インベントリ

インベントリは、ネットワーク上のすべてのワークロードの IP アドレスであり、それらを説明するラベルやその他のデータで注釈が付けられています。インベントリには、ベアメタルまたは仮想マシン、コンテナ、およびクラウドで実行されているワークロードが含まれます。パートナーネットワークで実行されているワークロードも含まれる場合があります（該当する場合）。

インベントリデータの収集は反復的なプロセスです。単一の IP アドレスのさまざまなソースからのデータをマージでき、新規および変更された IP アドレスを更新できます。通常、時間の経過とともに、インベントリの管理は徐々に動的になります。

各インベントリ項目に関連付けられているラベルと注釈に基づいて、検索、フィルタ、および範囲を使用してインベントリを操作し、グループ化します。ポリシーは、インベントリに定義したフィルタと範囲によって定義されたワークロードのグループに適用されます。

インベントリを操作するためのオプションは付与されているロールによって異なりますが、多くの場合検索、フィルタ、アップロードが含まれます。

ワークロードラベル

ラベル（タグ、注釈、属性、メタデータ、またはコンテキストと呼ばれることもありますが、これらの用語は必ずしも完全に同義ではありません）は、Cisco Secure Workload の能力の鍵です。

人間が読めるラベルでは、機能、場所、その他の基準に関してワークロードについて説明します。

Cisco Secure Workload は、以下のユーザーラベルの追加方法をサポートしています。

- インベントリ項目で実行されている Secure Workload エージェントによる検出
- カンマ区切り値（CSV）ファイルのアップロードによる手動インポート
- ユーザーインターフェイスによる手動割り当て
- エンドポイントのコネクタによる自動インポート
- インベントリ強化用のコネクタによる自動インポート
- オーケストレータで生成されたラベルとカスタムラベルの自動インポート（「外部オーケストレータ」を参照）
- クラウドコネクタからの自動インポート（「クラウドコネクタ」を参照）
- インストーラスクリプトを作成するときに、インベントリラベルを指定できます。スクリプトを使用してインストールされたエージェントにはすべて、インベントリラベルが自動的にタグ付けされます。この機能は、Linux および Windows ワークロードの展開でのみサポートされています。

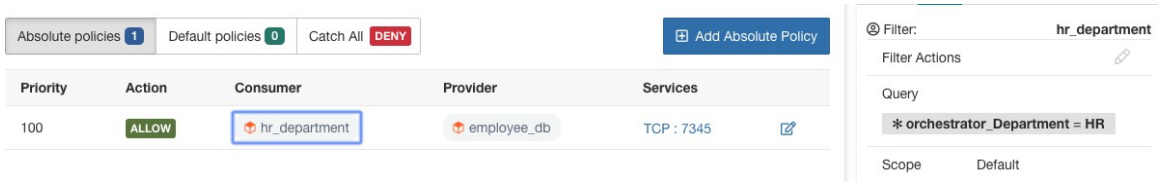
ラベルの重要性

ラベルを使用すると、論理ポリシーを定義できます。次に例を示します。

コンシューマ *hr_department* からプロバイダー *employee_db* へのトラフィックを許可する場合

コンシューマとプロバイダーのワークロード グループ メンバーを指定する代わりに、次の図に示すように、ラベルを使用して論理ポリシーを定義できます。これにより、論理ポリシーを変更することなく、コンシューマグループとプロバイダーグループのメンバーシップを動的に変更できるようになります。フリートからワークロードが追加または削除されるとと、外部オーケストレータやクラウドコネクタなど、設定したサービスによって Secure Workload に通知されます。これにより、Secure Workload はコンシューマグループ *hr_department* とプロバイダーグループ *employee_db* のメンバーシップを評価できます。

図 *1 :* ラベル付きポリシーの例



サブネットベースのラベル継承

サブネットベースのラベル継承がサポートされます。下位のサブネットと IP アドレスは、次の条件のいずれかが満たされている場合、それらが属する上位のサブネットからラベルを継承します。

- 下位サブネット/アドレスのラベルのリストに該当するラベルが含まれていない。
- 下位サブネット/アドレスのラベル値が空である。

次の例を考えてみます。

IP	名前	目的	環境	スピリットアニマル
10.0.0.1	server-1	webtraffic	実稼働	
10.0.0.2				カエル
10.0.0.3				ワシ
10.0.0.0/24	web-vlan		統合	
10.0.0.0/16		webtraffic		アナグマ
10.0.0.0/8			test	クマ

IP アドレス *10.0.0.3* のラベルは *{“name”: “web-vlan”, “purpose”: “webtraffic”, “environment”: “integration”, “spirit-animal”: “eagle”}* です。

ラベルのプレフィックス

ラベルは、情報のソースを識別するプレフィックス付きで自動的に表示されます。

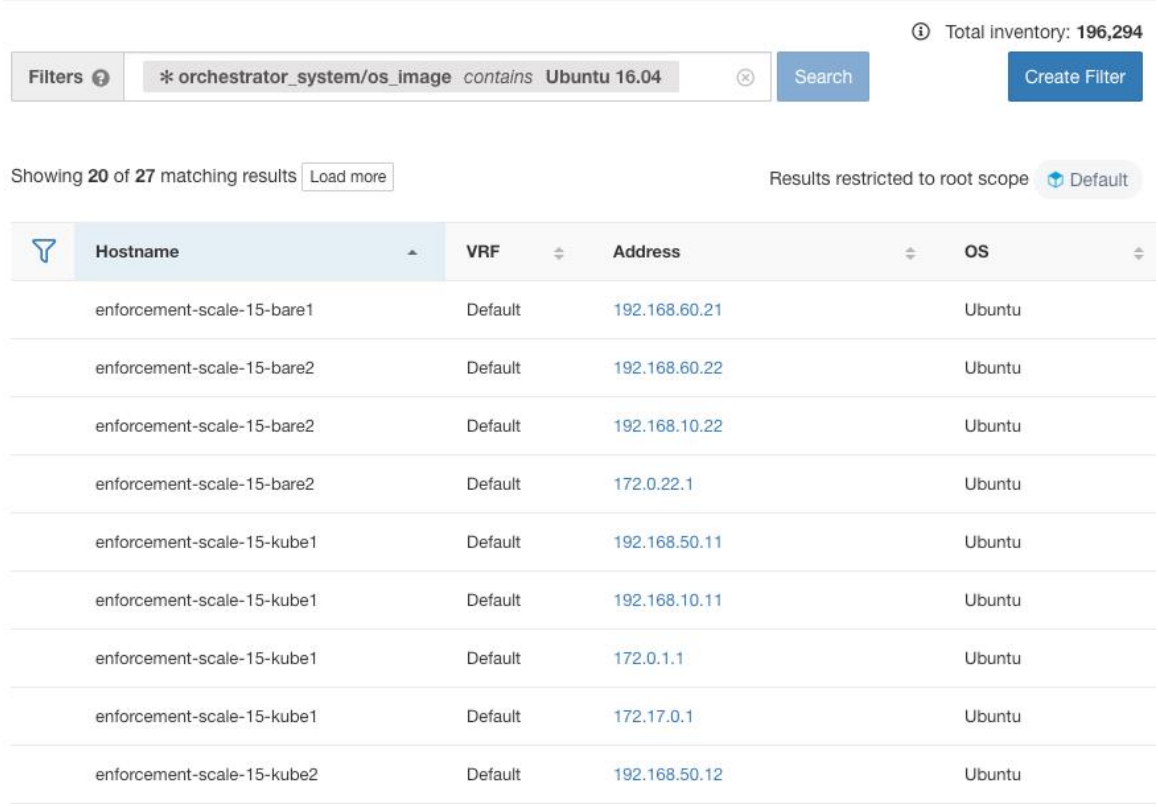
UI（*OpenAPI* では *user_*）では、すべてのユーザーラベルの先頭に * が付きます。さらに、外部オーケストレータまたはクラウドコネクタから自動的にインポートされたラベルには、orchestrator_ というプレフィックスが付きます。エンドポイントコネクタからインポートされたラベルについては、「エンドポイントのコネクタ」で詳細を参照してください。ただし、*ldap_* のプレフィックスが付いたラベルが含まれる場合があります。

たとえば、ユーザーがアップロードしたCSVファイルからインポートされた*department*のキーを持つラベルは、UIでは**department*と表示され、OpenAPIでは*user_department*と表示されます。外部オーケストレータからインポートされた*location*のキーを持つラベルは、UIでは**orchestrator_location*と表示され、OpenAPIでは*user_orchestrator_location*と表示されます。

次の図は、オーケストレータが生成したプレフィックス付きのラベルを使用したインベントリ検索の例を示しています。

orchestrator_system/os_image:

図 *2*:オーケストレータで生成されたラベルを使用したインベントリ検索の例



クラウドコネクタによって生成されたラベル

これらのラベルは、AWSおよびAzureからのデータに適用されます。これらのラベルの送信元は、AWS VPCまたはAzure VNetのワークロードとネットワーク インターフェイスです。送信元からのタグがマージされ、Cisco Secure Workloadに表示されます。たとえば、ワークロードタグが `env: prod` で、ネットワーク インターフェイス タグが `env: test` である場合、Cisco Secure Workloadのラベル値は `prod,test` であり、各コネクタページの[orchestrator_env]列の下に表示されます。

AKS、EKS、GKEに固有のラベルについては、「Kubernetesクラスタに関連するラベル」も参照してください。

表 *1:* クラウドコネクタを使用して収集されたすべてのインベントリに追加されるラベル

キー	値
orchestrator_system/orch_type	AWS または Azure
orchestrator_system/cluster_name	<*Cluster_name* はユーザーがこのコネクタの設定に付けた名前>
orchestrator_system/cluster_id	<仮想ネットワーク *ID*>

インスタンス固有のラベル

次のラベルは、各ノードに固有のものです。

キー	値
orchestrator_system/workload_type	vm
orchestrator_system/machine_id	<プラットフォームによって割り当てられた *InstanceID*>
orchestrator_system/machine_name	<AWS によってこのノードに指定された PublicDNS（FQDN）> – または – <Azure での InstanceName>
orchestrator_system/segmentation_enabled	<インベントリでセグメンテーションが有効になっているかどうかを判断するためのフラグ>
orchestrator_system/virtual_network_id	<インベントリが属する仮想ネットワークの *ID*>
orchestrator_system/virtual_network_name	<インベントリが属する仮想ネットワークの名前>
orchestrator_system/interface_id	<このインベントリに付属する elastic network interface の識別子>
orchestrator_system/region	<インベントリが属する地域>
orchestrator_system/resource_group	（このタグは Azure インベントリにのみ適用されます）
orchestrator_‘<Tag Key>‘	<Tag Value> クラウドポータルのインベントリに割り当てられた任意数のカスタムタグのキーと値のペア。

Kubernetes クラスタに関連するラベル

次の情報は、シンプルな Kubernetes、OpenShift、およびサポートされているクラウドプラットフォーム（EKS、AKS、および GKE）で実行されている Kubernetes に適用されます。

Secure Workload は、オブジェクトタイプごとに、オブジェクトに関連付けられたラベルを含むインベントリを Kubernetes クラスタからリアルタイムでインポートします。ラベルのキーと値はそのままインポートされます。

Secure Workload では、Kubernetes オブジェクト用に定義されたラベルのインポートに加えて、これらのオブジェクトをインベントリフィルタで使用しやすくするラベルも生成します。これらの追加のラベルは、範囲とポリシーを定義する際に特に役立ちます。

すべてのリソースに対して生成されたラベル

Secure Workload は、Kubernetes/OpenShift/EKS/AKS/GKE API サーバーから取得したすべてのノード、ポッド、およびサービスに次のラベルを追加します。

キー	値
orchestrator_system/orch_type	kubernetes
orchestrator_system/cluster_id	<*UUID of the cluster's configuration in |product|*>
orchestrator_system/cluster_name	<*Name given to this cluster's configuration*>
orchestrator_system/namespace	<この項目の *Kubernetes/OpenShift/EKS/AKS/GKE* 名前空間>

ノード固有のラベル

次のラベルは、ノードに対してのみ生成されます。

キー	値
orchestrator_system/workload_type	マシン
orchestrator_system/machine_id	<*Kubernetes/OpenShift* によって割り当てられた *UUID*>
orchestrator_system/machine_name	<このノードに指定された名前>
orchestrator_system/kubelet_version	<このノードで実行されている *kubelet* のバージョン>
orchestrator_system/container_runtime_version	<このノードで実行されているコンテナ ランタイム バージョン>

ポッド固有のラベル

次のラベルは、ポッドに対してのみ生成されます。

キー	値
orchestrator_system/workload_type	pod
orchestrator_system/pod_id	<*Kubernetes/OpenShift* によって割り当てられた *UUID*>
orchestrator_system/pod_name	<このポッドに指定された名前>

キー	値
orchestrator_system/hostnetwork	<*true*|*false*> ポッドがホストネットワークで実行されているかどうかを反映
orchestrator_system/machine_name	<ポッドが実行されているノードの名前>
orchestrator_system/service_endpoint	*[この*Pod*が提供しているサービス名のリスト]*

サービス固有のラベル

次のラベルは、サービスに対してのみ生成されます。

キー	値
orchestrator_system/workload_type	service
orchestrator_system/service_name	<このサービスに指定された名前>

- （クラウドマネージド型 Kubernetes の場合のみ）ServiceType：LoadBalancer のサービスは、メタデータの収集に対してのみサポートされ、フローデータの収集やポリシーの適用に対してはサポートされません。

ヒント **orchestrator_system/service_name** を使用して項目をフィルタリングすることと、**orchestrator_system/service_endpoint** を使用することは同じではありません。

たとえば、フィルタ **orchestrator_system/service_name = web** を使用すると、**web** という名前のすべてのサービスが選択されますが、 **orchestrator_system/service_endpoint = web** は、**web** という名前のサービスを提供するすべてのポッドを選択します。

Kubernetes クラスタのラベルの例

次の例は、Kubernetes ノードの部分的な YAML 表現と、Cisco Secure Workload によってインポートされた対応するラベルを示しています。

```
- apiVersion: v1
kind: Node
metadata:
annotations:
node.alpha.kubernetes.io/ttl: "0"
volumes.kubernetes.io/controller-managed-attach-detach: "true"
labels:
beta.kubernetes.io/arch: amd64
beta.kubernetes.io/os: linux
kubernetes.io/hostname: k8s-controller
```

表 *2 : Kubernetes* からインポートされたラベルキー

インポートされたラベルキー
orchestrator_beta.kubernetes.io/arch
orchestrator_beta.kubernetes.io/os
orchestrator_kubernetes.io/hostname
orchestrator_annotation/node.alpha.kubernetes.io/ttl
orchestrator_annotation/volumes.kubernetes.io/controller-managed-attach-detach
orchestrator_system/orch_type
orchestrator_system/cluster_id
orchestrator_system/cluster_name
orchestrator_system/namespace
orchestrator_system/workload_type
orchestrator_system/machine_id
orchestrator_system/machine_name
orchestrator_system/kubelet_version
orchestrator_system/container_runtime_version

カスタムラベルのインポート

カスタムラベルは、ユーザー定義データを特定のホストに関連付けるため、アップロードするか、手動による割り当てができます。このユーザー定義データは、関連するフローとインベントリに注釈を付けるために使用されます。

ラベルの入手元（手動入力または手動アップロード、コネクタまたは外部オーケストレータを使用した取り込みなど）にかかわらず、すべてのルート範囲でラベル付けできる IPv4/IPv6 アドレスまたはサブネットの数には制限があることに注意してください。詳細については、「ラベルの制限」を参照してください。

ラベルファイルのアップロードに関するガイドライン

ステップ 1 サンプルファイルを表示するには、左側のウィンドウで **[整理（Organize）]** > **[ユーザーがアップロードしたラベル（User Uploaded Labels）]** > **[CSVアップロード（CSV Upload）]**を選択し、[サンプルのダウンロード（Download a Sample）] をクリックします。

ステップ 2 ユーザーラベルのアップロードに使用するCSVファイルには、ラベルキー（IPアドレス）が含まれている必要があります。

ステップ 3 ラベルに英語以外の文字を使用するには、CSV ファイルを UTF-8 形式にする必要があります。

ステップ 4 CSV ファイルが「ラベルキースキーマ」セクションで説明されているガイドラインを満たしていることを確認します。

ステップ 5 アップロードされたすべてのファイルは、同じスキーマに従う必要があります。

ラベルキースキーマ

列名に関するガイドライン

- ラベルキースキーマでは、ヘッダー「IP」を持つ 1 つの列が必要です。さらに、IP アドレスの属性を含む他の列が少なくとも 1 つ必要です。
- [VRF] 列は、ラベルスキーマで特別な意味を持ちます。この値を指定する場合は、ラベルがアップロードされるルート範囲と一致する必要があります。範囲に依存しない API を使用して CSV ファイルをアップロードする場合、これは必須です。
- 列名に使用できる文字は、文字、数字、スペース、ハイフン、アンダースコア、およびスラッシュのみです。
- 列名は 200 文字を超えることはできません。
- 列名の前に「orchestrator_」、「TA_」、「ISE_」、「SNOW_」、または「LDAP_」のプレフィックスを付けることはできません。これらは内部アプリケーションのラベルと競合する可能性があるためです。
- CSV ファイルに重複する列名が含まれないようにしてください。

列の値に関するガイドライン

- 値は 255 文字に制限されていますが、可能な限り短くする必要があると同時に、ユーザーにとって明確で、わかりやすく意味のあるものでなければなりません。
- キーと値は大文字と小文字が区別されません。ただし、一貫性を持たせることをお勧めします。
- 「IP」列の下に表示されるアドレスは、次の形式に従う必要があります。
  - IPv4 アドレスの形式は、「x.x.x.x」および「x.x.x.x/32」です。
  - IPv4 サブネットは、「x.x.x.x/<netmask>」の形式にする必要があります。ここで、ネットマスクは 0 から 31 までの整数です。
  - IPv6 アドレスでは、長い形式（「x:x:x:x:x:x:x:x」または「x:x:x:x:x:x:x:x/128」）および標準形式（「x:x::x」または「x:x::x/128」）がサポートされています。
  - IPv6 サブネットでは、長い形式（「x:x:x:x:x:x:x:x/<netmask>」）と標準形式（「x:x::x/<netmask>」）がサポートされています。ネットマスクは 0 ～ 127 の整数である必要があります。

列の順序は重要ではありません。最初の 32 のユーザー定義列は、ラベルが自動的に有効になります。32 を超える列がアップロードされている場合は、ページの右側にあるチェックボックスを使用して、最大 32 の列を有効にすることができます。

カスタムラベルのアップロード

次の手順では、**サイト管理者**、**カスタマーサポート**、またはルート**範囲所有者**の各ロールを持つユーザーがラベルをアップロードする方法を説明します。

始める前に

カスタムラベルをアップロードするには、「ラベルファイルのアップロードに関するガイドライン」セクションに従って、CSV ファイルを作成します。

ステップ 1 左側のペインで、**[整理（Organize）]** > **[ユーザーがアップロードしたラベル（User Uploaded Labels）]** > **[CSVのアップロード（CSV Upload）** を選択し、[新しいラベルのアップロード（Upload New Labels）] で [ファイルの選択（Select File）] をクリックします。

ステップ 2 操作（[追加（Add）]、[マージ（Merge）]、または [削除（Delete）]）を選択します。

- [追加（Add）] : ラベルを新規および既存のアドレス/サブネットに追加します。既存のラベルの代わりに新しいラベルを選択して、競合を解決します。たとえば、データベース内の住所のラベルが *{"foo": "1", "bar": "2"}* で、CSV ファイルに *{"z": "1", "bar": "3"}* が含まれている場合、add` は、このアドレスのラベルを *{"foo": "1", "z": "1", "bar": "3"}* に設定します。
- [マージ（Merge）] : ラベルを既存のアドレス/サブネットにマージします。空の値の代わりに空でない値を選択することで、競合を解決します。たとえば、データベース内のアドレスのラベルが *{"foo": "1", "bar": "2", "qux": "", "corge": "4"}* で、CSV ファイルに *{"z": "1", "bar": "", "qux": "3", "corge": "4-updated"}* が含まれている場合、add` は、このアドレスのラベルを *{"foo": "1", "z": "1", "bar": "2", "qux": "3", "corge": "4-updated"}* に設定します。

  （注） “bar” の値は “”（空）にリセットされず、既存の値 “bar”=”2” が保持されます。

- [削除（Delete）] : このオプションにより、アドレス/サブネットのラベルが削除されます。このオプションは、範囲、フィルタ、ポリシー、および適用される動作に大きな影響を与える可能性があります。重要な詳細については、「ラベルの削除」を参照してください。

重要：この削除機能により、カスタムラベルのアップロード中に、指定された IP アドレス/サブネットに関連付けられたすべてのラベルが削除されます。削除の対象は、CSV ファイルに一覧表示されている列に限定されません。そのため、削除操作は慎重に使用する必要があります。

ステップ 3 [アップロード（Upload）] をクリックします。

検索ラベル

[サイト管理者（Site Admin）]、[カスタマーサポート（Customer Support）] または [範囲所有者（scope owner）] のロールを持つユーザーは、特定の IP アドレスまたはサブネットにラベルを割り当てることができます。

ステップ 1 [ユーザーがアップロードしたラベル（User Uploaded Labels）] ページで、[検索と割り当て（Search and Assign）] をクリックします。

ステップ 2 [IPまたはサブネット（IP or Subnet）] フィールドで、IPアドレスまたはサブネットを入力し、[次へ（Next）] をクリックします。

[ラベルの割り当て（Assign Labels）] ページに、入力した IP アドレスまたはサブネットの既存のラベルが表示されます。

カスタムラベルの手動割り当てまたは編集

[サイト管理者（Site Admin）]、[カスタマーサポート（Customer Support）] または [ルート範囲の所有者（Root Scope Owner）] のロールを持つユーザーは、特定の IP アドレスまたはサブネットにラベルを手動で割り当てることができます。

ステップ 1 [ユーザーがアップロードしたラベル（User Uploaded Labels）] ページで、[検索と割り当て（Search and Assign）] をクリックします。

ステップ 2 [IPまたはサブネット（IP or Subnet）] フィールドで、IPアドレスまたはサブネットを入力し、[次へ（Next）] をクリックします。

[ラベルの割り当て（ Assign Labels）] ページが表示されます。既存のラベルが表示され、編集できることに注意してください。

ステップ 3 新しいラベルを追加するには、**Labels for <IP address/subnet>** セクションで、ラベル名と値を入力し、[確認（Confirm）] をクリックします。[次へ（Next）] をクリックします。

ステップ 4 変更を確認し、[割り当て（Assign）] をクリックして確定します。

ラベルのダウンロード

サイト管理者、**カスタマーサポート**、またはルート**範囲の所有者**ロールを持つユーザーは、ルート範囲に属する事前に定義されたラベルをダウンロードできます。

ステップ 1 [ユーザーがアップロードしたラベル（User Uploaded Labels）] ページで、[CSVアップロード（CSV Upload）] タブをクリックします。

ステップ 2 [既存のラベルのダウンロード（Download Existing Labels）] セクションで、[ラベルのダウンロード（Download Labels）] をクリックします。

Secure Workloadで 使用されるラベルが CSV ファイルとしてダウンロードされます。

ラベルの変更

警告 ラベルを変更する必要がある場合は、慎重に行ってください。変更すると、既存のクエリ、フィルタ、範囲、クラスタ、ポリシー、およびそのラベルに基づいて適用された動作のメンバーシップと効果が変更されます。

ステップ 1 [ユーザーがアップロードしたラベル（User Uploaded Labels）] ページで、[検索と割り当て（Search and Assign）] タブをクリックします。

ステップ 2 [IPまたはサブネット（IP or Subnet）] フィールドで、IP アドレスまたはサブネットを入力し、[次へ（Next）] をクリックします。

Secure Workload が入力した IP アドレス/サブネットに対して使用しているラベルが表示されます。

ステップ 3 [アクション（Actions）] 列で、[編集（Edit）] アイコンをクリックして必要なラベルの名前と値を変更します。

ステップ 4 [確認（Confirm）] をクリックし、[次へ（Next）] をクリックします。

ステップ 5 変更を確認し、[割り当て（Assign）] をクリックします。

ラベルの無効化

スキーマを変更する 1 つの方法は、ラベルを無効にすることです。注意して続行してください。

ステップ 1 [ユーザーアップロードラベル（User Uploaded Labels）] ページで、[ラベル（Labels）] タブをクリックします。

ステップ 2 該当するラベルの [アクション（Actions）] 列で [無効化（Disable）] を選択し、次に [はい（Yes）] をクリックしてインベントリからラベルを削除することを確認します。

後でラベルを有効にする場合は、[有効化（Enable）] をクリックしてラベルを使用します。

ラベルを削除する

警告 スキーマを変更する1つの方法は、ラベルを無効にして削除することです。注意して続行してください。この操作により、選択したラベルが削除され、依存するすべての**フィルタ**と**範囲**に影響します。これらのラベルが使用されていないことを確認してください。この操作を取り消すことはできません。

ステップ1 ラベルを無効にします。disable_lables を参照してください。

ステップ2 [ゴミ箱（TrashCan）] アイコンをクリックし、[はい（Yes）] をクリックしてラベルの削除を確定します。

ラベルの使用状況の表示

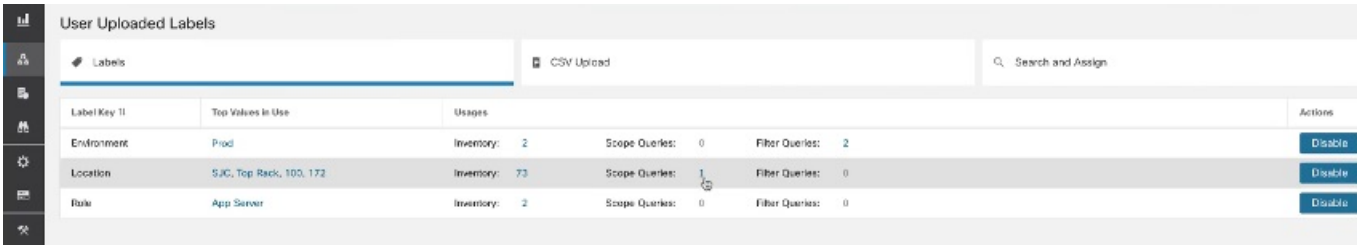
IP アドレスやサブネットインベントリは、CSV ファイルを使用してアップロードされたり、ユーザーによって手動で割り当てられたカスタムラベルで更新されます。次に、ラベルは範囲とフィルタの定義に使用され、このフィルタに基づいてアプリケーションポリシーが作成されます。したがって、ラベルを変更すると、Cisco Secure Workload の範囲、フィルタ、およびポリシーに直接影響するため、ラベルの使用状況を把握することが重要です。

ラベルの使用状況を表示するには、次の手順を実行します。

ステップ1 [ユーザーアップロードラベル（User Uploaded Labels）] ページで、[ラベル（Labels）] タブを選択します。ラベルキー、使用中のラベルの上位 5 つの値、インベントリ、範囲、フィルタ、およびカスタムラベルを使用するクラスタが表示されます。

ステップ2 [使用状況（Usages）] 列で、インベントリ、範囲、またはフィルタに対するカウント値をクリックします。たとえば、[ロケーション（Location）] ラベルを使用している範囲を表示するには、範囲クエリ数をクリックします。

図 *3*：選択したラベルの範囲を表示



[範囲とインベントリ（Scopes and Inventory）] ページが表示され、クエリによって、選択したラベルで範囲が自動的にフィルタ処理されます。

（注） CSVファイルを使用してアップロードされたラベル、またはIPアドレスやサブネットに手動で割り当てられたラベルの使用状況のみを表示できます。

ラベルのメンテナンスプロセスの作成

ネットワークとインベントリは変更されるため、ラベルを更新して変更を反映する計画を立てる必要があります。

たとえば、あるワークロードが廃止され、その IP アドレスが別の目的のワークロードに再度割り当てられた場合、そのワークロードに関連付けられているラベルを更新する必要があります。これは、手動でアップロードされるラベルと、構成管理データベース（CMDB）などの他のシステムで維持され、取り込まれるラベルの両方に当てはまります。

ラベルが定期的に継続して更新されるプロセスを作成し、そのプロセスをネットワーク メンテナンス ルーチンに追加します。

範囲とインベントリ

範囲とインベントリの概要

このセクションでは、範囲階層とそれに含まれるすべてのインベントリについて明らかにします。範囲は、階層構造を使用してすべてのインベントリを分類します。インベントリ （1ページ）を参照してください。左側は範囲ディレクトリのユーザーインターフェイスです。ここで、範囲階層を下位方向に移動できます。各範囲は範囲カードに表示されます。範囲の名前が表示されます。該当する場合は、子範囲の数、インベントリ数、未分類のインベントリも表示されます。範囲カードをクリックすると、右側のペインが更新され、その範囲に関する詳細と、そのすべてのインベントリのフィルタ可能なリストが表示されます。

範囲設計の原則

1. 動的クエリ一致に従って、インベントリが範囲ツリーに対して照合されます。
   - クエリは、IP/サブネットまたはラベル（推奨）に対して照合されます。
   - ツリーは、各層におけるクエリの結合によって形成されます。
2. 必要に応じて、範囲構造はロケーションに固有にすることができます。
   - クラウドの結合に対するデータセンター、クラウド固有に対する地理的ロケーション
3. 範囲ツリーの各レイヤーは、次のアンカーポイントを意味します。
   - ポリシー制御
   - ロール ベース アクセス制御（RBAC）（Role Based Access Control）

4. すべての子範囲は、その親範囲のサブセットである必要があります
   - 兄弟の範囲が重複していないことを確認してください（「範囲の重複」を参照）。

（注） すべての組織の構造は異なるため、業界に応じて異なるアプローチが必要です。範囲の階層を設計する際に、ロケーション、環境、またはアプリケーションといった注目点を1つ選択します。

（注） IPアドレスまたはサブネットを使用して、Kubernetesインベントリに関連する範囲を定義しないでください。これらのワークロードの範囲とポリシーの定義には、ラベルを使用する必要があります。Pod サービスを識別するには、IP アドレスだけでは不十分です。範囲定義に IP アドレスを使用すると、信頼性の低い結果が生成されます。

主な機能

範囲とインベントリの両方のフィルタリング機能により、範囲ツリーをすばやく下方向に移動したり、範囲階層をフィルタリングして選択した範囲のインベントリ項目をフィルタリングしたりすることができます。

インベントリ数は範囲カードに表示され、範囲内のワークロードの量をすばやく確認できます。

スコープ

範囲は、Cisco Secure Workload の構成とポリシーの基本的な要素です。範囲とは、階層に配置された一群のワークロードです。ワークロードは、位置、ロール、および環境内の機能に関するモデルを構築する属性として機能するようにラベル付けされます。範囲は、時間の経過とともに変化し得る IP に関連付けられた ID や属性などの動的メカニズムをサポートする構造を提供します。

範囲はデータセンターアプリケーションをグループ化するために使用され、ロールを使用してそれらの管理をきめ細かく制御できるようにします。たとえば、範囲はセグメンテーション、フロー、フィルタへのアクセスを定義するために製品全体で使用されます。

範囲は、[VRF] に対応するルートを持つ一連のツリーとして階層的に定義されます。その結果、それぞれの範囲ツリー階層は、別の範囲ツリーと重複しない分離されたデータを表示します。「範囲の重複」を参照してください。

範囲の定義

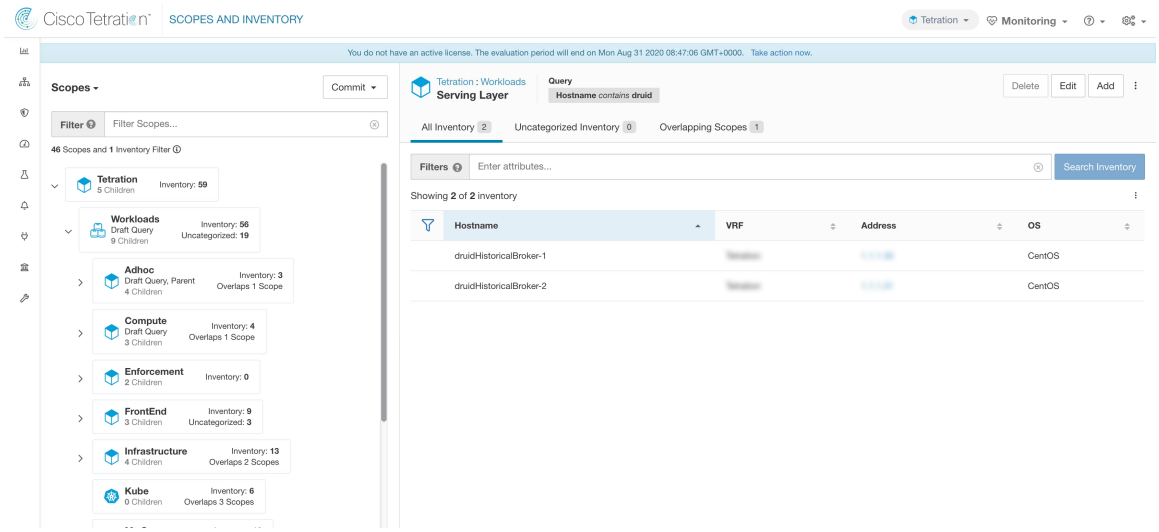
個々の範囲は、次の属性で定義されます。

属性	説明
[親範囲（Parent Scope）]	新しい範囲の親は、ツリー階層構造を定義します。
Name	範囲を識別する名前。
タイプ	タイプは、さまざまなカテゴリのインベントリを指定するために使用されます。該当がない場合、または範囲に混合タイプが含まれている場合は、空白のままにすることができます。
Query	個々の範囲を定義するクエリ。

（注） 範囲は、組織のアプリケーション所有権階層を模倣する階層で定義する必要があります。

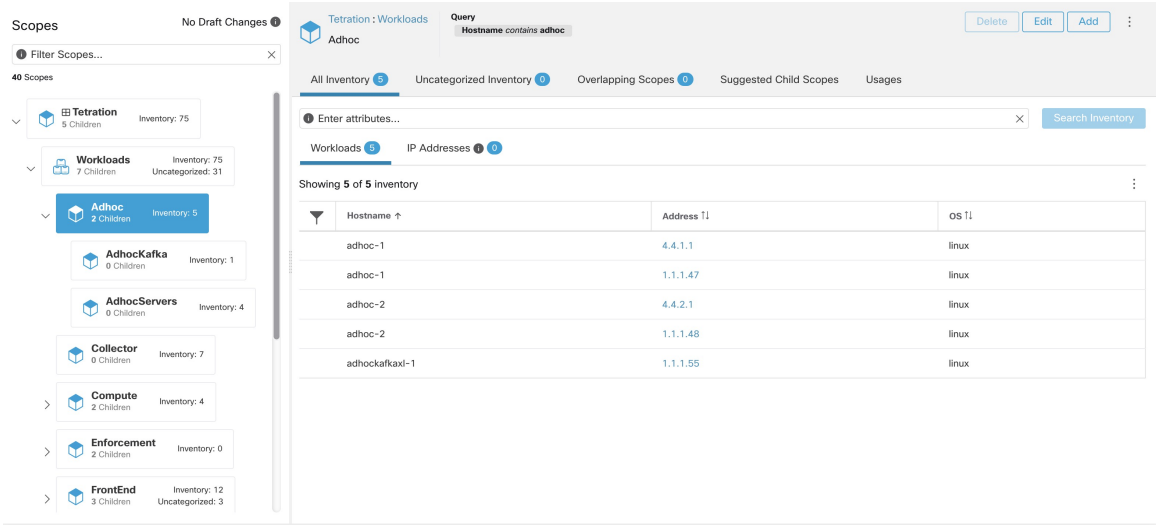
（注） クエリは、IP やサブネットまたはその他のインベントリ属性と一致させる場合があります。

図 *4:* 範囲階層を横断する例



範囲ディレクトリには、範囲階層と各範囲の詳細（インベントリ数、子範囲の数、ワークスペースなど）が表示されます。範囲をクリックするとその範囲が選択されます。右側の詳細ペインが、範囲およびその範囲のインベントリに関する詳細情報で更新されます。

図 *5:*インベントリ カウント



範囲フィルタ

ユーザーは、範囲フィルタを使用して、範囲の重複やクエリなど、さまざまな範囲の詳細をすばやく特定できます。フィルタ機能は、クエリの変更、親の変更などを特定するのにも役立ちます。

フィールド	説明
Name	範囲またはインベントリフィルタの名前でフィルタ処理します。
説明	範囲の説明に表示されるテキストでフィルタ処理します。
Query	クエリで使用されるフィールドまたは値でフィルタ処理します。
[クエリの変更（Query Change）]	コミットされていないクエリがある範囲でフィルタ処理します。
Parent Change	ドラフトで移動されたがコミットされていない範囲でフィルタ処理します。
[インベントリフィルタあり（Is Inventory Filter）]	所有権の範囲に制限されているインベントリフィルタを表示します。
[ワークスペースあり（Has Workspace）]	プライマリワークスペースがある範囲でフィルタ処理します。
[適用ワークスペースあり（Has Enforced Workspace）]	適用されているプライマリワークスペースがある範囲でフィルタ処理します。

