サポートされるコレクタとツール

ここでは、次の内容について説明します。

コレクタの説明

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

表 *1:* コレクタの説明

コレクター	説明	前提条件/注意事項	設定手順
基本的なトポロジ収集			

コレクター	説明	前提条件/注意事項	設定手順
IGP データベース	ログインと SNMP を使用して IGP トポロジを検出します。	これは、基本的なトポロジ収集です。結果として得られるネットワークモデルは、他のコレクタの送信元ネットワークとして使用されます。	IGP データベースコレクタを使用したトポロジ情報の収集 （4 ページ）を参照してください。
SR-PCE	SR-PCE 経由で BGP-LS を使用してレイヤ 3 トポロジを検出します。トポロジの送信元として生の SR-PCE データを使用します。ノードおよびインターフェース/ポートのプロパティは、SNMP を使用して検出されます。	• この収集を実行する前に、SR-PCE エージェントを設定する必要があります。詳細については、エージェントの設定 を参照してください。 • これは、SR-PCE を使用するネットワークの基本的なトポロジ収集です。結果として得られるネットワークモデルは、他のコレクタの送信元ネットワークとして使用されます。	SR-PCE コレクタを使用したトポロジ情報の収集 （6 ページ）を参照してください。
高度なモデリング収集			
LSP	SNMP を使用して LSP 情報を検出します。	• 基本的なトポロジ収集を備えたネットワークモデルが存在する必要があります。 • SR-PCE を使用している場合は、この収集を実行する前に SR-PCE コレクタを使用したトポロジ情報の収集 （6 ページ） を完了する必要があります。	LSP 情報の収集 （10 ページ）を参照してください。
PCEP LSP	（SR-PCE コレクタが基本トポロジコレクタとして選択されている場合にのみアクセス可能）SR-PCE を使用して PCEP LSP を検出します。	収集を実行する前に、SR-PCE コレクタを使用したトポロジ情報の収集 （6 ページ） を完了する必要があります。	SR-PCE を使用した PCEP LSP 情報の収集 （12 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 （18 ページ）を参照してください。

コレクター	説明	前提条件/注意事項	設定手順
VPN	レイヤ 2 およびレイヤ 3 VPN トポロジを検出します。	基本的なトポロジ収集を備えたネットワークモデルが存在する必要があります。	VPN トポロジの検出 （21 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 （31 ページ）を参照してください。
トラフィックとデマンドの収集			
インベントリ	ハードウェアインベントリ情報を収集します。	基本的なトポロジ収集を備えたネットワークモデルが存在する必要があります。	ハードウェアインベントリ情報の収集 （23 ページ）を参照してください。
マルチキャスト	特定のネットワークからマルチキャストフローデータを収集します。	基本的なトポロジ収集を備えたネットワークモデルが存在する必要があります。	ネットワークからのマルチキャスト フロー データのコレクタ （14 ページ）を参照してください。
レイアウト（Layout）	送信元モデルにレイアウトプロパティを追加して、視覚化を改善します。	• 集約ネットワークモデル。 • レイアウトコレクタを設定したら、レイアウトのプロパティを含むプランファイルをレイアウトモデルにインポートして戻す必要があります。	ネットワークモデルの可視化の向上 （35 ページ）を参照してください。
トラフィック収集	SNMP ポーリングを使用して、トラフィック統計情報（インターフェイス トラフィック、LSP トラフィック、MAC トラフィック、および VPN トラフィック）を収集します。	• 基本的なトポロジ収集を備えたネットワークモデルが存在する必要があります。 • LSP トラフィックを収集する場合、LSP を備えたネットワークモデルが存在する必要があります。LSP 情報の収集 （10 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 （21 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 （37 ページ）を参照してください

