在 Cisco Secure Workload 中管理策略生命周期

分段策略基础

分段和微分段策略的目的是只允许您的组织开展业务所需的流量，并阻止所有其他流量。目标是在不中断业务运营的情况下，减小网络的攻击面。

Cisco Secure Workload 分段策略会根据流量的源、目标、端口、协议和通常特定于平台的一些其他属性来允许或阻止流量。

您可以手动创建一些策略，并使用 Cisco Secure Workload 强大的自动策略发现功能根据现有网络流量来生成其他策略。

您可以查看、优化和分析自己的策略，然后在确信它们仅允许您的组织需要的流量时执行这些策略。

重要事项 微分段实质上会在每个工作负载周围创建防火墙。

因此，要使流量在每个使用者对之间传递，通信的两端都必须允许进行通信：使用者和提供者必须各自具有允许流量通过的策略。

注释 术语防火墙规则、边缘和集群边缘有时用于表示“策略”。

使用工作空间管理策略

工作空间（以前称为“应用工作空间”或“应用”）是您处理和管理策略的地方。

您可以在与特定范围关联的一个或多个工作空间中为该范围执行所有与策略相关的活动，如创建、分析和执行策略。

每个工作空间都提供了一个孤立的环境，可以在不影响其他工作空间的情况下进行试验。

控制用户访问工作空间

工作空间是供同一团队的多个用户使用的共享文档。

要控制对工作空间的访问，请为与工作空间关联的范围分配用户角色。有关详细信息，请参阅“角色”部分。

使用策略：导航至工作空间页面

- **要使用策略、查看现有应用工作空间或创建新应用工作空间，请执行以下操作：**

  从窗口的左侧的导航栏选择**防御 (Defend)** > **分段 (Segmentation)**。

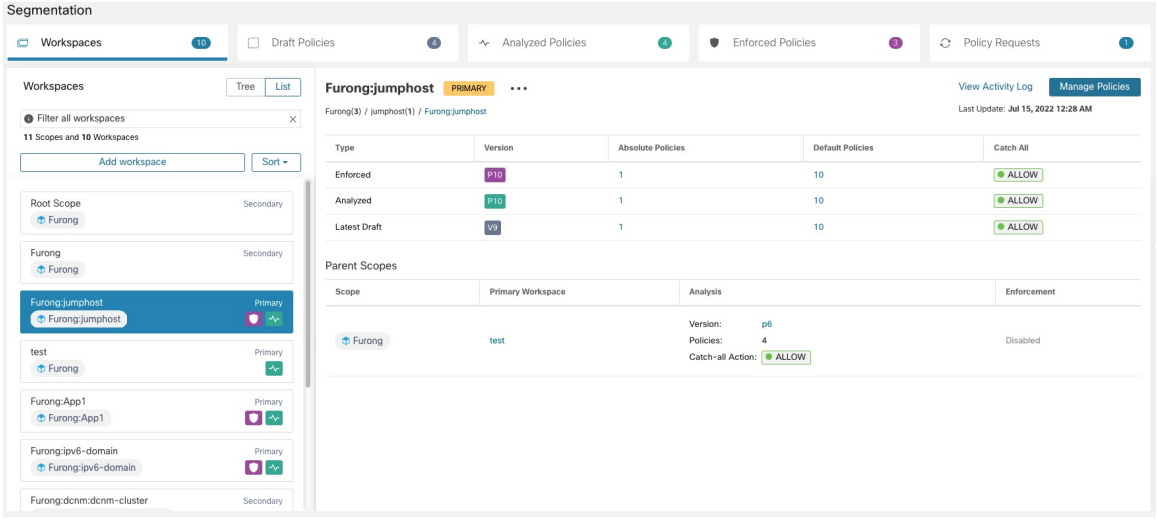
- **要查看特定工作空间，请执行以下操作：**

  在“工作空间”(Workspaces) 页面左侧的范围列表中，导航至与工作空间关联的范围，然后点击该工作空间。当前的活动工作空间会在列表中突出显示。

- **如果您正在查看工作空间并要返回工作空间列表，请执行以下操作：**

  点击您正在查看的页面左侧附近的**工作空间 (Workspaces)** 链接。

Figure 1: *“工作空间管理”(Workspace Management)* 页面



创建工作空间

要为某个范围创建策略，请先为该范围创建一个工作空间。

要创建工作空间，请执行以下操作：

1. 从窗口左侧的导航菜单中，选择**防御 (Defend)** > **分段 (Segmentation)**。
2. 在页面左侧的范围列表中，搜索或滚动到要创建策略的范围。
3. 将鼠标悬停在范围上方，直到出现一个蓝色加号，然后点击它。
4. 填写表单，完成后点击**创建 (Create)**。

如果该范围存在工作空间，则任何附加工作空间都会创建为辅助工作空间。

主要和辅助工作空间

对于每个范围，您可以创建一个主工作空间和多个辅助工作空间。

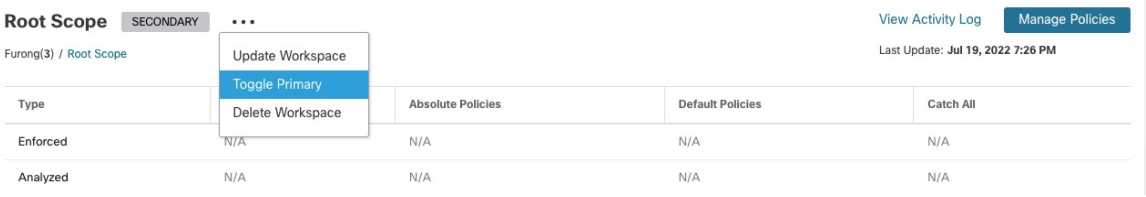
只能执行主工作空间。仅适用于主工作空间的其他功能包括能够管理使用者和提供者位于不同范围内的策略；实时策略分析；合规性报告；和协作安全策略定义。

如果想保留主工作空间中的现有策略，可以使用辅助工作空间来试验策略。

要将工作空间更改为主工作空间或辅助工作空间，请执行以下操作：

您可以随时将工作空间从主工作空间切换到辅助工作空间，也可以随时将其切换为辅助工作空间，只需点击页面顶部工作空间名称旁边的菜单图标，然后选择**切换主要**。

Figure 2: 在主工作空间和辅助工作空间之间切换



重命名工作空间

要重命名工作空间，请执行以下操作：

点击靠近页面顶部显示的工作空间类型（主或辅助）旁边的 •••，然后选择**更新工作空间 (Update Workspace)**。

查看范围内的工作负载

在任何工作空间中，点击**匹配资产 (Matching Inventories)** 选项卡。

在工作空间内搜索

要在工作空间中搜索工作负载、集群或策略，请执行以下操作：

1. 选择**防御 (Defend)** > **分段 (Segmentation)**。
2. 从左侧的范围列表中，点击所需的范围和工作空间。
3. 点击**管理策略 (Manage Policies)**。
4. 点击放大镜。
5. 输入搜索条件。

搜索条件

多个条件会被视为逻辑 AND。

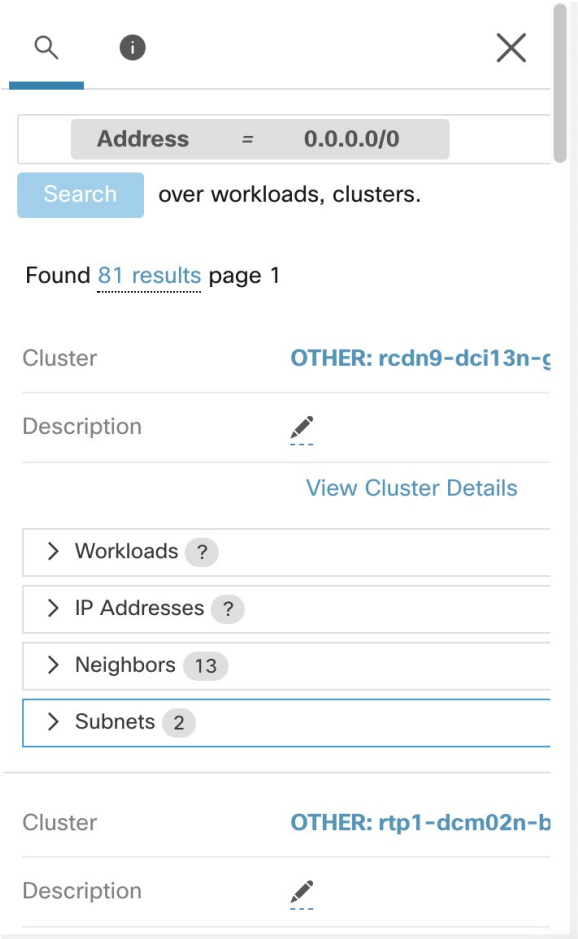
对于 IP 地址和数值：

- 使用逗号表示逻辑 OR：“port: 80,443”。
- 数字值还支持范围查询：‘port: 3000-3999’。

过滤器	说明
名称	输入集群或工作负载名称。执行区分大小写的子字符串搜索。
说明	搜索集群说明。

过滤器	说明
已批准	使用值“true”或“false”匹配已批准的集群。
地址	使用 CIDR 表示法输入子网或 IP 地址（例如，10.11.12.0/24）。匹配与此子网重叠的工作负载或集群。
超网	输入使用 CIDR 表示法的子网（例如 10.11.12.0/24），以匹配工作负载完全包含在此子网中的集群。
过程	使用区分大小写的子字符串搜索来搜索工作负载进程。
进程 UID	搜索工作负载进程用户名。
端口	搜索工作负载提供者端口和策略端口。
协议	搜索工作负载提供者协议和策略协议。
使用者名称	匹配策略的使用者集群名称。执行区分大小写的子字符串匹配。
提供者名称	匹配策略的提供者集群名称。执行区分大小写的子字符串匹配。
使用者地址	匹配使用者地址与提供的 IP 或子网重叠的策略。
提供者地址	匹配提供者地址与提供的 IP 或子网重叠的策略。

搜索示例

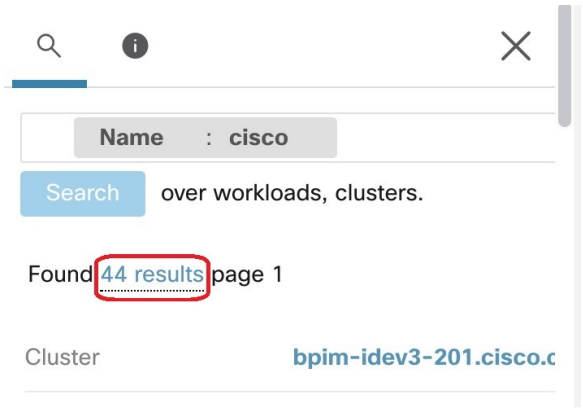


按特定类型过滤搜索结果

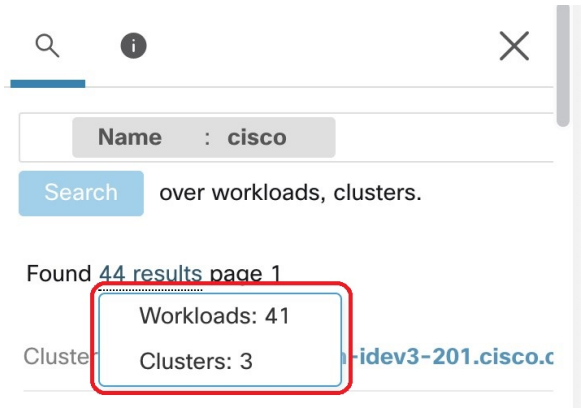
搜索结果可能包括多种类型的对象，例如工作负载和集群。

按特定类型来过滤搜索结果：

1. 点击结果总数：



2. 从下拉列表中选择类型：



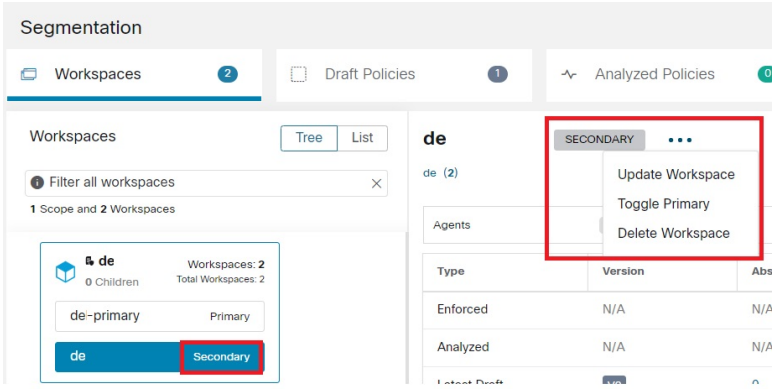
3. 系统将添加类型过滤器，然后重新运行搜索。

删除工作空间

只能删除辅助 (nonprimary) 工作空间。要将工作空间切换到辅助工作空间，请参阅主要和辅助工作空间, on page 3。

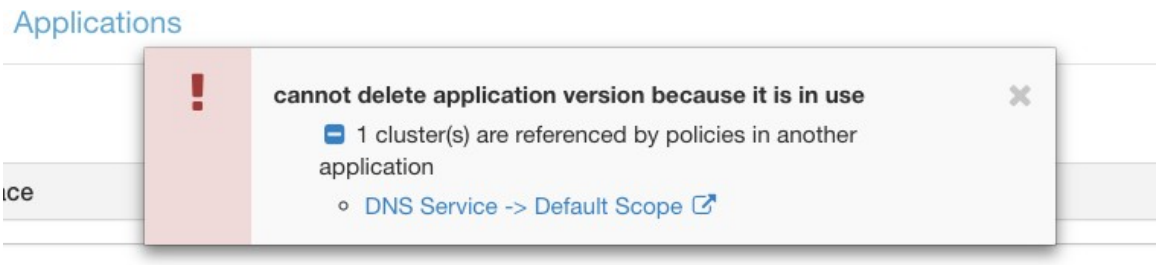
要删除工作空间，请执行以下操作：

1. 依次选择**防御 (Defend) > 分段 (Segmentation)**。
2. 在页面左侧的范围列表中，导航至包含要删除的工作空间的范围，然后点击它。
3. 点击要删除的工作空间。
4. 点击**辅助 (Secondary)** 旁边的•••，然后选择**删除工作空间 (Delete Workspace)**。



如果一个工作空间的工作负载或集群因提供服务而被另一个工作空间中的策略引用，则无法删除依赖的工作空间，并将返回依赖关系列表。此信息可用于修复依赖关系。

Figure 3: 防止删除工作空间的项目列表



在极少数情况下，可能存在交叉依赖关系，其中工作空间 A 依赖于工作空间 B 中的集群，而工作空间 B 依赖于工作空间 A 中的集群。在这种情况下，必须删除单个策略或已发布的策略版本 (p*)。“删除限制”错误提供了指向所有策略的链接，因此可以完成此操作。

要删除 p* 版本，请参阅查看、比较和管理分析的策略版本, on page 119或查看、比较和管理已执行的策略版本, on page 134。

关于策略

策略属性

Table 1: 策略属性

安全策略属性	说明
为其定义策略的范围	策略通常只影响与定义策略的工作空间相关联的范围中的工作负载。 （但是，另请参阅解决策略复杂性问题, on page 82下的主题。） 有关详细信息，请参阅策略示例, on page 10。

安全策略属性	说明
使用者	服务的客户端或连接的发起方。 任何范围、集群或资产过滤器均可用作策略中的使用者。 请参阅关于策略中的使用者和提供者, on page 10中的重要信息。
提供者	连接的服务器或接收方。 任何范围、集群或资产过滤器均可用作策略中的提供者。 请参阅关于策略中的使用者和提供者, on page 10中的重要信息。
协议和端口	应允许或阻止的提供者提供的服务的服务器（侦听）端口和 IP 协议。
操作	ALLOW 或 DENY：是允许还是丢弃在给定服务端口/协议上从使用者到提供者的流量。
等级和优先级	有关工作空间中策略等级和优先级的详细信息，请参阅策略等级：绝对、默认和捕获全部, on page 9。

策略等级：绝对、默认和捕获全部

策略等级确定策略是否被优先级列表中较低（或范围树中较低范围内）的更具体的策略覆盖。每个范围中优先级最低的策略始终是“捕获全部”规则。

策略等级	说明
绝对	即使绝对策略与策略列表中位置较低（因此优先级较低）或范围树中位置较低的特定于应用的策略相矛盾，这些策略也会生效。通常使用绝对策略来执行最佳实践，保护不同的区域或隔离区特定的工作负载。例如，使用绝对策略来控制流向 DNS 或 NTP 服务器的流量，或者满足法规要求。 绝对策略列在策略优先级列表中默认策略的上方。
默认	默认策略可被策略列表中较低级别的策略或范围树中较低级别的范围所覆盖。通常，精细策略是默认策略。 默认策略列在策略优先级列表中的绝对策略下方。

策略等级	说明
捕获全部	每个工作空间都有一个捕获全部策略，用于处理与工作空间中任何明确指定的策略都不匹配的每个方向的流量。捕获全部操作可以是“允许”(Allow)或“拒绝”(Deny)。 通常，按如下方式设置捕获全部策略： • **允许**范围树中较高范围内的流量，以便树中较低范围的策略可以评估流量。 • **拒绝**范围树底部最具体枝叶上的流量。 这样，树中所有范围的策略都有机会匹配流量，同时阻止不匹配任何范围中任何策略的流量。 捕获全部规则适用于工作空间中每个工作负载上的所有接口。

策略继承和范围树

由于您的工作负载被整理到层次结构范围树中，因此您可以在树顶部或附近的范围中创建常规策略一次，然后这些策略可以选择性地应用于树中该范围以下所有范围中的所有工作负载。

您可以指定一般策略是否可以被树中更低级别的特定策略覆盖。

请参阅策略等级：绝对、默认和捕获全部，第 9 页。

关于策略中的使用者和提供者

策略中规定的使用者和提供者具有以下作用：

- 它们指定了接收策略或防火墙规则的工作负载或 Cisco Secure Workload 代理。
- 它们指定了安装在工作负载上的防火墙规则所适用的 IP 地址集。

如果主机有多个接口（IP 地址），则策略适用于所有接口。

重要事项 以上是防火墙规则在工作负载上编程的默认行为。如果防火墙规则中指定的 IP 地址与安装策略的工作负载的 IP 地址不同，则需要在策略中将使用者和提供者这两个用途分开。请参阅有效使用者或有效提供者，第 101 页。

策略示例

以下策略示例说明了定义策略的范围的重要性、策略继承的影响，以及使用资产过滤器创建精确策略或适用于多个范围内工作负载的策略。

请考虑以下涉及三个范围的示例：

- **Apps**

  及其子范围

  - **Apps:HR** 和
  - **Apps:Commerce**

此外，资产过滤器 PRODUCTION 和 NON-PRODUCTION 分别指定生产和非生产主机。（您可以定义资产过滤器以应用于某个范围内或跨范围的主机。）

假设在**应用**范围内定义以下策略：

```
DENY PRODUCTION -> TCP 端口 8000（绝对）上的 NON-PRODUCTION
```

由于此策略是在**应用**范围下的主工作空间中定义的绝对策略，因此它会影响作为**应用**范围成员的所有生产/非生产主机，包括其后代范围的成员（属于 **Apps:HR** 和 **Apps:Commerce** 范围的主机）。

现在考虑在与 **Apps:HR** 范围关联的工作空间下定义完全相同的策略的情况。在这种情况下，策略只能影响属于 **Apps:HR** 范围成员的 PRODUCTION/NONPRODUCTION 主机。更准确地说，此策略会导致非生产 HR 主机（如有）上的入站规则拒绝来自**任何** PRODUCTION 主机的 TCP 端口 8000 上的连接，而生产 HR 主机（如有）上的出站规则会丢弃到**任何** NONPRODUCTION 主机的连接请求。

创建和发现策略

创建策略的最佳实践

- 有关整个分段过程的概述，请参阅 开始使用分段和微分段 及其子主题。
- 手动创建广泛应用于整个网络的策略。

  例如，阻止从网络外部向工作负载发送不需要的流量，或隔离易受攻击的主机。

  - 在范围树顶部或附近创建手动策略。

    例如，要阻止从网络外部到网络中每台主机的所有流量，可将策略置于树顶的范围中。

  - 如果您希望能够覆盖某些工作负载的一般策略（例如，按照上面的示例，希望阻止来自网络外部的一般访问，但又希望某些工作负载可从网络外部访问），则可将高级策略创建为默认策略。然后为适用的工作负载创建特定的策略。
  - 考虑使用模板来加速策略创建。
  - 请参阅手动创建策略，第 12 页、特定用途的策略，第 13 页和策略模板，第 15 页。

- （可选）一开始时为树分支中的所有范围自动发现树顶部附近的范围内的策略，以创建允许所有现有流量并限制未来不需要的流量的粗略策略。然后，您就可以建立更精细的策略，保护网络免受不必要或不需要的流量影响。

  有关信息，请参阅发现一个范围或范围树分支的策略，第 23 页和自动发现策略，第 20 页。

- 在准备好发现更精细的策略时，可自动为范围树底部或附近的范围发现策略，特别是在单个应用的范围中。

  有关信息，请参阅发现一个范围或范围树分支的策略，第 23 页和自动发现策略，第 20 页。

- 确保您的策略能处理不常见或不经常发生的活动和情况，如确保您的策略能解决不常见或不经常发生的活动和情况，如故障转移、从备份恢故障转移、从备份恢复、一年一次的活动等。
- 在确定并允许应用所需的流量后，再查找任何不应该出现的流量，并阻止此类情况的发生。

  首先查看进出最敏感应用的流量。

  例如，如果您发现从面向客户的 Web 应用到绝密研发应用数据库的流量，则需要进行调查。

- 与同事合作，确保正确的策略适用于正确的工作负载。
- 最初，在执行策略时，请考虑将捕获全部设置为“允许”(Allow)。然后，监控流量以查看与捕获全部规则匹配的流量。当没有必要的流量与捕获全部规则匹配时，可以将捕获全部设置为“拒绝”(Deny)。

手动创建策略

通常，您可以手动创建要广泛应用于整个网络的策略。

例如，您可以手动创建策略来执行以下操作：

- 允许所有内部工作负载访问 NTP、DNS、Active Directory 或漏洞扫描服务器。
- 除非得到明确许可，否则拒绝组织外的所有主机访问网络内的主机。
- 隔离易受攻击的工作负载。

您可以创建无法被更精细应用的策略覆盖的绝对策略，以及在存在更具体策略的情况下可以覆盖的默认策略。

您可以为靠近树顶的范围创建手动策略。

开始之前

- （可选）考虑使用**防御 (Defend) > 策略模板 (Policy Templates)** 中提供的模板之一。
- （可选）如果知道有一组工作负载会收到相同的策略，则可以使用资产过滤器对它们进行分组，这样就可以轻松地将策略应用到这组工作负载。资产过滤器可以只适用于一个范围，也可以适用于任何范围中的工作负载。请参阅创建资产过滤器。
- 确保此范围中的工作负载是您期望在此范围中出现的工作负载。请参阅查看范围内的工作负载，第 4 页。

过程

步骤 1 依次点击**防御 (Defend) > 分段 (Segmentation)**。

步骤 2 在左侧列表中，搜索或导航到要创建策略的范围。

步骤 3 点击要在其中创建策略的范围和工作空间。

如果尚未为此范围创建工作空间，请参阅创建工作空间，第 3 页。

步骤 4 点击**管理策略 (Manage Policies)**。

步骤 5 点击**策略 (Policies)** 选项卡（如果尚未选中）。

步骤 6 点击**添加策略 (Add Policy)**。

如果您没有看到“添加策略”(Add Policy) 按钮，请参阅如果“添加策略”(Add Policy) 按钮不可用，第 13 页。

步骤 7 输入信息。

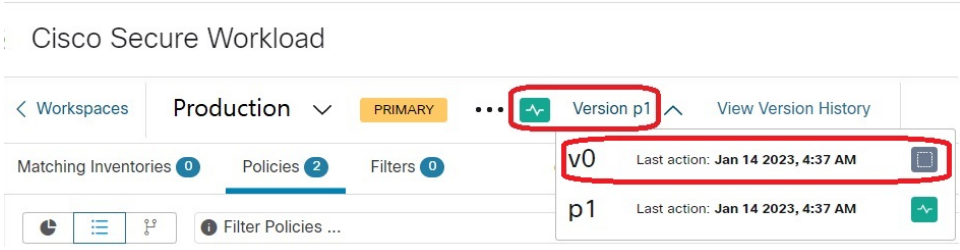
- 有关**绝对 (Absolute)** 复选框的信息，请参阅策略等级：绝对、默认和捕获全部，第 9 页。通常，如果您要创建不希望出现例外的策略，请启用此复选框。
- **优先级 (Priority)** 用于设置策略在列表中的顺序。有关设置策略顺序的详细信息，请参阅策略优先级，第 82 页和子主题。（您可以稍后再设置策略顺序。）
- 使用者和提供者可以是整个范围，或者，如果您使用资产过滤器创建了工作负载组（或同一范围的集群，但不太理想），则可以选择这些工作负载组。

下一步做什么

确保**捕获全部**操作适用于工作空间。请参阅策略等级：绝对、默认和捕获全部，第 9 页。

如果“添加策略”(Add Policy) 按钮不可用

如果您尝试创建策略并且**添加策略 (Add Policy)** 按钮不可用，请点击页面顶部显示的版本，然后选择最新的“v”版本（用灰色方块表示）：



特定用途的策略

创建 InfoSec 策略以阻止来自网络外部的流量

使用此步骤可快速创建一套完整的策略，以控制从网络外部进入网络的流量。默认策略集只允许使用常用端口和协议的流量，并拒绝所有其他流量。您可以修改默认策略集以满足自己的需求。

开始之前

如果满足以下标准，请使用此程序：

- 范围树在根范围的正下方有一个名为**内部 (Internal)** 的范围。

  此范围的成员包括或将要包括内部网络上所有工作负载的子网。

- 内部范围中尚未定义任何策略。

注释　或者，您可以使用**防御 (Defend) > 策略模板 (Policy Templates)** 中提供的 **InfoSec** 模板，通过几个额外的步骤来完成此任务。

过程

步骤 1　依次选择**防御 (Defend) > 分段 (Segmentation)**，

步骤 2　点击**内部**范围，然后点击主工作空间。

如果主工作空间尚不存在，请点击 + 按钮创建一个。

步骤 3　点击**管理策略 (Manage Policies)**。

步骤 4　点击**添加 InfoSec 策略 (Add InfoSec Policies)**。

步骤 5　验证列表中的所有策略（包括协议和端口）都是您想要的策略，并根据需要删除或修改策略。

步骤 6　点击**创建 (Create)**。

下一步做什么

（可选）向“内部”范围添加任何其他策略，例如允许特定工作负载访问某些外部流量的策略。

将任何特定策略放在列表中更通用的策略下方。

创建策略以解决即时威胁

如果必须解决直接威胁，可以手动将窄范围的绝对策略添加到范围树顶部或附近的范围，然后为该范围执行主工作空间。

修复威胁后，您可以删除该策略并重新执行工作空间。

创建用于隔离易受攻击的工作负载的策略

您可以执行以下操作：

- 提前创建策略，自动隔离存在特定已知漏洞或您指定的漏洞严重性阈值的工作负载。
- 创建策略，立即隔离检测到已知漏洞并认为问题足够严重的工作负载。

本主题概述了这两种情况的处理过程。

开始之前

查看查看漏洞控制面板以了解需要哪些策略。

过程

步骤 1 创建定义要隔离的漏洞或漏洞严重性阈值的资产过滤器：

a) 从窗口左侧的导航栏中，依次选择**整理 (Organize)** > **资产过滤器 (Inventory Filters)**。
b) 点击**创建资产过滤器 (Create Inventory Filter)**
c) 点击**查询 (Query)** 旁边的 **(i)** 按钮，然后输入 **CVE** 以查看相关过滤器选项。
d) 输入确定要隔离的工作负载的过滤条件。
e) 确保未选择**将查询限制为所有权范围 (Restrict query to ownership scope)**。

步骤 2 创建策略以隔离受影响的工作负载：

有关一般说明，请参阅手动创建策略，第 12 页。

建议：

- 在范围树顶部附近的**内部 (Internal)** 或其他范围内创建策略。
- 除非您想允许例外情况，否则策略应是绝对策略。请务必创建策略来解决任何异常。
- 为使用者和提供者创建单独的策略。
- 将每个策略的优先级设置为较低的数字，这样它就会在列表中的其他策略之前被执行。
- 将操作设置为**拒绝 (Deny)**。

步骤 3 查看、分析和执行策略。

下一步做什么

创建警报，以便在流量触及该策略时收到通知，从而修复问题并将流量恢复到易受攻击的工作负载。请参阅配置告警。

策略模板

策略模板用于将类似的策略集应用于多个工作空间。

Cisco Secure Workload 包括一些预定义的模板，而您也可以创建自己的模板。

策略模板需要根范围上的范围所有者功能。

系统定义的策略模板

要查看可用的策略模板，请导航至**防御 (Defend) > 策略模板 (Policy Templates)**。

要使用策略模板，请参阅应用模板 ， 第 19 页。

要修改系统定义的模板，请下载 JSON 文件并进行编辑，然后再上传。

创建自定义策略模板

策略模板的 JSON 架构

策略模板 JSON 架构旨在模仿导出工作空间的架构。您可以在工作空间中创建一组策略，将其导出为 JSON，修改 JSON，然后导入为策略模板。

属性	类型	说明
name	字符串	（可选）在导入期间用作模板的名称。
description	字符串	（可选）在应用过程中显示的模板说明。
parameters	参数对象	模板参数，请参阅以下内容。
absolute_policies	策略对象数组	（可选）绝对策略数组。
default_policies	策略对象数组	（必需）默认策略数组，可以为空。

参数对象

参数对象为可选，但可用于将过滤器动态定义为模板的参数。将使用 `consumer_filter_ref or provider_filter_ref` 策略属性来引用这些参数。

参数对象的键是引用名称。值是具有必需 `"type": "Filter"` 和可选说明的对象。参数对象示例如下所示：

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

可以在策略对象中引用这些参数，例如：`"consumer_filter_ref": "HTTP Consumer" or "provider_filter_ref": "HTTP Provider"`。

特殊参数引用

一些特殊引用会自动映射到过滤器，无需作为参数进行定义。

参考	说明
_workspaceScope	解析为应用模板的工作空间的范围。
_rootScope	解析为根/顶级范围。

策略对象

为了保持与工作空间导出 JSON 的兼容性，策略对象包含使用者和提供者的多个密钥。解决方法如下：

```
if *_filter_ref is defined
  use the filter resolved by that parameter
else if *_filter_id is defined
  use the filter referenced by that id
else if *_filter_name is defined
  use the filter that has that name
else
  use the workspace scope.
```

如果无法按照上述定义解析过滤器，则在应用和上传时都会返回错误。

属性	类型	说明
action	字符串	（可选）策略的操作：ALLOW 或 DENY（默认为 ALLOW）。
priority	整数	（可选）策略的优先级（默认值为 100）。
consumer_filter_ref	字符串	对参数的引用。
consumer_filter_name	字符串	按名称对过滤器的引用。
consumer_filter_id	字符串	已定义范围或资产过滤器的ID。
provider_filter_ref	字符串	对参数的引用。
provider_filter_name	字符串	按名称对过滤器的引用。
provider_filter_id	字符串	已定义范围或资产过滤器的ID。
l4_params	array of l4params	允许的端口和协议列表。
属性	类型	说明
proto	整数	协议整数值（NULL 表示所有协议）。

属性	类型	说明
port	整数	端口的包含范围，例如 [80, 80] 或 [5000, 6000]（NULL 表示所有端口）。

L4param 对象

属性	类型	说明
proto	整数	协议整数值（NULL表示所有协议）。
port	整数	端口的包含范围，例如 [80, 80] 或 [5000, 6000]（NULL 表示所有端口）。

模板示例

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

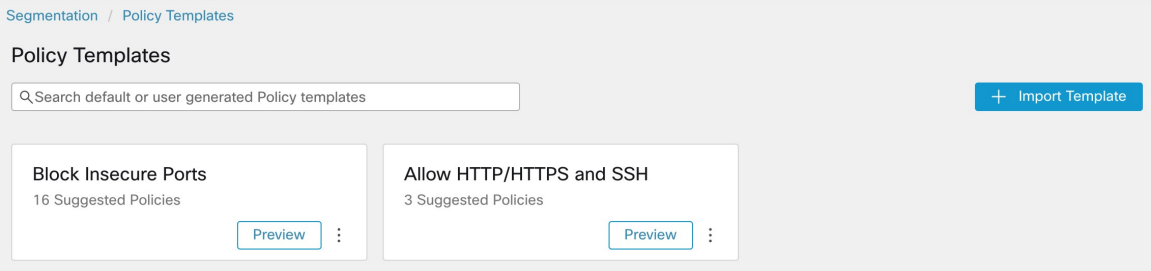
模板导入

策略模板显示在“策略模板”(Policy Templates) 页面上，可从“分段”(Segmentation) 主页面访问。在这里，可以使用“导入模板”(Import Template) 按钮导入/上传模板。