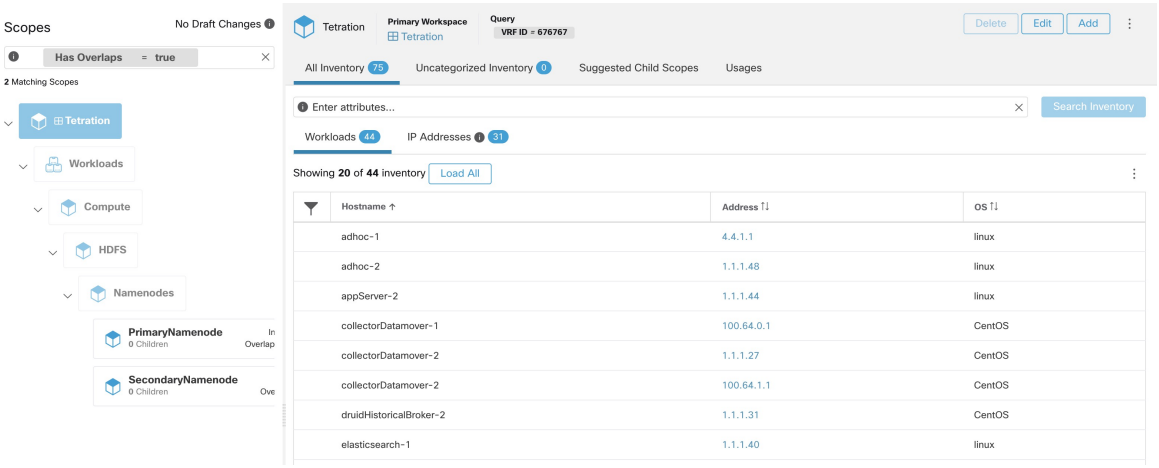
フィールド	説明
[重複あり（Has Overlaps）]	兄弟範囲と共通のインベントリがある範囲でフィルタ処理します。
[無効なクエリあり（Has Invalid Query）]	無効または不明なラベルを使用するクエリを含む範囲でフィルタ処理します。

例：

[重複あり（Has Overlaps）]

範囲の重複の例

図 *6 : Has Overlaps*

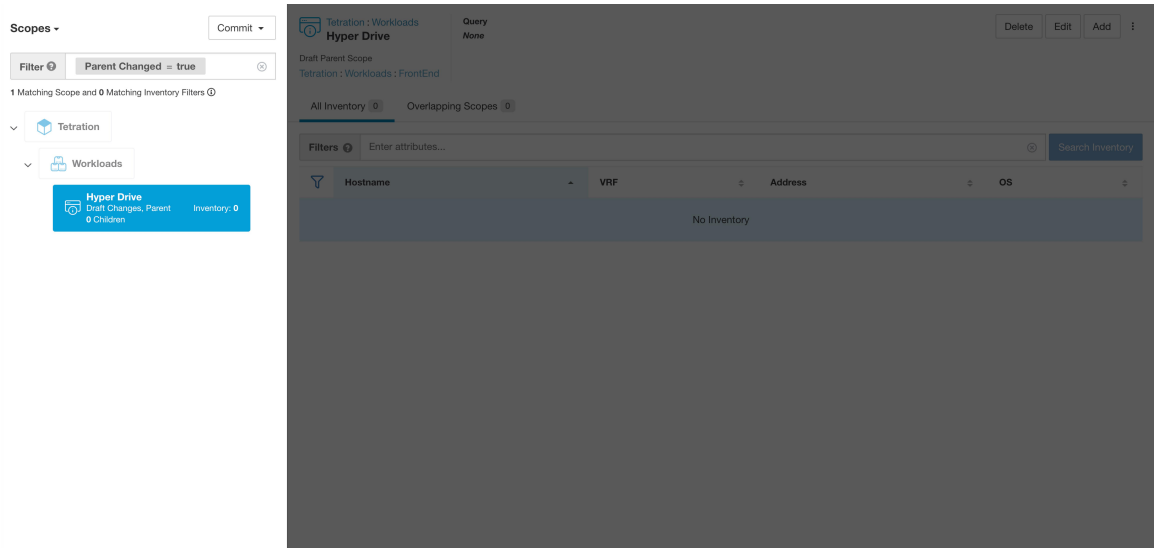


詳細については、「範囲の重複」の項を参照してください。

Parent Change

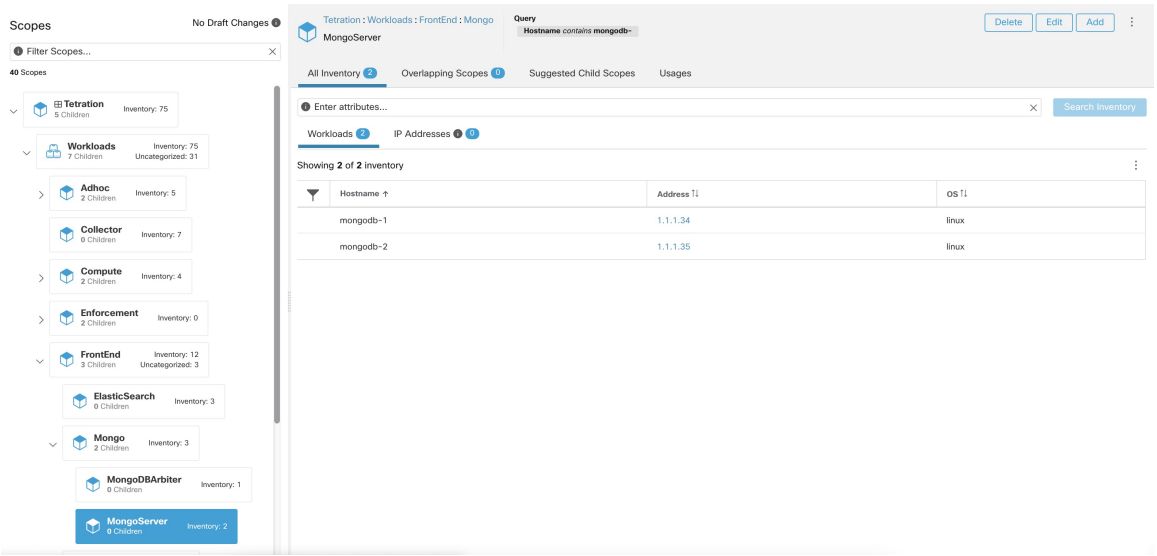
ドラフトで移動されたがまだコミットされていない範囲。

図 *7 : Parent Change*



フル範囲のクエリ

図 *8 :* 範囲階層の例



範囲の定義は階層型になっており、範囲のフルクエリは、すべての親と共に範囲の「論理積」として定義されます。上記の例では、アセットは`Workloads:FrontEnd:Mongo`に割り当てられています。

範囲の照合は次のようになります。

```
vrf_id = 676767 and (ip in 1.1.1.0/24) and (Hostname contains mongo).
```

vrf_id = 676767 はルート範囲クエリに基づき、1.1.1.0/24 の IP は親範囲クエリに基づきます。

（注） 同じレベルでクエリが重複しないようにすることを推奨します。これにより、順序付けの重要性がなくなり、混乱が軽減されます（「範囲の重複」を参照）。

範囲へのアクセスの提供

ユーザーには、範囲上での読み取り、書き込み、実行、適用、および所有者の権限が与えられます。概要を以下に示します。完全な情報については「ロール」を参照してください。

ユーザーには「サブツリー」（与えられた範囲およびそのすべての子範囲など）へのアクセス権が与えられます。上記の例を使用すると、`Workloads:FrontEnd`範囲への読み取りアクセス権があるユーザーは、継承により、以下を含む`Workloads:FrontEnd`の下のすべての範囲への読み取りアクセス権があります。

- `Workloads:FrontEnd:Mongo`
- `Workloads:FrontEnd:ElasticSearch`
- `Workloads:FrontEnd:Redis`
- `etc. . .`

複数の範囲にアクセス可能なロールを定義できます。たとえば、「Mongo Admin」ロールには、範囲への所有者アクセス権がある場合があります。

- `Workloads:FrontEnd:Mongo:MongoServer`
- `Workloads:FrontEnd:Mongo:MongoDBArbiter`

ロールと機能により、ユーザーは範囲階層への「水平な」アクセス権を持つことができます。

範囲の機能も継承されます。たとえば、範囲に書き込み機能があると、その情報の読み取りも可能です。

範囲の表示

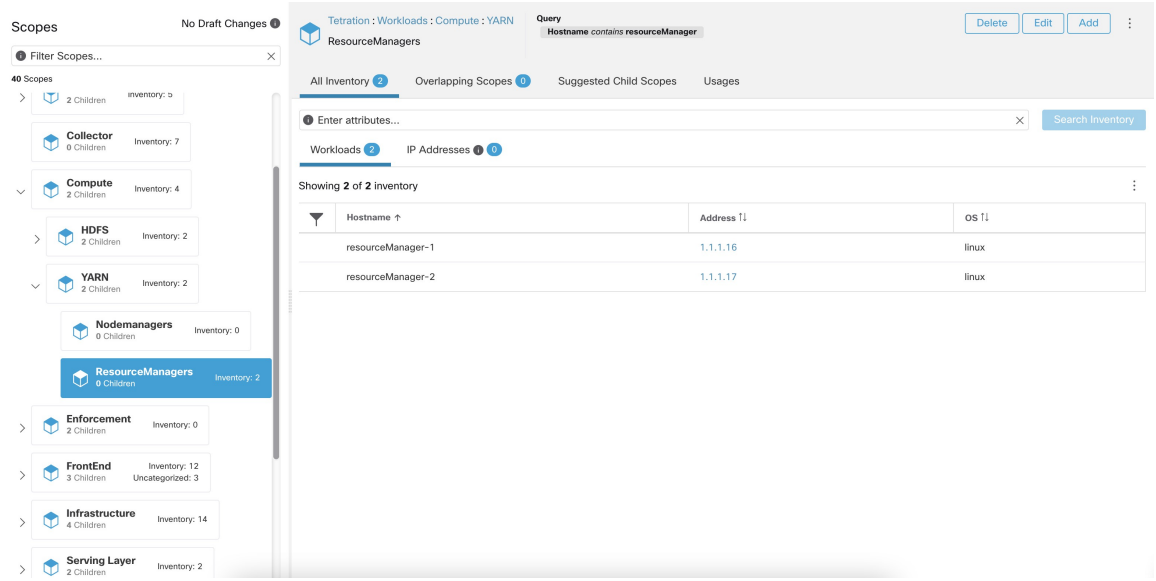
すべてのユーザーは、自分にアクセス権がある範囲ツリーを表示できます。ルート範囲の所有者権限を持つユーザーは、そのツリーの範囲を作成、編集、および削除できます。このビューにアクセスするには、以下を行います。

左側のナビゲーションバーで、**[整理（Organize）] > [範囲とインベントリ（Scopes and Inventory）]**をクリックします。

アクセス権のあるすべての範囲について、範囲階層全体（ルートまで）を横断できます。この完全な横断により、ユーザーが任意の範囲に対するポリシーを作成する際のコンテキストが提供されます。このページでは、いくつかのアクションを実行できます。

- 範囲階層の V 字の部分をクリックすると、その範囲の子が表示されます。
- 範囲カードをクリックすると、右側のペインが更新され、その範囲に関する詳細と、そのすべてのインベントリのフィルタ可能なリストが表示されます。

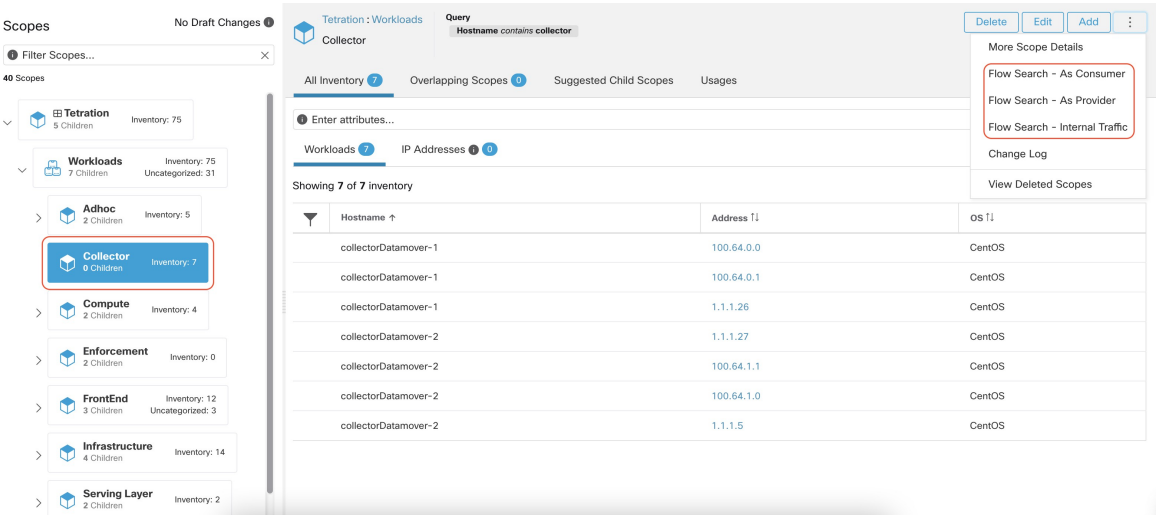
図 *9* : 非管理者ビューの例



範囲を参照するフローの検索

範囲ページには、ショートカットがいくつか用意されており、フローの一方または両方のエンドポイントが指定された範囲内にあるフローを検索する必要があるシナリオで役立ちます。

図 *10* : 範囲でのフローの検索



上の図に示すように、範囲ツリー（左側のパネル）で目的の範囲を選択した後、ユーザーは次の 3 つのオプションから選択できます。

1. [フロー検索（コンシューマとして）（Flow Search - As Consumer）] では、フロー検索ページへのショートカットが提供され、フローのコンシューマ範囲として選択された範囲でのフローの検索に役立ちます。つまり、フローのコンシューマエンドポイントまたは送信元エンドポイントは、選択した範囲に属します。

2. [フロー検索 （プロバイダーとして） （Flow Search - As Provider）] では、フロー検索ページへのショートカットが提供され、フローのプロバイダー範囲として選択された範囲でのフローの検索に役立ちます。つまり、フローのプロバイダーエンドポイントまたは宛先エンドポイントは、選択した範囲に属します。
3. [フロー検索 （内部トラフィック） （Flow Search - Internal Traffic）] では、フロー検索ページへのショートカットが提供され、選択した範囲に完全に制限されているフローの検索に役立ちます。つまり、フローの両方のエンドポイント（コンシューマとプロバイダー）は、選択した範囲に属します。

新しい範囲の作成

子範囲は、[範囲（Scopes）] 管理ページで作成します。このアクションには、ルート範囲の SCOPE_OWNER 権限が必要です。**サイト管理者**は、すべての範囲の所有者です。

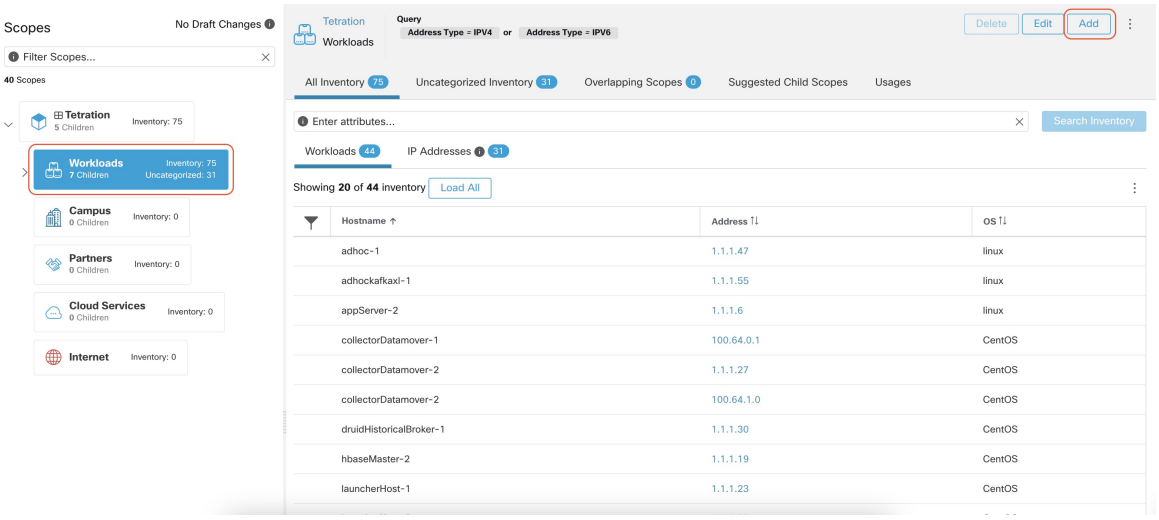
子範囲を作成すると、親範囲のアプリケーションインベントリ メンバーシップ（メンバーワークロード）に影響します。その結果、親範囲には「ドラフト変更」のマークが付けられます。変更をコミットして、依存関係の構造を更新する必要があります。「変更の確定」を参照してください。

ステップ 1 左側のナビゲーションバーで、**[整理（Organize）] > [範囲とインベントリ（Scopes and Inventory）]**をクリックします。このページには、システムで作成済みのテナントと VRF に対応するルート範囲が表示されます。

ステップ 2 範囲ディレクトリで子範囲を選択します。必要に応じて、最初に範囲をフィルタリングできます。

ステップ 3 [追加（Add）] ボタンをクリックします。

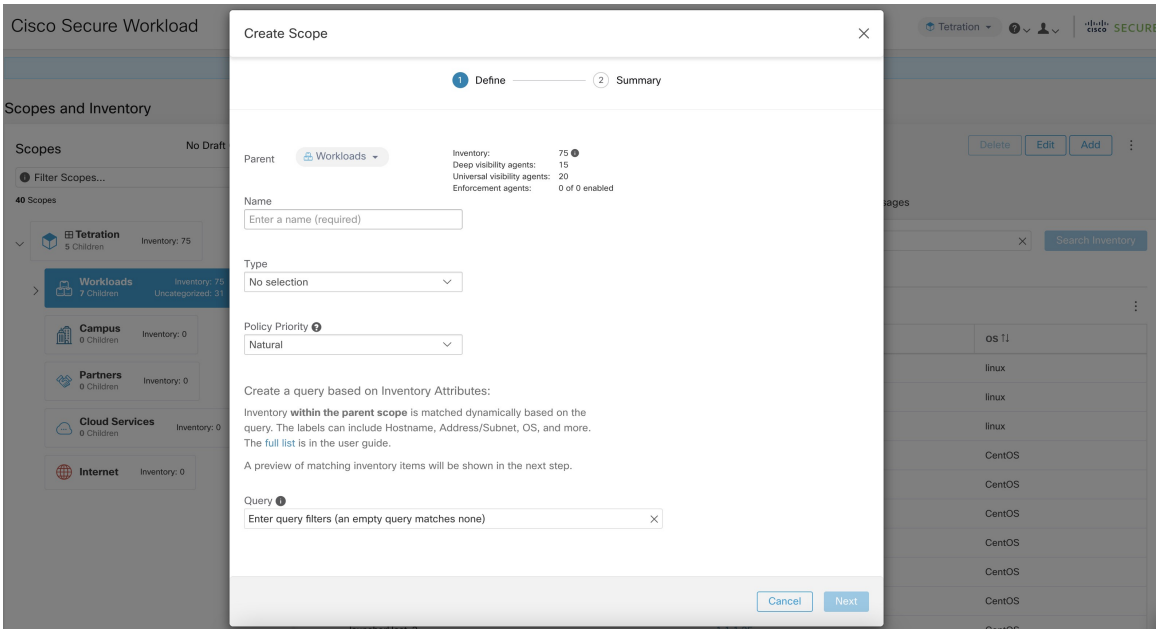
図 *11 : [範囲の追加（Scope Add）]* ボタン



ステップ 4 以下のフィールドに適切な値を入力します。

フィールド	説明
[親（Parent）]	新しい範囲の親。
[名前（Name）]	範囲を識別する名前。親範囲の下で一意である必要があります。
[タイプ（Type）]	新しい範囲のカテゴリを選択します。
[クエリ（Query）]	アセットに一致するクエリまたはフィルタ。

図 *12 :* 範囲作成モーダル

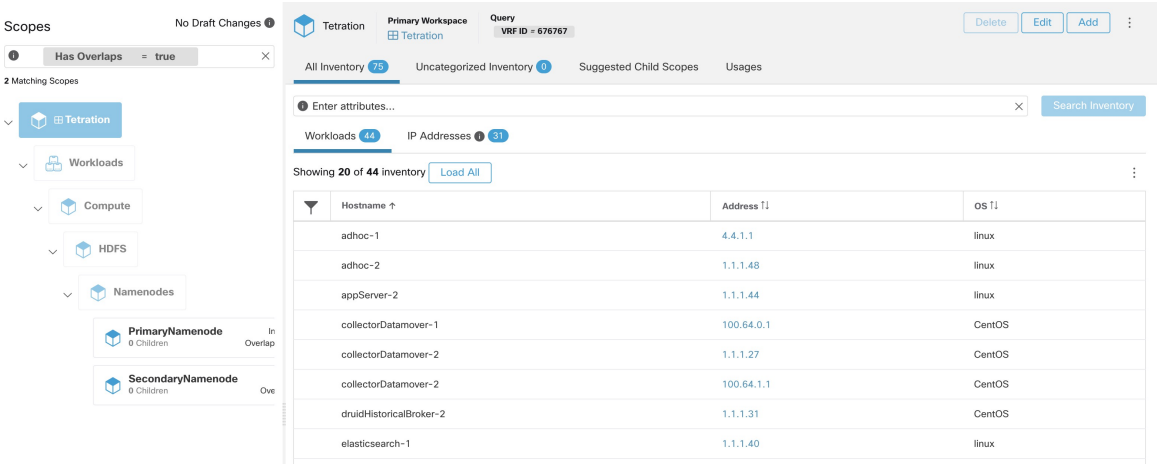


範囲の重複

範囲を追加するときは、範囲の重複を避けることをお勧めします。範囲が重複すると、重複する範囲に対して生成されたポリシーが、エンドユーザーの混乱を招く可能性があります。この機能は、範囲メンバーシップが重複している場合、つまり、同じインベントリが範囲ツリー（兄弟範囲）の同じ深さの複数の範囲に属している場合に、積極的にユーザーに通知します。その目的は、範囲ツリーの異なる部分に同じワークロードが存在することを避けることです。

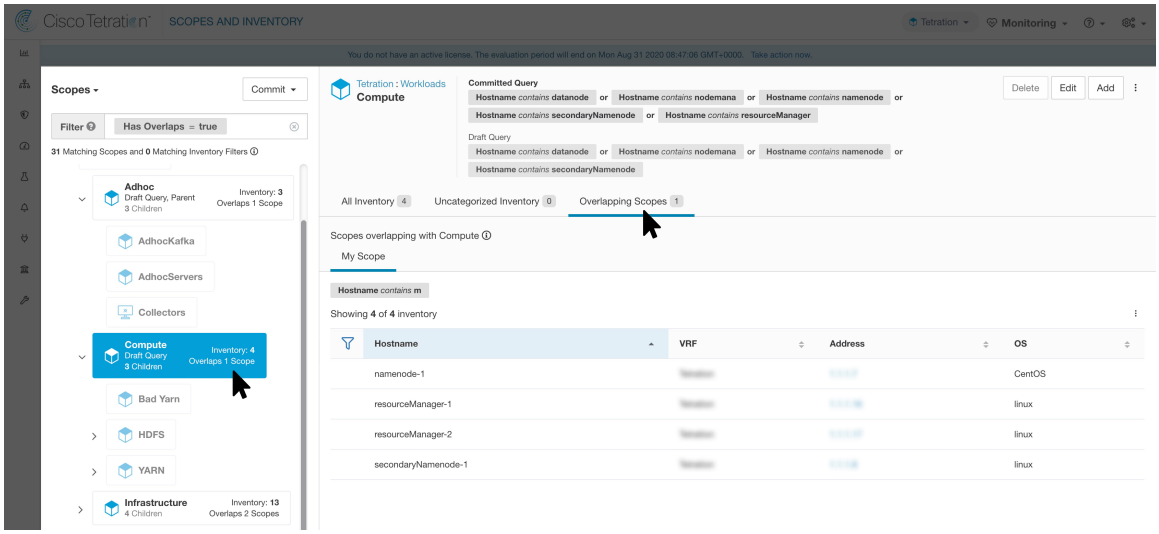
複数の範囲に属するインベントリ項目を表示するには、範囲フィルタを使用し、**Has Overlaps = true** ファセットを入力します。

図 *13* : 範囲フィルタでの重複ファセット



重複する範囲および対応する重複する IP アドレスのリストは、範囲ツリーを下に移動し、[重複する範囲（Overlapping Scopes）] タブを選択することで表示できます。

図 *14* : 範囲と *IP* の重複



スコープの編集

ルート範囲で SCOPE_OWNER 権限を持つユーザーのみが範囲を削除できます。サイト管理者は、すべての範囲の所有者です。

範囲名の編集

範囲名の編集は瞬時に完了しますが、更新が必要な子範囲の数によっては数分かかる場合があります。

（注） 範囲名を変更すると、範囲名によるフロー検索が影響を受けます。

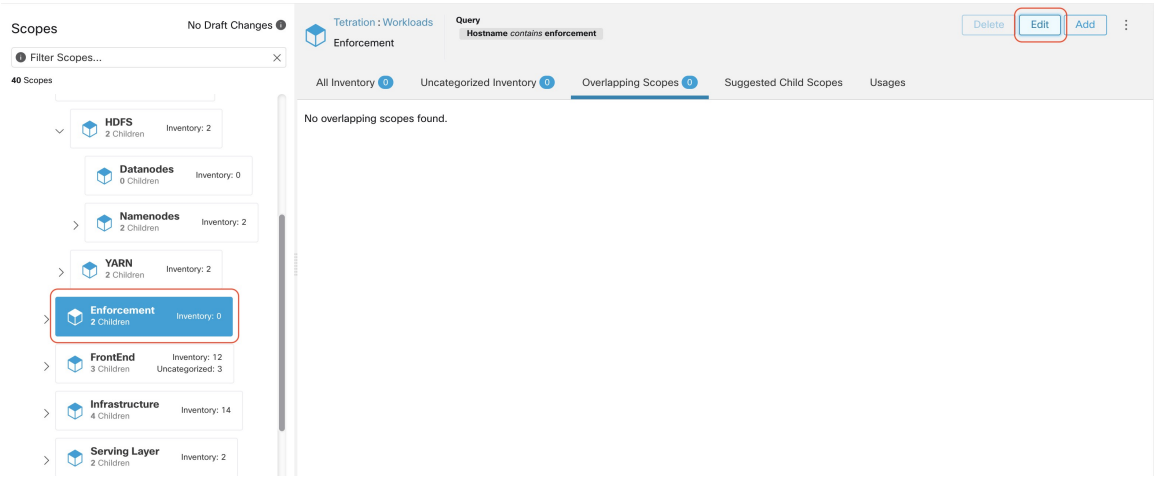
範囲クエリの編集

範囲のクエリが変更されると、直接の親と子の範囲が影響を受けます。これらの範囲は、確定されていない変更がツリーに加えられたことを示す「ドラフト変更」があるとマークされています。すべてのクエリの更新が完了したら、ユーザーは範囲ディレクトリの上にある [変更の確定（Commit Changes）] ボタンをクリックして、変更を永続化する必要があります。これにより、バックグラウンドタスクがトリガーされ、ワークスペース内のすべての範囲クエリと「動的クラスタクエリ」が更新されます。

警告 範囲クエリを更新すると、範囲のインベントリメンバーシップ（範囲のメンバーであるワークロード）に影響を与える可能性があります。変更は、変更の確定プロセス中に有効になります。リスクを軽減するために、[範囲/フィルタ変更の影響を確認する（Review Scope/Filter Change Impact）] ウィンドウから、メンバーシップの変更を比較して、影響を詳細に分析できます。範囲/フィルタ変更の影響を確認 （48 ページ）

新しいホスト ファイアウォール ルールが挿入され、関連するホスト上で既存のルールがすべて削除されます。

図 *15* : 範囲の編集



範囲を編集するには、次の手順を実行します。

ステップ 1 編集するそれぞれの範囲の**編集ボタン**をクリックします。

ステップ 2 選択した範囲の名前またはクエリを編集します。

ステップ 3 [クエリ変更の影響の確認（Review query change impact）] のリンク先に移動して、古いドラフトクエリと新しいドラフトクエリの間の変更を比較します。

ステップ 4 [保存（Save）] をクリックします。名前はすぐに更新されます。

ステップ 5 すべての範囲のクエリを更新するには、 [変更の確定（Commit Changes）] ボタンをクリックします。

ステップ 6 範囲の変更を実行した結果を示す確認ポップアップウィンドウが表示されます。更新は、バックグラウンドタスクで非同期に処理されます。

ステップ 7 [保存（Save）] をクリックします。変更の数によっては、保存に 1 分以上かかる場合があります。

図 *16* : クエリ変更の影響の確認

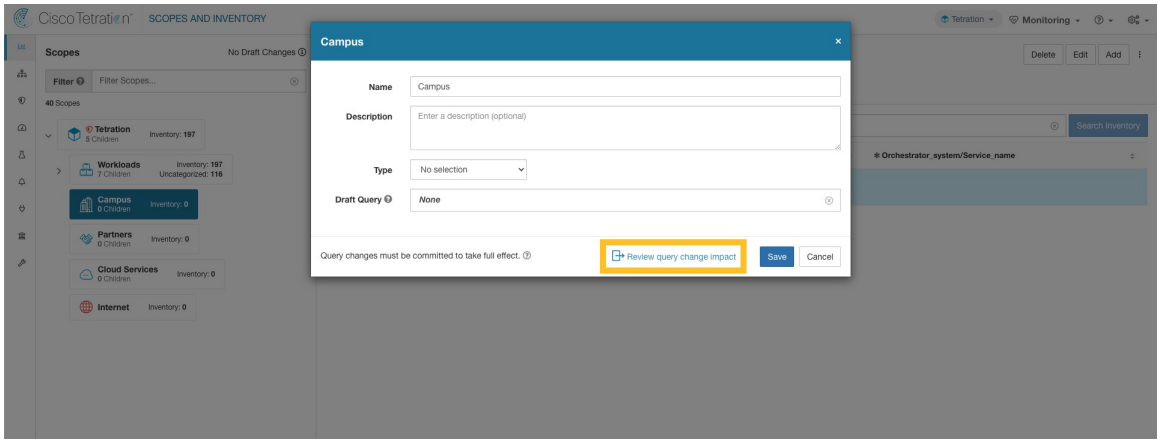
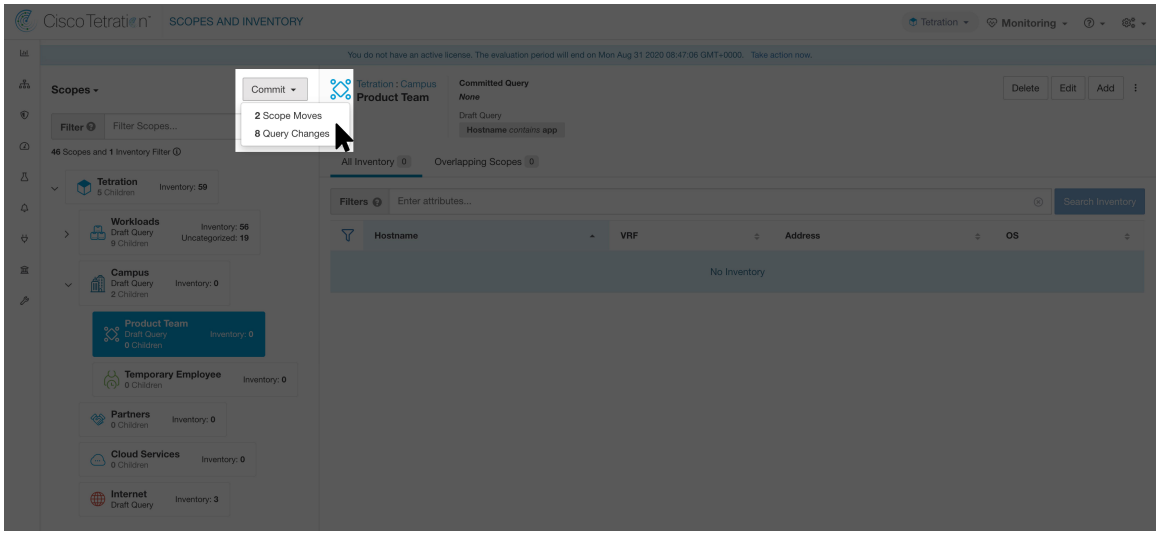


図 *17* : 変更の確定



範囲の親の編集

範囲の親が更新されると、範囲クエリが変更されます。この変更は、親スコープと子スコープの両方のメンバーシップに影響します。範囲クエリの編集と同様に、これらの変更は最初「ドラフト変更」として保存され、確定されない限り有効になりません。ユーザーは、[範囲の編集（Edit Scope）] モーダルで [クエリ変更の影響を確認（Review query change impact）] をクリッ

クして、確定する前にこの変更の影響を検証できます。検証が完了したら、[確定（Commit）] をクリックし、[範囲の移動（Scope Moves）] と [クエリの変更（Query Changes）] を承認することで、変更を確定できます。

範囲の親を編集するには、次の手順に従います。

ステップ 1 編集するそれぞれの範囲の [編集（Edit）] ボタンをクリックします。

ステップ 2 選択した範囲の親を編集します。

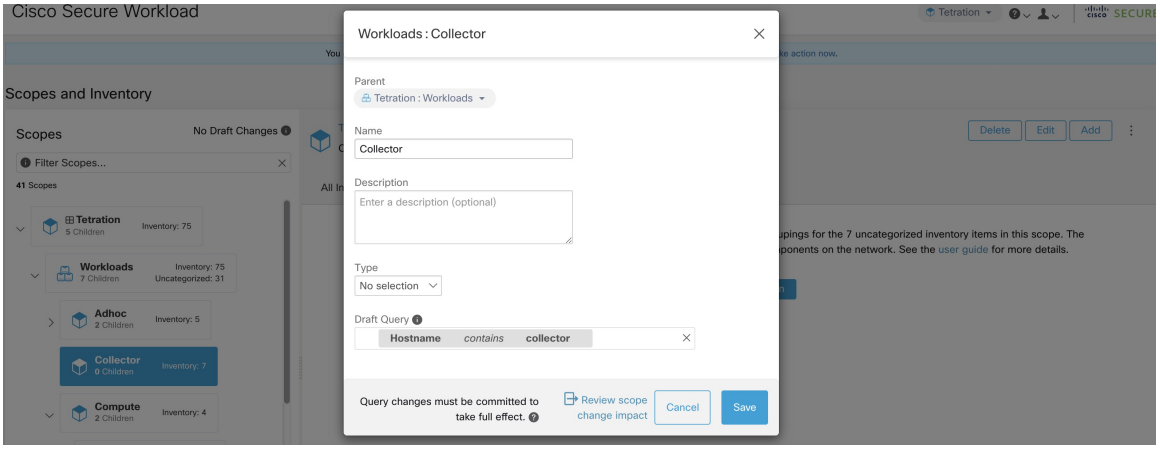
ステップ 3 [クエリ変更の影響の確認（Review query change impact）] リンクをクリックして、古いドラフトクエリと新しいドラフトクエリの間の変更点を比較します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 [確定（Commit）] をクリックし、[範囲の移動（Scope Moves）] と [クエリの変更（Query Changes）] を承認します。更新は、バックグラウンドタスクで非同期的に処理されます。

ステップ 6 この変更の影響を受けるワークロードの数によっては、処理に 1 分以上かかる場合があります。

図 *18 :* 親範囲をデフォルト範囲から *Default:ProdHosts* に変更する



スコープの削除

ルート範囲で SCOPE_OWNER 機能を持つユーザーのみが範囲を削除できます。サイト管理者は、すべての範囲の所有者です。

範囲を削除すると、親範囲（親範囲のメンバーであるワークロード）のアプリケーションインベントリ メンバーシップに影響があります。. その結果、親範囲は「ドラフト変更」を持つものとしてマークされます。変更のコミットおよび依存構造の更新が必要です。「変更の確定」を参照してください。

依存オブジェクトのある範囲は削除できません。次の場合はエラーが返されます。

- 範囲にワークスペースが定義されている。
- 範囲に割り当てられたインベントリフィルタがある。

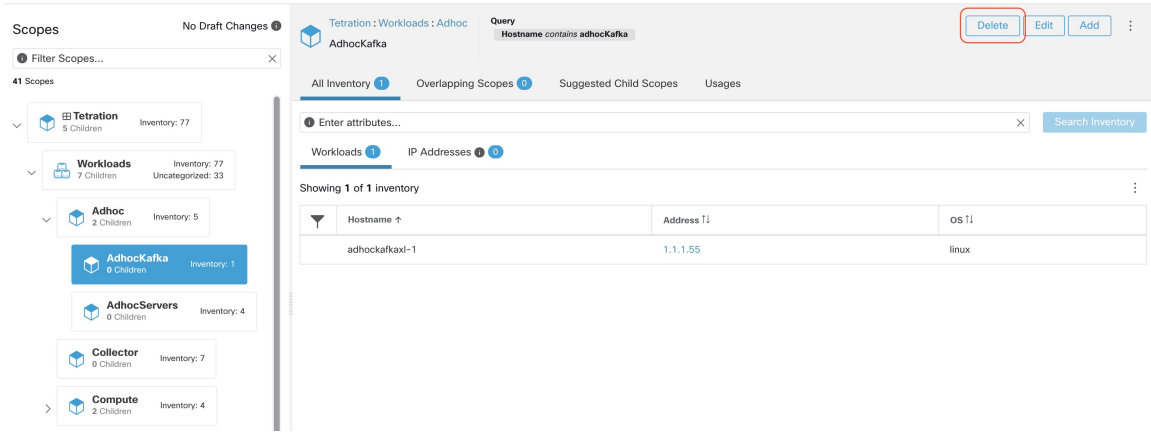
- 範囲を使用してコンシューマまたはプロバイダーを定義するポリシーが存在する。
- 範囲で Agent Config Intent が定義されている。
- 範囲で Interface Config Intent が定義されている。
- 範囲で Forensics Config Intent が定義されている。

範囲の依存関係をさらにドリルダウンするには、「範囲/フィルタ変更の影響を確認」ウィンドウから、[依存関係（Dependencies）] タブにアクセスします。

範囲を削除する前に、これらのオブジェクトを削除する必要があります。

1. 左側のナビゲーションバーで、**[整理（Organize）]>[範囲とインベントリ（Scopes and Inventory）]** をクリックします。
2. [範囲（scope）] を選択して再度クリックすると、子範囲が表示されます。削除する子範囲を選択します。
3. [編集（edit）] ボタンと [追加（add）] ボタンの横にある [削除（Delete）] ボタンをクリックします。