コレクター	説明	前提条件/注意事項	設定手順
デマンド推論	ネットワークからトラフィックデマンドに関する情報を収集します。	トラフィックデータを含む送信元 DARE ネットワークが存在する必要があります。	トラフィックデマンド情報の収集 （40 ページ）を参照してください。
NetFlow	エクスポートされた NetFlow および関連するフロー測定値を収集して集約します。	基本的なトポロジ収集を備えたネットワークモデルが存在する必要があります。	NetFlow 収集を構成する （42 ページ）を参照してください。
カスタム スクリプト			
外部スクリプト	カスタマイズされたスクリプトを実行して、送信元ネットワークモデルに追加データを付加します。	送信元ネットワークモデルとカスタムスクリプトが存在する必要があります。	ネットワークモデルに対する外部スクリプトの実行 （45 ページ）を参照してください

基本的なトポロジ情報の収集

基本的なトポロジ収集から得られるネットワークモデルは、追加のデータ収集のソースネットワークとして使用されます。Cisco Crosswork Planning 内には、この目的で使用される 2 つのコレクタ、**IGP データベース** と **SR-PCE** があります。トポロジ情報を収集するようにこれらのコレクタを設定する方法の詳細については、IGP データベースコレクタを使用したトポロジ情報の収集 （4 ページ）およびSR-PCE コレクタを使用したトポロジ情報の収集 （6 ページ）を参照してください。

IGP データベースコレクタを使用したトポロジ情報の収集

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

トポロジ収集に SR-PCE コレクタを使用するには、SR-PCE コレクタを使用したトポロジ情報の収集 （6 ページ）を参照してください。

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

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

始める前に

- ワークフロー：事前設定手順に記載されている手順を実行します。

IGP データベースコレクタを設定するには、次の手順を実行します。

手順

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

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

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

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

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

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

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

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

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

ステップ 6 （オプション）[詳細設定（Advanced settings）] パネルを展開し、関連するフィールドに詳細を入力します。詳細オプションの説明については、IGP および SR-PCE コレクタの詳細オプション （8 ページ）を参照してください。

ステップ 7 [次へ（Next）] をクリックします。

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

次のタスク

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

SR-PCE コレクタを使用したトポロジ情報の収集

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

トポロジ収集に IGP データベースコレクタを使用するには、「IGP データベースコレクタを使用したトポロジ情報の収集 （4 ページ）」を参照してください。

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

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

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

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

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

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

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

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

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

始める前に

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

SR-PCE コレクタを設定するには、次の手順を実行します。

手順

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

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

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

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

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

ステップ 4 （オプション）[詳細設定（Advanced settings）] パネルを展開し、関連するフィールドに詳細を入力します。詳細オプションの説明については、IGP および SR-PCE コレクタの詳細オプション （8 ページ）を参照してください。

ステップ 5 [次へ（Next）] をクリックします。

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

次のタスク

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

IGP および SR-PCE コレクタの詳細オプション

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

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

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

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

LSP 情報の収集

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

始める前に

ワークフロー：事前設定手順に記載されている手順を実行します。

LSP コレクタを設定するには、次の手順を実行します。

手順

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

ステップ 2 要件に応じて、いずれかの基本トポロジコレクタを選択します。

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

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

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

ステップ 5 次の設定パラメータを入力します。

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

ステップ 6 （オプション）[詳細設定（Advanced settings）] パネルを展開し、関連するフィールドに詳細を入力します。詳細オプションの説明については、LSP 収集の詳細オプション （11 ページ）を参照してください。

ステップ 7 [Next] をクリックします。

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

次のタスク

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

LSP 収集の詳細オプション

LSP コレクタを使用する場合は、いくつかの詳細オプションを設定できます。

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

SR-PCE を使用した PCEP LSP 情報の収集

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

始める前に

- ワークフロー：事前設定手順に記載されている手順を実行します。
- SR-PCE（SR-PC コレクタ）を使用した BGP-LS トポロジ収集がネットワークで完了していることを確認します。LSP を収集するための送信元ネットワークとしてこのモデルを使用する必要があります。詳細については、SR-PCE コレクタを使用したトポロジ情報の収集 （6 ページ）を参照してください。

