セグメンテーション

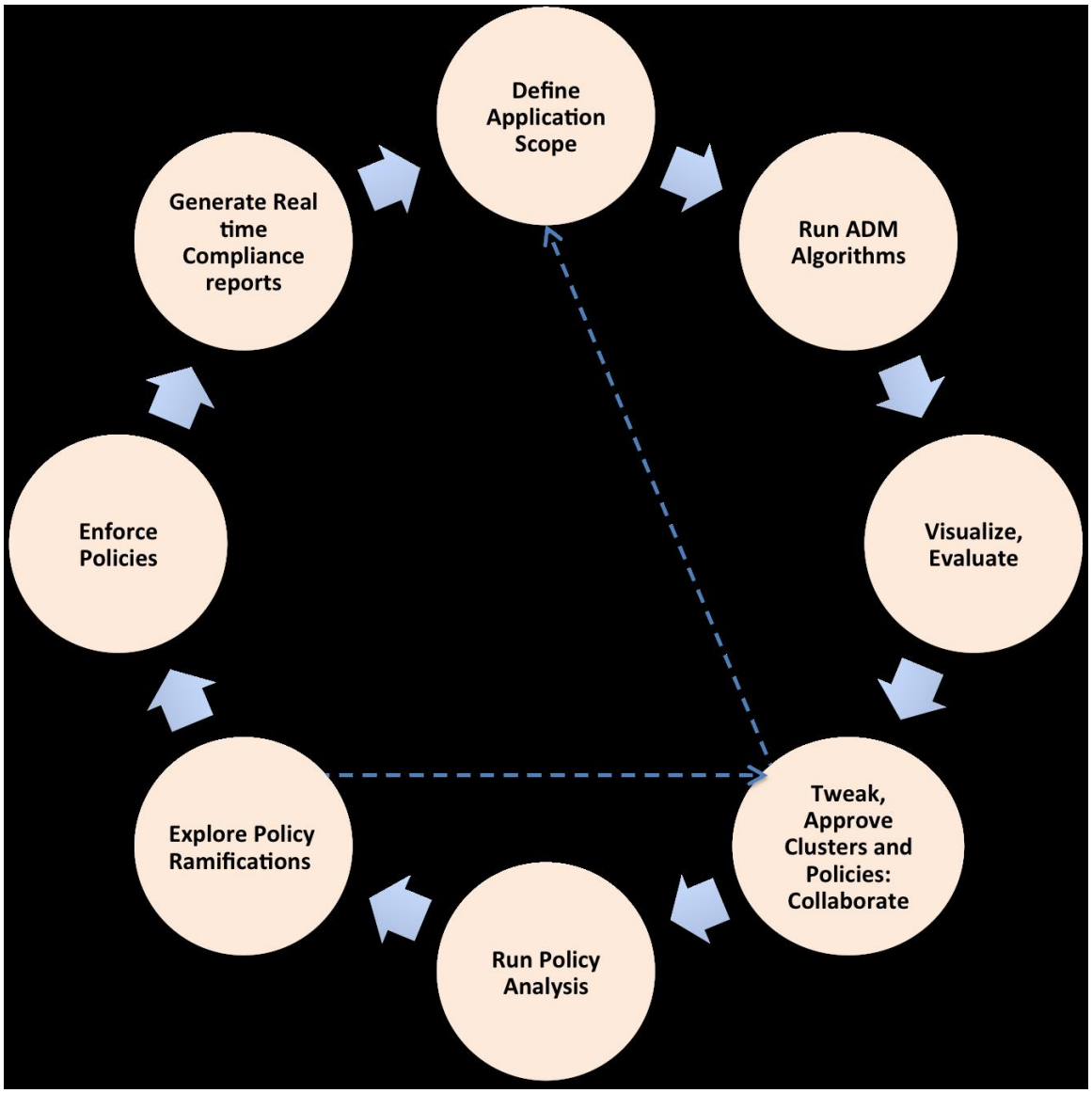
セグメンテーションポリシーは、組織のワークロード間で許可および拒否するトラフィックを制御します。

このポリシーは手動で作成することも、Secure Workloadがネットワーク上の既存の通信パターンに基づいてポリシーを提案することもできます。

ポリシーを確認、改良、分析し、組織が必要とするトラフィックのみを許可することが確実になったら、ポリシーを承認して適用します。

次の図は、セグメンテーションポリシーのライフサイクルの概要を示しています。

図 *1:* ポリシーのワークフローサイクル



セグメンテーション関連のページには、左側のナビゲーションバーの**[防御（Defend）]>[セグメンテーション（Segmentation）]**からアクセスできます。

- ポリシー管理用ワークスペース （3 ページ）
- デフォルトのポリシー検出設定 （8 ページ）
- ナビゲーション （10 ページ）
- ポリシーの自動検出 （17 ページ）
- クラスタ：範囲内のワークロードのグループ （44 ページ）
- 自動生成されたポリシーの確認 （50 ページ）
- カンバセーション （103 ページ）
- ポリシーテンプレート （111 ページ）

• その他の関数 （117 ページ）
• 自動ポリシー検出用の自動ロードバランサ設定（F5 のみ） （134 ページ）

ポリシー管理用ワークスペース

ワークスペース（以前は「アプリケーション ワークスペース」または「アプリケーション」と呼ばれていました）は、Secure Workload のポリシーを管理する場所です。

ワークスペース内の特定の範囲、またはその範囲に関連付けられたワークスペースのポリシーの定義、分析、適用など、ポリシー関連のアクティビティを実行します。

各ワークスペースは隔離された環境を提供するため、他のワークスペースに影響を与えずに実験を行うことができます。ネットワーク化されたアプリケーションのセット、および他の範囲のメンバーである「外部」ワークロードとの相互作用の分析に役立つ、多くの可視化ツールが提供されています。

ワークスペースへのユーザーアクセス

ワークスペースは、同じチームの複数のユーザーが共有ドキュメントとして使用するためのものです。

ワークスペースへのアクセスレベルは、ワークスペースに関連付けられた範囲に対して定義されたロールから定義できます。「ロール」を参照してください。

ワークスペースページへの移動

既存のアプリケーション ワークスペースを表示するか、新しいワークスペースを作成するには、ウィンドウの左側にあるナビゲーションバーから **[防御（Defend）]** > **[セグメンテーション（Segmentation）]** を選択します。

あるワークスペースを表示していて、ワークスペースのリストに戻りたい場合は、表示しているページの右上隅の近くにある [ワークスペースの切り替え（Switch Workspace）] リンクをクリックします。

ワークスペースの作成

新しいワークスペースを作成するには、次の手順を実行します。

1. [セグメンテーション（Segmentation）] ページで、[ワークスペース（Workspaces）] ボタンをクリックします。
2. 左ペインの範囲にカーソルを合わせ、青いプラス記号が表示されたらクリックします。
3. フォームに入力し、完了したら [作成（Create）] をクリックします。

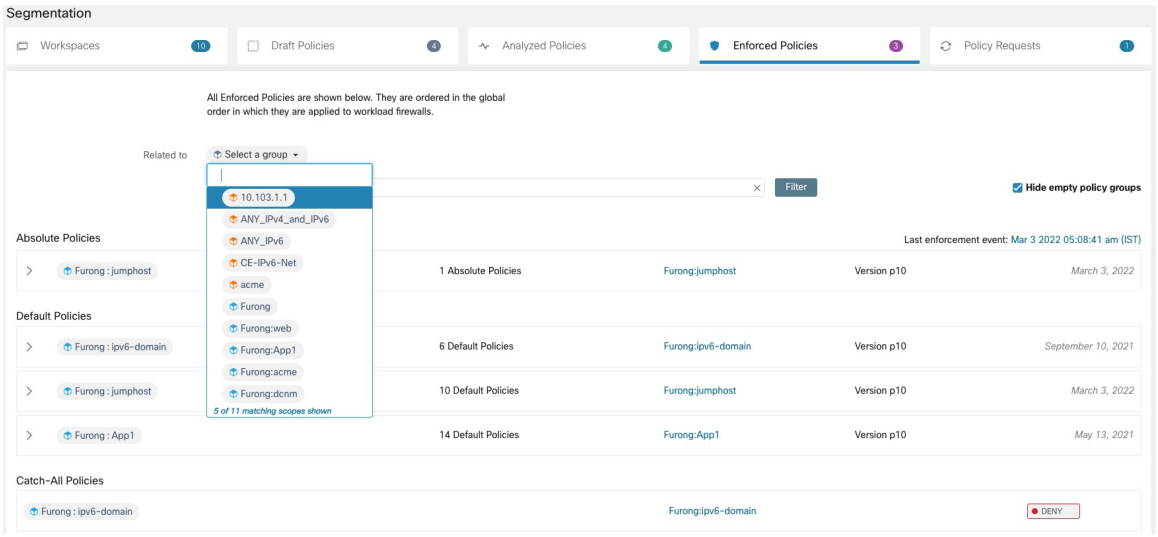
フィールドの説明：

フィールド名	定義
Name	ワークスペース名
説明	（オプション）後で参照するためのワークスペースの説明
スコープ	ワークスペースが関連付けられる範囲を指定します。これにより、このワークスペース内のポリシーの影響を受ける可能性のある一連のワークロードが決まります。 このワークスペースのユーザーロールとアクセス制御は、範囲を介して定義されます。 詳細については、「スコープ」の項を参照してください。

分析および適用されたポリシー

[セグメンテーション（Segmentation）] ページの上部にある [分析されたポリシー（Analyzed Policies）] タブと [適用されたポリシー（Enforced Polices）] タブには、分析されたポリシーと適用されたポリシーのグローバルビューがそれぞれ表示されます。このビューを使用して、親/祖先ワークスペースのポリシーの順序と優先度を検証できます。

図 *2:* ポリシーの優先度順の適用されたポリシーのリスト



同じルート範囲の下にある範囲またはフィルタを最初に選択し、選択した範囲またはフィルタをコンシューマまたはプロバイダーとして含むもののみにポリシーのリストを制限することができます。加えて、ポリシーのリストは、「ポート＝80」または「Action＝Deny」などの追加フィールドによってさらにフィルタリングできます。

使用可能なフィルタ：

フィルタ名	定義
ポート（Port）	照合するポリシーのポート（例：80）。
[Protocol]	照合するポリシーのプロトコル（TCPなど）。
承認済み（Approved）	[承認済み（Approved）] としてマークされているポリシーを照合します。承認済みポリシー（53 ページ）
外部？（External?）	ポリシーがワークスペース/範囲の境界を越えるかどうか。
アクション（Action）	ポリシーアクション：許可または拒否（Allow または Deny）

コンシューマとプロバイダーが異なる範囲にある場合：ポリシーオプション

次の状況は、クロス範囲ポリシーが必要な場合の例です。

範囲階層には、認証アプリケーション（プロバイダー）を含むネットワークサービス範囲が含まれています。範囲階層の別のブランチ上の範囲のメンバーである HR アプリケーションは、認証アプリケーションによって提供されるサービスのコンシューマです。

Cisco Secure Workload は、この状況に対処するいくつかの方法を提供します。組織に最適な方法は、組織内の範囲の所有状況、および複雑さと制御の望ましいバランスによって異なります。

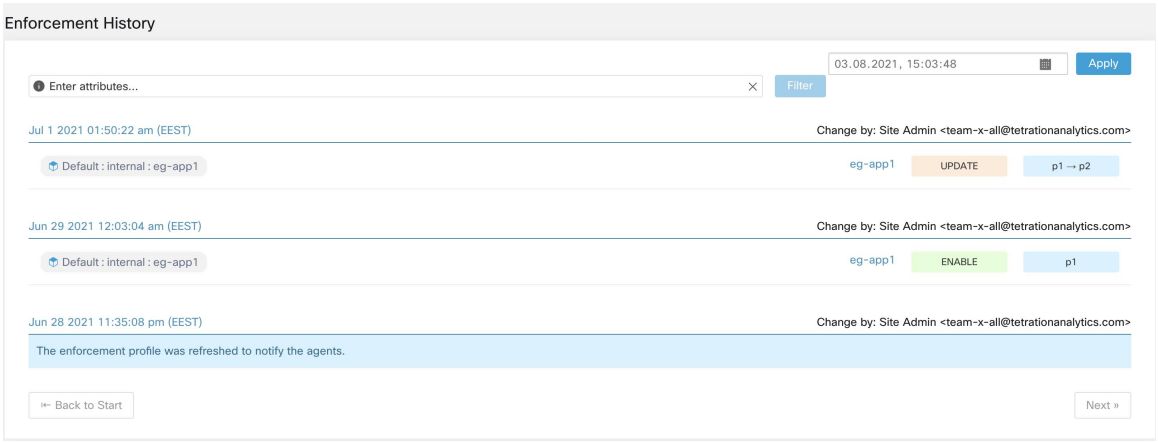
オプション	手順	長所と短所
コンシューマとプロバイダーの両方を子または子孫として含む親または祖先の範囲でこれらのポリシーを作成します。	• 共通祖先範囲に 1 つ以上のポリシーを手動で作成します。 （オプション）より正確なポリシーを得るには、インベントリフィルタを使用してワークロードをグループ化します。例と手順については、「インベントリフィルタの作成」を参照してください。 • ディープポリシー生成 （31 ページ） を使用して、共通祖先範囲のポリシーを自動的に検出します。	これらの方法は、実装が最も簡単です。 これらの方法では、コンシューマとプロバイダーのペアごとに 1 つのポリシーのみが必要です。

オプション	手順	長所と短所
クロス範囲ポリシーを作成するための高度な方法を使用する	ポリシー要求 （89 ページ）	この方法は実装が複雑になりますが、ワークロードが存在する範囲と同じ範囲にポリシーを存在させることができます。 この方法では、コンシューマポリシーとプロバイダーポリシーが異なる人によって所有されている場合にもポリシーを作成できます。 この方法では、コンシューマとプロバイダーのペアごとに、コンシューマ用のポリシーとプロバイダー用のポリシーの 2 つのポリシーが必要です。

適用履歴

適用履歴には、適用されたワークスペースとそのバージョンのリストに対する変更のリストが表示されます。適用履歴を表示するには、[セグメンテーション（Segmentation）] ページの右側にあるキャレット記号をクリックして [ツール（Tools）] メニューを展開し、[適用履歴（Enforcement History）] をクリックします。各セクションで、イベントと変更内容の概要が定義されます。イベントをクリックすると、その時点で適用されていたすべてのポリシーに関する詳細が表示されます。

図 *3*: 適用履歴ビュー



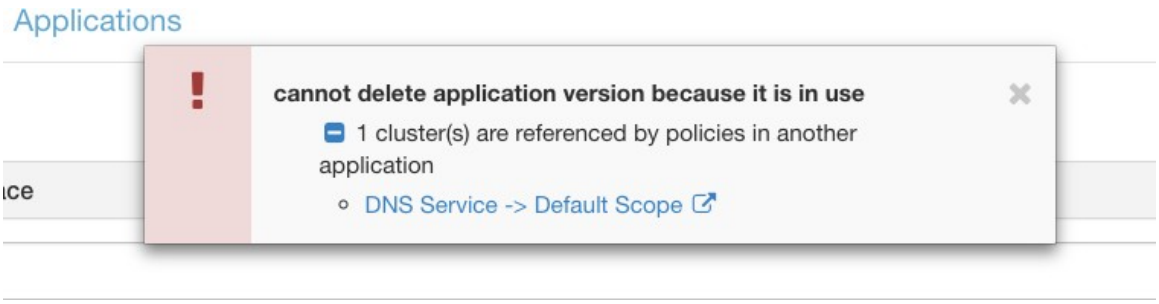
ワークスペースの削除

ワークスペースの横にあるメニューアイコンをクリックし、[ワークスペースの削除（Delete Workspace）] を選択すると、[セグメンテーション（Segmentation）] ページからワークスペー

スを削除できます。削除できるのは、セカンダリ（プライマリではない）ワークスペースのみです。

[提供されるサービス（Provided Service）] の結果として、あるワークスペース内のクラスタが別のワークスペース内のポリシーによって参照される可能性があります。この場合、従属ワークスペースは削除できず、依存関係のリストが返されます。この情報を使用して、依存関係を修正できます。

図 *4:* ワークスペースの削除を妨げる項目のリスト

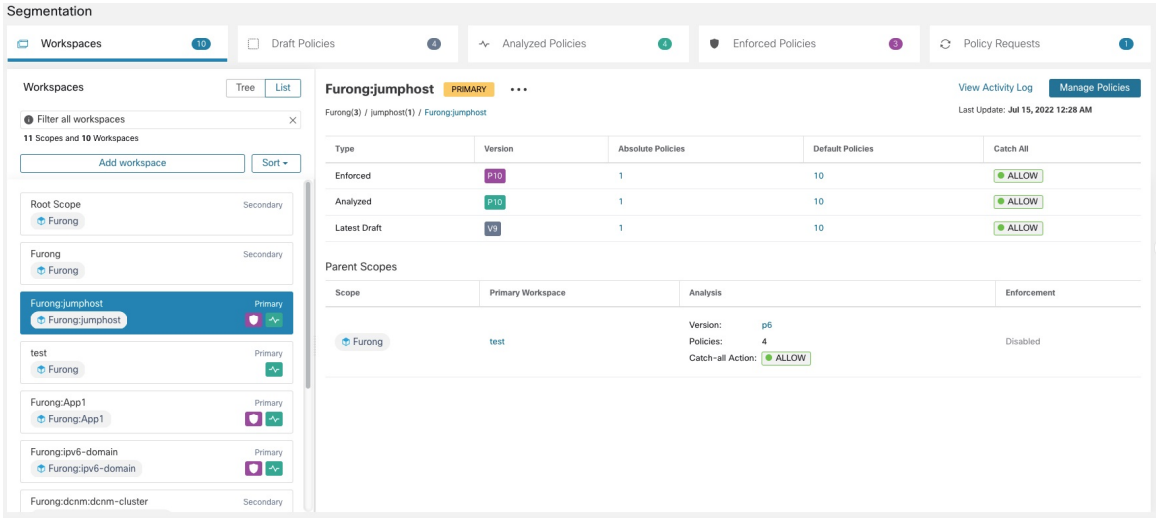


まれに、ワークスペースAがワークスペースBのクラスタに依存し、ワークスペースBがワークスペースAのクラスタに依存する相互依存関係が発生することがあります。この場合、個々のポリシーや公開されたポリシーバージョン（p*）を削除する必要があります。「削除制限」エラーでは、すべてのポリシーへのリンクが表示されるため、この削除を実行できます。

ワークスペースの表示または編集

既存のワークスペースの名前をクリックして、そのワークスペースを表示または編集します。現在アクティブなワークスペースがリストで強調表示されます。

図 *5:* ワークスペース管理ページ



プライマリおよびセカンダリワークスペース

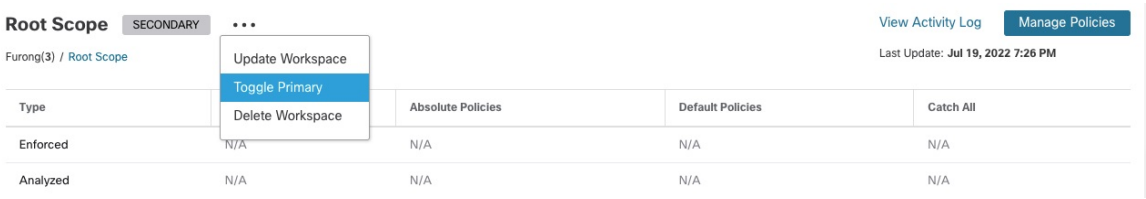
範囲ごとに、1 つのプライマリワークスペースと複数のセカンダリワークスペースを作成できます。

適用は、プライマリワークスペースのみで可能です。プライマリワークスペースでのみ使用できるその他の機能には、ライブ ポリシー コンプライアンス レポートとコラボレーティブ セキュリティ ポリシー定義があります。

セカンダリワークスペースを使用して、他のワークスペース（現在適用されているプライマリワークスペースを含む）に影響を与えずにポリシーを試すことができます。

ワークスペース名の横にあるメニューアイコンをクリックし、[プライマリの切り替え（Toggle Primary）] を選択することで、いつでもワークスペースをプライマリからセカンダリに、またはその逆に切り替えることができます。

図 *6:* プライマリとセカンダリの間でワークスペースを切り替える

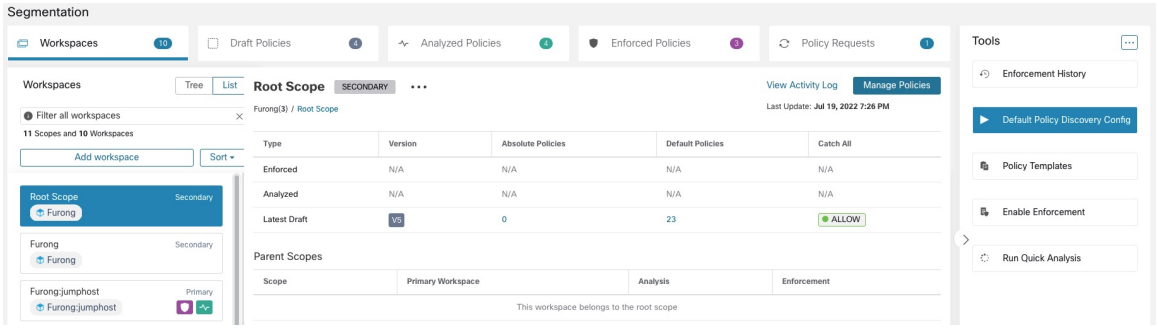


デフォルトのポリシー検出設定

ルート範囲全体の自動ポリシー検出のデフォルトオプションを設定するには、次の手順を実行します。

[防御（Defend）]>[セグメンテーション（Segmentation）]を選択し、ページの右側にあるキャレット記号をクリックして [ツール（Tools）] メニューを展開します。次に、[デフォルトのポリシー検出設定（Default Policy Discovery Config）] を選択します。

図 *7:* [デフォルトのポリシー検出設定（*Default Policy Discovery Config*）] ページへの移動



[デフォルトのポリシー検出設定（Default Policy Discovery Config）] ページのオプションについては、以下を参照してください。

- 外部依存関係 （21 ページ） およびサブトピック
- 自動ポリシー検出の詳細設定 （26 ページ） およびサブトピック
- デフォルトの除外フィルタ （9 ページ）

（注）
- 設定された外部依存関係は、以前の実行の依存関係よりも優先して使用されます。
- [詳細設定（Advanced Configuration）] オプションは、以前の実行を使用します（利用可能な場合）。

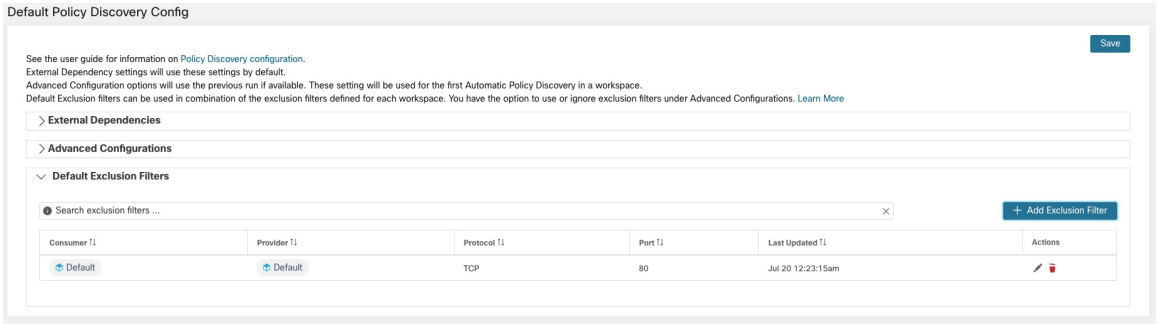
デフォルトの除外フィルタ

除外フィルタを使用して、検出対象外とするトラフィックフローを指定することで、自動ポリシー検出によって提案されたポリシーとクラスタを微調整できます。

詳細については、「除外フィルタ」を参照してください。

テナント内のすべてのワークスペースで使用できるグローバルなデフォルトの除外フィルタリストを作成し、ポリシーを検出するときにこのデフォルトリストを使用するかどうかをワークスペースごとに指定できます。

図 *8*: デフォルトの除外フィルタ



デフォルト除外フィルタの設定方法については、「除外フィルタの構成、編集、または削除（39 ページ）」を参照してください。

除外フィルタを有効または無効にする方法については、「除外フィルタを有効または無効にする （41 ページ）」を参照してください。

ナビゲーション

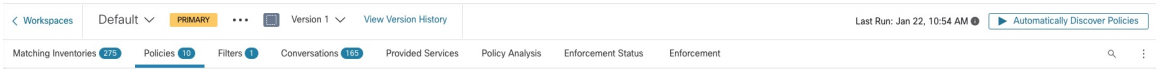
ワークスペースヘッダー

ワークスペースヘッダーには、次の 2 つの主な目的があります。

1. 名前を表示して、ワークスペースと最新の実行に関する高レベルのコンテキストと、ワークロードやクラスタの数などのワークスペースに関する高レベルの統計情報の提供。
2. 調査を簡素化し、自動ポリシー検出の結果を使用するように設計されている複数のビュー間のクイックナビゲーション。

次の図には、ヘッダー機能の一部が注釈とともに表示されています。

図 *9:* ワークスペースヘッダー



側面パネル

ワークスペース内でワークロード、クラスタ、またはポリシーを検索するには、次の手順を実行します。

1. **[防御（Defend）] > [セグメンテーション（Segmentation）]** の順に選択します。
2. 左側の範囲内にあるワークスペースをクリックします。
3. [ポリシーの管理（Manage Policies）] をクリックします。
4. 虫眼鏡マークをクリックします。

サイドパネル機能は、さまざまなワークスペースページで共有されます。サイドパネルには通常、[情報（Info）] と [検索（Search）] という 2 つのメインタブがあります。

[情報（Info）] タブには、選択したオブジェクトに関する詳細を表示することで、複雑な多数のチャートのコンテキストが提供されます。[情報（Info）] タブ内のコントロールを使用すると、他のビューに簡単に移動して、ホストやアプリケーションの特定の側面に関するより多くのインサイトを得られます。

[検索（Search）] タブは、ワークスペース内の関連するワークロード、クラスタ、またはポリシーを見つける最も簡単な方法です。検索は、一連の**フィルタ**を使用して定義されます。複数のフィルタは、論理 AND として扱われます。IP アドレスと数値の場合、「port: 80,443」のようにカンマを使用して論理 OR を指定できます。数値の範囲クエリ「port: 3000-3999」もサポートされています。

使用可能なフィルタ：

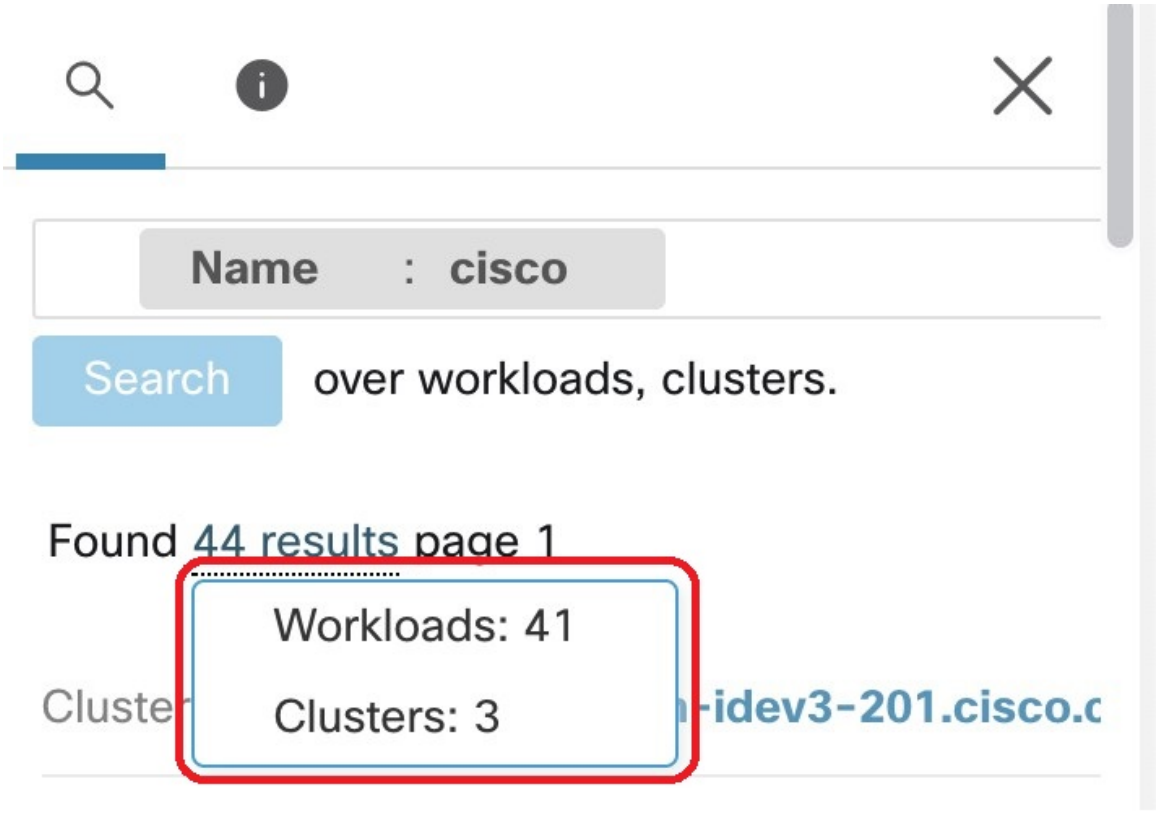
フィルタ	説明
Name	クラスタ名またはワークロード名を入力します。大文字と小文字を区別する部分文字列検索を実行します。
説明	クラスタの説明を検索します。
承認済み（Approved）	「true」または「false」の値を使用して、承認されたクラスタに一致します。
アドレス（Address）	CIDR 表記（例：10.11.12.0/24）を使用してサブネットまたは IP アドレスを入力します。このサブネットと重複するワークロードまたはクラスタに一致します。
スーパーネット（Supernet）	ワークロードがこのサブネットに完全に含まれているクラスタと一致するように、CIDR 表記（例：10.11.12.0/24）を使用してサブネットを入力します。
Process	大文字と小文字を区別する部分文字列検索を使用して、ワークロードプロセスを検索します。
プロセス UID（Process UID）	ワークロードプロセスのユーザー名を検索します。
ポート（Port）	ワークロードプロバイダーポートとポリシーポートの両方を検索します。
[Protocol]	ワークロードプロバイダープロトコルとポリシープロトコルの両方を検索します。
コンシューマ名（Consumer Name）	ポリシーのコンシューマクラスタ名に一致します。大文字と小文字を区別する部分文字列の一致を実行します。
プロバイダー名（Provider Name）	ポリシーのプロバイダークラスタ名に一致します。大文字と小文字を区別する部分文字列の一致を実行します。
コンシューマアドレス（Consumer Address）	提供された IP またはサブネットとコンシューマアドレスが重複するポリシーに一致します。
プロバイダーアドレス（Provider Address）	提供された IP またはサブネットとプロバイダー アドレスが重複するポリシーに一致します。

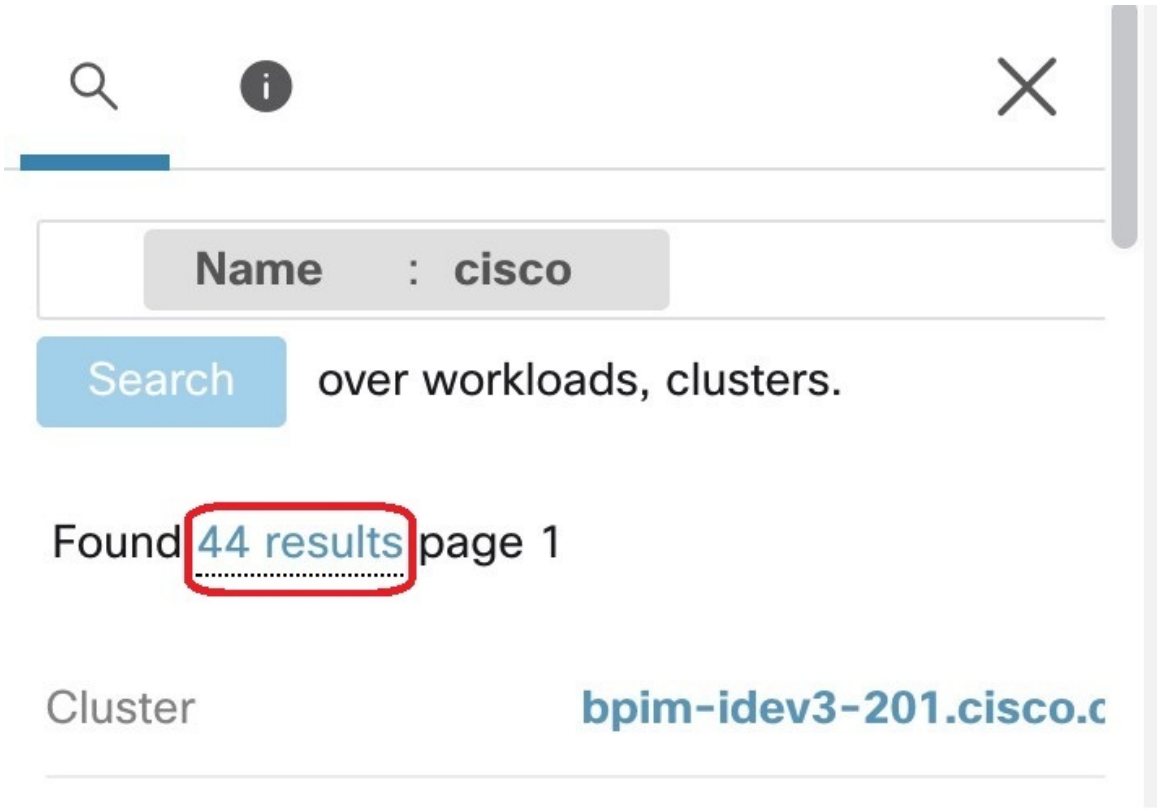
次の図は、サイドパネルの検索機能を示しています。

図 *10 :* サイドパネルの検索機能

特定のタイプでフィルタ処理するには、結果の合計をクリックし、ドロップダウンからタイプを選択します。タイプフィルタが追加され、検索が再実行されます。

図 *11* : 特定のタイプによる結果のフィルタリング

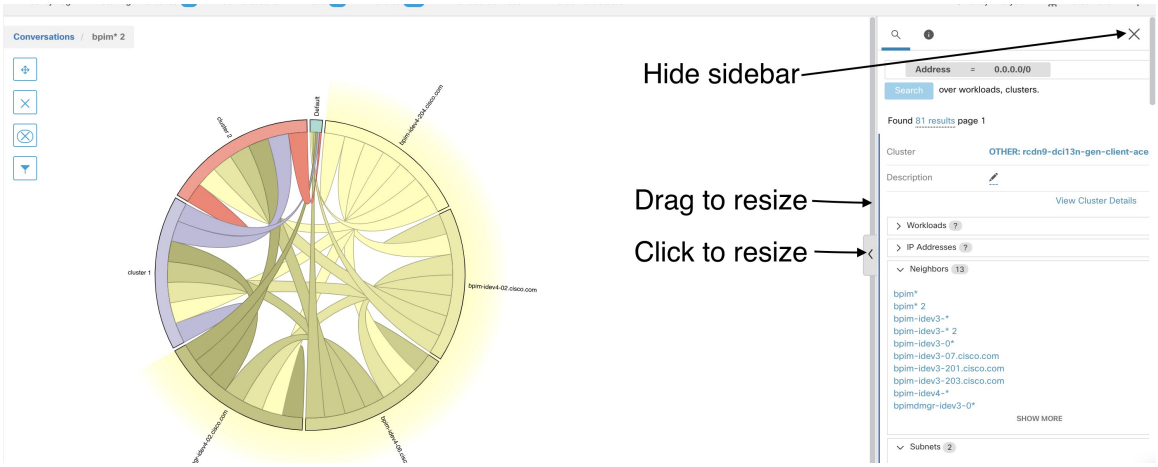




次の図は、チャート（ポリシービュー）の1つを選択するためのコンテキストを提供するサイドパネルを示しています。これは、多くのチャートで一般的な動作です。

（注） 端をドラッグして、サイドパネルのサイズを変更できます。

図 *12 : Policy View*



ポリシーの自動検出

範囲内にあるすべてのワークロードのポリシーを自動的に検出できます。

自動ポリシー検出（旧称アプリケーション依存関係マッピング（ADM））は、次のことを行います。

- コンピューティング動作の類似性に基づいて、ワークロードをクラスタにグループ化します
- 正常に完了したネットワークアクティビティに基づいて、一連の「許可」ポリシーを提案します。

通常、範囲のポリシーは、自動的に範囲ツリーの最下位付近（アプリケーションレベルなど）に表示されます。

ポリシー検出は必要な頻度で実行し、新しくインストールされたエージェントから得られた追加のフローデータ、検出期間内の別の時間範囲、およびオプションの高度なポリシー検出設定に基づいて、検出結果のポリシーを調整できます。

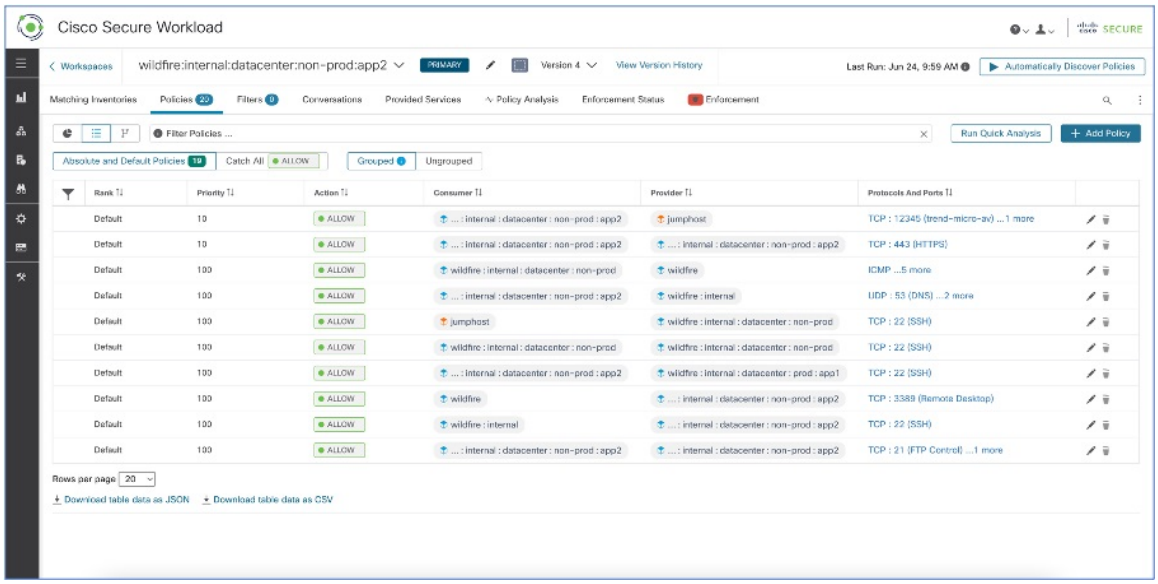
デフォルトでは、ポリシー検出は通信フロー（「カンバセーション」）を分析して結果を生成しますが、ワークロードで実行中のプロセスやロードバランサの設定といった他の情報をオプションで考慮に入れることができます。

自動ポリシー検出では、選択した時間範囲内で少なくとも一方の端が範囲メンバーワークロードであるカンバセーションが考慮されます。範囲のメンバーシップは、最新の範囲定義のみに基づきます。以前のメンバーシップは考慮されません。

ポリシーとクラスタの変更や承認を手動で行うこともできます。これにより、ポリシーとクラスタは引き継がれ、後続のポリシー検出が実行されても変更されません。

（注） 親および先祖範囲の最新プライマリワークスペースで手動で定義されたポリシーは、自動ポリシー検出の影響を受けません。

図 *13 :* 例：自動検出されたポリシー

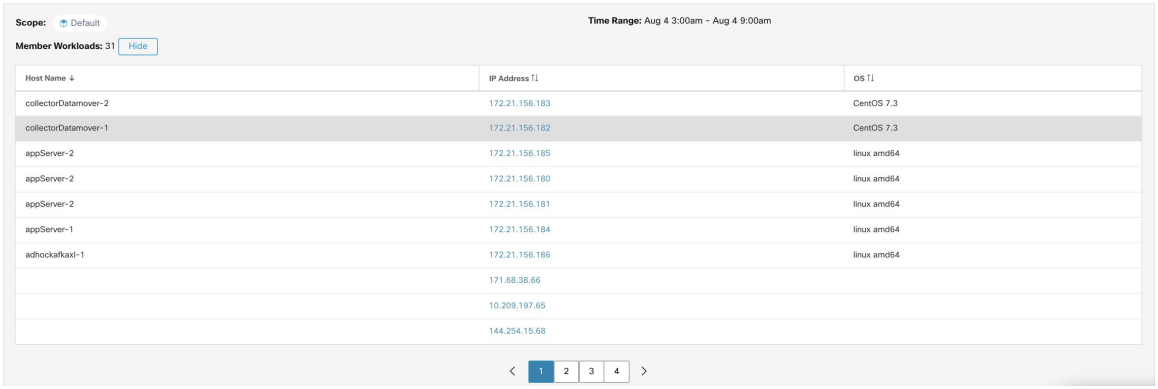


自動ポリシー検出に関連する複雑な概念の詳細については、「自動ポリシー検出の詳細設定（26 ページ）」を参照してください。

範囲内のワークロードの表示

ある範囲のメンバーのワークロードを表示するには、メンバーのワークロードカウントの横にある [表示（show）] ボタンをクリックします。

図 *14 :* メンバーのワークロードの表示



ポリシーの自動検出

この手順を使用して、特定の範囲のワークロードに対して推奨されるポリシーを生成します。

この手順を使用する場合：

- 通常、ツリーの下位の範囲、特にアプリケーション範囲のポリシーは自動的に検出されます。

  （高度な代替手段については、ディープポリシー生成 （31 ページ）を参照してください。）

- 範囲内のすべてのワークロードがその範囲においてサブ範囲のメンバーでもある場合、親範囲でポリシーを検出しても結果は生成されません。代わりに、サブ範囲でポリシーを検出します。

始める前に

- 自動ポリシー検出の制限を満たします。

  必要に応じて、大きな範囲を小さな子範囲に分割します。

- ポリシーを自動的に検出する前に、フローデータを収集する必要があります。

  これは通常、範囲内のワークロードにエージェントをインストール済みであるか、またはクラウドコネクタを使用してデータを設定および収集済みであるかを意味します。

  自動ポリシー検出で使用されるフローサマリーデータは、現在6時間ごとに計算されています。したがって、Cisco Secure Workload アプライアンスの初回の展開では、そのようなデータが利用可能になるまで、自動ポリシー検出はできません。

- 一般に、フローデータが多いほど、より正確な結果が得られます。

- ポリシーを検出したときに、特定の既存のポリシーを変更から保護する必要があります。承認済みポリシー （53 ページ）を参照してください。

- ポリシーを検出する前に範囲の変更をコミットしないと、設定された除外フィルタが期待どおりにフローと一致（除外）しない可能性があります。変更の確定を参照してください。

- （オプション）ポリシー検出を再実行する場合は次を参照してください。

  - 生成された既存のクラスタを保持する場合は、「自動ポリシー検出の再実行中のクラスタ変更の防止」を参照してください。

  - 既存の生成されたポリシーを保持する場合は、承認済みポリシー （53 ページ） を参照してください。

ステップ 1 **[防御（Defend）]** > **[セグメンテーション（Segmentation）]** の順に選択します。

ステップ 2 左側のペインの範囲ツリーまたは範囲のリストで、ポリシーを生成する範囲まで下にスクロールします。

ステップ 3 範囲内のワークスペース（プライマリまたはセカンダリ）をクリックします。

ステップ 4 [ポリシーの管理（Manage Policy）] をクリックします。

ステップ 5 [ポリシーを自動的に検出（Automatically Discover Policies）]（以前の [ADM実行を開始（Start ADM Run）]）をクリックします。

ステップ 6 含めるフローデータの時間範囲を選択します。

何度か試して、適切な時間範囲を見つけてください。最適な結果を得るため、何度でもポリシーを生成できます。

時間範囲を短くすると、結果の生成が速くなり、少なくなる可能性があります。

一般に、時間範囲が長いほど、より正確なポリシーが生成されます。ただし、範囲の定義が変更されている場合は、変更が行われる前の日付を含めないでください。

該当する場合は、時間範囲には定期的にのみ発生するトラフィック（たとえば、月次、四半期、年次など）を含める必要があります。たとえば、アプリケーションが他の時間にはアクセスしないソースから情報を収集する四半期レポートを生成する場合、時間範囲にはそのレポートのインスタンスが少なくとも 1 つ含まれていることを確認してください。

過去30日を超える時間範囲を設定するには、[カスタム（Custom）]範囲を選択し、時間選択ウィジェットのドロップダウンの下に希望の開始時刻と終了時刻を入力します。

ステップ 7 （オプション）[詳細設定（Advanced Settings）] を指定します。

通常は、最初の検出の実行では [詳細設定（Advanced Settings] は変更せず、必要な場合にのみ変更を行うことが推奨されます。

詳細については、自動ポリシー検出の詳細設定 （26 ページ）を参照してください。

ステップ 8 [ポリシーの検出（Discover Policies）] をクリックします。生成されたポリシーは、このページに表示されます。

次のタスク

- 自動ポリシー検出の進行状況の表示 （20 ページ） を表示します。
- 生成されたポリシーに別の範囲のプロバイダーが含まれているかどうかを確認します（コンシューマとプロバイダーが異なる範囲にある場合：ポリシーオプション （5 ページ）で状況が説明されています）。

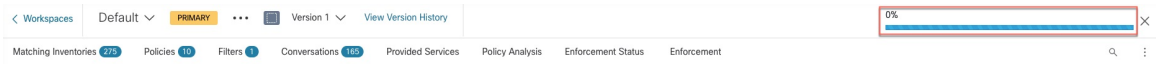
  含まれている場合は、そのトピックで説明されている方法のいずれかを使用して、このトラフィックのポリシーを作成します。

自動ポリシー検出の進行状況の表示

自動ポリシー検出の進行状況は常にヘッダーに表示されます。他のワークスペースに移動しても、進行状況には影響しません。[中止（abort）]ボタンを使用して、進行中に実行を中止できます。

実行が完了すると、メッセージが表示されます。成功した場合、[クリックして結果を表示（Click to see results）]をクリックして、実行前後の変更を示す別のビューに移動します。自動ポリシー検出が失敗した場合は、別のメッセージが表示され、場合によっては理由が示されます。

図 *15*：自動ポリシー検出の進行状況



外部依存関係

外部依存関係の設定は、自動ポリシー検出によって、コンシューマとプロバイダーが異なる範囲のメンバーに属しているポリシーが検出されたときに有効になります。

ポリシーが存在する範囲のメンバーではないワークロードは、外部ワークロードです。このようなワークロードは、（ポリシーが存在する範囲のメンバーである）ターゲットワークロードとの会話先です。

外部依存関係の設定は、ポリシーが検出された範囲以外の範囲のメンバーであるワークロードとの間の通信が関与する、自動検出されたポリシーを管理します（つまり、「外部ワークロード」が関与する通信）。