図 *19* : 範囲の削除



（注） 子のない範囲のみ削除できます

（注） [テナント（Tenants）] ページから VRF を削除して、ルート範囲を削除する必要があります。

範囲ツリーのリセット

上記の構成のいずれかが存在する場合は、範囲ツリーをリセットする前にそれらを削除する必要があります。これを行うまで、[リセット（Reset）] ボタンは使用できません。

範囲ツリーをリセットするには：

始める前に

範囲ツリー全体を削除して、最初からやり直すことができます。

範囲ツリーをリセットすると、すべての範囲、ラベル、ワークスペース、およびコレクションルールが削除されます。取り込まれたデータは削除されません。

ルート範囲で SCOPE_OWNER 機能を持つユーザーのみが、範囲ツリーをリセットできます。

ただし、ツリー内のいずれかの範囲に対して次のいずれかが定義されている場合、範囲ツリーをリセットすることはできません。

- ワークスペース（ウィザードを使用して範囲ツリーを作成した場合に作成された単一のワークスペースを除く）
- インベントリ フィルタ
- ポリシー
- エージェント構成インテント
- インターフェイス設定インテント
- フォレンジック構成インテント

ステップ 1 左側のナビゲーションメニューから、**[整理（Organize）] > [範囲とインベントリ（Scopes and Inventory）]** を選択します。

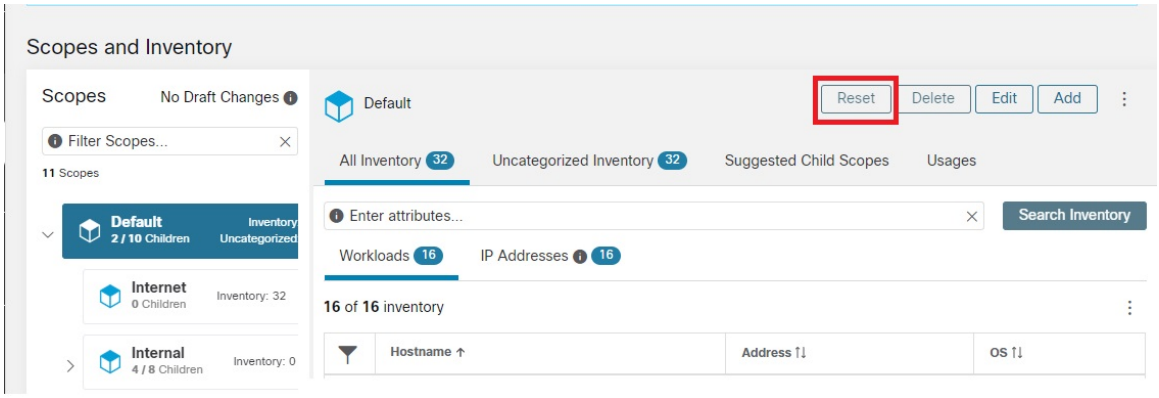
ステップ 2 ツリーの上部にある範囲をクリックします。

ステップ 3 [リセット（Reset）] をクリックします。

ステップ 4 選択を確認します。

ステップ 5 必要に応じて、ブラウザページを更新して続行します。

図 *20 :* 範囲ツリーのリセット



変更の確定

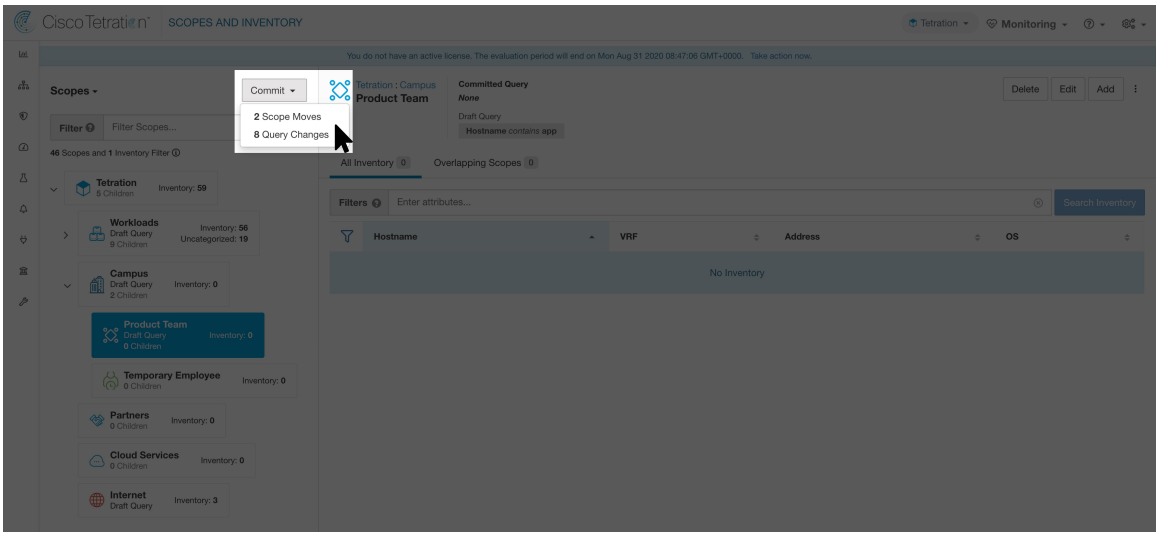
ある範囲のアプリケーション インベントリ クエリ定義は、その範囲のクエリとその直接の子のクエリによって定義されます。これが発生すると、範囲は「ドラフト変更」があるとマークされ、範囲のクエリ、ワークスペース、およびクラスタは、[変更の確定（Commit Changes）] バックグラウンドタスクが実行されるまで変更されません。範囲がドラフトの場合、影響を受ける範囲アイコンごとに三角の注意マークが表示され、[変更の確定（Commit Changes）] ボタンが [範囲（Scopes）] ページに表示されます（右上）。このボタンをクリックして [変更の確定（Commit Changes）] バックグラウンドタスクを実行する必要があります。

範囲をドラフトとしてマークできるイベントは次の通りです。

- クエリの更新
- 親のクエリが更新された
- 直接の子が追加された
- 直接の子が削除された
- 直接の子のクエリが更新された

範囲の名前を変更しても、範囲のドラフト状態は変更されません。

図 *21* : 変更の確定



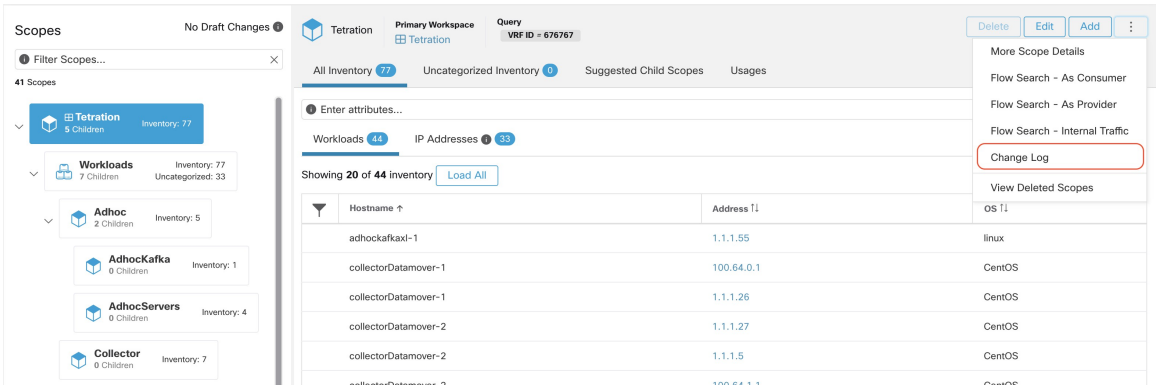
（注） [変更の確定（Commit Changes）] タスクは非同期です。通常は数秒かかりますが、大きな範囲ツリーでは数分かかることがあります。

（注） 範囲の更新タスクは、ルート範囲がドラフトでなくなると完了します。ページを更新して最新の状態を表示します。

ログの変更

サイト管理者およびルート範囲で SCOPE_OWNER 機能を持つユーザーは、右上のオーバーフローメニューの変更ログをクリックして、各範囲の変更ログを表示できます。

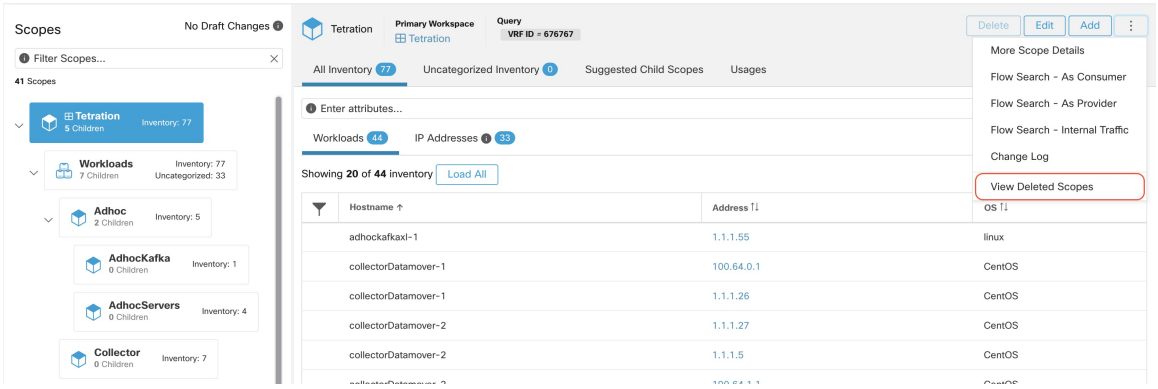
図 *22* : 変更ログ



変更ログの詳細については、「変更ログ」を参照してください。ルート範囲の所有者は、所有範囲に属するエンティティの変更ログエントリのみ表示できます。

そのようなユーザーは、右上隅のオーバーフローメニューにある[削除された範囲の表示（View Deleted Scopes）]リンクをクリックして、削除された範囲のリストを表示することもできます。

図 *23 :* 削除された範囲の表示（*View Deleted Scopes*）



新しいテナントの作成

ルートレベルの範囲は、テナント または [範囲（Scopes）] 管理ページから作成された VRF にマッピングされます。このアクションは、サイト管理者とカスタマーサポートのユーザーのみが利用できます。

ステップ 1 左側のナビゲーションバーで、**[プラットフォーム（Platform）]** > **[テナント（Tenants）]**をクリックします。

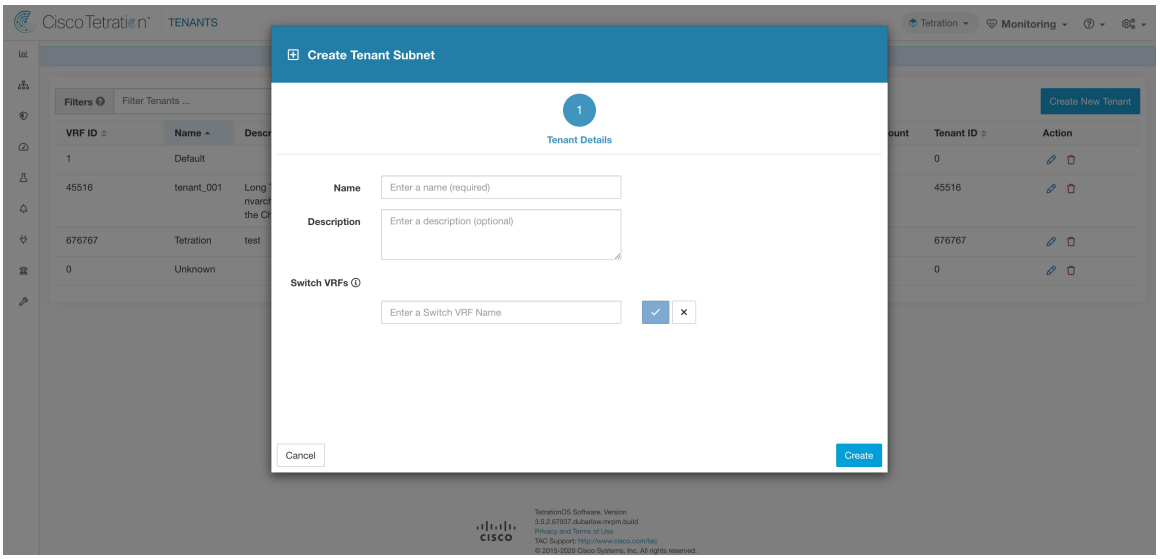
ステップ 2 [新しいテナントの作成（Create New Tenant）] ボタンをクリックします。

ステップ 3 以下のフィールドに適切な値を入力します。

フィールド	説明
Name	範囲を識別する名前。親範囲の下で一意である必要があります。
説明	任意の説明。
スイッチVRF（Switch VRFs）	複数のハードウェア（スイッチ）VRF をこの Secure Workload テナントにマッピングします。

ステップ 4 [作成（Create）] ボタンをクリックします。

図 *24* : テナントの作成（***Create Tenant***）



インベントリ

インベントリで作業するには、左側のナビゲーションバーで**[整理（Organize）]**>**[範囲とインベントリ（Scopes and Inventory）]** をクリックします。

収集ルールの適用後にネットワーク上で観察されたすべてのインベントリの合計は、ファセット入力の下の右側のパネルにデフォルトでロードされます。

[インベントリ検索（Inventory Search）]

ネットワーク上で検出されたすべてのインベントリが検索可能です。インベントリを検索するには、[インベントリの検索（Search Inventory）] ボタンを使用します。各インベントリ項目は、IP および VRF によって一意に識別でき、検索の実行に使用できます。サービスインベントリ項目は、自身の IP アドレスを使用して検索できません。サービスインベントリを検索するには、user_orchestrator_system/service_name など、サービスに関連付けられているユーザーラベルのいずれかを使用してください。ホストが見つかったら、[ホストプロファイル（host profie）] ページで、ホストに関する詳細情報を表示できます。

インベントリ構成要素

1. ルート範囲
   - 指定されたテナント下の範囲階層ルート
   - L3 アドレスドメインの論理的な分離を提供
2. スコープ

- 動的クエリで定義されたインベントリコンテナ
- 階層型ポリシーモデルの基礎
- ポリシー、RBAC、およびフィルタ設定のアンカーポイント

3. フィルタ
   - 動的なインベントリクエリに基づく柔軟な構築
   - インテント定義、提供サービス、ポリシー定義のアンカーポイント

（注） パートナーからのすべての IP アドレスと、使用中の環境内で通信しているすべてが含まれます。環境にエージェントが存在するかどうかにかかわらず、ラベルを使用して内容を定義する必要があります。

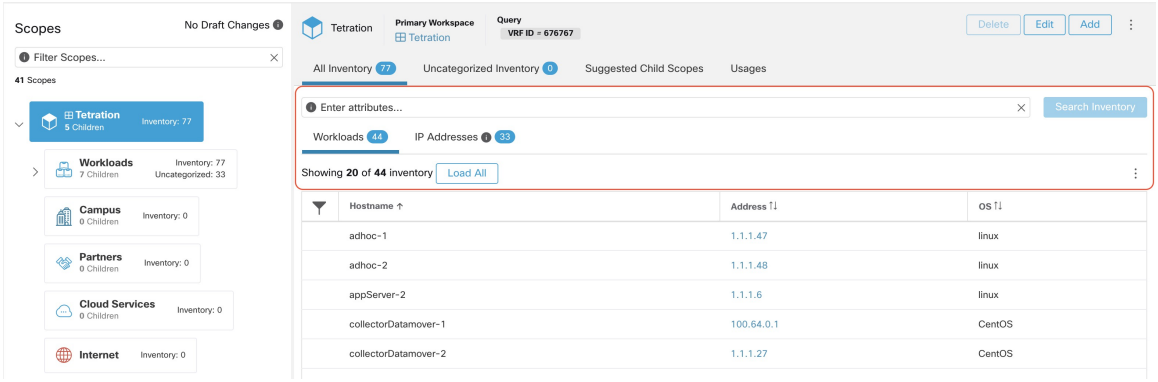
ラベルプランニングの考慮事項

1. データの送信元
   - ネットワークは、IPAM か。ルーティングテーブルか。スプレッドシートか。
   - ホストは、CMDB か。ハイパーバイザか。クラウドか。アプリケーションオーナーか。
2. データの精度
3. データがどの程度動的で、どのように更新されるか
   - 手動アップロードか。
   - API の統合か。
4. 基本から始めて進化させる
   - ネットワークラベルを使用して高度な範囲構造を構築する
   - ホストラベルを使用して、アプリケーションレベルでより詳細な範囲構造を構築する

インベントリの検索

インベントリを検索すると、特定のインベントリ項目に関する情報を表示できます。

図 *25 : [*インベントリ検索（***Inventory Search***）*]*



ステップ 1 トップレベルのメニューから、**[整理（Organize）]** > **[範囲とインベントリ（Scopes and Inventory）]** を選択します。

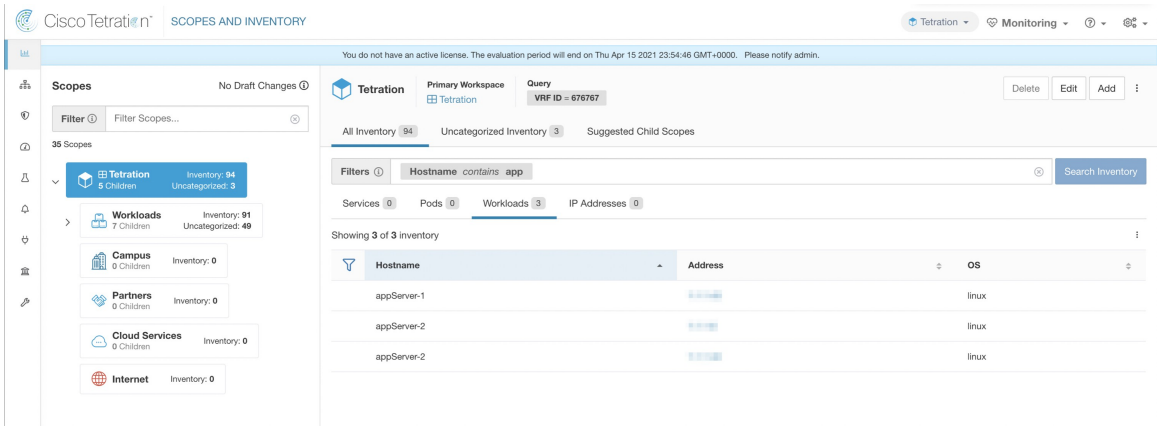
ステップ 2 [フィルタ（Filters）] フィールドに、探しているインベントリ項目の 属性を入力します。次のような属性があります。

属性	説明
ホスト名（Hostname）	ホスト名の全体または一部を入力します。
[VRF名（VRF Name）]	VRF 名を入力します。
VRF ID	VRF ID（数値）を入力します。
アドレス（Address）	有効な IP アドレス（IPv4 または IPv6）を入力します。
アドレス タイプ	IPv4 または IPv6 を入力します。
OS	OS 名（CentOS など）を入力します。
[OS Version]	OS バージョンを入力します（例：6.5）。
Interface Name	インターフェイス名を入力します（例：eth0）。
MAC	MAC アドレスを入力します。
収集ルールに含まれる（In Collection Rules?）	true または false を入力します。
プロセスコマンドライン（Process Command Line）	ホストで実行されているコマンド文字列の一部を入力します（注：このファセットはインベントリフィルタの一部として保存できません）。
プロセスバイナリハッシュ（Process Binary Hash）	ホストで実行されているコマンドのプロセスハッシュを入力します（注：このファセットはインベントリフィルタの一部として保存できません）。

属性	説明
パッケージ情報（Package Info）	必要に応じて、パッケージ名の後にパッケージバージョンを入力します（プレフィックス # を付けます）。
パッケージ CVE（Package CVE）	CVE ID の一部または全体を入力します。
CVE スコア v2（CVE Score v2）	CVSSv2（Common Vulnerability Scoring System）スコア（数値）を入力します。
CVE スコア v3（CVE Score v3）	CVSSv3（Common Vulnerability Scoring System）スコア（数値）を入力します。
ユーザーラベル（User Labels）	プレフィックスが付いたユーザーラベルに由来する属性

ステップ 3 [インベントリの検索（Search Inventory）] をクリックします。結果は、[フィルタ（Filter）] フィールドの下に、4 つのタブにグループ化されて表示されます。各タブには、関連するカラムを含むテーブルが表示されます。テーブルヘッダーのファネル（じょうご）アイコンをクリックすると、追加の列を表示できます。ユーザーラベルが使用可能な場合は、プレフィックスが付き、ここで切り替えることができます。

図 *26* : インベントリの検索結果



検索結果は、次の 4 つのタブにグループ化されます。

タブ	説明
サービス	外部オーケストレータを介して検出された Kubernetes サービスおよびロードバランサを一覧表示します。このタブは、関連する外部オーケストレータが構成されている場合を除き非表示になります。
ポッド	Kubernetes ポッドを一覧表示します。このタブは、関連する外部オーケストレータが構成されている場合を除き非表示になります。

タブ	説明
ワークロード	Secure Workload エージェントによって報告されたインベントリ項目を一覧表示します。
IP アドレス	インベントリのアップロードとフローを通じて検出されたインベントリ項目を一覧表示します。

各タブの横にインベントリ数も表示されます。検索ですぐに表示される情報には、ホスト名、IPアドレス、OS、OSバージョン、サービス名、ポッド名などがあります。表示されるカラムのリストは、テーブルヘッダーのファネル（じょうご）アイコンをクリックして切り替えることができます。検索結果は、範囲ディレクトリに表示されている現在選択されている範囲に制限されます。検索結果の項目をクリックすると、それぞれのプロファイルページで詳細情報を表示できます。

各ホストの詳細は、検索結果行の IP アドレスフィールドをクリックしてアクセスできる [ワークロードプロファイル（Workload Profile）] に表示されます。詳細については、「ワークロード プロファイル」を参照してください。

サイドバーからインベントリフィルタを作成するには、トップレベルメニューから **[整理（Organize）]** > **[インベントリフィルタ（Inventory Filters）]** を選択します。[フィルタの作成（Create Filter）] ボタンをクリックします。保存するフィルタに名前を付けることができるモーダルダイアログが表示されます。

子範囲の提案

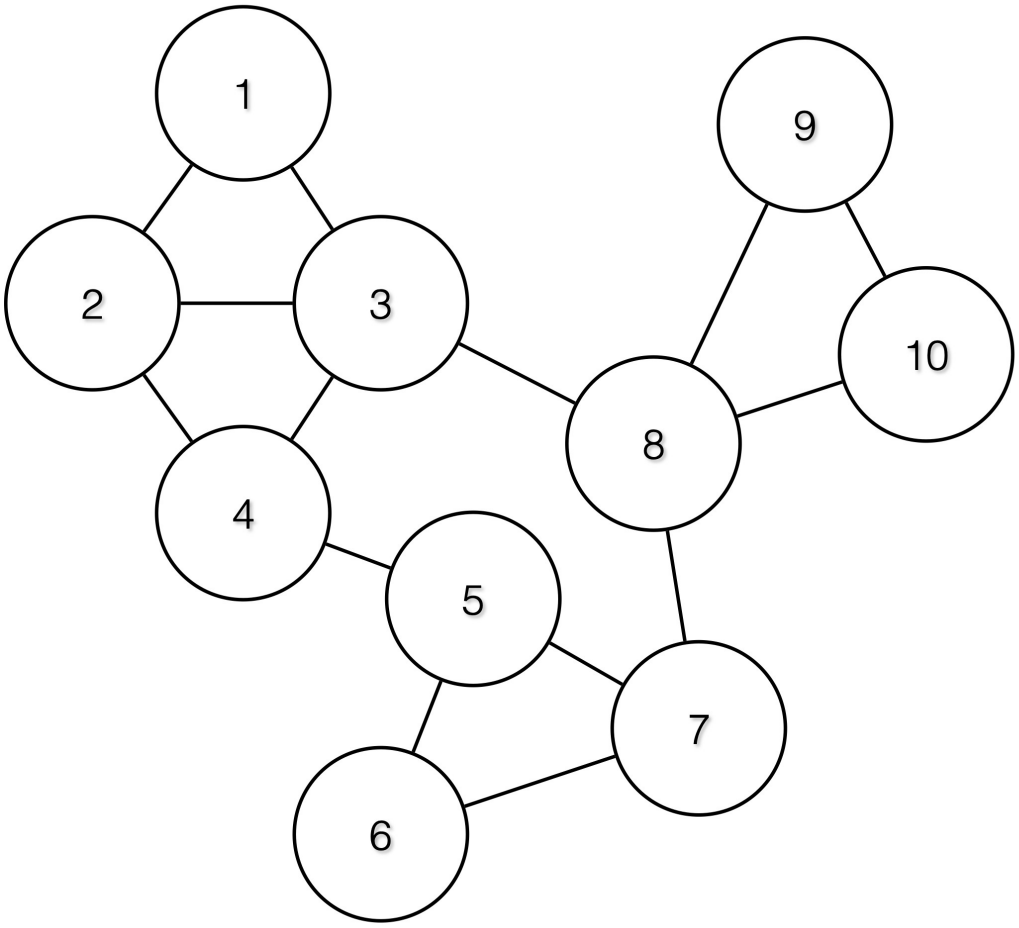
子範囲の提案は、機械学習アルゴリズム（ネットワークでのコミュニティ検出など）を使用して、範囲として機能する可能性のあるグループを検出するツールです。このツールは、範囲階層を構築するときに役立ち、特定の範囲に対してより詳細な子範囲を定義するプロセスを容易にします。候補の子範囲は提案として表示され、選択して追加できます。

概念レベルでのアルゴリズムの説明：親範囲の要求されていないメンバー間の通信に基づくグラフが最初に作成されて、グラフが処理されます（注：要求されていないメンバーとは、親の子範囲に属していないメンバーです）。たとえば、アルゴリズムでは、グラフ内の大部分を占める他のエンドポイントと通信するエンドポイントが識別されます。そのようなエンドポイントのグループが見つかった場合は、**共通サービス**グループの候補としてユーザーに表示されます。グラフの残りの部分は、**コミュニティ**として動作するグループを検出するために処理されます。コミュニティとして動作するとは、エンドポイントがグループ外のエンドポイントよりも不釣り合いに頻繁に（またはより多くのプロバイダーポートで）互いに通信することを意味します。そのような各グループは、アプリケーションまたは組織内の部門に対応している場合があります。そのようなパーティション分割により、範囲間でポリシーが希薄になる可能性もあります。

例：

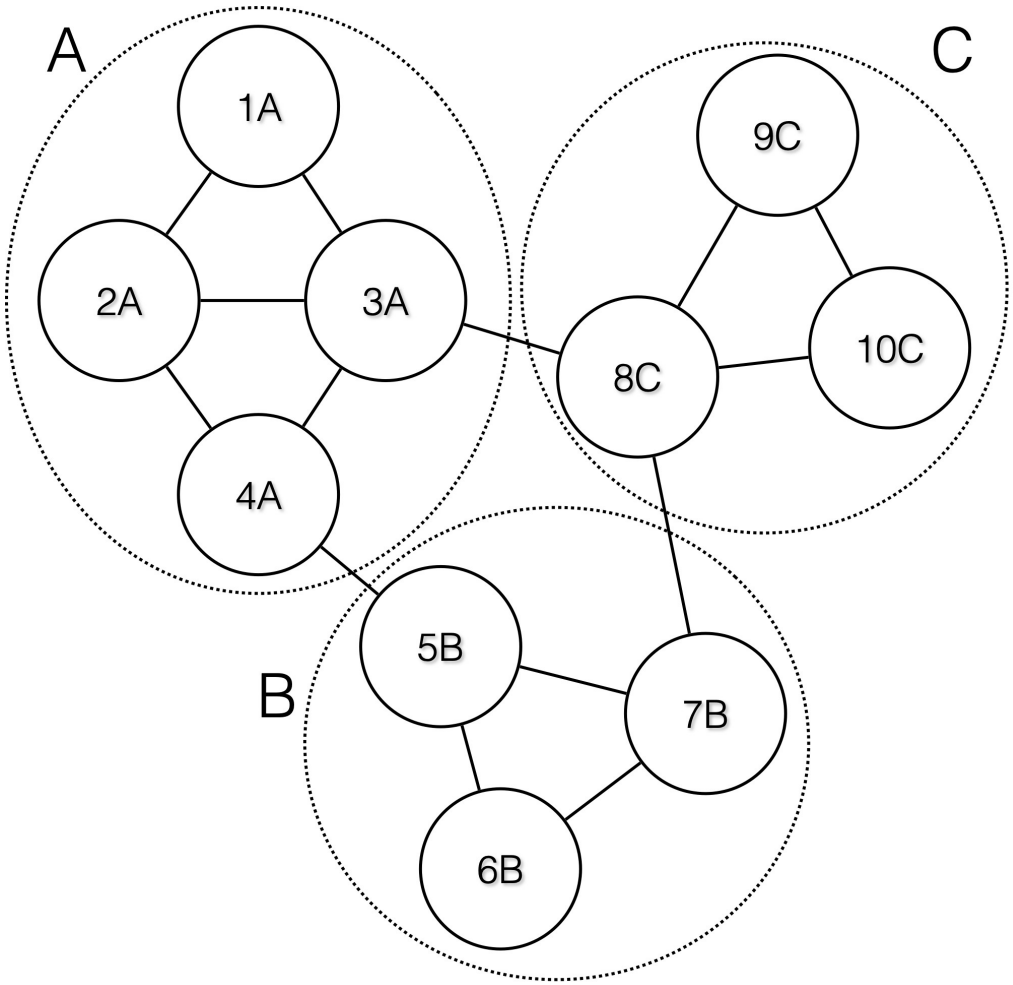
次の図の 1 から 10 を個々のエンドポイント IP とします。入力（通信）グラフは次のようになっているとします。

図 *27 :* 入力グラフ



次に、エンドポイント 1 ～ 4、5 ～ 7、および 8 ～ 10 では、相互に比較的高度な通信（エッジの数）が行われ、他のエンドポイントとの通信が比較的少ないため、一緒にグループ化されます。

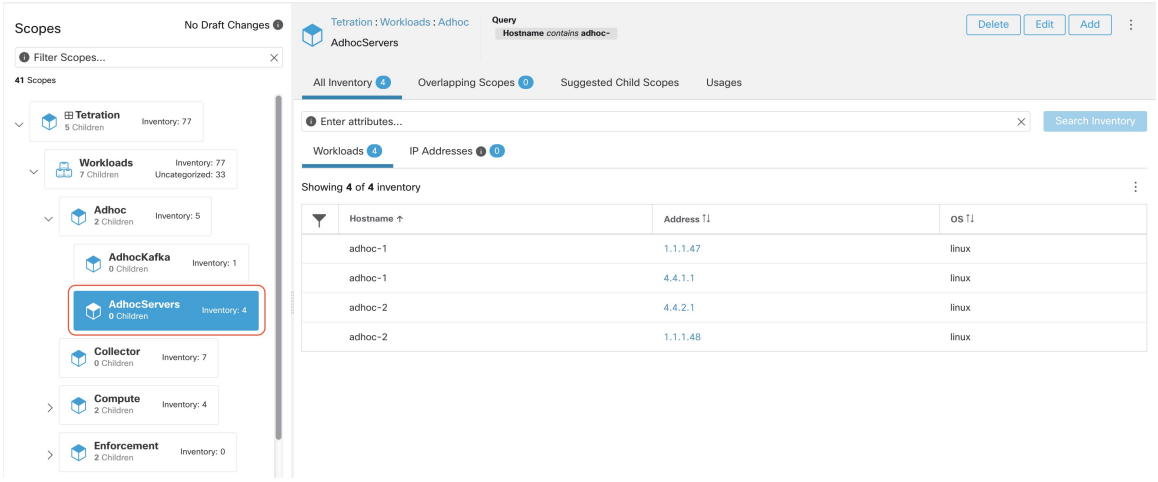
図 *28 :* 出力グループ



範囲の提案の実行手順

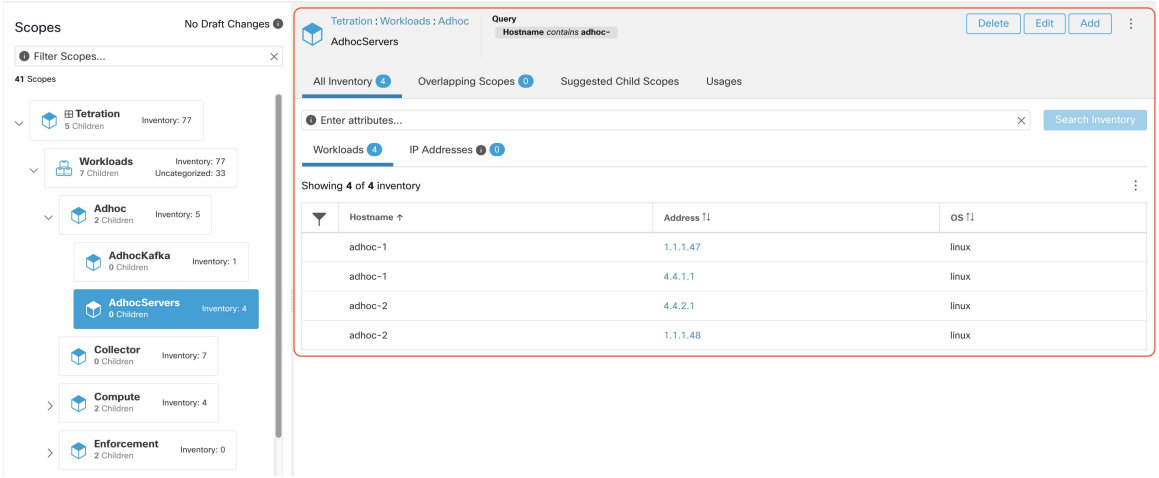
目的の範囲の範囲の提案を開始するには、範囲のページで範囲を検索して選択する必要があります。

図 *29* : 範囲の選択例



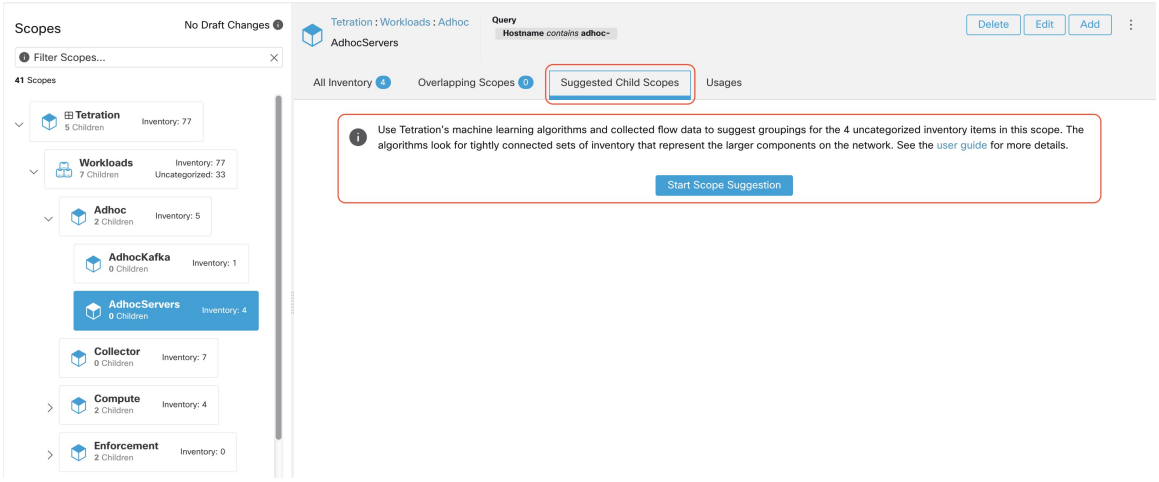
このウィンドウでは、ユーザーはインベントリ「未分類のインベントリ項目」を参照できます。つまり、現在選択されている範囲に属し、現在選択されている範囲のいずれの子範囲にも属さない項目を参照できます。**未分類のインベントリ項目**をクリックすると、このリストを表示できます。

図 *30* : 範囲ウィンドウの例



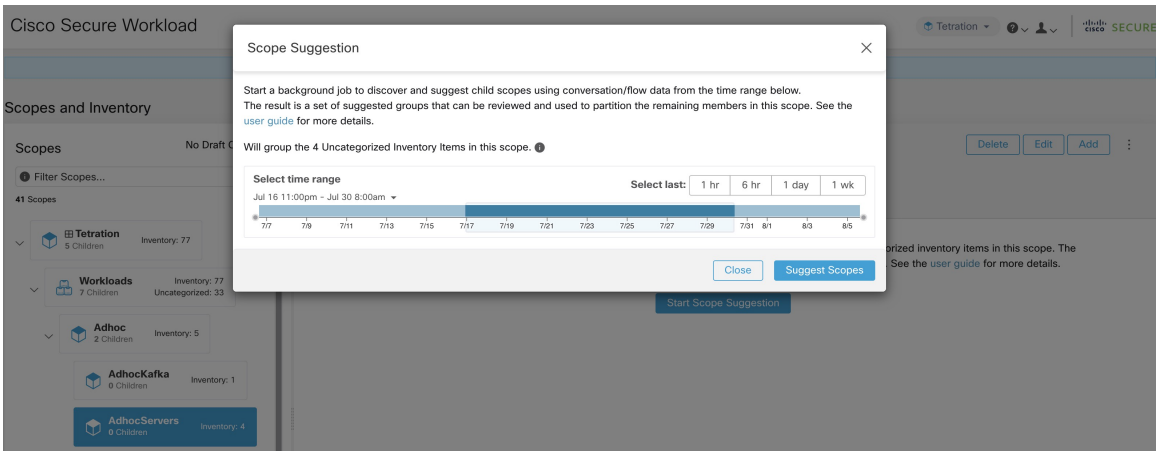
範囲を選択した後、ユーザーは[子範囲の提案（Suggest Child Scopes）]をクリックし、[範囲の提案の開始（Start Scope Suggestion）]をクリックできます（または、これが初めてでない場合は[再実行（Rerun）]をクリックします）。範囲提案の実行の入力は、分類されていないインベントリ項目になることに注意してください。

図 *31* : [子範囲の提案（*Suggest Child Scopes*）] タブ



ユーザーは、範囲提案の入力として日付範囲を設定し、[範囲の提案（Suggest Scopes）] をクリックできます。範囲の提案の実行は、全体的な負荷が中程度の場合は高速であることが多く、数万回の通信で 10 から数千のエンドポイントを処理するのに数分しかかかりません。

