管理 Cisco Secure Workload 的资产

资产是网络上所有工作负载的 IP 地址，并标注有标签和其他描述它们的数据。您的资产包括在裸机或虚拟机、容器和云中运行的工作负载。如果适用，还可包括在合作伙伴网络上运行的工作负载。

收集资产数据是一个反复进行的过程。可以合并来自不同来源的单个 IP 地址的数据，并更新新的和已更改的 IP 地址。随着时间的推移，资产管理会变得越来越动态化。

您将根据与每个资产项目相关联的标签和注释，使用搜索、过滤器和范围对资产项目进行处理和分组。策略会应用于工作负载组，这些工作负载组由您为资产定义的过滤器和范围所定义。

资产处理选项因您的角色而异，但可能包括**搜索 (Search)**、**过滤器 (Filters)** 和**上传 (Upload)**。

工作负载标签

标签（有时称为标签、注释、属性、元数据或上下文，尽管这些术语不一定总是完全同义）是 Cisco Secure Workload 功能的关键。

可读标签可根据工作负载的功能、位置和其他标准来对其进行描述。

Cisco Secure Workload 支持通过以下方法来添加用户标签：

- 通过在资产项目上运行的 Cisco Secure Workload 代理发现
- 通过上传逗号分隔值 (CSV) 文件手动导入

- 通过用户界面手动分配
- 通过面向终端的连接器自动导入
- 通过“用于资产增强的连接器”自动导入
- 自动导入协调器生成的标签和自定义标签（请参阅外部协调器）
- 从云连接器自动导入（请参阅云连接器）
- 在创建安装程序脚本时，可以指定资产标签。使用该脚本安装的所有代理都会自动标记上此类标签。只有 Linux 和 Windows 工作负载部署支持此功能。

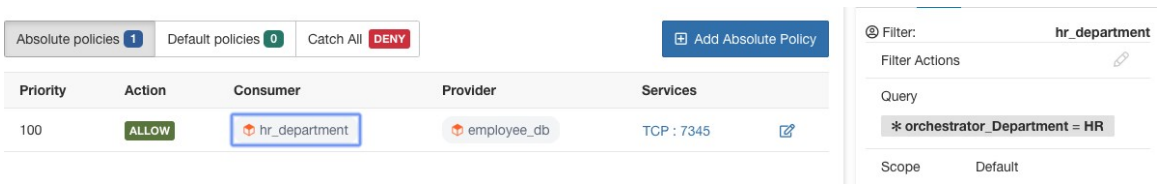
标签的重要性

标签允许您定义逻辑策略。例如：

允许从使用者 *hr_department* 到提供者 *employee_db* 的流量

如下图所示，我们可以使用标签来定义逻辑策略，而不是指定使用者和提供者工作负载组的成员。请注意，这样就可以动态修改使用者组和提供者组的成员身份，而无需修改逻辑策略。在队列中添加和删除工作负载时，会通知 Cisco Secure Workload 您已配置的服务（例如外部协调器和云连接器）。这使得 Cisco Secure Workload 能够评估使用者组 *hr_department* 和提供者组 *employee_db* 的成员关系。

Figure 1: 带标签的示例策略



基于子网的标签继承

支持基于子网的标签继承。当满足以下条件之一时，较小的子网和 IP 地址将继承其所属较大子网的标签：

- 较小子网/地址的标签列表中缺少该标签。
- 较小子网/地址的标签值为空。

请看下例：

IP	名称	目的	环境	灵性动物
10.0.0.1	server-1	webtraffic	生产	
10.0.0.2				青蛙

IP	名称	目的	环境	灵性动物
10.0.0.3				鹰
10.0.0.0/24	网络 VLAN		集成	
10.0.0.0/16		webtraffic		獾
10.0.0.0/8			测试	Bear

IP 地址 *10.0.0.3* 的标签为 *{“name”：“web-vlan”，“purpose”：“webtraffic”，“environment”：“integra- tion”，“spirit-animal”：“eagle”}*。

标签前缀

标签会自动显示可识别信息来源的前缀。

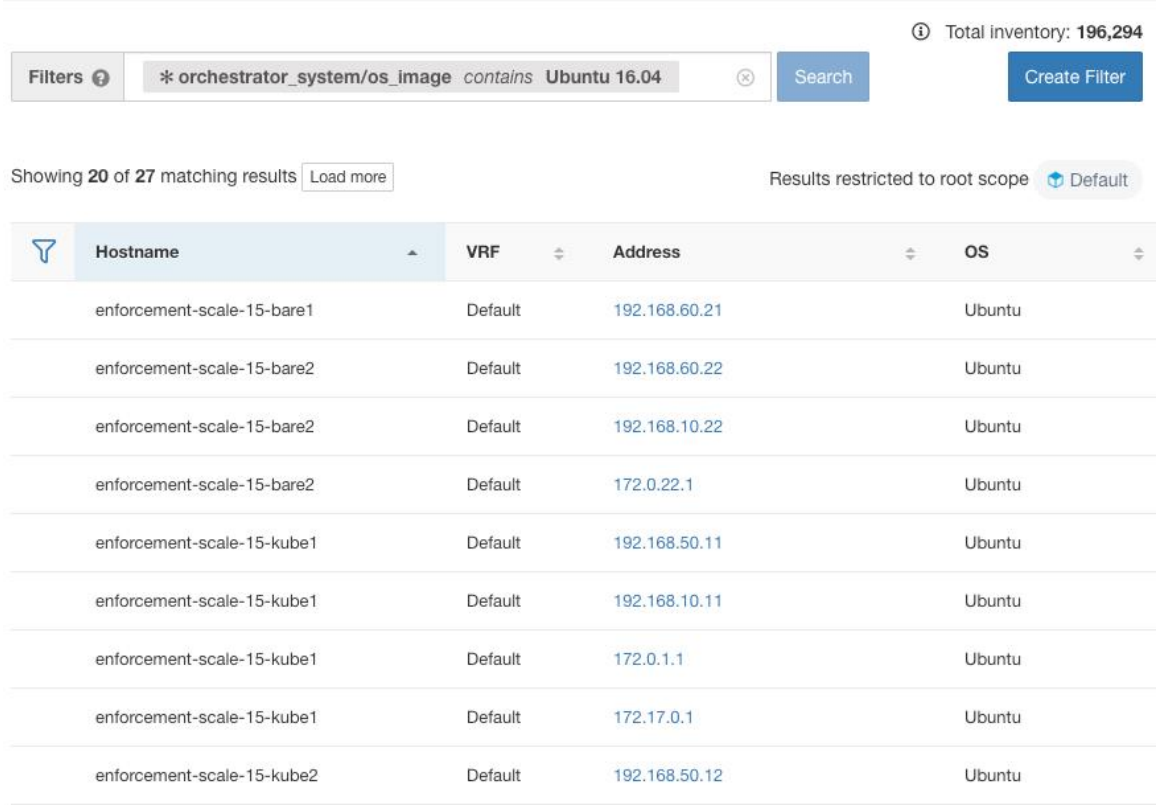
所有用户标签在 UI 中均以 * 为前缀（在 OpenAPI 中为 *user_*）。此外，从外部协调器或云连接器自动导入的标签会添加前缀 orchestrator_。对于从终端连接器导入的标签，请参阅面向终端的连接器中的详细信息，但它们可能包含以 *ldap_* 为前缀的标签。

例如，从用户上传的 CSV 文件导入的密钥为部门的标签会在 UI 中显示为 **department*，而在 OpenAPI 中显示为 *user_department*。具有从外部协调器导入的 *location* 密钥的标签会在 UI 中显示为 **orchestrator_location*，而在 OpenAPI 中显示为 *user_orchestrator_location*。

下图显示了使用协调器生成的前缀标签进行资产搜索的示例：

orchestrator_system/os_image：

Figure 2: 使用协调器生成的标签进行资产搜索的示例



云连接器生成的标签

这些标签适用于 AWS 和 Azure 的数据。这些标签的来源是 AWS VPC 或 Azure VNet 的工作负载和网络接口。源中的标签将合并并显示在 Cisco Secure Workload 中。例如，如果工作负载标签为

```
env: prod
```

，网络接口标签为

```
env: prod
```

，则安全工作负载中的标签值为

```
prod,test
```

，它会显示在相应连接器页面的 **orchestrator_env** 列下。

有关 AKS、EKS 和 GKE 的特定标签，另请参阅与 Kubernetes 集群相关的标签。

Table 1: 使用云连接器收集资产中的标签

键	值
orchestrator_system/orch_type	AWS 或 Azure
orchestrator_system/cluster_name	<*Cluster_name* 是用户为该连接器的配置所起的名称>

键	值
orchestrator_system/name	<连接器的名称>
orchestrator_system/cluster_id	<虚拟网络 *ID*>

实例特定标签

以下标签特定于每个节点：

键	值
orchestrator_system/workload_type	vm
orchestrator_system/machine_id	<由平台分配的 *InstanceID*>
orchestrator_system/machine_name	<由 AWS 赋予此节点的 PublicDNS(FQDN)> – 或 – <Azure 中的 InstanceName>
orchestrator_system/segmentation_enabled	<用于确定是否在资产上启用了分段的标志>
orchestrator_system/virtual_network_id	<资产所属虚拟网络的 *ID*>
orchestrator_system/virtual_network_name	<资产所属虚拟网络的名称>
orchestrator_system/interface_id	<连接到此资产的弹性网络接口的标识符>
orchestrator_system/region	<资产所属区域>
orchestrator_system/resource_group	（此标记仅适用于 Azure 资产）
orchestrator_‘<Tag Key>‘	分配给云门户中资产的任意数量的自定义标签的<Tag Value>键值对。

与 Kubernetes 集群相关的标签

以下信息适用于普通 Kubernetes、OpenShift 以及在受支持的云平台（EKS、AKS 和 GKE）上运行的 Kubernetes。

对于每个对象类型，Cisco Secure Workload 会从 Kubernetes 集群实时导入资产，包括与对象关联的标签。标签键和值将按原样导入。

除了导入为 Kubernetes 对象定义的标签外，Cisco Secure Workload 还会生成便于在资产过滤器中使用这些对象的标签。这些附加标签在定义范围和策略时特别有用。

为所有资源生成的标签

Cisco Secure Workload 会向从 Kubernetes/OpenShift/EKS/AKS/GKE API 服务器检索的所有节点、Pod 和服务添加以下标签。

键	值
orchestrator_system/orch_type	kubernetes
orchestrator_system/cluster_id	<|产品| 中集群配置的 *UUID*>
orchestrator_system/cluster_name	<*kubernetes* 集群的名称>
orchestrator_system/name	<连接器的名称>
orchestrator_system/namespace	<此项目的 *Kubernetes/OpenShift/EKS/AKS/GKE* 命名空间>

节点特定标签

以下标签仅针对节点生成。

键	值
orchestrator_system/workload_type	机器
orchestrator_system/machine_id	<由 *Kubernetes/OpenShift* 分配的 *UUID*>
orchestrator_system/machine_name	<为此节点提供的名称>
orchestrator_system/kubelet_version	<此节点上运行的 *kubelet* 版本>
orchestrator_system/container_runtime_version	<在此节点上运行的容器运行时版本>

Pod 特定标签

以下标签仅为 Pod 生成。

键	值
orchestrator_system/workload_type	pod
orchestrator_system/pod_id	<由 *Kubernetes/OpenShift* 分配的 *UUID*>
orchestrator_system/pod_name	<为此 *Pod* 提供的名称>
orchestrator_system/hostnetwork	<*true*|*false*> 反映 *Pod* 是否在主机网络中运行
orchestrator_system/machine_name	<*Pod* 在其上面运行的节点的名称>
orchestrator_system/service_endpoint	*[*此 *Pod* 提供的服务名称列表*]*

服务特定标签

以下标签仅为服务生成。

键	值
orchestrator_system/workload_type	service
orchestrator_system/service_name	<为此服务提供的名称>

- （仅适用于云管理的 Kubernetes）ServiceType: LoadBalancer 的服务仅支持用于收集元数据，不支持用于收集流数据或用于策略执行。

Tip 使用 **orchestrator_system/service_name** 过滤项目与使用 **orchestrator_system/service_endpoint** 过滤项目不同。

例如，使用过滤器 **orchestrator_system/service_name = web** 会选择名称为 **web** 的所有服务，而使用 **orchestrator_system/service_endpoint = web** 会选择提供名称为 **web** 的服务的所有 *Pod*。

Kubernetes 集群的标签示例

以下示例显示 Kubernetes 节点的部分 YAML 表示形式以及Cisco Secure Workload 导入的相应标签。

```
- 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
```

Table 2: 为从 ***Kubernetes*** 导入的键添加标签

导入的标签键
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

导入的标签键
orchestrator_system/workload_type
orchestrator_system/machine_id
orchestrator_system/machine_name
orchestrator_system/kubelet_version
orchestrator_system/container_runtime_version

导入自定义标签

您可以上传或手动分配自定义标签，以便将用户定义的数据与特定主机相关联。此用户定义的数据会别用于注释关联的流和资产。

无论标签源如何（手动输入或上传、使用连接器或外部协调器注入等），可在所有根范围内标记的 IPv4/IPv6 地址/子网的数量都有限制。有关详细信息，请参阅标签限制。

上传标签文件指南

Procedure

步骤 1 要查看示例文件，请在左侧窗格中选择**整理 (Organize)** > **标签管理 (Label Management)** > **用户定义标签上传 (User Defined Label Upload)**，然后点击**下载示例 (Download a Sample)**。

步骤 2 用于上传用户标签的 CSV 文件必须包含标签密钥（IP 地址）。

步骤 3 要在标签中使用非英文字符，CSV 文件必须为 UTF-8 格式。

步骤 4 确保 CSV 文件符合“标签密钥架构”部分中所述的准则。

步骤 5 所有上传的文件都必须遵循相同的架构。

标签密钥架构

列名管理准则

- 标签密钥架构中必须有一列带有“IP”标题。此外，还必须至少有一列包含 IP 地址的属性。
- “VRF”列在标签方案中具有特殊意义。如果提供，它应与您将标签上传到的根范围匹配。使用范围无关 API 上传 CSV 文件时，必须执行此操作。
- 列名只能包含以下字符：字母、数字、空格、连字符、下划线和斜线。
- 列名不能超过 200 个字符。
- 列名不能以“orchestrator_”、“TA_”、“ISE_”、“SNOW_”或“LDAP_”作为前缀，因为它们可能与来自内部应用的标签冲突。

- CSV 文件不应包含重复的列名。

列值管理准则

- 值限制为 255 个字符。但是，它们应尽可能简短，同时仍要清晰、独特，并对用户有意义。
- 键和值不区分大小写。但建议保持一致。
- “IP”列下显示的地址应符合以下格式：
  - IPv4 地址的格式可以是“xxxx”和“xxxx/32”。
  - IPv4 子网的格式应为“xxxx/<netmask> ”，其中 netmask 是 0 到 31 之间的整数。
  - 长整型格式（“x:x:x:x:x:x:x:x”或“x:x:x:x:x:x:x:x/128”）和规范格式（ “x:x::x”或“x:x::x/128”）。
  - IPv6 子网，采用长格式（“x:x:x:x:x:x:x:x/<netmask> ”）和规范格式（“x:x::x/ ”）。网络掩码必须是介于 0 和 127 之间的整数。

列的顺序无关紧要。系统将自动为标签启用前 32 个用户定义的列。如果上传的列超过 32 个，选中页面右侧的复选框最多可以启用 32 个。

上传自定义标签

以下步骤介绍具有**站点管理员**、**客户支持**或根**范围所有者**角色的用户如何上传标签。

Before you begin

要上传自定义标签，请根据“上传标签文件指南”部分创建一个 CSV 文件。

Procedure

步骤 1 在左侧窗格中，选择**整理 (Organize)** > **用户定义的标签上传 (User Defined Label Upload)** > **CSV 上传 (CSV Upload)**，然后在**上传新标签 (Upload New Labels)** 下点击**选择文件 (Select File)**。

步骤 2 在左侧窗格中，选择**整理 (Organize)** > **标签管理 (Label Management)**，然后在**上传新标签 (Upload New Labels)** 下点击**选择文件 (Select File)**。

步骤 3 选择操作 - 添加、合并或删除。

- **add**：将标签附加到新的和现有地址/子网。通过选择较新的标签而不是现有标签来解决冲突。例如，如果数据库中地址的标签为 *{"foo": "1", "bar": "2"}*，而 CSV 文件包含 *{"z": "1", "bar": "3"}*，则 add` 会为该地址将标签设置为 *{"foo": "1", "z": "1", "bar": "3"}*。
- **Merge**：将标签合并到现有地址/子网。通过选择非空值而不是空值来解决冲突。例如，如果数据库中地址的标签为 *{"foo": "1", "bar": "2", "qux": "", "corge": "4"}*，而 CSV 文件包含 *{"z": "1", "bar": "", "qux": "3", "corge": "4-updated"}*，则 merge` 会为该地址将标签设置为 *{"foo": "1", "z": "1", "bar": "2", "qux": "3", "corge": "4-updated"}*。

  Note 其中的“bar”值不会重置为“”（空），而是保留现有的“bar”=”2”值。

- **Delete**：此选项会删除地址/子网的标签，这可能会严重影响范围、过滤器、策略和强制行为。有关重要详细信息，请参阅删除标签。

重要提示：在上传自定义标签时，删除功能将删除与指定 IP 地址/子网关联的所有标签，而不限于 CSV 文件中列出的列。因此，必须谨慎使用删除操作。

步骤 4 点击**上传 (Upload)**。

搜索标签

具有**站点管理员**、**客户支持**或**根范围所有者**角色的用户可以搜索、查看和编辑分配给 IP 地址或子网的标签。

Procedure

步骤 1 在**标签管理 (Label Management)** 页面上，点击**搜索并分配 (Search and Assign)**。

步骤 2 在 **IP 或子网 (IP or Subnet)** 字段中，输入 IP 地址或子网，然后点击**下一步 (Next)**。

在“分配标签”(Assign Labels) 页面上，系统将显示输入的 IP 地址或子网的现有标签。

手动分配或编辑自定义标签

具有**站点管理员**、**客户支持**或**根范围所有者**角色的用户可以将标签手动分配给给定的 IP 地址或子网。

过程

步骤 1 在**标签管理 (Label Management)** 页面上，点击**搜索并分配 (Search and Assign)**。

步骤 2 在 **IP 或子网 (IP or Subnet)** 字段中，输入 IP 地址或子网，然后点击**下一步 (Next)**。

系统将显示“分配标签”(Assign Labels) 页面。请注意，将显示现有标签，并可对其进行编辑。

步骤 3 要添加新标签，请在 **<IP 地址/子网> 的标签 (Labels for <IP address/subnet>)** 部分中输入标签名称和值，然后点击**确认 (Confirm)**。点击**下一步 (Next)**。

步骤 4 查看更改，然后点击**分配 (Assign)** 进行提交。

下载标签

具有**站点管理员**、**客户支持**或**根范围所有者**角色的用户可以下载属于根范围的先前定义的标签。

Procedure

步骤 1 在**标签管理 (Label Management)** 页面上，点击**上传用户定义的标签 (User Defined Label Upload)**。

步骤 2 在**下载现有标签 (Download Existing Labels)** 部分下，点击**下载标签 (Download Labels)**。

Cisco Secure Workload 使用的标签会作为 CSV 文件下载。

更改标签

警告 如果需要更改标签，请谨慎操作，因为这样做会更改基于该标签的现有查询、过滤器、范围、集群、策略和强制行为的成员身份和影响。

过程

步骤 1 在**标签管理 (Label Management)** 页面上，点击**搜索并分配 (Search and Assign)** 选项卡。

步骤 2 在 **IP 或子网 (IP or Subnet)** 字段中，输入 IP 地址或子网，然后点击**下一步 (Next)**。

系统将显示 Cisco Secure Workload 用于输入的 IP 地址/子网的标签。

步骤 3 在**操作 (Actions)** 列下，点击**编辑**图标以更改所需标签的名称和值。

步骤 4 点击**确认 (Confirm)**，然后点击**下一步 (Next)**。

步骤 5 查看更改，然后点击**分配 (Assign)**。

禁用标签

更改架构的一种方法是禁用标签。请谨慎使用。

过程

步骤 1 导航至**标签管理 (Label Management)** 页面。

步骤 2 对于所需的标签，在**操作 (Actions)** 列下，选择**禁用 (Disable)**，然后点击**是 (Yes)** 以确认以从资产中删除标签。

如果您决定稍后启用该标签，请点击**启用 (Enable)** 以使用该标签。

查看标签更改影响

具有**站点管理员**、**客户支持**或**根范围所有者**角色的用户可以查看和编辑分配给 IP 地址或子网的标签。

过程

步骤 1 在**标签管理 (Label Management)** 页面上，点击**搜索并分配 (Search and Assign)**。

步骤 2 在 **IP 或子网 (IP or Subnet)** 字段中，输入 IP 地址或子网，然后点击**下一步 (Next)**。

请注意，从 IP 地址或子网继承的现有标签是可编辑的。

步骤 3 要添加新标签，请在 **Labels for** *IP address/subnet* 部分中输入标签名称和值，然后点击**确认 (Confirm)**。

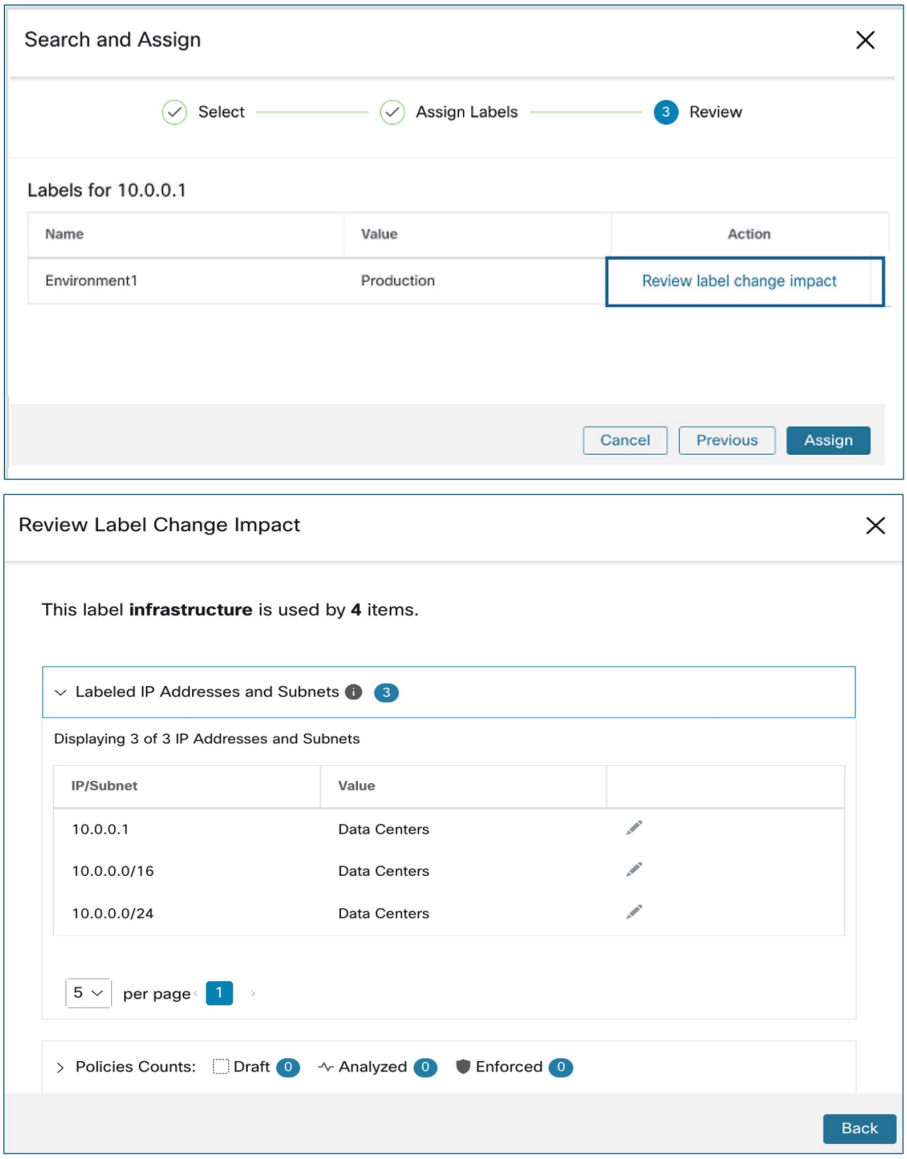
步骤 4 点击**下一步 (Next)**。

步骤 5 在**操作 (Action)** 列下，点击与要查看详细信息的标签对应的**查看标签更改影响 (Review Label Change Impact)** 链接。

步骤 6 点击**返回 (Back)** 关闭页面。

步骤 7 在**搜索和分配 (Search and Assign)** 页面中，点击**分配 (Assign)** 以确认更改。

图 3: 搜索和分配



删除标签

注意 更改架构的一种方法是禁用标签并将其删除。请谨慎决定。此操作会删除影响所有相关**过滤器**和**范围**的所选标签。确保这些标签未使用。此操作无法撤消。

过程

步骤 1 禁用标签。有关详细信息，请参阅**禁用标签**。

步骤 2 点击**垃圾桶**图标进行确认，然后点击**是 (Yes)** 删除标签。

查看标签使用情况

IP 地址或子网资产会根据使用 CSV 文件上传或用户手动分配的自定义标签进行更新。然后，标签可用于定义范围和过滤器，并根据这些过滤器创建应用策略。因此，了解标签的用法至关重要，因为对标签的任何修改都会直接影响 Cisco Secure Workload 中的范围、过滤器和策略。

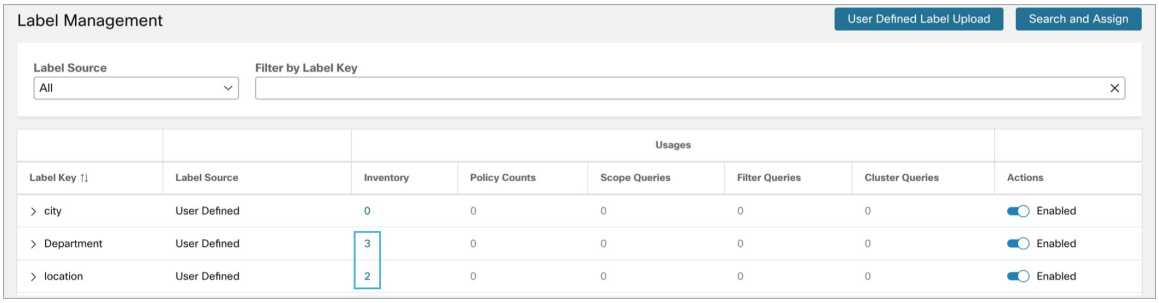
要查看标签的使用情况，请执行此程序。

过程

步骤 1 在**标签管理 (Label Management)** 页面上，将显示标签键、正在使用的标签的前五个值、资产、范围、过滤器和使用自定义标签的集群。

步骤 2 在**使用情况 (Usages)** 列中，点击资产、范围或过滤器旁边的计数值。例如，要使用“位置”(Location) 标签查看范围，请点击**范围查询 (Scope Queries)** 列中的相应计数。

图 *4:* 查看所选标签的范围



系统将显示**范围和资产 (Scopes and Inventory)** 页面，而查询会自动过滤具有所选标签的范围。

创建用于维护标签的流程

您的网络和资产将发生变化，因此必须计划更新标签以反映这些变化。

例如，如果某个工作负载已停用，并且其 IP 地址被重新分配给一个具有不同用途的工作负载，则需要更新与该工作负载关联的标签。这不仅适用于手动上传的标签，也适用于在其他系统 - 如配置管理数据库 (CMDB) 等系统中维护和注入的标签。

