのサイズ、未処理カウンタ TTL を増やします。
  - この例の推奨構成は次のとおりです。
    1. 次の値を設定します。

```
Interface traffic poll > Polling period 180
LSP traffic poll enabled
LSP traffic poll > Polling period 180
Minimum window length 400
Maximum window length 800
Raw counter TTL 15
Data collection timeout 60
```

    2. 400 秒ごとに実行されるようにトラフィック コレクション スケジューラーを構成します。

（注） トラフィック投入に対するデータ収集のタイムアウトは 60 分に調整されています。このタイムアウトは通常は使用されないため、十分な長さにする必要があります。

  - これらの数値は、CPU リソースとネットワーク帯域幅を節約するために、あまり積極的にならないように調整できます。手順
    1. 次の値を設定します。

```
Interface traffic poll > Polling period 240
LSP traffic poll enabled
LSP traffic poll > Polling period 240
Minimum window length 600
Maximum window length 1200
Raw counter TTL 20
Data collection timeout 60
```

2. 600秒ごとに実行されるようにトラフィック コレクション スケジューラーを構成します。

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

事前構成ワークフロー （11 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 新しいコレクションを作成するか、既存のコレクションを編集するかを決定します。詳細については、コレクションの設定 （30 ページ）またはコレクションの編集 （34 ページ）を参照してください。

ステップ 2 コレクション構成チェーンの最初の手順として外部スクリプトを使用する場合は、[スタートアップスクリプト（Startup Script）] オプションを選択します。（オプション）スタートアップスクリプトを選択した場合は、Basic Topology コレクタをスキップするか、スタートアップスクリプトをソースとして構成します。スタートアップスクリプトを使用しない場合は、必要に応じて、いずれかの Basic Topology コレクタを選択する必要があります。

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）]**、**[次へ（Next）]** の順に選択します。

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）
basic topology 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 **[送信元（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送信元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。

[メッシュステップを追加（Add Mesh Step）] ページで、[次へ（Next）]の詳細を入力します。

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）]** フィールドで、このステップの実行順序を入力します。
c) **[ツール（Tool）]** ドロップダウンリストで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、コピーデマンド、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、[有効化（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。オプションは、選択したツールによって異なります。
f) （オプション）**[詳細（Advanced）]** パネルを展開し、関連する詳細を入力します。
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、[メッシュステップを追加（Add Mesh Step）] ページで、**[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。

ステップ 9 収集ジョブのスケジュールを設定します。コレクション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、「コレクションのスケジュール （36 ページ）」を参照してください。

デマンド推論コレクタを構成して、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。

次のタスク

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、コレクションの編集 （34 ページ）を参照してください。

NetFlow データ収集

NetFlow データ収集は、Cisco Crosswork Planning が以下を実行するプロセスです。

- ネットワークデバイスから NetFlow および関連するフロー測定値を収集する
- これらの測定値を集約して、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する
- 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する

NetFlow コレクタは、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。

（注） NetFlow コレクタが複数のコレクションの一部である場合、それらのコレクションを同時に実行することはできません。NetFlow コレクタはコレクションの同時実行をサポートしていないため、各コレクションは個別に実行する必要があります。

収集されるデータの種類

Cisco Crosswork Planning は、これらのタイプのデータを収集して、時間の経過とともに、集約したフローとそのトラフィック測定値を使用して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 経由で収集されたインターフェイス トラフィックと BGP ピア情報
- ピアリングセッション上の BGP パス属性

NetFlow コレクション構成の要件

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。

構成要件は次のとおりです。

- ルータを構成して、フローをエクスポートし、フローコレクションサーバーとの BGP ピアリングを確立する必要があります。
- NetFlow v5、v9、およびIPFIXデータグラムをフローコレクションサーバーのUDPポート番号にエクスポートします。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。これにより、サーバーの過剰なメモリ消費を防ぐことができます。AS パスを含め、単一の

IP プレフィックスに付加された BGP 属性の合計長は、最大 64 KB と非常に大きくなる可能性があります。

NetFlow コレクションの設定

このトピックでは、**NetFlow** コレクタの構成方法について説明します。

始める前に

- 事前構成ワークフロー （11 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エージェントが構成されているか確認します。

手順

ステップ 1 新しいコレクションを作成するか、既存のコレクションを編集するかを決定します。詳細については、コレクションの設定 （30 ページ）またはコレクションの編集 （34 ページ）を参照してください。

ステップ 2 コレクション構成チェーンの最初の手順として外部スクリプトを使用する場合は、[スタートアップスクリプト（Startup Script）] オプションを選択します。（オプション）スタートアップスクリプトを選択した場合は、Basic Topology コレクタをスキップするか、スタートアップスクリプトをソースとして構成します。スタートアップスクリプトを使用しない場合は、必要に応じて、いずれかの Basic Topology コレクタを選択する必要があります。

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][次へ（Next）]** の順に選択します。

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）
basic topology 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 次の構成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 **[イングレス時のASフローの分割（Split AS flows on ingress）]** ドロップダウンリストで、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 コレクションの詳細オプション （113 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）]**および**[デマンド（Demands）]**パネルを展開し、必要に応じて、その他の関連する詳細フィールドを構成します。各オプションの説明については、NetFlow コレクションの詳細オプション （113 ページ）を参照してください。次に、[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。

ステップ 9 収集ジョブのスケジュールを設定します。コレクション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、「コレクションのスケジュール （36 ページ）」を参照してください。

これで、NetFlow コレクション構成は完了です。

次のタスク

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、コレクションの編集 （34 ページ）を参照してください。

NetFlow コレクションの詳細オプション

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。

表 *14 : NetFlow* コレクションの詳細オプション

オプション	説明
共通構成	
入力時の AS フローの分割	外部ASNのトラフィック集約方法を指定します。複数の外部ASNが IXP スイッチに接続されている場合、すべての ASN からのトラフィックデータを集約するか、MAC アカウンティング入力トラフィックに比例して分散するかを決定します。
ASN	ネットワーク内の内部 AS の ASN を指定します。
アドレス ファミリ	含めるプロトコルバージョンのリストを指定します。カンマ区切りのリストとしてバージョンを入力します。
外部ノードタグ	1 つ以上のノードタグを入力できます。**[+]**をクリックして、複数のノードタグを追加します。
出力時の AS フローの分割	出力 AS に接続されたすべてのインターフェースを介してネットワークから出るときに Inter AS フローを分割します。
追加集約	ドロップダウンリストで追加の集約キーを選択できるようにします。

オプション	説明
ログ レベル（Log level）	ツールのログレベルを指定します。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	並列計算で使用するスレッドの最大数を指定します。
IAS フロー	
AS 間フローのトリム	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/秒単位で指定します。
BGP 外部情報の照合	BGP ピア関係の出力 IP アドレスを照合するかどうかを指定します。
入力インターフェイスフィルタ	ノードとインターフェイスのフィルタを Node:InterfaceName の形式で指定します。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	ノードとインターフェイスのフィルタを Node:InterfaceName の形式で指定します。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。
マイクロフローのバックトラック	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 フローとの関係を示すファイルを生成するかどうかを指定します。
フローインポート ID	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	IAS フロー計算のタイムアウトを分単位で指定します。有効な範囲は、1 ～ 1440 です。デフォルトは 60 分です。
デマンド	
デマンド名	新しいデマンドの名前を指定します。
デマンドタグ	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指定します。
デマンドのトリム	設定したしきい値を下回るデマンドを破棄します（Mbits/秒）。
デマンドサービスクラス	デマンドのサービスクラスを指定します。
デマンドトラフィックレベル	デマンドのトラフィッククラスを指定します。

オプション	説明
欠落しているフロー	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指定します。

ネットワークモデルに対する外部スクリプトの実行

このトピックでは、ネットワークモデルに対して外部スクリプトを実行する方法について説明します。

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。既存のコレクタを指定できないネットワークからのデータを指定する必要がある場合は、この機能を使用します。この場合、Cisco Crosswork Planning で作成された既存のコレクションモデルを取得し、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。

カスタムスクリプトの例については、「インターフェイスの説明を更新するためのサンプルスクリプト （118 ページ）」を参照してください。

Before you begin

- 事前構成ワークフロー （11 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およびサポートファイルを、指定されたファイル形式または圧縮アーカイブのいずれかで用意します。

（注） Cisco WAE でスクリプトを使用していて、それを Cisco Crosswork Planning で使用する場合は、修正を加えないと期待通りに動作しない場合があります。これは、さまざまなファイルの参照方法を含む Cisco WAE と Cisco Crosswork Planning のアーキテクチャの違いによるものです。Cisco Crosswork Planning で使用するには、適切にスクリプトを調整する必要があります。

手順

ステップ 1 新しいコレクションを作成するか、既存のコレクションを編集するかを決定します。詳細については、コレクションの設定 （30 ページ）またはコレクションの編集 （34 ページ）を参照してください。

ステップ 2 必要に応じて、基本ストア登録情報コレクタの 1 つを選択します。オプションで、ニーズに合った別の高度なコレクタを選択します。

ステップ 3 [構成（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 **[+外部スクリプトを追加（+ 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）]**：このコレクション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、**[プランファイルを入力（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。また、送信元として、DARE または SAgE アグリゲータを選択することもできます。SAgE が送信元のスクリプトは、SAgE 集約とアーカイブタスク後に実行されます。
- **[入力ファイル（Input file）]**：カスタムスクリプトと、その正常な実行に必要なサポートファイルをアップロードします。複数のファイルが必要な場合は、アップロードする前に、それらを 1 つのアーカイブに圧縮します。有効なフォーマットは、.py、.sh、.pl、.zip、.tar、.gz および .tar.gz です。

  （注）
  ファイルがアップロードされるたびに、入力ファイルオプションが上書きされます。

- **[実行可能なスクリプト（Executable script）]**：スクリプト実行プロセスを開始するファイル名を入力します。これは、**[入力ファイル（Input file）]** フィールドにアップロードされたファイルの 1 つです。

  外部スクリプトエグゼキュータは、カスタムスクリプトによる特定のファイルいおよびホームディレクトリを有効にするコマンドライン引数を指定します。引数は事前定義されており、特定の順序に従います。各引数が何を表すかを理解することは、適切な使用を確保するために重要です。

  以下は、引数の詳細です。

  - argv[1]：送信元のプランファイル
  - argv[2]：出力プランファイル
  - argv[3]：デバイスアクセス認証ファイル
  - argv[4]：グローバル ネットワーク アクセス構成ファイル
  - argv[5]：ホームディレクトリ
  - argv[6]：ユーザーがアップロードした外部ファイルが利用可能なパス
  - argv[7]：アーカイブ ルート ディレクトリにアクセスするパス

  Example:

  インターフェイスの説明を更新するためのサンプルスクリプト（118 ページ） は、「description.xlsx」という名前の Excel ファイルのデータに基づき、ネットワークの各インターフェイスに、「My IGP metric is *value*」という説明を追加します。パラメータは、description.xlsx ファイルのホームディレクトリパスを指定します。スクリプトを正常に実行するには、**[入力ファイル（Input file）]** フィールド経由でアップロードする前に圧縮ファイルに Excel ファイルを含める必要があります。

- **[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。

ステップ7 収集ジョブのスケジュールを設定します。コレクション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、「コレクションのスケジュール （36ページ）」を参照してください。

カスタムスクリプトは、選択したネットワークモデルに対して実行されます。

外部スクリプト経由での動的データファイルへのアクセス

process_summary

Cisco Crosswork Planningでは、データファイルをCisco Crosswork Planningコレクタに直接アップロードできます。外部スクリプトは、スクリプトの再パッケージ化または再デプロイを必要とせずに、実行時にこれらのファイルにアクセスできます。これにより、Cisco Crosswork Planningコレクタ内のスクリプトで、実行時にユーザーがアップロードした最新のファイルを使用できるようになり、より効率的なカスタマイズがサポートされます。

このプロセスに関与する主要なコンポーネントは次のとおりです。

- データファイルアップローダ：更新されたデータファイルをコレクタにアップロードします。
- アップロードディレクトリ：データファイルがアップロードされるディレクトリ。
- 外部スクリプト：実行中に、アップロードされたデータファイルを読み取ります。

process_workflow

これらは、外部スクリプトを介して動的データファイルにアクセスする段階です。

1. REST API（https://{{server-ip:port}}/cp/collection-service/api/v1/file-gateway）を使用して、更新されたデータファイルをCisco Crosswork Planningコレクタのアップロードディレクトリにアップロードします。
2. 外部スクリプトを実行し、コマンドライン引数としてアップロードディレクトリ内のデータファイルへのパスを指定します。argv[6]は、アップロードディレクトリのパスを表します。スクリプトの実行の詳細については、「ネットワークモデルに対する外部スクリプトの実行 （115ページ）」を参照してください。