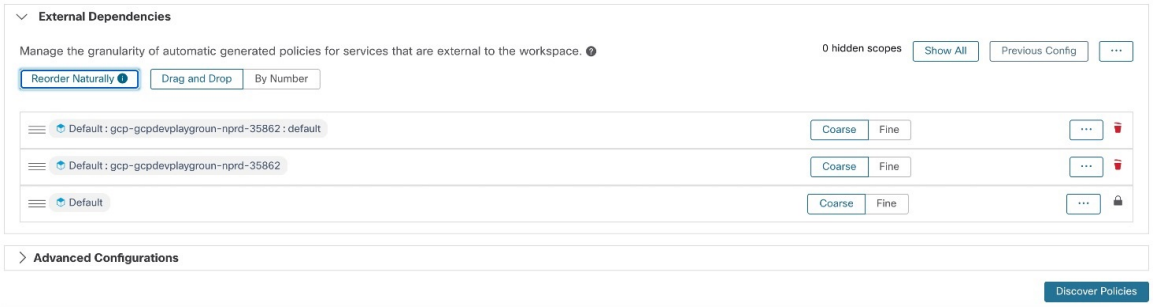
外部依存関係リストは、階層内のすべての範囲の順序付きリストです。リスト内の各範囲は、次のいずれかに設定されます。

- 特定のポリシーまたは（より安全な）改良ポリシーの生成、または
- より高度な範囲での大まかなポリシーの生成。こちらの方がより一般化しやすい場合があります（つまり、ポリシーの検出時に指定の時間範囲内で確認できなかった正当なフローを許可する可能性が高くなります）。

ポリシーの検出中に、ワークロードに一致する最初の範囲（またはクラスタ、またはカスタムフィルタ）を使用して「許可」ポリシーが生成されます。一致順（および結果的な粒度レベル）は、[外部依存関係（External Dependencies）]セクションに表示されるトップダウン方式のランク付けで決定されます。

デフォルトの範囲の順序が設定され、すべての範囲が「粗い（Coarse）」に設定されます。

図 *16*：デフォルトの外部依存関係



目的	操作手順
ワークスペースの外部依存関係を表示または微調整します。	ワークスペースに移動し、[ポリシーの自動検出（Automatically Discover Policies）] をクリックしてから、[外部依存関係（External Dependencies）] をクリックします。 範囲を並べ替え、それぞれの粒度オプションを選択するには、「ワークスペースの外部依存関係の微調整 （23 ページ）」を参照してください。
ルート範囲全体のデフォルトの外部依存関係を設定します。	デフォルトのポリシー検出設定 （8 ページ）を参照してください。

範囲のサブセットでのきめ細かいポリシーの検出

オプションで、範囲間よりもきめ細かいレベルでポリシーを検出して、範囲内のワークロードの指定されたサブセットへのトラフィックを制御できます。

たとえば、アプリケーション内の特定のタイプのホスト（API サーバーなど）に固有のポリシーを作成する場合、これらのワークロードをアプリケーション範囲内のサブセットにグループ化できます。

範囲内のワークロードのサブセットに対するポリシーを生成するには、以下を実行する必要があります。

1. 特定のポリシーを生成するサブセットごとに、インベントリフィルタを作成します。詳細と要件については、「ワークスペースの外部依存関係の微調整 （23 ページ）」の「始める前に」セクションを参照してください。
2. ポリシーを検出する場合：[外部依存関係（External Dependencies）] リストで、ポリシーを生成するインベントリフィルタを含むすべての範囲に対して [きめ細かい（Fine）] を選択します。

   完全な手順については、「ワークスペースの外部依存関係の微調整 （23 ページ）」を参照してください。

外部依存関係の調査に関するヒント

次のヒントを使用して、ポリシーが存在するワークスペースに関連付けられた範囲のメンバーではないワークスペースを含むポリシーの自動ポリシー検出の動作を調べます。

ヒント

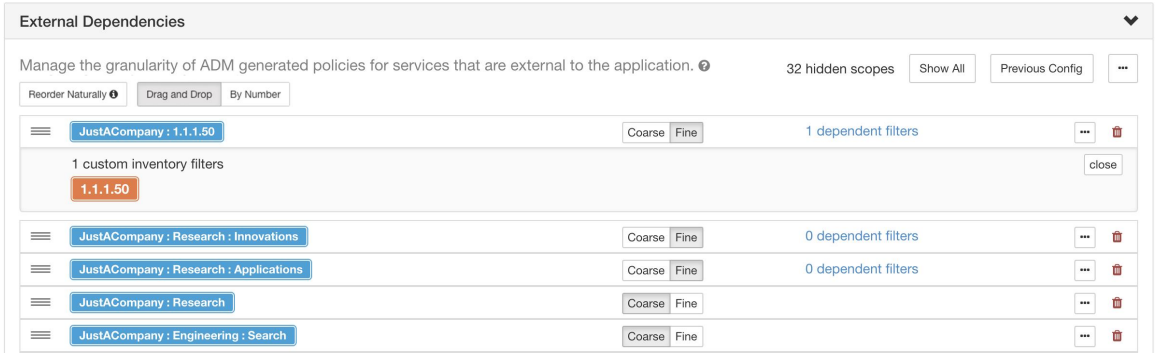
- リストを削除および再配置して、目的の粒度でポリシーを生成できます。たとえば、すべての Company:RTP サブ範囲を削除すると、Company:SJC 範囲に対してより高い粒度を維持しながら、個々のコンポーネントではなく Company:RTP 範囲全体に対する幅広いポリシーを生成できます。さらに、任意の範囲の横にある [詳細（Fine）] ボタンをクリックして、その範囲の下に定義されているより細かい候補の存在を確認できます。
- デフォルトでは、ルート範囲は外部依存関係リストの最下位のエントリとして構成されているため、自動ポリシー検出では可能な限り、常により具体的な範囲に対するポリシーが生成されます。最初は、比較的少数の大まかなポリシーを表示するために、ルート範囲を外部依存関係の最上位に一時的に配置できます。これで、自動ポリシー検出の後に、ワークスペースのすべての外部ポリシーが 1 つの範囲、つまりルート範囲にのみ接続されていることを確認できます（すべての外部ワークロードがルート範囲にマッピングされるため）。その結果、生成されるポリシーの数が少なくなり、調査と理解が容易になります。
- また、ワークスペースに関連付けられた範囲のメンバーであるすべてのワークロード（「内部ワークロード」）を 1 つのクラスタに一時的にバンドルし、クラスタを承認してから、ポリシーを検出することもできます。この場合も、クラスタリング（ワークスペースまたは範囲のサブパーティション化）が行われないため、一連のポリシーが減り、内部（内部ワークロードに接続）または外部（内部ワークロードを外部ワークロードに接続）するポリシーを表示できます。その後、内部ワークロードをバンドル解除したり、関心のある 1 つまたは複数の外部範囲をルートの上に配置したりすることで、徐々に詳細なポリシーを表示できます。
- **重要**ルート範囲を含むポリシーは、ネットワーク全体との間で送受信されるすべてのトラフィックを許可するため、常に注意深く調べてください。これは、ルート範囲が外部依存関係リストの下位に配置されていて、粗いポリシーの生成を意図していない場合に特に重要です。そのようなポリシーは、ワークスペース範囲に出入りするネットワーク全体のトラフィックに起因するポリシーではない可能性があります。むしろ、ルート範囲を超えて、より細かい範囲やインベントリフィルタの割り当てを受信できなかった複数の外部エンドポイントによってトリガーされる可能性があります。

  そのようなポリシーを監査するときは、関連する会話（「カンバセーション」を参照）を調べてエンドポイントを特定し、より細かい範囲またはインベントリフィルタに分類して、ルート範囲レベルでの安全性の低いポリシーを回避する必要があります。

ワークスペースの外部依存関係の微調整

ポリシーのプロバイダーがポリシーが検出されている範囲とは異なる範囲に属している場合、この手順を使用して、自動ポリシー検出時に（範囲全体ではなく）範囲内の指定されたワークロードのサブセット間でポリシーを作成します。

図 *17 :* 外部依存関係の微調整



始める前に

- 特定のポリシーを生成するワークロードのサブセットごとに、インベントリフィルタを設定します。任意の範囲で、任意の数のインベントリフィルタを作成できます。

  インベントリフィルタを作成するには、いくつかの方法があります。

  - 対象のクラスタをインベントリフィルタに変換する
  - 新しいインベントリフィルタを作成する。

    インベントリフィルタの作成を参照してください。

  インベントリフィルタでは、次のオプションを有効にする必要があります。

  - [クエリを所有権の範囲に制限する（Restrict Query to Ownership Scope）]

    [範囲外のサービスを提供する（Provides a service external of its scope）]

- （オプション）「外部依存関係の調査に関するヒント （22 ページ）」も参照してください。

ステップ 1 ポリシーを検出するワークスペースに移動します。

ステップ 2 [ポリシーを自動的に検出（Automatically Discover Policies）] をクリックします。

ステップ 3 [外部依存関係（External Dependencies）] をクリックします。

ステップ 4 必要に応じて、[すべての範囲を表示（Show All scopes）] をクリックします。

ステップ 5 （オプション）以前の設定を利用します。

- 最後にポリシーを検出したときにリストに加えた変更を再利用するには、[以前の設定（Previous Config）] をクリックします。
- グローバルな「デフォルトのポリシー検出設定」で外部依存関係を設定している場合は、[デフォルト設定（Default Config）] をクリックしてグローバルリストを使用できます。または、デフォルトのリストを取得した後、必要に応じて（そのワークスペースに対してのみ）変更し、[前の設定（revious Config）] を 1 回クリックすると、それ以降はカスタマイズされたバージョンを使用できます。

ステップ 6 必要に応じて範囲（および該当する場合はインベントリフィルタ）を並べ替えます。

ポリシーは、トラフィックに一致するリスト（上から順）の最初の範囲またはインベントリフィルタに基づいて適用されます。このためには、通常、トラフィックに一致する最も具体的なポリシーを適用する必要があるため、親（あまり具体的ではない）の上に子範囲（より具体的）が必要です。

- 新しい子範囲を最近作成した場合は、デフォルトでリストの一番下に追加されますが、リスト全体を並べ替えて、子範囲を親の上に配置します。

  [自然に並べ替える（Reorder Naturally）] をクリックします。

  図 *18 :* 自然に並べ替える

- リストを手動で並べ替えるには、次の手順を実行します。
  - [ドラッグアンドドロップ（Drag and Drop）] をクリックします。
  - [番号順（By Number）] をクリックします。

    外部依存関係には、10 の倍数で優先順位の値が割り当てられます。値を変更して順序を変更します。

    番号を変更したら、[表示（View）] をクリックしてリストの順序を更新し、10 の倍数を優先順位のそれぞれに再割り当てします。

ステップ 7 各行の精度を指定します。

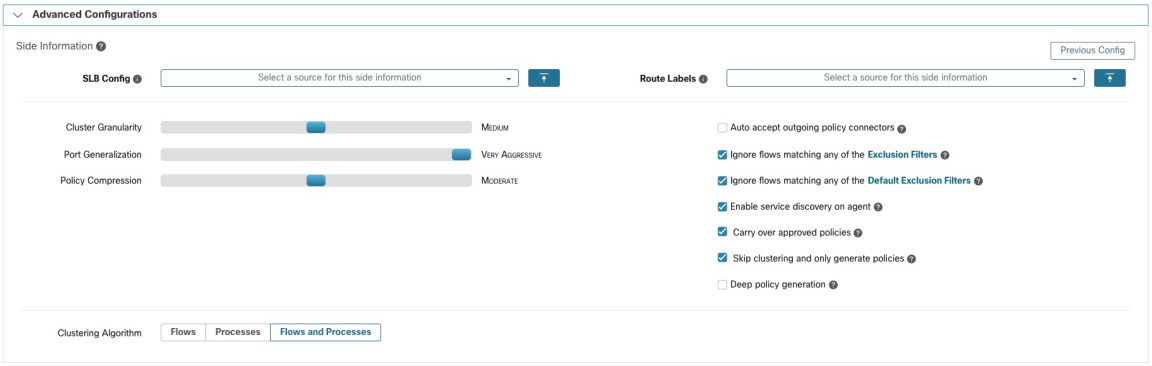
- 行ごとに、[粗い（Coarse）] または [細かい（Fine）] をクリックします。
- 範囲のすべてのサブ範囲に精度を適用するには、範囲の行の最後にある 3 つのドットのボタンをクリックします。 ···

自動ポリシー検出の詳細設定

詳細設定を使用して、ポリシーを検出する際に追加情報を指定することや、特定の環境に適応させることができます。

これらの設定にアクセスするには、該当するワークスペースで [ポリシーの自動検出（Automatically Discover Policies）] をクリックします。

図 *19 :* 自動ポリシー検出の詳細設定



ロードバランサとルータからのデータのアップロード

ロードバランサとルータからデータをアップロードして、自動ポリシー検出を通知できます。

次のオプションにアクセスするには、[自動ポリシー検出（Automatic Policy Discovery）] の設定で [詳細設定（Advanced Configurations）] をクリックし、[サイド情報（Side Informaton）] または [サイド情報（sideinfo）] セクションを確認します。

オプション	説明
SLB 構成 （ロードバランサ構成のアップロード）	ロードバランサからデータをダウンロードするには、「高度なポリシー検出設定を実現するためのロードバランサ設定の取得」を参照してください。 ロードバランサ構成のアップロードでサポートされている形式： • **F5 BigIP** • **Citrix NetScaler** • **HAProxy** • その他： **正規化された JSON** スキーマを使用します。 サポートされていないロードバランサ構成はこのスキーマに変換する必要があります。 この単純なスキーマには、仮想 IP（VIP）とバックエンド IP に関する基本情報が含まれています。 サンプル JSON ファイルをダウンロードするには、[SLB構成（SLB Config）] の横にある情報ボタンをクリックします。
ルートラベルのアップロード	プロビジョニングされたサブネットまたはルートのリストをルータからアップロードして、事前にプロビジョニングされた一連のサブネットに基づいてホストを分割できます。自動ポリシー検出によって生成されるクラスタリングの結果は、アップロードされたデータで定義されているサブネットの境界にまたがることはありません。自動ポリシー検出が完了したら、結果を変更できます。 サンプルの JSON ファイルをダウンロードするには、[ルートラベル（Route Labels）] の横にある情報ボタンをクリックします。

（注） クラスタはパーティションの境界にまたがりません。つまり、自動ポリシー検出によって計算されたクラスタには、2つの異なるパーティションのターゲットワークロードは含まれません。パーティションは、アップロードされたサイド情報（SLB、ルートなど）から計算されます。ただし、クラスタクエリ定義を変更すること（手動クラスタ編集）により、ワークロードをクラスタ間で自由に移動させたり、サイド情報のアップロードを無効化したりできます。

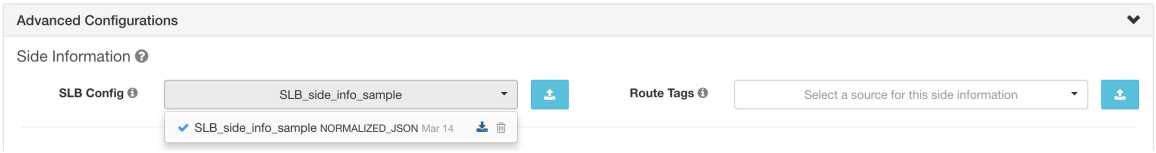
以前にアップロードした SLB 構成またはルートラベルファイルを表示または削除するには、次の手順を実行します。

1. [このサイド情報のソースを選択（Select a source for this side information）] というラベルの付いた個別のボックスをクリックします。

   アップロードしたファイルのリストが表示されます。

2. ファイルの横にあるダウンロードアイコンまたはゴミ箱アイコンをクリックして、ファイルを表示または削除します。

図 *20*：アップロードしたサイド情報



クラスタの細分度

クラスタリングの細分度を指定することで、自動ポリシー検出によって生成されるクラスタのサイズを制御できます。

- [細かい（Fine）]：クラスタの数が多くなりますが、サイズが小さくなります。
- [粗い（Coarse）]：クラスタの数は少なくなりますが、サイズは大きくなります。

（注） シスコのアルゴリズムでは、その他の多くのシグナルが考慮に入れられるため、結果に大きな変化が見られない場合があります。たとえば、生成されたクラスタの信頼度が非常に高い場合、このコントロールを変更しても結果はほとんど変わりません。

クラスタリングアルゴリズム（クラスタリングへの入力）

上級ユーザーは、クラスタリングアルゴリズムのデータの主なソース、つまり、ライブネットワークフロー、実行中のプロセス、またはその両方を選択できます。

ポートの一般化

自動ポリシー検出でのデフォルトポート（間隔）の一般化

Hadoop などの一部のアプリケーションは、32000 から 61000 など、一定の間隔で多くのサーバーポートを使用および変更します。自動ポリシー検出は、観察されたフローにおけるワークロードのサーバーポートの使用状況を使用して、各ワークロードでこうした動作を検出しようとします。自動ポリシー検出では、可能なポート（ただし 100 など多数のポート）の合計の一部のみを観察することで、任意のポート（たとえば 32000 から 61000）がワークロードによってサーバーポートとして使用できると「一般化」します。間隔内に含まれるポートは、このような間隔に置き換えられます（最小観測カウントについての特定の基準を満たす場合）。これにより、より少ない、よりコンパクトなポリシーが作成されます。間隔の推定は、正確なポリシーを計算するために重要です。十分な一般化が行われずにポリシーが適用された場合、将来の多数の正当なフローがドロップされてしまいます。多数のポートを 1 つまたはいくつかの間隔にマージすることにより、UI のレンダリング時間も大幅に高速化されます。

無効化を含むポートの一般化の程度を制御するには、以下で説明するオプションを使用します。

[詳細設定（Advanced Configurations）] の [ポート一般化（Port Generalization）] オプション

自動ポリシー検出の [詳細設定（Advanced Configurations）] の [ポート一般化（Port Generalization）] オプションは、ポートの一般化（つまり、単一のワークロードでサーバーポートとして使用される多数のポートをポート間隔に置き換えること）を実行するときに必要な統計的有意性のレベルを制御します。

ポートの一般化を無効にするには、スライダを左端に移動します。無効にすると、多数のサーバーポートがワークロードによって使用される場合、自動ポリシー検出および/または自動ポリシー検出の UI レンダリング時間が大幅に遅くなる可能性があることに注意してください。

スライダを右に動かすと、より積極的な一般化が行われます。ポート間隔を作成するために必要な証拠が少なくなり、元のポリシー（単一のポートを含む）をポート間隔に置き換えるための基準も緩和されます。

承認されたポリシーの引き継ぎ

このオプションは、デフォルトで有効です。

このフラグが設定されている場合、承認済みとしてマークされたすべてのポリシー（OpenAPI を使用して承認されたものを含む）が保持されます。これにより、自動ポリシー検出が「許可」ポリシーを検出した場合でも効力を発揮する必要がある特定の広範な拒否ルールを再定義する必要がなくなります。

詳細については、承認済みポリシー （53 ページ） を参照してください。

エージェントのサービス検出の有効化

このフラグが設定されている場合、エージェントノードに存在するサービスに関する一時的なポート範囲情報が報告されます。次に、報告されたポート範囲情報に基づいてポリシーが生成されます。

例：

- Windows Active Directory ドメインサーバーは、デフォルトの Windows エフェメラルポート範囲 49152 ～ 65535 を使用していくつかの要求を処理します。このフラグが設定されている場合、このポート範囲情報はエージェントによって報告され、この情報に基づいてポリシーが生成されます。

図 *21 :* サービス検出がエージェントで有効になっている

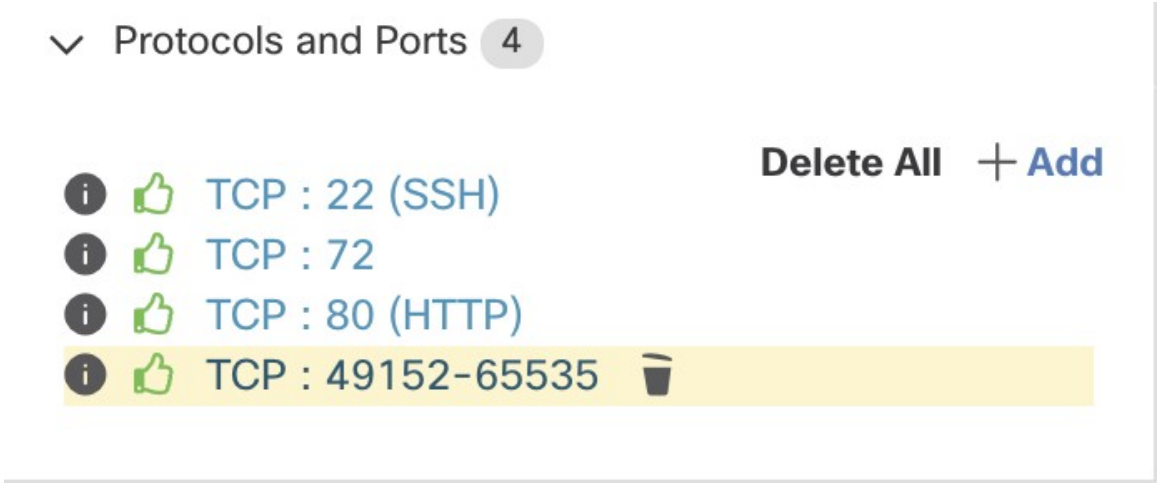
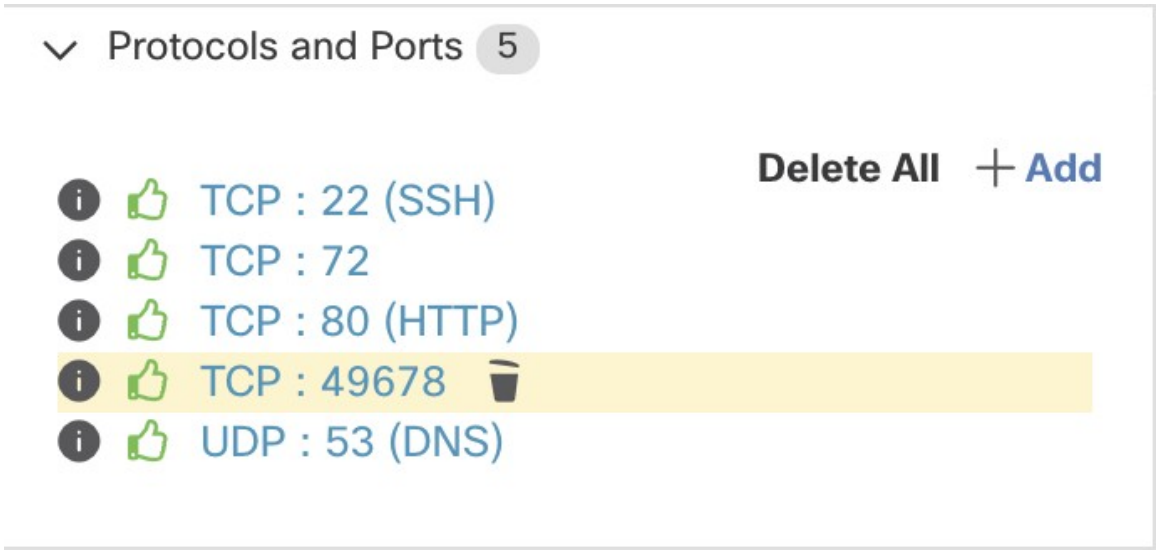


図 *22 :* サービス検出がエージェントで有効になっていない



ポリシー圧縮

ポリシー圧縮が有効になっている場合、ワークスペース内に生成されたクラスタの中で頻度が高いポリシー（同じプロバイダポートを使用するポリシー）は、まとめて親に移動される可能性があります。つまり、親範囲全体に適用可能な1つ以上のポリシーに置き換えられます。たとえば、ワークスペース内のすべてまたはほぼすべてのクラスタが同じコンシューマに同じポートを提供する場合、それらのポリシーはすべて親範囲からの1つのポリシーに置き換えられます。つまり、親範囲はそのポートでコンシューマに提供できます。したがって、ポリシーを圧縮すると、ポリシーの数を大幅に減らして簡素化することができます。また、ドロップされていた可能性のある正当なフローを今後は許可することにもつながる可能性があります（正確な一般化）。圧縮ノブの設定がより積極的であるほど、親ポリシーで置き換えるために必要なポリシー頻度のしきい値は小さくなります。

ディープポリシー生成オプションが選択されている場合：

このノブを使用して、階層型ポリシーの圧縮の積極性レベルを変更できます。

（注） 現在、自動ポリシー検出会話ページは、圧縮ポリシーが導かれた会話の表示をサポートしていません（圧縮を無効にするか、フロー検索を使用する必要がある場合があります）。

クラスタリングをスキップしてポリシーを作成

新しいクラスタは生成されず、既存の承認済みクラスタまたはインベントリフィルタからポリシーが生成されます。その他にも、ワークスペースに関連付けられた範囲全体が関係します（実際には、範囲全体を単一のクラスタとして扱います）。このオプションを使用すると、ポリシー数が大幅に減る (ただし、粗くなる) 可能性があります。

ディープポリシー生成

デフォルトでは、このオプションは無効になっており、ポリシー検出では、サブ範囲のメンバーではない範囲内のワークロードに関係する対話のみが考慮され、そのワークロードに対してのみポリシーが生成されます。

グローバルポリシー生成（例：範囲階層の最上位にある1つの範囲、またはツリーの最上位付近にあるいくつかの範囲）で**ディープポリシー生成**オプションを有効にすると、ほとんどすべてのワークロード間のトラフィックを許可する一連の粗いポリシーが生成されます。さまざまな範囲のメンバーであるワークロードと範囲階層のブランチ間のトラフィックも含まれます。

ディープポリシー生成が有効になっている場合：

- 範囲内のすべてのワークロード（サブ範囲のメンバー以外のワークロードだけでなく）に関係する対話は、ポリシーの生成に使用されます。

  したがって、ポリシーは、サブ範囲のメンバーでもあるかどうかに関係なく、範囲のメンバーであるすべてのワークロードに対して生成されます。

  これにより、範囲ツリーのブランチ全体のポリシーを生成できます。このとき、非常に多くのポリシーが生成される可能性があるので注意してください。

- ポリシーがサブ範囲または祖先範囲のワークロードのみに関係する場合でも、生成されたすべてのポリシーは、ディープポリシー検出が実行されたワークスペースに存在します。

  ポリシー検出が実行される範囲のメンバーであるかどうかに関係なく、対話のエンドポイントであるすべてのワークロードには、外部依存関係リストで指定された上から順序に、最も一致する範囲ラベルが割り当てられます。

- クラスタは作成されません。

このオプションが有効になっている場合の制限については、「自動ポリシー検出の制限」を参照してください。

（注） このオプションは、ルート範囲の所有者のみが使用できます。

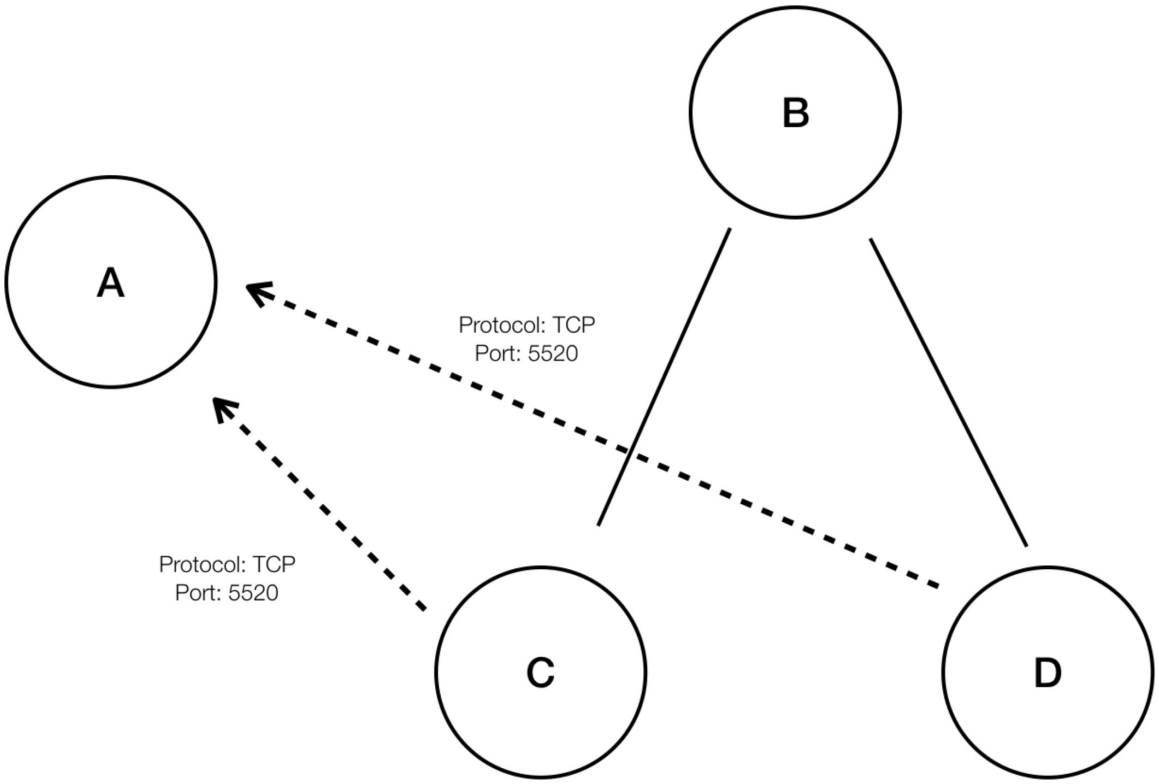
（注） 現在、自動ポリシー検出で表示されるワークロードの数には、サブ範囲のメンバーではないワークロードのみが含まれます。

階層型ポリシーの圧縮

ポリシー圧縮でも、ディープポリシー生成を行うこともできます。ポリシー圧縮ノブを使用して、階層型ポリシー圧縮の積極性レベルを変更できます。階層型ポリシー圧縮の例を以下に示します。

- A、B、C、D を範囲ツリーの範囲部分とし、「C」と「D」を「B」の子範囲とします。「C」→「A」をポート 5520 の TCP「ALLOW」ポリシーとし、「D」→「A」をポート 5520 の TCP「ALLOW」ポリシーとします。

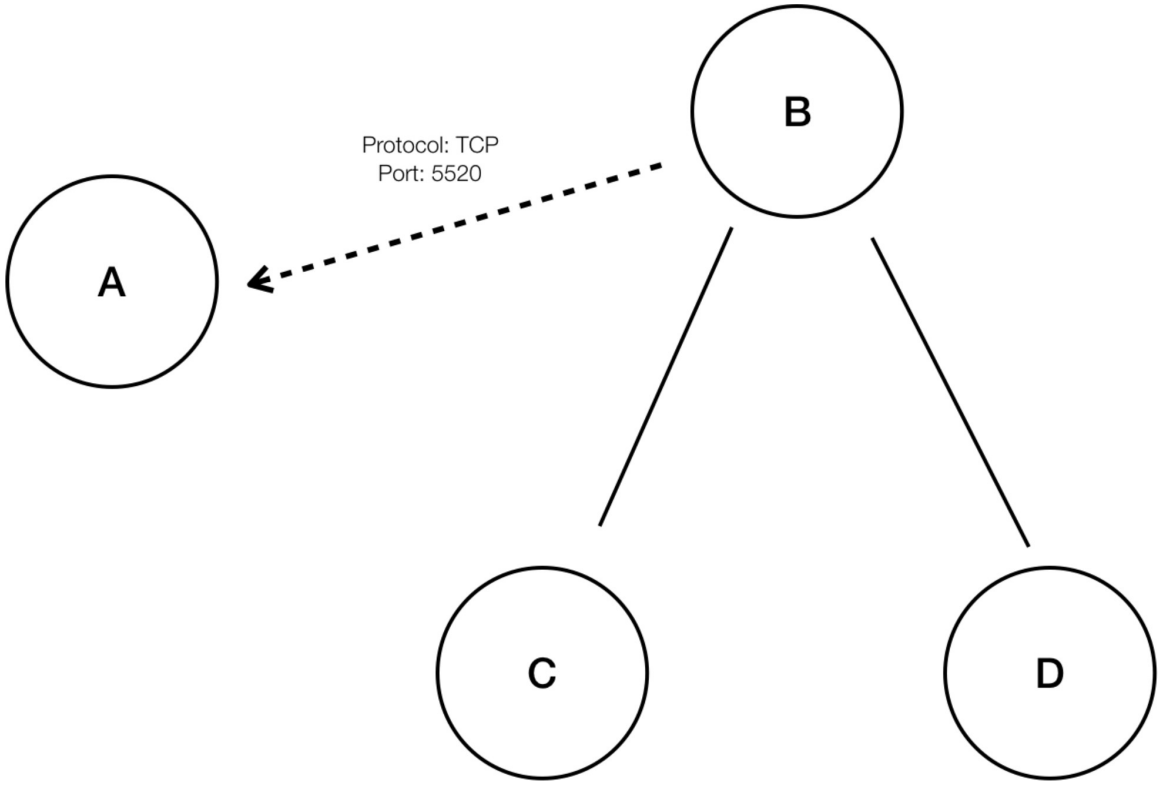
図 *23 :* 階層型ポリシー圧縮前



- 階層型ポリシー圧縮では、十分に大きなグループの子範囲が同じポート、プロトコル、宛先または送信元を共有するポリシーに関係している場合、これらのポリシーを、親範囲から共通の送信元または宛先に接続する一般化されたポリシーに置き換えることができま

す。上記の場合、「C」と「D」は「B」の子範囲であり、ポリシー「C」→「A」と「D」→「A」は同じ宛先、ポート、プロトコルを共有しています。「B」の子範囲の100%に同様のポリシーが含まれているため、ポリシーは「B」→「A」に昇格され、次のようになります。さらに、階層的な圧縮を繰り返すことができるため、一般化されたポリシーは、ディープポリシー生成が呼び出されるサブツリーのルートまでたどり着くことができます。

図 *24* : 階層型ポリシー圧縮後

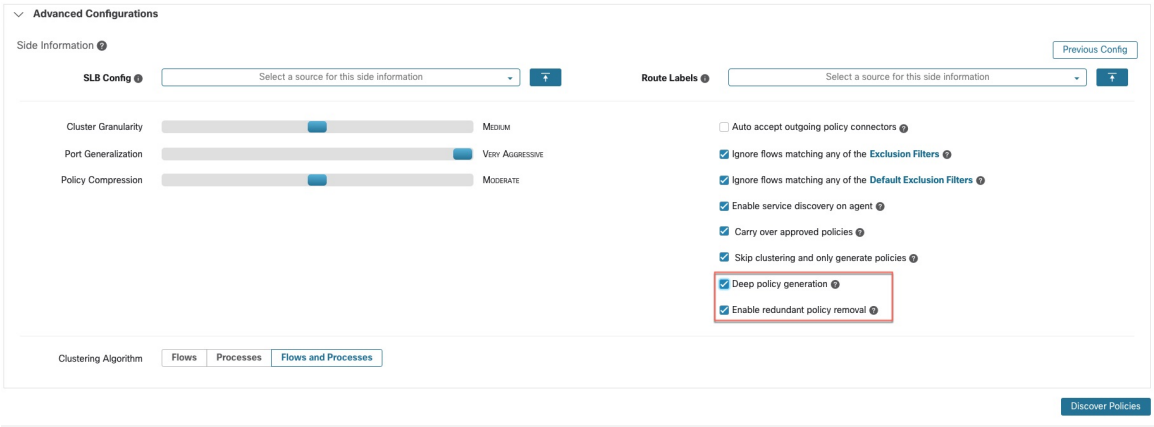


- ポリシー圧縮ノブを使用すると、ポリシーを共有する子範囲の、圧縮をトリガーする最小必要比率（通常は子範囲の総数に対する割合として測定される）を変更することにより、このような圧縮の積極性を調整できます。無効にすると、各ポリシーは、外部依存関係リストに基づいて、最も優先度の高い範囲間で生成されます。その後、自然に順序付けられた外部依存関係リストを適用することを選択した場合、生成されるポリシーは、数ある範囲の中で最も詳細なポリシーになります。

冗長ポリシー削除の有効化

このオプションは、ディープポリシー生成が有効になっている場合にのみ使用できます。

図 *25 :* ディープポリシー生成オプションが選択されている場合



このオプションは、冗長な詳細ポリシーの削除を有効/無効にします。

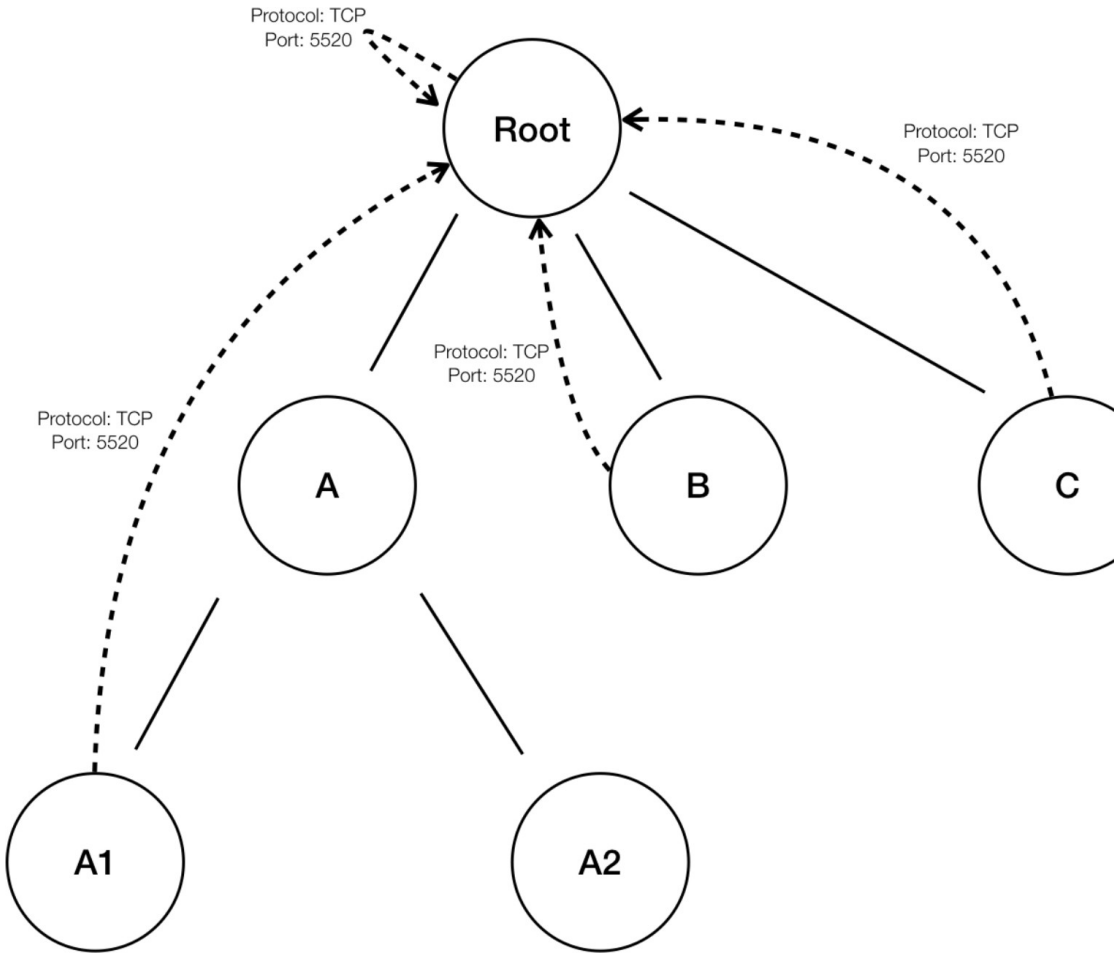
例：

- ルート、A、B、C、A1、およびA2を範囲ツリーの範囲部分とします。以下をポリシーとします。

1. “Root” → “Root”
2. “B” → “Root”
3. “C” → “Root”

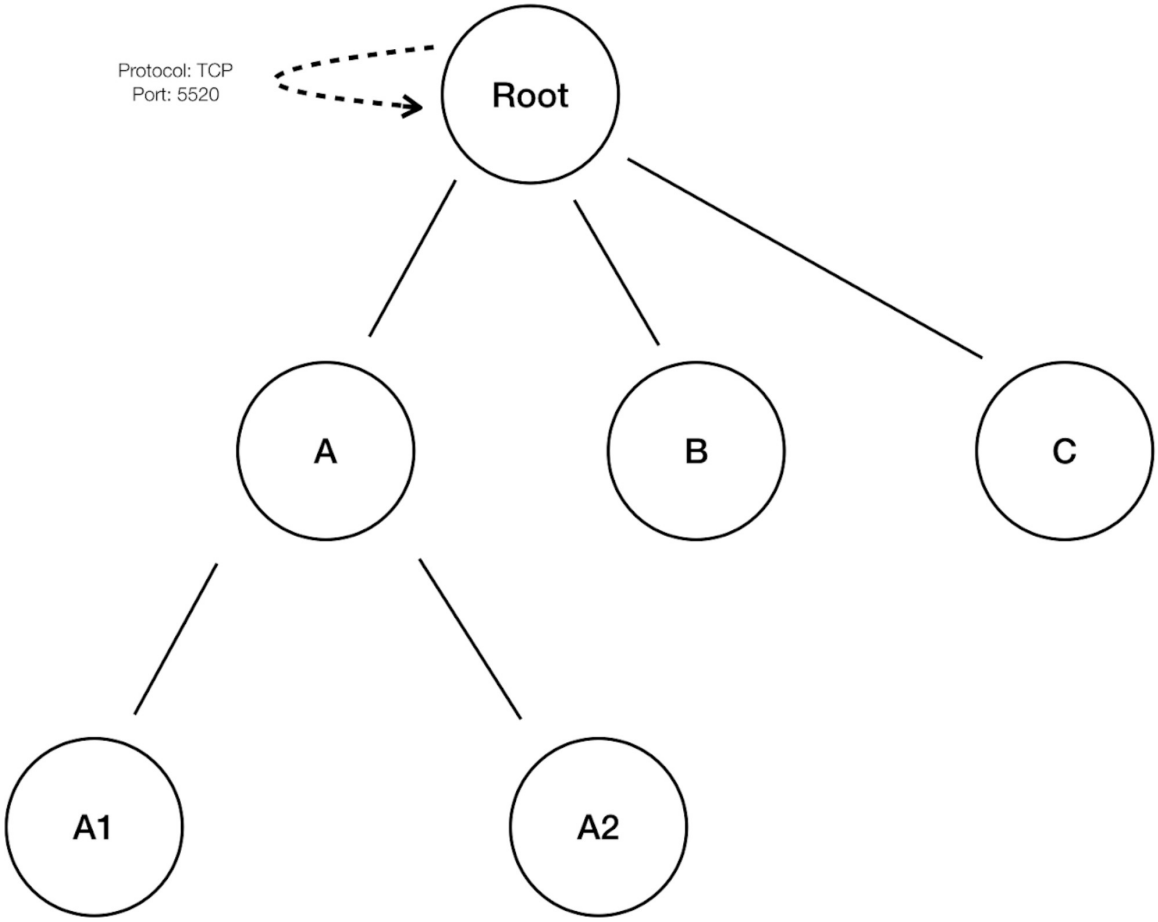
4. “A1” → “Root”

図 *26 :* 冗長ポリシーを削除する前



- ポリシー “B” →“Root”、“C” →“Root” および “A1”→ “Root” は、ポリシー “Root”→“Root” がこれらのポリシーをカバーしているため、冗長です。冗長ポリシーの削除機能は、そのようなポリシーをチェックして削除し、次のような単一のポリシー “Root” → “Root”のみを作成します。

図 *27 :* 冗長ポリシーを削除した後



冗長ポリシーの削除は、解釈可能なポリシーの簡潔なセットを維持するのに非常に役立ちます。縮小されたポリシーセットには、すべてのワークロードトラフィックをカバーするために選択された圧縮レベルで、最小限の数のポリシーが含まれます。ただし、ポリシー分析を通じてポリシーを常に監査し、対応するカンバセーションを調べて、結果として得られるポリシーの厳しさを評価する必要があります。より細かい範囲またはインベントリフィルタに分類されていないエンドポイントとの間のトラフィックが存在する場合、これは特に重要です。このようなエンドポイントは、ルート範囲を含むポリシーなど、意図したよりも粗いポリシーの生成を引き起こす可能性があります。それと同時に冗長ポリシーの削除が有効になっている場合、より粒度の高いポリシーは削除され、表示されなくなります。（圧縮された）ポリシーのソースを診断し、より細かいレベルのポリシーを確認するには、ポリシーの圧縮と冗長ポリシーの削除機能をオフにします。また、現在、自動ポリシー検出のカンバセーションページでは、圧縮/一般化されたポリシーにつながるカンバセーションが表示されない場合があることにも注意してください。これを回避するには、圧縮と冗長ポリシーの削除を無効にすると、生成されたポリシーにつながるカンバセーションを見つけやすくなります。

ヒント　ディープポリシー生成は、ワークスペース範囲をルートとする範囲サブツリーのすべてのポリシーを検出するため、これらのポリシーは、サブツリーの下のすべてのワークロードの自動ポリシー検出によって検出されるすべての合法的なトラフィックをカバーします。ポリシー分析（「ポリシー」を参照）などのツールを使用してこれらのポリシーを分析する場合は、サブ範囲に関連付けられたすべてのワークスペースでポリシー分析をオフにする必要があります。こうすると、（通常、より具体的な範囲定義のために高い優先度に設定される）サブ範囲ワークスペースに存在するポリシーがあっても優先されず、結果に干渉しません。ただし、サブ範囲ワークスペースのポリシーが、通常、サブ範囲に固有のより細かいインベントリフィルタまたはクラスタを含むさまざまなトラフィックセットをカバーするように設定されている場合は、例外が適用されます。

発信ポリシーコネクタの自動承諾

自動ポリシー検出中に作成されたすべての発信ポリシー要求は、自動的に受け入れられます。このオプションがデフォルトの自動ポリシー検出設定の一部として選択されている場合、手動で作成されたポリシー要求も自動的に受け入れられます。詳細については、「ポリシー要求」を参照してください。

（注）　このオプションは、ルート範囲の所有者のみが使用できます。

除外フィルタに一致するフローを無視する

指定したカンバセーションフローを無視するには、該当するオプションを有効にします。いずれかのフィルタリストを表示または変更するには、該当する [除外フィルタ（Exclusion Filters）] リンクをクリックします。詳細については、「除外フィルタ」、「デフォルトの除外フィルタ（9 ページ）」および「除外フィルタの構成、編集、または削除 （39 ページ）」を参照してください。

高度なポリシー検出設定を実現するためのロードバランサ設定の取得

サポートされているロードバランサ設定ファイルを Secure Workload に直接アップロード可能な形式で取得し、ポリシー検出で使用できるようにするための手順を以下で紹介します。詳細については、「自動ポリシー検出の詳細設定」および「ロードバランサとルータからのデータのアップロード （26 ページ）」を参照してください。

すべてのファイルは ASCII としてエンコードする必要があることに注意してください。

Citrix Netscaler

コンソールで `show run` の出力を連結し、ファイルをアップロードします。

「サンプル設定ファイル」を参照してください。

F5 BigIP

`bigip.conf` ファイルをアップロードします。.UCS 拡張子の付いたファイルがある場合は、アーカイブを解凍し、設定ダンプ内の `bigip.conf` ファイルのみをアップロードします。複数のファイルがある場合は、それらを連結してアップロードします。

「サンプル設定ファイル」を参照してください。

HAProxy

`haproxy.cfg` ファイルをアップロードします。通常、パスは `/etc/haproxy/haproxy.cfg` です。

「サンプル設定ファイル」を参照してください。

正規化された JSON

上記のオプションでは限定的だと思われる場合は、設定を次の JSON スキーマに変換し、それらを直接アップロードしてください。JSON ファイルのサンプルは、自動ポリシー検出用の [詳細な実行設定（Advanced Run Configurations）] の [SLB設定（SLB Config）] の横にある **i** アイコンをクリックして直接ダウンロードできます。

