ポリシー

セグメンテーションポリシーの基本

セグメンテーションポリシーとマイクロセグメンテーションポリシーの目的は、組織がビジネスを遂行するために必要なトラフィックのみを許可し、他のすべてのトラフィックをブロックすることです。事業運営を中断することなく、ネットワークの攻撃対象領域を縮小することが目標です。

Cisco Secure Workload のセグメンテーションポリシーは、送信元、宛先、ポート、プロトコル、および通常はプラットフォーム固有のその他のいくつかの属性に基づいて、トラフィックを許可またはブロックします。

一部のポリシーを手動で作成し、Cisco Secure Workload の強力な自動ポリシー検出機能を使用して、既存のネットワークトラフィックに基づいて他のポリシーを生成します。

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、ポリシーを適用します。

重要 マイクロセグメンテーションは、基本的には、各ワークロードの周囲にファイアウォールを作成します。

そのため、トラフィックがコンシューマとプロバイダーの各ペア間を通過するには、カンバセーションの両端でカンバセーションの発生が許可されている必要があります。つまり、コンシューマとプロバイダーのそれぞれに、トラフィックを許可するポリシーが必要です。

（注） ファイアウォールルール、エッジ、およびクラスタエッジという用語が、「ポリシー」を意味するために使用されることがあります。

ワークスペースを使用したポリシーの管理

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、ポリシーを使用および管理する場所です。

その範囲に関連付けられたワークスペース内のポリシーの作成、分析、適用など、特定の範囲のポリシー関連のすべて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。

ワークスペースへのユーザーアクセスの制御

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を制御するには、ワークスペースに関連付けられた範囲のユーザーロールを割り当てます。ロール を参照してください。

ポリシーの操作：[ワークスペース（Workspaces）] ページへの移動

- **ポリシーを操作したり、既存のアプリケーション ワークスペースを表示したり、新しいワークスペースを作成したりするには、次の手順を実行します。**

  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。

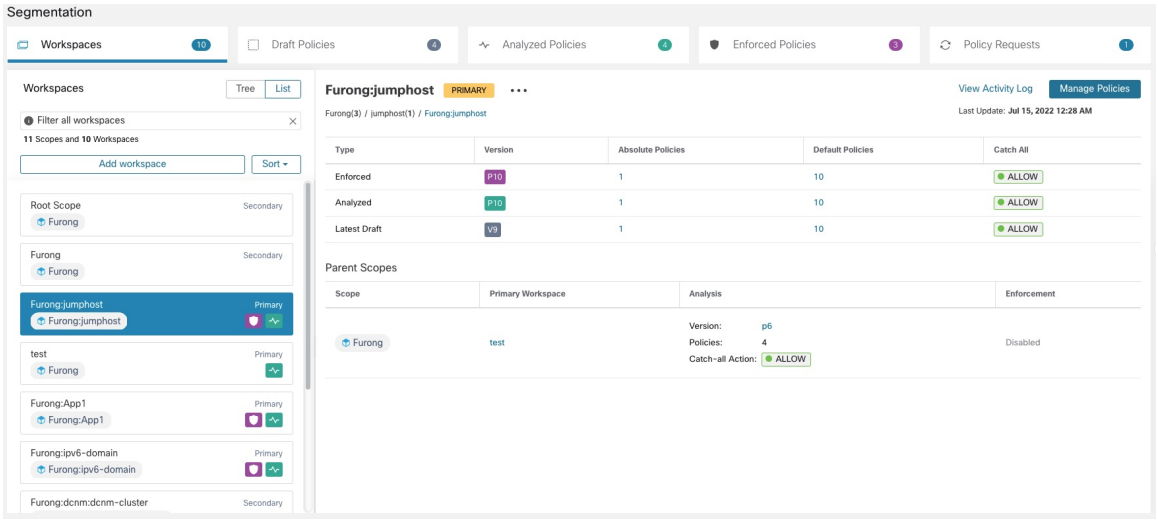
- **特定のワークスペースを表示するには、次の手順を実行します。**

  [ワークスペース（Workspaces）] ページの左側にある範囲のリストで、ワークスペースに関連付けられている範囲に移動し、ワークスペースをクリックします。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。

- ワークスペースを表示しているときに、ワークスペースのリストに戻るには、次の手順を実行します。

  表示しているページの左側付近にある [ワークスペース（Workspaces）] リンクをクリックします。

図 *1*: ワークスペース管理ページ



ワークスペースの作成

範囲のポリシーを作成するには、まずその範囲のワークスペースを作成します。

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. ウィンドウの左側のナビゲーションメニューから、**[防御（Defend）]**>**[セグメンテーション（Segmentation）]** を選択します。
2. ページの左側にある範囲のリストで、ポリシーを作成する範囲を検索するか、その範囲までスクロールします。
3. 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。
4. フォームに入力し、完了したら [作成（Create）] をクリックします。

範囲のワークスペースがすでに存在する場合、追加のワークスペースは自動的にセカンダリワークスペースとして作成されます。

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、コンシューマとプロバイダーが異なる範囲に存在するポリシーを管理する機能、ライブポリシー分析、コンプライアンスレポート、および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。

プライマリワークスペースの既存のポリシーを保持する場合は、セカンダリワークスペースを使用してポリシーを試します。

ワークスペースをプライマリまたはセカンダリに変更するには、次の手順を実行します。

ページ上部の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 *2:* 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

ワークスペース名の変更

ワークスペース名を変更するには、次の手順を実行します。

ページの上部付近に表示されるワークスペースタイプ（[プライマリ（Primary）] または [セカンダリ（Secondary）]）の横にある ••• をクリックし、[ワークスペースの更新（Update Workspace）] を選択します。

範囲内のワークロードの表示

任意のワークスペースで、[一致するインベントリ（Matching Inventories）] タブをクリックします。

ワークスペース内の検索

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. 左側の範囲のリストから、目的の範囲と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。
5. 検索条件を入力します。

検索条件

複数の条件は、論理 AND として扱われます。

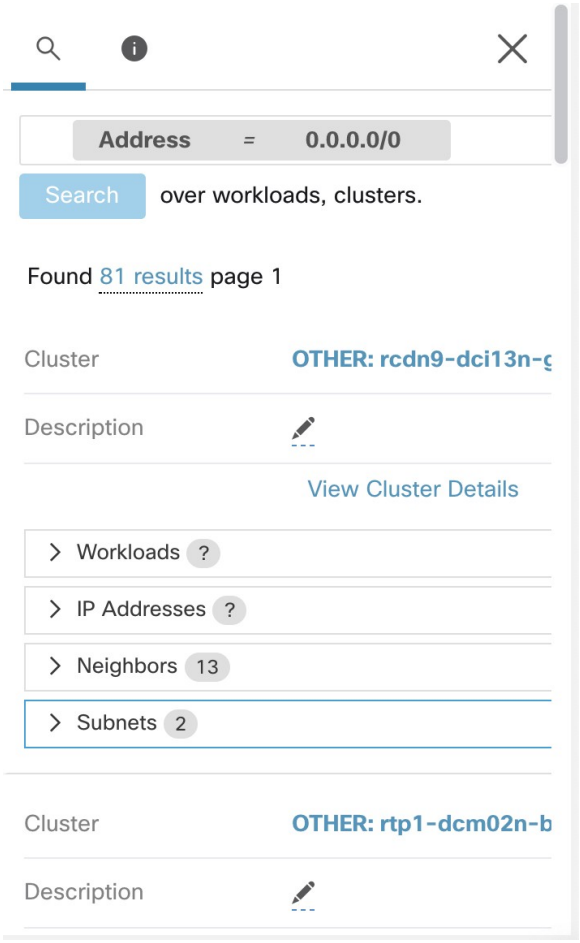
IP アドレスと数値の場合は、次のようになります。

- 'port: 80,443' のように、カンマを使用して論理 OR を指定します。
- 数値の範囲クエリ「port: 3000-3999」もサポートされています。

フィルタ	説明
名前	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。

フィルタ	説明
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。

検索の例

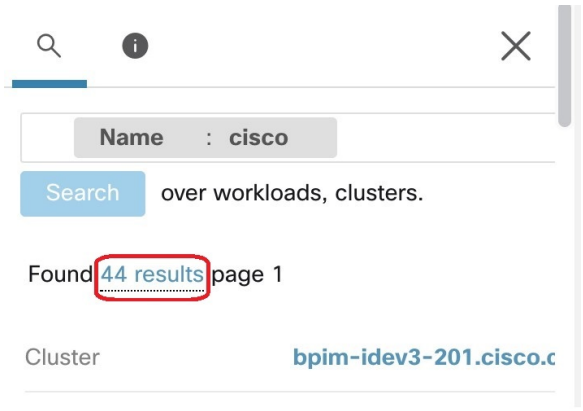


特定のタイプによる検索結果のフィルタリング

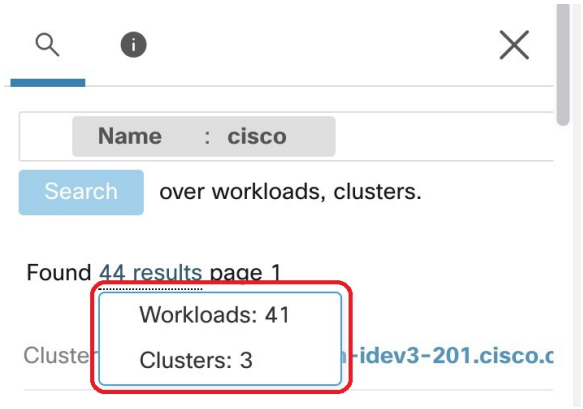
検索結果には、複数のタイプのオブジェクトが含まれている場合があります（ワークロードとクラスタなど）。

特定のタイプで検索結果をフィルタするには、次の手順を実行します。

1. 結果の合計をクリックします。



2. ドロップダウンからタイプを選択します。



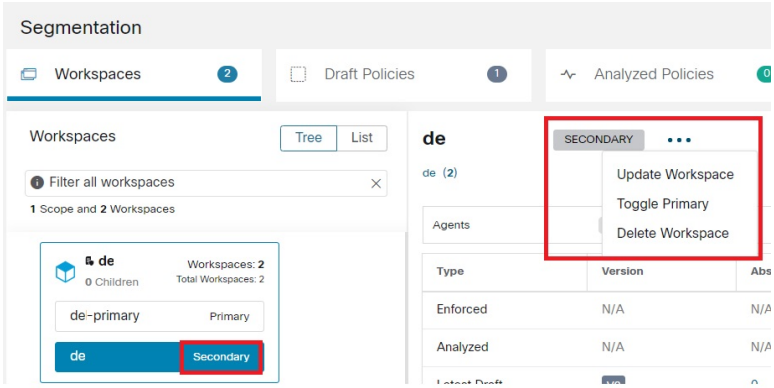
3. タイプフィルタが追加され、検索が再実行されます。

ワークスペースの削除

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。ワークスペースをセカンダリに切り替えるには、プライマリおよびセカンダリワークスペース （3 ページ）を参照してください。

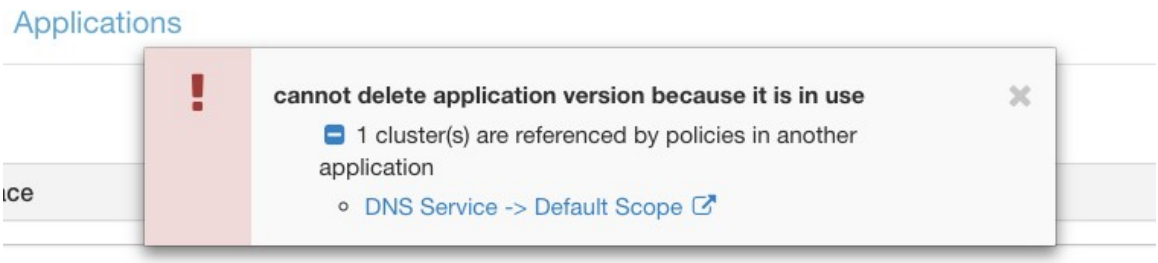
ワークスペースを削除するには、次の手順を実行します。

1. [防御（Defend）] > [セグメンテーション（Segmentation）] を選択します。
2. ページの左側にある範囲のリストで、削除するワークスペースが含まれている範囲に移動して、その範囲をクリックします。
3. 削除するワークスペースをクリックします。
4. [セカンダリ（Secondary）] の横にある ••• をクリックし、[ワークスペースの削除（Delete Workspace）] を選択します。



ワークスペース内のワークロードまたはクラスタが、提供サービスの結果として別のワークスペース内のポリシーによって参照されている場合、依存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 *3:* 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。

p*バージョンを削除するには、分析されたポリシーバージョンの表示、比較、および管理（140ページ）または適用されたポリシーバージョンの表示、比較、および管理（157ページ）を参照してください。

ポリシーについて

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
ポリシーが定義されている範囲	ポリシーは通常、ポリシーが定義されている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ワークロードにのみ影響します。 （ただし、ポリシーの複雑さの対処 （95 ページ）のトピックも参照してください）。 詳細については、「ポリシーの例 （11 ページ）」を参照してください。
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。 ポリシーでのコンシューマとプロバイダーについて （11 ページ）の重要な情報を参照してください。
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。 ポリシーでのコンシューマとプロバイダーについて （11 ページ）の重要な情報を参照してください。
プロトコルとポート[ぷろとこるとぽーと]	許可またはブロックする必要がある、プロバイダーによって利用可能になるサービスのサーバー（リスニング）ポートと IP プロトコル。
操作	許可または拒否：指定されたサービスのポートや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を示します。
ランクと優先順位	ワークスペース内のポリシーのランクと優先順位の詳細については、ポリシーのランク：絶対、デフォルト、キャッチオール （10 ページ）を参照してください。

ポリシーのランク：絶対、デフォルト、キャッチオール

ポリシーのランクは、優先順位リストの下位（または範囲ツリーの下位範囲）にあるより具体的なポリシーによってポリシーをオーバーライドできるかどうかを決定します。すべての範囲で最も優先順位の低いポリシーは、常にキャッチオールルールです。

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各方向のトラフィックを処理するキャッチオール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。 これにより、ツリーのすべての範囲内のポリシーにトラフィックを照合する機会が与えられ、どの範囲内のポリシーにも一致しないトラフィックはブロックされます。 キャッチオールルールは、ワークスペース内の各ワークロードのすべてのインターフェイスに適用されます。

ポリシーの継承と範囲ツリー

ワークロードは階層型範囲ツリーに編成されているため、ツリーの上位またはその近くの範囲で、一般的なポリシーを一旦作成することができます。必要に応じて、そのポリシーをツリー内のその範囲の下にあるすべての範囲内のすべてのワークロードに適用することができます。

ツリーの下位にあるより具体的なポリシーによって、一般的なポリシーをオーバーライドできるかどうかを指定します。

ポリシーのランク：絶対、デフォルト、キャッチオール （10 ページ） を参照してください。

ポリシーでのコンシューマとプロバイダーについて

ポリシーで指定されたコンシューマとプロバイダーには、次の目的があります。

- 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。
- 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が適用される IP アドレスのセットを指定します。

ホストに複数のインターフェイス（IP アドレス）がある場合、ポリシーはすべてのインターフェイスに適用されます。

重要 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 つの目的のコンシューマとプロバイダーを分ける必要がある場合があります。有効なコンシューマまたは有効なプロバイダー （117 ページ） を参照してください。

ポリシーの例

次のポリシーの例は、ポリシーが定義されている範囲の重要性、ポリシー継承の影響、および正確なポリシーまたは複数の範囲のワークロードに適用されるポリシーを作成するためのインベントリフィルタの使用を示しています。

3 つの範囲が含まれている次の例を考えてみましょう。

- **Apps**

  およびその子範囲

  - **Apps:HR** および
  - **Apps:Commerce**

さらに、インベントリフィルタ PRODUCTION および NON-PRODUCTION は、それぞれ実稼働ホストと非実稼働ホストを指定します（単一範囲内または複数範囲内のホストに適用するインベントリフィルタを定義できます）。

次のポリシーが **Apps** 範囲で定義されていると仮定します。

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

このポリシーは、**Apps** 範囲下のプライマリワークスペースで定義された絶対ポリシーであるため、**Apps** 範囲のメンバーであるすべての実稼働/非実稼働ホストに影響します。これには、子孫の範囲のメンバー（**Apps:HR** および **Apps:Commerce** の範囲に属するホスト）も含まれます。

ここで、**Apps:HR** 範囲に関連付けられている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**範囲のメンバーである実稼働/非実稼働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、非実稼働 HR ホスト（存在する場合）のインバウンドルールは、**任意の**実稼働ホストからの TCP ポート 8000 での接続を拒否し、実稼働 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**非実稼働ホストへの接続要求をドロップします。

ポリシーの作成と検出

ポリシーの作成のベストプラクティス

- セグメンテーションプロセス全体の概要については、セグメンテーションとマイクロセグメンテーションを使用する前におよびサブトピックを参照してください。
- ネットワーク全体に広く適用されるポリシーを手動で作成します。

  たとえば、ネットワークの外部からワークロードへの不要なトラフィックをブロックしたり、脆弱なホストを検疫したりします。

  - 範囲ツリーの最上位またはその近くにある範囲で手動ポリシーを作成します。

    たとえば、ネットワークの外部からネットワーク内のすべてのホストへのすべてのトラフィックをブロックするには、ツリーの最上位の範囲内にポリシーを配置します。

  - 一部のワークロードの一般的なポリシーを上書きできるようにする場合（たとえば、上記の例に従ってネットワークの外部からの一般的なアクセスをブロックし、一部のワークロードにはネットワークの外部からアクセスできるようにする場合）、高レベルのポリシーをデフォルトポリシーとして作成します。次に、該当するワークロードの固有のポリシーを作成します。

  - ポリシーの作成を迅速化するために、テンプレートの使用を検討してください。

  - ポリシーの手動作成 （13 ページ）、特定の目的のためのポリシー （15 ページ）、およびポリシーテンプレート （17 ページ）を参照してください。

- （オプション）最初に、ツリーの最上位近くの範囲でポリシーを自動的に検出し、ツリーのブランチ内のすべての範囲について、既存のすべてのトラフィックを許可し、将来の不要なトラフィックを制限できる粗いポリシーを作成します。その後、不要なトラフィックからネットワークをより適切に保護するきめ細かいポリシーを作成することができます。

  詳細については、1 つの範囲または範囲ツリーのブランチのポリシーの検出 （26 ページ）とポリシーの自動検出 （22 ページ）を参照してください。

- よりきめ細かいポリシーを検出する準備ができたら、範囲ツリーの最下位またはその近くにある範囲（特に個々のアプリケーションの範囲）のポリシーを自動的に検出します。

  詳細については、1つの範囲または範囲ツリーのブランチのポリシーの検出（26ページ）とポリシーの自動検出（22ページ）を参照してください。

- フェールオーバー、バックアップからの復元、1年に1回のアクティビティなど、一般的ではないまたは頻度の低いアクティビティとシナリオに対応するポリシーがあることを確認してください。

- アプリケーションに必要なトラフィックを特定して許可した後に、発生してはならないトラフィックを探して、そのようなインスタンスをブロックします。

  最初に、最も機密性の高いアプリケーションとの間のトラフィックを確認します。

  たとえば、顧客向けのWebアプリケーションから最高機密の研究開発アプリケーションのデータベースへのトラフィックを確認した場合は、調査します。

- 同僚と協力して、正しいポリシーが正しいワークロードに適用されていることを確認します。

- 最初に、ポリシーを適用する場合は、キャッチオールを[許可（Allow）]に設定することを検討してください。次に、トラフィックをモニターして、キャッチオールルールに一致するものを確認します。キャッチオールルールに一致する必要なトラフィックがない場合は、キャッチオールを[拒否（Deny）]に設定できます。

ポリシーの手動作成

通常は、ネットワーク全体に広く適用されるポリシーを手動で作成します。

たとえば、次の目的のためにポリシーを手動で作成できます。

- すべての内部ワークロードから、NTP、DNS、Active Directory、または脆弱性スキャンサーバーへのアクセスを許可する。
- 明示的に許可されていない限り、組織外のすべてのホストからネットワーク内のホストへのアクセスを拒否する。
- 脆弱なワークロードを検疫する。

より詳細に適用されるポリシーでオーバーライドできない絶対ポリシーと、より具体的なポリシーが存在する場合にオーバーライドできるデフォルトポリシーを作成できます。

通常、手動ポリシーは、ツリーの最上位に近い範囲に対して作成します。

始める前に

- （オプション）[防御（Defend）]>[ポリシーテンプレート（Policy Templates）]から使用可能なテンプレートのいずれかを使用することを検討してください。

- （オプション）同じポリシーを受信する必要があるワークロードのセットがあることがわかっている場合は、インベントリフィルタを使用してそれらをグループ化し、そのセットにポリシーを簡単に適用できるようにします。インベントリフィルタは、1 つの範囲にのみ適用することも、任意の範囲内のワークロードに適用することもできます。インベントリフィルタの作成を参照してください。
- この範囲内のワークロードがこの範囲内にあることが期待されているワークロードであることを確認してください。範囲内のワークロードの表示 （4 ページ）を参照してください。

手順

ステップ 1 [防御（Defend）] > [セグメンテーション（Segmentation）] をクリックします。

ステップ 2 左側のリストで、ポリシーを作成する範囲を検索するか、その範囲に移動します。

ステップ 3 ポリシーを作成する範囲とワークスペースをクリックします。

この範囲のワークスペースをまだ作成していない場合は、ワークスペースの作成 （3 ページ）を参照してください。

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

ステップ 5 まだ選択されていない場合は、[ポリシー（Policies）] タブをクリックします。

ステップ 6 [ポリシーを追加（Add Policy）] をクリックします。

[ポリシーの追加（Add Policy）] ボタンが表示されない場合は、[ポリシーの追加（Add Policy）] ボタンが使用できない場合 （15 ページ）を参照してください。

ステップ 7 情報を入力します。

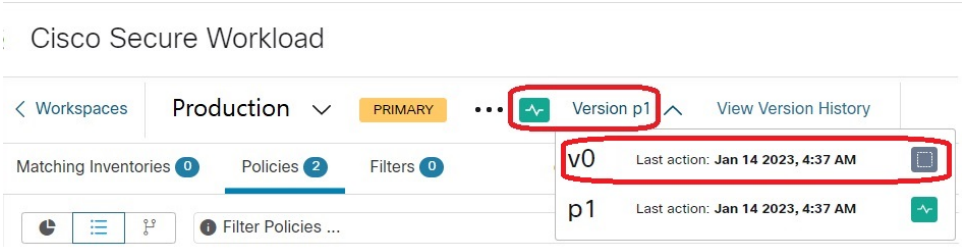
- [絶対（Absolute）] チェックボックスの詳細については、ポリシーのランク：絶対、デフォルト、キャッチオール （10 ページ）を参照してください。通常は、例外を想定しないポリシーを作成する場合に、このチェックボックスを有効にします。
- [優先順位（Priority）] は、リスト内のポリシーの順序を設定します。ポリシーの順序設定の詳細については、ポリシーの優先順位 （96 ページ）とサブトピックを参照してください（ポリシーの順序は後から設定できます）。
- コンシューマとプロバイダーを範囲全体にすることができます。または、インベントリフィルタ（または、最適ではありませんが、同じワークスペース内のクラスタ）を使用してワークロードのグループを作成している場合は、それらを選択できます。

次のタスク

[キャッチオール（Catch-all）] アクションがワークスペースに適していることを確認します。ポリシーのランク：絶対、デフォルト、キャッチオール （10 ページ） を参照してください。

[ポリシーの追加（Add Policy）] ボタンが使用できない場合

ポリシーを作成しようとしているときに [ポリシーの追加（Add Policy）] ボタンが使用できない場合は、ページの上部に表示されているバージョンをクリックし、灰色の正方形で示される最新の "v" バージョンを選択します。



特定の目的のためのポリシー

ネットワーク外部からのトラフィックをブロックするための InfoSec ポリシーの作成

ネットワークの外部からネットワークに入るトラフィックを制御する完全なポリシーセットをすばやく作成するには、この手順を使用します。デフォルトのポリシーセットは、共通のポートとプロトコルを使用するトラフィックのみを許可し、他のすべてのトラフィックを拒否します。必要に応じて、デフォルトのポリシーセットを変更できます。

始める前に

次の条件が満たされている場合は、この手順を使用します。

- 範囲ツリーのルート範囲のすぐ下に、**Internal** という名前の範囲がある。

  この範囲のメンバーに、内部ネットワーク上のすべてのワークロードを含むサブネットが含まれている、または含まれる予定である。

- Internal 範囲でまだポリシーが定義されていない。

（注） または、[防御（Defend）]>[ポリシーテンプレート（Policy Templates）] から入手可能な **InfoSec** テンプレートを使用し、いくつかの追加手順を行ってこれを実現することもできます。

手順

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

ステップ 2 **Internal** 範囲をクリックし、プライマリワークスペースをクリックします。

プライマリワークスペースがまだ存在しない場合は、[+] ボタンをクリックして作成します。

ステップ 3 [ポリシーの管理（Manage Policies）] をクリックします。

ステップ 4 [InfoSecポリシーの追加（Add InfoSec Policies）] をクリックします。

ステップ 5 プロトコルとポートを含む、リスト内のすべてのポリシーが必要なポリシーであることを確認し、必要に応じてポリシーを削除および変更します。

ステップ 6 [作成（Create）] をクリックします。

次のタスク

（オプション）特定の外部トラフィックを特定のワークロードに許可するポリシーなど、追加のポリシーを Internal 範囲に追加します。

具体的なポリシーは、リスト内でより一般的なポリシーの下に配置します。

差し迫った脅威に対処するポリシーの作成

差し迫った脅威に対処する必要がある場合は、対象を絞り込んだ絶対ポリシーを範囲ツリーの最上位またはその近くの範囲に手動で追加してから、その範囲のプライマリワークスペースを適用することができます。

脅威を修復した後は、そのポリシーを削除し、ワークスペースを再適用することができます。

脆弱なワークロードを検疫するポリシーの作成

次の操作を実行できます。

- 事前にポリシーを作成して、特定の既知の脆弱性または指定した脆弱性の重大度しきい値を持つワークロードを自動的に検疫します。
- オンザフライでポリシーを作成して、十分に問題があると判断した既知の脆弱性が検出されたワークロードをすぐに検疫します。

このトピックでは、このいずれかを行うプロセスの概要を示します。

始める前に

必要になる可能性があるポリシーについては、脆弱性ダッシュボードを参照してください。

手順

ステップ 1 検疫する脆弱性または脆弱性の重大度しきい値を定義するインベントリフィルタを作成します。

a) ウィンドウの左側にあるナビゲーションバーから、[整理（Organize）]>[インベントリフィルタ（Inventory Filters）] を選択します。

b) [インベントリフィルタの作成（Create Inventory Filter）] をクリックします。

c) [クエリ（Query）] の横にある [(i)] ボタンをクリックし、**CVE** と入力して、関連するフィルタオプションを表示します。

d) 検疫するワークロードを決定するフィルタ条件を入力します。
e) [クエリを所有権の範囲に制限する（Restrict query to ownership scope）] が選択されていないことを確認してください。

ステップ 2 影響を受けるワークロードを検疫するポリシーを作成します。

全般的な手順については、ポリシーの手動作成 （13 ページ）を参照してください。

推奨事項：

- **Internal** 範囲内、または範囲ツリーの上位付近にあるその他の範囲内にポリシーを作成します。
- 例外を許可する場合を除き、ポリシーは絶対ポリシーである必要があります。例外に対処するには、ポリシーを作成してください。
- コンシューマとプロバイダーに個別のポリシーを作成します。
- 各ポリシーの優先順位を低い数値に設定して、リスト内の他のポリシーよりも前にヒットするようにします。
- アクションを [拒否（Deny）] に設定します。

ステップ 3 ポリシーを確認、分析、および適用します。

次のタスク

トラフィックがこのポリシーにヒットしたときに通知されるようにアラートを作成して、問題を修正し、脆弱なワークロードへのトラフィックを復元できるようにします。アラートを参照してください。

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。

Cisco Secure Workload には、いくつかの事前定義されたテンプレートが含まれています。また、独自のテンプレートを作成することもできます。

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。

システム定義ポリシーテンプレート

使用可能なポリシーテンプレートを表示するには、[防御（Defend）]>[ポリシーテンプレート（Policy Templates）] を選択します。

ポリシーテンプレートを使用するには、テンプレートの適用 （21 ページ）を参照してください。

システム定義テンプレートを変更するには、JSON ファイルをダウンロードして編集し、アップロードします。

カスタム ポリシー テンプレートの作成

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。
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。