（注） 同じファイルを複数回アップロードすると、既存のファイルが上書きされます。

3. スクリプトは、実行時にデータファイルの最新バージョンを読み取り、最新のデータを処理するようにします。

インターフェイスの説明を更新するためのサンプルスクリプト

このサンプル Python スクリプト read-from-excel.py は、Excel ファイル description.xlsx からのデータを使用して、「My IGP metric is <*value*>」という説明をネットワークの各インターフェイスに追加します。

スクリプトの内容

```
import sys
import openpyxl
import os
from com.cisco.wae.opm.network import Network

src = sys.argv[1]
dest = sys.argv[2]
home = sys.argv[5]
srcNet = Network(src)
excel_file = os.path.join(home, "description.xlsx")
wb = openpyxl.load_workbook(excel_file)
sheet = wb.active

row_count = 1
for node in srcNet.model.nodes:
    for iface in node.interfaces:
        cell_obj = sheet.cell(row=row_count, column=1)
        iface.description = 'My IGP metric is ' + str(cell_obj.value)
        row_count = row_count + 1
        print(iface.description)

srcNet.write(dest)
```

サードパーティデバイスからデータを収集する方法

process_summary

サポートモジュールは、収集対象と収集方法を決定する引数を受け取る実行可能なプログラムです。収集されたデータは、指定されたプランファイルを増やし、出力プランファイルを生成するために使用されます。

サポートモジュールは、以下を満たす必要があります。

- SNMP などのデータ収集機能を含める
- ポーリングするデバイスへのアクセスを認証ために認証ファイルの入力を許可する

- ネットワークアクセス構成ファイルの入力を許可して、タイムアウト、再試行、デバイスごとの最大要求数などの収集の詳細を管理する
- ファイルを読み取り、書き込み

これらはすべて、Python ライブラリのテンプレートとして提供されるサポート モジュール フレームワークを構成し、サードパーティ製デバイスからのデータ収集のプロセスを簡素化します。

process_workflow

次の段階では、サポートモジュールを使用してサードパーティ製デバイスからデータを収集する方法について説明します。

1. サポートモジュールの書き込みが完了したら、サポートモジュールの設定を使用してそれらをコレクタに統合します。
2. サポートモジュールのタイプ、実行可能なスクリプトを指定します。最も簡単な方法は、Python で記述できる実行可能ファイルを使用することです）。次に、スクリプトのパスを指定します。
3. コレクタは、サポートモジュールを実行するように実行を再編成します。

モジュール構成をサポートするコレクタ

サードパーティのサポートモジュール構成は、次のコレクタで使用できます。

- IGP データベース（ノードとインターフェイス）
- SR-PCE（ノードとインターフェイス）
- LSP
- BGP
- VPN
- マルチキャスト（すべてのコレクタ）

サードパーティデバイスからデータを収集する

このトピックでは、サポートモジュールを使用してサードパーティ製デバイスからデータを収集する方法について説明します。

始める前に

- 必要なサポートモジュールがあることを確認します。
- 事前構成ワークフロー （11 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 新しいコレクションを作成するか、既存のコレクションを編集するかを決定します。詳細については、コレクションの設定 （30 ページ）またはコレクションの編集 （34 ページ）を参照してください。

ステップ 2 コレクション構成チェーンの最初の手順として外部スクリプトを使用する場合は、[スタートアップスクリプ（Startup Script）] オプションを選択します。（オプション）スタートアップスクリプトを選択した場合は、Basic Topology コレクタをスキップするか、スタートアップスクリプトをソースとして構成します。スタートアップスクリプトを使用しない場合は、必要に応じて、いずれかの Basic Topology コレクタを選択する必要があります。

ステップ 3 **[高度なモデリング（Advanced modeling）]** セクションで、モジュール構成をサポートするコレクタ （119 ページ） にリストされている必要なコレクタのいずれかを選択します。次に、[Next] をクリックします。

ステップ 4 左側の **[選択されたコレクタ（Selected collectors）]** ペインで、ステップ 3 で選択したコレクタを選択し、必要なすべての構成を変更します。詳細については、該当するコレクタのトピックを参照してください。

（注）
basic topology 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 サードパーティ製デバイスからデータを収集する

a) **3rd party support module** パラメータの横にある **[有効（Enabled）]** チェックボックスをオンにします。

すべてのサポートモジュール構成オプションが表示されます。

b) 次のパラメータの詳細を入力します。

- **[実行言語（Execute using）]**：サポートモジュールの実行に使用する言語を選択します。有効なスクリプト言語は、Python、Shell、および Perl です。
- **[実行可能なスクリプト（Executable script）]**：スタートアップスクリプトの完全なパスを入力します。このファイルには、サポートモジュールファイルのスタートアップスクリプト名を取得するためのオプションが含まれています。

  （注）
  スクリプトの完全なパスを指定していることを確認してください。たとえば、feature/src/supportmodule.py などです。パスにはスラッシュ（/）のみを使用し、パスの先頭に「./」または「/」を含めないでください。

- **[サポートモジュール（Support module）]**：**[参照（Browse）]** をクリックしてサポートモジュールを選択します。サポートモジュールが .zip または .tar 形式であることを確認します。

c) （オプション）**[オプションの引数（Optional Arguments）]** セクションで、関連する引数をキーと値のペアとして入力します。これは、サポートモジュールの特定の構成パラメータに基づいてデバイスからデータを収集する場合に必要です。

ステップ 6 選択したすべてのコレクタで必要な構成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 7 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。

ステップ 8 収集ジョブのスケジュールを設定します。コレクション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、「コレクションのスケジュール （36 ページ）」を参照してください。

システムは、提供されたサポートモジュールとパラメータを使用して、指定されたサードパーティデバイスからのデータ収集を開始します。

AS プランファイルのマージ

このトピックでは、**Merge AS** ツールを構成して、さまざまな自律システム（AS）からのプランファイルをマージする方法について説明します。

このツールは、プランファイル内のあらゆる競合を解決します。ネイティブ形式のプランファイルをサポートしています。

Important notes on the Merge AS tool

- 各 AS は、異なる Cisco Crosswork Planning サーバー上に配置できます。
- 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。
  - 実際の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接続先。
  - 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接続先。
  - 外部エンドポイントに関連付けられた送信元または接続先。
- 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接続先。
- 特定のプランファイルの場合、内部 ASN は他のプランファイルが外部 ASN として識別するものと一致する必要があり、マージするすべての AS 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

- 事前構成ワークフロー （11 ページ）に記載されている手順を実行します。
- さまざまな AS のトポロジ情報とトラフィック情報を収集します。
- さまざまな AS からのプロファイルが、同じ Cisco Crosswork Planning サーバー上にあり、それらのファイルパスが指定されていることを確認します。

手順

ステップ 1 新しいコレクションを作成するか、既存のコレクションを編集するかを決定します。詳細については、コレクションの設定 （30 ページ）またはコレクションの編集 （34 ページ）を参照してください。

ステップ 2 上部の **[ツール（Tool）]** ボタンをクリックします。

ステップ 3 **[ASをマージ（Merge AS）]**、**[次へ（Next）]** の順に選択します。

ステップ 4 次の構成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 **[Sourceコレクタ（Source Collector）]** セクションで、**[+Sourceコレクタを追加（+ Add source collector）]** をクリックし、関連するコレクションとコレクタ名を選択します。

ステップ 6 **[送信元DB（Source DB）]** セクションで、**[+送信元DBを追加（+ Add source DB）]**、**[参照（Browse）]**、システム内にある送信元プランファイルの順に選択します。

（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。

ステップ 9 収集ジョブのスケジュールを設定します。コレクション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、「コレクションのスケジュール （36 ページ）」を参照してください。

結果として得られるプランファイルでは、さまざまな AS からのデータが統合されます。

次のタスク

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、コレクションの編集 （34 ページ）を参照してください。

代表的なプランファイル

代表的なプランファイルは、ネットワークプランで、以下を行います。

- 一般的なネットワーク状態をより適切に表すビューを提供する
- アーカイブからの複数のスナップショットを使用して生成される
- 指定された時間間隔に対応する複数のトラフィックレベルが含まれる

プランファイルは、ある時点のネットワーク状態のスナップショットです。障害などの一時的なイベントがコレクション期間中に発生した場合、それらはスナップショットにキャプチャされます。収集されたトラフィックは、5 分以内のコレクション期間中に発生した特定のトラフィックです。そのため、通常、スナップショットはネットワーク運用の一般的な日または週全体のネットワーク状態を表すことはありません。したがって、長期的な設計および計画タスクの基礎として使用することは不適切です。これらのニーズに応えるために、**Create representative plan** ツールは、アーカイブからの複数のスナップショットを使用して、一般的なネットワーク状態をより代表する単一のプランを構築します。

代表的なプランファイルは、さまざまなインターフェイスで、ピーク使用率が不明またはさまざまな時間帯に発生するネットワークを計画する場合に特に役立ちます。すべてのトラフィックレベルで実行されたシミュレーション分析により、ピーク発生時の時間間隔が特定されます。

代表プランの特長

- トポロジは、デフォルトでは最新のスナップショットである基本プランから抽出されます。ただし、任意のプランファイルを基本プランとして指定できます。
- 代表的なプランには、指定された時間間隔ごとに 1 つずつ、複数のトラフィックレベルが含まれています。たとえば、1 時間あたり 1 つのトラフィックレベルです。
- デマンドは、これらの各時間間隔から選択したスナップショットから抽出されます。代表的なプランファイルの 1 つのデマンドには、指定された期間のそのデマンドに対するさまざまなトラフィック量を表すトラフィック値の範囲が含まれています。
- インターフェイス、LSP、およびノードの測定値は、これらの各時間間隔で選択したスナップショットから抽出されます。

代表的なプラン作成ツールの仕組み

process_summary

Create representative plan ツールは、アーカイブのスナップショットプランから 1 つのプロファイルを作成します。これは、プランでトラフィックレベルを作成し、それぞれが 1 日または 1 週間の特定の時間間隔のデマンドトラフィックを表します。

process_workflow

これらの段階では、ツールが代表的な計画を作成する方法について説明します。

1. このツールは、サンプル時間の範囲中に指定された時間間隔に該当するすべてのスナップショットを調べます。Cisco Crosswork Planning は、これらのスナップショットのうち、共

通の基本計画で、障害が発生した回路数が最も少なく、アクティブなインターフェイス数が最も多いものを選択します。関係がある場合は、デマンドトラフィックの量が最も多いスナップショットが選択されます。単一のトラフィックレベルのスナップショットのみが使用されます。

2. ツールは、基本プランからすべてのトラフィック間隔を削除します。
3. このツールでは、期間が日か週かに応じて、HHMM-HHMM または DDDHHMM-DDDHHMM の形式を使用して基本プランに新しいトラフィック間隔を作成します。

   たとえば、03:00-04:00 と Fri17:00-Fri18:00 です。
4. このツールは、時間間隔の該当するスナップショットからすべてのデマンドをインポートします。
   - スナップショットデマンドが基本プランに存在するデマンドと一致する場合、Cisco Crosswork Planning は、そのデマンドとスナップショット デマンド トラフィックを使用します。
   - 一致するデマンドがない場合、Cisco Crosswork Planning Design は 0 トラフィックでデマンドを作成します。
   - デマンドが基本プランに存在するが、スナップショットには存在しない場合、デマンドは 0 トラフィックで使用されます。
   - このツールは、必要なマルチキャストフローとマルチキャスト接続先を含むマルチキャストデマンドもインポートします。
5. このツールは、インターフェイス、LSP、および基本プランとスナップショットの両方に存在するノードの測定されたトラフィックをインポートします。

Result

結果として得られる各代表的なプランファイルには、各トラフィックレベルが行ごとに定義されるレポートセクションが含まれます。

ツールを使用した代表的なプランの作成

このトピックでは、アーカイブされた複数のネットワーク スナップショットを使用して、一般的なネットワーク状態を表すネットワークプランファイルを生成する方法について説明します。

このタスクは、特定の時点ではなく、ネットワーク全体の状態を反映した計画ファイルが必要な場合に使用します。これは、長期的なネットワーク設計と計画に役立ちます。

Before you begin

- 事前構成ワークフロー （11 ページ）に記載されている手順を実行します。
- アーカイブされたプランファイルがあることを確認します。

手順

ステップ 1 新しいコレクションを作成するか、既存のコレクションを編集するかを決定します。詳細については、コレクションの設定 （30 ページ）またはコレクションの編集 （34 ページ）を参照してください。

ステップ 2 [コレクション（Collection）] ページの上部にある **[ツール（Tools）]** をクリックします。

ステップ 3 **[代表プランを作成（Create representative plan成）]**、**[次へ（Next）]** の順に選択します。

ステップ 4 **[アーカイブ（Archive）]** ドロップダウンで、代表プランの作成元となるアーカイブを選択します。このツールは、アーカイブのスナップショットを使用して、最終的な代表プランを生成します。

ステップ 5 関連する構成パラメータを入力します。これらのパラメータの詳細については、Representative plan configuration パラメータ （125 ページ）を参照してください。