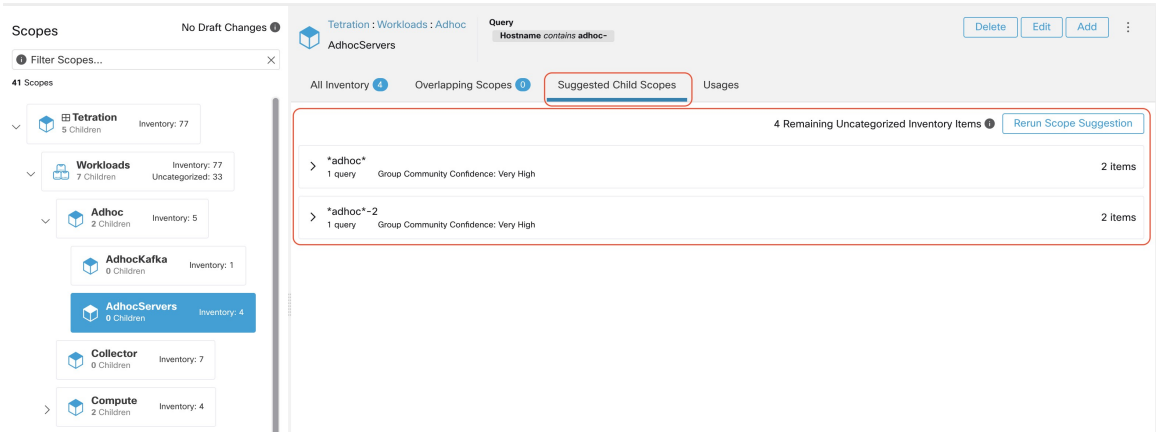
図 *32* : 範囲提案データ範囲セレクタの例



出力は、候補のリストとしてユーザーに表示されます。現在、最大20のグループが表示され、それぞれにグループの信頼度（品質）、候補範囲名、クエリなどの情報が付随しています。検出された各グループには、関連付けられた [グループコミュニティ信頼度（Group Community Confidence）] があり、次の値のいずれかが示されます。[非常に高（Very High）]、[高（High）]、[中（Medium）]、[低（Low）]。これは、グループの [コミュニティ（Community）] プロパティの基準となります。信頼度が高いほど、エンドポイントの特定のグループのコミュニティプロパティが高くなります（グループの内側に多くのエッジがあり、外側のエッジが比較的少ない）。表示されているグループのサブセットは、[グループコミュニティ信頼度（Group Community Confidence）] に基づいて選択されています。検出されたグループは、現在、次の 4 つのグループタイプのいずれかに分類されます。

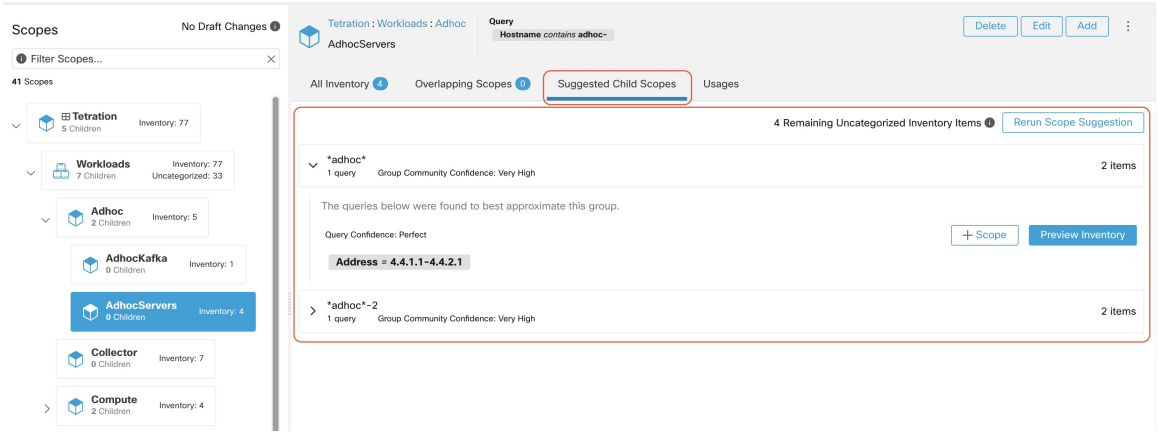
- [一般グループ（Generic Group）]：コミュニティプロパティに基づいて機械学習によって検出されたすべてのグループ。以下の特別なタイプで明示的に指定されていないグループは、一般グループであることに注意してください。
- [共通サービス（Common Service）]：このグループは、入力インベントリの多くと通信するエンドポイントで構成されます。これらのエンドポイントは、何らかの共有サービスを実行している可能性があります。
- [共通サービスクライアント（Common Service Clients）]：このグループは、[共通サービス（Common Service）] グループとのみ通信するエンドポイントで構成されます。
- [グループ化解除（Ungrouped）]：このグループは、十分な通信がないためにグループ化できないエンドポイントで構成されます。

図 *33*：範囲提案の出力例



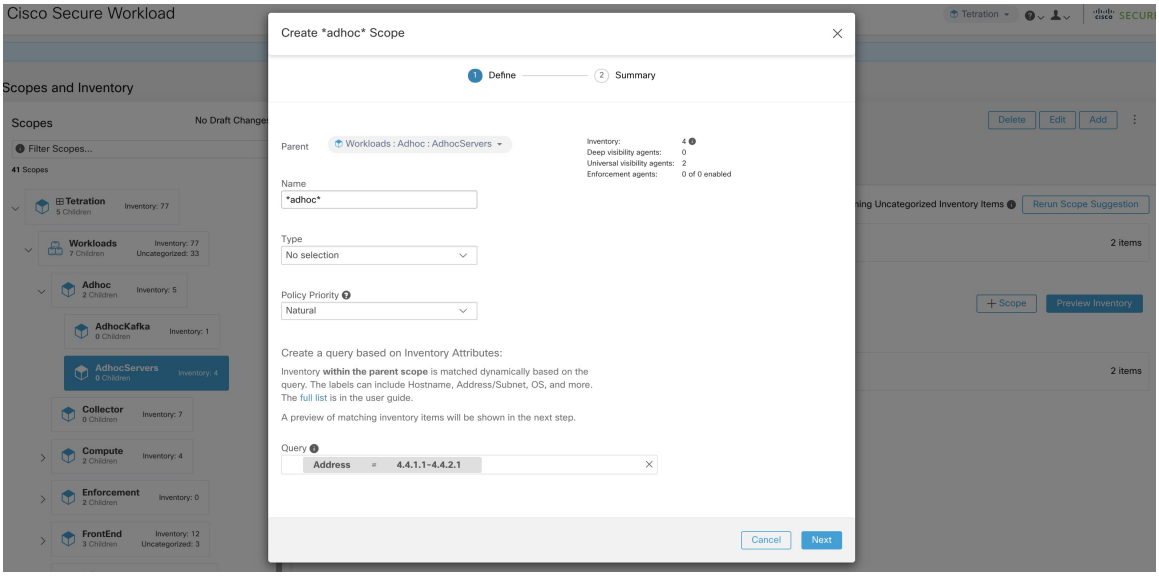
ユーザーは、検出されたグループをクリックして、選択したグループに対して生成されたクエリのリストを表示できます。ユーザーは、検出されたグループを厳密に定義するクエリの範囲と一致するインベントリをプレビューできます。クエリは、IP範囲、サブネット、ホスト名、およびユーザーがアップロードしたラベルで構成されます。各グループに関連付けられた信頼度基準があり、[クエリの信頼度（Query confidence）] と呼ばれます。次の値の範囲のいずれかとなります。 [完全（Perfect）]、[非常に高（Very High）]、[高（High）]、[中（Medium）]、[低（Low）]。クエリ生成では、まずグラフ処理と機械学習によってグループが検出され、次にグループごとにクエリが生成されます。[クエリの信頼度（Query confidence）]は、クエリの範囲がエンドポイントとどの程度一致するかの基準です。 [完全（Perfect）] のクエリ信頼度は、提案された（検出された）グループがクエリの範囲と正確に一致していることを示します。反対に、クエリの信頼度が[低（Low）]の場合は、クエリは多くの提案されたグループを取りこぼし、正確に一致できていないことを示しています。これは、クエリの範囲が[過剰なIP（Extra IPs）]となっている（検出されるグループの範囲外である）、またはクエリに多くの[欠落IP（Missing IPs）] がある（クエリの範囲外である）ことを意味します 。

図 *34* : 範囲提案出力クエリの例



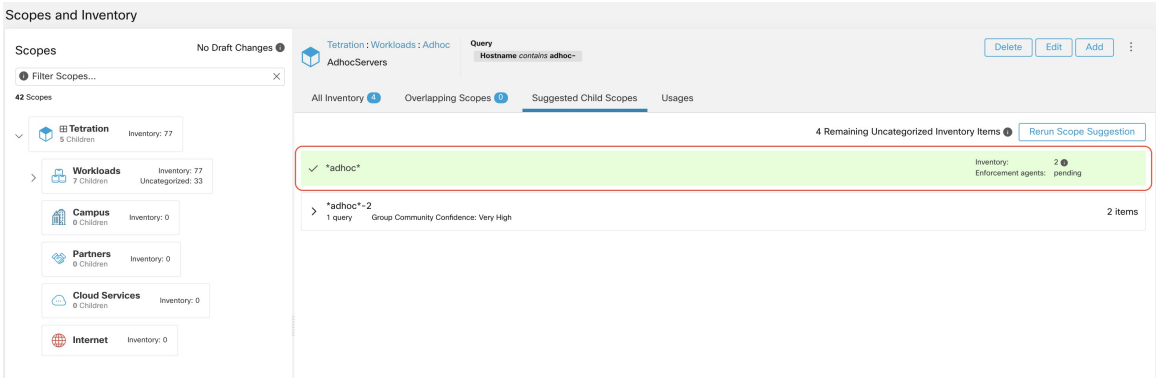
ユーザーは、[+範囲（+ Scope）] ボタンをクリックして、グループ名とグループクエリを編集できる編集ウィンドウに移動できます。ユーザーは、クエリおよび一致する IP を調べ、クエリを調整して一部の IP を追加または削除する必要があるかどうかを判断できます。問題がなければ、ユーザーは [次へ（Next）] をクリックして確認し、ドラフトビューキャンバスでグループを範囲に変換できます。

図 *35* : 範囲提案編集画面の例



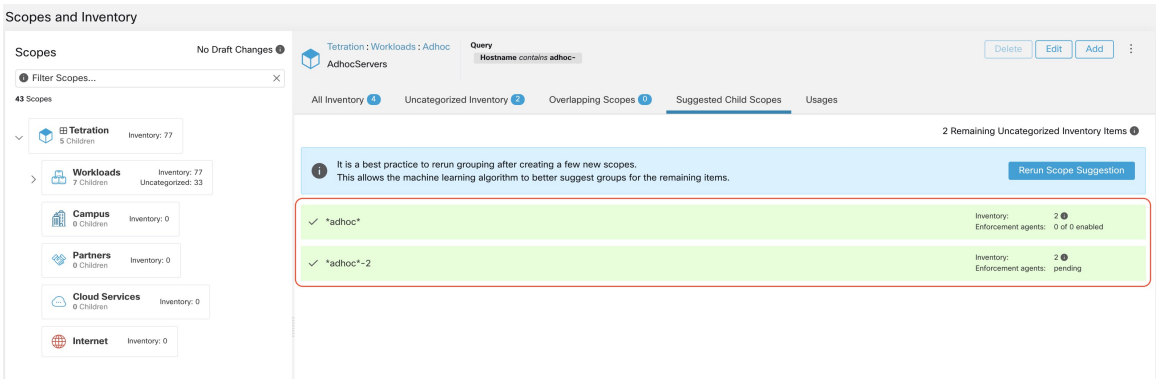
提案されたグループを範囲に変換すると、グループスロットが緑色になり、[未分類のインベントリ項目（Uncategorized Inventory Item）] の数が減少します。

図 *36 : 1* つの提案されたグループを範囲に変換した後の範囲提案出力の例



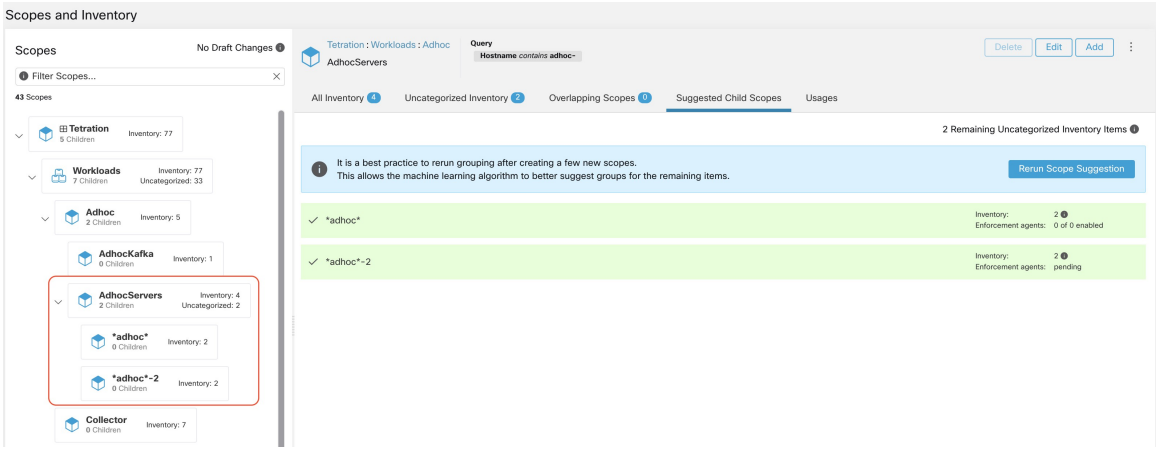
ユーザーは、グループの残りのリストから範囲作成のプロセスを繰り返すことができます。推奨されるワークフローは、1つ以上の範囲を作成してから、**範囲の提案**を再実行することです。[未分類のインベントリ項目（Uncategorized Inventory Item）]の数がゼロの場合は、（現在選択されている親範囲について）さらに範囲を限定するインベントリが残っていないことを示します。

図 *37 :* 複数の範囲作成後の範囲提案出力の例



範囲の作成プロセスが完了したら（未分類の数は 0）、ユーザーは、新しく作成された子範囲でこのプロセスを繰り返して、必要に応じてより深い範囲ツリーを生成できます。

図 *38* : 最初の範囲提案と作成後の範囲リストの例



（注） 範囲内の未分類の項目がうまく分類されない可能性もあります（例：コミュニティを形成しない）。その場合、アルゴリズムはグループ化を返さないことがあります（空の結果）。

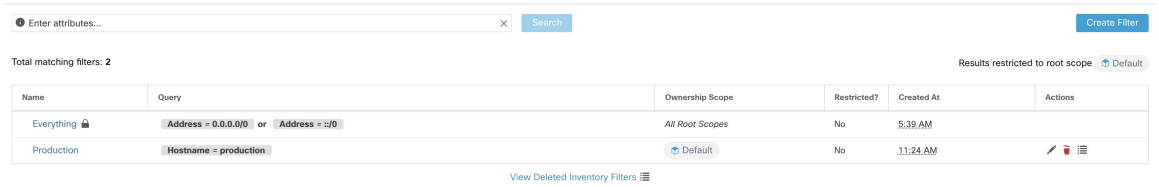
フィルタ

フィルタは、ポリシー、設定インテントなどを定義するときに使用できる、保存済みインベントリ検索です。各フィルタは、フィルタの所有範囲として定義されている範囲に関連付ける必要があります。

既存のフィルタを表示するには、左側のナビゲーションメニューから **[整理（Organize）]>[インベントリフィルタ（Inventory Filters）]** を選択します。また、該当する範囲の任意のワークスペースに含まれる任意の範囲に固有のインベントリフィルタを表示することもできます。

フィルタのリストは、現在選択されている範囲のルートに基づいて制限されます。

図 *39* : インベントリ フィルタ



選択した親範囲に関するインベントリメンバーシップの変更を確認するには、範囲/フィルタ変更の影響を確認 ウィンドウにアクセスします。

インベントリフィルタの作成

さまざまな目的でインベントリフィルタを作成できます。たとえば、インベントリフィルタを使用して次のことができます。

- 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作成または検出します。

  たとえば、APIインターフェイスを介してのみアクセスされるアプリケーションがある場合、範囲内にAPIサーバーのグループを作成して、そのトラフィックを許可し、そのアプリケーションの他のすべてのワークロードへのアクセスをブロックするポリシーを作成できます。

- 多くの範囲にまたがって存在する可能性のあるワークロードのポリシーを作成します。

  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ネットワーク上のすべてのワークロードに適用されるポリシーを作成する必要がある場合は、複数（またはすべて）の範囲にまたがるインベントリフィルタを作成できます。

さまざまな場所からインベントリフィルタを作成できます。

ステップ1 次のいずれかの場所に移動します。

- [整理（Organize）] > [インベントリフィルタ（Inventory Filters）] を選択します。
- インベントリフィルタを作成する範囲内の任意のワークスペースに移動し、[ポリシーの管理（Manage Policies）]、[フィルタ（Filters）]、[インベントリフィルタ（Inventory Filters）] の順にクリックします

（他の場所からインベントリフィルタを作成できる場合もあります）。

ステップ2 [フィルタの作成（Create Filter）] または [インベントリフィルタの追加（Add Inventory Filter）] をクリックします。

ステップ3 名前、説明、およびフィルタに含めるワークロードのみを指定したクエリを追加します。

ステップ4 [詳細オプションを表示（Show advanced options）] が表示されている場合は、このリンクをクリックします。

ステップ5 このフィルタの範囲を指定します。

選択した範囲によって、次のことが決定されます。

- このフィルタを変更できるユーザー:

  管理者がこのフィルタを変更するには、指定された範囲またはその先祖のいずれかへの書き込みアクセス権を持っている必要があります。

- フィルタに含まれるワークロード（この手順の他の設定に依存）。

ステップ6 設定オプションは次のとおりです。

目的	操作手順
このフィルタで指定された範囲のメンバーであるかどうかに関係なく、フィルタのクエリ条件を満たすワークロードを含めます。	[クエリを所有権の範囲に制限する（Restrict query to ownership scope）] の選択を解除します。
このフィルタで指定された範囲のメンバーであるワークロードのみを含めます。	[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。
自動ポリシー検出を許可して、このフィルタで定義された一連のワークロードに固有のポリシーを提案します。 これらのワークロードは、フィルタで指定された範囲のサブセットである必要があります。	[クエリを所有権の範囲に制限する（Restrict query to ownership scope）] と [範囲外のサービスを提供する（Provides a service external of its scope）] の両方を選択します。 後者を選択するには、前者を選択する必要があります。 このフィルタを使用するには、外部依存関係を設定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を参照してください。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 詳細を確認して [作成（Create）] をクリックします。

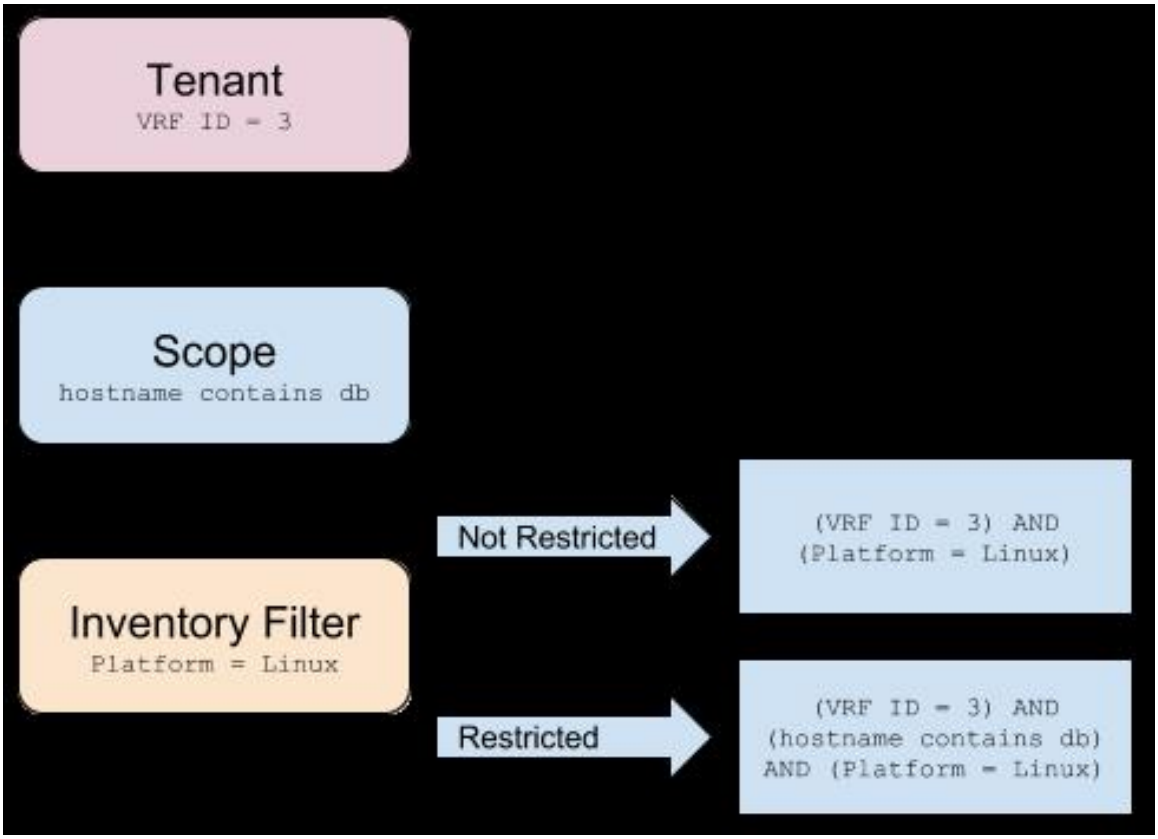
所有権の範囲に制限

範囲がフィルタによって一致するインベントリに影響を与えるかどうかは、[所有権の範囲に制限（Restrict to Ownership Scope?）] チェックボックスによって決まります。

たとえば、次のようなクエリ構造があるとします。

1. クエリで指定されたテナント：`VRF ID = 3`
2. クエリで指定されたこのテナント内の範囲：`hostname contains db`
3. クエリで指定されたこの範囲に割り当てられているインベントリフィルタ：`Platform = Linux`

図 *40 :* テナント、範囲、インベントリフィルタ構造



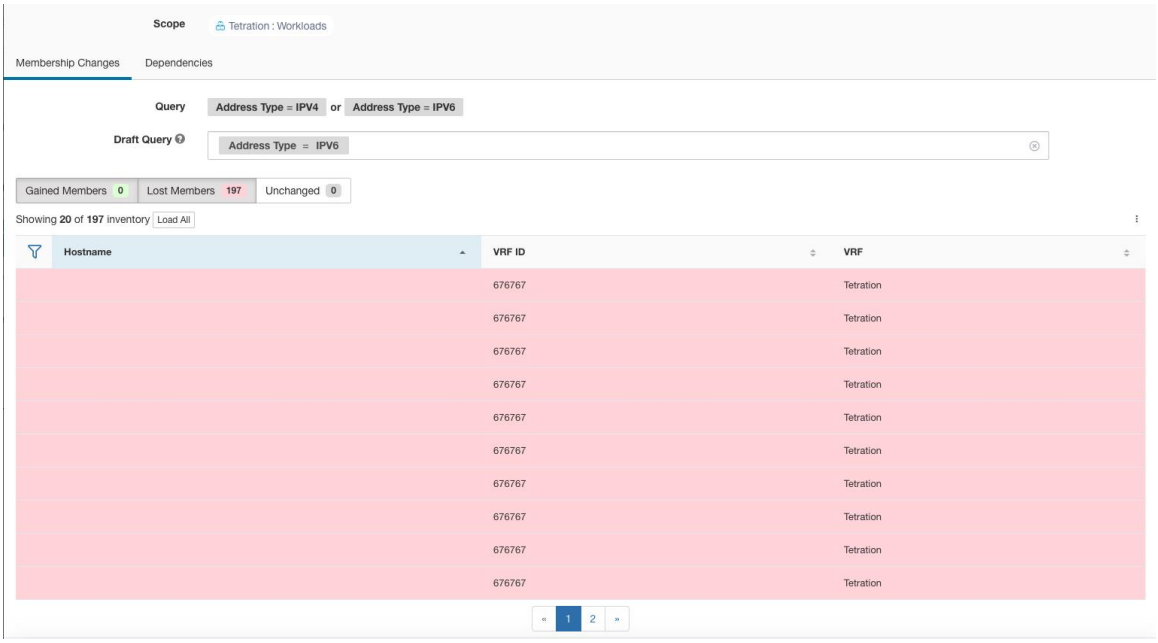
- [所有権の範囲に制限（Restrict to Ownership Scope）] チェックボックスがオフになっている場合、このフィルタは、インベントリフィルタにも一致するテナント内のすべてのホストに一致します。有効なクエリは `(VRF ID = 3) AND (Platform = Linux)` になります。
- [所有権の範囲に制限（Restrict to Ownership Scope）] チェックボックスがオンになっている場合、このフィルタは、インベントリフィルタにも一致するテナントと範囲内のホストのみに一致します。有効なクエリは `(VRF ID = 3) AND (hostname contains db) AND (Platform = Linux)` になります。

範囲/フィルタ変更の影響を確認

範囲クエリを更新すると、コミットされた後の範囲のインベントリメンバーシップに影響を与える可能性があります。同様に、直接保存されるフィルタクエリの変更も、範囲のインベントリメンバーシップに影響を与える可能性があります。[範囲（Scope）] または [フィルタ編集（Filter Edit)] モーダルのいずれかで [クエリ変更の影響の確認（Review query change impact）] リンクをたどることで、新しいクエリと古いクエリの間のメンバーシップの変更を確認できます。さらに、範囲またはフィルタの依存関係を把握すると、影響の分析に役立つだけでなく、

範囲の削除を妨げる必要なすべてのオブジェクトを削除する際にも役立ちます。詳細については、[依存関係（Dependencies）] タブにもアクセスして、範囲の依存関係ツリーを検討してください。

図 *41* : メンバーシップテーブルのダウンロード



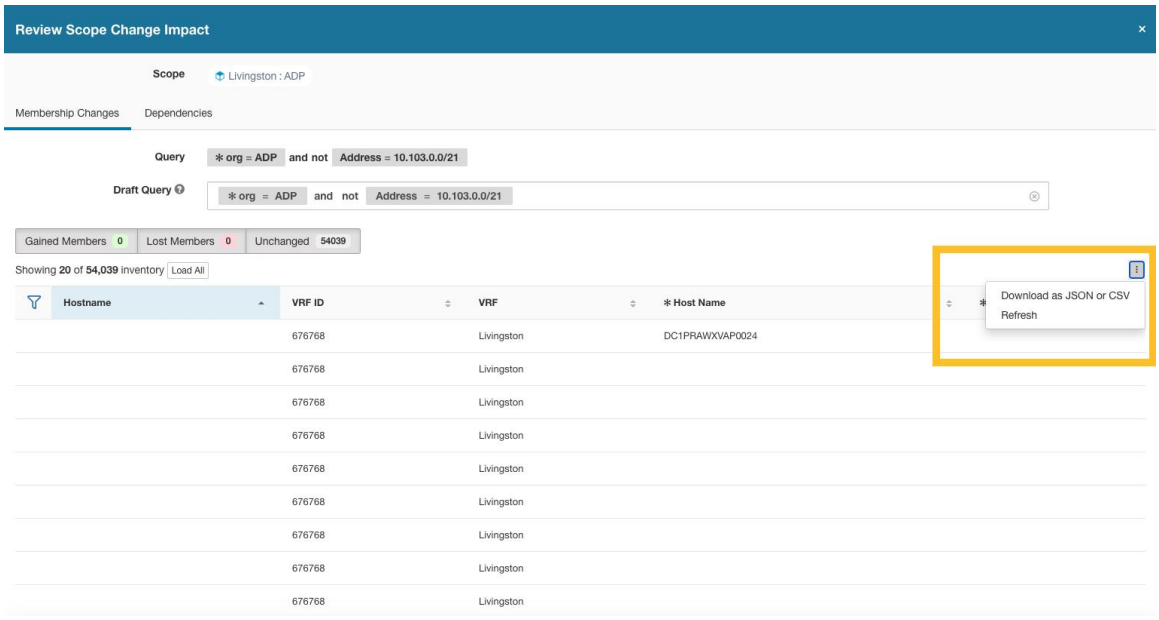
範囲クエリ変更影響モーダル

[メンバーシップの変更（Membership Changes）] タブと [依存関係（Dependencies）] タブの両方にアクセスするには、[範囲編集（Scope Edit）] ウィンドウで [クエリ変更の影響の確認（Review query change impact）] リンクをクリックします。

メンバーシップの変更

メンバーシップビューのインベントリテーブルには、デフォルトですべての列が表示されます。表示する行は選択できます。さらに、インベントリが[ゲイン（Gained）]、[喪失（Lost）]、[変更なし（Unchanged）] のいずれかであるかを識別する追加の Diff 列を含む、選択したメンバーシップ列と行の csv または json をダウンロードできます。ダウンロードに必要なすべてのテーブルの選択がテーブルビューに表示されていることを確認してください。

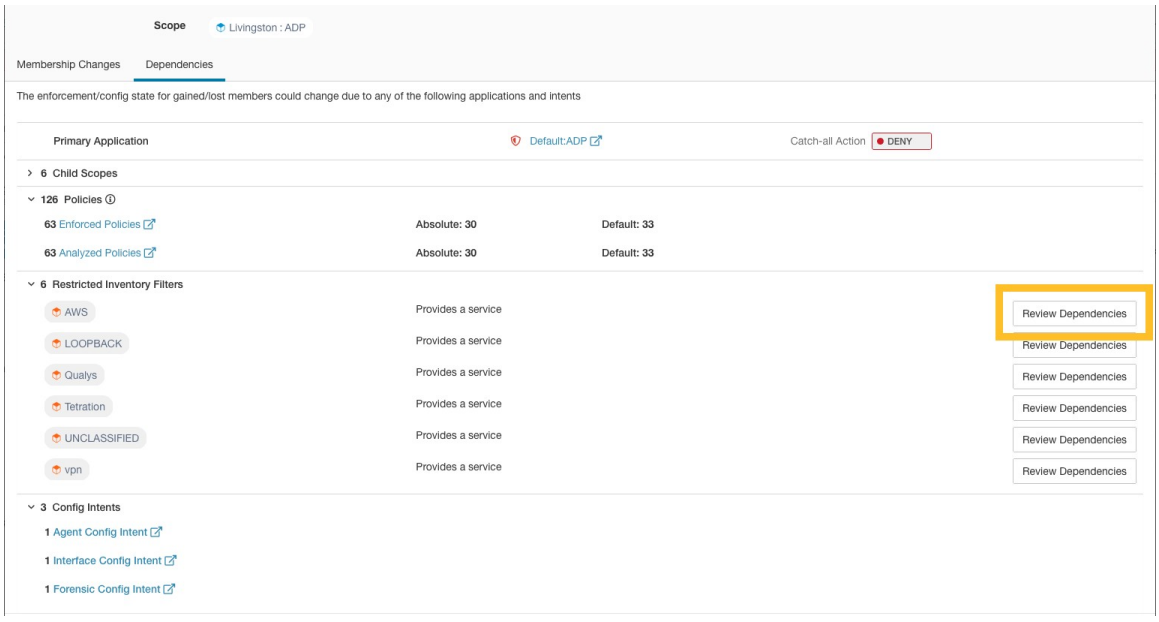
図 *42* : 範囲メンバーシップの変更



依存関係

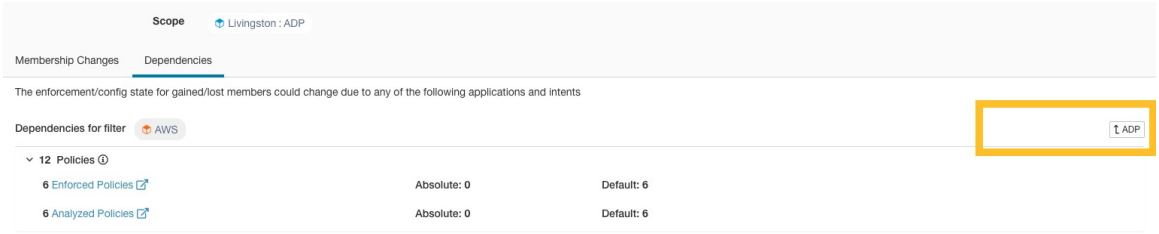
[依存関係の確認（Review Dependencies）] をさらに選択することで、ネストされた依存関係までトラバースできます。

図 *43* : 依存関係の確認



該当する親リンクを選択することで、依存関係ツリーをトラバースできます。

図 *44 :* 親リンク



存在する可能性のある範囲の依存関係は次のとおりです。

表 *3 :* 存在する可能性のある範囲の依存関係は次のとおりです

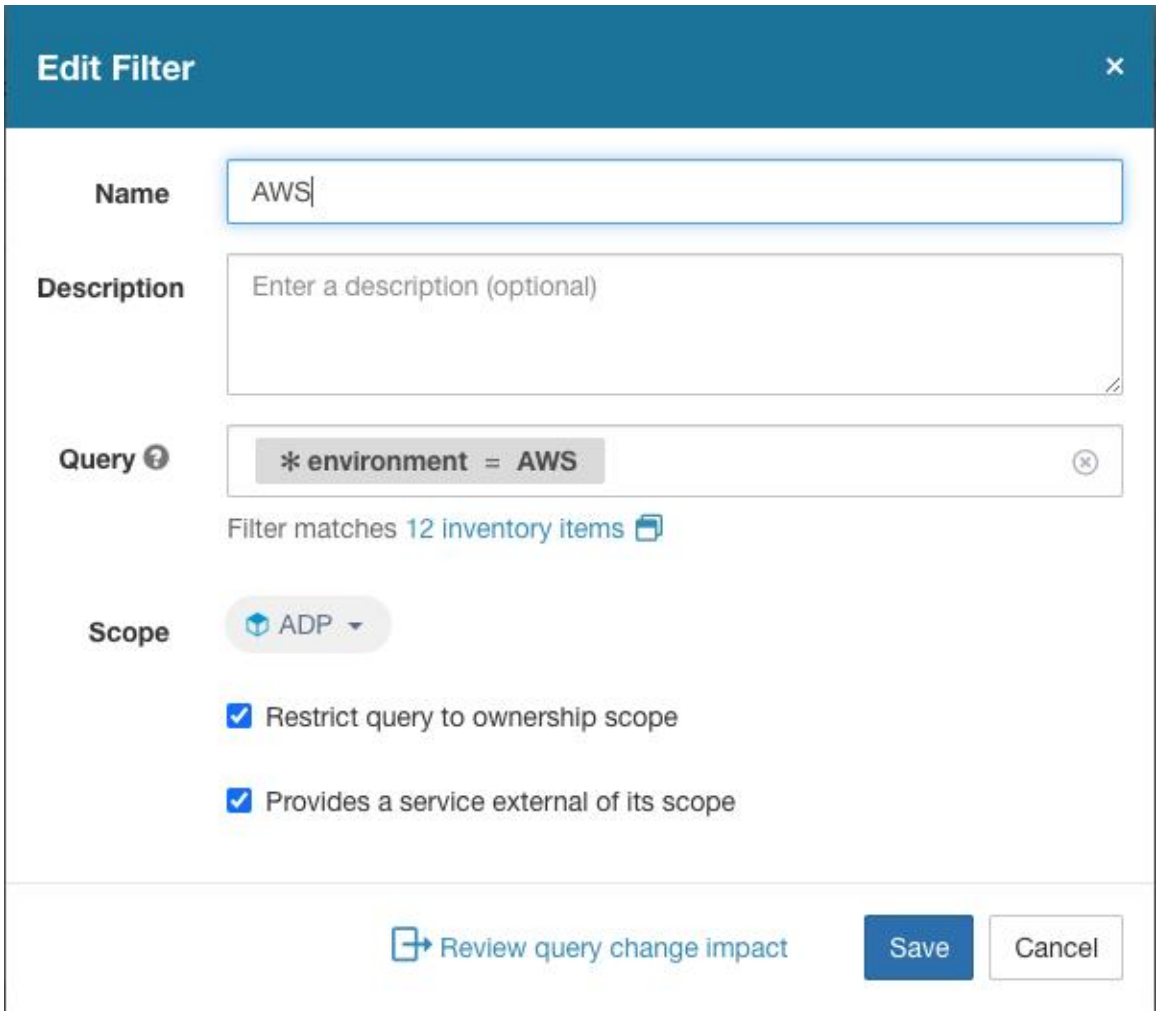
タイプ	説明
アプリケーション	プライマリおよびセカンダリアプリケーション名と、セグメンテーションの下にある特定のワークスペースへのリンクがあります。
子範囲	子範囲の名前と子範囲の詳細ビューへのリンクがあります。下位レベルの依存関係にドリルダウンできます。
ポリシー	分析および適用されたポリシーの数と、選択した範囲でフィルタ処理されたそれぞれのグローバルポリシービューへのリンクがあります。
制限付きインベントリフィルタ	フィルタの名前と子フィルタの詳細ビューへのリンクがあります。下位レベルの依存関係にドリルダウンできます。
構成インテント	構成インテントの名前、およびエージェント、インターフェイス、フォレンジックの構成インテントビューへのリンクがあります

フィルタクエリ変更影響モーダル

[メンバーシップの変更（Membership Changes）] タブと [依存関係（Dependencies）] タブの両方にアクセスするには、[インベントリフィルタの編集（Inventory Filter Edit）] ウィンドウで [クエリ変更の影響の確認（Review query change impact）] リンクをクリックします。

メンバーシップの変更

図 *45* : インベントリフィルタのメンバーシップの変更



依存関係

存在する可能性のあるフィルタの依存関係は次のとおりです。

タイプ	説明
ポリシー	分析および適用されたポリシーの数と、選択した範囲でフィルタ処理されたそれぞれのグローバルポリシービューへのリンク
[設定インテント（Config Intents）]	エージェント、インターフェイス、フォレンジック設定インテントビューへの名前およびリンクがあります