上传模板时，系统会验证模板的正确性。系统会提供有用的错误列表，以用于调试任何问题。

模板上传后，即可应用、下载或更新其名称和说明。

Figure 4: 显示可用模板



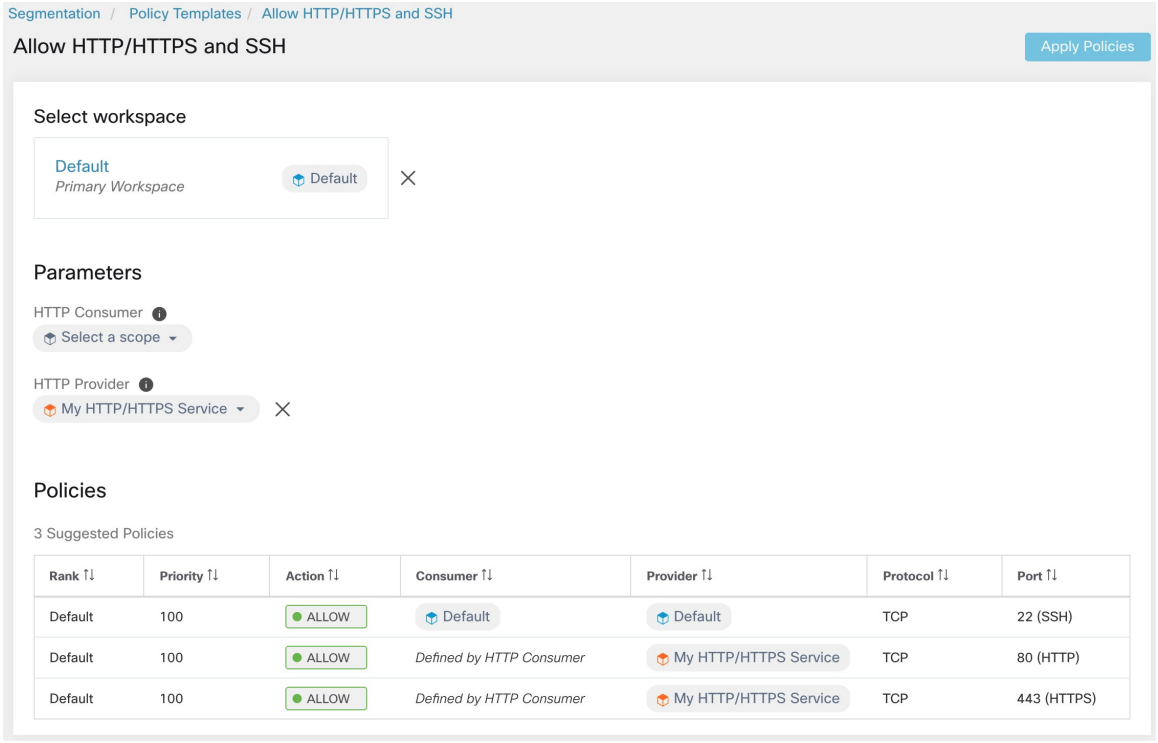
应用模板

将模板应用到工作空间需要执行几个步骤：

1. 选择要预览的模板。
2. 选择要应用模板的工作空间。
3. 如有必要，请填写参数。
4. 查看策略。
5. 应用策略。

策略将被添加到所选工作空间的最新版本。通过模板创建的策略可以使用 `From Template? = true` 过滤器。

Figure 5: 应用策略模板



自动发现策略

自动策略发现（有时称为策略发现，以前称为应用依赖关系映射 (ADM)）会使用现有流量和其他数据来执行以下操作：

- 根据现有的成功网络活动建议一组“允许”策略。

  这些策略的目标是识别组织所需的流量，同时阻止所有其他流量。

- 根据计算行为的相似性将工作负载分组到集群中

  例如，如果一个应用包括多个网络服务器，那么这些服务器可能会集群在一起。

  有关详细信息，请参阅集群, on page 72。

您可以发现每个范围的策略。通常，您会在范围树的底部或接近底部的位置发现范围的策略，例如在应用级别。但是，在初始部署时，您可能希望在更高级别的范围内发现策略，这样在创建更精细的策略时，您就准备好了通用的临时策略。

您可以根据需要随时发现策略，并根据其他信息完善建议的策略。

您可以手动修改建议的策略和集群，和/或批准其中的任何一项，这样这些策略和集群就会沿用下去，而不会在后续的发现运行中被修改。

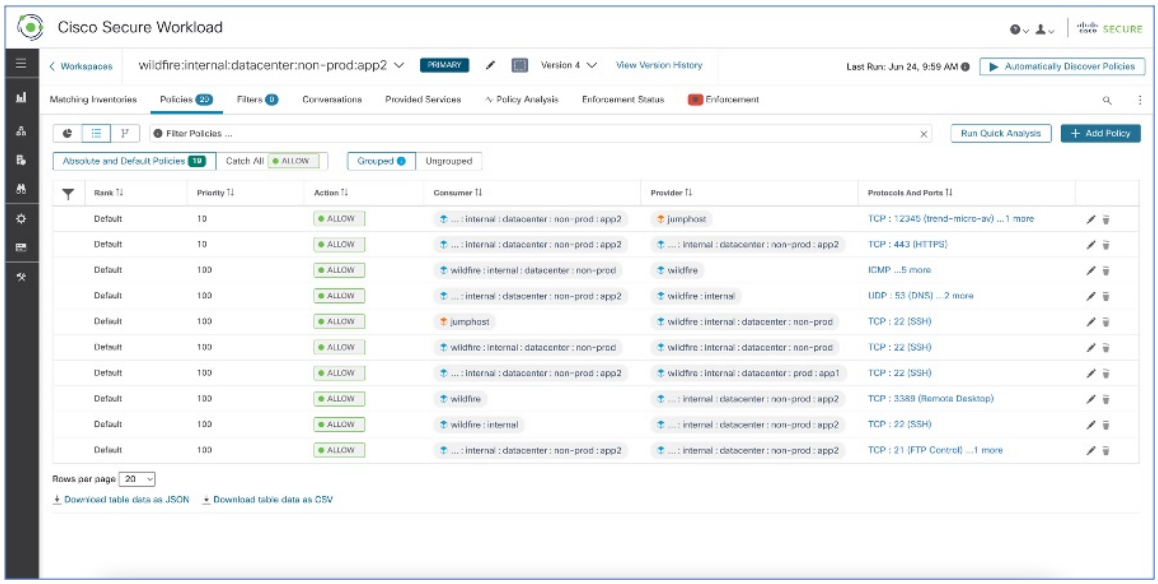
工作空间中既可以包含手动创建的策略，也可以包含发现的策略。

发现策略后，您将在执行策略之前对其进行查看和分析。

要开始发现策略，请参阅如何自动发现策略, on page 21。

有关详细信息，请参阅策略发现详细信息, on page 21。

Figure 6: 示例：自动发现的策略



策略发现详细信息

有关自动策略发现的其他信息：

- 自动策略发现会考虑在所选时间范围内至少有一个终端是范围内成员工作负载的对话。范围中的成员关系仅以最新的范围定义为依据，以前的成员身份不在考虑之列。
- 默认情况下，策略发现会通过分析通信流（“对话”）来生成策略和集群，但也可以选择考虑其他信息，例如在工作负载上运行的进程或负载均衡器配置。

  请参阅发现策略时包括来自负载均衡器和路由器的数据 ， 第 36 页。
- 您可以发现范围内任何工作空间中的策略。每个工作空间的发现结果都与范围内其他工作空间的结果无关。
- 有关与自动策略发现相关的复杂概念的详细讨论，请参阅自动策略发现的高级功能 ， 第 28 页和解决策略复杂性问题 ， 第 82 页。

如何自动发现策略

执行以下步骤：在任何时候，您都可以决定重新发现策略。

根据需要与同事合作完成这些步骤。

步骤	相应操作	更多信息
1	上传和标记您的工作负载资产，并收集通知策略发现的流数据。	请参阅开始使用分段和微分段以及子主题。
2	选择是否发现以下对象的策略： • 单个范围内的工作负载 • 范围树分支中所有范围的工作负载	请参阅发现一个范围或范围树分支的策略，第 23 页。 （您随时可以再次发现策略。）
3	选择发现策略的范围。	这部分取决于您是为单个范围还是为范围树的分支发现策略。
4	选择要在其中发现策略的工作空间。	一般来说，您会在范围的主工作空间中发现策略，因为您只能在主工作空间中分析策略。（但是，您以后可以随时将工作空间更改为主要工作空间。） 如果您选择的范围还没有工作空间，请参阅创建工作空间，第 3 页。
5	确认您希望包含在策略发现中的资产。	验证策略发现将应用于的工作负载，第 25 页
6	（可选）创建资产过滤器，对要作为一个组处理的工作负载进行分组。	请参阅创建资产过滤器。
7	设置工作空间的**捕获全部 (Catch-all)**操作。	请参阅策略等级：绝对、默认和捕获全部，第 9 页
8	发现策略	自动发现策略，第 20 页 请务必完成“准备工作”部分中的前提条件。
9	查看和管理策略发现创建的集群（工作负载组）。 （此步骤仅适用于为单个范围发现策略；为树的分支发现策略时不会生成集群）。	请参阅集群，第 72 页以及子主题。 评估建议的集群，根据需要选择性地编辑集群成员资格，并批准（或更好地转换为资产过滤器）您希望永久保留的任何集群。
10	考虑策略继承和跨范围策略等复杂情况。	请参阅解决策略复杂性问题，第 82 页。
11	查看生成的策略。	请参阅审核自动发现的策略，第 104 页以及子主题
12	批准您要保留的策略。	审批策略，第 47 页

步骤	相应操作	更多信息
13	根据需要再次发现策略，以反映额外的流量数据、范围成员的变化或其他变化。	重要提示：在重新运行自动策略发现之前，第 50 页 您可以随时重新运行策略发现。 每次发现策略时，请查看并批准策略和集群。
14	运行实时分析，查看策略对实际流量的影响。	如果您认为自己的策略符合预期，请启动实时策略分析，第 111 页。 如果更改策略或重新发现策略，请重启策略分析（以分析当前策略）。
15	如果您重新发现策略或进行其他更改，请重启实时分析。	请参阅在更改策略后分析最新策略，第 119 页。
16	当您确信策略不会阻止重要流量时，请执行工作空间。	请参阅执行策略和子主题。
17	验证执行是否按预期工作。	请参阅验证执行是否按预期工作，第 130 页
18	（可选） 配置默认策略发现设置，在任何工作空间中发现策略时均可选择应用这些设置。	请参阅默认策略发现配置，第 45 页和链接主题。 由于这些是高级设置，建议您只有在有特殊需要时才进行更改。您可以在流程中根据需要随时更改。

发现一个范围或范围树分支的策略

如果在发现特定范围的策略时，任一选项都不可行，则会为您做出选择，而您不会看到选项选择。

表 2: 发现以下对象的策略

范围树的一个分支	单个范围
当您开始使用 Cisco Secure Workload 时，可以将此方法作为起点，以便快速生成一组允许现有流量的临时粗略策略，同时帮助保护您的网络免受未来的威胁。	使用此方法可对分段策略进行微调，并确保所有允许的流都在预料之中；策略数量越少，越容易发现任何需要调查的现有异常情况。
通常，此方法用于更接近范围树顶部的范围。 分支的顶部可以是树中的任何范围。	通常，此方法用于范围树底部或附近的范围，例如专用于单个应用的范围。
仅在一个范围内 - 即您选择的分支顶部的范围发现策略。	根据需要发现分支机构中每个范围的策略。

范围树的一个分支	单个范围
所选范围内的所有工作负载以及所有子范围和后代范围都将包含在发现中。	同时也是任何子范围成员的工作负载不会包括在该范围的发现中。 仅为**整理 (Organize) > 范围和资产 (Scopes and Inventory)** 页面上该范围的**未分类资产 (Uncategorized Inventory)** 选项卡中显示的工作负载生成策略。 您可以分别发现子范围和后代范围中工作负载的策略。
分支中所有范围的工作负载的所有策略都位于分支顶部的范围中。	假设您还为子范围和后代范围中的工作负载创建了策略，那么策略就会驻留在多个范围中。
此方法通常会生成大量策略。	但这种方法在任何单个范围中生成的策略都较少。
发现的策略适用于整个范围；该选项无法创建特定于范围内工作负载子集的策略。	此选项可以生成应用于使用者和/或提供者范围内的工作负载子集的策略。（工作负载可按生成的集群和/或配置的资产过滤器分组，而策略只适用于这些子集）。
所有策略都是在分支顶部的单个范围中创建的，因此当策略的使用者和提供者位于不同的范围中时，不需要执行额外的步骤。	允许不同范围内使用者和提供者之间的流量需要执行额外的步骤。 请参阅当使用者和提供者处于不同范围时：策略选项，第 88 页。
即使一个范围没有任何已安装代理的成员工作负载，只要子范围有代理或外部协调器或连接器来收集流数据，就可以运行发现。	范围必须具有成员工作负载，而这些工作负载已安装用于收集流数据的代理或外部协调器或连接器。
此选项仅适用于根范围所有者和站点管理员。	您必须具有为此范围创建策略的权限。
每个选项的代理和对话的最大数量都不同。请参阅与策略相关的限制。	
此选项以前是用于自动策略发现的“深度策略生成”(Deep Policy Generation) 高级配置选项。行为未发生变化。	这是以前自动策略发现的默认行为。
有关其他详细信息，请参阅发现范围树分支的策略：其他信息，第 24 页。	--

发现范围树分支的策略：其他信息

- 作为对话终端的所有工作负载，无论它们是否是运行策略发现的范围的成员，都将根据外部依赖关系列表中给出的自上而下的顺序来分配最高匹配范围标签。

- 有关为范围树的分支生成策略时可用的高级配置选项，请参阅：
  - 启用冗余策略删除， 第 42 页
  - 策略压缩， 第 38 页和相关的子主题，分层策略压缩， 第 38 页
- 目前，为自动策略发现显示的工作负载计数仅包括不属于子范围成员的工作负载。

验证策略发现将应用于的工作负载

在自动发现策略之前，请确认策略发现所基于的工作负载实际上是您所期望的工作负载集。发现的策略将从代理在这些工作负载上捕获的流数据生成。

开始之前

决定可以使用发现一个范围或范围树分支的策略， 第 23 页中的哪些选项。

过程

步骤 1 从左侧的导航菜单中，选择**防御 (Defend) > 分段 (Segmentation)**。

步骤 2 点击要在其中发现策略的范围。

步骤 3 点击要在其中发现策略的工作空间。

步骤 4 点击**管理策略 (Manage Policies)**。

步骤 5 点击**匹配资产 (Matching Inventories)**。

步骤 6 如果您发现单个范围的策略：

a) 点击**未分类资产 (Uncategorized Inventory)**

此页面显示不属于子范围成员的工作负载。（在标准自动策略发现中，仅在此范围内为不属于子范围成员的工作负载生成策略和集群。）

b) 点击 **IP 地址 (IP addresses)**。

此页面上的 IP 地址未安装 Cisco Secure Workload 代理。

由于这些 IP 地址没有安装代理，因此在此范围的自动策略发现过程中不会考虑这些 IP 地址，除非：

- 策略正在通过云连接器进行管理
- IP 地址是基于容器的资产，在这种情况下，单个工作负载会显示在 **Pod** 选项卡上，或者
- 工作负载恰好与策略发现期间考虑的此范围内的工作负载通信。

在发现策略之前，可考虑在有需要的工作负载上安装代理，并留出一些时间来积累流数据。

c) 点击**工作负载 (Workloads)**。

策略和集群仅针对此页面上的工作负载和 IP 地址选项卡上的 IP 地址生成，这些工作负载和 IP 地址满足上述指定的考虑标准。

d) 如果您有 Kubernetes 或 OpenShift 资产，您将看到一个**服务 (Services)** 选项卡和一个 **Pods** 选项卡。

如果您已在 Kubernetes/OpenShift 工作负载上安装代理，请同时检查这些选项卡上的资产。

e) 如果您有负载均衡器资产，则该资产将显示在**服务 (Services)** 选项卡上。

步骤 7 如果发现树的分支的策略：

a) 点击**所有资产 (All Inventory)**

此过程会为该范围中的所有工作负载生成策略（但不生成集群），无论它们是否也是子范围的成员。

b) 点击 **IP 地址 (IP addresses)**。

此页面上的 IP 地址未安装 Cisco Secure Workload 代理。

由于这些 IP 地址没有安装代理，因此在此范围的自动策略发现过程中不会考虑这些 IP 地址，除非：

- 策略通过云连接器进行管理
- IP 地址是基于容器的资产，在这种情况下，单个工作负载会显示在 **Pod** 选项卡上，或者
- 工作负载恰好与策略发现期间考虑的此范围内的工作负载通信。

在发现策略之前，可考虑在这些工作负载上安装代理，并留出一些时间来积累流数据。

c) 点击**工作负载 (Workloads)**。

策略仅针对此页面上的工作负载和 IP 地址选项卡上的 IP 地址生成，这些工作负载和 IP 地址满足上述指定的考虑标准。

d) 如果您有 Kubernetes 或 OpenShift 资产，您将看到一个**服务 (Services)** 选项卡和一个 **Pods** 选项卡。

如果您已在 Kubernetes/OpenShift 工作负载上安装代理，请同时检查这些选项卡上的资产。

e) 如果您有负载均衡器资产，则该资产将显示在**服务 (Services)** 选项卡上。

步骤 8 验证工作负载是否符合您的预期。

自动发现策略

使用此程序可根据网络中的现有流量生成建议的“允许”策略。

您可以随时重新发现策略。

开始之前

- 首先收集流数据，然后才能有效地自动发现策略。

  通常，这意味着您已在范围内的工作负载上安装了代理，或已使用云连接器或外部协调器配置并收集了数据。

自动策略发现使用的流摘要数据会每 6 小时计算一次。因此，在初始部署 Cisco Secure Workload 时，除非此类数据可用，否则无法进行自动策略发现。

流数据越多，通常会产生更准确的结果。

在执行策略之前，您应收集足够的数据以包括仅定期（每月、每季度、每年等）发生的流量。例如，如果应用生成的季度报告从应用在其他时间无法访问的源收集信息，则应确保流数据中至少包含一个报告生成流程实例。

- 完成如何自动发现策略，第 21 页中此步骤之前的所有步骤。
- 符合策略发现相关的 与策略相关的限制。

  如有必要，可将较大的范围分解成较小的子范围。
- 在发现策略前提交任何范围更改，否则任何已配置的排除过滤器可能无法按预期匹配（排除）流量。请参阅确认更改。

重要事项 如果要重新运行策略发现，请先参阅重要注意事项：重要提示：在重新运行自动策略发现之前，第 50 页。

过程

步骤 1 依次选择**防御 (Defend)** > **分段 (Segmentation)**。

步骤 2 在左侧窗格的范围树或范围列表中，滚动到或搜索要生成策略的范围。

步骤 3 点击范围中的工作空间（主或辅助）。

步骤 4 点击**管理策略 (Manage Policies)**。

步骤 5 点击**发现发现策略 (Automatically Discover Policies)**。

步骤 6 如果看到发现分支或整个范围的策略的选项，请选择一个选项。

如果没有看到选项，则表示您正在发现策略的范围只能有一个选项。

有关详细信息，请参阅发现一个范围或范围树分支的策略，第 23 页。

步骤 7 选择要包括的流数据的时间范围。

尝试找到合适的时间范围；您可以根据需要随时生成策略，以获得最佳结果。

时间范围越短，产生结果的速度越快，但产生的结果也可能越少。

一般来说，时间范围越长，策略越准确。但是，如果范围定义发生了变化，则不要包含变化前的日期。

如果适用，您的时间范围应包括定期（每月、每季度、每年等）发生的流量。例如，如果应用生成的季度报告从其他时间无法访问的源收集信息，则应确保时间范围至少包括该报告生成流程的一个实例。

要配置超过最近30天的时间范围，请选择**自定义**范围，然后在下拉时间选择构件下填写所需的开始时间和结束时间。

步骤 8 （可选）指定高级设置。

通常，建议您不要更改初始发现运行的高级设置，然后仅根据需要进行更改以解决特定问题。

有关详细信息，请参阅自动策略发现的高级配置，第 35 页。

步骤 9 点击**发现策略 (Discover Policies)**。生成的策略显示在此页面上。

下一步做什么

- 查看停止正在进行的自动策略发现，第 28 页。
- 返回如何自动发现策略，第 21 页并继续执行表中的后续步骤。
- 您可以随时重新发现策略。有关应首先执行的操作，请参阅重要提示：在重新运行自动策略发现之前，第 50 页。

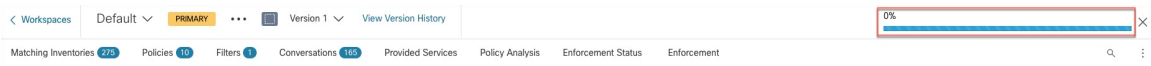
停止正在进行的自动策略发现

自动策略发现的进度始终显示在标头中。导航至其他工作空间不会影响进度。

要在运行过程中停止运行，请点击**中止**按钮。

运行完成后，系统会显示一条消息。如果成功，**点击查看结果 (Click to see results)** 会导航至显示运行前后更改的其他视图。如果自动策略发现失败，则会显示另一条消息和原因。

Figure 7: 自动策略发现进度



自动策略发现的高级功能

您必须指定发现运行的时间范围。如有必要，您可以配置高级选项。

您可以为每个工作空间配置高级选项，或为所有工作空间（整个根范围）设置默认值，然后根据需要修改单个工作空间的设置。

表 3: 配置自动策略发现的高级选项

对于工作空间	对于所有工作空间
单个工作空间的选项说明（第 1 列）也适用于所有工作空间（第 2 列）	
外部依赖关系，第 31 页	默认策略发现配置，第 45 页
自动策略发现的高级配置，第 35 页	默认策略发现配置，第 45 页
排除过滤器，第 29 页	默认排除过滤器，第 45 页

排除过滤器

如果某些流生成不需要的策略，则可以使用排除过滤器从自动策略发现中排除这些流。

例如，要在最终允许列表模型中禁止某些协议（例如ICMP），您可以创建一个排除过滤器，并将协议字段设置为 ICMP。

Note

- 出于策略生成和集群的目的，系统会排除与排除过滤器匹配的对话，但会保留在对话视图中，并带有红色的“已排除”图标（请参阅对话中的表视图）。同样，此类对话中的工作空间事件的工作负载也会保持可见。
- 使用工作空间中的集群或过滤器定义的排除过滤器仅在主工作空间中有效（否则，其集群定义将对标签系统不可见，并且不会排除任何匹配的对话）。
- 排除过滤器是版本控制的；要跟踪修改，请参阅活动日志和版本历史记录。
- 有关排除过滤器数量的限制，请参阅与策略相关的限制。

您可以创建以下一项或两项，然后在发现策略时启用其中一项或两项：

- 每个工作空间的排除过滤器列表。
- 适用于租户中所有工作空间的默认排除过滤器列表。

您还可以启用或禁用默认策略发现配置的任一或两个列表。

有关说明，请参阅配置、编辑或删除排除过滤器, on page 29和启用或禁用排除过滤器, on page 31。

配置、编辑或删除排除过滤器

您可以使用此过程为单个工作空间创建排除过滤器列表，或创建所有工作空间都可用的默认排除过滤器列表。

过程

步骤 1 执行以下操作之一：

要想	相应操作
为特定工作空间配置排除过滤器	导航至工作空间，然后执行以下操作之一： • 点击**管理策略 (Manage Policies)**，然后点击页面右上角附近的 ⋮，并选择**排除过滤器 (Exclusion Filters)**。 • 在自动策略发现配置页面中，点击“高级配置”(Advanced Configurations) 部分中的**排除过滤器 (Exclusion filters)** 链接。 • 删除已发现的策略；您将看到一个用于创建排除过滤器的选项。

要想	相应操作
配置可用于任何工作空间的默认排除过滤器	1. 依次选择**防御 (Defend)** > **分段 (Segmentation)**， 2. 点击页面右侧的插入符号以展开“工具”(Tools) 菜单，然后选择**默认策略发现配置 (Default Policy Discovery Config)**。 3. 滚动至页面底部。 4. 点击**默认排除过滤器 (Default Exclusion Filters)**。

步骤 2 要创建排除过滤器，请点击**添加排除过滤器 (Add Exclusion Filter)**。

步骤 3 在策略发现过程中，为要排除考虑的流量指定参数：

您无需为所有字段输入值。任何空字段都被视为匹配流的通配符。

在创建策略和集群时，将忽略与任何排除过滤器的所有字段相匹配的任何对话。

选项	说明
Consumer	匹配使用者地址是所选范围、资产过滤器或（仅适用于工作空间特定的排除过滤器，集群）成员的对话。您可以通过创建新的自定义过滤器来指定任意地址空间。
Provider	匹配提供者地址是所选范围、资产过滤器或（仅适用于工作空间特定的排除过滤器，集群）成员的对话。您可以通过创建新的自定义过滤器来指定任意地址空间。
Protocol	匹配具有指定协议的对话。
Port	使用与指定端口或端口范围相匹配的提供者（服务器）端口匹配对话。使用破折号分隔符输入端口范围，例如“100-200”

步骤 4 要编辑或删除排除过滤器，请将鼠标悬停在适用的行上以查看**编辑 (Edit)** 和**删除 (Delete)** 按钮。

步骤 5 如果要配置默认排除过滤器：

当配置的过滤器可供使用时，返回到**默认策略发现配置 (Default Policy Discovery Config)** 页面，然后点击**保存 (Save)** 以使更改适用于各个工作空间。

下一步做什么

重要事项 排除过滤器器在其配置的工作空间中默认为启用。

默认情况下，所有工作空间都会启用默认排除过滤器。

默认情况下，这两种类型的排除过滤器都会在默认策略发现配置中启用。

在发现策略之前：

- 启用或禁用排除过滤器和默认排除过滤器。
  - 在每个工作空间中
  - 在“默认策略发现配置”(Default Policy Discovery Config) 页面上

  有关说明，请参阅启用或禁用排除过滤器，第 31 页。
- 提交任何范围变更，否则过滤器可能与预期流不匹配（并因此排除）。请参阅确认更改。

启用或禁用排除过滤器

您可以在每个工作空间中创建排除过滤器，和/或创建一组可应用于所有工作空间的默认排除过滤器。

默认情况下，两种类型的排除过滤器都已启用。

进行更改

- 要为单个工作空间启用或禁用排除过滤器，请执行以下操作：

  在工作空间中，依次点击**管理策略 (Manage Policies)**、**自动发现策略 (Automatically Discover Policies)** 和**高级配置 (Advanced Configurations)**。 您可以为此工作空间启用排除过滤器和/或默认排除过滤器。
- 要在默认策略发现配置中启用或禁用排除过滤器，请执行以下操作：

  依次选择**防御 (Defend) > 分段 (Segmentation)**，然后点击页面右侧的插入符号以展开“工具”(Tools) 菜单。然后，选择**默认策略发现配置 (Default Policy Discovery Config)**。 滚动到或点击**高级配置 (Advanced Configurations)**。您可以启用排除过滤器和/或默认排除过滤器。

外部依赖关系

仅当使用（高级）创建跨范围策略, on page 89中所述的过程时，外部依赖关系才具有相关性。

“外部依赖关系”(External Dependencies) 设置适用于涉及与属于某个范围的工作负载（不是在其中发现策略的范围）的通信的自动发现的策略。（即涉及“外部工作负载”的通信。）

不属于策略所在范围成员的工作负载就是外部工作负载。此类工作负载是与目标工作负载（属于策略所在的范围）对话的另一端。

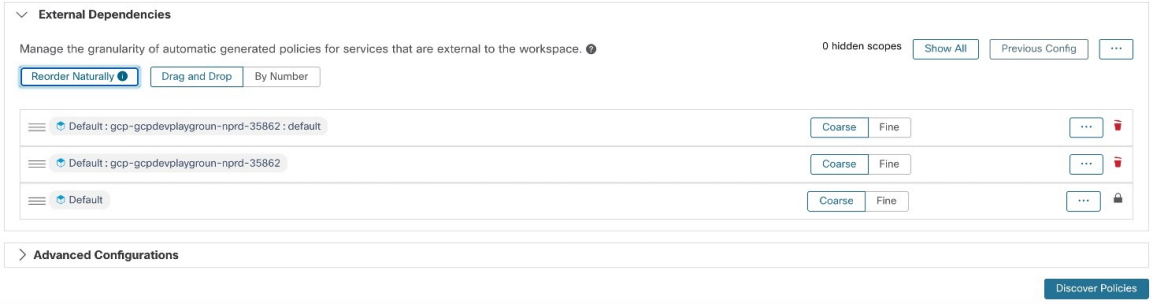
“外部依赖关系”(External Dependencies) 列表是层次结构中所有范围的有序列表。列表中的每个范围都被设置为以下之一：

- 生成特定或优化的策略（更安全），或者
- 在较高范围内生成粗略策略，这可能会更好地泛化（即更有可能允许在发现策略时指定的时间范围内未发现的合法流）。

在策略发现过程中，与工作负载相匹配的第一个范围（或集群或资产过滤器，请参阅下文）将用于生成“允许”策略，其中匹配顺序（以及随之而来的粒度级别）由“外部依赖关系”(External Dependencies) 部分中显示的自上而下的排序决定。

系统将为您配置默认范围顺序，所有范围都会默认设置为“粗略”(Coarse)。

Figure 8: 默认外部依赖关系



要想	相应操作
查看或微调工作空间的外部依赖关系：	导航至工作空间，点击**自动发现策略 (Automatically Discover Policies)**，然后点击**外部依赖关系 (External Dependencies)**。 要对范围重新排序并为每个范围选择精细选项，请参阅微调工作空间的外部依赖关系, on page 33。
为整个根范围配置默认外部依赖关系：	请参阅默认策略发现配置, on page 45。

外部依赖关系：涉及范围子集的精细策略

您可以选择在比范围到范围更精细地发现策略，以控制范围内指定工作负载子集的流量。

例如，您可能希望针对应用中的某类主机（如 API 服务器）创建特定策略；您可以在应用范围内将这些工作负载分组为一个子集。

要生成特定于范围内一部分工作负载的策略，请参阅微调工作空间的外部依赖关系, on page 33。

了解外部依赖关系的提示

使用以下提示来探索自动策略发现涉及工作空间的策略的行为，这些工作空间不属于与策略所在工作空间相关联的范围。

提示

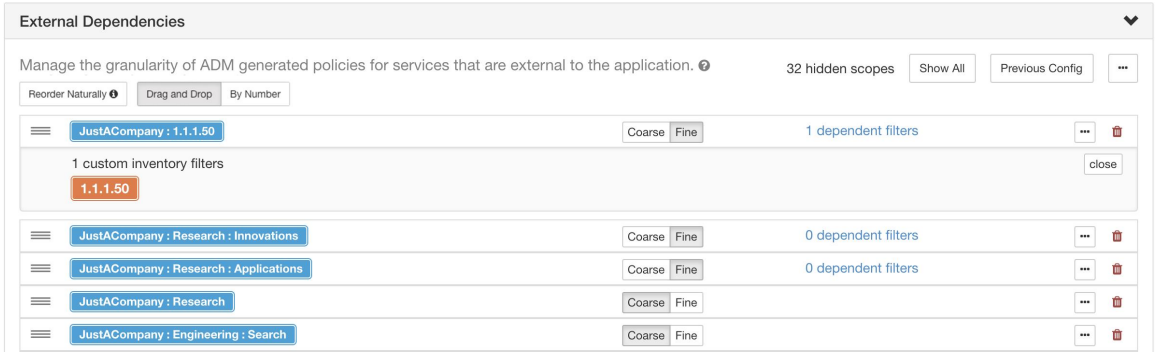
- 您可以删除并重新排列列表，从而以所需的粒度生成策略。例如，删除 Company: RTP 子范围将有助于为整个Company: RTP范围（而不是其单个组件）生成广泛的策略，同时保持公Company: SJC 范围的更高粒度。此外，您可以点击任何范围旁边的**精细 (Fine)** 按钮，查看该范围下是否定义了更精细的候选对象。
- 默认情况下，根范围配置为“外部依赖关系”(External Dependencies) 列表中的最低条目，以便自动策略发现始终尽可能生成更具体的范围的策略。最初，要查看相对较少的粗略粒度策略，可以暂时将根范围置于外部依赖关系的顶部。这样，在自动策略发现之后，您将看到工作空间的所有外部策略都只会连接到一个范围，即根范围（因为每个外部工作负载都映射到根范围）。最终的策略数量会更少，更易于检查和理解。
- 您还可以将属于与工作空间关联的范围成员的所有工作负载（“内部工作负载”）临时捆绑到一个集群中，批准该集群，然后再发现策略。此外，这样会导致策略集减少，因为不会发生集群（工作空间/范围的子分区），因此您可以查看内部策略（连接到内部工作负载）或外部策略（将内部连接到外部工作负载）。稍后，您可以通过取消捆绑内部工作负载并且/或者在根目录上方放置一个或几个关注的外部范围，逐步查看更精细的策略。
- **重要提示：**始终仔细检查涉及根范围的策略，因为这些策略允许进出整个网络的所有流量。当根范围在“外部依赖关系”(External Dependencies) 列表中处于较低位置且您不打算生成粗略策略时，这一点尤其重要。此类策略可能并非由进出工作空间范围的全网络流量产生。相反，它们可能是由几个外部终端触发的，而这些终端未能接收更精细的范围或超出根范围的资产过滤器分配。

  在审核这些策略时，您应检查关联的对话（请参阅对话）以识别这些终端，随后将其分类到更精细的范围或资产过滤器中，以避免根范围级别的安全性较低的策略。

微调工作空间的外部依赖关系

使用此程序可在自动策略发现期间在范围内指定的工作负载子集之间（而不是在整个范围之间）创建策略，当策略的提供者属于与发现策略的范围不同的范围时。

图 9: 微调外部依赖关系



开始之前

- 为要生成特定策略的每个工作负载子集配置资产过滤器。您可以在任何范围内创建任意数量的资产过滤器。

  创建资产过滤器有几种方法：

  - 将感兴趣的集群转换为资产过滤器。

    （请参阅将集群转换为资产过滤器，第 76 页），

    和/或

  - 创建新资产管理器。

    请参阅创建资产过滤器。

  这些过滤器必须启用以下选项：

  - **将查询限制为所有权范围**

    提供超出其范围的服务

- 另请参阅了解外部依赖关系的提示，第 32 页。

过程

步骤 1 导航至您将在其中发现策略的工作空间。

步骤 2 点击**发现发现策略 (Automatically Discover Policies)**。

步骤 3 点击**外部依赖关系 (External Dependencies)**。

步骤 4 如有必要，请点击**全部显示 (Show All)** 范围。

步骤 5 （可选）利用以前的配置：

- 要重新使用上次发现策略时对列表所做的更改，请点击**上一次配置 (Previous Config)**。
- 如果您已在全局“默认策略发现配置”(Default Policy Discovery Config) 中设置外部依赖关系，则可以通过点击**默认配置 (Default Config)** 来使用全局列表。或者，在获取默认列表后，您可以根据需要对其进行修改（仅适用于该工作空间），然后通过点击一次**上一次配置 (Previous Config)** 在后续运行中使用自定义版本。