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。

ステップ 7 収集ジョブのスケジュールを設定します。コレクション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、「コレクションのスケジュール （36 ページ）」を参照してください。

構成したパラメータに基づいて、代表的なプランファイルが生成されます。

次のタスク

次の操作を実行できます。

- Cisco Crosswork Planning Design アプリケーションから結果の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」を参照してください。
- Cisco Crosswork Planning Design アプリケーションからレポートを表示します。可視化ツールバーで、**[アクション（Actions）]** > **[レポート（Reports）]** > **[生成されたレポート（Generated reports）]** の順に選択します。レポートを表示するには、**[代表プラン（Regional Plan）]** リンクをクリックします。

Representative plan configuration パラメータ

結果を微調整して、特定の間隔で複数のトラフィックレベルの特定のスナップショットを含めることができます。このトピックでは、代表的なプランの構成パラメータについて説明します。

時間間隔パラメータ

これらのパラメータは、結果のプランファイルに対して作成される 1 日または 1 週間（**[期間（Time period）]**で定義）の時間間隔を定義します。

パラメータ	説明
期間	時間間隔を 1 日にするか、1 週間にするかを定義します。
時間間隔長	各トラフィック レベルの時間間隔長を分単位で指定します。デフォルトは 60 分です。 期間「日」の場合、上限は、60*24=1,440 分です。期間「週」の場合、上限は、60*24*7 =10,080 分です。
間隔の開始	UTC 期間での時間間隔の開始時間を定義します。たとえば、午後 4 時は 1600、月曜日の午後 4 時は Mon1600 などです。 1日の場合、形式は「HHMM」です。1 週間の場合、形式は「DDHHMM」です。 たとえば、午後 4 時は 1600、月曜日の午後 4 時は Mon1600 などです。 デフォルトは、その期間内のすべての時間間隔で、「0000」（日）または「Mon0000」（週）から始まります。

時間範囲パラメータの例

これらのパラメータは、アーカイブ内のデータの期間が、指定の時間間隔の入力に使用されるように定義します。

パラメータ	説明
サンプル時刻	サンプルの終了時刻を指定します。形式は、YYYYMMDD_HHMM です。デフォルトは、アーカイブの最終挿入日です。
サンプル時間長	サンプルの長さを日数単位で指定します。期間「日」のデフォルト値は 1、期間「週」のデフォルト値は 7 です。

その他のパラメータ

これらのパラメータは、アーカイブ内のデータの期間が、指定の時間間隔の入力に使用されるように定義します。

パラメータ	説明
アーカイブ	代表プランの作成元となるアーカイブ。このツールは、アーカイブのスナップショットを使用して、最終的な代表プランを生成します。

パラメータ	説明
アーカイブの基本時間	この時点でアーカイブ内のスナップショットを、アーカイブ内の他のスナップショットからのトラフィックレベルで増やす基本計画として指定します。形式は、YYYYMMDD_HHMMです）。 デフォルトは、サンプル期間の最新のスナップショットです。
基本プラン	アーカイブからのトラフィックレベルで増やすプランファイルを指定します。指定した場合、**[アーカイブの基本時間（Archive base time）]** で指定された値がオーバーライドされます。
冗長	ログメッセージの詳細レベルを設定します。デフォルト値は30で、有効な範囲は1 ～ 60です。

サンプルパラメータと代表的なプランの出力

このトピックでは、代表的なプランのサンプルパラメータと出力について説明します。

例 1

この例では、ネットワークのピーク時間は、毎日午後4時から午後7時です。このピークトラフィックをよりよく理解するために、この範囲内の各時間の代表的なトラフィックレベル（午後4時、午後5時、午後6時）を作成できます。週次予測を目的として、過去5日間のサンプルを使用してトラフィックレベルを作成します。出力ファイル名は「representation_day.pln」で、期間内の最新のスナップショット（110502_0347_UTC.pln）を基本プランとして使用します。このプランは、「バックボーン」という名前のアーカイブにあります。

使用するパラメータ：

- アーカイブ： バックボーン
- 基本プラン：110502_0347_UTC.pln
- 時間間隔長：60
- サンプル時間長：1
- 間隔の開始：1600、1700、1800

出力：

[トラフィックレベル（Traffic level）]	**Snapshot**	インターフェイスの照合	合計デマンドトラフィック	合計デマンド	デマンドがインポートされませんでした
16:00-17:00	110502_0347_UTC.pln	25	43534.32	453	4

[トラフィックレベル（**Traffic level**）]	**Snapshot**	インターフェイスの照合	合計デマンドトラフィック	合計デマンド	デマンドがインポートされませんでした
17:00-18:00	110502_0347_UTC.pln	25	47583.23	454	3
18:00-19:00	110502_0347_UTC.pln	25	50771.49	454	3

例 2

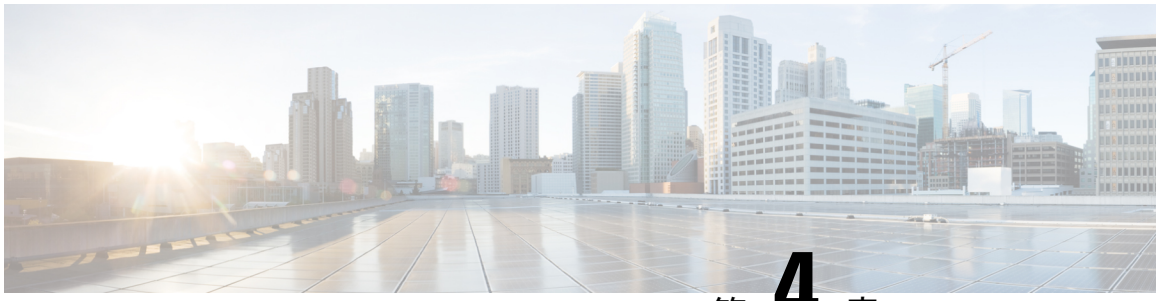
この例では、ネットワークのピーク時間は毎日午後 4 時前後と、金曜日の午後 8 時です。過去 2 週間における、これら 6 つの期間それぞれの代表的なトラフィックレベルを取得する必要があります。今日は火曜日であるため、昨日の午後 4 時 ～ 5 時の範囲と先週の月曜日の午後 4 時 ～ 5 時の範囲を使用して、午後 4 時トラフィックレベルが作成されます。代表的なプランファイルの名前は「weekly_peak.pln」です。基本プラン、110407_0423_UTC.pln は「acme」ディレクトリにあります。

使用するパラメータ：

- 基本プラン：110407_0423_UTC.pln
- 期間：週
- 時間間隔長：60
- サンプル時間長：14
- 時間間隔の開始：Mon1600、Tuesday1600、Wed1600、Thu1600、Fri1600、Fri2000

出力：

[トラフィックレベル（**Traffic level**）]	**Snapshot**	インターフェイスの照合	合計デマンドトラフィック	合計デマンド	デマンドがインポートされませんでした
Mon16:00-Mon17:00	110407_0423_UTC.pln	97	43534.32	6702	21
Tue16:00-Tue17:00	110407_0423_UTC.pln	97	47583.23	6702	21
Wed16:00-Wed17:00	110407_0423_UTC.pln	95	50771.49	6701	22
Thu16:00-Thu17:00	110407_0423_UTC.pln	97	56831.91	6702	21
Fri16:00-Fri17:00	110407_0423_UTC.pln	93	48732.18	6700	23
Fri120:00-Fri21:00	110407_0423_UTC.pln	97	53692.39	6702	21



第 4 章

ライセンスの管理

Cisco Smart Licensing

Cisco Smart Licensing は、柔軟背の高いライセンス管理モデルで、

- シスコポートフォリオと組織全体でソフトウェア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ます。
- ライセンス使用およびアクセスの集中管理を行います。
- セキュリティで保護され、ユーザーのアクセス権を管理します。

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。

Smart Licensing の利点

Smart Licensing の主な利点は次のとおりです。

- 簡単なアクティベーション：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。製品アクティベーションキー（PAK）は不要です。
- 統合管理：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し、保持しているあるいは使用しているものを把握できます。
- 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譲渡できます。

スマート ライセンスの設定

process_summary

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ます。シスコライセンスの有効化、ライセンス使用状況の監視、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。CSSM 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。このページでは、Cisco Crosswork Planning の登録、転送設定の編集、ライセンスの更新、アプリケーションの登録解除ができます。

process_workflow

Cisco Crosswork Planning で Cisco Smart Licensing を構成する段階は次のとおりです。

1. Cisco Software Central（software.cisco.com）でスマートアカウントを設定します。
    1. [スマートアカウント要求（Smart Account Request）] にアクセスします。
    2. 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。詳細については、「Cisco Crosswork Planning と CSSM 間のトランスポートモードの設定 （130 ページ）」を参照してください。
3. Cisco Crosswork Planning を CSSM に登録します。詳細については、トークンを介した Cisco Crosswork Planning の登録 （132 ページ）またはオフライン予約経由で Cisco Crosswork Planning を登録する （136 ページ）を参照してください。

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

このトピックでは、Cisco Crosswork Planning と CSSM の通信を制御する転送設定を構成方法について説明します。

Cisco Crosswork Planning は、CSSM と接続するために複数のトランスポートモードをサポートします。

- [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CSSMオンプレミスを介して通信します。このアプローチは、オンプレミスのすべての通信を維持しながら、クラウドベースのユーザーエクスペリエンスを複製します。CSSMオンプレミスオプションの詳細については、『Smart Software Manager ガイド』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**：プロキシが存在する場合、Cisco Crosswork Planning は、構成したプロキシ経由でダイレクト モード エンド ポイントに接続します。

Cisco Crosswork Planning とCSSM 間のトランスポートモードを構成するには、次の手順を実行します。

始める前に

Cisco Crosswork Planning が登録モードになっている間、転送設定は変更できません。転送設定を変更するには、まず製品の登録解除をする必要があります。

手順

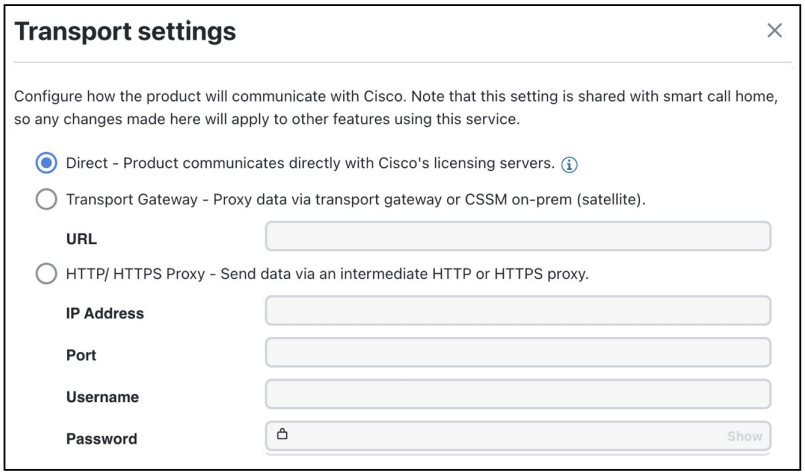
ステップ 1 メインメニューから、[ライセンス（Licensing）] を選択します。

[スマートライセンス（Smart License）] ページが開きます。

ステップ 2 **[転送設定（Transport settings）]** フィールドに、現在の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。

[転送設定（Transport Settings）] ページが表示されます。

図 *21* : 転送設定ページ



ステップ 3 適切な転送モードを選択します。すべての必要な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。

選択した転送モードと設定が保存されます。 Cisco Crosswork Planning は、CSSM との通信に設定された転送モードを使用します。

トークンを介した Cisco Crosswork Planning の登録

このトピックでは、登録トークンを使用して CSSM に Cisco Crosswork Planning を登録する方法について説明します。

ライセンスが付与された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 年間有効です。6 か月後に自動更新されるため、継続的な運用が保証されます。