インベントリプロファイル

（注） インベントリのプロファイルページは、さまざまな場所からリンクされています。インベントリプロファイルを表示する方法の1つは、インベントリの検索を実行し、IPアドレスをクリックしてそのプロファイルに移動することです。[範囲とインベントリ（Scopes and Inventory）] ページで作業している場合は、[ワークロード（Workloads）] タブの IP アドレスではなく、[IP アドレス（IP addresses）] タブの IP アドレスをクリックします（[ワークロード（Workloads）] タブで IP アドレスをクリックすると、インベントリプロファイルではなく、ワークロードプロファイルが表示されます）。

インベントリについては、次の情報が表示されます。

フィールド	説明
[範囲（Scopes）]	インベントリが属する範囲のリスト。
[インベントリタイプ（Inventory Type）]	• [フロー学習（Flow Learnt）] インベントリは、観測されたフローと収集ルールに基づいて登録されました。 • [ラベル付き（Labeled）] のインベントリは、インベントリ アップロードユーティリティを使用して手動でアップロードされました。 • [エージェント（Agent）] インベントリは、ホストにインストールされているソフトウェアエージェントによって報告されました。 • [タグ（Tagged）] インベントリは、コネクタまたは外部オーケストレータによって報告されました。
[ユーザーラベル（User Labels）]	このインベントリにユーザーがアップロードした属性のリスト。詳細については、「ワークロードラベル」を参照してください。

追加情報は、次の両方に該当する場合にのみ表示されます。

1. インベントリがクラウドコネクタを介して取り込まれている。
2. インベントリが存在する仮想ネットワークに対してセグメンテーションが有効になっている。

フィールド	説明
[適用の状態（Enforcement Health）]	ホスト ソフトウェア エージェントのステータス情報。詳細については、「[エージェントの正常性（Agent Health）] タブ」を参照してください。
[具体的なポリシー（Concrete Polices）]	このタブには、ホストに適用される Secure Workload の具体的な適用ポリシーが表示されます。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。
[セキュリティグループ（Security Groups）]	このインベントリに適用されるセキュリティグループとそのポリシーのリスト。

インベントリプロファイル情報

フィールド	説明
[試験的グループ（Experimental Groups）]	ポリシーのライブ分析に使用されるクラスタまたはユーザー定義のインベントリフィルタのリスト。
[適用グループ（Enforcement Groups）]	ポリシーの適用に使用されるクラスタまたはユーザー定義のインベントリフィルタのリスト。分析対象のポリシーやシステムで適用されているポリシーのバージョンによっては、適用グループが試験的グループとは異なる場合があります。

（注） 次の場合、IP アドレスのインベントリプロファイルの詳細が表示されない場合があります。

- インベントリが収集ルールから除外されている場合。
- 単方向フローではインベントリが 2 分間だけ使用できるようになり、その後に削除されます。
- 双方向フローでは、インベントリが 30 日間使用できますが、この 30 日間にこれ以上フローが観察されない場合、インベントリの詳細は削除されます。

ワークロード プロファイル

ワークロードプロファイルには、Secure Workload ソフトウェアエージェントがインストールされているホストに関する詳細情報が表示されます。ここでは、ワークロードプロファイルとそれに含まれる情報を表示する方法について説明します。

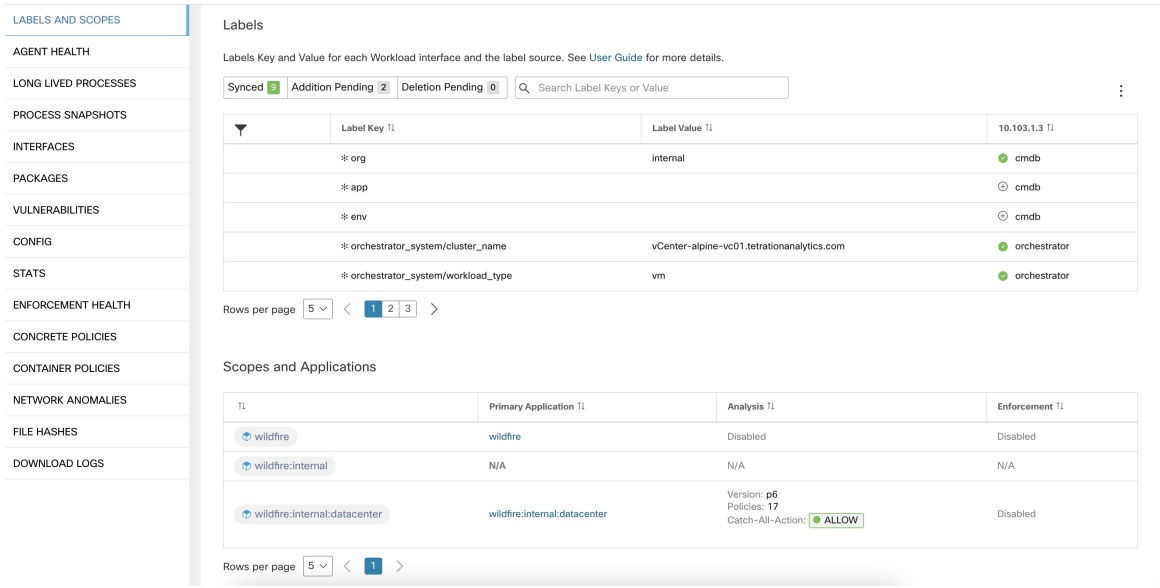
（注） ワークロードのプロファイルページは、さまざまな場所からリンクされています。ワークロードプロファイルを表示する方法の 1 つは、検索で説明したように、ホストの検索を実行することです。

インベントリ検索の結果から、ホストの IP アドレスをクリックして、そのプロファイルに移動します。ホストにインストールされているエージェントのタイプに基づいて、次のタブがページに表示されます。このインベントリが属するホストに Secure Workload ソフトウェアエージェントがインストールされていない場合、インベントリ プロファイル ページが表示される可能性があることに注意してください。

ラベルと範囲タブ

このタブには、適用グループと試験的グループ、ホストが属する範囲が含まれています。試験的グループは、ポリシーのライブ分析に使用するインベントリフィルタであり、適用グループはポリシーの適用に使用するフィルタです。これらのグループは、分析対象のポリシーやシステムで適用されているポリシーのバージョンに応じて異なる場合があります。

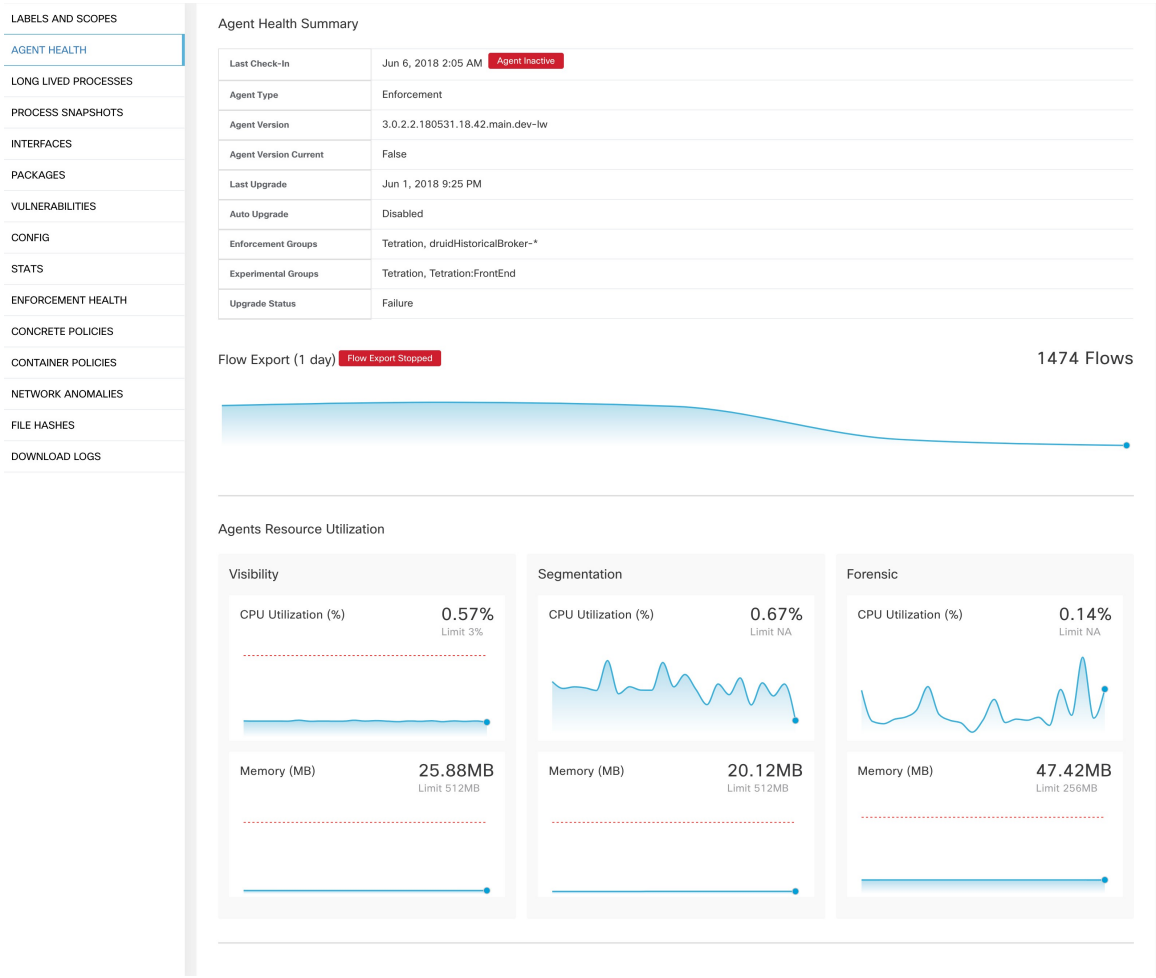
図 *46 :* ワークロードのラベルと範囲



[エージェントの正常性（Agent Health）] タブ

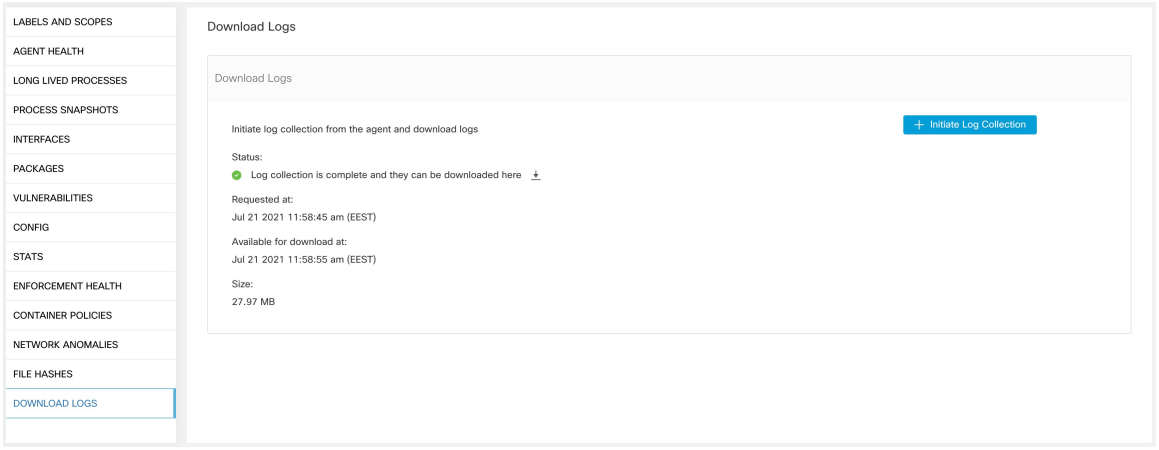
タイプ、OS プラットフォーム、エージェントのバージョン、最終チェックイン時刻などのホスト ソフトウェア エージェントのステータス情報も、[エージェントの正常性（Agent Health）] タブに表示されます。詳細については、「ソフトウェアエージェント設定」を参照してください。このタブには、1 日あたりに発生したトラフィックのバイト数とパケット数に関する詳細な時系列データも表示されます。

図 *47*：ワークロードエージェントの正常性の詳細



ルート範囲の所有者特権を持つユーザーの場合、概要ページには、そのルート範囲内の優れた可視性および適用エージェント（バージョン 3.3 以降）のためにエージェントログを収集およびダウンロードするセクションも含まれます。また、この機能は、プラットフォーム AIX および SUSE Linux Enterprise Server（IBM Z アーキテクチャ上の s390x-Linux）で実行されているエージェントでは使用できないことに注意してください。[ログ収集の開始（Initiate Log Collection）] ボタンを使用してエージェントからログを収集すると、数分でログをダウンロードできるようになります。ダウンロードに失敗した場合は、ログの収集を再試行してから、もう一度ダウンロードを試行してください。

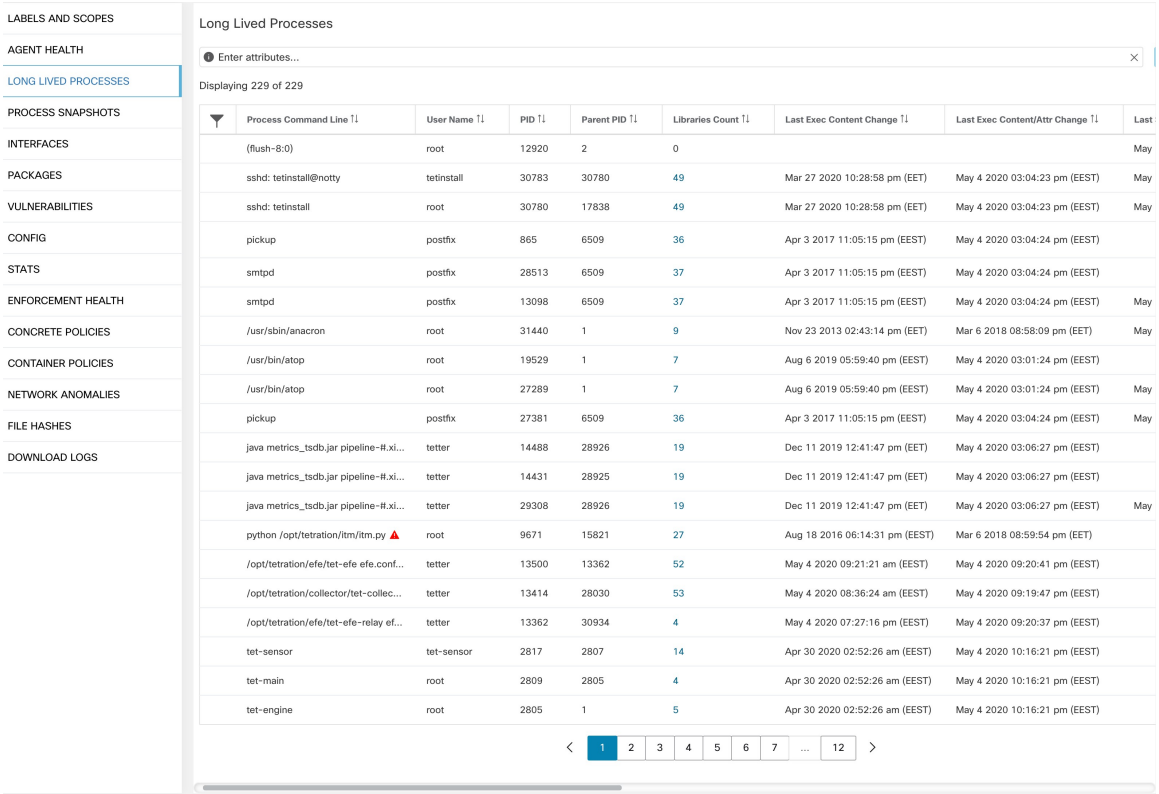
図 48 : Agent Logs



[プロセスリスト（Process List）] タブ

このタブには、ホストで実行されているプロセスのリストが表示されます。フィルタを使用して、以下の表ヘッダーに示されているプロセスの属性に基づいて、プロセスのリストを絞り込むこともできます。

図 49 : ワークロードプロセスリスト



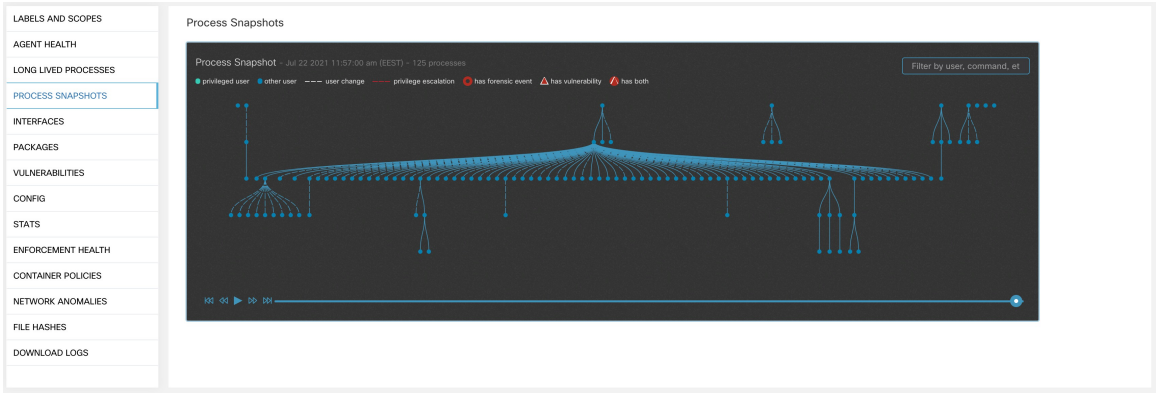
属性の説明：

属性	説明
最後の実行コンテンツの変更（Last Exec Content Change）	Linux の mtime に似ています。ファイルの内容のみが変更されたときのタイムスタンプです。
最後の実行コンテンツの変更（Last Exec Content Change）	Linux の ctime に似ています。ファイルの内容または属性が変更されたときのタイムスタンプです。
Last Seen	プロセスが最後に観察された時刻。プロセスが停止したときに使用できます。
CPU 使用率	過去 1 時間のプロセスによる CPU 使用率の傾向。
メモリ 使用法	過去 1 時間のプロセスによるメモリ使用量の傾向。
プロセスバイナリハッシュ（Process Binary Hash）	プロセスバイナリの 16 進文字列の SHA256 ハッシュ。略してプロセスハッシュとも呼ばれます。カーネルプロセスでは使用できません。
異常スコア（Anomaly Score）	プロセスハッシュ（異常）スコア。詳細については、「プロセスハッシュの異常検出」を参照してください。
判定	プロセスハッシュの判定（悪意があるまたは無害のいずれか）。判定は、プロセスハッシュがユーザー定義のハッシュリストまたは既知の脅威インテリジェンスハッシュデータベースに属しているかどうかに基づいて決定されます。詳細については、「プロセスハッシュの異常検出」を参照してください。
判定ソース（Verdict Source）	判定のソース。判定ソースは、ユーザー定義、Secure Workload クラウド、または NIST のいずれかです。この属性は、以前のリリースではハッシュ DB ソースと呼ばれていました。詳細については、「プロセスハッシュの異常検出」を参照してください。

[プロセススナップショット（Process Snapshot）] タブ

このタブには、ワークロードで観察された検索可能なプロセスツリーが表示されます。

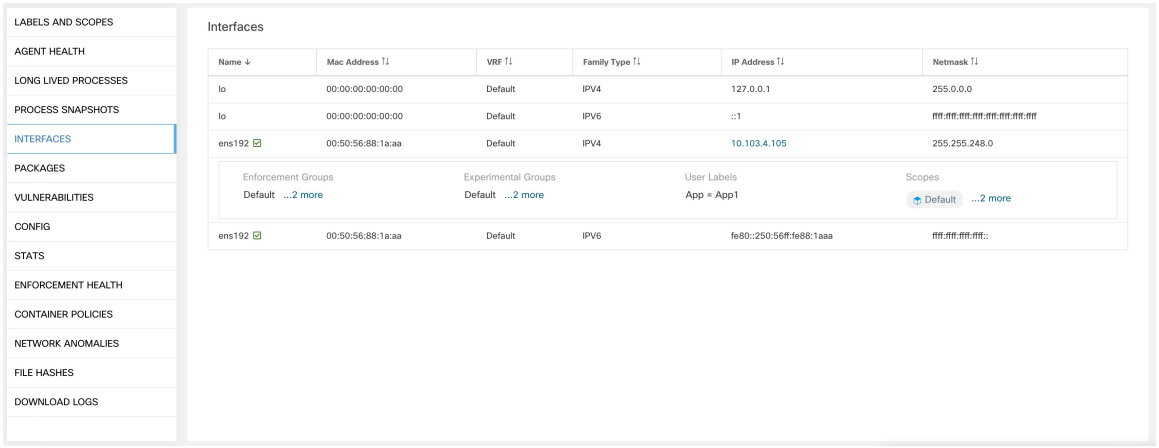
図 *50* : ワークロード プロセス スナップショット



[Interfaces] タブ

このタブには、ホストにインストールされているネットワーク インターフェイスに関する詳細が表示されます。すべてのタイプのソフトウェアエージェントで使用できます。

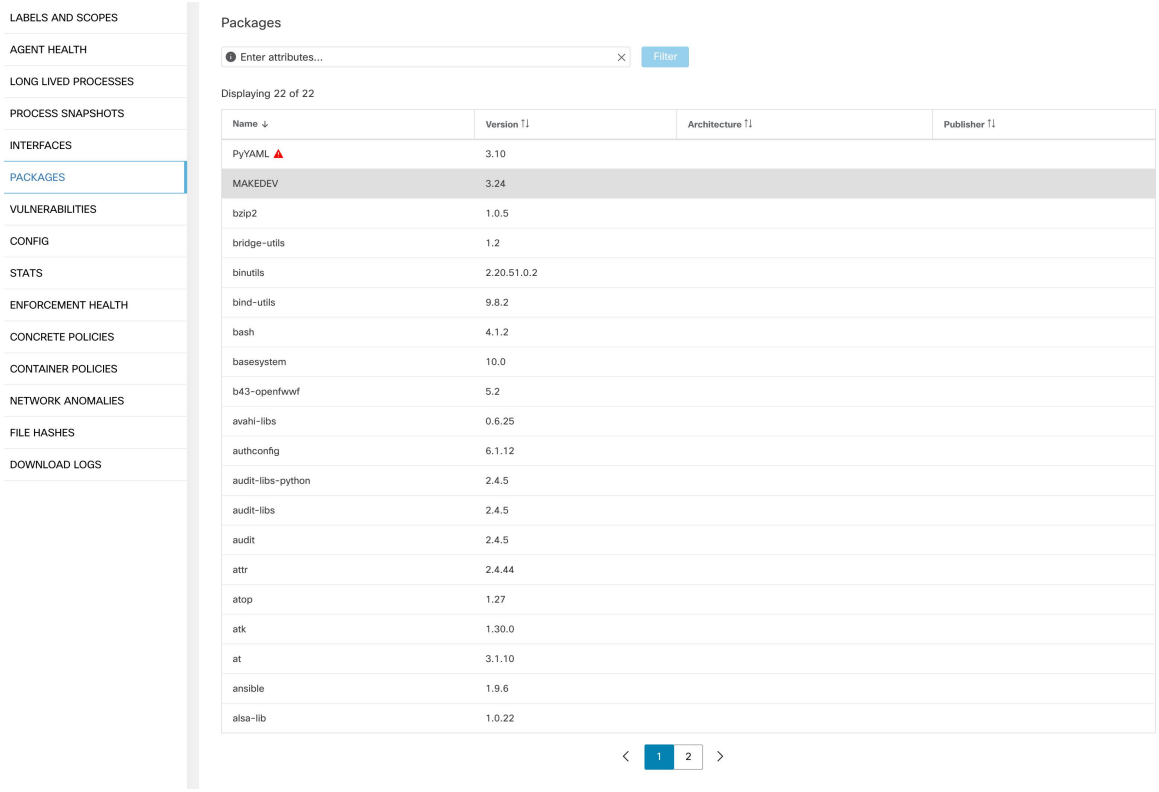
図 *51* : ワークロード インターフェイスのリスト



[ソフトウェアパッケージ（Software Packages）] タブ

このタブには、ホストにインストールされているパッケージのリストが表示されます。ユーザーは、テーブルヘッダーのパッケージ属性に基づいて、ソフトウェアパッケージを選択して表示できます。

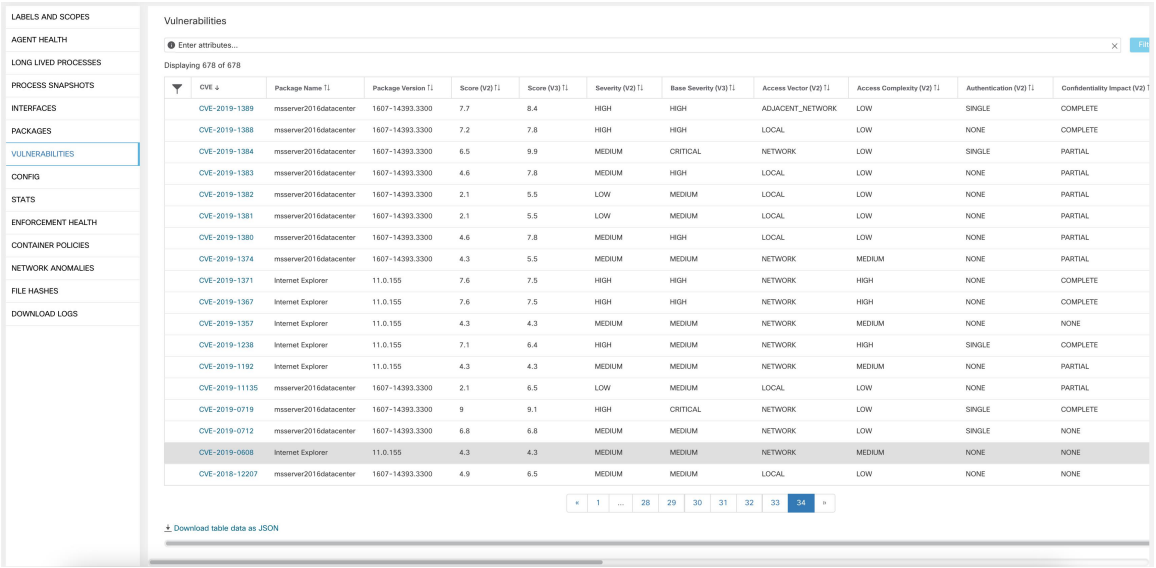
図 *52 :* ソフトウェアパッケージ一覧



[脆弱性（Vulnerabilities）] タブ

このタブには、Common Vulnerabilities and Exposures（CVE）システムに基づいてワークロードで観察された検索可能な脆弱性が表示されます。「脆弱性データの可視化」を参照してください。

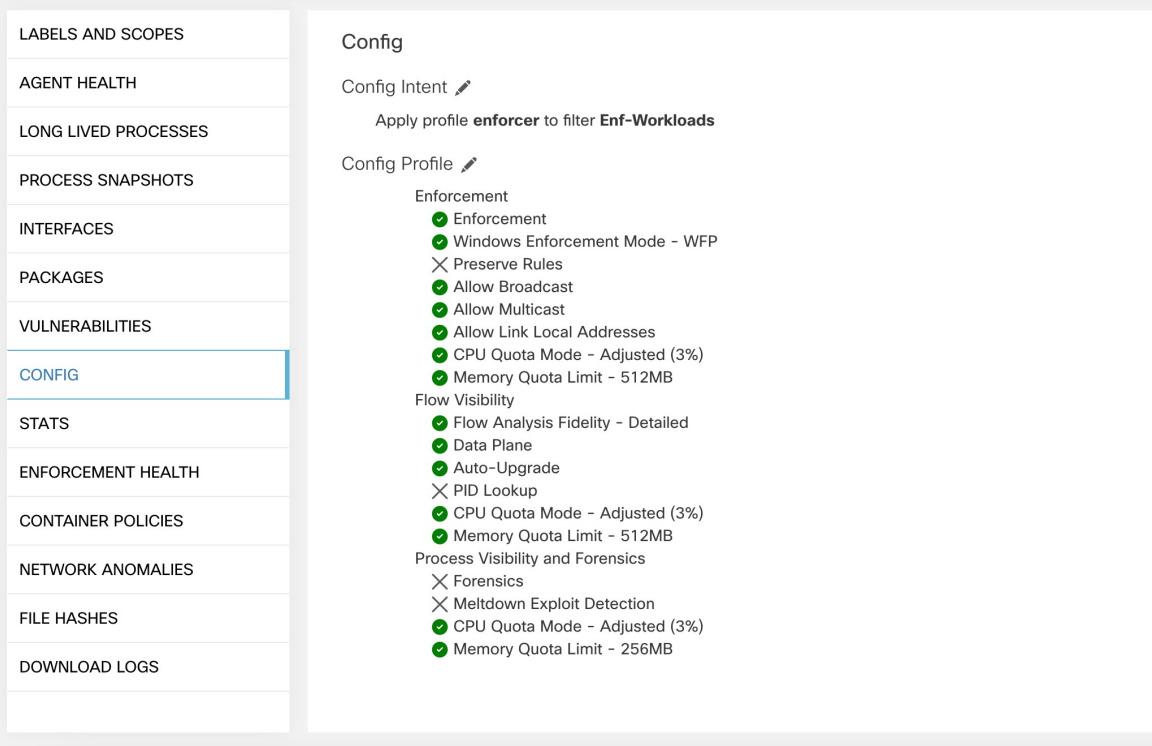
図 *53 : [*脆弱性（*Vulnerabilities*）*]* タブ



[エージェントの設定（Agent Configuration）] タブ

このタブには、ソフトウェアエージェントの設定が表示されます。優れた可視性エージェントおよび適用エージェントでのみ使用できます。これらの設定は、[エージェントの設定（Agent Configuration）]ページのエージェント設定インテントを使用して変更できます。「ソフトウェアエージェントの設定」を参照してください。

図 *54* : 適用されるワークロード設定



[エージェント統計情報（Agent Statistics）] タブ

このタブには、ホストにインストールされている Secure Workload エージェントに関する統計情報が表示されます。優れた可視性エージェントおよび適用エージェントでのみ使用できます。

図 *55* : エージェント統計情報

[具体的なポリシー（Concrete Policies）] タブ

このタブには、ホストに適用される Secure Workload の具体的な適用ポリシーが表示されます。この表の各行は、ホストに実装されているファイアウォールルールに対応しています。各ポリシー行をさらに展開して、この具体的なポリシーが派生した元の論理インテントを表示することができます。ルールごとにパケット数とバイト数の時系列表示も可能です。このタブではフィルタを使用して、以下の表ヘッダーに示されているポリシーの属性に基づいて、適用されるポリシーのリストを絞り込むこともできます。このタブは、適用エージェントでのみ使用できます。

図 *56* : 具体的なポリシーのリスト

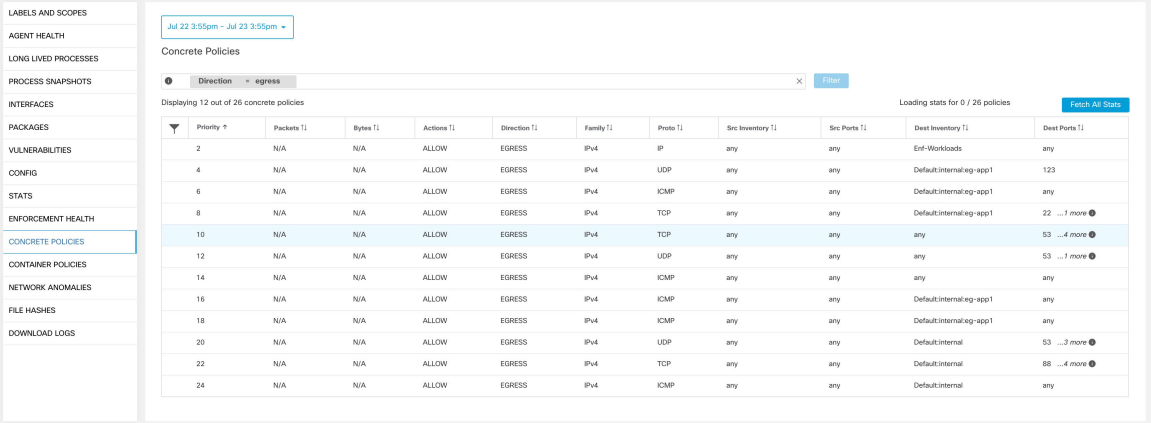
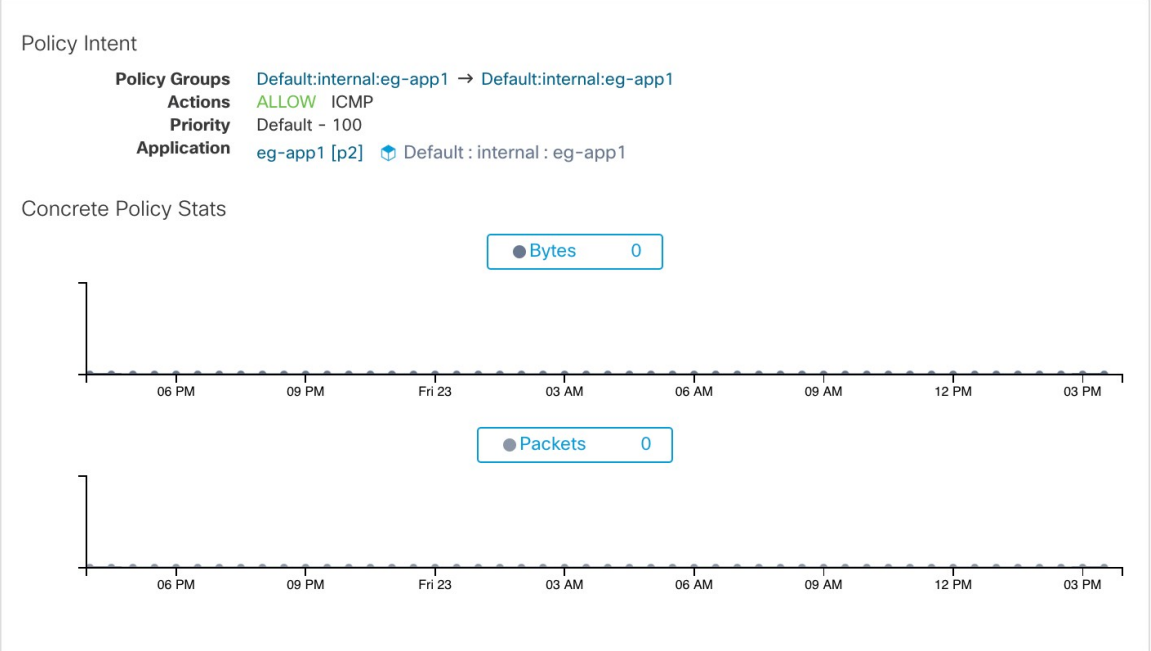


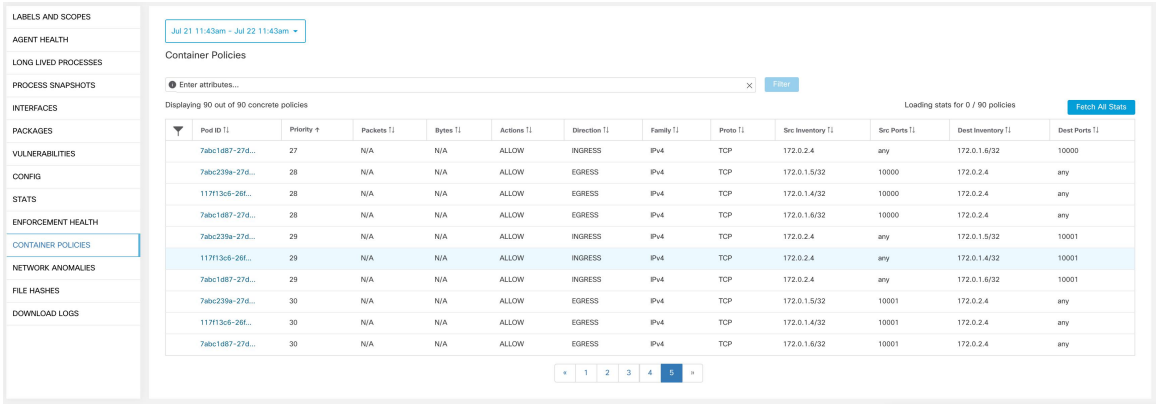
図 *57* : 具体的なポリシーの行



[コンテナポリシー（Container Policies）] タブ

このタブには、コンテナに適用される Secure Workload の具体的な適応ポリシーが表示されます。この表の各行は、コンテナポッドに実装されているファイアウォールルールに対応しています。

図 *58 :* コンテナの具体的なポリシー一覧



[ネットワーク異常（Network Anomalies）] タブ

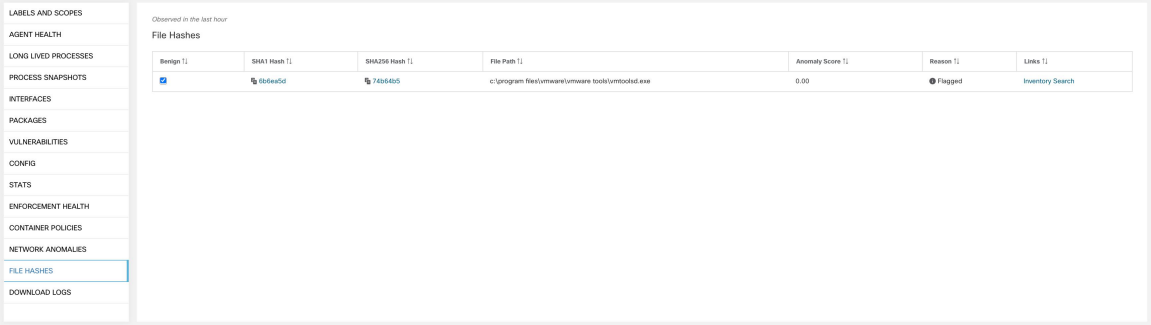
このタブは、このワークロードに出入りする大規模なデータの移動を伴うイベントを識別するのに役立ちます。詳細については、「PCR ベースのネットワーク異常検出」を参照してください。