创建一个流程，确保定期、持续更新标签，并将此流程添加到网络维护日常程序中。

范围和资产

范围和资产概览

此部分提供了范围层次结构及其包含的所有资产的可视性。范围采用分层结构来对可用资产进行分类。有关详细信息，请参阅管理 Cisco Secure Workload 的资产, on page 1。

从导航窗格中，选择**整理 (Organize)** > **范围和资产 (Scopes and Inventory)**，向下遍历范围层次结构。每个范围都显示在范围卡中。范围卡会显示以下内容：

- 范围名称
- 子范围数量
- 资产计数
- （可选）未分类的资产

点击范围卡可更新窗格，以显示该范围的详细信息及其所有资产的过滤列表。

范围设计原则

1. 根据动态查询匹配将资产与范围树进行匹配。
   - 根据 IP、子网或标签匹配查询（首选）
   - 通过在每一层的关联查询来形成范围树。
2. 范围结构可能针对具体位置 - 组合云与数据中心、特定云与地理位置
3. 范围树的每一层应代表一个锚点，用于：
   - 策略控制
   - 基于角色的访问控制 (RBAC)
4. 范围层不能太深。
5. 确保范围未重叠：
   - 每个子范围都应是其父范围的子集。
   - 确保同级范围不重叠，请参阅范围重叠。

Note 每个组织的结构不同，所处行业不同，需要的方法也不同。选择有助于设计范围层次结构的重点领域：位置、环境或应用。

Note 不要使用 IP 地址或子网来定义涉及 Kubernetes 资产的范围。您必须使用标签为这些工作负载定义范围和策略。单凭 IP 地址不足以识别 Pod 服务，因为使用 IP 地址定义范围会产生不可靠的结果。

6. 如果一台主机有多个接口，建议将属于该主机的所有 IP 保留在一个范围内，这样我们就可以从一个位置发现并执行所需的策略。
7. 将整体范围数保持在支持的限制范围内（请参阅限制部分）

主要特性

资产计数显示在范围卡中，让您能够快速查看范围中的工作负载数量。

范围和资产的过滤功能有助于向下遍历范围树，或过滤选定范围的范围层次结构和资产项目。

范围

范围是 Cisco Secure Workload 中配置和策略的基本元素。范围是按层次结构排列的工作负载集合。标记的工作负载作为属性，可以建立一个模型，说明它在环境中的位置、角色和功能。范围提供了一种结构来支持动态机制，如与 IP 相关的标识和属性，这些可能会随着时间的推移而改变。

范围用于对数据中心应用进行分组，并与角色一起实现对其管理的精细控制。例如，范围在整个产品中用于定义对 在 Cisco Secure Workload 中管理策略生命周期、流和过滤器的访问权限。

范围按层次结构定义为根与 **VRF** 对应的树集。因此，每个范围树层次结构表示不与其他范围树重叠的不相交数据，请参阅范围重叠。

范围定义

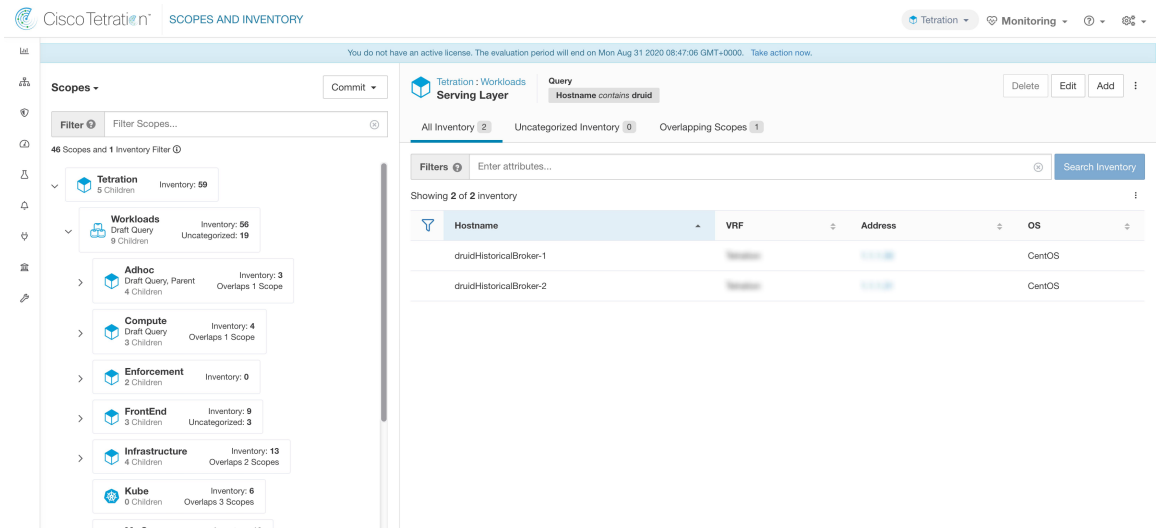
每个单独的范围都使用以下属性进行定义：

属性	说明
Parent Scope	新范围的父范围定义树形层次结构。
Name	用于标识范围的名称。
Type	这用于指定不同类别的资产。如果都不适用，或范围包含混合，则可将其留空。
Query	定义单个范围的查询。

Note 范围的定义层次结构应与组织的应用所有权层次结构相一致。

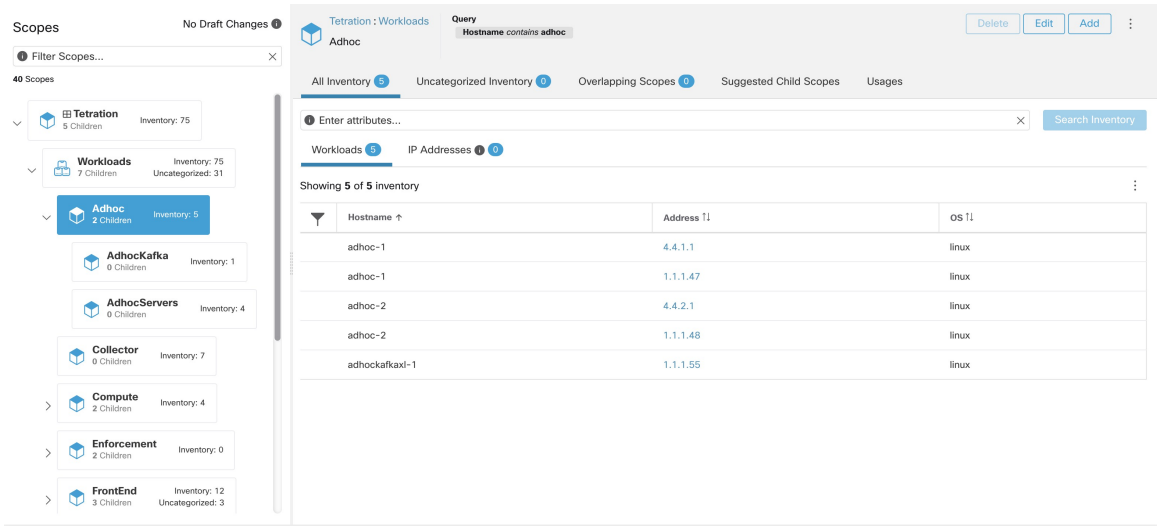
Note 查询可与 IP/子网或其他资产属性相匹配。

Figure 5: 遍历范围层次结构的示例



范围目录显示范围层次结构和每个范围的一些详细信息（例如，资产计数、子范围数量、工作空间）。点击某个范围就会选择该范围，右侧的详细信息窗格将更新，从而显示有关该范围和该范围资产的更多信息。

Figure 6: 资产计数



范围过滤器

用户可以使用范围过滤器来快速识别不同范围的详细信息，如重叠范围和查询。过滤器功能还有助于识别查询更改、父项更改等。过滤功能还有助于识别查询更改、父项更改等。

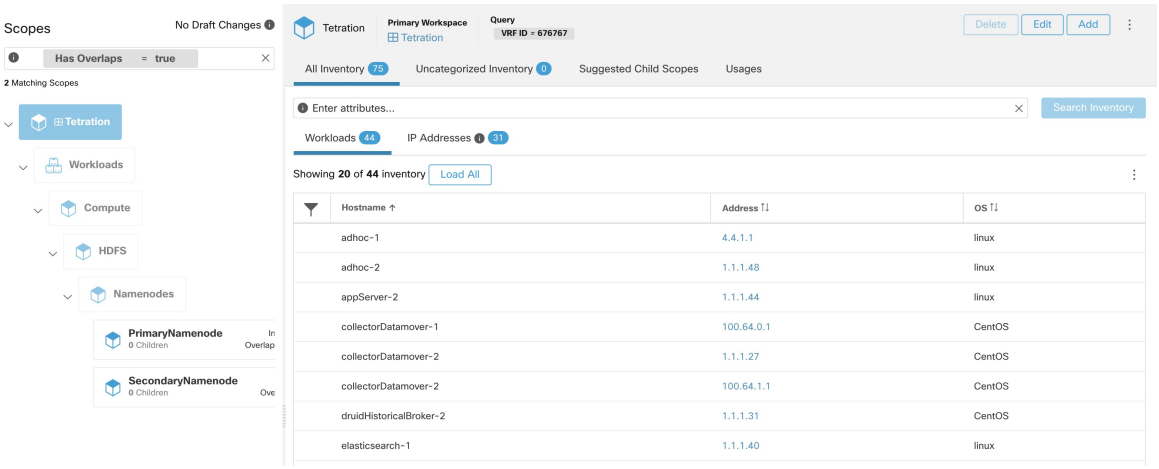
字段	说明
名称 (Name)	按范围或资产过滤器的名称进行过滤。
说明 (Description)	按范围说明中显示的文本进行过滤。
查询 (Query)	按查询中使用的字段或值过滤。
查询更改 (Query Change)	按具有未提交查询的范围进行过滤。
父项更改 (Parent Change)	按已在草稿中移动但未提交的范围进行过滤。
是资产过滤器 (Is Inventory Filter)	显示限制在其所有权范围内的资产过滤器。
有工作空间 (Has Workspace)	按具有主工作空间的范围进行过滤。
有已执行的工作空间 (Has Enforced Workspace)	按具有已执行主工作空间的范围进行过滤。
有重叠 (Has Overlaps)	按与同级范围具有共同资产的范围进行过滤。
包含无效查询 (Has Invalid Query)	按具有使用无效或未知标签的查询的范围进行过滤。

示例：

有重叠 (Has Overlaps)

范围重叠示例

Figure 7: 有重叠

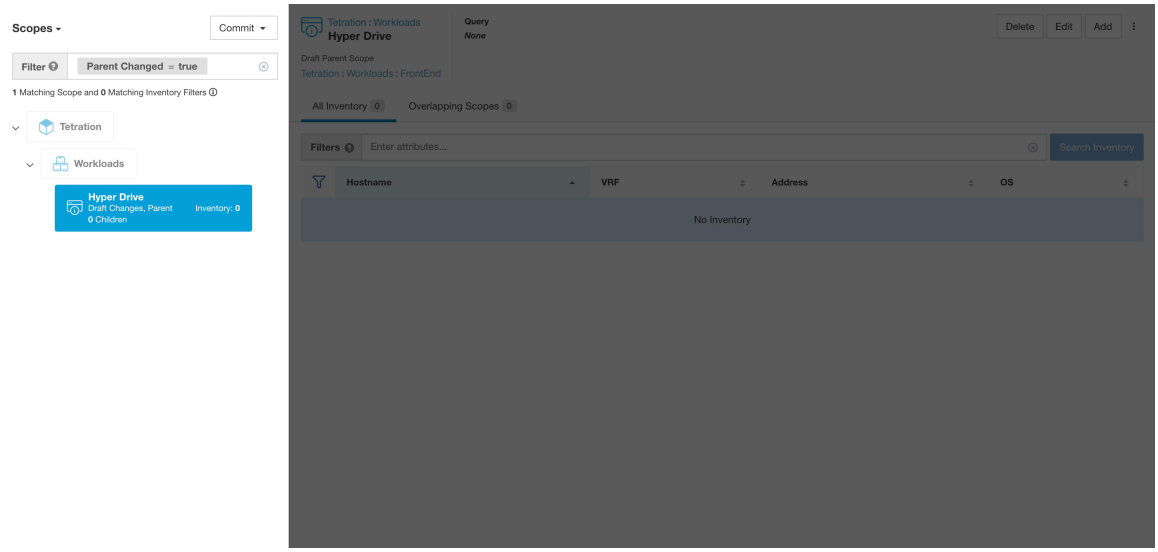


有关详细信息，请参阅范围重叠

父项更改 (Parent Change)

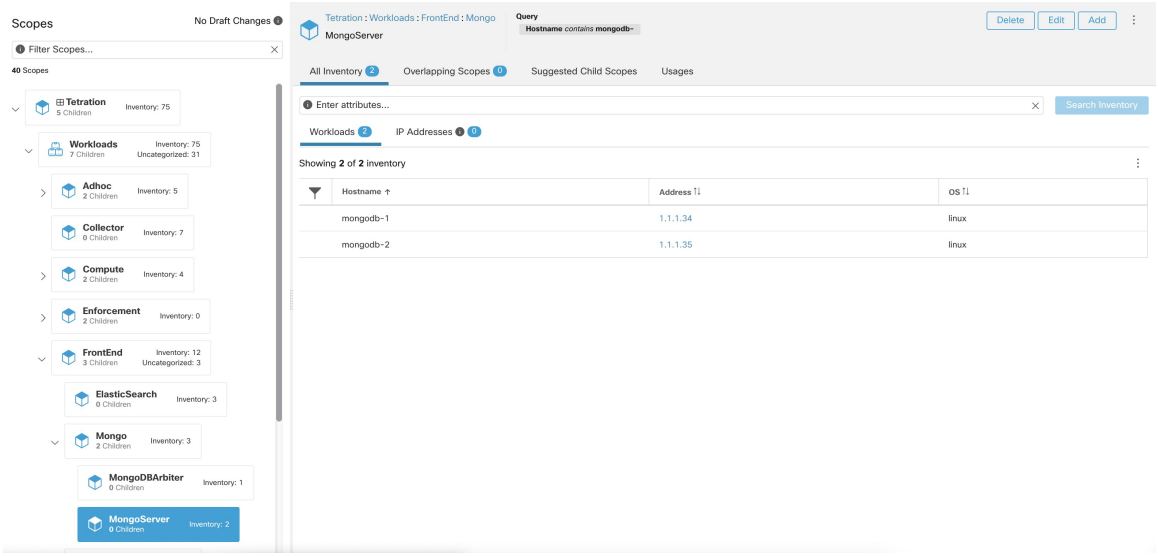
已在草稿中移动但尚未提交的范围。

Figure 8: 父项更改



完整范围查询

Figure 9: 范围层次结构示例



范围按层次结构定义，范围的完整查询定义为范围及其所有父范围的逻辑“and”。使用上面的示例，资产分配给 `Workloads:FrontEnd:Mongo`

范围将匹配：

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

其中，vrf_id = 676767 来自根范围查询，1.1.1.0/24 中的 ip 来自父范围查询。

Note 最佳实践是在同一级别没有重叠查询。这样就消除了排序的重要性，并减少了混乱。请参阅范围重叠

提供对范围的访问权限

您可以在范围上授予“读取”、“写入”、“执行”、“执行”和“所有者”功能。有关详细信息，请参阅《*Cisco Secure Workload* 用户指南》中的**角色**部分。

用户有权访问“子树”，即给定范围及其所有子项。通过使用前面的示例，您对 `Workloads:FrontEnd` 范围具有读取访问权限，通过继承，您将具有对 `Workloads:FrontEnd` 下所有范围的读取访问权限，包括：

- `Workloads:FrontEnd:Mongo`
- `Workloads:FrontEnd:ElasticSearch`
- `Workloads:FrontEnd:Redis`
- 等。。

可以定义具有多个范围访问权限的角色。例如，“Mongo 管理员”角色可能对范围具有所有者访问权限：

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

角色和功能允许您水平访问范围层次结构。

范围功能也会被继承。例如，对范围具有“写入”功能还让用户能够读取该信息。

查看范围

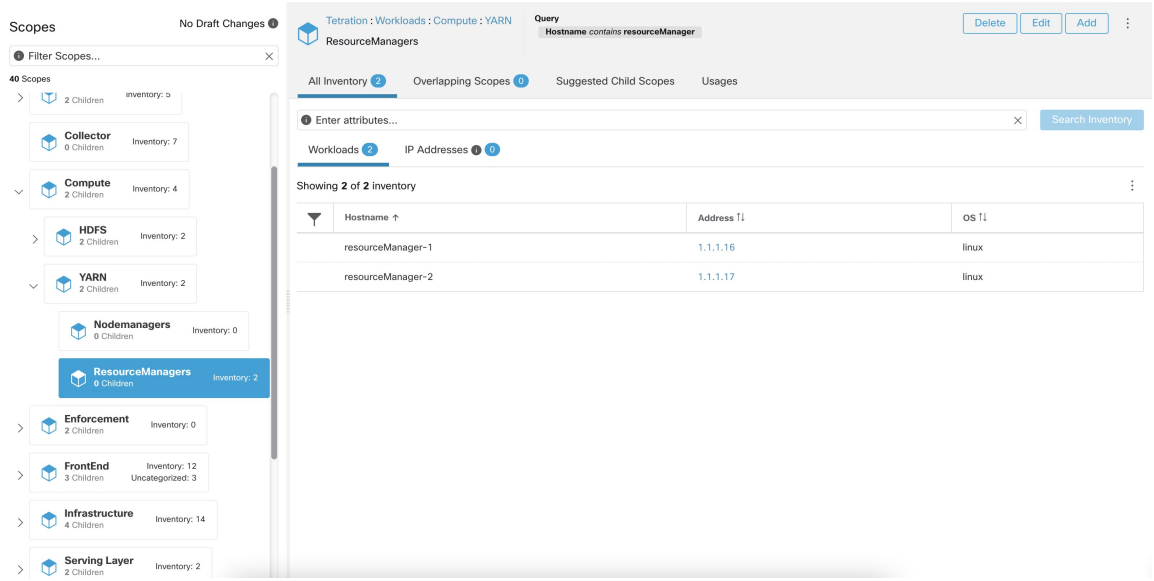
每位用户都可以查看他们有权访问的范围树。在根范围上拥有“所有者”权限的用户能够在该树中创建、编辑和删除范围。要访问此视图，请执行以下操作：

在左侧的导航栏中，点击**整理 (Organize)** > **范围和资产 (Scopes and Inventory)**。

您可以遍历自己有权访问的任何范围的完整范围层次结构（直至根）。这种完整的遍历提供了用户可以创建任何范围的策略的情景。在此页面上可执行多项操作：

- 点击范围层次结构中的 V 形图标可显示该范围的子项。
- 点击范围卡可更新右侧窗格，以便显示有关该范围的详细信息以及其所有资产的可过滤列表。

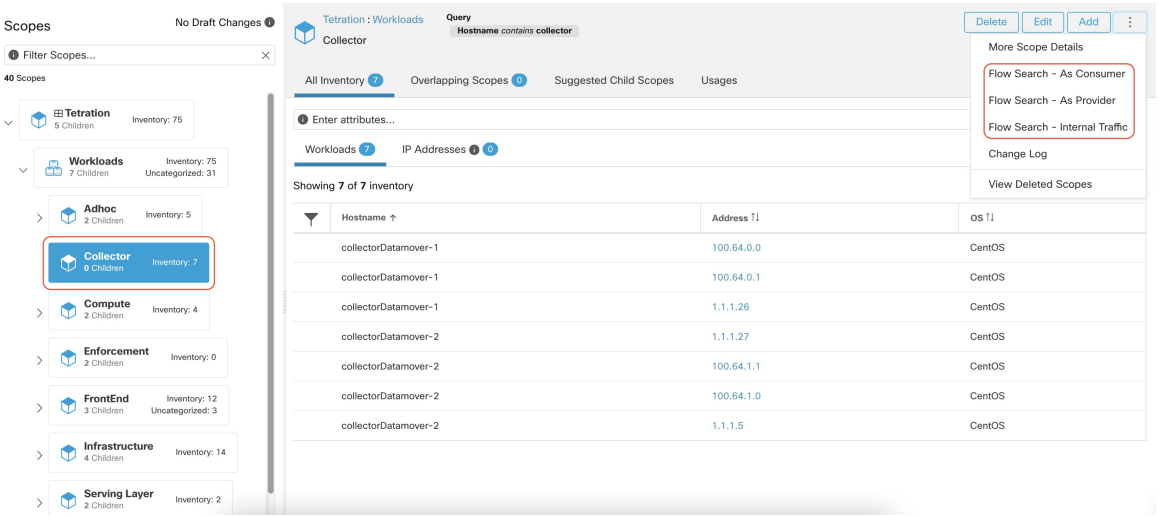
Figure 10: 非管理视图示例



搜索引用范围的流

“范围”(Scopes) 页面上提供了一些快捷方式，可帮助用户在需要搜索流的一个或两个终端都在提供的范围内的情况下搜索流。

Figure 11: 搜索范围的流



如上图所示，在范围树（左侧面板）中选择所需的范围后，用户可以在以下三个选项中进行选择：

1. 流搜索 - 作为使用者 *(Flow Search - As Consumer)* 提供流搜索页面的快捷方式，以帮助搜索选定范围为流的使用者范围的流。换句话说，流中的使用者或源终端属于所选的范围。
2. 流搜索 - 作为提供者 *(Flow Search - As Provider)* 提供流搜索页面的快捷方式，以帮助搜索选定范围为流的提供者范围的流。换句话说，流中的提供者或目标终端属于所选范围。

3. 流搜索 - 内部流量 *(Flow Search - Internal Traffic)* 提供流搜索页面的快捷方式，以帮助搜索完全限制在所选范围内的流。换句话说，流的两个终端（使用者和提供者）都属于所选范围。

创建新范围

子范围在**范围 (Scopes)** 管理页面上创建。此操作需要使用根范围上的 `SCOPE_OWNER` 功能。 **站点管理员**是所有范围的所有者。

创建子范围将影响父范围的应用资产成员身份（成员工作负载）。因此，父范围将被标记为具有“草稿更改”。这些更改需要提交，依赖结构也需要更新。请参阅确认更改。

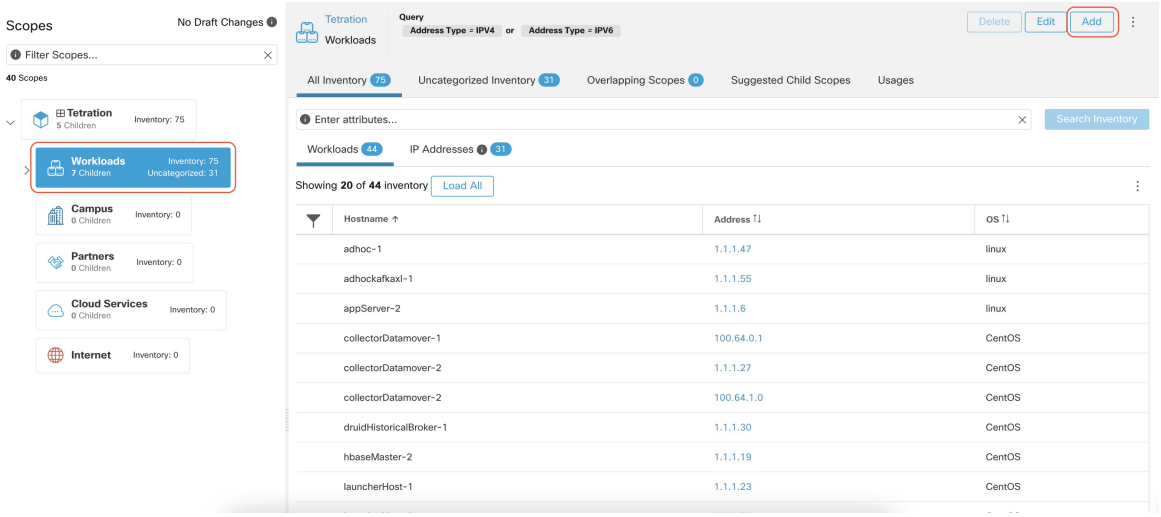
Procedure

步骤 1 在左侧的导航栏中，点击**整理 (Organize)** > **范围和资产 (Scopes and Inventory)**。该页面显示与系统中已创建的租户 + VRF 相对应的根范围。

步骤 2 在范围目录中选择一个子范围。如有必要，您可以先过滤范围。

步骤 3 点击**添加 (Add)** 按钮。

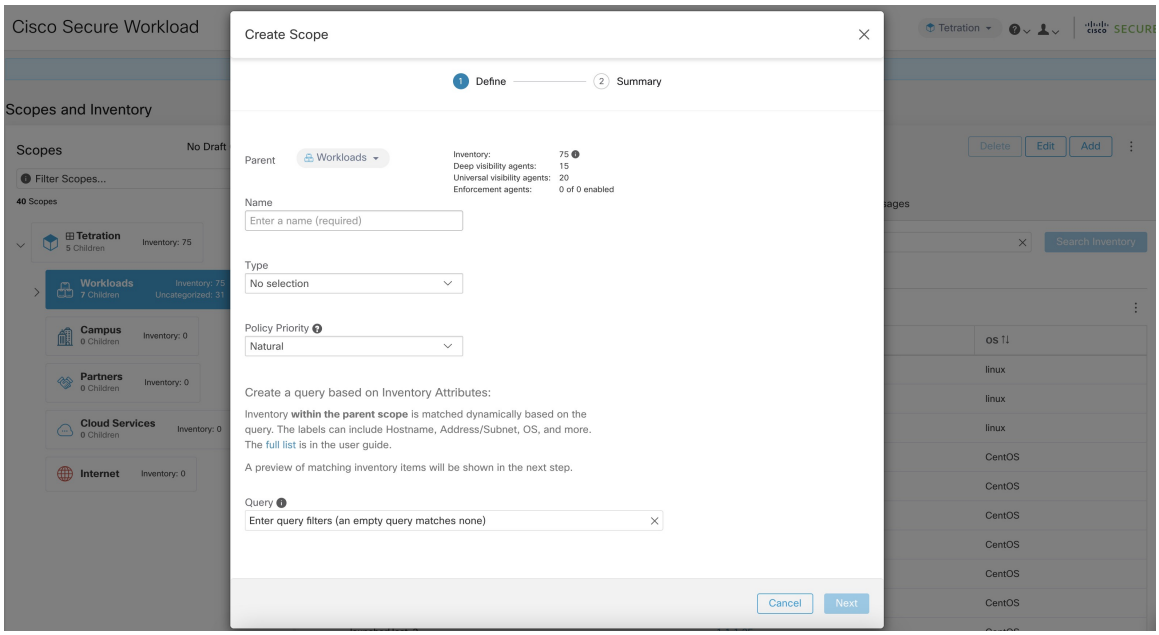
Figure 12: 范围添加按钮



步骤 4 在以下字段中输入适当的值：

字段	说明
父 (Parent)	新范围的父范围。
名称 (Name)	用于标识范围的名称。在父范围内必须是唯一的
类型 (Type)	选择新范围的类别。
查询 (Query)	查询/过滤器以匹配资产。