始める前に

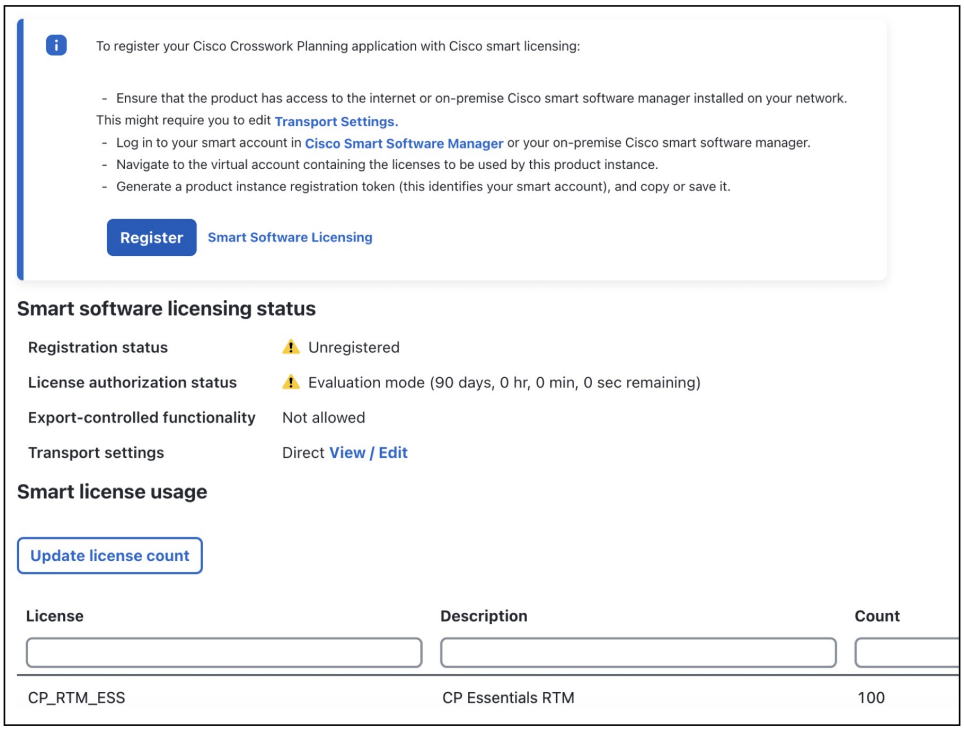
- スマートアカウントがあることを確認します。ない場合は、[スマート アカウント要求（Smart Account Request）] にアクセスして、指示に従って作成します。
- 製品インスタンス登録トークンがあることを確認します。トークンの生成に関するガイダンスについては、Cisco Software Central のサポートリソースを参照してください。

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。

登録状態とライセンス認証状態は、それぞれ **[未登録（Unregistered）]** と **[評価（Evaluation）]** モードになります。

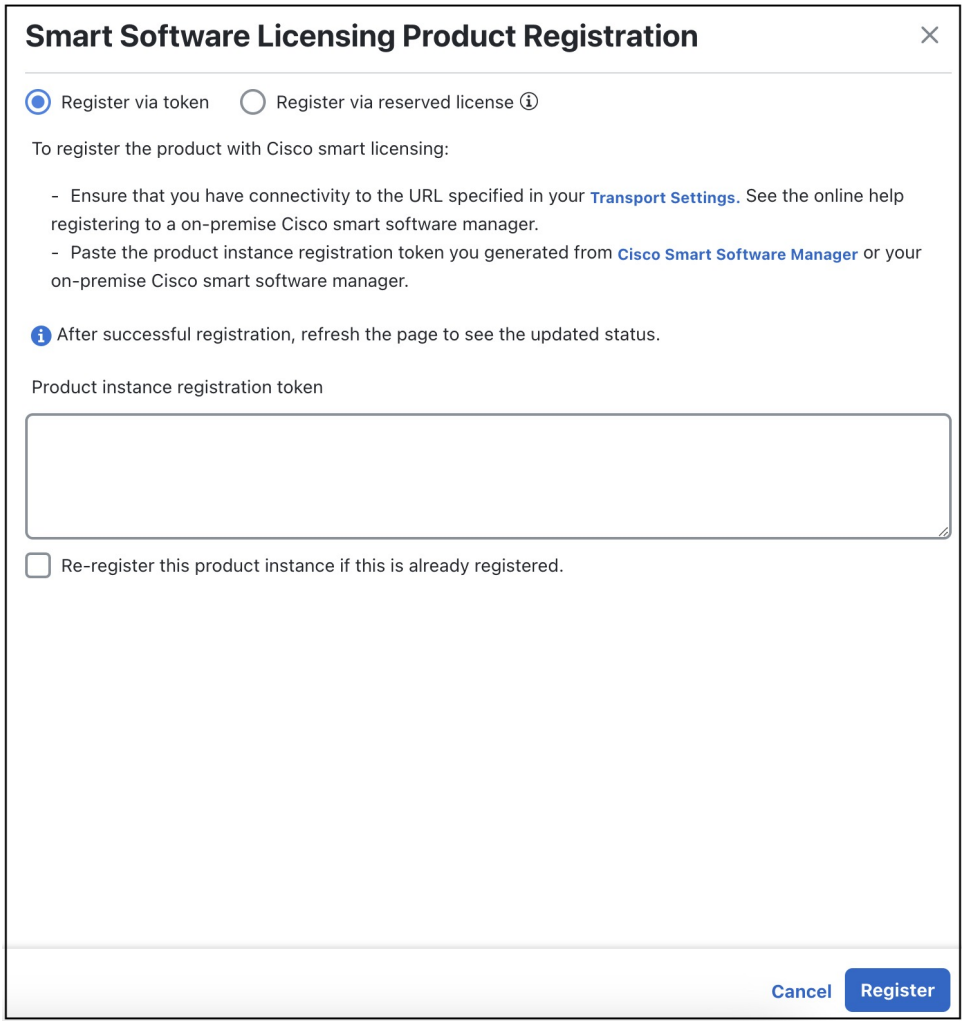
図 *22*：スマート ソフトウェア ライセンスの未登録の例



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）] 領域で、**[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シング製品の登録（Smart Software Licensing Product Registration）] ページが表示されます。

図 *23 : [*スマートソフトウェアライセンシング製品の登録（***Smart Software Licensing Product Registration***）*]* ページ



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。

（注）

- 要求が成功するまで、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ます。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、ページを手動で更新して更新された状態を確認する必要があります。

登録が成功すると、「製品登録が正常に完了しました」というメッセージが表示されます。

登録トークンを使用して、Cisco Crosswork Planning が CSSM に登録されます。登録状態とライセンス承認状態が、それぞれ、**[登録済み（Registered）]** と **[承認済み（Authorized）]** に更新されます。

ライセンスアクションの手動実行

このトピックでは、Cisco Crosswork Planning でライセンスを手動で更新、登録、または登録解除する方法について説明します。

デフォルトでは、Cisco Crosswork Planning は登録と承認の更新を自動的に処理します。ただし、アプリケーションとシスコのサーバー間の通信に障害が発生した場合は、**[アクション（Actions）]** ドロップダウンメニューを使用して特定のライセンスアクションを手動で開始します。

始める前に

Cisco Crosswork Planning アプリケーションが [登録済み（Registered）] 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ます。

ステップ 3 必要に応じてこれらのオプションのいずれかを選択します。

a) **認証の更新**：30 日後に自動更新が失敗した場合、承認を手動で更新します。
b) **登録の更新**：6 か月後に自動更新が失敗した場合に、手動で登録を更新します。
c) **再登録**：登録トークンの期限が切れた場合などに、アプリケーションを再登録します。
d) **登録解除**：転送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）
アプリケーションの登録を解除すると、評価期間があれば**[評価（Evaluation）]**モードになります。それ以外の場合は、**[評価期限切れ（Evaluation Expired）]** モードに入ります。詳細については、ライセンス認証状態 （141 ページ） を参照してください。

選択した手動ライセンスアクションが完了したら、それに応じてアプリケーションのライセンス状態が更新されます。

オフライン予約経由で Cisco Crosswork Planning を登録する

このトピックでは、オフライン予約を使用して CSSM に Cisco Crosswork Planning を登録する方法について説明します。

Smart Licensing を使用する場合、Cisco Crosswork Planning は、定期的に使用状況情報を CSSM 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。ない場合は、[スマートアカウント要求（Smart Account Request）] にアクセスして、指示に従って作成します。

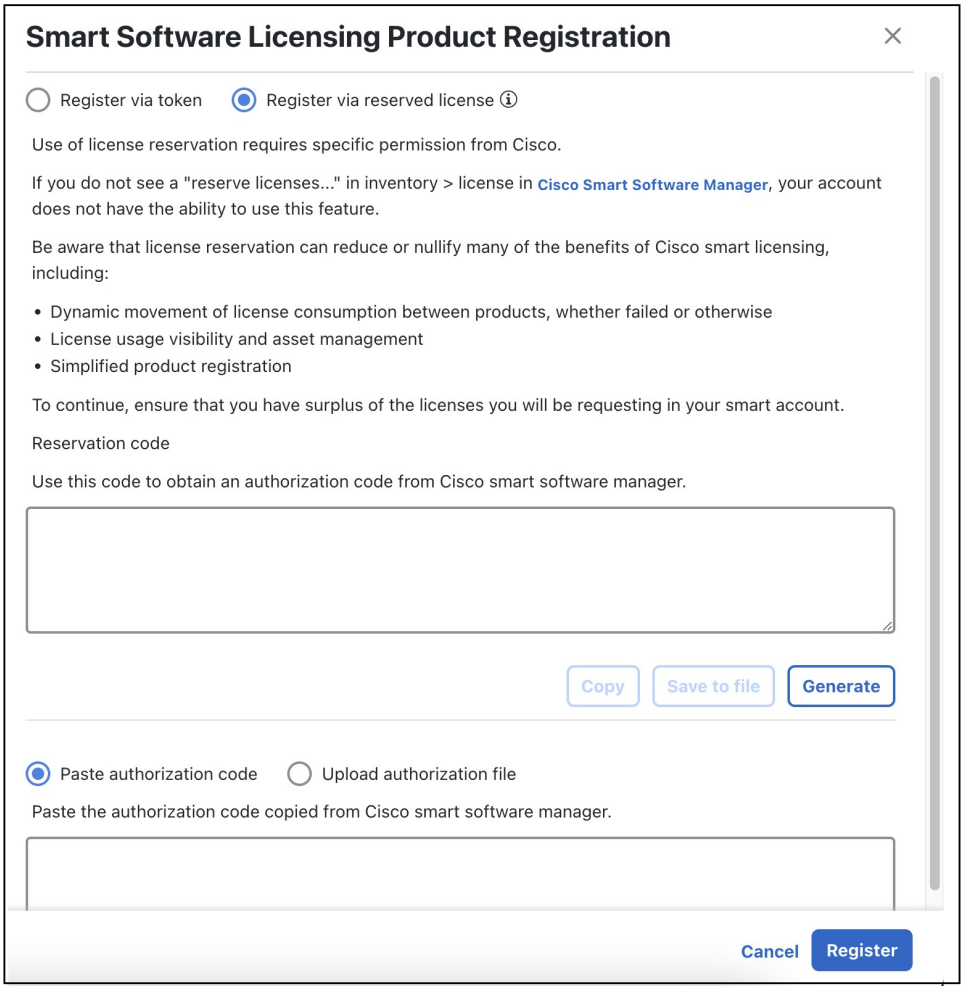
手順

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 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シング製品の登録（Smart Software Licensing Product Registration）] ページが表示されます。

図 *24 : [*スマートソフトウェアライセンシング製品の登録（***Smart Software Licensing Product Registration***）*]* ページ



ステップ 3 **[予約済みライセンス経由で登録（Register via Reserved License）]** オプションを選択します。

ステップ 4 予約要求コードを生成します。

a) [予約コード（Reservation code）] セクションにある **[生成（Generate）]** ボタンをクリックします。予約要求コードがテキストフィールドに表示されます。

b) 生成されたコードをコピーするには、**[コピー]** ボタンをクリックします。

ステップ 5 CSSM で承認コードを生成する

a) CSSM にログインし、適切なバーチャルアカウントを選択します。

b) **[ライセンス（Licenses）]** タブをクリックし、**[ライセンスの予約（License Reservation）]** をクリックします。

c) 手順 4 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。

d) [ライセンスを選択（Select Licenses）] ページで、必要な予約のタイプを選択して、**[次へ（Next）]** をクリックします。

e) [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。

f) **[クリップボードにコピー（Copy to Clipboard）]** ボタンを使用して生成されたコードをコピーします。

ステップ 6 Cisco Crosswork Planning の [スマートソフトウェアライセンシング製品の登録（Smart Software Licensing Product Registration）] ページに戻ります。

ステップ 7 **[認証コードを貼り付ける（Paste authorisation code）]** オプションを選択して、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 8 [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。

Cisco Crosswork Planning が、オフライン予約方式を使用して CSSM に登録されます。登録状態とライセンス認証状態は、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

このトピックでは、オフライン予約を使用する製品インスタンスに関連付けられているライセンス数を更新する方法について説明します。

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。[スマートソフトウェアライセンシング状態（Smart Software Licensing Status）] の製品インスタンス名を書き留めます。

ステップ 2 CSSM で承認コードを生成する

a) CSSM にログインし、適切なバーチャルアカウントを選択します。

b) [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。

c) この製品インスタンスの場合、**[アクション（Actions）]** > **[予約を更新（Update Reservation）]** の順に選択します。

d) [ライセンスを選択（Select Licenses）] ページで、必要な予約の種類を選択し、リストから必要なライセンスの数を更新し、**[次へ（Next）]** をクリックします。

e) [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。

f) **[クリップボードに（Copy to Clipboard）]** を使用して、生成された承認コードをコピーします。

ステップ 3 Cisco Crosswork Planning UI の [スマートライセンス（Smart License）] ページに戻ります。

ステップ 4 **[アクション（Actions）]** > **[予約を更新（Update Reservation）]** の順に選択します。

ステップ 5 手順 2 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状態（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 6 CSSM に確認コードを入力します。

a) CSSM に戻り、必要な製品インスタンス名をクリックします。

b) **[アクション（Actions）]** > **[確認コードを入力（Enter Confirmation Code）]** の順に選択します。
c) 手順 5 で生成された予約確認コードを入力して、貼り付けます。
d) [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