「サンプル設定ファイル」を参照してください。

除外フィルタ

除外フィルタを使用して、検出対象外とするトラフィックフローを指定することで、自動ポリシー検出によって提案されたポリシーとクラスタを微調整できます。

たとえば、最終的な許可リストモデルで ICMP などの特定のプロトコルを禁止するには、プロトコルフィールドを ICMP に設定して除外フィルタを作成できます。

（注）

- 除外フィルタに一致するカンバセーションは、ポリシーの生成とクラスタリングの目的で除外されますが、赤色の [除外（Exclude）] アイコン付きでカンバセーションビューに残ります（「カンバセーション」のテーブルビューを参照）。同様に、そのようなカンバセーションでのワークスペースインシデントのワークロードも表示されたままになります。
- ワークスペースのクラスタ定義やフィルタ定義を使用する除外フィルタは、プライマリワークスペースでのみ有効です（それ以外の場合、そのクラスタ定義はラベルシステムに対する可視性はないため、一致するカンバセーションは除外されません）。
- 除外フィルタはバージョン管理されています。変更を追跡するには、「履歴と差分」を参照してください。
- 除外フィルタ数の制限については、「自動ポリシー検出の制限」を参照してください。

次のいずれか1つまたは両方を作成し、ポリシーの検出時にいずれかまたは両方を有効にできます。

- 各ワークスペースの除外フィルタのリスト。
- テナント内のすべてのワークスペースで使用できるデフォルトの除外フィルタのリスト。

デフォルトのポリシー検出設定のいずれか1つまたは両方のリストを有効または無効にすることもできます。

手順については、「除外フィルタの構成、編集、または削除（39ページ）」および「除外フィルタを有効または無効にする（41 ページ）」を参照してください。

除外フィルタの構成、編集、または削除

この手順を使用して、1 つのワークスペースの除外フィルタのリスト、またはすべてのワークスペースで使用可能な既定の除外フィルタのリストを作成できます。

ステップ 1 次のいずれかを実行します。

目的	操作手順
特定のワークスペースの除外フィルタを設定する	ワークスペースに移動し、次のいずれかを実行します。 • [ポリシーの管理（Manage Policies）] をクリックし、次にページの右上付近にある ⋮ をクリックして、[除外フィルタ（Exclusion Filters）] を選択します。 • 自動ポリシー検出の設定ページで、[詳細設定（Advanced Configurations ）] セクションの [除外フィルタ（Exclusion filters）] リンクをクリックします。 • 検出されたポリシーを削除します。除外フィルタを作成するオプションが表示されます。
すべてのワークスペースで使用可能な既定の除外フィルタを設定する	1. **[防御（Defend）] > [セグメンテーション（Segmentation）]** の順に選択します。 2. ページの右側にあるキャレット記号をクリックして[ツール（Tools）] メニューを展開し、[デフォルトのポリシー検出設定（Default Policy Discovery Config）] を選択します。 3. ページの下部までスクロールします。 4. [デフォルトの除外フィルタ（Default Exclusion Filters）] をクリックします。

ステップ 2 除外フィルタを編集または削除するには、該当する行にカーソルを合わせて、[編集（Edit）] および [削除（Delete）] ボタンを表示します。

ステップ 3 除外フィルタを作成するには、[除外フィルタの追加（Add Exclusion Filter）] をクリックします。

ステップ 4 設定オプションは次のとおりです。

設定するフィールドは 4 つありますが、すべてが必須というわけではありません。空白のフィールドは、一致するフローのワイルドカードとして扱われます。

除外フィルタのすべてのフィールドに一致するカンバセーションは、ポリシーの作成とクラスタリングの目的においては無視されます。

オプション	説明
コンシューマ	コンシューマアドレスが選択したクラスタ/フィルタ/範囲のメンバーであるカンバセーションに一致させます。新しいカスタムフィルタを作成することにより、任意のアドレス空間を指定できます。
プロバイダ（Provider）	プロバイダーアドレスが選択したクラスタ/フィルタ/範囲のメンバーであるカンバセーションに一致させます。新しいカスタムフィルタを作成することにより、任意のアドレス空間を指定できます。
[Protocol]	指定されたプロトコルとのカンバセーションに一致させます。
ポート（Port）	指定されたポートまたはポート範囲に一致するプロバイダー（サーバー）ポートとのカンバセーションに一致させます。ダッシュ区切りを使用してポート範囲を入力します（例：「100-200」）。

次のタスク

重要 除外フィルタは、設定されているワークスペースでデフォルトで有効になっています。

デフォルトの除外フィルタは、すべてのワークスペースでデフォルトで有効になっています。

デフォルトのポリシー検出設定では、両方のタイプの除外フィルタがデフォルトで有効になっています。

ポリシーを検出する前に、次を実行します。

- 除外フィルタとデフォルトの除外フィルタを、次の場所で有効または無効にします
  - 各ワークスペース
  - [デフォルトのポリシー検出設定（Default Policy Discovery Config）] ページ

  この説明については、除外フィルタを有効または無効にする （41 ページ） を参照してください。
- 範囲の変更をコミットしないと、予定されるフローとフィルタが一致しない（そのため除外される）可能性があります。「変更の確定」を参照してください。

除外フィルタを有効または無効にする

各ワークスペースで除外フィルタを作成したり、すべてのワークスペースに適用できるデフォルトの除外フィルタのセットを作成したりすることができます。

デフォルトでは、両方のタイプの除外フィルタが有効になっています。

変更するには、次の手順に従います。

- 単一のワークスペースの除外フィルタを有効または無効にするには：

  ワークスペースで、[ポリシーの管理（Manage Policies）] をクリックしてから、[ポリシーの自動検出（Automatically Discover Policies）] をクリックし、次に [詳細設定（Advanced Configurations）] の順にクリックします。 このワークスペースの除外フィルタおよび/またはデフォルトの除外フィルタを有効にすることができます。

- [デフォルトのポリシー検出設定（Default Policy Discovery Config）] で除外フィルタを有効または無効にするには：

  [防御（Defend）]>[セグメンテーション（Segmentation）] を選択し、ページの右側にあるキャレット記号をクリックして [ツール（Tools）] メニューを展開します。次に、[デフォルトのポリシー検出設定（Default Policy Discovery Config）] を選択します。 [詳細設定（Advanced Configurations）] までスクロールするか、これをクリックします。除外フィルタおよび/またはデフォルトの除外フィルタを有効にすることができます。

自動ポリシー検出の再実行

自動ポリシー検出はいつでも再実行できます。自動ポリシー検出を再実行する最大の理由は、前回の実行時に含まれていなかった追加情報を含めることです。たとえば、以下を行うことができます。

- 前回の実行以降にインストールされた（または設定された）エージェントからデータを収集します。
- クラスタとポリシーの生成に使用する期間を長くします。
- 詳細設定（サイド情報またはその他の実行設定）を変更します。
- いくつかのクラスタを編集して承認します。これにより、再実行時に他のクラスタリングを改善できます。

ポリシーの自動検出を再度実行するには、実行設定ページに移動し、設定を変更して、[ポリシーの検出（Discover Policies）] をクリックします。

冗長ポリシーの削除後続の自動ポリシー検出では、プライマリワークスペースで承認されたポリシーによって、ポリシー生成のために一致するカンバセーションが削除されるため、冗長ポリシーは生成されません。除外フィルタの場合と同様に、ポリシーが非プライマリワークスペースで定義されたクラスタフィルタを使用している場合、この機能は非プライマリワークスペースでは完全に機能しない可能性があることに注意してください。非プライマリワークスペースからのクラスタフィルタはアクティブではなく、どのフローにも一致しないため、自動

ポリシー検出中に非プライマリワークスペースで冗長ポリシーが引き続き生成される可能性があります。

自動ポリシー検出の再実行の影響

既存のワークスペースでポリシーを再度自動検出すると、ワークスペース内のクラスタとポリシーの内容が変更される場合があります。ホストがワークスペースの範囲内になくなった場合、その後の自動ポリシー検出の実行時に、そのホストはどのクラスタにも表示されません。ホストが承認されたクラスタ内にあった場合、そのクラスタに表示されなくなります。時間枠または設定が異なる同じメンバーワークロードのセットであっても、自動ポリシー検出によって異なるクラスタが生成される場合があります。

アプリケーションビュー（アプリケーションビュー）も、ポリシー検出の再実行の影響を受ける可能性があります。再実行の結果、クラスタの内容が変更された場合、新しいクラスタを古いクラスタと一致させるために最善の努力が払われます。たとえば、10個のワークロードを持つクラスタの1つまたは2つのメンバーが変更された場合、それは同じクラスタであると見なされ、アプリケーションビューは変更されません。このシナリオでは、アプリケーションビューは、古いものではなく、新しいクラスタおよび新しく生成されたポリシーを、それぞれノードとエッジの参照として参照します。ただし、クラスタの内容が大幅に変更された場合、たとえば10個のワークロードのクラスタがサイズ5の2つのクラスタに分割された場合は、古いクラスタが削除されて2つの新しいクラスタが追加されたと見なされます。この場合、アプリケーションビューに適切なグラフが表示されない可能性があり、正しい依存関係のセットを反映するようにユーザーが編集する必要があります。

自動ポリシー検出を再実行する必要があるが、特定のクラスタの内容を変更してはならない場合は、自動ポリシー検出の再実行中のクラスタ変更の防止 （42 ページ） で説明されているように、それらのクラスタを承認する必要があります。

（注）

- クラスタを承認し、ポリシーを再度自動検出すると、範囲内の残りのワークロードのクラスタリングが改善される場合があります。
- 親および先祖範囲の最新のプライマリワークスペースで手動で定義されたポリシーは、自動ポリシー検出の影響を受けません。

自動ポリシー検出の再実行中のクラスタ変更の防止

今後、ワークスペースのポリシーを自動的に検出するときに、自動ポリシー検出（旧称 ADM（によってクラスタが変更されないようにするには、クラスタを承認します。

たとえば、クラスタクエリを編集し、新しいワークロードを範囲に追加して、既存のポリシーに影響を与えずにそれらをクラスタ化する必要がある場合は、クラスタを承認します。クラスタを承認すると、クラスタのコンテンツと属性が現在の状態に固定されます。自動ポリシー検出は、承認されたクラスタを変更しません。

クラスタの承認 （43 ページ）を参照してください。

クラスタの承認

クラスタを承認しても、その後の自動ポリシー検出によってそのクラスタのクエリが変更されることはありません。承認されたクラスタのメンバーシップは、ワークスペースのメンバーが変更された場合にのみ変更される可能性があります。

承認されたクラスタのメンバーであるワークロードは、「承認されたワークロード」と呼ばれることがあります。

クラスタを承認するには、次の手順を実行します。

目的のクラスタがサイドパネルに表示されていることを確認します。これを行うには、クラスタを検索するか、いずれかのビューのチャートで目的のクラスタをクリックします。次に、以下に示すように、サイドパネルのクラスタ情報の右上隅にあるチェックボックスをオンにします。クラスタが承認されると、将来の自動ポリシー検出によってそのクラスタが変更されることはないことが示されます。承認を削除するには、チェックボックスをオフにします。

図 *28 :* クラスタの承認

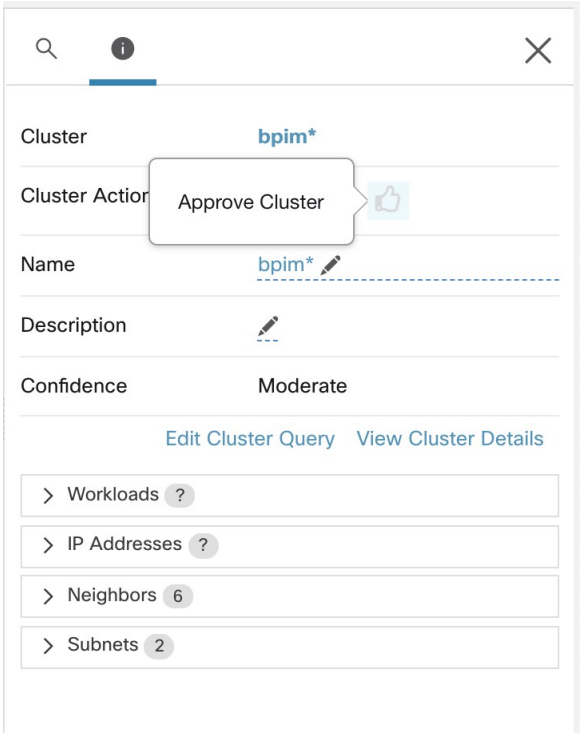
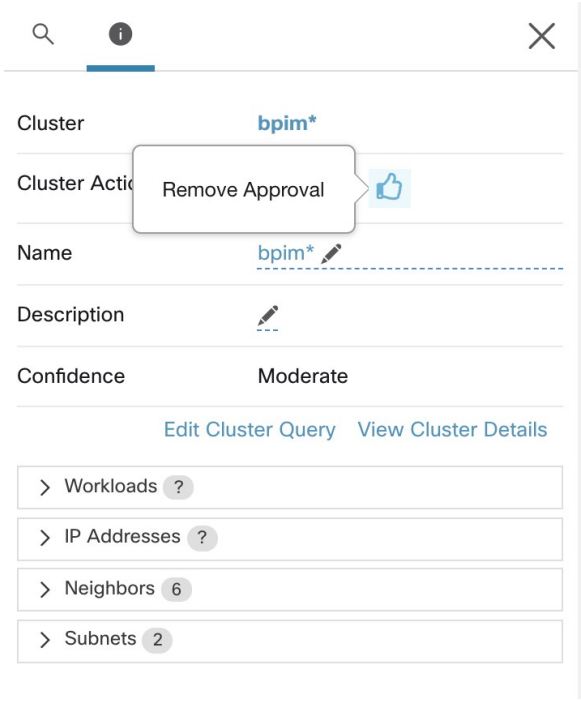


図 *29 :* クラスタの承認の削除



クラスタ：範囲内のワークロードのグループ

クラスタは、ワークスペース内でグループ化された一連のワークロードです。（Secure Workload の展開もクラスタと呼ばれることもありますが、この 2 つの用途は無関係です）

たとえば、アプリケーションの範囲に、アプリケーションを構成する他の多くのタイプのサーバーとホストの中に数台の Web サーバーが含まれている場合、このアプリケーションの範囲内に Web サーバーのクラスタが必要になる可能性があるため、これらの Web サーバーにのみ特定のポリシーを割り当てられます。

自動ポリシー検出は、設定の実行中に指定された時間枠で観測されたシグナルに基づいて、ワークロードをクラスタにグループ化します。

各クラスタはクエリによって定義される

クラスタクエリは、特定の IP アドレスで定義しない限り動的です。動的クエリを使用すると、クラスタメンバーシップは時間の経過とともに変化し、インベントリの変更を反映できます。クエリに一致させるワークロードは多いか、少ないか、または別のものになります。

たとえば、クラスタクエリが部分文字列「HR」を含むホスト名に基づいており、HR を含むホスト名を持つホストがワークスペースに追加された場合、クラスタには自動的に追加のホストが含まれます。

自動ポリシー検出は、ワークロードに関連付けられたホスト名とラベルを調べます。自動ポリシー検出により、ホスト名とこれらのラベルに基づいて候補クエリの短いリストがクラスタご

とに生成されます。これらのクエリから1つを選択して、必要に応じて編集し、クラスタに関連付けられます。自動ポリシー検出においてホスト名とラベルに基づく簡単なクエリが作成できない場合もあり、そのときは（代替の）クエリが提案されないことに注意してください。

承認済みクラスタのワークロードは、将来のポリシー検出の影響を受けない

関連するワークスペース内で承認済みクラスタのメンバーになっていないワークロードのみが、ポリシー検出の影響を受けます。**承認済みクラスタ**は、手動で承認したクラスタです。詳細については、クラスタの承認 （43 ページ）を参照してください。

クラスタを編集してグループ化を強化する

次のセクションでは、クラスタリング結果を編集、強化、および承認するためのいくつかのワークフローについて説明します。ワークスペースの最新バージョンでのみクラスタを変更/承認できることに注意してください（「履歴と差分」を参照）。

クラスタに変更を加える （47 ページ）を参照してください。

Kubermentes インベントリを含むクラスタ

（注） ワークスペースに複数のKubernetes名前空間からのインベントリが含まれている場合、各クラスタクエリを名前空間でフィルタ処理する必要があります。名前空間フィルタがまだ存在しない場合は、各クエリに名前空間フィルタを追加します。クエリを変更すると、ポリシーが自動的に再検出されます。

クラスタは、単一のワークロードで構成されている場合があります。

単一のワークロードのみを含むポリシーの作成が必要になる場合があります。

クラスタはインベントリフィルタに変換される場合があります。

承認済みクラスタと同様に、インベントリフィルタに昇格されたクラスタは、その後のポリシー検出中に変更されません。

クラスタとは異なり、インベントリフィルタはワークスペースに関連付けられていませんが、Cisco Secure Workload 展開においてグローバルに使用できます。

クラスタをインベントリフィルタに昇格させると、コンシューマとプロバイダーが異なる範囲にある場合、ワークロードのサブセットを含むポリシーを作成できます。これにより、より安全できめ細かいポリシーが実現できます。「コンシューマとプロバイダーが異なる範囲にある場合：ポリシーオプション （5 ページ）」を参照してください。

クラスタの信頼度

クラスタの信頼度スコアまたは品質スコアを使用して、改善が必要なクラスタを特定します。

クラスタの信頼度は、メンバーワークロードの信頼度の平均値です。一般に、ワークロードが割り当てられたクラスタの他のメンバーと類似しているほど、また最も近い（最も類似した）代替クラスタのワークロードと類似していないほど、そのワークロードの信頼度は高くなります。

フローがクラスタリングに使用される場合、2つのワークロードは、カンバセーションのパターンが類似している場合は類似しています（カンバセーショングラフ内の類似したネイバーセット、つまりコンシューマワークロードおよびプロバイダーワークロードとポートの類似したセットなど）。

（注）
- 次の場合、クラスタの信頼度は計算されません（未定義になります）。
  - 1 つのワークロードのみを含むクラスタ
  - 承認済みのクラスタ
  - 通信が観測されなかった範囲内のワークロード（プロセスベースのクラスタリングが選択された場合、プロセス情報の利用は不可）
- クラスタがパーティション境界を越えて構成されることはありません（サブネット境界など。高度な自動ポリシー検出設定のルートラベルを参照）。ただし、信頼度と代替クラスタの計算では、そのような境界は無視されます。これは、異なるサブネットにあるにもかかわらず、非常によく似た動作をするワークロードまたはクラスタが存在する可能性があることを示しています。
- クラスタの編集後、ポリシーが再度検出されるまで再計算は行われないため、信頼度スコアが不正確になる可能性があります。

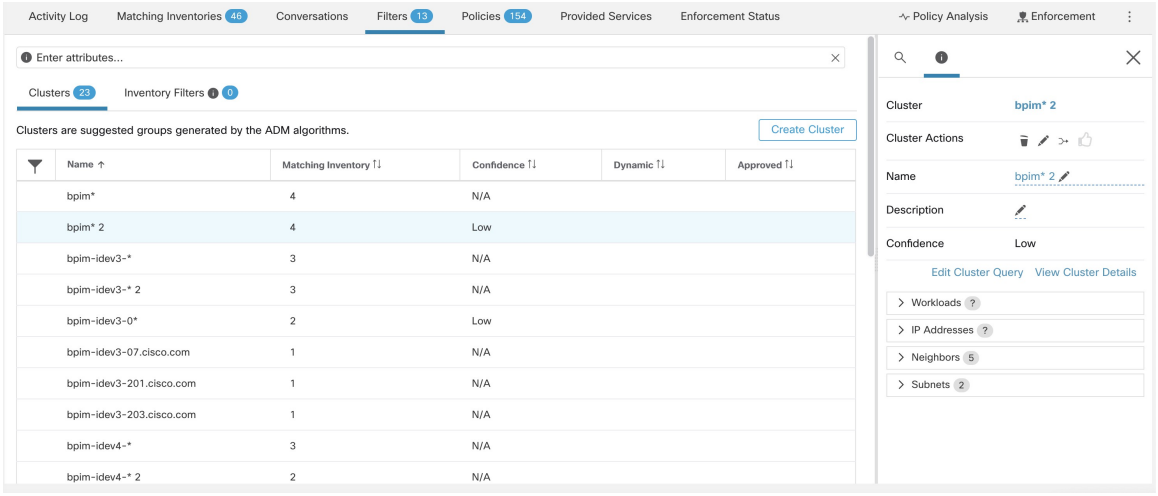
クラスタの信頼度を表示する方法については、「クラスタ ビュー （46 ページ）」を参照してください。

クラスタ ビュー

クラスタビューは、クエリとクラスタの関連付け、およびクエリの編集をサポートします。

クラスタビューでは、特定の列（名前、ワークロードの数、信頼度など）に基づいてクラスタをランク付けできます。各クラスタの行をクリックすると、説明、提案または承認されたクエリ、メンバーワークロードなどの詳細なクラスタ情報が右側のパネルに表示されます。これらのフィールドのいくつかは編集可能です。

図 30 : クラスタ ビュー



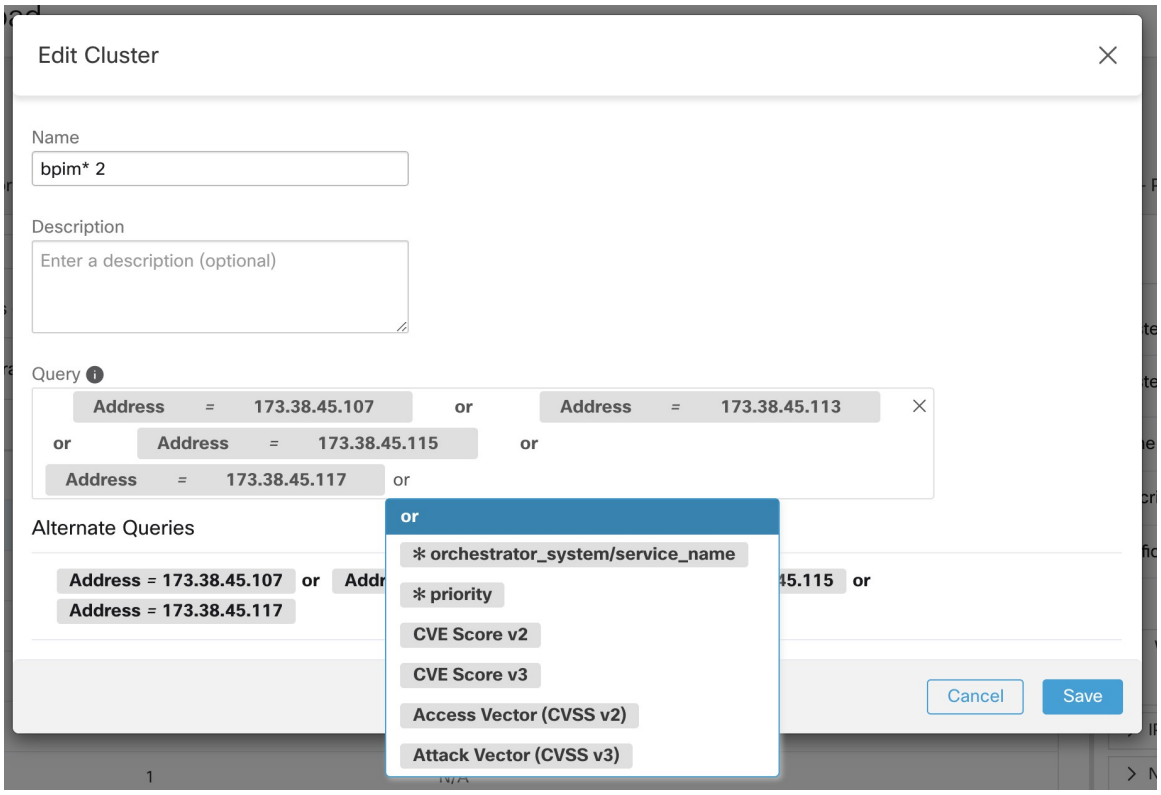
クラスタに変更を加える

自動ポリシー検出では、クラスタごとに 1 つ以上の候補クエリが作成されます。

クラスタリングの結果が期待と完全に一致しない場合は、クエリを編集してグループ化を改善できます。

クラスタを参照および編集するには：ページの上部にある [クラスタ（clusters）] ボックスをクリックします。クラスタを変更、たとえば、クラスタのメンバーを変更するか、そのクエリを選択または変更するには、以下に示すように、クラスタのクエリを選択または編集します。

図 *31* : クラスタの編集



明示的な IP アドレスを追加または削除するか、提供された代替のリストから別のクエリを選択して、クエリを編集できます。クラスタのクエリは、アドレス、ホスト名、およびラベルで表現されたクエリフィルタにできます。明示的な IP アドレスではなくラベルに基づいてクエリを定義すると、クラスタは動的になり、適切にラベル付けされた新規、変更、または削除されたインベントリは、クラスタに自動的に含まれるか、クラスタから除外されます。

クエリの選択と可能な編集が完了したら、[保存（Save）] をクリックします。[保存（Save）] ボタンをクリックすると、クラスタは自動的に承認済みとしてマークされ、承認済みの親指アイコンが（変更の有無に関係なく）青色に変わります。必要に応じて、承認済みアイコンを切り替えて、承認済みステータスを変更できます。詳細については、クラスタの承認 （43 ページ）を参照してください。

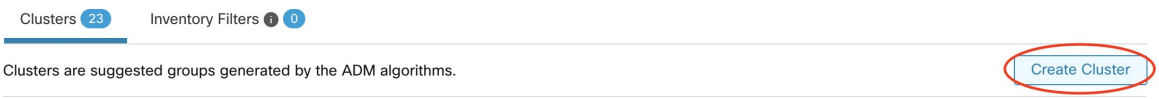
重要 クラスタのメンバーシップが変更された場合、変更されたクラスタ間のフローの変更が正確に反映されている更新されたポリシーを取得するために、ポリシーを再度検出する必要がある場合があります。これは、クラスタへの新しいノードの追加などにより、クラスタメンバーシップが変更された可能性があるためです。ワークスペースに対応する範囲が編集された場合、または一般にワークスペースのメンバーシップが変更された場合、同様の状況が発生する可能性があります。同様に、クラスタのメンバーシップが変更されると、クラスタの確実性スコアが正確でなくなる可能性があります。これらすべての場合において、ポリシーの自動検出は、更新されたポリシーとクラスタの確実性スコア（未承認のクラスタの更新された確実性）を取得するのに役立ちます。

クラスタクエリを編集すると、そのクエリに関連付けられたクラスタが重複する可能性があります。

クラスタの作成または削除

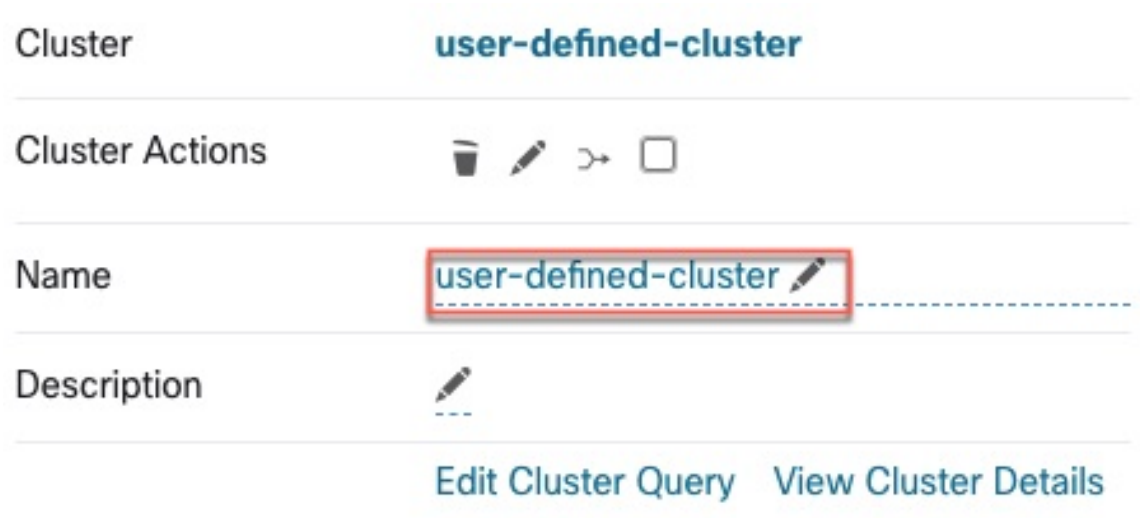
クラスタページの [クラスタの作成（Create Cluster）] ボタンをクリックして、新しい空のクラスタを作成します。または、[開始する（Get Started）] サイドバーの [フィルタの作成（Create Filter）] ボタンをクリックし、モーダルで [クラスタ（Clusters）] を選択して、[自動ポリシー検出（Automatic Policy Discovery）] ページからクラスタを作成できます。

図 *32 :* 新しいクラスタの作成



新しいユーザー定義クラスタはサイドパネルに表示され、必要に応じて名前を変更できます。

図 *33 :* クラスタの名前の変更



空のクラスタを削除するには、いずれかのビューでクラスタを選択して詳細をサイドパネルに表示し、クラスタ詳細ビューのヘッダーにあるごみ箱ボタンをクリックします。上の図を参照してください。

自動生成されたポリシーの確認

ポリシー属性

表 *1:* ポリシー プロパティ

セキュリティポリシーのプロパティ	説明
コンシューマ	サービスのクライアントまたは接続のイニシエータ。 範囲、クラスタ、またはユーザー定義のインベントリフィルタは、すべてポリシーのコンシューマとして使用できます。
プロバイダ	サーバーまたは接続の受信側。 範囲、クラスタ、またはユーザー定義のインベントリフィルタは、すべてポリシーのプロバイダーとして使用できます。
サービス	プロバイダーによって利用可能になるサービス。これを許可またはブロックする必要があります。これは、サーバー（リスニング）ポートと IP プロトコルを意味します。 ポリシーは、コンシューマからプロバイダーへのトラフィック、またはその逆方向、またはその両方に適用できます。
操作（Action）	ALLOW または DENY：指定されたサービスポート/プロトコルでのコンシューマからプロバイダーへのトラフィックを許可するかドロップするか。
ランクと優先順位	**絶対ルール**、**デフォルトルール**、**Catch-all ルール**など、ワークスペース内のポリシーのランクと優先度の詳細については、次の表および「ポリシーの優先順位 （55 ページ）」を参照してください。

表 *2*：ポリシーのランクと優先順位：絶対、デフォルト、*Catch-all*

ポリシーランク	説明
絶対値（Absolute）	絶対ポリシーは、ポリシーリストの下位の（したがって優先度の低い）アプリケーション固有のポリシーまたは範囲ツリーの下位の範囲で矛盾する場合でも有効です。一般に、絶対ポリシーを使用して、ベストプラクティスを適用したり、さまざまなゾーンを保護したり、特定のワークロードを検疫したりします。たとえば、絶対ポリシーを使用して、DNS またはNTP サーバーへのトラフィックを制御したり、規制要件を満たしたりします。 絶対ポリシーは、ポリシー優先順位リストのデフォルトポリシーの上にリストされます。
デフォルト	デフォルトポリシーは、ポリシーリストの下位のポリシー、または範囲ツリーの下位の範囲のポリシーによってオーバーライドされます。一般に、非常にきめの細かいポリシーがデフォルトポリシーです。 デフォルトポリシーは、ポリシー優先順位リストの絶対ポリシーの下にリストされています。
Catch-All	各ワークスペースには、ワークスペースで明示的に指定されたすべてのポリシーと一致しないトラフィックを処理する Catch-All ポリシーがあります。Catch-All アクションは、許可または拒否です。 一般に、Catch-All ポリシーは次のように設定します。 • 範囲ツリーの上位の範囲のトラフィックを**許可**し、ツリーの下位の範囲のポリシーがトラフィックを評価できるようにします。 • 範囲ツリーの下部にある最も限定的なリーフでトラフィックを**拒否**します。

ポリシー スコープ

ポリシー属性 （50 ページ） に加えて、各セキュリティポリシーの効果は、それが定義されているワークスペースの範囲によって制限されます。各ポリシーの範囲は、セキュリティポリシーが潜在的に影響を与える可能性のあるすべてのインベントリ項目（ワークロード）のセットを定義します。

Apps、**Apps:HR**、**Apps:Commerce** の 3 つの範囲を持つ簡単な例を考えてみましょう。**Apps:HR** と **Apps:Commerce** には、**Apps** の項目の重複するサブセットが含まれている可能性があります。**Apps** 範囲の所有者が次のポリシーを定義していると仮定します。

```
DENY PROD -> NON-PROD on TCP port 8000 (Absolute)
```

ここで、PROD と NON-PROD は、それぞれすべての実稼働ホストと非実稼働ホストを指定するフィルタです。このポリシーは、プライマリワークスペースの *Apps* 範囲で定義されているため、すべての PROD/NON-PROD ホスト（*Apps:HR* または *Apps:Commerce* 範囲に属するホストを含む）に影響します。

ここで、*Apps:HR* 範囲を持つワークスペースでまったく同じポリシーが定義されている場合を考えてみましょう。このシナリオでは、ポリシーは *Apps:HR* 範囲の PROD/NON-PROD ホストにのみ影響します。より正確には、このポリシーにより、NON-PROD HR ホスト（存在する場合）のインバウンドルールは、**任意の** PROD ホストからの TCP ポート 8000 での接続を拒否し、PROD HR ホスト（存在する場合）のアウトバウンドルールは、**任意の** NON-PROD ホストへの接続要求をドロップします。

（注） ポリシーで指定されたコンシューマとプロバイダーのインベントリフィルタには、次の目的があります。

- これらのフィルタまたはグループは、ワークロードにインストールされているファイアウォールルールで使用される IP アドレスのセットを指定します。
- これらのフィルタは、ポリシーまたはファイアウォールルールを受け取るワークロードまたは Secure Workload エージェントを指定します。

具体的な例として、アクションが ALLOW であるポリシー内のプロバイダーフィルタに、サブネット 1.1.1.0/24 のすべてのインベントリが含まれているとします。このポリシーが Secure Workload エージェントを使用してワークロードにインストールされ、IP アドレス 1.1.1.2 が含まれている場合、ファイアウォールルールは次のようになります。

1. 着信トラフィックの場合、ファイアウォールルールは、サブネット 1.1.1.0/24 全体ではなく、厳密に 1.1.1.2 宛てのトラフィックのみを許可します。
2. 発信トラフィックの場合、ファイアウォールルールは、サブネット 1.1.1.0/24 全体からではなく、厳密に 1.1.1.2 からのトラフィックのみを許可します。

上記は、ワークロードでのファイアウォールルールのプログラミング方法のデフォルトの動作です。ファイアウォールルールで指定された IP アドレスが、ポリシーがインストールされているワークロードの IP アドレスと異なる場合は、ポリシーで 2 つの目的のフィルタを分ける必要がある場合があります。「ポリシーの有効なコンシューマまたは有効なプロバイダー（82 ページ）」を参照してください。

信頼度の低いポリシーへの対処

自動ポリシー検出の後、信頼度の評価によって、ポリシーで指定した各サービス（ポートとプロトコル）について、検出された各ポリシーの正確度と適切性が示されます。

検出された信頼度の低いポリシーを特定するには、次の手順を実行します。

1. 該当するワークスペースに移動し、[ポリシー（Policies）] をクリックします。
2. [ポリシー（Policies）] リストで、[グループ化されていないポリシーリストビュー（Ungrouped Policy List View）] ボタンをクリックします。
3. [信頼度（Confidence）] 列見出しをクリックして、ポリシーリストを信頼度レベル順に並べ替えます。

4. [ポート（Port）] または [プロトコル（Protocol）] 列の値をクリックして、ウィンドウの右側にパネルを開きます（どちらのリンクも同じ情報を表示します）。
5. [プロトコルとポート（Protocols and Ports）] セクションでは、指定した各サービス（ポートとプロトコル）の信頼度がそれぞれの [C] の色で示されます。

   [C] にカーソルを合わせると、信頼度レベルが表示されます。
6. リスト内でサービスの信頼度の低い指標を探します。
7. 該当する場合は、不要なポリシーを削除または編集するか、ポリシーを追加します。

特定のポリシーの信頼度レベルを表示するには、次の手順を実行します。

1. [ポリシー（Policies）] リストで、そのポリシーの [プロトコルとポート（Protocols and Ports）] 列の値をクリックします。

   ウィンドウの右側に [ポリシーサイドビュー（Policy Side View）] パネルが開きます。
2. [プロトコルとポート（Protocols and Ports）] セクションでは、指定した各サービス（ポートとプロトコル）の信頼度がそれぞれの [C] の色で示されます。

   [C] にカーソルを合わせると、信頼度レベルが表示されます。

高度な詳細：検出されたポリシーの正確度は、フローの方向が正しく識別されたかに左右されます。フローの方向が正しく識別されていない場合、自動ポリシー検出結果の信頼度が低下する場合があります。ポリシー作成のために分析される通信フロー方向の決定については、「クライアントサーバーの分類」を参照してください。

承認済みポリシー

ポリシーを承認すると、次にワークスペースのポリシーを検出するときに、ポリシーは変更されずに引き継がれます。一般に、自動ポリシー検出では、承認されたポリシーの効果と重複するポリシーは提案されません（ただし、以下の注意事項と詳細を参照してください）。

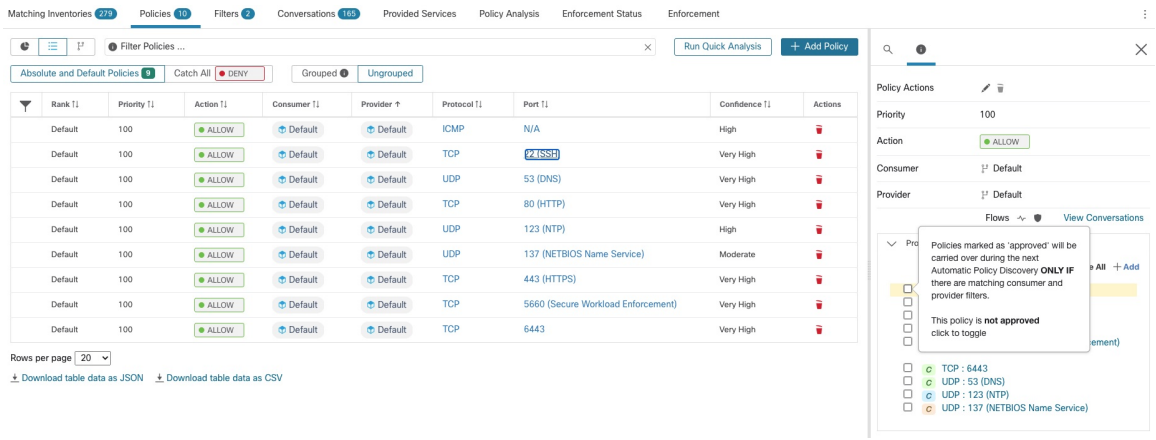
承認されたポリシーは次のとおりです。

- 手動で作成されたポリシー。
- 手動で承認された検出済みのポリシー。

  （ポリシーが意図したとおりに動作することを確認したら、ポリシーを承認して将来自動的に変更されないようにします）
- アップロードされたポリシー（明示的に `approved: false` とマークされていない場合に限ります）。
- 親および祖先範囲から（特に、プライマリワークスペースの最新バージョンから）継承された承認済みポリシー。
- コンシューマとプロバイダーが異なる範囲にある場合：ポリシーオプション（5ページ）で説明されている高度な方法を使用してクロス範囲ポリシーを処理する場合に、別のワークスペースからのポリシーリクエストが受け入れられたときに作成されるポリシー。

承認されたポリシーは、ポリシーサイドビューのプロトコルタイプの横にある親指アイコンとともに表示されます。承認状態を変更するには、チェックボックスをオンにします。

図 *34*：承認済みポリシー



承認済みポリシー保護の例外

ポリシーの両端が承認済みクラスタ、インベントリフィルタまたは外部範囲、またはメンバーシップを大幅に変更しないクラスタのいずれかである場合、承認済みポリシーは将来の自動ポリシー検出時にも保持されます（ただし、最後のケースではクラスタメンバーシップが変更されている可能性があります）。

ポリシーのいずれかの端が非承認クラスタであり、自動ポリシー検出時に、そのようなクラスタと十分に重複している新しく生成されたクラスタがない場合、承認済みポリシーは、将来の自動ポリシー検出の実行中に保護されない可能性があります。

未承認のクラスタを含むポリシーを保護するには、ポリシーの両端でクラスタを明示的に承認する必要があります。

承認済みポリシー：トラブルシューティング

承認済みポリシーが引き継がれません

承認済みポリシーが期待どおりに引き継がれない場合は、自動ポリシー検出の詳細設定またはデフォルトの構成設定で、[承認済みポリシーの引き継ぎ（Carry over approved policies）] オプションが選択されていることを確認してください。

ポリシー生成から除外されるカンバセーションを探す

自動ポリシー検出中に、既存の承認済みポリシーの基準に一致するカンバセーションは、ポリシー生成から除外されます。この省略により、同じカンバセーションをカバーする冗長なポリシーが生成されなくなります。（このプロセスは、ポリシーの代わりに一致フィルタを定義する除外フィルタとは異なります（「除外フィルタ」を参照）。除外フィルタは、一致するカンバセーションが自動ポリシー検出のあらゆる部分で表示されないようにします）

これらのカンバセーションから冗長ポリシーは生成されませんが、自動ポリシー検出がクラスタを分析して生成するときに、カンバセーションは引き続き考慮されることに注意してください。

既存の承認済みポリシーによって自動ポリシー検出から除外されているカンバセーションを確認するには、次の手順を実行します。

[カンバセーション（Conversation）] ビュー（「カンバセーション」を参照）で、除外フラグを使用してカンバセーションをフィルタリングします。また、カンバセーションの横にある除外アイコンをクリックして、ポリシーサイドビューでこれらのカンバセーションを除外する既存の承認済みポリシーを調べることもできます。

ポリシーの優先順位

トラフィック処理は、次の影響を受けます。

- 範囲内のポリシーの優先順位、および
- ポリシーのグローバルな順序付けと競合の解決 （55 ページ）

範囲内のポリシーの優先順位

ワークスペース内では、リスト内のポリシーの順序には各ポリシーの相対的な優先順位が反映されており、最も優先順位の高いポリシーがリストの一番上にあり、最も低い優先順位のポリシーがリストの一番下にあります。

各ワークスペースでは、絶対ポリシーがデフォルトポリシーよりも優先されます。Catch-All ポリシーはワークスペースで最も優先順位の低いポリシーです。

絶対ポリシー、デフォルトポリシー、および Catch-All ポリシーの詳細については、ポリシー属性 （50 ページ）を参照してください。

ポリシーのグローバルな順序付けと競合の解決

異なる範囲で定義された異なるポリシー間で競合が発生する場合があります。具体的な例を挙げると、親と子など複数の範囲に属するワークロード（インベントリ項目）に矛盾するポリシーがある場合に競合が発生します。

範囲のメンバーシップには動的な性質があるため、このような競合を手動で解決することは現実的ではありません。ワークロードは、プロパティの変更に応じて範囲に出入りできます。したがって、以下に説明するように、定義されている範囲に応じて、すべてのポリシーに対するグローバルな順位付けが必要になります。関連するポリシーのリスト（コンシューマ、プロバイダーなど範囲に応じて）がワークロードごとに識別され、グローバルな順序で並べ替えられます。フローを許可するかドロップするかは、並び替えられたリストで最初に一致したポリシーに基づいて決定されます。

ネットワーク管理者はセキュリティポリシーのグローバルな順序付けスキームを理解することで、正しい範囲とその優先順位を定義して、ワークロードに必要なポリシー全体を適用できます。アプリケーションオーナーは、各範囲内でそれぞれのワークロードにきめ細かいポリシーを適用することができます。

グローバル ネットワーク ポリシーには、次の特性があります。

- 一連の範囲が優先度順に従って（優先度の高いものから順に）並び替えられます。
- 各範囲のプライマリワークスペースには、絶対ポリシー、デフォルトポリシー、およびキャッチオールアクションが設定されています。
- 各ワークスペース内の絶対ポリシーやデフォルトポリシーの各グループは、ローカルの優先順位に従って（高いものから順に）並べ替えられます。

ポリシーのグローバルな順序は次のように定義されます。

- 全範囲のプライマリワークスペースの絶対ポリシーグループ（優先順位が高いものから順に並べられます）。
- 全範囲のプライマリワークスペースのデフォルトポリシーグループ（優先順位が低いものから順に並べられます）。
- 全範囲のキャッチオールポリシー（優先順位が低いものから順に並べられます）。

範囲の順序は、個々のポリシーではなく、カテゴリ 1 と 2 のポリシーグループに適用されることに注意してください。各グループ内では、優先順位番号が低い個々のポリシーが優先されます。

特定のワークロードの場合、最初にそれが属する範囲のサブセットが決定され、次に上記の順序が適用されます。このワークロードが属する最も優先順位の低い（適用された）ワークスペースのキャッチオールポリシーが適用可能なキャッチオールになります（ただし、絶対ポリシーやデフォルトポリシーによってオーバーライドされる場合があります）。そのワークロードの特定のフローに対して、最も一致するポリシーのアクションが適用されます。

（注）

- ワークスペースに絶対ポリシーもデフォルトポリシーも定義されていない場合、ワークスペースは無視されます。ワークスペースのキャッチオールポリシーは、グローバルな順序付けの対象ではありません。
- グローバルな順序付けにおけるデフォルトポリシーの順序は、範囲の優先順位の逆です。これにより、ポリシーの適用が有効になっていないワークスペースを含むすべてのワークスペースの境界を保護するために、すべての範囲に対して広範なポリシーを定義できます。同時に、範囲の適用を有効にしているアプリケーションオーナーは、デフォルトポリシーをオーバーライドすることができます。
- 範囲の重複は推奨されません。詳細については、「範囲の重複」を参照してください。ただし、ワークロードに2つ以上のインターフェイスがあり、範囲が重複または分離している場合、適用が有効になっている最も優先順位の低いワークスペースのキャッチオールポリシーが（適用可能なすべてのキャッチオールポリシーの中で）適用されます。

前の 3 つの範囲の例を拡張して、この順序付けスキームについて説明します。3 つの範囲に次の優先順位が割り当てられていると仮定します（範囲の優先順位を変更する方法については、「ポリシー管理用ワークスペース」を参照してください）。

1. アプリ
2. アプリ：人事
3. アプリ：コマース

これらの各範囲のプライマリワークスペースには、絶対ポリシー、デフォルトポリシー、およびキャッチオールアクションが設定されています。各ワークスペース内の絶対ポリシーやデフォルトポリシーの各グループは、ローカルの優先順位に従って並べ替えられます。

ポリシーのグローバルな順序は次のとおりです。

1. アプリの絶対ポリシー
2. アプリ：人事の絶対ポリシー
3. アプリ：コマースの絶対ポリシー
4. アプリ：コマースのデフォルトポリシー
5. アプリ：人事のデフォルトポリシー
6. アプリのデフォルトポリシー
7. アプリ：コマースのキャッチオール
8. アプリ：人事のキャッチオール
9. アプリのキャッチオール

アプリの範囲に属するワークロードは、指定された順序で次のポリシーのみを受け取ります。

1. ワークロードに一致するアプリの絶対ポリシー
2. アプリのデフォルトポリシー
3. アプリのキャッチオール

アプリおよびアプリ：コマースの範囲に属するワークロードは、指定された順序で次のポリシーのみを受け取ります。

1. アプリの絶対ポリシー
2. アプリ：コマースの絶対ポリシー
3. アプリ：コマースのデフォルトポリシー
4. アプリのデフォルトポリシー
5. アプリ：コマースのキャッチオール

アプリおよびアプリ：人事の範囲に属するワークロードは、指定された順序で次のポリシーのみを受け取ります。

1. アプリの絶対ポリシー

2. アプリ：人事の絶対ポリシー
3. アプリ：人事のデフォルトポリシー
4. アプリのデフォルトポリシー
5. アプリ：人事のキャッチオール

ポリシーの順序と重複する範囲

重要 次のシナリオでは、範囲が重複しています。兄弟範囲が重複しないように注意する必要があります。ワークロードは、範囲ツリーの複数のブランチメンバーであってはなりません。詳細については、範囲の重複を参照してください。