Figure 13: 范围创建模式

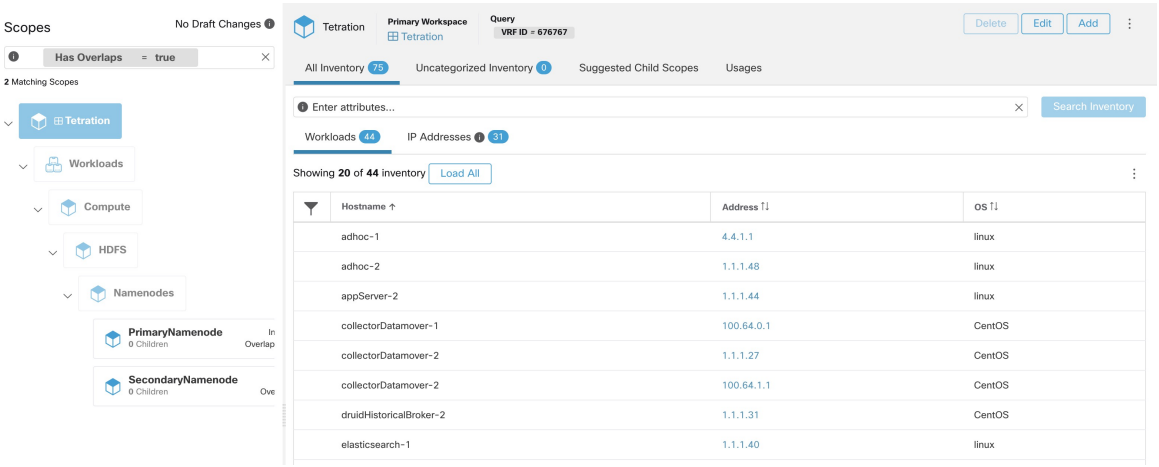


范围重叠

在添加范围时，建议避免范围重叠。当范围重叠时，为重叠范围生成的策略最终可能会让最终用户感到困惑。如果存在任何重叠的范围成员身份，即同一资产属于范围树中同一深度的多个范围（同级范围），则此功能会主动通知用户。目的是避免相同的工作负载存在于范围树的不同部分。

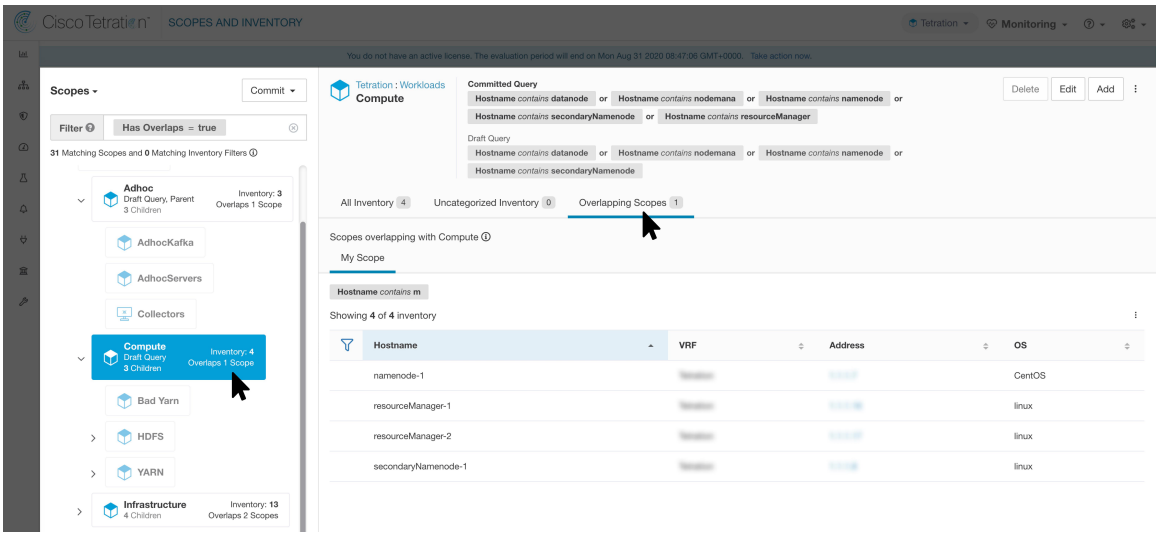
要查看属于多个范围的资产项目，请使用范围过滤器并输入 **Has Overlaps = true** 分面。

Figure 14: 范围过滤器中的重叠分面



通过向下遍历范围树并选择**重叠范围 (Overlapping Scopes)** 选项卡，可以查看重叠范围列表和相应的重叠 IP 地址。

Figure 15: 重叠范围和 *IP*



编辑范围

只有在根范围上具有 SCOPE_OWNER 功能的用户才能编辑范围。站点管理员是所有范围的所有者。

编辑范围名称

编辑范围名称会立即进行，根据需要更新的子范围的数量，可能需要几分钟时间。

Note 在更改范围名称时，按范围名称进行的流搜索将受到影响。

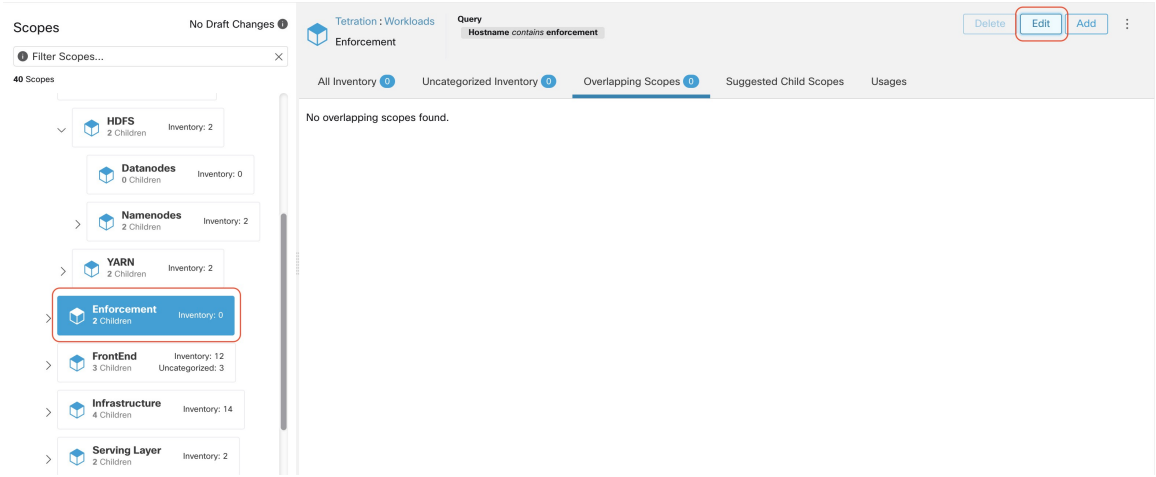
编辑范围查询

当范围的查询发生更改时，会影响直接父范围和子范围。这些范围被标记为具有“草稿更改”(draft changes)，表示已对树进行了尚未提交的更改。完成所有查询更新后，用户必须点击“范围目录”(Scope Directory) 上方的 **提交更改 (Commit Changes)** 按钮，使更改成为永久更改。这将触发后台任务，从而更新工作空间中的所有范围查询和“动态集群查询”。

Warning 更新范围查询可能会影响范围资产成员身份（作为范围成员的工作负载）。更改将在**提交更改**过程中生效。要降低风险，您可以比较成员身份更改，以便从查看范围/过滤器更改影响窗口进行进一步的影响分析。

将在相关主机上插入新的主机防火墙规则，并删除任何现有规则。

Figure 16: 编辑范围



要编辑范围，请执行以下操作：

Procedure

步骤 1 点击要编辑的相应范围上的**编辑按钮**。

步骤 2 编辑所选范围的名称或查询。

步骤 3 点击**查看查询更改影响 (Review query change impact)** 链接，比较新旧查询草稿之间的更改。

步骤 4 点击**保存 (Save)**。名称会立即更新。

步骤 5 要更新所有范围的查询，请点击**确认更改 (Commit Changes)** 按钮。

步骤 6 您将看到一个确认弹出窗口，其中说明了执行范围更改的后果。更新在后台任务中异步处理。

步骤 7 点击**保存 (Save)**。这可能需要一分钟或更长时间，具体取决于更改的数量。

Figure 17: 查看查询更改的影响

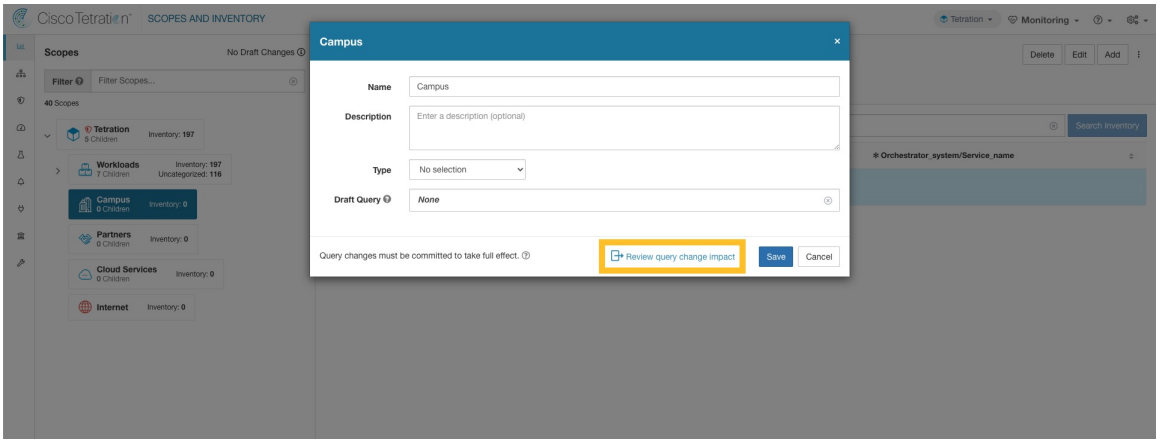
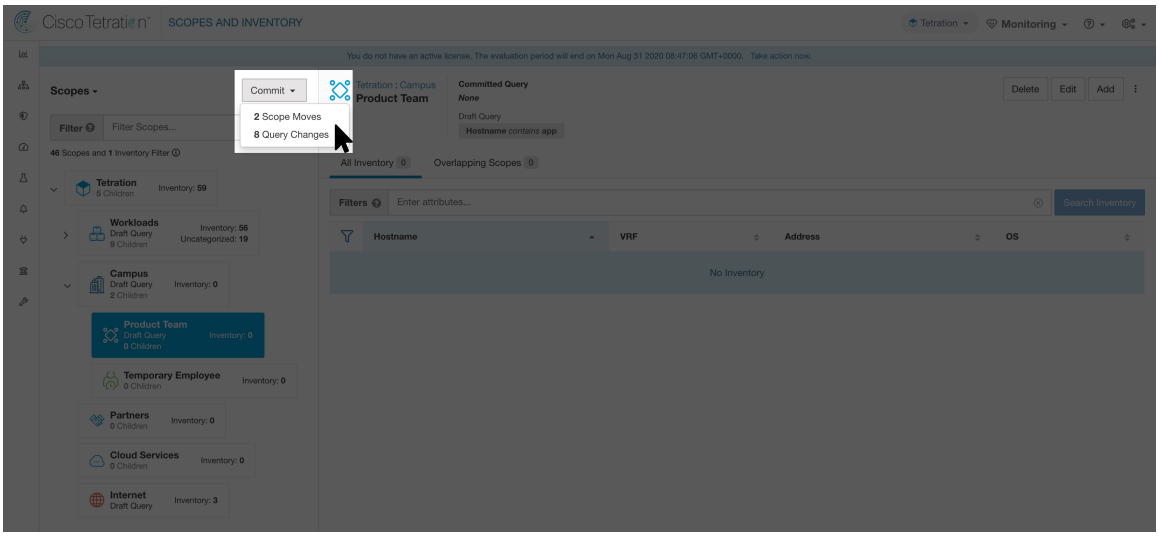


Figure 18: 确认更改



编辑父范围

当范围的父范围更新时，范围查询会更改。此更改会影响父范围和子范围的成员身份。与编辑范围查询类似，这些更改最初保存为“更改草稿”，除非提交，否则不会生效。用户可以在提交之前，点击“编辑范围”(Edit Scope) 模式窗 口上的“查看查询更改影响”(Review query change impact) 来验证此更改的影响。验证后，可以通过点击“提交”(Commit) 并接受“范围移动”和“查询更改”来提交更改。

要编辑父范围，请执行以下操作：

Procedure

步骤 1 点击要编辑的相应范围上的**编辑按钮**。

步骤 2 编辑所选范围的父项。

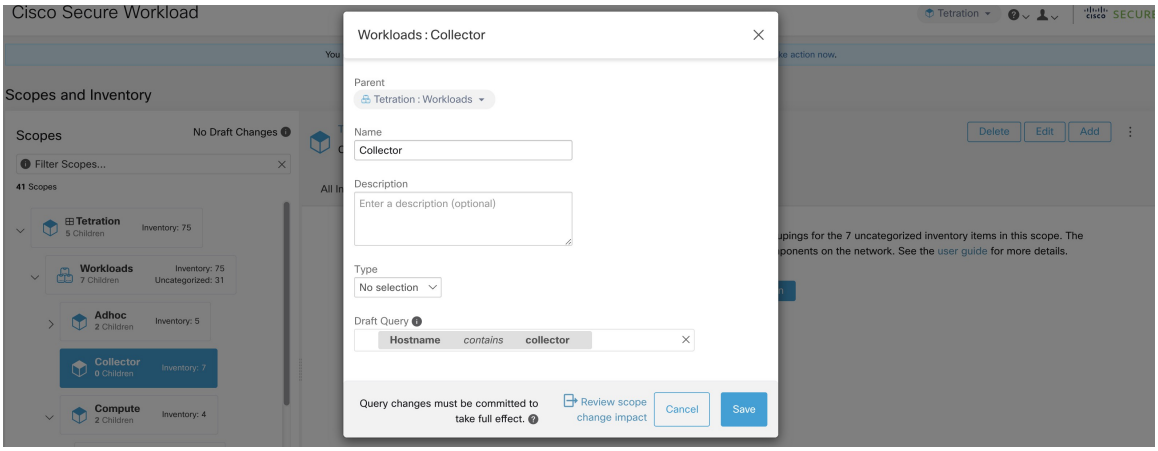
步骤 3 点击**查看查询更改影响 (Review query change impact)** 链接，以便比较新旧查询草稿之间的更改。

步骤 4 点击**保存 (Save)**。

步骤 5 点击“提交”(Commit) 并接受“范围移动”和“查询更改”。更新在后台任务中异步处理。

步骤 6 这可能需要一分钟或更长时间，具体取决于此更改影响的工作负载数量。

Figure 19: 将父范围从默认范围更改为默认： ***ProdHosts***



删除范围

仅当您具有根范围所有者权限时，才能删除范围。站点管理员是所有范围的所有者。

删除范围会影响父范围的应用资产成员资格（父范围成员的工作负载）。删除范围后，父范围的状态会更改为草稿更改。提交更改以及工作空间、策略和配置意图等依赖关系。有关详细信息，请参阅确认更改。

无法删除具有从属对象的范围。在以下情况下会显示错误消息：

- 为范围定义了工作空间。
- 将资产过滤器分配给范围。
- 存在使用范围定义其使用者或提供者的策略。
- 代理配置意图在范围中定义。
- 接口配置意图在范围中定义。
- 取证配置意图在范围中定义。

  有关查看范围/过滤器更改影响页面中范围依赖关系的详细信息，请点击**依赖关系 (Dependencies)**选项卡。请先删除冗余对象，然后再删除范围。

Note

- 删除没有任何子范围的范围。
- 要删除根范围，请先从**租户 (Tenants)** 页面中删除 VRF。

1. 从导航窗格中，点击**整理 (Organize)** > **范围和资产 (Scopes and Inventory)**。
2. 点击要查看其相应子**范围**的范围。

3. 选择要删除的子范围。
4. 点击**编辑 (Edit)** 和**添加 (Add)** 按钮旁边的**删除 (Delete)** 按钮。
5. 点击**查看范围更改影响 (Review Scope Change Impact)** 链接以在删除范围之前查看范围更改。
6. 点击**返回 (Back)** 关闭页面。

Figure 20: 删除范围

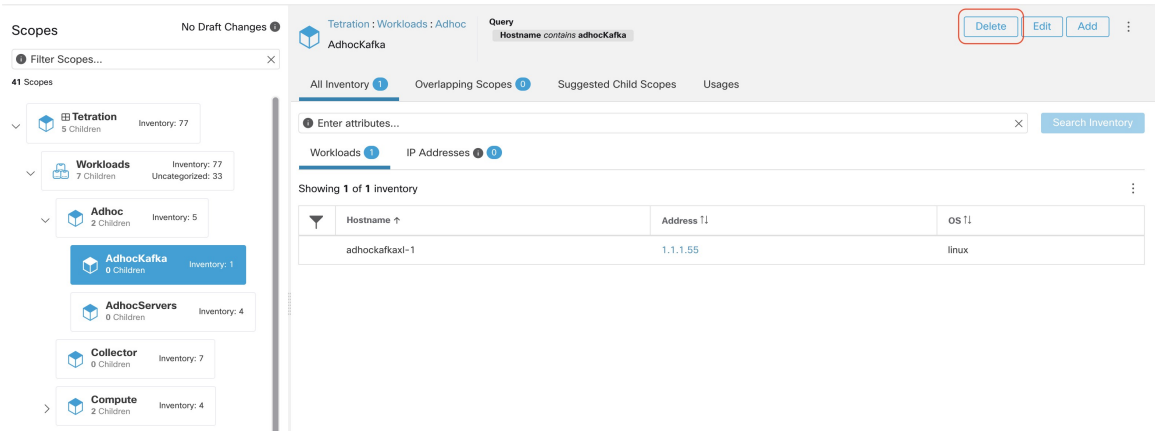
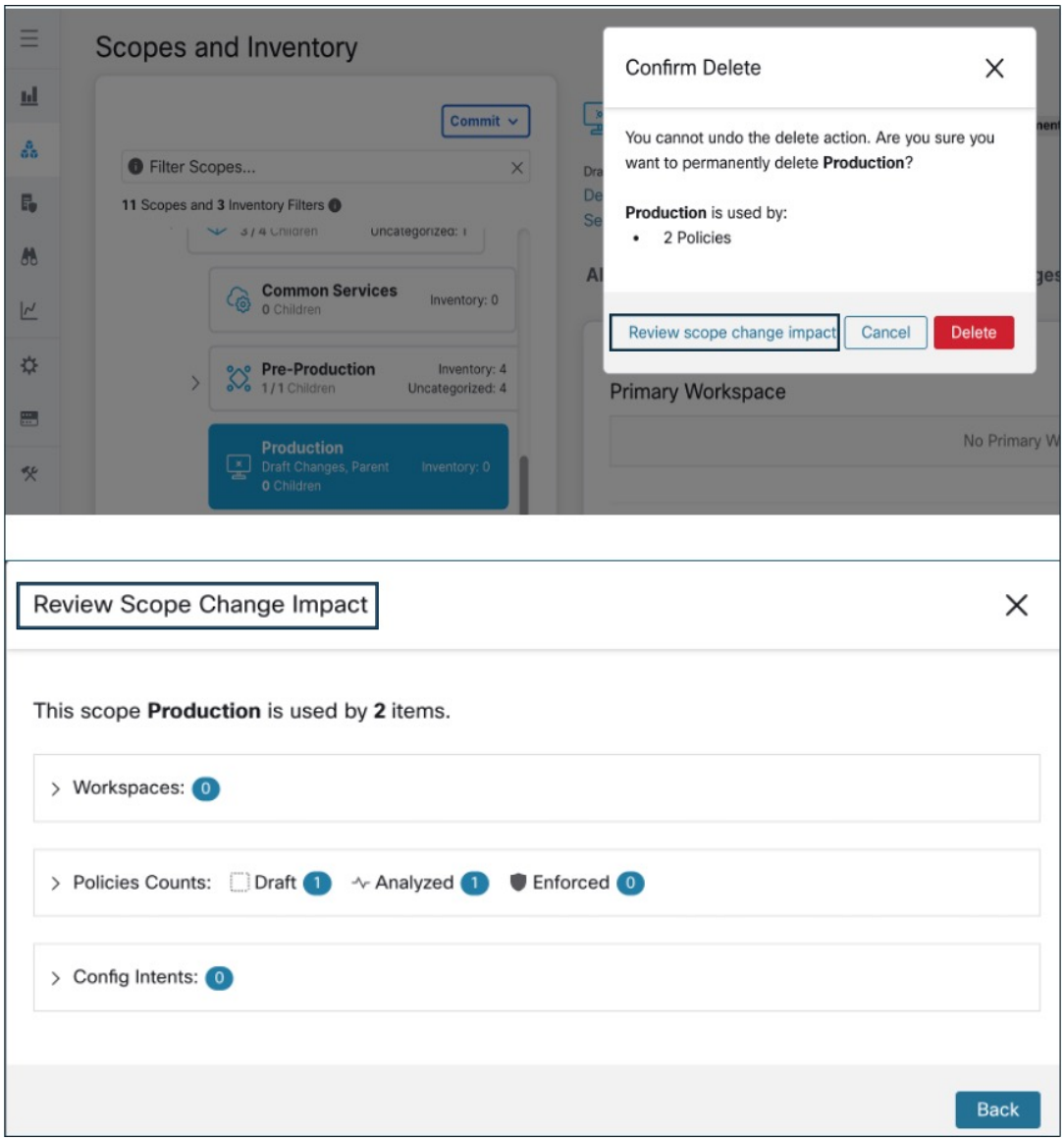


Figure 21: 删除范围



7. 点击**删除 (Delete)** 以删除范围。

重置范围树

如果存在上述任何配置，则必须先将其删除，然后才能重置范围树。在执行重置之前，重置按钮将不可用。

要重置范围树，请执行以下操作：

开始之前

您可以删除整个范围树并重新开始。

重置范围树会删除所有范围、标签、工作空间和收集规则。它不会删除任何注入的数据。

只有在根范围上具有 SCOPE_OWNER 功能的用户才能重置范围树。

但是，如果为范围树中的任何范围定义了以下内容，则无法重置范围树：

- 工作空间（使用向导创建范围树时创建的单个工作空间除外）
- 资产过滤器
- Policies
- 代理配置意图
- 接口配置意图
- 取证配置意图

过程

步骤 1 从左侧的导航菜单中，选择**整理 (Organize)** > **范围和资产 (Scopes and Inventory)**。

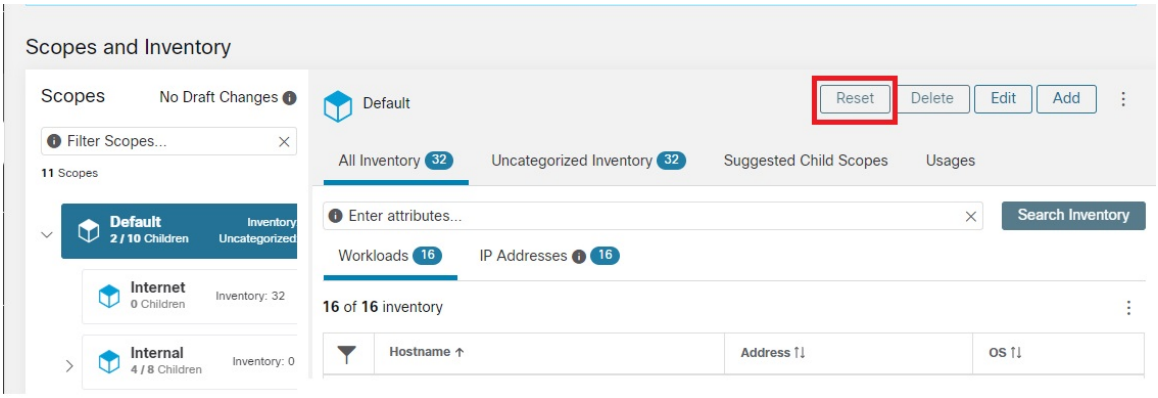
步骤 2 点击树顶部的范围。

步骤 3 点击**重置**。

步骤 4 确认您的选择。

步骤 5 如有必要，请刷新浏览器页面以继续。

图 *22:* 重置范围树



确认更改

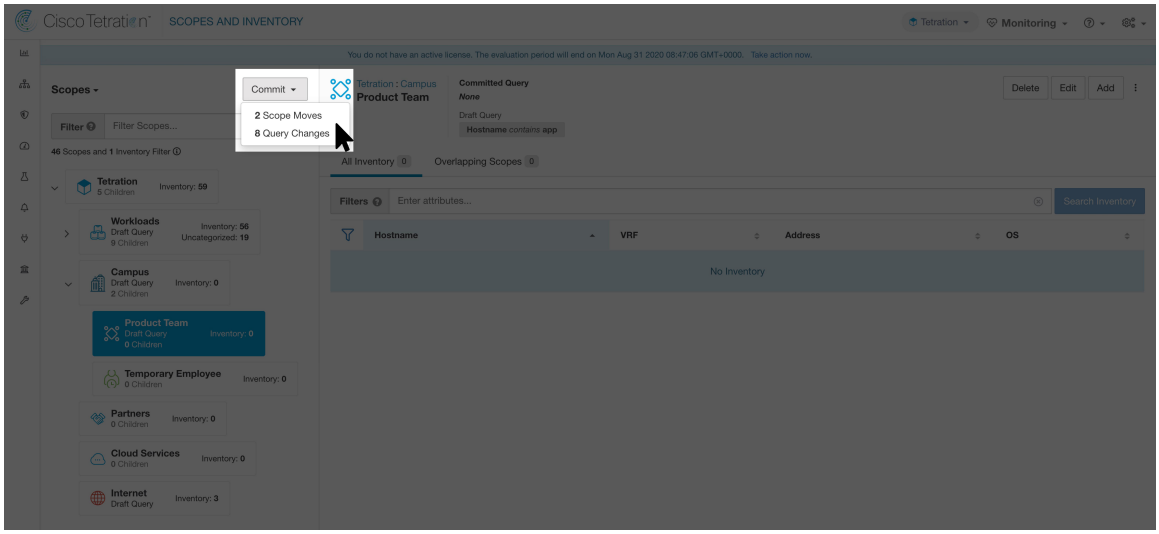
范围的应用资产查询定义是由其查询及其直接子范围的查询定义的。发生这种情况时，范围被标记为具有“草稿更改”，并且在运行**提交更改 (Commit Changes)** 后台任务之前，范围的查询、工作空间和集群不会更改。当范围处于草稿状态时，受影响的范围图标会显示警告三角形，并且“提交更改”(Commit Changes) 按钮显示在“范围”(Scopes) 页面（右上角）上，应点击该按钮以运行**提交更改 (Commit Changes)** 后台任务。

可将范围标记为草稿的事件：

- 查询更新
- 任何父项的查询都会被更新。
- 直接子项已被添加。
- 直接子项已删除。
- 直接子项的查询已被更新。

更改范围名称不会更改范围的草稿状态。

Figure 23: 确认更改



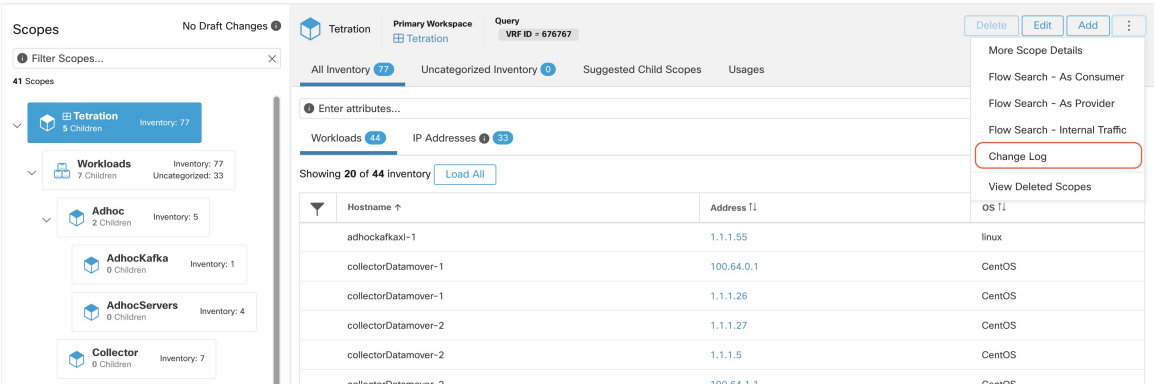
Note **提交更改**任务是一个异步任务。这通常需要几秒钟，但大型范围树可能需要几分钟。