このトピックでは、Cisco Crosswork Planning の予約済みライセンスをリリースする方法について説明します。

予約済みライセンスをリリースすると、それらのライセンスはプールに戻り、アプリケーションによる予約済みライセンスの消費が停止されます。ライセンスをリリースした後、評価期間があれば、アプリケーションは **[評価（Evaluation）]** モードになります。それ以外の場合は、**[評価期限切れ（Evaluation Expired）]** モードに入ります。

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。[スマートソフトウェアライセンシング状態（Smart Software Licensing Status）] の製品インスタンス名を書き留めます。

ステップ 2 **[アクション（Actions）]**、> **[予約を返却（Return Reservation）]** の順に選択します。

ステップ 3 [予約の返却を確認（Confirm Return Reservation）] ページで、**[確認（Confirm）]** をクリックします。

システムが、リリースコード（予約リターンコード）を生成します。**[コピー]**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 に予約要求コードを入力します。

a) CSSM にログインし、適切なバーチャルアカウントを選択します。
b) [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。
c) この製品インスタンスに対して、**[アクション（Actions）]**、> **[削除（Remove）]**の順に選択します。
d) [予約を削除（Remove Reservation）] ページで、手順 3 で生成した予約リターンコードを貼り付け、**[予約を削除（Remove Reservation）]** をクリックします。

ステップ 5 Cisco Crosswork Planning UI で [スマートライセンス（Smart License）] ページに戻ります。[登録（Registration）] 状態が、**[未登録（Unregistered）]** に変わったことを確認します。

ステップ 6 **[アクション（Actions）]**、> **[ライセンス予約を無効化（Disable License Reservation）]** の順に選択します。

予約済みライセンスがリリースされます。アプリケーションは、可能な場合は [評価（Evaluation）] モードになるか、[評価期限切れ（Evaluation Expired）] モードに入ります。

ライセンス数の更新

このトピックでは、Cisco Crosswork Planning でライセンス数を更新して、Cisco Crosswork Planning Design アプリケーションでコンプライアンスと適切なツールの操作を確実にする方法について説明します。

始める前に

CSSMの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。そうしないと、ライセンスはコンプライアンス違反となります。

手順

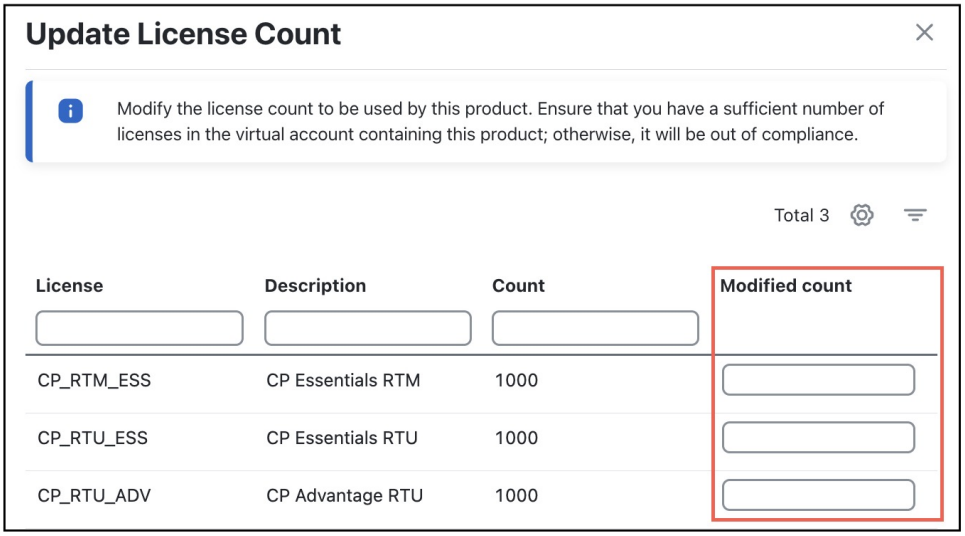
ステップ 1 メインメニューから、[ライセンス（Licensing）] を選択します。

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

[ライセンス数を更新（Update license count）] ページが表示されます。

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 *25 : [ライセンス数を更新（Update license count）] ページ*



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、ライセンスが 1 つしかなくても機能します。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**：Cisco Crosswork Planning コレクタと Design アプリケーションの両方のカウント値を 1 にしても十分に機能します。
- **CP_RTU_ADV**：Cisco Crosswork Planning コレクタと Design アプリケーションの両方のカウント値を 1 にしても十分に機能します。

ステップ 4 [保存（Save）] をクリックします。

システムが更新され、ライセンスの数が適用されます。

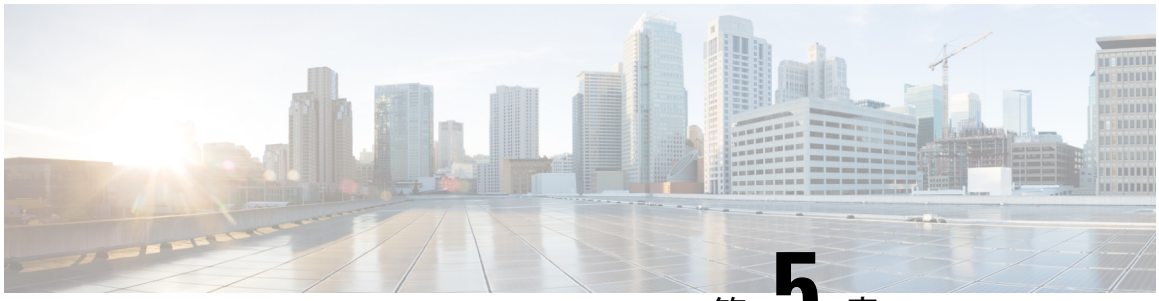
ライセンス認証状態

システム登録状態に基づいて、アプリケーションはいくつかの異なるライセンス承認状態を表示します。表 15 : ライセンス認証状態 （141 ページ） では、登録状態とライセンス承認状態の考えられる各組み合わせおよび、それぞれのアプリケーションの使用が何を示すかについて説明しています。

表 *15 :* ライセンス認証状態

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、未登録状態に戻る原因となります。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。

登録ステータス	ライセンス認証ステータス	説明
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をすべて使用できます。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

証明書を管理する

証明書とは？

証明書は、個人、サーバー、会社などのエンティティを識別し、公開キーにリンクする電子文書です。証明書の作成時、公開キーと一致する秘密キーの両方が生成されます。TLS プロトコルでは、公開キーがデータを暗号化し、秘密キーが復号化します。

証明書は、「親」証明書として機能する発行者（多くの場合、認証局（CA））によって署名されます。このプロセスは自己署名することもできます。TLS の交換では、証明書の信頼チェーンにより発行者の有効性が確認されます。このチェーンには、自己署名ルート CA 証明書、複数の中間 CA 証明書、およびエンドエンティティ証明書の 3 種類のエンティティが含まれます。中間証明書が、サーバー証明書をルート CA に接続するため、セキュリティが強化されます。ルート証明書の秘密キーから始めて、チェーン内の各証明書が次の証明書に署名して発行し、サーバーまたはクライアントの認証に使用されるエンドエンティティ証明書で終わります。

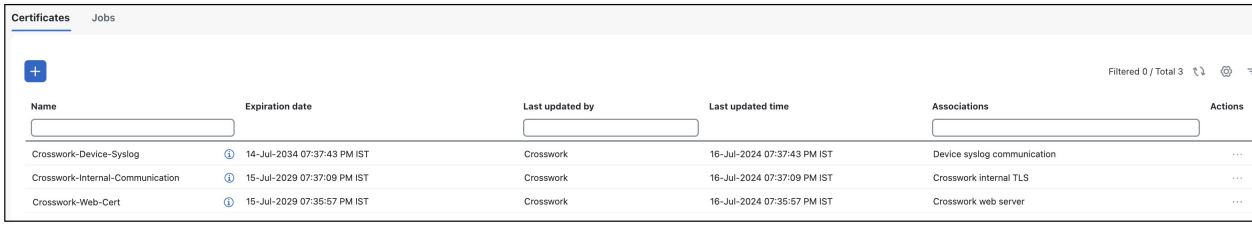
Cisco Crosswork Planning の証明書

Cisco Crosswork Planning は、TLS プロトコルを使用して、デバイスとコンポーネント間をセキュアに通信します。TLS は X.509 証明書を使用してデバイスを認証し、データを暗号化し、その完全性を確保します。システムでは、生成された証明書とクライアントによってアップロードされた証明書の組み合わせが使用されます。アップロードされた証明書は、認証局（CA）から購入するか、自己署名することができます。たとえば、システムの VM でホストされる Web サーバーとクライアント ブラウザ インターフェイスは、セキュアな通信のために TLS 経由で交換されるシステム生成の X.509 証明書を使用します。

Crosswork Cert Manager は、分散フレームワーク内の複数のマイクロサービスおよびサービスのプロキシであり、すべての Crosswork 証明書を管理します。[証明書管理（Certificate Managemen）] ページ**[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。

図 26 : [証明書管理（Certificate management）] ページ （144 ページ） は、Cisco Crosswork Planning が提供するデフォルトの証明書を表示しています。

図 *26 : [*証明書管理（*Certificate management***）*] ページ***



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	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-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（164 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 Planning 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（144 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）
[セキュアLDAP通信（Secure LDAP communication）] オプションのみが Cisco Crosswork Planning に該当します。

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）]** を選択します。

ステップ 2 証明書を更新するには、次の手順を実行します。

a) **[アクション（Actions）]** 列で、変更する証明書の [⋯] をクリックし、**[証明書を更新（Update certificate）]** を選択します。

b) 更新する証明書に基づいて、フィールドに適切な値を入力します。詳細については、フィールドの横にある ⓘ アイコンをクリックします。

c) [保存（Save）] をクリックして、変更内容を保存します。

ステップ 3 Web 証明書のクライアント証明書認証を有効にするには、次の手順を実行します。

a) **[アクション（Actions）]** 列で、変更する Crosswork web 証明書の [⋯] をクリックし、**[クライアント証明書認証を構成（Configure client certificate authentication）]** を選択します。

[クライアント証明書認証を構成（Configure client certificate authentication）] ページが表示されます。

b) [有効（Enable）] チェックボックスをオンにします。

[証明書のスキーマ（Certificate schema）] と [OCSP] の設定が表示されます。

[OCSP] 設定はデフォルトで有効になっていますが、必要に応じて無効にすることができます。有効にした場合、オンライン証明書ステータスプロトコル（OCSP）を使用して、証明書の失効ステータスを確認できます。

c) [証明書のスキーマ（Certificate schema）] の値を選択します。

- **[自動（Automatic）]**：代替サブジェクト名領域でユーザープリンシパル名（UPN）を検索します。UPNが見つからない場合、システムは共通名の値を使用します。これはデフォルトの選択肢です。
- **[手動（Manual）]**：ユーザー アイデンティティ ソースと指定された正規表現に基づいて、サブジェクト領域でユーザー名を検索します。

d) （オプション） [OCSP] の値を選択します。

- **[自動（Automatic）]**：証明書からレスポンダ URL を抽出し、それを使用して OCSP 検証を実行します。
- **[手動（Manual）]**：OCSP レスポンダ URL を指定する必要があります。

e) [保存（Save）] をクリックして、変更内容を保存します。

ステップ 4 1 ステップで証明書を更新してクライアント認証を設定するには、次の手順を実行します。

a) 変更する Crosswork Web 証明書で [⋯] をクリックし、**[証明書の更新とクライアント認証の構成（Update Certificate and Configure Client Authentication）]** を選択します。

[証明書の更新とクライアント認証の構成（Update Certificate and Configure Client Authentication）] ページが表示されます。

（注）
証明書を更新してクライアント認証を設定する複合オプションを選択すると、Crosswork サーバーの再起動中のダウンタイムが最小限に抑えられます。これは、これらのアクションを個別に実行した場合は再起動が 2 回発生するのに対し、この複合オプションでは再起動が 1 回しか発生しないためです。

b) ステップ 2 とステップ 3 の指示に従ってデータを入力します。
c) [保存（Save）] をクリックして、変更内容を保存します。

証明書のダウンロード

証明書を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 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。

ステップ 3 ルート証明書と中間証明書を個別にダウンロードするには、証明書の横にある [⬇] をクリックします。証明書を一度にダウンロードするには、**[すべてエクスポート（Export all）]** をクリックします。