アプリ、アプリ：人事、およびアプリ：コマースの3つの範囲に属するワークロードは、指定された順序で次のポリシーのみを受け取ります。

1. アプリの絶対ポリシー
2. アプリ：人事の絶対ポリシー
3. アプリ：コマースの絶対ポリシー
4. アプリ：コマースのデフォルトポリシー
5. アプリ：人事のデフォルトポリシー
6. アプリのデフォルトポリシー
7. アプリ：コマースのキャッチオール

アプリ：人事の範囲とアプリ：コマースの範囲の相対的な順序は、2 つの範囲が重複する場合（つまり、両方の兄弟範囲に属するワークロードがある場合）にのみ問題になります。これは、ポリシーが常に範囲の下で定義されるためです。1つの範囲のみに属するワークロードは、他の範囲のポリシーの影響を受けないため、順序は関係ありません。

（上級）ポリシーの優先順位の変更

注意 範囲ポリシーの優先順位の変更はほぼ必要ありません。ポリシーの優先順位を変更すると、すべてのワークスペースでの適用結果に影響を与える可能性があるため、変更は慎重に行ってください。

この機能へのアクセスは、サイト管理者などの非常に高い権限ロールを持つユーザーに制限されています。

始める前に

範囲の優先順位を変更する前：

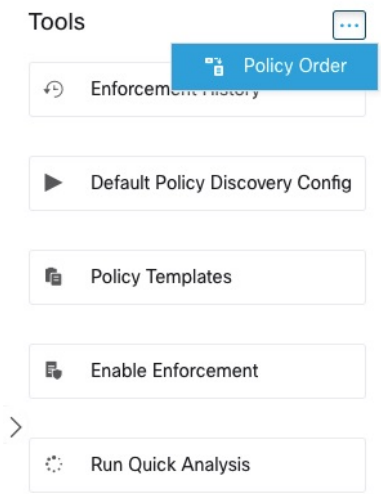
- ポリシーの並べ替えロジックと、範囲におけるポリシーの優先順位が個々のポリシーインテントの順序付けにどのように変換されるかを理解します。ポリシーの優先順位（55ページ）を参照してください。
- 兄弟範囲の重複は推奨されていないため、範囲クエリを更新して、重複を修正します。
- 新しい順序が期待どおりだと確信できるまで、セカンダリワークスペースで変更を行います。
- 次のガイドラインを考慮して、変更を計画します。

  並べ替えるときは、範囲ツリーの階層構造を利用するために、親優先の順序（親範囲が子範囲の上）を維持します。

  （兄弟範囲が重複している場合、兄弟範囲とその子の順序を変更する必要がある場合があります）。

ステップ 1 ポリシーの優先順位を並べ替えるには、[ツール（Tools）]の横にあるメニューアイコンをクリックし、[ポリシーの順序（Policy Order）] を選択します。

図 *35 : [ポリシーの優先順位（Policy Priorities）]* ページへの移動



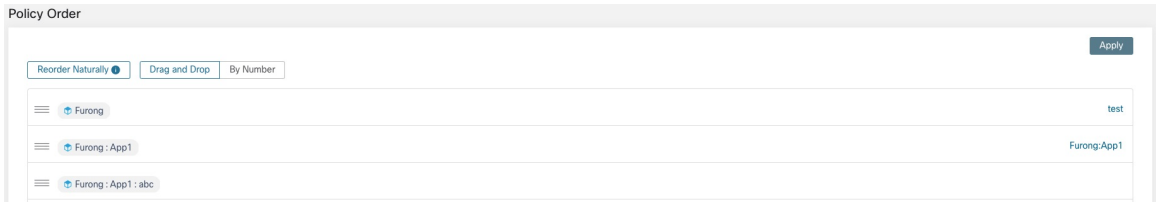
[ポリシーの順序（Policy Order）] ページでは、現在のポリシーの優先順位に従って、すべての範囲と範囲に対応するプライマリワークスペースのリストを確認できます。

ステップ 2 範囲を並べ替える方法は複数あります。

- リスト全体を並べ替えて、親範囲を子範囲の上に配置（「事前整列」）するには、[自然に並べ替える（Reorder Naturally）] をクリックします。これは推奨される順序であり、逸脱する場合は注意が必要です。

- リストを手動で並べ替えるには、次の手順を実行します。
  - 行を上下にドラッグします。
  - [番号順（By Number）]をクリックして、並べ替えに使用する各範囲の番号を設定します。この方法は、大きなリストの場合は簡単です。

図 *36 :* 範囲のポリシー優先順位の設定



次のタスク

簡易分析を実行して、変更の結果を確認します。

グループ化されたポリシーテーブルの表示

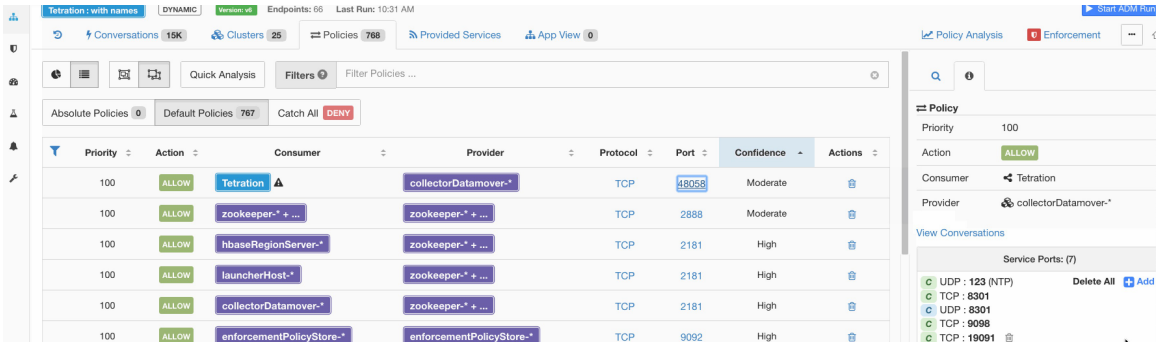
ポリシーテーブル（リスト）ビューは、特定のワークスペースのポリシーを表示、編集、および理解するための簡単な方法を提供します。リストアイコンをクリックして、[ポリシーリスト（policy list）] ページに移動します。

絶対ポリシー、デフォルトポリシー、およびキャッチオールポリシーを区切る3つのタブが表示されます。すべてのポリシーは、より簡潔に表示できるように、コンシューマ/プロバイダー/アクションごとにグループ化されています。[サービス（Services）] 列のエントリをクリックすると、サービス（すべてのポート）などの要素を検証できます。一度クリックすると、右側のパネルでポートの完全なリストが表示され、[カンバセーションの表示（view conversations）] をクリックして、ポリシーを生成したカンバセーションを表示できます（「カンバセーション」を参照）。

グループ化されていないポリシーテーブルビュー

このグループ化されていないリストビューは、コンシューマ/プロバイダ/アクションに加えて、ポート（ポート範囲）で区別されます。そのため、ポートに基づいて行を簡単に検索またはフィルタリングできます。

図 *37* : ポリシーのグループ化されていないリストビュー



ポリシーの視覚的表現

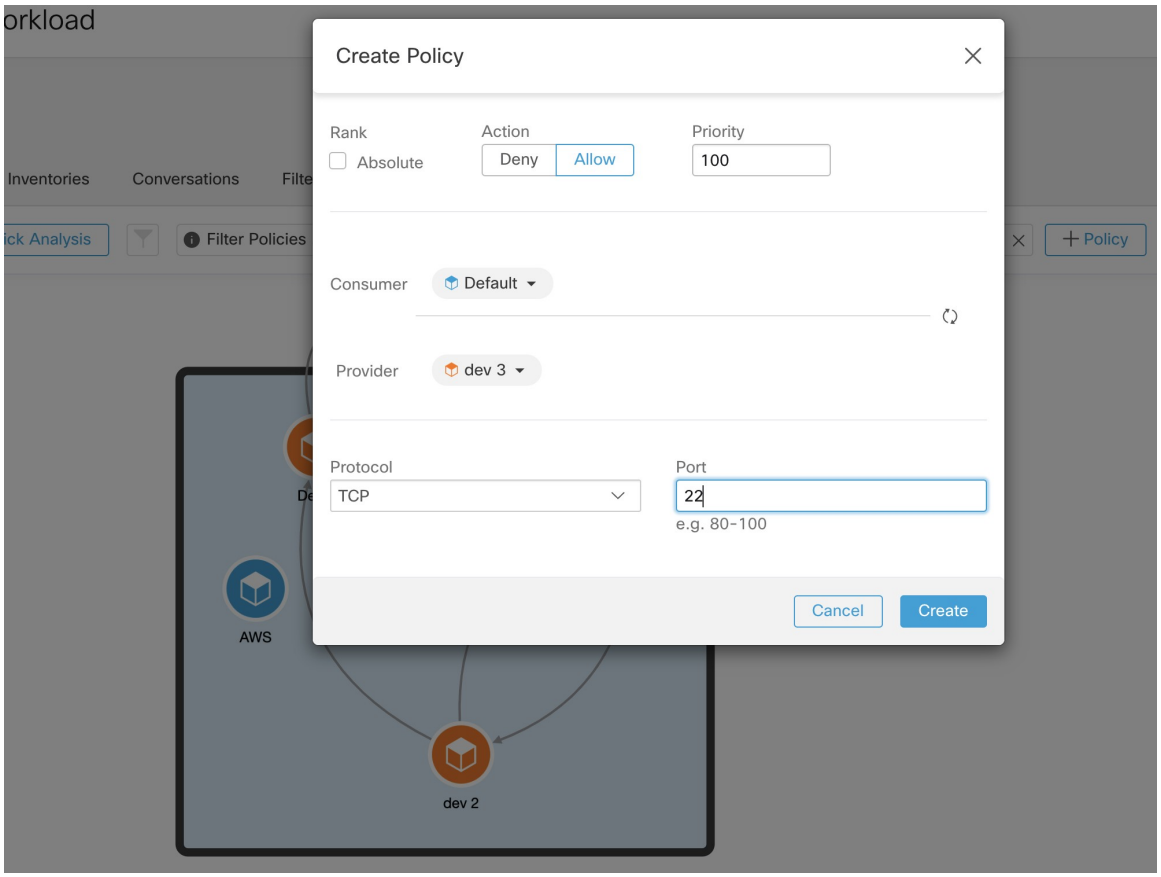
ポリシーの視覚的表現により、ポリシーのグラフィカルビューが可能になります。

ポリシーの視覚的表現のページに移動するには、リストアイコンの右側にあるグラフアイコンをクリックします。

グラフィカルビューは、ノードとポリシーで構成されます。キャンバス上のノードは、ポリシーのコンシューマとプロバイダーを表します。このページでのコンシューマとプロバイダーには、クラスタ（紫色）、インベントリフィルタ（オレンジ色）、または範囲（青色）が含まれます。コンシューマまたはプロバイダーに含まれるワークロードのリストを表示するには、ノードをダブルクリックします。コンシューマとプロバイダーの間の線は、1つ以上のポリシーを表します。サービス（ポート）、アクション（許可/拒否）、およびコンシューマとプロバイダー間のプロトコルなどのポリシーの詳細を表示するには、それらをつないでいる線をクリックします。

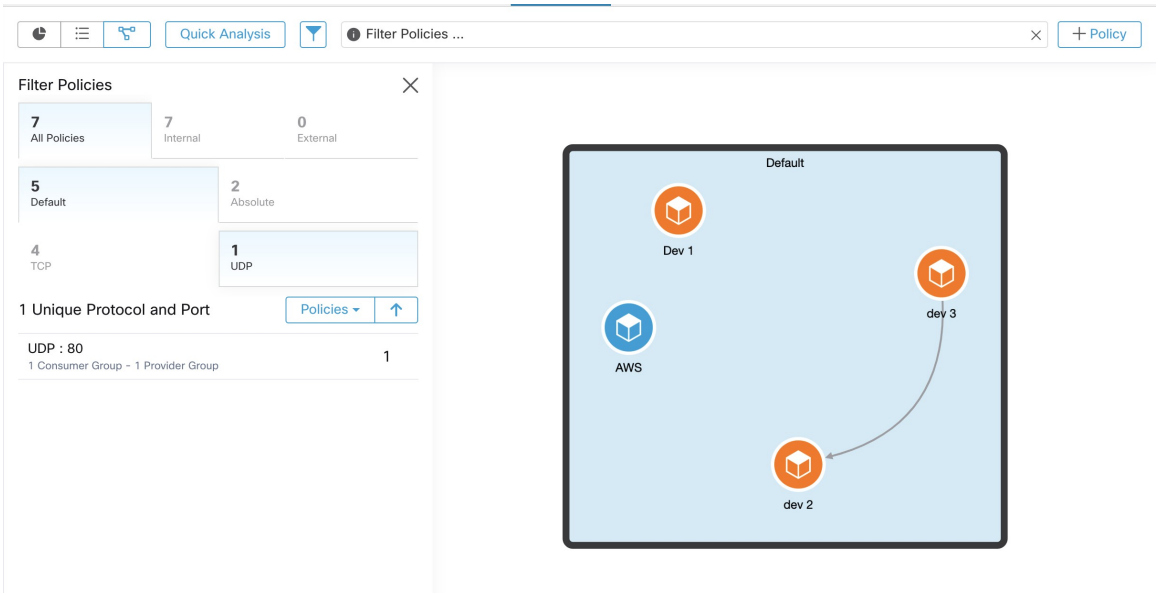
ポリシーを作成するには、コンシューマにカーソルを合わせ、「+」記号が表示されたら、ポリシーをクリックしたままプロバイダーにドラッグします。絶対ポリシーを作成するには、モーダルの [絶対（Absolute）] チェックボックスをオンにします。それ以外の場合、ポリシーはデフォルトポリシーとして作成されます。ポリシーは、線をクリックして、ポップアップリストからポリシーを選択することによっても管理できます。ポリシーがサイドバーに表示されます。

図 *38* : グラフィカルビューでのポリシー作成



ノードに送受信されるポリシーを表示するには、ノードをクリックします。高度なフィルタリングを行うには、テキスト入力欄の左側にあるフィルタボタンを切り替えます。ポリシーをフィルタリングするには、複数のタブを使用してドリルダウンします。フィルタリングの最初のレイヤーでは、内部ポリシーと外部ポリシーをフィルタリングできます。2番目のレイヤーでは、ポリシーランク（絶対/デフォルト）などに基づいてポリシーをフィルタリングできます。たとえば、[dev] 範囲に入出力される TCP プロトコルを使用するすべてのデフォルトポリシーを表示するには、キャンバスで [dev] 範囲をクリックしてから、パネルの複数のタブを使用して目的のポリシーセットをフィルタリングします。

図 *39* : グラフィカルビューでのポリシーのフィルタリング



ポリシーコードビュー

（注） ポリシーコードビューは廃止され、次のシスコ Secure Workload リリースで削除されます。

ポリシーコードビューには、すべての ALLOW ポリシーのトップレベルのグラフビューを 1 つのコードチャートで示し、情報をドリルダウンおよびフィルタ処理するさまざまな方法が示されます。

次の図は、ポリシーコードチャートの基本的な概念の一部を示しています。チャートの周囲にある円弧は、クラスタまたはパーティション（クラスタのグループ）を表します。拡張されたパーティションは、すべてのメンバークラスタの周りに光って表示されます。

コードは、クラスタ、フィルタ、または範囲のペア間にあるすべてのポリシーインテントのグループを表します。コードがパーティションで開始または終了する場合、そのパーティション内にある全クラスタの全ポリシーの結合を表します。

コードは、ポリシーの双方向セットを表します。各サイドのコードの太さは、対応するクラスタまたはパーティションによって消費されるサービスの数に比例します。

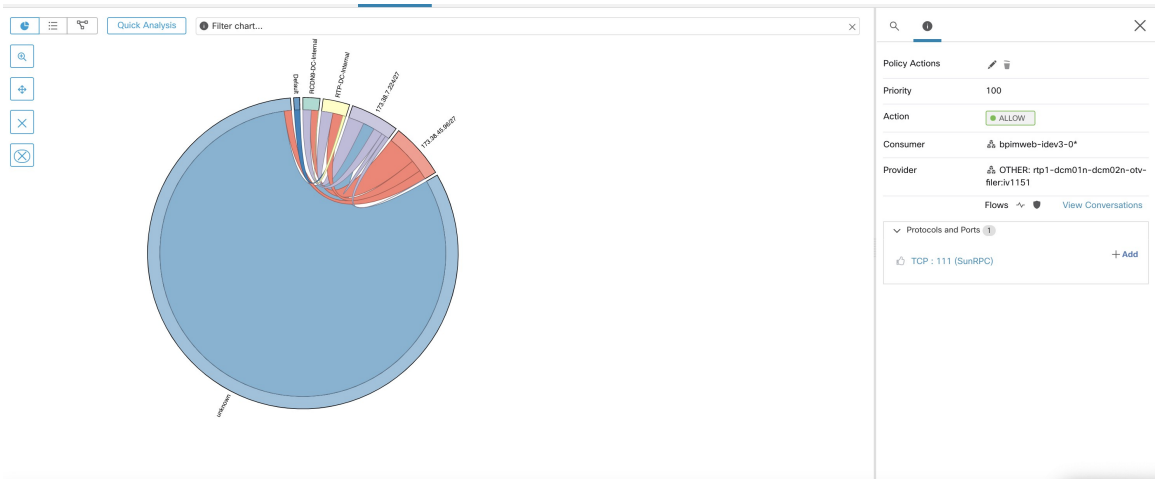
ヒント：

- クラスタの編集ビュー（「クラスタ：範囲内のワークロードのグループ」を参照）を使用して、クラスタとそのコンテンツをすばやく表形式で表示できます。通信（エッジまたはポリシー）を表示する場合は、ポリシービューを使用します。

（注）

- パーティションの円弧をダブルクリックして、そのパーティションを展開または折りたたみます。
- チャート要素（つまり、パーティション、クラスタ、またはポリシー）のいずれかをシングルクリックすると、その要素が選択または選択解除されます。さらに、サイドパネルは、最後にクリックされた要素に関するコンテキスト情報で更新されます。
- チャートを元の状態にリセットするには、チャートの外側のキャンバスをダブルクリックします。

図 *40* : ポリシーコードビュー

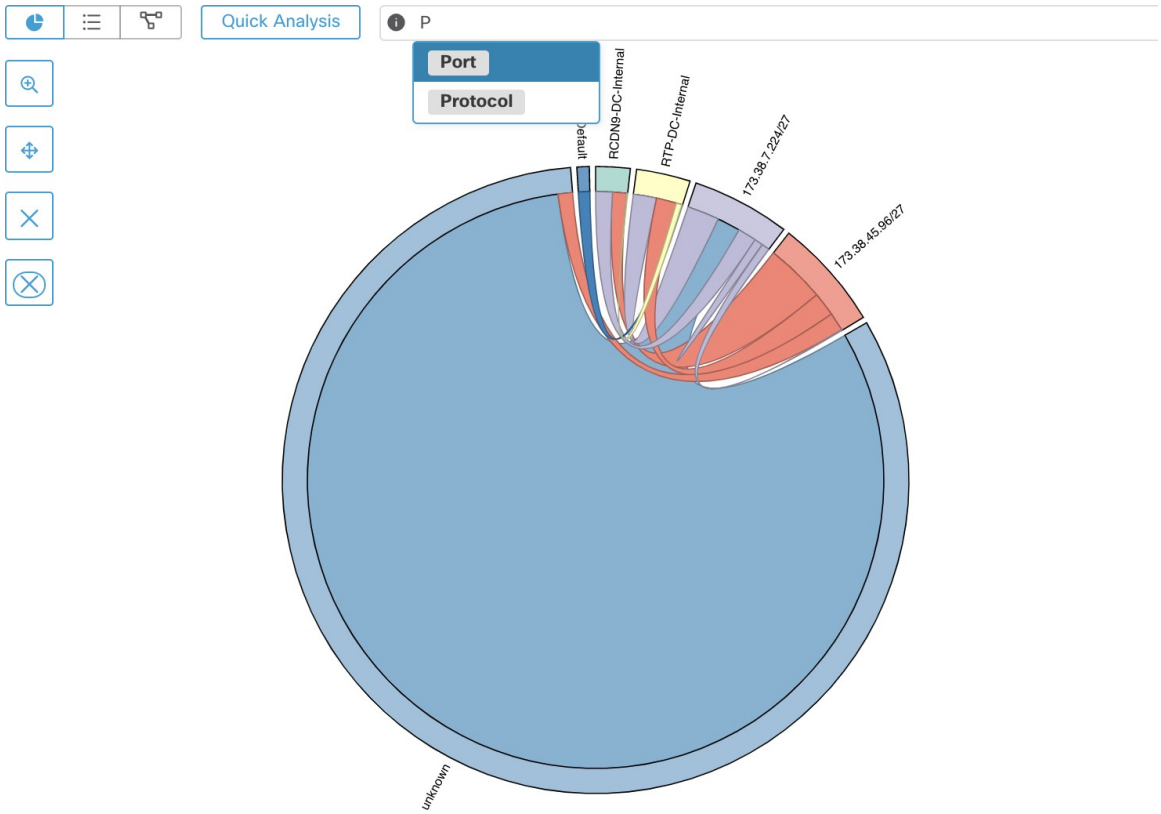


コードチャートツールバー

ポリシービューページの左上隅にある一連のコントロールやツールバーは、大きく複雑なチャートを使用したインタラクションを簡素化するために設計されており、ユーザーはクラスタやポリシーのサブセットに集中することができます。

[フィルタ（Filter）]ボタンは、ポートやプロトコルを指定してポリシーをフィルタリングするのに役立ちます。緑色のボタンは、フィルタがアクティブであることを示します。[無効化（disable）] をクリックするだけで、フィルタリングを解除できます。次の例を参照してください。

図 *41* : コードチャートツールバー



[クラスタの詳細を表示（Show Cluster Detail）] ボタンは、選択したクラスタのコンテンツをドリルダウンし、クラスタ内のホストのカンバセーションや接続状況を観察するのに役立ちます。

（注） クラスタのドリルダウン機能を使用するには、少なくとも 1 つのクラスタ（パーティションではない）を選択する必要があります。残りのコントロール機能は、その名前が示すとおり、不要なクラスタやポリシーを削除したり、チャートの対象をクラスタの 1 つまたは複数のネイバーのみに制限したりするのに役立ちます。

簡易分析

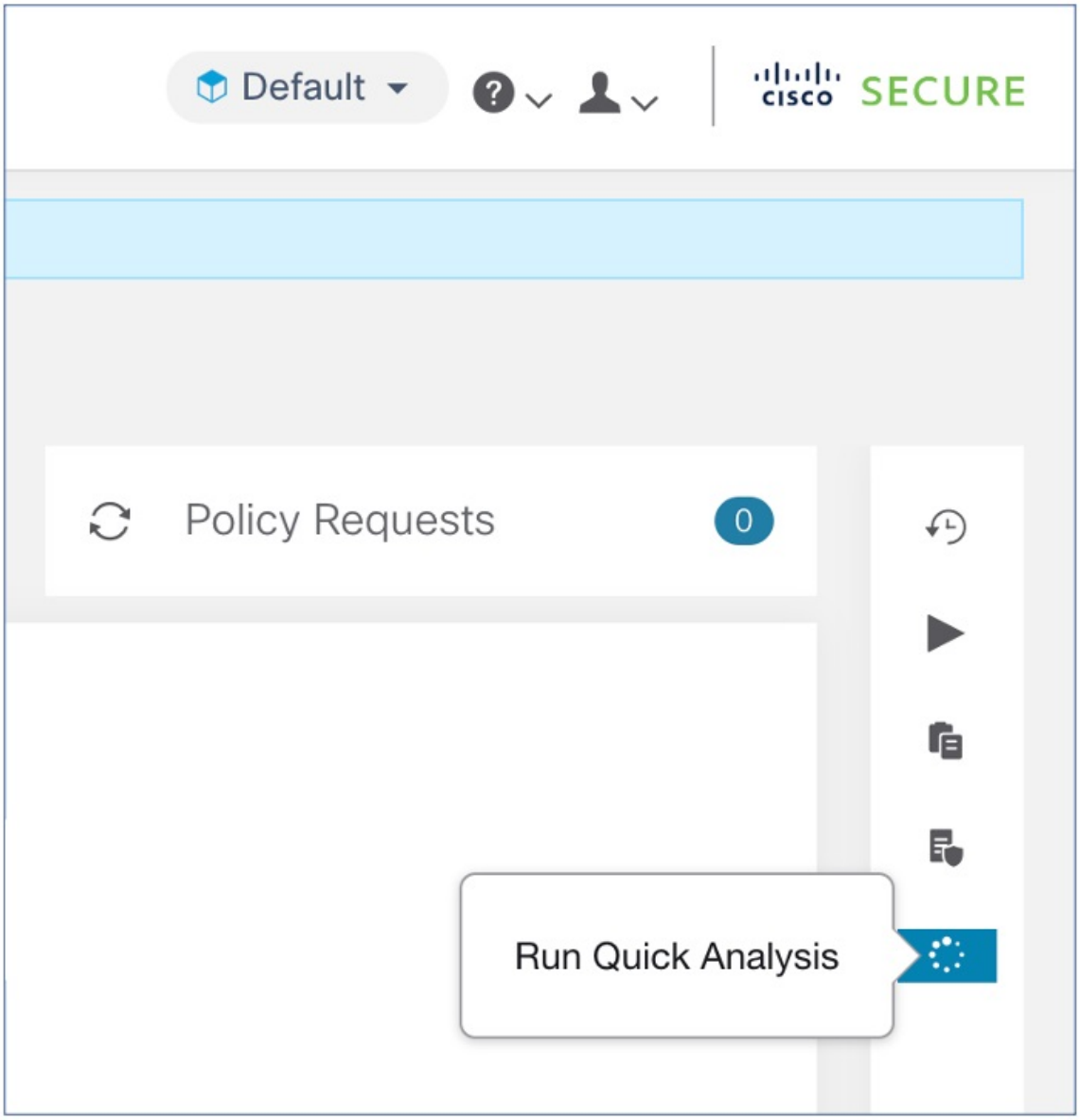
簡易分析により、現在のワークスペース内の全ポリシー、および他のワークスペースからの全関連ポリシーに対する仮想フローをテストできます。簡易分析により、ワークスペースを公開しなくても、さまざまなセキュリティポリシーを使用したデバッグと試験が容易になります。

制約事項

- 簡易分析は、プライマリワークスペースでのみ実行できます。
- 簡易分析は現在、Kubernetes サービスからのフローではサポートされていません。

右側のナビゲーションウィンドウで [簡易分析の実行（Run Quick Analysis）] タブをクリックして、ダイアログを表示します。

図 *42 : [*簡易分析（*Quick Analysis***）*]* タブ**



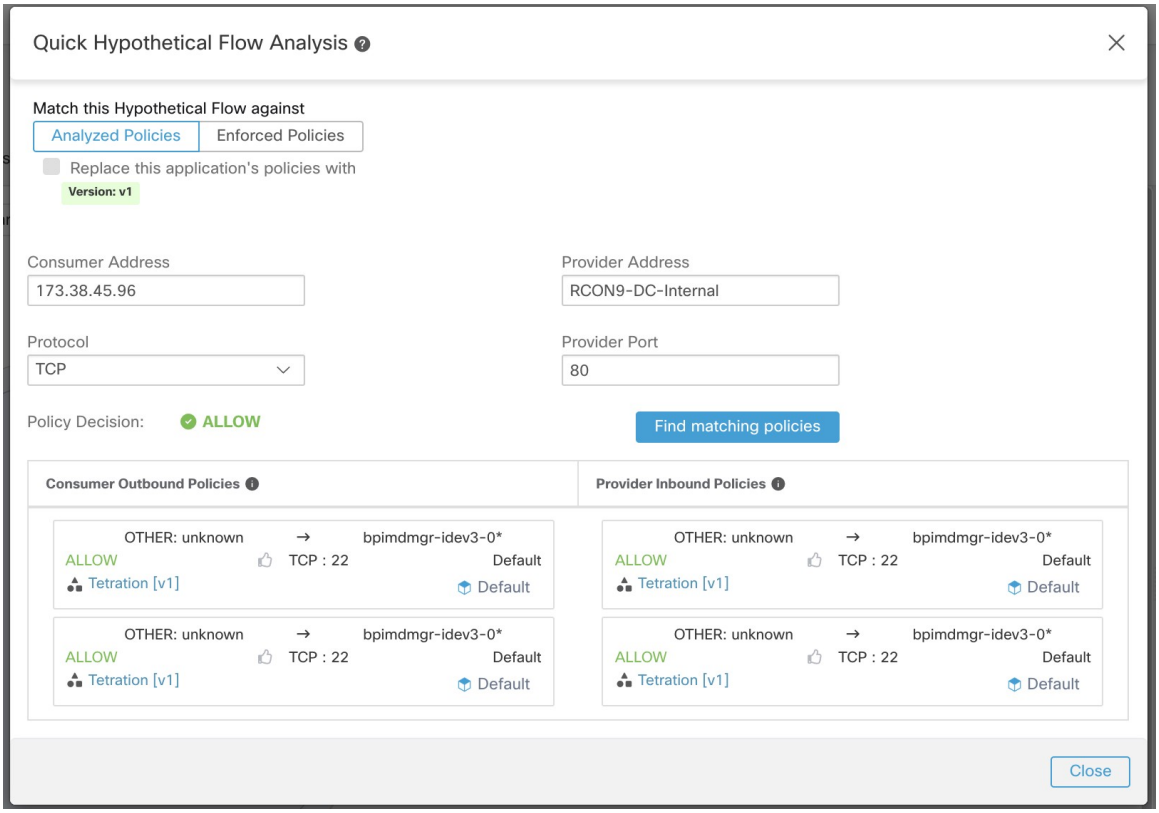
仮想フローのコンシューマ（クライアント）IP、プロバイダー（サーバー）IP、ポート、およびプロトコルを入力し、[一致するポリシーの検索（Find Policy Match）] ボタンをクリックします。

ワークスペースの最新バージョンのポリシー定義と、ライブポリシー分析のために既にプッシュされている関連したワークスペースからの他の全ポリシーを考慮して、仮想フローが許可または拒否されるかどうかを示すポリシー決定が表示されます。

ダイアログの下部に、一致するアウトバウンドポリシーとインバウンドポリシーが個別に、一括で並べ替えられた順序で表示されます。有効なものは、いずれかの側の最初の行のみです。接続を正常に確立するには、コンシューマ側の最上位のアウトバウンドルールとプロバイダー側の最上位のインバウンドルールの両方が ALLOW ルールである必要があります。

他のすべての一致するポリシーを順番に表示すると、特定のポリシーが有効になっていないように見える場合に、ポリシー定義の問題を整理するのに役立つデバッグツールが提供されます。ワークスペースからポリシーを追加、更新、または削除し、すぐに分析を繰り返すことができます。ワークスペースの公開は必要ありません。

図 *43* : 簡易ポリシー分析



ライブ分析

ポリシー分析は、許可リストモデルを使用したセキュリティポリシー生成の重要な要素です。自動ポリシー検出によって生成された一連のネットワーク セキュリティ ポリシーを確認して承認した後、ポリシーを適用エンジンにプッシュする前に、いくつかの質問に対する答えを知る必要があります。

1. ポリシーの適用をすぐに開始すると、既存のアプリケーションまたはワークスペースはポリシーによってどのような影響を受けますか。
2. 新しい一連のポリシーを適用していたなら、既知のセキュリティ攻撃/リスクを防ぐことができたでしょうか。

3. ネットワーク適用エンジンは、ポリシーの意図を正しく施行していますか。
4. 各セキュリティルールに関連付けられている平均ネットワーク使用量や、その他のテレメトリ データはどれほどですか。

許可リストモデル化ポリシーを生成するために自動ポリシー検出によって使用されるフロー監視では、アプリケーションのすべてのアクティブコンポーネントが完全にキャプチャされない可能性があるため、最初の質問は特に重要です。

これは自動ポリシー検出に設定した時間範囲が短いことが原因である可能性があります。そのため、分析チェックなしで新しいポリシーをプッシュすると、アプリケーションが正常に機能しなくなる可能性があります。

ポリシー分析は、自動ポリシー検出によって生成されユーザーによって強化されたポリシーを、ネットワークのライブトラフィックと照合するために実施されます。ポリシー分析ワークフローの最初のステップは、ワークスペースで[ポリシー分析の有効化（Enable policy analysis）]を行って、ポリシーをネットワーク内の進行中のフローと照合できるようにすることです。各ワークスペースを個別に公開することは可能ですが、すべてのワークスペースを公開する必要はありません。

ポリシーの有効化

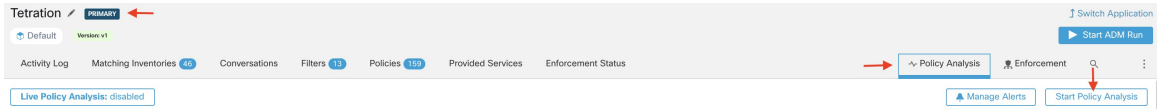
ワークスペースでの自動ポリシー検出の結果を確認したら、ワークスペースで[ポリシー分析の有効化（Enable Policy Analysis）]をクリックして分析を開始できます。**ポリシー分析を有効にする**には、次の手順に従います。

ステップ 1 ヘッダーのワークスペース名の横にある[セカンダリ（Secondary）]をクリックして、ワークスペースを**プライマリ**に切り替えます。

ステップ 2 [ポリシー分析（Policy Analysis）]タブに移動します。

ステップ 3 右側の[ポリシー分析の開始（Start Policy Analysis）]ボタンをクリックします。

図 *44* : ポリシー分析の有効化



ポリシーなしでの分析

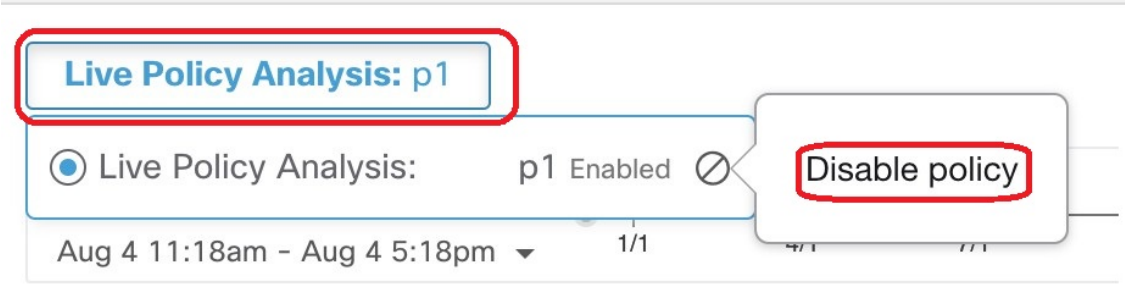
ワークスペースに関連付けられた範囲へのフロー、そのような範囲からのフロー、および範囲内のフローは、他のワークスペースで公開されたポリシーの影響を受ける可能性があります。このワークスペースでポリシー分析が有効になっていない場合、フローは、システムに含まれる他の公開ワークスペースのフローでマーキングされます。

（注） ポリシーが公開されているワークスペースがない場合、時系列チャートは空になります。

ライブ分析ポリシーの無効化

公開されたポリシーを無効にしても、ワークスペースの内容には影響しません。ポリシー分析ツールからポリシーが削除されるだけです。他のポリシーが一部のフローよりも優先される場合があり、それに応じてマークが付けられます。

図 *45*：ライブ分析ポリシーの無効化



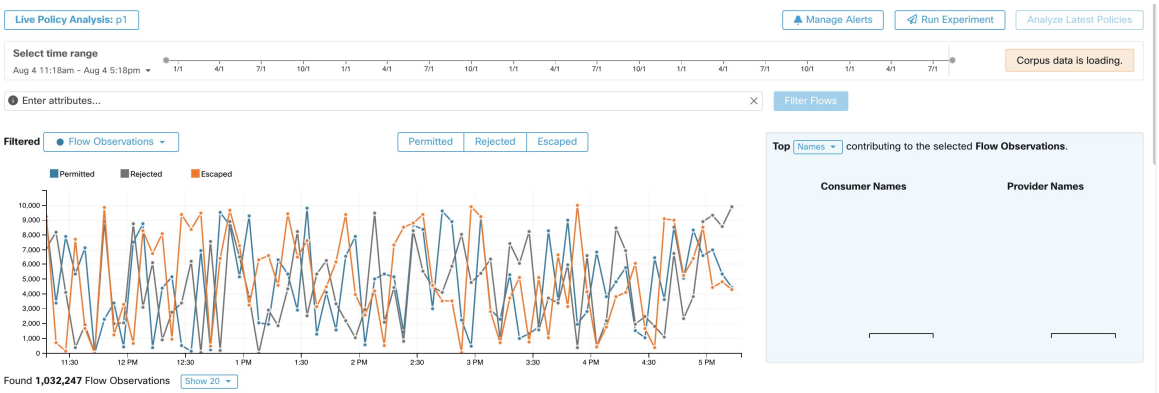
ポリシー分析の概要

[ポリシー分析（Policy Analysis）] ページには、公開されたポリシーをライブ ネットワーク トラフィックと照合した結果が表示されます。ポリシー分析ツールは、ワークスペースに関連付けられた範囲に出入りするすべてのフローを 3 つのカテゴリに分類します。

1. **許可**：フローはネットワークによって許可され、ポリシーグループによっても許可されました。
2. **エスケープ**：フローはネットワークによって許可されましたが、ポリシーグループに従ってドロップされました。
3. **拒否**：フローはネットワークとポリシーグループによってドロップされました。

次のスクリーンショットでは、このページの概要を確認できます。午後12時頃までは、フローが許可されています。その後、新しいポリシーが別のワークスペースによって公開され（このワークスペースで公開されると、ラベルフラグが作成されます）、フローがエスケープ済みとしてマークされました。

図 *46 :* ポリシー分析の概要



フロー検索ページと同様に、ファセットフィルタバーを使用して、このページに表示されるフロー情報をフィルタ処理できます。[フローのフィルタ処理（Filter Flows）] ボタンをクリックすると、それに応じてすべてのチャートが更新されます。チャートにカーソルを合わせると、そのタイムスタンプの時点で集約された観測フローの割合が表示されます。

さらに、そのタイムスタンプをクリックすると、フィルタ処理されたすべてのフローのリストが下の表に表示され、さらに分析できます。

時系列チャートの上部にあるカテゴリを選択または選択解除することで、インタラクションを 3 つのカテゴリのいずれかに制限することもできます。

フロー検索ページと同様に、右側に上位N件チャートがあります。これは、左側の時系列チャートに示されているデータに影響を与えた上位のホスト名、アドレス、ポートなどを示しています。ユースケースの例としては、時系列チャートをエスケープされたフローだけに制限し、上位N件チャートで「ポート」を選択して、エスケープされたフローに影響を与えた上位のポートを表示することができます（詳細は以下を参）。

上級ユーザー向けの詳細なポリシー分析

フローの処置

ポリシーライブ分析では、フローが**許可**、**エスケープ**、または**拒否**のいずれであるかを決定するには、最初にネットワークの観点からフローの**処置**を判定する必要があります。各フローは、Cisco Secure Workload ソフトウェアエージェント（リアルタイムのフロー データをキャプチャする優れた可視性エージェントと適用エージェントにのみ適用される）によって提供されるシグナルと観察から派生した、**ALLOWED**、**DROPPED**、または**PENDING** の処置を受け取ります。フローのパスに沿ったエージェント構成およびフロータイプに基づいた多くのシナリオがあります。

初めに、フロータイプに関係なく、フローのパスに沿ったいずれかのエージェント（優れた可視性エージェントまたは適用エージェント）で、フローが破棄されたことが報告されると、フローは DROPPED の処置を受け取ります。

フローのパスに沿ったエージェントによって破棄が報告されない場合、双方向フローと単方向フローの場合を別々に検討します。双方向フローが観察される場合、送信元、宛先ポート、プ

ロトコル、およびタイミングに基づいて、フローをペア（順方向と逆方向）で調査します。同じことは、単方向フローにはできません。

双方向フローの場合、優れた可視性エージェントまたは適用エージェントがインストールされ、両端でデータプレーンが有効になっている場合、送信元と宛先の両方のエージェントがフローが観察されたことを報告すると、順方向フローは ALLOWED の処置を受け取ります。それ以外の場合、順方向フローは PENDING の処置を取得します。送信元または宛先のいずれか一方に優れた可視性エージェントたは適用エージェントが 1 つしかインストールされていない場合、エージェントが **60** 秒の時間枠内に後続の逆方向フローを観察した場合に限り、順方向フローは ALLOWED の処置を受け取ります。それ以外の場合は、PENDING ステータスが順方向フローに割り当てられます。双方向フローの逆方向部分の処置は、送信元と宛先が逆になったことを除いて、同じロジックに従います。たとえば、一方の側にのみエージェントが存在する場合、逆方向フローの処置が PENDING か ALLOWED かは、同じロジックに基づく後続の順方向フローの観測とタイミングに依存します。

ファイアウォールがサイレントドロップを実装していると想定していることに注意してください。**同じ**フローで拒否メッセージが送信された場合（例：RST + ACK で TCP SYN を拒否）、逆方向のフローが検出され、以前の順方向のフローが ALLOWED としてマークされます。ただし、拒否メッセージが別のフローで送信される場合（例：ICMP メッセージで TCP SYN を拒否する場合）、順方向フローは PENDING のままになります。

単方向フローの場合、双方向フローの場合と同様に、いずれかのエージェントによって DROPPED と報告された場合、そのフローは DROPPED と見なされます。ただし、一致する逆方向フローがないため、両方のエージェントがフローを観察した場合、フローの処置ステータスは PENDING になります。

違反タイプ

フロー処置は、分析されているポリシーに照らしてチェックされ、最終的な違反の種類が決定されます。

フローの違反タイプは次の通りです。

- **許可**：その処置が ALLOWED または PENDING であり、その決定ポリシーアクションが ALLOW である場合
- **エスケープ**：その処置が ALLOWED であり、その決定ポリシーアクションが DENY である場合
- **拒否**：その処置が DROPPED または PENDING であり、その決定ポリシーアクションが DENY である場合

バージョン 3.4 以降では、Secure Workload ポリシー分析で [誤廃棄（Misdropped）] フローカテゴリが報告されないことに注意してください。Secure Workload システムは、関連するエージェントが明示的に DROPPED ステータスを報告しているフローにのみ、DROPPED ステータスを割り当てます。エージェントでドロップの明示的な報告がない場合、Secure Workload はフローがドロップされたかどうかを推測しなくなり、そのようなフローは PENDING ステータスを受け取ります。

処置が PENDING の場合、ポリシーの動作が信頼されます。具体的には、次の選択を行います。

- 処置が PENDING で、ポリシーアクションが DENY の場合、違反タイプは拒否に設定されます。
- 処理が PENDING で、ポリシーアクションが ALLOW の場合、違反タイプは許可に設定されます。

双方向フローの場合、フローの順方向部分と逆方向部分のポリシー違反のタイプが一致する場合、ポリシー分析または適用分析ページには1つのタイプのみが表示されます。それ以外の場合は、PERMITTED:REJECTED のように、順方向と逆方向が別々に表示されます。

次に、処置と違反のロジックに基づく、フロー違反タイプのシナリオの例をいくつか示します。

1. 送信元側の適用でパケットがドロップされた。
   - この場合、送信元側の Secure Workload 出力エージェントは、フローが DROPPED であると報告します。
2. パケットが送信元から出力された。
   - 送信元側に優れた可視性エージェントまたは適用エージェントのみが存在する場合、60秒の時間枠でエージェントによって逆方向パケットも観察された場合、フローは出力エージェントによって ALLOWED として報告されます。
   - 送信元側と宛先側の両方に優れた可視性エージェントがある場合、入力エージェントがフローが DROPPED であると報告した場合に限り、フローには DROPPED 処置ステータスが与えられます。それ以外の場合、フローは ALLOWED として報告されます。
3. 宛先でフローパケットが受信されたが、逆方向トラフィックがない。- 宛先側エージェントがない場合、フローはPENDINGステータスを取得します。それ以外の場合は、ALLOWED ステータスが割り当てられます。

ポリシー分析を使用した詳細な診断

3 つの違反タイプの定義を考えると、**エスケープした**フローは、特別な注意が必要であることが容易にわかります。それは、これらの実際のフローの処置が、現在分析されているポリシーの意図されたアクションと異なるためです。現在分析されているポリシーを適用すると、これらのフローがブロックされる可能性があります。これらのフローの一部が特定のアプリケーションの通常の動作にとって重要なフローである場合、このようなフローをブロックすると、それらのアプリケーションのパフォーマンスまたは機能に悪影響を及ぼす可能性があります。

したがって、最新のポリシーを適用しても意図しない適用結果が生じないことを保証するために、このカテゴリのポリシー結果を分析で調べることが重要です。次に、ポリシー結果についての診断を実施するときに、特定のフローへのドリルダウンに最も一般的に使用される、いくつかのフィルタ（および説明）に焦点を当てます。

1. エスケープしたフローまたは拒否されたフローのみをチェック

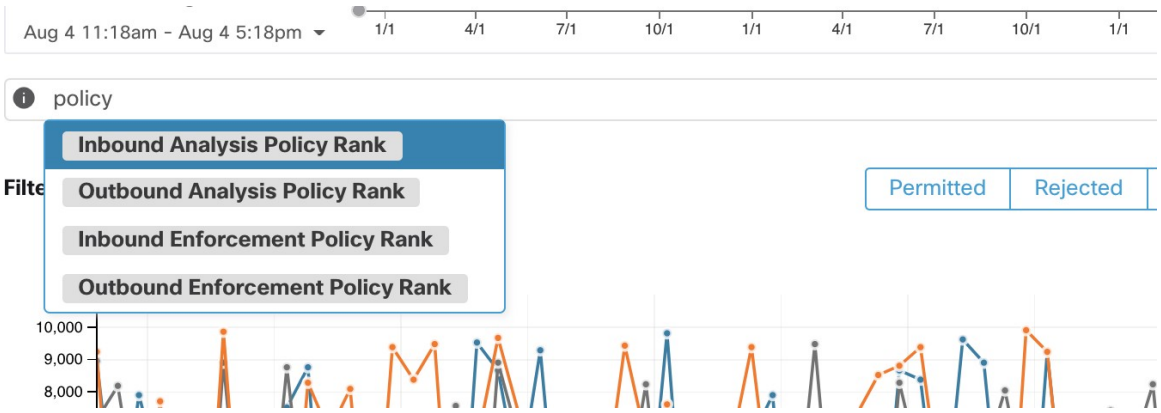
   ポリシー分析ページで特定のタイプのフローのみに注目するために、さまざまな違反タイプのフローをクリックして選択できます。

2. 着信および発信のポリシーランクを使用して、Catch-all ポリシーに一致するフローを特定する

   特に許可リストポリシーモデルでは、どのフローが Catch-all ポリシーに一致するかを理解することが重要です。これらのフローが正当であっても、これらのフローに対して明示的な許可ポリシーが構成されていない場合、ユーザーは、対応する着信または送信範囲に適切な明示的なポリシーを追加する必要がある場合があります。一方で、疑わしいフローであれば、迅速に特定し、詳細を調査する必要があります。

   これらのフローに焦点を当てるために、以下に示すように、注目するのが着信、発信、または両側なのかに応じて、**inbound_policy_rank** または **out-bound_policy_rank** の catch-all 値に基づいてフィルタを適用できます。

   図 *47*:



3. *RST* がある *TCP* フローの除外：順方向フラグ 次を含まない（*Fwd flags does not contain* ）*RST*、逆方向フラグ 次を含まない（*Rev flags does not contain*） *RST*