Note 当根范围不再是草稿时，范围更新任务将完成。刷新页面以获取最新状态。

变更日志

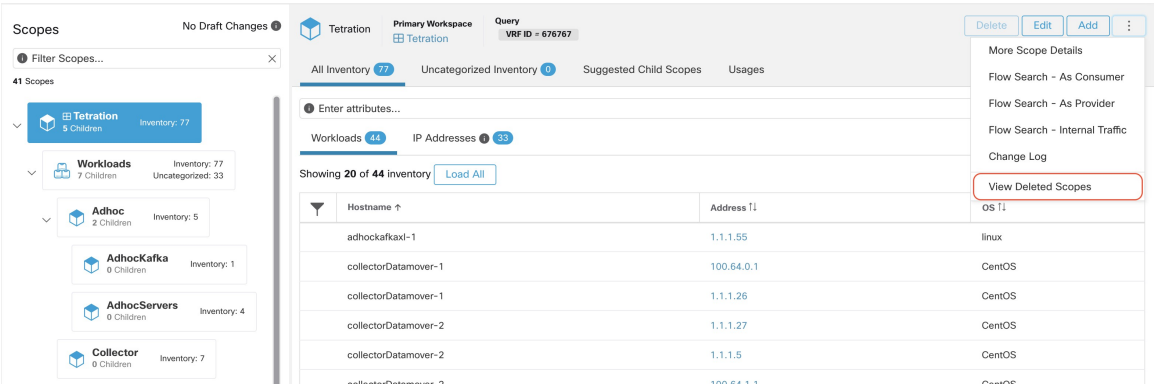
站点管理员和在根范围上具有 SCOPE_OWNER 功能的用户可以通过点击右上角的溢出菜单中的更改日志来查看每个范围的更改日志。

Figure 24: 变更日志



这些用户还可以通过点击右上角的溢出菜单中的**查看已删除范围 (View Deleted Scopes)** 链接来查看已删除范围的列表。

Figure 25: 查看已删除的范围



创建新租户

根级别范围映射到在租户下或通过**范围 (Scopes)** 管理页面创建的 VRF。此操作仅适用于**站点管理员**和**客户支持用户**。

Procedure

步骤 1 在左侧的导航栏中，点击**平台 (Platform)** > **租户 (Tenants)**。

步骤 2 点击**创建新租户 (Create New Tenant)**按钮。

步骤 3 在以下字段中输入适当的值：

字段	说明
名称 (Name)	用于标识范围的名称。在父范围内必须是唯一的。
说明 (Description)	可选说明。

步骤 4 点击**创建 (Create)** 按钮。

Figure 26: 创建租户

资产

要使用资产，请点击左侧导航栏中的**整理 (Organize)** > **范围和资产 (Scopes and Inventory)**。

资产搜索

在网络上检测到的所有资产均可搜索。要搜索资产，请使用**搜索资产 (Search Inventory)** 按钮。每个资产项目都可通过 IP 和 VRF 进行唯一标识，并可用于执行搜索。服务资产项目无法通过使用其 IP 地址来搜索。使用与服务关联的任何用户标签（例如 user_orchestrator_system/service_name）搜索服务资产。找到主机后，您就可以在主机配置文件页面上查看有关该主机的详细信息。

资产构建基块

1. 根范围
   - 给定租户下范围层次结构的根
   - 为 L3 地址域提供逻辑分隔
2. 范围
   - 动态查询定义的资产容器
   - 分层策略模型的基础
   - 策略、RBAC 和过滤器配置的锚点

3. 过滤
    - 基于动态资产查询的灵活构建
    - 意图定义、提供的服务和策略定义的锚点

Note 包括来自合作伙伴的所有 IP 地址以及在您的环境中通信的任何内容。无论它们是否具有代理，您都应通过标签来定义它们。

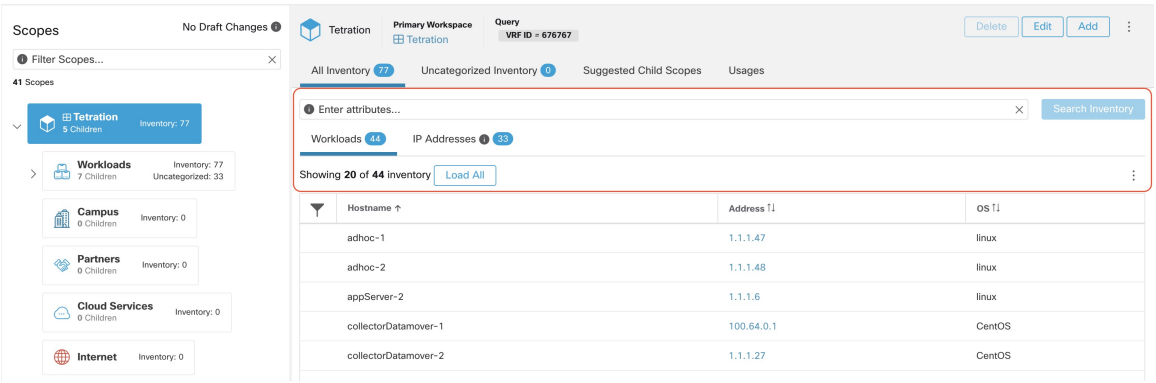
标签规划注意事项

1. 数据源
    - 网络 - IPAM？路由表？电子表格？
    - 主机 - CMDB、虚拟机监控程序、云、应用所有者？
2. 数据准确性
3. 数据的动态程度及其更新方式。
    - 手动上传？
    - API 集成？
4. 从基础开始，不断发展。
    - 使用网络标签来构建高级范围结构。
    - 使用主机标签在应用级别构建更详细的范围结构。

搜索资产

搜索资产会显示特定资产项目的信息。

Figure 27: 资产搜索



Procedure

步骤 1 从导航窗格中，选择**整理 (Organize)** > **范围和资产 (Scopes and Inventory)**。

步骤 2 在**过滤器 (Filters)** 字段中输入您要查找的资产项目的属性。属性包括以下内容：

属性	说明
主机名	输入完整或部分主机名。
VRF 名称	输入 VRF 名称。
VRF ID	输入 VRF ID（数字）。
地址	输入有效的 IP 地址（IPv4 或 IPv6）。
地址类型	输入 IPv4 或 IPv6。
操作系统	输入操作系统名称（例如 CentOS）。
OS 版本	输入操作系统版本（例如 6.5）。
接口名称	输入接口名称（例如 eth0）。
MAC	请输入 MAC 地址。
在收集规则中？	输入 true 或 false。
进程命令行	输入在主机上运行的命令的子字符串（注意：此分面不能保存为资产过滤器的一部分）。
进程二进制文件散列	输入在主机上运行的命令的进程散列（注意：此分面不能保存为资产过滤器的一部分）。
软件包信息	输入软件包名称（可选），然后输入软件包版本（前缀为 #）。
软件包 **CVE**	输入部分或完整的 CVE ID。
CVE 评分 v2	输入 CVSSv2（通用漏洞评分系统）评分（数字）。
CVE 评分 v3	输入 CVSSv3（通用漏洞评分系统）评分（数字）。
思科安全风险评分	输入思科安全风险评分（数字）。
严重性（思科安全风险评分）	输入思科安全风险评分严重性：“高”(High)、“中”(Medium) 或“低”(Low)。

属性	说明
活动互联网漏洞（思科安全风险评分）	指明CVE是否是跨组织的活动互联网漏洞活动的一部分。输入 true 或 false。
易被利用（思科安全风险评分）	指明CVE是否具有已知的漏洞攻击包。输入true或 false。
可用修复（思科安全风险评分）	指明是否有可用于 CVE 的修复程序。输入 true 或 false。
可被恶意软件利用（思科安全风险评分）	指明CVE是否会被恶意软件（包括特洛伊木马、蠕虫、勒索软件等）主动利用。输入 true 或 false。
热门目标（思科安全风险评分）	指明其他思科漏洞管理客户端是否检测到大量CVE。输入 true 或 false。
预测可利用（思科安全风险评分）	指明CVE未来是否预计会存在活动互联网漏洞。输入 true 或 false。
用户标签	带有来自用户标签的前缀的属性。

步骤 3 点击**搜索资产 (Search Inventory)**。结果显示在**过滤器 (Filters)** 字段下方，该字段分为四个选项卡。每个选项卡显示一个包含相关列的表。点击表格标题的漏斗图标可显示其他列。如果有任何用户标签，则会带有前缀，并可在此处进行切换。

Figure 28: 资产搜索结果

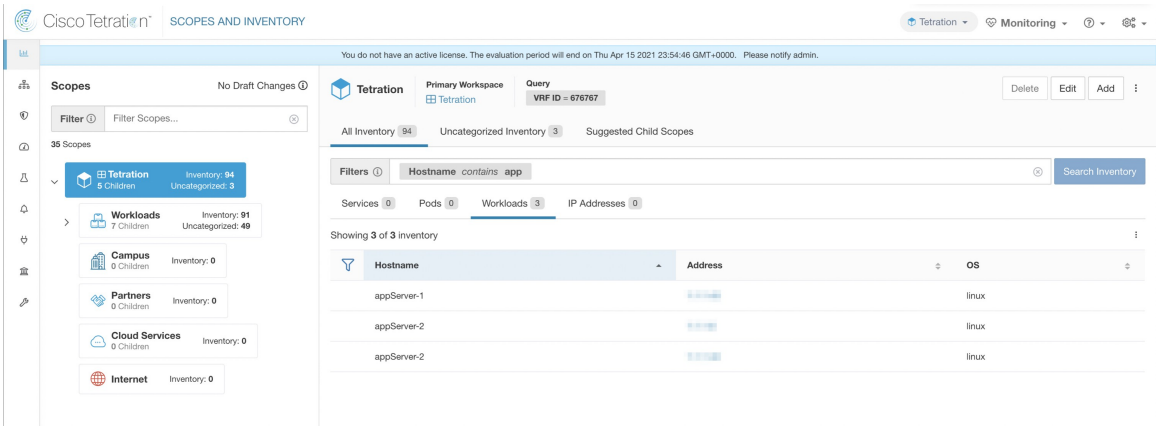
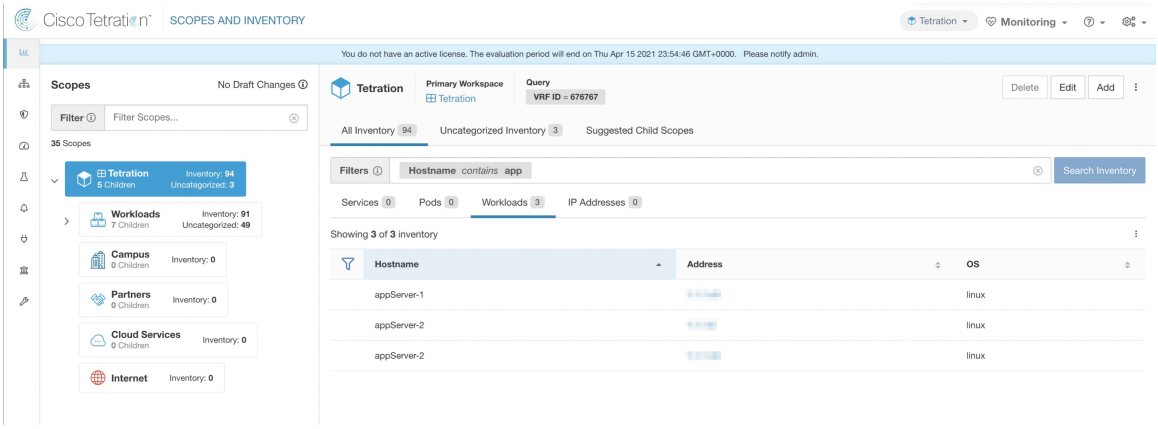


Figure 29: 资产搜索结果



搜索结果分为四个选项卡：

选项卡	说明
服务 (Services)	列出通过外部协调器发现的 Kubernetes 服务和负载均衡器。除非配置了相关的外部协调器，否则此选项卡会隐藏。
Pod	列出 Kubernetes Pod。除非配置了相关的外部协调器，否则此选项卡会隐藏。
工作负载 (Workloads)	列出 Cisco Secure Workload 代理报告的资产项目。

每个选项卡旁边还会提及库存计数。搜索中立即可用的信息包括主机名、IP 地址及子网、操作系统、操作系统版本、服务名称和 Pod 名称。可以通过点击表标题中的漏斗图标来切换显示的列的列表。搜索结果仅限于范围目录中显示的当前选定范围。点击搜索结果中的项目，可在相应的配置文件页面上看到更多信息。

工作负载配置文件 (Workload Profile) 中显示了有关每个主机的更多详细信息，可通过点击搜索结果行的 IP 地址字段进行访问。有关详细信息，请参阅适用的工作负载。

要通过边栏创建资产过滤器，请执行以下操作：从顶级菜单中选择**整理 (Organize)** > **资产过滤器 (Inventory Filters)**。点击**创建过滤器 (Create Filter)** 按钮。系统将显示一个模式对话框，您可以在其中命名已保存的过滤器。

建议子范围

“建议子范围”是一种使用机器学习算法（如网络中的社群检测）来发现可作为范围的分组的工具。在构建范围层次结构时，该工具很有帮助，有助于为给定的范围定义更精细的子范围。候选子范围会以建议的形式显示，然后可以选择并添加。

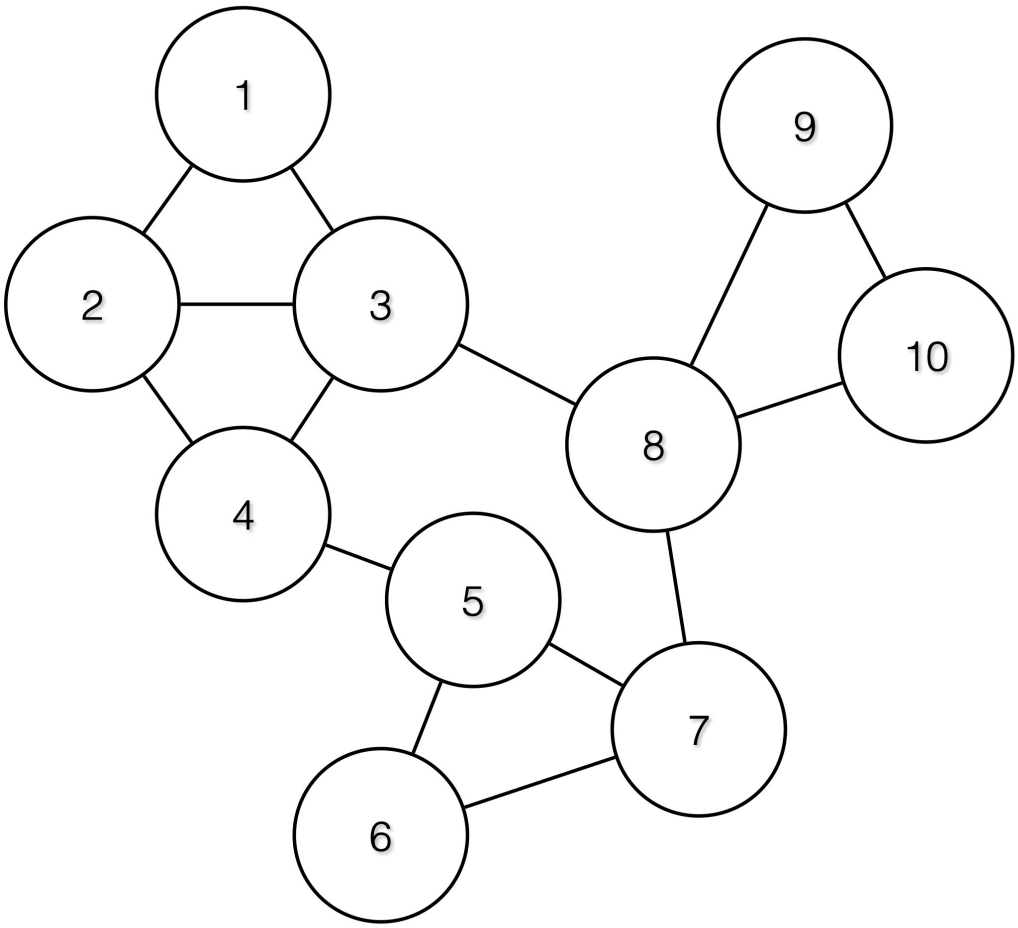
算法说明：首先创建一个基于父范围中未被认领的成员之间通信的图（注意：未被认领的成员指那些不属于父范围的任何子范围的成员），然后对图进行预处理，例如，算法会尝试识别与图中比例

足够高的其他终端进行通信的终端。如果找到这样的一组终端，则会作为候选**通用服务**分组向用户显示。处理该图的其余部分以检测行为类似于**社区**的组，这大致意味着终端之间的通信频率（或在更多提供者端口上）要比与该组外部的终端通信的频率更高。每个这样的分组可以对应于组织内的一个应用或一个部门。此类分区还可能导致范围之间的策略更稀疏。

示例：

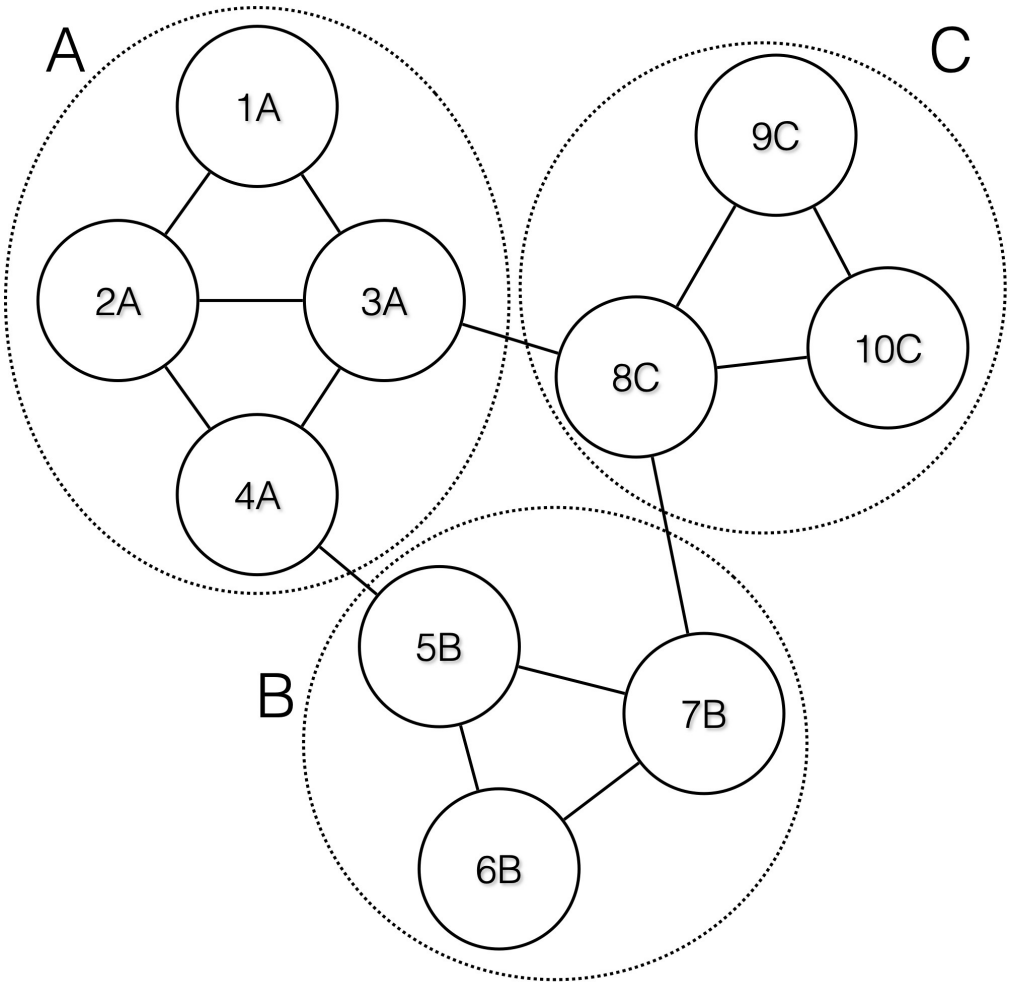
将 1 至 10 设为单个终端 IP。假设输入（通信）图如下：

Figure 30: 输入图



然后，终端 1-4、5-7 和 8-10 将被分组在一起，因为它们彼此之间的通信程度（边缘数量）相对较高，而与其他终端的通信相对较少。

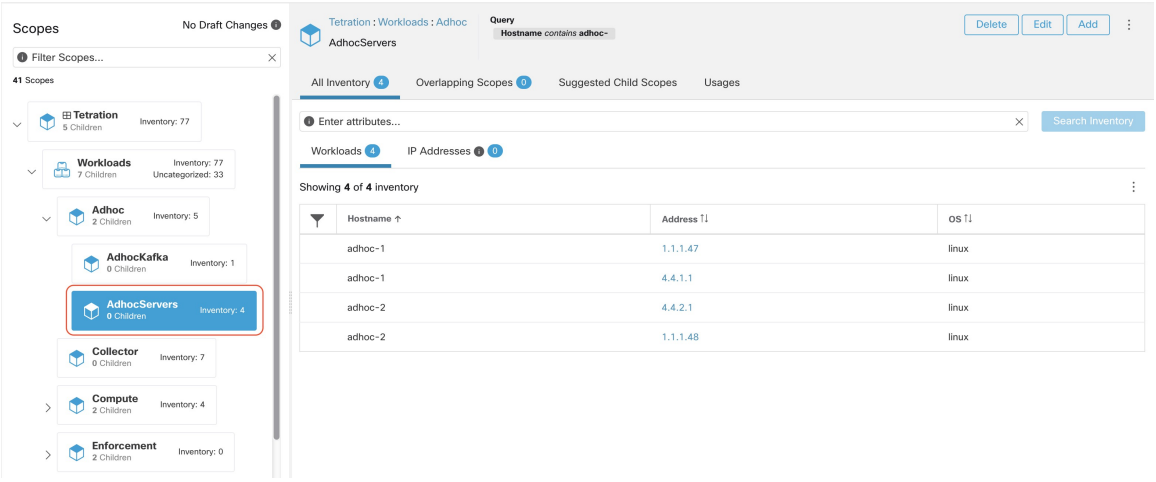
Figure 31: 输出组



执行范围建议的步骤

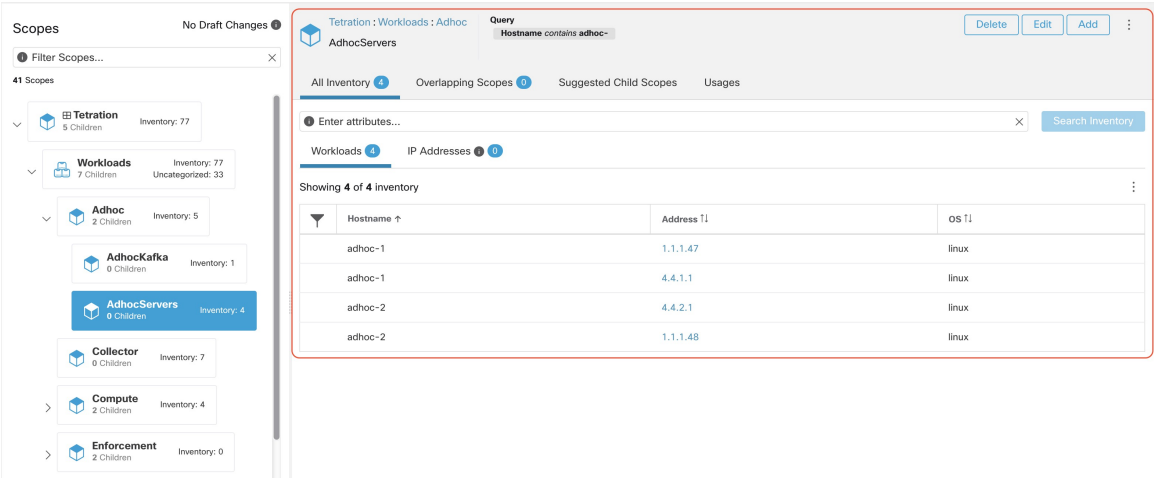
要为所需范围调用范围建议，用户应在范围页面上找到并将其选中。

Figure 32: 选择范围



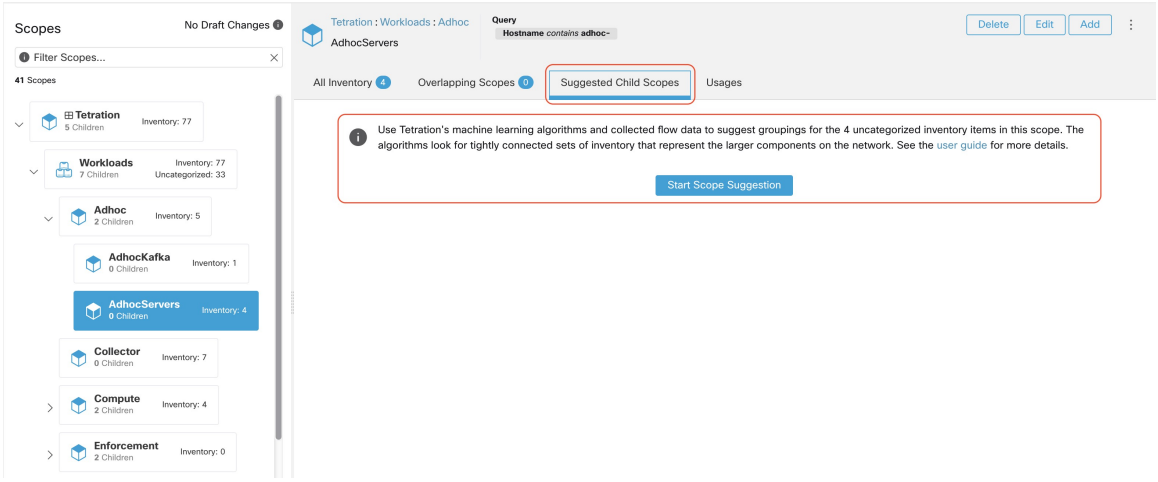
在窗口中，用户可以浏览资产、未分类的资产项目，即属于当前所选范围但不属于当前所选范围的任何子范围的项目。点击**未分类的资产项目**可查看此列表。