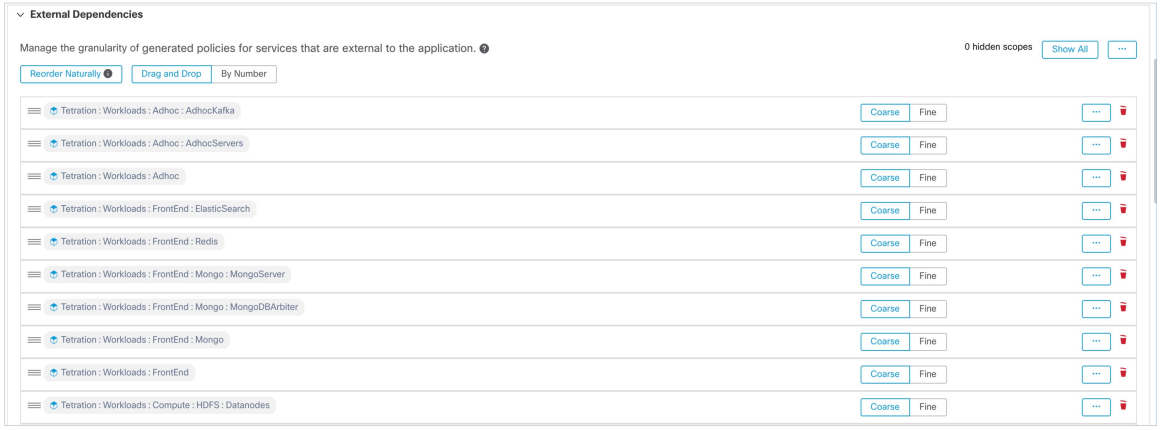
步骤 6 根据需要对范围（和资产过滤器，如适用）进行重新排序。

根据列表中与流量匹配的第一个范围或资产过滤器（从顶部开始）应用策略。为此，您通常希望应用最具体的策略来匹配流量，因此希望子范围（更具体）高于其父范围（不太具体）。

- 如果您最近创建了新的子范围（默认情况下会添加到列表底部），请对整个列表重新排序，将子范围置于父范围之上：

  （推荐）点击**自然重新排序 (Reorder Naturally)**。

图 *10:* 自然重新排序



- （如果您有特定原因）要对列表手动重新排序，请执行以下操作：
  - 点击**拖放 (Drag and Drop)**。
  - 点击**按编号 (By Number)**：

    外部依赖关系的优先级值将以 10 的倍数进行分配。更改数值就能改变顺序。

    修改数字后，点击**查看 (View)** 以更新列表顺序，并为每个优先级重新分配 10 的倍数。

步骤 7 指定每一行的粒度：

- 对于要为其生成特定于已配置资产过滤器或集群的策略的每一行，点击**精细 (Fine)**。

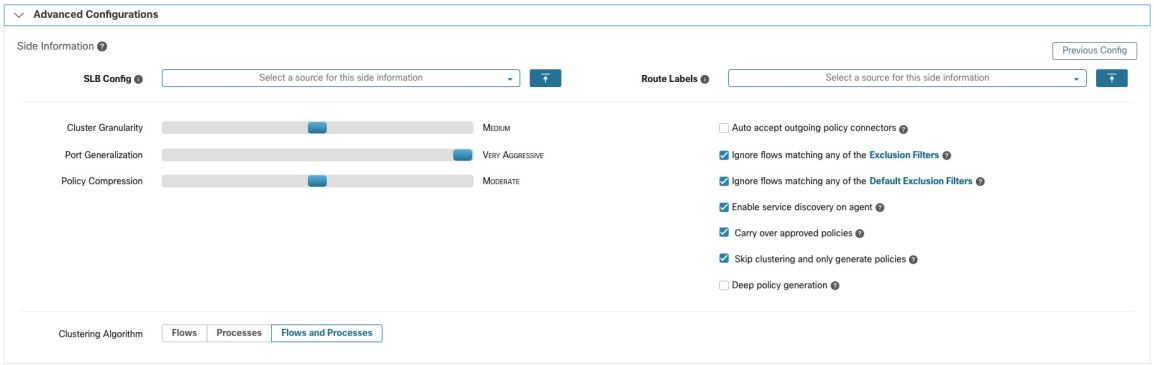
  点击**粗略 (Coarse)** 以生成适用于整个范围的策略。
- 要将粒度应用于某个范围的所有子范围，请执行以下操作：点击范围行末尾的按钮。

自动策略发现的高级配置

使用高级设置可在发现策略时包含更多信息，或适应特定环境。

- 要访问特定工作空间的这些设置，请点击相应工作空间中的**自动发现策略 (Automatically Discover Policies)**。
- 要更改所有工作空间的默认值，请参阅默认策略发现配置, on page 45。

Figure 11: 高级自动策略发现配置



发现策略时包括来自负载均衡器和路由器的数据

您可以从负载均衡器和路由器上传数据，以通知自动策略发现。

要访问以下选项，请点击自动策略发现设置中的**高级配置 (Advanced Configurations)**，并查看“Side Informaton”或“sideinfo”部分。

选项	说明
SLB 配置 (SLB Config) （上传负载均衡器配置）	要以正确的格式从负载均衡器下载数据，请参阅检索高级策略发现配置的负载均衡器配置。 上传负载均衡器配置的支持格式： • **F5 BIG-IP** • **Citrix Netscaler** • **HAProxy** • 其他： 使用**规范化 JSON** 架构。 您必须将任何不受支持的负载均衡器配置转换到此架构中。 此简单方案包括有关虚拟 IP (VIP) 和后端 IP 的基本信息。 要下载示例 JSON 文件，请点击 **SLB 配置 (SLB Config)** 旁边的信息按钮。
上传**路由标签**	您可以从路由器上传已调配的子网/路由列表，以帮助根据预调配的子网集对主机进行分区。自动发现策略生成的集群结果永远不会跨越上传数据所定义的子网边界。您可以在自动策略发现完成后修改结果。 要下载示例 JSON 文件，请点击**路由标签 (Route Labels)** 旁边的信息按钮。

Note 集群不会跨越分区边界，这意味着通过自动策略发现计算出的集群不会包含来自两个不同分区的目标工作负载。分区是根据上传的负载均衡器或路由器数据计算得出的。但是，您可以自由地将工作负载从一个集群移动到另一个集群，例如通过更改集群查询定义（手动集群编辑），或禁用任何辅助信息的上传。

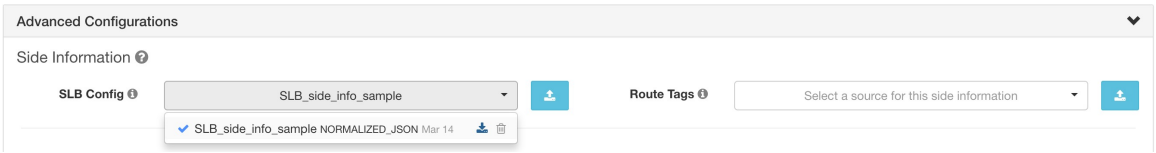
要查看或删除之前上传的负载均衡器（SLB 配置）或路由标签文件，请执行以下操作：

1. 点击标记为**选择此辅助信息的源 (Select a source for this side information)** 的相应框。

   将显示已上传文件的列表。

2. 点击要查看或删除的文件旁边的下载或垃圾桶图标。

Figure 12: **上传的辅助信息**



集群粒度

通过集群粒度，您可以控制自动策略发现生成的集群的大小。

- **精细**会产生更多但较小的集群
- **粗略**会生成较少但较大的集群

Note 由于我们的算法考虑了许多其他信号，因此您可能并不会观察到结果的显著变化。例如，如果生成的集群的可信度非常高，则更改此控件对结果的影响很小。

端口泛化

用于自动策略发现的**高级配置 (Advanced Configurations)** 中的**端口泛化 Port Generalization)** 选项控制执行端口泛化时所需的统计显著性级别，即将在单个工作负载上用作服务器端口的大量端口替换为端口间隔。

此设置会影响策略的准确性、数量和紧凑性，以及生成策略所需的时间。

要禁用端口泛化，请将滑块移动到最左侧。请注意，如果禁用，自动策略发现和/或自动策略发现 UI 呈现时间可能会显著减慢，以防工作负载使用许多服务器端口。

随着滑块向右移动，泛化程度越高，创建端口间隔所需的证据更少，并且用端口间隔替换原始策略（涉及单个端口）的标准也会放宽。

背景

一些应用（如 Hadoop）会在一定时间间隔内使用和更改许多服务器端口，例如从 32000 到 61000。自动策略发现尝试通过观察流中工作负载的服务器端口使用情况来检测每个工作负载的此类行为：通过观察全部可能端口中的一小部分（但端口数量众多，例如 100 个），自动策略发现可以“概括”出 32000 到 61000 中的任何端口都可能被工作负载用作服务器端口。处于间隔内的端口将替换为此类间隔（当满足最小观察计数的某些条件时）。这样会产生更少、更紧凑的策略。间隔估计对于计算准确的策略非常重要：如果没有充分的泛化，如果执行策略，许多未来的合法流将被丢弃。通过将多个端口合并到一个或几个间隔中，UI 的呈现时间也会显著加快。

您可以控制端口泛化的程度，包括禁用端口泛化。

策略压缩

启用策略压缩后，如果工作空间中多个集群中的策略相似，则可以用一个或多个适用于整个父范围的策略来替换这些策略。例如，如果工作空间中的所有或几乎所有集群都向同一个使用者提供相同的端口，那么所有这些集群特定的策略都会被父范围中的一个策略所取代。这会显著减少策略数量，最大限度地减少混乱，并且还可能允许本应丢弃的合法未来流（准确泛化）。

压缩设置越激进，策略频率所需的阈值就越小，这样才能以适用于整个父节点的策略来取代特定组群的策略。

为范围树的分支生成策略时：

此旋钮可用于更改分层策略压缩中的激进程度。

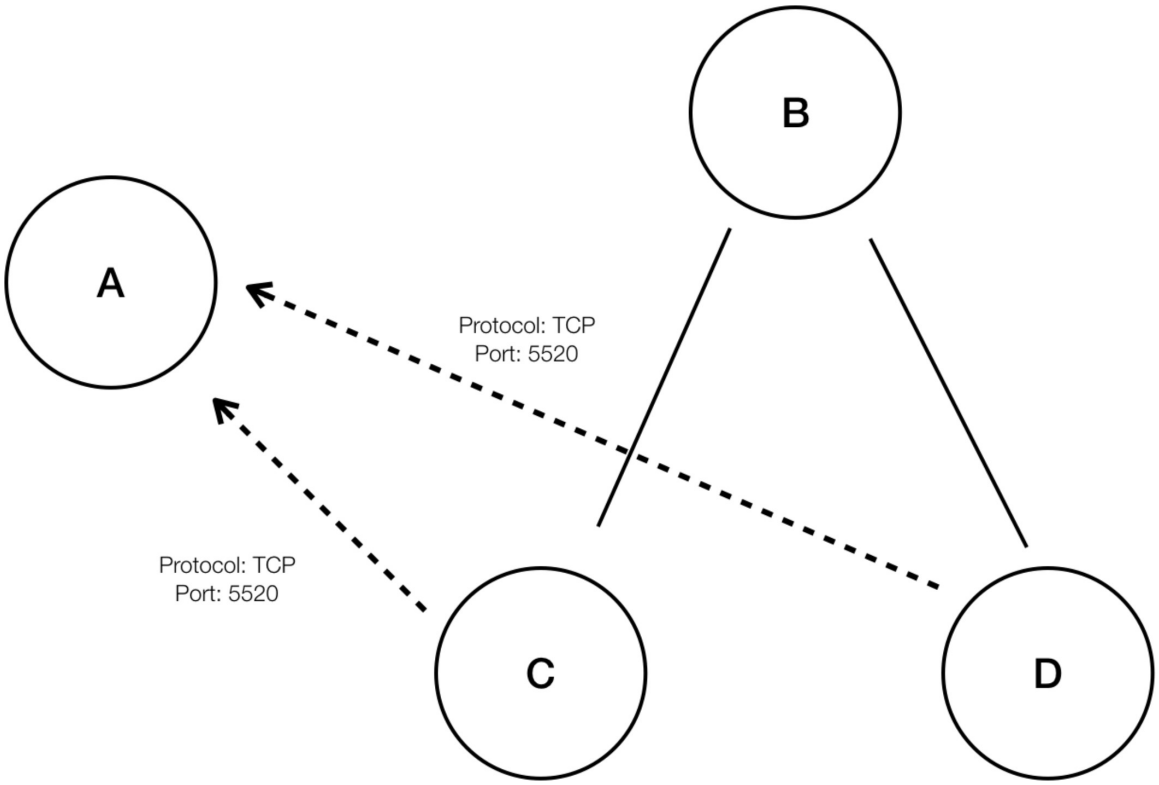
Note 目前，自动策略发现对话页面不支持显示导致压缩策略的对话（您可能需要禁用压缩或使用流量搜索）。

分层策略压缩

在为范围树的一个分支生成策略时，也可以执行策略压缩。策略压缩旋钮可用于更改分层策略压缩中的积极程度。分层策略压缩的示例如下所示。

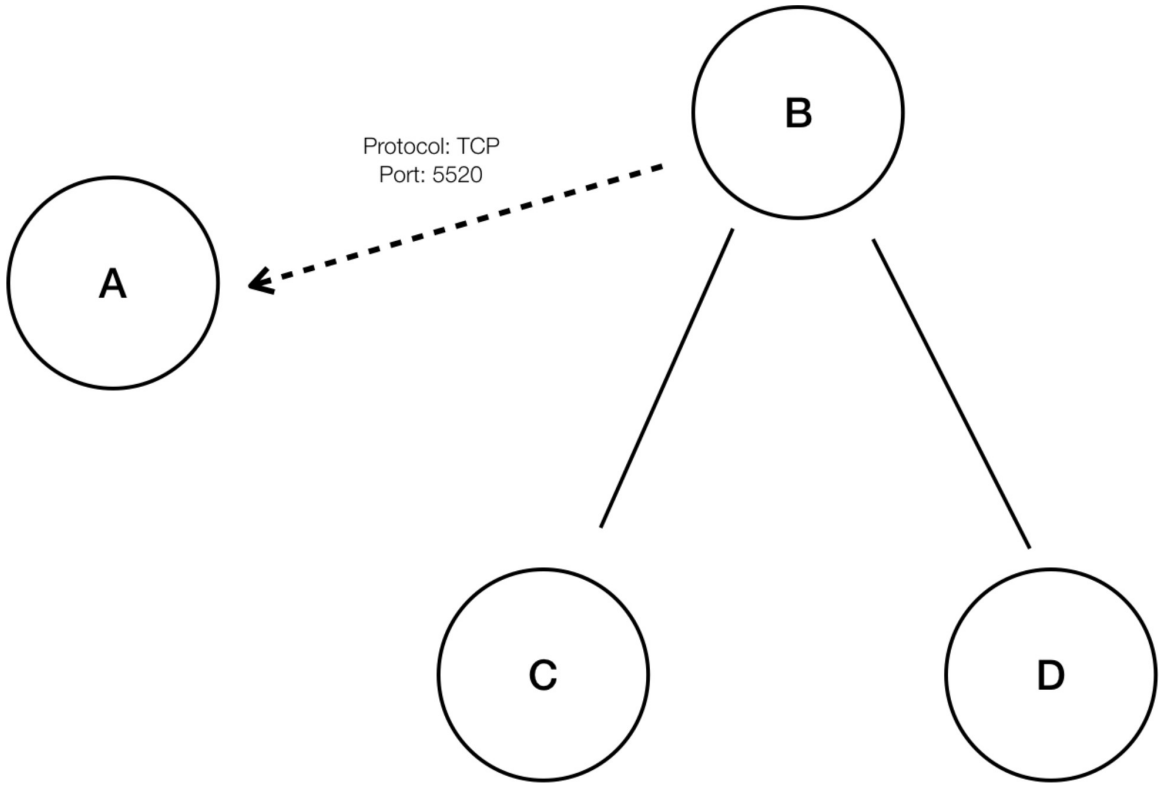
- 假设 A、B、C 和 D 是范围树中的范围，其中“C”和“D”是“B”的子范围。设“C” → “A”是端口 5520 上的 TCP “ALLOW”策略，而“D” → “A”是端口 5520 上的 TCP “ALLOW”策略。

Figure 13: 分层策略压缩之前



- 在分层策略压缩中，如果有足够大的组子范围涉及共享相同端口、协议和目标或源的策略，这些策略将被连接父范围和公共源或目标的通用策略所取代。在上述情况下，“C”和“D”是“B”的子范围，而策略“C”→“A”和“D”→“A”共享相同的目标、端口和协议。由于“B”的 100% 子范围包含类似策略，因此策略将升级为“B”→“A”，结果如下。此外，分层压缩可以重复，因此通用策略可以一直到的子树（范围树的分支）的根。

Figure 14: 分层策略压缩后



- 策略压缩旋钮让您能够通过更改触发压缩的策略共享子范围的最低要求比例（通常以子范围总数的分数来衡量）来调整此类压缩的积极性。如已禁用，系统会根据“外部依赖关系”(External Dependencies) 列表在最高优先级范围之间生成每个策略。随后，如果选择实施自然排序的外部依赖关系列表，则生成的策略将是范围中最精细的策略。

集群算法（集群的输入）

高级用户可以选择集群算法的主要数据源，即实时网络流和/或正在运行的进程，或两者兼而有之。

自动接受传出策略连接器

仅当您使用自动策略发现来使用 （高级）创建跨范围策略, on page 89 中所述的方法创建跨范围策略时，此选项才适用。

在自动发现策略过程中创建的任何传出策略请求都将被自动接受。

有关完整信息，请参阅自动接受策略连接器, on page 98和策略请求。

Note 此选项仅适用于根范围所有者和站点管理员。

自动批准生成的策略

如果要批准策略发现生成的所有策略，则适用此选项。

Note 请注意，如果您选择了该选项，以后如果需要修改或撤销任何更改，则只能手动进行。

有关详细信息，请参阅 自动接受策略连接器, on page 98 和策略请求。

Note 根范围所有者和网站管理员可使用此选项。

忽略匹配排除过滤器的流

要忽略您指定的对话流，请启用适用的选项。要查看或修改任一过滤器列表，请点击相应的**排除过滤器 (Exclusion Filters)** 链接。有关详细信息，请参阅排除过滤器、默认排除过滤器, on page 45和配置、编辑或删除排除过滤器, on page 29。

在代理上启用服务发现

在某些应用中，可能会指定使用大量端口，但在策略发现所包含的时间段内，实际流量可能只使用了这些端口的一个子集。此选项允许将这些应用的整个指定端口池纳入这些应用的策略中，而不仅仅是在实际流量中看到的端口。

启用该选项后，就可以收集有关代理节点上存在的服务的短暂端口范围信息。然后根据这些端口范围信息生成策略。

示例：

- Windows Active Directory 域服务器会使用默认 Windows 临时端口范围 **49152-65535** 来处理请求。设置此标志后，代理将报告端口范围信息，并根据此信息生成策略。

Figure 15: 在代理上启用服务发现

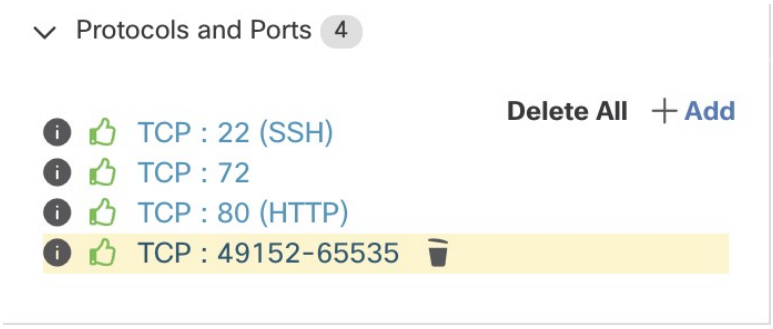
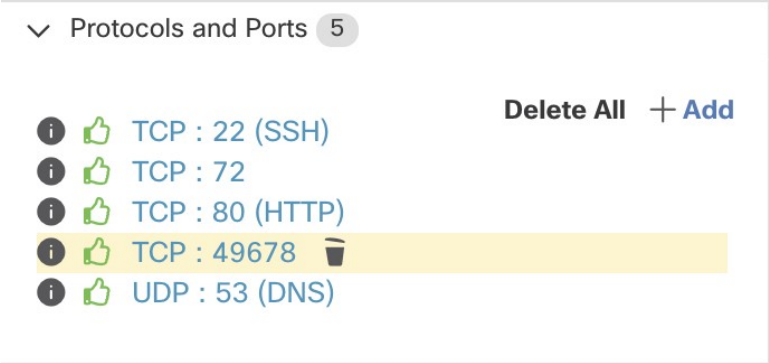


Figure 16: 在代理上未启用服务发现



沿用已批准的策略

默认情况下，此选项已启用。

设置此标志后，您标记为已批准的所有策略（包括使用 OpenAPI 批准的策略）都将被保留。这样，不管自动策略发现发现的“允许”策略如何，您都不必重新定义应生效的特定广泛 DENY 规则。

有关详细信息，请参阅已批准的策略, on page 47。

跳过集群并仅生成策略

如果选择此选项，则不会生成新的集群，而是从任何现有的已批准集群或资产过滤器生成策略，否则会涉及与工作空间关联的整个范围（实际上是将整个范围视为单个集群）。此选项可导致显著减少（但更粗略）的策略。

启用冗余策略删除

此选项仅在为范围树的分支生成策略时可用。

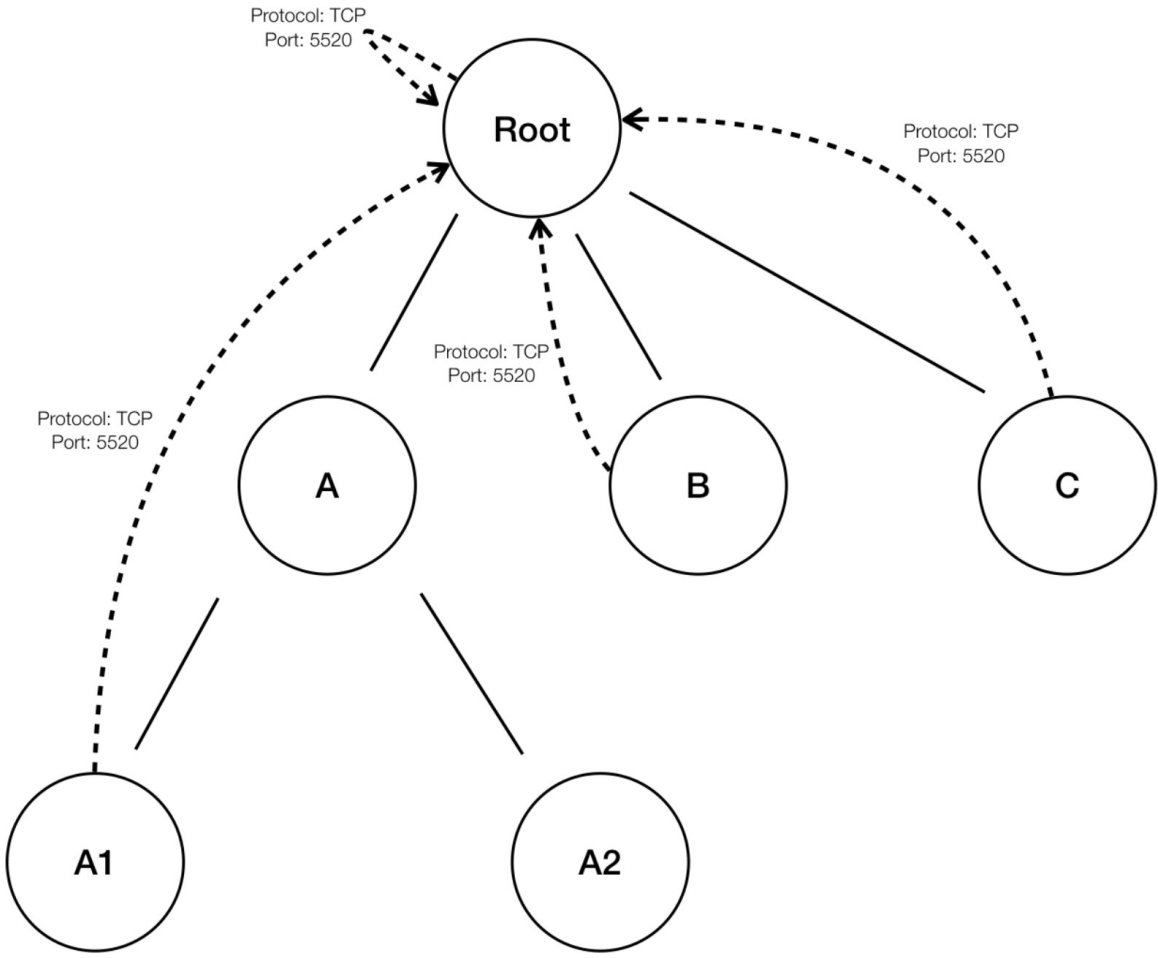
此选项允许/禁止删除冗余精细策略。

示例：

- 将根、A、B、C、A1 和 A2 设为范围树的范围部分。将以下设置为策略：

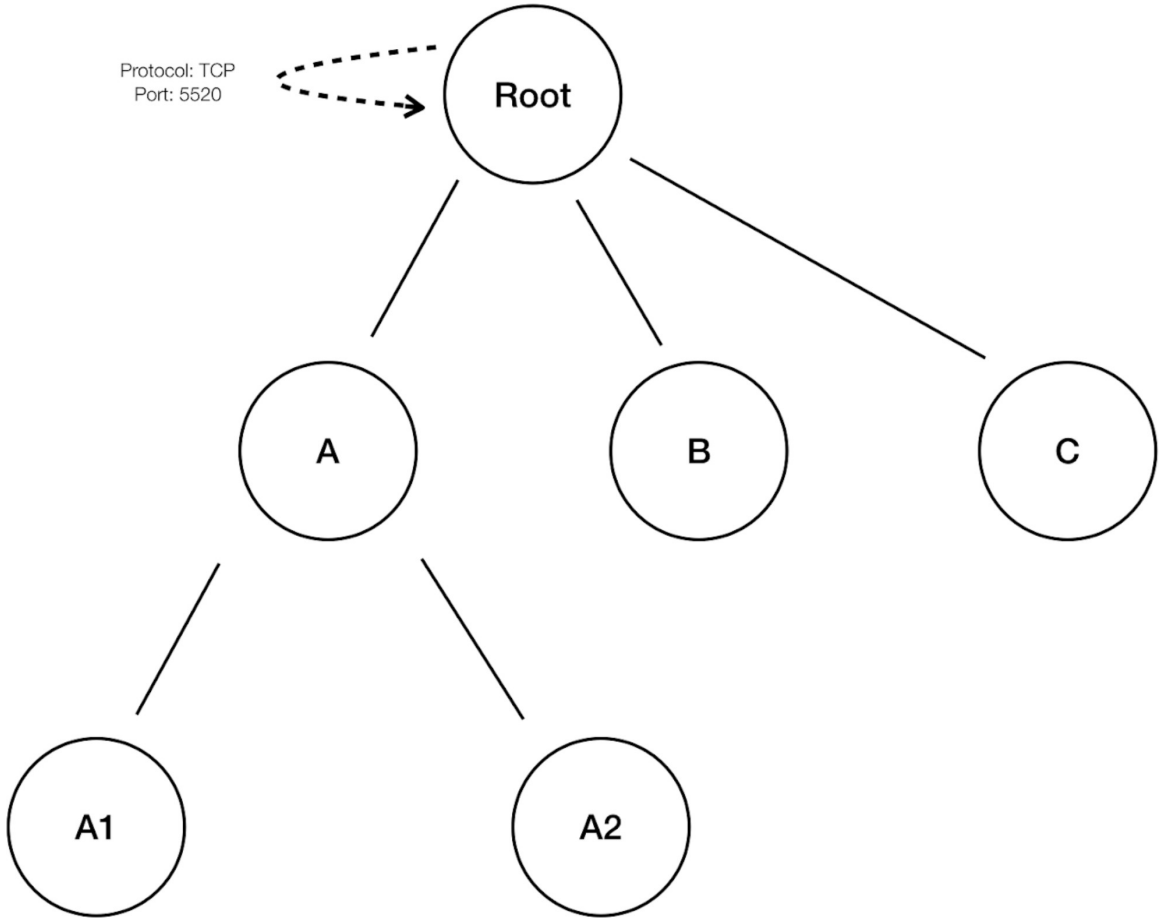
1. “Root” → “Root”
2. “B” → “Root”
3. “C” → “Root”
4. “A1” → “Root”

Figure 17: 删除冗余策略之前



- 策略“B”→“Root”、“C”→“Root”和“A1”→“Root”是冗余策略，因为策略“Root”“Root”涵盖了这些策略。删除冗余策略功能将检查并删除此类策略，从而仅生成一个策略“Root”→“Root”，如下所示。

Figure 18: 删除冗余策略后



删除冗余策略对于维护一套简洁的可解释策略非常有用。缩减后的策略集包含所选压缩级别下的最少策略数量，以覆盖所有工作负载流量。但是，您应始终通过策略分析来审核策略，并检查相应的对话，以评估所产生的策略的严格性。当存在未被归类到更细范围或资产过滤器的终端流量时，这一点尤为重要。此类终端可能会触发生成比预期更粗略的策略，如涉及根范围的策略。如果同时启用了冗余策略删除，则系统将删除更精细的策略，并且不会向您显示。要诊断（压缩）策略的源并查看更精细级别的策略，请关闭策略压缩和冗余策略删除。还要注意的是，目前自动发现策略对话页面可能无法显示导致压缩/概括策略的对话；因此要解决这个问题，可以关闭压缩和冗余策略删除，这样就能更容易地找到导致生成策略的对话。

Tip 由于发现范围树分支的策略会发现以工作空间范围为根的范围子树的所有策略，因此这些策略将涵盖子树下所有工作负载的自动策略发现发现的所有合法流量。使用策略分析（请参阅策略）等工具来分析这些策略时，应在与子范围关联的所有工作空间中关闭策略分析。这样，驻留在子范围工作空间中的策略（如有）（通常会由于范围定义更具体而获得高优先级）将不会获得优先级并干扰结果。但是，当子范围工作空间中的策略被配置为涵盖通常涉及特定于子范围的更精细的资产过滤器或集群的不同流量集时，例外情况适用。

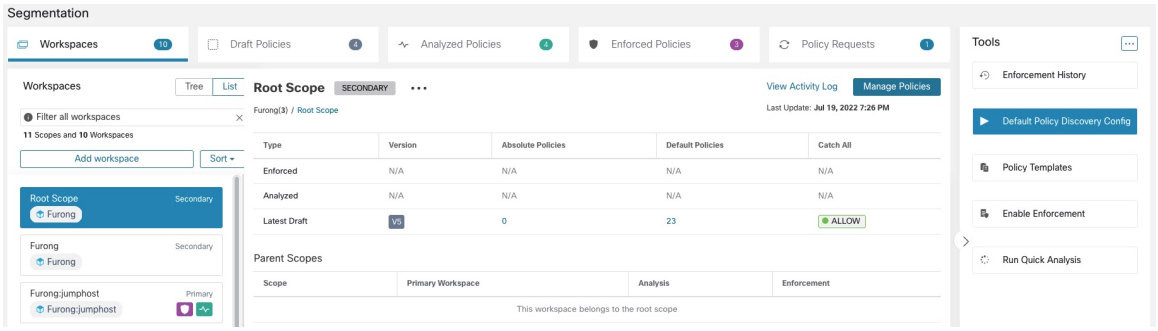
默认策略发现配置

您可以配置默认自动策略发现设置，可以选择在整个根范围内的任何工作空间中使用这些设置。您可以配置默认的自动策略发现设置，这些设置可选择用于整个根范围内的任何工作空间。

要配置策略发现的默认选项，请执行以下操作：

依次选择**防御 (Defend)** > **分段 (Segmentation)**,然后点击页面右侧的插入符号以展开“工具”(Tools)菜单。然后选择**默认策略发现配置 (Default Policy Discovery Config)**。