PCEP LSP コレクタを設定するには、次の手順を実行します。

手順

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

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

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

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

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

ステップ 5 次の設定パラメータを入力します。

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

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

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

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

ステップ 7 [次へ（Next）] をクリックします。

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

次のタスク

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

ネットワークからのマルチキャストフローデータのコレクタ

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

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

始める前に

ワークフロー：事前設定手順に記載されている手順を実行します。

マルチキャストを設定するには、次の手順を実行します。

手順

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

ステップ 2 要件に応じて、いずれかの基本トポロジコレクタを選択します。

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

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

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

ステップ 5 次の設定パラメータを入力します。

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

ステップ 6 （オプション）[コレクタ設定（Collector Settings）] パネルを展開し、関連するフィールドに詳細を入力します。前のステップで選択したコレクタに基づいて、オプションが異なります。詳細オプションの説明については、マルチキャストコレクタの詳細オプション （15 ページ）を参照してください。

ステップ 7 [次へ（Next）] をクリックします。

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

次のタスク

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

マルチキャストコレクタの詳細オプション

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

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

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

BGP ピアリングの検出

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

始める前に

ワークフロー：事前設定手順に記載されている手順を実行します。

BGP コレクタを設定するには、次の手順を実行します。

手順

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

ステップ 2 要件に応じて、いずれかの基本トポロジコレクタを選択します。

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

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

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

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

ステップ 6 （オプション）[詳細設定（Advanced settings）] パネルを展開し、関連するフィールドに詳細を入力します。詳細オプションの説明については、BGP トポロジの詳細オプション （19 ページ）を参照してください。

ステップ 7 [次へ（Next）] をクリックします。

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

次のタスク

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

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

BGP トポロジの詳細オプション

BGP コレクタを使用する場合は、いくつかの詳細オプションを設定できます。

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

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

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

VPN トポロジの検出

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

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

始める前に

ワークフロー：事前設定手順に記載されている手順を実行します。

VPN コレクタを設定するには、次の手順を実行します。

手順

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

ステップ 2 要件に応じて、いずれかの基本トポロジコレクタを選択します。

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

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

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

ステップ 5 次の設定パラメータを入力します。

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

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

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

ステップ 7 [次へ（Next）] をクリックします。

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

次のタスク

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

ハードウェアインベントリ情報の収集

インベントリコレクタは、ハードウェアインベントリ情報を収集します。

収集されるハードウェア

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

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

ハードウェア階層

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

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

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

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

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

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

インベントリを処理するためのテーブル

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

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

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

ハードウェア テンプレートの設定

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

HWInventoryTemplates テーブル

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

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

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

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

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

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

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

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

複数の名前ソース列をコロンで指定できます。

例：Container,0,Model:Name

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

例：

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

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

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

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

HWInventoryTemplates エントリの追加

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

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

HWNameFormatRules テーブル

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

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

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

例：

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

テーブルの各エントリは次のように機能します。

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

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

モデルまたは名前によるハードウェアの除外

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

例：

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

テーブルの各エントリは次のように機能します。

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

HardwareSpec

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

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

例：

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

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

インベントリ収集の設定

始める前に

ワークフロー：事前設定手順に記載されている手順を実行します。

インベントリコレクタを設定するには、次の手順を実行します。

手順

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

ステップ 2 要件に応じて、いずれかの基本トポロジコレクタを選択します。

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

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

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

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

ステップ 6 （オプション）[詳細設定（Advanced settings）] パネルを展開し、関連するフィールドに詳細を入力します。詳細オプションの説明については、インベントリ収集の詳細オプション （29 ページ）を参照してください。

ステップ 7 [次へ（Next）] をクリックします。

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

次のタスク

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

インベントリ収集の詳細オプション

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

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

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

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

構成解析を使用したポート、LSP、SRLG、および VPN 情報の収集

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

始める前に

ワークフロー：事前設定手順に記載されている手順を実行します。

構成解析コレクタを設定するには、次の手順を実行します。

手順

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

ステップ 2 要件に応じて、いずれかの基本トポロジコレクタを選択します。

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

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

（注）

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

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

ステップ 6 [構成の取得（Get Config）] パネルと[構成の解析（Parse config）] パネルを展開し、関連するフィールドに詳細を入力します。フィールドの説明については、構成解析の詳細オプション （32 ページ）を参照してください。