属性	タイプ	説明
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] }
        ]
      }
    ]
}
```

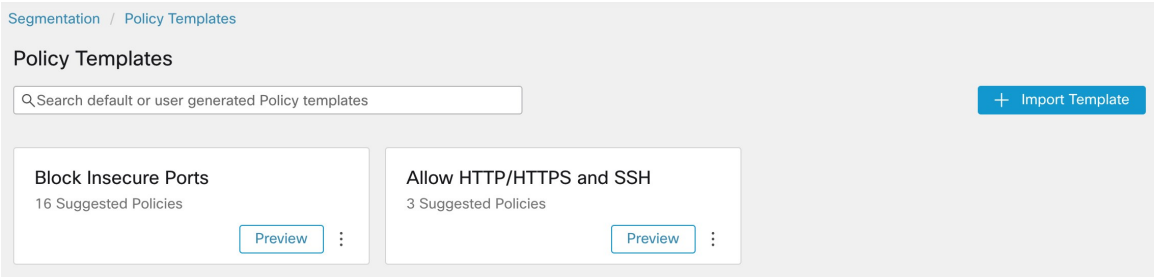

テンプレートインポート

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 *4*：利用可能なテンプレートの表示



テンプレートの適用

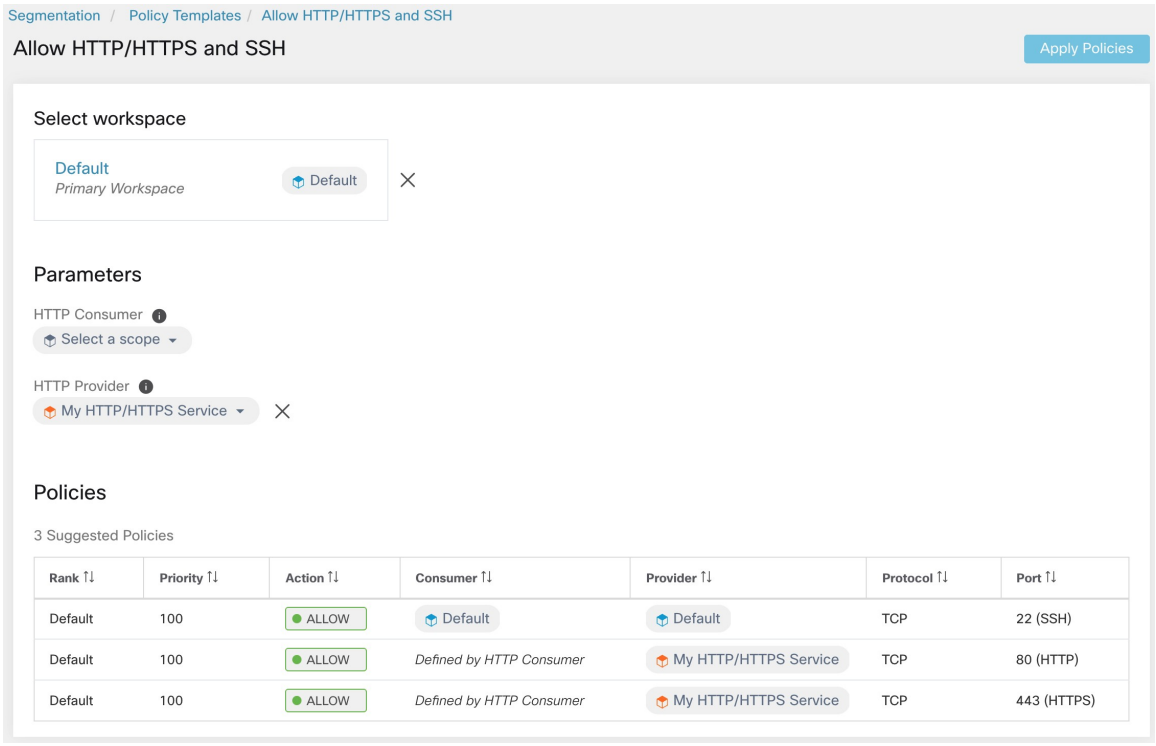
テンプレートをワークスペースに適用するには、いくつかの手順を実行します。

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 *5:* ポリシーテンプレートの適用



ポリシーの自動検出

自動ポリシー検出は、ポリシー検出とも呼ばれ、以前はアプリケーション依存関係マッピング（ADM）と呼ばれていました。自動ポリシー検出は既存のトラフィックフローとその他のデータを使用して、次の処理を実行します。

- 既存の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。

  これらのポリシーの目的は、組織が必要とするトラフィックを識別し、他のすべてのトラフィックをブロックすることです。

- 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。

  たとえば、アプリケーションに複数の Web サーバーが含まれている場合、それらは一緒にクラスタ化される可能性があります。

  詳細については、「クラスタ （84 ページ）」を参照してください。

各範囲のポリシーを検出できます。通常、範囲のポリシーは、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。ただし、初期展開では、より上位の範囲でポリシーを検出することで、より改善されたポリシーを作成しながら、一般的で一時的なポリシーを使用することもできます。

必要に応じて何度でもポリシーを検出し、追加情報に基づいて推奨されるポリシーを改善することができます。

提案されたポリシーとクラスタの変更や承認を手動で行うことができます。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。

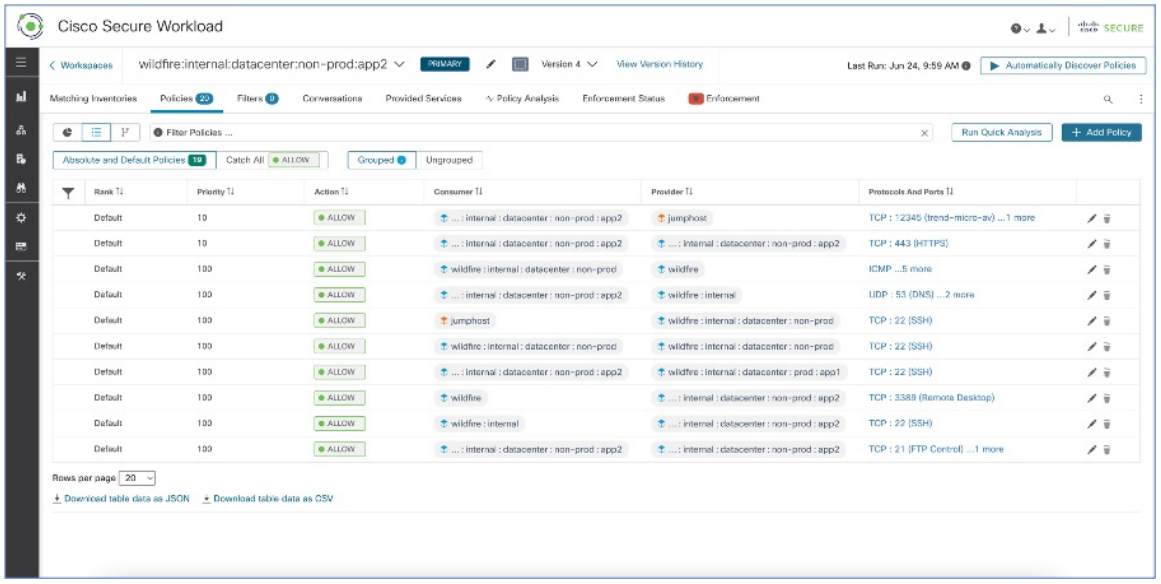
手動で作成したポリシーと検出されたポリシーの両方を、ワークスペースに含めることができます。

ポリシーを検出したら、適用する前に確認および分析します。

ポリシーの検出を開始するには、ポリシーを自動的に検出する方法 （24 ページ）を参照してください。

詳細については、ポリシー検出の詳細 （23 ページ）を参照してください。

図 *6:* 例：自動検出されたポリシー



ポリシー検出の詳細

自動ポリシー検出に関する追加情報：

- 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。
- 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」）を分析してポリシーとクラスタを生成しますが、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。

  ポリシーの検出時にロードバランサとルータからのデータを含める （42 ページ）を参照してください。
- 範囲内の任意のワークスペースでポリシーを検出できます。各ワークスペースの検出結果は、範囲内の他のワークスペースの結果とは無関係です。
- 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高度な機能 （33 ページ）およびポリシーの複雑さの対処 （95 ページ）を参照してください。

ポリシーを自動的に検出する方法

次のステップを実行します。いつでもポリシーを再検出できます。

必要に応じて同僚と協力して、これらの手順を完了します。

手順	操作手順	詳細情報
1	ワークロードインベントリをアップロードしてラベルを付け、ポリシー検出に情報を提供するためにフローデータを収集します。	「セグメンテーションとマイクロセグメンテーションを使用する前に」およびサブトピックを参照してください。
2	次のどちらのポリシーを検出するかを選択します。 • 単一範囲内のワークロード • 範囲ツリーのブランチ内のすべての範囲内のワークロード	1 つの範囲または範囲ツリーのブランチのポリシーの検出 （26 ページ）を参照してください。 （ポリシーはいつでも再検出できます）。
3	ポリシーを検出する範囲を選択します。	これは、単一範囲のポリシーを検出するか、範囲ツリーのブランチのポリシーを検出するかによって部分的に異なります。

手順	操作手順	詳細情報
4	ポリシーを検出するワークスペースを選択します。	ポリシーはプライマリワークスペースでのみ分析できるため、通常は範囲のプライマリワークスペースでポリシーを検出します（ただし、ワークスペースは後からいつでもプライマリに変更できます）。 選択した範囲にまだワークスペースがない場合は、ワークスペースの作成 （3 ページ）を参照してください。
5	ポリシー検出に含めるインベントリを確認します。	ポリシー検出が適用されるワークロードの確認 （29 ページ）
6	（オプション）グループとして扱うワークロードをグループ化するインベントリフィルタを作成します。	インベントリフィルタの作成を参照してください。
7	ワークスペースの[キャッチオール（Catch-all）]アクションを設定します。	ポリシーのランク：絶対、デフォルト、キャッチオール （10 ページ）を参照してください
8	ポリシーを検出します。	ポリシーの自動検出 （22 ページ） 「はじめる前に」の項の前提条件を満たしていることを確認してください。
9	ポリシー検出によって作成されるクラスタ（ワークロードのグループ）を表示および管理します。 （この手順は、単一範囲のポリシーを検出する場合にのみ適用されます。ツリーのブランチのポリシーを検出する場合、クラスタは生成されません）。	「クラスタ （84 ページ）」およびサブトピックを参照してください。 提案されたクラスタを評価し、必要に応じてクラスタメンバーシップを編集して、永続化するクラスタを承認します（または、インベントリフィルタに変換する方がより適切です）。
10	ポリシーの継承やクロス範囲ポリシーなどの複雑さについて検討します。	ポリシーの複雑さの対処 （95 ページ）を参照してください。
11	生成されたポリシーを確認します。	自動検出されたポリシーの確認 （121 ページ）およびサブトピックを参照してください。
12	保持するポリシーを承認します。	ポリシーの承認 （54 ページ）

手順	操作手順	詳細情報
13	必要に応じてポリシーを再検出し、追加のフローデータ、範囲メンバーシップの変更、またはその他の変更を反映します。	重要：自動ポリシー検出を再実行する前に（58ページ） ポリシー検出はいつでも再実行できます。 ポリシーを検出するたびに、ポリシーとクラスタを確認して承認します。
14	ライブ分析を実行して、ポリシーが実際のトラフィックにどのように影響するかを確認します。	ポリシーが期待どおりに機能していると確信できたら、ライブポリシー分析（129ページ）を開始します。 ポリシーを変更したり、ポリシーを再検出したりした場合は、ポリシー分析を再開します（現在のポリシーを分析するため）。
15	ポリシーを再検出したり、その他の変更を行ったりした場合は、ライブ分析を再開します。	ポリシーの変更後の、最新のポリシーの分析（139ページ）を参照してください。
16	ポリシーが重要なトラフィックをブロックしないことを確認できたら、ワークスペースを適用します。	「ポリシーの適用（142ページ）」およびサブトピックを参照してください。
17	適用が予想どおりに機能することを確認します。	適用が予想どおりに機能することの確認（153ページ）を参照してください。
18	（オプション）任意のワークスペースでポリシーを検出するときにオプションで適用されるデフォルトのポリシー検出設定を設定します。	デフォルトのポリシー検出設定（52ページ）およびリンク先のトピックを参照してください。 これらは詳細設定なので、変更する具体的な必要性がある場合にのみ変更することを推奨します。必要に応じて、プロセス中にいつでも変更できます。

1 つの範囲または範囲ツリーのブランチのポリシーの検出

特定の範囲のポリシーを検出するときにいずれかのオプションが使用できない場合は、選択が自動的に行われ、オプションの選択肢は表示されません。

表 *2*: ポリシーの検出の対象

範囲ツリーのブランチ	単一範囲
Cisco Secure Workload の使用を開始する場合は、この方法を開始点として使用して、既存のトラフィックを許可すると同時に将来の脅威からネットワークを保護するための、一時的な大まかなポリシーのセットを迅速に生成します。	セグメンテーションポリシーを微調整し、許可されたすべてのフローが想定されるようにするために、この方法を使用します。ポリシーの数が少ないほど、調査が必要な既存の異常を簡単に確認できるようになります。
通常、この方法は範囲ツリーの最上位に近い範囲に使用します。 ブランチの最上位は、ツリー内の任意の範囲にすることができます。	通常、この方法は、単一のアプリケーション専用の範囲など、範囲ツリーの最下位またはその付近にある範囲に使用します。
1 つの範囲（選択したブランチの最上位にある範囲）でのみポリシーを検出します。	必要に応じて、ブランチ内の各範囲のポリシーを検出します。
選択した範囲内のすべてのワークロードと、すべての子および子孫の範囲が検出に含まれます。	子範囲のメンバーでもあるワークロードは、この範囲の検出には含まれません。 ポリシーは、[整理（Organize）]>[範囲とインベントリ（Scopes and Inventory）] ページでその範囲の [未分類のインベントリ（Uncategorized Inventory）] タブに表示されるワークロードに対してのみ生成されます。 子および子孫の範囲内のワークロードのポリシーを個別に検出できます。
ブランチ内の全範囲内のワークロードのポリシーすべてが、ブランチの最上位にある範囲内に存在します。	子および子孫の範囲内のワークロードのポリシーも作成すると仮定すると、ポリシーは複数の範囲内に存在します。
この方法では、通常、非常に多数のポリシーが生成されます。	この方法では、個々の範囲内に生成されるポリシーは少なくなります。
検出されたポリシーは、範囲全体に適用されます。このオプションでは、範囲内のワークロードのサブセットに固有のポリシーを作成できません。	このオプションでは、コンシューマやプロバイダーの範囲内のワークロードのサブセットに適用されるポリシーを生成できます（ワークロードは、生成されたクラスタや設定されたインベントリフィルタによってグループ化でき、ポリシーはこれらのサブセットにのみ適用されます）。

範囲ツリーのブランチ	単一範囲
すべてのポリシーがブランチの最上位にある単一範囲内に作成されるため、ポリシーのコンシューマとプロバイダーが異なる範囲にある場合、追加の手順は必要ありません。	異なる範囲内のコンシューマとプロバイダーの間のトラフィックを許可するには、追加の手順が必要です。 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 （103ページ）を参照してください。
子孫の範囲にフローデータを収集するエージェント、外部オーケストレータ、またはコネクタがある限り、インストールされたエージェントを持つメンバーワークロードが範囲にない場合でも、検出を実行できます。	範囲には、フローデータを収集するインストールされたエージェント、外部オーケストレータ、またはコネクタを持つメンバーワークロードが必要です。
このオプションは、ルート範囲の所有者とサイト管理者が使用できます。	この範囲のポリシーを作成する権限が必要です。
エージェントとカンバセーションの最大数は、オプションごとに異なります。ポリシーに関連する制限を参照してください。	
このオプションは、以前は自動ポリシー検出用のディープポリシー生成の詳細設定オプションでした。動作は、変更されていません。	これは、以前は自動ポリシー検出用のデフォルトの動作でした。
詳細については、範囲ツリーのブランチのポリシーの検出：追加情報 （28ページ）を参照してください。	--

範囲ツリーのブランチのポリシーの検出：追加情報

- 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。
- 範囲ツリーのブランチのポリシーを生成するときに使用できる詳細設定オプションについては、次を参照してください。
  - 冗長ポリシー削除の有効化 （49 ページ）
  - ポリシー圧縮 （45 ページ）および関連するサブトピック、階層型ポリシーの圧縮 （45 ページ）
- 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。

ポリシー検出が適用されるワークロードの確認

ポリシーを自動的に検出する前に、ポリシー検出のベースとなるワークロードが、実際に想定した一連のワークロードであることを確認します。検出されたポリシーは、これらのワークロードでエージェントによってキャプチャされたフローデータから生成されます。

始める前に

1 つの範囲または範囲ツリーのブランチのポリシーの検出 （26 ページ）のどのオプションを使用するかを決定します。

手順

ステップ 1 左側のナビゲーションメニューから、[防御（Defend）]>[セグメンテーション（Segmentation）] を選択します。

ステップ 2 ポリシーを検出する範囲をクリックします。

ステップ 3 ポリシーを検出するワークスペースをクリックします。

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

ステップ 5 [一致するインベントリ（Matching Inventories）] をクリックします。

ステップ 6 単一範囲のポリシーを検出する場合は、次の手順を実行します。

a) [未分類のインベントリ（Uncategorized Inventory）] をクリックします。

このページには、子範囲のメンバーではないワークロードが表示されます（標準の自動ポリシー検出では、子範囲のメンバーではないワークロードに対してのみ、この範囲内にポリシーとクラスタが生成されます）。

b) [IPアドレス（IP addresses）] をクリックします。

このページの IP アドレスには、Cisco Secure Workload エージェントがインストールされていません。

エージェントがインストールされていないため、次の場合を除き、この範囲の自動ポリシー検出中にこれらの IP アドレスは考慮されません。

- ポリシーがクラウドコネクタを介して管理されている。
- IP アドレスがコンテナベースのインベントリである。この場合、個々のワークロードが [ポッド（Pods）] タブに表示されます。
- ポリシー検出中に考慮されるこの範囲内のワークロードと通信するためにワークロードが発生する。

ポリシーを検出する前に、エージェントを必要とするワークロードにエージェントをインストールし、フローデータが蓄積されるまでしばらく待つことを検討してください。

c) [ワークロード（Workloads）] をクリックします。

ポリシーとクラスタは、このページのワークロードと、[IPアドレス（IP addresses）] タブの IP アドレスのうち、考慮するために上記で指定されている基準を満たす IP アドレスに対してのみ生成されます。

d) Kubernetes または OpenShift インベントリがある場合は、[サービス（Services）] タブと [ポッド（Pods）] タブも表示されます。

Kubernetes/OpenShift ワークロードにエージェントをインストールしている場合は、それらのタブのインベントリも確認します。

e) ロードバランサインベントリがある場合、そのインベントリは [サービス（Services）] タブに表示されます。

ステップ 7 ツリーのブランチのポリシーを検出する場合は、次の手順を実行します。

a) [すべてのインベントリ（All Inventory）] をクリックします。

このプロセスは、子範囲のメンバーでもあるかどうかに関係なく、この範囲内のすべてのワークロードのポリシーを生成します（ただし、クラスタは生成しません）。

b) [IPアドレス（IP addresses）] をクリックします。

このページの IP アドレスには、Cisco Secure Workload エージェントがインストールされていません。

エージェントがインストールされていないため、次の場合を除き、この範囲の自動ポリシー検出中にこれらの IP アドレスは考慮されません。

- ポリシーがクラウドコネクタを介して管理されている。
- IP アドレスがコンテナベースのインベントリである。この場合、個々のワークロードが [ポッド（Pods）] タブに表示されます。
- ポリシー検出中に考慮されるこの範囲内のワークロードと通信するためにワークロードが発生する。

ポリシーを検出する前に、これらのワークロードにエージェントをインストールし、フローデータが蓄積されるまでしばらく待つことを検討してください。

c) [ワークロード（Workloads）] をクリックします。

ポリシーは、このページのワークロードと、[IPアドレス（IP addresses）] タブの IP アドレスのうち、考慮するために上記で指定されている基準を満たす IP アドレスに対してのみ生成されます。

d) Kubernetes または OpenShift インベントリがある場合は、[サービス（Services）] タブと [ポッド（Pods）] タブも表示されます。

Kubernetes/OpenShift ワークロードにエージェントをインストールしている場合は、それらのタブのインベントリも確認します。

e) ロードバランサインベントリがある場合、そのインベントリは [サービス（Services）] タブに表示されます。

ステップ 8 ワークロードが想定どおりのセットであることを確認します。

ポリシーの自動検出

この手順を使用して、ネットワーク上の既存のトラフィックに基づいて推奨される許可ポリシーを生成します。

ポリシーはいつでも再検出できます。

始める前に

- ポリシーを効果的に自動検出するには、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、あるいはクラウドコネクタまたは外部オーケストレー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、Secure Workload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。

  定期的に（月次、四半期、年次など）のみ発生するトラフィックを含めるために、ポリシーを適用する前に十分なデータを収集する必要があります。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、フローデータにそのレポート生成プロセス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。

- ポリシーを自動的に検出する方法 （24 ページ）のここまでの手順を完了します。
- ポリシー検出関連のポリシーに関連する制限を満たします。

  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。

重要 ポリシー検出を再実行する場合は、最初に重要な考慮事項を参照してください（重要：自動ポリシー検出を再実行する前に （58 ページ））。

手順

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スクロールするか、その範囲を検索します。

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 Policies）] 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）] をクリックします。

ステップ 6 ブランチまたは範囲全体のポリシーを検出するオプションが表示された場合は、オプションを選択します。

オプションが表示されない場合は、ポリシーを検出している範囲で使用できるオプションは 1 つだけです。

詳細については、「1 つの範囲または範囲ツリーのブランチのポリシーの検出（26 ページ）」を参照してください。

ステップ 7 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（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生成プロセス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 8 （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、特定の問題に対処するために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（42 ページ）を参照してください。

ステップ 9 [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

- 進行中の自動ポリシー検出の停止（33 ページ） を表示します。
- ポリシーを自動的に検出する方法（24 ページ）に戻り、表の次のステップに進みます。
- ポリシーはいつでも再検出できます。最初に実行する必要があるアクションについては、重要：自動ポリシー検出を再実行する前に（58 ページ）を参照してください。

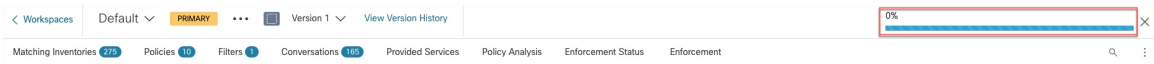
進行中の自動ポリシー検出の停止

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。

進行中に実行を停止するには、[中止（abort）] ボタンをクリックします。

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 *7:* 自動ポリシー検出の進行状況



自動ポリシー検出の高度な機能

検出実行の時間範囲のみを指定する必要がある場合があります。必要に応じて、詳細オプションを設定できます。

各ワークスペースの詳細オプションを設定するか、すべてのワークスペース（ルート範囲全体）のデフォルトを設定してから、必要に応じて個々のワークスペースの設定を変更することができます。

表 *3:* 自動ポリシー検出の詳細オプションの設定

単一のワークスペースの場合	すべてのワークスペースの場合
個々のワークスペース（1列目）のオプションの説明が、すべてのワークスペース（2列目）にも適用されます	
外部依存関係 （37 ページ）	デフォルトのポリシー検出設定 （52 ページ）
自動ポリシー検出の詳細設定 （42 ページ）	デフォルトのポリシー検出設定 （52 ページ）
除外フィルタ （33 ページ）	デフォルトの除外フィルタ （53 ページ）

除外フィルタ

特定のフローが不要なポリシーを生成している場合は、除外フィルタを使用してそのフローを自動ポリシー検出から除外することができます。

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、「アクティビティログとバージョン履歴」を参照してください。
- 除外フィルタ数の制限については、「ポリシーに関連する制限」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 （34ページ）」および「除外フィルタを有効または無効にする （37 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。

手順

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 3 ポリシー検出時に考慮しないフローのパラメータを指定します。

すべてのフィールドに値を入力する必要はありません。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、選択した範囲またはインベントリフィルタ（または、ワークスペース固有の除外フィルタの場合のみ、クラスタ）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。

オプション	説明
プロバイダ（Provider）	プロバイダーアドレスが、選択した範囲またはインベントリフィルタ（または、ワークスペース固有の除外フィルタの場合のみ、クラスタ）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」）。

ステップ 4 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 5 デフォルトの除外フィルタを設定する場合は、次の手順を実行します。

設定したフィルタを使用する準備ができたら、[デフォルトのポリシー検出設定（Default Policy Discovery Config）] ページに戻り、[保存（Save）] をクリックして、個々のワークスペースで変更を使用できるようにします。

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 （37 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。

外部依存関係

外部依存関係は、（上級）クロス範囲ポリシーの作成（104 ページ）で説明されているプロセスを使用する場合にのみ関連します。

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に適用されます（つまり、「外部ワークロード」が関与する通信）。

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。

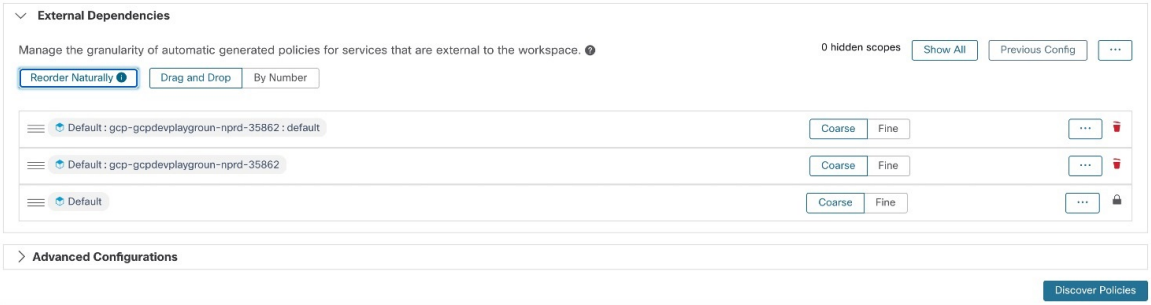
外部依存関係リストは、階層内のすべての範囲の順序付きリストです。リスト内の各範囲は、次のいずれかに設定されます。

- 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、またはインベントリフィルタ。以下を参照）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、すべての範囲がデフォルトで[粗い（Coarse）]に設定されます。

図 *8*: 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 （39 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 （52 ページ）を参照してください。

外部依存関係：範囲のサブセットを含むきめ細かいポリシー

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固有のポリシーを生成するには、ワークスペースの外部依存関係の微調整 （39 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

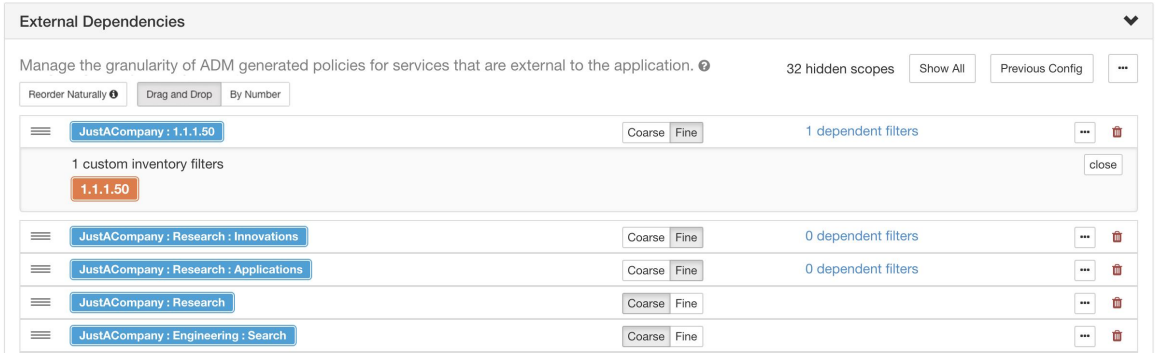
- リストを削除および再配置して、目的の粒度でポリシーを生成できます。たとえば、すべての Company:RTP サブ範囲を削除すると、Company:SJC 範囲に対してより高い粒度を維持しながら、個々のコンポーネントではなく Company:RTP 範囲全体に対する幅広いポリシーを生成できます。さらに、任意の範囲の横にある [詳細（Fine）] ボタンをクリックして、その範囲の下に定義されているより細かい候補の存在を確認できます。
- デフォルトでは、ルート範囲は外部依存関係リストの最下位のエントリとして構成されているため、自動ポリシー検出では可能な限り、常により具体的な範囲に対するポリシーが生成されます。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 *9:* 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。

    （クラスタをインベントリフィルタに変換する （89 ページ）を参照）

    および/または

  - 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）]

- 外部依存関係の調査に関するヒント （38 ページ）も参照してください。

手順

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。

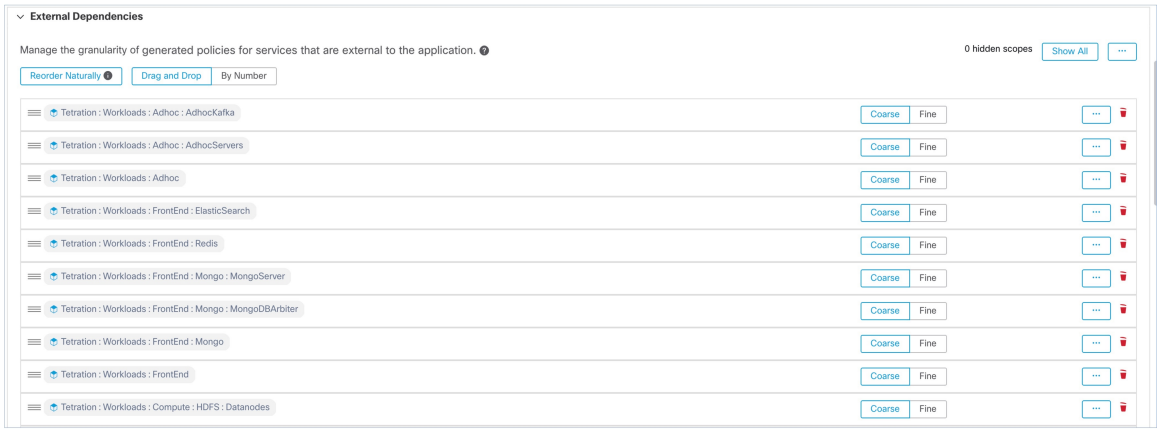
ステップ 6 必要に応じて範囲（および該当する場合はインベントリフィルタ）を並べ替えます。

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。

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

  図 *10*：自然に並べ替える



- （特定の理由がある場合）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。

- 設定されたインベントリフィルタまたはクラスタに固有のポリシーを生成するには、各行の [細かい（Fine）] をクリックします。

  範囲全体に適用するポリシーを生成するには、[粗い（Coarse）] 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。

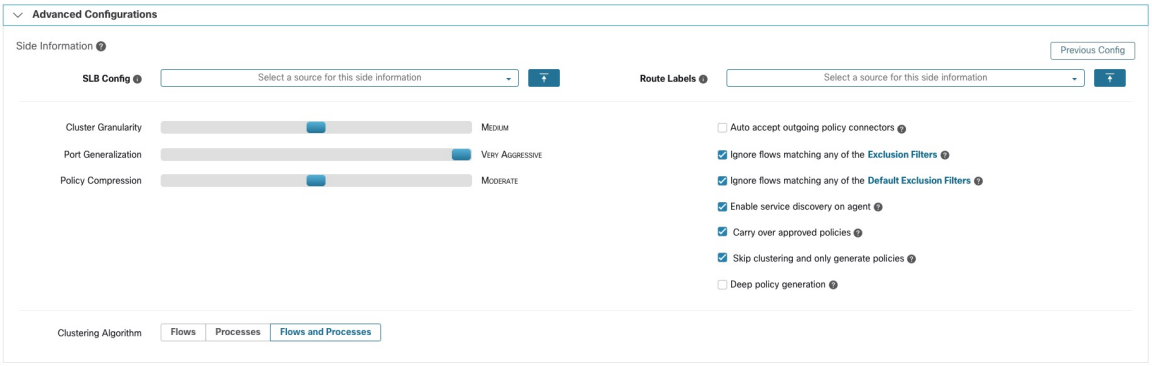
自動ポリシー検出の詳細設定

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。

通常、特別な理由がない限り、これらのオプションは変更しないことを推奨します。

- 特定のワークスペースの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。
- すべてのワークスペースのデフォルトを変更するには、デフォルトのポリシー検出設定（52 ページ）を参照してください。

図 *11* : 自動ポリシー検出の詳細設定



ポリシーの検出時にロードバランサとルータからのデータを含める

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）	正しい形式で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 BIG-IP** • **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ロードバランサまたはルータのデータから計算されます。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。

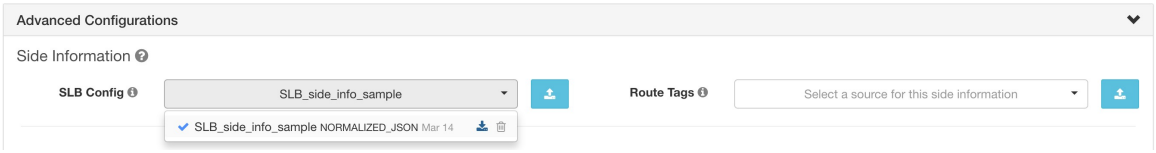
以前にアップロードしたロードバランサ（SLB 構成）またはルートラベルファイルを表示または削除するには、次の手順を実行します。

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 *12*：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。

ポートの一般化

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。

この設定は、ポリシーの精度、数、簡潔さ、およびポリシーの生成に必要な時間に影響を与える可能性があります。

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。

背景

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ことができます。

ポリシー圧縮

ポリシー圧縮が有効になっていて、ワークスペース内の複数のクラスタ内のポリシーが類似している場合、それらのポリシーを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ることができます。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、それらのクラスタ固有のポリシーはすべて親範囲内の1つのポリシーに置き換えられます。これにより、ポリシーの数を大幅に減らして、可能な限り簡素化することができます。また、ドロップされていた正当なフローを今後は許可できる可能性もあります（正確な一般化）。

圧縮の設定がより積極的であるほど、クラスタ固有のポリシーを親全体に適用できるポリシーに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。

範囲ツリーのブランチのポリシーを生成する場合：

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。

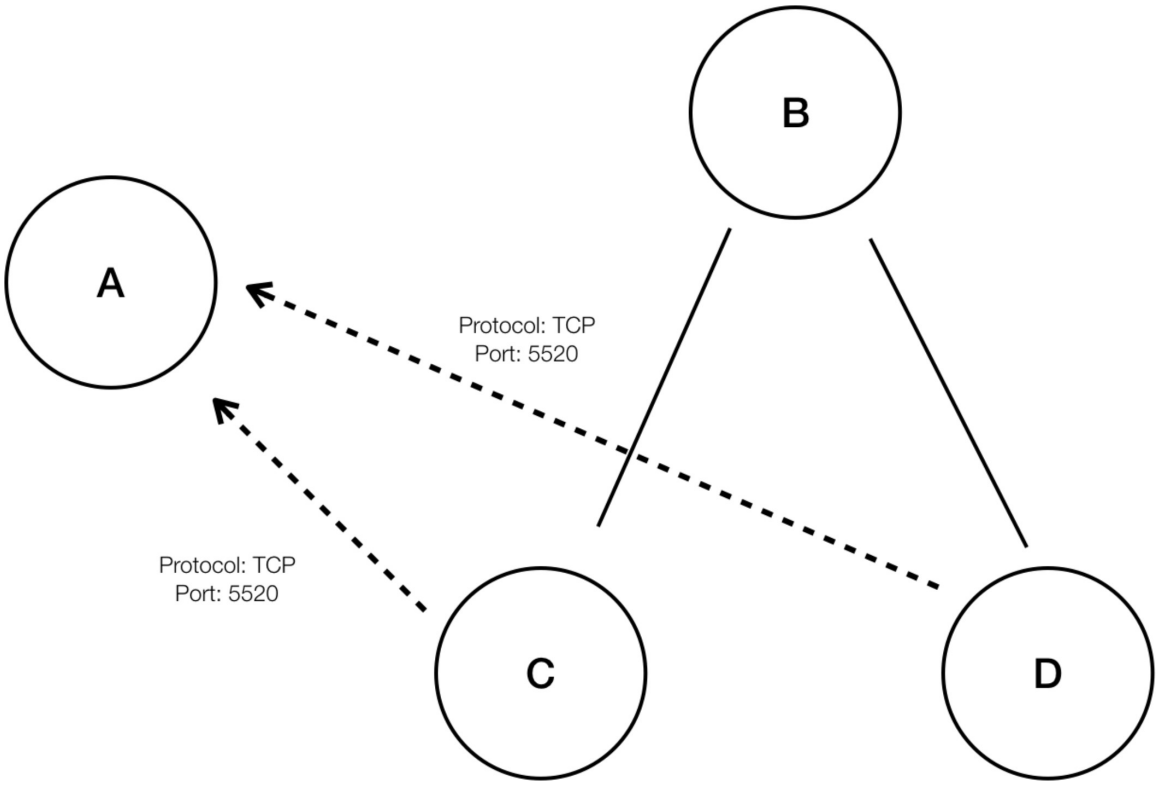
（注） 現在、自動ポリシー検出会話ページは、圧縮ポリシーが導かれた会話の表示をサポートしていません（圧縮を無効にするか、フロー検索を使用する必要がある場合があります）。

階層型ポリシーの圧縮

ポリシーの圧縮は、範囲ツリーのブランチのポリシーを生成するときにも実行できます。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。

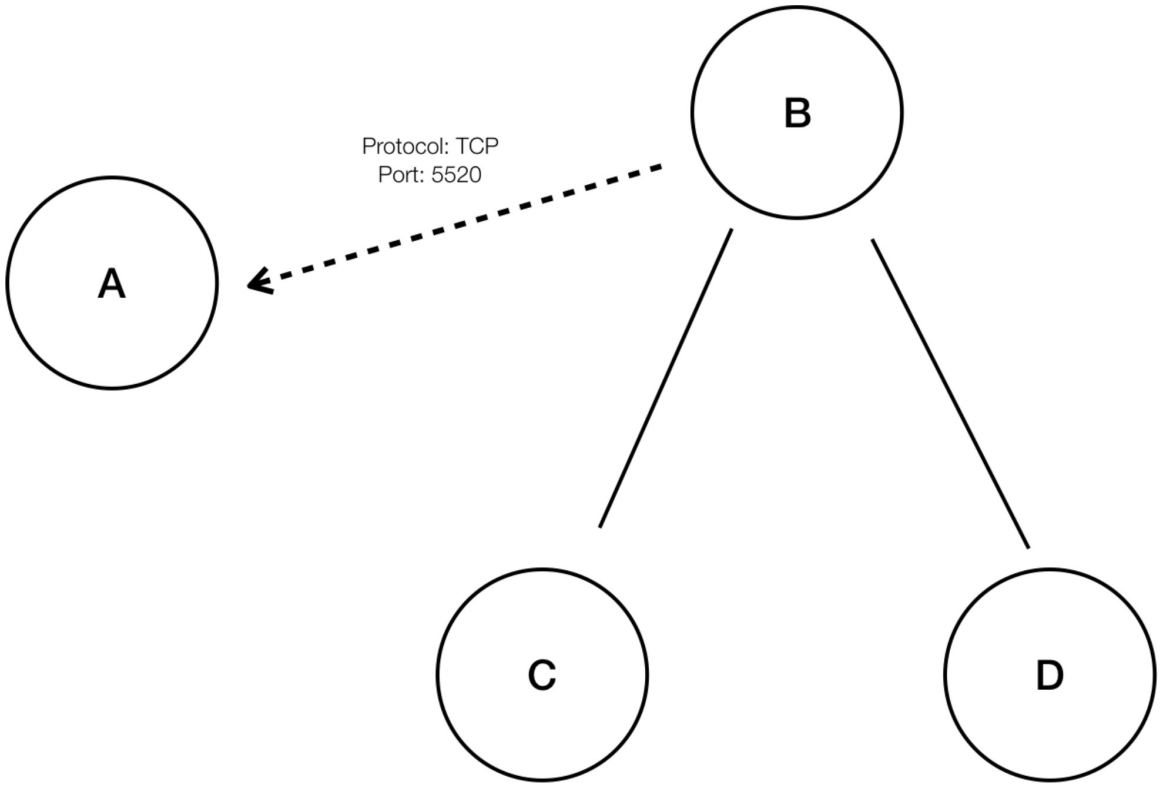
- A、B、C、Dを範囲ツリーの範囲部分とし、「C」と「D」を「B」の子範囲とします。「C」→「A」をポート5520のTCP「ALLOW」ポリシーとし、「D」→「A」をポート5520のTCP「ALLOW」ポリシーとします。

図 *13 :* 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、サブツリー（範囲ツリーのブランチ）のルートまでたどり着くことができます。

図 *14 :* 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。

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。

発信ポリシーコネクタの自動承諾

このオプションは、（上級）クロス範囲ポリシーの作成（104ページ）で説明されている方法を使用して、自動ポリシー検出を使用してクロス範囲ポリシーを作成する場合にのみ適用できます。

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。

詳細については、自動承諾ポリシーコネクタ（114ページ）および「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とサイト管理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（53 ページ）」および「除外フィルタの構成、編集、または削除 （34 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

特定のアプリケーションでは、広範囲のポートを使用するように指定されているものの、実際のトラフィックでは、ポリシー検出に含まれる期間中にこれらのポートのサブセットのみが使用される場合があります。このオプションを使用すると、実際のトラフィックで確認されたポートだけでなく、これらのアプリケーションに指定されたポートのプール全体を、これらのアプリケーションのポリシーに含めることができます。

このオプションを有効にすると、エージェントノードに存在するサービスに関連するエフェメラルポート範囲情報を収集できます。次に、この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 *15*：サービス検出がエージェントで有効になっている

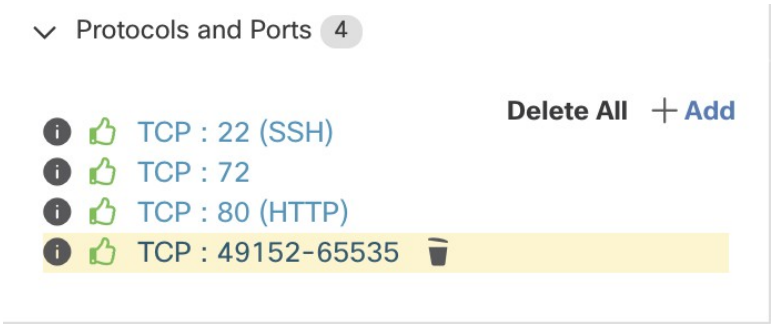
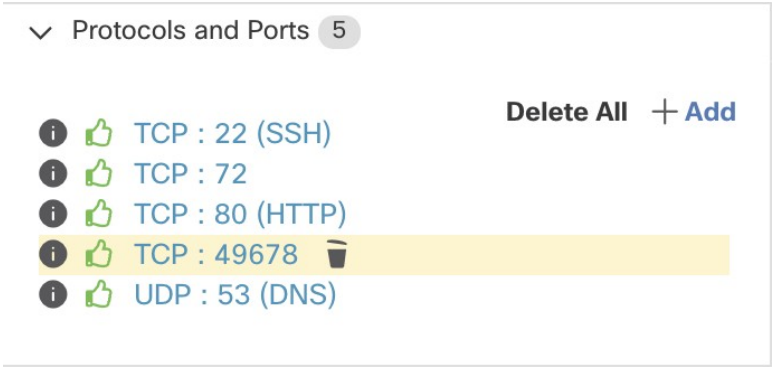


図 *16* : サービス検出がエージェントで有効になっていない



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 （54 ページ） を参照してください。

クラスタリングをスキップしてポリシーを作成

このオプションが選択されている場合、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。

冗長ポリシー削除の有効化

このオプションは、範囲ツリーのブランチのポリシーを生成する場合にのみ使用できます。

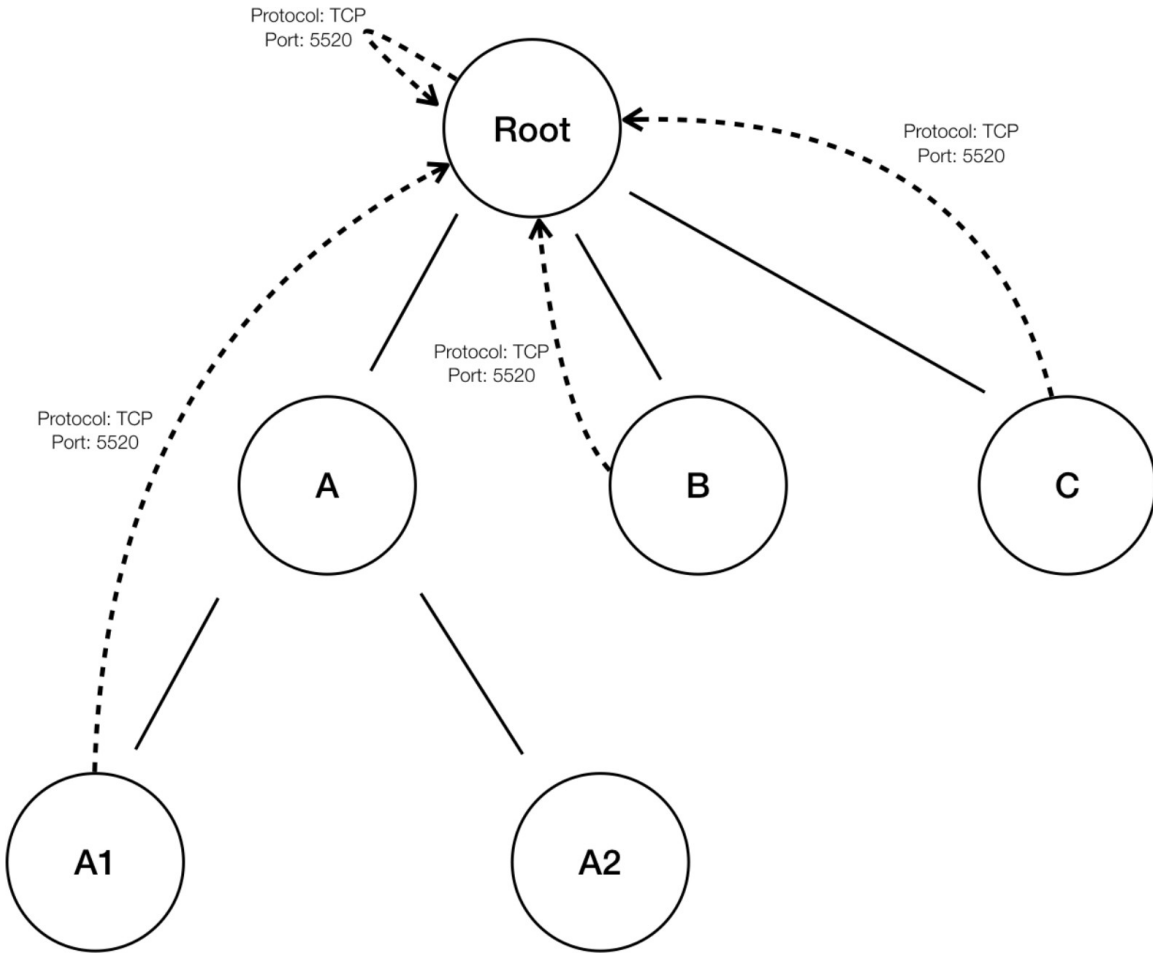
このオプションは、冗長な詳細ポリシーの削除を有効/無効にします。

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。

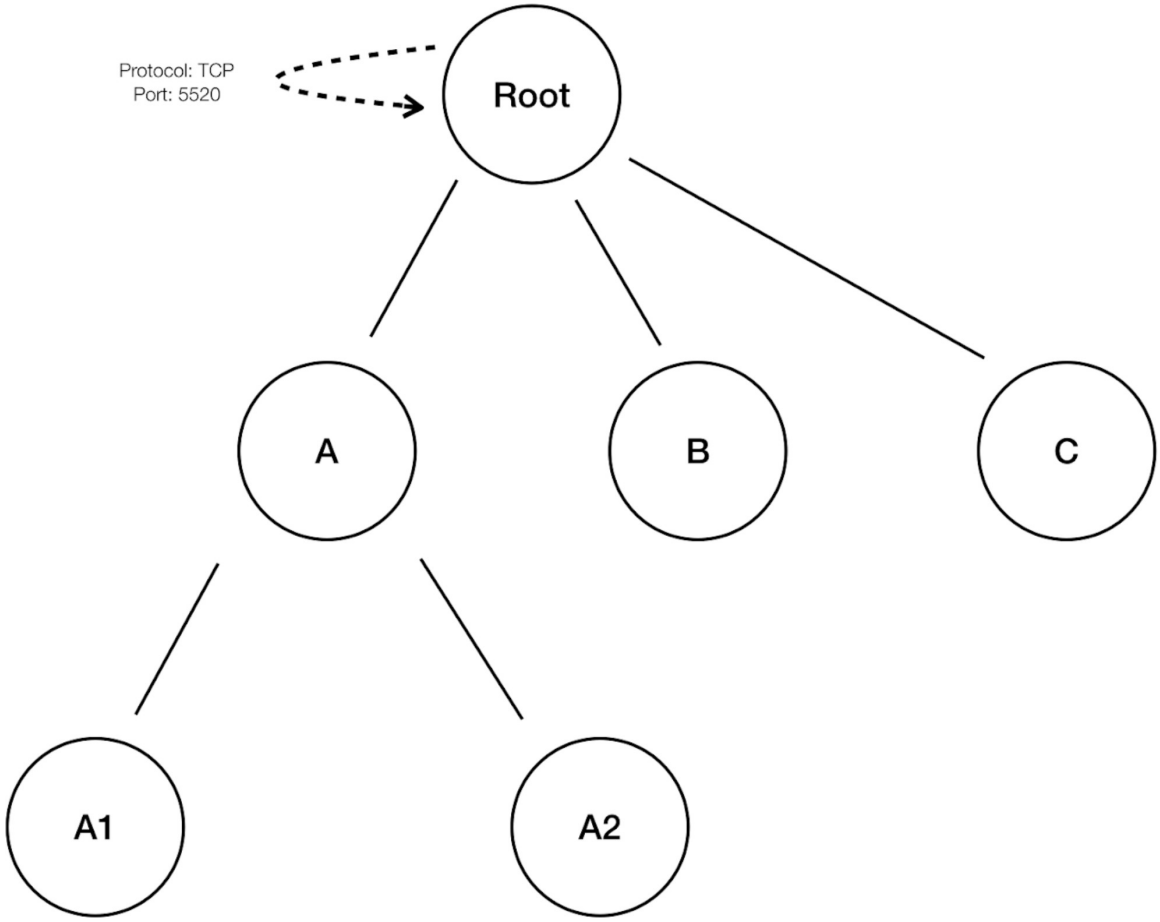
  1. “Root” → “Root”
  2. “B” → “Root”
  3. “C” → “Root”
  4. “A1” → “Root”

図 *17:* 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 *18 :* 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　範囲ツリーのブランチのポリシーの検出は、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。

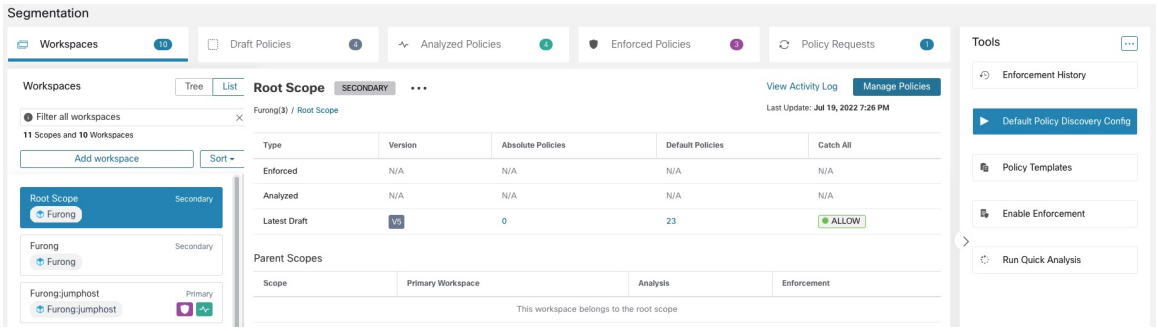
デフォルトのポリシー検出設定

ルート範囲全体の任意のワークスペースでオプションで使用できる、デフォルトの自動ポリシー検出設定を設定することができます。

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 *19 : [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 （37 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 （42 ページ） およびサブトピック
- デフォルトの除外フィルタ （53 ページ）

重要　デフォルト設定が完了し、個々のワークスペースで使用する準備ができたら、[保存（Save）] をクリックします。

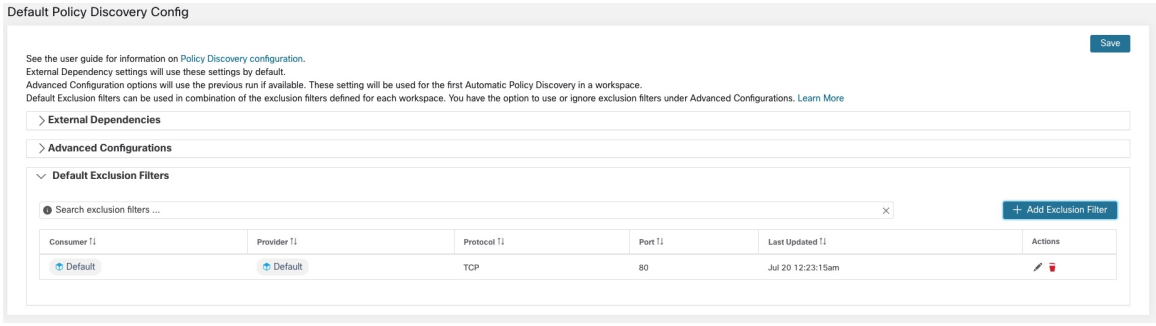
デフォルトの除外フィルタ

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 *20*：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（34 ページ）」を参照してください。

デフォルトの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 （37 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「ポリシーの検出時にロードバランサとルータからのデータを含める （42 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 BIG-IP

`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。

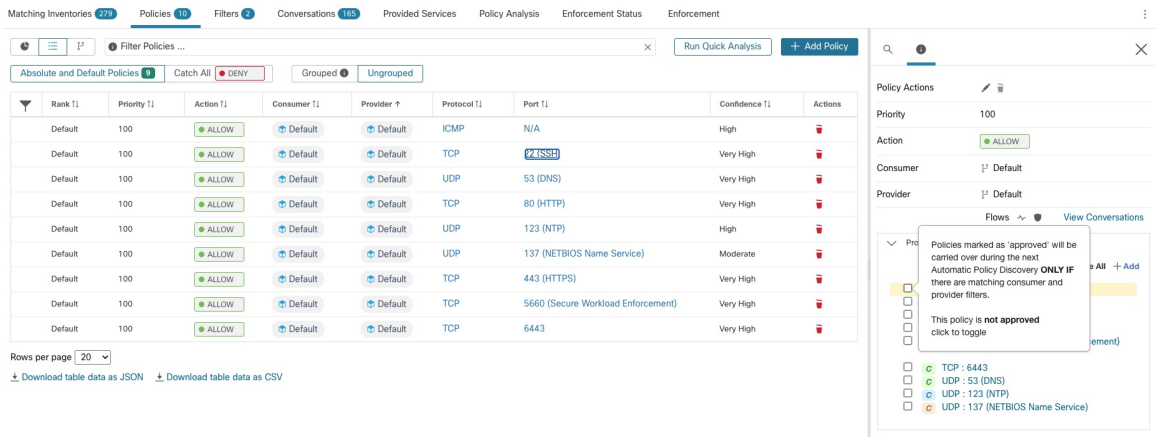
ポリシーの承認

ポリシー検出の結果を確認しているときに、検出されたポリシーのうち保持したいものを承認すると、その後ポリシーを検出したときにそのポリシーがそのまま引き継がれます。詳細については、承認済みポリシー （54 ページ）を参照してください。

ポリシーを承認するには、次の手順を実行します。

1. [ポリシー（Policies）] ページで、保護するポリシーの [プロトコルとポート（Protocols and Ports）] 列の値をクリックします。
2. 右側に表示されるパネルで、今後のポリシー検出時にポリシーを保持する各プロトコルとポートの左側にあるチェックボックスを選択します。

図 *21* : ポリシーの承認



この手順を使用して、ポリシーから承認を削除することもできます。

承認済みポリシー

一般的に、承認済みポリシーは自動ポリシー検出中に変更されず、自動ポリシー検出では、承認済みポリシーの効果と重複するポリシーは提案されません。

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の自動ポリシー検出中に変更されないようにします。ポリシーの承認 （54 ページ） を参照してください。）
- 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）。
- 親および先祖の範囲で（特に、プライマリワークスペースの最新バージョンから）定義された、この範囲内のワークロードに適用される承認済みポリシー。
- 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 （103 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。たとえば、提供されるサービス （116 ページ） タブから含まれるポリシーが含まれます。

ポリシーのポートやプロトコルのリンクをクリックして、ページの右側のパネルに詳細を表示すると、プロトコルタイプの横にある親指アイコンで承認済みポリシーが示されます。

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、受け入れられたポリシー要求（クロス範囲ポリシーの場合）、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。

また、デフォルトで有効になっている自動ポリシー検出の詳細設定もあります。承認済みポリシーを変更から保護しない場合は、ワークスペースまたはグローバルのデフォルトポリシー検出設定についてこのオプションの選択を解除できます。承認されたポリシーの引き継ぎ （49 ページ） を参照してください。

承認されたポリシーの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、ページの右側に表示されるポリシーの詳細ビューで、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の結果を調べることもできます。これを行うには、ポリシー内のポートとプロトコルのリンクをクリックして、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ます（適切なアイコンを見つけるには、アイコンにカーソルを合わせます）。

反復的なポリシーの変更

単一の範囲およびネットワーク全体のポリシーの定義と調整は、反復的なプロセスになります。

検出されたポリシーと手動で作成されたポリシーの両方を変更できます。

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、または役に立たない情報を除外することです。たとえば、以下を行うことができます。

- 追加のエージェントをインストールするか、追加のコネクタを設定して、一部のフローデータが蓄積されるようにする。
- 検出に使用する期間を長くして、より多くのデータを含める。
- （最初に編集するかどうかに関係なく）クラスタを承認する。これにより、再実行時に他のワークロードのクラスタリングを改善できます。クラスタの承認 （93 ページ）を参照してください。
- ポリシーに影響を与えないことがわかっているフローを除外して、編集の必要をなくす。除外フィルタ （33 ページ）を参照してください。
- 詳細設定を変更する（詳細については、自動ポリシー検出の詳細設定 （42 ページ）を参照してください）。
- ポリシーの複雑さの対処 （95 ページ）に変更を加えた後に変更をキャプチャする。

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、ワークスペース内に異なるクラスタとポリシーが生成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。

（注） ポリシー検出中に変更されないポリシーのタイプのリストについては、承認済みポリシー（54ページ）を参照してください。

（注） 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。

重要：自動ポリシー検出を再実行する前に

重要 ワークスペースでポリシーを再検出する前に、次の各項目に対処します。

- デフォルトでは、特定のワークスペースでポリシーを検出するたびに、以前に検出されたポリシーとクラスタのセットは、新しい検出期間に含まれているデータに基づいて上書きされます。一部のポリシーとクラスタを保持し、他は保持しない場合は、保持するポリシーとクラスタを承認します。
- 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」またはクラスタの承認 （93 ページ）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、ポリシーの承認 （54 ページ） を参照してください。
- 変更しない限り、以前の検出実行で設定された既存の [詳細設定（Advanced Configuration）] の設定が使用されます。

  ただし、設定されたデフォルトの外部依存関係は、以前の実行の依存関係よりも優先して使用されます。
- 検出されたポリシーの現在表示されているバージョンが最新バージョンではなく、以前に検出されたバージョンを保持する場合は、ページの上部に表示されているバージョンをクリックし、最新の v* バージョンを選択します。

  以前のバージョンが表示されている場合は、そのバージョンと新しく検出されたバージョンの間のバージョンが削除されます。

  詳細は、検出されたポリシーバージョンの表示、比較、および管理 （58 ページ）を参照してください。

ポリシー検出を再実行するには、ポリシーの自動検出 （31 ページ）を参照してください。このトピックの項目に対処した後は、ポリシーを検出するたびに同じプロセスになります。

検出されたポリシーバージョンの表示、比較、および管理

ワークスペースでポリシーを検出するたびに、一連のポリシーに割り当てられたバージョン番号（v*）が増加します。

詳細については、ポリシーバージョン（v* および p*）について （161 ページ） を参照してください。

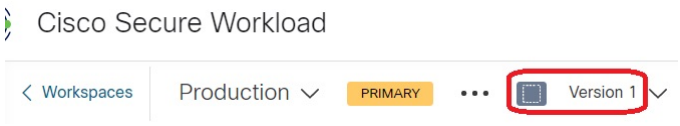
手順

ステップ 1 [防御（Defend）] > [セグメンテーション（Segmentation）] をクリックします。

ステップ 2 ワークスペースに移動します。

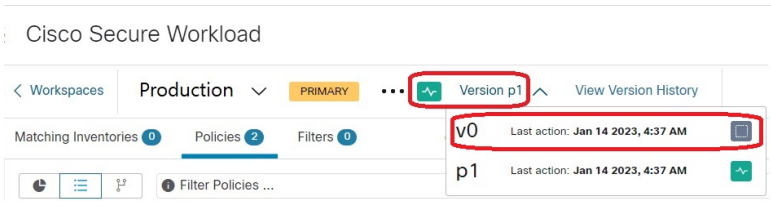
ステップ 3 [ポリシーの管理（Manage Policies）] をクリックします。

ステップ 4 自動ポリシー検出によって生成された、現在表示されているポリシーのバージョンがページの上部に表示されます。



すでにポリシーを分析または適用している場合、表示されるバージョンには、ポリシー検出バージョン、分析されたポリシーバージョン、または適用されたバージョンがあります。

ステップ 5 次のいずれかを実行します。

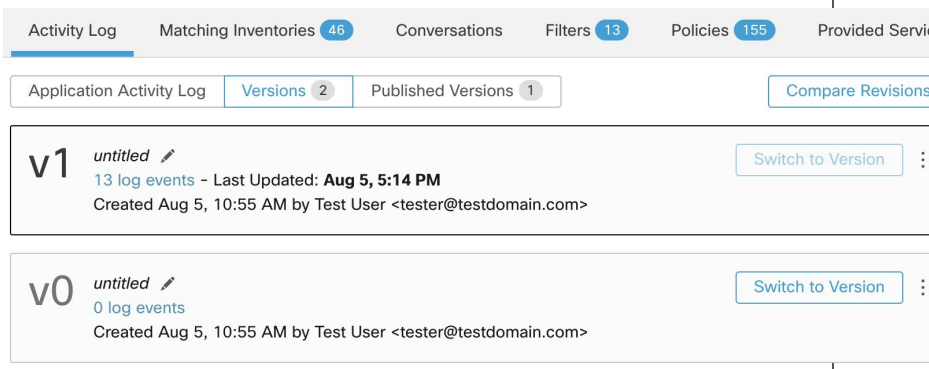
自動ポリシー検出によって生成された別のバージョンのポリシーを表示する。	現在のバージョンをクリックし、別の v* バージョンを選択します。 （p* バージョンが表示されている場合、それらは検出されたポリシーのバージョンではなく、分析されたバージョンや適用されたバージョンです）。  **重要**：この手順の最後にある「次の作業」の項の注意事項を参照してください。

バージョンに関する詳細を表示する。	

1. ページ上部の現在のバージョンの横にある [バージョン履歴の表示（View Version History）] をクリックします。
2. [バージョン（Versions）] タブをクリックして、検出されたポリシーのバージョンを表示します（[公開されたバージョン（Published Versions）] タブではありません）。

   バージョンのリストが表示されます。

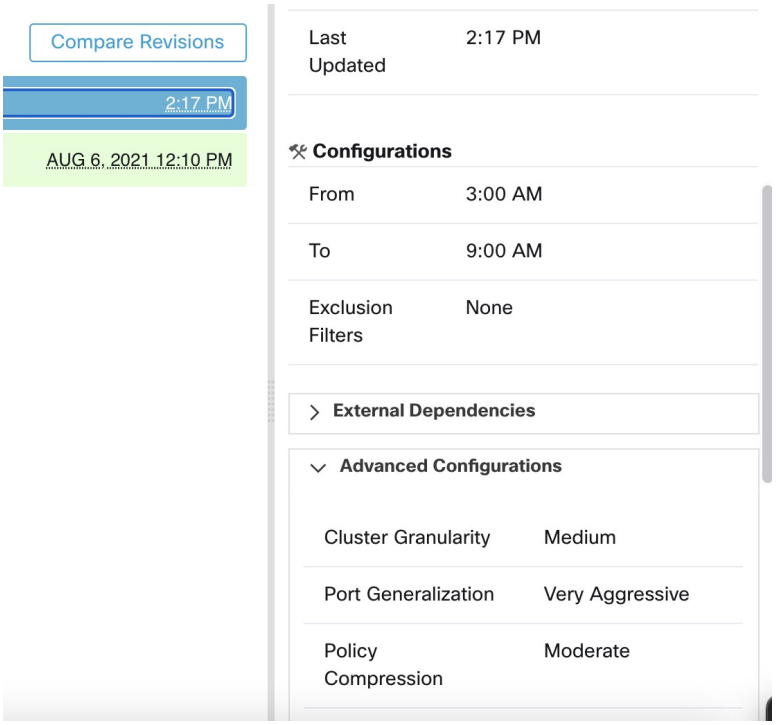
   図 *22*：概要情報を含む生成されたポリシーバージョンのリスト



3. バージョンの [ログイベント（log events）] リンクをクリックします。
4. イベント行のリンクをクリックします。

   使用可能な詳細には、統計、除外フィルタ、外部依存関係、および実行の設定があります。

   図 *23*：特定の自動ポリシー検出の実行に使用される設定

	
2 つのバージョンを比較して変更点を確認する。	**1.** [リビジョンの比較（Compare Revisions）] をクリックします。 **2.** 比較するバージョンを選択します。 **3.** 結果の詳細については、ポリシーバージョンの比較：ポリシーの差分（164 ページ）を参照してください。
不要なバージョンを削除する。	バージョンの ⋮ をクリックし、[削除（Delete）] を選択します。 自動ポリシー検出によって生成された（v* バージョンの）最後に残っているバージョンは、削除できません。
バージョンをエクスポートする。	バージョンの ⋮ をクリックし、[エクスポート...（Export...）] を選択します。

次のタスク

重要 検出されたポリシーの以前のバージョンを保持する場合は、古いバージョンでの作業が完了したときに、検出されたポリシーの現在のバージョンを常に表示します。

次にこのワークスペースのポリシーを検出したときに、検出されたポリシーの最新バージョンが表示されていない場合は、古いバージョンが削除される可能性があります。

たとえば、検出されたポリシーの最新バージョンが v4 であり、ポリシーを再度検出したときに v2 が表示されている場合、既存の v3 と v4 が削除され、新しく検出されたポリシーのバージョンは v3 になります。

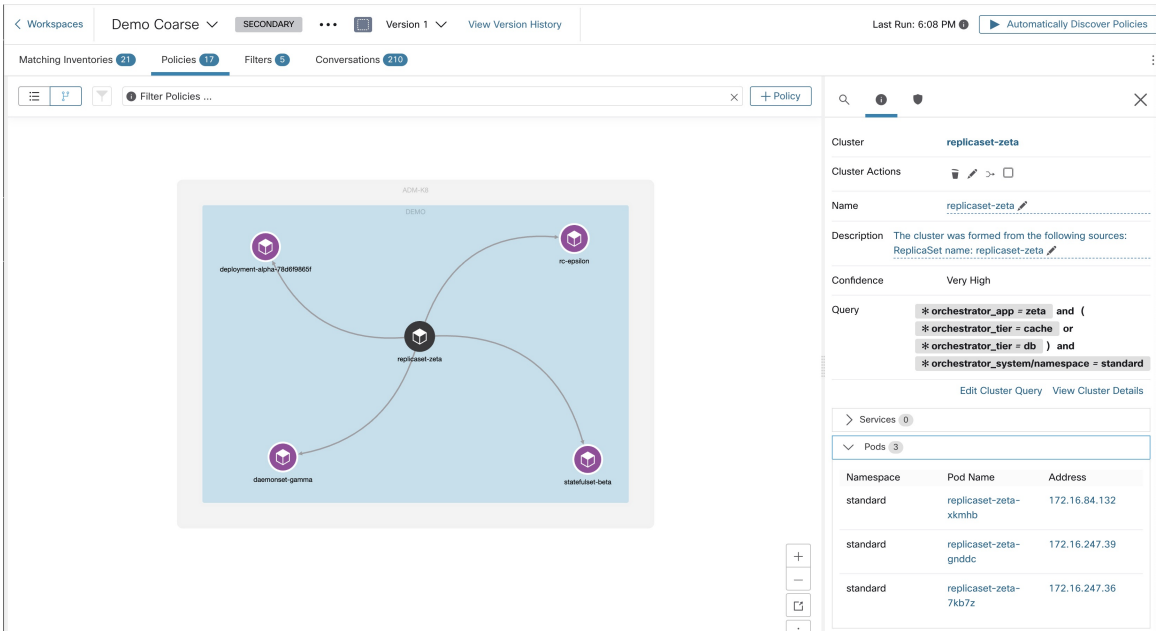
この動作により、バージョン履歴が直線的になり、必要に応じて以前のバージョンに簡単に戻すことができます。

さらに、最新の v* バージョンが表示されている場合にのみ、ポリシーを手動で作成することができます。

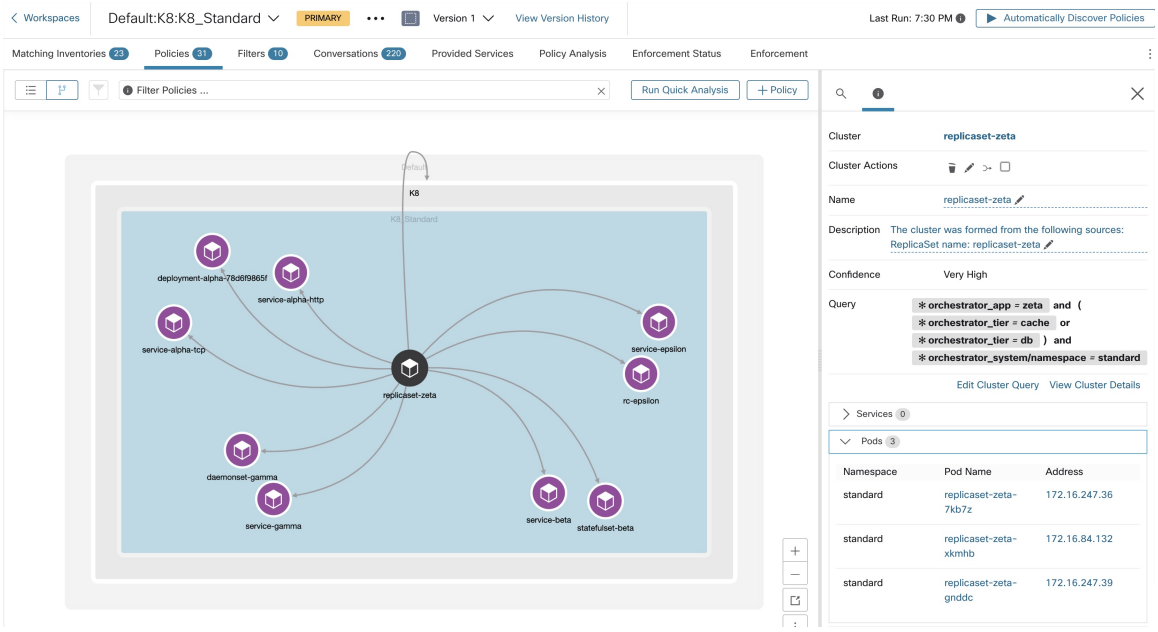
ポリシー検出の Kubernetes のサポート

ポリシー検出では、Kubernetes 設定のポッドとサービスに関する情報が使用されて、ポッドとサービス両方のクラスタが作成され、それぞれのポリシーが生成されます。

クラスタ粒度が粗いまたは非常に粗いに設定されている場合、サービスとそれらを支援するポッドが一緒にクラスタ化されます。



クラスタ粒度が、中、細かい、または非常に細かいに設定されている場合、サービスとそれらを支援するポッドが個別にクラスタ化されます。



ポッドクラスタの場合は、ソース情報がクラスタの説明の一部として追加され、説明の各クラスタには、クラスタが形成される原因となったエンティティの情報が含まれます。

たとえば、[説明（Description）]：「このクラスタは次のソースから形成されました：ReplicaSet 名前：replicaset-zeta（The cluster was formed from the following sources: ReplicaSet name: replicaset-zeta）」などです。

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。

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

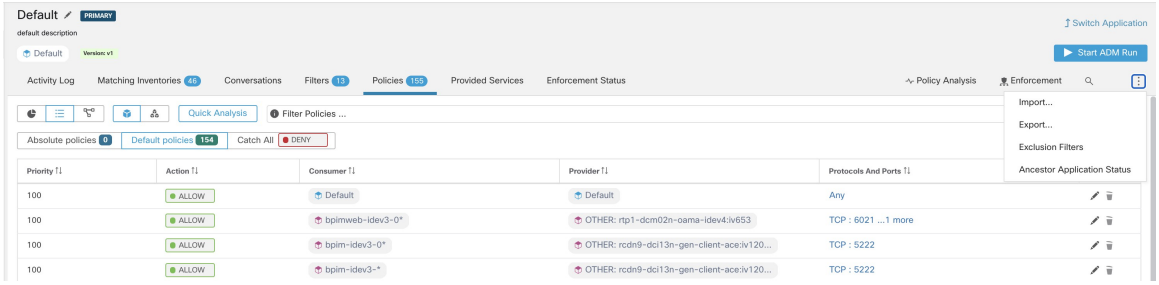
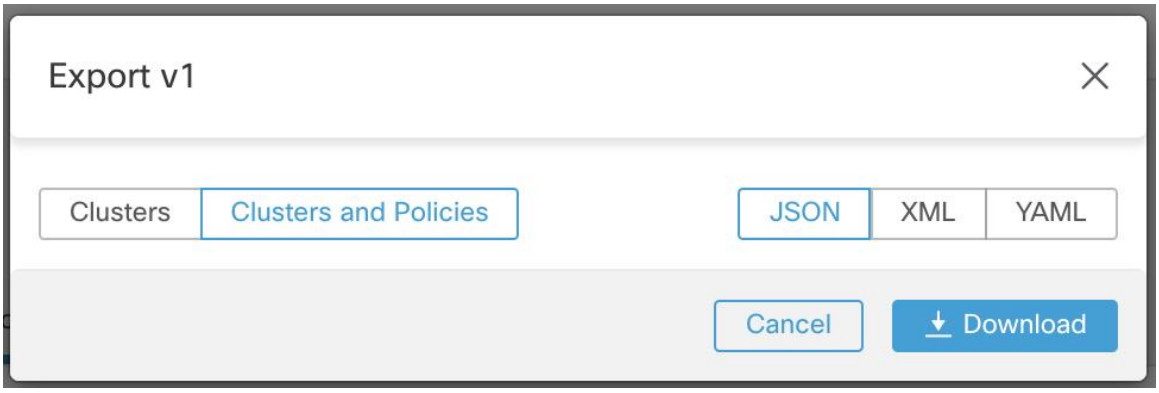


図 *25 :* ワークスペースのポリシーのエクスポート



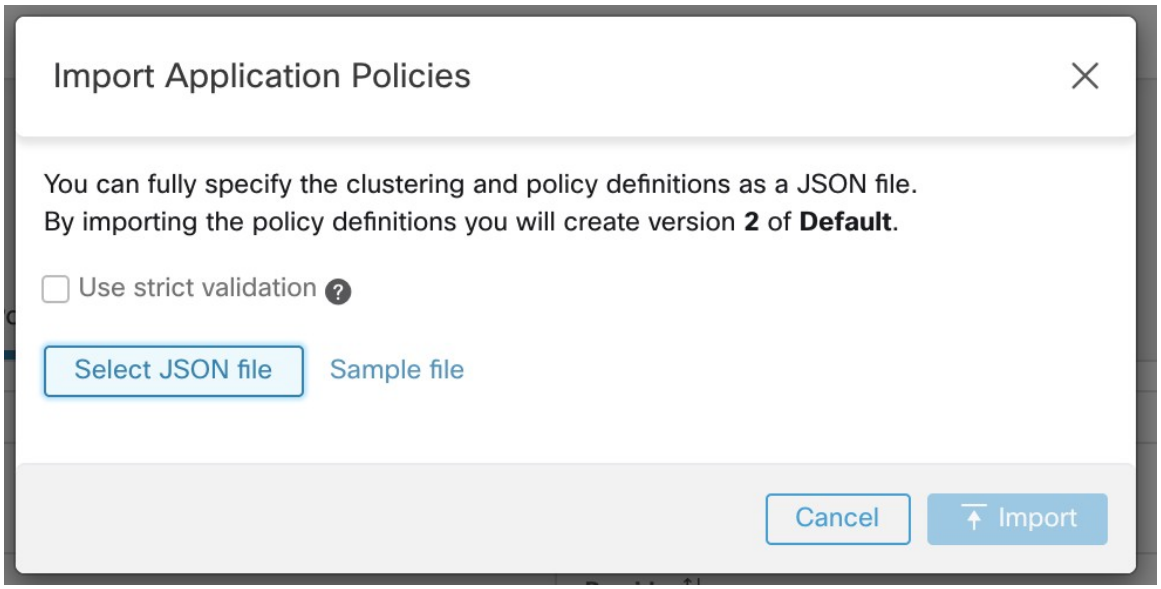
ワークスペースをエクスポートすると、自動ポリシー検出構成の [発信ポリシーコネクタの自動承諾（Auto accept outgoing policy connectors）] 設定が含まれ、インポートされたワークスペースでアクティブになります。

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 *26 :* 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 （54 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。

プラットフォーム固有のポリシー

エージェントが各プラットフォームでポリシーを適用する方法に関する重要な詳細については、エージェントによるポリシーの適用を参照してください。Kubernetes/OpenShift については、コンテナへの適用 （151 ページ）を参照してください。

Windows

Windows OS ベースの推奨ポリシー設定

可能な場合は、常にポリシーでポートとプロトコルを指定します。任意のポート、任意のプロトコルを許可することはお勧めしません。

たとえば、ポートとプロトコルの制限を含めて生成されたポリシーは次のようになります。