図 *59 :* ワークロードネットワークの異常

[ファイルハッシュ（File Hashes）] タブ

このタブは、システム全体のプロセスバイナリハッシュの一貫性を評価することにより、プロセスハッシュの異常を検出します。詳細については、「プロセスハッシュの異常検出」を参照してください。

図 *60 :* ワークロードファイルのハッシュ



Software Packages

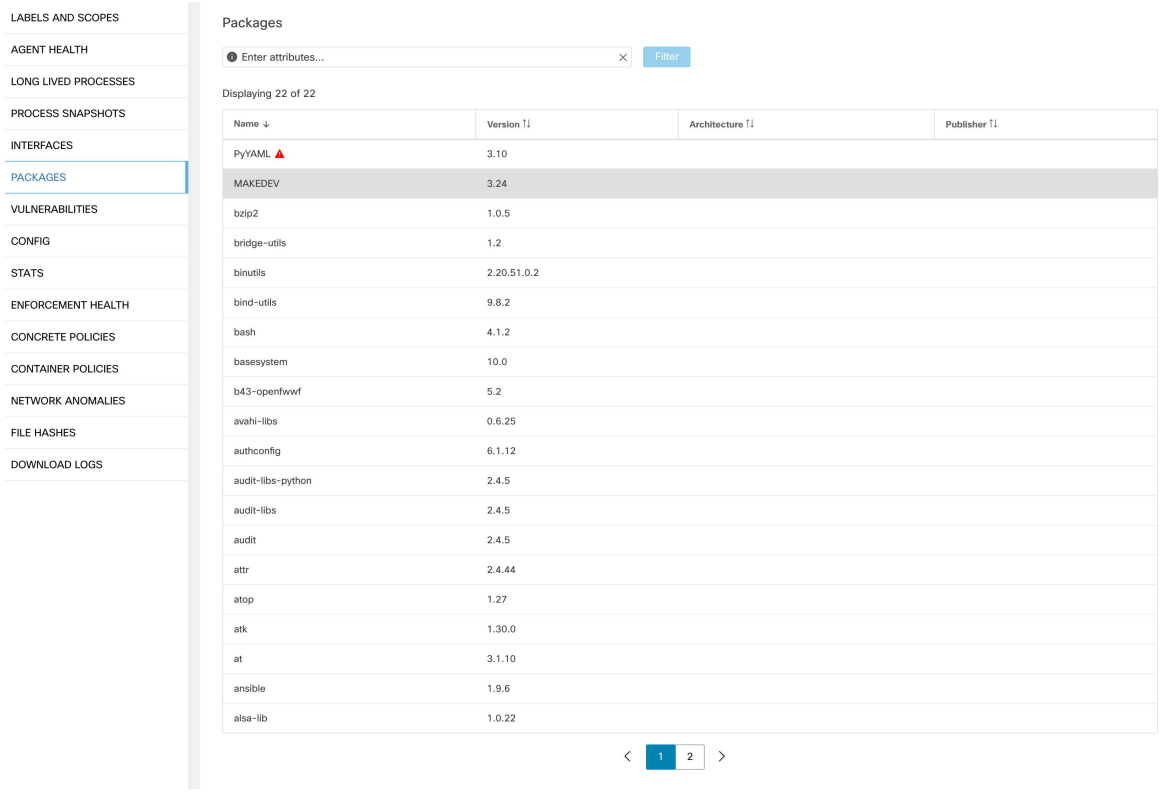
ソフトウェアパッケージ機能セットを使用すると、ホストにインストールされているパッケージと、それらに影響を与える脆弱性を表示できます。具体的には、次のことが可能になります。

- 次のパッケージマネージャに登録されているパッケージを表示します。
  - Linux：Redhat パッケージマネージャ（RPM）および Debian パッケージマネージャ（dpkg）
  - Windows：Windows レジストリサービス
- ホストにインストールされているパッケージに影響を与える Common Vulnerabilities and Exposures（CVE）を表示します。
- パッケージ名とバージョンを使用してインベントリフィルタを定義します。

[Packages] タブ

ホストにインストールされているパッケージを表示するには、ワークロード プロファイルの ワークロード プロファイル ページの [パッケージ（packages）] タブに移動します。

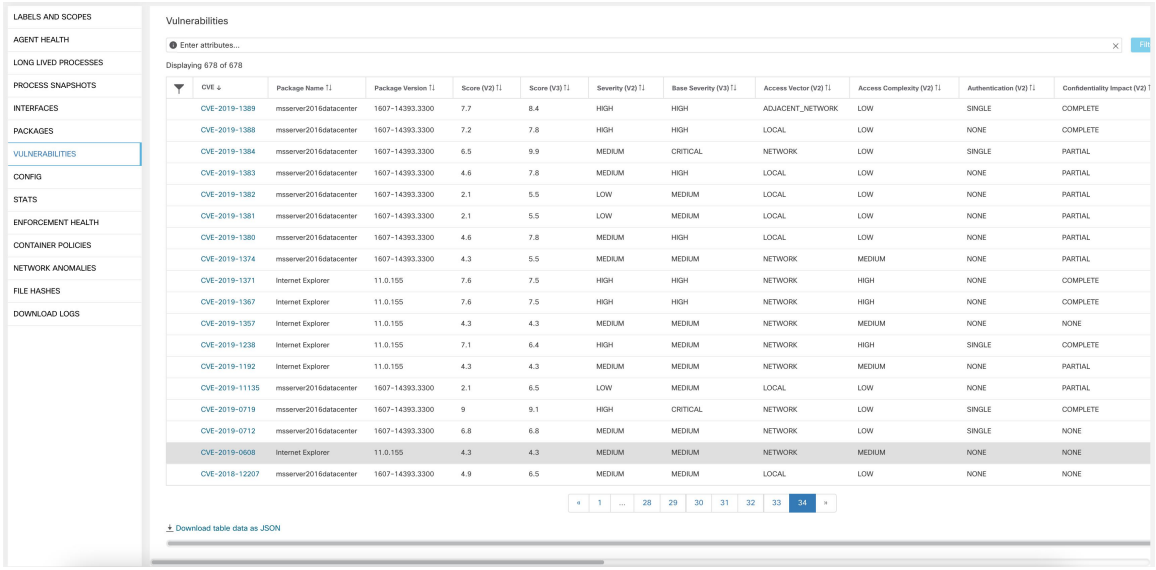
図 *61* : ワークロード プロファイル パッケージ



Common Vulnerabilities and Exposures（CVE）

[パッケージ（Packages）] タブでは、パッケージが表示されるだけでなく、パッケージに影響を与える一般的な脆弱性とその重大度も表示されます。各脆弱性には、特定の脆弱性に関する詳細情報を提供する Nation Vulnerability Database（NVD）へのリンクが含まれています。CVE ID の表示に加えて、脆弱性の重大度を示す影響スコア（10 段階）も表示されます。

図 *62 :* ワークロード プロファイル パッケージ *CVE*



Windows パッケージと CVE

次のセクションでは、Cisco Secure Workload へのパッケージ情報の報告に関する Windows エージェントの動作について説明します。

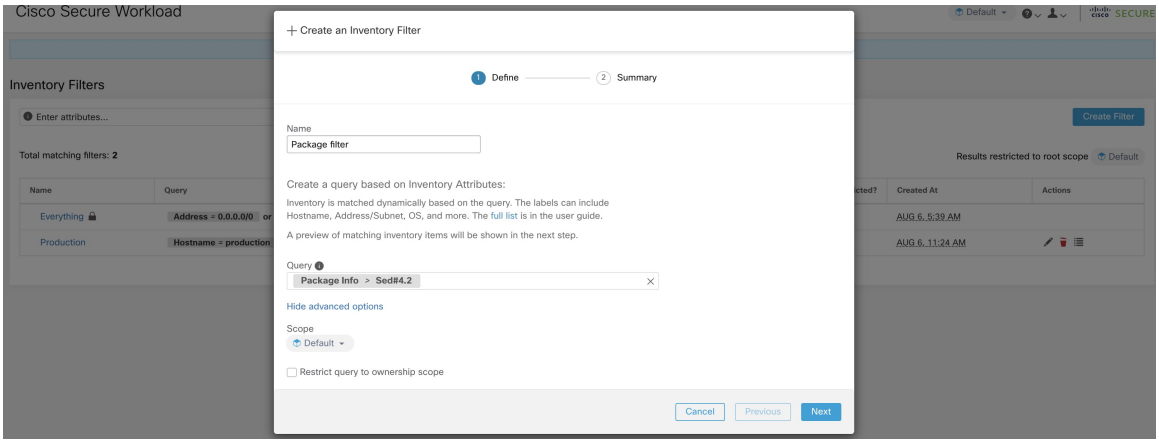
- Windows アプリケーション、PowerShell、IE はパッケージとして報告されます。.net フレームワークもパッケージとして報告されます。
- notepad.exe、cmd.exe、mstsc.exe など、その他の Windows アプリケーションは報告されません。
- Windows サーバーで設定されたロールと機能はパッケージとして報告されますが、バージョンが正しくない可能性があります。例：DNS サーバーが設定されている場合、報告されるバージョンは 0 または 8 のいずれかになります。
- Windows エージェントは、MSI インストーラまたは exe インストーラを使用してインストールされたサードパーティ製品を報告します。
  - MSI インストーラの場合、MSI API を使用してパッケージ情報（バージョン、発行元、パッケージ名など）を取得します。
  - exe インストーラを使用してパッケージをインストールする場合、パッケージ情報はレジストリから取得されます。
  - バージョン、発行元などの [パッケージインストーラ（Package installer）] フィールドはオプションです。バージョンが不明な場合、パッケージは報告されません。
  - 製品が zip ファイルから抽出されているか、アプリとしてインストールされている場合、パッケージリストで報告されません。

インベントリフィルタ

パッケージ名とバージョン（オプション）でインベントリフィルタを定義することで、パッケージ関連の情報を検索できます。

このフィルタのシンタックスは、PackageName#PackageVersion です。

図 *63* :インベントリパッケージ



次の操作がサポートされます。

- 等号：PackageName と PackageVersion（指定した場合）が一致するパッケージを搭載したホストを返します。
- 等号否定：PackageName は一致するが PackageVersion（指定した場合）は一致しないパッケージを搭載したホストを返します。
- 超過：PackageName が一致し、バージョンが PackageVersion より大きいパッケージを搭載したホストを返します。
- 以上：PackageName が一致し、バージョンが PackageVersion 以上のパッケージを搭載したホストを返します。
- 未満：PackageName が一致し、バージョンが PackageVersion 未満のパッケージを搭載したホストを返します。
- 以下：PackageName が一致し、バージョンが PackageVersion 以下のパッケージを搭載したホストを返します。

脆弱性データの可視化

脆弱性データの可視化機能により、ホスト上のパッケージとプロセスに影響を与える脆弱性を検出して表示できます。インベントリフィルタは、次を使用して定義できます。

```
- CVE IDs.- CVSS v2 and v3 scores.- CVSS v2 access vector and access complexity.- CVSS v3 attack vector, attack complexity, and privilege required.
```

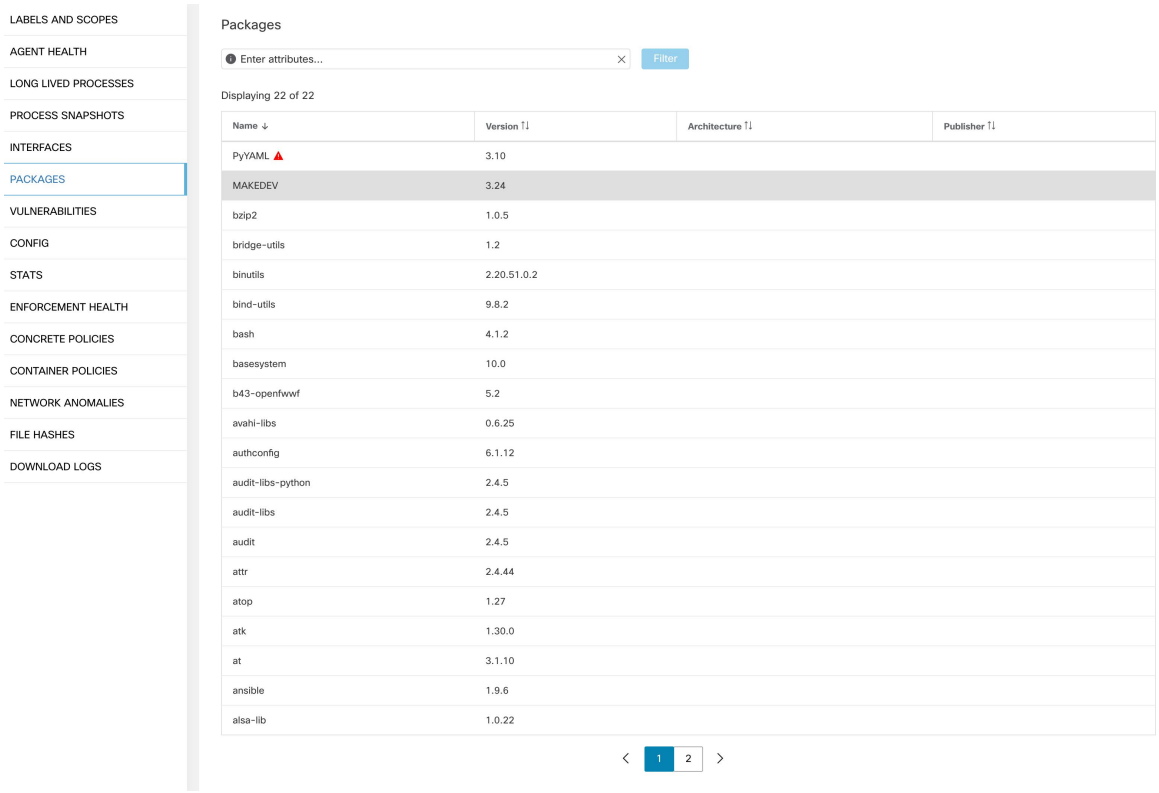
ワークロード プロファイル ページ

システム上のパッケージとプロセスに影響を与える脆弱性関連の情報は、ワークロード プロファイル ページに表示されます。

[Packages] タブ

[パッケージ（Packages）] タブには、ホストにインストールされているパッケージと、それらに影響を与える脆弱性が一覧表示されます。

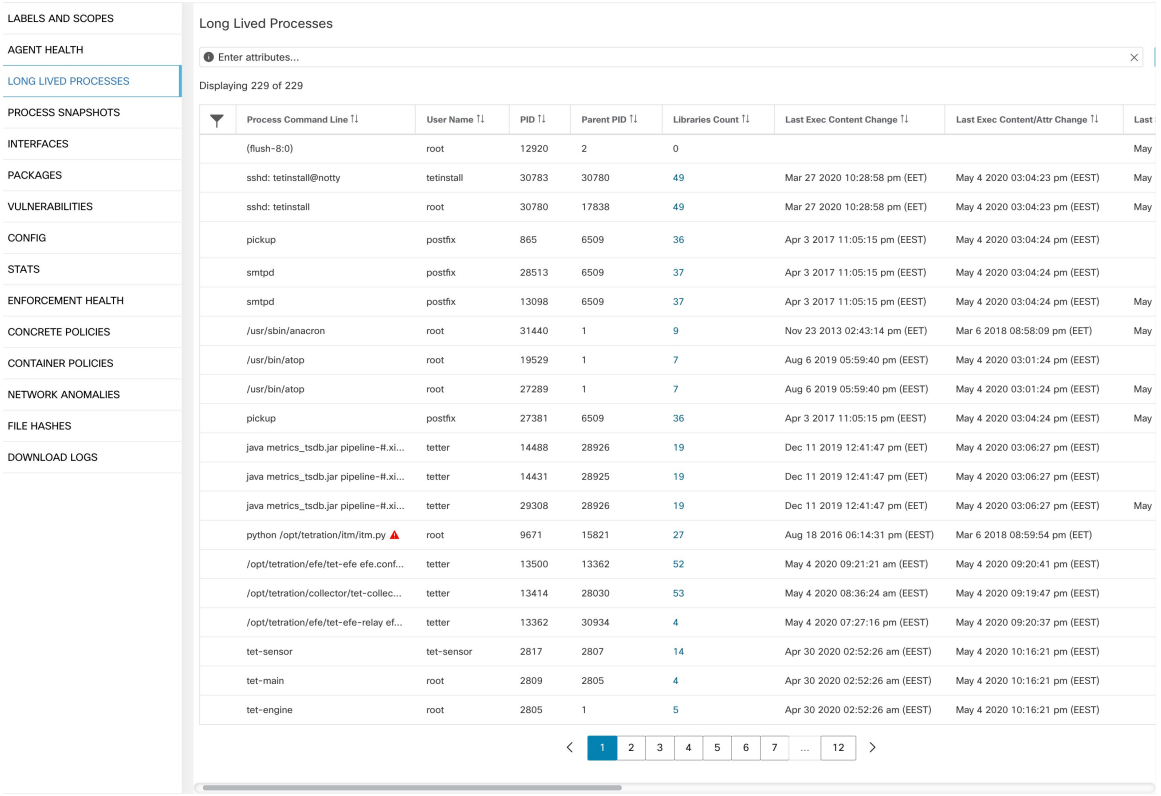
図 *64 :* ワークロード プロファイル パッケージ



[プロセスリスト（Process List）] タブ

存続期間の長いプロセスは、プロセスリストタブに表示されます。

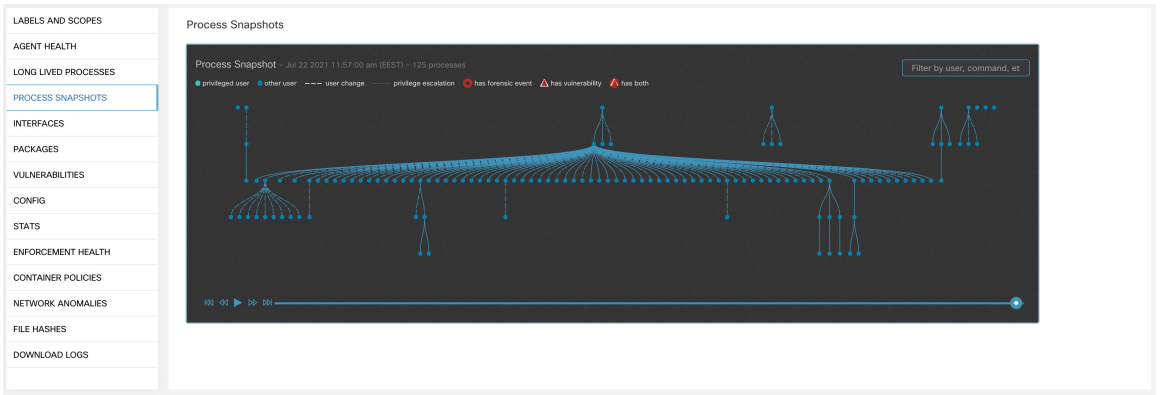
図 *65 :* ワークロードプロファイルのプロセスリスト



[プロセススナップショット（Process Snapshot）] タブ

[プロセススナップショット（Process Snapshot）] タブの下の下にあるプロセスツリーには、すべてのプロセスに関する脆弱性情報が表示されます。

図 *66 :* ワークロードプロファイルの *[プロセススナップショット（Process Snapshot）]* タブ



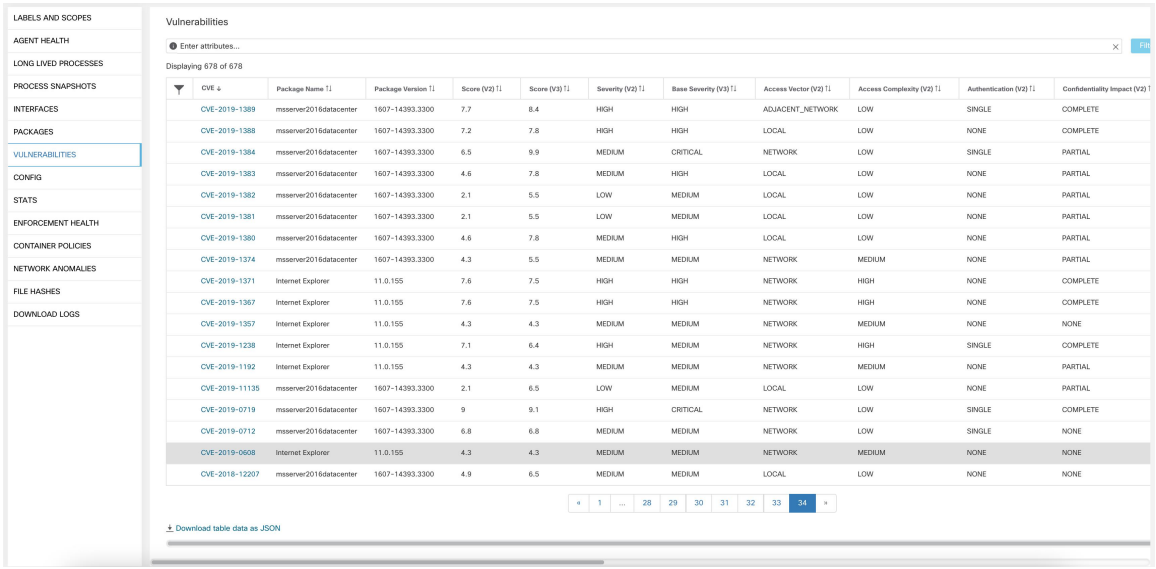
[脆弱性（Vulnerabilities）] タブ

[脆弱性（vulnerability）] タブには、ワークロードで観察された脆弱性のリストが表示されます。

CVE ごとに、基本的な影響指標に加えて、脅威インテリジェンスに基づくエクスプロイト情報が表示されます。

- エクスプロイト数：昨年、CVE が実際に悪用されたのが確認された回数
- 最終エクスプロイト：脅威インテリジェンスによって、CVE が実際に悪用されたのが最後に確認された時間

図 *67 :* ワークロードプロファイルの脆弱性タブ



インベントリフィルタ

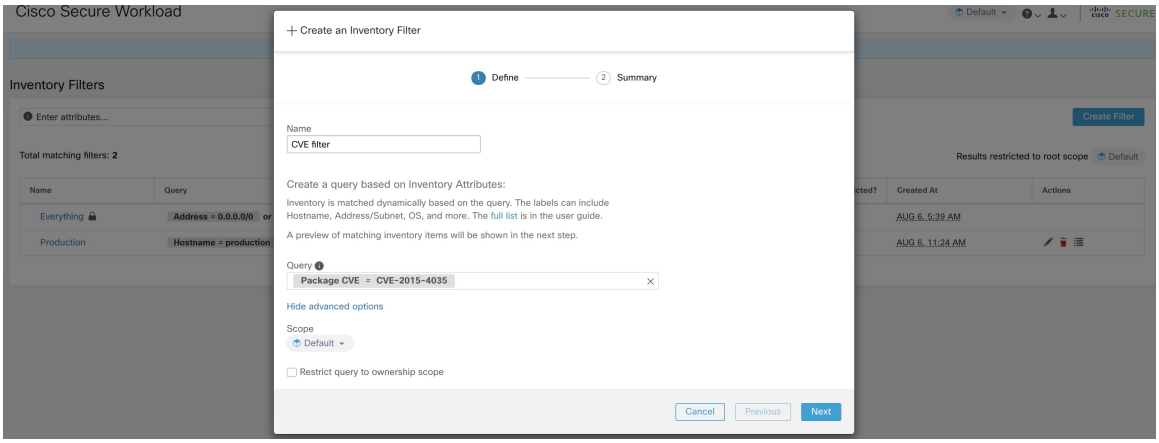
次のタイプのインベントリフィルタを定義して、脆弱なパッケージを持つホストを特定できます。

CVE ID ベースのフィルタ

このフィルタにより、特定の CVE または任意の CVE の影響を受けるホストを検索できます。

特定の CVE の影響を受けるホストを検索するには、CVE ID を CVE-XXXX-XXXX の形式で指定します。

図 *68* : インベントリフィルタ *CVE*



次の操作がサポートされます。

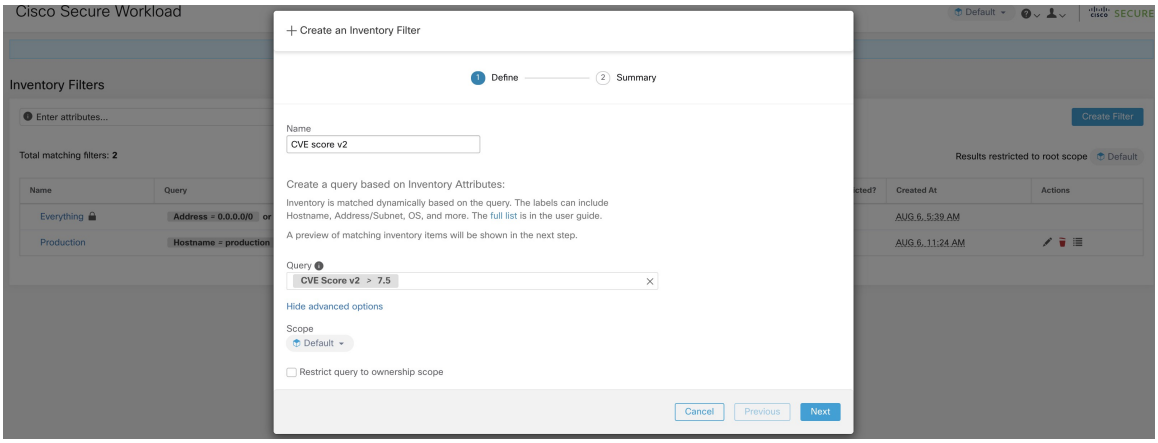
- [等価（Equality）]：CVE ID の影響を受けるパッケージを持つホストを返します。
- [非等価（Inequality）]：CVE ID の影響を受けないパッケージを持つホストを返します。
- [含む（Contains）]：入力文字列に存在する CVE の影響を受けるパッケージを持つホストを返します（「cve」と入力すると、CVE の影響を受けるホストが返されます）。
- [含まない（Doesn't contain）]：入力文字列に存在する CVE の影響を受けないパッケージを持つホストを返します（「cve」と入力すると、CVE の影響を受けないホストが返されます）。

CVSS（共通脆弱性評価システム）インパクトスコアベースのフィルタ

このフィルタにより、指定された CVSSv2 または CVSSv3 影響スコアがある CVE を持つホストを検索できます。影響スコア（v2 または v3）の CVE を持つホストを検索するには、スコアを数値形式で指定します。

CVSSv2 影響スコアが 7.5 を超える CVE を持つホストを検索します。

図 *69*：インベントリフィルタ *CVSS*



次の操作がサポートされます。

- [等価（Equality）]：指定された CVSSv2 または CVSSv3 影響スコアがある CVE を持つホストを返します。
- [非等価（Inequality）]：指定された CVSSv2 または CVSSv3 影響スコアがある CVE を持たないホストを返します。
- [より大きい（Greater Than）]：指定された CVSSv2 または CVSSv3 影響スコアそれぞれよりも大きい CVSSv2 または CVSSv3 影響スコアがある CVE を持つホストを返します。
- [以上（Greater Than or Equal To）]：CVSSv2 または CVSSv3 影響スコアがそれぞれ指定された CVSSv2 または CVSSv3 影響スコア以上である CVE を持つホストを返します。
- [より少ない（Less Than）]：指定された CVSSv2 または CVSSv3 影響スコアそれぞれよりも小さい CVSSv2 または CVSSv3 影響スコアがある CVE を持つホストを返します。
- [以下（Less Than or Equal To）]：CVSSv2 または CVSSv3 影響スコアがそれぞれ指定された CVSSv2 または CVSSv3 影響スコア以下である CVE を持つホストを返します。

CVSSv2 ベースのフィルタ

インベントリフィルタは、脆弱なホストを特定するため、Access Vector とアクセスの複雑さを使用して作成できます。これらのフィルタは、次のタイプの操作をサポートします。

- Equality：フィルタに一致する脆弱性の影響を受けるパッケージを持つホストを返します。
- Inequality：フィルターに一致する脆弱性の影響を受けないパッケージを持つホストを返します。

Access Vector

Access Vector は、脆弱性がどのようにエクスプロイトされるかを反映します。攻撃者が脆弱なシステムから遠ざかるほど、ベーススコアは高くなります。以下の表は、さまざまな Access Vector とそのアクセス要件を示しています。

値	アクセスの種類
LOCAL	物理またはローカル（シェル）。
ADJACENT_NETWORK	ブロードキャストまたはコリジョン。
NETWORK	リモートでエクスプロイト可能。

アクセスの複雑さ

このメトリックは、攻撃者が標的のシステムにアクセスできるようになった後に、脆弱性をエクスプロイトする際の複雑さを測定します。ベーススコアは、アクセスの複雑さに反比例します。さまざまなタイプのアクセスの複雑さは次のとおりです。

値	説明
HIGH	特殊なアクセス条件が存在します。
[中（Medium）]	アクセス条件はやや特殊です。
LOW	特殊なアクセス条件は存在しません。

CVSSv3 ベースのフィルタ

攻撃元区分、攻撃の複雑さ、および特権は、CVSSv3 スコアに影響を与えるために必要であり、インベントリフィルタで使用できます。これらのフィルタは、次の操作をサポートします。

- Equality：フィルタに一致する脆弱性の影響を受けるパッケージを持つホストを返します。
- Inequality：フィルターに一致する脆弱性の影響を受けないパッケージを持つホストを返します。

攻撃元区分

このメトリックは、脆弱性のエクスプロイトが可能になるコンテキストを表します。攻撃者が脆弱なコンポーネントから遠ざかるほど、ベーススコアは高くなります。以下の表に、さまざまな攻撃元区分とそのアクセス要件を示します。

値	アクセスの種類
LOCAL	ローカル（キーボード、コンソール）またはリモート（SSH）。
PHYSICAL	物理的なアクセスが必要です。
ADJACENT_NETWORK	ブロードキャストまたはコリジョン。
NETWORK	リモートでエクスプロイト可能。

Attack Complexity

このメトリックは、脆弱性をエクスプロイトするために存在する必要がある条件を示します。ベーススコアは、最も複雑でない攻撃に対して最大です。さまざまなタイプのアクセスの複雑さは次のとおりです。

値	説明
HIGH	攻撃の設定と実行には多大な労力が必要です。
LOW	特殊なアクセス条件は存在しません。

必要な権限

このメトリックは、脆弱性のエクスプロイトを成功させるために攻撃者が持っている必要がある権限レベルを表しています。ベーススコアは、攻撃を実行するための権限が必要ない場合に最大です。必要な権限のさまざまな値は次のとおりです。

値	必要な権限
HIGH	脆弱なコンポーネントに対する重要な制御を提供する権限。
LOW	機密でないリソースへのアクセスを許可する低い権限。
NONE	攻撃の実行に特権は必要ありません。

サービス プロファイル

Cisco Secure Workload は、外部オーケストレータを介して取り込まれたすべての Kubernetes サービスや他のロードバランサの可視性を提供します。サービスプロファイルページには、特定のサービスの詳細が表示されます。

（注） サービスプロファイルページはさまざまな場所からリンクされています。サービスプロファイルを表示する方法の 1 つは、検索で説明されているようにサービスの検索を実行することです。

検索結果から、[サービス（Services）] タブの下の [サービス名（Service Name）] をクリックして、そのプロファイルに移動します。このサービスについては、次の情報が利用できます。

ヘッダー（Header）

ヘッダーは次の情報で構成されます。

- [オーケストレータ名（Orchestrator Name）]：このサービスを報告した外部オーケストレータの名前。
- [オーケストレータタイプ（Orchestrator Type）]：外部オーケストレータのタイプ。
- [名前空間（Namespace）]：サービスの名前空間。
- [サービスタイプ（Service Type）]：サービスのタイプ。値は、ClusterIP、NodePort、LoadBalancer のいずれかです。

IP とポート

この表には、このサービスにアクセスできる IP とポートのすべての可能な組み合わせが記載されています。NodePort タイプのサービスの場合、この表には ClusterIP:Port と NodeIp:NodePort の両方の関連付けが表示されます。

ユーザーラベル

このサービスに対してユーザーがアップロードしたラベルおよびオーケストレータ システムによって生成されたラベルのリスト。

範囲

ポッドが属する範囲のリスト。

ポッドプロファイル

Cisco Secure Workload は、Kubernetes 外部オーケストレータを介して取り込まれたすべての Kubernetes ポッドの可視性を提供します。ポッドプロファイルページには、特定のポッドの詳細が表示されます。

（注） ポッドプロファイルページはさまざまな場所からリンクされています。ポッドプロファイルを表示する方法の 1 つは、検索で説明しているようにポッドの検索を実行することです。

検索結果から、[ポッド（Pod）] タブの下の [ポッド名（Pod Name）] をクリックして、そのプロファイルに移動します。ポッドに関する次の情報を入手できます。

ヘッダー（Header）

ヘッダーは次の情報で構成されます。

- [オーケストレータ名（Orchestrator Name）]：このポッドを報告した外部オーケストレータの名前。
- [オーケストレータタイプ（Orchestrator Type）]：外部オーケストレータのタイプ。
- [名前空間（Namespace）]：ポッドの名前空間。

- [IPアドレス（IP Address）]：ポッドの IP アドレス。

ユーザーラベル（User Labels）

このポッドに対してユーザーがアップロードしたラベルおよびオーケストレータ システムによって生成されたラベルのリスト。

スコープ

サービスが属する範囲のリスト。

近隣

（注） 近隣は廃止され、次の Cisco Secure Workload リリースで削除されます。

近隣アプリケーションを使用すると、ユーザーは集約されたフローデータを地理的位置ごとに、またはノード間のエッジやパスなどのノード周辺の近隣について調べることができます。近隣アプリケーションでは、地理関連のアラートや、ノード、エッジ、ホップベースのアラートなど、いくつかのタイプのアラートを設定することもできます。

（注） **前提条件**：

1. 範囲階層を作成するか、ポリシーを自動的に検出して、ライブ分析を有効にして実際に近隣グラフを表示します。グラフを表示するには、近隣はフロー上でサブ範囲、フィルタ**、またはクラスタ** に注釈が付けられている必要があります。** フィルタとクラスタは、ライブ分析または適用が有効になっているプライマリワークスペースの一部である必要があり、そのワークスペースの範囲の一部である必要があります。
2. 近隣地理情報には、脅威インテリジェンスを介して地域データパックがアップロードされている必要があります。
3. 近隣地理情報では、ユーザーの Web ブラウザは、マップのレンダリングのために Mapbox API へのアクセス権が必要です。

アクセス

近隣には、左側のメニューの [調査（investigate）] からアクセスできます。

有効化/無効化の方法

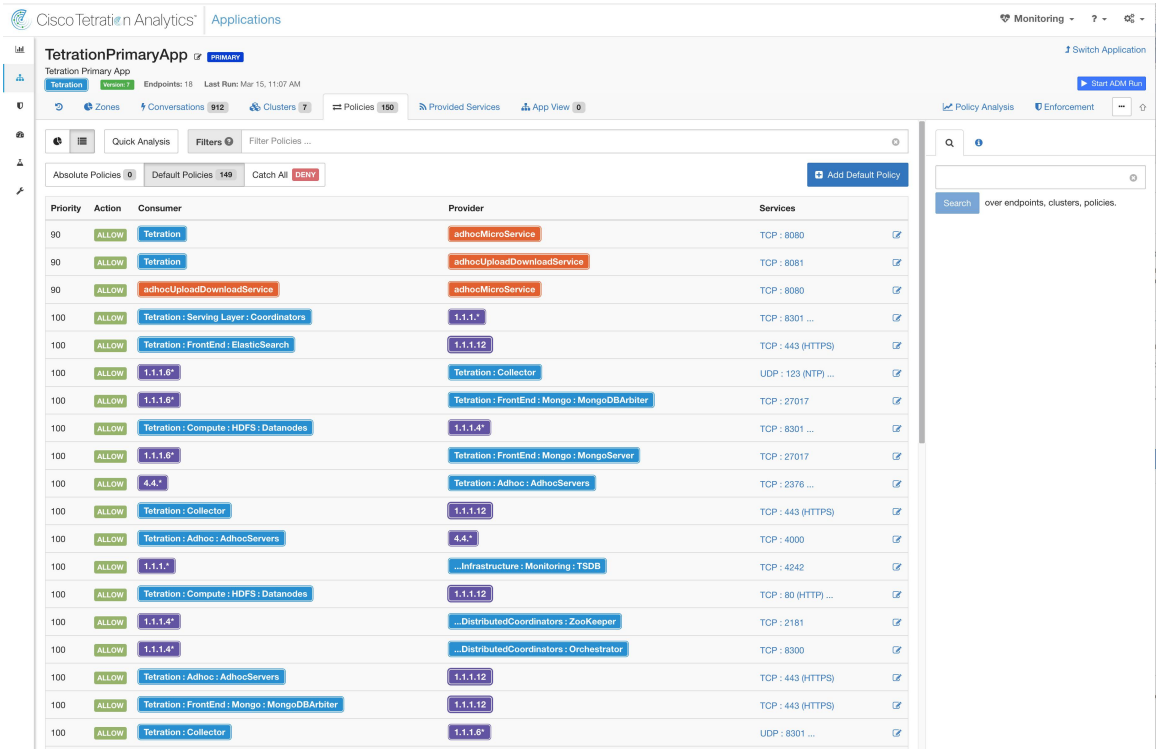
近隣は、すべてのルート範囲で自動的に有効になります。

用語

ノード

- ノードは、ライブ分析または適用が有効になっているプライマリ アプリケーション ワークスペースの一部である範囲またはインベントリフィルタ/クラスタです。さらに、フィルタには、ライブ分析または適用が有効になっているワークスペースに対応する所有範囲が必要です。

図 *70*:アプリケーションライブ分析



制限事項

- インベントリフィルタとクラスタについて、個々の範囲には 500 のサイズ制限があります。
- 優先順位は、最新のインベントリフィルタ、次に最新のクラスタの順に与えられます。最新は、更新時間で決まります。