   一部のエスケープした TCP フローには、RST フラグが設定されています。これらのフローは、コンシューマまたはプロバイダーのいずれかによってリセットされます。これらは基本的にデータ交換のない確立されていない接続ですが、エージェントがハンドシェイクパケットを認識するため、ALLOWED と報告される場合があります。最初から接続が確立されていないため、現在分析されているポリシーが適用されても影響を受けません。いずれかの側で RST フラグが設定されている TCP フローを除外すると、現在分析されているポリシーによって確立された接続がブロックされる、より意味のある重要なエスケープフローに集中できます。

4. アドレスタイプ（*address type*） *= IPv4*、アドレスタイプ（*address type*） *!= IPv6*

   ほとんどのトラフィックが IPv4 を使用している場合は、IPv4 フローのみに注目します。リンクローカルアドレスを除外することにも役立ちます。

5. 上位のホスト名、上位のポート、上位のアドレス、上位の範囲

   TopN 機能ウィンドウからホスト名、ポート、またはアドレスを選択すると、分析されるフローの状況をすばやく調査できます。通常、これらを他のフィルタと組み合わせて、ポリシーを診断するときに特定のタイプのトラフィックにドリルダウンできます。これは、診断の次のステップでどのフローに注目するかの優先順位付けに役立ちます。

6. コンシューマホスト名が次の文字列を含む（*Consumer Hostname contains*）*{something}*、プロバイダホスト名が次の文字列を含む（*Provider Hostname contains*）*{something}*、プロバイダーポート（*Provider Port*） *= {some port number}*、プロトコル（*Protocol*） *= TCP*プロトコル（*TCP Protocol*） *!= ICMP*

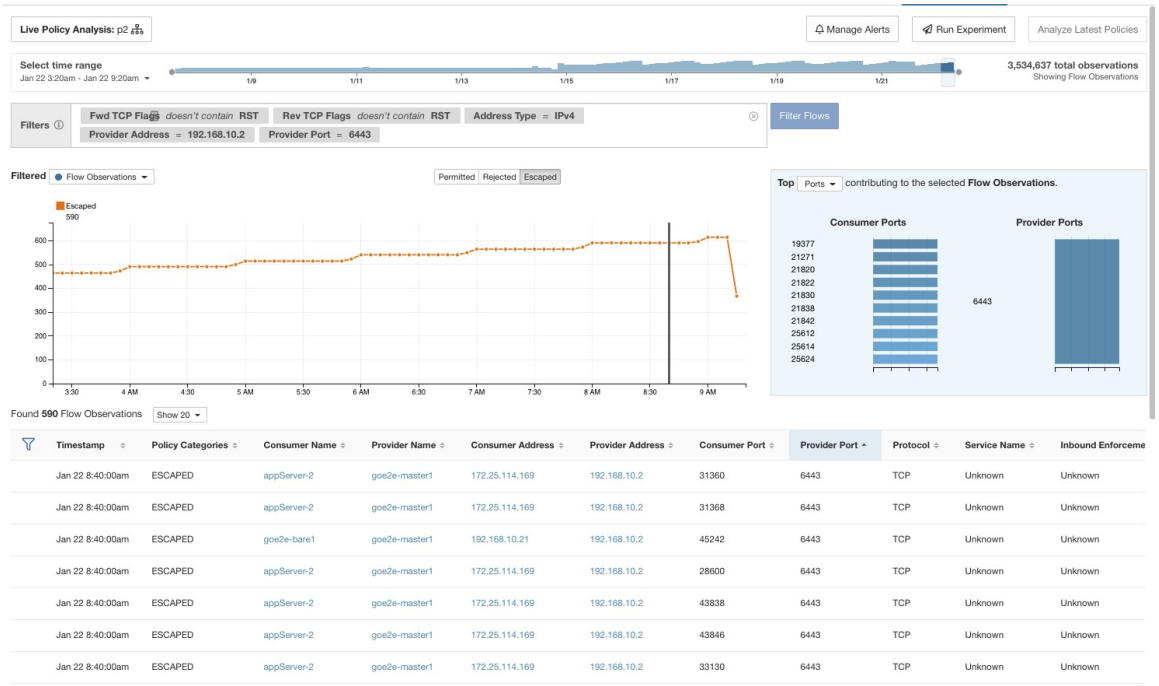
   ホスト名、ポートなどに関して、対象となるフローの上位候補について心当たりがあれば、上位Nクエリウィンドウで取得した値から直接ドリルダウンフィルタを適用するか、フロー検索フィルタバーに関連するフィルタを手動で入力して、フローをドリルダウンすることを選択できます。

7. 個々のフローを確認して迅速に分析

   最後に、フローに対応する行をクリックすることで、特定のフローに注目して、そのポリシーの結果を調べることができます。フローに一致したポリシー、およびコンシューマとプロバイダーの両方のアドレスの範囲に着目してください。ポリシーアクションが意図したアクションと一致しない場合は、コンシューマまたはプロバイダー（またはその両方）の範囲に関連付けられたワークスペースに適切なポリシーを作成して、ポリシーアクションを変更する必要があります。

   次の図は、ここで説明したフィルタリングの一部を使用して、エスケープしたフローを絞り込むワークフローの例を示しています。検索入力は、「-」を範囲クエリに変換することにより、ポート、コンシューマアドレス、プロバイダーアドレスで「,」および「-」をサポートします。

図 *48* : ポリシー分析診断の例



現在のポリシーの分析

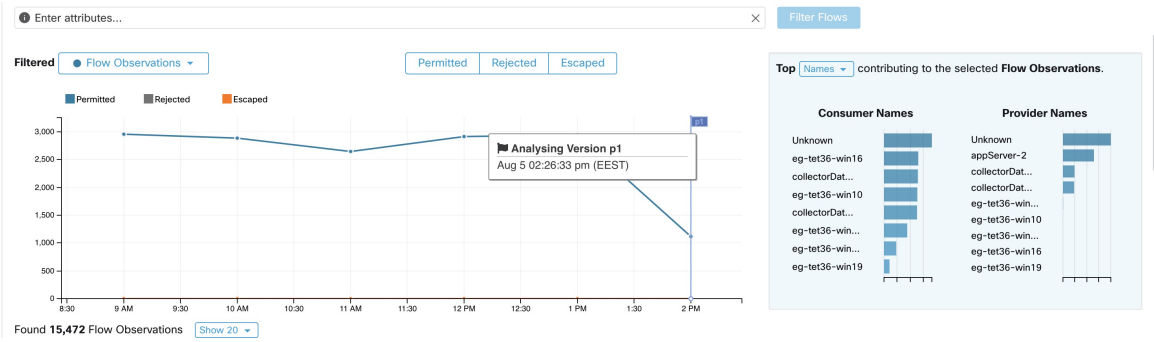
ワークスペースへの変更は、ポリシー分析ツールに自動的に同期されませんが、[最新のポリシーの分析（Analyze Latest Policies）] をクリックして変更を反映することで、ワークスペースを何度でも再公開できます。

特定のワークスペースを公開すると、そのワークスペースで定義されているすべてのクラスタとポリシーのスナップショットが取得され、詳細な分析が可能になります。それらのスナップショットは**ポリシー分析バージョン**と呼ばれ、「p1」のように文字「p」で始まります。

ポリシーラベルのフラグ

公開されたすべてのポリシーバージョンは、**ポリシーラベルのフラグ**を介してポリシー分析時系列チャートで調べることができます。フラグをクリックすると、[セマンティクスと表示（Semantics and Viewing）] ページの特定のポリシー分析バージョンに移動します。ポリシー属性 （50 ページ）

図 *49*：ポリシーラベルのフラグ



ポリシーラベル付きの時系列チャートには、時間の経過に伴うポリシーグループの変化が示されるため、複数のユーザーが元のワークスペースに変更を加え、分析のためにそれらのポリシーを公開した場合に、公開されたポリシーの変更を追跡できます。

適用ポリシーの結果のみが Secure Workload Data Platform で利用できます。

ポリシー実験

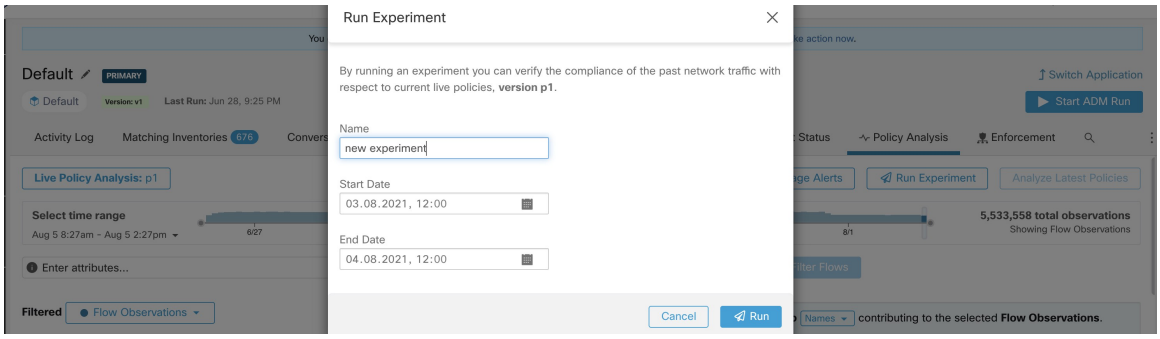
公開済みポリシーの分析のデフォルト動作は、ポリシーグループで定義されたルールに従ってライブネットワークトラフィックをマーキングすることです。ただし、特定の短期間のフロー（既知の攻撃など）は、該当するネットワークでは発生しないかもしれません。公開済みポリシー適用時の架空ネットワークセキュリティの動作を検証するために、以前の日付でのポリシー実験を作成できます。言い換えれば、このポリシー実験は「攻撃時にこの一連のネットワークポリシーがあったとしたらどうなるか」という質問に答えるのに役立ちます。

ポリシー実験を実行するには、次の 2 つの手順があります。

ステップ 1 ポリシー分析ページの右隅にある [実験の実行（Run Experiment）] ボタンをクリックします。

ステップ 2 新しいダイアログで、ポリシー実験の名前と期間を選択します。

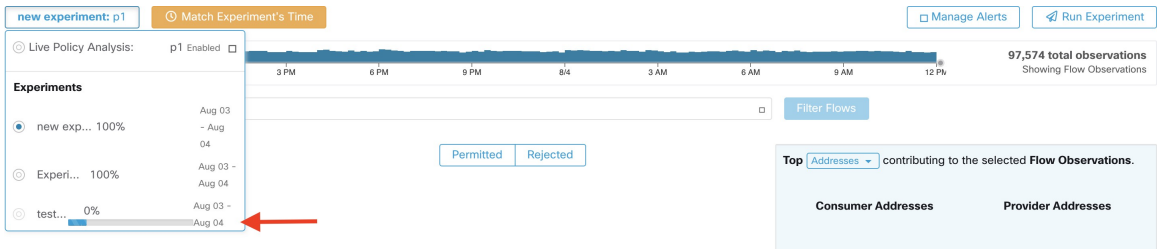
図 *50* : [実験の実行（*Run Experiment*）] フォーム



これにより、時間をさかのぼって、選択された公開済みポリシーに対して選択された期間内のすべてのフローを再分析する新しいポリシー分析ジョブが開始されます。

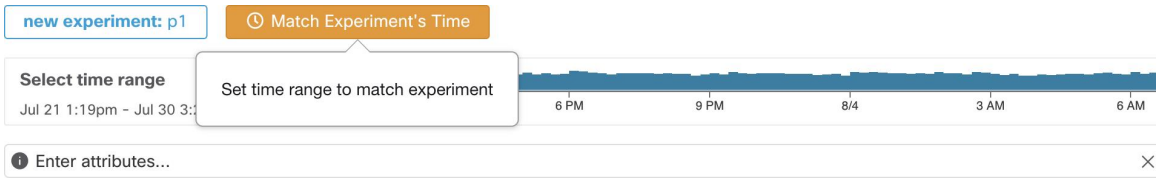
選択した期間によっては、このジョブに数分かかる場合があります。進行状況は、ポリシーセレクタメニューに表示されます。結果を表示する準備ができたら、他の公開済みポリシーと同様にポリシー実験を選択できるようになり、さまざまなフローカテゴリを示す時系列チャートが選択に応じて更新されます。

図 *51* : 実験



（注） ポリシー実験を選択したときにフローが表示されない場合は、時間範囲の不一致が原因である可能性があります。たとえば、チャートの現在の時間範囲が過去 1 時間なのに、実験期間は過去 6 時間になっている場合などです。時間範囲を実験期間に合うようにリセットするには、ポリシーセレクタの横にある時計アイコンをクリックします。

図 *52* : 時間範囲の適合化



ポリシー分析のアクティビティログ

すべてのワークスペースユーザーは、ワークスペース履歴のポリシー分析ページで行われた変更に関連するアクティビティログを表示できます（「履歴と差分」を参照）。

1. ポリシー分析の有効化

図 *53* : ポリシー分析の有効化

2. ポリシー分析の無効化

図 *54* : ポリシー分析の無効化

3. ポリシー分析の更新

図 *55* : ポリシー分析の更新

施行

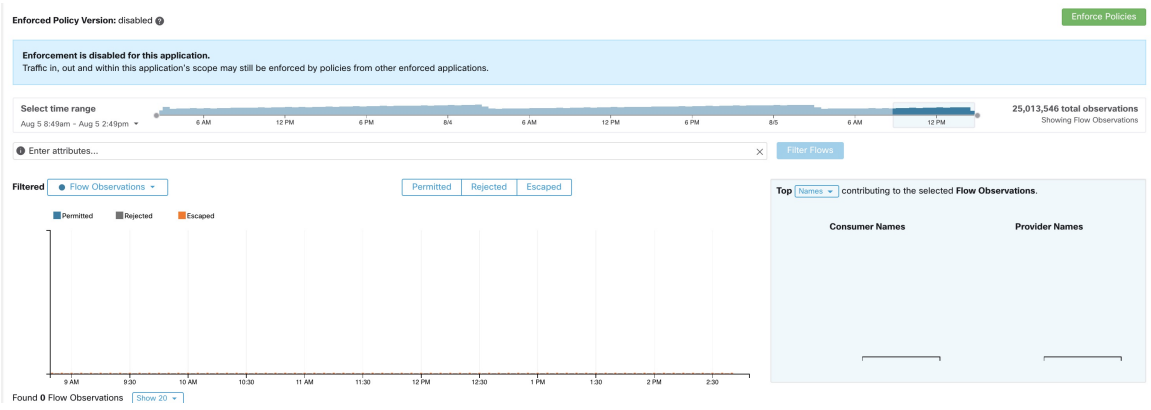
Secure Workloadは、統合されたロードバランサ（F5およびCitrix）やファイアウォール（Cisco Secure Firewall Management Center 経由）とともに、展開されたエージェントを介してワークロード全体にポリシーを直接適用できます。ポリシーは、サードパーティのオーケストレータにストリーミングして、サードパーティのインフラストラクチャで適用することもできます。

ポリシーの適用はライブ分析と似ていますが、ポリシーが範囲内でアセットにプッシュされ、**新しいファイアウォール ルールが書き込まれる**点が異なります。

（注） 続行する前に、ライブ分析の概念をよく理解してください。

警告 この機能を使用すると、**新しいホスト ファイアウォール ルールが挿入され**、関連するホスト上で既存のルールがすべて削除されます。

図 *56* : 適用が無効化されている *[*ポリシーの適用（ *Policy Enforcement*）*]* ページ



ポリシーの適用の有効化

ポリシーの適用においては、ユーザーはその範囲で適用以上の機能を持っている必要があります。範囲で他の機能を持つユーザーは引き続きこのページを表示できますが、新しいポリシーの適用（または無効化）はできません。機能の詳細については、「ロール」を参照してください。

ワークスペースでポリシーの適用を有効化する前は、[ポリシーの適用（Policy Enforcement）] ページには、別の範囲に関連付けられたワークスペースで作成されたポリシーによって、フローがどのように適用されているかが表示されます。たとえば、「Prod は非 Prod ホストと通信すべきではない」という広範なポリシーが親範囲の適用ワークスペースに存在し、この範囲におけるワークロードのトラフィックに影響を与える場合があります。

ポリシーの適用を有効化する手順は次のとおりです。

ステップ 1 ワークスペースが範囲における「プライマリ」であることを確認します。

ステップ 2 ライブ分析ツールを使用して、ポリシーが正しいことを確認します。

ステップ 3 このワークスペースの範囲に「適用」機能があることを確認します。

ステップ 4 ヘッダーの右側にある [ポリシーの適用（Policy Enforcement）] タブをクリックして、 [ポリシーの適用（Policy Enforcement）] ページに移動します。

ステップ 5 緑色の [ポリシーを適用する（Enforce Policies）] ボタンをクリックします。

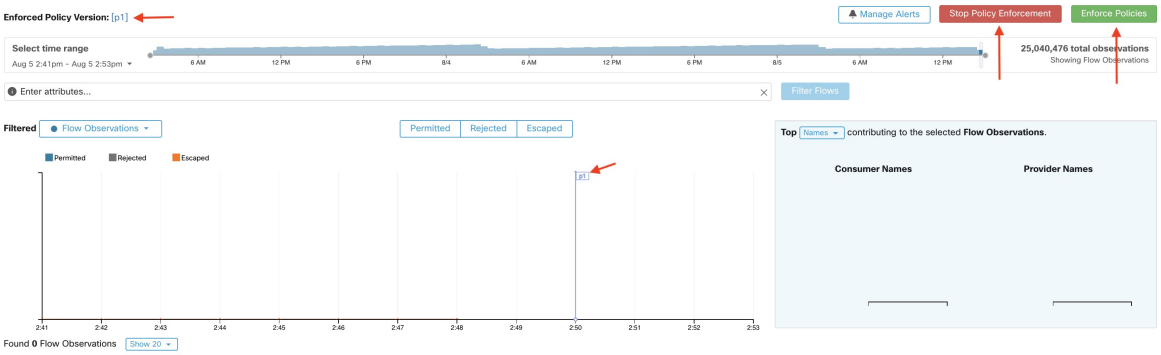
ステップ 6 適用の影響を確認し、新しいファイアウォールのルールがホストに書き込まれることを示す警告を受け入れます。

この時点で、新しいファイアウォールのルールが、この範囲に関連付けられたワークスペースに割り当てられたアセットにプッシュされます。キャッチオールルールはワークロードに広く適用されるため、範囲外のインターフェイスに影響を与える可能性があります。適用時にラベルフラグが作成されます。次のスクリーンショットを参照してください。

（注） 適用チャートに新しい情報が表示されない場合は、正しい時間範囲が選択されているかどうかを確認してください。

（注） 適用する前にポリシー分析を実行することが推奨されます。

図 *57 :* 適用が有効化されている *[*ポリシーの適用（ ***Policy Enforcement***）*]* ページ



ポリシー適用ウィザード

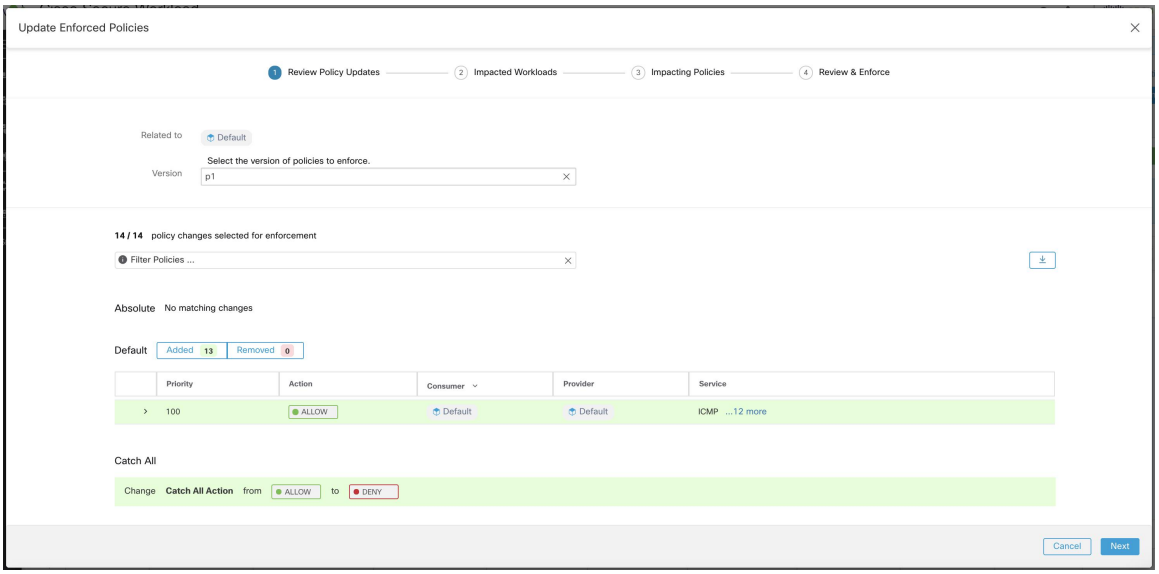
ポリシー適用ウィザードは、ワークロードに実装される前に、適用されたポリシーに対する可視性と予測可能性を提供します。また、適用（またはロールバック）するポリシーの変更を選択し、ワークスペース内で影響を受ける可能性のあるワークロードを確認するためのメカニズムを提供します。

ポリシー適用ウィザードには次の 4 つのステップがあります。

1. ポリシー更新の選択

   ワークロードに適用するポリシーのバージョンを選択でき、現在適用されているポリシーと選択したバージョンのポリシーの違いが表示されます。最新バージョンが選択されている場合、適用する変更のサブセットを選択できます。以前のバージョンが選択されている場合（ロールバックシナリオ）、ポリシーの変更は選択はできません。「ポリシーの差分」と同様に、ポリシーの変更をフィルタ処理して確認し、CSV としてダウンロードできます。

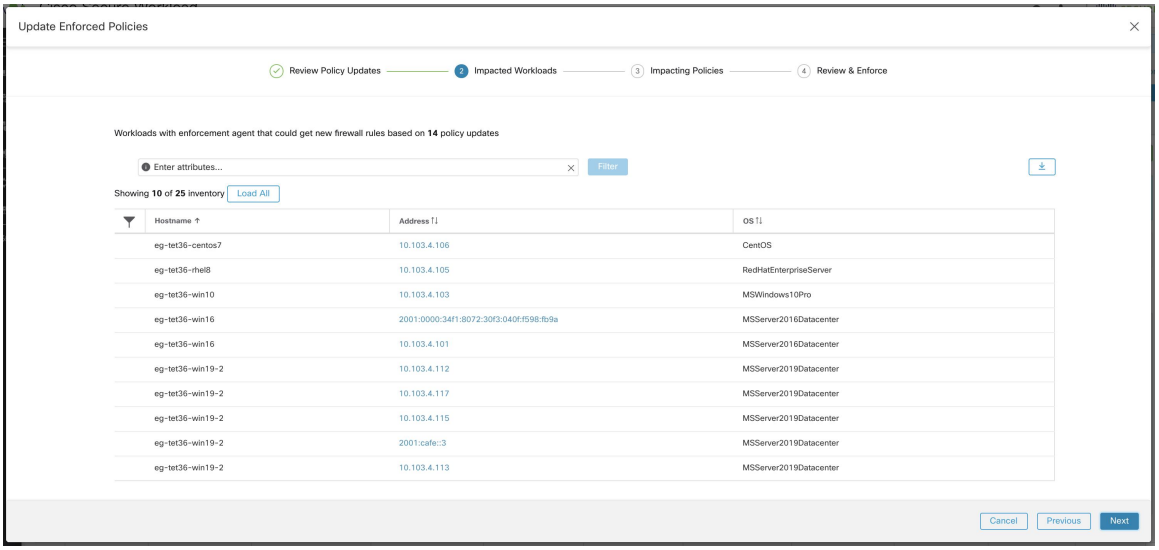
図 *58* : 適用するポリシーの変更を選択



2. 影響を受けるワークロード

このステップでは、選択したポリシーの変更から生成された新しいファイアウォールルールの影響を受けるワークロードが表示されます。結果は、選択したポリシー変更のコンシューマまたはプロバイダーの結合内に適用エージェントが存在するすべてのワークロードを検索した結果です。影響を受ける可能性のあるワークロードの数は、範囲内のワークロードの総数を超えることはありませんが、[エージェント構成インテント（Agent Config Intents）]などの他の要因により、実際に影響を受けるワークロードは少なくなる可能性があります。

図 *59* : 影響を受けるワークロードのリスト

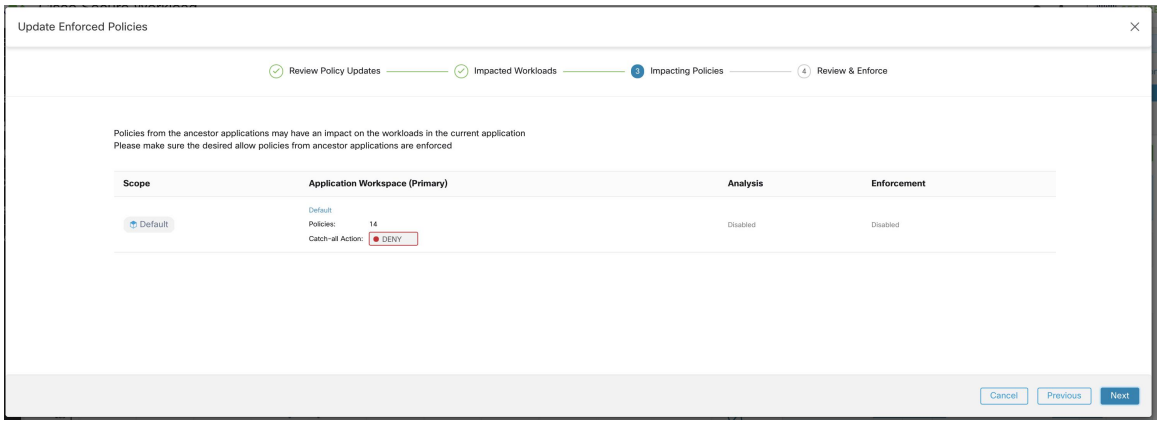


インベントリ項目の表示、フィルタリング、ダウンロードの詳細については、インベントリを参照してください。

3. 影響を与えるポリシー

先祖ワークスペースのポリシーは、現在のワークスペースのワークロードに影響を与える可能性があるため、ユーザーは、先祖ワークスペースから必要な許可ポリシーが適用されていることを確認する必要があります。

図 *60*：先祖ワークスペースと適用バージョンのリスト

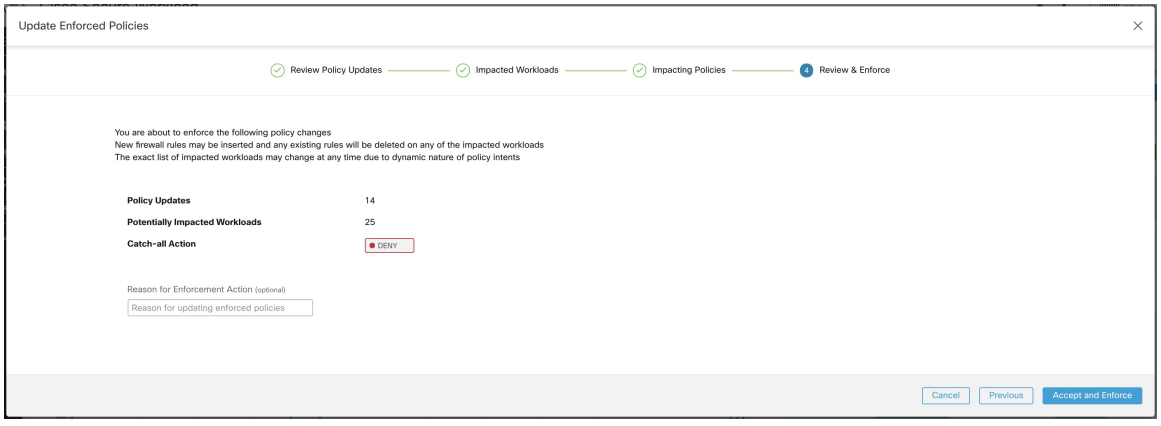


4. 確認と同意

この最後のステップでは、適用されるポリシー変更の概要、影響を受ける可能性のあるワークロードの数、適用されるCatch-Allアクションが提供されます。[同意して適用（Accept and Enforce）]ボタンが押されると、ポリシーインテントを使用して、関連するワークロードに設定される新しいファイアウォールルールが計算されます。

後で参照できるように、新しく適用されたポリシーの名前、説明、およびアクションの理由を提供するオプションがあります。ロールバックの場合、過去のバージョンの名前と説明は変更できないため、アクションの理由の設定のみが許可されます。

図 *61*：概要の確認およびポリシーの変更の適用



適用されたポリシーの表示

ポリシーが適用されると、新しいワークスペースバージョンが作成されます。このバージョンは「p*」の形式で、他のワークスペースバージョンと同様に表示されます。現在適用されている「p*」バージョンが、左側にリストされます。たとえば、上のスクリーンショットでは [適用されているポリシーバージョン（Enforced Policy Version）：[p1]] と表示されています。

「[p1]」または時系列チャートのラベルフラグをクリックすると、ワークスペースがそのバージョンに切り替わり、ポリシー属性が表示されます。

新しいポリシーの適用

適用のためにポリシーが公開されると、新しい（改善された）ポリシーを公開することができます。これを行うには、ページの右上にある [最新のポリシーを適用（Enforce latest policies）] ボタンをクリックします。上のスクリーンショットを参照してください。

ポリシー適用の無効化

ポリシーの適用を無効にするには、[ポリシー適用（Policy Enforcement）] ページに移動し、赤色の [ポリシー適用の停止（Stop Policy Enforcement）] ボタンをクリックします。これにより、先祖ワークスペースで適用されたポリシーに基づいて、範囲内のアセットに新しいファイアウォールルールが書き込まれます。「x」の付いたラベルフラグが時系列チャートに作成されます。上のスクリーンショットを参照してください。

ポリシーの有効なコンシューマまたは有効なプロバイダー

Cisco Secure Workload は、ポリシーの有効なコンシューマと有効なプロバイダーと呼ばれるポリシーモデルにおいて、詳細オプションをいくつか公開しています。これらのオプションを理解するには、ワークスペース内にあるポリシーのコンシューマフィルタやプロバイダーフィルタの意味を理解することが重要です。ポリシーのコンシューマフィルタやプロバイダーフィルタは、インストールされたファイアウォール ルールで使用される一連の IP アドレスの他に、ポリシーを受け取る Secure Workload エージェントの一連のワークロードを制御します。Secure Workload エージェントがポリシーを受け取ると、そのワークロードに固有のファイアウォールルールが書き込まれます。次の例でこれを詳しく説明します。

1.1.1.0/24 サブネットが指定されたプロバイダーフィルタを持つ許可ポリシーがあるとします。このポリシーが IP アドレス 1.1.1.2 の Linux ワークロードでプログラムされている場合、ホストのファイアウォールルールは次のようになります。

1. 着信トラフィックの場合、ファイアウォールルールは、サブネット 1.1.1.0/24 全体ではなく、厳密に 1.1.1.2 宛てのトラフィックのみを許可します。
2. 発信トラフィックの場合、ファイアウォールルールは、サブネット 1.1.1.0/24 全体からではなく、厳密に 1.1.1.2 からのトラフィックのみを許可します（スプーフィングを防ぐため）。

必然的に、1.1.1.0/24 サブネット内に IP アドレスを持たないワークスペースに属するエージェントのワークロードは、上記のファイアウォールルールを受け取りません。ただし、ポリシーを受信するワークロードとは異なるファイアウォールルールで、ポリシーが使用する一連の IP

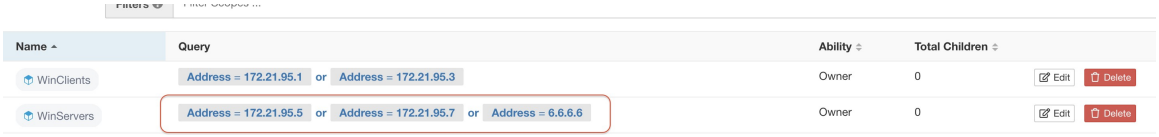
アドレスを指定する必要が生じることがあります。このような場合に、ユーザーは詳細ポリシーオプションを使用して、有効なコンシューマや有効なプロバイダーを指定できます。

この機能の使い方を説明するために、仮想 IP（VIP）の背後にある一連のワークロードのポリシーを設定する例を紹介します。これはキープアライブや Windows フェールオーバー クラスタリング ソリューションと似ています。

IP アドレス（*172.21.95.5* および *172.21.95.7*）を持ち、VIP - *6.6.6.6* の背後でサービスを提供する一連のワークロードについて考えてみます。この VIP はフローティング VIP であり、常に 1 つのワークロードのみが VIP を所有します。このクラスタ内のすべてのワークロードにファイアウォールルールをプログラムして、*6.6.6.6* へのトラフィックを許可することが目標です。

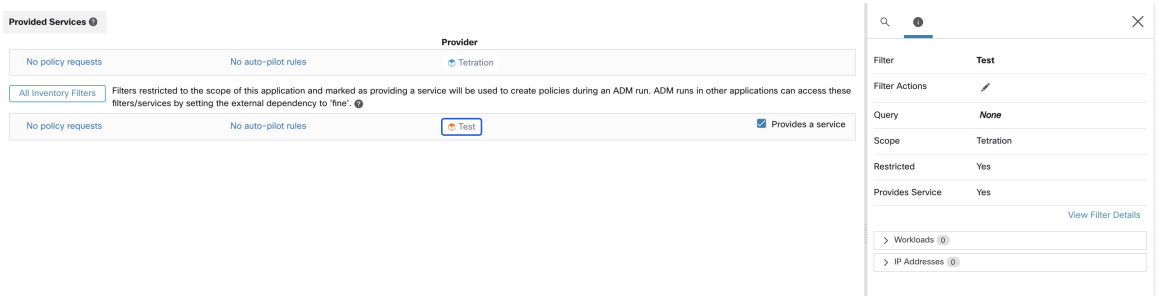
このセットアップでは、ワークロードのクラスタ（*172.21.95.5* および *172.21.95.7*）と VIP（*6.6.6.6*）で構成される範囲と対応するワークスペースがあります。

図 *62 : VIP* とワークロードのクラスタで構成される範囲



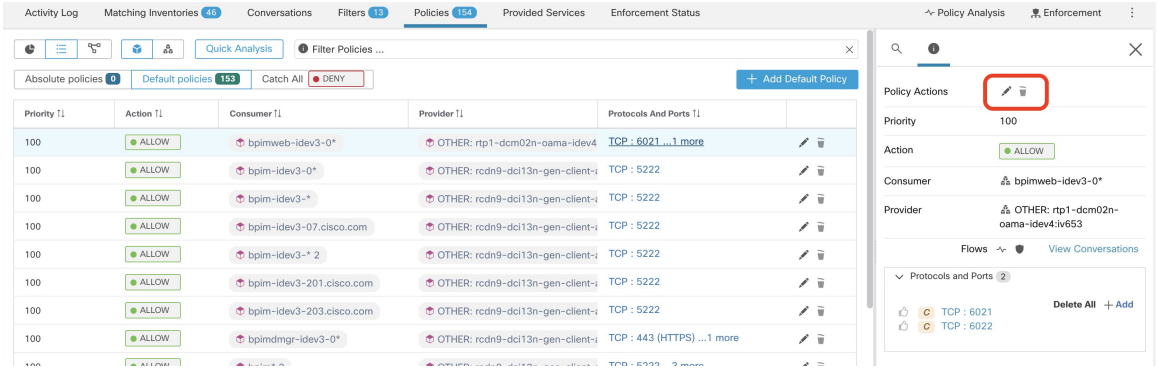
以下に示すように、VIP は提供サービスとしてこのワークスペースに公開されます。

図 *63 :* 提供サービスとして公開された *VIP*



このサービスのクライアントからサービス VIP にポリシーを追加することにした場合、（デフォルトでは）VIP へのトラフィックを許可するファイアウォールルールは、VIP を所有するワークロードでのみプログラムされます。このアプローチの問題は、フェールオーバーイベントが発生すると、その後サービス VIP を所有する新しいワークロードが適切なファイアウォールルールを取得するまでに時間がかかる場合があり、トラフィックが短時間中断される可能性があることです。

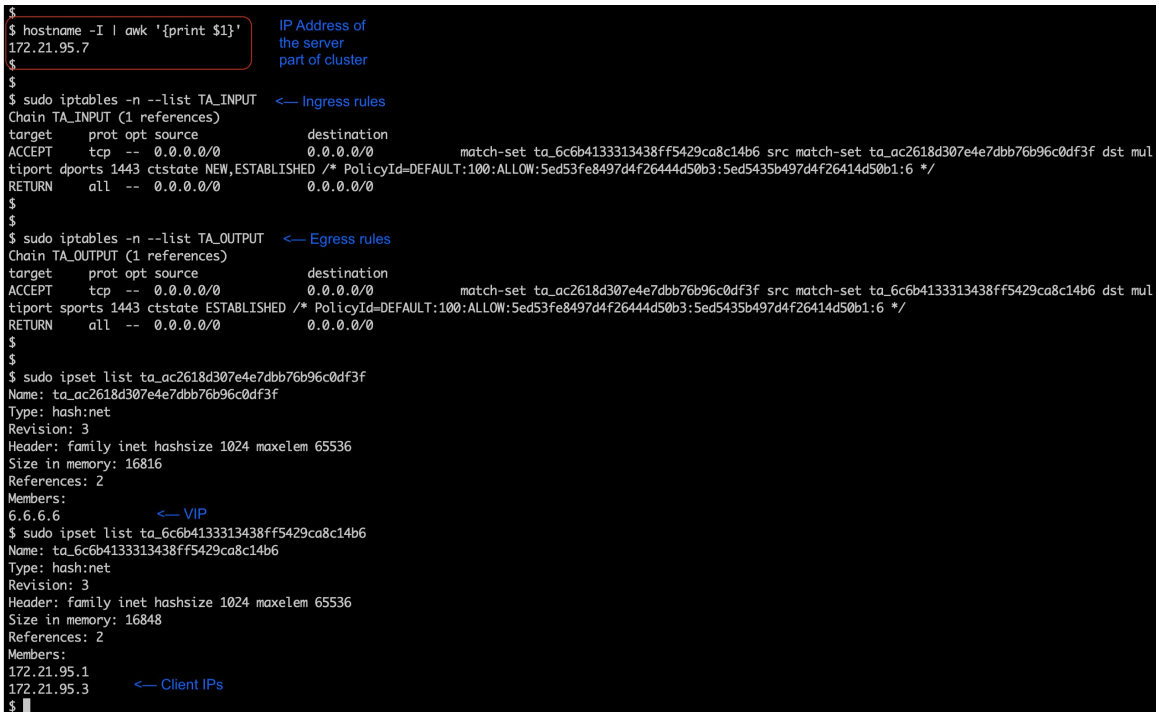
図 *64 :* クライアントからサービス *VIP* へのトラフィックを許可するポリシー



このようなシナリオでは、ユーザーはポリシーの右上にある [編集（Edit）] ボタンをクリックして、詳細ポリシーオプションに移動できます。このウィジェットには、[有効なコンシューマ（Effective Consumer）] と [有効なプロバイダー（Effective Provider）] の 2 つのオプションがあります。このユースケースでは [有効なプロバイダー（Effective Provider）] の設定で、サービス VIP へのトラフィックを許可するファイアウォールルールのプログラミングが必要な一連のワークロードを指定します。これらのワークロードのいずれかが VIP を所有しているかどうかは関係ありません。

[有効なプロバイダー（Effective Provider）] が設定されている場合、ワークロードが VIP を所有していない場合でも、6.6.6.6 へのトラフィックを許可するファイアウォール ルールがワークロード上でプログラムされていることを確認できます。サービスをサポートするすべてのワークロードをこれらのルールでプログラムできる場合、新しいプライマリワークロード（VIP を所有）には必要なファイアウォールルールがプログラムされるため、フェールオーバーイベント中にトラフィックが中断することはありません。

図 *65 : VIP* サービスへのトラフィックを許可するホストのファイアウォールルール



コンテナへの適用

Secure Workload は Kubernetes と OpenShift によって管理されるコンテナワークロード内でのポリシー適用をサポートします。これには、Kubernetes や OpenShift API サーバー用に外部オーケストレータ構成を追加し、サポート対象プラットフォームのいずれかで適用エージェントを使用する必要があります。詳細については、「外部オーケストレータ」および「ソフトウェアエージェントの展開」を参照してください。

注目 **Kubernetes や OpenShift ホストで稼働しているエージェントは、既存のルールを保持するように設定する必要があります。**

適用エージェントが Kubernetes によって追加された iptables ルールに干渉しないようにするには、[ルールの保持（Preserve Rules）] オプションが有効になっているプロファイルを使用してエージェントを設定する必要があります。「エージェント設定プロファイルの作成」を参照してください。

コンテナにポリシーを適用すると、Secure Workload は Kubernetes および OpenShift のサービス抽象化をプロバイダーとして使用できるようにします。内部的には、サービス抽象化のポリシーは、プロバイダーポッドとそれらが実行されているノードのルールに変換されます。この変換は、Kubernetes および OpenShift サービスのタイプに依存し、API サーバーから変更を受け取るたびに動的に更新されます。

次の例は、この機能によって実現する柔軟性を示しています。*db* という名前の *NodePort* タイプの Kubernetes サービスに対して、ラベル *environment = prod* を持つすべてのホストとポッドからのトラフィックを許可する次のポリシーについて考えます。このサービスは一連のポッドで TCP ポート 27017 を公開しています。

コンシューマ	プロバイダー	プロトコル/ポート	アクション
environment = prod OR orchestrator_environment = prod	orchestrator_system/service_name = db	TCP 27017	許可

このポリシーにより、次のファイアウォールルールが適用されます。

- *environment = prod* の注釈が付けられたホストとポッドで、サービスが属するクラスタのすべての Kubernetes ノードへの発信接続を許可します。このルールは、Kubernetes によってこのサービスに割り当てられたノードポートを使用します。
- ラベルが *environment = prod* のポッドで、Kubernetes によってこのサービスに割り当てられた ClusterIP への発信接続を許可します。このルールは、サービスによって公開されているポートを使用します（TCP 27017）。
- サービスが属するクラスタの Kubernetes ノードで、プロバイダーポッドへの発信接続を許可します。このルールは、サービスによって公開されているターゲットポートを使用します（TCP 27017）。
- サービスデータベースを提供するポッドでは、すべての Kubernetes ノード、およびコンシューマホストとポッドからのすべての着信接続を許可します。このルールは、サービスによって公開されているターゲットポートを使用します（TCP 27017）。

サービスのタイプ、ポート、および一連のプロバイダーポッドの変更は、Secure Workload のルールジェネレータによってすぐに取得され、生成されたファイアウォールルールを更新するために使用されます。

警告 **Warning（注意）：Kubernetes および OpenShift 項目を含むポリシーは、Kubernetes クラスタの内部操作との競合を避けるために慎重に設計する必要があります。**

Secure Workload によってインポートされた Kubernetes および OpenShift 項目には、Kubernetes クラスタを構成するポッドとサービスが含まれます（例：kube-system 名前空間のポッド）これにより、Kubernetes クラスタ自体を保護するために正確なポリシーを定義できますが、不適切に設計されたポリシーがクラスタの操作に影響を与える可能性もあります。

ポリシー更新の一時停止

すべての適用エンドポイントでルールの更新を防止するには、[適用ステータス（Enforcement Status）] に移動して一時停止または一時停止解除を行います。適用ステータスこの機能は、サイト管理者およびカスタマーサポート用です。

図 *66* : ルールを継続的に更新

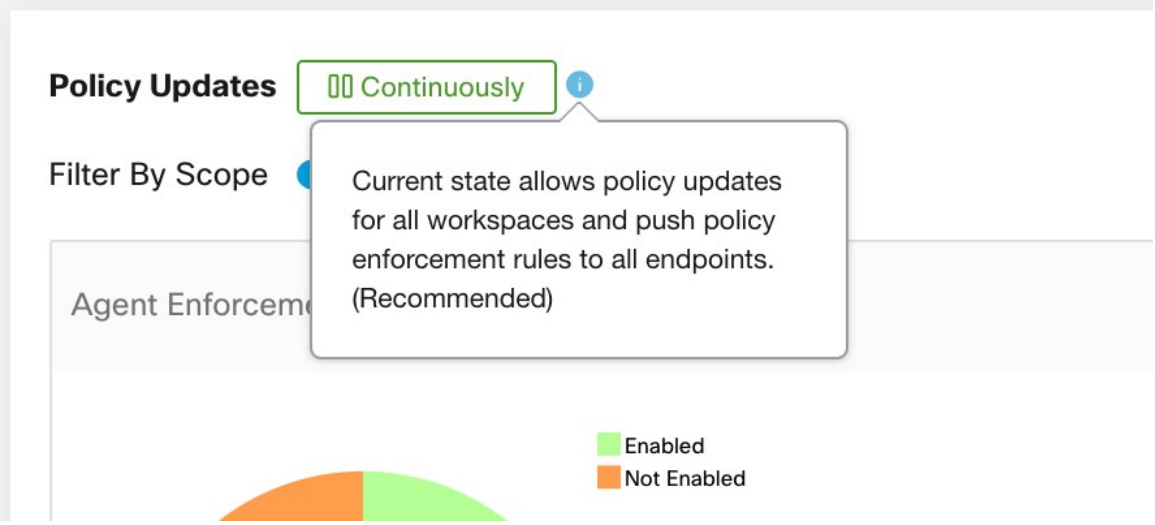


図 *67* : ルールの更新を一時停止中

アプリケーション間の連携例

範囲が異なるコンシューマとプロバイダーなどのクロス範囲トラフィックの例を以下で詳しく紹介します。この例では、コンシューマのポリシー担当者がプロバイダーのポリシー担当者とは異なることを想定しているため、これらのポリシーの詳細な設定方法について説明します。

複数の層とサービスで構成される認証アプリケーションについて考えてみます。この認証アプリケーションは、他の多くのアプリケーション向けインフラストラクチャとして機能し、特定のポートで特定の認証サーバー群へのアクセスを必要とします。

依存関係を持つ（コンシューマ）アプリケーション（HR など）で認証アプリケーションの認証サービスを使用するポリシーを作成すると、HR マシンのアウトバウンドルールにのみ影響

します。これは、ポリシーの適用範囲がHRアプリケーションに限定されているためです。ポリシーがカンバセーションの両端でトラフィックを分析または適用する場合、両端のポリシーはそのようなフローを許可する必要があります。

このシナリオでは、HRの所有者（コンシューマ）は、認証アプリケーションの所有者（プロバイダー）に正しいポートで認証サーバーへのアクセスを許可するポリシーを作成してもらう必要があります。HRアプリケーションの所有者が認証アプリケーションとのカンバセーションを許可するポリシーを作成すると、認証アプリケーション（プロバイダー）に同じトラフィックを許可するように求めるポリシー要求が自動的に生成されます。ポリシー要求は、認証アプリケーションが属する範囲のプライマリワークスペース内にある [提供サービス（Provided Services）] タブに表示されます。