Figure 33: “范围” ***(Scope)*** 窗口



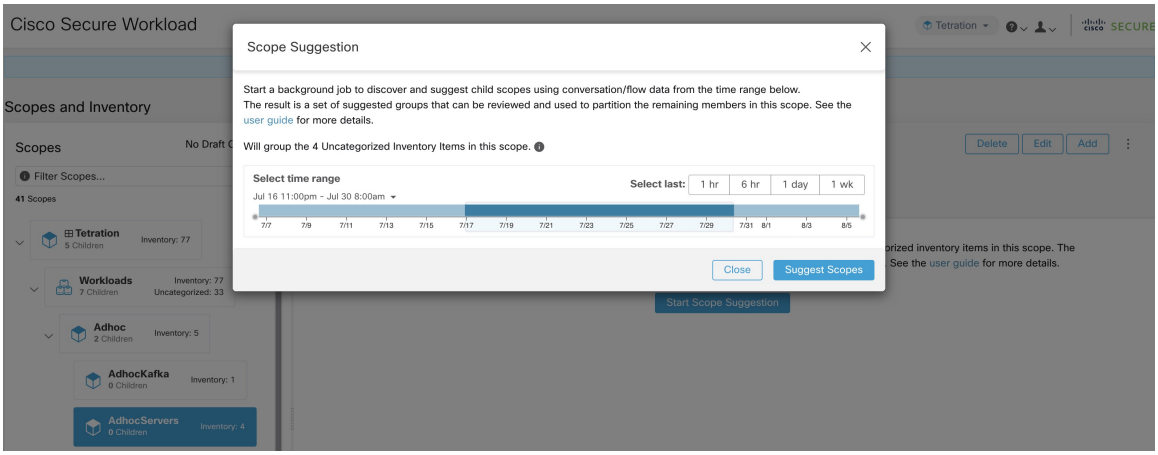
选择范围后，用户可以点击**建议子范围 (Suggest Child Scopes)**，然后点击**启动范围建议 (Start Scope Suggestion)**（或点击重新运行，以防这并非第一次）。请注意，范围建议运行的输入将是未分类的资产项目。

Figure 34: 子范围



用户可以将日期范围设置为范围建议的输入，然后点击**建议范围 (Suggest Scopes)**。在中等整体负载下，范围建议运行速度通常很快，并且只需几分钟即可处理十到数千个终端以及数万个对话。

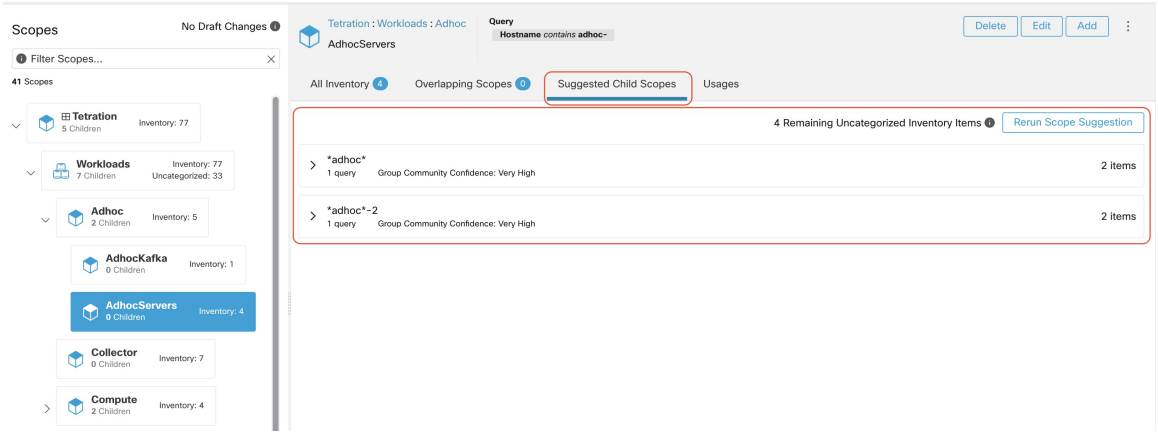
Figure 35: 范围建议数据范围选择器



输出以候选项列表的形式向用户显示，当前最多20个组（如图所示），每个组都附带组可信度（质量）、候选项范围名称和查询等信息。每个已发现的组都有一个关联的**组社区可信度**，可能的值包括：**非常高 (Very High)**、**高 (High)**、**中 (Medium)** 和**低 (Low)**。这是对组的**社区 (Community)** 属性的度量：可信度越高，给定的一组终端的社区属性越高（组内部的边缘很多，外部的边缘相对较少）。目前，系统根据“组社区可信度”(Group Community Confidence) 选择要显示的组子集。发现的组当前可以属于以下四种组类型之一：

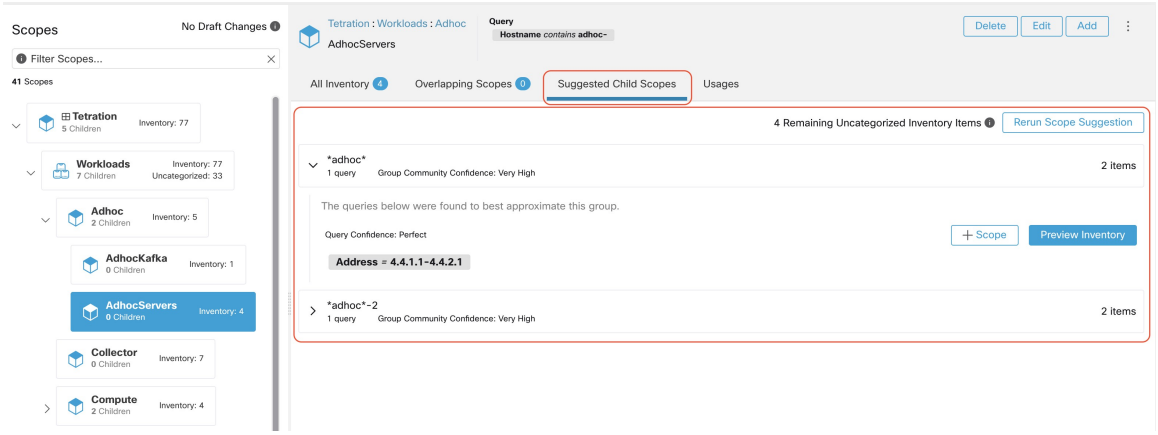
- **通用组**：基于社区属性通过机器学习发现的任何组。请注意，任何未明确指定以下特殊类型的组均为通用组。
- **通用服务**：此组包含与大部分输入资产进行通信的终端。这些终端可能正在运行某种共享服务。
- **公共服务客户端**：此组包含仅与**公共服务**组通信的终端。
- **未分组**：此组包含因通信不足而无法分组的终端。

Figure 36: 范围建议输出



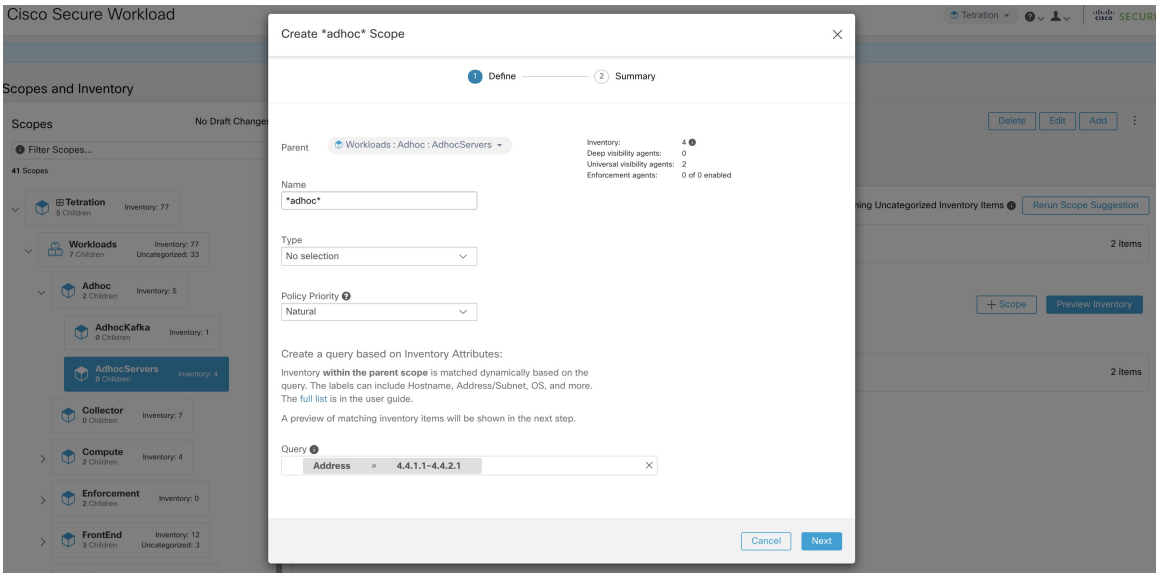
用户可以点击已发现的组，以便查看为所选组生成的查询列表。用户可以预览查询所涵盖的资产，这将严格定义所发现的组。查询内容包括 IP 范围、子网、主机名和用户上传的标签。有一个与每个组关联的可信度度量，称为**查询可信度**，它可以具有以下值范围中的一个：**完美 (Perfect)**、**非常高 (Very High)**、**高 (High)**、**中 (Medium)** 和**低 (Low)**。在生成查询时，首先通过图处理和机器学习发现组别，然后为每个组别生成查询。**查询可信度**用于衡量查询覆盖终端的程度。查询可信度为**完美**表示查询完全涵盖建议的（已发现）组。另一方面，**低**查询可信度表示查询明显错过准确捕获建议的组，这意味着查询涵盖许多**额外 IP**（不属于已发现的组）和/或具有许多**缺失 IP**（不在查询范围内）。

Figure 37: 范围建议输出查询



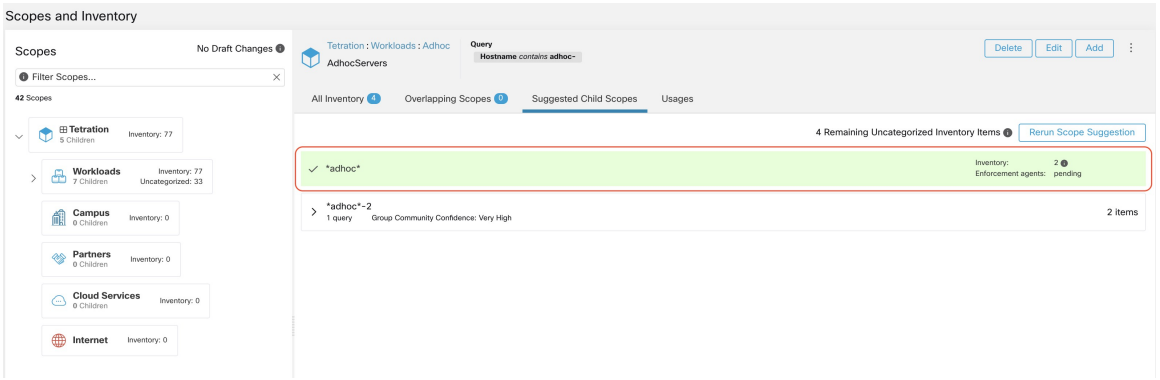
用户可以点击 **+ 范围 (+ Scope)** 按钮，这会将用户带到编辑窗口，用户可以在其中编辑组名称和组查询。用户可以检查查询及其匹配的 IP，并通过调整查询决定是否需要添加或删除某些 IP。满足要求后，用户可以点击**下一步 (Next)**，以查看该组并将其转换为草稿视图画布上的范围。

Figure 38: 范围建议编辑窗口



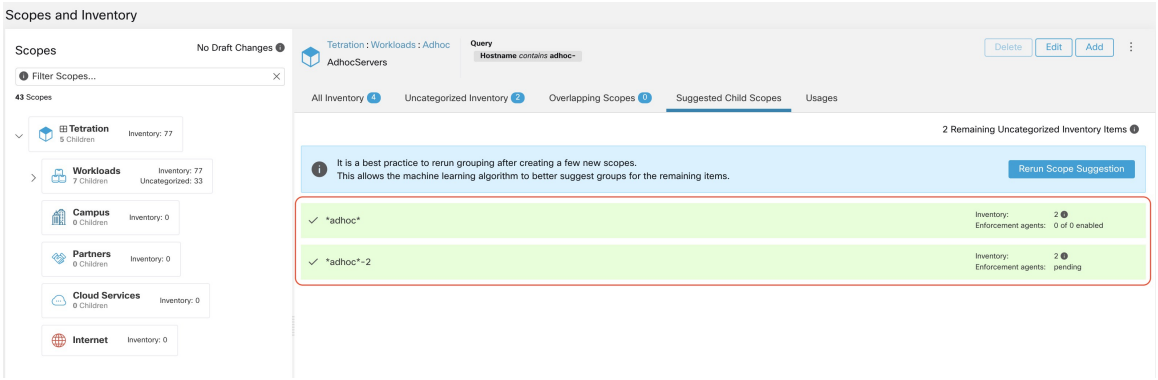
在用户将建议的组转换为范围后，组槽位会变为绿色，并且**未分类的资产项目**计数会减少。

Figure 39: 将一个建议组转换为范围后的范围建议输出示例



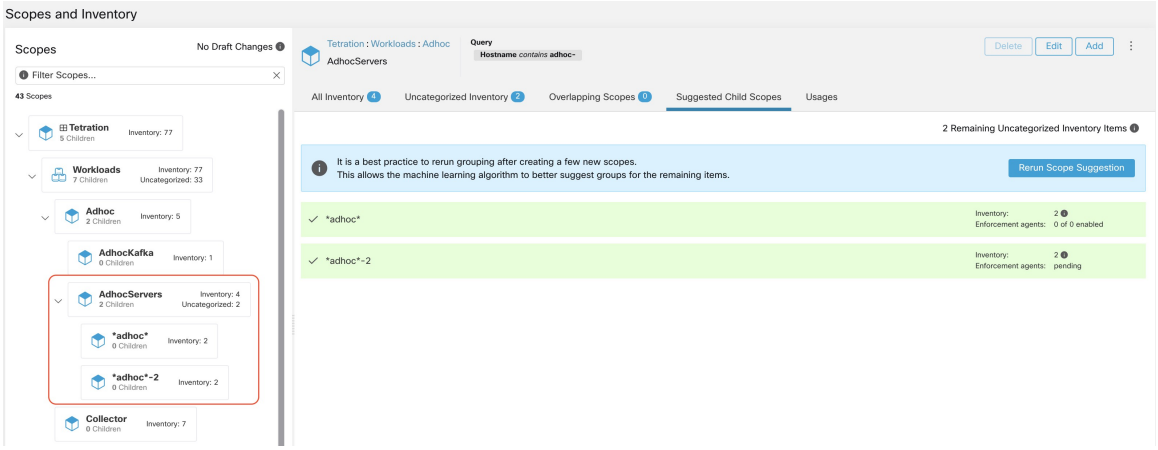
用户可以从剩余的组列表中重复创建范围的过程。用户可以从剩余的组列表中重复创建范围的过程。建议的工作流程是创建一个或多个范围，然后重新运行**范围建议**。 **未分类资产项目**的计数为零表示没有剩余要进一步确定范围（用于当前选定的父范围）的资产。

Figure 40: 多个范围创建的范围建议输出



在范围创建过程结束后（未分类计数为 0），用户可以在新创建的子范围上重复此过程，以便根据需要生成更深的范围树。

Figure 41: 初始范围建议和创建后的范围列表



Note 还有一种可能是，范围中未分类的项目无法很好地划分（例如，没有形成社区）。在这种情况下，算法可能不会返回任何分组（空结果）。

过滤器

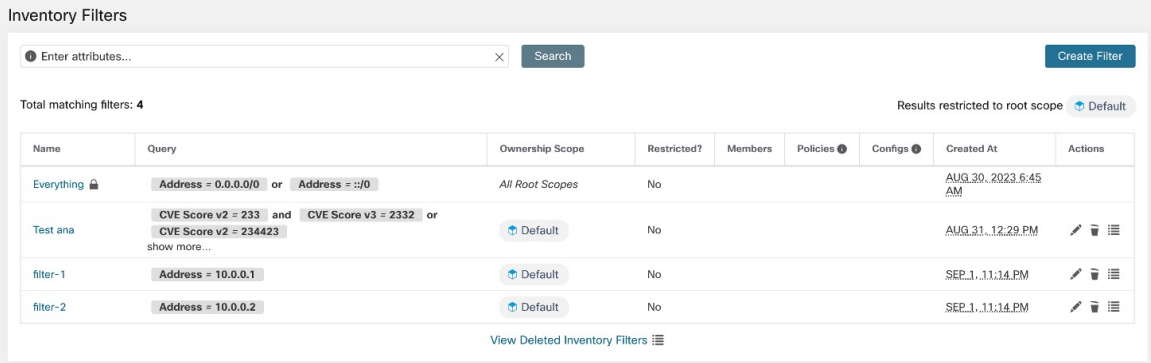
过滤器是保存的资产搜索，用于定义策略、配置意图等。避免任何与范围相关联的过滤器，该范围定义了过滤器的所有权范围。

要查看现有过滤器，请点击导航栏上的**整理 (Organize)** > **资产过滤器 (Inventory Filters)**。您还可以查看特定于任何范围的任何工作空间的资产过滤器。

会根据当前所选范围的根对过滤器列表加以限制。

过滤器还会显示成员的数量、它所涉及的策略数量以及草稿分析和执行策略的总和。

Figure 42: 资产过滤器



您可以通过访问查看范围/过滤器更改影响 窗口来查看与所选父范围相关的资产成员身份更改。

创建资产过滤器

创建资产过滤器，以便：

- 创建或发现特定于范围内工作负载子集的策略。

  例如，在范围内创建一组 API 服务器，这些服务器必须可通过 API 接口访问。创建策略以便仅允许经许可的流量，而阻止访问该应用的所有其他工作负载。

- 为跨多个范围的工作负载创建策略。

  例如，要创建一个适用于网络上运行特定操作系统的所有工作负载的策略，可创建一个跨越多个或所有范围的资产过滤器。

提示 要将现有集群转换为资产过滤器，请参阅将集群转换为资产过滤器。

过程

步骤 1 导航至以下位置之一：

- 依次选择**整理 (Organize)** > **资产过滤器 (Inventory Filters)**。
- 导航至范围中要为其创建资产过滤器的任何工作空间，然后点击**管理策略 (Manage Policies)** > **过滤器 (Filters)** > **资产过滤器 (Inventory Filters)**。

步骤 2 点击**创建过滤器 (Create Filter)** 或**添加资产过滤器 (Add Inventory Filter)**。

步骤 3 添加名称、说明和查询，其中包括所有且仅包含要包含在过滤器中的工作负载。

步骤 4 点击**显示高级选项 (Show Advanced Options)**。

步骤 5 指定过滤器的范围。

- 要修改过滤器，您必须拥有对指定范围或其任何祖先的写入权限。
- （取决于此程序中的其他设置）过滤器中包含的工作负载。

步骤 6 配置选项：

要想	相应操作
包括符合过滤器查询条件的工作负载，无论它们是否属于此过滤器中指定的范围。	取消选择**将查询限制为所有权范围 (Restrict Query to Ownership Scope)**
仅包括属于此过滤器中指定范围成员的工作负载。	选择**将查询限制为所有权范围 (Restrict query to ownership scope)**。
允许自动发现策略，针对此过滤器定义的工作负载集提出策略建议。 这些工作负载必须是过滤器中指定范围的子集。	选择**将查询限制为所有权范围 (Restrict Query to Ownership Scope)**和**提供超出其范围的服务 (Provides a Service External of its Scope)**。 要使用此过滤器，必须配置外部依赖关系。 有关详细信息，请参阅微调工作空间的外部依赖关系。

步骤 7 点击**下一步 (Next)**。

步骤 8 查看详细信息，然后点击**创建 (Create)**。

查看过滤器更改影响

在修改过滤器之前，请注意，对过滤器的更改将修改成员身份，并影响现有查询、资产和依赖关系，例如过滤器、范围、策略和基于该标签的强制行为。

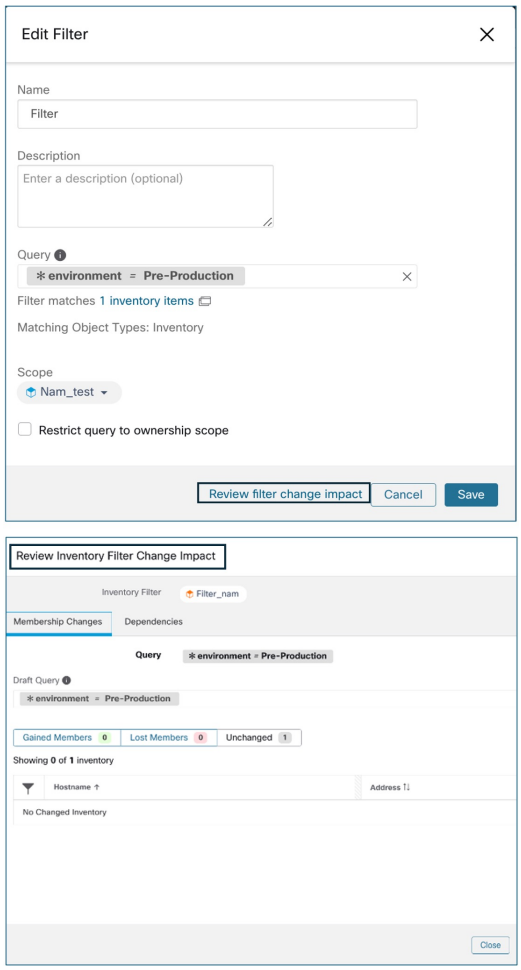
过程

步骤 1 在**资产过滤器 (Inventory Filter)** 页面的**操作 (Actions)** 选项卡下，点击**编辑**（铅笔）图标。

步骤 2 在**编辑过滤器 (Edit Filter)** 页面上，在进行任何更改之前，请点击**查看过滤器更改影响 (Review filter change impact)** 以查看资产过滤器。

步骤 3 在**查看资产过滤器更改影响 (Review Inventory Filter Change Impact)** 页面上，查看**成员身份更改 (Membership Changes)** 和**依赖关系 (Dependencies)** 选项卡下的策略和配置意图过滤器。

图 *43:* 编辑过滤器



步骤 4 验证资产过滤器后，要返回到**编辑过滤器 (Review filter change impact)** 页面，请点击**关闭 (Close)**。

限制为所有权范围

选中**限制为所有权范围？(Restrict to Ownership Scope?)** 复选框，以确定范围是否影响与过滤器匹配的资产。例如，在以下结构中：

1. 具有查询的租户

   ```
   VRF ID = 3
   ```

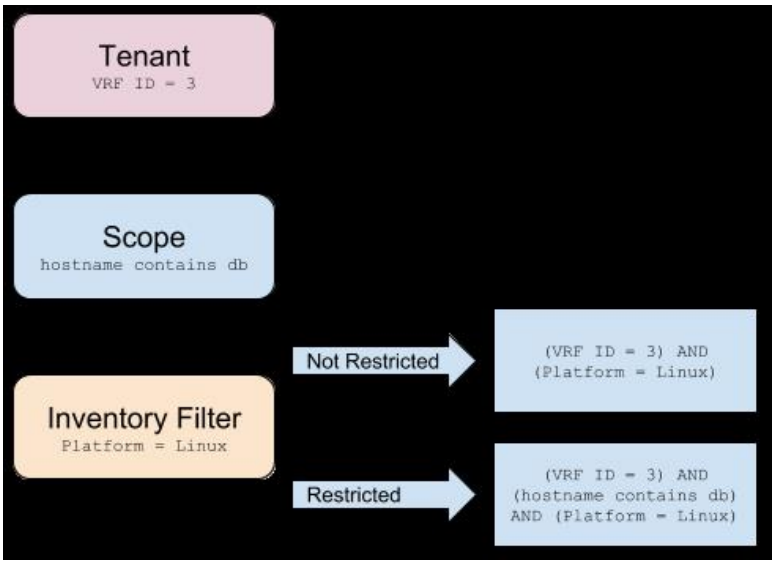
2. 具有查询的租户内的范围

   ```
   hostname contains db
   ```

3. 附加到范围的具有以下查询的资产过滤器。

   ```
   Platform = Linux
   ```

Figure 44: 租户、范围和资产过滤器结构



- 如果您不选择**限制为所有权范围 (Restrict to Ownership Scope)**，则过滤器将匹配租户中也与过滤器匹配的所有主机。输入以下查询：

  ```
  (VRF ID = 3) AND (Platform = Linux)
  ```

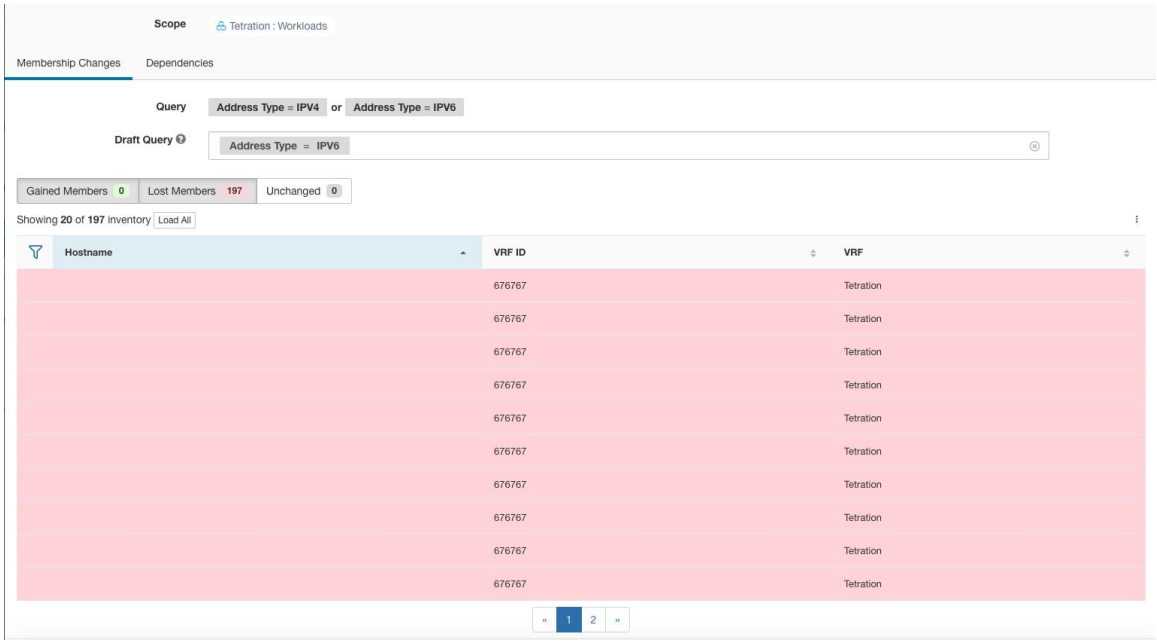
- 如果选择**限制为所有权范围 (Restrict to Ownership Scope)**，则过滤器将仅匹配租户内的主机以及也与过滤器匹配的范围。输入以下查询：

  ```
  (VRF ID = 3) AND (hostname contains db) AND (Platform = Linux)
  ```

查看范围/过滤器更改影响

在提交后，更新范围查询可能会影响范围的资产成员身份。同样，直接保存的过滤器查询更改也会影响范围资产成员身份。您可以通过点击范围或过滤编辑模式上的**查看查询更改影响 (Review query change impact)** 链接来识别新旧查询之间的成员身份更改。此外，了解范围或过滤器的依赖关系有助于进行影响分析和删除所有必要的对象，以防止删除范围。另请访问**依赖关系 (Dependencies)** 选项卡，遍历范围依赖关系树以了解更多信息。