証明書署名要求を使用した Web 証明書の更新

Cisco Crosswork Planning は、中間認証局（CA）証明書をインポートすることで Web 証明書を更新できます。バージョン 7.0.1 以降では、証明書署名要求（CSR）による Web 証明書の更新もサポートされています。

このアプローチにより、Cisco Crosswork Planning の外部に秘密キーを公開することなく、エンタープライズまたは商用 CA によって署名された証明書を取得できます。

始める前に

- 証明書を更新すると、クライアント認証に使用される既存の証明書信頼チェーンが破壊される可能性があるため、慎重に操作を進めてください。
- このプロセスでは Crossworkサーバーを再起動する必要があるため、完了するまで数分かかります。
- クライアント認証を有効にするには、AAA モードをローカルに設定します。

手順

ステップ 1 メインメニューで、**[管理（Administration）]** > **[証明書管理（Certificate Management）]** の順に選択します。

ステップ 2 Web 証明書（`Crosswork-Web-Cert`）の [⋯] をクリックして、**[証明書を更新（Update certificate）]** を選択します。

[証明書の更新方法（Certificate Update Method）] ページが表示されます。

ステップ 3 CSR を作成して、認証局（CA）に送信します。

a) **[証明書署名要求（CSR）を作成（Create a certificate signing request (CSR)）]** ラジオボタン、**[証明書を更新（Update certificate）]** の順に選択します。

[証明書署名要求（CSR）（Certificate Signing Request (CSR)）] ページが表示されます。。

b) **[CSR の作成（Create CSR）]** をクリックします。

[証明書署名要求（CSR）を作成（Create Certificate Signing Request (CSR)）] ページが表示されます。

c) 指定されたフィールドに、関連する値を入力します。詳細については、フィールドの横にあるアイコンをクリックします。次のフィールドは必須です。

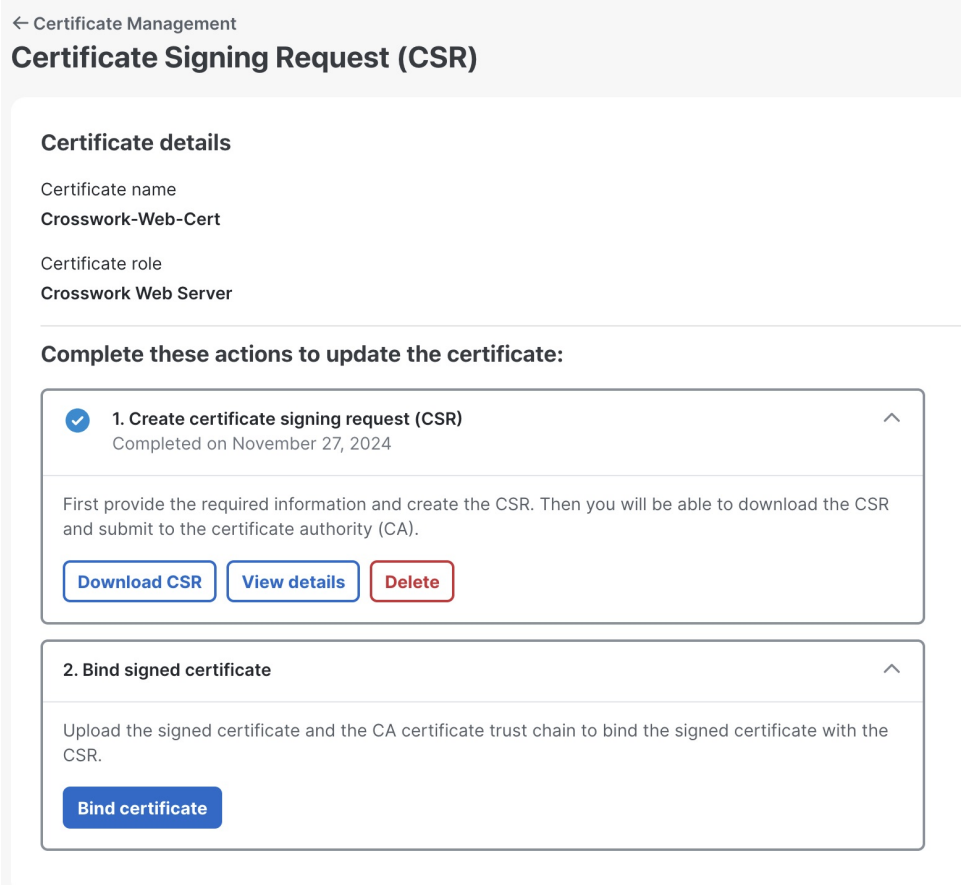
- **[共通名（CN）（Common name (CN)）]**：デフォルトでは、これはサーバーの完全修飾ドメイン名（FQDN）ですが、サーバーを識別する任意の一意の名前にすることができます。64 文字まで使用できます。
- **[IPアドレス（IP address）]**：これは、このデプロイメントで使用される Crosswork VIPアドレスです。追加の IP アドレスは、証明書の検証に必要な場合にのみ追加する必要があります。

- **[キータイプ（Key Type）]**：オプションは、[RSA] と [ECDSA] です。デフォルト値は、[RSA] です。
- **[キーのサイズ（ビット単位（Key Size (in bits)）]**：オプションは [2048]、[3072]、および [4096] です。デフォルト値は、[2048] です。
- **[キーダイジェスト（Key Digest）]**：オプションは、[SHA-256]、[SHA-384]、[SHA-224]、および [SHA-512] です。デフォルト値は、[SHA-256] です。

d) **[CSRを作成（Create CSR）]** をクリックして、アクションを完了します。

ステップ 4 CSR を生成したら、**[ダウンロード（Download）]** をクリックして、CSR をダウンロードして使用し、CA からの署名済み証明書を取得します。

図 *27 : [*証明書署名要求（*CSR***）（***Certificate Signing Request (CSR)***）]* ページ**

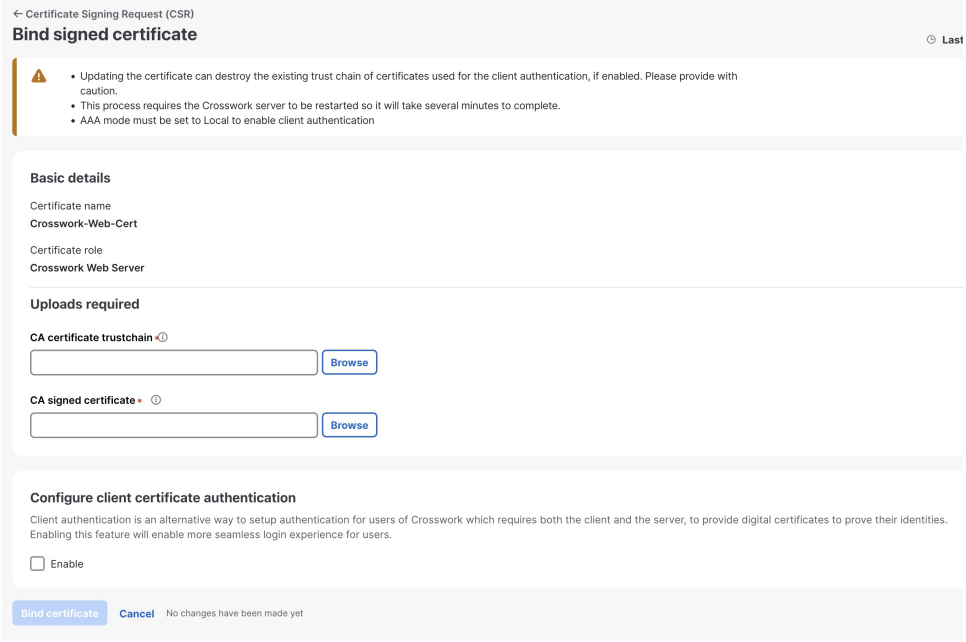


ステップ 5 CA 署名付き証明書と CA 証明書信頼チェーンをアプリケーションして、証明書をバインドします。

a) **[証明書署名要求（CSR）（Certificate Signing Request (CSR)）]** ウィンドウで、**[証明書をバインド（Bind certificate）]** をクリックします。

[署名付き証明書をバインド（Bind signed certificate）] ウィンドウが表示されます。

図 *28* : 署名付き証明書のバインド



b) 表示されたフィールドに関連データをアップロードします。詳細については、フィールドの横にあるⓘアイコンをクリックします。

- **[CA証明書信頼チェーン（CA certificate trustchain）]**：これは、CA から取得した Web サーバー証明書の証明書信頼チェーンです。
- **[CAあ署名済み証明書（CA signed certificate）]**：これは、CA から取得した Web サーバーの最終的な署名済み証明書です。

c) （オプション）**[有効（Enable）]** チェックボックスをクリックして、クライアント証明書認証を構成します。

d) **[証明書をバインド（Bind certificate）]** をクリックして、操作を完了します。

バインドアクションが完了すると、Web 証明書がアップロードされ、新しい Web 証明書で Tyk が再起動されます。

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 ロールの作成 （154 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 （186 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。

ユーザーロール、関数カテゴリ、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 *16*：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 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 （151 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 （156 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 （151 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 （156 ページ）」を参照）。

（注） 一部のAPI権限はシステム管理者ロールで事前に定義されており、複製されたロールでも変更されません。たとえば、システム管理者ロールには、**Alarms & Events API** 向けのデフォルトの **[読み取り（Read）]** および **[書き込み（Write）]** 権限があります。これらの権限は、元の管理者ロールと複製された管理者ロールの両方に対して構成することはできません。

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 *17 :* 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	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、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 （186 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。

注意 この項の手順に従って操作を行うと、Crosswork のユーザーインターフェイスへのすべての新しいログインに影響することに注意してください。セッションの中断を最小限に抑えるために、すべての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。

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（170 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承認を持つユーザーのみに Remote Authentication Servers Integration 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 ロールの作成（154 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。

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+]** タブの順に選択します。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 *18 : 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（IP address）]	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 name）]	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。
[ポート（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。

フィールド	説明
[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。
[サービス（Service）]	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（Policy 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。
[Device Access Group属性（Device access group attribute）]	Device Access Group 属性値は、（ISE/スタンドアロン）TACACS+ サーバー属性でデバイスアクセスグループに使用されるキーに基づいています。これらの値は、1 つまたは複数のカンマで区切られたエントリにすることができます。 TACACS+ のコンテキストでは、Device Access Group 属性は、通常、TACACS+ サーバーがネットワークデバイスに送り返すカスタム属性または承認属性です。この属性により、認証されたユーザに適用されるネットワークデバイスのグループ、またはデバイスのアクセスポリシーのレベルを指定します。Device Access Group 属性は、ポリシー ID と同期して動作し、デバイス間でのユーザー権限を定義します。
[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。
[再試行（Retries）]	許可される認証の再試行回数を指定します。

フィールド	説明
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（146 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 *19 : 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（Name）]	LDAP ハンドラの名前。
[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（Secure connection）]	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（Port）]	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。

フィールド	説明
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。
[ポリシーID（Policy 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 Crossworks 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。
[Device Access Group属性（Device access group attribute）]	Device Access Group 属性値は、LDAP サーバー属性でデバイスアクセスグループに使用されるキーに基づいています。これらの値は、1つまたは複数のカンマで区切られたエントリにすることができます。 LDAP のコンテキストでは、Device Access Group 属性は、通常、LDAP サーバーがネットワークデバイスに送り返すカスタム属性または承認属性です。この属性により、認証されたユーザに適用されるネットワークデバイスのグループ、またはデバイスのアクセスポリシーのレベルを指定します。Device Access Group 属性は、ポリシー ID と同期して動作し、デバイス間でのユーザー権限を定義します。
[接続タイムアウト（Connection 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。

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**：

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**：

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 メインメニューで、**[管理（Administration）] > [AAA] > [サーバー（Servers）] > [RADIUS]** タブの順に選択します。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 *20 : 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（IP address）]	RADIUS 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 name）]	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（Port）]	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（Service）]	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。
[ポリシーID（Policy 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。

フィールド	説明
[Device Access Group属性（Device access group attribute）]	Device Access Group 属性値は、RADIUS サーバー属性でデバイスアクセスグループに使用されるキーに基づいています。これらの値は、1つまたは複数のカンマで区切られたエントリにすることができます。 RADIUS のコンテキストでは、Device Access Group 属性は、通常、RADIUS サーバーがネットワークデバイスに送り返すカスタム属性または承認属性です。この属性により、認証されたユーザに適用されるネットワークデバイスのグループ、またはデバイスのアクセスポリシーのレベルを指定します。Device Access Group 属性は、ポリシー ID と同期して動作し、デバイス間でのユーザー権限を定義します。
[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。
[再試行（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 （161 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。

Crossworkは SSO 相互起動をサポートしており、サービスプロバイダーとのナビゲーションを容易にします。設定が完了すると、ウィンドウの右上隅にある起動アイコン（ ）を使用して URL を起動できます。