図 *68 :* 異なる範囲に属するアプリケーションへのサービスの提供

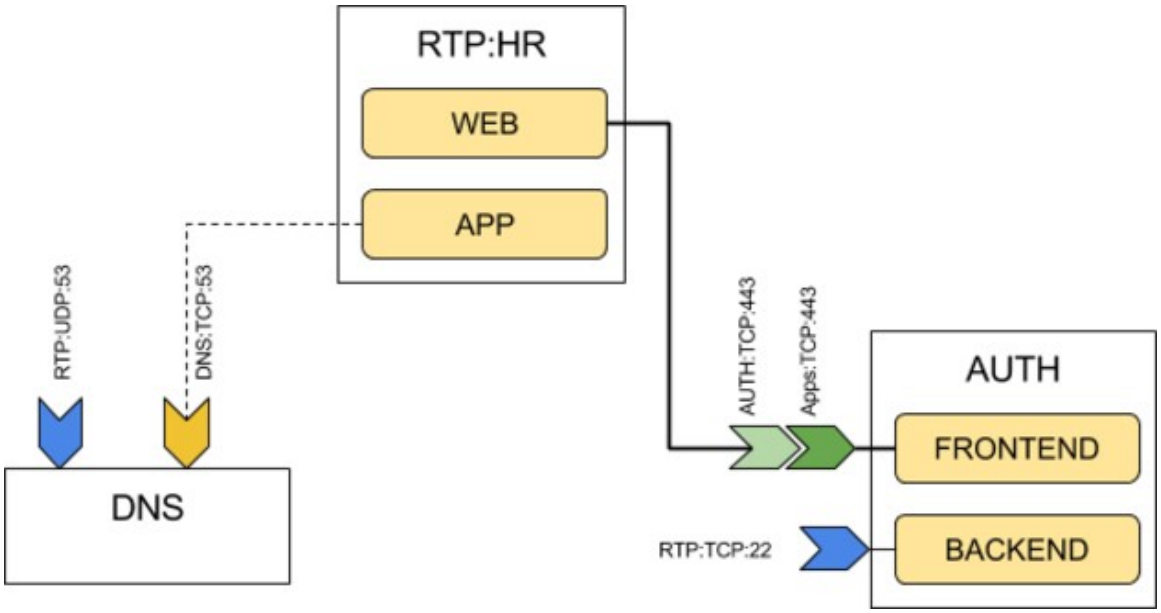
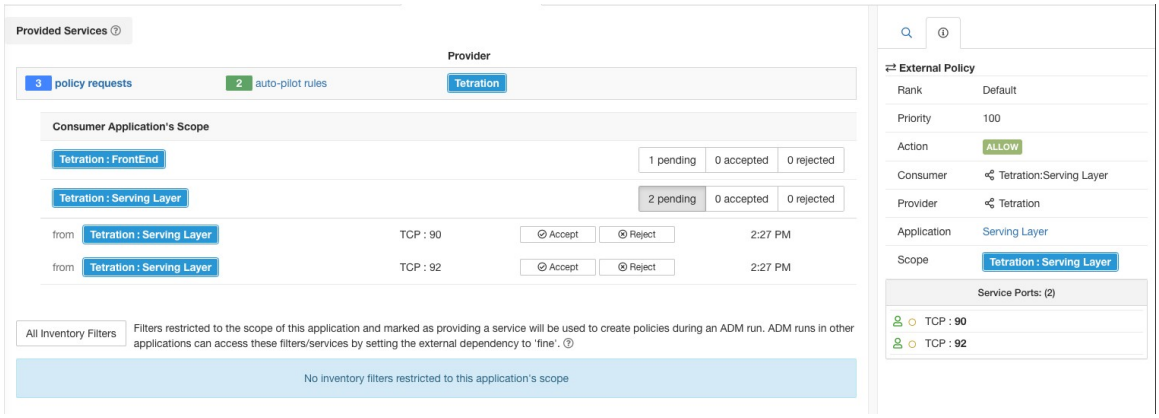


図 *69 :* コンシューマ アプリケーションから提供サービスへのポリシー要求



提供されるサービス

このページのオプションの詳細については、

- ポリシー要求 （89 ページ）
- オートパイロットルール （96 ページ）
- インベントリフィルタの作成 および 外部依存関係 （21 ページ） （[サービスの提供（Provides a service）] オプションに関する情報）を参照してください。

このページにアクセスするには、プライマリワークスペースに移動し、[ポリシーの管理（Manage Policies）]、[提供されるサービス（Provided Services）] の順にクリックします。

ポリシー要求

プロバイダーが別の範囲のメンバーであるときに、コンシューマ範囲のプライマリワークスペースにポリシーが作成されるたびに、プロバイダーの範囲に関連付けられたプライマリワークスペースにポリシーがまだ存在しない場合、ポリシー要求が生成されます。

このポリシー要求は、依存するアプリケーションに必要なサービスへのアクセスを許可するようプロバイダーアプリケーションの所有者に警告します。

「ポリシー要求の表示、承認、および拒否 （91 ページ）」および「」で、ポリシー要求を表示および応答するためのオプションを参照してください。

ポリシーリクエストに関するその他の詳細

- 提供されるサービスページ（ポリシー要求が表示される）は、プライマリワークスペースでのみ使用できます。これは、セカンダリワークスペースでの隔離された実験によって、他のプライマリワークスペースで通知が作成されないようにするためです。
- 外部範囲（ポリシーで指定されたプロバイダーがコンシューマとは異なる範囲に属している場合）にプライマリワークスペースがない場合、要求は送信されません（たとえば、ルート範囲の場合や、組織外のワークロードに対して定義された範囲の場合に該当する可能性があります）。外部範囲がポリシーを公開していない場合、ポリシーの分析と適用はコンシューマ側でのみ実行されます。
- プロバイダーがコンシューマとは異なる範囲にある場合、クラスタはサポートされません。ポリシーのコンシューマがクラスタの場合、ポリシー要求がコンシューマアプリケーションの範囲からのものであるかのように作成されます。プロバイダーからの同じサービスを消費する複数のポリシーをグループ化できます。
- ポリシー要求はプロバイダーに対してのみ生成され、コンシューマに対しては生成されません。コンシューマワークスペースがポリシーを分析または適用している場合、自動ポリシー検出または明示的な手動ポリシー作成によって、すべての正当な消費フローを許可するポリシーを明示的に含める必要があります（外部プロバイダーワークスペースからのポリシー要求は生成されません）。

ポリシー要求の例

次の例では、FrontEnd アプリケーションが、**FrontEnd** 範囲から **Tetration** 範囲へ TCP ポート 22 と UDP ポート 514 で 2 つのポリシーを作成しています。Serving Layer アプリケーションは、**ServingLayer** 範囲から **Tetration** 範囲へ、TCP ポート 90 と UDP ポート 92 で 2 つのポリシーを作成しています。

2 つのポリシー要求が Tetration ワークスペース（Tetration 範囲のプライマリワークスペース）にすぐに送信され、FrontEnd アプリケーションと ServingLayer アプリケーションのポリシーは保留中の状態で表示されます。

図 *70* : コンシューマアプリケーションのワークスペースで作成されたポリシー

ポリシー要求のステータスが、保留中（FrontEnd）と表示されています。

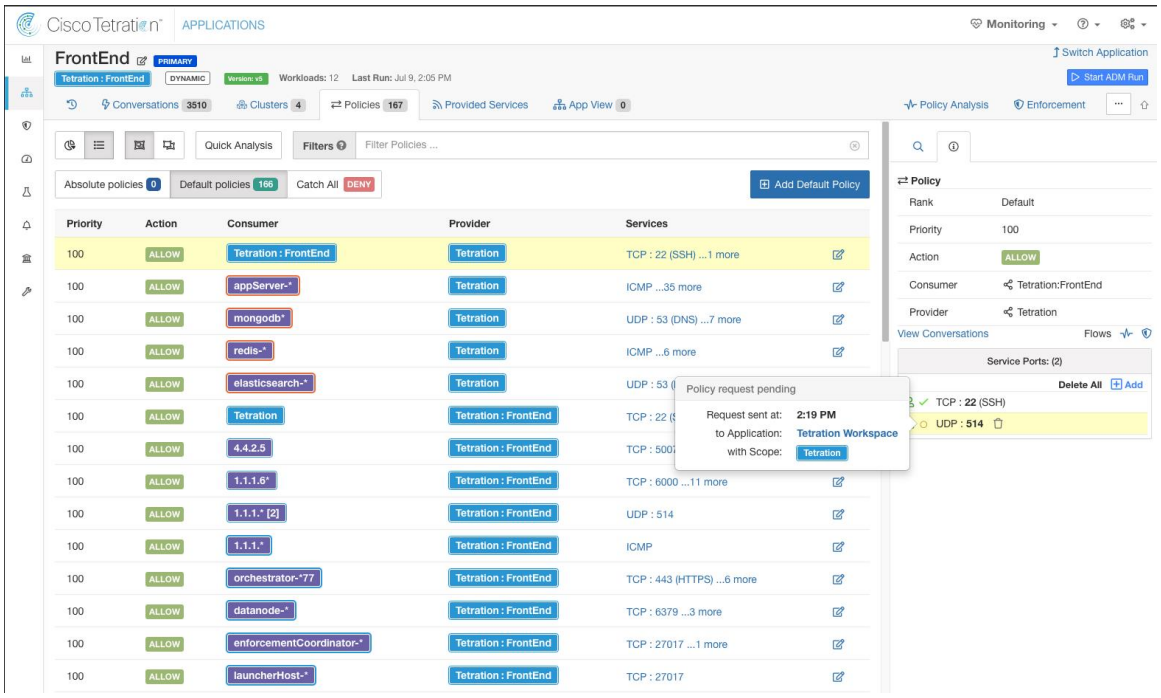
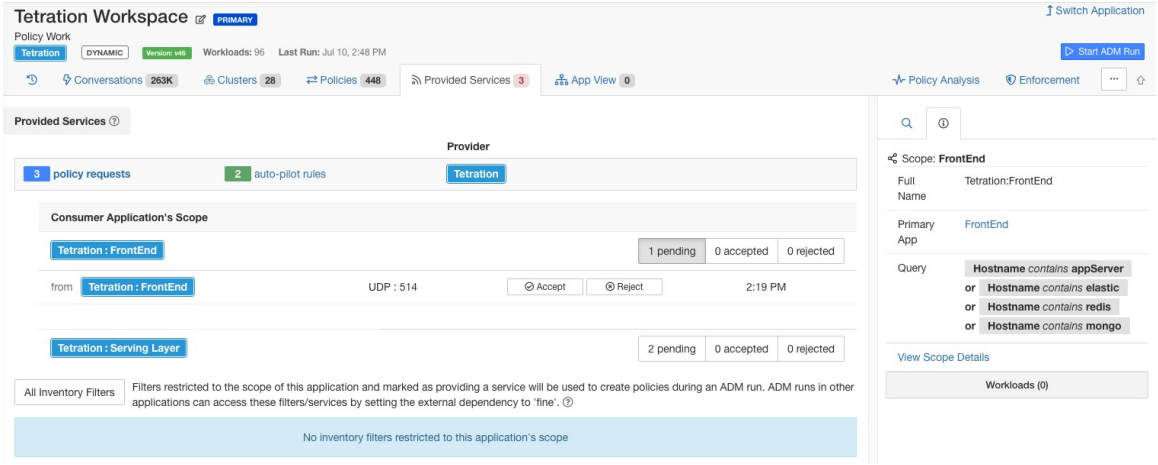


図 *71* : プロバイダー アプリケーション ワークスペース（*Tetration* ワークスペース）で保留中のポリシー要求



ポリシー要求の表示、承認、および拒否

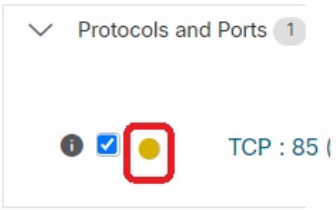
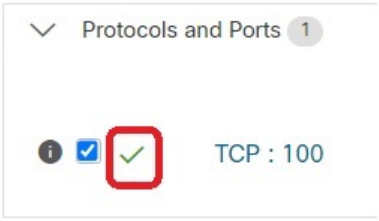
コンシューマの範囲のプライマリワークスペースでクロス範囲ポリシーが作成されると、プロバイダーの範囲のプライマリワークスペースでポリシー要求が自動的に作成されます。

このトピックの情報を使用して、要求を受け入れる（プロバイダー範囲で必要なポリシーを作成する）か、要求を拒否します（拒否するとクロス範囲ポリシーは有効になりません）。

ポリシー要求を表示、承認、または拒否する方法：

目的	操作手順
すべてのポリシー要求を表示する	**1.** [防御（Defend）] > [セグメンテーション（Segmentation）] の順に選択します。 **2.** ポリシーページの最上部にある [ポリシー要求（Policy Requests）] をクリックします。 **3.** 特定のコンシューマ範囲をクリックして、その範囲からのポリシー要求を表示します。

目的	操作手順
特定の範囲のポリシー要求を表示する	プロバイダー範囲の保留中のポリシー要求を表示するには、次の手順を実行します。 **1.** [防御（Defend）] > [セグメンテーション（Segmentation）] の順に選択します。 **2.** 該当する範囲のプライマリワークスペースをクリックします。 **3.** [ポリシーの管理（Manage Policy）] をクリックします。 **4.** [提供されるサービス（Provided Services）] をクリックします。 タブに数値が表示されない場合、このワークスペースに保留中のポリシー要求はありません。 **5.** [ポリシー要求（Policy Requests）] をクリックします。 **6.** 特定のコンシューマ範囲をクリックして、その範囲からのポリシー要求を表示します。
要求を手動で受け入れると、プロバイダー範囲に必要なポリシーが自動的に作成されます。	上記のいずれかの場所で、ポリシー要求の横にある [承認（Accept）] をクリックします。
要求を手動で拒否する	上記のいずれかの場所で、ポリシー要求の横にある [拒否（Reject）] をクリックします。

目的	操作手順
コンシューマワークスペースからポリシー要求ステータスを表示する	プライマリ コンシューマ ワークスペースの [ポリシー（Policies）] ページで、ポリシーをクリックしてから、ポート/プロトコルの値をクリックします。ステータスは、右側に開くパネルに表示されます。 保留中の要求は、黄色のドットで表示されます。  要求が承認されると、ドットが緑色のチェックマークに  変わります。 詳細についてはインジケータをクリックしてください。
プロバイダーのワークスペースからポリシー要求ステータスを表示する	上記の [提供されるサービス（Provided Services）] タブで要求ステータスを表示します。
ポリシー検出でプロバイダーに必要なポリシーを作成できるようにする	対応するフローが確実に表示される時間範囲を使用して、プロバイダー範囲のプライマリワークスペースでポリシーを自動的に検出し、ポリシーを公開します。

ポリシー要求の承認：詳細

サービスでポリシー要求を承認することは、コンシューマとしての要求されたフィルタから、プロバイダーとしてのサービスに向けてポリシーを作成することと同じです。さらに、ポリシー要求を承認すると、コンシューマ アプリケーションのワークスペース（この例では、FrontEnd アプリと Serving Layer）からの元のポリシーが承認済みとしてマークされます（下の図を参照）。

図 *72*：ポリシー要求の承認/拒否

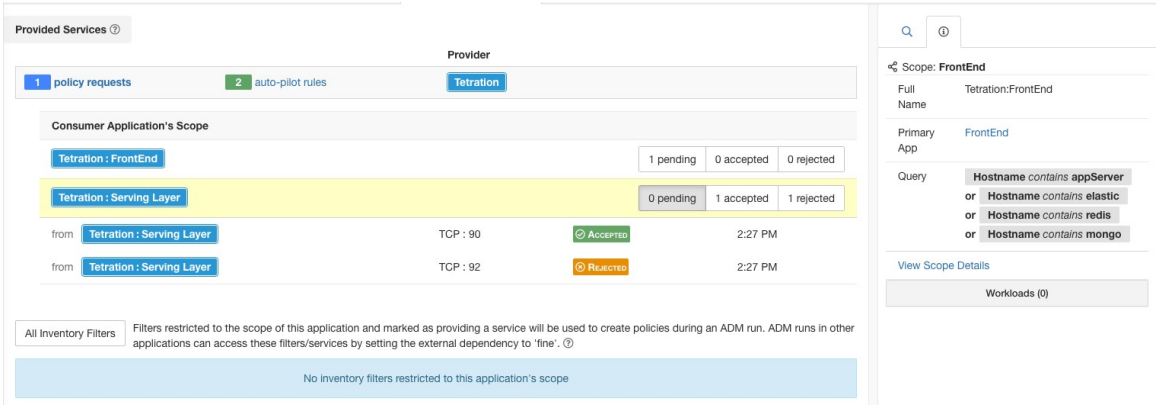
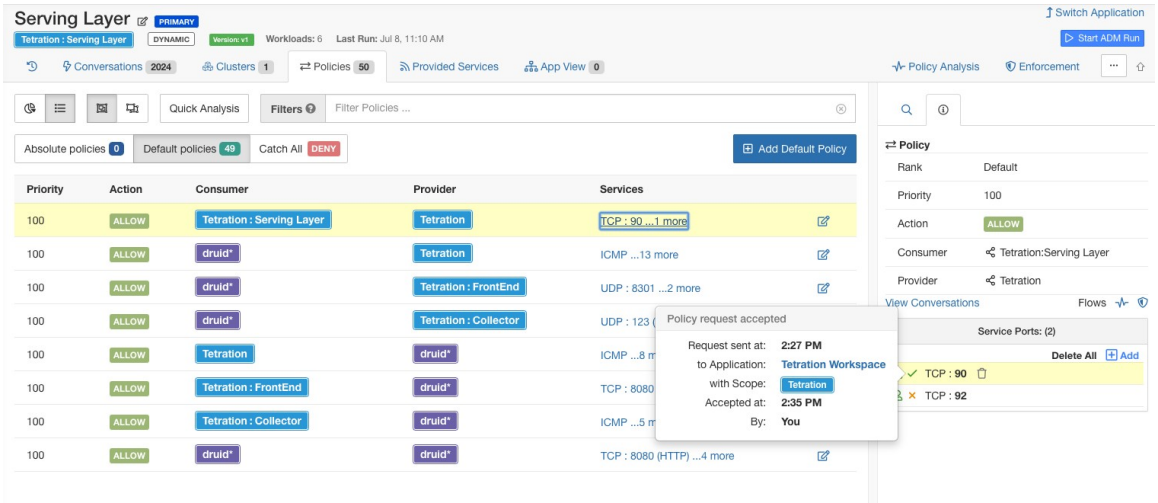


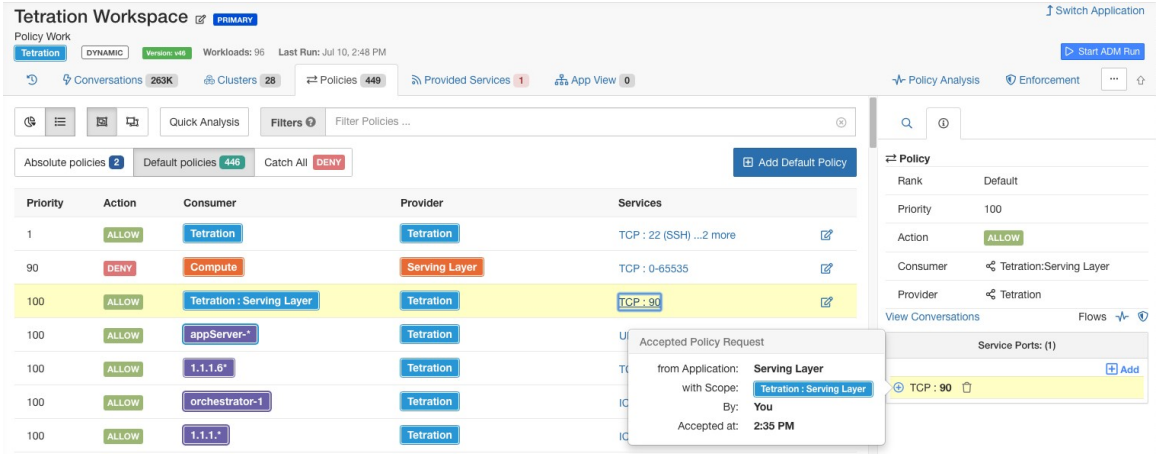
図 *73*：承認済みとして表示されるポリシーのステータス



プロバイダー アプリケーションのワークスペース（この例では、ワークスペースの名前は Tetration）で作成された新しいポリシーには、このポリシーが外部ポリシー要求によって作成されたことを示す [プラス（plus）] アイコンが付いています。

（注） ポリシー要求が承認された後に、コンシューマ側の元のポリシーが削除された場合、プロバイダー側のポリシーは削除されません。ただし、ポリシーの横にあるツールチップには、元のポリシーがイベントのタイムスタンプとともに削除されたものとして表示されます。

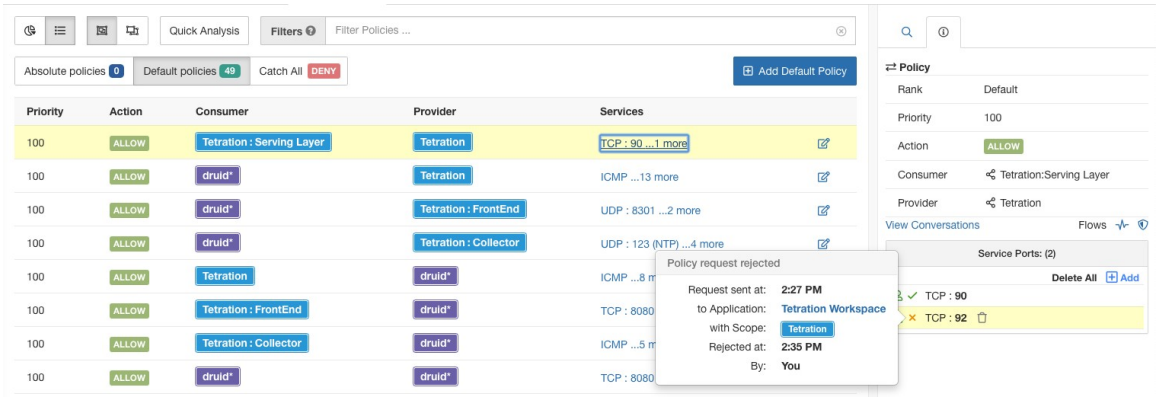
図 *74 :* ポリシー要求を承認することによって作成されたプロバイダー側のポリシー



ポリシー要求の拒否：詳細

ポリシー要求を拒否した場合、いかなるポリシーも作成または更新されません。コンシューマアプリケーションのワークスペース（この例では、Serving Layer アプリ）の元のポリシーは拒否されたことが示されますが、そのポリシーは有効なままです。つまり、アウトバウンドトラフィックは引き続き許可されます。拒否されたポリシーの横にあるツールチップには、プロバイダーアプリケーション、ポリシー要求を拒否したユーザー、拒否の時刻に関する情報が表示されます。

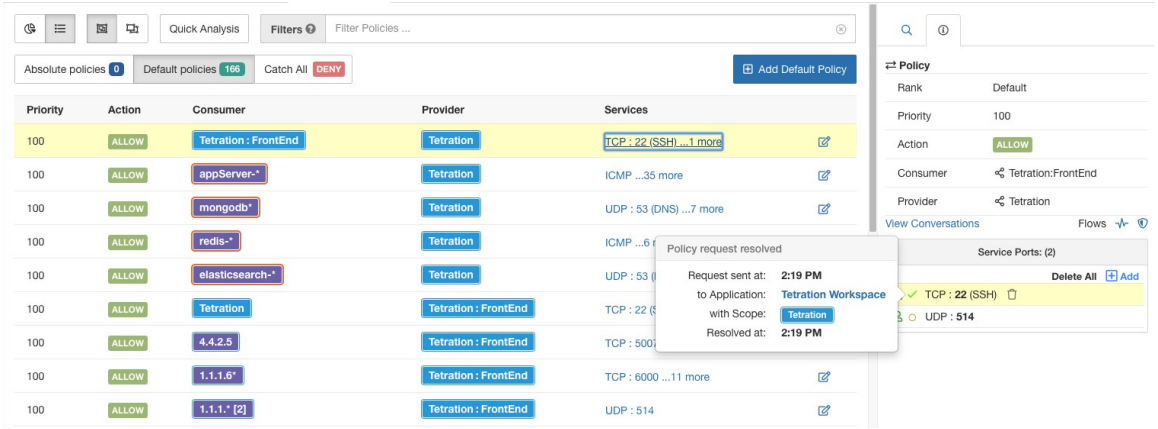
図 *75 :* 拒否されたと表示されるポリシーのステータス



解決済みのポリシー要求

ポリシー要求を作成するためのすべての条件が満たされているが、プロバイダーアプリケーションのワークスペースに既存の一致するポリシーが存在する場合、コンシューマアプリケーションのワークスペースで作成されたポリシーは解決済みとしてマークされ、プロバイダーアプリケーションのワークスペースが要求されたポートを介してトラフィックをすでに許可していることを示します。

図 *76 :* ポリシーのステータスが解決済みとして表示されている



オートパイロットルール

データセンター内の他の多くのアプリケーションにサービスを提供するインフラストラクチャアプリケーションには、他のアプリケーションからのポリシー要求が殺到する可能性があります。

将来の一致するポリシー要求を自動的に受け入れるか拒否するオートパイロットルールを作成することで、殺到を減らすことができます。

（注） オートパイロットルールは、既存のポリシー要求には適用されません。将来のポリシー要求にのみ影響します。

オートパイロットルールを使用してポリシー要求を自動的に受諾または拒否する

指定されたポートで、指定されたコンシューマとプロバイダーのペア間のポリシー要求を自動的に受け入れるか拒否するようにオートパイロットルールを構成します。オートパイロットルールは、広範囲（範囲間）にすることも、各範囲内のワークロードのサブセットにのみ適用することもできます。サブセットは、インベントリフィルタによって構成されます。コンシューマ、プロバイダー、またはそれぞれに対してインベントリ フィルタを使用できます。

1. オートパイロットルールを範囲全体ではなく、範囲内のワークロードのサブセットに適用する場合は、次のようにします。

   関連する範囲でインベントリフィルタを作成して、ワークロードをグループ化します。範囲のメンバーであるワークロードのみがフィルタに含まれるように、各インベントリフィルタで [クエリを所有権の範囲に制限する（Restrict Query to Ownership Scope）] オプションが選択されていることを確認してください。

2. [防御（Defend）] > [セグメンテーション（Segmentation）] を選択します。

3. 特定のプロバイダーに関連するポリシー要求を自動的に受け入れるか拒否するコンシューマ範囲のプライマリワークスペースをクリックします。

4. [ポリシーの管理（Manage Policy）] をクリックします。
5. [提供されるサービス（Provided Services）] をクリックします。
6. インベントリフィルタに対してこのルールを作成する場合は、目的のインベントリフィルタに対して次の手順を実行します（インベントリフィルタはオレンジ色のアイコンで識別されます）。

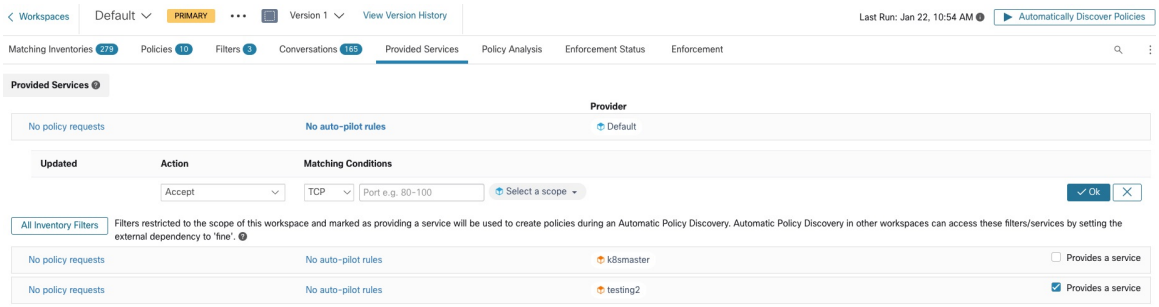
   それ以外の場合は、範囲に対してこれらの手順を実行します（範囲は青いアイコンで識別されます）。

   正しい場所をクリックしていることを確認してください。
7. [オートパイロットルールなし（No Auto-Pilot Rules）] または [オートパイロットルール（Auto-Pilot Rules）] のいずれか表示されている方をクリックします。
8. **[新規オートパイロットルール（New Auto-Pilot Rule）]** をクリックします。
9. オートパイロットルールを構成します。プロバイダーを表す範囲またはインベントリフィルタを選択します。
10. [OK] をクリックします。

オートパイロットルールの例

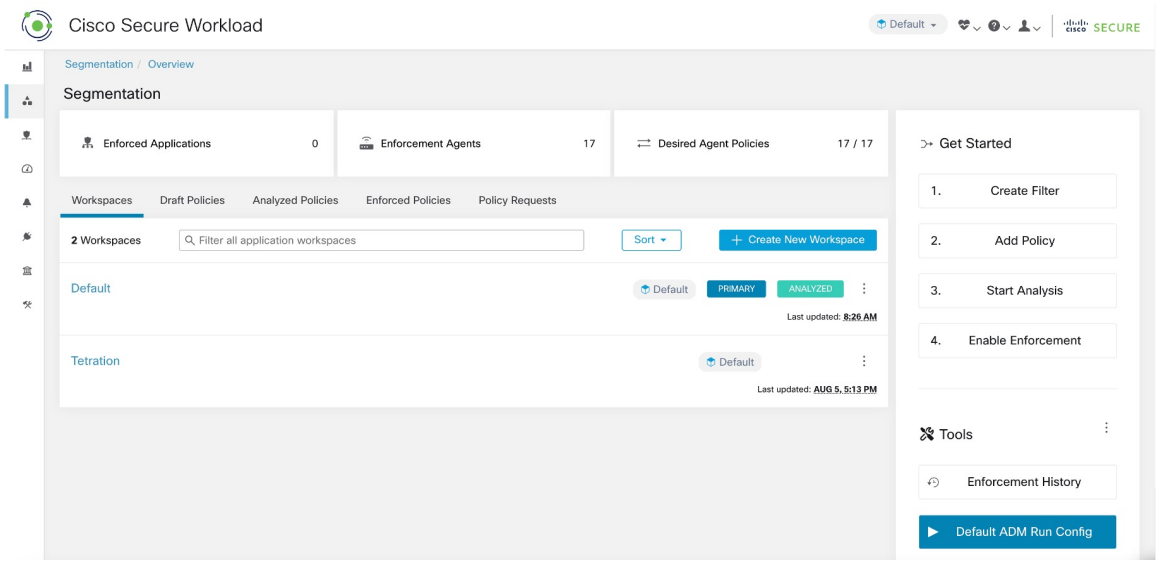
以下の例では、Tetration:Adhoc に含まれる任意のコンシューマからプロバイダーサービス Tetration への、ポート範囲 1 ～ 200 における TCP ポリシー要求を拒否する新しいオートパイロットルールを作成します。

図 *77*:オートパイロットルールの作成/更新



次に、FrontEnd アプリケーションのワークスペースに TCP ポート 23 における新しいポリシーを作成します。ポリシーはオートパイロットルールに一致するため、自動的に拒否されます。ポリシー拒否のステータスと理由が、拒否されたポリシーの横のツールチップに表示されます。

図 *78 :* オートパイロットルールによってポリシーが自動的に拒否される



オートパイロットルールによって作成されたポリシーの数を表示する

ワークスペースで最後に公開されたポリシーバージョン（p*）が作成されて以降、オートパイロットルールによってワークスペースで作成されたポリシーの数を表示する方法：

関連するプライマリワークスペースの [提供されるサービス（Provided Services）] ページに移動し、「自動作成された」ポリシーの数を探します。

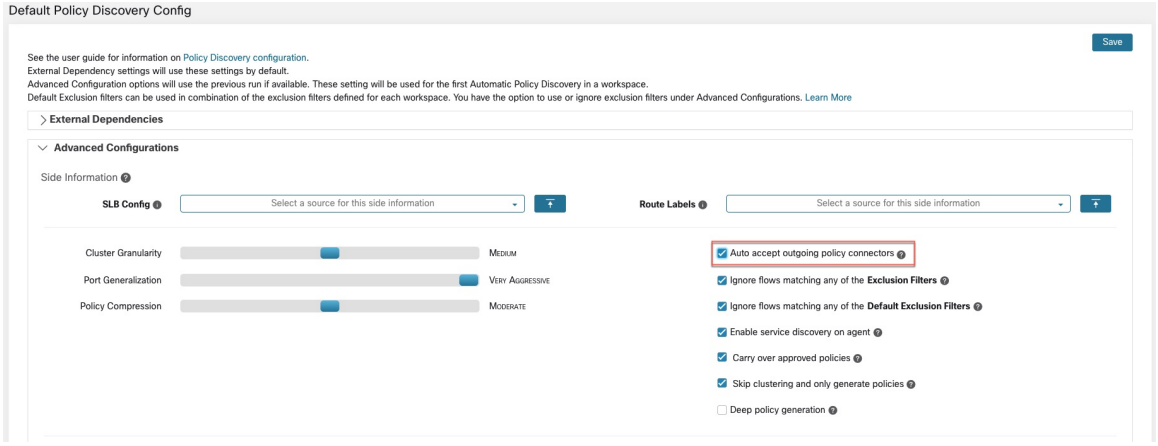
自動承諾ポリシーコネクタ

自動ポリシー検出構成ページの [発信ポリシーコネクタを自動的に受け入れる（Auto accept outgoing policy connectors）] オプションを使用すると、自動ポリシー検出、手動ポリシー作成、またはワークスペースインポートの一部として作成されたポリシー要求を自動的に受け入れることができます。

（注） このオプションは、ルート範囲の所有者のみが使用できます。

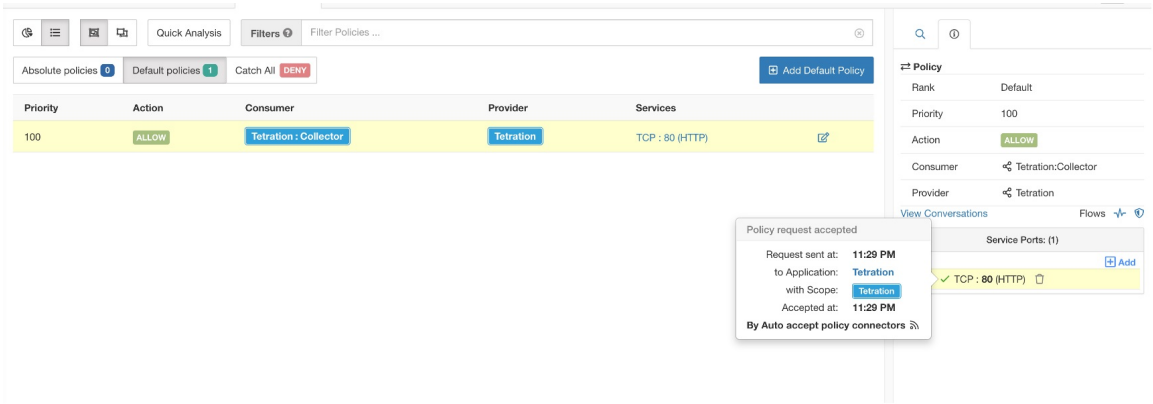
このオプションは、デフォルトのポリシー検出構成として設定するか、各ワークスペースの自動ポリシー検出の詳細オプションで設定できます。

図 *79* : 発信ポリシーコネクタの自動受け入れオプション



このオプションを設定すると、該当するワークスペースで作成されたポリシー要求は、すべて自動的に受け入れられます。

図 *80* : ポリシーはポリシーコネクタの自動受け入れによって自動的に受け入れられる



ポリシーパブリッシャ

ポリシーパブリッシャは Cisco Secure Workload の高度な機能であり、サードパーティベンダーは、ロードバランサやファイアウォールなどのネットワークアプライアンス向けに最適化された独自の適用アルゴリズムを実装できます。この機能は、定義済みのポリシーを Secure Workload クラスタ内にある Kafka インスタンスに公開し、お客様に Kafka クライアント証明書を提供することによって実現されます。これにより、サードパーティー ベンダー コードは Kafka からポリシーを取得でき、これらのポリシーを独自のネットワークアプライアンス構成に適宜変換できます。

このセクションの目的は、サードパーテベンダー、つまり以下におけるユーザーが Linux 上の Java でポリシーパブリッシャ機能を利用するために実行する必要がある手順を説明することです。

前提条件

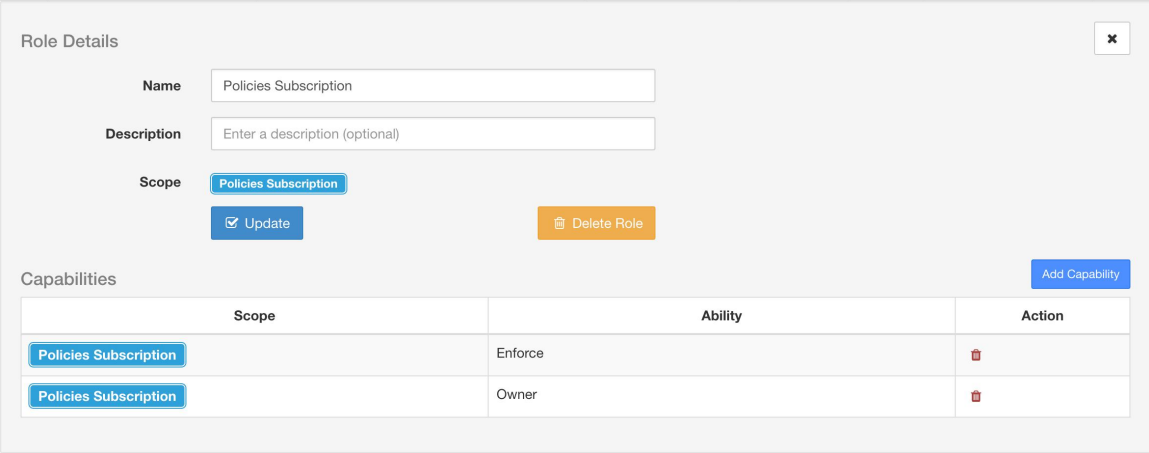
Ubuntu 16.04 などを搭載している Linux システムに次のソフトウェアパッケージがインストールされていること：

- Java 8 JDK
- Apache Kafka クライアント：kafka-clients-1.0.0.jar
- プロトコルバッファコア：protobuf-java-3.4.1.jar
- Apache Log4j：log4j-1.2.17.jar
- Java 用のシンプルなロギングファサード：slf4j-api-1.7.25.jar, slf4j-log4j12-1.7.25.jar
- Java 用のシンプルなコンプレッサ/デコンプレッサ：snappy-java-1.1.4.jar

Kafka クライアント証明書の取得

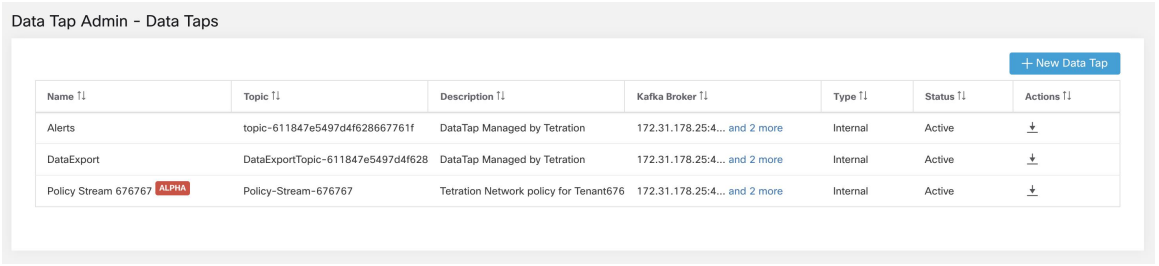
- 「所有者」のケーパビリティを持つユーザーロールを作成し、選択したユーザーアカウントに割り当てます。

図 *81 : Kafka* からポリシーを受け取るためのユーザーロール設定



- 「施行」の説明に従って、ポリシーの適用を実行します。この最初のステップは、アクティブな範囲に関連付けられた Kafka トピックを作成するために必要です。
- **[管理（Manage）] > [データタップ管理者（Data Tap Admin）]**に移動します。
- [データタップ（Data Taps）] タブを選択し、[アクション（Actions）] 列のダウンロードボタンをクリックして、Kafka クライアント証明書をダウンロードします。ダウンロードダイアログで [Javaキーストア（Java Keystore）] フォーマットを選択してください。

図 *82 : [データタップ（Data Taps）] ビュー*



- ダウンロードされたクライアント証明書ファイルには、通常、*Policy-Stream-10-Policies-Subscription.jks.tar.gz* のような名前が付いています。ディレクトリを作成し、作成したディレクトリの下に以下のように解凍します。

```
mkdir Policy-Stream-10-Policies-Subscription
tar -C Policy-Stream-10-Policies-Subscription -zxf Policy-Stream-10-Policies-
Subscription.jks.tar.gz
```

Protobuf 定義ファイル

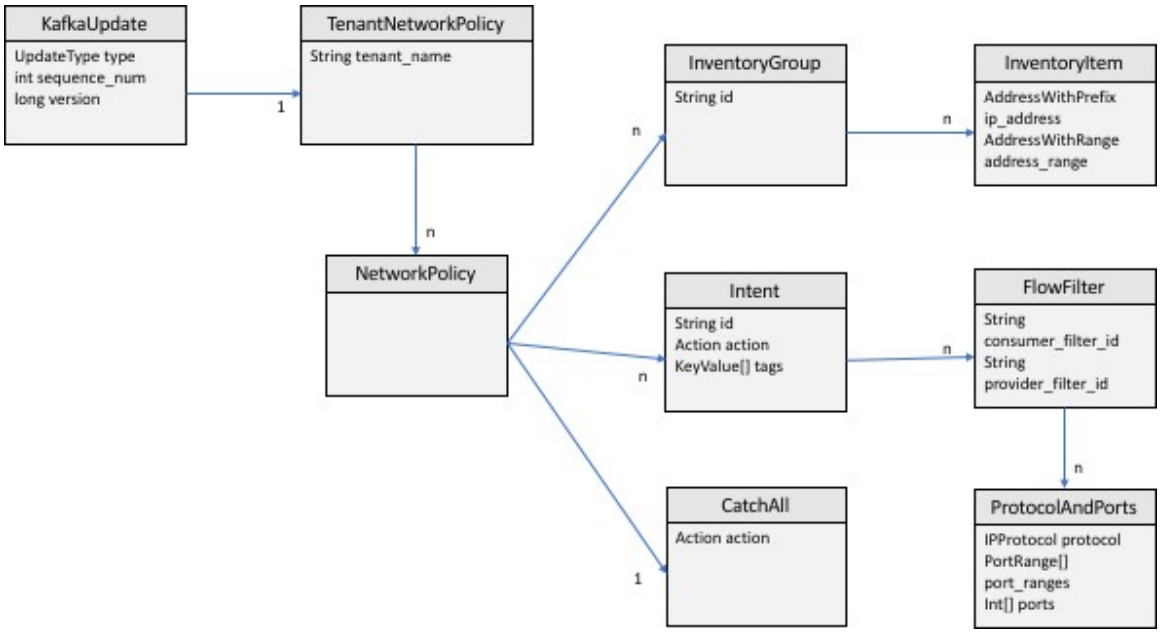
Secure Workload バックエンドによって Kafka に公開されるネットワークポリシーは、Google Protocol Buffers 形式でエンコードされます。Linux システムにダウンロードしてインストールする方法については、こちらのガイドを参照してください。

Secure Workload ネットワークポリシーの proto ファイルは、こちらからダウンロードできます。

Secure Workload ネットワークポリシーのデータモデル

下の図は、Kafka に接続されている Secure Workload エンティティの簡略化された UML ダイアグラムを示しています。

図 *83 : Secure Workload* ネットワークポリシーのデータモデル



protobuf でモデル化された Secure Workload ネットワークポリシーは、InventoryGroups のリスト、Intents のリスト、および CatchAll ポリシーで構成されます。各ポリシーには、1 つのルート範囲に属するすべての項目が含まれています。InventoryGroup には、単一のネットワーク ドレス、サブネット、またはアドレス範囲など、ネットワークアドレスを指定することによってサーバーやアプライアンスなどの Secure Workload エンティティを表す InventoryItems のリストが含まれます。Intent は、ネットワークフローが特定のコンシューマの InventoryGroup、プロバイダーの InventoryGroup、およびネットワークプロトコルとポートと一致するときに実行されるアクション（許可または拒否）を記述します。CatchAll は、Secure Workload 内部のルート範囲に対して定義されたキャッチオールアクションを表します。適用が有効になっているワークスペースがルート範囲に存在しない場合、デフォルトポリシーである ALLOW が生成されたポリシーに書き込まれます。

ユーザーまたはインベントリグループの変更によって適用がトリガーされると、Secure Workload バックエンドは、定義されたネットワークポリシーの完全なスナップショットを、KafkaUpdates として表される一連のメッセージとして Kafka に送信します。これらのメッセージを完全なスナップショットに再構築する方法と、エラー状態を処理する方法の詳細については、tetration_network_policy.proto ファイル内の KafkaUpdate のコメントを参照してください。

KafkaUpdate メッセージのサイズが 10MB を超える場合、Secure Workload バックエンドはこのメッセージをそれぞれのサイズが 10MB の複数のフラグメントに分割します。複数のフラグメントでは、最初のフラグメントのみに TenantNetworkPolicy の ScopeInfo フィールドがあります。ScopeInfo は、KafkaUpdate メッセージの残りのフラグメントで nil に設定されます。

Secure Workload ネットワーク ポリシー クライアントのリファレンス実装

リファレンス実装とデモクライアントをコンパイルして実行する方法については、Java でのこの tnp-enforcement-client を参照してください。

この実装により、Kafka のみを介して Secure Workload ポリシーストリームからネットワークポリシーを読み取るための共通コードが提供されます。実際のポリシーをネットワークデバイスにプログラムするベンダー固有のコードは、必要なインターフェイス PolicyEnforcementClient を実装することでプラグインできます。

カンバセーション

カンバセーションとは、特定のポートの 1 つのホストによって提供され、別のホストによって消費されるサービスとして定義されます。このようなカンバセーションは、異なるタイミングの多数のフローから出現します。自動ポリシー検出は、そのようなすべてのフローを取得し、一時/エフェメラルポートを無視し、それらを重複排除してカンバセーショングラフを生成します。サーバー（プロバイダー）ポート N でのホスト A とホスト B の間の特定のカンバセーションでは、自動ポリシー検出が実行された時間枠内で、ポート N での A から B へのフローが少なくとも 1 回観測されています。

フローデータを使用すると、自動ポリシー検出中に生成されたクラスタを評価しながら、どのフローがどのプロセスに関連付けられているかをより深く理解できるようになります。

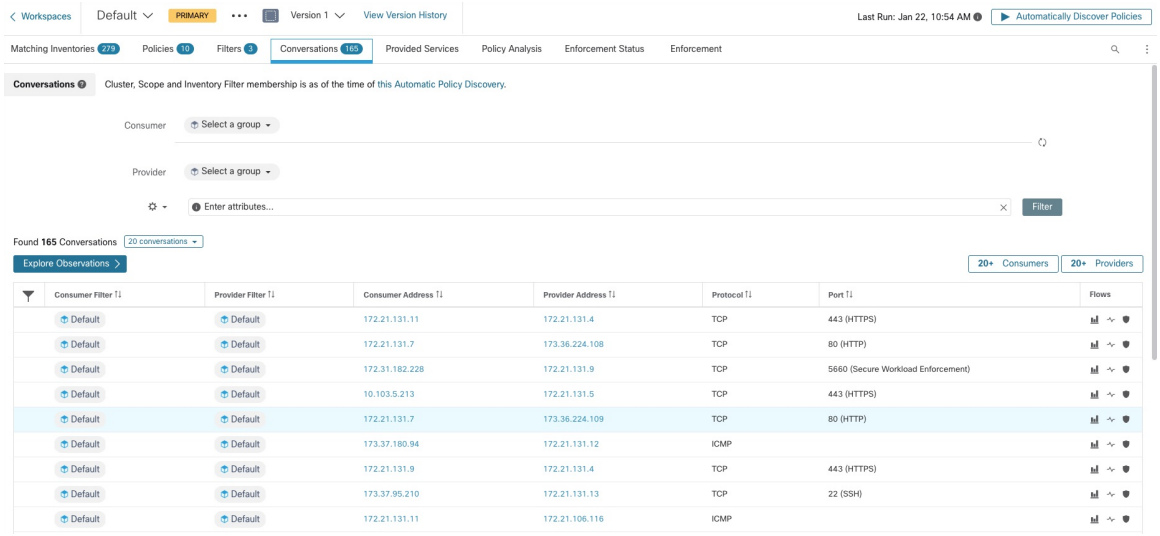
さらに、エージェントによって収集された情報は、未使用の L4 ポートを可視化します。未使用のポートとは、自動ポリシー検出に選択された間隔にわたり通信が確認されなかったポートです。この情報を使用して、これらのポートでの通信に関するポリシーを開いたり、未使用のポートにバインドされているアプリケーションを閉じたりして、ワークロードの攻撃対象領域を減らすことができます。