Figure 45: 下载成员关系表



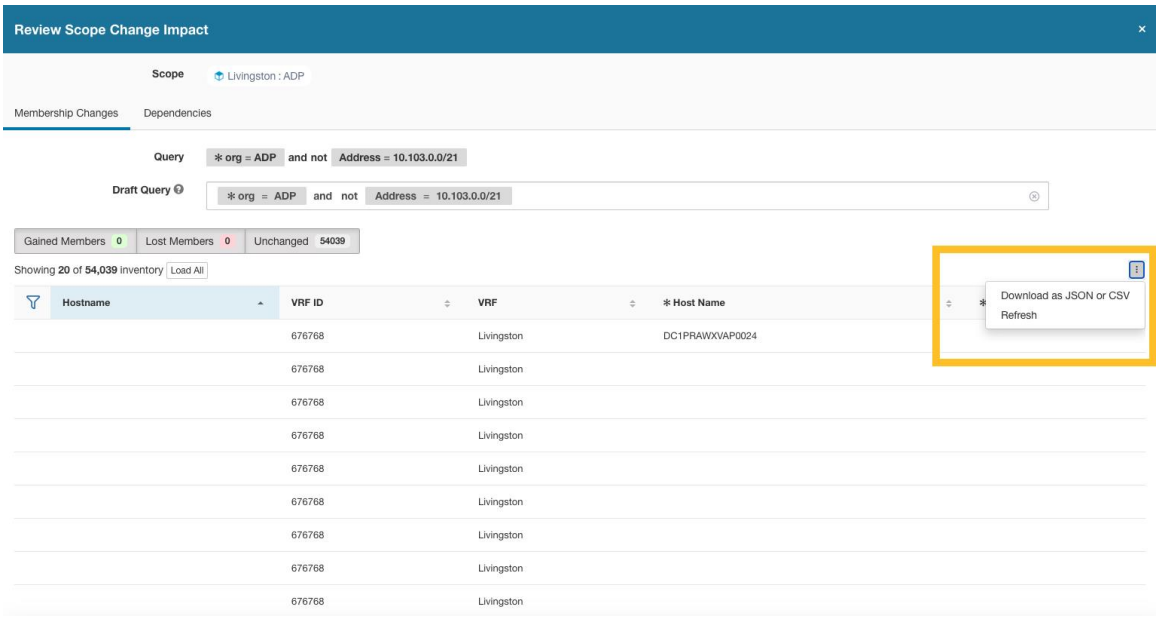
范围查询更改影响模式

通过点击“范围编辑”(Scope Edit) 窗口中的**查看查询更改映像 (Review query change impact)** 链接，可访问**成员身份更改 (Membership Changes)** 和**依赖关系 (Dependencies)** 选项卡。

成员身份更改

默认情况下，“成员身份”(Membership) 视图下的资产表将显示所有的列。您可以选择要显示的列。此外，您还可以下载所选成员列和行的 csv 或 json 文件，其中包含一个额外的差异列，用于标识资产是**已获得**、**已丢失**还是**未更改**。确保所有需要下载的表格选择在表格视图中可见。

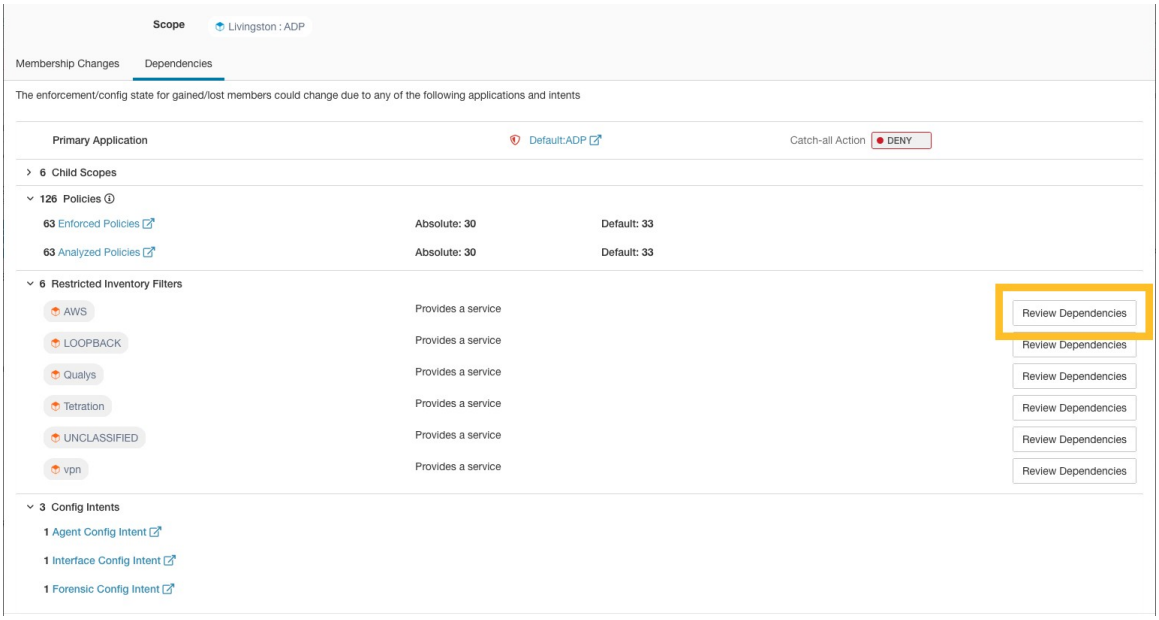
Figure 46: 范围成员身份更改



依赖关系

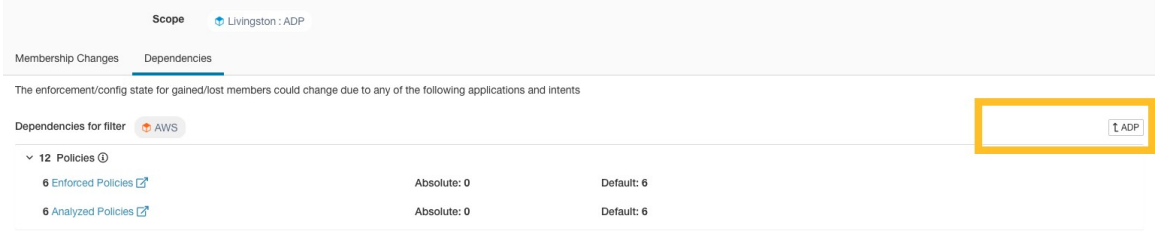
您可以通过进一步选择**查看依赖关系 (Review Dependencies)** 来遍历嵌套依赖关系

Figure 47: 查看依赖关系



您可以通过选择所选的“父”链接来向后遍历依赖关系树：

Figure 48: 父链接



以下是可能存在的范围依赖关系：

Table 3: 以下是可能存在的范围依赖关系

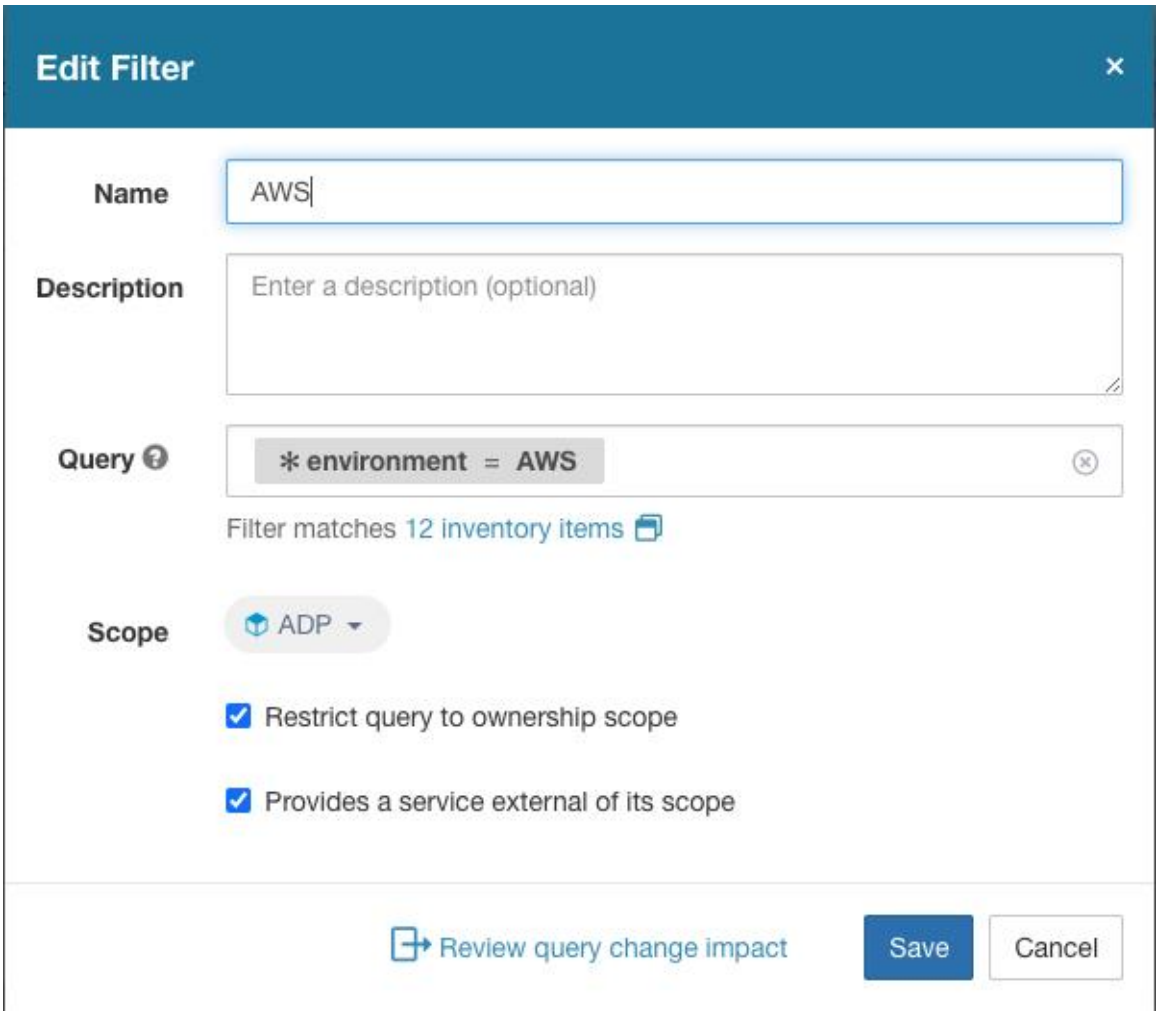
类型	说明
应用	具有主要和辅助应用名称，并可链接到“分段”下的特定工作空间。
子范围	包含名称和指向子“范围详细信息”(Scope Detail)视图的链接。允许向下钻取到较低级别的依赖关系。
策略	已分析并执行策略计数以及指向按所选范围过滤的相应全局策略视图的链接。
受限资产过滤器	包含名称和指向子“过滤器详细信息”(Filter Detail)视图的链接。允许向下钻取到较低级别的依赖关系。
配置意图	具有代理、接口和取证配置意图视图的名称和链接。

过滤器查询更改影响模式

通过点击“资产过滤器编辑”(Inventory Filter Edit)窗口中的**查看查询更改映像 (Review query change impact)** 链接，可访问**成员身份更改 (Membership Changes)** 和**依赖关系 (Dependencies)** 选项卡。

成员身份更改

Figure 49: 资产过滤器成员身份更改



依赖关系

以下是可能存在的过滤器依赖关系：

类型	说明
策略	已分析并执行策略计数以及指向按所选范围过滤的相应全局策略视图的链接
配置意图	具有代理、接口和取证配置意图视图的名称和链接

资产配置文件

Note 资产配置文件页面可从多个位置的链接进行访问。查看资产配置文件的一种方法是搜索资产，然后点击某个 IP 地址即可转至其配置文件。如果您是在“范围和资产”(Scopes and Inventory) 页面上，请点击“IP 地址”(IP addresses) 选项卡中的 IP 地址，而不是“工作负载”(Workloads) 选项卡中的 IP 地址。（点击“工作负载”(Workloads) 选项卡中的 IP 地址将显示工作负载配置文件，而不是资产配置文件。）

以下信息可用于资产：

字段	说明
范围	资产所属的范围列表。
资产类型	• **已获知流**的资产已根据观察到的流注册，。 • **已标记资产**已使用资产上传实用程序手动上传。 • **代理**资产由主机上安装的软件代理报告。 • **已标记**资产由连接器或外部协调器报告。
用户标签	用户为此资产上传的属性列表。有关详细信息，请参阅工作负载标签。

仅当满足以下两个条件时，其他信息才可用：

1. 已通过云连接器注入资产。
2. 已为资产所在的虚拟网络启用分段。

字段	说明
执行状况 (Enforcement Health)	主机软件代理的状态信息。有关详细信息，请参阅“代理运行状况”(Agent Health) 选项卡。
具体策略 (Concrete Policies)	此选项卡显示在主机上应用的 Cisco Secure Workload 个具体执行策略。有关详细信息，请参阅“具体策略”(Concrete Policies) 选项卡。
安全组	应用于此资产的安全组及其策略的列表。

资产配置文件信息

字段	说明
试验 (Experimental) 组	用于策略实时分析的集群或用户定义的资产过滤器列表。
执行 (Enforcement) 组	用于策略执行的集群或用户定义的资产过滤器列表。根据系统中正在分析和/或执行的策略版本，它们可能与试验组不同。

Note 在以下情况时，某个 IP 地址的资产配置文件详细信息可能不可用：

- 资产已从收集规则中排除。
- 在单向流中，资产仅可用两分钟，然后将被删除。
- 在双向流中，资产的可用期限为 30 天。如果在这 30 天内未观察到更多流，则会删除资产详细信息。

适用的工作负载

工作负载配置文件显示有关安装了 Cisco Secure Workload 软件代理的主机的详细信息。本部分介绍如何查看工作负载配置文件及其包含的信息。

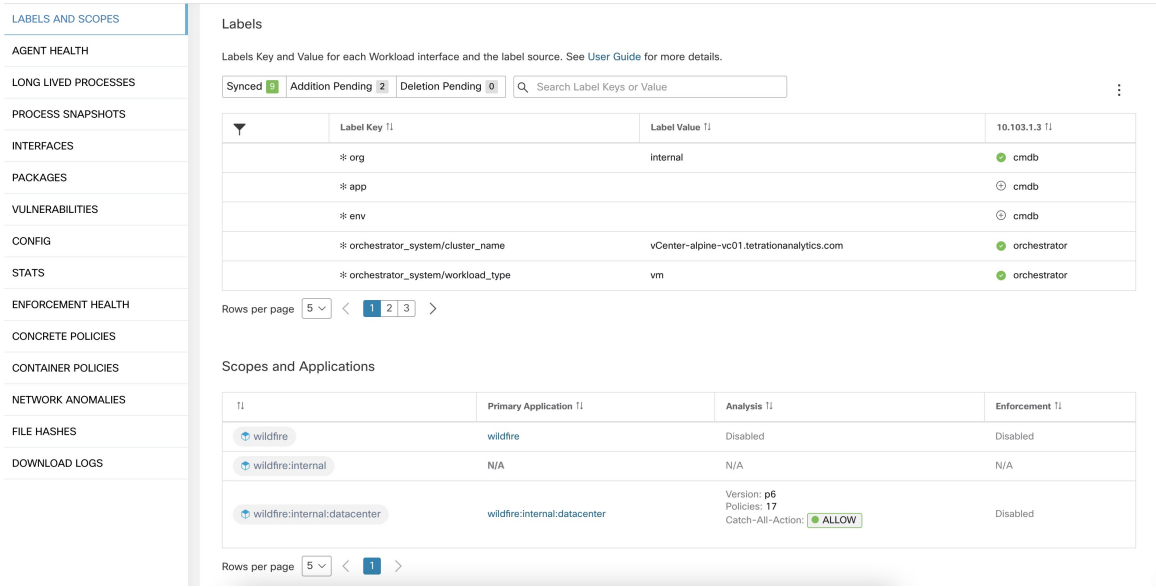
Note 工作负载配置文件页面可从多个位置的链接进行访问。查看工作负载配置文件的方法之一是对主机执行搜索，如“搜索”中所述

在资产搜索结果中，点击主机的 IP 地址即可转到其配置文件。根据主机上安装的代理类型，页面上会提供以下选项卡。请注意，如果此资产所属的主机上未安装 Cisco Secure Workload 软件代理，您最终可能会进入资产配置文件页面。

“标签和范围”(Labels and Scopes) 选项卡

此选项卡包括执行组和试验组以及主机所属的范围。试验组是用于策略实时分析的资产过滤器，而执行组是用于策略执行的过滤器。它们可以不同，具体取决于系统中正在分析和/或执行的策略版本。

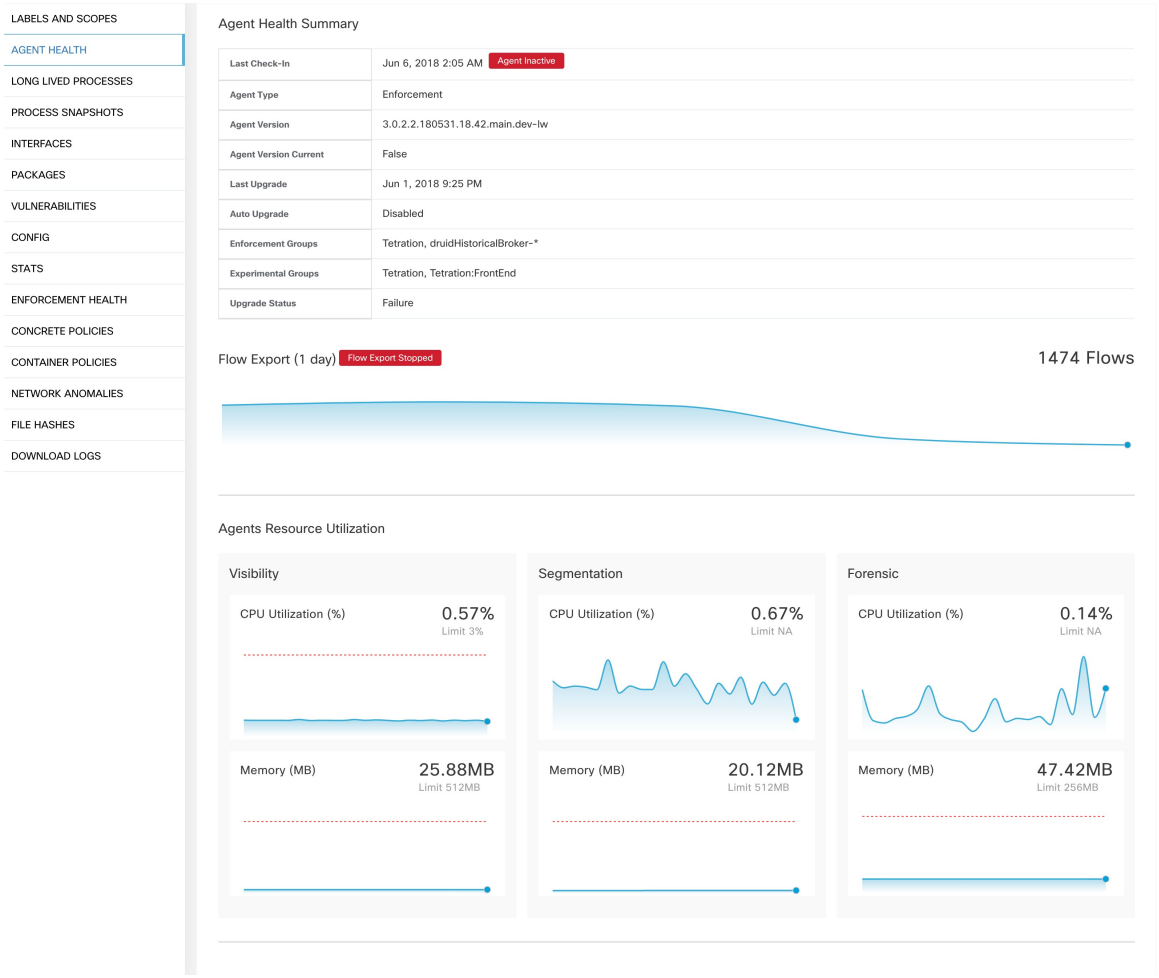
Figure 50: 工作负载标签和范围



“代理运行状况”(Agent Health) 选项卡

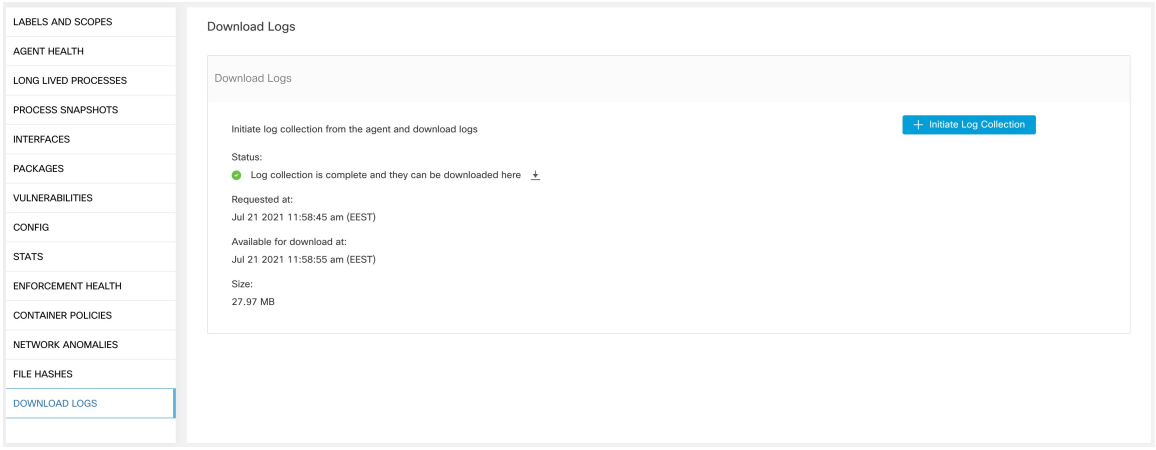
主机软件代理的状态信息（例如代理类型、操作系统平台、代理版本和上次签入时间）也会显示在**代理运行状况 (Agent Health)** 选项卡中。有关详细信息，请参阅软件代理配置。此选项卡还会显示每天发生的流量字节和数据包的详细时间序列数据。

Figure 51: 工作负载代理运行状况详细信息



对于具有根范围所有者权限的用户，摘要页面还包括一个部分，用于收集和下载该根范围内的深度可视性和执行代理（版本 3.3 或更高版本）的代理日志。另请注意，此功能不适用于在平台 AIX 和 SUSE Linux Enterprise Server（IBM Z 架构上的 s390x-Linux）上运行的代理。使用“启动日志收集”(Initiate Log Collection) 按钮从代理收集日志，然后在几分钟后即可下载日志。如果下载失败，请重新尝试收集日志，然后再次尝试下载。

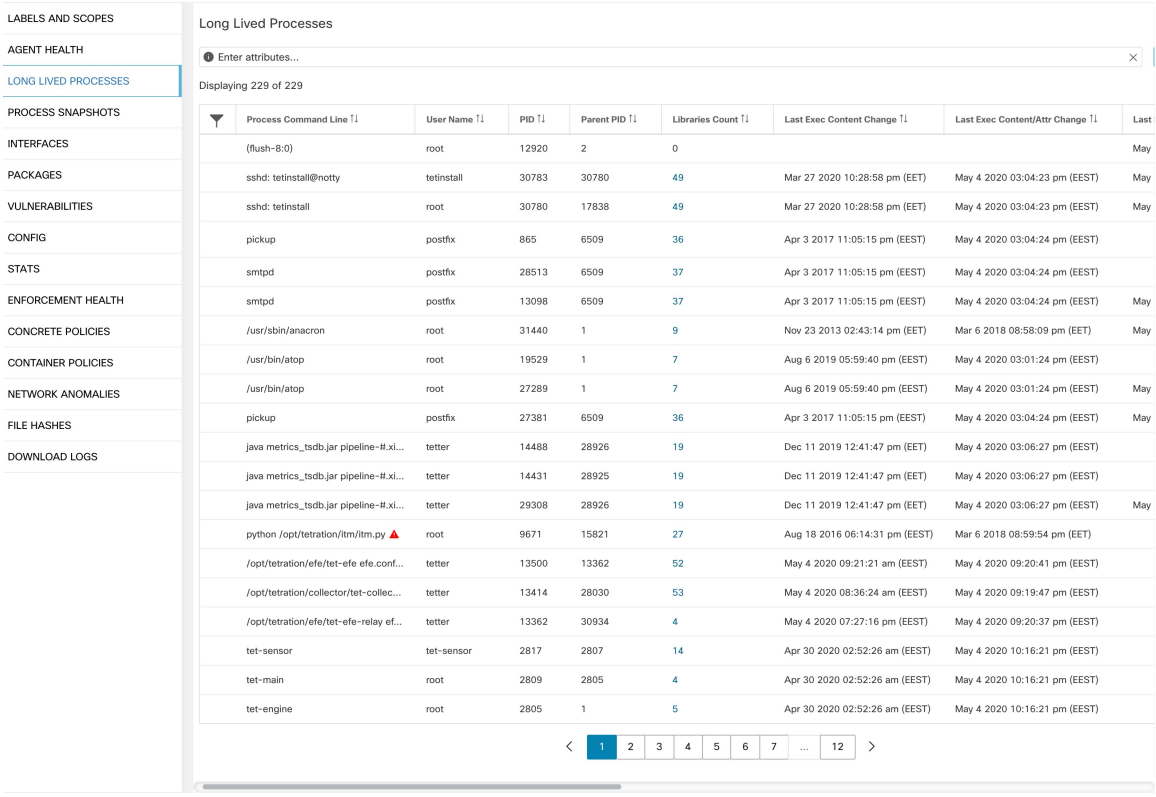
Figure 52: 代理日志



“进程列表”(Process List) 选项卡

此选项卡列出了主机上正在运行的进程。也可以使用过滤器，根据下表标题中显示的进程属性来缩小进程列表的范围。

Figure 53: 工作负载进程列表



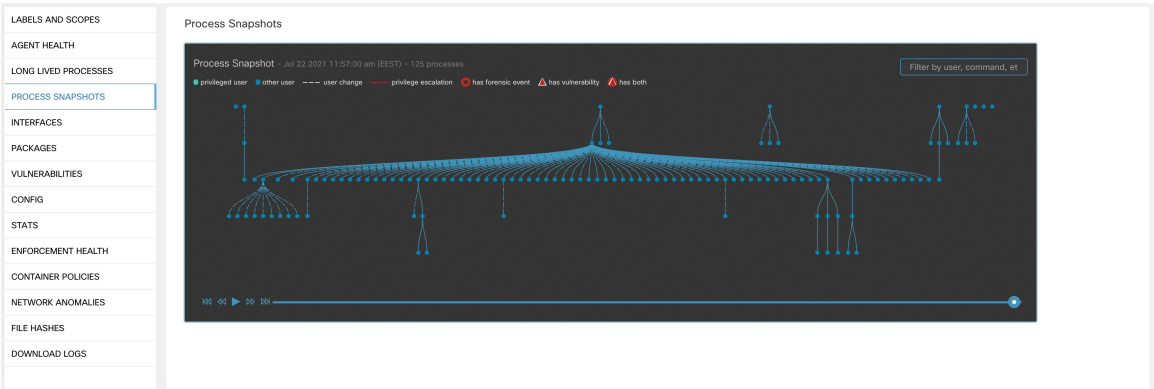
属性说明：

属性	说明
Last Exec Content Change	类似于 Linux 中的 mtime。这是仅更改文件内容时的时间戳。
Last Exec Content Change	类似于 linux 中的 ctime。它是文件内容或属性发生变化时的时间戳。
Last Seen	上次观察到该进程的时间。当进程终止时可用。
CPU Usage	过去一小时内进程的 CPU 使用率趋势。
Memory Usage	过去一小时内进程的内存使用率趋势。
Process Binary Hash	以十六进制字符串表示的进程二进制 SHA256 散列，也称为进程散列。不适用于内核进程。
Anomaly Score	进程散列（异常）评分。有关详细信息，请参阅进程散列异常检测。
Verdict	进程散列的判定（恶意或良性）。根据进程散列是否属于任何用户定义的散列列表或已知的威胁智能散列数据库来确定判定。有关详细信息，请参阅进程散列异常检测。
Verdict Source	判定的来源。判定源可以是用户定义、Cisco Secure Workload 云或 NIST。此属性在以前的版本中称为散列数据库源。有关详细信息，请参阅进程散列异常检测。