近隣データの探索

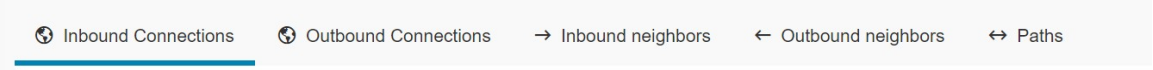
「Neighborhood」アプリをクリックすると、ビューが Neighborhood UI に変わり、近隣データを探索することができます。

Neighborhood には 5 つの異なるビューがあります。

1. 地理インバウンド
2. 地理アウトバウンド
3. インバウンドネイバー

4. アウトバウンドネイバー
5. パス

図 *71* : 近隣探索オプション



地理データの探索

近隣地域地理情報は、地理データを 2 つの方向で提供します。

1. インバウンド：特定の地理的位置（国など）から特定の範囲（つまりフィルタ/クラスタ）へのフローの集約ビュー。
2. アウトバウンド：特定の範囲（つまりフィルタ/クラスタ）から特定の地理的位置（国など）へのフローの集約ビュー。

地理ビューは、データの方向ではなく、送信元/コンシューマ範囲（アウトバウンド）または宛先/プロバイダー範囲（インバウンド）に基づいていることに注意してください。選択した地理ビュー内で、[送信バイト数（Bytes Sent）] または [受信バイト数（Bytes Received）] を選択できます。

図 *72* : インバウンド：地理的位置 → ノード

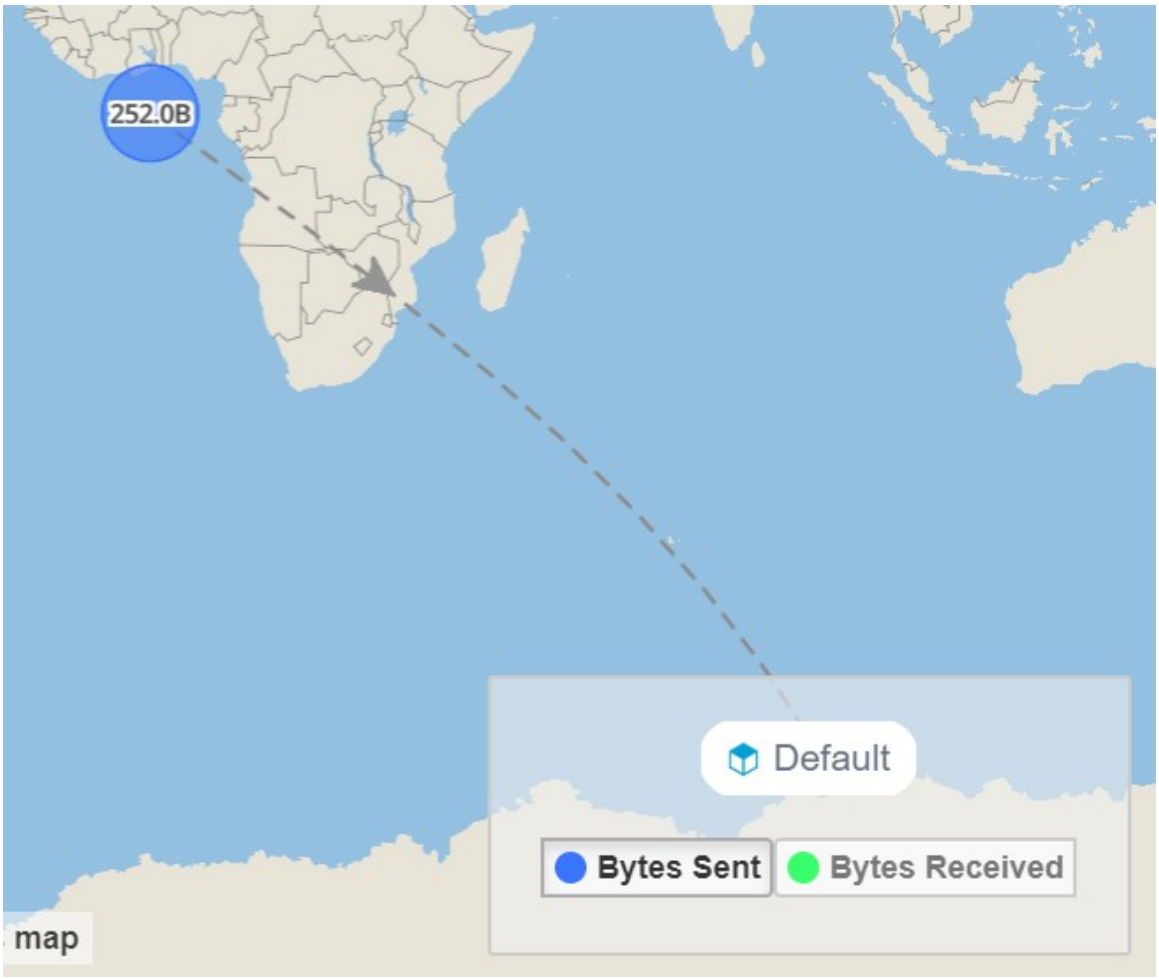
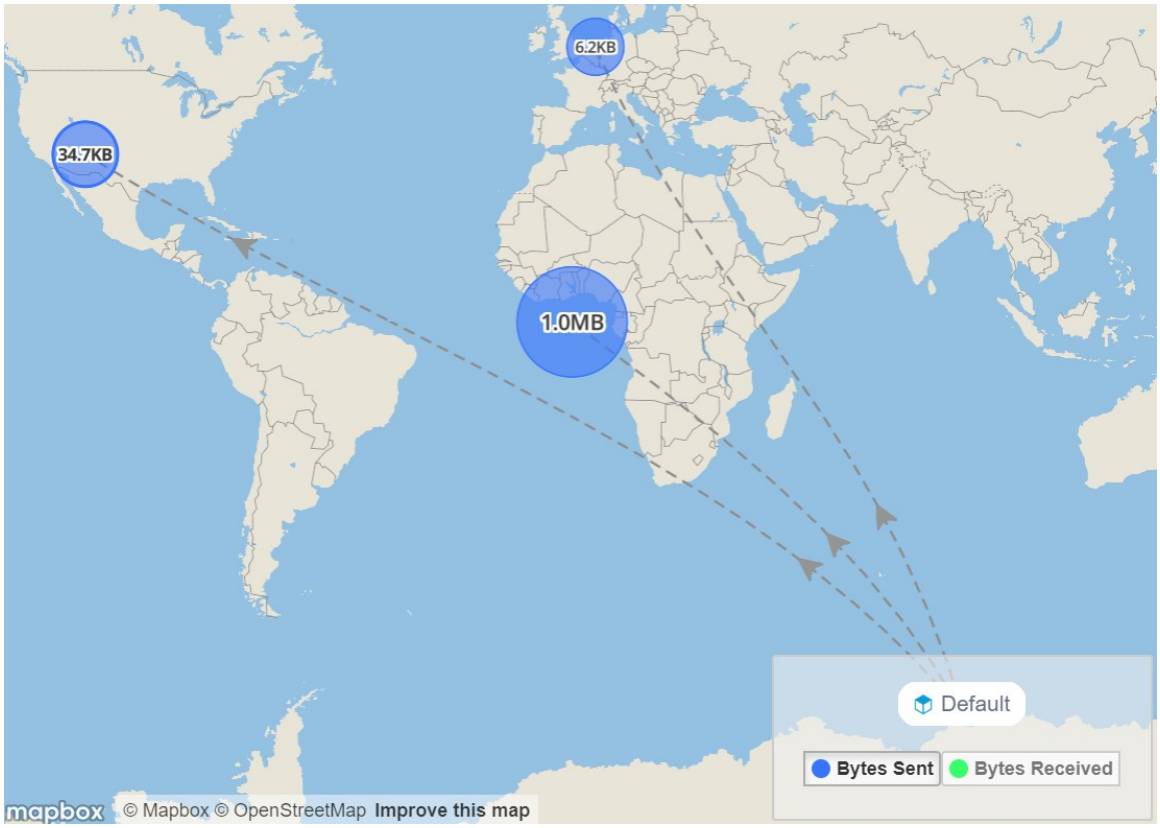
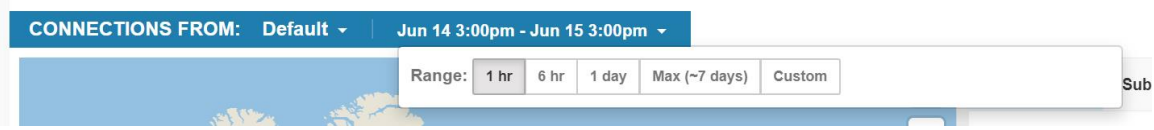


図 *73 :* アウトバウンド：ノード → 地理的位置



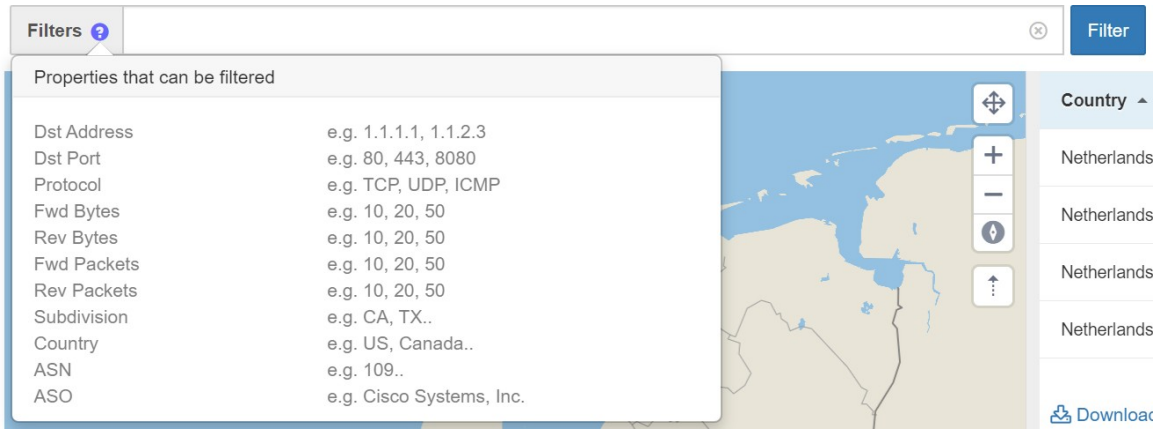
サポートされているフィルタ

図 *74 :* データを集計する時間範囲を選択するためのオプション



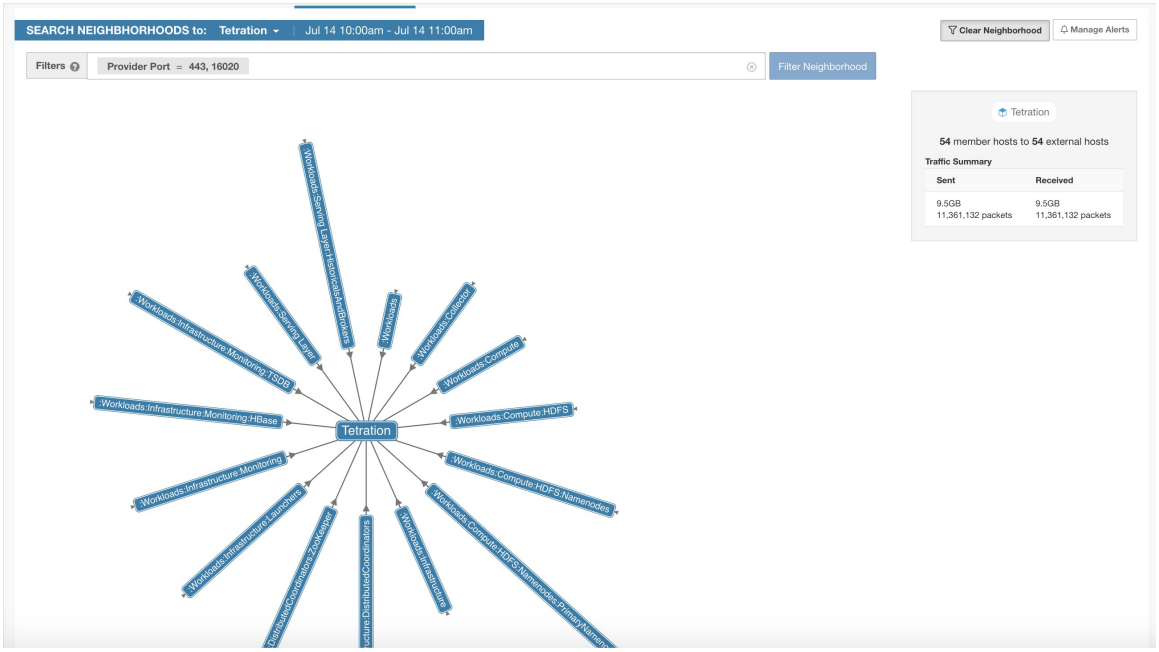
（注） 過去 7 日間まで。

図 *75* : 近隣データをフィルタリングするためのオプション



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。以下は、有効なフィルタの例です。

図 *76* : 例：フィルタ入力機能はポートの「,」をサポートします



ナビゲーション

[地理（Geo）] ページをナビゲートするための主なポイント：

ステップ 1 [インベントリプロファイル（Inventory Profile）] に移動して、より多くの過去の地理データを含む詳細なインベントリ情報を確認します。

ステップ 2 ノードを選択します。注：地理データが利用可能な範囲のみがドロップダウンリストに表示されます。

ステップ 3 時間範囲を選択します。

ステップ 4 フィルタ選択をオンまたはクリアに切り替えます。

ステップ 5 地理位置情報が不明なデータは、「ヌル島」からのデータ、または「ヌル島」に向かうデータとして表示されます。

ステップ 6 矢印にフローの送信元が範囲またはノード（ここに表示）であるか、または世界であるかが示されます。

ステップ 7 複数の地理位置情報がマップ上でグループ化される場合があります。手のひらアイコンは、クラスタをクリックして拡大し、曖昧さを解消できるかどうかを示します。

ステップ 8 表の行をクリックすると、国と区画がフィルタとして設定され、マップが拡大されて複数の住所が表示されます。

ステップ 9 マップをフルスクリーンモードにします。

ステップ 10 マウスの下にある地域を中心にマップを拡大します。

ステップ 11 マップを縮小します。

ステップ 12 ボタンを所定の位置にドラッグして、マップの方位を変更して、より 3D のような外観にします。

ステップ 13 表示されたポップアップとともに線と矢印をオフにして、データクラスタを強調します。

ステップ 14 マップの水平方向の**サイズを変更**して、マップまたはテーブルの表示を強調します。

その他の注意点：

- マップの右下に、選択した [ノード/範囲（Node/Scope）] が表示されます。[送信バイト数（Bytes Sent）] または [受信バイト数（Bytes Received）] を選択できます。
- 表の下部に、JSON データのダウンロードリンクが表示されます。

図 *77* : 地理の強調表示されたナビゲーションポイント

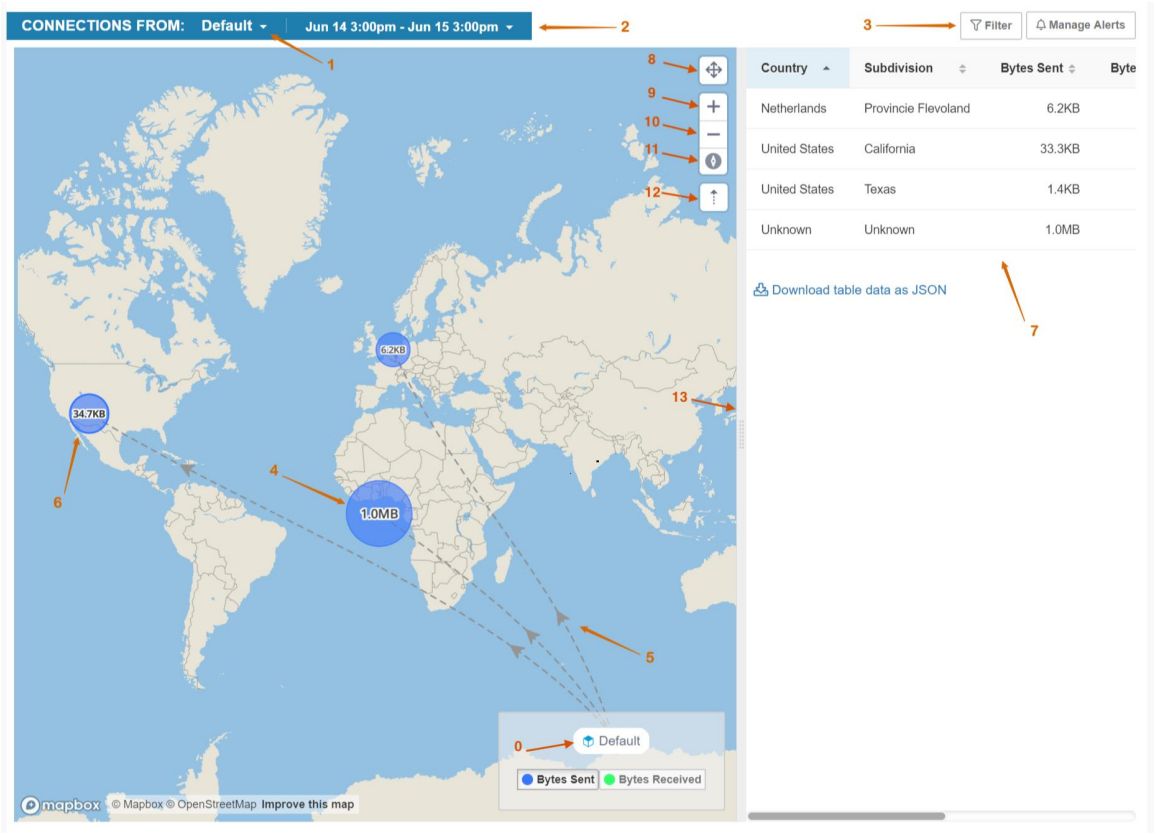
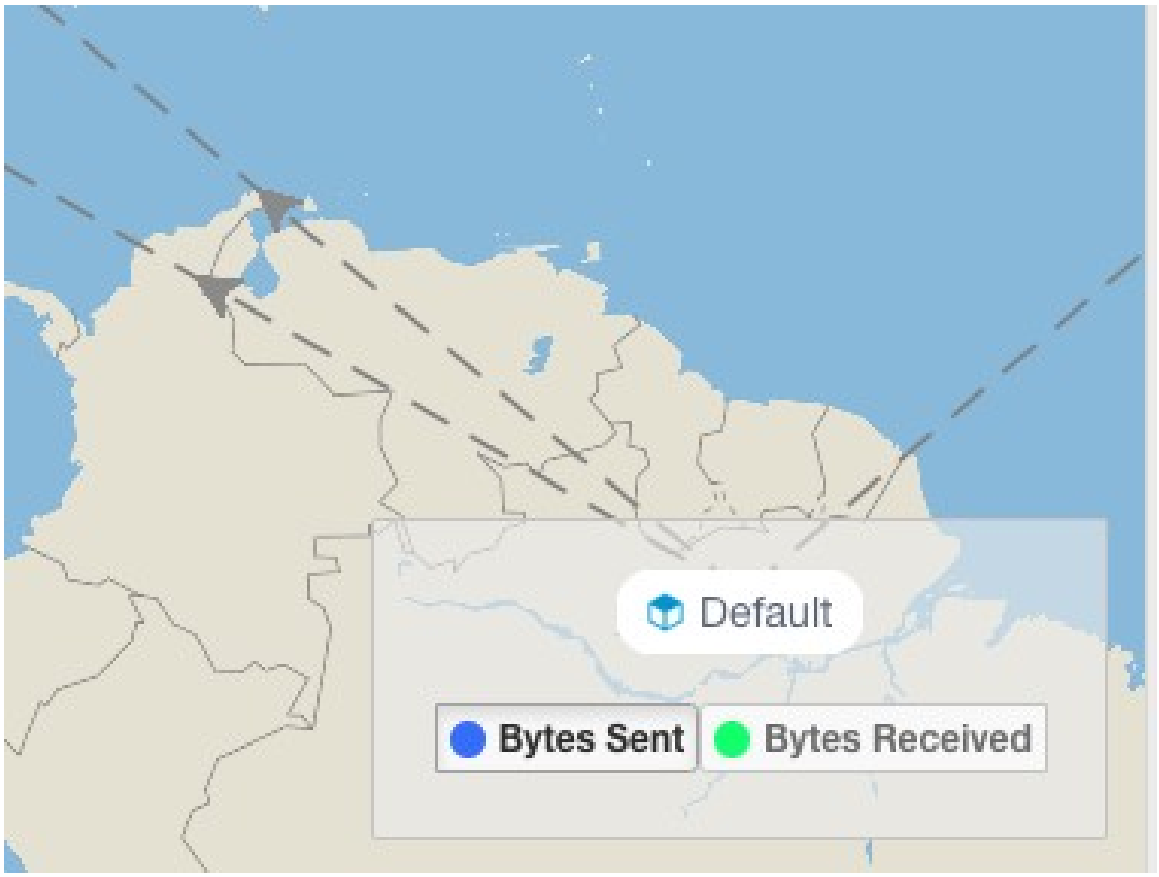
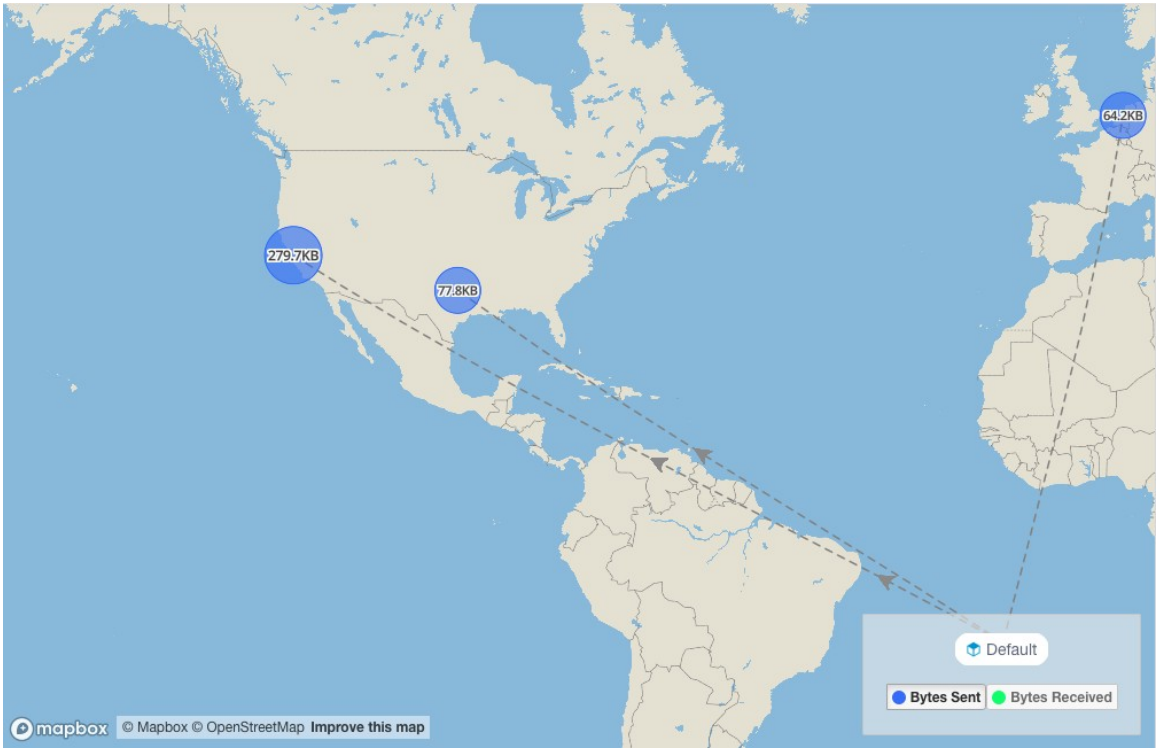


図 *78 : 例 0*



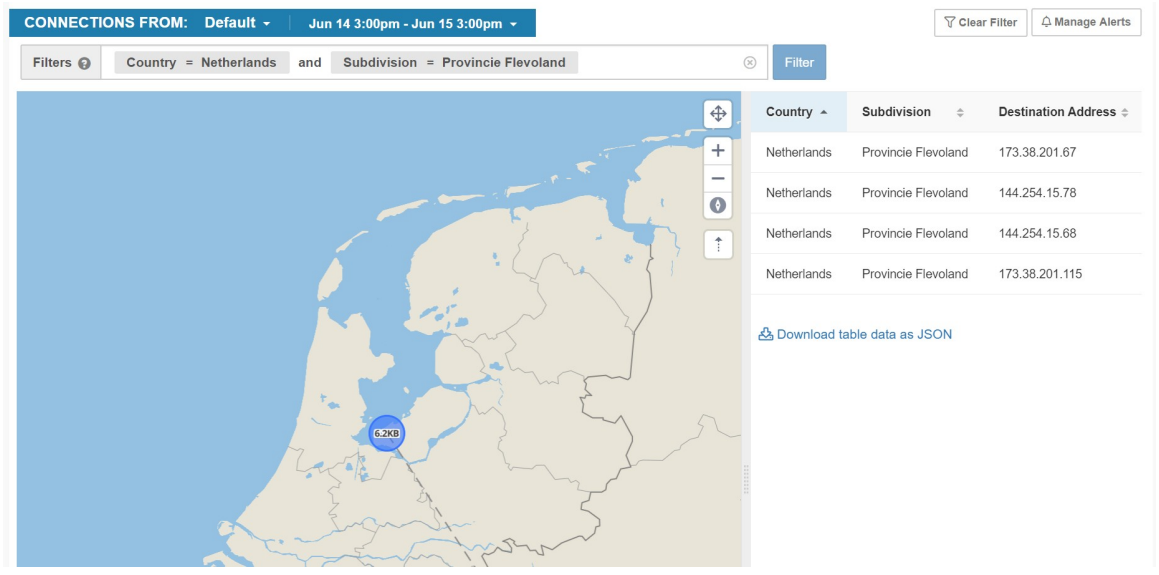
[ノード/範囲（Node/Scope）]をクリックすると、[インベントリプロファイル（Inventory Profile）]に移動します。インベントリプロファイル （53 ページ）

図 *79* : 例 *6*



マップ上のクラスタ化されたポイントのグループ（手のアイコンで識別）をクリックすると、拡大されて複数のクラスタ化されたポイントが明確になります。

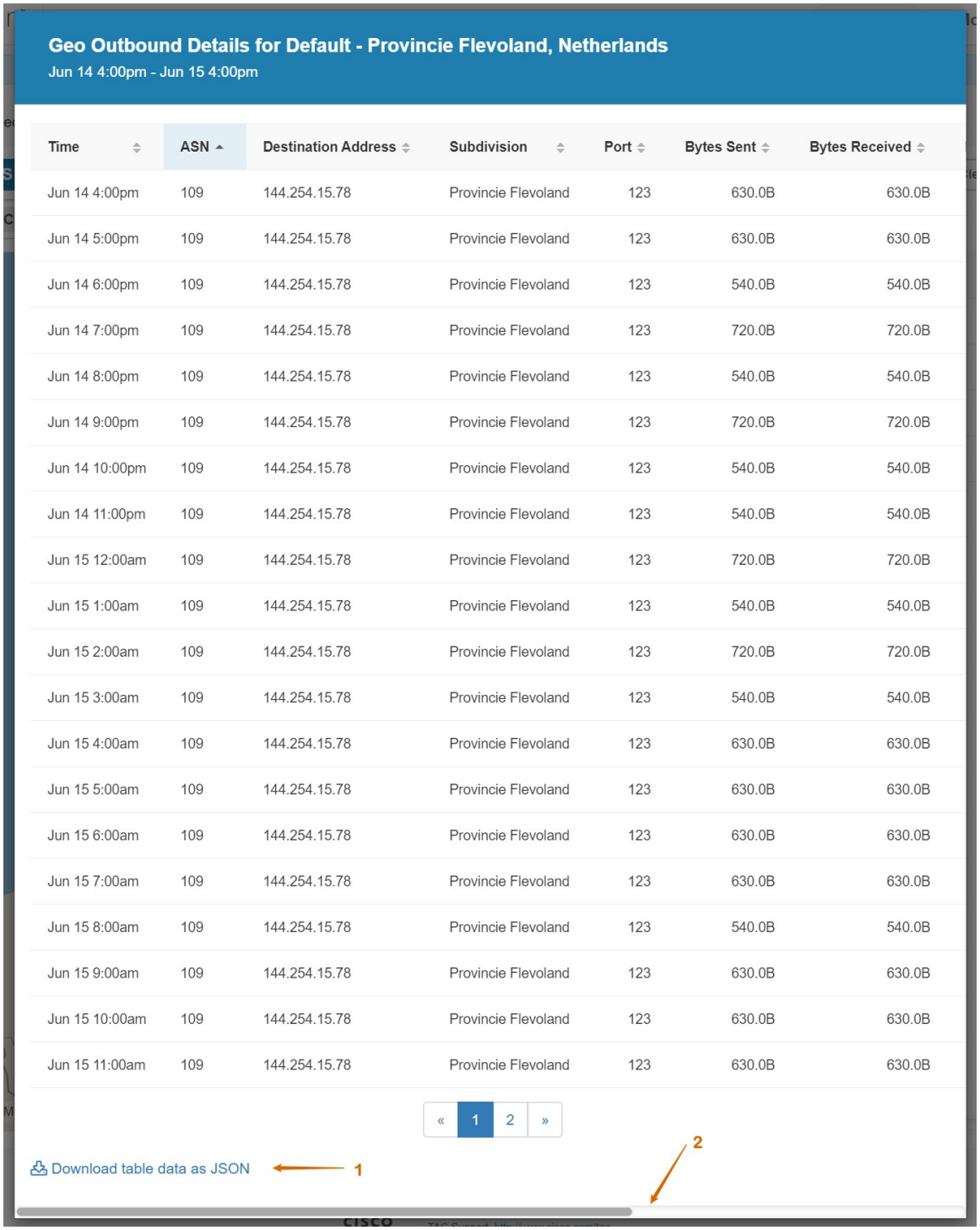
図 *80* : 例 *7*



テーブルの行をクリックすると、プロパティがフィルタに設定され、拡大されて複数のアドレスがテーブルに表示されます。

特定の送信元と宛先を選択すると、詳細ビューがポップアップ表示されます。

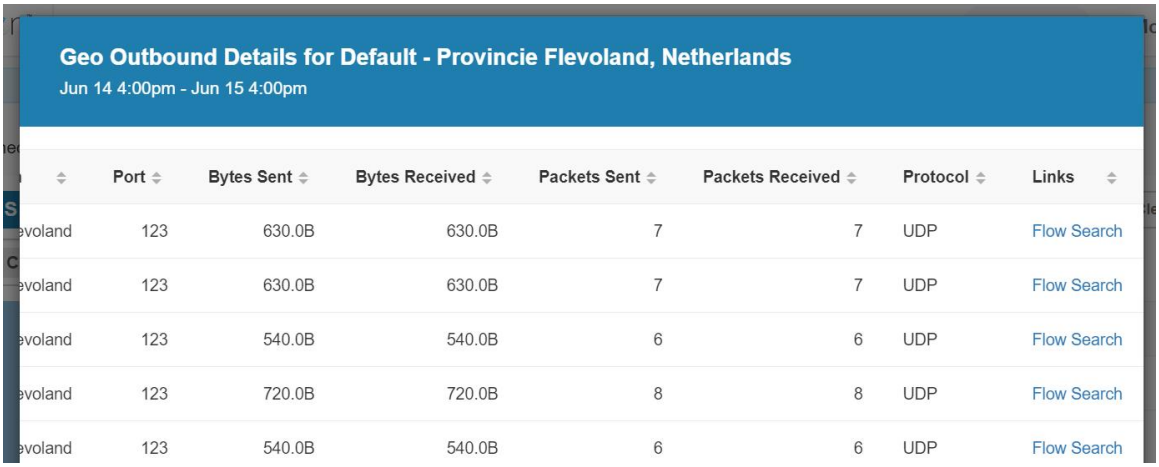
図 *81* : 以前のアドレスリストビューの行をクリックして、詳細ビューをポップアップ表示する



1. このデータはダウンロードできます。

2. 右にスクロールして、フロー検索リンクなどの追加の列に移動します。

図 *82*：詳細ビューで右にスクロールした後



詳細ビューからのフロー検索リンク。

近隣の探索

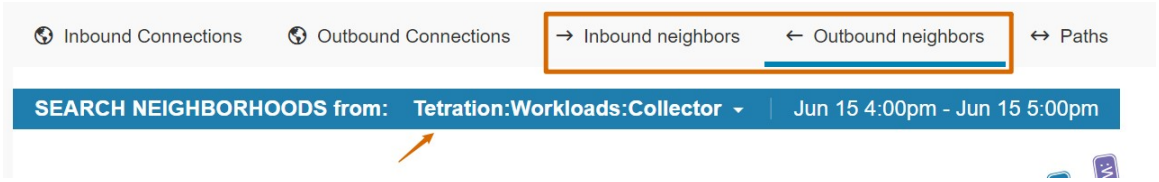
集約されたノード（範囲、フィルタ、クラスタ）データの調査には3つのバージョンがあります。

1. インバウンド：選択されたノードを宛先とする集約されたフロー
2. アウトバウンド：選択されたノードを送信元とする集約されたフロー
3. パス：1 つの送信元ノードと 1 つの宛先ノードが制約されているフローの、集約されたビューこれらはノードツーノードのエッジを集約したものですが、それ以外では無関係であることに注意してください。

インバウンドおよびアウトバウンドの探索

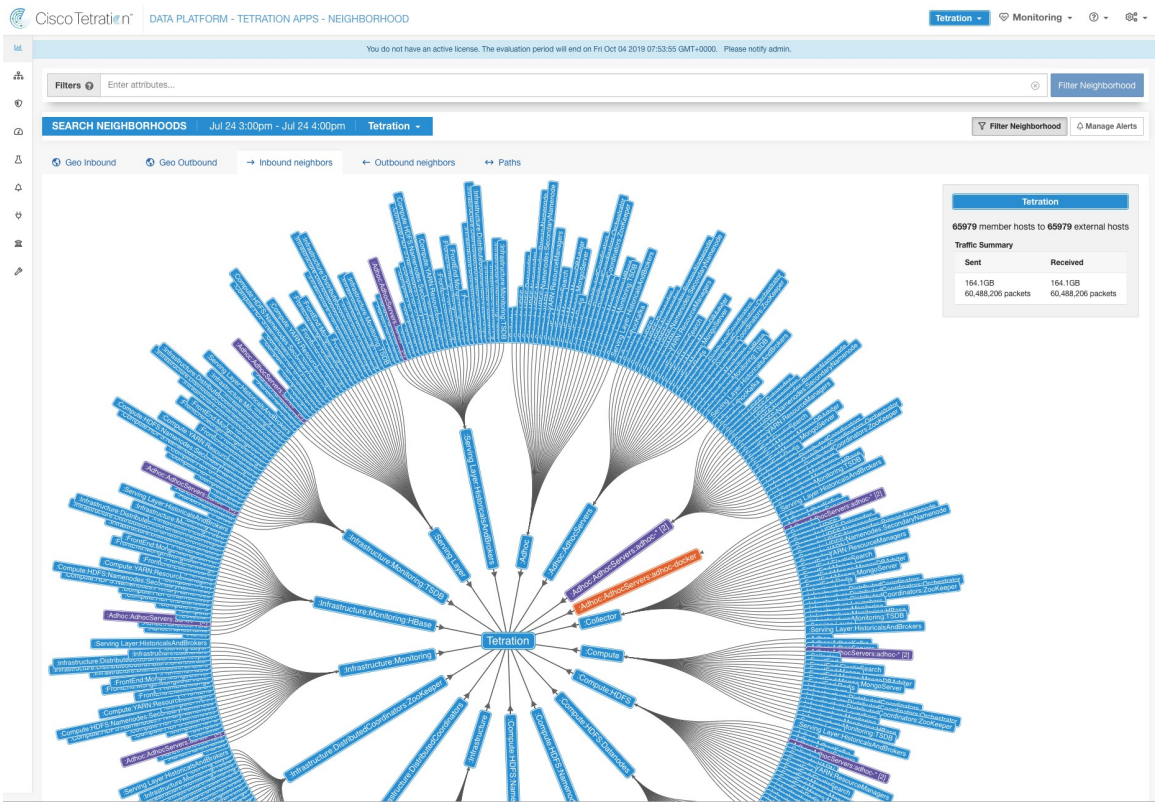
目的のノードを入力することを選択します。次に、インバウンドまたはアウトバウンドのいずれかを選択します

図 *83*：近隣データの探索



選択されたノードを中心に放射状のツリーが表示され、最大2ホップ離れた隣接ノードが内側に放射状に広がります。放射状ツリーの下には、選択されたノードへのパスのリストが表示されます。