```
 dst_ports {
  start_port: 22
  end_port: 22
  consumer_filters {
    application_name: "c:\\test\\putty.exe"
  }
 }}
 ip_protocol: TCP
```

対照的に、任意のプロトコルと任意のポートを使用して iperf.exe によって開始されたネットワーク接続を許可する場合、生成されるポリシーは次のようになります。

```
match_set {
  dst_ports {
    end_port: 65535
    consumer_filters {
      application_name: "c:\\test\\iperf.exe"
    }
  }
  address_family: IPv4
  inspection_point: EGRESS
  match_comment: "PolicyId=61008290755f027a92291b9d:61005f90497d4f47cedacb86:"
}
```

上記のフィルタの場合、Secure Workload はプロバイダーのネットワークトラフィックを許可するポリシールールを次のように作成します。

```
match_set {
    dst_ports {
    end_port: 65535
  }
  address_family: IPv4
  inspection_point: INGRESS
  match_comment: "PolicyId=61008290755f027a92291b9d:61005f90497d4f47cedacb86:"
}
```

このネットワークルールは、プロバイダーのすべてのポートを開きます。任意のプロトコルを使用して OS ベースのフィルタを作成しないことをお勧めします。

Windows 属性のポリシーの設定

Windows ベースのワークロードにポリシーを適用する際の精度をさらに高めるために、次の方法でネットワークトラフィックをフィルタリングできます。

- アプリケーション
- サービス名（Service Name）

- ユーザー名（ユーザーグループありまたはなし）

これは、WAF および WFP モードでサポートされています。Windows OS ベースのフィルタは、生成されたネットワークポリシーでコンシューマフィルタとプロバイダーフィルタに分類されます。コンシューマフィルタは、コンシューマワークロードで開始されたネットワークトラフィックをフィルタリングします。プロバイダーフィルタは、プロバイダーワークロード宛てのネットワークトラフィックをフィルタリングします。

始める前に

この手順は、既存のポリシーを変更していることが前提となります。Windows OS ベースのフィルタを追加するポリシーを作成していない場合は、最初にそのポリシーを作成します。

重要 Windows 属性を含むポリシーについては、警告および既知の制限事項を参照してください。

手順

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 Windows OS ベースのフィルタを設定するポリシーを含む範囲をクリックします。

ステップ 3 ポリシーを編集するワークスペースをクリックします。

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

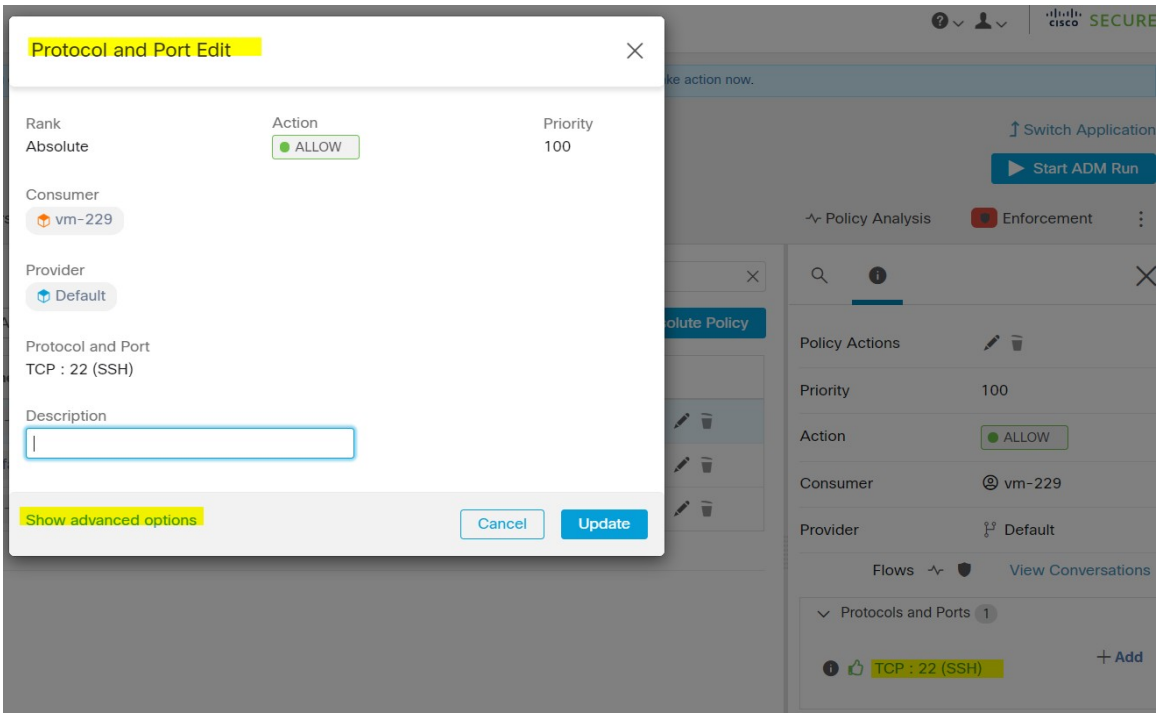
ステップ 5 編集するポリシーを選択します。

重要コンシューマとプロバイダーには、Windows ワークロードのみを含める必要があります。

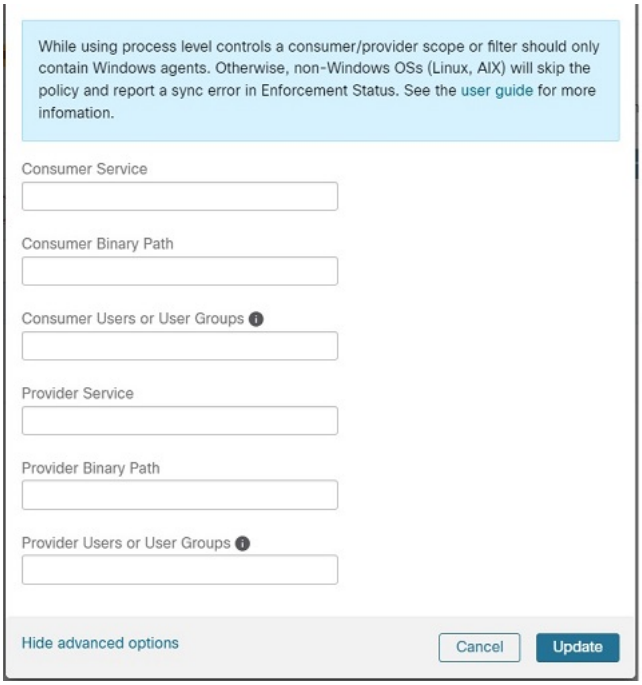
ステップ 6 編集するポリシーのテーブル行で、[プロトコルとポート（Protocols and Ports）] 列の既存の値をクリックします。

ステップ 7 右側のペインで、[プロトコルとポート（Protocols and Ports）] の下にある既存の値をクリックします。

この例では、[TCP : 22 (SSH)] をクリックします。



ステップ 8 [詳細オプションの表示（Show advanced options）] をクリックします。



ステップ 9 アプリケーション名、サービス名、またはユーザー名に基づいてコンシューマフィルタを設定します。

- アプリケーション名はフルパス名にする必要があります。

- サービス名は短いサービス名にする必要があります。
- ユーザー名は、ローカルユーザー名（tetter など）またはドメインユーザー名（sensor-dev@sensor-dev.com、sensor-dev\sensor-dev など）にできます。
- ユーザーグループは、ローカルユーザーグループ（管理者など）またはドメインユーザーグループ（domain users\\sensor-dev など）にできます。
- 複数のユーザー名および（または）ユーザーグループ名は「,」で区切って指定できます（例：sensor-dev\@sensor-dev.com,domain users\\sensor-dev）。
- サービス名とユーザー名は同時に設定できません。

ステップ 10 アプリケーション名、サービス名、またはユーザー名に基づいてプロバイダーフィルタを設定します。

前のステップのコンシューマフィルタと同じガイドラインに従います。

ステップ 11 必要に応じてバイナリへのパスを入力します。

たとえば、**`c:\test\putty.exe`** と入力します。

ステップ 12 [更新（Update）]をクリックします。

既知の制限事項

- Windows 2008 R2 は、Windows OS ベースのフィルタリングポリシーをサポートしていません。
- ネットワークポリシーは単一のユーザー名で設定できますが、MS Firewall UI は複数のユーザーをサポートします。

警告

- Windows OS ベースのポリシーを使用している場合、コンシューマやプロバイダーの範囲またはフィルタには Windows エージェントのみを含める必要があります。そうしないと、Windows 以外の OS（Linux、AIX）ではポリシーがスキップされ、適用ステータスで同期エラーが報告されます。
- フィルタリング基準が緩い Windows OS フィルタを作成しないでください。不要なネットワークポートが開く可能性があります。
- ネットワークフローのプロセスコンテキスト、ユーザーコンテキスト、またはサービスコンテキストに関する知識が乏しいか、知識がまったくないために、ポリシーに Windows OS ベースのフィルタがある場合、ポリシー分析に矛盾が生じます。

Windows OS ベースのフィルタリング属性を使用したポリシーの確認とトラブルシューティング

Windows OS ベースのフィルタリング属性を使用する場合は、次のトピックを使用して、ポリシーが期待どおり動作することをワークロードで確認します。

Cisco TAC は、必要に応じてこの情報を使用して、このようなポリシーのトラブルシューティングを行うことができます。

アプリケーション名に基づくポリシー

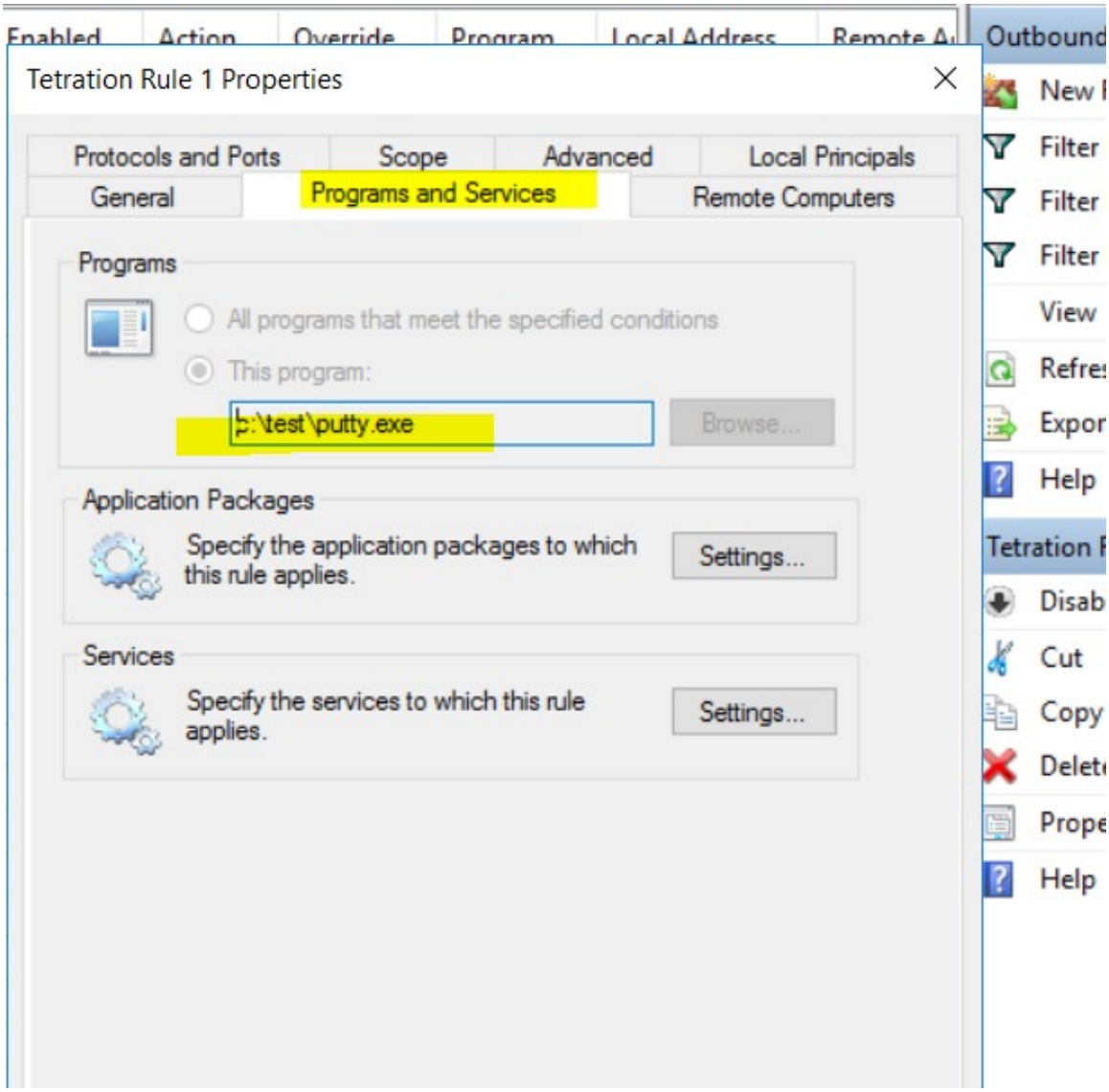
次の情報を使用して、アプリケーション名に基づく Windows OS ワークロードのポリシーを確認およびトラブルシューティングします。

次のセクションでは、**c:\test\putty.exe** として入力されたアプリケーションバイナリのワークロードにポリシーを表示させる方法について説明します。

アプリケーション名に基づくポリシーの例

```
dst_ports {
start_port: 22
end_port: 22
consumer_filters {
application_name: “c:\test\putty.exe”
}
}}
ip_protocol: TCP
address_family: IPv4
inspection_point: EGRESS
```

生成されたファイアウォールルール



netsh を使用して生成されたフィルタ

高度なポリシーにフィルタが追加されていることをネイティブの Windows ツールで確認するには、次の手順を実行します。

- 「管理者」権限を使用して「cmd.exe」を実行します
- 「netsh wfp show filters」を実行します
- 出力ファイル filters.xml が、現在のディレクトリに生成されます。
- 出力ファイル（filters.xml）の FWPM_CONDITION_ALE_APP_ID でアプリケーション名を確認します。

```
<fieldKey>FWPM_CONDITION_ALE_APP_ID</fieldKey>
                      <matchType>FWP_MATCH_EQUAL</matchType>
                      <conditionValue>
                             <type>FWP_BYTE_BLOB_TYPE</type>
                             <byteBlob>
                                    <data>
‹→5c00640065007600690063006500 5c006800610072006400640069007300 6b0076006f006
‹→</data>
                                 <asString>\device\harddiskvolume2\temp\putty.exe</
‹→asString>
                 </byteBlob>
        </conditionValue>
```

tetenf.exe -l -f を使用して生成された WFP フィルタ

```
Filter Name:                    Secure Workload Rule 1
---------------------------------------------------------
EffectiveWeight:                18446744073709551592
LayerKey:                       FWPM_LAYER_ALE_AUTH_CONNECT_V4
Action:                         Permit
RemoteIP:                       10.195.210.15-10.195.210.15
Remote Port:                    22
Protocol:                       6
AppID:                          \device\harddiskvolume2\test\putty.exe
```

アプリケーション名が無効な場合

- WAF モードでは、無効なアプリケーション名に対してファイアウォールルールが作成されます。
- WFP モードでは、無効なアプリケーション名に対して WFP フィルタは作成されませんが、NPC は拒否されません。エージェントは警告メッセージをログに記録し、残りのポリシールールを構成します。

サービス名に基づくポリシー

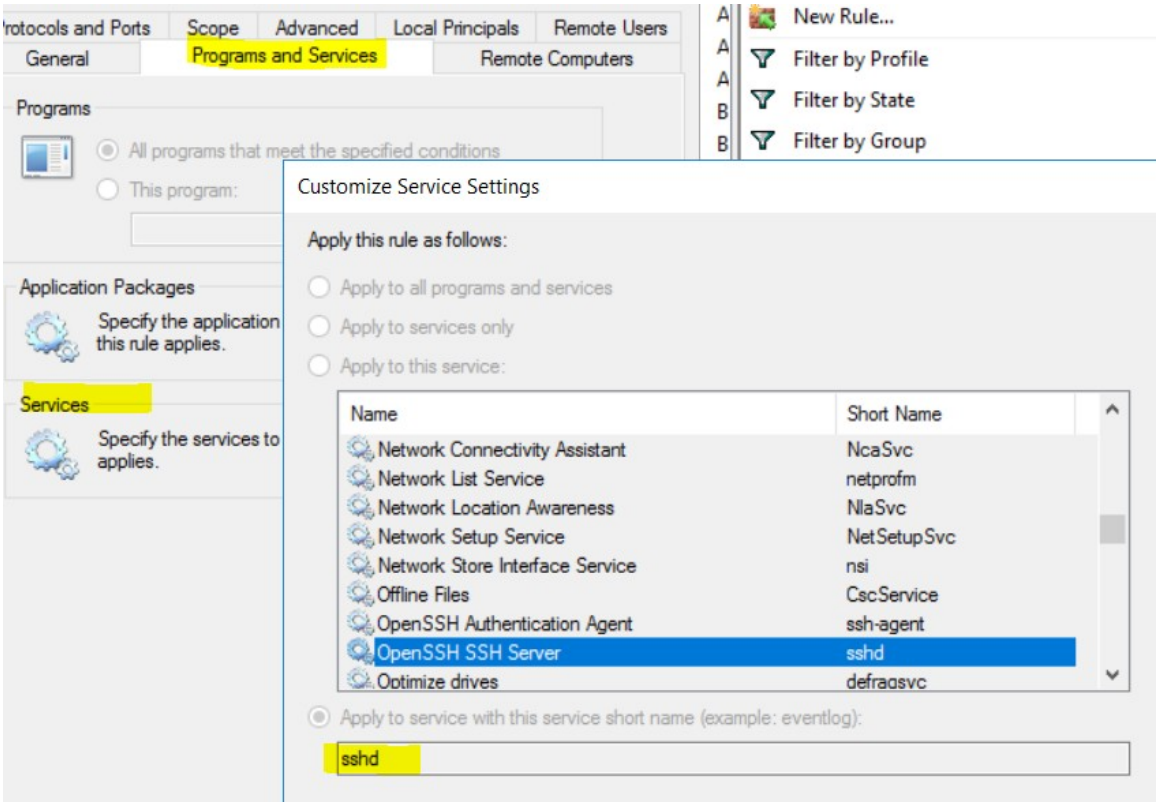
次の情報を使用して、サービス名に基づく Windows OS ワークロードのポリシーを確認およびトラブルシューティングします。

次のセクションでは、ワークロードにポリシーを表示させる方法について説明します。

サービス名に基づくサンプルポリシー

```
    dst_ports {
             start_port: 22
             end_port: 22
             provider_filters {
                    service_name: "sshd"
             }
         }}
         ip_protocol: TCP
         address_family: IPv4
         inspection_point: INGRESS
```

生成されたファイアウォールルール



netsh を使用して生成されたフィルタ

高度なポリシーにフィルタが追加されていることをネイティブの Windows ツールで確認するには、次の手順を実行します。

- 「管理者」権限を使用して「cmd.exe」を実行します
- 「netsh wfp show filters」を実行します
- 出力ファイル filters.xml が現在のディレクトリに生成されます
- 出力ファイル（filters.xml）でユーザー名の FWPM_CONDITION_ALE_USER_ID を確認します。

```
<item>
                    <fieldKey>FWPM_CONDITION_ALE_USER_ID</fieldKey>
                    <matchType>FWP_MATCH_EQUAL</matchType>
                    <conditionValue>
                              <type>FWP_SECURITY_DESCRIPTOR_TYPE</type>

<sd>O:SYG:SYD:(A;;CCRC;;;S-1-5-80-3847866527-469524349-687026318-
→516638107)</sd>
                    </conditionValue>
</item>
```

tetenf.exe -l -f を使用して生成された WFP フィルタ