Figure 19: 导航至“默认策略发现配置”***(Default Policy Discovery Config)*** 页面



有关“默认策略发现配置”(Default Policy Discovery Config) 页面上的选项的信息，请参阅：

- 外部依赖关系, on page 31 和子主题
- 自动策略发现的高级配置, on page 35 和子主题
- 默认排除过滤器, on page 45

Important 当默认配置完成并准备好在各个工作空间中使用时，点击**保存 (Save)**。

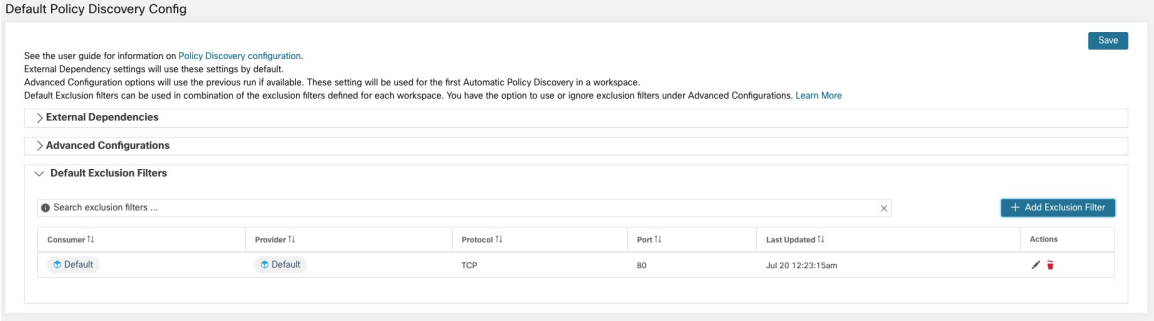
默认排除过滤器

排除过滤器通过指定要从发现输入中排除的流量，可帮助您微调自动策略发现建议的策略和集群。

有关详细信息，请参阅排除过滤器。

您可以创建一个全局默认排除过滤器列表，以供租户中的所有工作空间使用，然后为每个工作空间指定在发现策略时是否使用该默认列表。

Figure 20: 默认排除过滤器



要配置默认排除过滤器，请参阅配置、编辑或删除排除过滤器, on page 29。

要启用或禁用默认排除过滤器，请参阅启用或禁用排除过滤器, on page 31。

检索高级策略发现配置的负载均衡器配置

以下是以可直接上传到 Cisco Secure Workload 的格式检索受支持的负载均衡器配置文件的说明，以便在策略发现中使用。有关详细信息，请参阅自动策略发现的高级配置和发现策略时包括来自负载均衡器和路由器的数据, on page 36。

请注意，所有文件都必须以 ASCII 编码。

Citrix Netscaler

在控制台中连接 `show run` 的输出并上传文件。

请参阅配置文件示例

F5 BIG-IP

上传 `bigip.conf` 文件。

Note 如果您有扩展名为 .UCS 的文件，请解压缩存档文件夹，然后仅上传配置转储中的 `bigip.conf 文件`。如果有多个 `bigip.conf 文件`，请合并后再上传这些文件。

请参阅配置文件示例

HAProxy

上传 `haproxy.cfg` 文件。路径通常为 `/etc/haproxy/haproxy.cfg`。

请参阅配置文件示例

规范化 *JSON*

如果您发现上述选项受限，请将配置转换为以下 JSON 架构并直接上传。可以通过点击“高级运行配置”(Advanced Run Configurations) 中的 SLB 配置旁边的 **i** 图标直接下载示例 JSON 文件，以实现自动策略发现。

请参阅配置文件示例

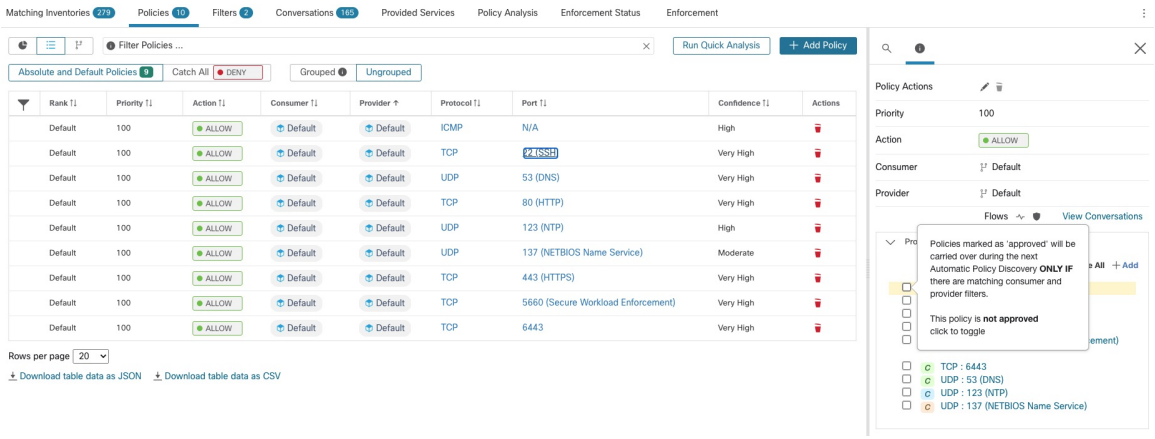
审批策略

在查看策略发现结果时，批准已发现且希望保留的策略，以便在将来发现策略时原封不动地继续使用这些策略。有关完整的详细信息，请参阅 已批准的策略，第 47 页。

要批准策略，请执行以下操作：

1. 在“策略”(Policies) 页面上，对于要保护的策略，点击**协议和端口 (Protocols and Ports)** 列中的值。
2. 在右侧打开的面板中，选中要在今后发现策略时保留策略的每个协议和端口左侧的复选框。

图 *21:* 审批策略



您还可以使用此程序从策略中删除批准。

已批准的策略

一般来说，在自动发现策略期间，已批准的策略不会更改，自动发现策略也不会建议重复或重叠已批准策略效果的策略。

以下是已批准的策略：

- 手动创建的策略。
- 已发现的手动批准的策略。

  （当您对策略的行为符合预期感到满意时，则可以批准该策略，以防止在未来自动发现策略时对其进行更改。请参阅审批策略, on page 47。）
- 已上传的策略，除非明确标记为已批准：`false (approved: false)`。
- 适用于本范围中工作负载的父范围和祖先范围中定义的已批准策略（具体来说，来自其主要工作空间的最新版本）。

- 在使用当使用者和提供者处于不同范围时：策略选项, on page 88中所述的高级方法处理跨范围策略时，从其他工作空间接受策略请求时创建的策略。例如，这包括从 提供的服务, on page 100 选项卡包含的策略。

点击策略的端口或协议链接并在页面右侧的面板中查看详细信息时，已批准的策略会在协议类型旁边显示一个大拇指向上的图标。

已批准策略保护的例外情况

如果策略的两端是以下任意一种情况，则在未来自动策略发现过程中会保留已批准的策略：已批准的集群；资产过滤器；已接受的策略请求（适用于跨范围策略）；或不会显著更改成员身份的集群。（但是，在最后一种情况下，集群成员身份可能已发生变化。）

如果策略的任一端是未获批准的集群，并且在自动发现策略时，没有新生成的集群与该集群有足够高的重叠度，则已批准的策略在未来的自动发现策略运行中可能不受保护。

要保护涉及未批准集群的策略，应明确批准策略两端的集群。

此外，还有一个默认启用的自动发现策略高级配置。如果您不想保护已批准的策略免遭更改，则可以为工作空间或全局默认策略发现配置取消选择此选项。请参阅沿用已批准的策略, on page 42。

对已批准的策略进行故障排除

已批准的策略不会沿用

如果已批准的策略未按预期沿用，请确保在自动策略发现的高级和/或默认配置设置中选择**沿用已批准的策略 (Carry over approved policies)** 选项。

查找从策略生成中排除的对话

在自动发现策略的过程中，任何符合现有已批准策略标准的对话都会被排除在策略生成之外。此排除可防止生成涵盖相同对话的冗余策略。（此过程与排除过滤器（请参阅排除过滤器）不同，在后者中，您要定义匹配过滤器而不是策略。排除过滤器可防止向自动策略发现的所有部分显示匹配的对话。）

请注意，虽然不会从这些对话中生成冗余策略，但在自动策略发现分析和生成集群时，仍会考虑这些对话。

要查看现有已批准策略从自动策略发现中排除的对话，请执行以下操作：

在对话视图中（请参阅对话），使用**排除**标志来过滤对话。点击策略中的端口和协议链接，然后点击对话旁边的排除图标，在页面右侧打开的策略详细信息视图中，还可以探索哪些现有已批准策略会导致排除这些对话。（将鼠标悬停在图标上可查找正确的图标。）

反复修改策略

为单个范围和整个网络定义和优化策略将是一个迭代过程。

您可能需要修改已发现的策略和手动创建的策略。

重新运行自动策略发现

您可以随时重新运行自动策略发现。重新运行自动策略发现主要是为了包括上次运行中未包括的其他信息，或者排除无用的信息。例如，您可以：

- 安装其他代理或配置其他连接器，并允许累积一些流数据。
- 增加用于发现的时间跨度，以包含更多数据。
- 批准集群（无论是否先编辑），这可以在重新运行时改善其他工作负载的集群。请参阅批准集群, on page 80。
- 排除您知道不希望影响策略的流，这样就不必通过编辑将其删掉。请参阅排除过滤器, on page 29。
- 更改高级设置（有关详细信息，请参阅自动策略发现的高级配置, on page 35。）
- 在对 解决策略复杂性问题, on page 82 进行更改后捕获更改。

如果在现有工作空间中再次自动发现策略，则可能会在工作空间中生成不同的集群和策略。

如果一台主机不再在工作空间范围内，在随后的自动策略发现运行中，该主机将不会出现在任何集群中；如果它在已批准的集群中，也不会再出现在该集群中。即使具有相同的成员工作负载集，但具有不同的时间框架或配置，自动策略发现可能会产生不同的集群。

Note 有关在策略发现期间未修改的策略类型的列表，请参阅已批准的策略, on page 47。

Note 删除冗余策略 在后续自动策略发现中，主工作空间中已批准的策略将删除匹配的策略生成对话，因此不会生成冗余策略。请注意，与排除过滤器一样，如果策略使用工作空间中定义的集群过滤器，则此功能可能无法在非主工作空间上完美运行。来自非主工作空间的集群过滤器会处于非活动状态，并且不会匹配任何流，因此在自动策略发现期间，非主工作空间中可能仍会生成冗余策略。

重要提示：在重新运行自动策略发现之前

Important 在重新发现工作空间中的策略之前，先处理以下各项：

- 默认情况下，每次在特定工作空间中发现策略时，系统会根据新发现期中包含的数据覆盖之前发现的策略和集集群。如果您想保留某些策略和集群，而不想保留其他策略和集群，请批准这些策略和集群。
- 如果要保留任何现有的已生成集群，请参阅在自动策略发现重新运行期间防止修改集群或批准集群, on page 80。
- 如果要保留任何现有的已生成策略，请参阅审批策略, on page 47。
- 除非更改，否则将使用在上次发现运行中配置的任何现有**高级配置 (Advanced Configuration)**设置。

  但是，系统将使用任何已配置的默认外部依赖关系，覆盖上次运行的外部依赖关系。
- 如果当前显示的已发现策略版本并非最新版本，而您又想保留以前发现的版本，请点击页面顶部显示的版本，然后选择最新的 v* 版本。

  如果显示的是之前的版本，该版本与新发现的版本之间的任何版本都将被删除。

  有关详细信息，请参阅查看、比较和管理发现的策略版本, on page 50。

要重新运行策略发现，请参阅自动发现策略, on page 26。解决本主题中的要点后，每次发现策略的过程均相同。

查看、比较和管理发现的策略版本

每次在工作空间中发现策略时，分配给策略集的版本号 (v*) 都会递增。

有关信息，请参阅关于策略版本（v* 和 p*），第 137 页。

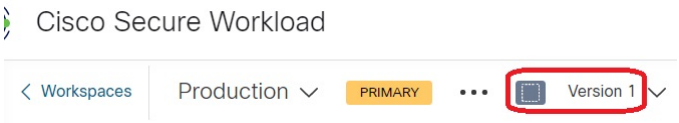
过程

步骤 1 依次点击**防御 (Defend) > 分段 (Segmentation)**。

步骤 2 浏览至工作空间

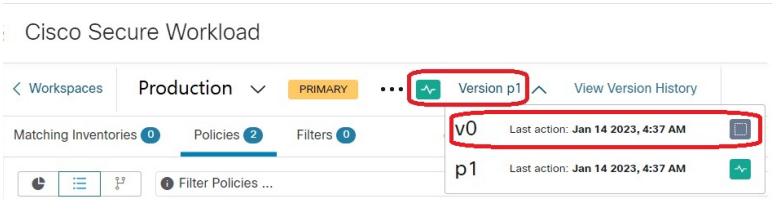
步骤 3 点击**管理策略 (Manage Policies)**。

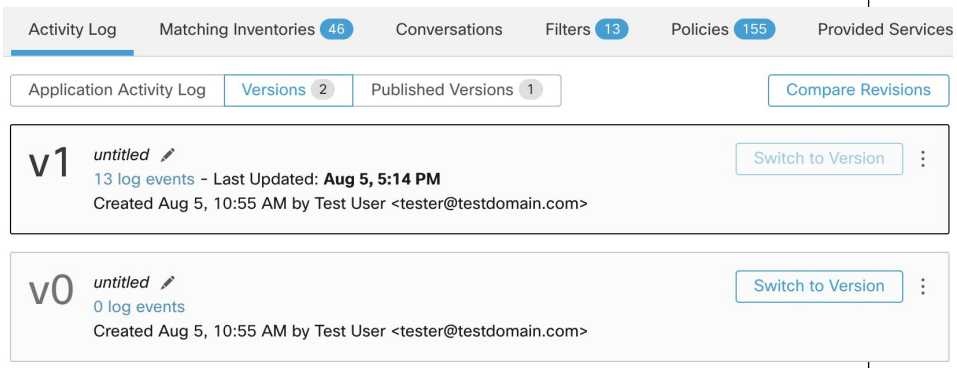
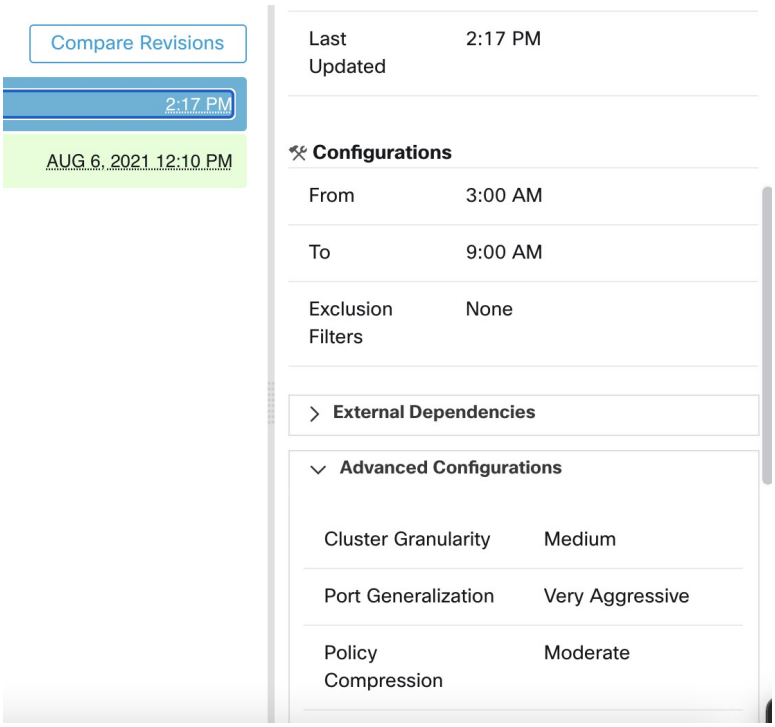
步骤 4 页面顶部显示的是当前显示的由自动发现策略生成的策略版本：



如果您已分析或执行策略，则显示的版本可能是策略发现版本、已分析策略版本或执行版本。

步骤 5 执行以下操作之一：

显示自动发现策略生成的不同版本的策略：	点击当前版本，然后选择其他 v* 版本。 （如果您看到 p* 版本，则这些版本是已分析和/或执行的版本，而不是已发现策略的版本。）  **重要信息！！**请参阅此程序末尾的“后续操作”部分中的警告。

查看有关版本的详细信息	**1.** 点击页面顶部当前版本旁边的**查看版本历史记录 (View Version History)**。 **2.** 点击**版本 (Versions)** 选项卡以查看已发现策略的版本。（不是“发布的版本”(Published Versions) 选项卡。） 版本列表会显示： 图 ***22:*** 生成的策略版本列表及摘要信息  **3.** 点击版本中的**日志事件 (log events)** 链接。 **4.** 点击事件行中的链接。 可用详细信息包括统计信息、排除过滤器、外部依赖关系和运行配置。 图 ***23:*** 用于特定自动策略发现运行的配置 

比较两个版本以查看更改内容：	1. 点击**比较修订 (Compare Revisions)**。 2. 选择要比较的版本。 3. 有关结果详细信息，请参阅策略版本比较：策略差异，第 139 页。
删除不需要的版本：	点击版本对应的 ⋮，然后选择**删除 (Delete)**。 您无法删除自动策略发现生成的最后一个剩余版本（v* 版本）。
导出版本：	点击版本对应的 ⋮，然后选择**导出... (Export...)** 。

下一步做什么

重要事项 如果要保留已发现策略的以前版本，在完成旧版本的处理后，始终要显示已发现策略的当前版本。

如果下次为该工作空间发现策略时未显示已发现策略的最新版本，则旧版本可能会被删除。

例如，如果已发现策略的最新版本是 v4，而再次发现策略时显示的是 v2，那么现有的 v3 和 v4 将被删除，新发现的策略版本将是 v3。

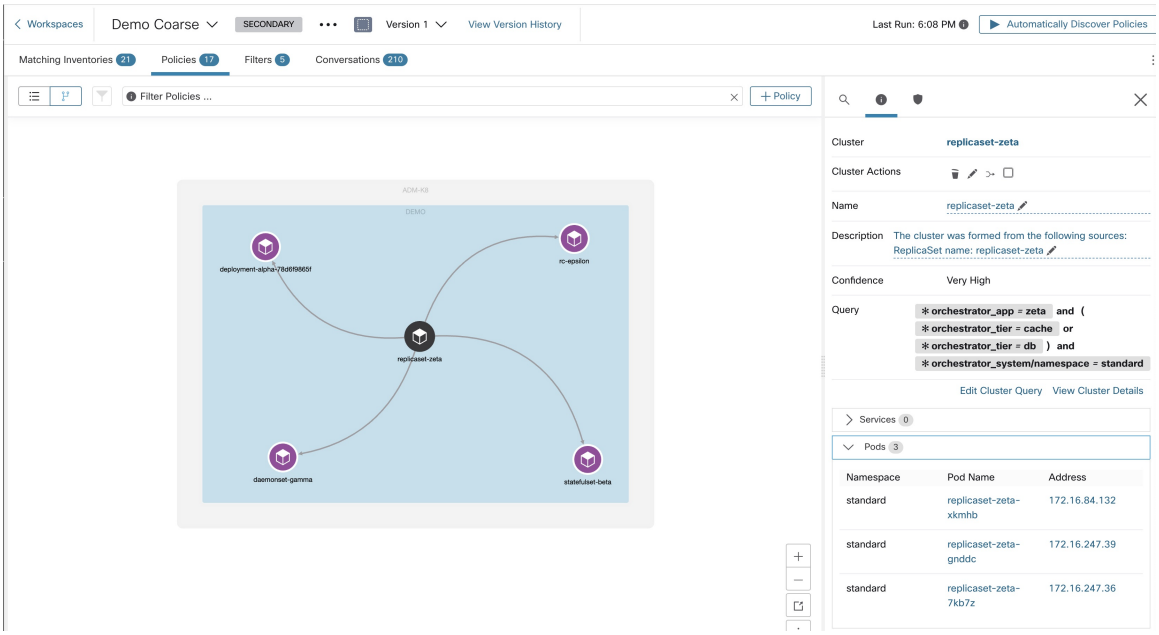
此行为确保了线性版本历史，从而简化了在需要时恢复到先前版本的过程。

此外，只有在显示最新 v* 版本时，才能手动创建策略。

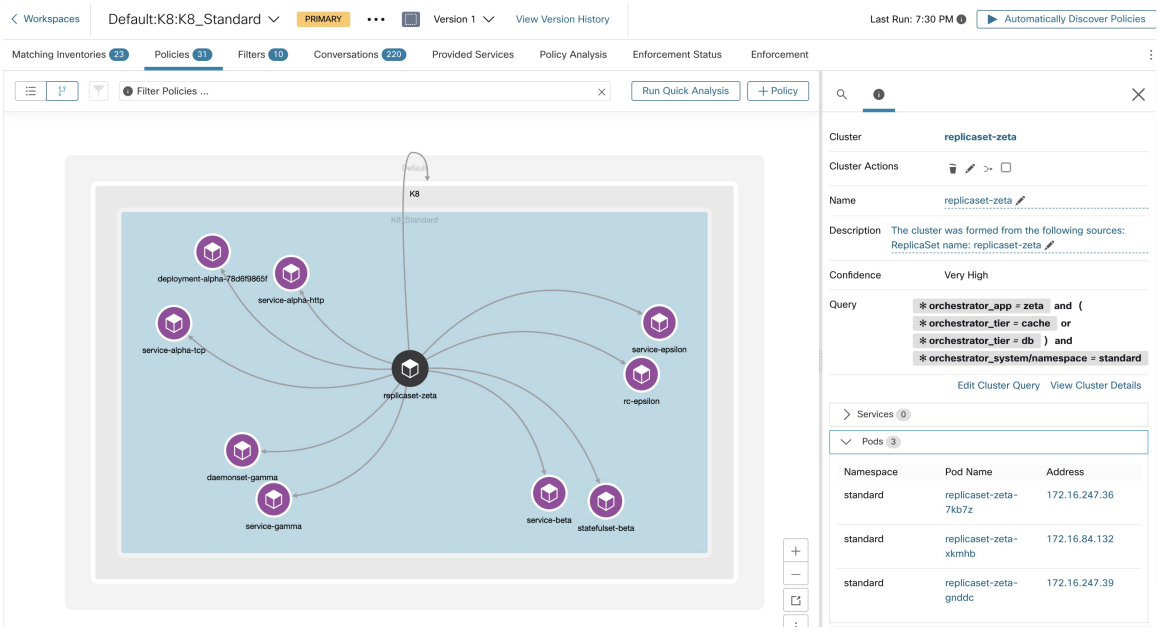
策略发现 Kubernetes 支持

策略发现会使用 Kubernetes 配置中有关 Pod 和服务的信息，为 Pod 和服务创建集群，并生成相应的策略。

如果集群粒度设置为“粗略”(COARSE) 或“非常粗略”(VERY COARSE)，则服务和支持这些服务的 Pod 将集群在一起。



如果集群粒度设置为“中”(Medium)、“精细”(Fine)或非常精细，则服务以及支持这些服务的 Pod 将单独集群。



对于 Pod 集群，源信息被作为集群说明的一部分添加，说明中的每个集群都包含导致集群形成的实体信息。

例如，**说明**：“集群形成于以下源：*ReplicaSet* 名称：*replicaset-zeta*”(The cluster was formed from the following sources: ReplicaSet name: replicaset-zeta)。

导入/导出

导出工作空间

每个工作空间中集群和策略的所有相关内容都能以 JSON、XML 和 YAML 等多种常用的结构化文档格式作为单一文件下载。其他策略执行或分析工具可以使用此类文件进行进一步的内部处理或注入。

导航至 **...** 菜单项，然后点击**导出**项。这样将显示导出对话框。您可以选择导出的文件是只包括集群内容，还是包括集群内容以及根据真实网络流自动发现策略生成的集群间安全策略。选择所需的格式，然后点击下载，将文件下载到本地文件系统中。

Figure 24: 导入/导出菜单项

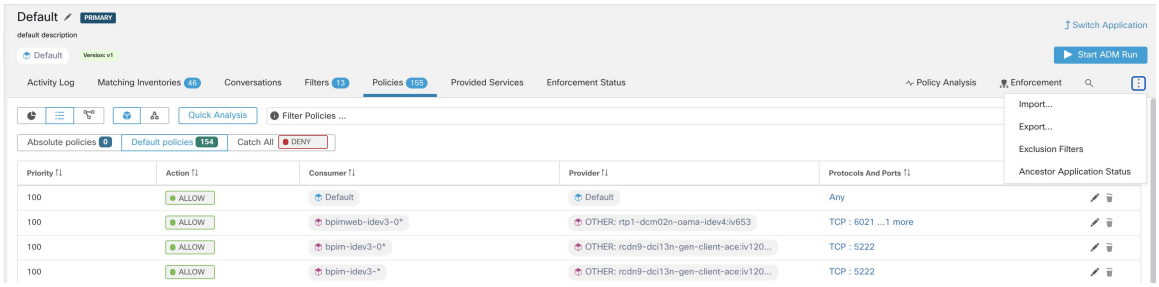
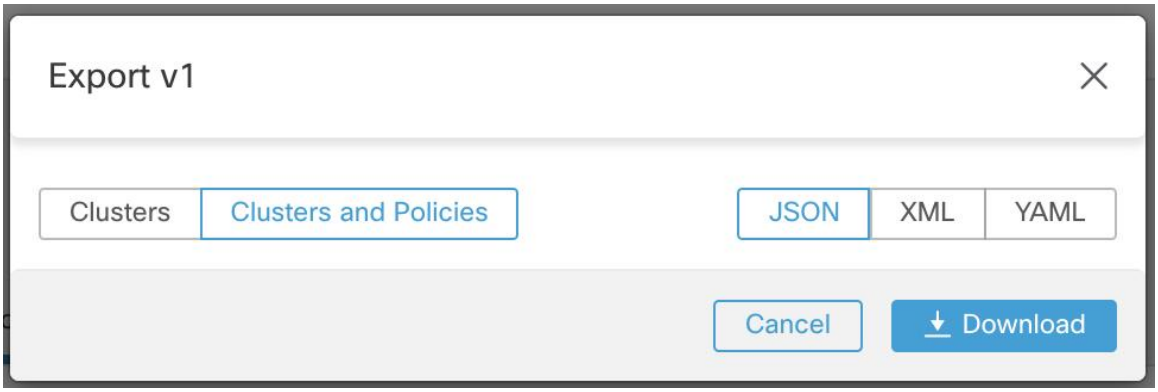


Figure 25: 导出工作空间的策略



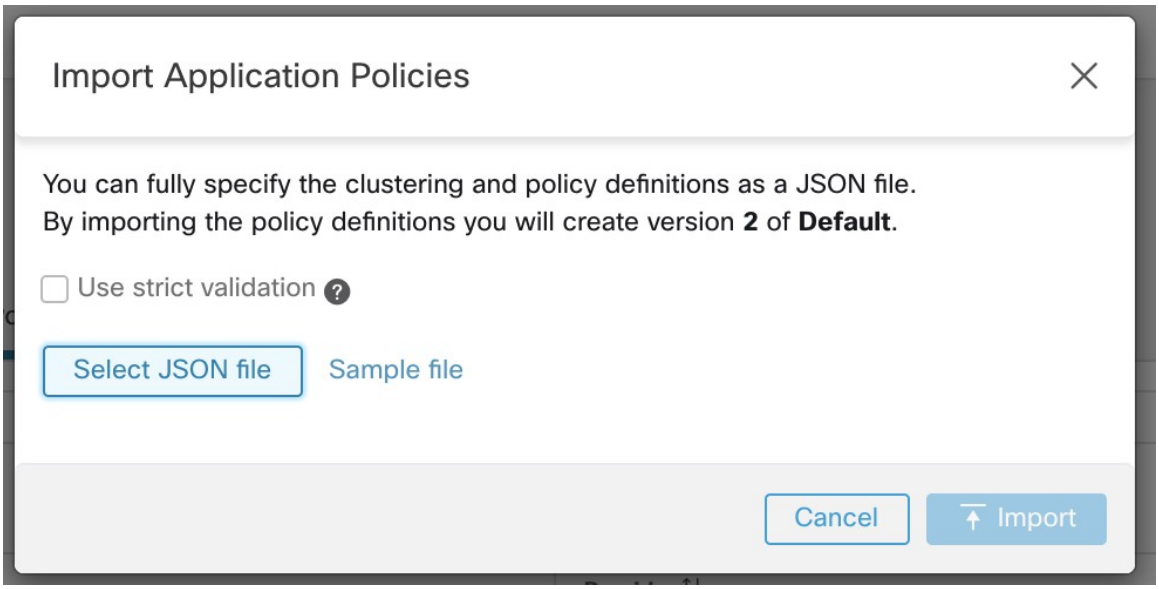
导出工作空间时，自动策略发现配置中的“自动接受传出策略连接器”(Auto accept outgoing policy connectors) 设置 会包含在内，并将在导入的工作空间中处于活动状态。

导入

您可以直接上传 JSON 文件，将已知集群和策略定义导入工作空间。与自动发现策略类似，将策略上传到现有工作空间会创建一个新版本，并将集群和策略定义置于新版本之下。缺少过滤器和不正确的属性值将返回错误。

点击**导入 (Import)** 菜单项（从工作空间标题中的 **...** 菜单）。在导入对话框中，您可以选择格式有效的 JSON 文件。点击**示例 (Sample)** 按钮，可以找到演示策略和集群架构的小型示例 JSON 文件。

Figure 26: 导入集群/策略



启用**严格验证 (Strict Validation)** 后，如果 JSON 包含无法识别的属性，则会返回错误。这对于查找错别字或识别错误的可选字段非常有用。

Note 默认情况下，所有导入的策略都标记为已批准，除非明确标记为 `approved: false`。在自动策略发现过程中，您可以选择保留这些已批准的策略，以生成一组新的策略。有关详细信息，请参阅已批准的策略, on page 47。

专家提示：通过导出应用工作空间检索到的 JSON 文件的架构与将策略导入工作空间的预期格式兼容。因此，可以使用导出后导入的方法将策略从一个应用工作空间克隆到另一个应用工作空间。请注意，在导出和导入策略时，许多功能可能无法正常工作。例如，支持策略的对话不会包含在导出中，在导入策略时也不会显示。

特定于平台的策略

有关代理如何在每个平台上执行策略的重要详细信息，请参阅使用代理的执行策略。对于 Kubernetes/OpenShift，请参阅容器上的执行 ， 第 129 页。

Windows

建议的基于 Windows 操作系统的策略配置

尽可能在策略中指定端口和协议；建议不要允许任何端口、任何协议。

例如，生成的具有端口和协议限制的策略可能如下所示：

```
dst_ports {
```

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

相反，如果您允许 iperf.exe 使用任何协议和任何端口发起的网络连接，则生成的策略将如下所示：

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

对于上述过滤器，Cisco Secure Workload 创建一条策略规则以允许提供者上的网络流量，如下所示：

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

此网络规则会打开提供者上的所有端口。我们强烈建议不要使用 *Any* 协议来创建基于操作系统的过滤器。

为 Windows 属性配置策略

要在基于 Windows 的工作负载上执行策略时更精细地执行策略，则可以通过以下方式来过滤网络流量：

- 应用名称
- 服务名称
- 带或不带用户组的用户名

WAF 和 WFP 模式均支持此选项。基于 Windows 操作系统的过滤器在生成的网络策略中分为使用者过滤器和提供者过滤器。使用者过滤器会过滤在使用者工作负载上发起的网络流量，而提供者过滤器会过滤发往提供者工作负载的网络流量。

开始之前

此程序假定您要修改现有的策略。如果尚未创建要添加基于 Windows 操作系统的过滤器的策略，请先创建该策略。

重要事项	有关涉及 Windows 属性的策略，请参阅警告和已知限制。

过程

步骤 1 在导航窗格中，点击**防御 (Defend)** > **分段 (Segmentation)**。

步骤 2 点击包含要为其配置基于 Windows 操作系统的过滤器的策略的范围。

步骤 3 点击要在其中编辑策略的工作空间。

步骤 4 点击**管理策略 (Manage Policies)**。

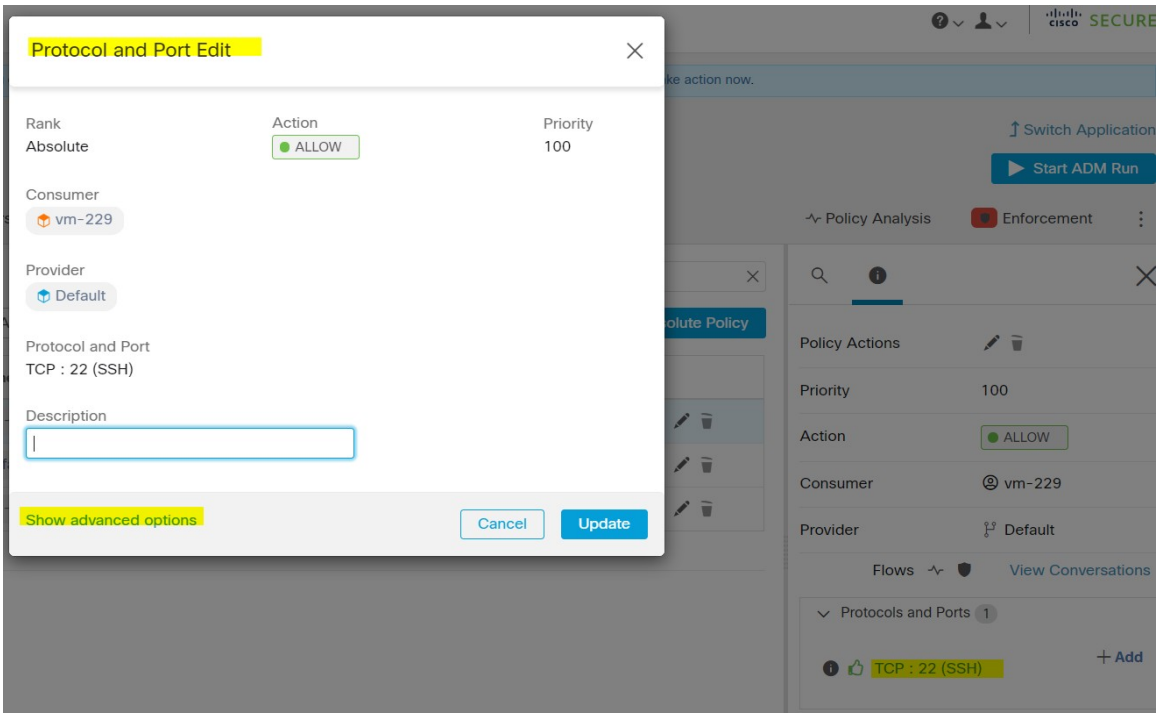
步骤 5 选择要编辑的策略。

重要事项 使用者和提供者必须仅包含 Windows 工作负载。

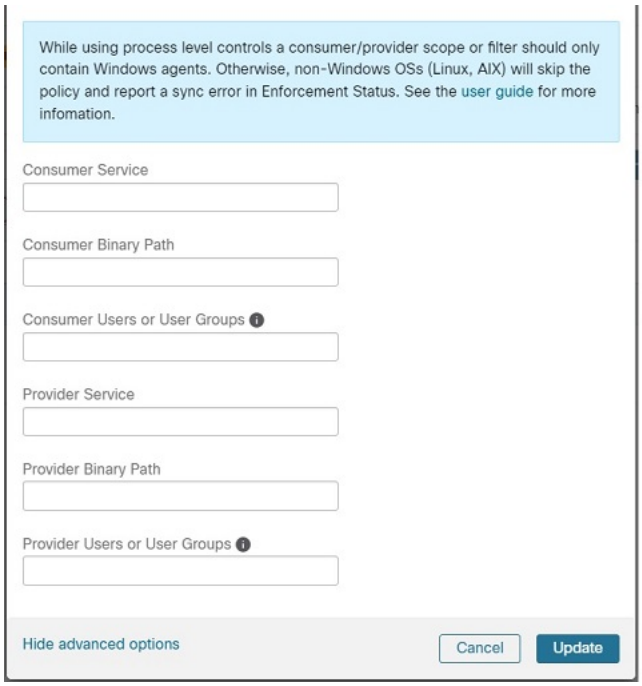
步骤 6 在要编辑的策略的表行中，点击**协议和端口 (Protocols and Ports)** 列中的现有值。