“进程快照”(Process Snapshot) 选项卡

此选项卡显示在工作负载上观察到的可搜索进程树。

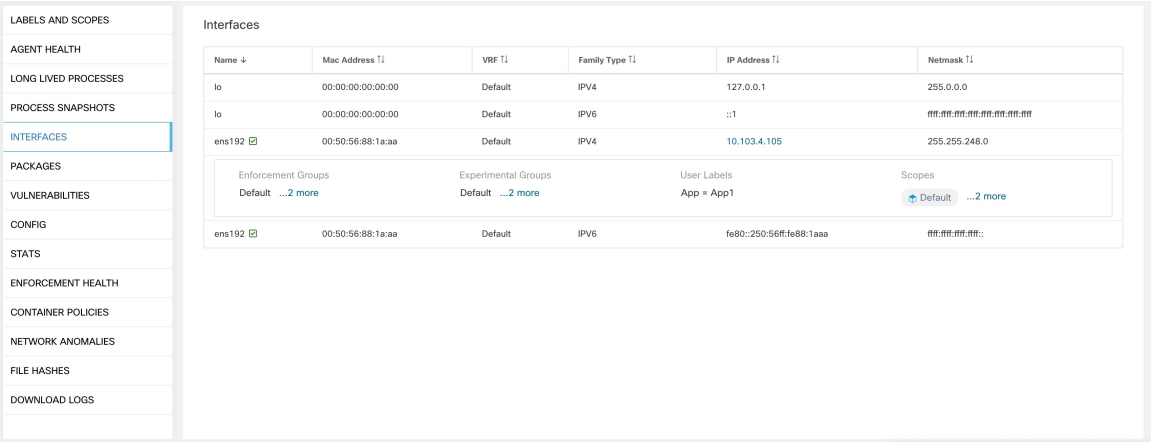
Figure 54: 工作负载进程快照



“接口”(Interfaces) 选项卡

此选项卡显示有关主机上安装的网络接口的详细信息。它适用于所有类型的软件代理。

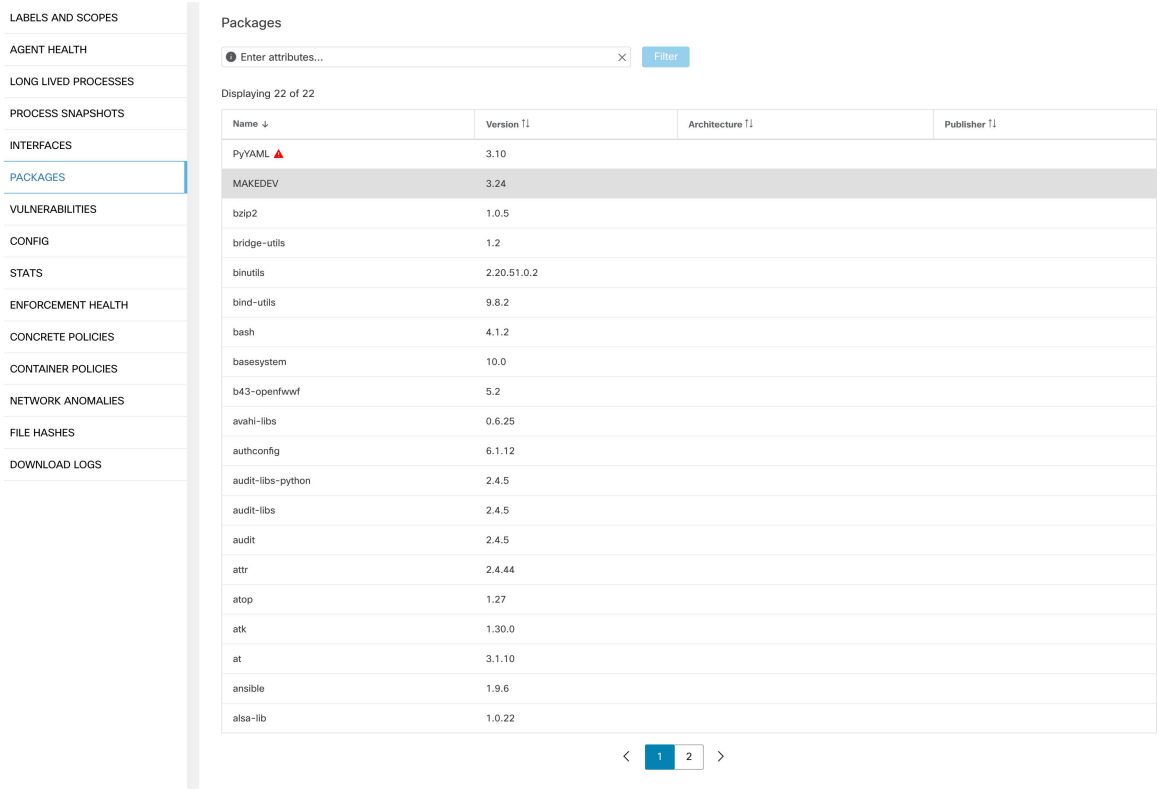
Figure 55: 工作负载接口列表



“软件包”(Software Packages) 选项卡

此选项卡显示了主机上安装的软件包的列表。您可以根据表标题中的软件包属性选择性地查看软件包。

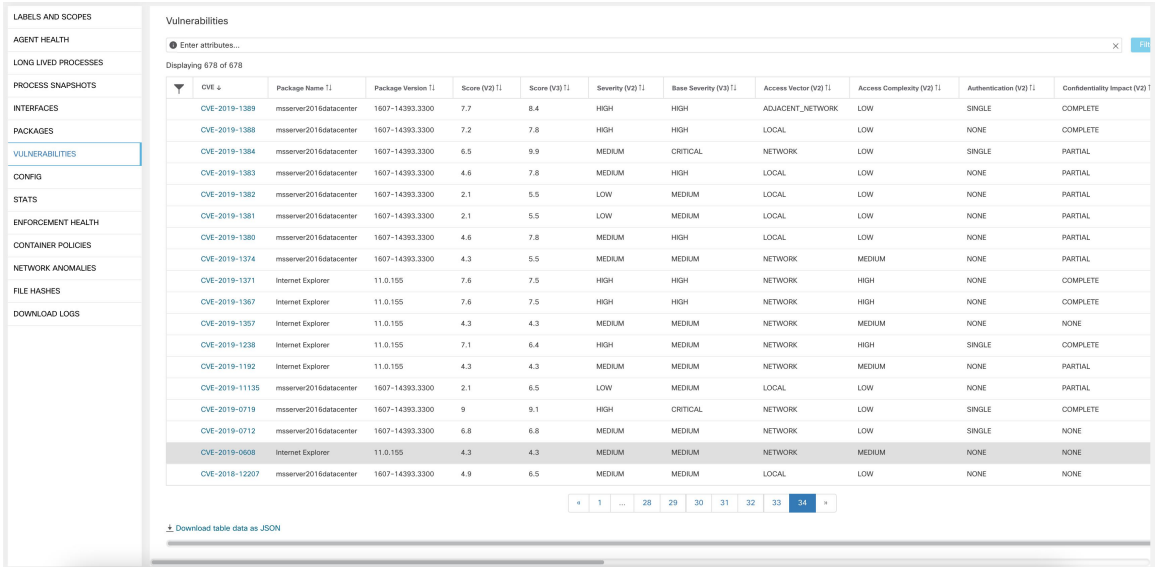
Figure 56: 软件包列表



“漏洞”(Vulnerabilities) 选项卡

漏洞 (VULNERABLITIES) 选项卡显示根据通用漏洞评分系统（CVSS V2、V3）和思科安全风险评分在工作负载上识别的 CVE。

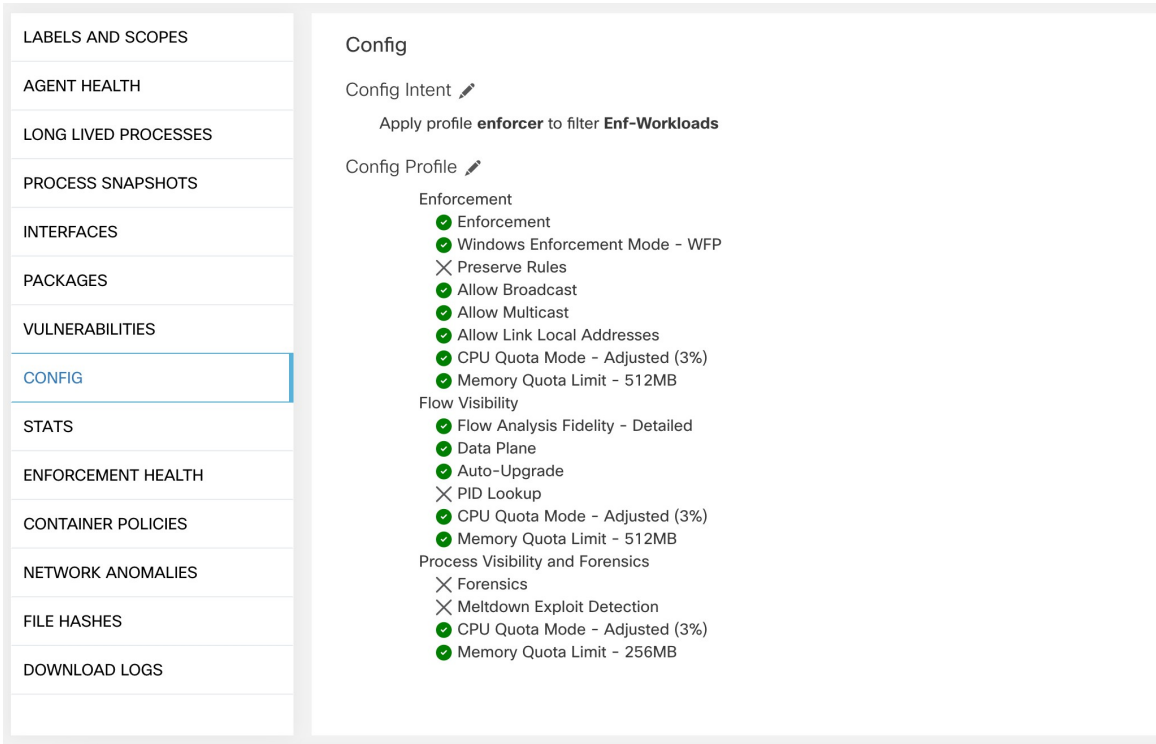
Figure 57: *“漏洞”(Vulnerabilities)* 选项卡



“代理配置”(Agent Configuration) 选项卡

此选项卡显示软件代理设置。它仅适用于深度可视性和执行代理。这些设置可通过代理配置页面使用“代理配置意图”(Agent Configuration Intents) 进行修改。请参阅软件代理配置

Figure 58: *应用的工作负载配置*



“代理统计信息”(Agent Statistics) 选项卡

此选项卡会显示有关主机上安装的 Cisco Secure Workload 代理的统计信息。它仅适用于深度可视性和执行代理。

Figure 59: 代理统计信息

“具体策略”(Concrete Policies) 选项卡

在执行工作空间时，每个工作负载只会接收该工作空间中特定于该工作负载的策略。在每个工作负载上实际编程的这些策略称为具体策略。

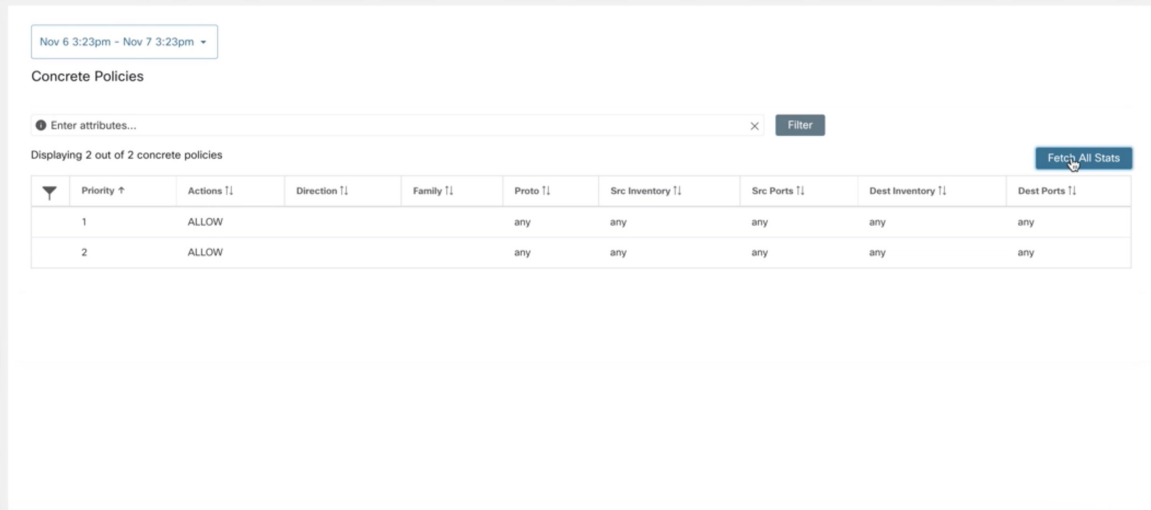
例如，假设在具有操作 ALLOW 的策略中指定的提供者包括子网 1.1.1.0/24 中的所有资产。在具有 Cisco Secure Workload 代理且 IP 地址为 1.1.1.2 的工作负载上安装此策略时，防火墙规则如下所示：

1. 对于传入流量，防火墙规则允许专门发往 1.1.1.2 的流量，而不是发往整个子网 1.1.1.0/24 的流量。
2. 对于传出流量，防火墙规则明确允许来自 1.1.1.2 的流量，而不是来自整个子网 1.1.1.0/24 的流量。

工作负载配置文件中的“具体策略”(CONCRETE POLICIES) 选项卡显示在主机上应用的 Cisco Secure Workload 个具体执行策略。此表中的每一行对应于在主机上实施的防火墙规则。每个策略行都可以进一步展开，以显示此具体策略所源自的逻辑意图。数据包和字节计数时序视图也可用于每个规则。

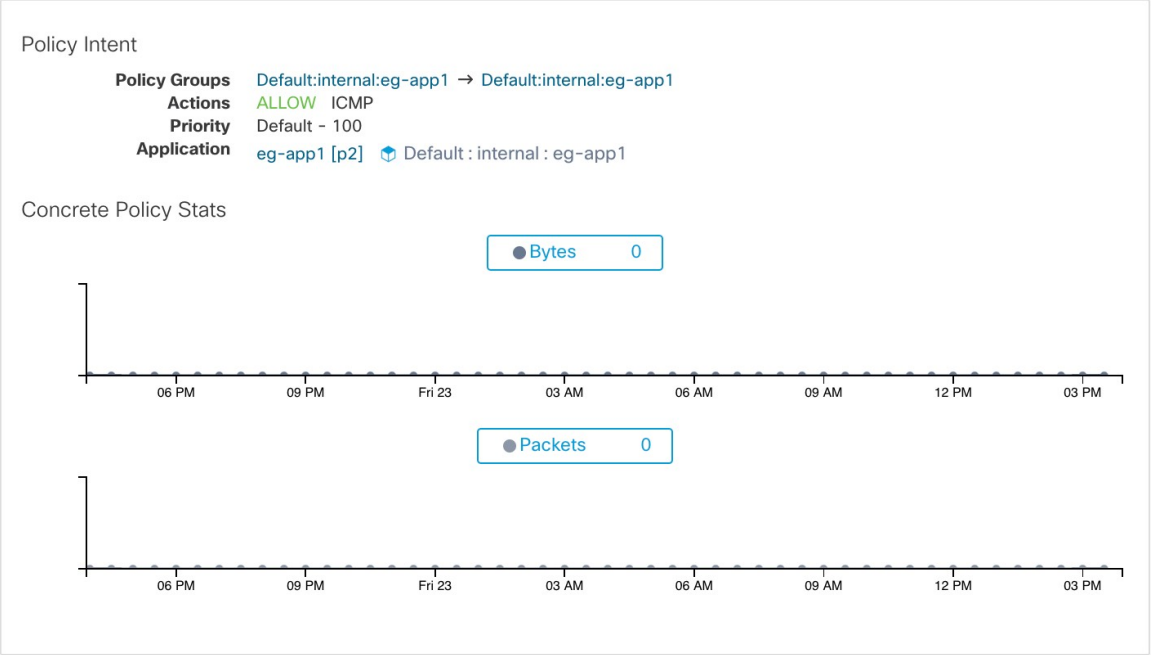
点击**获取所有统计 (Fetch All Stats)** 信息按钮以查看每个规则的数据包和字节数。此选项卡中还有一个过滤器，可根据下表标题所示的策略属性来缩小执行策略列表的范围。此选项卡仅在对已安装的代理启用执行时才可用。

Figure 60: 具体策略列表



在下图中，**策略组 (Policy Groups)** 显示了使用者和提供者：

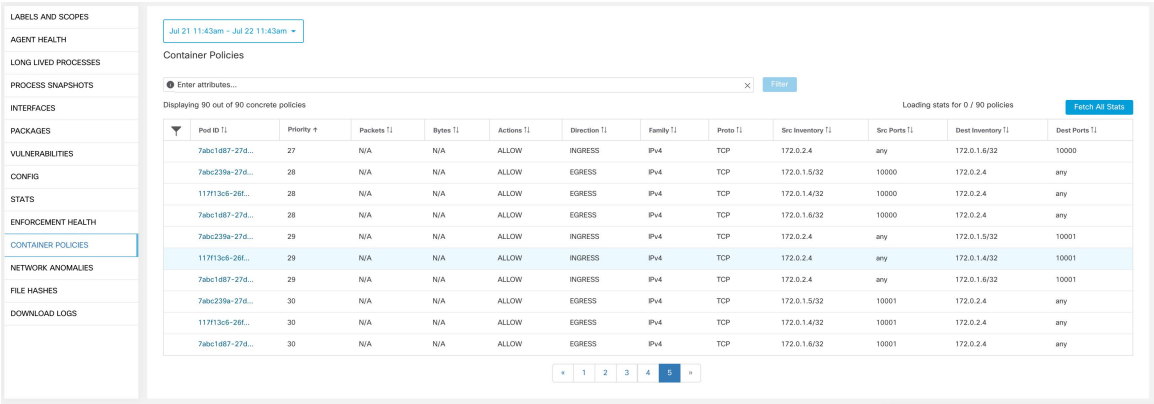
Figure 61: 具体策略行



“容器策略”(Container Policies) 选项卡

此选项卡显示在容器上应用的 Cisco Secure Workload 具体执行策略。此表中的每一行都与容器 Pod 上实施的防火墙规则相对应。

Figure 62: 容器具体策略列表



“网络异常”(Network Anomalies) 选项卡

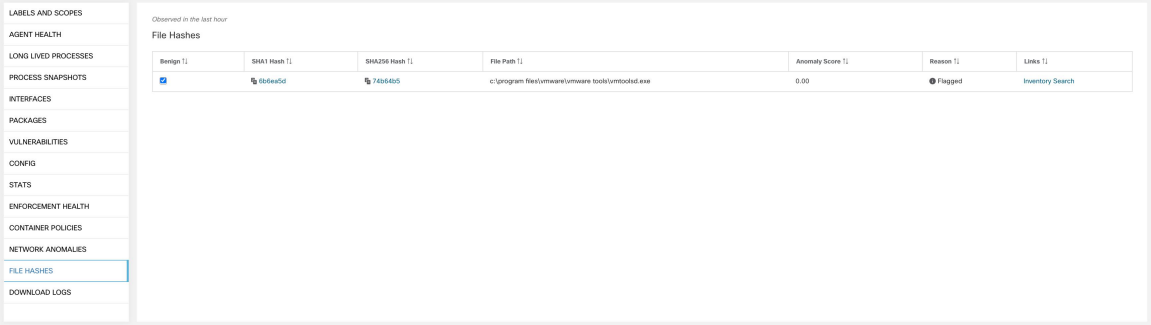
此选项卡有助于识别大量数据移入或移出此工作负载的事件。有关详细信息，请参阅基于 PCR 的网络异常检测。

Figure 63: 工作负载网络异常

“文件散列”(File Hashes) 选项卡

此选项卡通过评估整个系统中进程二进制文件散列的一致性来检测进程散列异常。有关详细信息，请参阅进程散列异常检测。

Figure 64: 工作负载文件散列



软件包

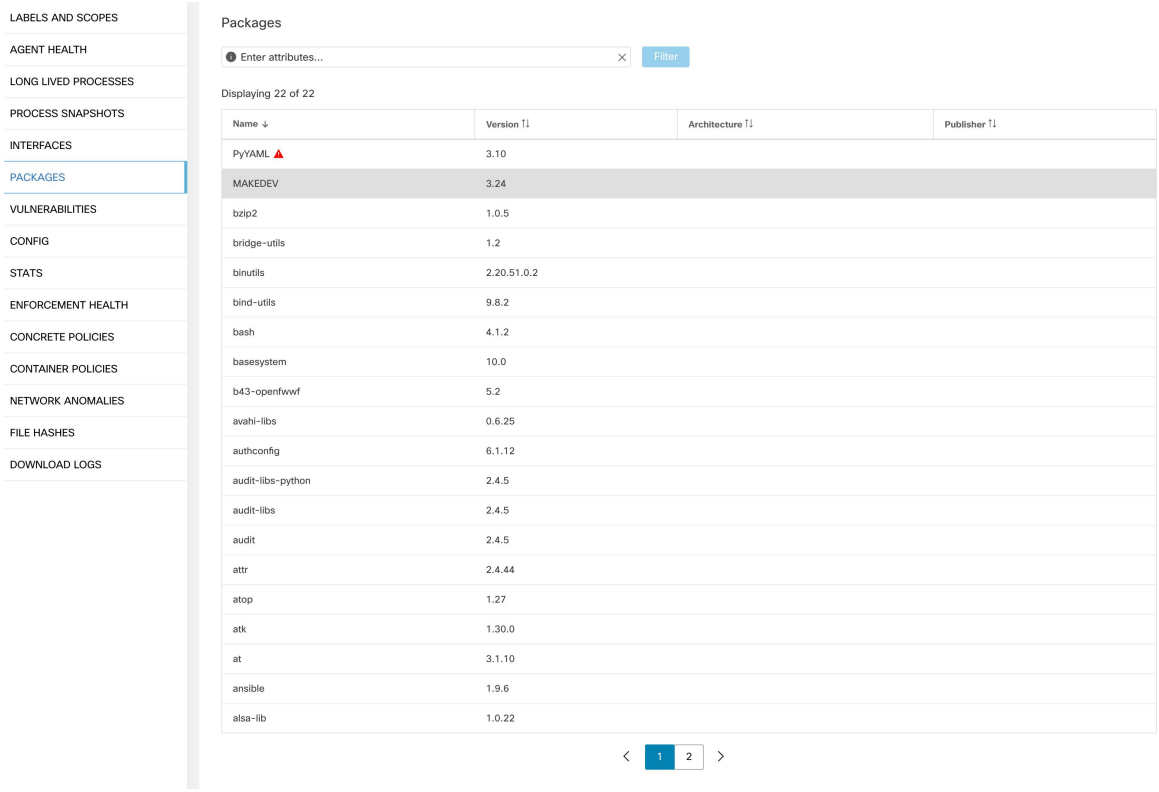
软件包功能集允许查看主机上安装的软件包以及影响这些软件包的漏洞。具体而言，它允许：

- 查看向以下软件包管理器注册的软件包：
  - Linux：Red Hat 软件包管理器 (RPM) 和 Debian 软件包管理器 (dpkg)
  - Windows：Windows 注册表服务
- 查看影响主机上安装的软件包的常见漏洞和风险 (CVE)。
- 使用软件包名称和版本定义资产过滤器。

“软件包”(Packages) 选项卡

要查看主机上安装的软件包，请导航至工作负载配置文件适用的工作负载 页面上的软件包选项卡。

Figure 65: 工作负载配置文件包



常见漏洞和风险

与软件包一起，**漏洞 (VULNERABILITIES)** 选项卡将提供有关在您的工作负载中识别的 CVE 的详细信息。每个漏洞都包含一个指向国家漏洞数据库 (NVD) 的链接，该数据库提供有关特定漏洞的更多信息。除了显示 CVE ID 之外，我们还会根据评分方法（CVSS V2 和 CVSS V3）以及漏洞的严重性显示影响评分（满分为 10 分）。

Windows 软件包和 CVE

以下部分列出了 Windows 代理在向 Cisco Secure Workload 报告软件包信息方面的行为。

- Windows 应用程序、PowerShell 和 IE 被报告为软件包。.net 框架也被报告为软件包。
- 不会报告其他 Windows 应用，例如 notepad.exe、cmd.exe、mstsc.exe 等。
- Windows 服务器配置的角色和功能被报告为软件包，但版本可能不正确。例如：如果已配置 DNS 服务器，则报告的版本为 0 或 8。
- Windows 代理会报告使用 MSI 安装程序或 exe 安装程序安装的第三方产品：
  - 对于 MSI 安装程序，MSI API 用于检索软件包信息。例如，版本、发布服务器、软件包名称。

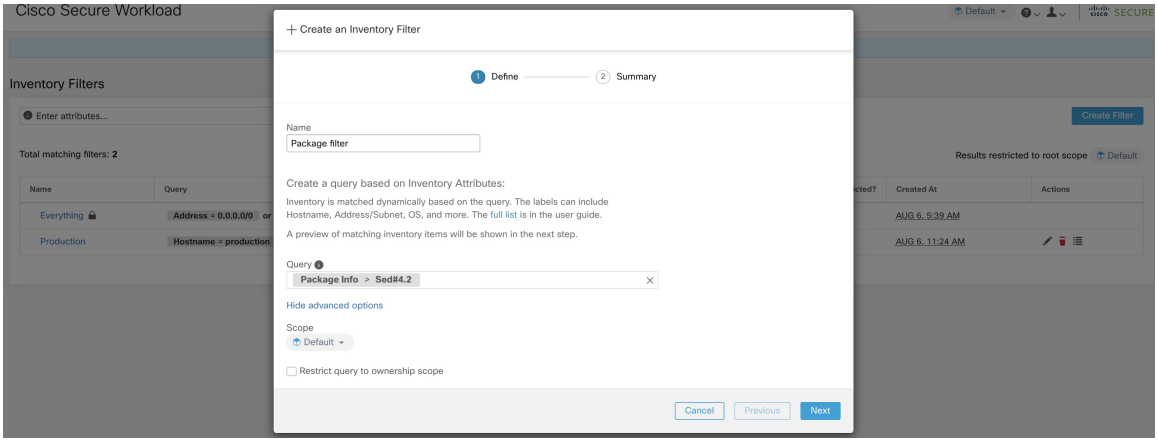
- 如果使用 exe 安装程序来安装软件包，则会从注册表中获取软件包信息。
- 软件包安装程序字段（例如版本、发布服务器）为可选项。如果缺少版本，则不会报告软件包。
- 如果产品是从压缩文件中解压缩或作为应用程序安装的，则不会在软件包列表中报告。