```
Filter Name:       Secure Workload Rule 3
-----------------------------------------------------
EffectiveWeight:            18446744073709551590
LayerKey:                   FWPM_LAYER_ALE_AUTH_RECV_ACCEPT_V4
Action:                     Permit
Local Port:                 22
Protocol:                   6
User or Service:            NT SERVICE\sshd
```

サービス名が不正な場合

- WAF モードで、存在しないサービス名に対してファイアウォールルールが作成されます
- WFP モードでは、存在しないサービス名に対して WFP フィルタは作成されません
- サービス SID タイプは「無制限」または「制限付き」である必要があります。サービスの種類が「なし」の場合、ファイアウォールルールと WFP フィルタを追加できますが、効果はありません。

  SID タイプを確認するには、次のコマンドを実行します。

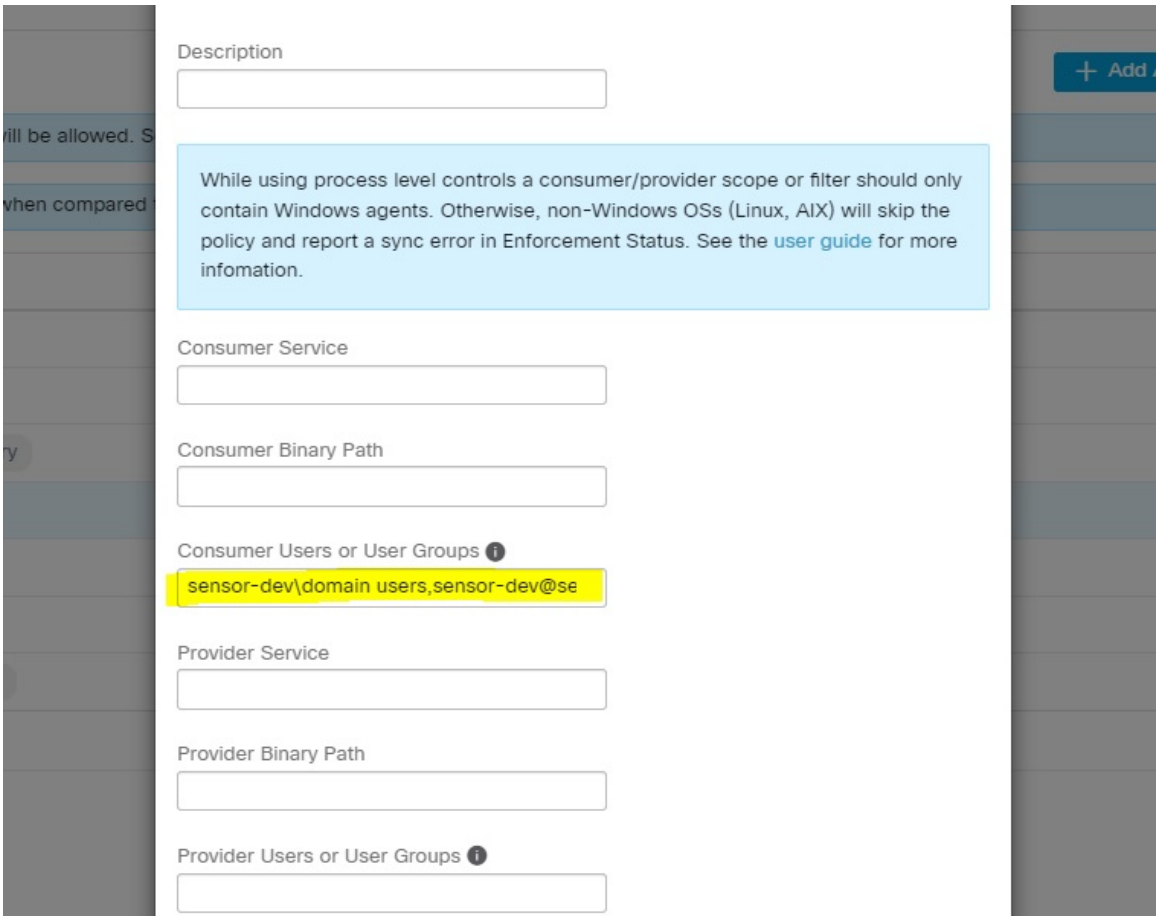
  ```
  sc qsidtype <service name>
  ```

ユーザーグループまたはユーザー名に基づくポリシー

次の情報を使用して、ユーザーグループ名の有無にかかわらず、ユーザー名に基づく Windows OS ワークロードのポリシーを確認およびトラブルシューティングします。

このトピックのセクションでは、ワークロードにポリシーを表示する方法について説明します。

このトピックの例は、次の情報を使用して設定されたポリシーに基づいています。



ユーザー名に基づくサンプルポリシー

```
dst_ports {
          start_port: 30000
          end_port: 30000
          provider_filters {
               user_name: “sensor-dev\sensor-dev”
           }
}}
ip_protocol: TCP
address_family: IPv4
inspection_point: EGRESS
```

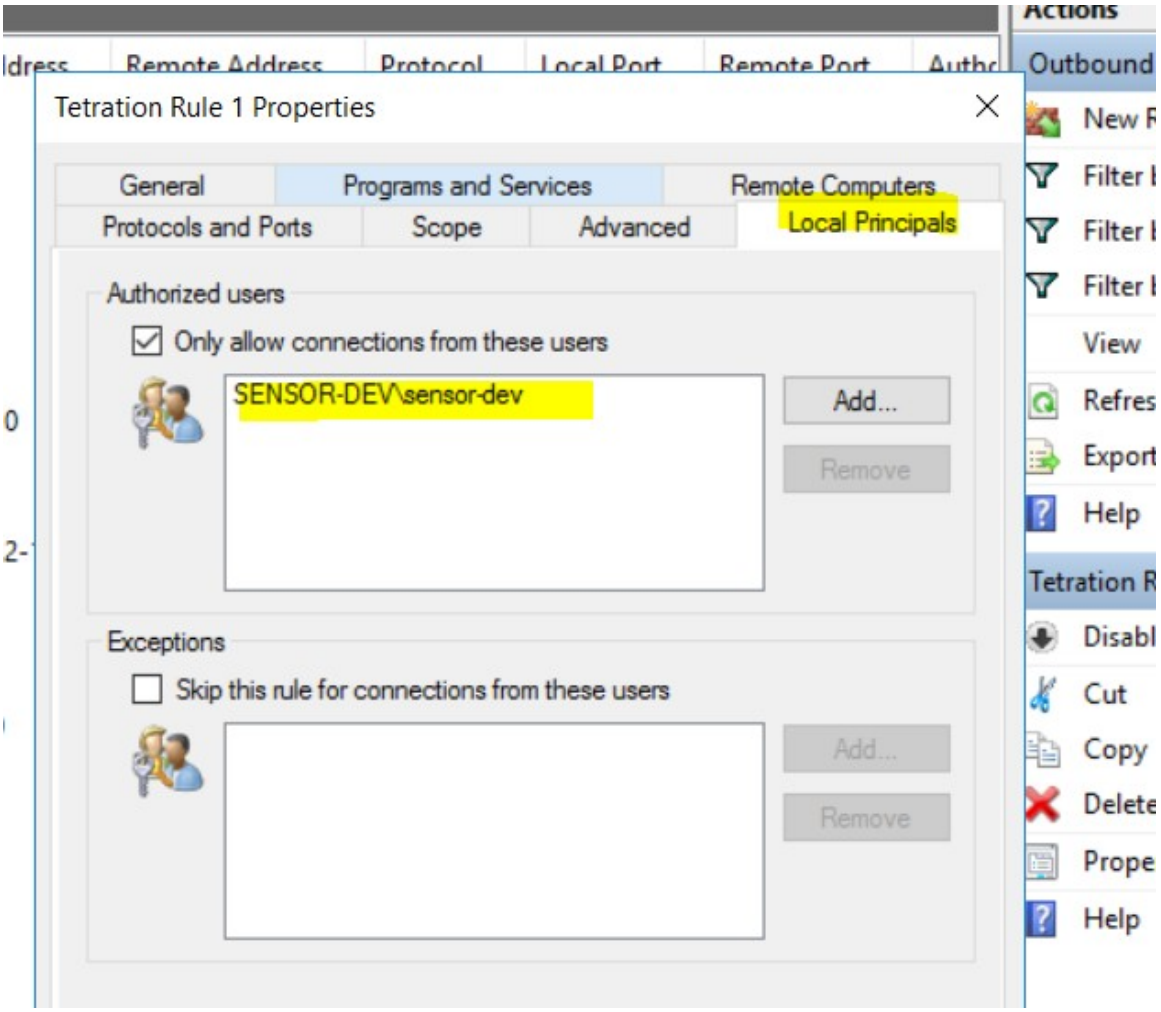
ユーザーグループとユーザー名に基づくサンプルポリシー

```
dst_ports {
start_port: 30000
end_port: 30000
provider_filters {
user_name: “sensor-dev\domain users,sensor-dev\sensor-dev”
}
}}
ip_protocol: TCP
address_family: IPv4
inspection_point: EGRESS
```

生成されたファイアウォールルール

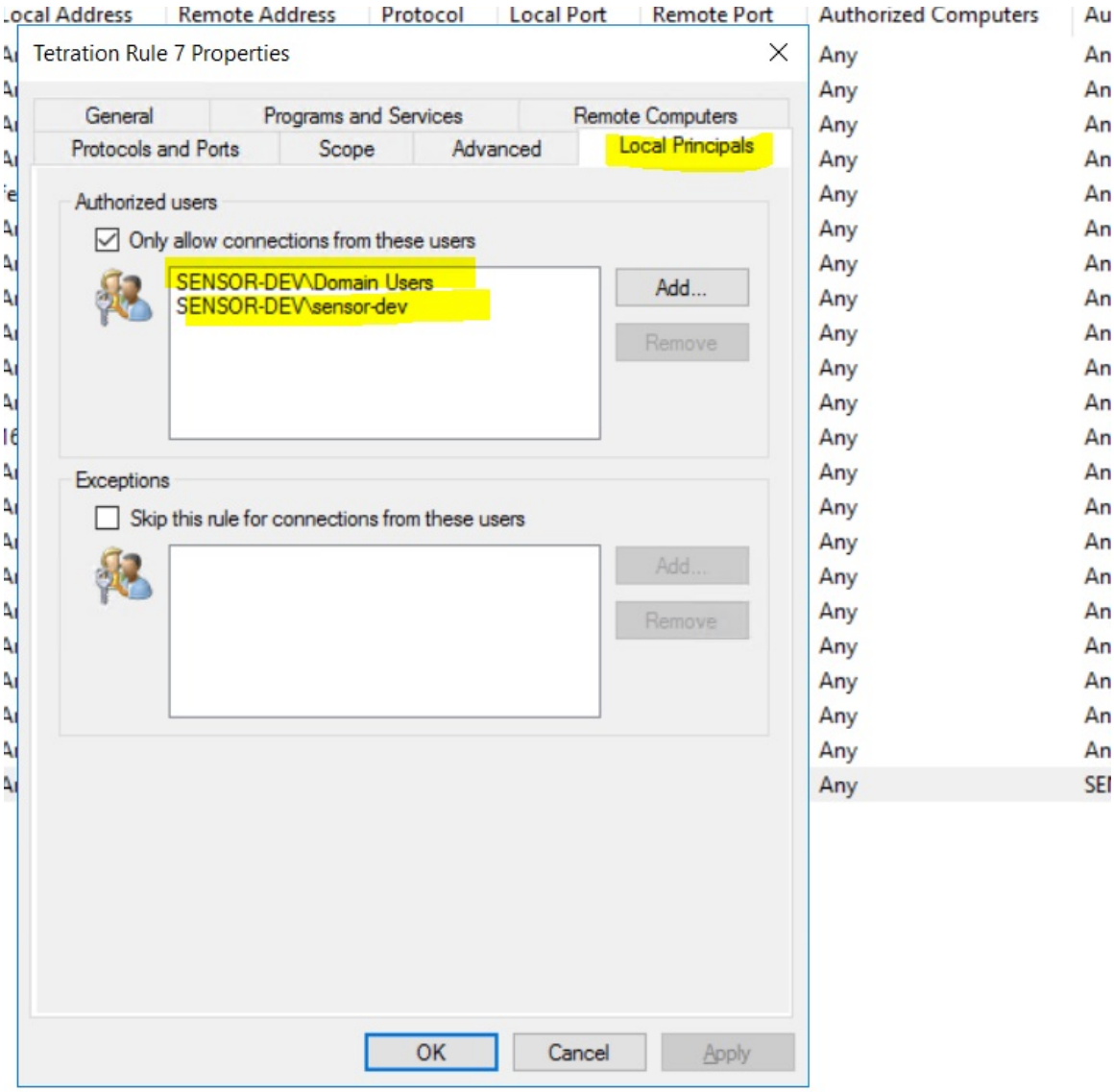
ユーザー名に基づくファイアウォールルール

例：ユーザー名 sensor-dev\\sensor-dev に基づくファイアウォールルール



ユーザーグループとユーザー名に基づくファイアウォールルール

例：ユーザー名 sensor-dev\\sensor-dev およびユーザーグループ domain users\\sensor-dev に基づくファイアウォールルール



netsh を使用して生成されたフィルタ

高度なポリシーにフィルタが追加されていることをネイティブの Windows ツールで確認するには、次の手順を実行します。

- 「管理者」権限を使用して「cmd.exe」を実行します
- 「netsh wfp show filters」を実行します
- 出力ファイル filters.xml が、現在のディレクトリに生成されます。
- 出力ファイル（filters.xml）でユーザー名の FWPM_CONDITION_ALE_USER_ID を確認します。

```
<item>
            <fieldKey>FWPM_CONDITION_ALE_USER_ID</fieldKey>
            <matchType>FWP_MATCH_EQUAL</matchType>
            <conditionValue>
                   <type>FWP_SECURITY_DESCRIPTOR_TYPE</type>
                  <sd>O:LSD:(A;;CC;;;S-1-5-21-4172447896-825920244-2358685150)</sd>

            </conditionValue>
</item>
```

tetenf.exe -l -f を使用して生成された WFP フィルタ

ユーザー名に基づくフィルタ

例：ユーザー名 SENSOR-DEV\sensor-dev に基づく WFP ルール

```
Filter Name:                    Secure Workload Rule 1
---------------------------------------------------
EffectiveWeight:                18446744073709551590
LayerKey:                       FWPM_LAYER_ALE_AUTH_CONNECT_V4
Action:                         Permit
RemoteIP:                       10.195.210.15-10.195.210.15
Remote Port:                    30000
Protocol:                       6
User or Service:                SENSOR-DEV\sensor-dev
```

ユーザーグループとユーザー名に基づくフィルタ

例：ユーザー名 SENSOR-DEV\\sensor-dev およびユーザーグループ名 SENSOR-DEV\\Domain Users に基づく WFP ルール

```
Filter Name:          Secure Workload Rule 1
-----------------------------------------------------
EffectiveWeight:              18446744073709551590
LayerKey:                     FWPM_LAYER_ALE_AUTH_CONNECT_V4
Action:                       Permit
RemoteIP:                     10.195.210.15-10.195.210.15
Remote Port:                  30000
Protocol:                     6
User or Service:              SENSOR-DEV\Domain Users, SENSOR-DEV\sensor-dev
```

ネットワークポリシールールにサービス名とユーザー名を設定することはできません。

ユーザー名またはユーザーグループが不正な場合

- ユーザー名またはユーザーグループが無効な場合、ネットワークポリシーはWindowsエージェントによって拒否されます。

Kubernetes と OpenShift

（オプション）Kubernetes ワークロードの追加ポリシー

次の手順は、Kubernetes 環境に応じたオプションです。

ホストネットワークモードで実行されている *Kubernetes Nginx Ingress* コントローラのポリシー

Cisco Secure Workload は、Kubernetes Ingress オブジェクトを使用して外部クライアントにポッドが公開されるときに、Nginx Ingress コントローラとバックエンドポッドの両方でポリシーを適用します。

（注） Ingress コントローラがホストネットワークモードで実行されていない場合は、IngressControllerAPI を参照してください。

（注） IBM-ICP は、デフォルトで Kubernetes Nginx Ingress コントローラを使用し、ホストネットワークモードのコントロールプレーンノードで実行されます。

Kubernetes Nginx Ingress コントローラを使用してポリシーを適用する手順は次のとおりです。

手順

ステップ 1 ここに記載する説明に従って、Kubernetes または OpenShift の外部オーケストレータを作成します。

```
→  ~
→  ~ k8s get ingress
NAME           HOSTS   ADDRESS          PORTS   AGE
test-ingress   *       192.168.60.100   80      7s
→  ~
```

ステップ 2 Kubernetes クラスタに入力オブジェクトを作成します。入力オブジェクトの作成で使用する yaml ファイルのスナップショットを次の図に示します。

```
▶ k8s get ingress
NAME                       HOSTS   ADDRESS          PORTS   AGE
svc-ce2e-teeksitlbiwlc     *       192.168.10.13    80      74s
```

```
~
▶ k8s get ingress -o yaml
apiVersion: v1
items:
- apiVersion: extensions/v1beta1
  kind: Ingress
  metadata:
    annotations:
      virtual-server.f5.com/ip: 192.168.10.13
      virtual-server.f5.com/partition: k8scluster
    creationTimestamp: "2020-06-26T21:31:01Z"
    generation: 1
    labels:
      e2e-test: "yes"
    name: svc-ce2e-teeksitlbiwlc
    namespace: default
    resourceVersion: "1074475"
    selfLink: /apis/extensions/v1beta1/namespaces/default/ingresses/svc-ce2e-teeksitlbiwlc
    uid: 5526b4a3-b7f4-11ea-aa09-525400d58002
  spec:
    backend:
      serviceName: svc-ce2e-teeksitlbiwlc
      servicePort: 80
  status:
    loadBalancer:
      ingress:
      - ip: 192.168.10.13
kind: List
metadata:
  resourceVersion: ""
  selfLink: ""
```

ステップ 3 Kubernetes クラスタに Kubernets Nginx Ingress コントローラを展開します。IBM-ICP Ingress コントローラポッドは、デフォルトでコントロールプレーンノードで実行されています。

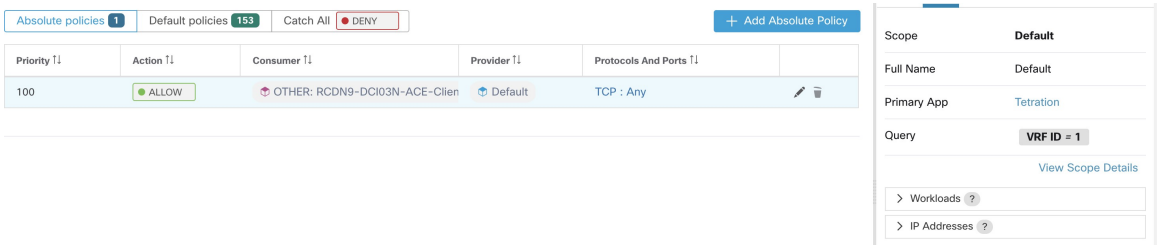
```
~
▶ k8s get pods -o wide -n ingress-nginx
NAME                                       READY   STATUS    RESTARTS   AGE     IP              NODE                        NOMINATED NODE
nginx-ingress-controller-6bc9c6745c-scfzs   1/1     Running   0          2m11s   192.168.10.13   enforcement-scale-16-kube3   <none>

~
▶ k8s get node enforcement-scale-16-kube3 -o wide
NAME                        STATUS   ROLES    AGE    VERSION   INTERNAL-IP     EXTERNAL-IP   OS-IMAGE           KERNEL-VERSION      CONTAINER-RUNTIME
enforcement-scale-16-kube3   Ready    <none>   7d5h   v1.12.3   192.168.10.13   <none>        Ubuntu 16.04.5 LTS   4.4.0-139-generic   docker://18.6.1
```

ステップ 4 クラスタ外のコンシューマがアクセスするバックエンドサービスを作成します。次の例では、簡単な *svc-ce2e-teeksitlbiwlc* （http-echo）サービスを作成しています。