步骤 7 在右侧窗格中，点击**协议和端口 (Protocols and Ports)**下的现有值。

在本示例中，点击 **`TCP : 22 (SSH)`**。



步骤 8 点击**显示高级选项 (Show advanced options)**。



步骤 9 根据应用名称、服务名称或用户名配置使用者过滤器。

- 应用名称必须是完整路径名。
- 服务名称必须是短服务名称。
- 用户名可以是本地用户名（例如，tetter）或域用户名（例如，sensor-dev@sensor-dev.com 或 sensor-dev\sensor-dev）
- 用户组可以是本地用户组（例如，Administrators）或域用户组（例如，domain users\sensor-dev）
- 可以指定多个用户名和/或用户组名并以“,”分隔。（例如，sensor-dev\@sensor-dev.com,domain users\sensor-dev）
- 服务名称和用户名不能同时配置。

步骤 10 根据应用名称、服务名称或用户名配置提供者过滤器。

遵循上一步中为使用者过滤器提供的相同准则。

步骤 11 输入二进制文件的路径（如适用）。

例如，输入 **`c:\test\putty.exe`**

步骤 12 点击**更新 (Update)**。

已知限制

- Windows 2008 R2 不支持基于 Windows 操作系统的过滤策略。

- 可以使用单个用户名来配置网络策略，而 MS 防火墙 UI 支持多个用户。

警告

- 在使用基于Windows操作系统的策略时，使用者/提供者范围或过滤器应仅包含Windows代理。否则，非 Windows 操作系统（Linux、AIX）会跳过策略并在“执行状态”(Enforcement Status) 中报告同步错误。
- 避免创建过滤条件宽松的 Windows 操作系统过滤器。此类条件可能会打开不需要的网络端口。
- 如果操作系统过滤器是为使用者配置的，那么策略只适用于使用者，同样，如果是为提供者配置的，那么策略只适用于提供者。
- 由于对网络流的进程上下文、用户上下文或服务上下文了解有限或一无所知，如果策略采用基于 Windows 操作系统的过滤器，策略分析就会出现偏差。

使用基于 *Windows* 操作系统的过滤属性对策略进行验证和故障排除

如果使用基于 Windows 操作系统的过滤属性，则以下主题将为您提供验证和故障排除信息。

思科 TAC 可以根据需要使用这些信息来对此类策略进行故障排除。

基于应用名称的策略

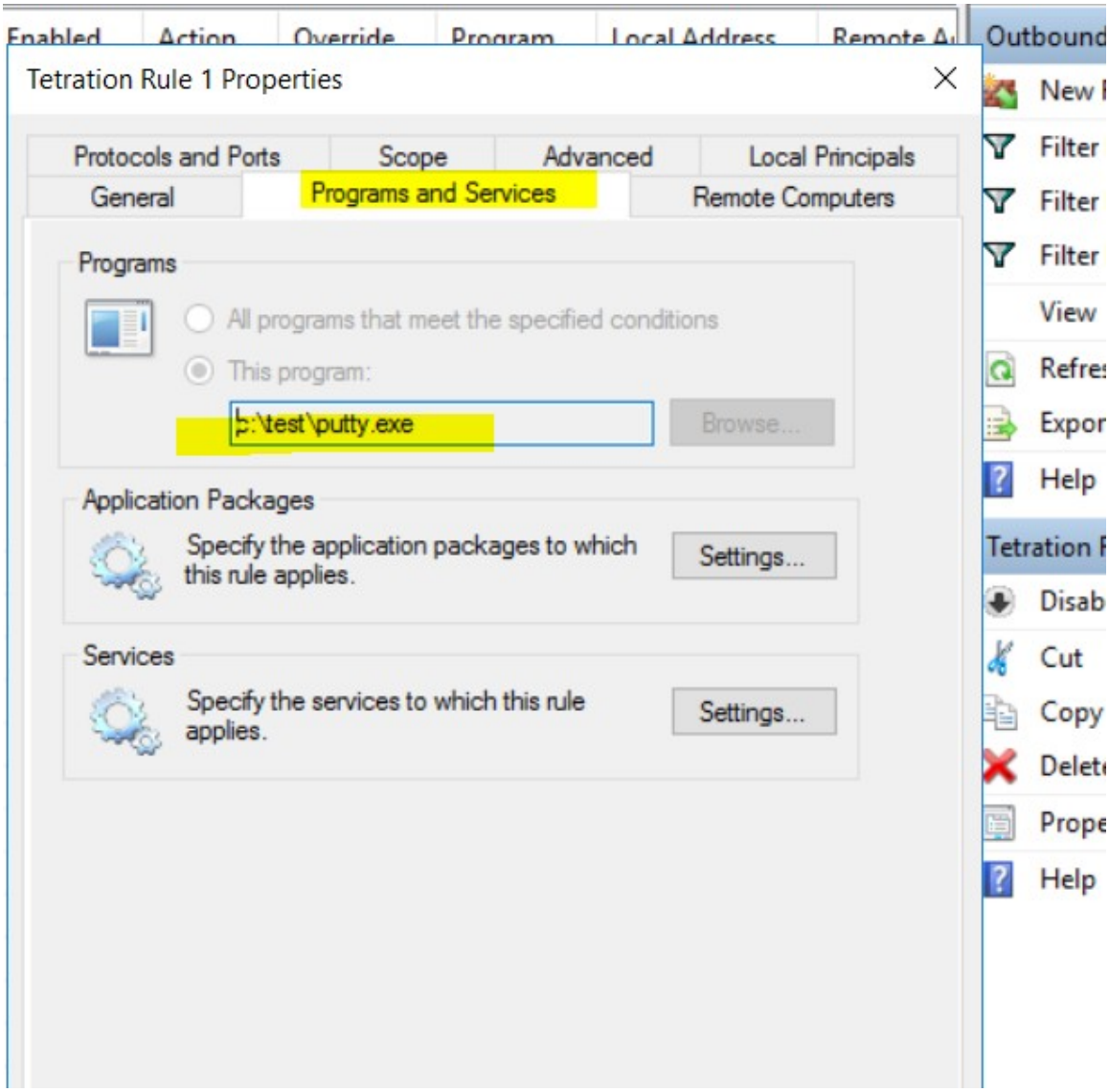
使用以下信息验证 Windows 操作系统工作负载上基于应用名称的策略并排除故障。

以下部分介绍策略在输入为 **c:\test\putty.exe** 的应用二进制文件的工作负载上应如何显示。

基于应用名称的示例策略

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

生成的防火墙规则



使用 **netsh**生成的过滤器

要使用本地 Windows 工具验证过滤器是否已添加到高级策略中，请执行以下操作：

- 使用管理权限运行 `cmd.exe`。
- 运行 `netsh wfp show filters`。
- 在当前目录中生成输出文件 **filters.xml**。
- 检查 FWPM_CONDITION_ALE_APP_ID 以获取输出文件中的应用名称：filters.xml。

```
<fieldKey>FWPM_CONDITION_ALE_APP_ID</fieldKey>
                    <matchType>FWP_MATCH_EQUAL</matchType>
                    <conditionValue>
```

```
                              <type>FWP_BYTE_BLOB_TYPE</type>
                              <byteBlob>
                                     <data>
→5c00640065007600690063006500 5c00680061007200640064006900 73006b0076006f006
→</data>
                                  <asString>\device\harddiskvolume2\temp\putty.exe</
→asString>
                </byteBlob>
        </conditionValue>
```

使用 tetenf.exe -l -f 生成的 WFP 过滤器

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

无效的应用名称

- 在 WAF 模式下，为无效的应用名称创建了防火墙规则。
- 在 WFP 模式下，不会为无效的应用名称创建 WFP 过滤器，但不会拒绝 NPC。代理会记录警告消息并配置其余策略规则。

基于服务名称的策略

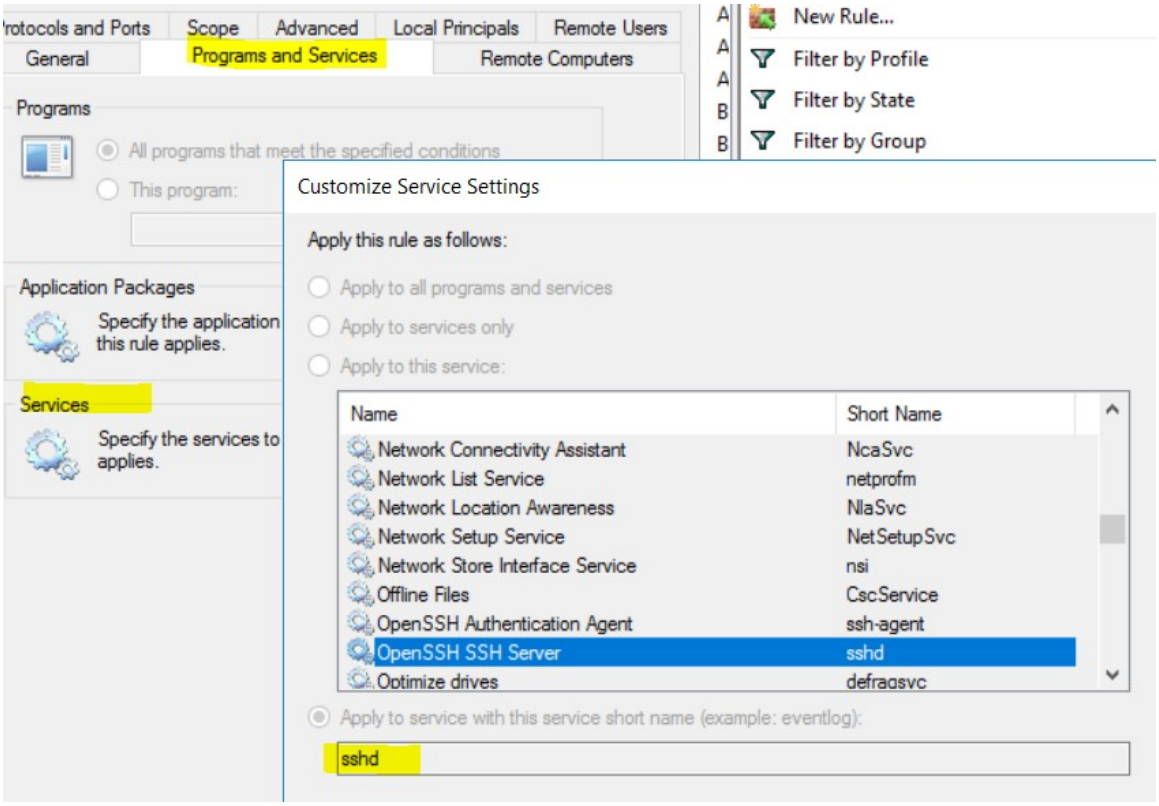
使用以下信息会根据 Windows 操作系统工作负载上的服务名称来验证策略并进行故障排除。

以下各节介绍策略应在工作负载上显示的方式。

基于服务名称的示例策略

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

生成的防火墙规则



使用 netsh生成的过滤器

要使用本地 Windows 工具验证是否已为高级策略添加过滤器，请执行以下操作：

- 使用管理权限运行 `cmd.exe`。
- 运行 `netsh wfp show filters`。
- 在当前目录中生成输出文件 **filters.xml**。
- 检查 FWPM_CONDITION_ALE_USER_ID 以获取输出文件 filters.xml 中的用户名。

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

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

使用 tetenf.exe -l -f 生成的 WFP 过滤器

```
Filter Name:       Cisco Secure Workload Rule 3
----------------------------------------------------------
```

```
EffectiveWeight:            18446744073709551590
LayerKey:                   FWPM_LAYER_ALE_AUTH_RECV_ACCEPT_V4
Action:                     Permit
Local Port:                 22
Protocol:                   6
User or Service:            NT SERVICE\sshd
```

无效的服务名称

- 在 WAF 模式下，系统会为不存在的服务名称创建防火墙规则。
- 在 WFP 模式下，系统不会为不存在的服务名称创建 WFP 过滤器。
- 服务 SID 类型必须为不受限制 *(Unrestricted)* 或受限制 *(Restricted)*。如果服务类型为无 *(None)*，则可以添加防火墙规则和 WFP 过滤器，但它们不起作用。

  要验证 SID 类型，请运行以下命令：

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

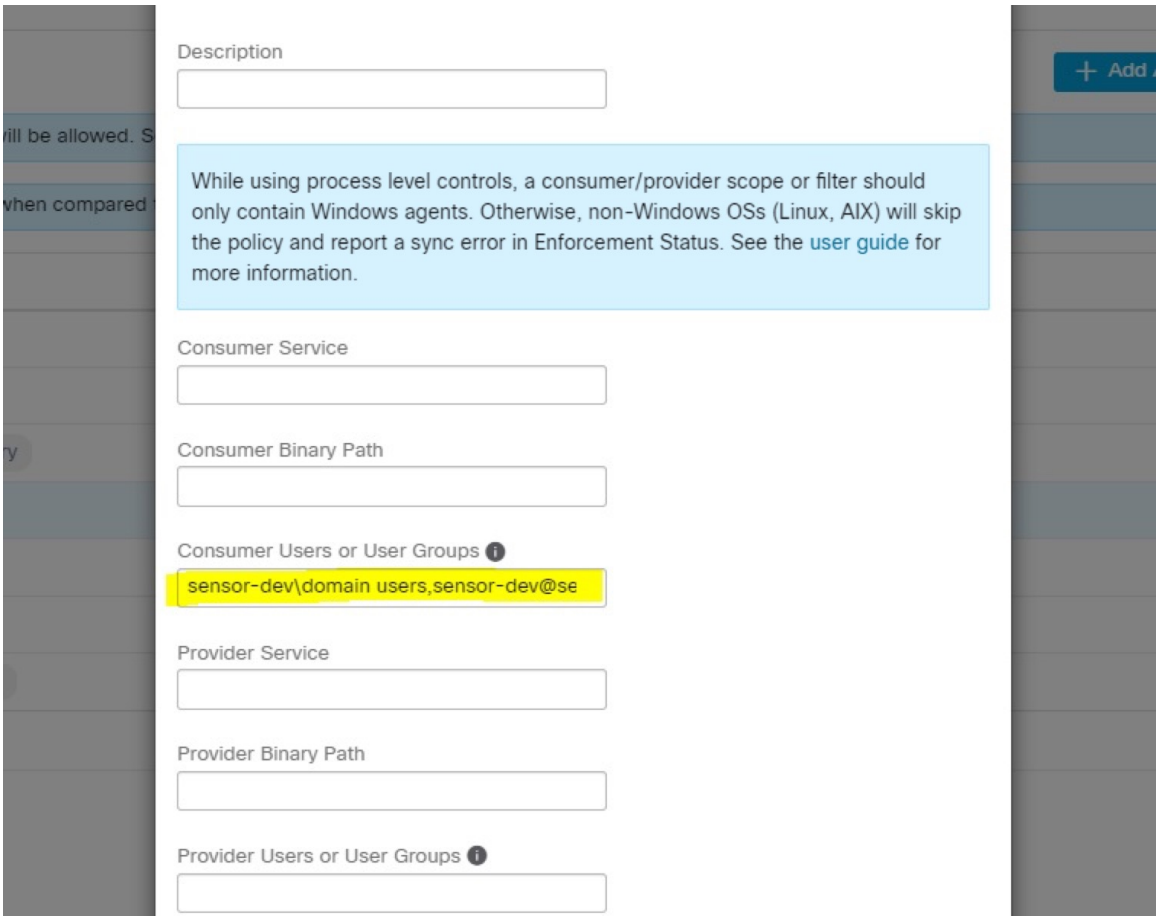
基于用户组或用户名的策略

使用以下信息会根据 Windows 操作系统工作负载上的用户名（带和不带用户组名称）来验证策略并进行故障排除。

本主题中的部分介绍策略应在工作负载上显示的方式。

本主题中的示例基于使用以下信息配置的策略：

Figure 27: 基于用户组或用户名的策略



基于用户名的策略示例

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

基于用户组和用户名的策略示例

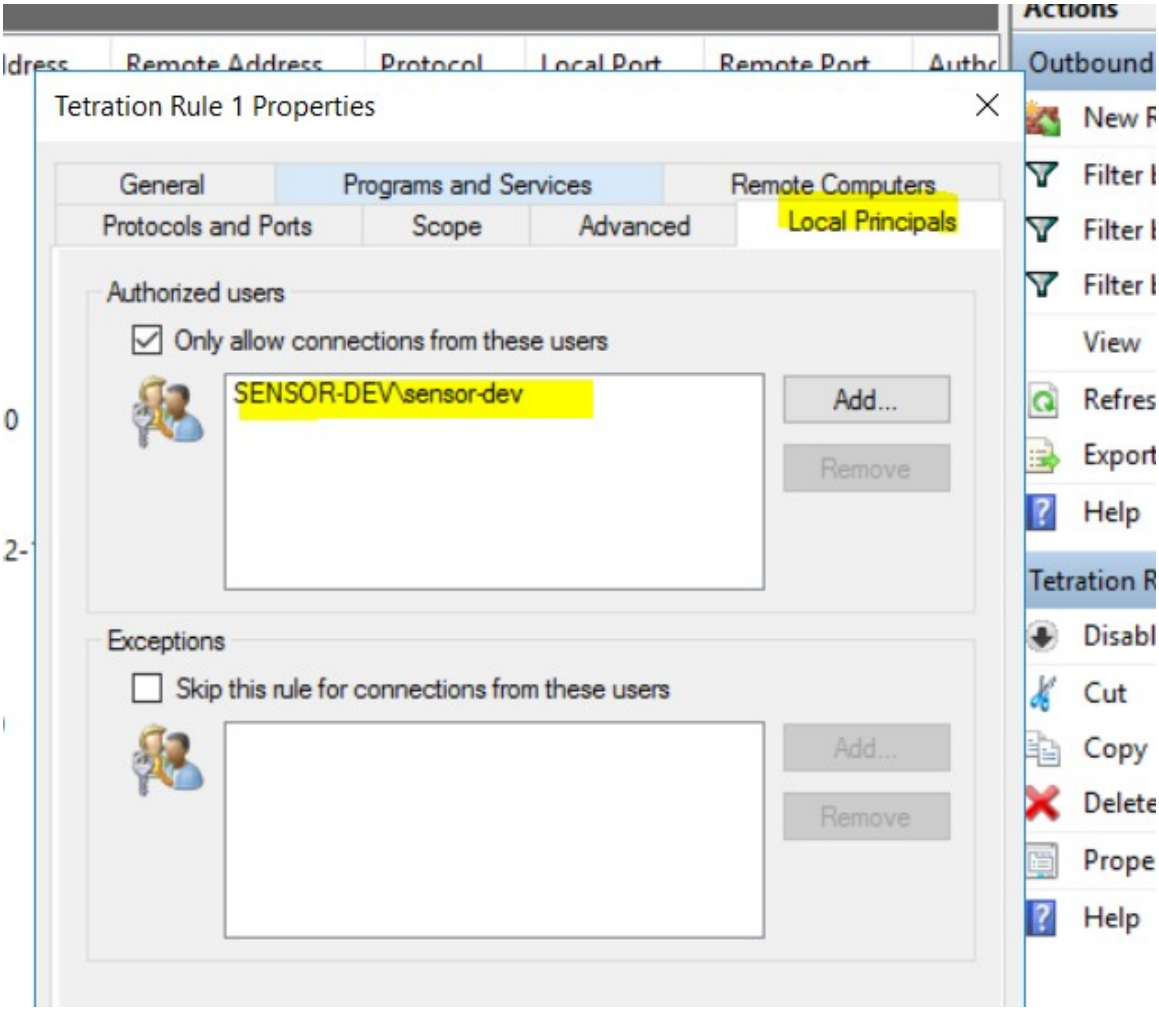
```
dst_ports {
start_port: 30000
end_port: 30000
provider_filters {
user_name: “sensor-dev\domain users,sensor-dev\sensor-dev”
}
}}
ip_protocol: TCP
```

```
address_family: IPv4
inspection_point: EGRESS
```

生成的防火墙规则

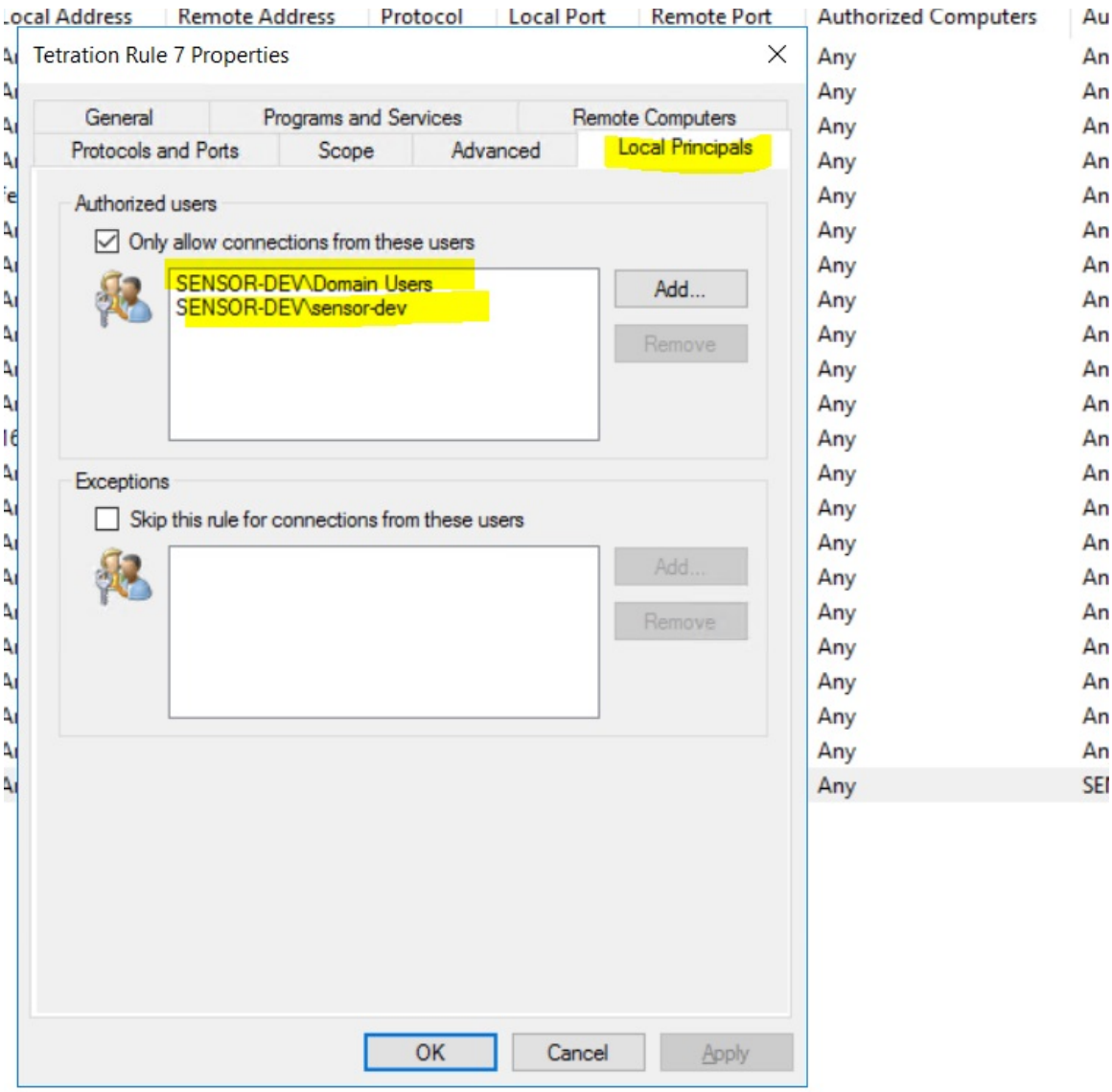
基于用户名的防火墙规则

示例：基于用户名 sensor-dev\sensor-dev 的防火墙规则



基于用户组和用户名的防火墙规则

示例：基于用户名 sensor-dev\sensor-dev 和用户组 domain users\sensor-dev 的防火墙规则



使用 netsh生成的过滤器

要使用本地 Windows 工具验证是否已为高级策略添加过滤器，请执行以下操作：

- 使用管理权限运行 `cmd.exe`。
- 运行 `netsh wfp show filters`。
- 在当前目录中生成输出文件 **filters.xml**。
- 检查 FWPM_CONDITION_ALE_USER_ID 以获取输出文件 filters.xml 中的用户名。

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

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

使用 tetenf.exe -l -f 生成的 WFP 过滤器

基于用户名过滤

示例：基于用户名 SENSOR-DEV\sensor-dev 的 WFP 规则

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

基于用户组和用户名过滤

示例：基于用户名 SENSOR-DEV\sensor-dev 和用户组名 SENSOR-DEV\Domain Users 的 WFP 规则

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

无法为网络策略规则配置服务名称和用户名。

Note 如果用户名或用户组无效，则网络策略会被 Windows 代理拒绝。

Kubernetes 和 OpenShift

（可选）Kubernetes 工作负载的其他策略

以下程序为可选，具体取决于您的 Kubernetes 环境。

在主机网络模式下运行的 *Kubernetes Nginx* 入口控制器的策略

当 Pod 使用 Kubernetes 入口对象暴露给外部客户端时，Cisco Secure Workload 会在 Nginx 入口控制器和后端 Pod 上执行策略。

Note 如果入口控制器不是在主机网络模式下运行，请参阅 IngressControllerAPI

Note IBM-ICP 默认使用 Kubernetes Nginx 入口控制器，并以主机网络模式在控制平面节点上运行。

以下是使用 Kubernetes Nginx 入口控制器执行策略的步骤。

Procedure

步骤 1 如此处所述，为 Kubernetes/OpenShift 创建外部协调器。

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

步骤 2 在 Kubernetes 集群中创建入口对象。下图提供了用于创建入口对象的 yaml 文件的快照。

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

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

步骤 3 在 Kubernetes 集群中部署 Kubernetes Nginx Ingress 控制器。IBM-ICP 入口控制器 Pod 默认在控制平面节点上运行。