资产过滤器

可以通过使用软件包名称和版本（可选）定义资产过滤器来搜索软件包相关信息。

此过滤器的语法如下：PackageName#PackageVersion

Figure 66: 资产数据包



支持以下操作：

- 相等 - 返回软件包与 PackageName 和 PackageVersion（如果提供）匹配的主机。
- 不相等 - 返回软件包与 PackageName 匹配但不与 PackageVersion（如果提供）匹配的主机。
- 大于 - 返回软件包与 PackageName 匹配且版本高于 PackageVersion 的主机。
- 大于或等于 - 返回软件包与 PackageName 匹配且版本高于或等于 PackageVersion 的主机。
- 小于 - 返回软件包与 PackageName 匹配且版本低于 PackageVersion 的主机。
- 小于或等于 - 返回软件包与 PackageName 匹配且版本小于或等于 PackageVersion 的主机。

漏洞数据可视性

通过使用漏洞数据可视性，您可以检测和查看影响主机上的软件包和进程的漏洞。使用以下方法定义资产过滤器：

- CVE ID

- CVSS V2 评分
- CVSS V3 评分
- CVSS V2 属性
- CVSS V3 属性

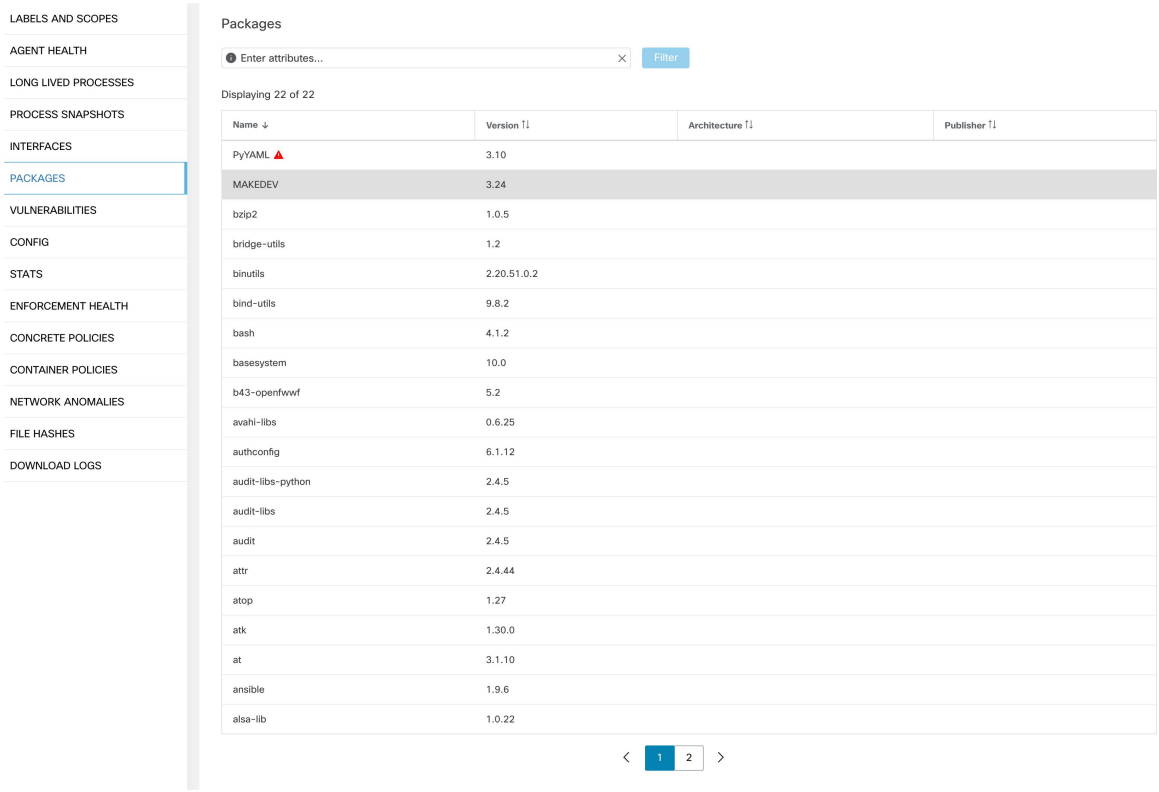
“工作负载配置文件”(Workload Profile) 页面

影响系统上的软件包和进程的漏洞相关信息显示在适用的工作负载 页面上。

“软件包”(Packages) 选项卡

软件包选项卡会列出主机上安装的软件包以及影响这些软件包的漏洞。

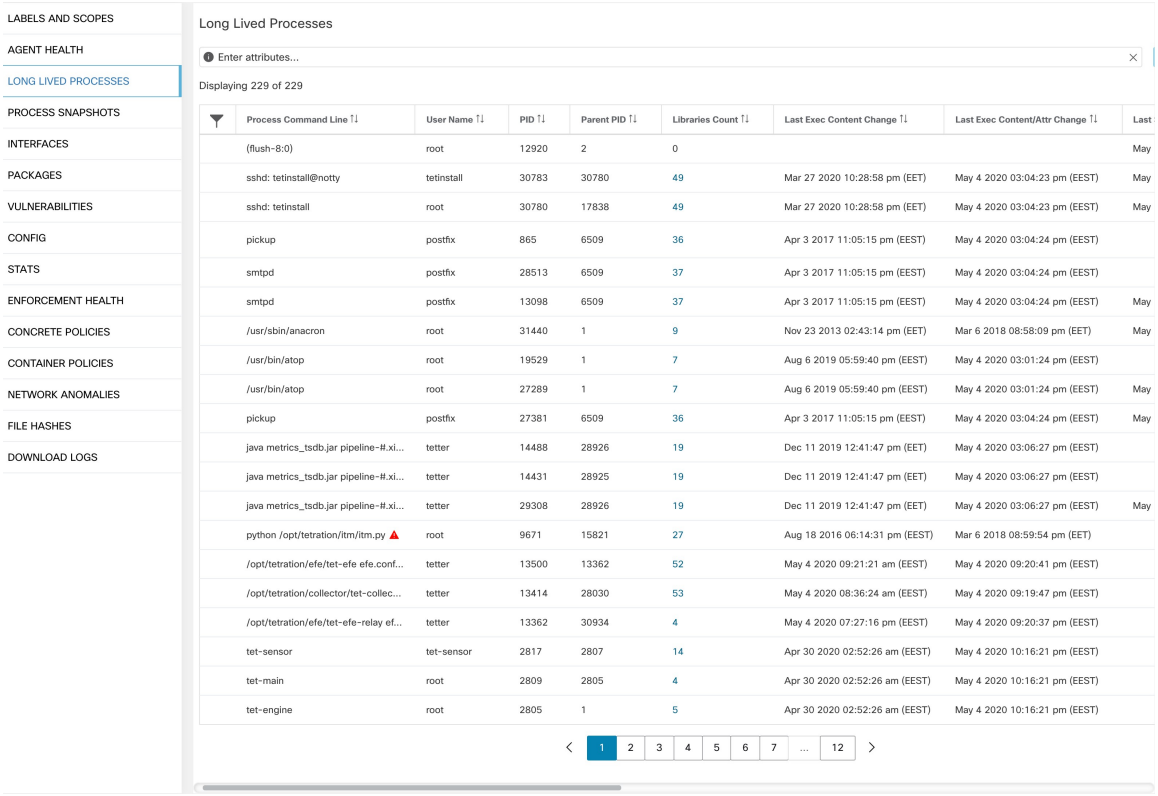
Figure 67: 工作负载配置文件包



“进程列表”(Process List) 选项卡

长期进程会显示在进程列表选项卡下。

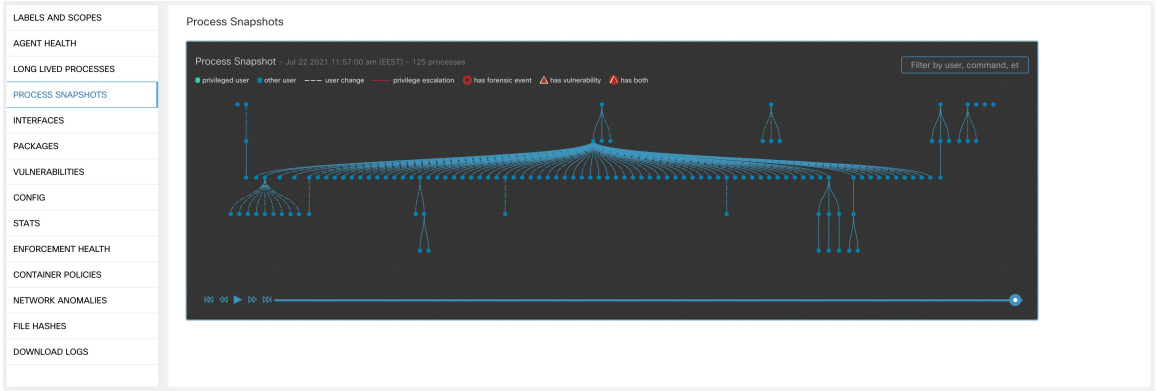
Figure 68: 工作负载配置文件进程列表



“进程快照”(Process Snapshot) 选项卡

系统会在进程快照选项卡下显示进程树中所有进程的漏洞信息。

Figure 69: 工作负载配置文件进程快照选项卡



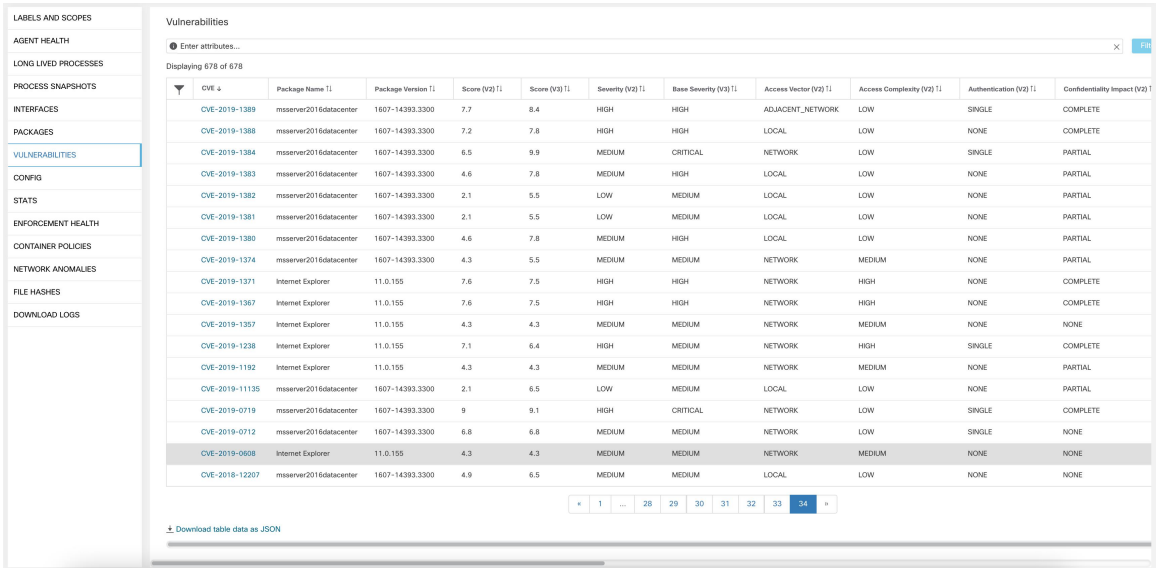
“漏洞”(Vulnerabilities) 选项卡

漏洞 (VULNERABILITIES) 选项卡显示 Cisco Secure Workload 在工作负载上识别的 CVE。

对于每个 CVE，除了基本影响指标外，还会显示基于威胁智能的漏洞攻击信息：

- 漏洞利用计数：过去一年 CVE 被广泛利用的次数
- 上次被利用：我们的威胁智能上次发现 CVE 被广泛利用的时间

Figure 70: 工作负载配置文件：“漏洞”***(Vulnerabilities)*** 选项卡



资产过滤器

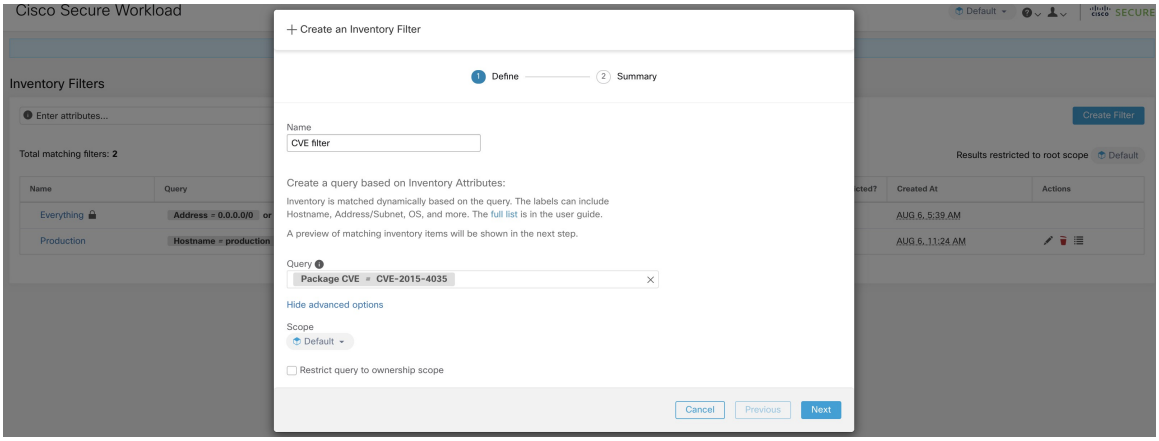
可以定义以下类型的资产过滤器来识别包含易受攻击软件包的主机：

基于 CVE ID 的过滤器

使用 CVE ID 创建的资产过滤器可以搜索受特定 CVE 影响的主机。

要搜索受特定 CVE 影响的主机，请按以下格式输入 CVE ID：`CVE-XXXX-XXXX`

Figure 71: 资产过滤器 ***CVE***



支持以下操作：

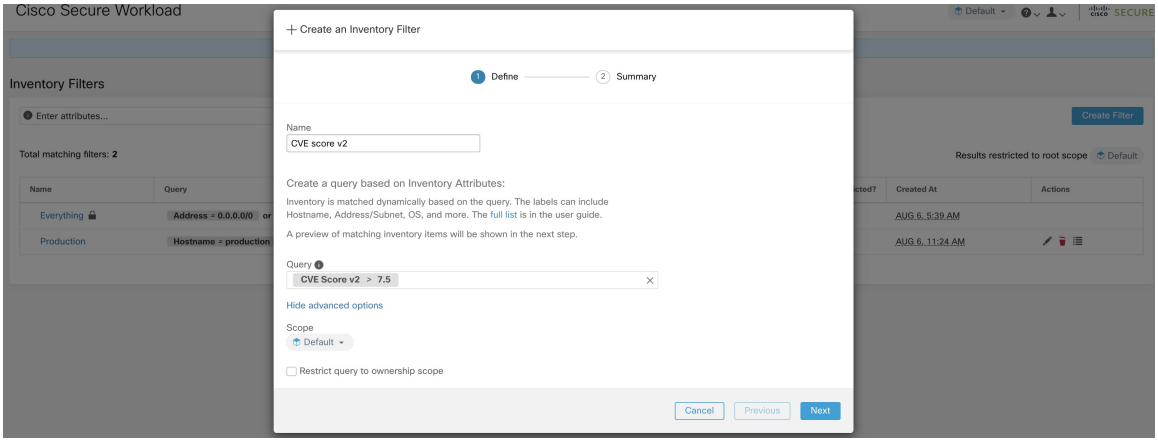
- =：返回包含受 CVE ID 影响的软件包的主机。
- ≠：返回包含不受 CVE ID 影响的软件包的主机。
- **包含 (contains)**：返回输入字符串中存在受 CVE 影响的软件包的主机（输入 **cve** 会返回受 CVE 影响的主机）。
- **不包含 (doesn't contain)**：返回包含不受输入字符串中存在的 CVE 影响的软件包的主机（输入 **cve** 会返回不受 CVE 影响的主机）。
- **匹配 (matches)**：返回包含受与输入字符串匹配的 CVE 影响的软件包的主机。

基于通用漏洞评分系统影响评分的过滤器

基于通用漏洞评分系统 (CVSS) 的过滤器允许通过输入数字格式的评分来搜索具有指定 CVSS V2 或 CVSS V3 影响评分的 CVE 的主机。

例如，要搜索 CVSS V2 影响评分大于 7.5 的 CVE 的主机，则查询为 `CVE Score v3 > 7.5`。

Figure 72: 资产过滤器 ***CVSS***



支持以下操作：

- =：返回具有具有指定 CVSS V2 或 V3 影响评分的 CVE 的主机。
- ≠：返回不具有具有指定 CVSS V2 或 V3 影响评分的 CVE 的主机。
- >：返回 CVE 的 CVSS V2 或 V3 影响评分大于指定的 CVSS V2 或 V3 影响评分的主机。
- ≥：返回具有 CVSS V2 或 V3 影响评分大于或等于指定 CVSS V2 或 V3 影响评分的 CVE 的主机。
- <：返回具有 CVSS V2 或 V3 影响评分分别小于指定 CVSS V2 或 V3 影响评分的 CVE 的主机。
- ≤：返回 CVE 的 CVSS V2 或 V3 影响评分小于或等于指定的 CVSS V2 或 V3 影响评分的主机。

基于 CVSS V2 属性的过滤器

可以使用访问向量和访问复杂性来创建资产过滤器，以识别易受攻击的主机。过滤器支持以下操作：

- =：返回包含受与过滤器匹配的漏洞影响的软件包的主机。
- ≠：返回包含不受与过滤器匹配的漏洞影响的软件包的主机。

访问向量

访问向量反映了漏洞被利用的方式。攻击者离易受攻击的系统越远，基本评分就越高。下表列出了不同的访问向量及其访问要求：

值	访问类型
本地	物理或本地（外壳）。
ADJACENT_NETWORK	广播或冲突。
网络	可远程利用。

访问复杂性

此指标衡量攻击者能够访问目标系统后利用漏洞的复杂性。基本评分与访问复杂性成反比。不同类型的访问复杂性如下所示：

值	说明
高	存在专门的访问条件。
中	访问条件具有一些专门性。
LOW	不存在专门的访问条件。

基于 CVSS V3 属性的过滤器

攻击媒介、攻击复杂性和影响 CVSS V3 评分所需的权限可用于资产过滤器。过滤器支持以下操作：

- =：返回包含受与过滤器匹配的漏洞影响的软件包的主机。
- ≠：返回包含不受与过滤器匹配的漏洞影响的软件包的主机。

攻击媒介

该指标反映可能出现漏洞攻击的情景。攻击者离易受攻击组件的距离越远，基本评分就越高。下表列出了不同的攻击媒介及其访问要求：

值	访问类型
本地	本地（键盘、控制台）或远程 (SSH)。

值	访问类型
物理	需要物理访问。
ADJACENT_NETWORK	广播或冲突。
网络	可远程利用。

攻击复杂性

此指标描述了利用漏洞必须具备的条件。最不复杂攻击的基本评分最高。不同类型的访问复杂性如下所示：

值	说明
高	设置和执行攻击需要耗费大量精力。
LOW	不存在专门的访问条件。

所需权限

此指标描述攻击者在成功利用漏洞前必须获得的权限等级。当执行攻击不需要权限时，基本评分最高。所需的不同权限值如下所示：

值	所需权限
高	可对易受攻击组件进行重要控制的权限。
LOW	授予对非敏感资源的访问权限的低权限。
无	执行攻击不需要权限。

服务配置文件

通过 Cisco Secure Workload，可以查看通过外部协调器注入的所有 Kubernetes 服务和其他负载均衡器。服务配置文件页面显示给定服务的详细信息。

Note 服务配置文件页面可从多个位置的链接进行访问。查看服务配置文件的方法之一是对服务执行搜索，如“搜索”中所述

在搜索结果中，点击“服务”(Services) 选项卡下的“服务名称”(Service Name) 以转到其配置文件。以下信息可用于服务：

标头

标头包括以下内容：

- **协调器名称**：报告此服务的外部协调器的名称。
- **协调器类型**：外部协调器的类型。
- **命名空间**：服务的命名空间。
- **服务类型**：服务的类型。可能的值包括 ClusterIP、Node、Port 和 LoadBalancer。

IP 和端口

下表列出了访问此服务所使用的所有可能的 IP 和端口组合。对于类型为 NodePort 的服务，此表显示 ClusterIP:Port 与 NodeIp:NodePort 相关联。

用户标签

为此服务上传的和协调器系统生成的标签的列表。

范围

Pod 所属的范围列表。

Pod 配置文件

通过 Cisco Secure Workload，您可以查看通过 Kubernetes 外部协调器注入的所有 Kubernetes Pod。Pod 配置文件页面显示给定 Pod 的详细信息。

Note Pod 配置文件页面可从多个位置的链接进行访问。查看 Pod 配置文件的方法之一是对 Pod 执行搜索，如“搜索”中所述

在搜索结果中，点击“Pod”选项卡下的“Pod 名称”(Pod Name) 以转到其配置文件。以下信息可用于 Pod：

标头

标头包括以下内容：

- **协调器名称**：报告此 Pod 的外部协调器的名称。
- **协调器类型**：外部协调器的类型。
- **命名空间**：Pod 的命名空间。
- **IP 地址**：Pod 的 IP 地址。

用户标签

用户上传的和协调器系统为此 Pod 生成的标签的列表。

范围

服务所属的范围列表。

容器漏洞扫描

为了保持正常运行状况并找出潜在的安全漏洞，我们建议定期扫描 Kubernetes pod。

前提条件

- 确保 Kubernetes 集群已激活。
- 将 CSW Kubernetes 守护进程集代理作为 Kubernetes 集群的一部分进行安装。有关详细信息，请参阅安装 Kubernetes 或 OpenShift 代理以实现深度可视性和执行。

过程

步骤 1 导航至**管理 (Manage)** > **工作负载 (Workloads)** > **Kubernetes**。

注释 **集群 (Clusters)** 选项卡显示所有载入的集群以及关联资产（例如服务和 Pod）的列表。

步骤 2 点击 **Pod 漏洞扫描 (Pod Vulnerability Scanning)**。

步骤 3 要开始扫描，请启用**操作 (Actions)** 下的切换。默认情况下，此切换已被禁用。

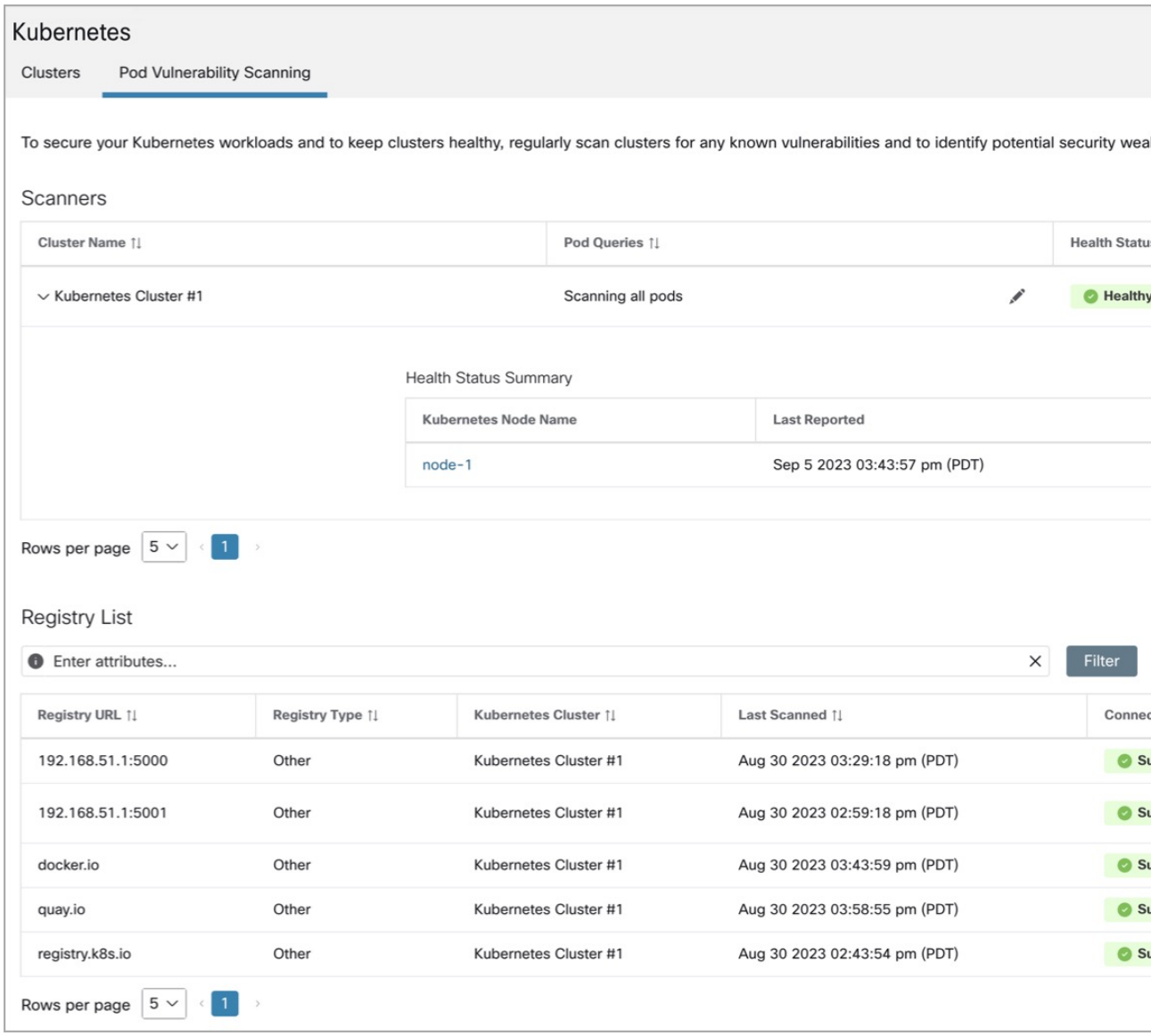
步骤 4 点击编辑图标以修改查询，并选择集群中运行的 Pod 子集。

注释
- 默认情况下会填充 Pod 查询，以扫描集群中的所有 Pod 资产。但您也可以编辑 Pod 查询，以便选择要扫描的 Pod。
- 目前，不支持扫描 Windows 容器映像。

步骤 5 展开集群以查看**运行状况摘要 (Health Status Summary)**。

- 点击 Kubernetes 节点名称，以便查看工作负载配置文件。
- 启用切换，将其他信息自动下载到主机，以便执行扫描程序。

图 *73: Pod* 漏洞扫描



步骤 6 验证连接状态，并在必要时输入证书。**注册表列表 (Registry List)** 会显示所有检测到的注册表。

注释 凭证因注册表类型而异。

Registry Type	**凭证**
Azure	租户 ID、客户端 ID、密钥
AWS	访问秘钥、密钥
GCP	JSON 格式的服务帐户密钥
其他	用户名、密码

故障排除

请按照以下步骤操作，以确保连接成功：

1. 扫描程序 Pod 能够连接到注册表。
2. 制定了所需的网络策略。
3. 必要时输入凭证。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。