```
~
▶ k8s get svc svc-ce2e-teeksitlbiwlc
NAME                    TYPE        CLUSTER-IP      EXTERNAL-IP   PORT(S)   AGE
svc-ce2e-teeksitlbiwlc   ClusterIP   10.102.30.231   <none>        80/TCP    6m11s
```

ステップ 5 外部コンシューマとバックエンドサービスの間にポリシーを作成します。



ステップ 6 準備ができたら、ポリシーを適用します。

ステップ 7 Nginx Ingress コントローラの場合、Secure Workload ソフトウェアでは、送信元は上記の手順で指定されたコンシューマであり、宛先は対応する Ingress コントローラポッド IP である、適切な許可/ドロップルールが適用されます。バックエンドポッドの場合、Secure Workload ソフトウェアでは、送信元は入力ポッドであり、宛先はバックエンドポッド IP である、適切な許可/ドロップルールが適用されます。

Deployment/Daemonset として実行されている *Kubernetes Nginx/Haproxy Ingress* コントローラのポリシー

Cisco Secure Workload は、Kubernetes Ingress オブジェクトを使用して外部クライアントにポッドが公開されるときに、Ingress コントローラとバックエンドポッドの両方でポリシーを適用します。

Ingress コントローラにポリシーを適用する手順は次のとおりです。

手順

ステップ 1 OpenAPI を使用して、Kubernetes/OpenShift の外部オーケストレータを作成/更新します。OpenAPI を使用して外部オーケストレータを作成する方法については、「オーケストレータ」を参照してください。外部オーケストレータ設定のための Ingress コントローラの情報を追加します。

ステップ 2 Kubernetes クラスタで Ingress オブジェクトを作成します。

ステップ 3 Kubernetes クラスタで Ingress コントローラを展開します。

ステップ 4 クラスタ外のコンシューマがアクセスするバックエンドサービスを作成します。

ステップ 5 外部コンシューマとバックエンドサービスの間にポリシーを作成します。

ステップ 6 準備ができたら、ポリシーを適用します。

ステップ 7 Ingress コントローラの場合、Secure Workload ソフトウェアでは、送信元は上記の手順で指定されたコンシューマであり、宛先は対応する Ingress コントローラポッド IP である、適切な許可/ドロップルールが適用されます。バックエンドポッドの場合、Secure Workload ソフトウェアでは、送信元は入力ポッドであり、宛先はバックエンドポッド IP である、適切な許可/ドロップルールが適用されます。

ワークロードのグループ化：クラスタとインベントリフィルタ

クラスタとインベントリフィルタの目的は似ていますが、いくつかの重要な違いがあります。

表 *4:* クラスタとインベントリフィルタの比較

クラスタ	[インベントリフィルタ（Inventory Filters）]
範囲内のワークロードのサブセットにポリシーを適用するために使用されます。	範囲内のワークロードのサブセットにポリシーを適用するために使用できます。 また、範囲に関係なくワークロードにポリシーを適用するためにも使用できます（たとえば、特定のオペレーティングシステムを実行しているすべてのワークロードにポリシーを適用するために使用できます）。
クエリによって定義されます。	クエリによって定義されます。
単一範囲内のワークロードのみを含めることができます。	単一範囲に制限されたメンバーシップを持つことも、任意の範囲内のワークロードを含めることもできます（たとえば、フィルタがオペレーティングシステムに基づいている場合）。
同じワークスペースおよびワークスペースバージョンのポリシーでのみ使用できます。	任意の範囲と任意のワークスペースのポリシーで使用できます。
自動ポリシー検出中に自動的に作成できます。	手動で作成するか、既存のクラスタから変換する必要があります。
承認されていない場合は、自動ポリシー検出中に上書きできます。既知の良好なクラスタを承認すると、今後の検出実行で他のクラスタの精度を向上させることができます。	自動ポリシー検出によって変更されることはありません。
自動ポリシー検出の重要な機能を活用できます。次の機能があります。 • グループ内のワークロードが一緒に属しているかどうかを評価するために役立つ信頼度評価があります。 • 同じワークスペースで他のポリシー検出の実行中に生成されたクラスタと比較できます。	--

クラスタ	[インベントリフィルタ（Inventory Filters）]
外部依存関係 （37ページ）を設定する場合、およびクロス範囲ポリシーとポリシー検出に関連するその他の機能を設定する場合は使用できません。	外部依存関係、およびクロス範囲ポリシーに関連するその他の機能（オートパイロットルールなど）を含む、きめ細かいポリシーを設定するために使用できます。
「クラスタ （84ページ）」およびサブトピックを参照してください。	インベントリフィルタの作成およびクラスタをインベントリフィルタに変換する （89ページ）を参照してください。

クラスタ

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 （93 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（「アクティビティログとバージョン履歴」を参照）。

クラスタに変更を加える （87 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。

クラスタとインベントリフィルタの比較については、ワークロードのグループ化：クラスタとインベントリフィルタ （83 ページ）を参照してください。

クラスタをインベントリフィルタに変換する （89 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、「クラスタの表示 （86 ページ）」を参照してください。

クラスタの表示

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、テーブルの列見出しをクリックして、その列（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並べ替えることができます。

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。

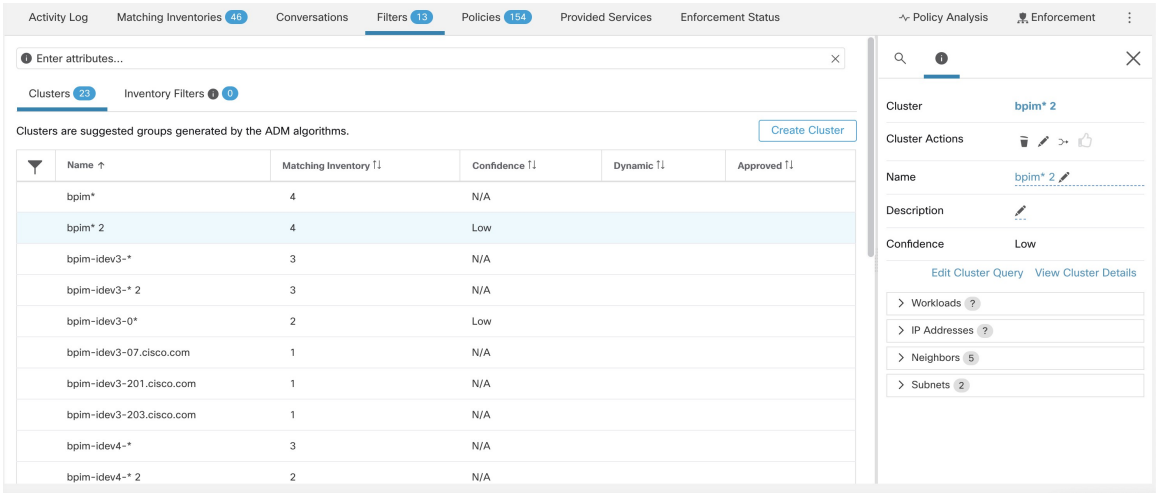
クラスタとその詳細を表示するには、次の手順を実行します。

1. 目的の範囲とワークスペースに移動します。

   クラスタはワークスペースに固有です。範囲内の各ワークスペースは、異なるクラスタを持つことができます。現在のワークスペースの外部でクラスタを使用できるようにするには、クラスタをインベントリフィルタに変換する （89 ページ）を参照してください。
2. [ポリシーの管理（Manage Policies）] をクリックします。
3. [フィルタ（Filters）] をクリックします。
4. [クラスタ(Clusters)] をクリックします。
5. クラスタに関する情報を表示するには、クラスタをクリックします。
   1. 右側に開くパネルを確認します。
   2. 詳細については、[クラスタの詳細の表示（View cluster details）] をクリックします。

[クラスタの詳細（Cluster Details）] ページが別のブラウザタブで開きます。

図 *27* : クラスタ ビュー



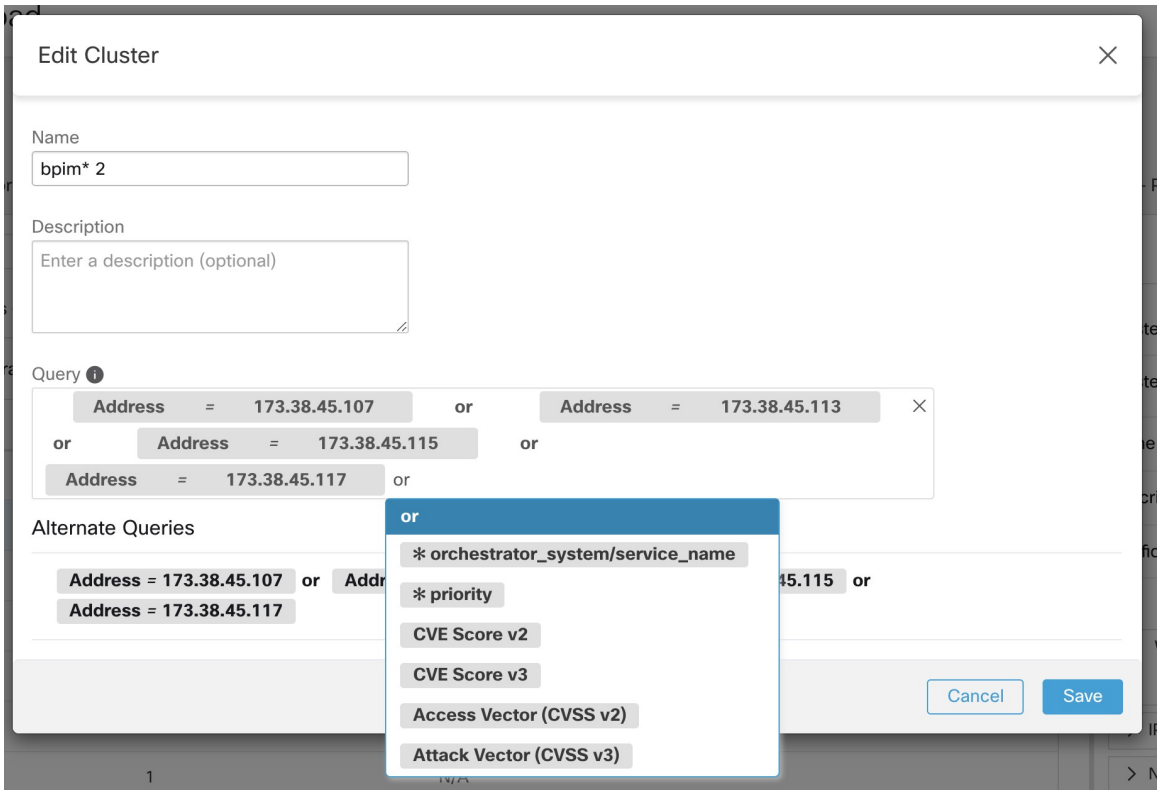
クラスタに変更を加える

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 *28 :* 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 （93 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。

クラスタをインベントリフィルタに変換する

次の場合、クラスタをインベントリフィルタに変換します。

- クラスタを承認するためのより用途の広い代替手段として、将来の自動ポリシー検出の実行によってクラスタが変更されないようにする必要があります。
- クラスタをワークスペースとワークスペースのバージョンから独立させる必要があります。
- コンシューマとプロバイダーが異なる範囲に属するポリシーを作成または検出し、範囲全体に関係するポリシーだけでなく、範囲内のワークロードのサブセットに固有のポリシーを作成する必要があります。

  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（103ページ）で説明されている詳細な方法を使用してクロス範囲ポリシーを作成する場合や、範囲ごとよりも細かいポリシーが必要な場合は、クラスタの代わりにインベントリフィルタを使用する必要があります。

手順

ステップ1 昇格するクラスタを含むワークスペースに移動します。

ステップ2 [ポリシーの管理（Manage Policies）] をクリックします。

ステップ3 [フィルタ（Filters）] をクリックします。

ステップ4 [クラスタ(Clusters)] をクリックします。

ステップ5 クロス範囲ポリシーで使用するクラスタをクリックします。

ステップ6 右側のパネルにある [クラスタアクション（Cluster Actions）] セクションで、（[インベントリフィルタに昇格（Promote to Inventory Filter）]）をクリックします。

ステップ7 名前、説明、およびクエリが期待どおりの内容であることを確認します。

ステップ8 [クエリを所有権の範囲に制限する（Restrict Query to Ownership Scope）] を選択します。

（インベントリフィルタが範囲の境界を越えることはできますが、この目的のためには不要な動作です。このフィルタにはこの範囲内のワークロードのみを含める必要があります）。

ステップ 9 このインベントリフィルタによって定義されたアプリケーションを、自動ポリシー検出中に生成されたポリシーのプロバイダーにする場合は、[範囲外のサービスを提供する（Provides a service external of its scope）] を選択します。

このアプリケーションがプロバイダーではなくコンシューマである場合、または手動で作成されたポリシーに対してのみこのインベントリフィルタを使用する場合は、このオプションを有効にする必要はありません。

ステップ 10 [クラスタの昇格（Promote Cluster）] をクリックします。

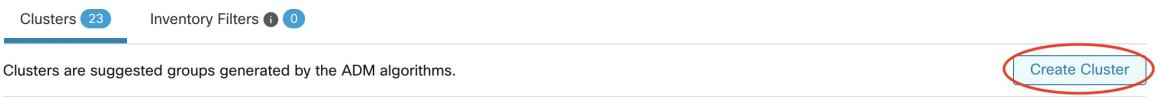
ステップ 11 クラスタが [インベントリフィルタ（Inventory Filters）] タブに移動したことを確認します。

確認するには、ページの更新が必要な場合があります。

クラスタの作成または削除

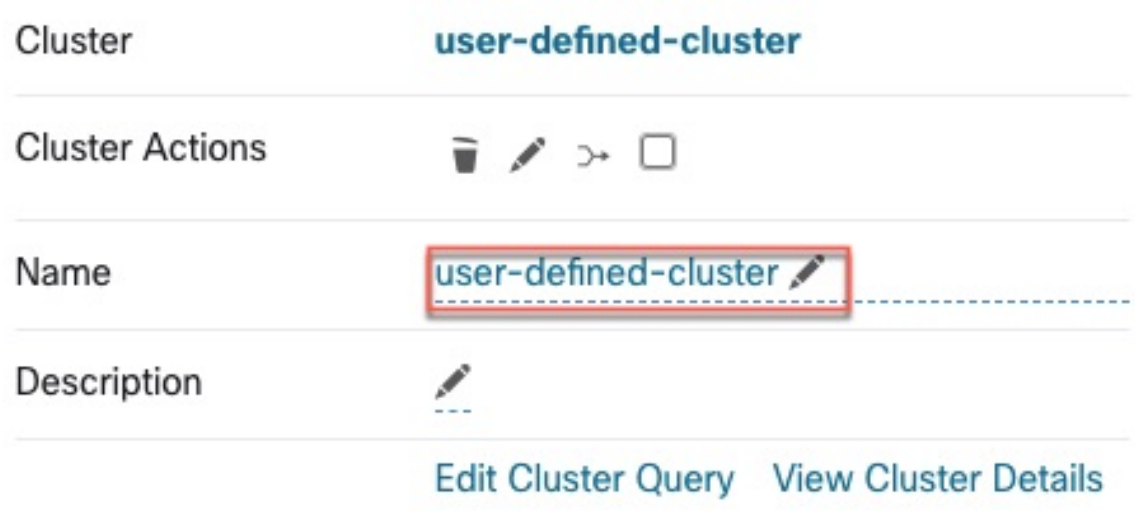
クラスタページの [クラスタの作成（Create Cluster）] ボタンをクリックして、新しい空のクラスタを作成します。または、[開始する（Get Started）] サイドバーの [フィルタの作成（Create Filter）] ボタンをクリックし、モーダルで [クラスタ（Clusters）] を選択して、[自動ポリシー検出（Automatic Policy Discovery）] ページからクラスタを作成できます。

図 *29 :* 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 *30 :* 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。

生成されたクラスタのバージョンの比較：差分ビュー

ワークスペースに対して少なくとも2回ポリシーを自動的に検出した後に、異なる検出の実行で生成されたクラスタを比較することができます。

手順

ステップ1 次のいずれかの方法を使用して、クラスタの差分ビューに移動します。

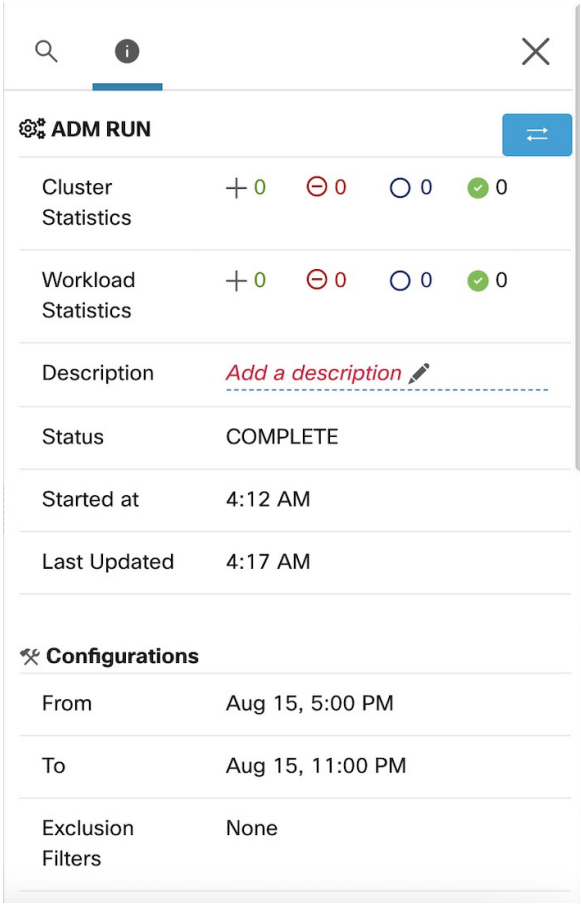
- ポリシーの検出に成功すると、検出結果を示す差分ビューに移動するリンクとともに、成功を示すメッセージが表示されます。結果のリンクをクリックします。

図 *31*：正常に実行された自動ポリシー検出

- バージョンビューからリビジョンを比較します。
  1. 検出されたポリシーバージョンの表示、比較、および管理 （58 ページ） の手順を実行します。
  2. [リビジョンの比較（Compare Revisions）] をクリックした後、[クラスタ（Clusters）] をクリックします。

- バージョンの詳細のサイドパネルから、次の手順を実行します。
  1. 検出されたポリシーバージョンの表示、比較、および管理 （58 ページ）のバージョンの詳細を表示するための手順に従います。
  2. サイドパネルで、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ているときに、サイドパネルの右上隅にある二重矢印ボタンをクリックします。

図 *32*：コンテキスト情報の表示



ステップ 2 比較するバージョンを選択します。

ステップ 3 比較の結果を確認します。

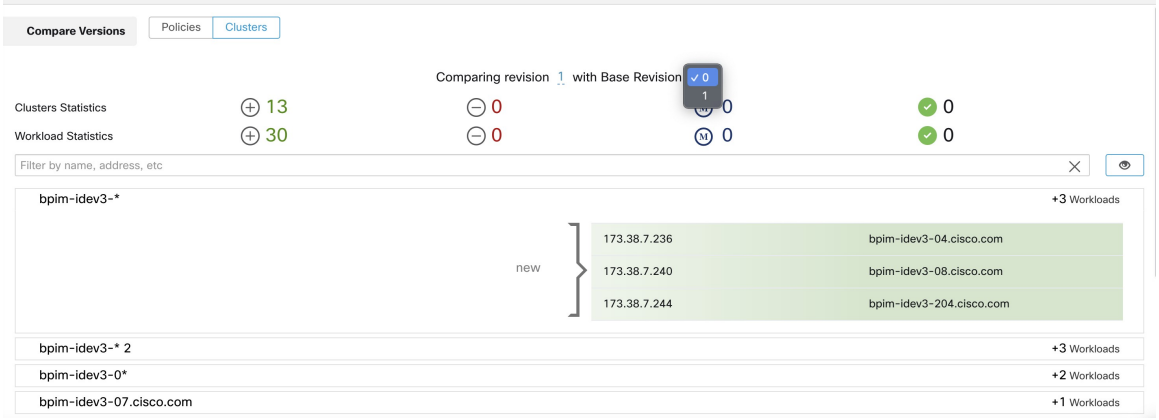
トップレベルでは、自動的に検出されたポリシーの差分ビューには、追加、削除、変更された、および未変更のクラスタとワークロードの数を示す、クラスタとワークロードの変更に関する高レベルの統計が表示されます。

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。クラスタの内容がどのように変化したかを確認するには、クラスタを表す行のいずれかをクリックして、その行を展開します。

（注） デフォルトでは、未変更のクラスタは非表示になっています。未変更のクラスタを表示するには、目のアイコンが表示されているボタンをクリックします。

図 *33* : クラスタの差分ビュー



次のタスク

ポリシーの同様の比較を表示するには、「ポリシーバージョンの比較：ポリシーの差分」を参照してください。

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 （93 ページ）を参照してください。

または、クラスタをインベントリフィルタに昇格させることもできます。これは、ポリシー検出によって変更されることはありません。クラスタをインベントリフィルタに変換する （89 ページ） を参照してください。

クラスタの承認

（注） クラスタをインベントリフィルタに変換する （89 ページ） も参照してください。こちらの方がより適切にニーズを満たすオプションである可能性があります。

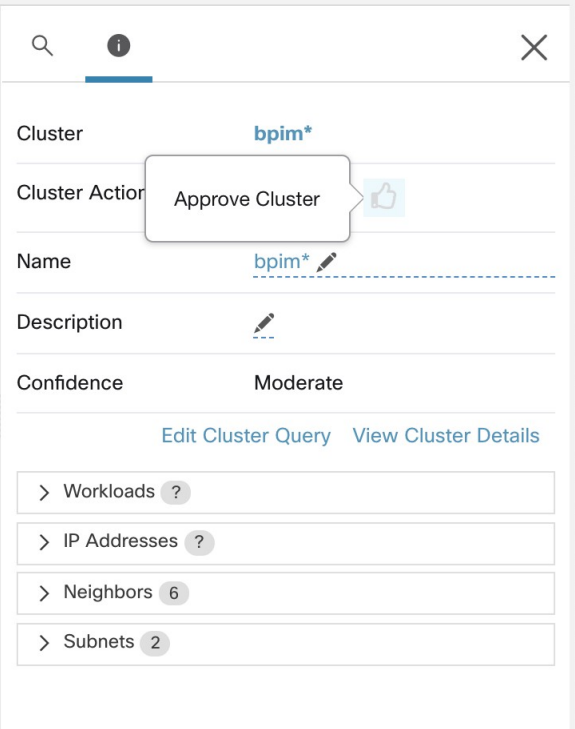
クラスタを承認しても、その後の自動ポリシー検出によってそのクラスタのクエリが変更されることはありません。承認されたクラスタのメンバーシップは、ワークスペースのメンバーが変更された場合にのみ変更される可能性があります。

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。

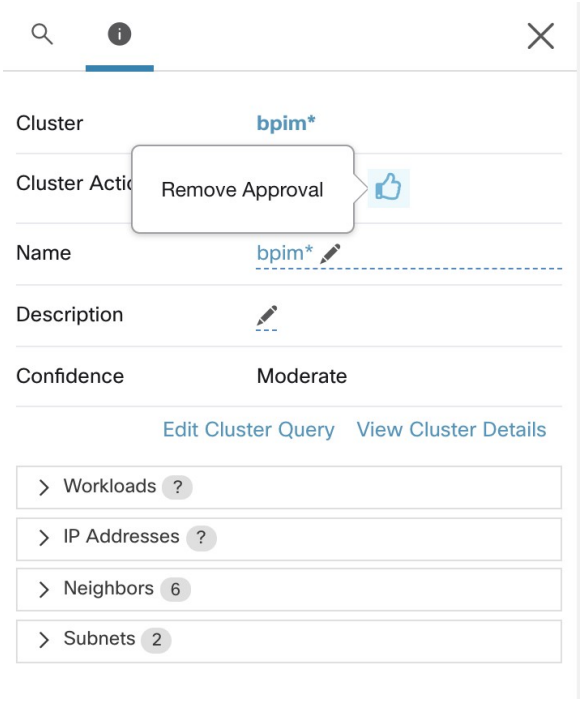
目的のクラスタがサイドパネルに表示されていることを確認します。これを行うには、クラスタを検索するか、いずれかのビューのチャートで目的のクラスタをクリックします。次に、以下に示すように、サイドパネルのクラスタ情報の右上隅にあるチェックボックスをオンにします。クラスタが承認されると、将来の自動ポリシー検出によってそのクラスタが変更されることはないことが示されます。

図 *34* : クラスタの承認



クラスタの承認を削除するには、承認アイコンをクリックします。

図 *35 :* クラスタの承認の削除



ポリシーの複雑さの対処

適用結果は、次の要因の影響を受けます。

- ルールのタイプとランク：
  - 絶対ポリシー対デフォルトポリシー
  - ワークスペースのキャッチオール設定

  ポリシーのランク：絶対、デフォルト、キャッチオール （10 ページ）を参照してください。
- ワークスペース内でのポリシーの順序

  ポリシーの優先順位 （96 ページ）を参照してください。
- キャッチオールルールを含む、親範囲または先祖範囲から継承されたポリシー

  トラフィックにヒットすることが期待されるポリシーよりも先に、優先順位の高いポリシーがそのトラフィックにヒットしないようにする必要があります。

  先祖範囲のポリシーの影響を確認するには、関連するすべての範囲でライブポリシー分析を実行します。ライブポリシー分析 （129 ページ）を参照してください。

ワークスペースでポリシーを適用する準備ができると、ワークスペースのワークロードに影響を与える継承されたポリシーがウィザードに表示されます。詳細については、ポリシー適用ウィザード （149 ページ） を参照してください。

- クロス範囲ポリシーの相互作用

  （コンシューマとプロバイダーが異なる範囲にある場合、またはカンバセーションの一方の端がポリシーとは異なる範囲にある場合）

  「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 （103 ページ）」を参照してください。

- ポリシー内の実際のコンシューマまたはプロバイダーが、デフォルトで設定されたコンシューマおよびプロバイダーと異なる場合がある状況（フェールオーバーシナリオなど）

  有効なコンシューマまたは有効なプロバイダー （117 ページ） を参照してください。

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 （96 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。

詳細は、ポリシーのランク：絶対、デフォルト、キャッチオール （10 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、「ワークスペースを使用したポリシーの管理」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

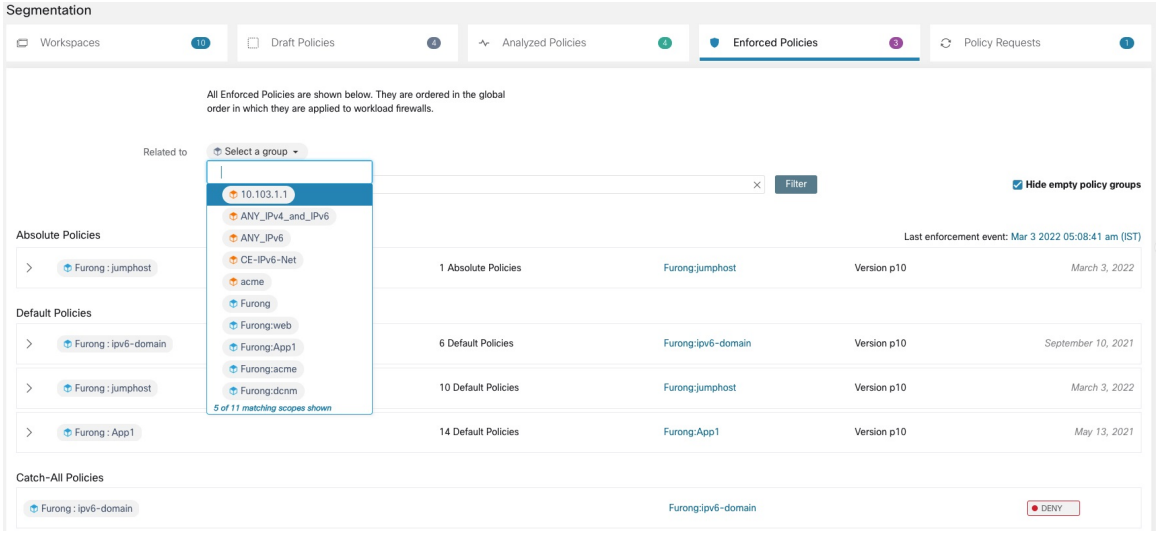
7. アプリ：コマースのキャッチオール

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。

ポリシーの順序と優先順位の検証

親/先祖ワークスペース内のポリシーの順序と優先順位を検証するには、[防御（Defend）]>[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）] タブまたは [適用されたポリシー（Enforced Policies）] タブをクリックします。これらのビューは、それぞれ、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を提供します。

図 *36 :* 例：ポリシーの優先度順の適用されたポリシーのリスト



- ポリシーのリストを、コンシューマまたはプロバイダーとして特定の範囲またはフィルタを含むポリシーのみに制限するには、範囲を選択するか、フィルタを入力します。
- 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 （54 ページ）
外部？（External?）	コンシューマとプロバイダーが異なる範囲内にあるポリシー。

フィルタ名	定義
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）

（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（96ページ）を参照してください。
- 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。

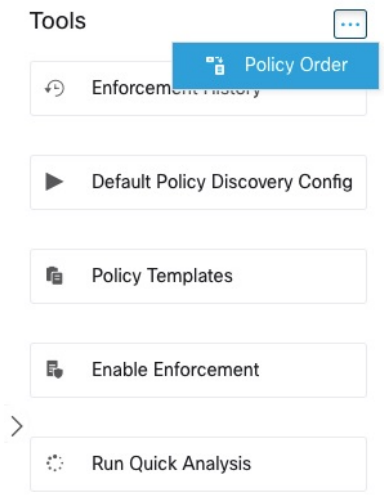
  並べ替えるときは、範囲ツリーの階層構造を利用するために、親優先の順序（親範囲が子範囲の上）を維持します。

  （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。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。範囲の重複 を参照してください。）

手順

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

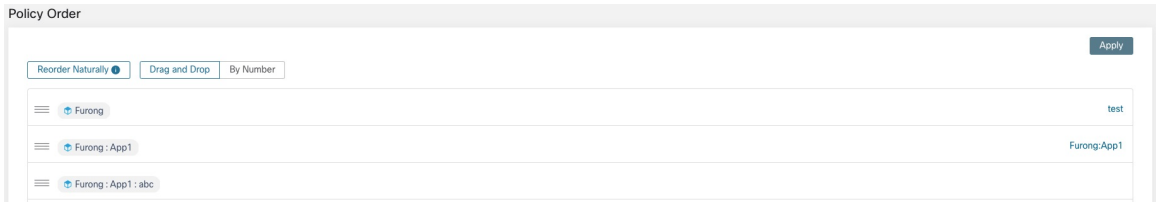


[ポリシーの順序（Policy Order）]ページでは、現在のポリシーの優先順位に従って、すべての範囲と範囲に対応するプライマリワークスペースのリストを確認できます。

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 *38 :* 範囲のポリシー優先順位の設定



次のタスク

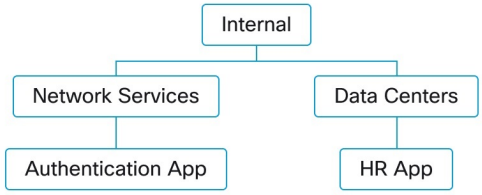
簡易分析を実行して、変更の結果を確認します。

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

シナリオ例

次の状況は、クロス範囲トラフィックを示す例です。

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。



ポリシーオプション

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。

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。 • 範囲ツリーのブランチ全体に対して、共通の先祖範囲内のポリシーを自動的に検出します。	これらが、クロス範囲ポリシーに対処する最も簡単な方法です。 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。 自動ポリシー検出の使用を検討している場合は、1 つの範囲または範囲ツリーのブランチのポリシーの検出（26 ページ）の重要なその他の考慮事項を参照してください。

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	個々の各範囲のポリシーを自動的に検出します。 （上級）クロス範囲ポリシーの作成（104ページ）を参照してください。 （この手順は、手動で作成されたポリシーと検出されたポリシーの両方に適用されます）	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。 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ポリシーを作成できます。 1 つの範囲または範囲ツリーのブランチのポリシーの検出 （26 ページ）のその他の考慮事項を参照してください。

（上級）クロス範囲ポリシーの作成

この手順では、クロス範囲ポリシー（コンシューマとプロバイダーが異なる範囲にあるポリシー）を作成する詳細な方法について説明します。この手順は、手動で作成されたポリシーと自動的に検出されたポリシーの両方に当てはまります。

この方法では、会話の両端で会話の発生を許可する必要があるため、コンシューマとプロバイダーのペアごとに 2 つのポリシーが必要です。

- コンシューマの範囲内のポリシーでは、プロバイダーとの会話を許可する必要があります。

  および

- プロバイダーの範囲内のポリシーでは、コンシューマとの会話を許可する必要があります。

この手順には、クロス範囲ポリシーを作成するために各範囲の所有者が実行する必要がある手順が含まれています。自分のアクセス権限で両方の範囲を変更できる場合は、すべての手順を実行できます。

始める前に

- クロス範囲トラフィックを処理するためのより簡単なオプションを検討してください。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 （103 ページ）を参照してください。
- この方法を使用するポリシーは、コンシューマとプロバイダーの両方のプライマリワークスペースで作成する必要があります。

  ポリシーで指定するプロバイダー範囲にプライマリワークスペースがない場合は、この方法を使用してクロス範囲ポリシーを作成する前にプライマリワークスペースを作成します。

- ポリシー要求を作成するには、ポリシーにALLOWアクションを含める必要があります。
- これらの要件に関する追加の詳細については、ポリシー要求 （106ページ）を参照してください。
- （オプション）クロス範囲ポリシー要求の自動処理に関するオプションを検討します。クロス範囲ポリシー要求の自動処理 （111 ページ）を参照してください。
- （オプション）クロス範囲ポリシーを、範囲全体ではなく、コンシューマ範囲またはプロバイダー範囲内にあるクラスタ内のワークロードにのみ適用する場合は、クラスタをインベントリフィルタに変換する （89 ページ）を参照してください。この手順を使用して作成されたクロス範囲ポリシーでは、クラスタを使用できません。

  ポリシーを自動的に検出している場合は、外部依存関係 （37ページ）およびワークスペースの外部依存関係の微調整 （39 ページ）も参照してください。

手順

ステップ 1 コンシューマのプライマリワークスペースで、手動で、または自動ポリシー検出を使用して、目的のポリシーを作成します。

作成したクロス範囲ポリシーごとに、プロバイダーに対するポリシー要求が自動的に作成されます。

ポリシー要求を表示するには、ポリシー要求の表示、承認、および拒否 （106ページ）を参照してください。

注：プロバイダーアプリケーションのワークスペース内の既存のポリシーがこのトラフィックに一致する場合、新しいポリシーは不要なため、要求は作成されません。この状況は、解決済みのポリシー要求 （115 ページ）で説明されているように示されます。

ステップ 2 ユーザー（またはプロバイダーアプリケーションの所有者）は、各ポリシー要求に応答する必要があります。

ポリシー要求の表示、承認、および拒否 （106 ページ）を参照してください。

ポリシー要求を受け入れると、プロバイダーのプライマリワークスペースに必要なポリシーが自動的に作成され、2 つのアプリケーション間のトラフィックが許可されます。

要求元のアプリケーションからのトラフィックを許可しない場合、要求は拒否されます。

ステップ 3 （オプション）ポリシーを自動的に検出している場合、ワークスペースの外部依存関係の微調整 （39 ページ） が必要な場合があります

ステップ 4 両方のプライマリワークスペースを確認して分析します。

次のタスク

ポリシーを適用する準備ができたら、両方のプライマリワークスペースを適用する必要があります。

ポリシー要求

ポリシー要求は、「（上級）クロス範囲ポリシーの作成（104ページ）」で説明している方法を使用してクロス範囲ポリシーを作成すると生成されます。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（106ページ）」および「クロス範囲ポリシー要求の自動処理（111ページ）」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）。

ポリシー要求の表示、承認、および拒否

（上級）クロス範囲ポリシーの作成（104ページ）で説明されている方法を使用してクロス範囲ポリシーを作成する場合、コンシューマの範囲のポリシーに加えて、プロバイダーの範囲のプライマリワークスペースにもポリシーが必要です。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。
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 Policies）] 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。 または コンシューマ範囲からのポリシー要求を表示するには、次の手順を実行します。 コンシューマ範囲のプライマリワークスペースの [ポリシー（Policies）] タブで、[プロトコルとポート（Protocols and Ports）] 列の値をクリックし、ページの右側に表示されるパネルを確認します。[プロトコルとポート（Protocols and Ports）] セクションで、黄色のドットをクリックして、保留中のポリシー要求を表示します。

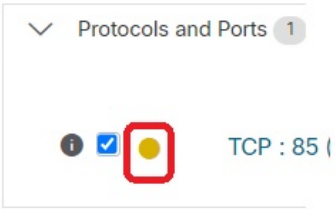
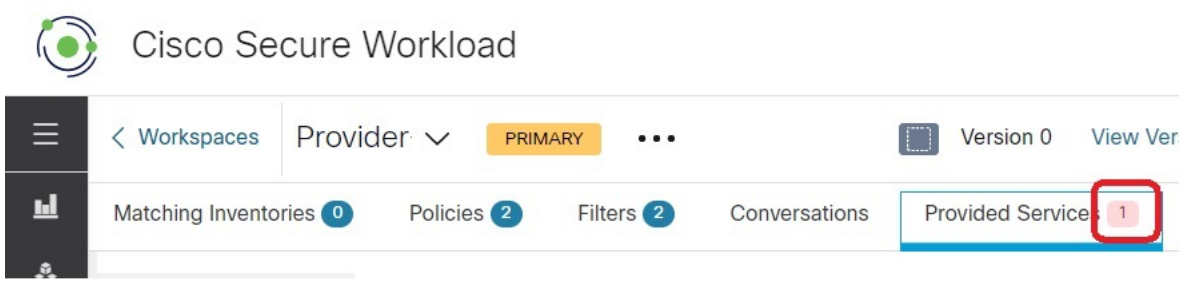
目的	操作手順
要求を手動で受け入れると、プロバイダー範囲に必要なポリシーが自動的に作成されます。	上記のいずれかの場所で、ポリシー要求の横にある [承認（Accept）] をクリックします。
要求を手動で拒否する	上記のいずれかの場所で、ポリシー要求の横にある [拒否（Reject）] をクリックします。
コンシューマワークスペースからポリシー要求ステータスを表示する	プライマリ コンシューマ ワークスペースの [ポリシー（Policies）] ページで、ポリシーをクリックしてから、ポート/プロトコルの値をクリックします。ステータスは、右側に開くパネルに表示されます。 保留中の要求は、黄色の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。
ポリシー要求の処理を自動化するためのオプションも参照してください	クロス範囲ポリシー要求の自動処理 （111 ページ）

図 *39* : プロバイダーの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 *40* : ポリシー要求の承認/拒否

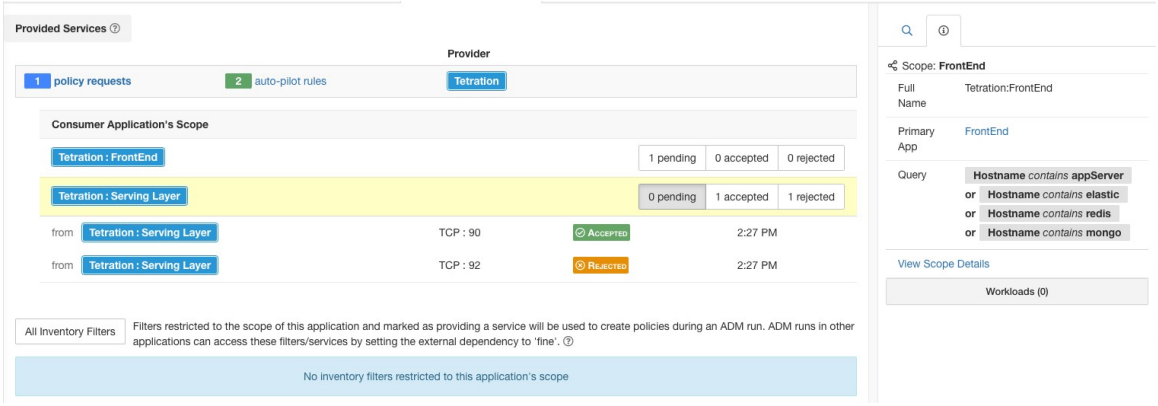
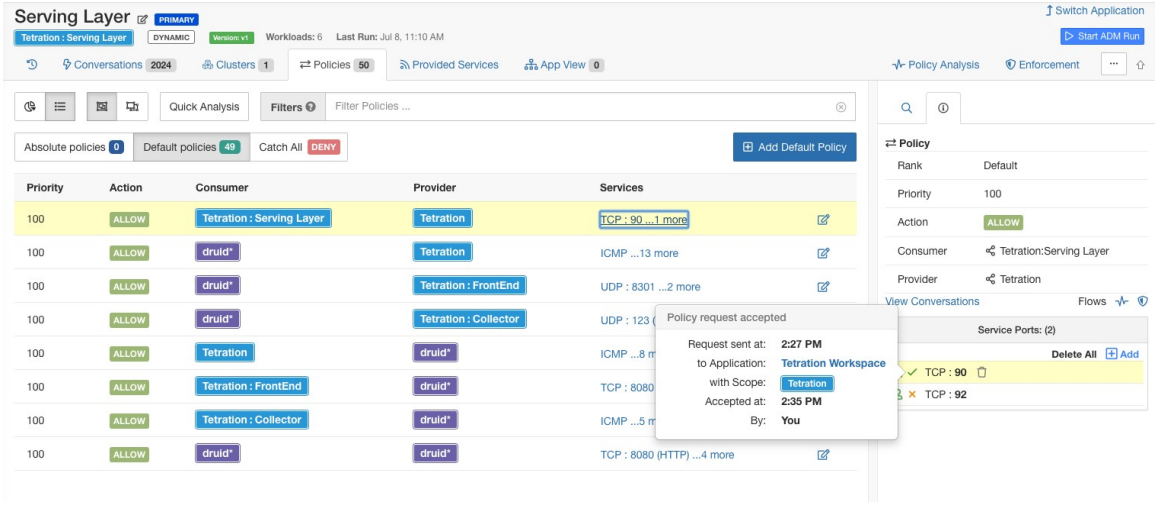


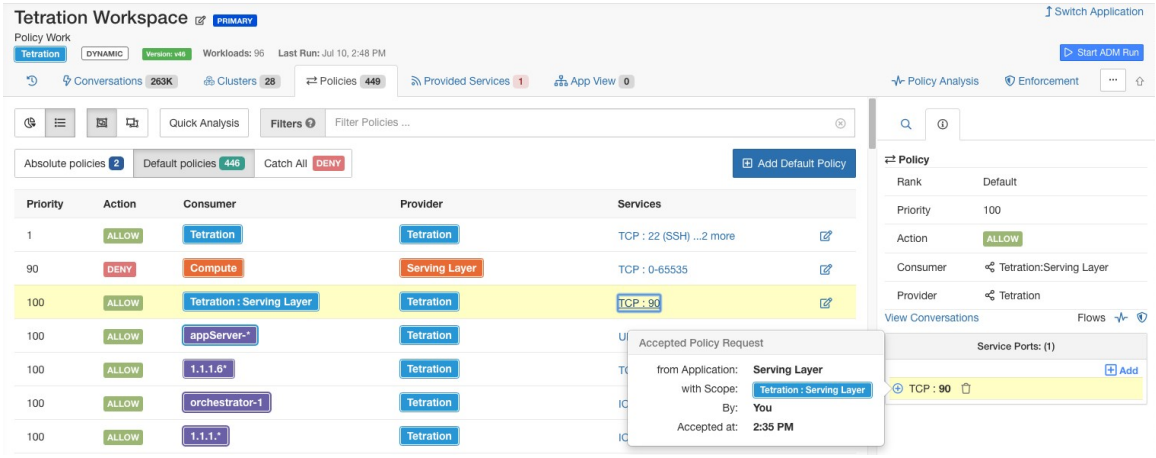
図 *41* : 承認済みとして表示されるポリシーのステータス



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 *42* : 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

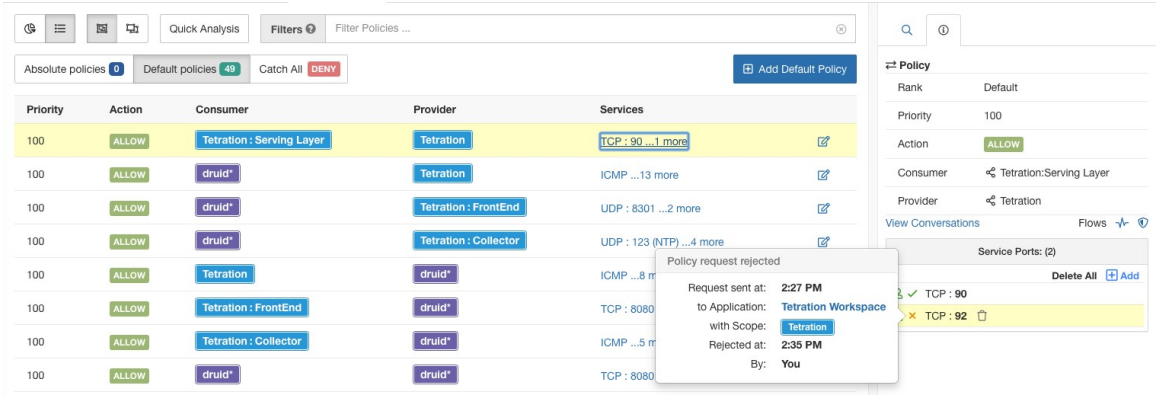


ポリシー要求の拒否：詳細

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 *43*：拒否されたと表示されるポリシーのステータス



クロス範囲ポリシー要求の自動処理

ポリシー要求は、「（上級）クロス範囲ポリシーの作成 （104 ページ）」で説明している方法を使用してクロス範囲ポリシーを作成すると生成されます。

クロス範囲ポリシーを作成するときに生成されるポリシー要求の数を減らすには、いくつかのオプションがあります。

表 *5*：ポリシー要求を自動的に処理するためのオプション

目的	操作手順
特定のコンシューマとプロバイダーのペア間のポリシー要求の処理を指定する	オートパイロットルール （112 ページ）を参照してください。 必要な権限を持っている必要があります。
特定のワークスペースでのポリシー検出中に作成されたすべてのクロス範囲ポリシーについて、プロバイダーに必要なすべてのポリシーを自動的に作成する	自動ポリシー検出の実行を開始するときは、[詳細設定（Advanced Configurations）]セクションの[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）]オプションを有効にします。 このオプションは、ルート範囲の所有者とサイト管理者が使用できます。 詳細については、次を参照してください。 自動ポリシー検出の詳細設定 （42 ページ）および 自動承諾ポリシーコネクタ （114 ページ）

目的	操作手順
すべてのワークスペースからのすべてのポリシー要求のデフォルトの処理を指定する	[デフォルトのポリシー検出設定（Default Policy Discovery Config）] ページで、[詳細設定（Advanced Configurations）] セクションの [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）] オプションを有効にします。 このオプションは、ルート範囲の所有者とサイト管理者が使用できます。 詳細については、次を参照してください。 デフォルトのポリシー検出設定 （52 ページ）および 自動ポリシー検出の詳細設定 （42 ページ）および 自動承諾ポリシーコネクタ （114 ページ）

オートパイロットルール

この機能は、「（上級）クロス範囲ポリシーの作成 （104ページ）」で説明されている方法を使用してクロス範囲ポリシーを作成する場合にのみ適用できます。

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は、他のアプリケーションから多数のポリシー要求を受信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、ポリシー要求の数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 Policies）] 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）。

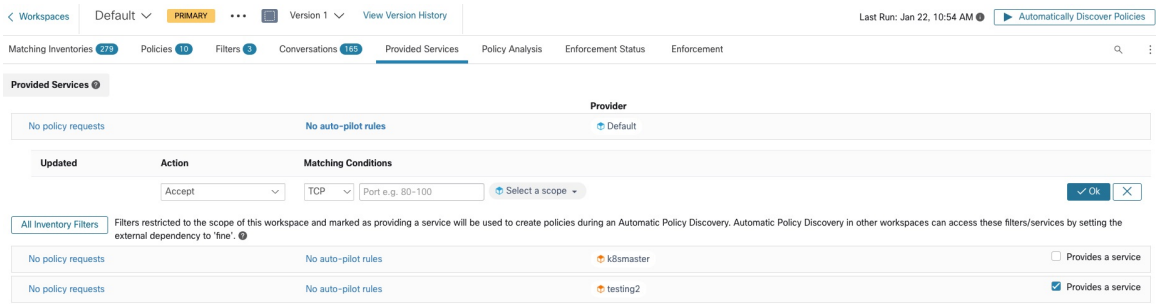
   それ以外の場合は、範囲に対してこれらの手順を実行します（範囲は青いアイコンで識別されます）。

   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

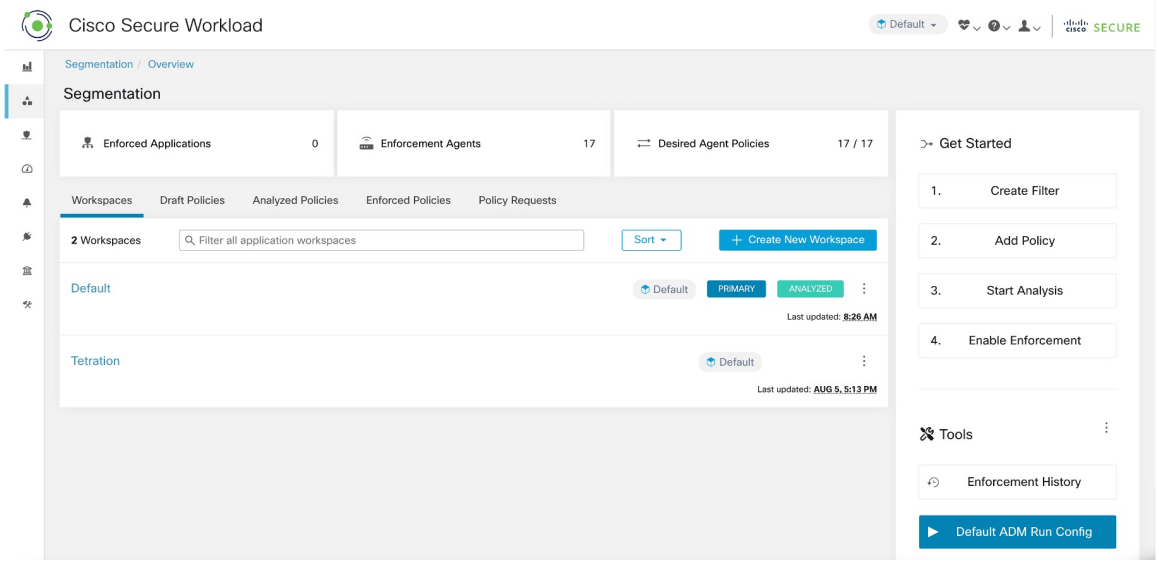
以下の例では、Tetration:Adhoc に含まれる任意のコンシューマからプロバイダーサービス Tetration への、ポート範囲 1 ～ 200 における TCP ポリシー要求を拒否する新しいオートパイロットルールを作成します。

図 *44*：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 *45 :* 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最近作成されたポリシーの数の表示

ワークスペースに対してライブポリシー分析が最後に開始（または再開始）されてから、オートパイロットルールによってワークスペース内に作成されたポリシーの数を表示するには、次の手順を実行します。

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

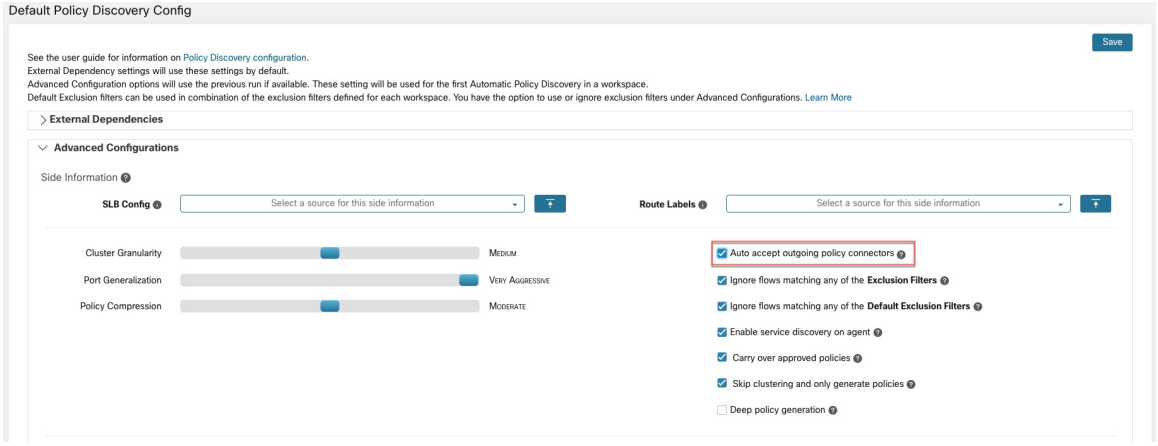
このオプションは、デフォルトのポリシー検出構成として設定するか、各ワークスペースの自動ポリシー検出の詳細オプションで設定できます。

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。

このオプションがデフォルトの自動ポリシー検出設定で有効になっている場合、手動で作成されたポリシー要求またはワークスペースのインポートによって作成されたポリシー要求も自動的に受け入れられます。

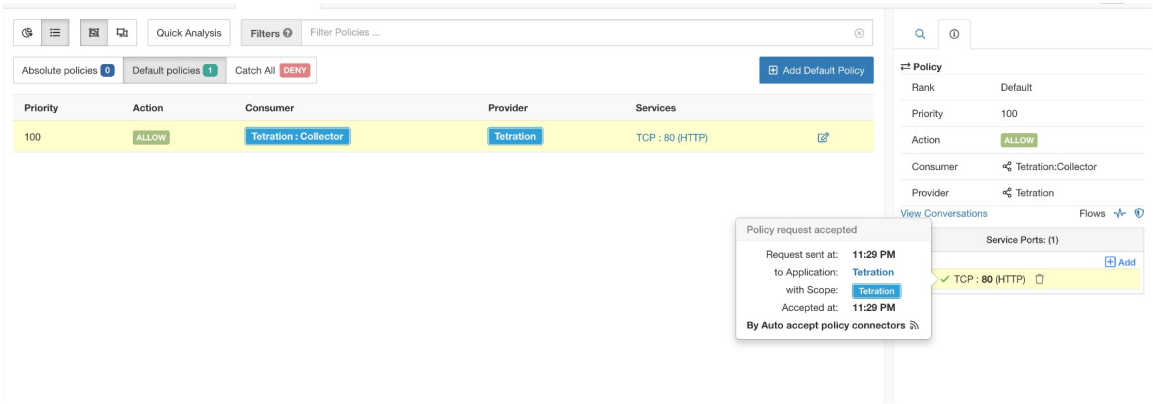
（注） このオプションは、ルート範囲の所有者またはサイト管理者のみが使用できます。

図 *46* : 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、ルート範囲の任意のワークスペースまたは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。

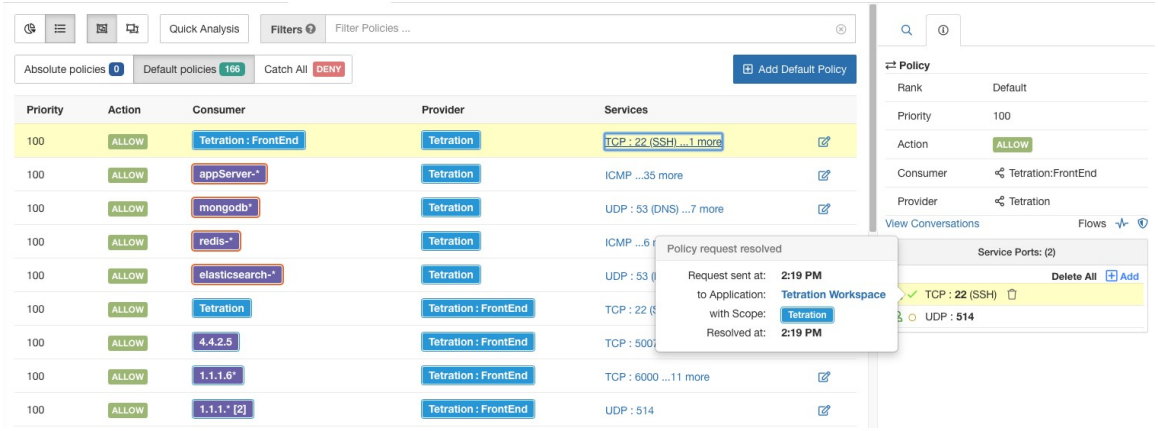
図 *47* : ポリシーはポリシーコネクタの自動受け入れによって自動的に受け入れられる



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 *48 :* 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



提供されるサービス

このページは、コンシューマとプロバイダーが異なる範囲にあるポリシーを作成する場合、および（上級）クロス範囲ポリシーの作成 （104 ページ） で説明されている方法を使用している場合にのみ使用されます。

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 （106 ページ）
- オートパイロットルール （112 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 （37 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。

クロス範囲ポリシーのトラブルシューティング

（上級）クロス範囲ポリシーの作成 （104 ページ） で説明されている方法を使用してクロス範囲ポリシーを作成した場合は、コンシューマワークロードとプロバイダーワークロードのそれぞれのプライマリワークスペースに、トラフィックを許可するポリシーが必要です。必要なポリシーが両方のワークスペースに存在することを確認します。

いずれかのポリシーが削除または変更されても、通知は行われません。

ポリシーの検出中にポリシーペアが生成された場合は、ポリシーの承認に関する情報を参照して、後続の検出の実行から保護します。ポリシーの承認 （54 ページ） を参照してください。

（上級）クロス範囲ポリシーの作成 （104 ページ） に記載されている他の要件が引き続き満たされていることを確認します。

必要なポリシーを持つコンシューマとプロバイダーの両方のワークスペースを適用する必要があります。

クロス範囲ポリシーに役立つツール

- ポリシーを検出した範囲とは異なる範囲にプロバイダーが存在するポリシーを見つけるには、[外部？（External?）] フィルタオプションを使用します。
- ポリシーのビジュアルビューには、外部ポリシーを表示するオプションがあります。ポリシーの視覚的表現 （125 ページ）を参照してください。

デフォルトのポリシー検出設定を使用している場合

デフォルトの外部依存関係の設定を個々のワークスペースで使用できるように変更した後、[デフォルトのポリシー検出設定（Default Policy Discovery Config）] ページで [保存（Save）] をクリックしたことを確認します。

有効なコンシューマまたは有効なプロバイダー

ポリシーで指定されたコンシューマとプロバイダーによって、次のことが決まります。

- ポリシーを受信する Secure Workload エージェントを含む一連のワークロード。
- インストールされているファイアウォールルールの影響を受ける一連の IP アドレス。

デフォルトでは、これらは同じです。

ただし、ポリシーを受信するワークロードの IP アドレスとは異なる IP アドレスのグループを、ファイアウォールルールで指定する必要が生じることがあります（以下の例を参照してください）。

このニーズに対処するために、有効なコンシューマや有効なプロバイダーを設定できます。

コンシューマとプロバイダーのデフォルトの動作

デフォルトでは、Secure Workload エージェントがポリシーを受け取ると、ファイアウォールルールはそのワークロードに固有のものになります。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 のワークロードでプログラムされている場合、ファイアウォールルールは次のようになります。

- 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。
- 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。

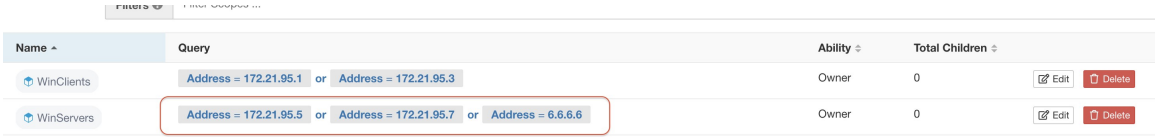
例：有効なコンシューマまたは有効なプロバイダー

この例では、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。有効なコンシューマや有効なプロバイダーを使用して、フェールオーバーイベント中にトラフィックが中断されないようにします。

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、任意の時点で 1 つのワークロードのみが VIP を所有します。目標は、フリート内のすべてのワークロードでファイアウォールルールをプログラムし、6.6.6.6 へのトラフィックを許可することです。

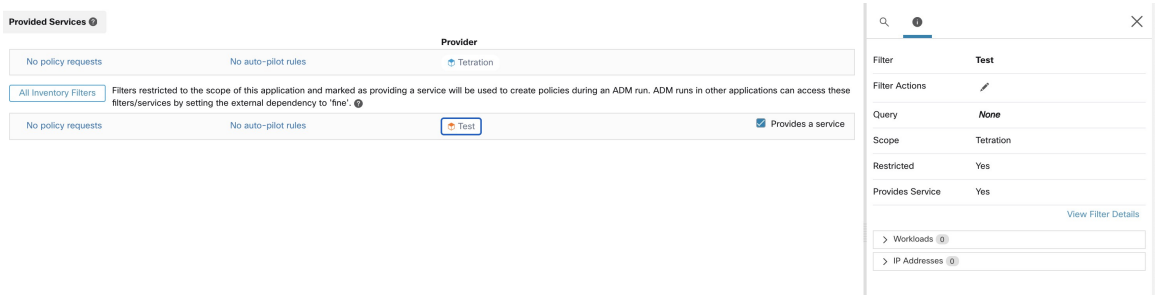
このセットアップでは、フリートを表すワークロードのクラスタ（172.21.95.5 および 172.21.95.7）と VIP（6.6.6.6）を含む範囲と対応するワークスペースがあります。

図 *49*：*VIP* とワークロードのクラスタで構成される範囲



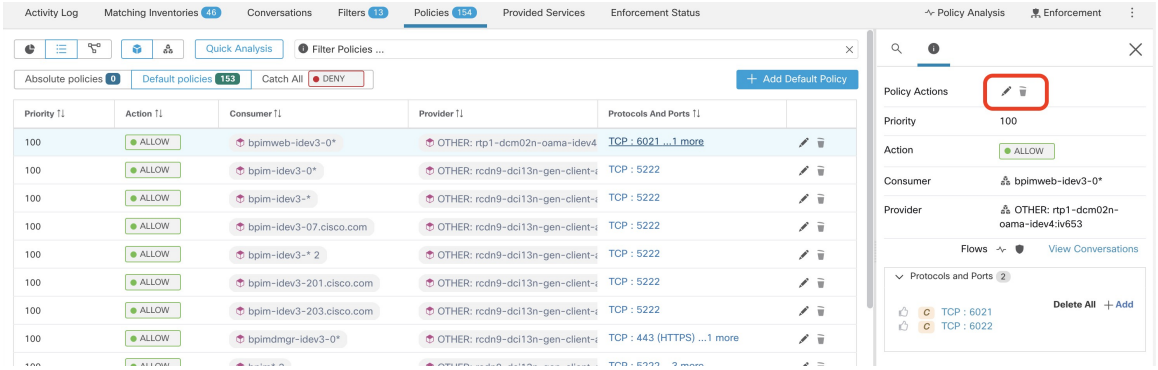
以下に示すように、VIP は提供サービスとしてこのワークスペースで公開されます。

図 *50*：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。ただし、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り、トラフィックが短時間中断される場合があります。

図 *51* : 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



この問題に対処するために、（以下の手順を使用して）有効なプロバイダーを設定します。具体的には、[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する場合、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されることはありません。

図 *52* : *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