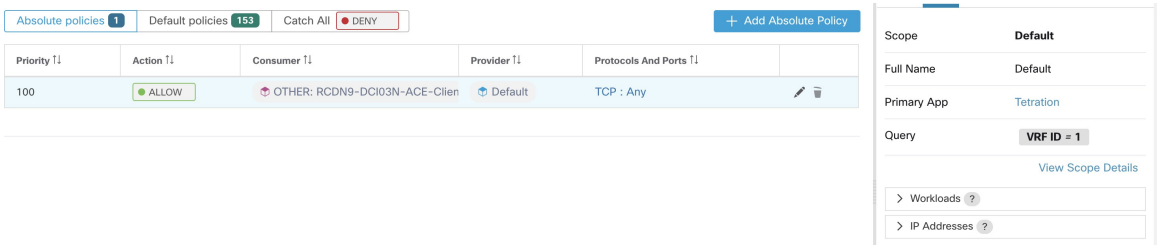
```
~
▶ k8s get pods -o wide -n ingress-nginx
NAME                                        READY   STATUS    RESTARTS   AGE     IP              NODE                          NOMINATED NODE
nginx-ingress-controller-6bc9c6745c-scfzs   1/1     Running   0          2m11s   192.168.10.13   enforcement-scale-16-kube3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

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

步骤 4 创建一个后台服务，以供集群外的使用者访问。在下面提供的示例中，我们创建了一个简单的 *svc-ce2e-teeksitlbiwlc* (http-echo) 服务。

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

步骤 5 在外部使用者和后端服务之间创建策略。



步骤 6 准备就绪后，执行策略。

步骤 7 如果是 Nginx 入口控制器 Cisco Secure Workload，则软件将应用适当的允许/丢弃规则，其中源将是上述步骤中指定的使用者，目标将是相应的入口控制器 Pod IP。对于后端 Pod，Cisco Secure Workload 软件将应用适当的允许/丢弃规则，其中源为入口 Pod，目标为后端 Pod IP。

作为部署/守护程序集运行的 *Kubernetes Nginx/Haproxy* 入口控制器的策略

当 Pod 使用 Kubernetes 入口对象暴露给外部客户端时，Cisco Secure Workload 将在入口控制器和后端 Pod 上执行策略。

以下是在入口控制器上执行策略的步骤。

Procedure

步骤 1 使用 OpenAPI 创建/更新用于 Kubernetes/OpenShift 的外部协调器。有关使用 OpenAPI 来创建外部协调器的信息，请参阅协调器。为外部协调器配置添加入口控制器信息。

步骤 2 在 Kubernetes 集群中创建入口对象。

步骤 3 在 Kubernetes 集群中部署入口控制器。

步骤 4 创建一个后台服务，以供集群外的使用者访问

步骤 5 在外部使用者和后端服务之间创建策略。

步骤 6 准备就绪后，执行策略。

步骤 7 如果是入口控制器，Cisco Secure Workload 软件将应用适当的允许/丢弃规则，其中源将是上述步骤中指定的使用者，目标将是相应的入口控制器 Pod IP。对于后端 Pod，Cisco Secure Workload 软件将应用适当的允许/丢弃规则，其中源为入口 Pod，目标为后端 Pod IP。

分组工作负载：集群和资产过滤器

集群和资产过滤器的用途类似，但有一些重要区别：

表 4: 集群和资产过滤器的比较

集群	资产过滤器
用于将策略应用于范围中的部分工作负载。	可用于将策略应用于范围中的部分工作负载。 也可用于将策略应用于任何范围的工作负载（例如，将策略应用于运行特定操作系统的所有工作负载。）
由查询定义	由查询定义。
只能包括单个范围中的工作负载。	成员身份可以仅限于单一范围，也可以包括任何范围内的工作负载（例如，如果过滤器基于操作系统）。
只能由同一工作空间和工作空间版本中的策略使用。	可供任何范围和任何工作空间中的策略使用。
可以在自动策略发现期间自动创建。	必须手动创建集群或从现有集群转换。
如果未经批准，可在自动策略发现期间被覆盖。批准已知良好的集群可以提高其他集群在未来发现运行中的准确性。	绝不会被自动策略发现所修改。
受益于自动策略发现的重要功能。多年服务合同具有以下优势： • 具有可帮助您评估组中的工作负载是否属于同一类别的可信度评级。 • 可与同一工作空间上的其他策略发现运行期间生成的集群进行比较。	--
不能在配置 外部依赖关系， 第 31 页 以及与跨范围策略和策略发现相关的其他功能时使用。	可用于配置涉及外部依赖关系和与跨范围策略相关的其他功能（例如自动引导规则）的精细策略。
请参阅集群， 第 72 页以及子主题。	请参阅创建资产过滤器和将集群转换为资产过滤器， 第 76 页

集群

集群是在一个工作空间内分组的一组工作负载。（Cisco Secure Workload 部署也可以称为集群，但这两种用法无关紧要。）

例如，如果您的应用范围包括构成应用的许多其他类型的服务器和主机中的几个网络服务器，您可能希望在此应用范围内有一个网络服务器集群，这样您就可以只为这些网络服务器分配特定的策略。

自动策略发现功能可根据运行配置过程中指定的时间范围内观察到的信号，将工作负载分组到集群中。

每个集群由一个查询定义

集群查询是动态的，除非您使用特定的 IP 地址来定义它们。通过动态查询，集群成员身份可以随时间而改变，以反映资产的变化：更多的工作负载、更少的工作负载或不同的工作负载都能与查询相匹配。

例如，如果集群查询基于包含子字符串“HR”的主机名，并且有更多主机名包含 HR 的主机被添加到工作空间，那么集群就会自动包含新增的主机。

自动策略发现会检查与工作负载相关的主机名和标签。对于每个集群，自动策略发现会根据主机名和这些标签生成一个候选查询的简短列表。您可以从这些查询中选择一个，也可以对其进行编辑，并将其与集群相关联。请注意，在某些情况下，如果自动策略发现无法根据主机名和标签制定足够简单的查询，则不建议进行（备用）查询。

已批准集群中的工作负载不受未来策略发现的影响

只有尚未成为相关工作空间中已批准集群成员的工作负载才会受到策略发现的影响。 **已批准的集群**是您手动批准的集群。有关详细信息，请参阅批准集群, on page 80。

编辑集群以改进分组

在以下部分中，我们将介绍一些编辑、增强和批准集群结果的工作流程。请注意，只能在最新版本的工作空间中更改/批准集群（请参阅活动日志和版本历史记录）。

请参阅对集群进行更改, on page 75。

涉及 Kubernetes 资产的集群

Note 如果工作空间包含多个 Kubernetes 命名空间的库存，则每个集群查询都必须按命名空间过滤。如果还没有命名空间过滤器，则将其添加到每个查询中。如果更改了任何查询，则会再次自动发现策略。

集群可能包含单个工作负载。

您可能只想创建涉及单一工作负载的策略。

集群可以转换为资产过滤器

与已批准的集群一样，升级为资产过滤器的集群在随后的策略发现过程中也不会改变。

与集群不同，资产过滤器不与工作空间绑定，而是在 Cisco Secure Workload 部署中全局可用。

有关集群和资产过滤器的比较，请参阅分组工作负载：集群和资产过滤器, on page 71。

请参阅将集群转换为资产过滤器, on page 76。

集群可信度

使用集群的可信度或质量评分来确定需要改进的集群。

集群的可信度是成员工作负载的平均可信度。通常，工作负载与所分配集群的其他成员越相似，与最接近（最相似）的替代集群的工作负载越不相似，该工作负载的可信度就越高。

在使用流进行集群时，如果两个工作负载具有相似的对话模式（如对话图中相似的邻域集，即相似的使用者和提供者工作负载和端口集），那么这两个工作负载就是相似的。

Note

- 未计算（未定义）以下对象的集群可信度：
  - 仅包含一个工作负载的集群
  - 已批准的集群
  - 范围内未观察到通信的工作负载（如果选择基于进程的集群，则无进程信息可用）
- 集群不会跨越分区边界（如子网边界，请参阅高级自动策略发现配置中的路由标签）。但在计算可信度和备用集群时，这些边界会被忽略。这表示可能存在行为非常相似的工作负载或集群，即使它们位于不同的子网中也是如此。
- 编辑集群后，可信度评分可能会变得不准确，因为在您再次发现策略之前不会对它们进行重新计算。

要查看集群可信度，请参阅查看集群, on page 74。

查看集群

集群视图支持查询到集群的关联和查询编辑。

在集群视图中，您可以点击表列标题以根据该列（例如名称、工作负载数量或可信度）对集群进行排序。

对于每个集群，点击其行即可在右侧面板中查看更多集群信息，如说明、建议或批准的查询以及成员工作负载。其中一些字段可以编辑。

要查看集群及其详细信息，请执行以下操作：

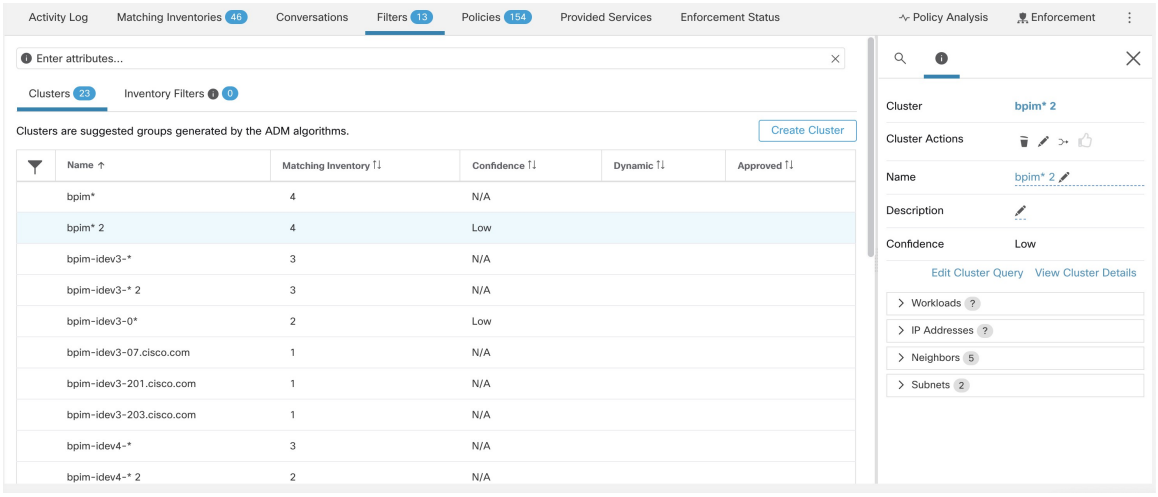
1. 导航至所需的范围和工作空间。

   集群特定于工作空间；范围中的每个工作空间都可以具有不同的集群。要使集群在其当前工作空间之外可用，请参阅将集群转换为资产过滤器, on page 76。

2. 点击**管理策略 (Manage Policies)**。
3. 点击**过滤器 (Filters)**。
4. 点击**集群 (Cluster)**。
5. 要查看有关集群的信息，请点击集群。
   a. 查看右侧打开的面板。
   b. 有关更多详细信息，请点击**查看集群详细信息 (View cluster details)**。

系统将在单独的浏览器选项卡中打开“集群详细信息”(Cluster Details) 页面。

Figure 28: 集群视图



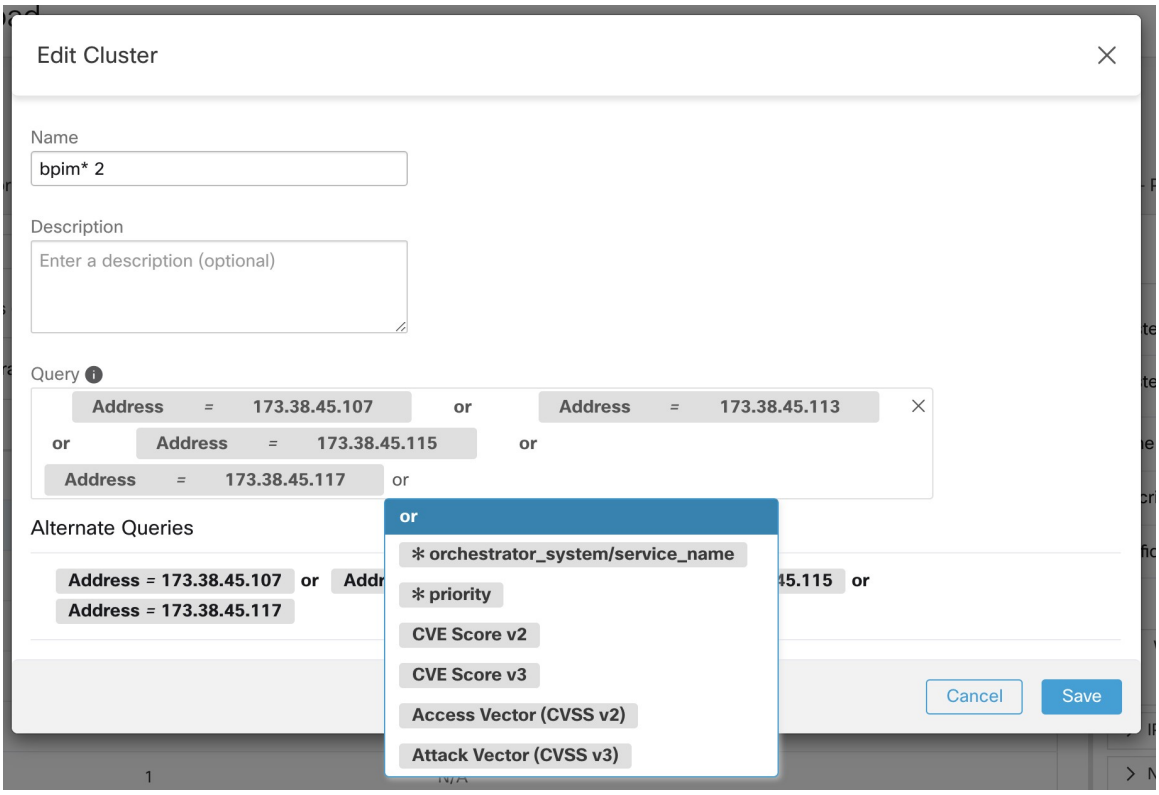
对集群进行更改

自动发现策略可为每个集群创建一个或多个候选查询。

如果集群结果不完全符合您的预期，则可以通过编辑查询来改进分组。

要浏览和编辑集群，请执行以下操作：点击页面顶部的**集群**框。要更改集群（例如更改集群成员或选择/更改其查询），请选择/编辑集群的查询，如下图所示。

Figure 29: 编辑集群



您可以添加或删除显示 IP 地址，或从提供的备选列表中选择另一个查询并编辑该查询。集群的查询可以是任何以地址、主机名和标签表示的查询过滤器。如果基于标签而不是显式 IP 地址定义查询，则集群将是动态的，并且正确标记的新资产、更改的资产或删除的资产都将自动包含在集群中或从集群中排除。

在完成查询选择和可能的编辑后，点击保存。请注意，点击“保存”(SAVE) 按钮后，集群会自动标记为已批准，已批准的大拇指向上图标会变为蓝色（无论是否进行了更改）。可以切换已批准图标以根据需要来更改已批准状态。请参阅批准集群, on page 80中的详细信息

Important 当集群成员发生变化时，可能需要再次发现策略，以获得能准确反映变化集群间流变化的更新策略。这是因为集群成员身份可能已发生变化（如集群中添加了新的节点）。如果工作空间对应的范围被编辑，或者工作空间成员身份发生了变化，则也会出现类似情况。同样，集群可信度评分可能随着集群成员身份的更改而不再准确。在所有这些情况下，再次自动发现策略对于获取更新的策略和集群可信度评分（未经批准的集群上的更新可信度）非常有用。

如果编辑集群查询，与查询相关的集群可能会重叠。

将集群转换为资产过滤器

在以下情况时，将集群转换为资产过滤器：

- 您不希望集群在今后的自动策略发现运行中被修改，这是批准集群的一种更通用的替代方法。
- 您希望集群独立于工作空间和工作空间版本。
- 您在创建或发现策略时，使用者和提供者属于不同的范围，您希望创建特定于范围中工作负载子集的策略，而不仅仅是涉及整个范围的策略。

  如果使用 当使用者和提供者处于不同范围时：策略选项，第 88 页 中所述的高级方法来创建跨范围策略，并且希望策略比范围到范围更精细，则必须为此目的使用资产过滤器而不是集群。

过程

步骤 1 导航至包含要升级的集群的工作空间。

步骤 2 点击**管理策略 (Manage Policies)**。

步骤 3 点击**过滤器 (Filters)**。

步骤 4 点击**集群 (Cluster)**。

步骤 5 点击要在跨范围策略中使用的集群。

步骤 6 在右侧面板的**集群操作 (Cluster Actions)** 部分中，点击 （升级为资产过滤器。）

步骤 7 验证名称、说明和查询是否符合预期。

步骤 8 选择**将查询限制为所有权范围 (Restrict Query to Ownership Scope)**。

（资产过滤器可以跨越范围边界，但您不希望为此目的出现这种行为；您希望此过滤器只包含此范围中的工作负载。）

步骤 9 如果希望此资产过滤器定义的应用成为自动策略发现期间生成的策略中的提供者，请选择**提供超出其范围的服务 (Provides a service external of its scope)**。

如果此应用是使用者而不是提供者，或者如果只将此资产过滤器用于手动创建的策略，则无需启用此选项。

步骤 10 点击**升级集群 (Promote Cluster)**。

步骤 11 验证集群是否已移至**资产过滤器 (Inventory Filters)** 选项卡。

您可能需要刷新页面才能看到此更改。

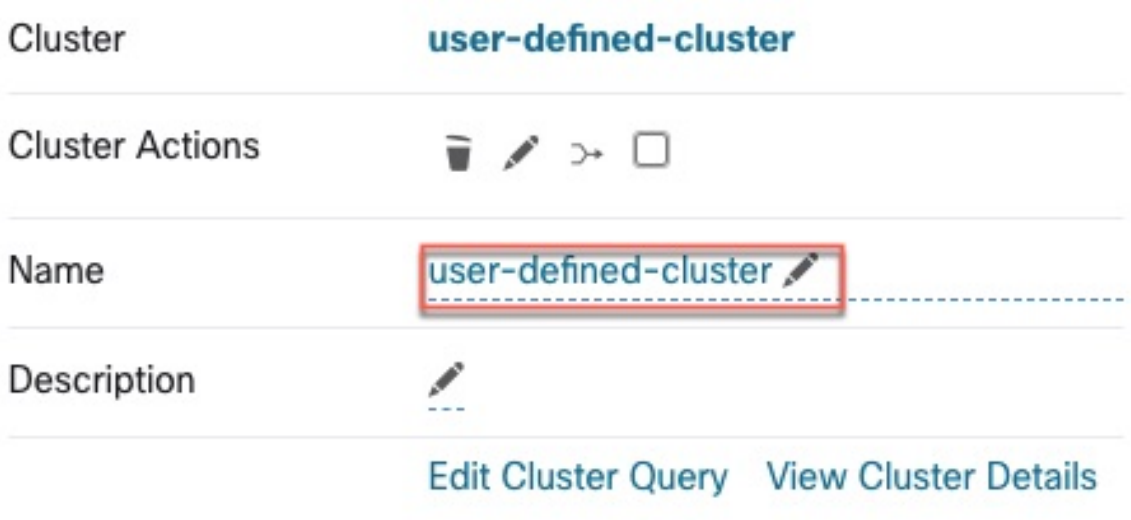
创建或删除集群

点击集群页面上的**创建集群 (Create Cluster)** 按钮以创建新的空集群。或者，您也可以点击“开始”侧栏中的 **创建过滤器 (Create Filter)** 按钮，然后在模式中选择集群，以便从自动策略发现页面创建集群。

Figure 30: 创建新的集群

新的用户定义集群将显示在侧板上，如有必要，可重新命名。

Figure 31: 重命名集群



删除空集群的方法是在任何视图中选择集群，使其详细信息显示在侧面板上，然后点击集群详细信息视图标题上的垃圾桶按钮。请参阅上图。

比较生成的集群的版本：差异视图

在为一个工作范围自动发现策略至少两次后，就可以比较不同发现运行中生成的集群。

Procedure

步骤 1 使用以下路径之一导航至集群差异视图：

- 成功发现策略后，将显示一条消息，指示成功发现一个链接，用于导航至显示发现结果的差异视图。点击结果链接。

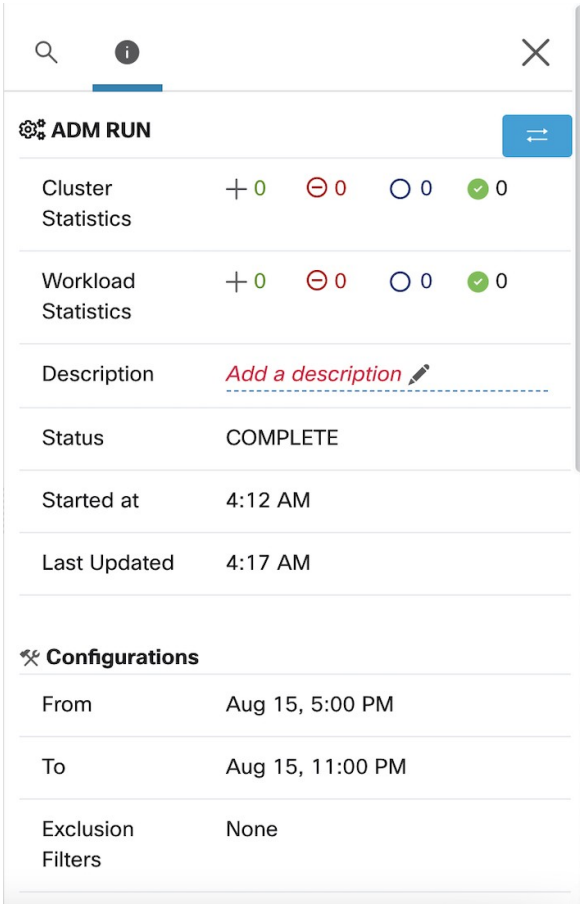
  Figure 32: 自动策略发现运行成功

- 从版本视图比较修订：
  a. 请执行查看、比较和管理发现的策略版本, on page 50中的步骤。
  b. 点击**比较修订 (Compare Revisions)** 后，点击**集群 (Clusters)**。
- 在版本详细信息侧面板中：
  a. 按照 查看、比较和管理发现的策略版本, on page 50 中的步骤查看版本详细信息。

b. 当侧面板显示自动策略发现运行的上下文信息时，点击侧面板右上角的双箭头按钮：

Figure 33: 显示上下文信息



步骤 2 选择要比较的版本。

步骤 3 查看比较结果：

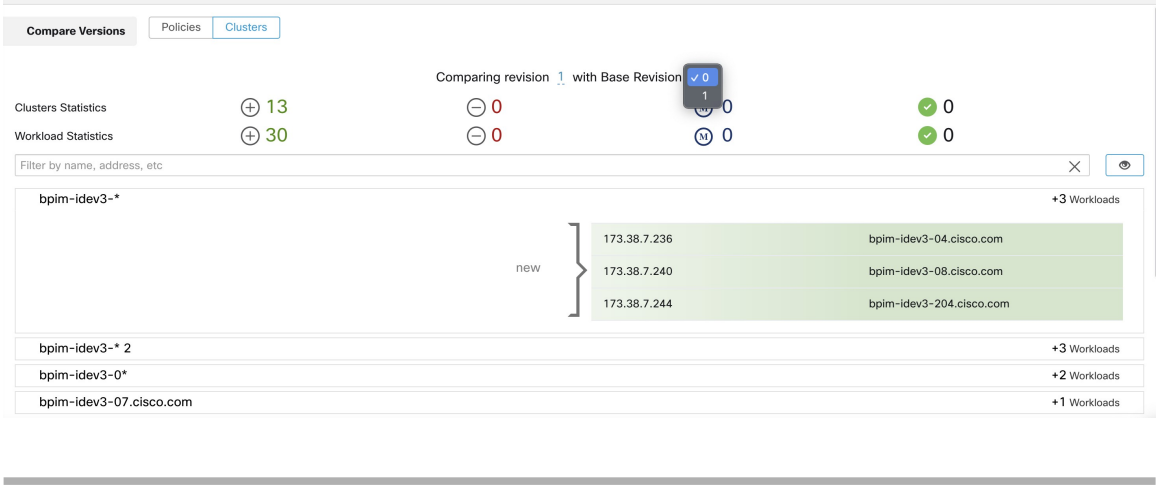
在顶层，自动发现策略的差异视图会显示集群和工作负载变化的高级统计信息，从而显示添加、删除、修改和未更改的集群和工作负载数量。

视图的其余部分按添加、删除、修改和未更改的顺序整理为集群列表，每种颜色编码以反映状态以及添加到集群或从集群删除的工作负载数量。

您可以按名称或IP地址来搜索特定集群或工作负载。要查看集群内容的变化情况，请点击代表集群的任意行将其展开。

Note 默认情况下，系统会隐藏未更改的集群。要显示未更改的集群，请点击眼睛图标按钮。

Figure 34: “集群差异” *(Cluster Diff)* 视图



What to do next

要查看策略的类似比较，请参阅策略版本比较：策略差异。

在自动策略发现重新运行期间防止修改集群

如果不想让自动策略发现（以前称为 ADM）在将来为工作空间自动发现策略时修改集群，请批准集群。

例如，如果您已编辑集群查询，则批准集群，并且现在需要将新工作负载添加到范围并对它们进行集群，而不会影响现有策略。批准集群会将集群内容和属性以当前状态冻结。自动策略发现不会更改已批准的集群。

请参阅批准集群，第 80 页。

或者，也可以将集群提升为资产过滤器，这样就不会被策略发现修改。请参阅将集群转换为资产过滤器，第 76 页。

批准集群

Note 另请参阅将集群转换为资产过滤器, on page 76，这可能是更适合您需求的选项。

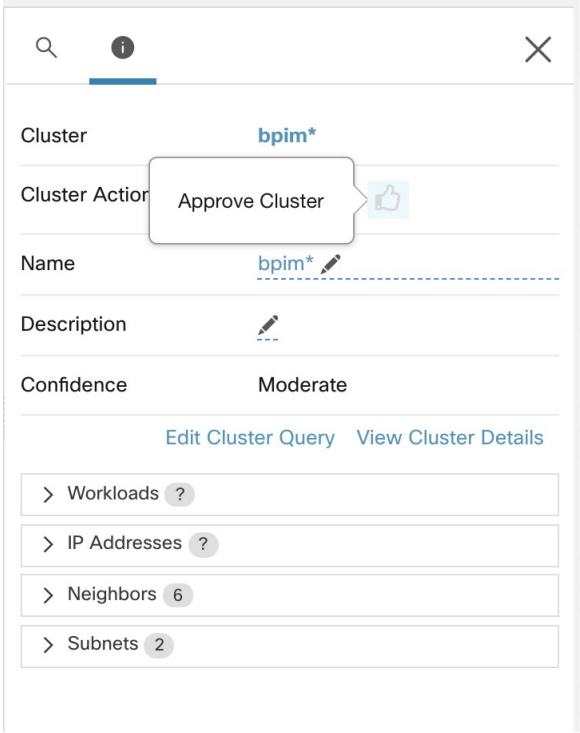
在批准集群后，后续自动策略发现不会更改该集群的查询。只有当工作空间的成员发生变化时，已批准集群的成员身份才能更改。

属于已批准集群的成员的工作负载可能被称为“已批准工作负载”。

要批准集群，请执行以下操作：

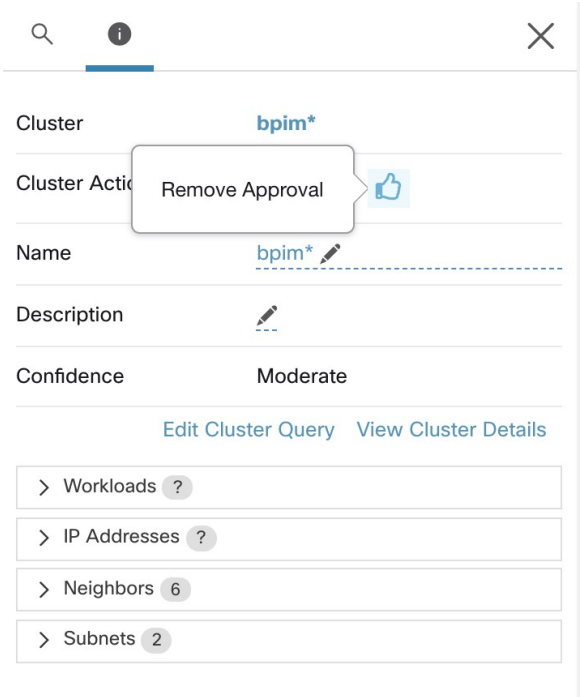
确保侧面板上显示了关注的集群。您可以通过搜索集群，或在任何视图中点击图表上所需的集群来实现这一功能。然后选中侧板上集群信息右上角的复选框，如下所示。集群获得批准后，它会表明其在未来的自动策略发现中将保持不变。

Figure 35: 批准集群



要删除集群的批准，请点击批准图标 。

Figure 36: 删除集群的批准



解决策略复杂性问题

执行结果受以下因素影响：

- 规则类型和等级：
  - 绝对策略与默认策略
  - 工作空间的捕获全部设置

  请参阅策略等级：绝对、默认和捕获全部，第 9 页。
- 工作空间中的策略顺序

  请参阅策略优先级，第 82 页。
- 从父范围或祖先范围继承的策略，包括捕获全部规则

  您需要确保优先级较高的策略不会在预期命中流量的策略之前命中流量。

  要查看祖先范围中策略的影响，请对所有相关范围运行实时策略分析。请参阅实时策略分析，第 111 页。

  当您准备在工作空间中执行策略时，向导会显示哪些继承的策略会对工作空间中的工作负载产生影响。有关信息，请参阅策略执行向导，第 127 页。
- 跨范围策略交互

  （当使用者和提供者在不同的范围内，或者对话的一端与策略的范围不同时）

  请参阅当使用者和提供者处于不同范围时：策略选项，第 88 页。
- 策略中的实际使用者或提供者可能与默认配置的使用者和提供者不同的情况，例如在确保您的策略能解决不常见或不经常发生的活动和情况，如故障转移、从备份恢故障转移场景中。

  请参阅有效使用者或有效提供者，第 101 页。

策略优先级

流量处理受以下因素影响：

- 范围内策略的优先级，以及
- 策略全局排序和冲突解决方法, on page 83

范围内的策略优先级

在工作空间内，列表中的策略顺序反映了每个策略的相对优先级，优先级最高的策略位于列表顶部，优先级最低的策略位于列表底部。

在每个工作空间中，绝对策略的优先级高于默认策略，且捕获全部策略是工作空间中优先级最低的策略。

有关详细信息，请参阅策略等级：绝对、默认和捕获全部, on page 9。

策略全局排序和冲突解决方法

不同范围下定义的不同策略之间可能会发生冲突。更具体地说，当属于多个范围（例如父/子范围）的工作负载（资产项目）具有相互冲突的策略时，就会发生冲突。

由于范围成员身份的动态性质，手动解决此类冲突是不可行的；工作负载会随着其属性的变化而进入或离开范围。因此，系统会根据定义所有策略的范围为所有策略实施全局顺序，如下所述。对于每个工作负载，相关策略列表（根据使用者/提供者/范围）按全局顺序进行标识和排序。根据排序列表中的第一个匹配策略会做出允许或丢弃流的决定。

通过了解安全策略的全局排序方案，网络管理员就可以定义正确的范围及其优先级，从而在工作负载上应用所需的整体策略。在每个范围内，应用所有者保持对其各自工作负载执行精细策略的能力。

全局网络策略具有以下特征：

- 一组按优先级排序的范围（优先级最高的在前）。
- 每个范围的主工作空间都有绝对策略、默认策略和捕获全部操作。
- 每个工作空间中的每组绝对策略或默认策略会根据其本地优先级（从高到低）进行排序。

策略的全局顺序定义如下：

- 所有范围的主工作空间中的绝对策略组（按优先级从高到低排列）。
- 主工作空间所有范围内的默认策略组（按优先级从最低到最高排列）。
- 来自所有范围的捕获全部策略（按优先级从最低到最高排列）。

请注意，范围顺序适用于类别 1 和 2 中的策略组，而不是单个策略。在每个组中，具有较低策略优先级编号的单个策略优先。

对于特定工作负载，首先确定其所属的范围子集，然后应用上述顺序。此工作负载所属的最低优先级（已执行）工作空间的捕获全部策略是适用的捕获全部（但绝对或默认策略可能会覆盖）。对于该工作负载上的给定流，系统将应用最高匹配策略的操作。

Note

- 如果工作空间未定义绝对策略和默认策略，则会忽略该工作空间。工作空间的捕获全部策略不会包含在全局顺序中。
- 默认策略在全局顺序中的顺序与范围优先级相反。这使您可以为所有范围定义广泛的策略，以保护所有工作空间的边界，包括未启用策略执行的工作空间。同时，已在其范围上启用执行的应用所有者能够覆盖这些默认策略。
- 不建议使用重叠范围；有关详细信息，请参阅范围重叠。但是，如果工作负载有两个或更多接口，并且处于重叠或不相交的范围内，则将应用启用了执行的最低优先级工作空间的捕获全部策略（在所有适用的捕获全部策略中）。

我们扩展了之前的三范围示例来说明此排序方案。假设为三个范围分配了以下优先级（有关如何更改范围优先级的说明，请参阅使用工作空间管理策略）：