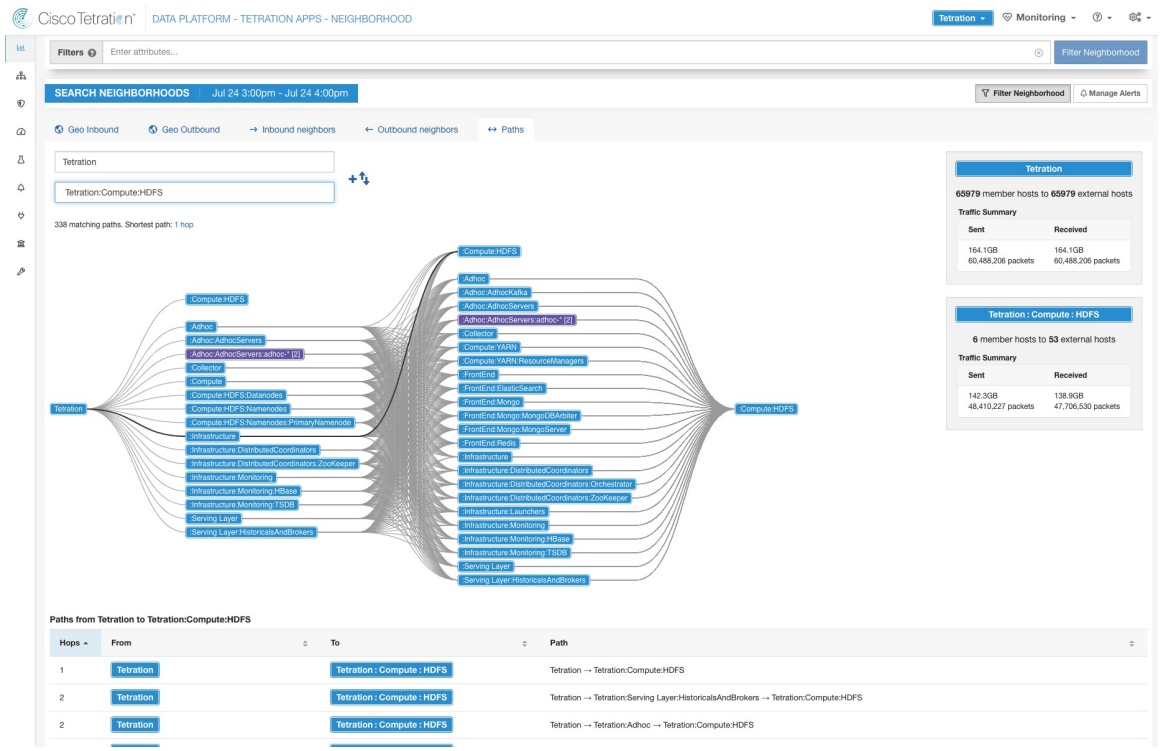
図 *84 :* ノード



パスの探索

インバウンドまたはアウトバウンドの代わりに「パス」を選択すると、送信元と宛先の両方を指定できます。

図 *85* : パス



フィルターオプション（Filter Options）

追加のフィルタオプションを指定することで、近隣グラフをフィルタ処理できます。現在サポートされているフィルタは、プロバイダーポートとプロトコルです。

図 *86* : ノードのフィルタリング

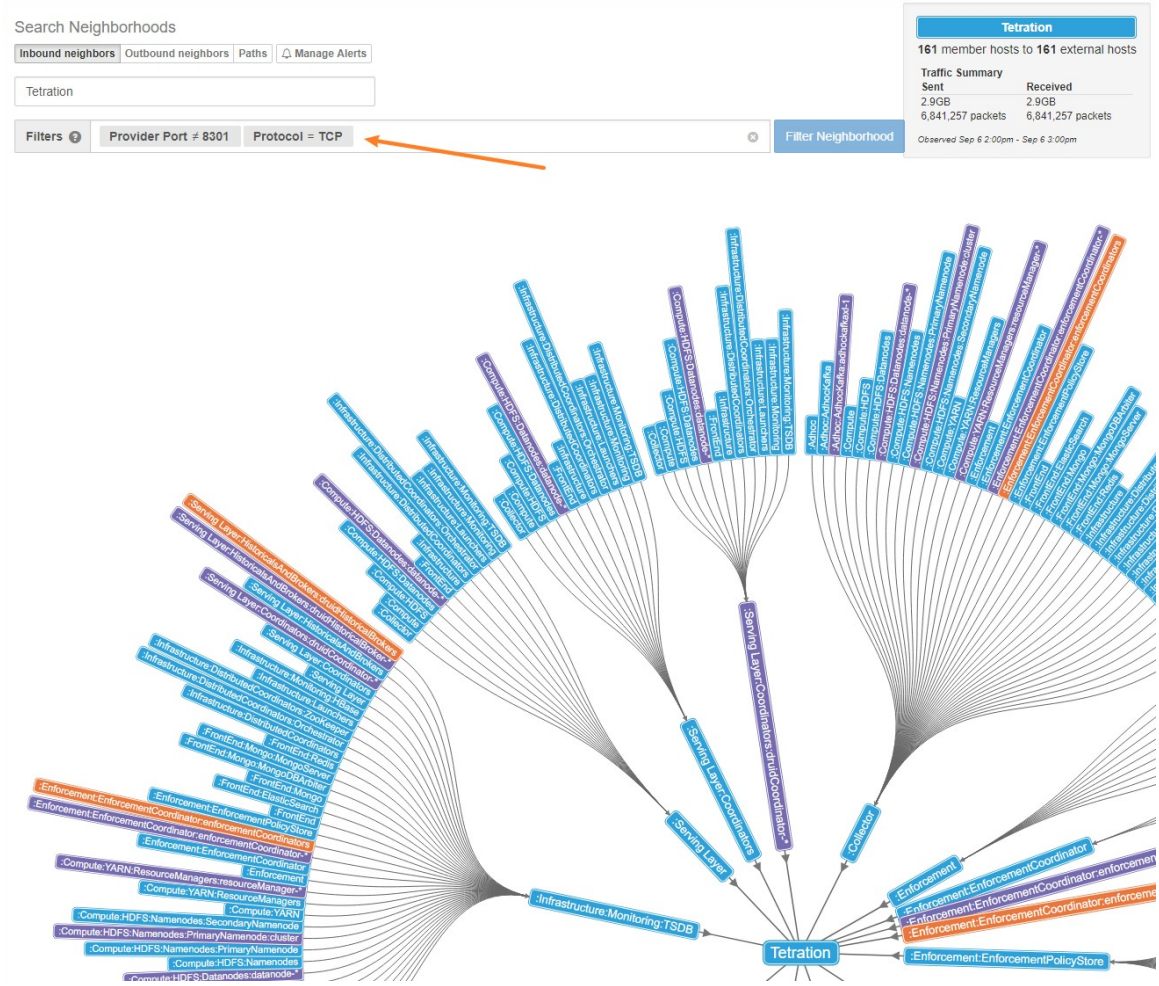
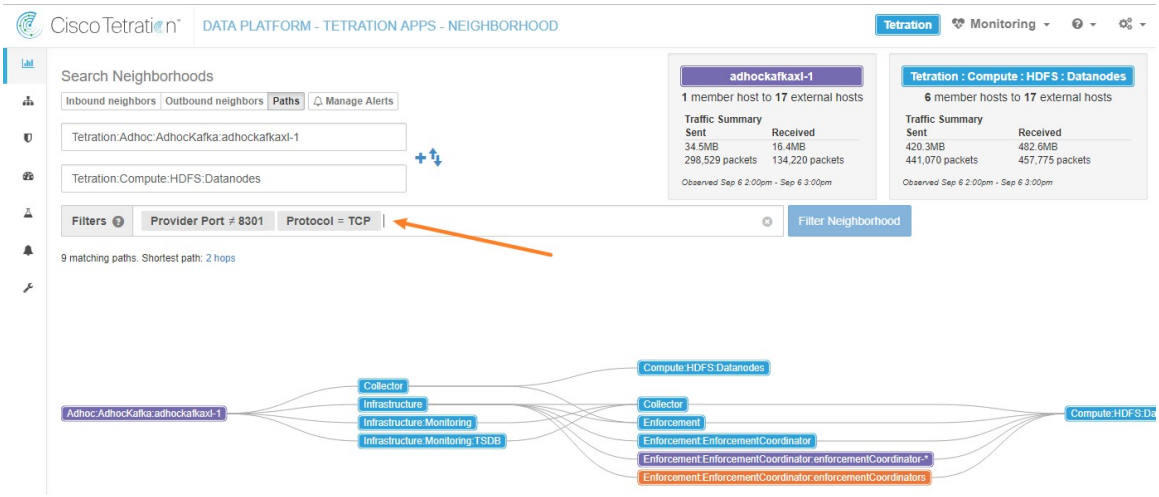
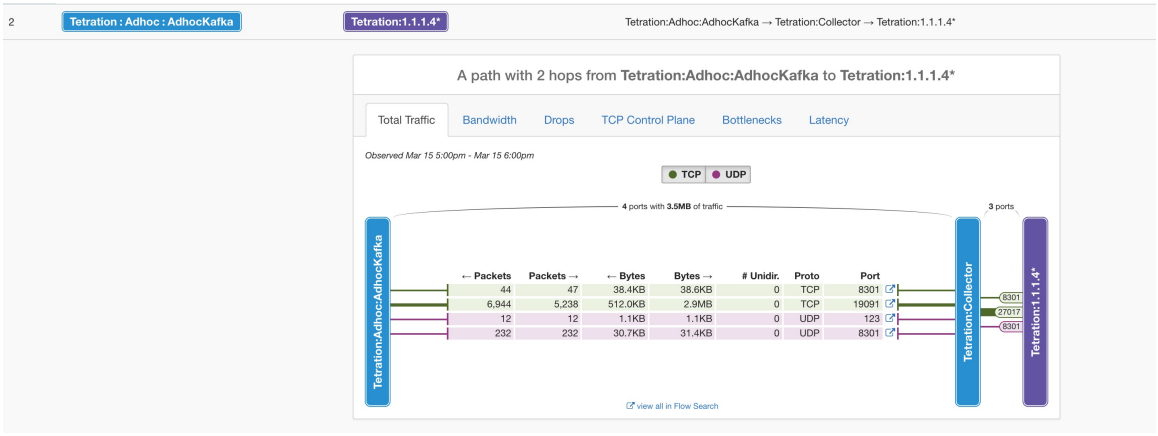


図 *87* : パスのフィルタリング



グラフの下にリストされているパスのいずれかをクリックすると、パスに関する詳細が展開され、フロー検索へのリンクが提供されます。

図 *88* : パスの詳細

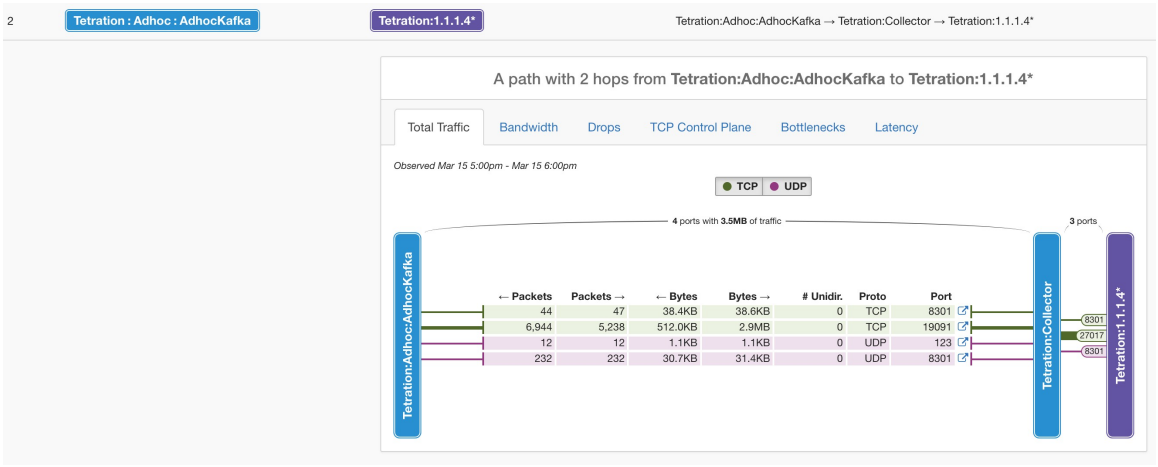


パスの詳細

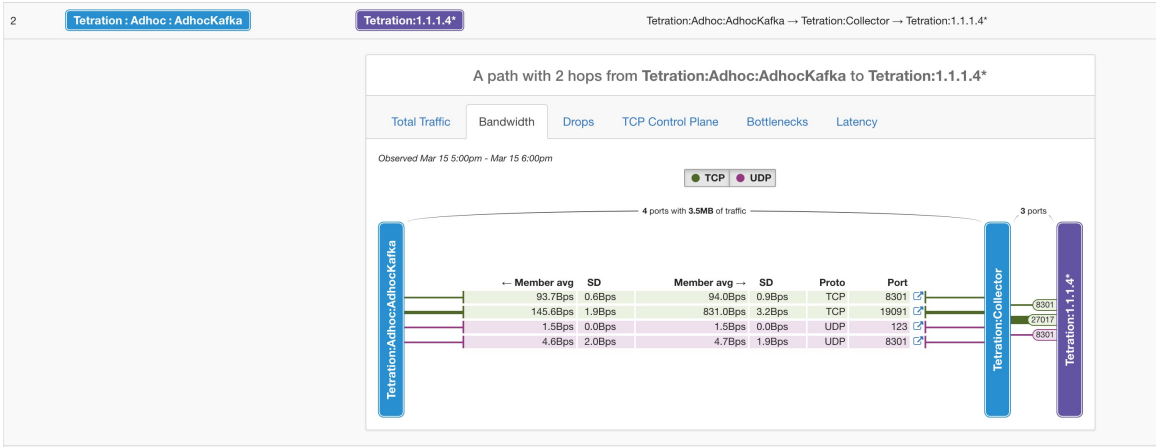
パスの詳細には、総トラフィック、帯域幅、ドロップ、TCP コントロールプレーン、ボトルネック、遅延など、さまざまなメトリックのグループを示すタブが含まれています。

（注） フローデータの収集メソッドによっては、一部のメトリックを使用できない場合があります。

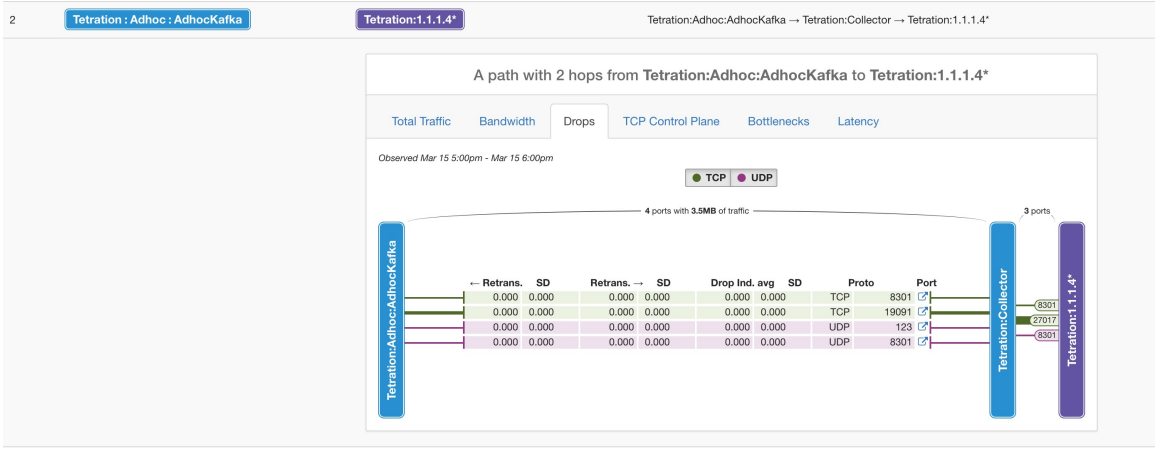
合計トラフィック



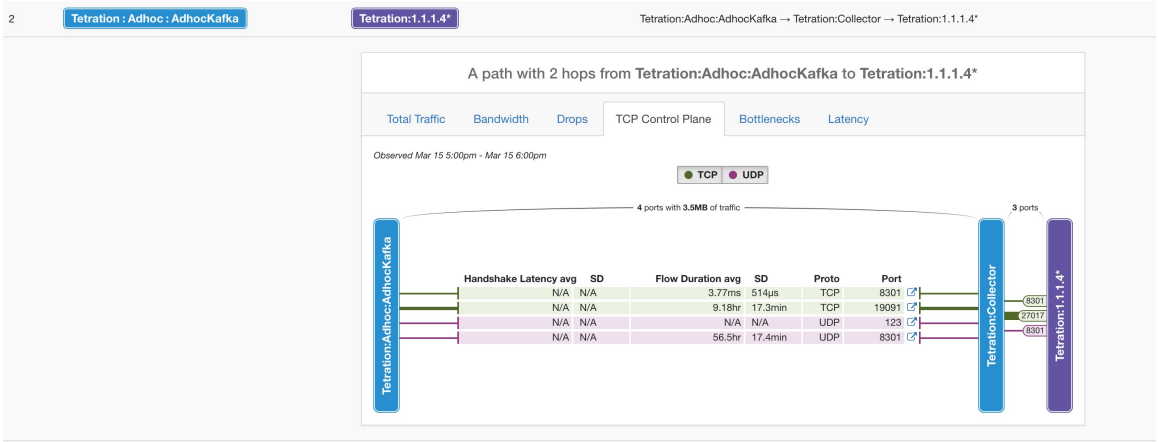
Bandwidth



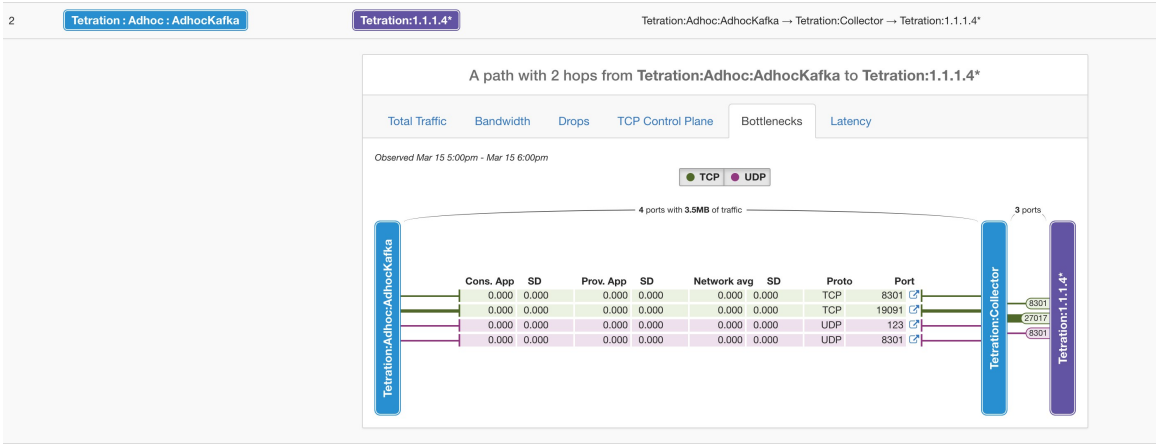
Drops



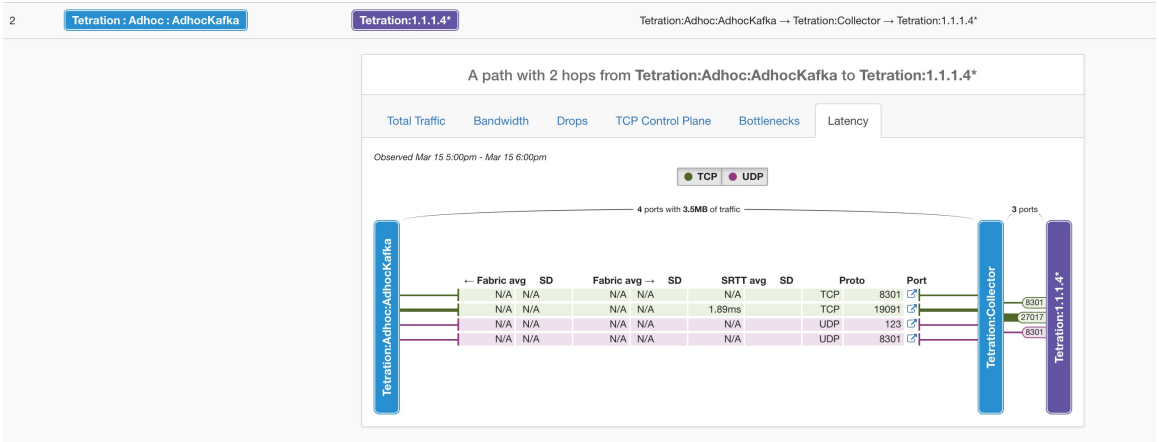
TCP コントロールプレーン



ボトルネック



遅延（Latency）



近接アラート

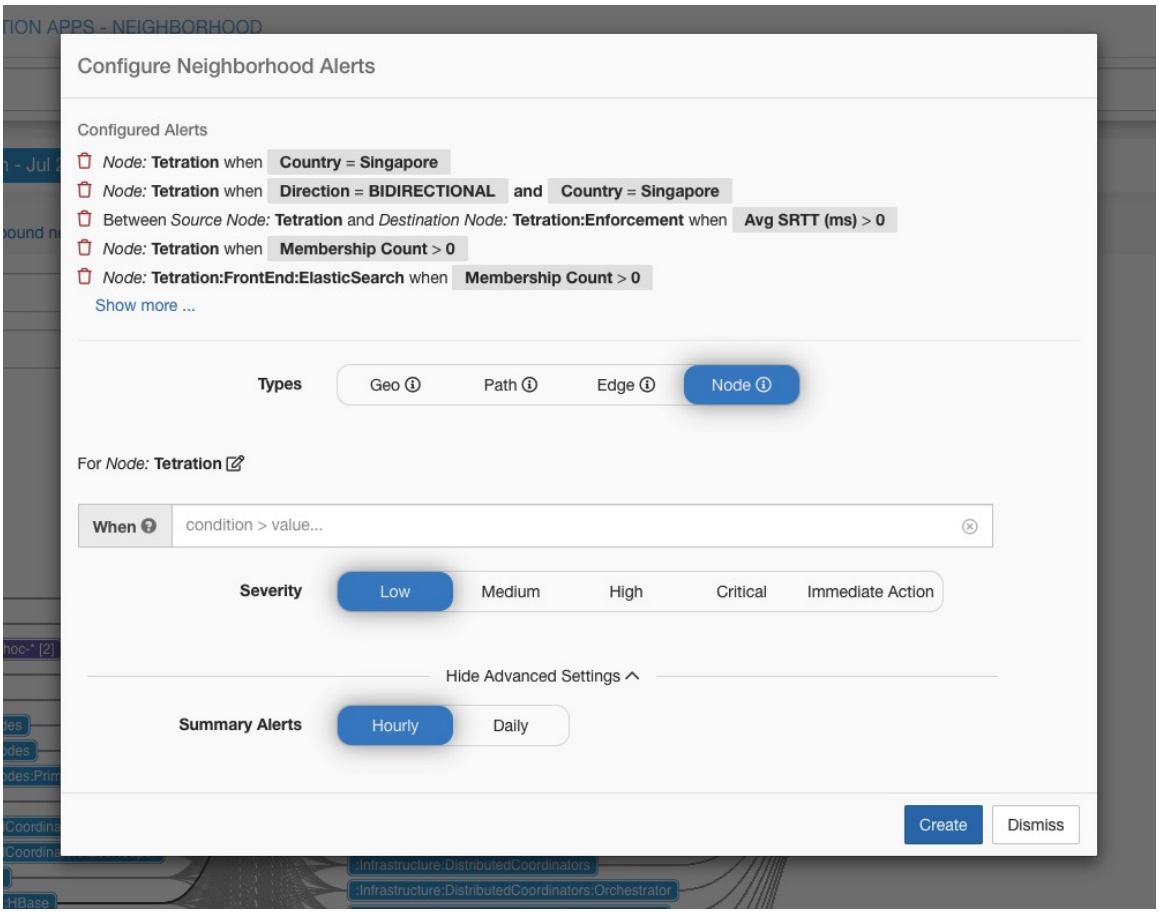
アラートの設定方法

- アラートを設定するには、[アラートの管理（Manage Alerts）] ボタンをクリックします。ボタンをクリックすると、アラート設定モーダルが開きます。ノード、エッジ、およびパスには、さまざまなタイプのアラートが用意されています。
- それぞれで使用可能なアラートトリガー設定を確認するには、ユーザーがタイプ（ノードなど）を選択し、クリックしてオプションを表示します。
- アラートトリガーの作成後、ユーザーはアラート設定を展開してアラートの頻度を変更できます。デフォルトの頻度は「毎時」ですが、「毎日」にも変更できます。

サポートされているアラート

タイプ	条件	コメント
地域	方向（Direction）	** ASO および国と組み合わせて使用する場合のみ
地域	ASO	方向（上）に応じて ASO の条件（= または≠）を確認
地域	国（Country）	方向（上）に応じて国の条件（= または/=）を確認
Path	任意のホップ	指定されたノードを経由しないパスをチェック
パス	パス	パスサイズを指定された値と比較
Edge	平均 SRTT	平均 SRTT を指定された値と比較
Edge	最大 SRTT	最大 SRTT を指定された値と比較
Edge	単方向のフロー	単方向のフローかどうかをチェック
ノード	メンバーシップの数	メンバーシップの数を指定された値と比較
ノード	隣接数	隣接数を指定された値と比較

図 *89 :* アラートの管理



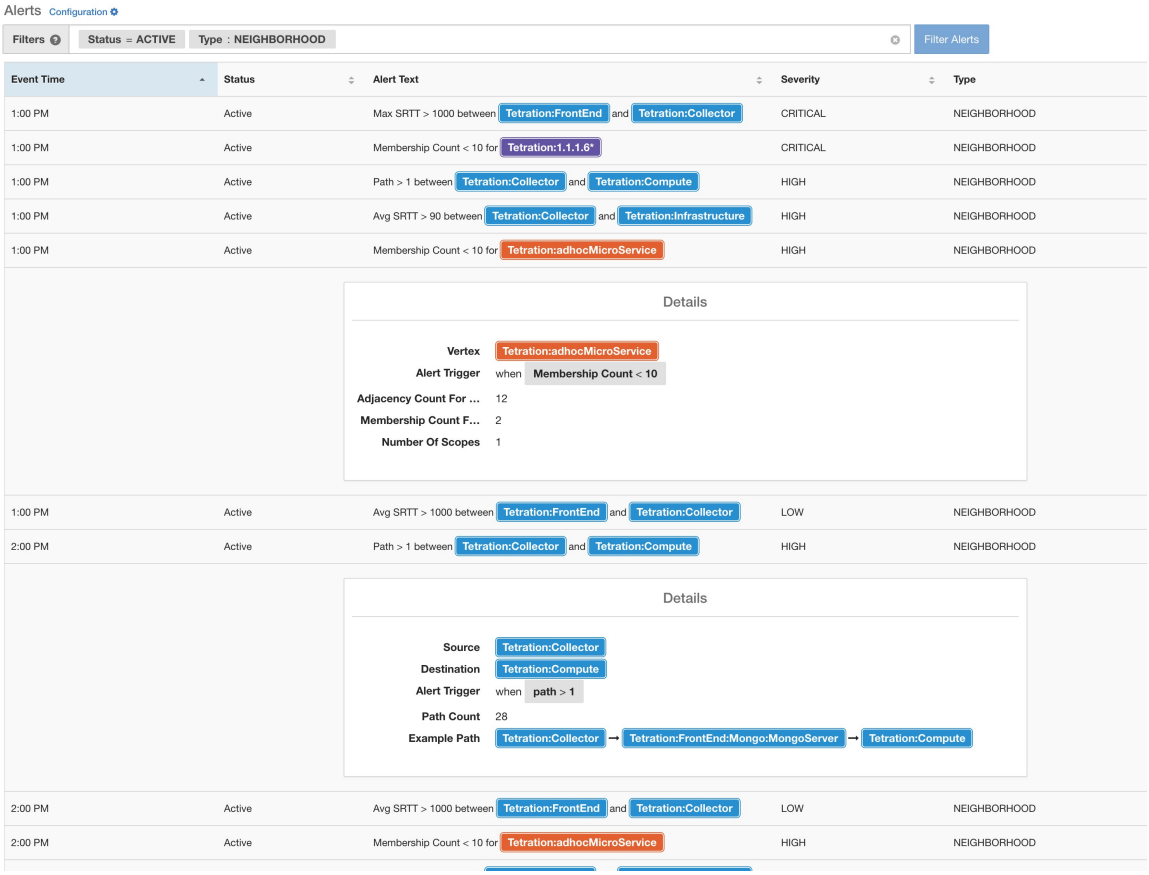
警告 サブ範囲またはフィルタが削除されても、サブ範囲またはフィルタで設定されたアラートは自動的に削除されません。同等のクエリを持つ新しいクラスタの関連性は維持されますが、クラスタまたはフィルタが最新のライブ分析ポリシーで使用されなくなった場合、それらのクラスタとフィルタを使用するアラートは生成されず、古いアラート設定が残ります。設定されたアラートを定期的に見直して、関連性を維持していることを確認する必要があります。

アラートの表示方法

- 近接アラートに対して有効な DataTap を選択する必要があります。アラートは、成功した場合のみ UI に表示されます。
  - アラートパブリッシャと通知者は、[アラート（Alerts）] → [構成（Configuration）]（[ルート範囲の所有者（Root Scope Owners）] または [サイト管理者（Site Admins）]）から選択できます。
- アラートを設定し、DataTap を設定すると、アラートは、[アラート（Alerts）] → [現在のアラート（Current Alerts）] の UI で確認できます。

- ユーザーは、フィルタ選択ボックスで **Type = NEIGHBORHOOD** を使用できます。その他のフィルタリングオプションについては、「現在のアラート」を参照してください。
- アラートをクリックすると、アラートの詳細が表示されます。

図 *90* : 近接アラート



アラート詳細

一般的なアラート構造とフィールドに関する情報については、「共通アラート構造」を参照してください。alert_details フィールドは構造化されており、近隣アラートの次のサブフィールドが含まれています。

（注） サブジェクト（ノードの間隔名）は、アラートをトリガーした近隣ノードです。

フィールド	アラートタイプ	フォーマット	説明
neighborhood_subjects_id	*all*	string	近隣ノード ID
neighborhood_subjects_name	*all*	string	近隣ノード名
internal_trigger	*all*	処理のために	アラートトリガーを説明するクエリ（詳細は次の表を参照）
country	*geo*	string	国名
subdivision	*geo*	string	区画名
aso	*geo*	string	組織名
flow	*geo*	string	アラートをトリガーしたフローの詳細（src および dst ip）
vertex_neighborhood_subjects_id	*all*	string	neighbor_subjects_id と同じ
adjacency_count_for_example_vertex	*node*	integer	指定されたノードの隣接カウント
membership_count_for_example_vertex	ノード	integer	指定されたノードのメンバーシップ数
src_neighborhood_subjects_id	*edge*、*path*	string	送信元近隣のサブジェクトID（範囲、クラスタ、またはフィルタ）
src_neighborhood_subjects_name	*edge*、*path*	string	送信元近隣のサブジェクト名（範囲、クラスタ、またはフィルタ）
dst_neighborhood_subjects_id	*edge*、*path*	string	宛先近隣のサブジェクト ID（範囲、クラスタ、またはフィルタ）
dst_neighborhood_subjects_name	*edge*、*path*	string	宛先近隣のサブジェクト名（範囲、クラスタ、またはフィルタ）
number_of_edges	エッジ	integer	アラートがトリガーされたエッジの数

フィールド	アラートタイプ	フォーマット	説明
max_srtt	エッジ	integer	条件がトリガーされたフロー全体の SRTT の最大値
avg_srtt	エッジ	integer	トリガーされたアラートのフロー SRTT の平均値
unidirectional_flow_count	エッジ	string	フロー数（複数）
example_path_neighborhood_subject_id	*path*	array[string]	トリガー条件に一致する 1 つのサンプルパスを構成する範囲、クラスタ、またはフィルタで構成される ID のリスト
example_path_neighborhood_subject_name	*path*	array[string]	トリガー条件に一致する 1 つのサンプルパスを構成する範囲、クラスタ、またはフィルタで構成されるサブジェクトのリスト
number_of_unique_paths	*path*	integer	トリガー条件に一致する一意のパスの数

internal_trigger フィールドは構造化されており、アラートトリガーの次のサブフィールドが含まれています。

フィールド	フォーマット	説明
datasource	string	アラートタイプ
rules	string	クエリ評価ルールのコレクション
filters	string	組み合わせクエリルールのリスト
type	string	クエリルールタイプ（eq、lt、gt など. .）
値	string	アラート設定のユーザー入力値
label	string	「アラートのトリガー」

Geo（ASO）アラートの alert_details の例


```
{
"neighborhood_subjects_id":"5efcfdf5497d4f474f1707c2",
"country":"United States",
"subdivision":"Texas",
"internal_trigger":{
"datasource":"geo",
"rules":{
"filters":[
{
"field":"direction",
"type":"eq",
"value":"BIDIRECTIONAL"
},
{
"field":"aso",
"type":"eq",
"value":"CISCOSYSTEMS"
}
],
"type":"and"
},
"label":"Alert Trigger"
},
"neighborhood_subjects_name":"Default",
"vertex_neighborhood_subjects_id":"5efcfdf5497d4f474f1707c2",
"flow":"72.163.32.44 -> Default"
}
```


Geo（国）アラートの alert_details の例


```
{
"neighborhood_subjects_id":"5efcfdf5497d4f474f1707c2",
"country":"Netherlands",
"subdivision":"Provincie Flevoland",
"internal_trigger":{
"datasource":"geo",
"rules":{
"field":"country",
"type":"eq",
"value":"Netherlands"
},
"label":"Alert Trigger"
},
"neighborhood_subjects_name":"Default",
"vertex_neighborhood_subjects_id":"5efcfdf5497d4f474f1707c2",
"flow":"173.38.201.67 -> Default"
}
```


ノード（隣接数）アラートの alert_details の例


```
{
"adjacency_count_for_example_vertex":7,
"neighborhood_subjects_id":"5efcfdf5497d4f474f1707c2:c_5f04b0efc5445388852786b6",
"internal_trigger":{
"datasource":"vertex",
"rules":{
"field":"adjacency_count",
"type":"gt",
"value":-1
},
```

```
"label":"Alert Trigger"
},
"neighborhood_subjects_name":"Default:cluster",
"vertex_neighborhood_subjects_id":"5efcfdf5497d4f474f1707c2:c_
→5f04b0efc5445388852786b6"
}
```


ノード（メンバーシップ数）アラートの alert_details の例


```
{
"neighborhood_subjects_id":"5efcfdf5497d4f474f1707c2",
"internal_trigger":{
"datasource":"vertex",
"rules":{
"field":"membership_count",
"type":"gt",
"value":0
},
"label":"Alert Trigger"
},
"neighborhood_subjects_name":"Default",
"membership_count_for_example_vertex":156,
"vertex_neighborhood_subjects_id":"5efcfdf5497d4f474f1707c2"
}
```


Edge (srtt avg) アラートの alert_details の例


```
{
"internal_trigger":{
"datasource":"edge",
"rules":{
"field":"srtt_usec_avg",
"type":"gt",
"value":-1
},
"label":"Alert Trigger"
},
"src_neighborhood_subjects_id":"5efcfe0f497d4f49adebc74e",
"dst_neighborhood_subjects_name":"Tetration:AdhocKafka",
"dst_neighborhood_subjects_id":"5efcfe0f497d4f49adebc6ee",
"number_of_edges":2,
"max_srtt":0,
"avg_srtt":0,
"src_neighborhood_subjects_name":"Tetration:Collector"
}
```


Edge（max srtt）アラートの alert_details の例


```
{
"internal_trigger":{
"datasource":"edge",
"rules":{
"field":"srtt_usec_max",
"type":"gt",
"value":-1
},
"label":"Alert Trigger"
},
"src_neighborhood_subjects_id":"5efcfe0f497d4f49adebc74e",
"dst_neighborhood_subjects_name":"Tetration:AdhocKafka",
"dst_neighborhood_subjects_id":"5efcfe0f497d4f49adebc6ee",
"number_of_edges":2,
```

```
"max_srtt":0,
"avg_srtt":0,
"src_neighborhood_subjects_name":"Tetration:Collector"
}
```

Edge（一方向フロー）アラートの alert_details の例

```
{
"unidirectional_flow_count":1,
"internal_trigger":{
"datasource":"edge",
"rules":{
"field":"num_unidirectional_flows",
"type":"gt",
"value":0
},
"label":"Alert Trigger"
},
"src_neighborhood_subjects_id":"5efcfe0f497d4f49adebc74e",
"dst_neighborhood_subjects_name":"Tetration:AdhocKafka",
"dst_neighborhood_subjects_id":"5efcfe0f497d4f49adebc6ee",
"number_of_edges":1,
"src_neighborhood_subjects_name":"Tetration:Collector"
}
```

パス（指定された 2 つのノード間のホップサイズ）アラートの alert_details の例

```
{
"number_of_unique_paths":2,
"example_path_neighborhood_subjects_id":[
"5efcfdf5497d4f474f1707c2",
"5efcfdf5497d4f474f1707c2:c_5f04b0efc5445388852786b6",
"5efcfdf5497d4f474f1707c2:c_5f04b0efc5445388852786b7"
],
"internal_trigger":{
"datasource":"hop",
"rules":{
"field":"hops",
"type":"gt",
"value":0
},
"label":"Alert Trigger"
},
"src_neighborhood_subjects_id":"5efcfdf5497d4f474f1707c2",
"dst_neighborhood_subjects_name":"Default:collectorDatamover-*",
"dst_neighborhood_subjects_id":"5efcfdf5497d4f474f1707c2:c_5f04b0efc5445388852786b7
→",
"src_neighborhood_subjects_name":"Default",
"example_path_neighborhood_subjects_name":[
"Default",
"Default:cluster",
"Default:collectorDatamover-*"
]
}
```

パス（指定されたノードを経由しない任意のホップ）アラートの alert_details の例

```
{
"number_of_unique_paths":2,
"example_path_neighborhood_subjects_id":[
"5efcfdf5497d4f474f1707c2",
"5efcfdf5497d4f474f1707c2:c_5f04b0efc5445388852786b6",
```

```
"5efcfdf5497d4f474f1707c2:c_5f04b0efc5445388852786b7"
],
"internal_trigger":{
"datasource":"hop",
"rules":{
"filter":{
"field":"path_by_neighborhood_subjects_id",
"type":"contains",
"value":"5efcfdf5497d4f474f1707c2:c_5f04b0efc5445388852786b5"
},
"type":"not"
},
"label":"Alert Trigger"
},
"src_neighborhood_subjects_id":"5efcfdf5497d4f474f1707c2",
"dst_neighborhood_subjects_name":"Default:collectorDatamover-*",
"dst_neighborhood_subjects_id":"5efcfdf5497d4f474f1707c2:c_5f04b0efc5445388852786b7
‹→",
"src_neighborhood_subjects_name":"Default",
"example_path_neighborhood_subjects_name":[
"Default",
"Default:cluster",
"Default:collectorDatamover-*"
]
}
```

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。