```
$
$ hostname -I | awk '{print $1}'          IP Address of
172.21.95.7                               the server
$                                         part of cluster
$
$ sudo iptables -n --list TA_INPUT   <— Ingress rules
Chain TA_INPUT (1 references)
target     prot opt source               destination
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           match-set ta_6c6b4133313438ff5429ca8c14b6 src match-set ta_ac2618d307e4e7dbb76b96c0df3f dst mul
tiport dports 1443 ctstate NEW,ESTABLISHED /* PolicyId=DEFAULT:100:ALLOW:5ed53fe8497d4f26444d50b3:5ed5435b497d4f26414d50b1:6 */
RETURN     all  --  0.0.0.0/0            0.0.0.0/0
$
$
$ sudo iptables -n --list TA_OUTPUT   <— Egress rules
Chain TA_OUTPUT (1 references)
target     prot opt source               destination
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           match-set ta_ac2618d307e4e7dbb76b96c0df3f src match-set ta_6c6b4133313438ff5429ca8c14b6 dst mul
tiport sports 1443 ctstate ESTABLISHED /* PolicyId=DEFAULT:100:ALLOW:5ed53fe8497d4f26444d50b3:5ed5435b497d4f26414d50b1:6 */
RETURN     all  --  0.0.0.0/0            0.0.0.0/0
$
$
$ sudo ipset list ta_ac2618d307e4e7dbb76b96c0df3f
Name: ta_ac2618d307e4e7dbb76b96c0df3f
Type: hash:net
Revision: 3
Header: family inet hashsize 1024 maxelem 65536
Size in memory: 16816
References: 2
Members:
6.6.6.6              <— VIP
$ sudo ipset list ta_6c6b4133313438ff5429ca8c14b6
Name: ta_6c6b4133313438ff5429ca8c14b6
Type: hash:net
Revision: 3
Header: family inet hashsize 1024 maxelem 65536
Size in memory: 16848
References: 2
Members:
172.21.95.1
172.21.95.3          <— Client IPs
$
```

有効なコンシューマまたは有効なプロバイダーの設定方法

1. 編集するポリシーをクリックします。
2. 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します。
3. [有効なコンシューマ（Effective Consumer）] または [有効なプロバイダー（Effective Provider）] をクリックします。
4. 目的のアドレスを指定します。
5. 有効なコンシューマと有効なプロバイダーの両方のアドレスを指定する必要がある場合があります。

ポリシーの削除について

重要 ポリシーを削除する前に、コンシューマとプロバイダーが異なる範囲内にある場合、そのポリシーが必要なポリシーのペアの 1 つではないことを確認してください。

これを確認するには、[プロトコルとポート（Protocols and Ports）] 列でポリシーのリンクをクリックします。ページの右側に表示されるパネルで、[プロトコルとポート（Protocols and Ports）] セクションを確認します。クロス範囲ポリシー要求を受け入れることによって作成されたポリシーは、ポートとプロトコルの横のプラス記号で示されます。

プラス記号をクリックすると、クロス範囲ポリシーの作成者と、対応するコンシューマポリシーへのリンクが表示されます。

（注） 自動ポリシー検出によって提案され、承認されていないポリシーは、それらを生成したトラフィックフローが後続のポリシー検出の実行中に見られない場合、後続の実行後に存在しなくなる可能性があります。提案されたポリシーを保持するには、ポリシーの承認 （54 ページ）を参照してください。

ポリシーの確認と分析

ポリシーを適用する前に、ポリシーに意図した効果があること（また、意図していない効果がないこと）を確認することが不可欠です。

自動検出されたポリシーの確認

ポリシーを検出したワークスペースの [ポリシー（Policies）] ページでポリシー検出結果を確認します。

最初に確認すること

最初に、ポリシーで次の各領域が対処されているかどうかを、この推奨される順序で確認することを推奨します。

- 重要な一般ポート
- インターネットに接続するトラフィック
- 異なるアプリケーション間のトラフィック（これらのフローには、異なる範囲内のワークロードが関係する場合があります）
- 同じアプリケーション内のトラフィック（これらのフローには、同じ範囲内のワークロードが関係する可能性が高いです）

ポリシーの確認に役立つツール

- この作業をより管理しやすくするには、ポリシーをフィルタしてソートし、関連するポリシーをグループとして確認できるようにします。
  - コンシューマ、プロバイダー、ポート、プロトコルなどで列をソートするには、テーブルの見出しをクリックします。
  - 特定のサブセットを表示するには、ポリシーリストの上部にあるフィルタを使用します。

    フィルタに使用できるプロパティのリストを表示するには、[ポリシーのフィルタ（Filter Policies）] ボックスの [(i)] ボタンをクリックします。

- 生成されたポリシーのグラフィカル表示を確認します。

  [ポリシービジュアルビュー（Policy Visual View）] ボタン（  ）をクリックします。

  詳細については、「ポリシーの視覚的表現 （125 ページ）」を参照してください。

- ポートに基づいて行を検索またはフィルタするには、[グループ化解除（Ungrouped）] ボタンをクリックします。

- デフォルトでは、ポリシーは、コンシューマ、プロバイダー、アクションでグループ化されています。このビューに戻るには、[グループ化（Grouped）]ボタンをクリックします。
- ポリシーを検出した範囲とは異なる範囲にプロバイダーが存在するポリシーを見つけるには、[外部？（External?）] フィルタオプションを使用します。

  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（103ページ）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。
- 生成されたポリシーの信頼度レベルを確認します。信頼度の低いポリシーへの対処 （123ページ）を参照してください。
- ワークロードの詳細については、[ワークロードプロファイル（Workload Profile）] を参照してください。IP アドレスをクリックし、右側のペインで [ワークロードプロファイルの表示（View Workload Profile）] をクリックします。
- 特定のポリシーの生成に使用されたトラフィックフローを表示するには、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、開いたサイドパネルで [カンバセーションの表示（View Conversations）] をクリックします。

  詳細については、カンバセーション （167 ページ）を参照してください。

  必要に応じて、[フロー検索（Flow Search）] をクリックしてさらにドリルダウンし、カンバセーションのフローを表示することができます。

その他の必要な作業と確認

- 不明な IP アドレス（フェールオーバーやその他のフローティング IP など）を識別し、それらが何であるかがわかるようにラベルでタグ付けします。

  [インベントリプロファイル（Inventory Profile）] ページで、役立つ詳細を確認できます。IP アドレスをクリックし、右側のペインで [インベントリプロファイルの表示（View Inventory Profile）] をクリックします。
- 明らかに望ましくない、または理にかなっていないものを探します。
- 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、単一のポリシーで複数のワークロードに対応できるようにします。インベントリフィルタの作成を参照してください。
- 必要に応じて、他のネットワーク管理者を調べて連絡し、表示されるポリシーの必要性を把握します。
- ポリシーの複雑さの対処 （95 ページ）の下のトピックも参照してください。各トピックには、手動および承認済みのポリシー、および自動的に検出されたポリシーが含まれます。
- 一般的に、範囲内のポリシーの最大数は、約500個以下にすることを推奨します。これよりも多くのポリシーがある場合は、同様のポリシーを統合できるかどうかを確認するか、範囲を分割することを検討してください。

- 確認しながら、正しいことがわかったポリシーをそのまま承認して、今後の検出の実行で保持します。

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. 該当する範囲とワークスペースに移動し、[ポリシーの管理（Manage Policies）] をクリックします。
2. [Policies] タブをクリックします。
3. [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。
4. [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。
5. [プロトコルとポート（Protocols and Ports）] 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。
6. [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。

   信頼度の説明を表示するには、[C] にカーソルを合わせます。
7. リスト内でサービスの信頼度の低い指標を探します。
8. 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）] タブで、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。

   信頼度の説明を表示するには、[C] にカーソルを合わせます。

フローの方向とポリシーの信頼度

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。

自動ポリシー検出結果のトラブルシューティング

自動ポリシー検出結果が予期したものでない場合は、次の点を確認します。

選択した時間範囲を拡張してより多くのデータを含める

時間枠を拡張してより多くのデータを含め、まれに発生するイベントをキャプチャします。たとえば、アプリケーションが複数のプロバイダーアプリケーションから取得したデータを使用して複雑な四半期レポートを生成する場合は、そのトラフィックが含まれている時間範囲が含まれていることを確認します。

特定の変更の前にデータが収集されないようにする

範囲の定義が変更された場合、または特定の時間より前に収集されたデータが何らかの理由で無効になった場合は、時間範囲にその時点より前のデータが含まれていないことを確認します。

紛らわしいトラフィックフローを除外する

除外フィルタを設定または変更する必要が生じる場合があります。

除外フィルタは複数の場所で設定でき、複数の場所で有効または無効にできます。それぞれの場所を確認します。

- ワークスペースに設定されている除外フィルタを確認します。
- [デフォルトのポリシー検出設定（Default Policy Discovery Config）] ページの下部で設定されている、デフォルトの除外フィルタを確認します。
- 自動ポリシー検出のワークスペースの設定の [詳細設定（Advanced Configurations）] セクションで、どの除外フィルタが有効になっているかを確認します。
- [デフォルトのポリシー検出設定（Default Policy Discovery Config）] ページの [詳細設定（Advanced Configurations）] セクションで、どの除外フィルタが有効になっているかを確認します。
- デフォルトの除外フィルタを使用する場合は、[デフォルトのポリシー検出設定（Default Policy Discovery Config）] ページで [保存（Save）] をクリックして、これらの設定を個々のワークスペースで使用できるようにしていることを確認します。

詳細については、除外フィルタ （33 ページ）およびサブトピックを参照してください。

コンシューマとプロバイダーが異なる範囲内にあるポリシーのトラブルシューティング

クロス範囲ポリシーのトラブルシューティング （116 ページ）を参照してください。

承認済みポリシーのステータスの確認

承認されたポリシーのトラブルシューティング （55 ページ） を参照してください。

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、[ポリシー（Policies）]ページで、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。

ポリシービューの要素

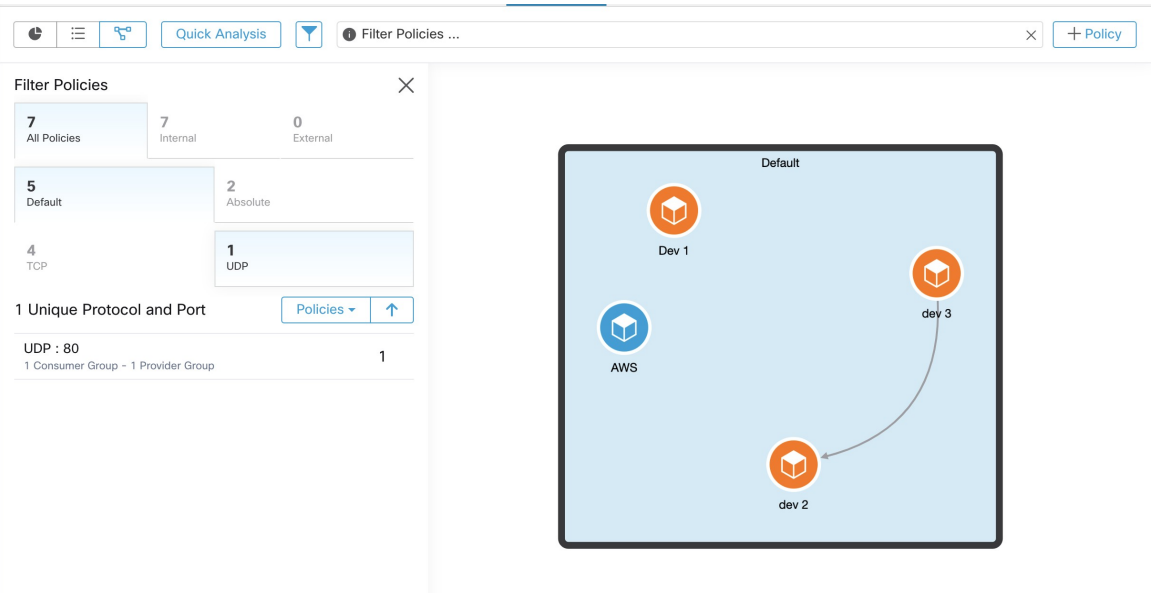
ポリシービューの視覚的な要素は次のとおりです。

要素	表す内容
青、オレンジ、または紫のアイコン	ノード（ポリシーのコンシューマまたはプロバイダー）
青のアイコン	範囲
オレンジのアイコン	インベントリフィルタ
紫のアイコン	クラスタ
2 つのアイコンをつないでいる線	1 つ以上のポリシー

ポリシービューのオプション

目的	操作手順
コンシューマノードまたはプロバイダーノードに含まれるワークロードのリストを表示する	ノードのアイコンをダブルクリックします。
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	それらをつないでいる線をダブルクリックします。右側のペインに詳細が表示されます。
ノードに送受信されるポリシーを表示する	アイコンをクリックします。
範囲内のワークロード間のポリシーのみを表示する	[内部（Internal）] ボタンをクリックします。
プロバイダーがコンシューマとは異なる範囲内にあるポリシーのみを表示する	[外部（External）] ボタンをクリックします。
詳細なフィルタリングオプションを使用する	フィルタテキスト入力ボックスの左側にある [(i)] ボタンをクリックしてオプションを表示し、フィルタ条件を入力します。

図 *53 :* グラフィカルビューでのポリシーのフィルタリング



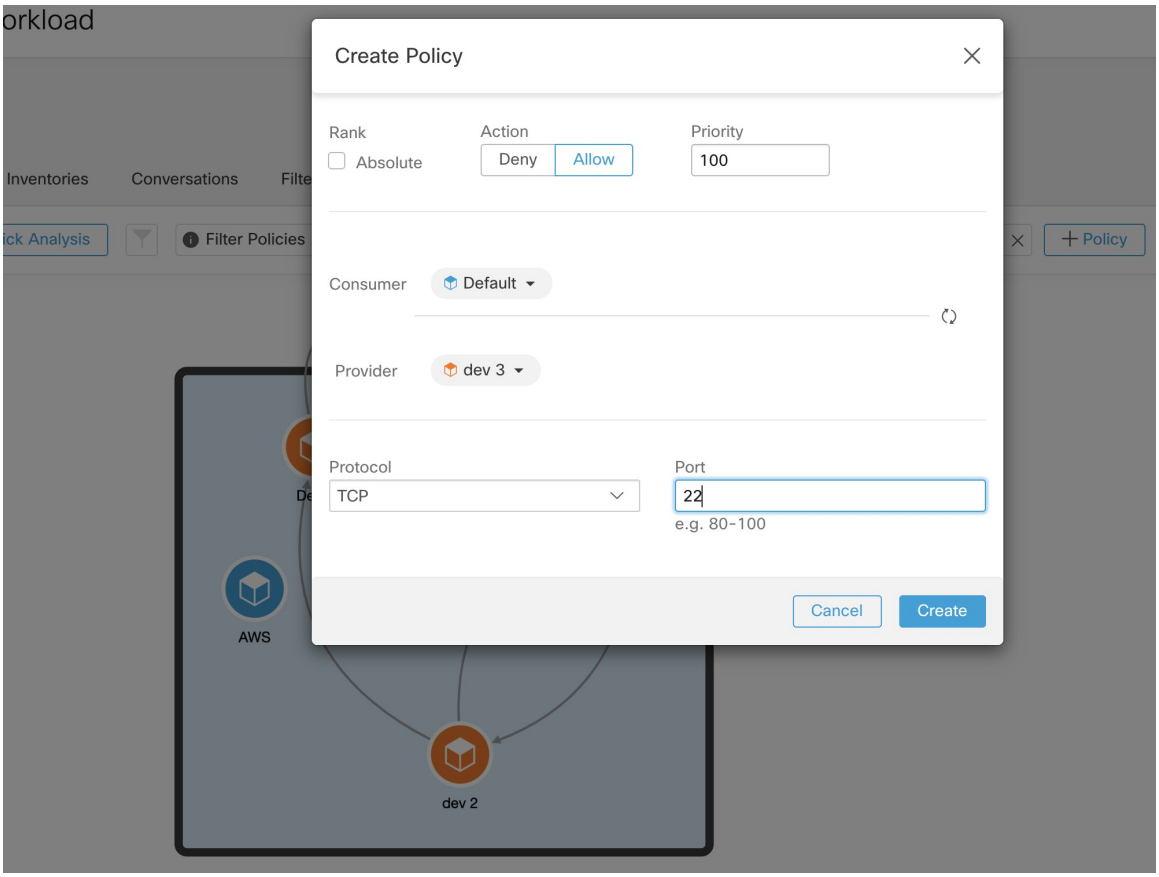
ポリシーのグラフィカルビューの高解像度画像をダウンロードするには、次の手順を実行します。

1. グラフの右下隅にある省略記号アイコンをクリックし、[画像のエクスポート（Export Image）] をクリックします。
2. 必要な解像度と画像のタイプを選択します。
3. [ダウンロード（Download）] をクリックします。

ポリシーの追加（ポリシービューページ）

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 *54* : グラフィカルビューでのポリシー作成



簡易分析

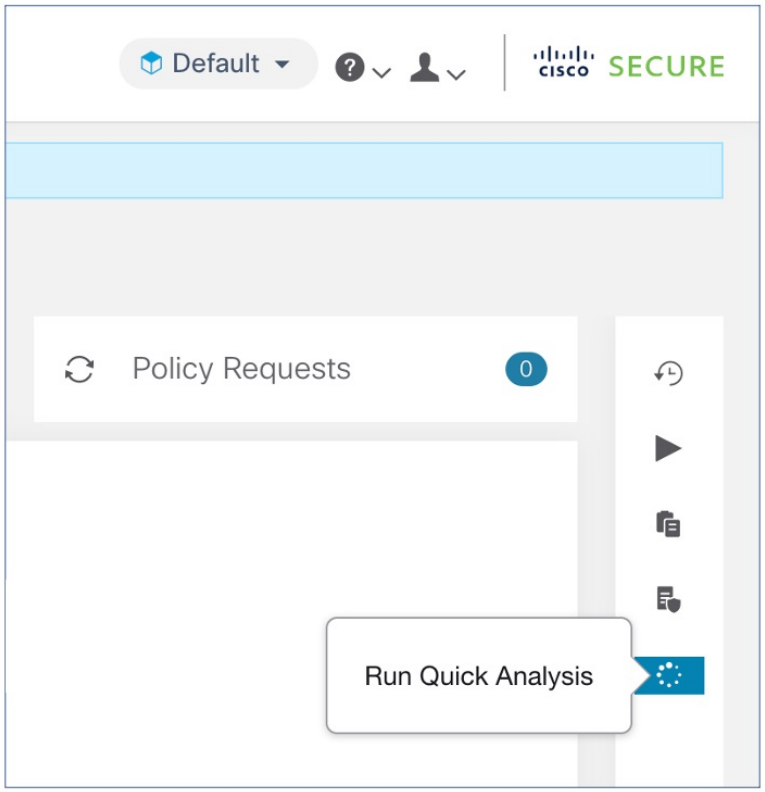
簡易分析により、現在のワークスペース内の全ポリシー、および他のワークスペースからの全関連ポリシーに対する仮想フローをテストできます。簡易分析により、ワークスペースのライブポリシー分析を実行しなくても、さまざまなセキュリティポリシーを使用したデバッグと試験が容易になります。

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 *55 : [*簡易分析（*Quick Analysis*）*]* タブ



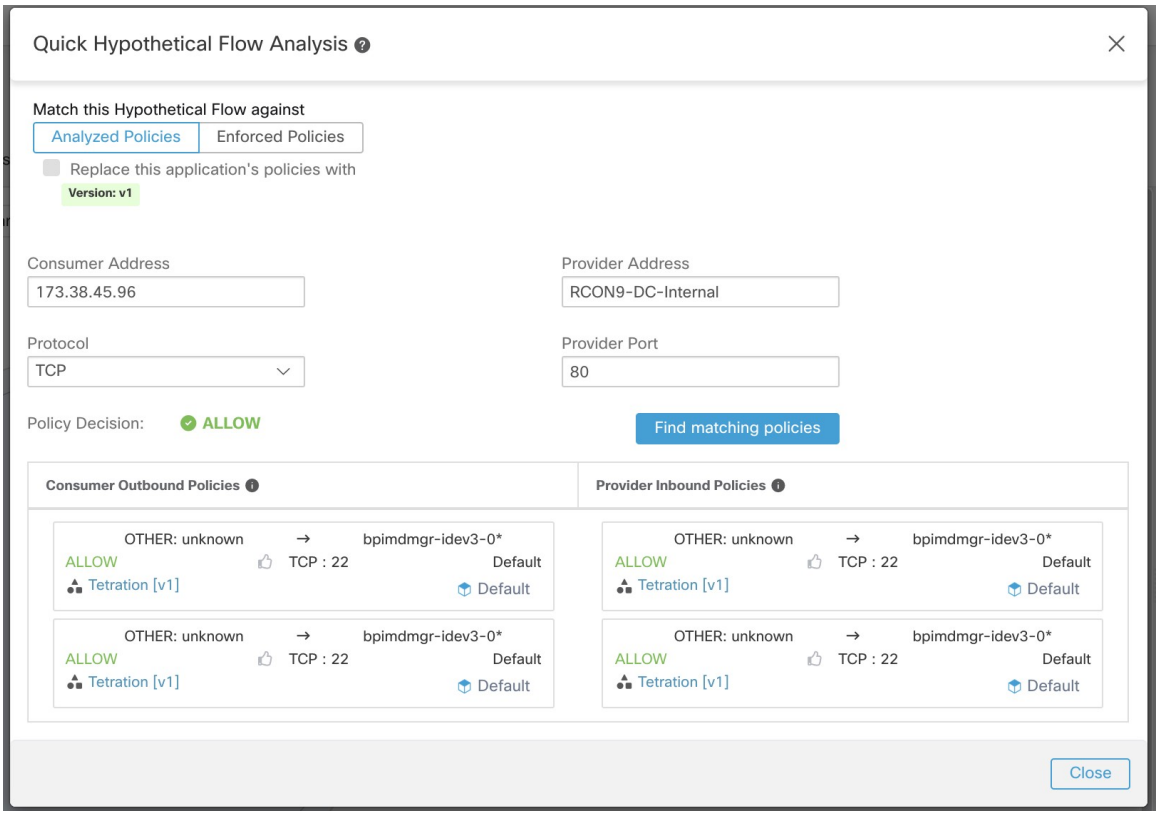
仮想フローのコンシューマ（クライアント）IP、プロバイダー（サーバー）IP、ポート、およびプロトコルを入力し、[一致するポリシーの検索（Find Policy Match）] ボタンをクリックします。

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。ワークスペースでのライブポリシー分析の実行は必要ありません。

図 *56* : 簡易ポリシー分析



ライブポリシー分析

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、ポリシーを適用する前に、ライブポリシー分析を使用して、ポリシーがネットワーク上の実際のトラフィックにどのように影響するかを確認する必要があります。

ライブポリシー分析は、次の質問に答えるために役立ちます。

- このワークスペースのポリシーがすぐに適用された場合、この範囲のアプリケーションにはどのような影響がありますか。
- 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。

  過去のトラフィックに対して現在のポリシーをテストするポリシー実験の実行（137 ページ）を参照してください。

- ポリシーは期待どおりに機能しますか。

ポリシーがあるすべてのワークスペースに対してポリシー分析を実行する必要があります。特定の範囲内のワークロードが他の範囲内のポリシーの影響を受ける可能性があるため、範囲にポリシーを適用する前に、単一の範囲に対してのみポリシー分析を実行しないでください。特

定の範囲内のトラフィックに影響を与える可能性のあるすべての範囲のポリシーを分析することを検討してください。

次に例を示します。

- ツリー内のこの範囲の上にある範囲で定義されたポリシーが、この範囲内のワークロードに適用される場合があります。
- この範囲内のワークロードが別の範囲内のワークロードと通信する場合、その範囲内のポリシーがこの通信に影響を与える場合があります。その範囲内でポリシー分析が開始されると（または、その範囲でのポリシーの変更後に最新のポリシーが分析されると）、この範囲のポリシー分析結果に影響する可能性があります。

変更によってアプリケーションが破損しないように、ポリシーを変更するたびにポリシー分析を実行する必要があります。

ワークスペースに対してライブポリシー分析を実行することは、ワークスペースの「パブリッシング」と呼ばれることがあります。

ライブポリシー分析の開始

自動ポリシー検出によってワークスペースで生成されたポリシーを確認し、希望どおりであることが確認できたら、ポリシー分析を開始できます。

始める前に

重要 ライブ分析には、同様にライブ分析を実行している他のワークスペースのポリシーの影響が含まれます。いずれかのワークスペースで適用を有効にしていて、そのワークスペースで分析が実行されていない場合、または適用されたポリシーのバージョンが分析されたポリシーのバージョンと同じでない場合、そのワークスペースのライブ分析結果は正確でない可能性があります。

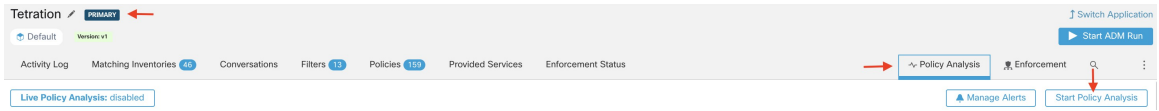
手順

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）] の右側の ••• をクリックして、ワークスペースを [プライマリ（Primary）] 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）] をクリックします。

図 *57*：ポリシー分析の有効化



次のタスク

- 他の範囲のポリシーをこの範囲のワークロードに適用できるため、この範囲の分析結果に影響を与える可能性がある他の範囲のポリシーを同時に分析することを検討してください。例：他の範囲で分析されたポリシーの影響 （132 ページ）を参照してください。
- エスケープされたフローが検出されたときに通知を受け取るには、[アラートの管理（Manage Alerts）] をクリックします。
- このページのツールを使用して、データをフィルタします。使用可能なフィルタ条件を表示するには、フィルタボックスの [(i)] ボタンをクリックします。
- ポリシー分析の開始後にポリシーを追加または変更した場合は、分析に変更内容を含めるために、分析を再起動する必要があります。ポリシーの変更後の、最新のポリシーの分析（139 ページ） を参照してください。

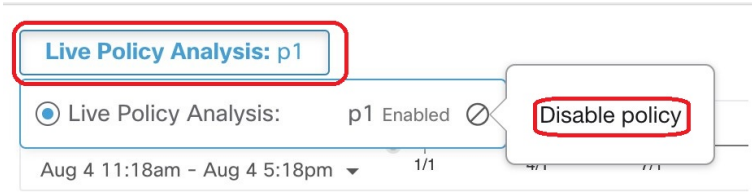
ライブポリシー分析の停止

通常、このワークスペースのポリシーは、分析している他のワークスペースのポリシー分析結果に影響を与える可能性があるため、ポリシーを適用した後でも、ポリシー分析の実行を続行する必要があります。

ライブポリシー分析を停止するには、次の手順を実行します。

[ライブポリシー分析：P<number>（Live Policy Analysis: P<number>）] ボタンをクリックし、[ポリシーの無効化（Disable policy）] をクリックします。

図 *58 :* ライブ分析ポリシーの無効化

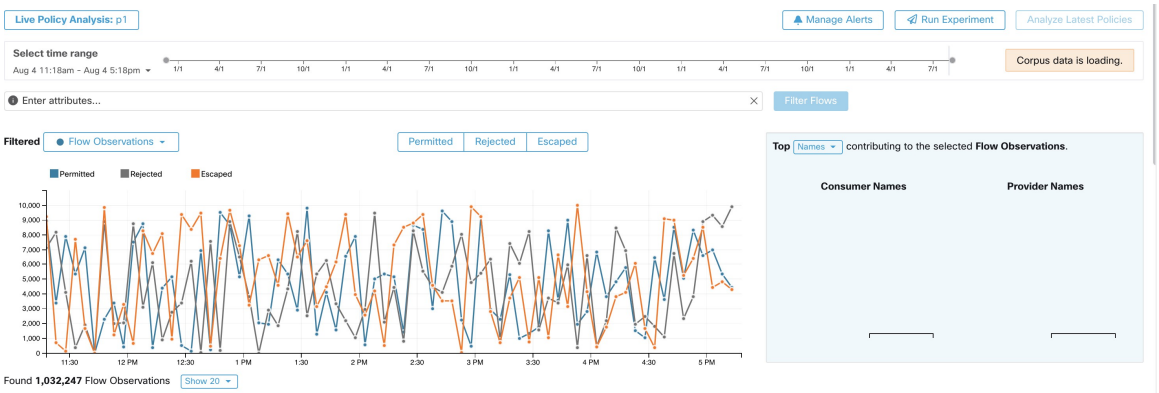


ポリシー分析結果：基本の理解

ポリシー分析中に、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と、その範囲内で移動するすべてのフローに、次のいずれかの結果が割り当てられます。

- [許可（Permitted）] : フローはネットワークによって許可され、分析されたポリシーによっても許可されました。
- [エスケープ（Escaped）] : フローはネットワークによって許可されましたが、分析されたポリシーに従ってドロップされました。
- [拒否（Rejected）] : フローは、ネットワークと分析されたポリシーによってドロップされました。

図 *59 :* ポリシー分析ページ



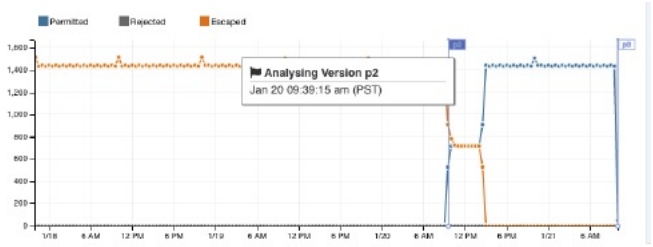
方向性を定めるために、次の点に注目してください。

- 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。
- 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タイプ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 つの結果タイプのいずれかに制限することができます。
- 右側にある上位N件チャートには、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、ポートなどが示されています。

  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（Ports）] を選択すると、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。

例：他の範囲で分析されたポリシーの影響

次の例では、午後 12 時頃までは、フローが許可されています。その時点で、別の範囲に関連付けられたワークスペースでポリシー分析が開始され、この範囲内のワークロードを持つトラフィックに影響を与えることで、フローがエスケープ済みとしてマークされます（この変更は、このワークスペースで新しく分析されたポリシー変更の結果ではないことがわかっています。この場合は、ラベルフラグが作成されるためです）。



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、分析されている他のワークスペースの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ライブ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ライブポリシー分析が有効になっている他のワークスペースのフローでマーキングされます。

（注） ライブポリシー分析を実行し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。

ポリシー分析の詳細

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、Secure Workload エージェントによって提供される信号と観察に基づいて、**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、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ワークロードのいずれかにエージェントがインストールされていて、両方には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

DROPPED ステータスは、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割り当てられます。エージェントでドロップが明示的に報告されていない場合、フローは PENDING ステータスを受け取ります。

処置が PENDING の場合は次のようになります。

- 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。
- 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。

シナリオの例：

- 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。
- パケットが送信元から出力された。

- 送信元側のエージェントのみが存在する場合、60秒以内に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可視性のみの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。
- 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 ステータスを受け取ります。それ以外の場合は、ALLOWED ステータスが割り当てられます。

フローを調査するための推奨手順

ポリシーの結果を調べるときに特定のフローにドリルダウンする場合は、次の提案とフィルタが役立つ場合があります。

1. まず、エスケープされたフローに焦点を当てます。

   エスケープされたフローには、特別な注意が必要です。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に基づいて意図されたアクションと異なるためです。これらのポリシーを適用しても、必要なフローがブロックされたり、アプリケーションに悪影響が及んだりすることがないことを調査して確認します。

   [エスケープ（Escaped）] などの違反タイプをクリックします。

   （後で、必要に応じて拒否されたフローと許可されたフローを確認できます）。

   エスケープされたフローは、以下を含みますがこれらに限定されない、さまざまな理由で発生する可能性があります。

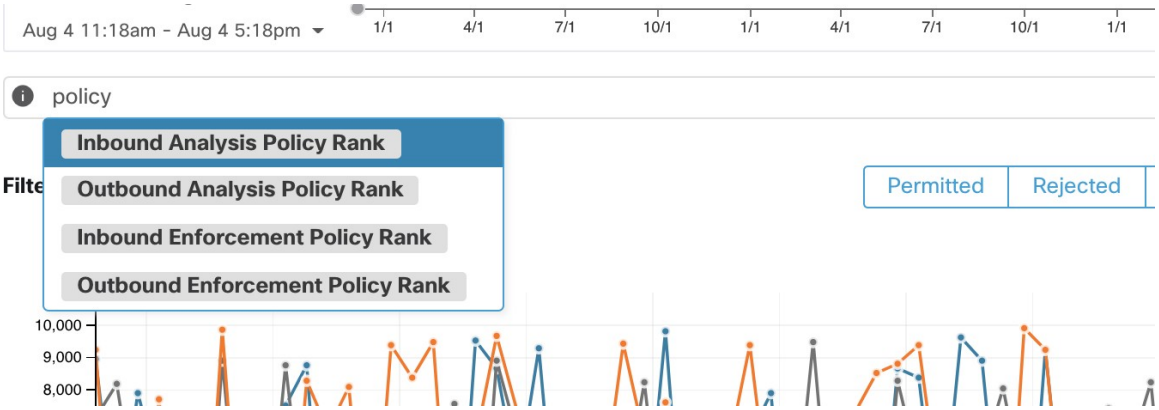
   - 優先順位の高い別のポリシーが有効になっている
   - トラフィックが、ポリシーで扱われるルートとは異なるパスを使用している
   - トラフィックが該当すると予想されるポリシーが、分析されていない（[ポリシー分析（Policy Analysis）] ページでエスケープされたフローを確認している場合）または適用されていない（[適用（Enforcement）] ページでエスケープされたフローを確認している場合）ワークスペース内にある。たとえば、先祖範囲内の場合や、同じ範囲内のセカンダリワークスペース内の場合も該当します。

2. キャッチオールポリシー（インバウンドとアウトバウンド）に一致したフローを特定します。

   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、対応するインバウンドまたはアウトバウンド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、注目するのがインバウンド、アウトバウンド、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します。

図 *60*：ランクのポリシー分析フィルタリングオプション



3. *Fwd flags does not contain RST, Rev flags does not contain RST* を使用して、RST がある TCP フローを除外します。

   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されたフローに集中できます。

4. 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。

   address type = IPv4, address type != IPv6 を使用してフィルタします。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. エスケープされたトラフィックに関連する最も頻繁なホスト名、ポート、アドレス、範囲などを特定することで、次の診断手順で焦点を当てるフローに優先順位を付けます。

   [上位N件（TopN）]機能ペインから、[ホスト名（Hostname）]、[ポート（Ports）]、または[アドレス（Addresses）]を選択します。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。