クライアント/サーバーの分類は、自動ポリシー検出のカンバセーションビューに影響することに注意してください。これは、アグリゲーションでどのポートがドロップされる（エフェメラルと見なされる）かを示します。「クライアントサーバーの分類」を参照してください。

会話テーブルビュー

会話テーブルビューには、コンシューマポートが削除され、レコードが常に 1 つしかない自動ポリシー検出の期間からの集約されたフローを表示する簡単な方法が示されます。ポリシーはフィルタ間を移動し、会話は IP アドレス間を移動します。

図 *84 :* 会話テーブルビュー

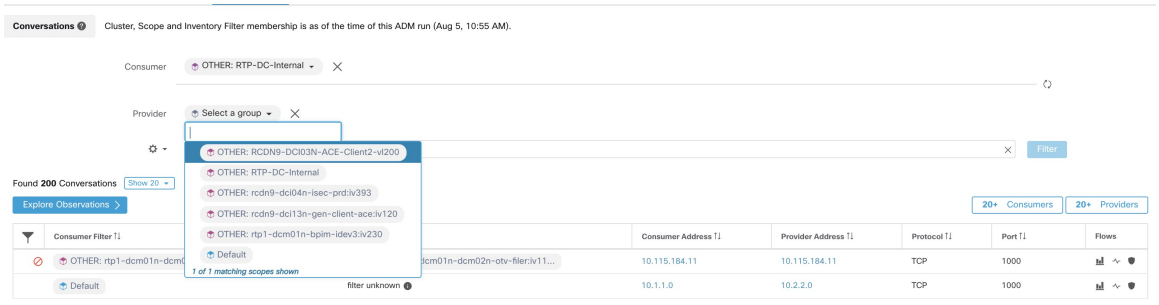


コンシューマまたはプロバイダーの選択

コンシューマとプロバイダーは、下の例に示すように、インベントリフィルタ、範囲、およびクラスタを選択できる、先行入力ドロップダウンセレクタによって選択できます。選択したコンシューマとプロバイダー間のすべてのカンバセーションが表示されます。注：既存のフィルタを削除するには、「x」アイコンをクリックします（フィルタを削除しても機能しない場合があります）。

デフォルトでは、コンシューマとプロバイダーは、自動ポリシー検出中に、IPアドレスがメンバーになっているすべてのインベントリフィルタと照合されます。たとえば、「ルート範囲」を検索すると（一部の IP はより具体的な範囲に一致する可能性がありますが）、すべてのカンバセーションに一致します。より具体的な一致を実行するには、ファセットフィルタ入力の左側にある設定ドロップダウンから[範囲フィルタ処理をIPのベストマッチに制限する（Restrict scope filtering to an IP's best match）] を選択します。

図 *85 :* コンシューマまたはプロバイダーの選択



カンバセーションフィルタ

図 *86* : カンバセーションフィルタ

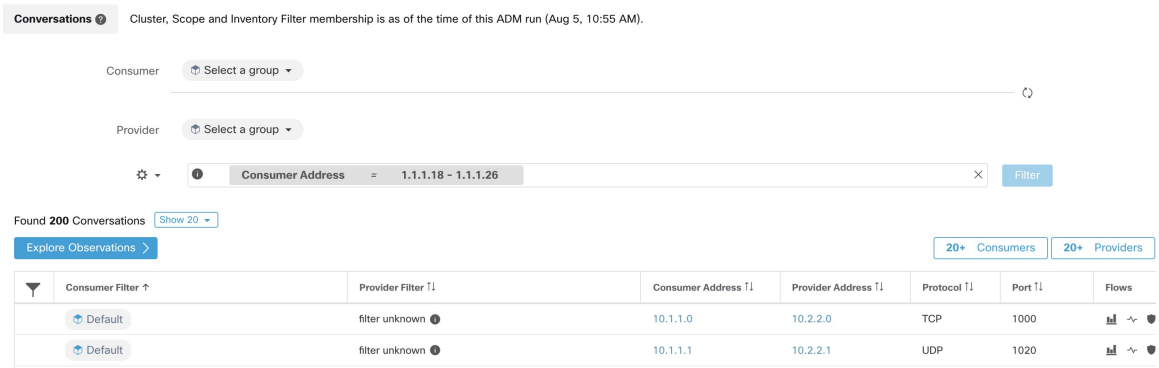
ここで、検索結果を絞り込むためのフィルタを定義します。[フィルタ（Filters）] という文字の横にある [?] アイコンをクリックすると、ディメンションの候補がすべて表示されます。ユーザーラベルデータについては、これらの列も適切な間隔で使用できます。この入力では、キーワード and、or、not、括弧もサポートされており、これらを使用してより複雑なフィルタ条件を表現できます。たとえば、IP 1.1.1.1 と 2.2.2.2 間の方向に依存しないフィルタは次のように記述できます。

Consumer Address = 1.1.1.1 and Provider Address = 2.2.2.2 or Consumer Address = 2.2.2.2 and Provider Address = 1.1.1.1 And to additionally filter on Protocol = TCP:

(Consumer Address = 1.1.1.1 and Provider Address = 2.2.2.2 or Consumer Address = 2.2.2.2 and Provider Address = 1.1.1.1) and Protocol = TCP

フィルタ入力機能は、「-」を範囲クエリに変換することで、ポート、コンシューマアドレス、プロバイダーアドレスの「,」と「-」もサポートします。以下に有効なフィルタの例を示します。

図 *87* : コンシューマアドレスの範囲クエリをサポートするフィルタ入力機能



使用可能なフィルタ：

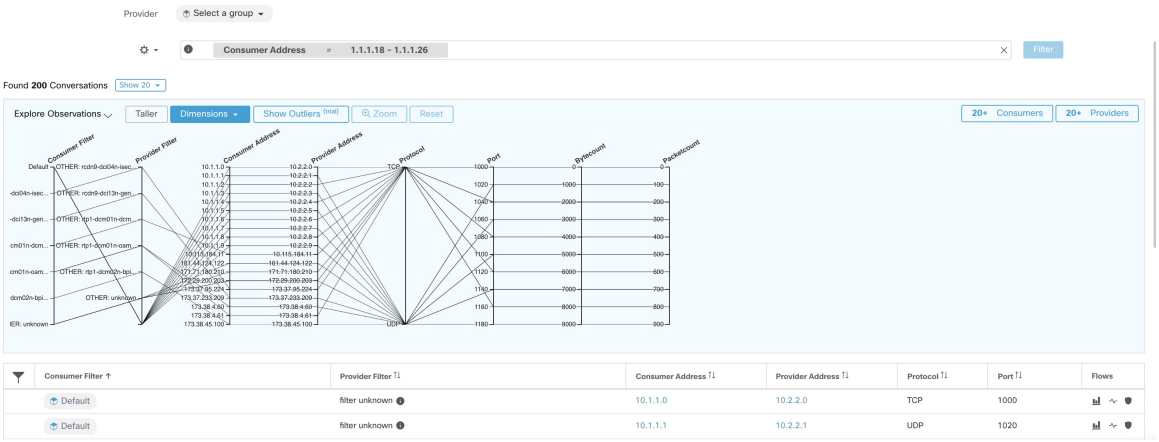
フィルタ	説明
コンシューマアドレス（Consumer Address）	CIDR 表記を使用してサブネットまたは IP アドレスを入力します（例：10.11.12.0/24）。コンシューマアドレスが入力した IP アドレスやサブネットと一致するフロー観測データを照合します。

フィルタ	説明
プロバイダーアドレス（**Provider Address**）	CIDR 表記を使用してサブネットまたは IP アドレスを入力します（例：10.11.12.0/24）。プロバイダーアドレスが入力した IP アドレスやサブネットと一致するフロー観測データを照合します。
ポート（**Port**）	ポートが入力したポートと一致する通信フローを照合します。
プロトコル（**Protocol**）	プロトコルタイプ（TCP、UDP、ICMP）を指定して通信フローの観測データをフィルタリングします。
アドレス タイプ（**Address Type**）	アドレス タイプ（IPv4、IPv6、DHCPv4）を指定して対話フローの観測データをフィルタリングします。
信頼性（**Confidence**）	フローの方向の信頼性を示します。入力可能値：[高い（High）]、[非常に高い（Very High）]、[中程度（Moderate）]。
除外対象?（**Excluded?**）	除外フィルタまたは承認済みポリシーを指定して除外対象の対話データを照合します。
除外基準（**Excluded By**）	特定のフィルタを指定して除外対象の対話データを照合します。入力可能値：[除外フィルタ（Exclustion Filter）]、[ポリシー（Policy）]。

観察結果の参照

[観察結果の参照（Explore Observations）] ボタンをクリックすると、チャートビューが有効になり、[平行座標（Parallel Coordinates）] チャートを介して高次元データをすばやく探索できます。最初は少し難しいかもしれませんが、関心のある次元のみを有効にする場合（[次元（Dimensions）] ドロップダウンの項目のチェックを外す)や、次元の順序を並べ替える場合、このチャートは非常に便利です。このチャートの 1 本の線は 1 つの観察値を表し、その線がさまざまな軸と交差する場所は、その次元での観察値を示しています。観察値は、チャートの下の観察リストにカーソルを合わせ、チャート内で観察を表す強調表示された線を見ると、より明確になります。

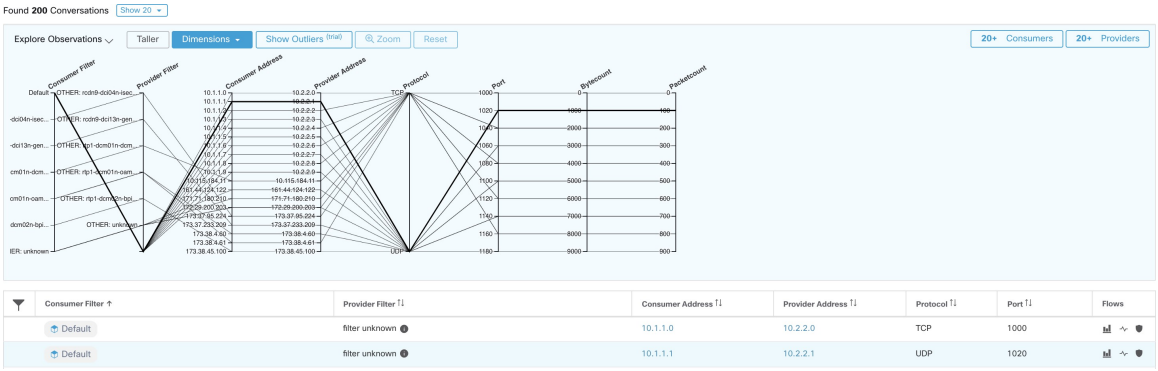
図 *88 :* 観察結果の参照



ホバーによるカンバセーション観測

カンバセーションデータの高次元の性質により、このチャートはデフォルトではかなり幅が広く、チャート全体を表示するには右にスクロールする必要があります。このため、関心のある次元以外はすべて無効にすると便利です。[カンバセーションの詳細確認（Explore Conversations）] のホバー状態は、各カンバセーションをテーブルリストビューにマッピング（ホバー）するために提供されます。

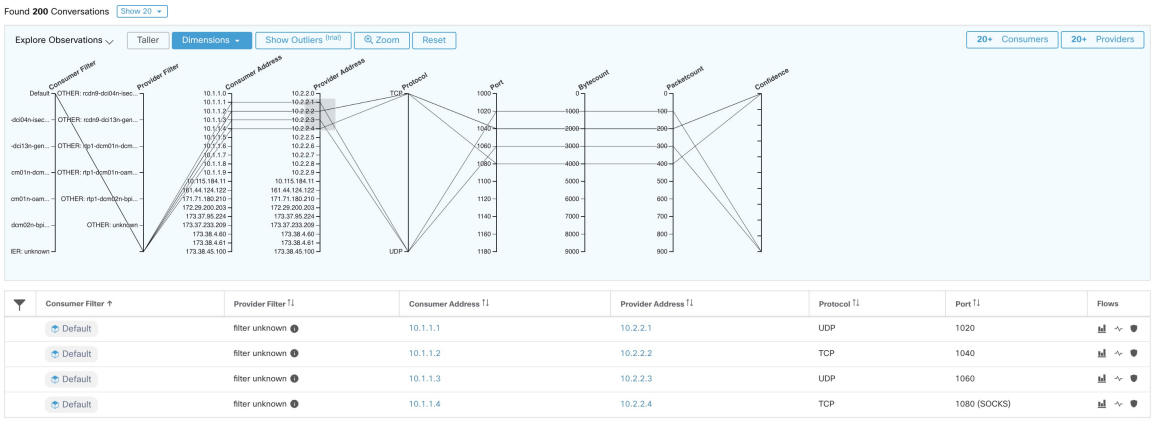
図 *89 :* ホバーによるカンバセーション観測



Filtering

いずれかの軸に沿ってカーソルをドラッグすると、選択範囲に一致する監視データのみを表示する選択範囲が作成されます。軸を再度クリックすると、いつでも選択範囲を削除できます。一度に任意の数の軸を選択できます。監視データのリストが更新され、選択した会話のみが表示されます。

図 *90 : Filtering*

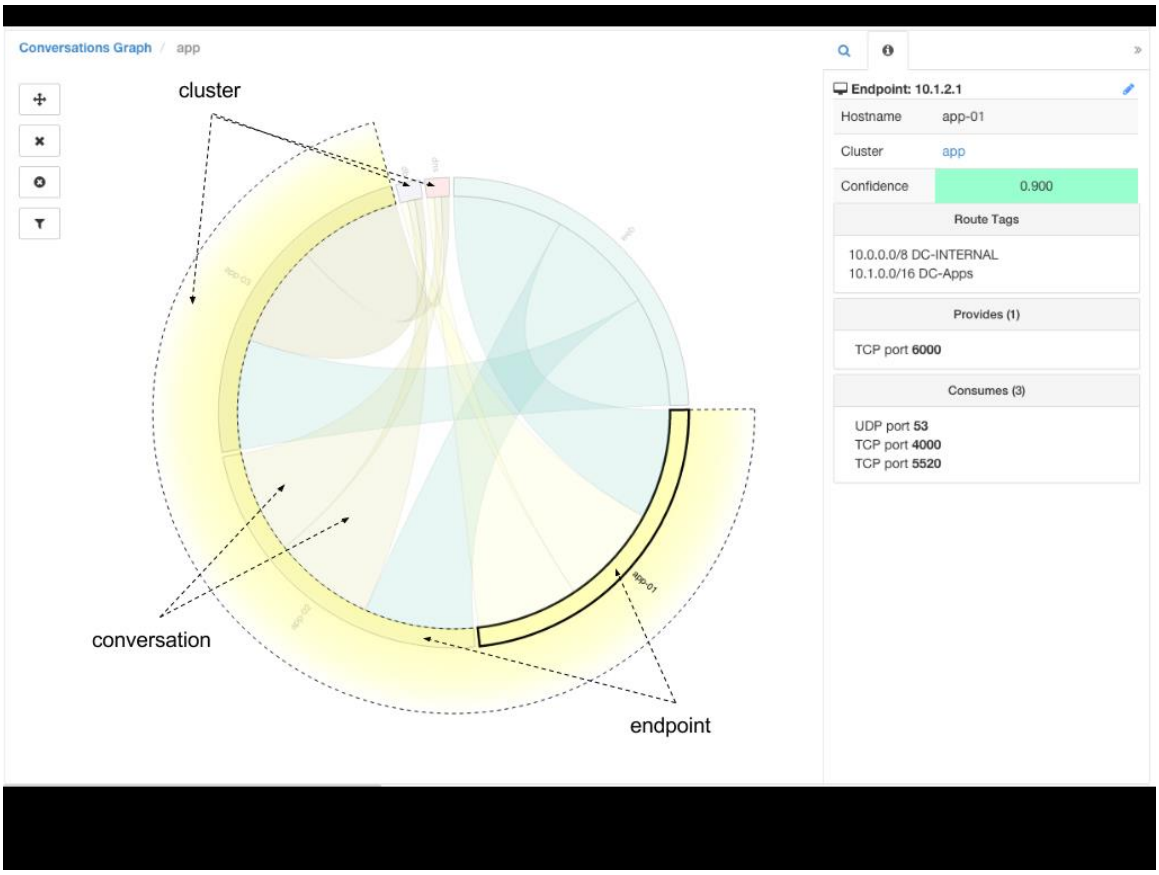


会話チャートビュー

会話チャートビューは、パーティション/クラスタ/ポリシーの代わりにクラスタ/ワークロード/会話に焦点を当てていることを除いて、[ポリシービュー（Policy View）] ページと非常に似たルックアンドフィールを備えています。下の図に示すように、上位レベルの外側の弧はクラスタを表し、展開してメンバーのホスト/ワークロードを内側の弧として表示できます。コードは会話や接続を表します。

会話ビューのコントロールとサイドパネルは、ポリシービューと同様に動作しますが、サイドパネルの情報には、使用または提供されたサービスなどの選択したワークロードに関する詳細情報、および親クラスタへのリンクとプロセス情報（可能な場合）も表示される点が異なります。

図 *91* : 会話チャートビュー



カンバセーションにおける上位のコンシューマとプロバイダー

選択したフィルタを反映したカンバセーションに基づく上位のコンシューマまたはプロバイダーの数は、カンバセーションテーブルの上部にある2つのボタンから確認できます。それぞれのボタンをクリックすると、カンバセーション数の列と、各コンシューマおよびプロバイダーのアドレス、ホスト名、およびその他のユーザー注釈の列を含む表を含むダイアログが表示されます。

図 *92* : カンバセーションテーブルの上部

図 *93 :* 上位のコンシューマモーダル

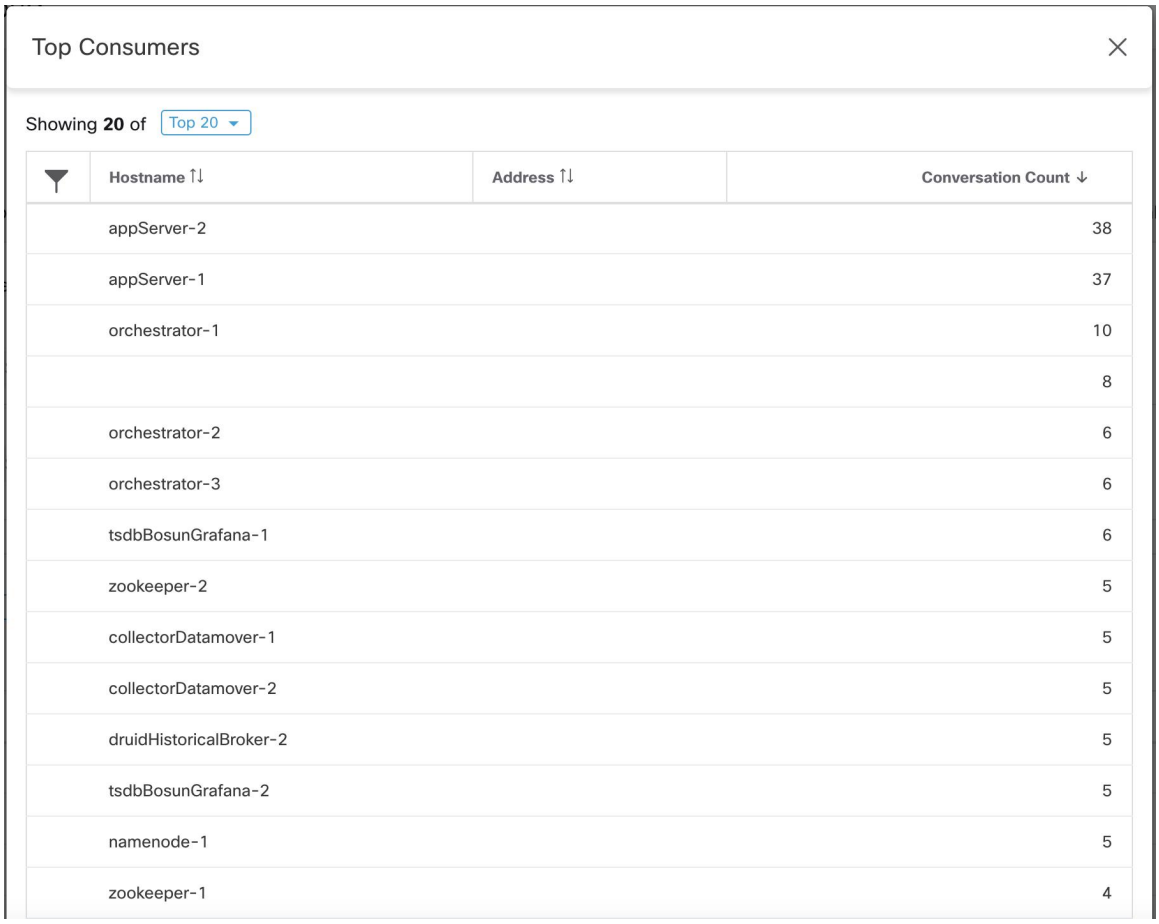
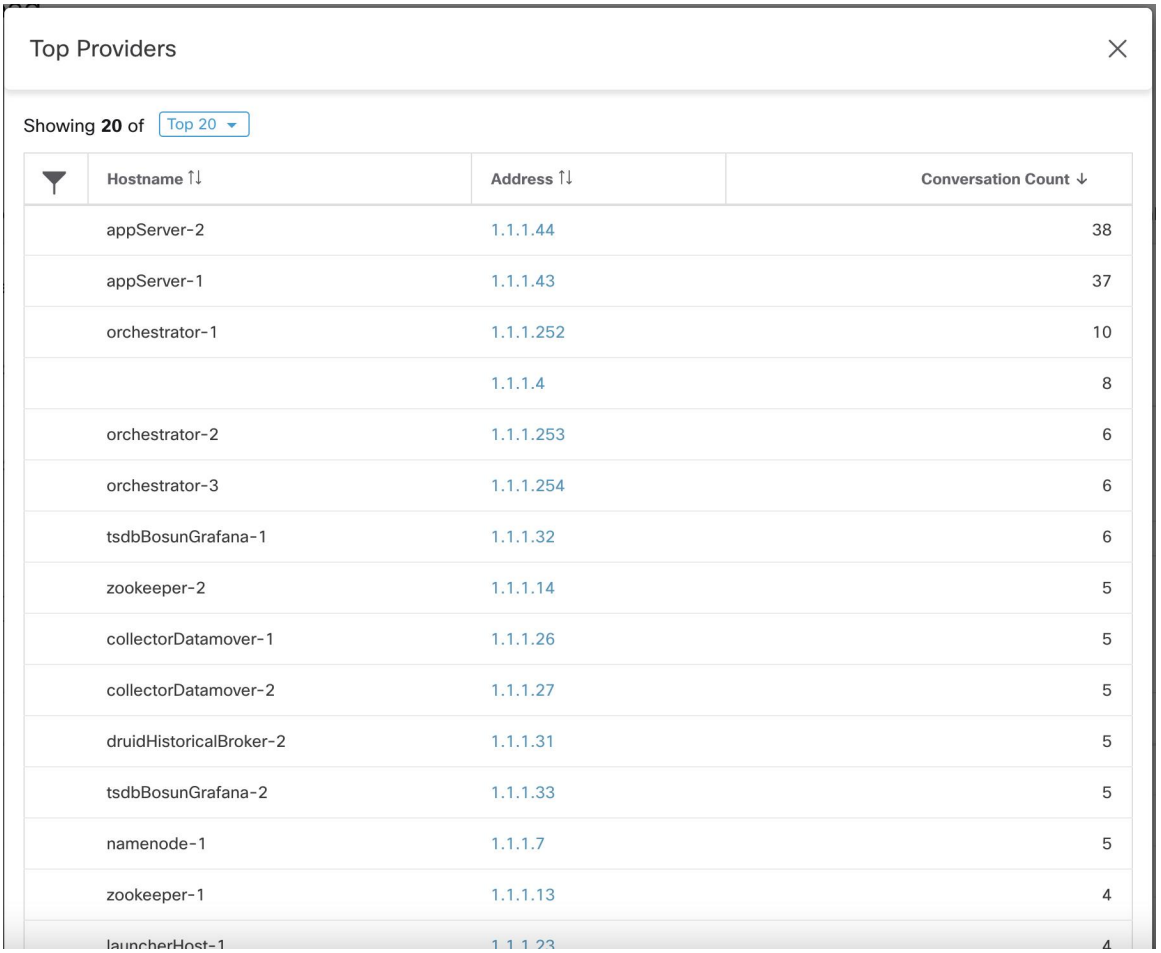


図 *94* : 上位のプロバイダーモーダル



ポリシーテンプレート

ポリシーテンプレートを使用して、同様のポリシーセットを複数のワークスペースに適用できます。これらは、ワークスペースのエクスポートのスキーマと同様の JSON スキーマを使用して定義されます。ワークスペースでポリシーを作成し、JSON としてエクスポートし、JSON を変更してから、ポリシーテンプレートとしてインポートできます。

ポリシーテンプレートには、ルート範囲の範囲所有者機能が必要です。

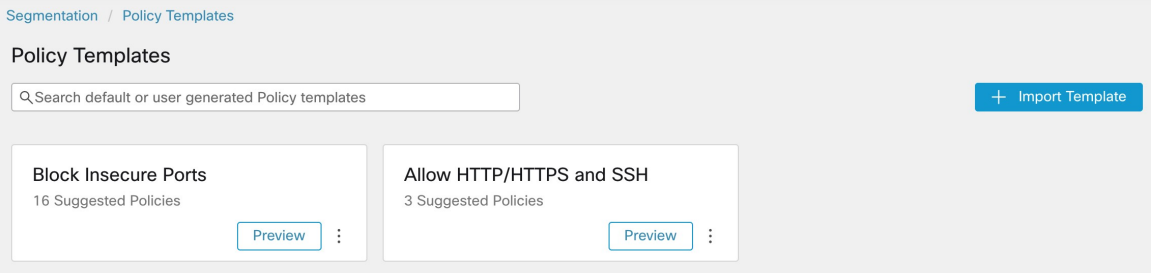
テンプレートインポート

ポリシーテンプレートは、メインの [セグメンテーション（Segmentation）] ページからアクセスできる [ポリシーテンプレート（Policy Templates）] ページに表示されます。この場所で [テンプレートのインポート（Import Template）] ボタンを使用してテンプレートをインポート/アップロードできます。

テンプレートは、アップロード時に正確性が検証されます。問題をデバッグするのに役立つエラーのリストが表示されます。

テンプレートがアップロードされると、テンプレートの適用、ダウンロード、または名前と説明の更新を行うことができます。

図 *95*：利用可能なテンプレートの表示



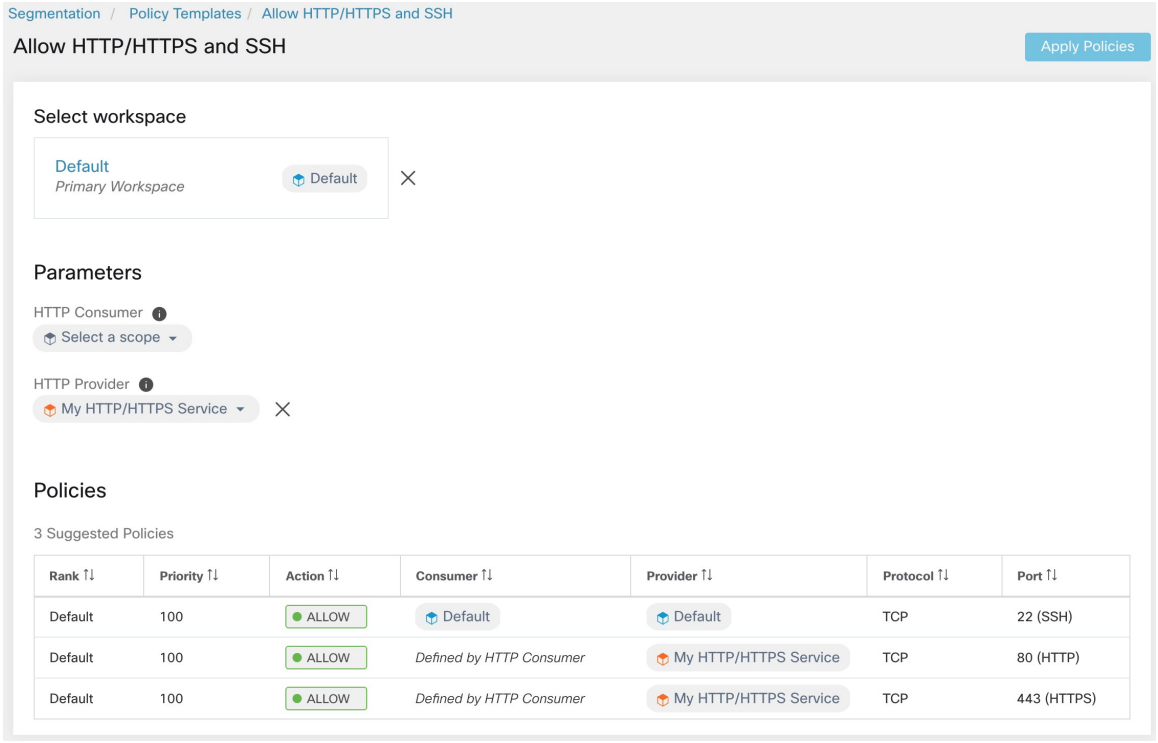
テンプレートの適用

テンプレートをワークスペースに適用するには、いくつかの手順を実行します。

1. プレビューするテンプレートを選択します。
2. テンプレートを適用するワークスペースを選択します。
3. 必要に応じてパラメータを入力します。
4. ポリシーを確認します。
5. ポリシーを適用します。

ポリシーは、選択したワークスペースの最新バージョンに追加されます。テンプレートを介して作成されたポリシーは、`From Template? = true` フィルタを使用してフィルタリングできます。

図 *96* : ポリシーテンプレートの適用



ポリシーテンプレートの JSON スキーマ

ポリシーテンプレート JSON スキーマは、ワークスペースのエクスポートのスキーマを模倣するように設計されています。ワークスペースで一連のポリシーを作成し、それを JSON としてエクスポートし、JSON を変更してから、ポリシーテンプレートとしてインポートできます。

属性	タイプ	説明
name	string	（オプション）インポート時にテンプレートの名前として使用されます。
説明	string	（オプション）適用プロセス中に表示されるテンプレートの説明。
パラメータ	パラメータオブジェクト	テンプレートパラメータ、下記を参照。
absolute_policies	ポリシーオブジェクトの配列	（オプション）絶対ポリシーの配列。

属性	タイプ	説明
default_policies	ポリシーオブジェクトの配列	（必須）デフォルトポリシーの配列、空にすることが可能。

パラメータオブジェクト

パラメータオブジェクトはオプションですが、テンプレートのパラメータとしてフィルタを動的に定義するために使用できます。パラメータは、`consumer_filter_ref` または `provider_filter_ref` ポリシー属性を使用して参照されます。

パラメータオブジェクトのキーは参照名です。値は、必須の `"type": "Filter"` とオプションの説明を含むオブジェクトです。パラメータオブジェクトの例を以下に示します。

```
{
"parameters": {
"HTTP Consumer": {
"type": "Filter",
"description": "Consumer of the HTTP and HTTPS service"
},
"HTTP Provider": {
"type": "Filter",
"description": "Provider of the HTTP and HTTPS service"
}
}
}
```

パラメータは、ポリシーオブジェクトで参照できます（例：`"consumer_filter_ref": "HTTP Consumer"` または `"provider_filter_ref": "HTTP Provider"`）。

特殊なパラメータ参照

いくつかの特殊な参照は、自動的にフィルタにマッピングされます。パラメータとして定義する必要はありません。

Ref	説明
_workspaceScope	テンプレートが適用されているワークスペースの範囲に解決されます。
_rootScope	ルート/トップレベルの範囲に解決されます。

ポリシー オブジェクト

ワークスペースエクスポート JSON との互換性を維持するため、ポリシーオブジェクトには、コンシューマとプロバイダーの複数のキーが含まれています。それらは次のように解決されます。

```
            if *_filter_ref is defined
  use the filter resolved by that parameter
else if *_filter_id is defined
  use the filter referenced by that id
```

```
else if *_filter_name is defined
  use the filter that has that name
else
  use the workspace scope.
```

上で定義したようにフィルタを解決できない場合、適用時とアップロード時の両方でエラーが返されます。

属性	タイプ	説明
action	string	（オプション）ポリシーのアクション、ALLOW または DENY（デフォルトは ALLOW）。
priority	integer	（オプション）ポリシーの優先順位（デフォルトは100）。
consumer_filter_ref	string	パラメータへの参照。
consumer_filter_name	string	名前によるフィルタへの参照。
consumer_filter_id	string	定義された範囲またはインベントリフィルタの ID。
provider_filter_ref	string	パラメータへの参照。
provider_filter_name	string	名前によるフィルタへの参照。
provider_filter_id	string	定義された範囲またはインベントリフィルタの ID。
l4_params	l4params の配列	許可されたポートとプロトコルのリスト。
属性	タイプ	説明
proto	整数	プロトコル整数値（NULL はすべてのプロトコルを意味します）。
port	integer	ポートの包含範囲。[80, 80] または [5000, 6000] など（NULL はすべてのポートを意味します）。

L4param オブジェクト

属性	タイプ	説明
proto	整数	プロトコル整数値（NULL はすべてのプロトコルを意味します）。
port	integer	ポートの包含範囲。[80, 80] または [5000, 6000] など（NULL はすべてのポートを意味します）。

テンプレートのサンプル

```
{
"name": "Allow HTTP/HTTPS and SSH",
"parameters": {
"HTTP Consumer": {
"type": "Filter",
"description": "Consumer of the HTTP and HTTPS service"
},
"HTTP Provider": {
"type": "Filter",
"description": "Provider of the HTTP and HTTPS service"
}
},
"default_policies": [
{
"action": "ALLOW",
"priority": 100,
"consumer_filter_ref": "__rootScope",
"provider_filter_ref": "__workspaceScope",
"l4_params": [
{ "proto": 6, "port": [22, 22] },
]
},
{
"action": "ALLOW",
"priority": 100,
"consumer_filter_ref": "HTTP Consumer",
"provider_filter_ref": "HTTP Provider",
"l4_params": [
{ "proto": 6, "port": [80, 80] },
{ "proto": 6, "port": [443, 443] }
]
}
]
}
```

その他の関数

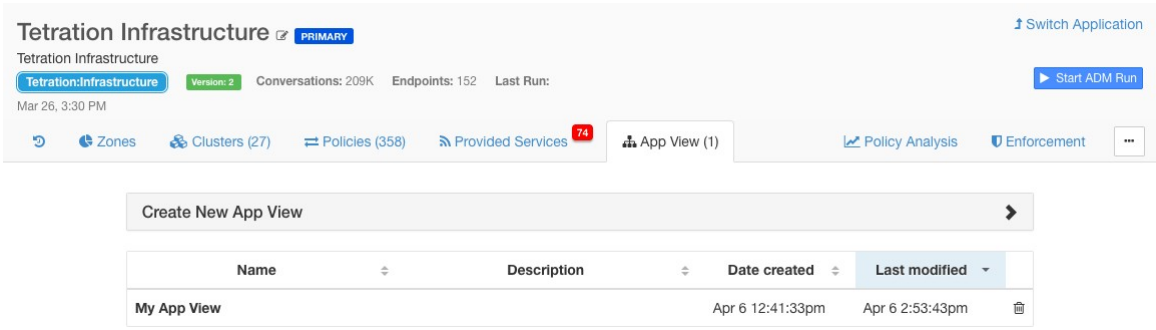
アプリケーションビュー

（注） アプリビューは廃止され、次の Cisco Secure Workload リリースで削除されます。

アプリケーションビューは、自動ポリシー検出で中心的な役割を果たし、ネットワークチームとアプリケーションチームの間のギャップを埋めるのに役立ちます。言い換えれば、アプリケーションビューは、Web アプリケーションのような多層データセンター アプリケーションについての情報を把握することを目的として、ボトムアップ方式で自動ポリシー検出の結果を調査することを可能にします。データセンターでは、何千ものそのようなアプリケーションが実行されているかもしれません。アプリケーションビューは、ユーザーが特定のビューに焦点を合わせ、他のユーザーとビューを共有するのに役立ちます。

自動ポリシー検出ワークフローと同様に、アプリケーション リスト ビューは、表形式のビューをクリックして、新しいアプリケーションビューを作成し、既存のビューを表示することを可能にします。

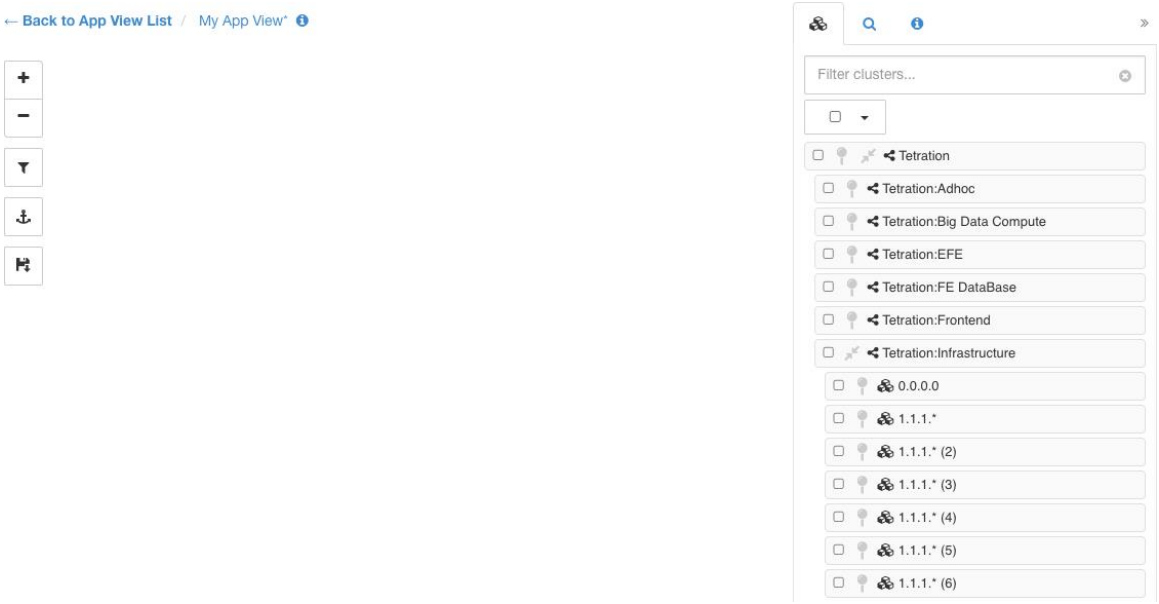
図 *97* : アプリビューリスト



アプリケーションビューのレイアウト構築

新しいアプリケーションビューを作成すると、ノード（クラスタ、ユーザー定義フィルタ、および範囲）のリストを含む空のキャンバスが表示されます。ユーザーは、特定のノードをキャンバスに [ピン（pin）] 留めして、ネットワーク ポリシーの意味で隣接ノードの探索開始を選択できます。このページの右側のパネルには、すべてのノードのリストを含む追加のタブが表示されていることに注意してください。

図 *98 :* アプリケーションビューの空のキャンバス



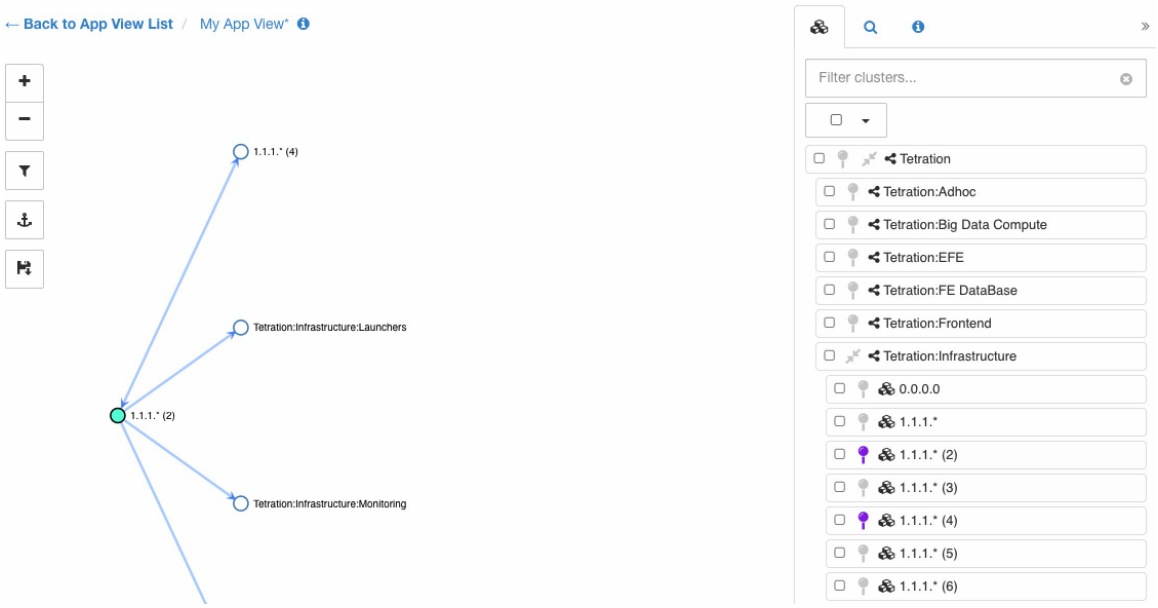
左側のツールは、次の機能を提供します。

- [拡大（Zoom in）]
- [縮小（Zoom out）]
- 表示可能なポリシーのフィルタ処理
- 選択したノード位置の固定
- アプリケーションビューの状態の保存、ノード/ポリシーデータのコピーまたはエクスポート

アプリケーションビューへのノードの追加

各項目の横にある**ピン**ボタンをクリックしてそのノードをキャンバスに追加し、キャンバス上の任意のノードをダブルクリックしてその隣接ノードを**表示**または**非表示**にします。

図 *99* : アプリケーションビューのピン留めとノードの展開



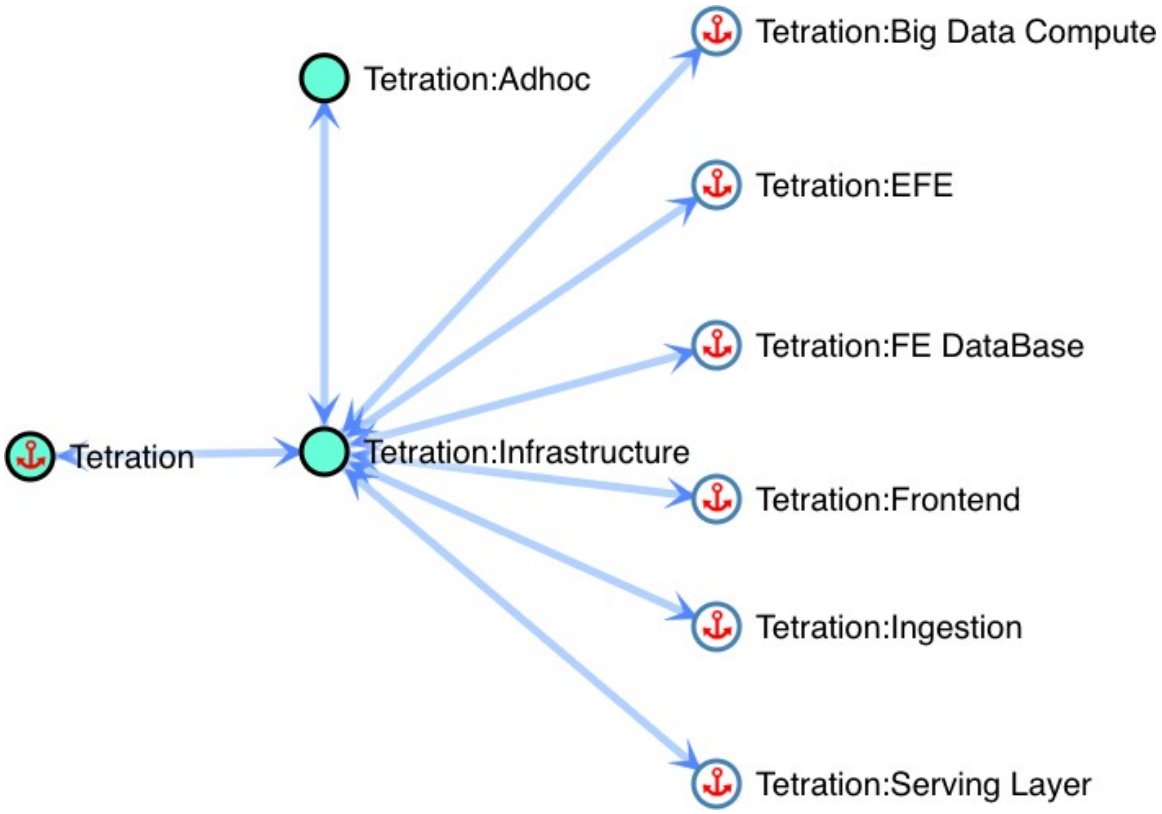
アプリケーションビューのレイアウト調整

（注） 2 つのノード間のエッジは、一連のノード間のネットワークポリシーを表します。ノード間の 1 つ以上のカンバセーションがロードバランサを通過している場合（高度な自動ポリシー検出設定でアップロードされる参考情報の一部として定義されます）、ロードバランサアイコンがエッジ上に表示されます。表示された要素にカーソルを合わせるかクリックすると、詳細情報が表示されます。

ノードを任意の位置に移動して、目的のレイアウトを実現できます。その場合、ユーザーの選択が尊重され、アンカーアイコンがノードに表示されます。[位置指定（anchored）] されたノードの位置をリセットするには、ツールバーの [アンカー（anchor）] ボタンをクリックします。

次の図は、サンプルの多階層アプリケーションの、完全に展開されたグラフを示しています。

図 *100 :* アンカーノードを使用したアプリケーションビューのレイアウト



多層アプリケーションの例

ツールバーの保存ボタンをクリックして、現在のレイアウトを保存します。これにより、他のユーザーは、この特定のワークスペースをまったく同じレイアウトで表示できます。

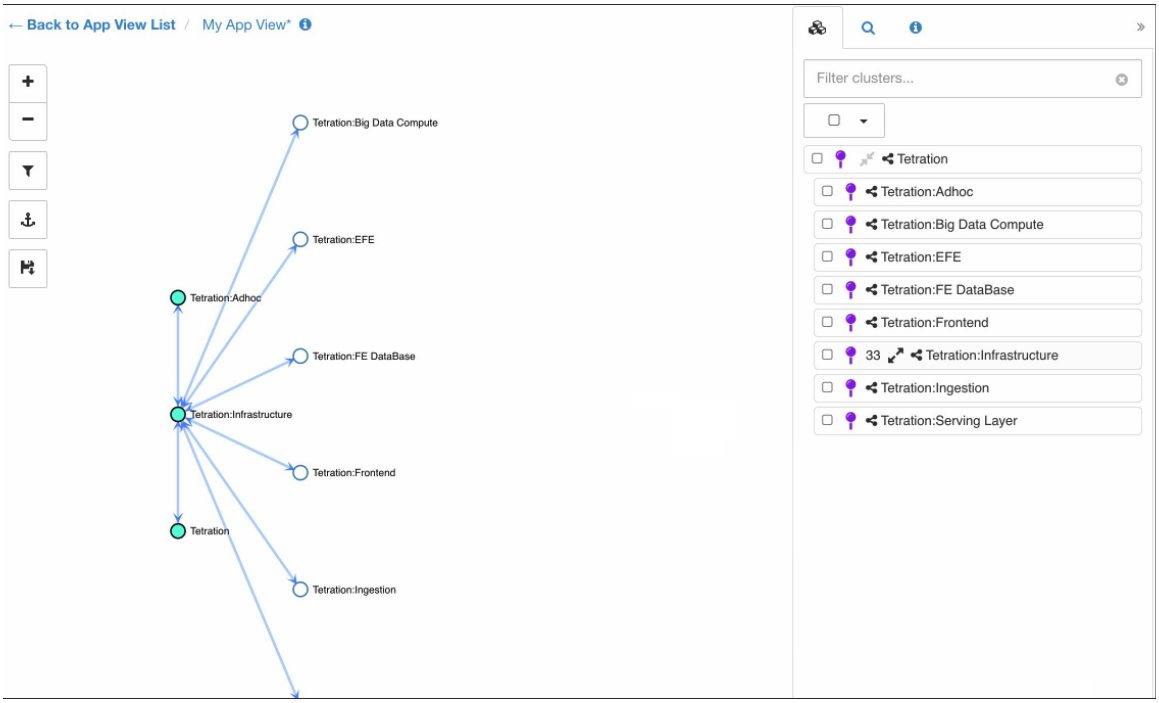
（注） Shift キーを押しながら選択したノードのいずれかをドラッグすると、選択した複数のノードを一度に移動できます。