注目

- Crossworkを再インストールまたは移行するときは、Crosswork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。[アイデンティティプロバイダー（Identity Provider）] ウィンドウが表示されます。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) [サービスプロバイダー（Service 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 エンティティの名前を入力します。

  （注）
  URL を指定すると、[アイデンティティプロバイダー（Identity Provider）] ウィンドウの [サービス名（Service name）] 列のエントリがハイパーリンクになります。

- [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。ここにサービスプロバイダーの URL を入力して、相互起動を行うことができます。

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 設定の構成

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）
Crossworkは、同時接続ユーザーに対して5～200の並列セッションをサポートします。並列セッション数を超えると、Crossworkへのログイン時にエラーが表示されます。

（注）
Crossworkは、50～400件の同時NBIセッションをサポートします。

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監視

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。

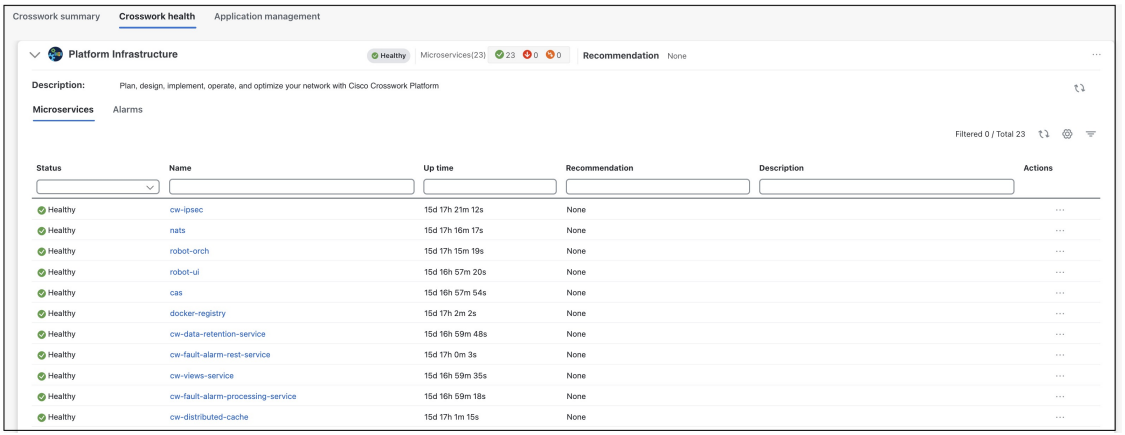
プラットフォームインフラストラクチャとアプリケーション正常性の監視

[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 *29 : [Crosswork* 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 *30 : [*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。

- アクティブなアラームをフィルタリングします。
- アラームの詳細をドリルダウンするには、アラームの説明をクリックします。
- アラームの状態変更（確認、未確認、クリア）
- アラームへメモを追加します。
- 製品内のイベントのリストを表示します。
- 各イベントの相関アラームを表示します。

システム正常性チェック例

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。

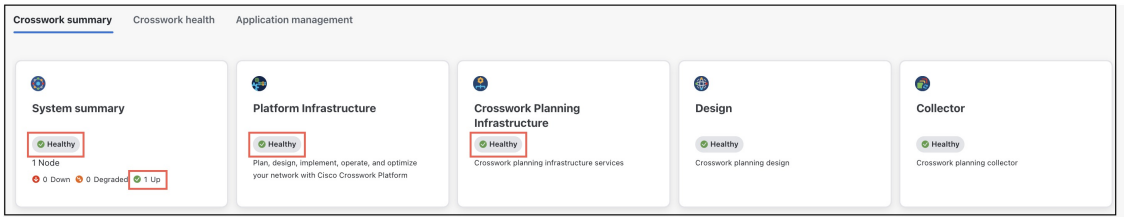
手順

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 *31 : [Crosswork* の概要（*Crosswork Summary*）*]* タブ

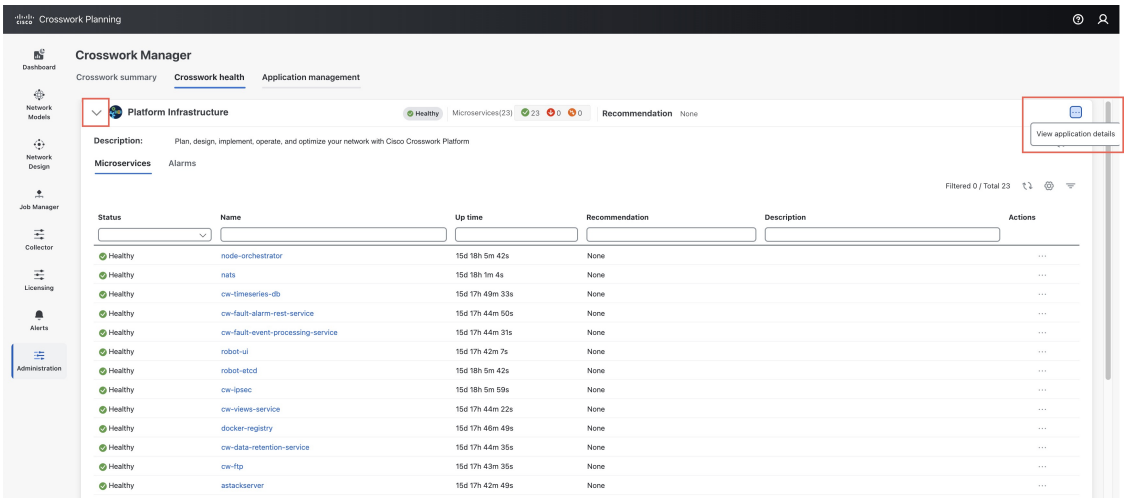


ステップ 2 Crosswork プラットフォーム インフラストラクチャの一部として実行されているマイクロサービスに関する詳細情報を確認および表示します。

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

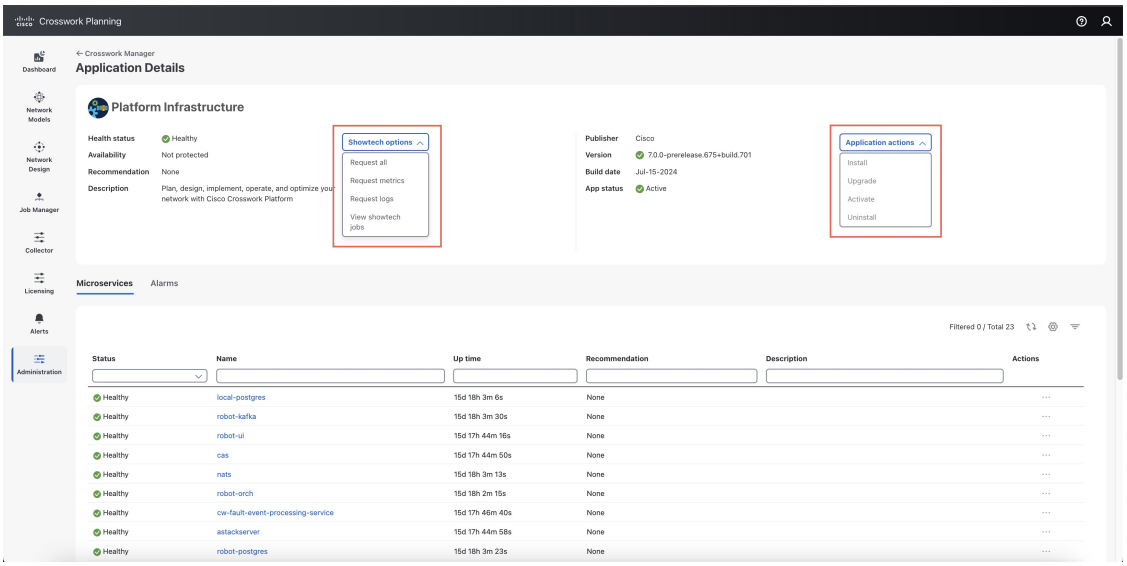
b) [Crossworkプラットフォームインフラストラクチャ（Crosswork Platform Infrastructure）] の行を展開し、 をクリックして [アプリケーション詳細を表示（View application details）] を選択します。

図 *32 : [Crosswork* 正常性（*Crosswork health*）*]* タブ



c) [アプリケーションの詳細（Application Details）] ページでは、マイクロサービスの詳細をチェックおよび見直し、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。

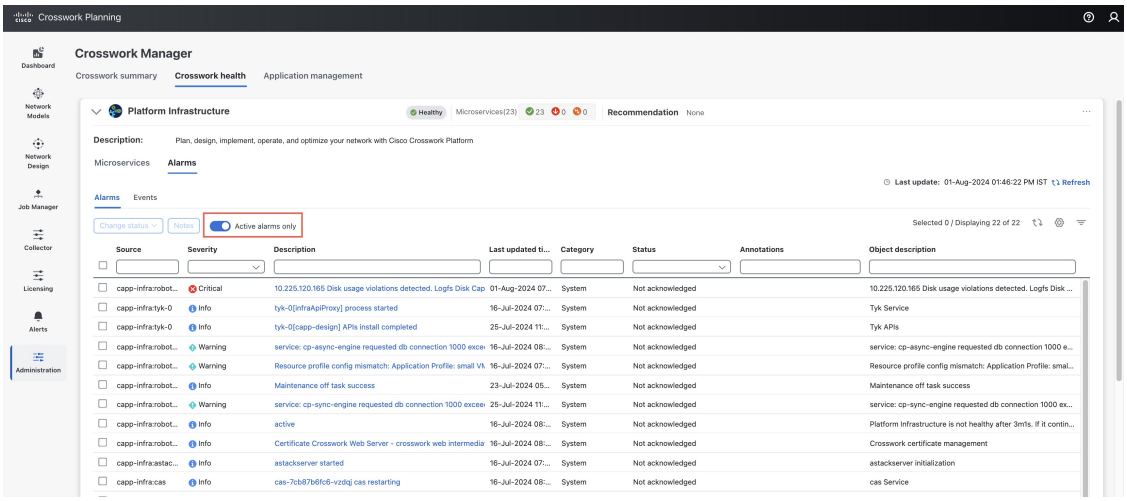
図 *33* : *[*アプリケーションの詳細（***Application Details***）*]* ページ



ステップ 3 マイクロサービスに関連するアラームとイベント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 *34* : *[*アラーム（***Alarms***）*]* タブ



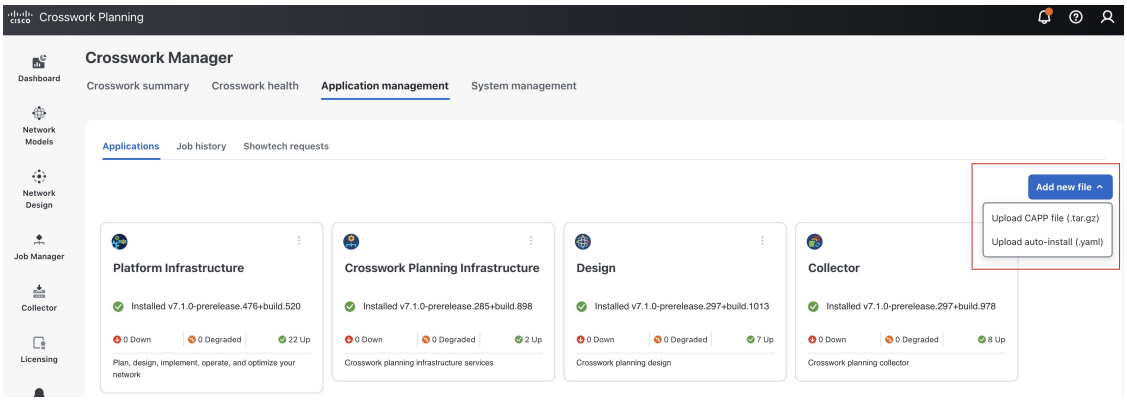
b) [イベント（Events）] タブをクリックします。リストには、すべての Crosswork Platform Infrastructure イベントおよび関連するアラームが表示されます。

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) メインメニューで、**[管理（Administration）]**、**>[Crosswork Manager]**、**>[アプリケーション管理（Application Management）]** タブ、**[アプリケーション（Applications）]** の順に選択します。このページには、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。**[新しいファイルを追加**

（**Add new file**）] をクリックして、別のアプリケーションバンドルまたは自動インストールファイルをアップロードすることで、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 *35 : [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 *21 : 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、Backup and Restore の管理（178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（障害発生後に Cisco Crosswork Planning を復旧する （182 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、障害発生後に Cisco Crosswork Planning を復旧する （182 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）]（詳細については、「バックアップと復元を使用してデータを移行する（184ページ）」を参照）	Cisco Crosswork Planning の古いバージョンから新しいバージョンにデータを移行します。

Backup and Restore 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。
- Cisco Crosswork Planning 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。