6. 前の手順で特定したホスト名、ポート、プロトコルなどのフローデータを検索します。

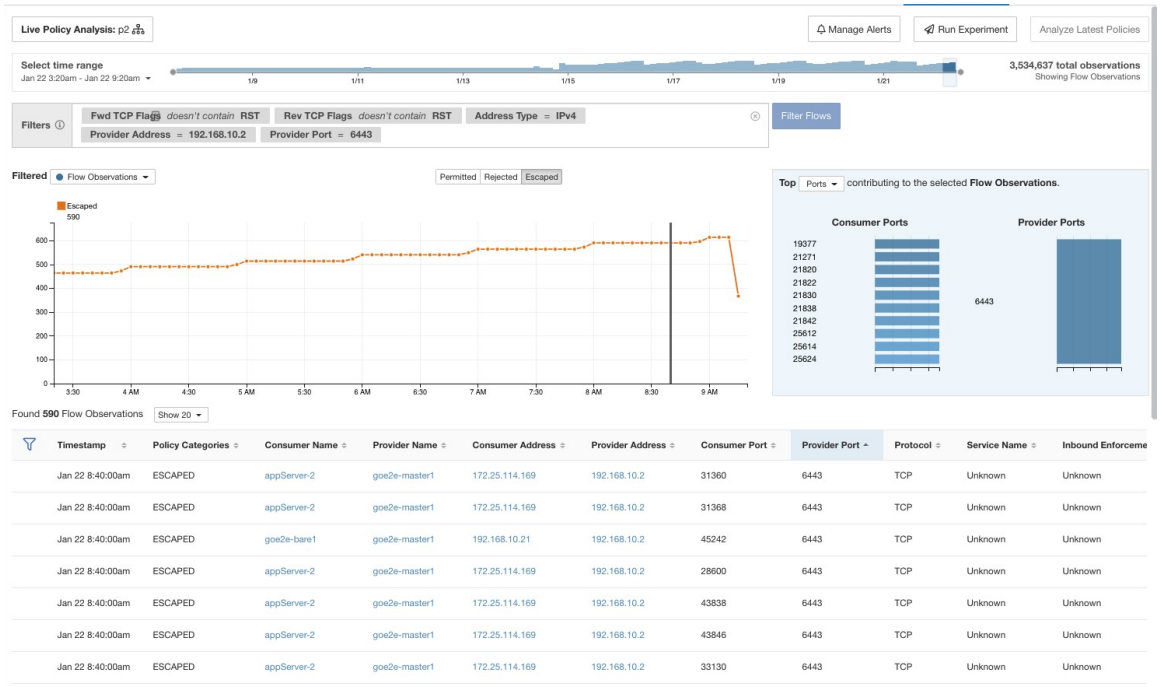
   対象となるフローのホスト名やポートなどに基づいた上位候補について心当たりがあれば、上位N件のクエリウィンドウで取得した値から直接ドリルダウンフィルタを適用するか、フロー検索フィルタバーに関連するフィルタを手動で入力して、フローをドリルダウンすることを選択できます。例：*Consumer Hostname contains {something}, Provider Hostname contains {something}, Provider Port = {some port number}, Protocol = TCP Protocol != ICMP*

7. 個々のフローを確認して迅速に分析します。

   最後に、フローに対応するテーブル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、上記で説明したフィルタリングの一部を使用して、エスケープされ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 *61* : ポリシー分析診断の例



過去のトラフィックに対して現在のポリシーをテストするポリシー実験の実行

既知の攻撃またはその他の重大な短期トラフィックパターンが過去に発生していて、現在のポリシー（または別のバージョン管理されたポリシーセット）でそのトラフィックがどのように処理されるかを確認する場合は、[実験の実行（Run Experiment）] 機能を使用できます。

始める前に

ヒント　この手順の代わりに、関連する時間範囲を含めて自動ポリシー検出を再度実行し、どのような異なるポリシーが提案されるかを確認することができます。

手順

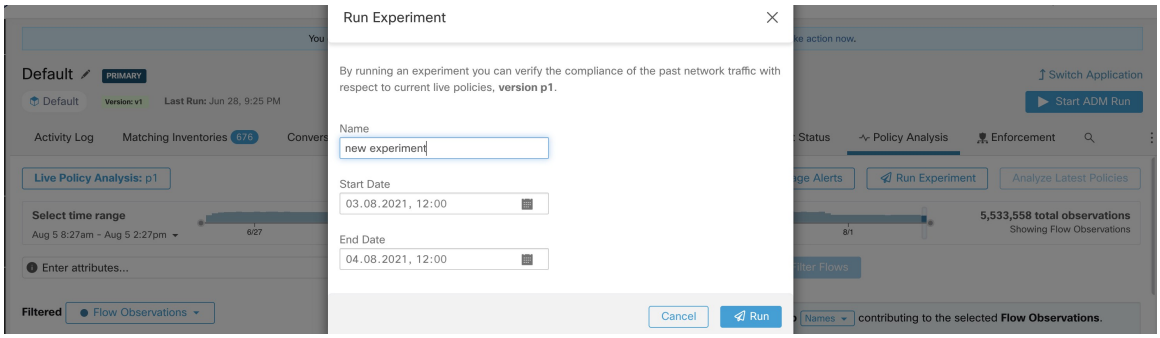
ステップ 1　選択したワークスペースの [ポリシー分析（Policy Analysis）] ページに移動します。

ステップ 2　ページの上部から、テストするポリシーバージョンを選択します。

ステップ 3　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 4　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。

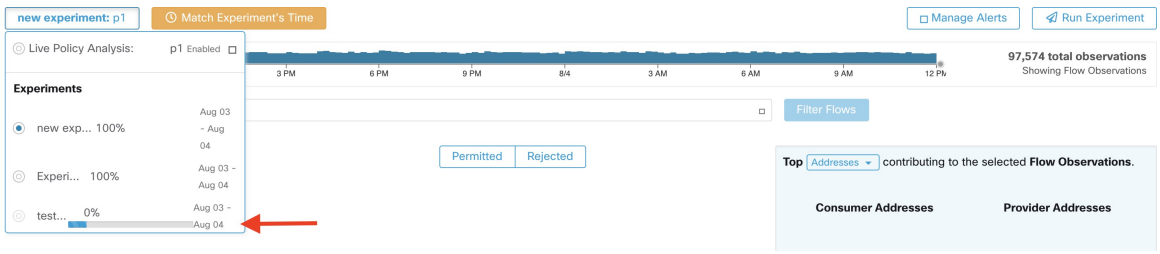
図 *62 : [*実験の実行（*Run Experiment***）*]* フォーム**



これにより、時間をさかのぼって、選択されたバージョン管理された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。

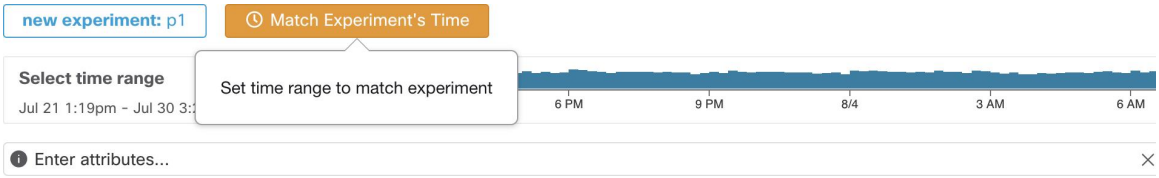
選択した期間によっては、このジョブに数分かかる場合があります。進行状況は、ポリシーセレクタメニューに表示されます。結果を表示する準備ができたら、他のバージョン管理されたポリシーと同様にポリシー実験を選択できるようになり、さまざまなフローカテゴリを示す時系列チャートが選択に応じて更新されます。

図 *63 :* 実験ステータスの表示



（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 *64 :* 時間範囲の適合化



ポリシーの変更後の、最新のポリシーの分析

ポリシー分析では、ワークスペース内のポリシーの変更は自動的に反映されません。変更を加えた後に現在のポリシーのセットを分析する準備ができたら、[最新のポリシーの分析（Analyze Latest Policies）] をクリックして、ポリシー分析に変更を反映させます。

ポリシー分析が最後に開始されてからワークスペース内のポリシーが変更されていない場合、またはポリシー分析が現在有効になっていない場合、[最新のポリシーの分析（Analyze Latest Policies）] ボタンは使用できません。ボタンをクリックできる場合は、まだ分析に含まれていないポリシー変更があります。

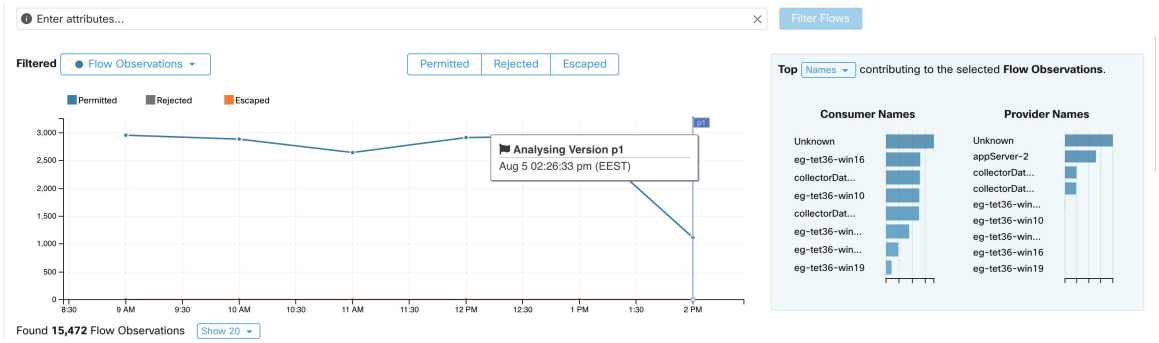
分析されたポリシーバージョンの表示、比較、および管理（140ページ）も参照してください。

ポリシーラベルのフラグ

ポリシー分析の時系列チャートでは、分析が開始された時点と、最新のポリシーとクラスタの変更を反映するために分析が再開始された各時点が、ポリシーラベルのフラグでマークされます。

フラグをクリックすると、そのフラグに関連付けられているポリシーのバージョンが表示されます。

図 *65 :* 時系列チャートのポリシーラベルのフラグ



ポリシーラベルのフラグをクリックすると、対応するバージョンの[ポリシー（Policies）]ページが開き、そのポリシー分析バージョンによって分析されたポリシーが表示されます。

分析されたポリシーバージョンの表示、比較、および管理

変更後にワークスペース内のポリシーを分析または再分析するたびに、新しい分析バージョン（p*）が作成されます。

バージョン管理の詳細については、ポリシーバージョン（v* および p*）について （161 ページ）を参照してください。

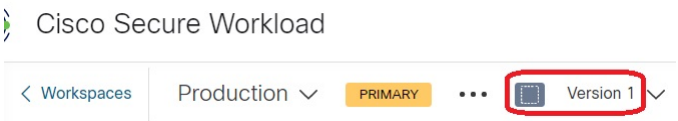
手順

ステップ 1 [防御（Defend）] > [セグメンテーション（Segmentation）] をクリックします。

ステップ 2 関連する範囲とプライマリワークスペースに移動します。

ステップ 3 [ポリシーの管理（Manage Policies）] をクリックします。

ステップ 4 現在表示されているポリシーのバージョンがページの上部に表示されます。



表示されるバージョンには、ポリシー検出バージョン、分析されたポリシーバージョン、または適用されたバージョンがあります。

ステップ 5 次の操作を実行できます。

別のバージョンのポリシーを表示するには、次の手順を実行します。	現在のバージョンをクリックし、別のバージョンを選択します。 バージョンの説明については、ポリシーバージョン（v* および p*）について （161 ページ）を参照してください。 **重要**v* バージョンを選択した場合は、このトピックの代わりに、トピックの最後にある重要な注意事項も含めて検出されたポリシーバージョンの表示、比較、および管理（58 ページ）を参照してください。
分析されたバージョンの詳細を表示するには、次の手順を実行します。	1. ページ上部の現在のバージョンの横にある[バージョン履歴の表示（View Version History）] をクリックします。 2. [公開されたバージョン（Published Versions）] タブをクリックして、分析および適用されたポリシーのバージョンを表示します。 3. バージョンのログエントリを表示するには、バージョン内のリンクをクリックします。 淡い緑色の行は、分析アクティビティを表しています。 明るい緑色の行は、適用アクティビティを表しています。

2つのバージョンを比較して変更点を確認するには、次の手順を実行します。	**1.** [リビジョンの比較（Compare Revisions）] をクリックします。 **2.** 比較するバージョンを選択します。 最新のドラフトバージョン、分析されたバージョン、および適用されたバージョンを比較できます。 **3.** 結果の詳細については、ポリシーバージョンの比較：ポリシーの差分 （164 ページ）を参照してください。
不要なバージョンを削除するには、次の手順を実行します。	バージョンの ⋮ をクリックし、[削除（Delete）] を選択します。 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。
バージョンをエクスポートするには、次の手順を実行します。	バージョンの ⋮ をクリックし、[エクスポート...（Export...）] を選択します。 ワークスペースのエクスポート （64 ページ）も参照してください。

次のタスク

バージョンの操作が完了したら、ワークスペースページの上部にあるバージョンを、最新の検出されたポリシーバージョン（v*）に変更します。

これにより、検出されたポリシーバージョンの意図しない削除を防ぐことができ、ワークスペースでポリシーを手動で作成することができます。

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（「アクティビティログとバージョン履歴」を参照）。

- ポリシー分析の有効化

  図 *66*：ポリシー分析の有効化

- ポリシー分析の無効化

  図 *67*：ポリシー分析の無効化

- ポリシー分析の更新

図 *68* : ポリシー分析の更新

ポリシーの適用

Secure Workload は、次の方法でポリシーを適用できます。

- 個々のワークロードにインストールされたソフトウェアエージェント：
  - Linux
  - Windows
  - Kubernetes/OpenShift

  各プラットフォームでのエージェントの動作に関する技術的な詳細については、エージェントによるポリシーの適用およびコンテナへの適用 （151 ページ）を参照してください。
- クラウドコネクタ：
  - AWS コネクタを介した AWS
  - Azure コネクタを介した Azure
- 外部オーケストレータを介した統合ロードバランサ：
  - F5 BIG-IP
  - Citrix Netscaler
- Cisco Secure Firewall Management Center との統合
- サードパーティのインフラストラクチャでの適用のための、サードパーティのオーケストレータへのストリーミング

注意 ポリシーを適用すると、**影響を受けるホストに新しい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。

エージェントの正常性と適用の準備状況の確認

これらのチェックの一部は、ポリシーを適用する前または後に実行できます。

エージェントまたはコネクタの機能を変更するには、権限が必要な場合があります。関連する章の要件と前提条件を参照してください。

ポリシーを適用する予定のないワークロードに対しては、これらのチェックを実行する必要はありません。

確認内容：	詳細情報
エージェントが、適用されたワークスペースに関連付けられた範囲内のすべてのワークロードにインストールされている	[防御（Defend）]>[セグメンテーション（Segmentation）]をクリックし、関連する範囲とワークスペースに移動します。[一致するインベントリ（Matching Inventories）]をクリックし、[IPアドレス（IP Addresses）]をクリックします。 このタブのIPアドレスには通常はエージェントがインストールされていないため、ポリシーを適用するには通常はエージェントをインストールする必要があります。 例外：[IPアドレス（IP Addresses）]タブに表示される次のタイプのインベントリに対しては、適用が行われます。 • クラウドコネクタを使用してポリシーが適用される、クラウドベースのインベントリ（個々のワークロードへのエージェントのインストールはオプションです）。 • エージェントが個々のワークロードポッドにインストールされている場合、Kubernetesアドレスが[IPアドレス（IP Addresses）]リストに表示されます。エージェントがインストールされたKubernetesインベントリが[ポッド（Pods）]タブに表示されます。
インストールされているエージェントのバージョンが最新であり、サポートされている	インストールされているエージェントのバージョンの概要については、[管理（Manage）]>[エージェント（Agents）]をクリックしてから、[分布（Distribution）]をクリックして、[エージェントソフトウェアバージョンの分布（Agent Software Version Distribution）]チャートを確認します。 詳細については、[管理（Manage）]>[エージェント（Agents）]をクリックしてから、[エージェントリスト（Agents List）]をクリックします。
インストールされているエージェントに適用機能がある	[管理（Manage）]>[エージェント（Agents）]をクリックしてから、[適用エージェントに変換（Convert to Enforcement Agent）]をクリックします。 [フィルタ（Filter）]ボックスに、**`Agent Type = Deep Visibility`**と入力します。 ポリシーを適用する必要があるすべてのエージェントを変換します。

確認内容：	詳細情報
すべてのエージェントで適用が有効になっている	（この要件は、エージェントに適用機能があることを確認することや、ワークスペースで適用を有効にすることとは異なります）。 **重要**展開によっては、ワークスペースを適用する前または後にこれを行う必要があります。 「エージェントの適用が有効になっていることの確認」の項を参照してください。
エージェント以外の適用メカニズムで適用が有効になっている	**重要**：ワークスペースでポリシーを適用するまでは、エージェントを使用せずにクラウドコネクタで適用を有効にしないでください。 また、適用を可能にするには、適用をサポートする外部オーケストレータも有効にする必要があります。
エージェント設定プロファイルの [ルールの保持（Preserve Rules）] 設定が、ワークロードプラットフォームに適している	• Kubernetes/OpenShift については、「コンテナへの適用」の項を参照してください。 • 他のプラットフォームについては、「ソフトウェアエージェント」の項の各プラットフォームの情報を参照してください。 ヒント：このドキュメントで「ルールの保持」を検索すると、役立つ情報が見つかります。
（ワークスペースが適用された後に）すべてのエージェントがワークロードに適用可能なポリシーを受信した	「適用されたポリシーがエージェントにプッシュされていることの確認」の項を参照してください。

確認内容：	詳細情報
エージェントが正常である	上記のソースに加えて、次の場所にエージェントの正常性に関する情報があります。 • [管理（Manage）] > [エージェント（Agents）] をクリックしてから、[モニター（Monitor）] をクリックします。 [適用エージェント（Enforcement Agents）] の下の情報を確認します。 • [管理（Manage）] > [エージェント（Agents）] をクリックしてから、[分布（Distribution）] をクリックします。 ページの上部からエージェントタイプを選択します。 • [整理（Organize）] > [範囲とインベントリ（Scopes and Inventory）] をクリックして、対象の特定のワークロードを見つけるためにフィルタし、IP アドレスをクリックします。 [エージェントの正常性（Agent Health）] パネルが含まれている別のブラウザウィンドウで、[ワークロードプロファイル（Workload Profile）] ページが開きます。 詳細については、「ワークロードプロファイル」の項を参照してください。

ポリシーの適用の有効化

⚠

注意 ポリシーを適用すると、既存のファイアウォールルールが削除され、このワークスペースの影響を受ける範囲内のすべてのワークロードに対して新しいファイアウォールルールが作成されます。

ポリシーが正しく機能することを適切に検証していない場合、ポリシーを適用すると、アプリケーションの動作方法が変更され、事業運営が中断される可能性があります。

始める前に

- 最初に、ポリシーを適用する場合は、キャッチオールを [許可（Allow）] に設定することを検討してください。次に、トラフィックをモニターして、キャッチオールルールに一致するものを確認します。キャッチオールルールに一致する必要なトラフィックがない場合は、キャッチオールを [拒否（Deny）] に設定できます。
- 一度に複数の範囲でワークスペースを適用する場合は、分析されたワークスペースのみを適用できます。以下の手順で説明する2番目の方法を使用して単一のワークスペースを適用する場合は、適用する前にワークスペース内のポリシーを分析することを強く推奨しますが、必須ではありません。

「ライブポリシー分析」およびサブトピックを参照してください。

- 単一の範囲を適用するためのウィザードは、複数の範囲を同時に適用するオプションを提供するウィザードよりも詳細です。ポリシー適用ウィザード（149ページ）の機能が必要な場合は、以下の手順で説明する 2 番目の方法を使用します。
- **重要**：ポリシーが正しいことを確認します。

  ワークスペースのポリシー結果は、他の範囲の適用されたポリシーの影響を受ける場合があります。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の適用されたポリシーによって、フローがどのような影響を受けるかが表示されます。たとえば、「実稼働ホストは非実稼働ホストと通信すべきではない（Production hosts should not talk with Non-Production hosts）」という広範なポリシーが親範囲の適用されたワークスペースにあると、子範囲のアプリケーションに属す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。

  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。

  [適用（Enforcement）]ページに表示される情報については、「ライブポリシー分析」およびサブトピックを参照してください（ライブ分析と同じ情報が [ポリシーの適用（Policy Enforcement）] ページにも適用されます）。

  ライブ分析の結果が [適用（Enforcement）] ページの結果と異なる場合は、分析対象の範囲、ポリシーバージョン、および時間範囲が、[適用（Enforcement）]ページで結果を生成するために使用されている範囲、ポリシーバージョン、および時間範囲と同じであることを確認します。

- エージェントが各プラットフォームでポリシーを適用する方法を理解します。参照先：
  - Windows と Linux のワークロードについては、エージェントによるポリシーの適用およびサブトピックを参照してください。
  - Kubernetes と OpenShift については、以下を参照してください。

    コンテナへの適用 （151 ページ）。
  - ロードバランサについては、以下を参照してください。

    Citrix Netscaler のポリシーの適用および

    F5 BIG-IP のポリシーの適用。
  - クラウドコネクタを使用して設定されたクラウドベースのワークロードについては、以下を参照してください。
    - AWS インベントリにセグメンテーションポリシーを適用するときのベストプラクティスおよびリンク先のトピック。
    - Azure Inventory にセグメンテーションポリシーを適用するときのベストプラクティスおよびリンク先のトピック。

- ポリシーを適用するには、必要な権限を持っている必要があります。

  範囲に対して適用以上の機能が必要です。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。詳細については、「ロール」を参照してください。

- 関連するすべてのインストールされたエージェントと、クラウドコネクタなどのその他の適用エンドポイントについて、ポリシーを適用する準備ができていることを確認します。

  エージェントの正常性と準備状況チェックのリストについては、エージェントの正常性と適用の準備状況の確認（142ページ）を参照してください（これらのチェックの一部は、適用後まで待機する必要があります。たとえば、ワークスペースで適用を有効にする前ではなく、有効にした後に、クラウドコネクタで適用を有効にする必要があります。インストールされたエージェントについては、通常、ワークスペースを適用する前にエージェント設定で適用を有効にします）。

手順

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

ステップ2 1つの範囲または同時に複数の範囲にポリシーを適用できます。

同時に複数の範囲にポリシーを適用するには、次の手順を実行します。

（このプロセスを使用して適用できるのは、分析済みのワークスペースのみです）。

a) 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）]ペインを表示します。

b) [適用の有効化（Enable Enforcement）] をクリックします。

c) [次へ（Next）] をクリックして、ウィザードを開始します。

d) 適用するワークスペースを1つ選択します。

（追加の範囲にワークスペースを適用するオプションは、ウィザードの最後のページにあります）。

e) [次へ（Next）] をクリックします。

f) 適用するそのワークスペースのバージョンを選択し、[次へ（Next）] をクリックします。

g) 別の範囲のポリシーを同時に適用するには、[+別のワークスペースの追加（+ Add Another Workspace）] をクリックし、手順を完了します。

必要に応じて、追加の範囲に対して繰り返します。

h) [同意して適用（Accept and Enforce）] をクリックします。

単一範囲にポリシーを適用するには、次の手順を実行します。

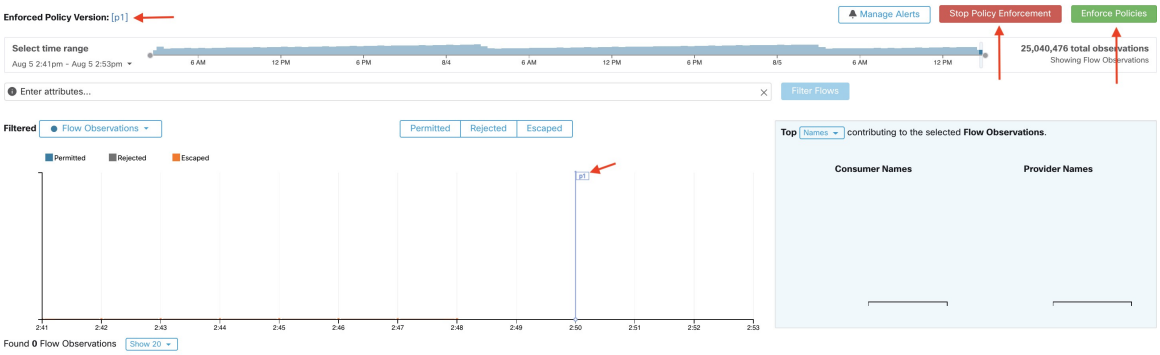
a) ポリシーを適用する範囲のプライマリワークスペースに移動します。
b) [ポリシーの管理（Manage Policies）] をクリックします。
c) [適用（Enforcement）] をクリックします。
d) [ポリシーの適用（Enforce Policies）] をクリックします。
e) ウィザードの手順に従います。

ウィザードの詳細については、ポリシー適用ウィザード （149 ページ）を参照してください。

ステップ 3 ウィザードの最後のページで [同意して適用（Accept and Enforce）] をクリックすると、このワークスペース内のポリシーの影響を受けるアセットに、新しいファイアウォールルールがプッシュされます。

適用時にラベルフラグが作成されます。

図 *69 :* 適用が有効化されている *[*ポリシーの適用（ *Policy Enforcement*）*]* ページ



フラグを表示するために、ページを更新する必要がある場合があります。

次のタスク

- 単一のワークスペースにポリシーを適用した場合は、予想される適用結果を得るために、他の範囲のワークスペースにも適用する必要があるかどうかを検討してください。

  たとえば、先祖範囲、またはクロス範囲ポリシーに関連するワークロードを含む範囲のワークスペースにも適用する必要がある場合があります。

- ポリシーを適用するエージェント、クラウドコネクタ、外部オーケストレータに対して適用が有効になるまで、適用は行われません。

- エージェントがインストールされているワークロードの場合は、関連する範囲とインベントリフィルタのエージェント設定でポリシーを適用します。「ソフトウェアエージェントの設定」およびサブトピックを参照してください。
- クラウドコネクタを使用して設定されたクラウドベースのワークロードについては、以下を参照してください。
  - AWS インベントリにセグメンテーションポリシーを適用するときのベストプラクティスおよびリンク先のトピック。
  - Azure Inventory にセグメンテーションポリシーを適用するときのベストプラクティスおよびリンク先のトピック。
- Kubernetes と OpenShift については、以下を参照してください。
  - コンテナへの適用 （151 ページ）
  - ソフトウェアエージェントの設定
- ロードバランサについては、以下を参照してください。
  - F5 BIG-IP のポリシーの適用

    F5 入力コントローラのポリシーの適用
  - Citrix Netscaler のポリシーの適用
- 適用が期待どおりに機能していることを確認します。適用が予想どおりに機能することの確認 （153 ページ）を参照してください。
- 適用が有効になった後にフローが拒否された場合など、問題が発生した場合に通知されるようにアラートを設定します。

ポリシー適用ウィザード

ワークスペースの [適用（Enforcement）] ページから単一のワークスペースにポリシーを適用する場合、ポリシー適用ウィザードでは次のことができます。

- ワークロードに導入する前にポリシーを確認する。

  これには、先祖範囲から継承されたポリシーが含まれます。
- 確認のためにポリシーの変更をダウンロードする。
- ポリシーバージョンを比較する。
- 適用するワークスペースの分析されたバージョンを選択する。
- 以前のバージョンにポリシーをロールバックする。

ポリシー適用ウィザードのステップ：

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。

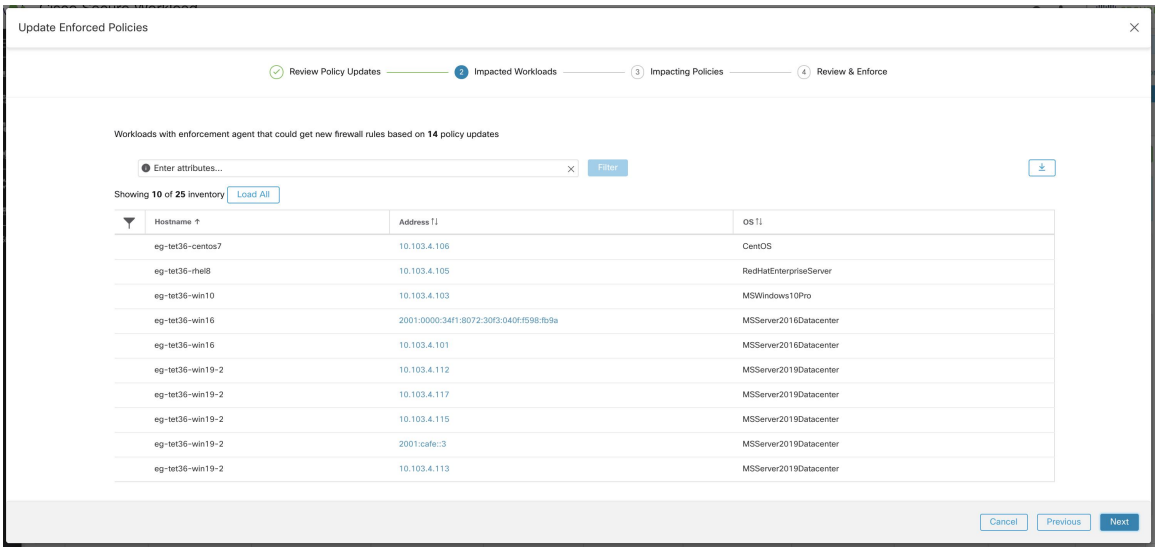
   「ポリシーバージョンの比較：ポリシーの差分」と同様に、ポリシーの変更をフィルタして確認し、CSV としてダウンロードすることができます。

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 *70*：影響を受けるワークロードのリスト

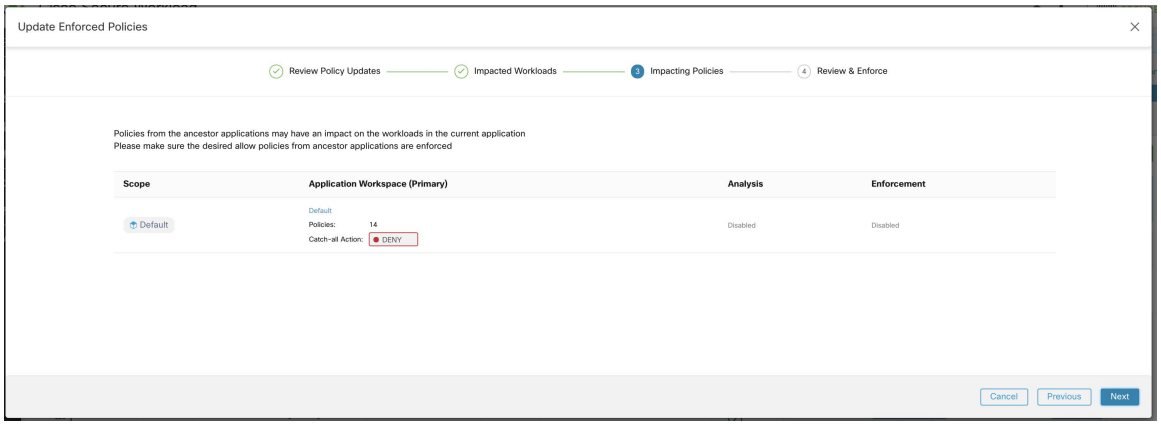


   インベントリ項目の表示、フィルタリング、ダウンロードの詳細については、インベントリを参照してください。

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、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 *71* : 先祖ワークスペースと適用バージョンのリスト

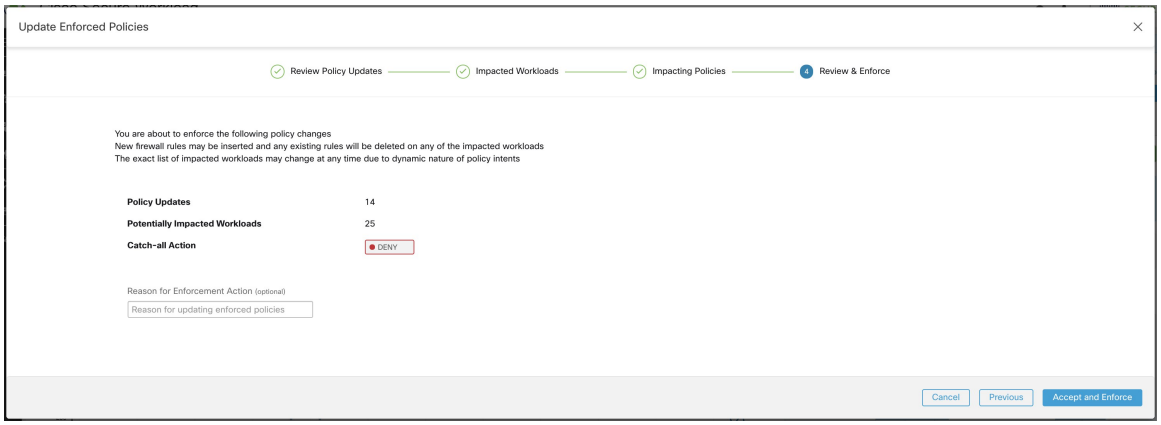


4. 確認と同意

この最後のステップでは、適用されるポリシー変更、影響を受ける可能性のあるワークロードの数、適用されるキャッチオールアクションの概要が示されます。[同意して適用（Accept and Enforce）] をクリックすると、ワークスペースのポリシーを使用して、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、理由のみを指定できます。

図 *72* : 概要の確認およびポリシーの変更の適用



コンテナへの適用

Kubernetes と OpenShift によって管理されるコンテナベースのワークロードでセグメンテーションを設定するために必要な手順の概要については、Kubernetes ベースのワークロードに対するマイクロセグメンテーションの設定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。**

Kubernetes によって追加された iptables ルールが適用によって干渉され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 = production 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 = production または orchestrator_environment = production	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 = production のラベル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 = production 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。

注意 **Kubernetes や OpenShift インベントリを含むポリシーは、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。

適用が予想どおりに機能することの確認

エージェントの確認

エージェントの正常性と適用の準備状況の確認 （142 ページ）を参照してください。

エスケープされたフローと拒否されたフローの確認

画面の左側のメニューで、[概要（Overview）] をクリックします。

[セキュリティダッシュボード（Security Dashboard）] ページで、[セグメンテーションコンプライアンススコア（Segmentation Compliance Score）] を確認します。

これが 100 未満の場合は、エスケープまたは拒否されたフローがある可能性があります。どちらもポリシー設定に問題があることを示しています。

詳細は、セグメンテーション コンプライアンス スコアを参照してください。

これらの状況の調査の詳細については、ポリシー分析結果：基本の理解 （131 ページ）とサブトピックを参照してください（これらのトピックの情報は、[適用（Enforcement）] タブに表示される適用されたポリシーと、[ポリシー分析（Policy Analysis）] タブに表示される分析されたポリシーに適用されます）。

欠落しているポリシーを追加するか、プロトコルやポートの追加などにより既存のポリシーを変更して、必要な正当なトラフィックを許可します。

その後、再適用する前に再分析します。

特定のワークロードの適用されたポリシー（具体的なポリシー）の表示

この手順を使用して、特定のワークロードに適用されているすべてのポリシー（つまり、そのワークロードの具体的なポリシー）を表示します。ワークスペース内のすべてのポリシーがワークスペース内のすべてのワークロードに適用されない場合や、複数のワークスペース内のポリシーが特定のワークロードに適用される場合があるため（たとえば、親または先祖の範囲内の継承されたポリシー）、このビューが役立ちます。

具体的なポリシーは、優先順位順にリストされます。優先順位の影響の詳細については、「ポリシーの優先順位」の項を参照してください。

始める前に

（注） 具体的なポリシーには、適用されたワークスペースのポリシーのみが含まれます。ワークスペースが適用されていない場合、ワークスペースが適用された場合にワークロードに適用されるポリシーは、リストに表示されません。

手順

ステップ 1 [インベントリ（Inventory）] ページまたはワークスペースから、ワークロードの [具体的なポリシー（Concrete Policies）] ページに移動できます。