1. 应用
2. Apps:HR
3. Apps:Commerce

其中每个范围的主工作空间具有绝对策略、默认策略和捕获全部操作。每个工作空间中的每组绝对策略或默认策略会根据其本地优先级进行排序。

策略的全局排序如下：

1. 应用绝对策略
2. Apps:HR 绝对策略
3. Apps:Commerce 绝对策略
4. Apps:Commerce 默认策略
5. Apps:HR 默认策略
6. 应用默认策略
7. Apps:Commerce 捕获全部
8. Apps:HR 捕获全部
9. 应用捕获全部

属于应用范围的工作负载将仅按给定顺序接收以下策略：

1. 与工作负载匹配的应用绝对策略
2. 应用默认策略
3. 应用捕获全部

属于 *Apps* 和 *Apps:Commerce* 范围的工作负载仅按给定顺序接收以下策略：

1. 应用绝对策略
2. Apps:Commerce 绝对策略
3. Apps:Commerce 默认策略
4. 应用默认策略
5. Apps:Commerce 捕获全部

属于 *Apps* 和 *Apps:HR* 范围的工作负载将仅按给定顺序接收以下策略：

1. 应用绝对策略
2. Apps:HR 绝对策略
3. Apps:HR 默认策略
4. 应用默认策略
5. Apps:HR 捕获全部

策略顺序和重叠范围

Important 以下场景涉及重叠范围。您应避免使用重叠的同级范围 - 工作负载不应是范围树多个分支的成员。有关详细信息，请参阅范围重叠。

属于 *Apps*、*Apps:HR* 和 *Apps:Commerce* 所有三个范围的工作负载将按给定顺序接收以下策略：

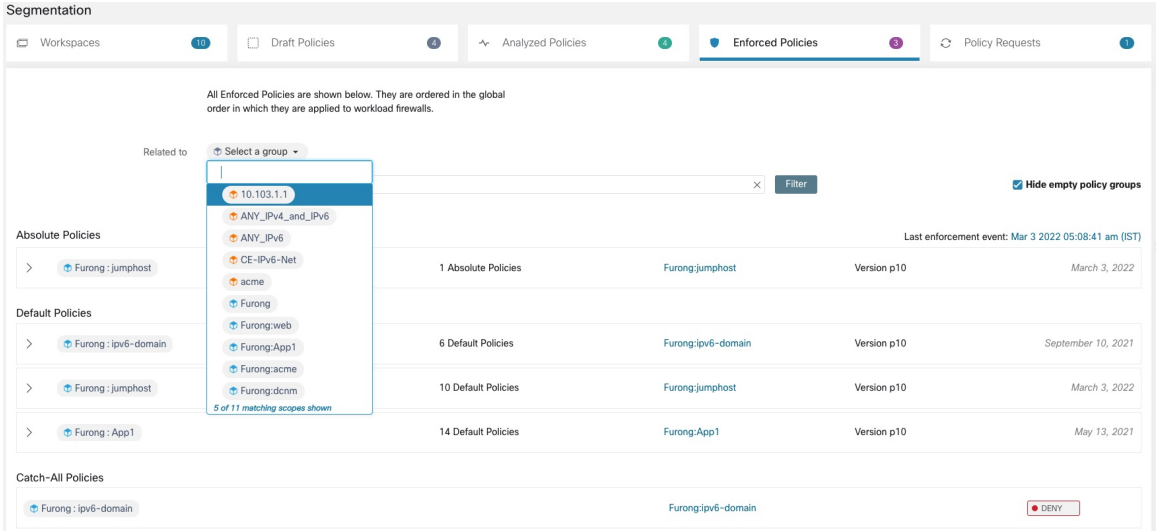
1. 应用绝对策略
2. Apps:HR 绝对策略
3. Apps:Commerce 绝对策略
4. Apps:Commerce 默认策略
5. Apps:HR 默认策略
6. 应用默认策略
7. Apps:Commerce 捕获全部

请注意，仅当两个范围重叠时（即，存在同时属于两个同级范围的工作负载），*Apps:HR* 和 *Apps:Commerce* 范围的相对顺序才有意义。这是因为策略始终在范围下定义。只属于一个范围的工作负载不会受到另一个范围策略的影响，因此顺序并不重要。

验证策略的顺序和优先级

要验证父/祖先工作空间中策略的顺序和优先级，请点击“防御”(Defend) >“分段”(Segmentation)页面顶部的**已分析策略 (Analyzed Policies)** 或**已执行的策略 (Enforced Polices)** 选项卡。这些视图分别提供了分析策略和执行策略的全局视图。

Figure 37: 示例：按策略优先级顺序排列的执行策略列表



- 要将策略列表限制为只包含作为使用者或提供者的特定范围或过滤器的策略，请选择范围或输入过滤器。
- 可用过滤器：

过滤器名称	定义
端口	要匹配的策略端口，例如 80。
协议	要匹配的策略协议，例如 TCP。
已批准	匹配已标记为已批准的策略 的策略。
外部？	使用者和提供者在不同范围内的策略。
操作	策略操作：允许或拒绝

（高级）更改策略优先级

注意 范围策略优先级顺序很少需要更改。由于更改策略优先级会影响所有工作空间的执行结果，因此要谨慎更改。

只有具有极高权限角色的用户（例如站点管理员）才能访问此功能。

开始之前

在更改范围优先级顺序之前：

- 了解策略排序逻辑，以及范围上的策略优先级如何转化为单个策略意图的排序。请参阅策略优先级，第 82 页。
- 在辅助工作空间内进行更改，直到确信新顺序符合预期。
- 计划更改时，请考虑以下准则：

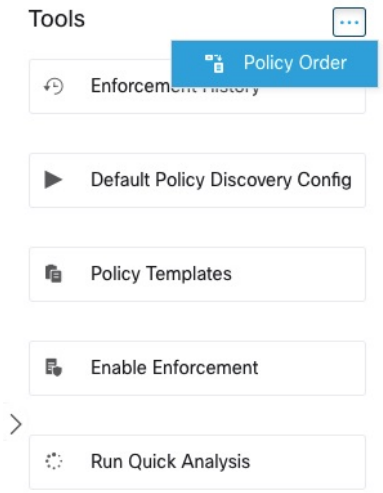
  在重新排序时，请保持父项优先顺序（父范围在子范围之上），以充分利用范围树的层次结构。

  （如果您有重叠的同级范围，则可能需要对同级范围及其子项重新进行排序。不建议使用重叠的同级范围。通过更新范围查询来修复这些问题。请参阅范围重叠。）

过程

步骤 1 要重新排序策略优先级，请点击**工具 (Tools)** 旁边的菜单图标，然后选择**策略顺序 (Policy Order)**：

图 *38:* 导航至“策略优先级”*(Policy Priorities)* 页面



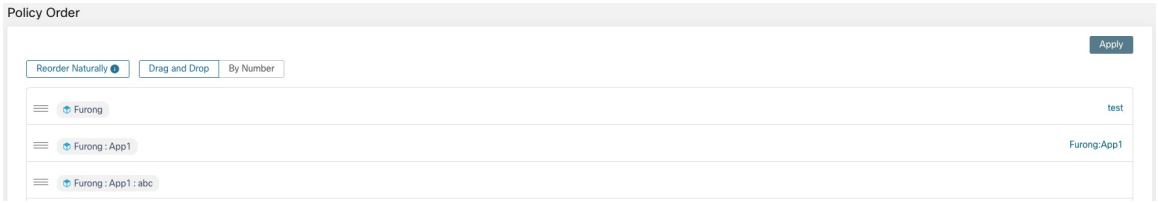
进入“策略顺序”(Policy Order) 页面后，您可以根据当前策略优先级查看所有范围及其对应的主工作空间的列表。

步骤 2 有几种方法可以对范围重新排序：

- 要对整个列表重新排序以将父范围置于子范围之上（“预购”）：点击**自然重新排序 (Reorder Naturally)**。这是建议的顺序，任何偏差都应谨慎行事。
- 要手动重新排序列表，请执行以下操作：
  - 上下拖动行。

- 点击**按编号 (By Number)**，为要用于排序的每个范围设置一个编号。这对大型列表来说可能更容易。

图 *39*: 设置范围的策略优先级



下一步做什么

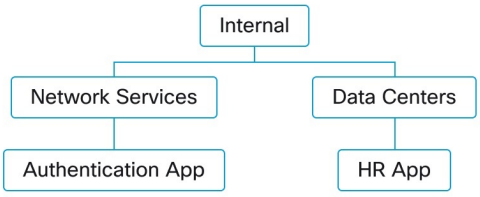
运行快速分析以查看更改的结果。

当使用者和提供者处于不同范围时：策略选项

示例场景

以下情况是显示跨范围流量的示例：

您的范围层次结构包括一个包含身份验证应用（提供者）的网络服务范围。作为范围层次结构不同分支上范围成员的 HR 应用是身份验证应用提供的服务的使用者。



策略选项

Cisco Secure Workload 提供多种方法来解决这种情况：

选项	说明	优缺点
在将使用者和提供者都列为子范围或后代的父范围或祖先范围中创建这些策略	• 在共同祖先范围内手动创建一个或多个策略。 （可选）要获得更精确的策略，请使用资产过滤器对工作负载进行分组。有关示例和说明，请参阅创建资产过滤器。 • 自动发现范围树整个分支的共同祖先范围内的策略。	这些方法是解决跨范围策略的最简单方法。 这些方法仅要求每个使用者-提供者对有一个策略。 如果您正在考虑使用自动策略发现，请参阅发现一个范围或范围树分支的策略, on page 23中的重要注意事项。
使用高级方法创建跨范围策略	自动发现每个范围的策略。 请参阅（高级）创建跨范围策略, on page 89。 （此程序适用于手动创建的策略以及发现的策略。）	此方法要求每个使用者-提供者对使用两个策略：使用者策略和提供者策略。 此方法允许在使用者和提供者策略由不同的人拥有时创建策略。 请参阅发现一个范围或范围树分支的策略, on page 23中的其他考虑事项。

（高级）创建跨范围策略

此程序介绍创建跨范围策略（使用者和提供者位于不同范围内的策略）的高级方法。它适用于手动创建的策略和自动发现的策略。

此方法要求每个使用者-提供者对使用两个策略，因为通信的两端都必须允许进行通信：

- 使用者范围内的策略必须允许与提供者的对话，

  且

- 提供者范围内的策略必须允许与使用者进行对话。

此程序包括每个范围的所有者为创建跨范围策略而必须执行的步骤。如果您的访问权限允许修改两个范围，那么您就可以执行所有步骤。

开始之前

- 请考虑使用更简单的选项来处理跨范围流量。请参阅当使用者和提供者处于不同范围时：策略选项，第 88 页。
- 必须在使用者和提供者的主工作空间中创建使用此方法的策略。

  如果要在策略中指定的提供者范围还没有主工作空间，请先创建主工作空间，然后再使用此方法创建跨范围策略。
- 策略必须具有 ALLOW 操作，才能创建策略请求。
- 有关与这些要求相关的一些其他详细信息，请参阅策略请求，第 90 页。

- （可选）考虑自动处理跨范围策略请求的选项。请参阅自动处理跨范围策略请求，第 95 页。
- （可选）如果希望跨范围策略仅应用于使用者或提供者范围内的集群中的工作负载，而不是整个范围，请参阅将集群转换为资产过滤器，第 76 页。集群不能用于使用此程序创建的跨范围策略。

  如果要自动发现策略，另请参阅外部依赖关系，第 31 页和微调工作空间的外部依赖关系，第 33 页。

过程

步骤 1 在使用者的主工作空间中，通过手动方式或使用自动策略发现功能创建所需的策略。

对于创建的每个跨范围策略，将自动为提供者创建一个策略请求。

要查看策略请求，请参阅查看、接受和拒绝策略请求，第 91 页。

注意：如果提供者应用工作空间中的现有策略与此流量匹配，则不需要新策略，也不会创建请求。此情况如已解决的策略请求数，第 99 页中所述。

步骤 2 您（或提供者应用的所有者）必须响应每个策略请求：

请参阅查看、接受和拒绝策略请求，第 91 页。

接受策略请求会自动在提供者的主工作空间中创建所需的策略，从而允许两个应用之间的流量。

如果您不想允许来自请求应用的流量，请拒绝该请求。

步骤 3 （可选）如果要自动发现策略，则可能需要微调工作空间的外部依赖关系，第 33 页。

步骤 4 查看并分析两个主工作空间。

下一步做什么

在准备好执行这些策略时，您必须执行两个主工作空间。

策略请求

当您使用（高级）创建跨范围策略, on page 89中所述的方法创建跨范围策略时，会生成策略请求。当提供者是不同范围的成员时，每次在使用者范围的主工作空间中创建策略时，如果与提供者范围关联的主工作空间中还不存在该策略，就会生成一个策略请求。

此策略请求会提醒提供者应用的所有者，允许相关应用访问必要的服务。

请参阅查看、接受和拒绝策略请求, on page 91和自动处理跨范围策略请求, on page 95中用于查看和响应策略请求的选项。

有关策略请求的其他详细信息

- 提供的服务页面（策略请求显示在该页面上）只适用于主工作空间。这是为了确保辅助工作空间上的独立试验不会在其他主工作空间上创建通知。

- 如果外部范围（当策略中指定的提供者与使用者属于不同的范围时）没有主工作空间，则不会发送请求（例如，根范围或定义的任何范围都可能属于这种情况）适用于组织外部的工作负载）。如果外部范围没有发布任何策略，则策略分析和执行仅在使用者端进行。
- 当提供者与使用者处于不同范围时，不支持集群。如果策略的使用者是一个集群，则策略请求将按照使用者应用范围内的策略请求进行处理。使用来自提供者的相同服务的多个策略可以组合在一起。
- 仅为提供者生成策略请求，而不为使用者生成。如果使用者工作空间正在分析或执行策略，则它必须通过自动策略发现或通过显式手动制定策略（不会向其生成来自外部提供者工作空间的策略请求）来明确包含允许其所有合法消费流的策略。

查看、接受和拒绝策略请求

在使用（高级）创建跨范围策略, on page 89中所述的方法创建跨范围策略时，除了使用者范围内的策略之外，还需要提供者范围内的主工作空间中的策略。在使用者范围的主工作空间中创建跨范围策略时，系统会在提供者范围的主工作空间中自动创建策略请求。

使用本主题中的信息接受请求（在提供者范围内创建所需的策略）或拒绝请求（在这种情况下，跨范围策略将不会生效）。

要查看、接受或拒绝策略请求，请执行以下操作：

要想	相应操作
查看所有策略请求	**1.** 依次选择**防御 (Defend) > 分段 (Segmentation)**。 **2.** 点击页面顶部的**策略请求 (Policy Requests)**。 **3.** 点击使用者范围可查看来自该范围的策略请求。

要想	相应操作
查看特定范围的策略请求	要查看提供者范围的待处理策略请求，请执行以下操作： **1.** 依次选择**防御 (Defend) > 分段 (Segmentation)**。 **2.** 点击适用范围的主工作空间。 **3.** 点击**管理策略 (Manage Policies)**。 **4.** 点击**提供的服务 (Provided Services)**。 如果选项卡未显示数字，则表示此工作空间没有待处理的策略请求。 **5.** 点击**策略请求 (Policy Requests)**。 **6.** 点击使用者范围可查看来自该范围的策略请求。 或 要从使用者范围查看策略请求，请执行以下操作： 在使用者范围的主工作空间的策略选项卡中，点击**协议和端口 (Protocols and Ports)** 列中的值，然后查看页面右侧打开的面板。在**协议和端口 (Protocols and Ports)** 部分中，点击黄点以查看待处理的策略请求。
手动接受请求并在提供者范围内自动创建所需的策略	从上述任一位置，点击策略请求旁边的**接受 (Accept)**。
手动拒绝请求	从上述任一位置，点击策略请求旁边的**拒绝 (Reject)**。

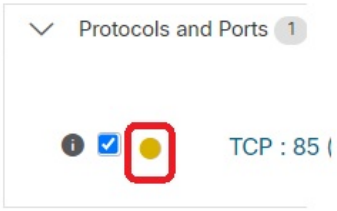
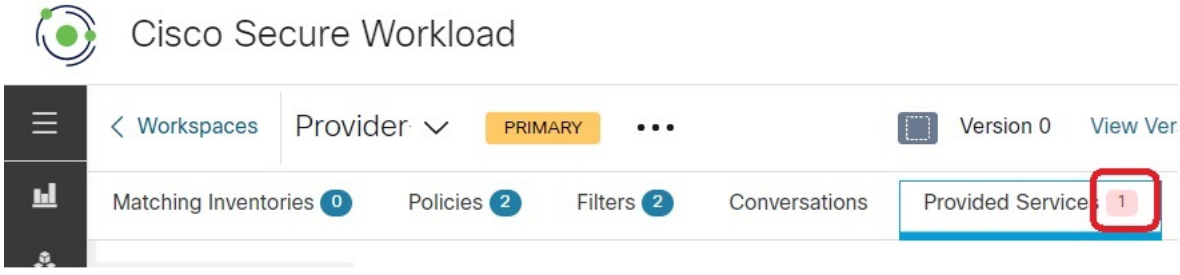
要想	相应操作
从使用者工作空间查看策略请求状态	在主要使用者工作空间的策略页面上，点击策略，然后点击端口/协议值。状态将显示在右侧打开的面板中。  待处理请求用黄点显示： 当请求被接受时，圆点会变为绿色复选标记：  点击指示器以查看详细信息。
从提供者的工作空间查看策略请求状态	在上述**提供的服务 (Provided Services)** 选项卡中查看请求状态。
允许策略发现为提供者创建所需的策略	使用可确保看到相应流的时间范围自动发现提供者范围的主工作空间中的策略，然后发布策略。
另请参阅用于自动处理策略请求的选项	自动处理跨范围策略请求, on page 95

Figure 40: 提供者工作空间中的待处理策略请求



接受策略请求：详细信息

接受服务的策略请求相当于创建一个策略，从作为使用者的请求过滤器到作为提供者的服务。此外，在接受策略请求后，使用者应用工作空间（在本示例中为前端应用和服务层）的原始策略将被标记为已接受（请参见下图）

Figure 41: 接受/拒绝策略请求

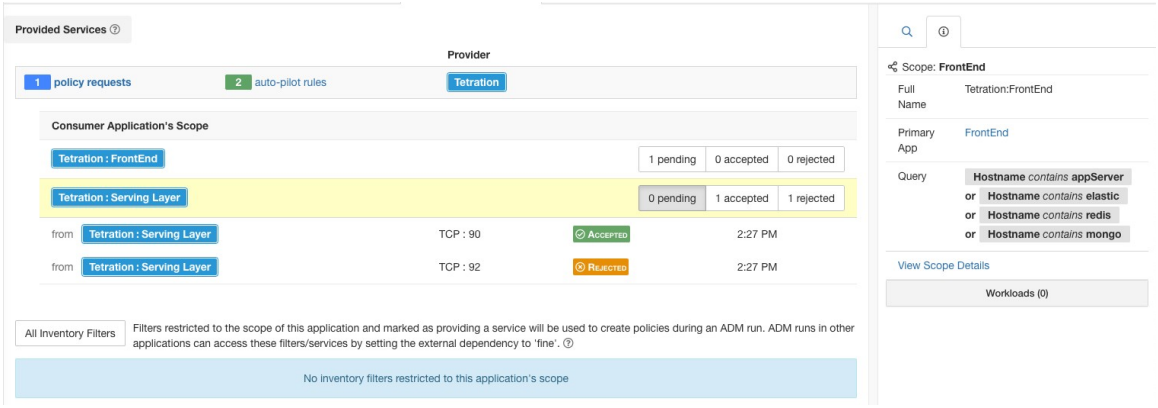
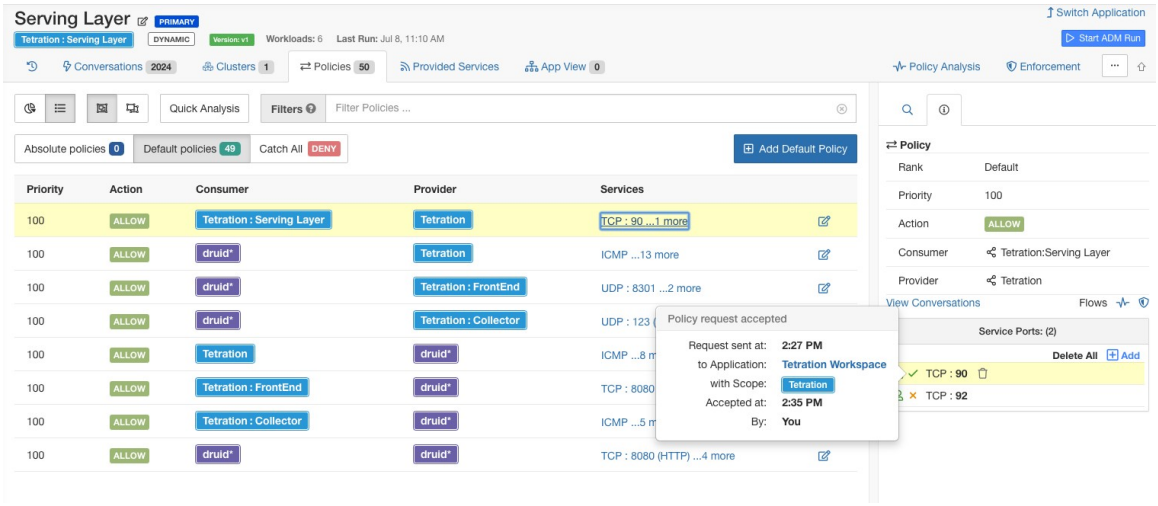


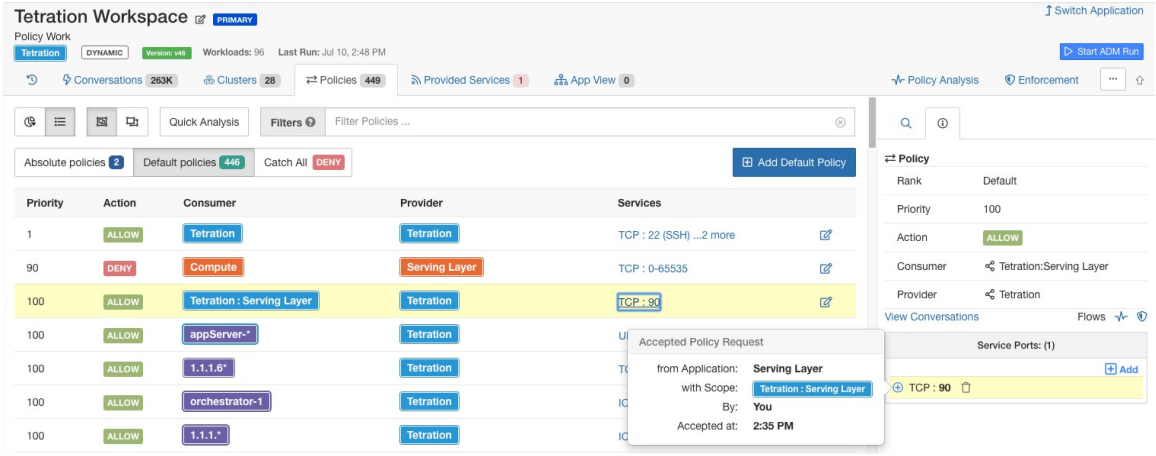
Figure 42: 策略状态显示为“已接受”***(Accepted)***



在提供者应用的工作空间（在本例中，工作空间名为 Tetration）上创建的新策略会标有**加号**图标，表示此策略是应外部策略请求创建的。

Note 如果在接受策略请求后删除使用者端的原始策略，则不会删除提供者端的策略。但是，策略旁边的工具提示会将原始策略显示为已删除，并带有事件时间戳：

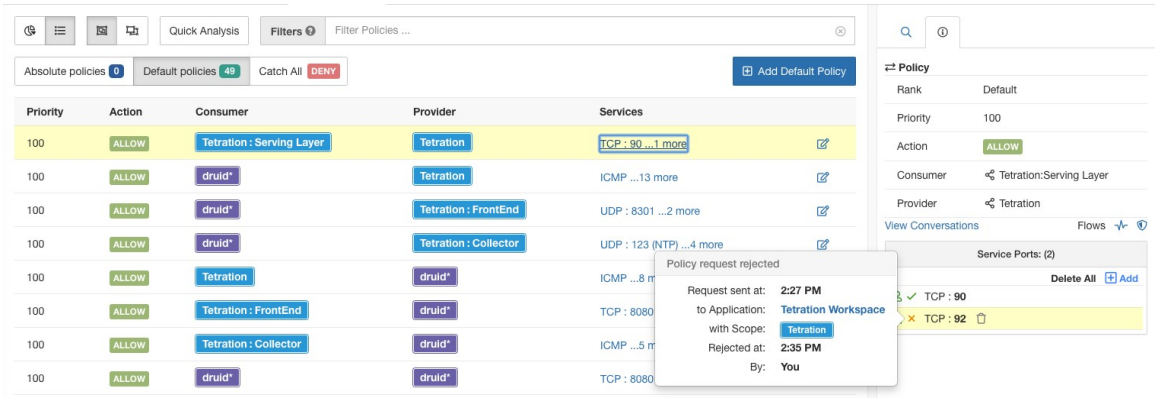
Figure 43: 提供者端策略，通过接受策略请求创建



拒绝策略请求：详细信息

拒绝策略请求不会创建或更新任何策略。使用者应用工作空间中的原始策略（在本示例中为服务层应用）将被标记为已拒绝，但策略保持有效，即仍将允许出站流量。拒绝策略旁边的工具提示包含有关提供者应用、拒绝策略请求的用户以及拒绝时间的信息。

Figure 44: 策略状态显示为“已拒绝”***(Rejected)***



自动处理跨范围策略请求

当您使用（高级）创建跨范围策略，第 89 页中所述的方法创建跨范围策略时，会生成策略请求。

有多个选项可以减少创建跨范围策略时生成的策略请求数量：

表 *5:* 用于自动处理策略请求的选项

要想	相应操作
指定如何处理特定使用者-提供者对之间的策略请求	请参阅自动引导规则，第 96 页。 您必须拥有所需的权限。

要想	相应操作
为特定工作空间中策略发现期间创建的所有跨范围策略自动创建提供者所需的所有策略	在启动自动策略发现运行时，请在“高级配置”(Advanced Configurations) 部分启用**自动接受传出策略连接器 (Auto accept outgoing policy connectors)** 选项。 此选项仅适用于根范围所有者和站点管理员。 有关详细信息，请参阅： 自动策略发现的高级配置，第 35 页，以及 自动接受策略连接器，第 98 页
指定对来自所有工作空间的所有策略请求的默认处理	在“默认策略发现配置”(Default Policy Discovery Config) 页面上，启用“高级配置”(Advanced Configurations) 部分中的**自动接受传出策略连接器 (Auto accept outgoing policy connectors)** 选项。 此选项仅适用于根范围所有者和站点管理员。 有关详细信息，请参阅： 默认策略发现配置，第 45 页，以及 自动策略发现的高级配置，第 35 页，以及 自动接受策略连接器，第 98 页

自动引导规则

仅当使用（高级）创建跨范围策略, on page 89中所述的方法创建跨范围策略时，此功能才适用。

为数据中心中许多其他应用提供服务的基础设施应用可能会收到来自其他应用的大量策略请求。

您可以通过创建自动引导规则来自动接受或拒绝未来的匹配策略请求，从而减少策略请求的数量。

Note 自动引导规则不适用于现有策略请求。它们只会影响未来的策略请求。

使用自动引导规则自动接受或拒绝策略请求

配置自动引导规则，以便自动接受或拒绝指定端口上指定使用者-提供者对之间的策略请求。自动引导规则既可以很广泛（范围到范围），也可以仅应用于每个范围内的一部分工作负载（由资产过滤器配置。您可以对使用者、提供者或两者使用资产过滤器。）

1. 如果希望将自动引导规则应用于某个范围内的一部分工作负载，而不是整个范围，请执行以下操作：

   在相关范围中创建资产过滤器，以便对工作负载进行分组。请确保在每个资产过滤器中选择**将查询限制为所有权范围 (Restrict Query to Ownership Scope)** 选项，以确保过滤器仅包括属于该范围成员的工作负载。

2. 依次选择**防御 (Defend) > 分段 (Segmentation)**。

3. 点击要为其自动接受或拒绝与特定提供者相关的策略请求的使用者范围的主工作空间。
4. 点击**管理策略 (Manage Policies)**。
5. 点击**提供的服务 (Provided Services)**。
6. 如果要为资产过滤器创建此规则，请对所需资产过滤器执行以下步骤（资产过滤器用橙色图标标识。）

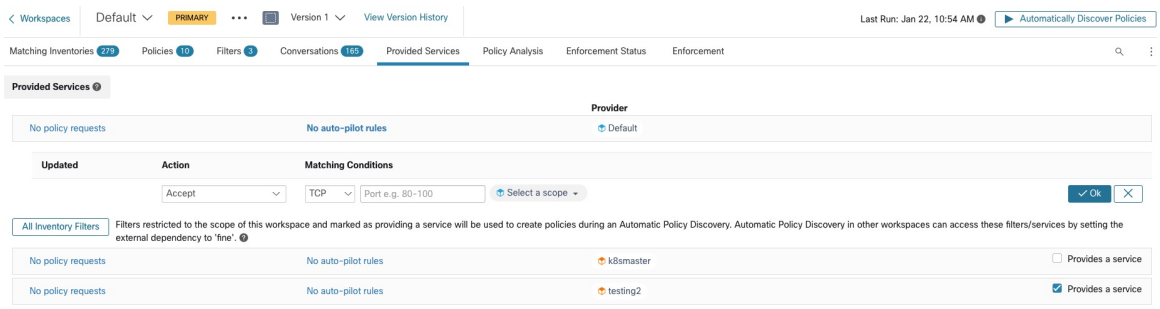
   否则，请对范围执行这些步骤（范围会以蓝色图标标识。）

   确保点击了正确的位置。
7. 点击**无自动引导规则 (No Auto-Pilot Rules)** 或**自动引导规则 (auto-pilot rules)**（以显示的为准）。
8. 点击**新建自动引导规则 (New Auto-Pilot Rule)**。
9. 配置自动引导规则。选择代表提供者的范围或资产过滤器。
10. 点击**确定 (OK)**。

自动引导规则示例

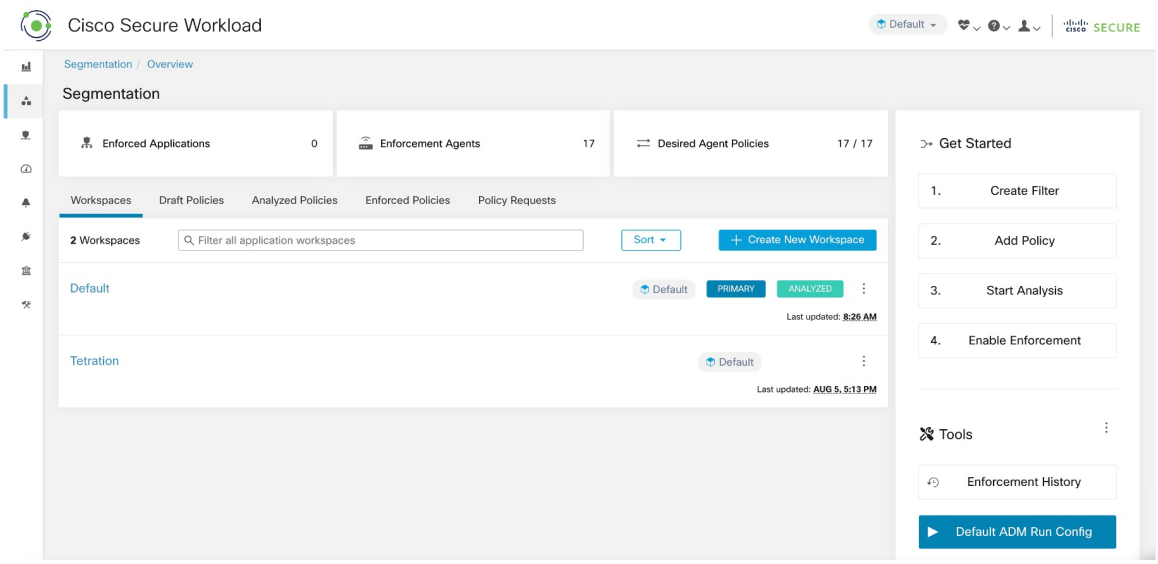
在下面的示例中，我们创建了一个新的自动引导规则，以拒绝从 Tetration:Adhoc 中包含的任何使用者到提供者服务 Tetration 的 TCP 策略请求（端口范围为 1-200）

Figure 45: 创建/更新自动引导规则



然后，在工作空间中为 TCP 端口 23 上的 *FrontEnd App* 创建新策略。由于策略与自动引导规则匹配，因此它将被自动拒绝。策略拒绝的状态和原因在被拒绝策略旁边的工具提示中指明。

Figure 46: 策略自动被自动引导规则拒绝



查看自动引导规则最近创建的策略计数

要按自动引导规则查看自上次为工作空间启动（或重启）实时策略分析以来在工作空间中创建的策略数，请执行以下操作：

导航至相关主工作空间的“已提供服务”(Provided Services) 页面，查找“已自动创建”(Auto Created) 策略的计数。

自动接受策略连接器

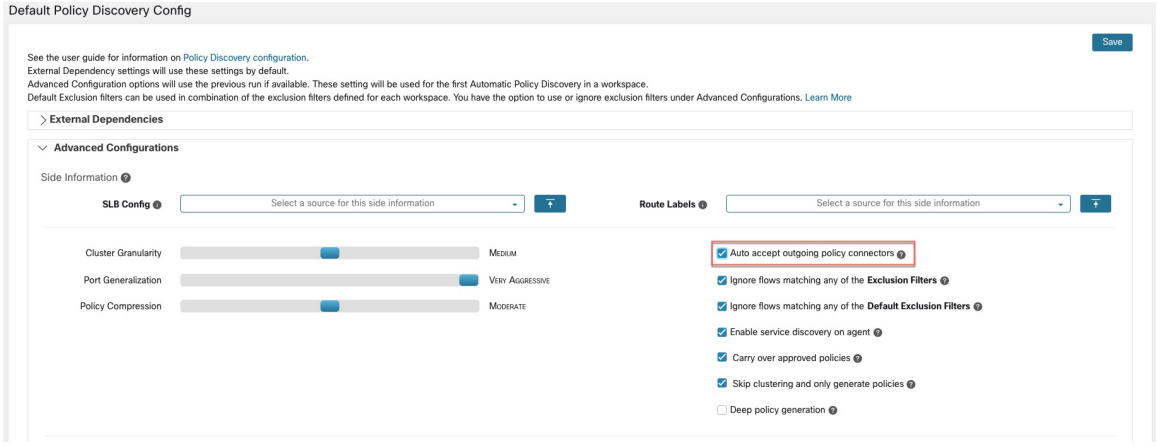
您可以将此选项设置为默认策略发现配置，也可以在每个工作空间的自动策略发现高级选项中进行设置。

通过自动策略发现配置页面上的**自动接受传出策略连接器 (Auto accept outgoing policy connectors)** 选项，您可以自动接受在自动策略发现过程中创建的任何策略请求。

如果在默认自动策略发现配置中启用了此选项，则手动或通过导入工作空间创建的策略请求也将被自动接受。

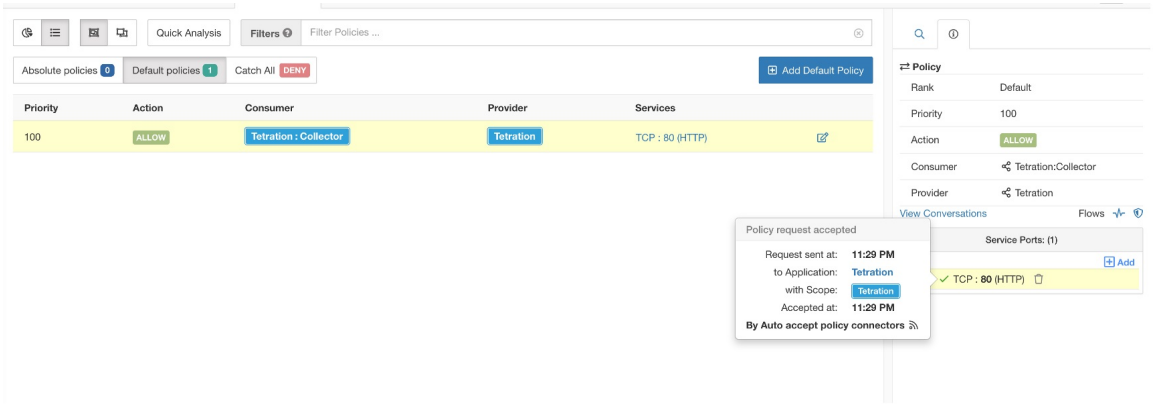
Note 此选项仅适用于根范围所有者或站点管理员。

Figure 47: 自动接受传出策略连接器选项



设置此选项后，在根范围或 适用工作空间中的任何工作空间中创建的任何策略请求都将被自动接受。

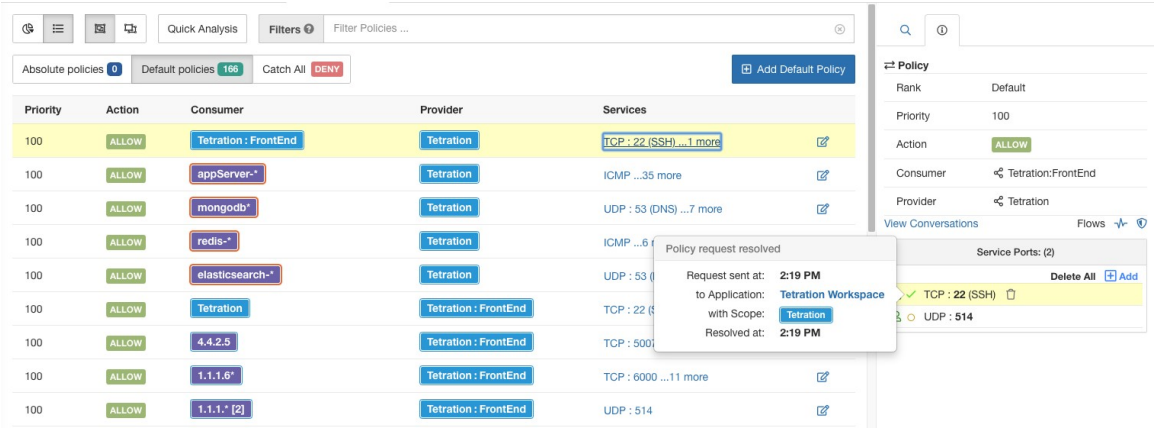
Figure 48: 自动接受策略连接器自动接受策略



已解决的策略请求数

如果创建策略请求的所有条件均已满足，但提供者应用的工作空间中已存在匹配的策略，则在使用者应用的工作空间中创建的策略将被标记为已解析，表示提供者应用的工作空间已允许流量通过请求的端口。

Figure 49: 策略状态显示为“已解决”*(Resolved)*



提供的服务

此页面仅用于创建使用者和提供者位于不同范围内的策略，并且仅限您使用（高级）创建跨范围策略, on page 89中所述的方法时使用。