Cisco Crosswork Planning のバックアップの作成時または復元時は、次の手順を実行します。

- 最初のログイン時に、バックアップファイルを保存する接続先 SCP サーバーを設定します。これは1回限りのセットアップであり、バックアップを作成したり、復元操作を開始したりする前に完了する必要があります。
- バックアップ操作または復元操作は、スケジュールされているメンテナンス期間に行います。これらの操作中、ユーザーはシステムにアクセスしてはいけません。バックアップではシステムが約 10 分間オフラインになりますが、復元操作には時間がかかり、他のアプリケーションが一時停止し、データ収集ジョブに影響を与える可能性があります。
- バックアップの作成に使用したものと同じプラットフォームイメージを災害後の復元に使用します。異なるソフトウェアバージョンは、災害後の復元と互換性がありません。
- ダッシュボードを使用して、バックアップまたは復元プロセスの進行状況をモニターします。エラーや内容の誤りを防ぐために、これらのプロセス中にシステムを使用しないでください。
- 一度に実行できるバックアップまたは復元操作は 1 つだけです。
- Cisco Crosswork Planning と SCP サーバーの両方が、同じ IP 環境（たとえば、両方とも IPv6 を使用）にあることを確認します。
- バックアップサーバーの領域を確保するために、古いバックアップを削除することもできますが、これらはジョブリストに引き続き表示されます。
- より多くの変更を行うオペレータは、より頻繁に（できれば毎日）バックアップする必要がありますが、他のオペレータは、週に1回または主要なシステムのアップグレードの前にバックアップを行えば十分です。
- デフォルトでは、システムが正常であると見なされない場合、バックアップは許可されませんが、トラブルシューティングのために強制できます。

- コレクタエージェントを使用している場合は、Backup and Restore 操作後、停止状態のままになる可能性があるため、手動で再起動します。

始める前に

作業を開始する前に、次を確認してください。

- セキュアな SCP サーバーのホスト名または IP アドレスおよびポート番号。サーバーに十分なストレージがあることを確認してください。
- バックアップファイルの接続先として使用する SCP サーバー上のファイルパス。
- 接続先 SCP サーバーのリモートパスに対するファイルの読み取り/書き込み権限を持つアカウントのユーザークレデンシャル。
- 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、**[接続先を編集（Edit destination）]** ドロワーパネルを表示します。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）]** > **[データをバックアップ（Data backup）]** の順に選択し、宛先サーバーの詳細が事前に入力された **[データバックアップ（Data Backup）]** ドロワーパネルを表示します。
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) VM またはいずれかのアプリケーションの状態が、[正常（Healthy）]状態ではない場合に、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。

（注）
[Force] オプションは、シスコ カスタマー エクスペリエンス チームに相談した後にのみ使用する必要があります。

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/ロケーション（Remote path/Location）]**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）]**をクリックすると、Cisco Crosswork Planningにバックアップを完了するための十分な空きリソースがあるかを確認できます。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。

検証に失敗した場合は、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。

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（状態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。

（注）
バックアップ操作が完了したら、宛先 SCP サーバーディレクトリに移動し、バックアップファイルが作成されていることを確認します。このバックアップファイルは、アップグレードプロセスの後の段階で必要になります。

（注）
リストにバックアップジョブが表示されない場合は、[Backup and Restore Job Sets] テーブルを更新します。

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：[Job Details] パネルの [Status] アイコンのすぐ下にある [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）
SCPバックアップサーバーとの接続の問題（たとえば、ログイン情報の誤り、ディレクトリまたはディレクトリの権限の欠落、パスの欠落など）が原因でアップロードに失敗することがあります。こうした原因によることは、タスク `uploadBackupToRemote` の失敗によって示されます。このような状況が発生した場合は、SCP サーバーの詳細を確認し、誤りを修正してから再試行してください。または、[Upload backup] をクリックする前に、[Destination] ボタンを使用して、別の SCP サーバーとパスを指定できます。

ステップ 3 バックアップファイルから復元するには、次の手順を実行します。

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

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

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

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

推奨事項：復元後のアクション

復元プロセスが完了したら、通常のシステム操作を再開するために、次のアクションが実行されていることを確認します。

コレクションの編集

バックアップを復元した後、**[コレクタ（Collector）]**、>**[コレクション（Collections）]**ページで、一覧されている各コレクションで、Edit collection 操作を実行します。変更を加えずにコレクションを保存します。これにより、構成データが適切に更新されます。

エージェントの再起動

復元プロセスは、データベースとファイルシステムデータのみをコピーします。復元プロセスが完了すると、すべてのエージェントが停止状態になり、Cisco Crosswork Planning UI から手動で再起動する必要があります。

- **[エージェントをセットアップ（Setup Agent）]**ページで（**[コレクタ（Collector）]**、>**[エージェント（Agents）]**）、それぞれのエージェントに対して、**[起動（Start）]オプションを使用して**、NetFlow と SR-PCE エージェントを再起動します。詳細については、エージェント設定の編集 （27 ページ） を参照してください。
- [Traffic コレクタ（Traffic collector）] 構成ページで、**[トラフィックコレクション（Traffic collection）]**オプションを無効にしてから有効にして、トラフィックポーラーエージェントを再起動します。詳細については、トラフィック統計情報の収集 （102 ページ） を参照してください。

スケジューラーの実行

- 「今すぐ実行」スケジューラーを使用している場合は、スケジューラーを手動で実行します。
- スケジューラーに CRON ジョブが設定されている場合、スケジューラーは CRON ジョブの設定に基づいて自動的にトリガーされます。

障害発生後に Cisco Crosswork Planning を復旧する

ディザスタリカバリは、自然災害または人為的な災害によって Cisco Crosswork 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 7.2* 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。通常、これは作成した最新のバックアップファイルとなります。 Cisco Crosswork Planningバックアップファイルの名前は通常、次の形式に従います。

  `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`

- データのバックアップが作成されたときに古いCisco Crosswork Planningサーバーに存在していたアプリケーションの正確なバージョンをインストールします。バージョンが一致しないと、データの損失や復元ジョブの失敗につながる可能性があります。
- 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してください。異なるソフトウェアバージョンで作成されたバックアップを使用してクラスタを復元することはできません。
- システムの状態を、災害が発生する前に存在していた状態に正確に回復できるように、バックアップを最新の状態に保ちます。前回のバックアップ以降に新しいアプリケーションやパッチをインストールした場合は、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 Smart Licensing 登録は、障害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。

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。

バックアップと復元を使用してデータを移行する

データ移行のバックアップと復元を使用することは、Cisco Crosswork Planning インストールを新しいソフトウェアバージョンにアップグレードするとき、または既存のデータを新しいインストールに移動するときの前提条件です。

データ移行バックアップを作成する場合は、次のガイドラインに従ってください。

- データ移行ファイルを格納する宛先 SCP サーバーが設定されていることを確認してください。この設定は 1 回限りのアクティビティです。
- Cisco Crosswork Planning と SCP サーバーの両方は、同じ IP 環境内に存在する必要があります。たとえば、Cisco Crosswork Planning を IPv6 経由で通信している場合は、バックアップサーバーも IPv6 で通信している必要があります。
- Cisco Crosswork Planning インストールをアップグレードする場合にのみデータ移行バックアップを作成し、スケジュールされたアップグレードウィンドウ中にのみ作成することをお勧めします。データ移行のバックアップまたは復元操作の実行中は、Cisco Crosswork Planning にアクセスしないでください。

始める前に

次を保持していることを確認します。

- セキュアな接続先 SCP サーバーのホスト名または IP アドレスおよびポート番号。
- データ移行用バックアップファイルの接続先として使用する SCP サーバー上のファイルパス。
- 接続先 SCP サーバーのリモートパスに対するファイルの読み取り/書き込み権限を持つアカウントのユーザーログイン情報。

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、**[接続先を追加（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) データを別のインストールに移行する Cisco Crosswork Planning インストールに管理者としてログインします。

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

c) **[アクション（Actions）]** > **[データをバックアップ（Data backup）]** の順に選択し、宛先サーバーの詳細が事前に入力された **[データバックアップ（Data Backup）]** ダイアログボックスを表示します。

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

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

f) 必要に応じて残りのフィールドにも入力します。

別のリモートサーバーアップロード先を指定する場合：事前に入力された **[ホスト名（Host name）]**、**[ポート（Port）]**、**[ユーザー名（Username）]**、**[パスワード（Password）]**、および **[リモートパス/ロケーション（Remote path/Location）]** フィールドを編集して、別の接続先を指定します。

g) **[バックアップ（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一式を作成し、それを **[ジョブ一式をバックアップしてリストア（Backup and Restore Job Sets）]** テーブルに追加します。[Job Details] パネルには、完了した各バックアップステップのステータスが表示されます。

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

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

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

リモートサーバーの問題が原因でアップロードが失敗した場合は、[バックアップのアップロード（Upload backup）] をクリックする前に、[接続先（Destination）] ボタンを使用して別のリモートサーバーとパスを指定します。

ステップ 3 バックアップの新しいインストールへの移行（**Migrate the backup to the new installation**）

a) バックアップからデータを移行する先の Cisco Crosswork Planning インストールに管理者としてログインします。

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

c) **[アクション（Actions）]** > **[データ移行（Data Migration）]** の順に選択し、リモートサーバーの詳細が事前に入力された **[データ移行（Data Migration）]** ダイアログボックスを表示します。

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

e) **[移行を開始（Start Migration）]** をクリックして、データ移行操作を開始します。Cisco Crosswork Planning は、対応するデータ移行ジョブ一式を作成し、それをジョブリストに追加します。

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

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。

エクスポートアイコン（）を使用すると、ログをCSV形式でエクスポートできます。CSVをエクスポートする場合は、デフォルトのファイル名を使用するか、一意の名前を入力するかを選択できます。

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バナーに表示する免責事項メッセージが必要です。バナーにより、権限を持つユーザーに対してシステムを使用する際の義務を通知したり、権限を持たないユーザーに警告することができます。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、次を実行できます。

- **[プレビュー（Preview）]** をクリックすると、Crosswork ログインプロンプトの前に表示される変更を確認できます。
- [変更の破棄（Discard changes）] をクリックすると、最後に保存したバージョンのバナーに戻ります。
- [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）]** の順に選択し、**[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構成の更新

[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）] > [コレクションの設定（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構成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 メインメニューで、**[管理（Administration）] > [設定（Settings）] > [システム設定（System settings）] > [コレクションの設定（Collection settings）] > [コレクタ機能（Collector capability）]** の順に選択します。

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。

コレクタ機能構成のダウンロード

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。

エージング設定の構成

このトピックでは、非アクティブな回路、ポート、ノード、またはリンクをシステムがネットワークから完全に削除するまで保持する期間を設定する方法について説明します。

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、永久に削除されます。削除された項目を復元するには、その項目を再検出する必要があります。エージングを設定すると、これらの要素がシステムから消去されるまでの保持期間を制御できます。

始める前に

⚠

注意 変更はグローバルに適用され、すべてのコレクション、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 メインメニューで、**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [コレクション設定（Collection Settings）] > [パージ遅延（Purge delay）]** の順に選択します。

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 ポートを非アクティブにした後、ネットワークに保持する時間を指定します。
- **L3 ノード**：L3ノードを非アクティブにした後、ネットワークに保持する時間を指定します。
- **L3 回路**：L3 回路を非アクティブにした後、ネットワークに保持する時間を指定します。

（注）
L3 ノードの値は、**L3 ポート** の値と同等かそれ以上にする必要があります。つまり、**L3 回路**の値以上にする必要があります。

ステップ 4 [保存（Save）] をクリックして変更を保存します。

システムは、非アクティブな回路、ポート、ノード、およびリンクを指定された期間保持してから、完全に削除します。

アーカイブされたプランファイル消去の設定

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）] > [コレクションの設定（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 ルートを設定します。

スタティックルートは、データインターフェイス経由で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。

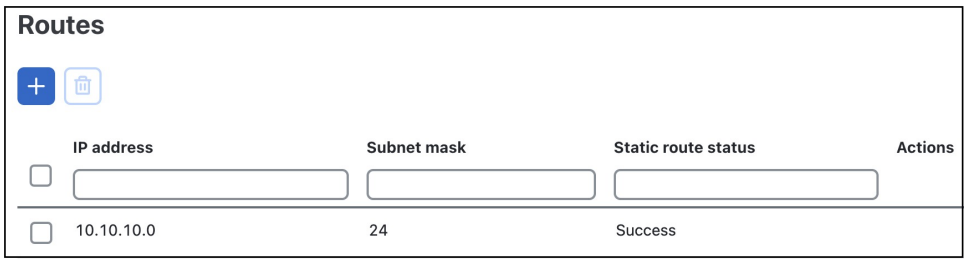
（注） スタティックルートの適用後、Crosswork シェルプロンプトで、**ip rule list** コマンドを実行すると、対応するエントリが表示されます。

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。