範囲の展開と折りたたみ

アプリケーション内の二重矢印アイコンを使用して、範囲を [展開（Expand）] にするか、[折りたたみ（collapse）] にします。折りたたむと、すべての子孫ノードとそのポリシーが折りたたまれた範囲にロールアップされます。折りたたむことにより、2 つのノードを直接接続するポリシーがなくても、折りたたまれた範囲の子の 1 つがそのノードに対するポリシーを持っているため、折りたたまれた範囲と他のノードの間にエッジが作成される可能性があります。ロールアップされたエッジは、集約されたポートリストとともにアプリケーションビューのエクスポートに反映されます。

新しいアプリケーションビューでは、すべての範囲がデフォルトで展開されます。

図 *101* : アプリケーションビューの折りたたまれた範囲



履歴と差分

履歴ビューには、多くのユーザーが共有および編集したワークスペースに適用された変更のタイムラインが表示されます。履歴ビューで強調表示されるイベントには、ワークロードとクラスタの追加、削除、名前変更、クラスタ間でのワークロードの移動、アプリケーションビューの作成と更新、参考情報のアップロード、自動ポリシー検出の送信と中止など、多くのイベントが含まれます。また、履歴ビューには、どのユーザーがどのような変更をワークスペースに加えたかが表示されます。

自動ポリシー検出ページ上部の対応するボタンをクリックすると、履歴ビューに移動できます（下の図を参照）。

履歴ビューは、[ワークスペースアクティビティログ（Workspace Activity Log）]、[バージョン（Versions）]、[ポリシーバージョン（Policy Versions）] の 3 つのセクションに分かれています。最初のセクションには、自動ポリシー検出イベントや適用イベントなど、ワークスペース全体に適用されるイベントが含まれています。後者の2つには、概要情報を含むバージョンのリストが表示されます。ユーザーは、リストからバージョンの履歴のより詳細なビューに移動できます。

自動ポリシー検出は、ワークスペースの新しい自動ポリシー検出バージョン（v*）を作成するため、結果が予期していなかったものだった場合、ユーザーは実行を元に戻すことができます。ポリシーを初めて自動検出すると、バージョン1が生成され、クラスタの（再実行ではない）編集や承認など、実行後のすべての変更もバージョン1にグループ化されます。以降、ポ

リシーを自動的に検出すると、新しいバージョンが生成されます（検出が失敗した場合を除く）。

ポリシーを分析するか、最新のポリシーを適用すると、新しい公開ポリシーバージョン（p*）が作成されます。これらのバージョンは編集できず、完全な削除のみを実行できます。

（注） 公開済み（p*）バージョンは、合計 100 までに制限されます。この制限に達した場合、UI または API を使用して古いバージョンを削除する必要があります。

バージョン間のクラスタリングの変更、および分析または適用されたポリシーを比較できます。「差分ビュー」を参照してください。バージョンのリストを表示しているときに [切り替え後のバージョン（Switch to Version）] をクリックすると、任意のバージョンに切り替えることができます。以下の例では、ワークスペースがバージョン 1 に切り替えられています。

（注） 古いバージョンのワークスペースに切り替えた後にポリシーを自動的に検出すると、以降のバージョンがすべて削除され、リニア履歴ビューが維持されます。同じ例で、バージョン 2 に切り替えた後にポリシーを自動的に検出すると、成功時にはバージョン 3 が削除されることになります。

履歴ビューでいずれかのイベントをクリックすると、そのイベントに関する詳細なコンテキスト情報がサイドペインに表示されます。

たとえば、自動ポリシー検出イベントをクリックすると、その自動ポリシー検出インスタンスのステータス、期間、および設定に関する多くの有用な情報が表示されます。さらに、サイドパネルには、実行による既存のクラスタとワークロードへの変更に関する概要レベルの統計が表示されます。詳細については「差分ビュー」で説明されています。

図 *102*：概要情報を含む生成されたポリシーバージョンのリスト

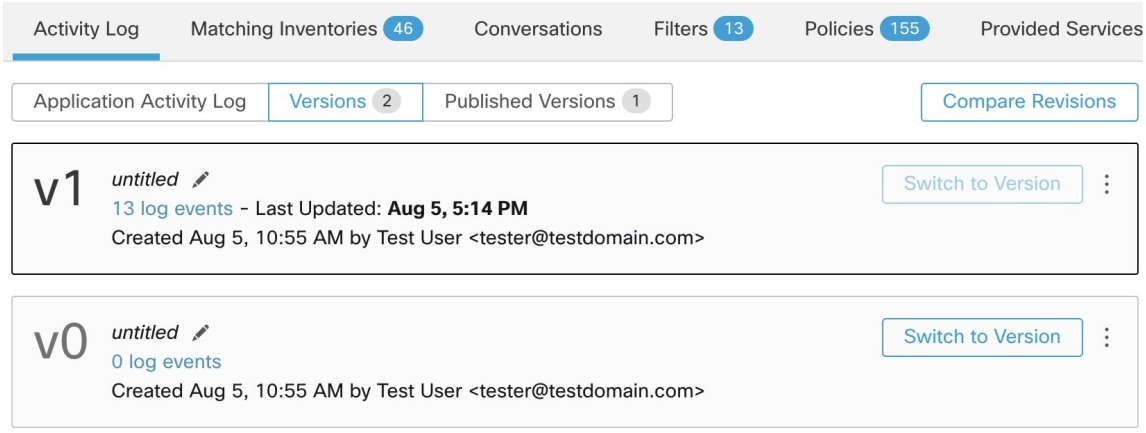
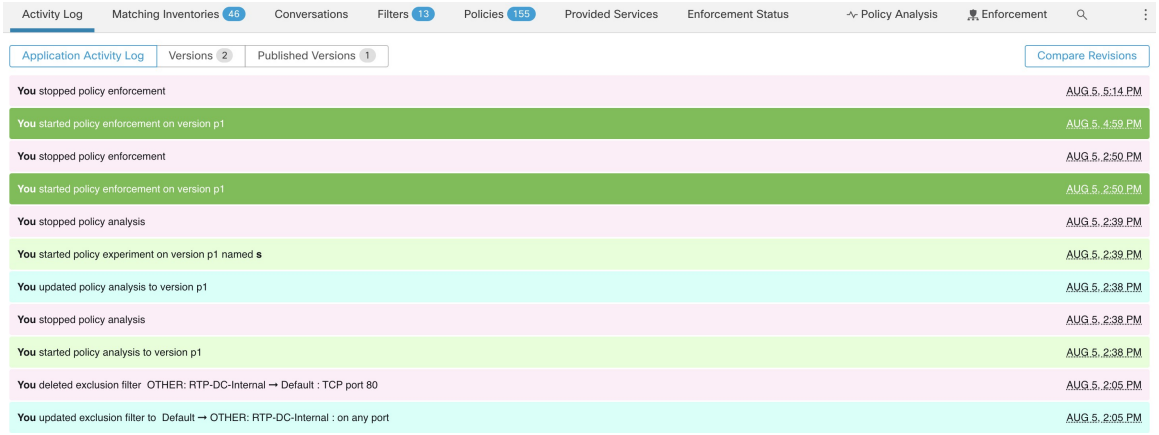
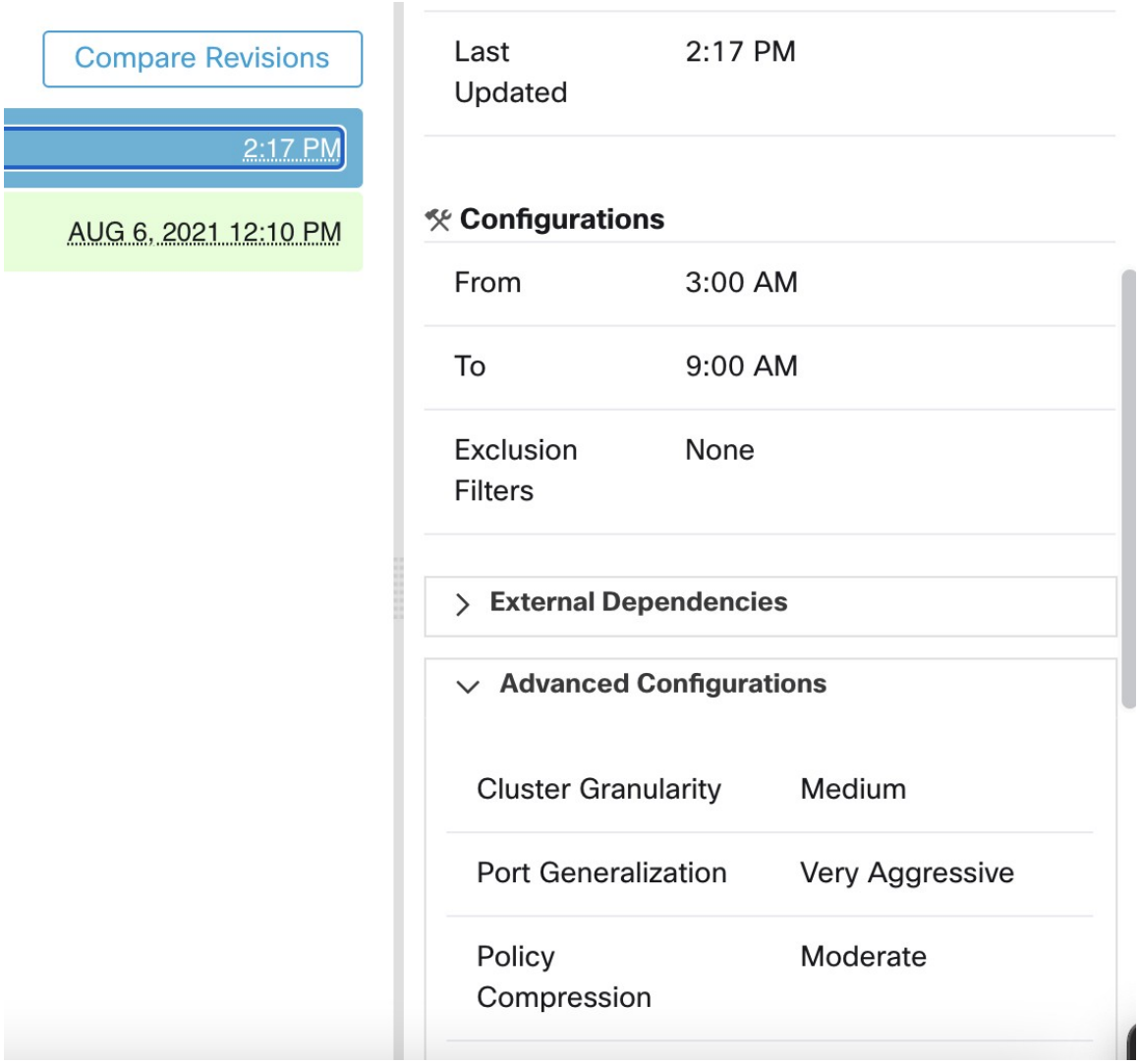


図 *103* : このワークスペースのバージョン *v1* に該当するイベントのログ



これらのイベントをクリックすると、除外フィルタ、外部依存関係、使用された高度な設定など、過去の自動ポリシー検出実行からの詳細情報が表示されます。

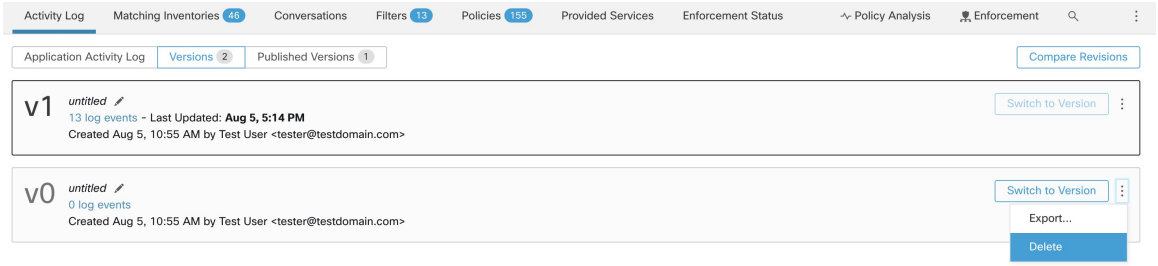
図 *104* : 特定の自動ポリシー検出の実行に使用される設定



ワークスペースバージョンの削除

自動ポリシー検出によって生成されたワークスペースバージョン（v*バージョン）は、それが最後に残っているバージョンでない限り、削除できます。公開されたポリシーバージョン（p*バージョン）は、バージョンがアクティブに分析または適用されていない限り、削除できます。

図 *105* : ワークスペースバージョンの削除



差分ビュー

自動検出されたポリシーのクラスタの差分ビューは、既存のクラスタとワークロードのメンバーシップに対する複数の自動ポリシー検出の実行における影響に関して、ユーザーがワークスペースの2つのバージョンを比較できるように設計されています。ポリシーの差分ビューもサポートされています。「ポリシーの差分」を参照してください。

クラスタの差分ビューには、3 つの方法で移動できます。

ステップ 1 ポリシーの自動検出に成功すると、実行の結果を示す差分ビューに移動するリンクとともに、成功を示すメッセージが表示されます。

図 *106* : 正常に実行された自動ポリシー検出

ステップ 2 ページの右上隅にある [リビジョンの比較（Compare Revisions）] ボタンをクリックして、履歴ビューから移動します。

ステップ 3 サイドパネルから移動します（サイドパネルの右上隅にあるボタンをクリックすると、自動ポリシー検出の実行のコンテキスト情報が表示される場合）。次の図を参照してください。

図 *107 :* コンテキスト情報の表示

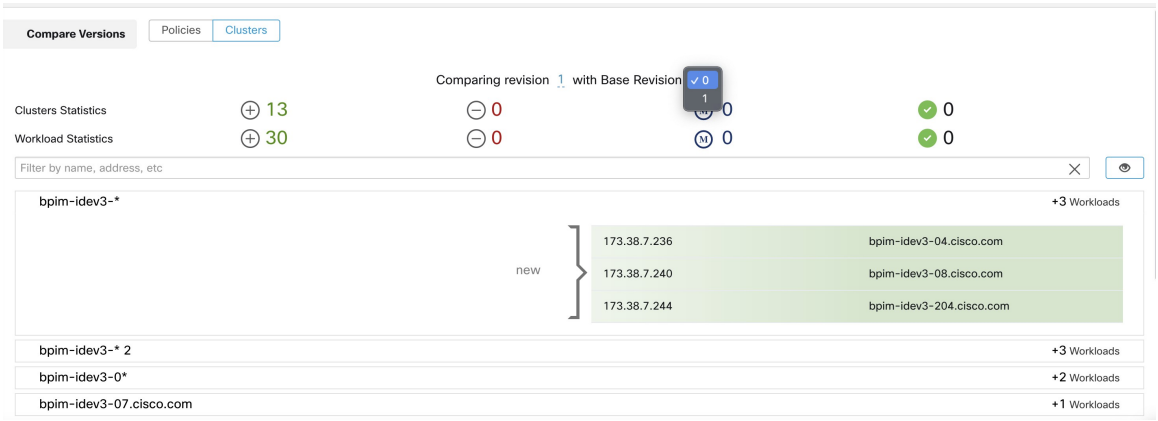
トップレベルでは、自動的に検出されたポリシーの差分ビューには、追加、削除、変更、および未変更のクラスタとワークロードの数を示す、クラスタとワークロードの変更に関する高レベルの統計が表示されます。

ビューの残りの部分は、追加、削除、変更、未変更の順序でクラスタのリストとして編成されています。それぞれ、クラスタに追加またはクラスタから削除されたワークロードの数だけでなく、ステータスを反映するように色分けされています。

特定のクラスタやワークロードは、名前またはIPアドレスで検索できます。クラスタを表す行のいずれかをクリックすると、その行が展開され、そのクラスタの内容がどのように変更されたかが示されます。

（注） デフォルトでは、未変更のクラスタはすべて非表示になっていますが、目のアイコンの付いたボタンをクリックすると表示できます。差分ビューを切り替えて他の 2 つのリビジョンを比較することは、リビジョン番号をクリックしてドロップダウンメニューから別のリビジョンを選択するのと同じくらい簡単です。

図 *108 :* クラスタの差分ビュー



ポリシーの差分

ポリシーの差分ビューは、クラスタの差分ビューと同様に選択できます。ベースバージョンと比較バージョンを選択すると、ポリシーの変更が3つのカテゴリ（[絶対（Absolute）]、[デフォルト（Default）]、[Catch All]）で表示されます。差分テーブルには、次のような機能があります。

- 同じポリシーに属するさまざまなサービスがグループ化されます
- ポリシーの変更をファセットまたは差分タイプでフィルタします
- ポリシーの変更とサービスはページ分けされます
- フィルタリングされたポリシーの変更を CSV としてダウンロードできます

表 *3:* ファセットフィルタのプロパティ

プロパティ	説明
優先順位	例：100
アクション（**Action**）	例：ALLOW、DENY
コンシューマ	例：コンシューマクラスタ
プロバイダ（**Provider**）	例：プロバイダークラスタ
ポート（**Port**）	例：80
[Protocol]	例：TCP

表 *4: CSV* 出力列

カラム	説明
ランク	ポリシーのカテゴリ。例：ABSOLUTE、DEFAULT、CATCH_ALL
差分（**Diff**）	変更の差分タイプ。例：ADDED、REMOVED、UNCHANGED
優先順位	例：100
アクション（**Action**）	例：ALLOW、DENY
コンシューマ名（**Consumer Name**）	コンシューマクラスタの名前。
コンシューマ ID（**Consumer ID**）	コンシューマクラスタの ID。
プロバイダー名（**Provider Name**）	プロバイダークラスタの名前。
Provider ID	プロバイダークラスタの ID。
[Protocol]	例：TCP
ポート（**Port**）	例：80

次の図では、ポリシー バージョン p1 と v1 が比較されています。

図 *109* : ポリシー差分ビュー

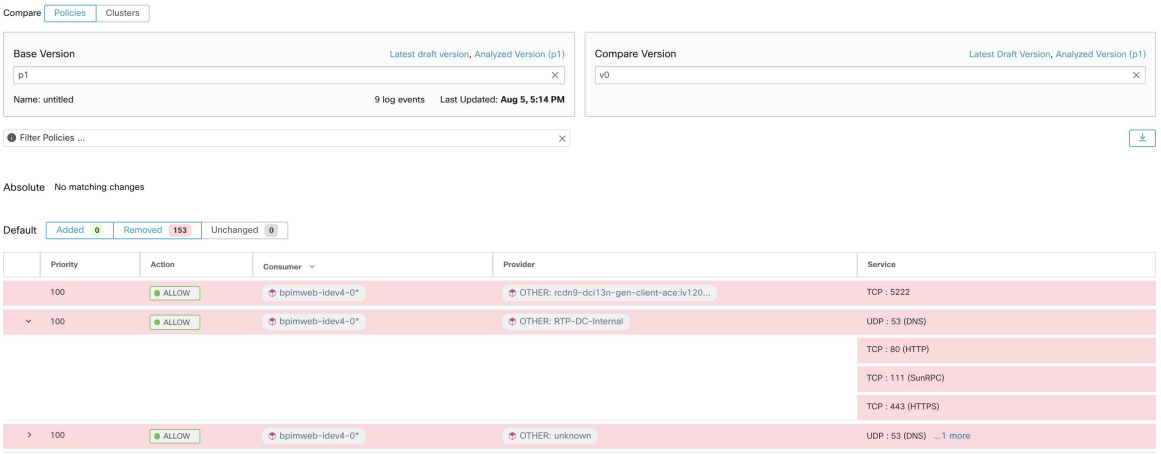


図 *110* : ポリシー差分ビューのダウンロードボタン

図 *111* : ポリシー差分ビューのフィルタリング

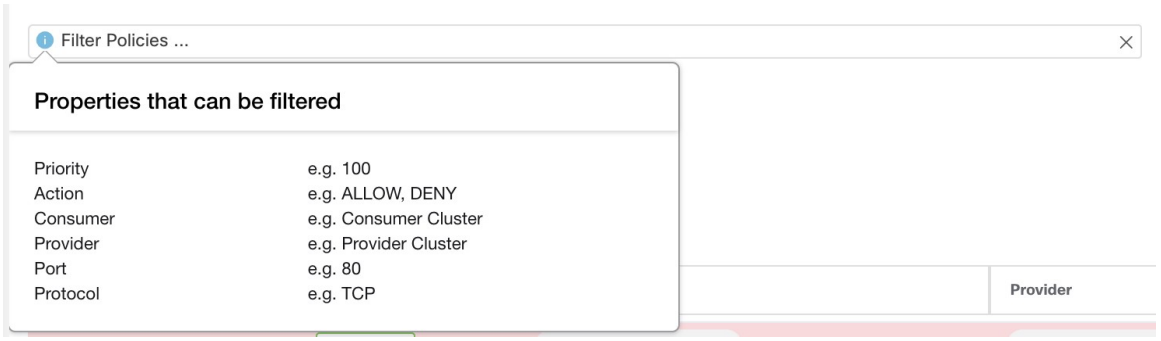


図 *112* : ポリシー差分ビューの差分タイプフィルタ

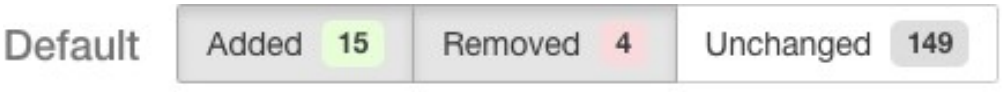


図 *113* : ポリシー差分ビューのグループ化

図 *114* : ポリシー差分ビューの *CSV* 出力

Rank	Diff	Priority	Action	Consumer Name	Consumer ID	Provider Name	Provider ID	Protocol	Port
DEFAULT	ADDED	100	ALLOW	bpimweb-idev4-0*	610bcda7a51e713db909da40	OTHER: rcdn9-dci13n-gen-client-ace:iv120	610bcda7a51e713db909d9f1	TCP	5222
DEFAULT	ADDED	100	ALLOW	bpimweb-idev4-0*	610bcda7a51e713db909da40	OTHER: RTP-DC-Internal	610bcda7a51e713db909d9fe	UDP	53
DEFAULT	ADDED	100	ALLOW	bpimweb-idev4-0*	610bcda7a51e713db909da40	OTHER: RTP-DC-Internal	610bcda7a51e713db909d9fe	TCP	80
DEFAULT	ADDED	100	ALLOW	bpimweb-idev4-0*	610bcda7a51e713db909da40	OTHER: RTP-DC-Internal	610bcda7a51e713db909d9fe	TCP	111
DEFAULT	ADDED	100	ALLOW	bpimweb-idev4-0*	610bcda7a51e713db909da40	OTHER: RTP-DC-Internal	610bcda7a51e713db909d9fe	TCP	443
DEFAULT	ADDED	100	ALLOW	bpimweb-idev4-0*	610bcda7a51e713db909da40	OTHER: unknown	610bcda7a51e713db909da45	UDP	53
DEFAULT	ADDED	100	ALLOW	bpimweb-idev4-0*	610bcda7a51e713db909da40	OTHER: unknown	610bcda7a51e713db909da45	TCP	443
DEFAULT	ADDED	100	ALLOW	bpimweb-idev3-0*	610bcda7a51e713db909da26	OTHER: rcdn9-dci13n-gen-client-ace:iv120	610bcda7a51e713db909d9f1	TCP	5222

インポート/エクスポート

ワークスペースのエクスポート

各ワークスペースのクラスタとポリシーに関連するすべてのコンテンツは、JSON、XML、YAML などの一般的な構造化ドキュメント形式の 1 つのファイルとしてダウンロードできます。これらのファイルを使用して、社内でさらに処理したり、他のポリシー適用や分析ツールで取り込んだりできます。

に移動します。.ワークスペースヘッダーの メニュー項目に移動し、[エクスポート（Export）] 項目をクリックすると、エクスポートダイアログが表示されます。エクスポートされたファイルに、実際のネットワークフローに基づいた自動ポリシー検出によって生成されたクラスタ間のセキュリティポリシーおよびクラスタコンテンツを含めるか、クラスタコンテンツのみを含めるかを選択できます。目的の形式を選択し、[ダウンロード（Download）] をクリックして、ファイルをローカルファイルシステムにダウンロードします。

図 *115* : *[インポート/エクスポート（Import/Export）]* メニュー項目

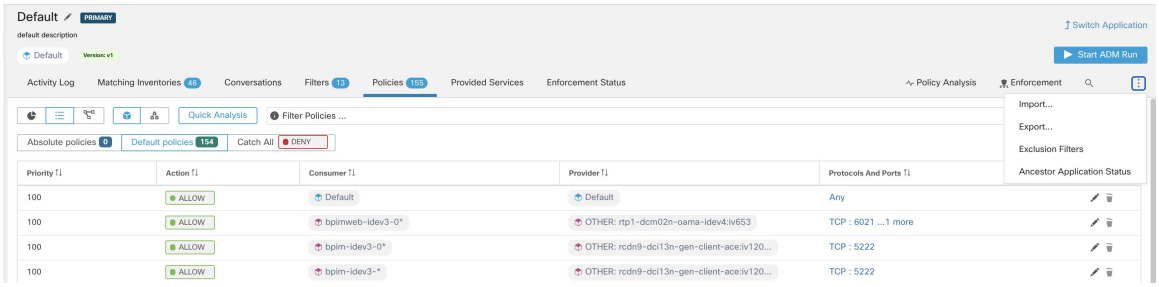
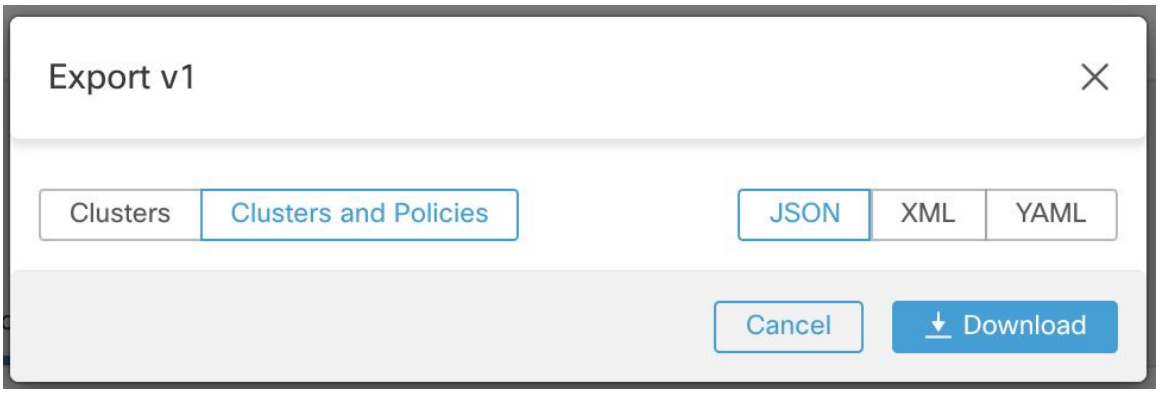


図 *116* : ワークスペースのポリシーのエクスポート



ワークスペースをエクスポートすると、自動ポリシー検出構成の [発信ポリシーコネクタの自動承諾（Auto accept outgoing policy connectors）] 設定が含まれ、インポートされたワークスペースでアクティブになります。

アプリケーションビューのエクスポート

範囲が非常に大きく、数千のワークロードと数百のクラスタがある場合は、特定のワークスペースビューに関するコンテンツのみエクスポートすることが望ましい場合があります。さらに、自動ポリシー検出によって生成されるよりも粗い粒度でポリシーをエクスポートすることが望ましい場合があります。アプリケーションビューの多くの機能を使用して、特定の範囲を折りたたむことで、ポリシーのより限定されたビューや大まかなビューを構築できます。エクスポートされたファイルには、アプリケーション ビュー キャンバスに表示されるグラフに近いポリシー定義が含まれます。

エクスポートするには、アプリケーションビューに移動し、左側のツールバーのボタンをクリックします。これで、エクスポートオプションを含むドロップダウンメニューが表示されます。まず、[保存（Save）] メニュー項目をクリックして、アプリケーションビューが保存されていることを確認します。[エクスポート（Export）] 項目をクリックすると、前述のダイアログと同様のダイアログが表示されます。

図 *117*：特定のアプリケーションビューのエクスポート

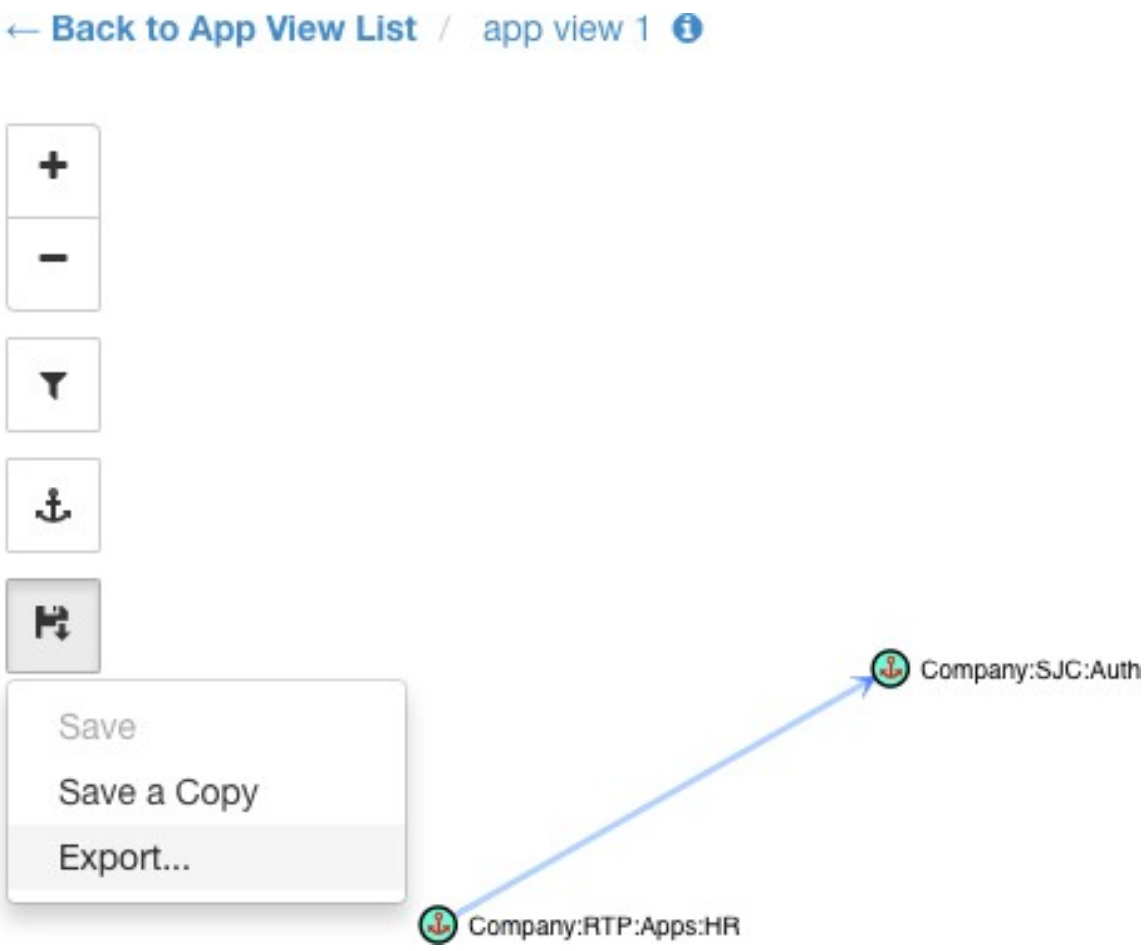


図 *118*：アプリケーションビューのポリシーのエクスポート

（注） アプリケーションビューには、DENYポリシーと自己ループ、つまり、同じコンシューマとプロバイダーのポリシーは表示されません。

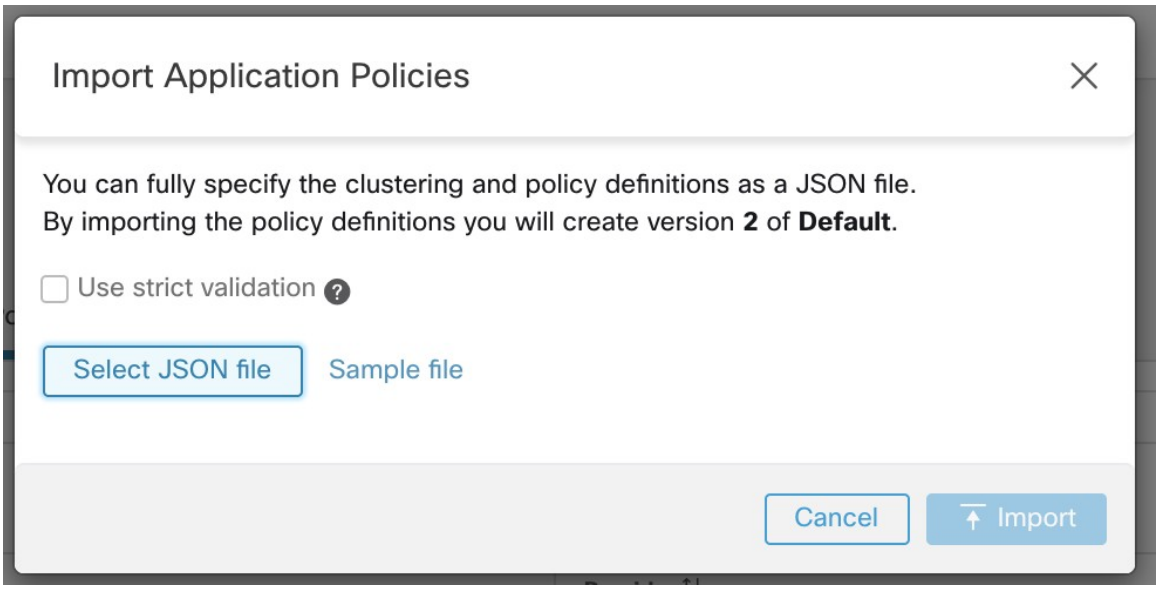
ただし、エクスポートされたファイルには、DENY ポリシー、自己ループ、および Catch-All アクションに関連する情報もすべて含まれます。

Import

JSON ファイルを直接アップロードすることで、既知のクラスタとポリシーの定義をワークスペースにインポートできます。自動ポリシー検出と同様に、ポリシーを既存のワークスペースにアップロードすると、新しいバージョンが作成され、クラスタとポリシー定義が新しいバージョンの下に配置されます。欠落しているフィルタと正しくないプロパティ値がある場合、エラーが返されます。

ワークスペースヘッダーの **...** メニューのメニュー項目 [インポート（Import）] をクリックします。インポートダイアログで、有効な形式の JSON ファイルを選択できます。[サンプル（Sample）] ボタンをクリックすると、ポリシーとクラスタのスキーマを示す小さいサイズのサンプル JSON ファイルが見つかります。

図 *119*: クラスタ/ポリシーのインポート



厳密な検証 有効にすると、JSON に認識されない属性が含まれている場合にエラーが返されます。このオプションは、タイプミスや間違って識別されたオプションフィールドを見つけるのに役立ちます。

（注） 明示的に承認済みとして表示されていない限り、インポートされたすべてのポリシーはデフォルトで `approved: false` として表示されます。新しいポリシーセットを生成するための自動ポリシー検出中に、この種の承認済みポリシーを保持し続けるオプションがあります。詳細な情報については、「承認済みポリシー （53 ページ）」を参照してください。

専門的なヒント：アプリケーションワークスペースまたはアプリビューをエクスポートすることによって取得される JSON ファイルのスキーマには、ポリシーをワークスペースにインポー

トするために必要な形式とのスキーマ互換性があります。したがって、エクスポートとその後のインポートを使用して、あるアプリケーション ワークスペースから別のアプリケーション ワークスペースにポリシーを複製できます。ポリシーをエクスポートしてからインポートすると、多くの機能が同じように動作しない場合があることに注意してください。たとえば、ポリシーを支援するカンバセーションはエクスポートに含まれず、ポリシーのインポート時にも存在しません。

ガベージコレクション

クリーンアップジョブは、最新のバージョンを除き、6 か月間アクセスされていないすべてのワークスペースバージョンの削除を毎週実行します。このジョブは、過去 30 日間にアクセスされなかった古いポリシー実験も削除します。

自動ポリシー検出用の自動ロードバランサ設定（F5 のみ）

重要 **これは実験段階の機能です**

この機能と API は**アルファ版**であり、今後のリリースで変更および拡張される可能性があります。

自動ポリシー検出は、外部オーケストレータに接続されたロードバランサの設定からポリシーを生成します。設定からポリシーを生成すると、フローデータへの依存が最小限に抑えられ、検出されるクラスタとポリシーの精度が向上します。

このトラフィックを許可するポリシーを生成するためのロードバランサへのフローの報告は、コネクタに依存しています。

用語

VIP 仮想 IP：クライアントがサービス宛てのトラフィックを送信する IP。

SNIP SNAT IP：トラフィックをバックエンドホストに送信するためにロードバランサによって使用される IP。

BE バックエンドエンドポイント：バックエンドホストの IP。

HIP ヘルスチェック IP：ヘルスチェックトラフィックをバックエンドホストに送信するためにロードバランサが使用するソース IP。

（注） HIP は、自動マップモードの SNIP と同じです。ただし、SNAT プールが設定されている場合、HIP と SNIP は異なる場合があります。

展開

図 *120 :* 展開

次のように、ロードバランサの VIP、SNIP、および HIP が *lb* 範囲の一部であり、BE が *be* 範囲の一部である展開を検討してください。範囲は次のように作成されます

- client

  クライアントの範囲には、ロードバランサと通信するクライアントが含まれます。上記の例では、クライアントの範囲のクエリは次のようになります。

  ```
  address eq 192.168.60.21 or address eq 192.168.60.22
  ```

- lb

  F5 外部オーケストレータは、ロードバランサによって使用される VIP、SNIP、HIP、および BE にラベルを付けます。これらのラベルを使用して範囲クエリを構築できます。ここで、*orchestrator_system/service_name* は、サービスの VIP、*orchestrator_system/service_startpoint* SNIP、*orchestrator_system/service_healthcheck_startpoint* HIP の選択に使用されます。上記の例では、サービス db の VIP、SNIP、および HIP を含む範囲クエリは次のとおりです。

  ```
  user_orchestrator_system/cluster_id eq 1234 and
  (user_orchestrator_system/service_name eq db or
  user_orchestrator_system/service_startpoint eq db or
  user_orchestrator_system/service_healthcheck_startpoint eq db)
  ```

（注） SNIP と VIP は同じ範囲の一部である必要があります。

- be

  user_orchestrator_system/service_endpoint は、サービスの BE を選択します。上記の例では、サービス db の BE を含む範囲クエリは次のとおりです。

  ```
  user_orchestrator_system/cluster_id eq 1234 and
  user_orchestrator_system/service_endpoint eq db
  ```

クラスタ

各サービスは、最大4つの検出済みクラスタを生成します。このうち、サービスクラスタのみがユーザーに表示されます。SNIP、HIP、およびBEクラスタは、サービスクラスタの関連クラスタとして表示されます。HIPおよびBEクラスタは、*lb*範囲にHIPとBEが存在する場合にのみ生成されます。

上記の例では、自動ポリシー検出により、サービスのSNIPとHIPを含む*lb*範囲にSNIPクラスタとHIPクラスタが生成されます。BEは*lb*範囲の外にあるため、自動ポリシー検出でバックエンドクラスタは生成されませんが、代わりに*db*の関連クラスタのリストに*be*範囲が追加されます。

クラスタは次のように生成されます。

- サービス

  サービスクラスタには、サービスのVIPが含まれます。サービスクラスタのクエリは次のとおりです。

  ```
  user_orchestrator_system/cluster_id eq 1234 and
  user_orchestrator_system/namespace eq common and
  user_orchestrator_system/service_name eq db
  ```

- SNIP

  サービスのSNIPは、SNIPクラスタに含まれています。SNIPクラスタのクエリは次のとおりです。

  ```
  user_orchestrator_system/cluster_id eq 1234 and
  user_orchestrator_system/service_startpoint eq db
  ```

- HIP

  サービスのHIPは、HIPクラスタに含まれています。HIPクラスタのクエリは次のとおりです。

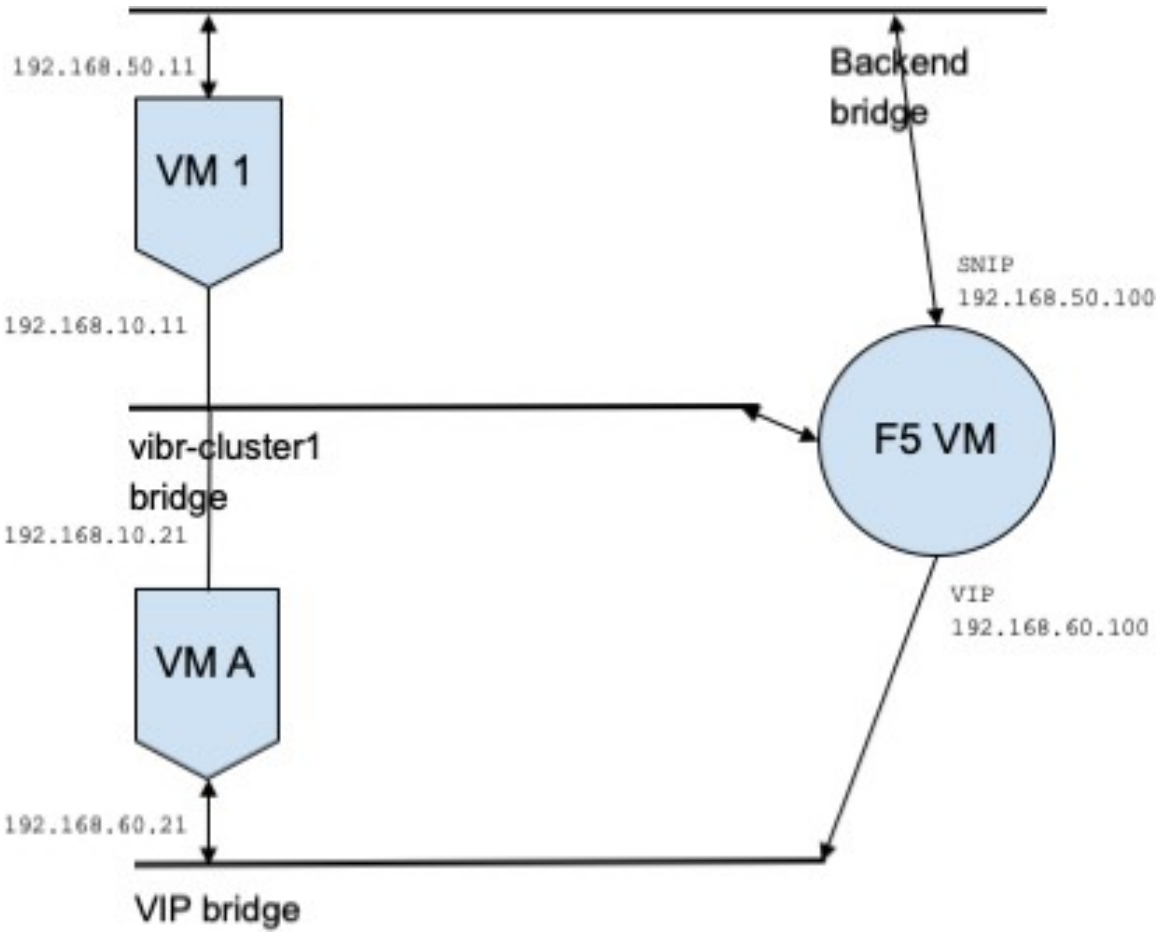
  ```
  user_orchestrator_system/cluster_id eq 1234 and
  user_orchestrator_system/service_healthcheck_startpoint eq db
  ```

- バックエンド

  1つ以上のBEが*lb*範囲の一部である場合、サービスのバックエンドクラスタが生成されます。これは上記の例には当てはまらないため、*lb*範囲ではバックエンドクラスタが生成されません。

ポリシー

図 *121* : ポリシーの生成



VIP アドレス *192.168.60.100*、SNIP アドレス *192.168.50.100* を持つサービス *db* があるとします。また、IP アドレス *192.168.50.11* を持つバックエンド VM がポート 10000 でリッスンしています。クライアント VM *192.168.60.21* から *db* へのトラフィックのポリシーは次のようになります。

- クライアントから VIP へのポリシー

  次のポリシーは、クライアント VM からサービス *db* へのアクセスを許可します。

```
{
"src": "<uuid of client scope>",
"dst": "<uuid of service cluster>",
"l4_params": [
{
"port": [
10000,
10000
],
"proto": 6,
}
```

```
]
}
```

- SNIP から BE へのポリシー。

  SNIPからBEへのトラフィックを許可するポリシーは、設定に基づいて自動生成され、*db* の関連ポリシーとして表示されます。

```
{
"src": "<uuid of SNIP cluster>",
"dst": "<uuid of be scope>",
"l4_params": [
{
"port": [
10000,
10000
],
"proto": 6,
}
]
```

  lb 範囲から *be* 範囲へのポリシーコネクタは、次のポリシーをプッシュします。

コンシューマ	プロバイダー	ポート	プロトコル	アクション
SNIP	be	10000	TCP	許可

  これにより、BEホスト192.168.50.11にファイアウォールルールが生成され、ポート10000のLB SNIP 192.168.50.100からの着信トラフィックが許可されます。

- HIP から BE へのポリシー。

  HIP から BE へのトラフィックを許可するポリシーは、設定に基づいて自動生成され、*db* の関連ポリシーとして表示されます。

```
{
"src": "<uuid of HIP cluster>",
"dst": "<uuid of be scope>",
"l4_params": [
{
"port": [
0,
0
],
"proto": ICMP,
}
]
}
```

  lb 範囲から *be* 範囲へのポリシーコネクタは、次のポリシーをプッシュします。

コンシューマ	プロバイダー	ポート	プロトコル	アクション
HIP	be	0	ICMP	許可

  これにより、BE ホスト *192.168.50.11* にファイアウォール ルールが生成され、LB HIP *192.168.50.2* からの着信 ICMP トラフィックが許可されます。

警告

- 同じロードバランサインスタンスからの複数のサービスが同じ名前を持つ場合、これらのサービスのいずれかに対して生成されるバックエンドルールには、それらすべてのバックエンドプールが含まれます。つまり、ルールは必要以上に寛容になります。

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。