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

ステップ 7 [次へ（Next）] をクリックします。

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

次のタスク

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

構成解析の詳細オプション

構成解析コレクタを使用する場合は、いくつかの詳細オプションを設定できます。

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

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

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

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

ネットワークモデルの可視化の向上

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

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

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

始める前に

ワークフロー：事前設定手順に記載されている手順を実行します。

レイアウトコレクタを設定するには、次の手順を実行します。

手順

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

ステップ 2 要件に応じて、いずれかの基本トポロジコレクタを選択します。

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

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

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

ステップ 5 次の設定パラメータを入力します。

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

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

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

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

ステップ 7 [次へ（Next）] をクリックします。

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

次のタスク

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

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

トラフィック統計情報の収集

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

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

始める前に

- ワークフロー：事前設定手順に記載されている手順を実行します。
- VPN トラフィックを収集する場合、VPN ネットワークモデルが存在する必要があります。VPN トポロジの検出 （21 ページ） を参照してください。
- LSP トラフィックを収集する場合、LSP ネットワークモデルが存在する必要があります。LSP 情報の収集 （10 ページ） を参照してください。

トラフィック収集コレクタを設定するには、次の手順を実行します。

手順

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

ステップ 2 要件に応じて、いずれかの基本トポロジコレクタを選択します。

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

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

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

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

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

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

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

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

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

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

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

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

ステップ 10 （オプション）[SNMP トラフィック計算（SNMP traffic computation）] パネルを展開し、関連するフィールドに詳細を入力します。フィールドの説明については、トラフィック収集の詳細オプション（39 ページ）を参照してください。

ステップ 11 [Next] をクリックします。

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

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

次のタスク

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

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

トラフィック収集の詳細オプション

トラフィック収集を使用する場合は、いくつかの詳細オプションを設定できます。

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

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

トラフィックデマンド情報の収集

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

始める前に

ワークフロー：事前設定手順に記載されている手順を実行します。

デマンド推論コレクタを設定するには、次の手順を実行します。

手順

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

ステップ 2 要件に応じて、いずれかの基本トポロジコレクタを選択します。

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

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

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

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

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

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

設定にさらにステップを追加するには、このステップを繰り返します。

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

ステップ 7 [次へ（Next）] をクリックします。

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

次のタスク

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

NetFlow データ収集

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

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

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

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

NetFlow 収集の構成

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

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

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

NetFlow 収集を構成する

始める前に

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

NetFlow コレクタを設定するには、次の手順を実行します。

手順

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

ステップ 2 要件に応じて、いずれかの基本トポロジコレクタを選択します。

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

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

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

ステップ 5 次の設定パラメータを入力します。

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

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

（オプション）他のフィールドに情報を入力します。フィールドの説明については、NetFlow 収集の詳細オプション （44 ページ）を参照してください。

ステップ 7 （オプション）[IASフロー（IAS flows）] パネルと [デマンド（Demands）] パネルを展開し、関連するフィールドに詳細を入力します。各オプションの説明については、NetFlow 収集の詳細オプション （44 ページ）を参照してください。

ステップ 8 [次へ（Next）] をクリックします。

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

次のタスク

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

NetFlow 収集の詳細オプション

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

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

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

ネットワークモデルに対する外部スクリプトの実行

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

始める前に

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

ネットワークモデルに対して外部手順を実行するには、次の手順を実行します。

手順

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

ステップ 2 要件に応じて、いずれかの基本トポロジコレクタを選択します。

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

ステップ 4 次の詳細を入力します。

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

ステップ 5 [次へ（Next）] をクリックします。

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

次のタスク

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

AS プランファイルのマージ

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

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

（注）

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

始める前に

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

手順

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

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

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

ステップ 4 次の設定パラメータを入力します。

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

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

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

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

ステップ 7 [次へ（Next）] をクリックします。

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

次のタスク

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

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。