[範囲とインベントリ（Scopes and Inventory）] ページから移動するには、次の手順を実行します。

a) [整理（Organize）] > [範囲とインベントリ（Scopes and Inventory）] を選択します。
b) 対象のワークロードの IP アドレスを検索してクリックします。

[ワークロードプロファイル（Workload Profile）] が別のタブで開きます。

一般的に、エージェントなしで管理されるクラウドベースのワークロードと、Kubernetes および OpenShift のワークロードを除いて、IP アドレスが [IPアドレス（IP Addresses）] タブには表示されていて、[ワークロード（Workloads）] タブには表示されていない場合は、エージェントがワークロードにインストールされていないことを意味します。そのため、ポリシーを適用できず、具体的なポリシーのリストもありません。

[セグメンテーション（Segmentation）] ページから移動するには、次の手順を実行します。

a) [防御（Defend）] > [セグメンテーション（Segmentation）] を選択します。
b) 範囲をクリックします。
c) プライマリワークスペースをクリックします。
d) [ポリシーの管理（Manage Policies）] をクリックします。
e) [一致するインベントリ（Matching Inventories）] タブをクリックします。
f) 対象のワークロードの IP アドレスを検索してクリックします。
g) 右側に表示されるパネルで、[ワークロードプロファイルの表示（View Workload Profile）] をクリックします。

[ワークロードプロファイル（Workload Profile）] が別のタブで開きます。

ステップ 2 [ワークロードプロファイル（Workload Profile）] ページの左側にあるメニューから、[具体的なポリシー（CONCRETE POLICIES）] をクリックします。

ステップ 3 行をクリックして、詳細を表示します。

詳細については、「[具体的なポリシー（Concrete Policies）] タブ」を参照してください。

ステップ 4 各ポリシーにヒットしたトラフィックの量を表示するには、次の手順を実行します。

a) [すべての統計情報の取得（Fetch All Stats）] をクリックします。

b) 目的の各ポリシーをクリックします。

ステップ 5 Kubernetes または OpenShift のワークロードに関する情報を表示するには、[コンテナポリシー（CONTAINER POLICIES）] をクリックします。

次のタスク

具体的なポリシーのステータスについては、 [モニター（Monitor）] > [適用ステータス（Enforcement Status）] を選択します。たとえば、ポリシーがスキップされたかどうかを確認できます。詳細については、「適用ステータス」の項を参照してください。

エージェントの適用が有効になっていることの確認

手順

ステップ 1 [防御（Defend）] > [適用ステータス（Enforcement Status）] をクリックします。

ステップ 2 特定の範囲の適用ステータスのみを表示するには、[範囲でフィルタ（Filter by Scope）] コントロールを切り替えて、範囲を選択します。

ステップ 3 [適用が有効なエージェント（Agent Enforcement Enabled）] チャートを確認します。

いずれかのエージェントが [非適用（Not Enforced）] であることがチャートに示されている場合は、この手順を続行します。

それ以外の場合は、すべてのエージェントで適用が有効になっているため、この手順の残りの部分はスキップします。

ステップ 4 チャートのオレンジの [非適用（Not Enforced）] セクションをクリックすると、チャートの下の表に影響を受けるワークロードが表示されます。

ステップ 5 エージェント設定プロファイルを変更して、これらのワークロードで適用を有効にします。

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。

適用されたポリシーがエージェントにプッシュされていることの確認

適用を行うには、各ワークロードに固有のポリシーが、そのワークロードにインストールされているエージェントに正常にプッシュされる必要があります。エージェントがインストールされていない場合でも、クラウドコネクタによって管理されているポリシー適用のステータスは表示されます。

始める前に

少なくとも 1 つの範囲にポリシーを適用します。

手順

ステップ 1 [防御（Defend）] > [適用ステータス（Enforcement Status）] をクリックします。

ステップ 2 特定の範囲の適用ステータスのみを表示するには、[範囲でフィルタ（Filter by Scope）] コントロールを切り替えて、範囲を選択します。

ステップ 3 [エージェントの具体的なポリシー（Agent Concrete Policies）] チャートを確認します。

チャートでいずれかに [スキップ（Skipped）] と表示されている場合は、この手順を続行します。

そうでない場合は、この手順の残りはスキップします。

ステップ 4 この問題の影響を受けるワークロードのリストを表示するには、チャートの赤色の [スキップ（Skipped）] スライスをクリックします。

影響を受けるワークロードが、チャートの下のテーブルに表示されます。

ステップ 5 この問題の原因を確認するには、次の手順を実行します。

検索結果の各ワークロードについて、[具体的なポリシー（Concrete Policies）] 列の [スキップ（Skipped）] の横にある [(i)] ボタンをクリックします。

エラー メッセージ	詳細情報
エージェントに Windows OS がありません（Agent doesn't have Windows OS）	Windows ワークロードにのみ適用されるポリシーの少なくとも 1 つに、Windows OS を実行していないコンシューマやプロバイダーが含まれています。 そのワークロードをそのポリシーから削除してください。
ポリシーの最大数に達しています（Maximum number of policies has been reached）	エージェントのポリシーが多すぎる場合（156 ページ）を参照してください。

次のタスク

（オプション）今後この状況が発生した場合に通知されるようにアラートを設定します。アラート を参照してください。

エージェントのポリシーが多すぎる場合

すべての適用できる具体的なポリシーを特定のエージェントにプッシュできない場合、ポリシーの最新バージョンはプッシュされません。

背景：各エージェントでサポートされるポリシーの数には制限があります。この制限は、クラウドコネクタを使用して適用されるポリシーにも適用されます。制限の情報が役立つ場合があります。

始める前に

適用されたポリシーがエージェントにプッシュされていることの確認（155ページ）でエージェントが適用されたすべてのポリシーに対応できないことが示された場合、その問題を解決するにはこの手順を使用します。

手順

ステップ1 影響を受ける範囲のプライマリワークスペースに移動します。

ステップ2 プライマリワークスペースでポリシーを変更します。

コンシューマまたはプロバイダーで、ポリシー数の削減と、IPアドレスの長いリストの削減を試みます。

たとえば、既存のポリシーを統合したり、IPアドレスの大規模なリストではなく、サブネットに基づくポリシーを使用したりします。

クラウドコネクタを使用して適用されるポリシーの場合、プラットフォームによって課される制限を増やすこともできます。クラウドプラットフォームのマニュアルを参照してください。

ステップ3 変更を加えたら、ワークスペースの最新バージョンを適用し、スキップされたポリシーを再度確認します。

ステップ4 この問題が発生している他の範囲に対して、この手順を繰り返します。

適用されたポリシーの変更

新規および変更されたポリシーの適用

適用後にポリシーを変更する必要がある場合は、通常、同じプライマリワークスペースで変更を行います。次に、変更を慎重に確認し、ワークスペースを再度分析して、期待どおりの効果があることを確認します。変更によって目的の効果が得られることを確認したら、ページの右上にある [最新のポリシーの適用（Enforce Latest Policies）] ボタンをクリックします。

適用されたポリシーバージョンの表示、比較、および管理

変更後にワークスペース内のポリシーを適用または再適用するたびに、新しいバージョン（p*）が作成されます。

バージョン管理の詳細については、ポリシーバージョン（v* および p*）について （161 ページ）を参照してください。

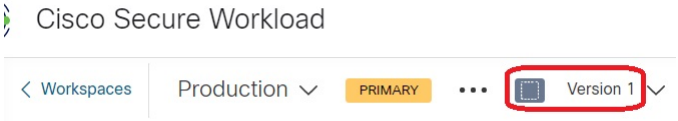
手順

ステップ 1 [防御（Defend）] > [セグメンテーション（Segmentation）] をクリックします。

ステップ 2 関連する範囲とプライマリワークスペースに移動します。

ステップ 3 [ポリシーの管理（Manage Policies）] をクリックします。

ステップ 4 現在表示されているポリシーのバージョンがページの上部に表示されます。



表示されるバージョンには、ポリシー検出バージョン、分析されたポリシーバージョン、または適用されたバージョンがあります。

ステップ 5 次のいずれかを実行します。

別のバージョンのポリシーを表示するには、次の手順を実行します。	現在のバージョンをクリックし、別のバージョンを選択します。 バージョンの説明については、ポリシーバージョン（v* および p*）について （161 ページ）を参照してください。 **重要**v* バージョンを選択した場合は、このトピックの代わりに、トピックの最後にある重要な注意事項も含めて検出されたポリシーバージョンの表示、比較、および管理 （58 ページ）を参照してください。
分析されたバージョンの詳細を表示するには、次の手順を実行します。	1. ページ上部の現在のバージョンの横にある [バージョン履歴の表示（View Version History）] をクリックします。 2. [公開されたバージョン（Published Versions）] タブをクリックして、分析および適用されたポリシーのバージョンを表示します。 3. バージョンのログエントリを表示するには、バージョン内のリンクをクリックします。 淡い緑色の行は、分析アクティビティを表しています。 明るい緑色の行は、適用アクティビティを表しています。

2つのバージョンを比較して変更点を確認するには、次の手順を実行します。	**1.** [リビジョンの比較（Compare Revisions）] をクリックします。 **2.** 比較するバージョンを選択します。 最新のドラフトバージョン、分析されたバージョン、および適用されたバージョンを比較できます。 **3.** 結果の詳細については、ポリシーバージョンの比較：ポリシーの差分 （164 ページ）を参照してください。
不要なバージョンを削除するには、次の手順を実行します。	バージョンの ⋮ をクリックし、[削除（Delete）] を選択します。 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。
バージョンをエクスポートするには、次の手順を実行します。	バージョンの ⋮ をクリックし、[エクスポート...（Export...）] を選択します。 ワークスペースのエクスポート （64 ページ）も参照してください。

次のタスク

バージョンの操作が完了したら、ワークスペースページの上部にあるバージョンを、最新の検出されたポリシーバージョン（v*）に変更します。

これにより、検出されたポリシーバージョンの意図しない削除を防ぐことができ、ワークスペースでポリシーを手動で作成することができます。

適用されたポリシーを以前のバージョンに戻す

適用されたポリシーを以前のバージョンにロールバックするには、ポリシーの適用の有効化（145 ページ）で説明されているプロセスのいずれかに従って、適用する以前のバージョンを選択します。

ポリシー適用の無効化

- **複数の範囲のポリシー適用を同時に無効にするには、次の手順を実行します。**

  ポリシーの適用の有効化（145 ページ）で説明されている、複数の範囲で同時にポリシーを適用する手順に従います。ウィザードの [バージョンを選択（Select Version）] ページで、[バージョンを選択してください（Select a version）] をクリックし、[適用の無効化（Disable Enforcement）] を選択します。

- **単一範囲のポリシー適用を無効にするには、次の手順を実行します。**

範囲のプライマリワークスペースの [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。

ポリシー更新の一時停止

⚠

注意 このオプションは、全範囲内のすべてのワークロードのポリシー更新を一時停止します。

この機能には、サイト管理者またはカスタマーサポートの権限が必要です。

全範囲内のすべての適用エンドポイントのルール更新を一時停止するには、次の手順を実行します。

1. [防御（Defend）] > [適用ステータス（Enforcement Status）] を選択します。
2. [ポリシー更新（Policy Updates）] の横にあるステータスをクリックします。
3. 注意を読んで同意します。

図 *73 :* ファイアウォールルールが継続的に更新されている場合

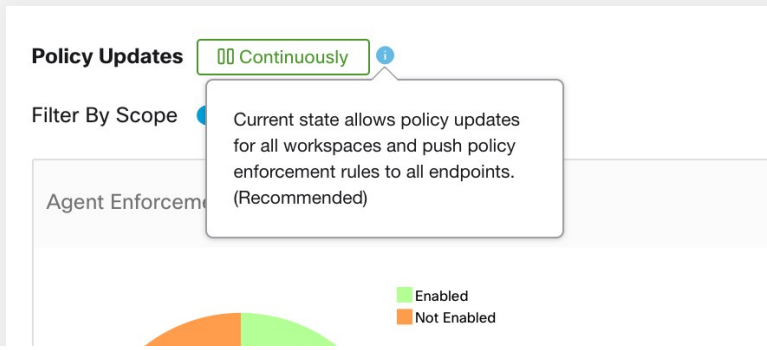


図 *74 :* ファイアウォールルールの更新が一時停止されている場合

適用履歴

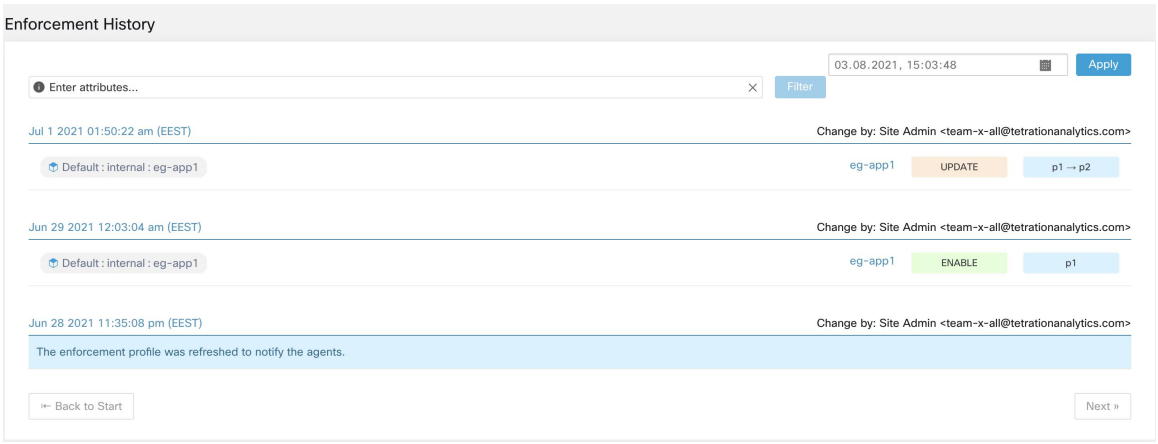
適用履歴には、適用されたワークスペースとそのバージョンのリストに対する変更のリストが表示されます。

適用履歴を表示するには、次の手順を実行します。

1. [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）] メニューを展開します。
2. [適用履歴（Enforcement History）] をクリックします。

   各セクションで、イベントについて説明され、変更内容の概要が表示されています。
3. 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 *75*：適用履歴ビュー

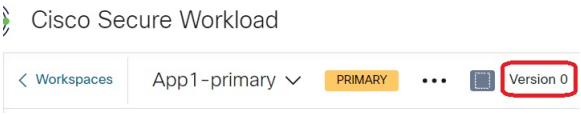


ポリシーバージョン（v* および p*）について

ポリシーバージョンは、ワークスペースバージョンと呼ばれることもあります。

表示されるバージョン

現在作業しているポリシー（およびクラスタ）のバージョンは、ワークスペースページの上部に表示されます。



- V* バージョンは、自動ポリシー検出によって生成されます。

  詳細については、以下を参照してください。

- P* バージョンは、分析されたバージョンや適用されたバージョンです。

  詳細については、以下を参照してください。

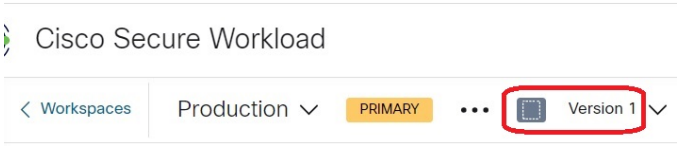
バージョン番号の横に、次のアイコンが表示される場合があります。

表 *6*: バージョンアイコン

	現在分析されているポリシーのバージョンを示します
	現在適用されているポリシーのバージョンを示します
	自動的に検出されたポリシーの最新バージョンを示します
（アイコンなし）	バージョンがそのタイプの最新バージョンではないことを示します

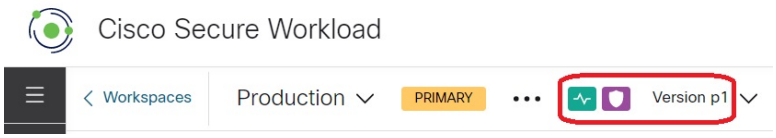
例：

- 表示されているバージョンは、ポリシーの最新の検出されたバージョンです。



- 表示されているバージョンは、現在分析されているポリシーのバージョンです。

- 表示されているバージョンは、現在分析および適用されているポリシーのバージョンです。



ポリシー検出バージョン（v*）

ワークスペースのポリシーを自動的に検出するたびに、バージョン（v*）が増加します。

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）。

ポリシーをインポートした場合も、v* バージョンが増加します。

v*バージョンを使用するには、検出されたポリシーバージョンの表示、比較、および管理（58ページ）を参照してください。

公開されたポリシーバージョン（p*）

ワークスペースの「公開された」ポリシーバージョン（p*）という用語は、次のいずれかを指します。

- 分析されたポリシーのバージョン、または
- 適用されたポリシーのバージョン

これらは、コンテキストに依存する、2 つの独立した類似しているバージョンです。

- 分析のポリシーバージョン：

  ワークスペースでポリシーを分析するたびに、または変更を行った後に [最新のポリシーの分析（Analyze Latest Policies）] をクリックするたびに、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、分析の「公開された」ポリシーバージョン（p*）の数字が増加します。最新の [ライブポリシー分析（Live Policy Analysis）] バージョンは、プライマリワークスペースの [ポリシー分析（Policy Analysis）] タブのページの左上に表示されます。

- 適用のポリシーバージョン：

  ワークスペースでポリシーの適用を有効にするたびに、または変更を行った後に適用を再度有効にするたびに、適用の「公開された」ポリシーバージョン（p*）が、適用ウィザードで選択した分析されたバージョンの番号になります。そのため、分析されたバージョン 5 を適用すると、たとえば、ワークスペースに初めてポリシーが適用された場合でも、適用されたバージョンもバージョン 5 になります。現在の [適用されたポリシーバージョン（Enforced Policy Version）] は、プライマリワークスペースの [適用（Enforcement）] タブのページの左上に表示されます。

公開された（p*）バージョンの管理

公開されたポリシー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） 公開されたポリシーバージョン（p*）は、合計100までに制限されます。この制限に達した場合、古いバージョンを削除する必要があります。

p*バージョンを管理および削除するには、分析されたポリシーバージョンの表示、比較、および管理 （140 ページ）または適用されたポリシーバージョンの表示、比較、および管理 （157 ページ）を参照してください。

API を使用して、公開されたバージョンを削除することもできます。

ポリシーバージョンの比較：ポリシーの差分

ポリシーを比較するには、検出されたポリシーバージョンの表示、比較、および管理（58ページ）、分析されたポリシーバージョンの表示、比較、および管理（140ページ）、または適用されたポリシーバージョンの表示、比較、および管理（157ページ）のトピックを参照してください。

ポリシーの変更は、3つのカテゴリ（[絶対（Absolute）]、[デフォルト（Default）]、[キャッチオール（Catch All）]）で表示されます。比較表の説明を以下に示します。

- 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 *7:* 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 *8* : *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 *76* : ポリシー差分ビュー

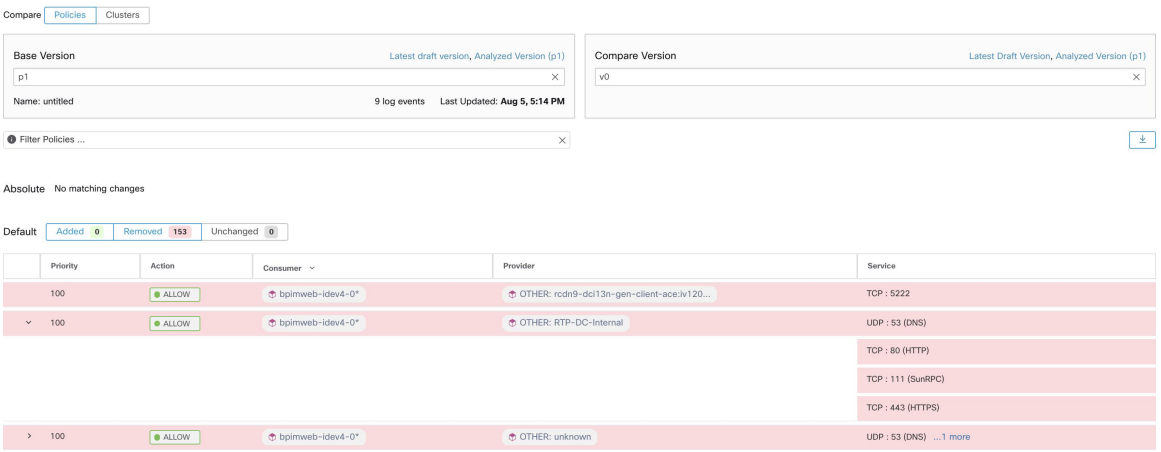


図 *77* : ポリシー差分ビューのダウンロードボタン

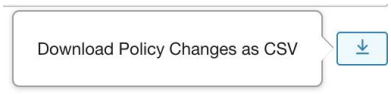


図 *78* : ポリシー差分ビューのフィルタリング

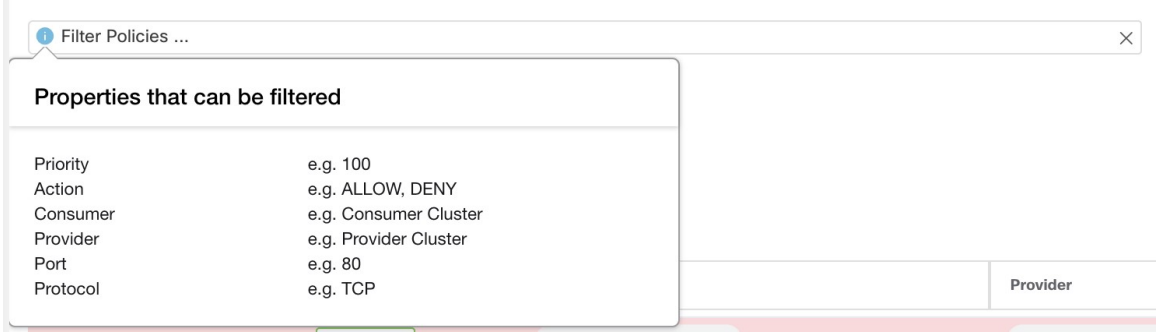


図 *79* : ポリシー差分ビューの差分タイプフィルタ

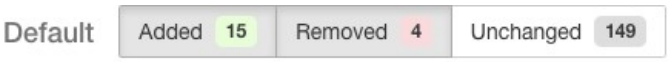


図 *80* : ポリシー差分ビューのグループ化

図 *81* : 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

ヒント 生成されたクラスタのバージョンの比較：差分ビュー （91 ページ）も参照してください。

アクティビティログとバージョン履歴

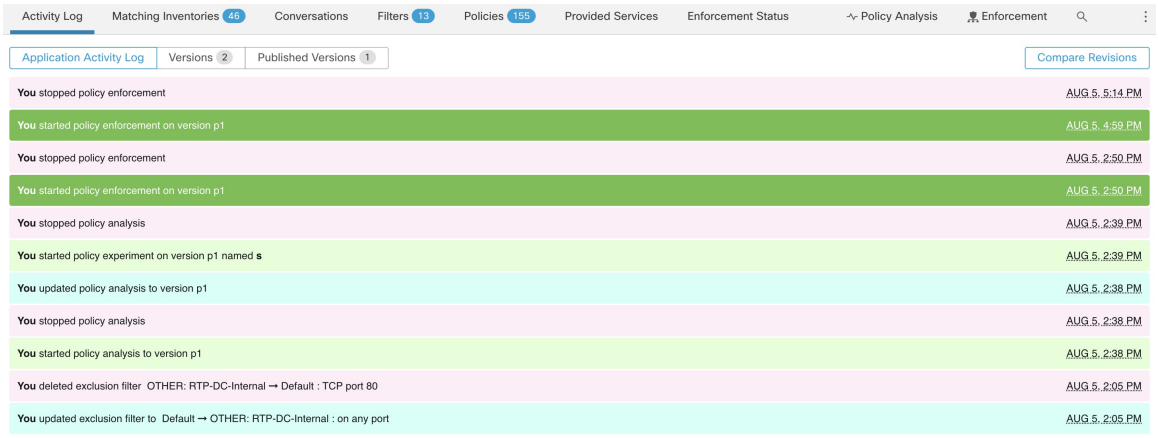
アクティビティログには、すべてのユーザーによる、ワークスペースに適用された変更の履歴が記録されます。表示されるイベントには、ワークロードとクラスタの追加、削除、名前変更、クラスタ間でのワークロードの移動、参考情報のアップロード、自動ポリシー検出の送信と中止などが含まれます。このビューには、それぞれの変更を行ったユーザーが表示されます。

ワークスペースの変更履歴を表示するには、ワークスペースの [アクティビティログ（Activity Log）] リンクをクリックします。

次に例を示します。

1. [防御（Defend）] > [セグメンテーション（Segmentation）] をクリックします。
2. 関連する範囲とワークスペースをクリックします。
3. [アクティビティログの表示（View Activity Logs）] リンクをクリックします。
4. [ワークスペースアクティビティログ（Workspace Activity Log）] タブをクリックします。

図 *82 : 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



ページのバージョン関連のタブとオプションについては、次を参照してください。

- ポリシーバージョン（v* および p*）について （161 ページ）
- 検出されたポリシーバージョンの表示、比較、および管理 （58 ページ）
- 分析されたポリシーバージョンの表示、比較、および管理 （140 ページ）
- 適用されたポリシーバージョンの表示、比較、および管理 （157 ページ）

古いポリシーバージョンの自動削除

6ヵ月間アクセスされていないワークスペースバージョンと、過去30日間アクセスされていないポリシー実験は、毎週自動的に削除されます。

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。

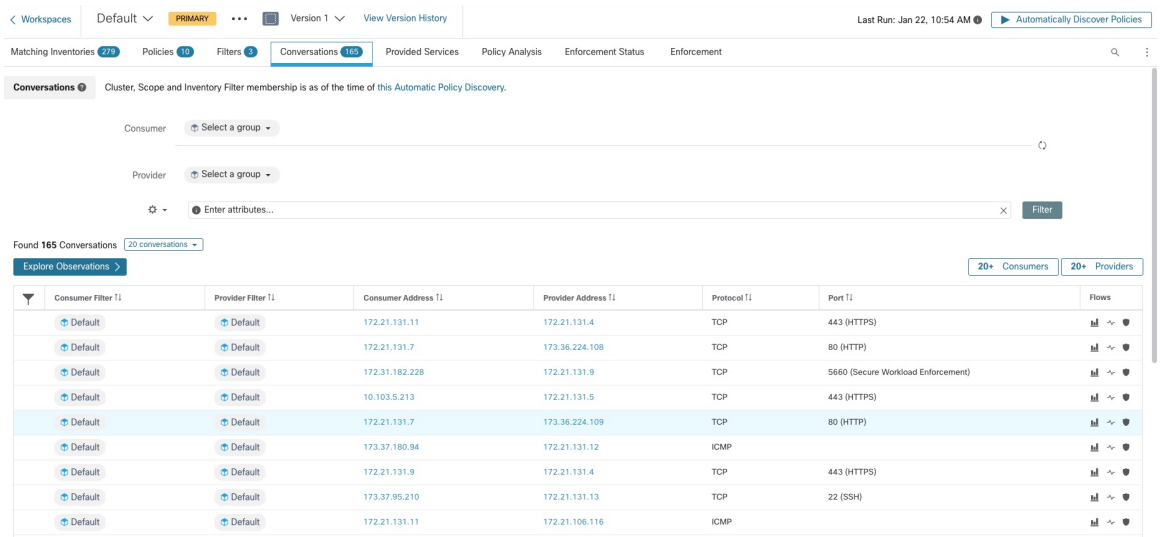
さらに、エージェントによって収集された情報は、未使用の L4 ポートを可視化します。未使用のポートとは、自動ポリシー検出に選択された間隔にわたり通信が確認されなかったポートです。この情報を使用して、これらのポートでの通信に関するポリシーを開いたり、未使用のポートにバインドされているアプリケーションを閉じたりして、ワークロードの攻撃対象領域を減らすことができます。

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 *83*：会話テーブルビュー

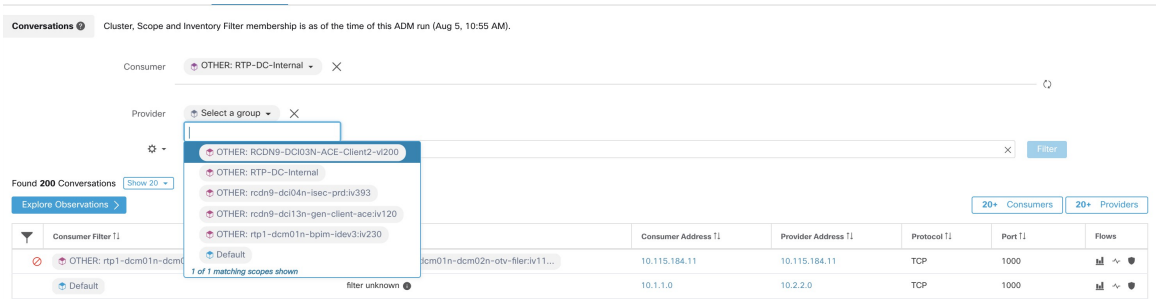


コンシューマまたはプロバイダーの選択

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 *84* : 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 *85* : カンバセーションフィルタ

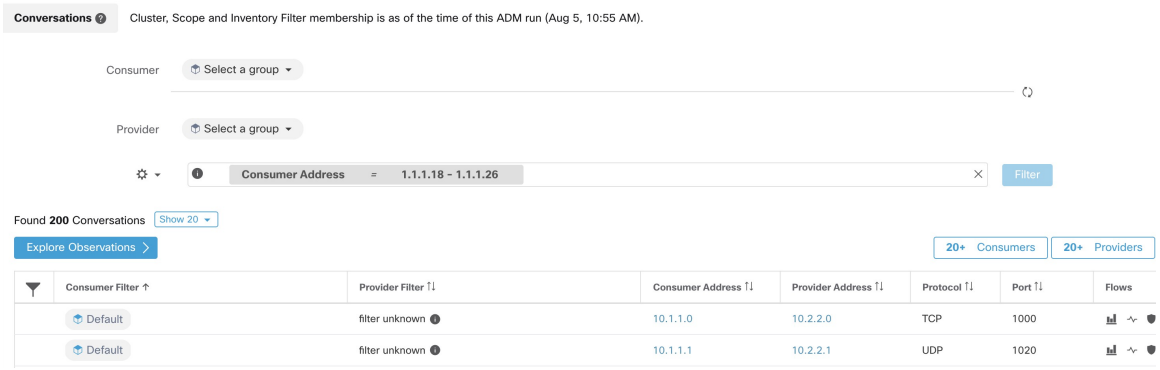
ここで、検索結果を絞り込むためのフィルタを定義します。[フィルタ（Filters）] という文字の横にある [?] アイコンをクリックすると、ディメンションの候補がすべて表示されます。ユーザーラベルデータについては、これらの列も適切な間隔で使用できます。この入力では、キーワード and、or、not、括弧もサポートされており、これらを使用してより複雑なフィルタ条件を表現できます。たとえば、IP 1.1.1.1 と 2.2.2.2 間の方向に依存しないフィルタは次のように記述できます。

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 *86 :* 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：

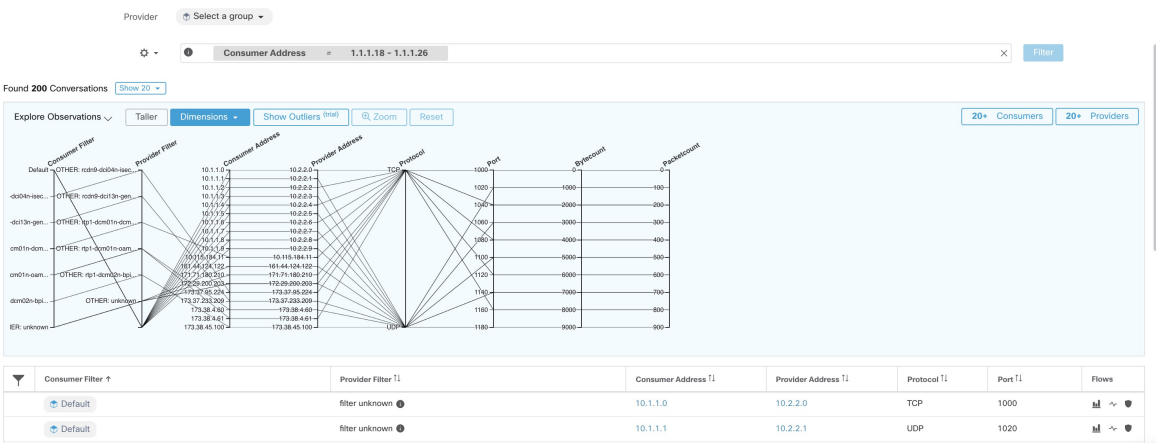
フィルタ	説明
コンシューマアドレス（**Consumer Address**）	CIDR 表記を使用してサブネットまたは IP アドレスを入力します（例：10.11.12.0/24）。コンシューマアドレスが入力した IP アドレスやサブネットと一致するフロー観測データを照合します。
プロバイダーアドレス（**Provider Address**）	CIDR 表記を使用してサブネットまたは IP アドレスを入力します（例：10.11.12.0/24）。プロバイダーアドレスが入力した IP アドレスやサブネットと一致するフロー観測データを照合します。
ポート（**Port**）	ポートが入力した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

フィルタ	説明
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）]。

観測結果の確認

[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 つの観測値を表し、その線がさまざまな軸と交差する場所は、その次元での観測値を示しています。より明確にするには、チャートの下にある観測結果のリストにカーソルを合わせます。これにより、チャート内の観測結果を示す線が強調表示されます。

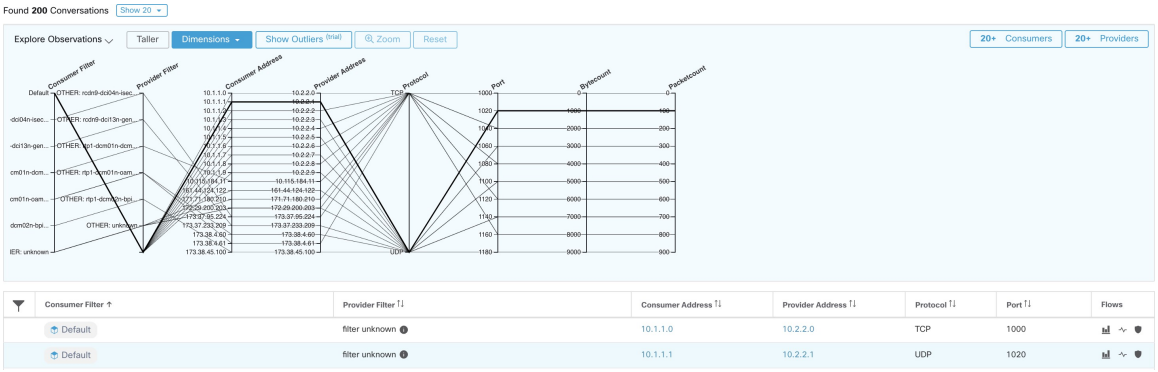
図 *87* : 観測結果の確認



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。

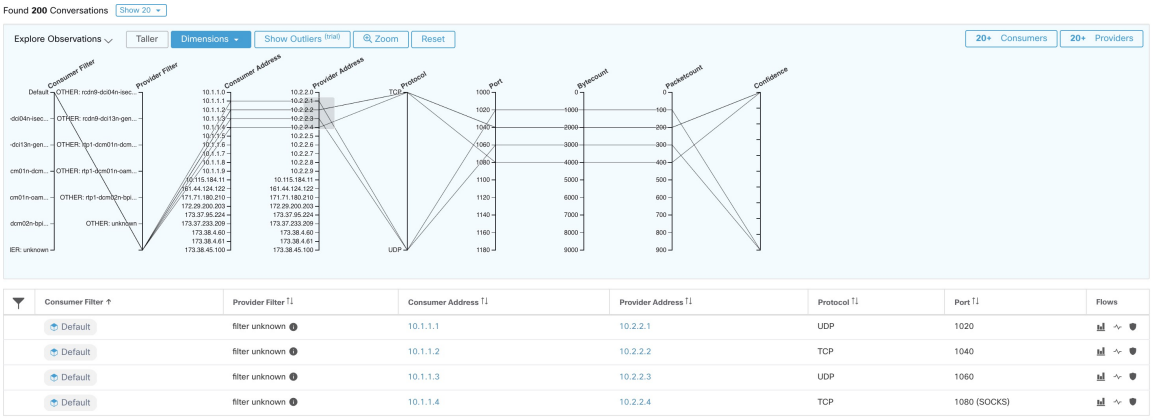
図 *88 :* ホバーによるカンバセーション観測



フィルタリング

いずれかの軸に沿ってカーソルをドラッグすると、選択範囲が作成され、その選択範囲に一致する観測データのみが表示されるようになります。軸を再度クリックすると、いつでも選択範囲を解除できます。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 *89 : Filtering*

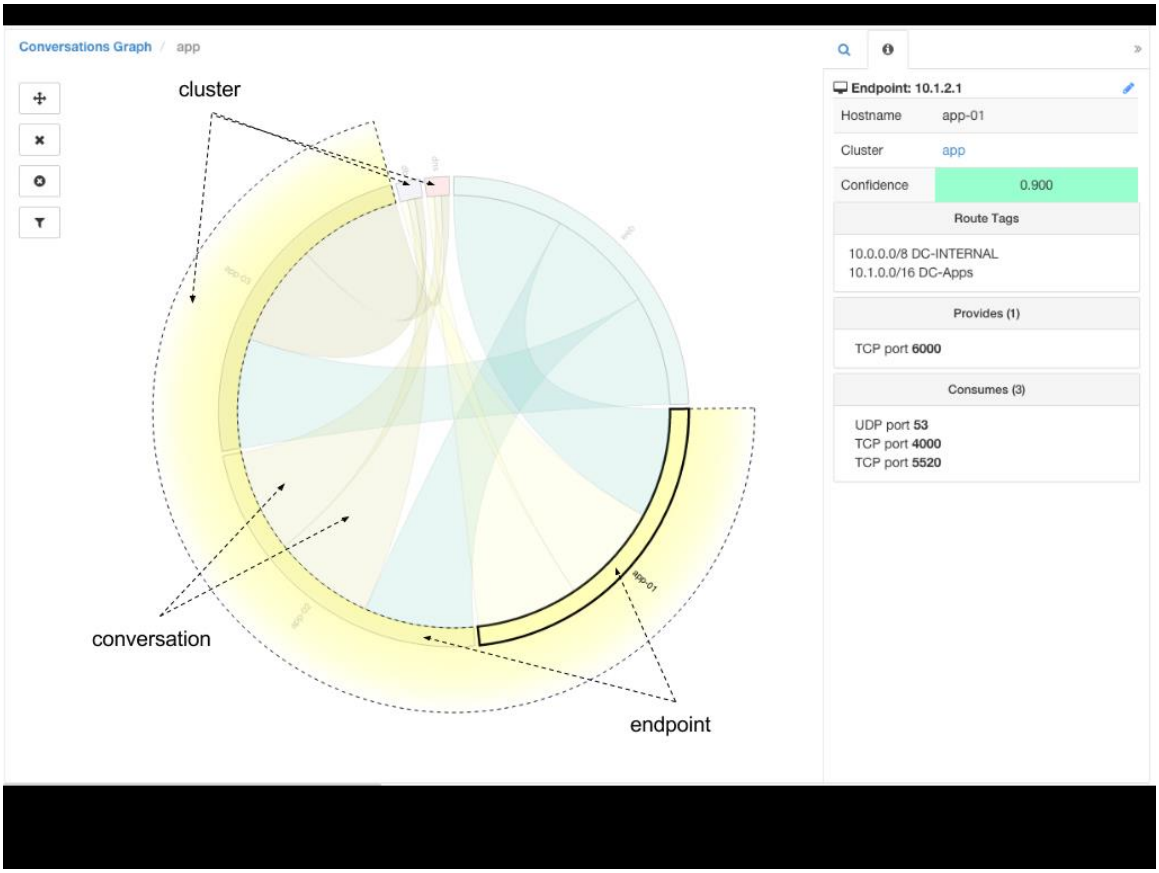


会話チャートビュー

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 *90* : 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 *91* : カンバセーションテーブルの上部

図 *92 :* 上位のコンシューマモーダル

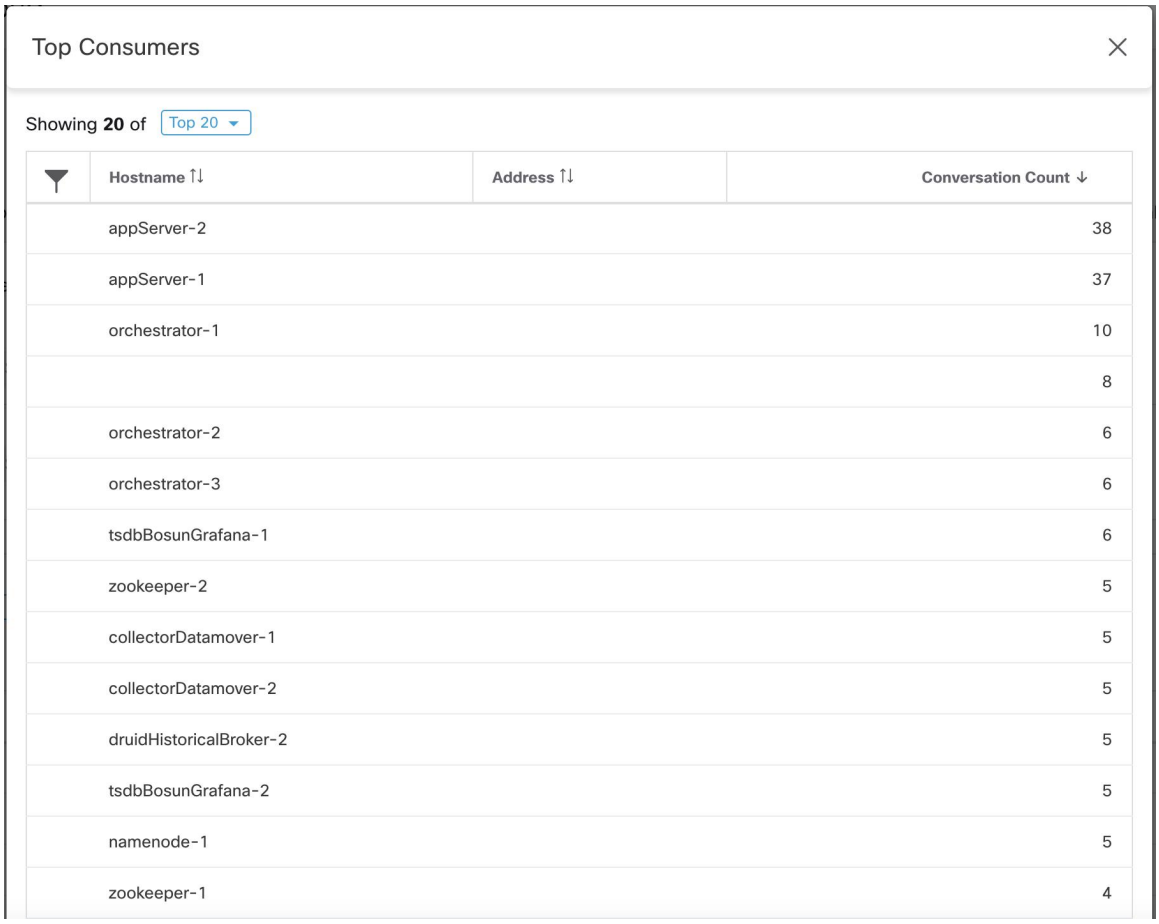
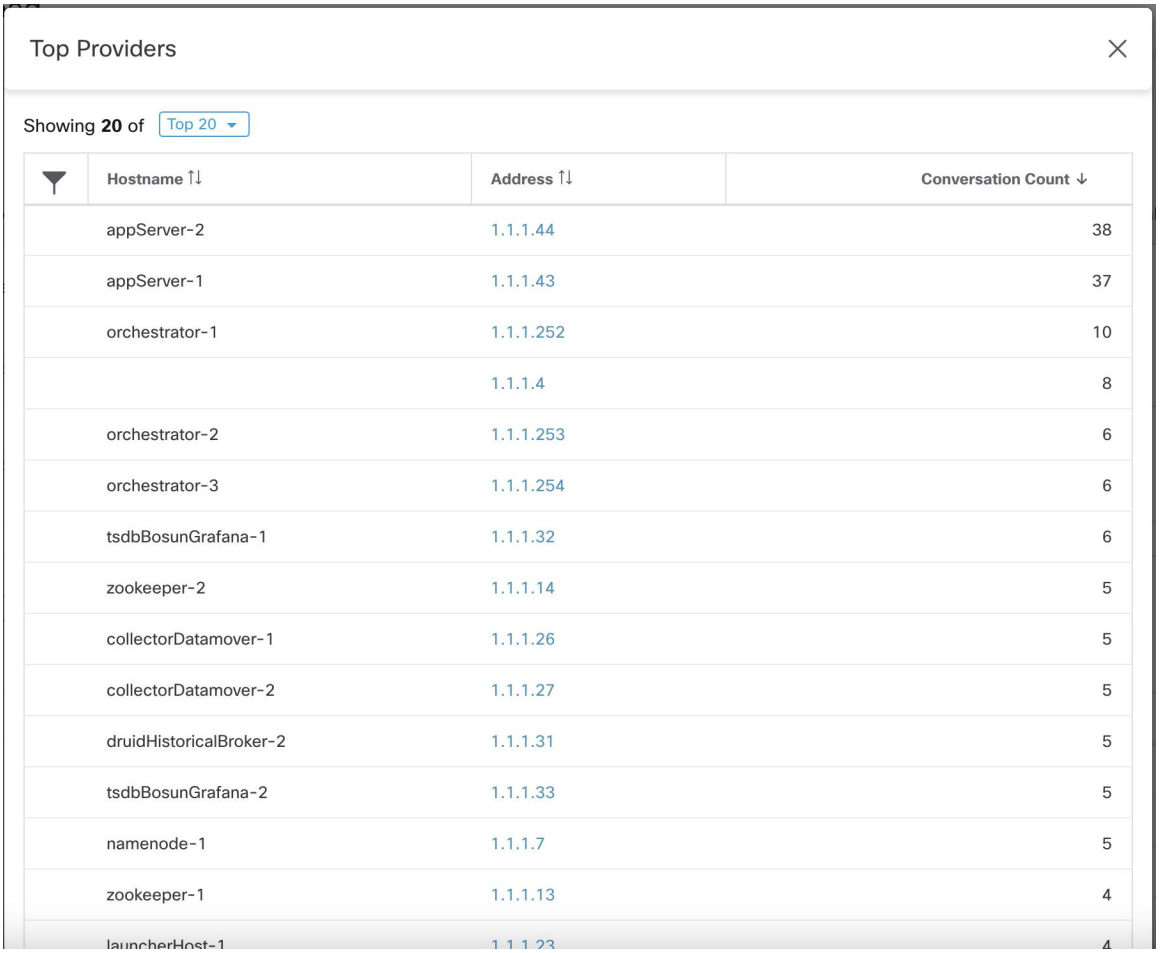


図 *93* : 上位のプロバイダーモーダル



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。

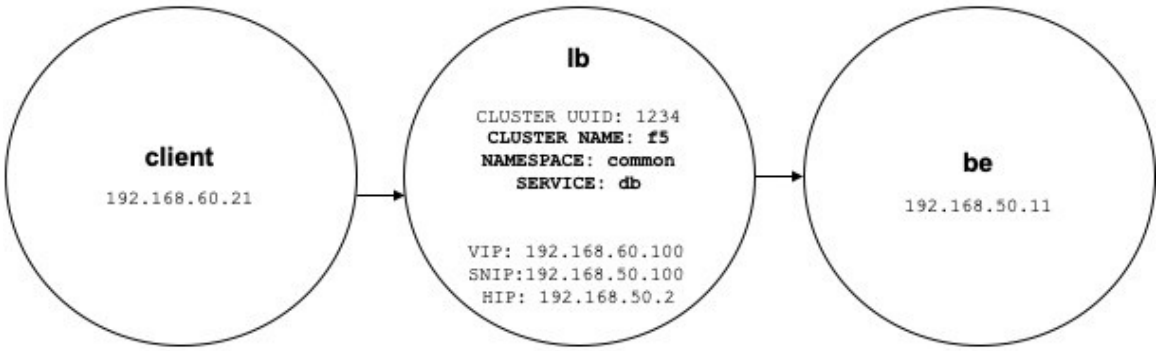
BE バックエンドエンドポイント：バックエンドホストの IP。

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（Deployment）

図 *94 :* 展開（*Deployment*）



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、*orches-*

trator_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。

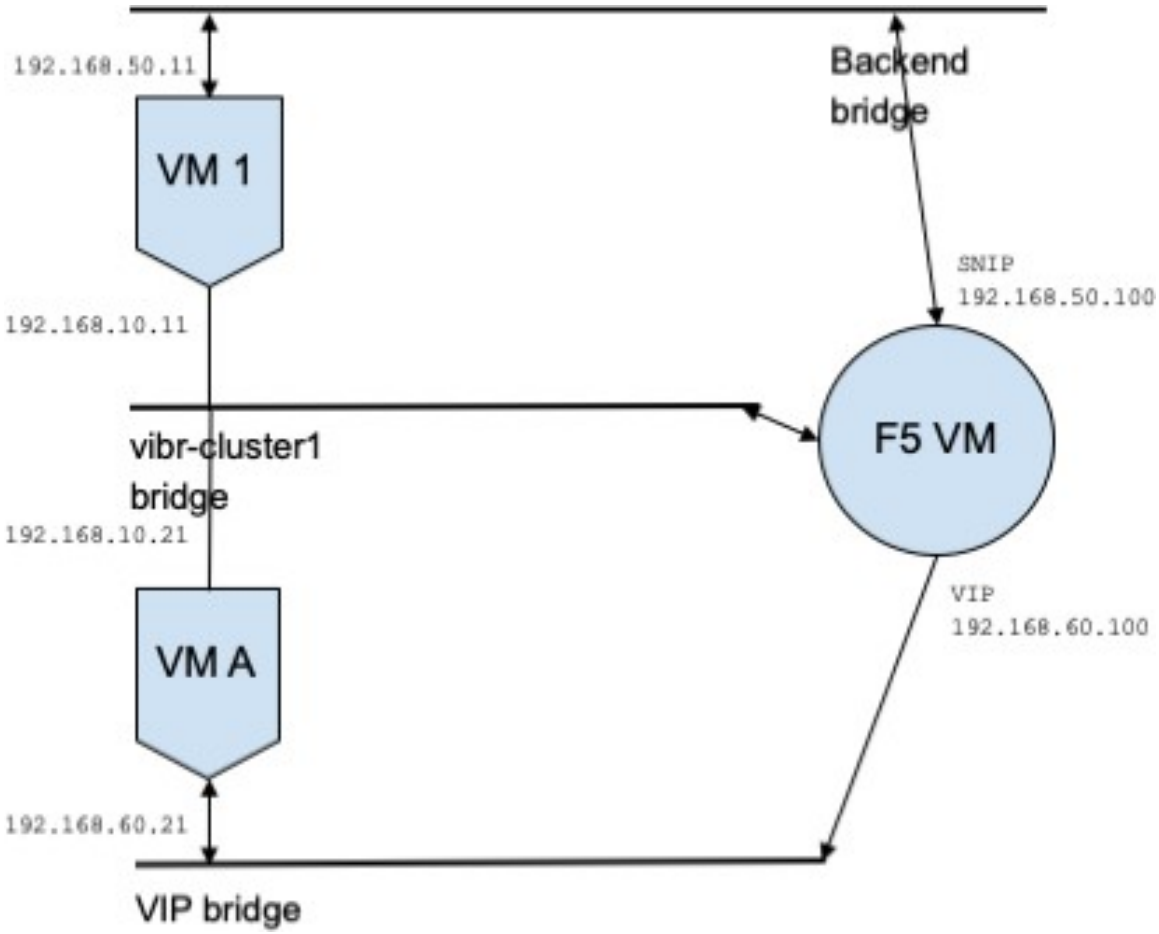
```
user_orchestrator_system/cluster_id eq 1234 and
user_orchestrator_system/service_healthcheck_startpoint eq db
```

- 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 *95 :* 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。

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

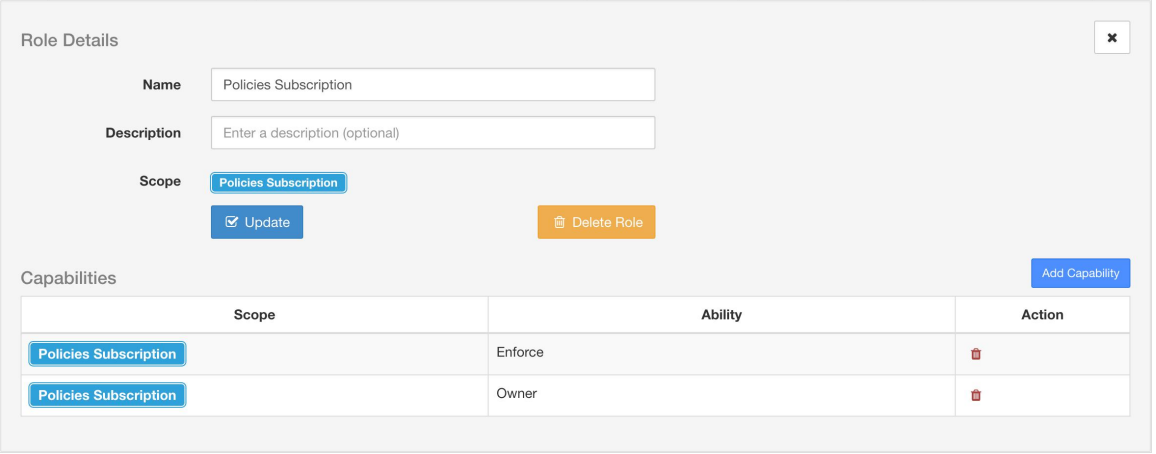
Ubuntu 16.04 などを搭載している Linux システムに次のソフトウェアパッケージがインストールされていること：

- 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

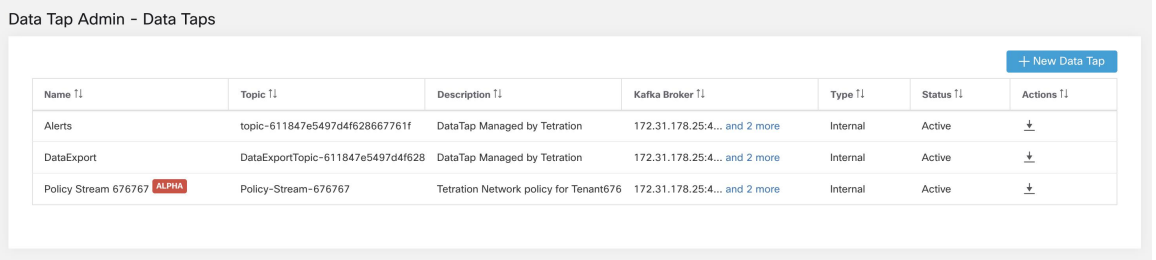
- 「所有者」のケーパビリティを持つユーザー ロールを作成し、選択したユーザーアカウントに割り当てます。

図 *96 : Kafka* からポリシーを受け取るためのユーザーロール設定



- 「ポリシーの適用」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 *97 : [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

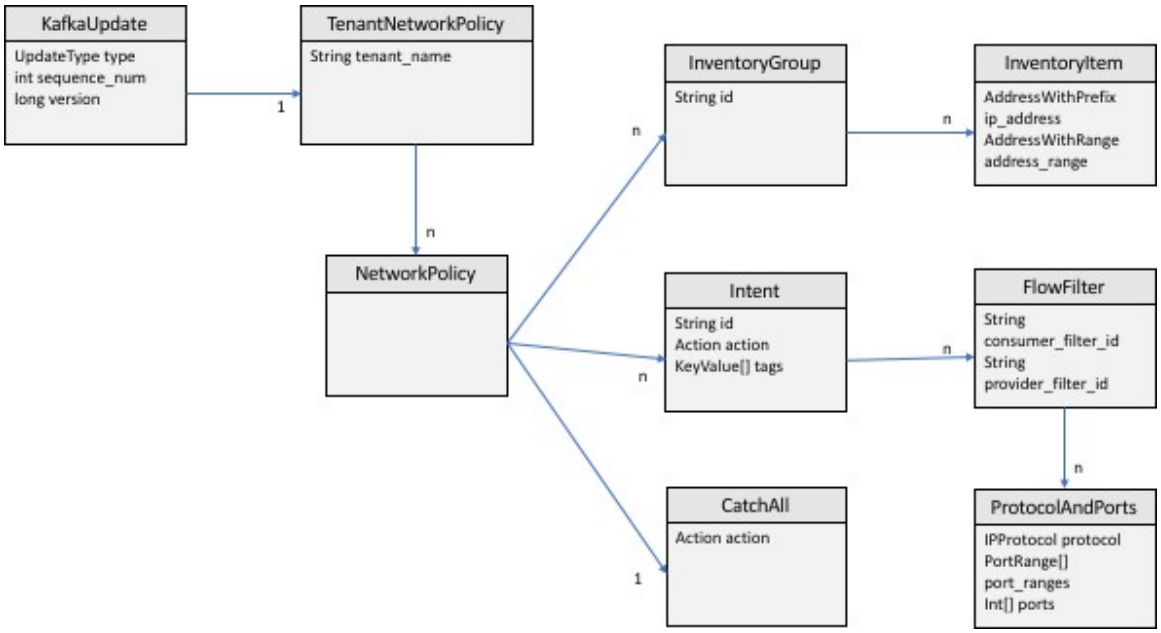
Secure Workload バックエンドによって Kafka に公開されるネットワークポリシーは、Google Protocol Buffers 形式でエンコードされます。Linux システムにダウンロードしてインストールする方法については、こちらのガイドを参照してください。

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 *98 : 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。

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。