有关此页面上的选项的详细信息，请参阅：

- 策略请求, on page 90
- 自动引导规则, on page 96
- 创建资产过滤器和外部依赖关系, on page 31（有关**提供服务 (Provides a service)** 选项的信息）

要访问此页面，请导航至主工作空间，然后点击**管理策略 (Manage Policies)**和**提供的服务 (Provided Services)**。

跨范围策略故障排除

如果使用（高级）创建跨范围策略，第 89 页中所述的方法来创建跨范围策略，则使用者和提供者工作负载的主工作空间必须各自具有允许流量的策略。确保两个工作范围都存在所需的策略。

如果其中一个策略被删除或修改，则不会发出通知。

如果策略对是在策略发现过程中生成的，请参阅有关批准策略以保护其免受后续发现运行影响的信息。请参阅审批策略，第 47 页。

验证是否仍满足（高级）创建跨范围策略，第 89 页中所列的其他要求。

使用者和提供者工作空间都必须执行所需的策略。

用于跨范围策略的有用工具

- 使用**外部？(External?)** 过滤器选项来查找提供者与您发现策略的范围不同的策略。
- 策略可视化视图有一个显示外部策略的选项。请参阅策略可视化表示，第 107 页。

如果您使用的是默认策略发现配置

确保在进行更改后点击**默认策略发现配置 (Default Policy Discovery Config)** 页面上的**保存 (Save)**，以使默认外部依赖关系配置可用于各个工作空间。

有效使用者或有效提供者

策略中指定的使用者和提供者可确定：

- 具有接收策略的 Cisco Secure Workload 代理的工作负载集。
- 受已安装的防火墙规则影响的 IP 地址集。

默认情况下，它们是相同的。

但是，您可能需要在防火墙规则中指定一组 IP 地址，该组 IP 地址与接收策略的工作负载的 IP 地址不同。（请参阅下面的示例。）

要满足此需求，您可以配置有效使用者和/或有效提供者。

使用者和提供者的默认行为

默认情况下，当 Cisco Secure Workload 代理收到策略时，防火墙规则将特定于该工作负载。下面的例子最能说明这一点：

请考虑使用指定 1.1.1.0/24 子网的提供者过滤器的 ALLOW 策略。在 IP 地址为 1.1.1.2 的工作负载上设置该策略时，防火墙规则如下：

- 对于传入流量，防火墙规则允许专门指向 1.1.1.2 的流量，而不允许指向整个子网 1.1.1.0/24 的流量。
- 对于传出流量，防火墙规则允许专门来自 1.1.1.2 的流量，而不是来自整个子网 1.1.1.0/24 的流量（以防止欺骗）。

因此，对属于工作空间的任何代理工作负载，如果其 IP 地址不在 1.1.1.0/24 子网内，则不会收到上述防火墙规则。

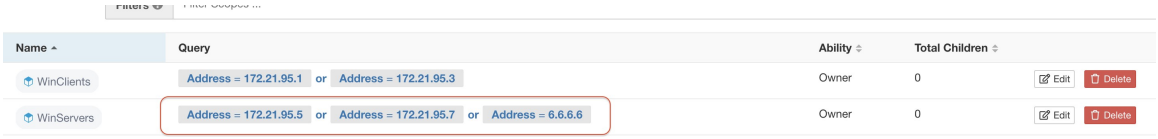
示例：有效使用者或有效提供者

在此示例中，假设您正在为虚拟 IP (VIP) 后面的工作负载群配置策略，类似于 keepalive 或 windows 故障转移集群解决方案。您将使用有效使用者和/或有效提供者来确保流量在确保您的策略能解决不常见或不经常发生的活动和情况，如故障转移、从备份恢故障转移事件期间不会中断。

考虑具有 IP 地址（*172.21.95.5* 和 *172.21.95.7*）的一组工作负载，它们提供位于 VIP *6.6.6.6* 后面的服务。此 VIP 是一个浮动 VIP，在任何时候都只有一个工作负载拥有该 VIP。目标是在集群的所有工作负载上设置防火墙规则，以允许流量通过 *6.6.6.6*。

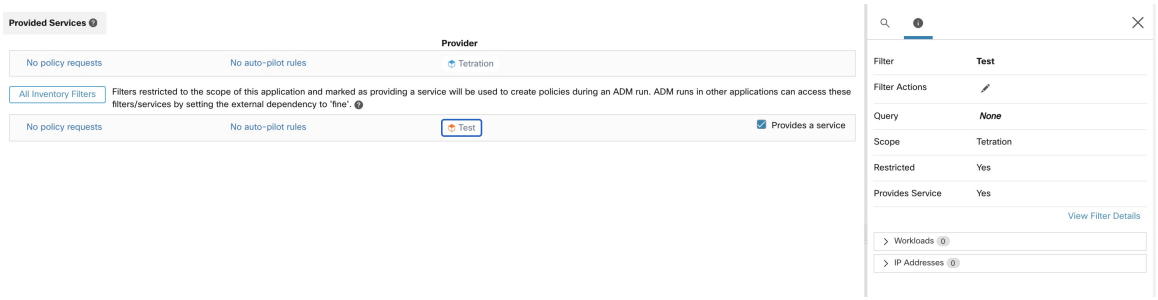
在此设置中，我们有一个范围和一个相应的工作空间，其中包含代表队列（*172.21.95.5* 和 *172.21.95.7*）以及 VIP（*6.6.6.6*）的工作负载集群。

Figure 50: 范围包括 ***VIP*** 和工作负载集群



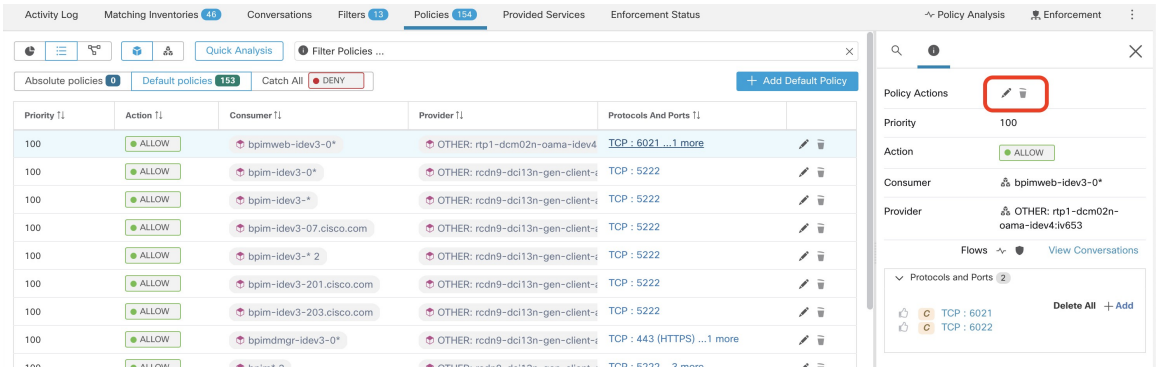
VIP 作为提供的服务显示在此工作空间中，如下所示：

Figure 51: VIP 显示为提供的服务



如果我们要将该服务客户端的策略添加到服务 VIP，那么（默认情况下）只会在拥有 VIP 的工作负载上对允许向 VIP 传输流量的防火墙规则进行编程。但是，在发生确保您的策略能解决不常见或不经常发生的活动和情况，如故障转移、从备份恢故障转移事件时，随后拥有服务 VIP 的新工作负载可能需要一些时间才能获取正确的防火墙规则，并且流量可能会在短时间内中断。

Figure 52: 允许流量从客户端发送到服务 ***VIP*** 的策略



要解决此问题，我们会配置有效提供者（使用以下程序）。具体而言，我们将“有效提供者”设置为包括需要对允许流向服务 VIP 的流量的防火墙规则进行编程的一组工作负载，而无论这些工作负载中是否有任何工作负载拥有该 VIP。

如果设置了“有效提供者”，即可在工作负载上看到，即使工作负载不拥有 VIP，也会对允许流向 6.6.6.6 的流量的防火墙规则进行编程。当支持服务的所有工作负载都使用这些规则编程时，在故障转移事件中流量将不会中断，因为新的主工作负载（拥有 VIP）已编程了必要的防火墙规则。

Figure 53: 主机上允许向服务 ***VIP*** 传输流量的防火墙规则

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

如何配置有效使用者或有效提供者

1. 点击策略进行编辑。
2. 点击策略右上角的编辑按钮以转到高级策略选项。
3. 点击**有效使用者 (Effective Consumer)** 或**有效提供者 (Effective Provider)**。
4. 指定所需的地址。
5. 您可能需要同时指定有效的使用者和提供者地址。

关于删除策略

重要事项 在删除策略前，请检查确定它不是使用者和提供者处于不同范围时所需的一对策略之一。

要确定这一点：点击“协议和端口”(Protocols and Ports) 列中的策略链接。在页面右侧打开的面板中，查看“协议和端口”(Protocols and Ports) 部分。通过接受跨范围策略请求创建的策略由端口和协议旁边的加号表示：

点击加号可查看跨范围策略的创建者，以及指向相应使用者策略的链接。

注释 如果在随后的策略发现运行过程中没有看到产生这些策略的流量流，那么在随后的策略发现运行之后，自动策略发现所建议的尚未批准的策略可能不会出现。要保留建议的策略，请参阅审批策略，第 47 页。

查看和分析策略

在执行策略之前，请务必确保策略能够达到预期效果（并且不会产生任何非预期效果）。

审核自动发现的策略

在您发现策略的工作空间的“策略”(Policies) 页面上查看策略发现结果。

从此处开始审核

建议您首先检查策略是否按建议顺序解决以下每个方面：

- 关键、通用端口
- 面向互联网的流量
- 不同应用之间的流量（这些流可能涉及不同范围的工作负载）
- 同一应用中的流量（这些流可能涉及同一范围内的工作负载）

用于查看策略的有用工具

- 为使这项工作更易于管理，可对策略进行过滤和排序，以便将相关策略作为一个组进行审核。
  - 点击表标题可对列进行排序，例如按使用者、提供者或端口/协议。
  - 使用策略列表顶部的过滤器查看特定子集。

    要查看可以过滤的属性列表，请点击“过滤策略”(Filter Policies) 框中的 (i) 按钮。
- 查看生成的策略的图形表示：

  点击“策略可视视图”(Policy Visual View) 按钮（  ）。

  有关详细信息，请参阅策略可视化表示, on page 107。
- 要根据端口搜索或过滤行，请点击**已取消分组 (Ungrouped)** 按钮。
- 默认情况下，策略将按使用者/提供者/操作分组。要返回此视图，请点击**已分组 (Grouped)** 按钮。
- 使用**外部？(External?)** 过滤器选项来查找提供者与您发现策略的范围不同的策略。

  使用当使用者和提供者处于不同范围时：策略选项, on page 88中所述的方法之一为此流量创建策略。
- 查看生成的策略的可信度。请参阅处理低可信度策略, on page 106。
- 查看工作负载配置文件，了解有关工作负载的详细信息。点击 IP 地址，然后点击右侧窗格中的**查看工作负载配置文件 (View Workload Profile)**。
- 要查看用于生成特定策略的流量，请点击该策略的**协议和端口 (Protocols and Ports)** 列中的值，然后在打开的侧面板中点击**查看对话 (View Conversations)**。

  有关详细信息，请参阅对话, on page 143。

  如有需要，您可以通过点击**流搜索 (Flow Search)** 来查看对话的流，进一步向下展开。

其他待办事项和检查

- 识别未知 IP 地址（例如确保您的策略能解决不常见或不经常发生的活动和情况，如故障转移、从备份恢故障转移或其他浮动 IP）并为其添加标签，以便了解它们是什么。

  您可以在“资产配置文件”(Inventory Profile) 页面上找到有用的详细信息。点击 IP 地址，然后点击右侧窗格中的**查看资产配置文件 (View Inventory Profile)**。
- 查找明显不需要或没有意义的任何内容。
- 使用资产过滤器对工作负载进行分组，以便单个策略可以处理多个工作负载。请参阅创建资产过滤器。
- 调查并根据需要联系其他网络管理员，了解对您所看到的策略的需求。
- 请参阅解决策略复杂性问题, on page 82下的主题，其中可能涉及手动和已批准的策略以及自动发现的策略。

- 通常，建议范围内的最大策略数不超过约 500 个。如果您的策略不止于此数量，请查看是否可以整合类似策略或考虑拆分范围。
- 在查看时，按原样批准您知道正确的任何策略，以便在将来的发现运行中保留它们。

处理低可信度策略

自动策略发现后，可信度评级指明策略中指定的每个服务（端口和协议）的每个已发现策略的准确性和适当性。

要识别已发现的低可信度策略，请执行以下操作：

1. 导航至适用的范围和工作空间，然后点击**管理策略 (Manage Policies)**。
2. 点击**策略 (Policies)** 选项卡。
3. 点击**取消分组的策略列表视图 (Ungrouped Policy List View)** 按钮。
4. 点击**可信度 (Confidence)** 列标题可按可信度级别对策略列表进行排序。
5. 点击**协议和端口 (Protocols and Ports)** 列中的值，在窗口右侧打开一个面板。
6. 在**协议和端口 (Protocols and Ports)** 部分中，每个 **C** 的颜色表示策略中指定的每个服务（端口和协议）的可信度。

   要解释置信水平，请将鼠标悬停在 **C** 上。
7. 在列表中查找任何服务的低可信度指示器。
8. 如果适用，请删除或编辑不需要的策略，或者添加其他策略。

要查看特定策略的可信度，请执行以下操作：

1. 在“策略”(Policies) 选项卡中，点击**协议和端口 (Protocols and Ports)** 列中该策略的值。

   系统将在窗口右侧打开“策略侧视图”(Policy Side View) 面板。
2. 在**协议和端口 (Protocols and Ports)** 部分中，每个 **C** 的颜色表示策略中指定的每个服务（端口和协议）的可信度。

   要解释置信水平，请将鼠标悬停在 **C** 上。

流方向和策略可信度

已发现策略的准确性取决于对流方向的正确识别。如果流方向识别不正确，自动策略发现结果的可信度可能会降低。有关为创建策略而分析的对话确定流方向的信息，请参阅客户端/服务器分类。

自动策略发现结果故障排除

如果自动策略发现结果不符合您的预期，请检查以下内容：

扩展所选时间范围以包含更多数据

扩展时间窗口以包含更多数据并捕获不常发生的事件。例如，如果应用使用从多个提供者应用中提取的数据生成复杂的季度报告，请确保包含包含该流量的时间范围。

避免在某些更改之前收集数据

如果范围定义已更改，或者在某个时间之前收集的数据因其他原因而无效，请确保您的时间范围不包括该时间之前的数据。

排除误导性流量

可能需要配置或修改排除过滤器。

可以配置多个位置排除过滤器，并且可以启用或禁用多个位置。检查每个位置：

- 检查为工作空间配置的排除过滤器。
- 检查在默认策略发现配置页面底部配置的默认排除过滤器。
- 检查在工作空间设置的“高级配置”(Advanced Configurations) 部分中为自动策略发现启用了哪些排除过滤器。
- 检查在“默认策略发现配置”(Default Policy Discovery Config) 页面的“高级配置”(Advanced Configurations) 部分中启用了哪些排除过滤器。
- 如果您使用的是默认排除过滤器，请确保已点击**默认策略发现配置 (Default Policy Discovery Config)** 页面上的**保存 (Save)**，以使这些配置可用于各个工作空间。

有关详细信息，请参阅排除过滤器，第 29 页和子主题。

对使用者和提供者范围不同的策略进行故障排除

请参阅跨范围策略故障排除，第 100 页。

检查已批准策略的状态

请参阅对已批准的策略进行故障排除，第 48 页。

策略可视化表示

策略可视化表示提供策略的图形视图。

要导航至策略可视化表示页面：在“策略”(Policies)页面上，点击列表图标右侧的图形图标（  ）。

策略视图元素

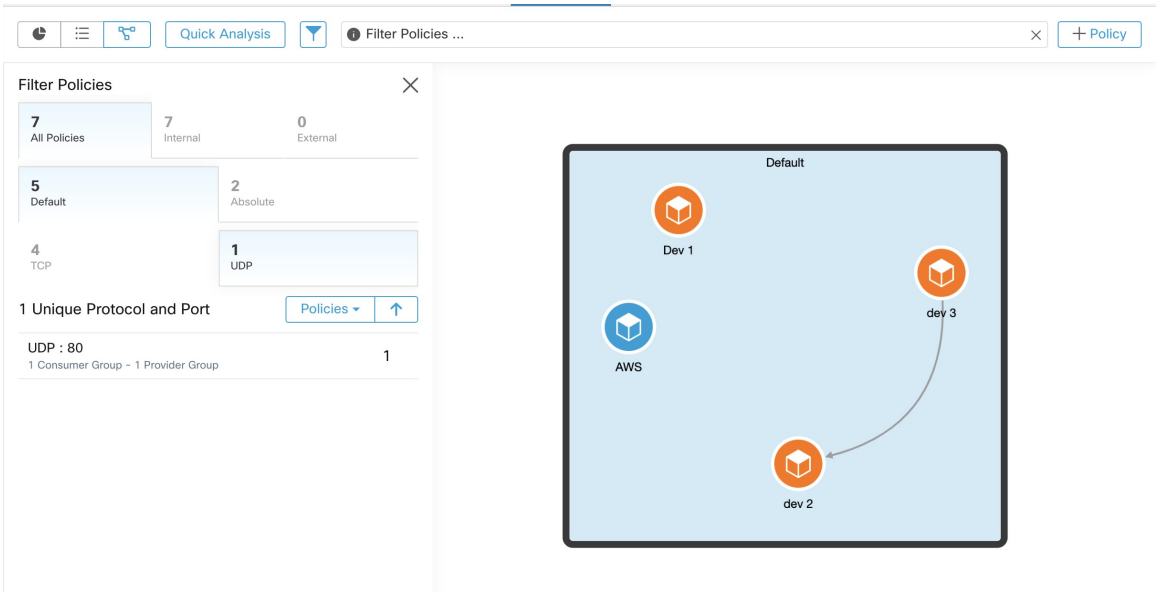
策略视图上的可视元素包括：

该元素	表示
蓝色、橙色或紫色图标	节点（策略的使用者或提供者）
蓝色图标	范围
橙色图标	资产过滤器
紫色图标	集群
连接两个图标的线条	一个或多个策略。

策略视图选项

要想	相应操作
查看使用者或提供者节点中包含的工作负载列表	双击节点的图标。
查看用户和提供商之间的服务（端口）、操作（允许/拒绝）和协议等策略详细信息	双击连接它们的线条。详细信息将显示在右侧窗格中。
查看进入和离开节点的策略	点击图标。
仅查看范围内工作负载之间的策略	点击**内部 (Internal)** 按钮。
仅查看提供者与使用者范围不同的策略	点击**外部 (External)** 按钮。
使用高级过滤选项	点击过滤器文本输入框左侧的 (i) 按钮以查看选项，然后输入过滤条件。

Figure 54: 图形视图中的过滤策略



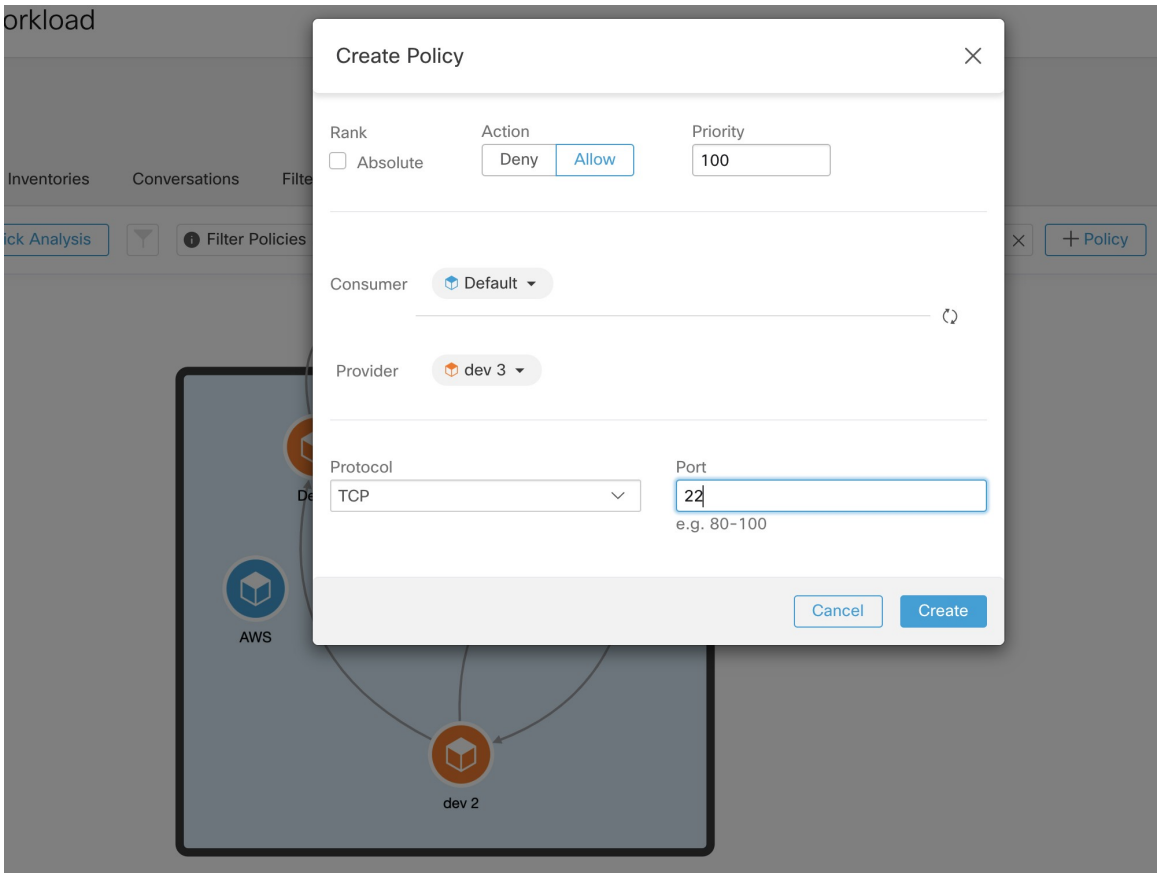
要下载策略图形视图的高分辨率映像，请执行以下操作：

1. 在图形的右下角，点击省略号图标，然后点击**导出映像 (Export Image)**。
2. 选择所需的分辨率和图像类型。
3. 点击**下载 (Download)**。

添加策略（“策略视图”(Policy View) 页面）

要创建策略，请将鼠标悬停在使用者上方，直到看到“+”号，然后按住策略并将其拖动到提供者上。要创建绝对策略，请切换模式中的“绝对”(Absolute) 复选框。否则，该策略将创建为默认策略。也可以通过点击某一行并从弹出列表中选择策略来管理策略。策略将显示在侧栏中。

Figure 55: 在图形视图中创建策略



快速分析

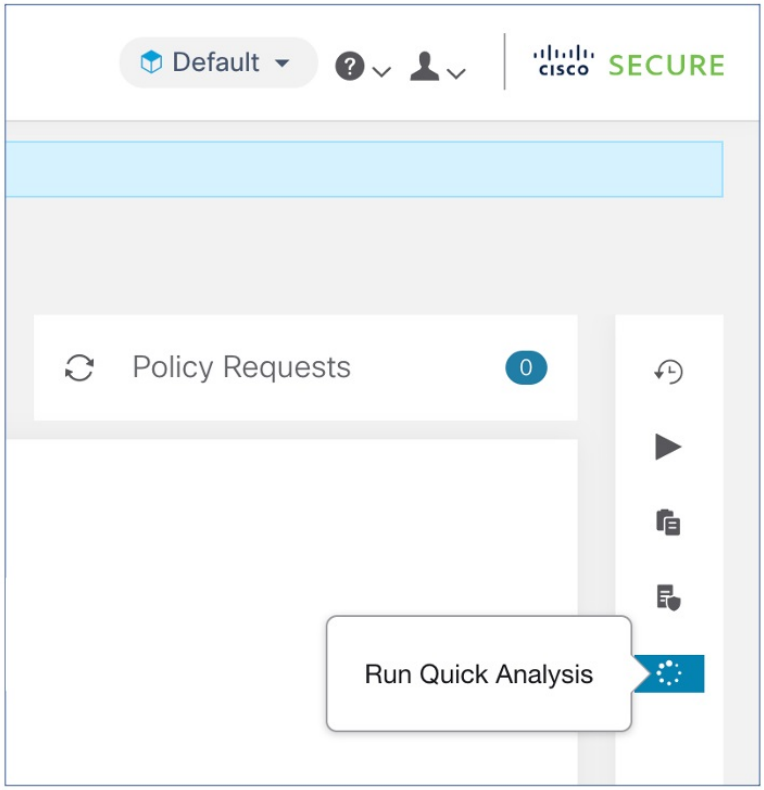
通过快速分析，可以根据当前工作空间的所有策略和其他工作空间的所有相关策略对假设流程进行测试。快速分析有助于调试和试验不同的安全策略，而无需为工作空间运行实时策略分析。

Restriction

- 只能在主工作空间上运行快速分析。
- 目前，Kubernetes 服务的流量不支持快速分析。

点击右侧导航窗格中的**运行快速分析 (Run Quick Analysis)** 选项卡以查看对话框。

Figure 56: 快速分析选项卡



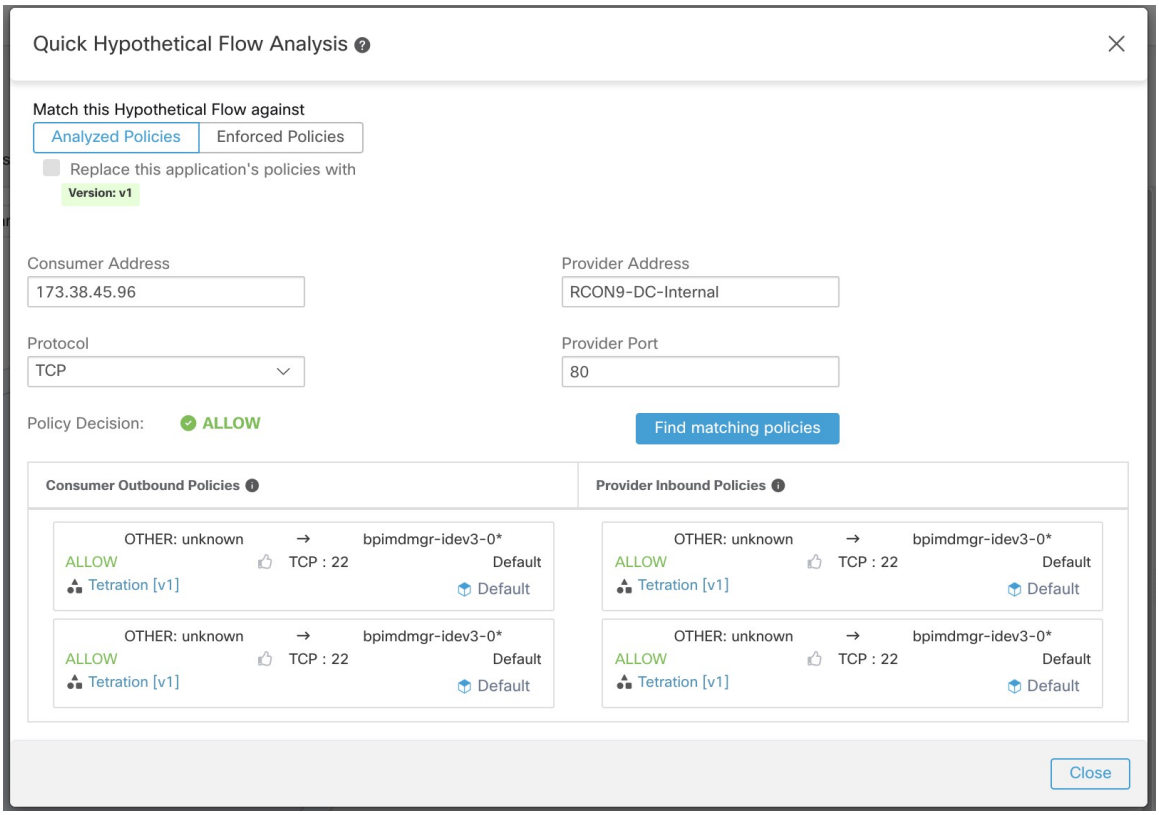
输入假设流的使用者（客户端）IP、提供者（服务器）IP、端口和协议，然后点击**查找匹配的策略 (Find Matching Policies)** 按钮。

在最新版工作空间的策略定义和已推送用于实时策略分析的相关工作空间的所有其他策略的情况下，将显示一个策略决定，说明是允许还是拒绝假设流量。

在对话框底部，我们将分别显示匹配的出站和入站策略，并按全局进行排序。只有两侧的第一行才会生效。要成功建立连接，我们需要将使用者端的排名靠前的出站规则和提供者端的排名靠前的入站规则设为 ALLOW 规则。

按顺序显示所有其他匹配的策略，提供了一个宝贵的调试工具，当某个策略似乎没有任何效果时，可帮助找出策略定义中的问题。您可以添加、更新或删除工作空间中的策略，并立即重复分析，而无需在工作空间中运行实时策略分析。

Figure 57: 快速策略分析



实时策略分析

查看并批准自动策略发现生成的网络安全策略集后，在执行策略之前，应使用实时策略分析来观察策略将如何影响网络上的实际流量。

实时策略分析可帮助您解答以下问题：

- 如果现在执行此工作空间中的策略，对此范围的应用有什么影响？
- 我们是否可以通过执行新的策略集来阻止先前已知的安全攻击/风险？

  请参阅运行策略试验，根据过去的流量测试当前策略, on page 118。
- 我们的策略是否按预期发挥作用？

您应该对任何有策略的工作空间运行策略分析。由于任何特定范围中的工作负载都可能受到其他范围中策略的影响，因此在执行该范围的策略之前，不应只针对单一范围运行策略分析。考虑分析可能影响特定范围流量的所有范围的策略。

例如：

- 在树中此范围上方的范围中定义的策略可能适用于此范围内的工作负载。

- 如果此范围中的工作负载与不同范围中的工作负载通信，则该范围中的策略可能会影响这些通信。当在此范围中开始策略分析时（或在此范围中的策略变更后分析最新策略时），这可能会影响该范围的策略分析结果。

每次修订策略时都应执行策略分析，以确保更改不会中断应用。

在工作空间上运行实时策略分析有时称为“发布”工作空间。

启动实时策略分析

在查看了自动策略发现功能在工作空间中生成的策略后，如果认为这些策略符合您的要求，就可以开始进行策略分析。

Before you begin

Important 实时分析包括也在运行实时分析的其他工作空间中的策略效果。如果您已在任何工作空间上启用执行，但分析未在该工作空间上运行，或者策略的执行版本与策略的分析版本不同，则此工作空间的实时分析结果可能不准确。

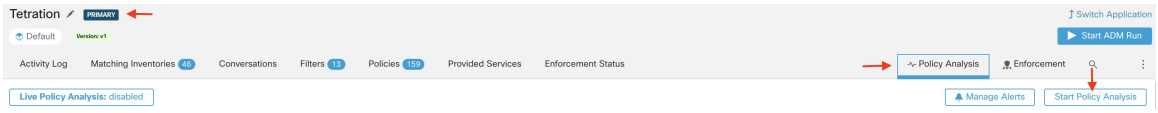
Procedure

步骤 1 点击标题中工作空间名称旁边的“辅助”(Secondary) 右侧的•••，将工作空间切换为**主 (Primary)**。

步骤 2 导航到**策略分析 (Policy Analysis)** 选项卡。

步骤 3 点击右侧的**启动策略分析 (Start Policy Analysis)**。

Figure 58: 启用策略分析



What to do next

- 由于其他范围中的策略可能适用于本范围中的工作负载，因此应考虑同时分析其他范围中可能影响本范围分析结果的策略。请参阅示例：在其他范围内分析的策略的影响, on page 114。
- 如果要在检测到转义流时收到通知，请点击**管理警报 (Manage Alerts)**。
- 使用页面上的工具来过滤数据。要查看可用的过滤条件，请点击过滤框中的 (i) 按钮。
- 如果在启动策略分析后添加或更改策略，则必须重启分析才能将更改包含在分析中。请参阅在更改策略后分析最新策略, on page 119。

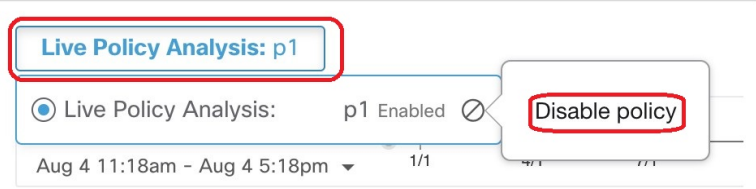
停止实时策略分析

通常，即使在执行策略后，也应让策略分析继续运行，因为此工作空间中的策略可能会影响您正在分析的其他工作空间中的策略分析结果。

要停止实时策略分析，请执行以下操作：

点击**实时策略分析：P<number> (Live Policy Analysis: P<number>)**按钮，然后点击**禁用策略 (Disable policy)**：

Figure 59: 禁用实时策略分析

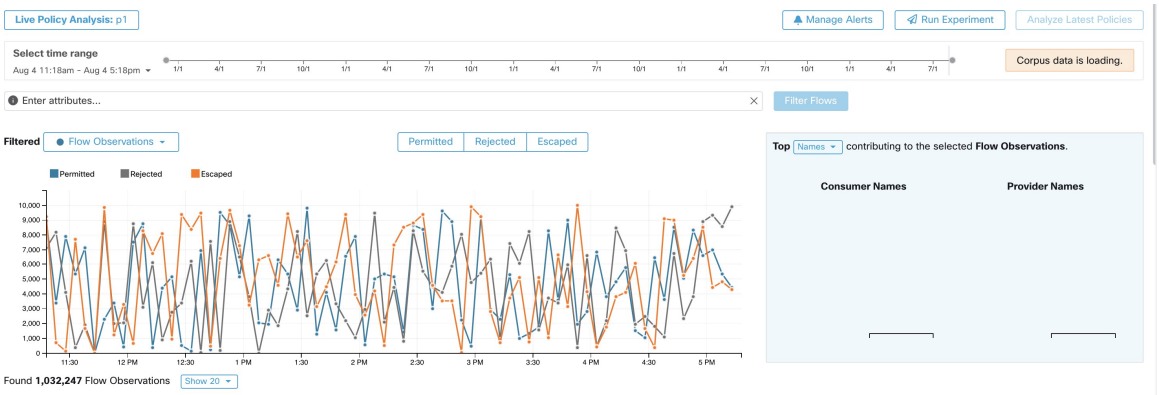


策略分析结果：了解基础知识

在策略分析期间，系统会为传入、传出与工作空间关联的范围内的所有流分配以下结果之一：

- **允许**：网络和分析的策略均允许流。
- **转义**：网络允许流，但根据分析的策略应已丢弃流。
- **拒绝**：流已被网络丢弃，也被分析的策略丢弃。

Figure 60: “策略分析” ***(Policy Analysis)*** 页面



为确定方向需要注意的一些事项：

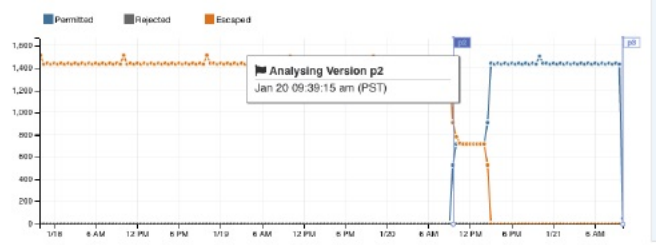
- 您可以通过分面过滤栏来过滤此页面中显示的流信息。点击**过滤器流 (Filter Flows)** 按钮会相应地更新所有图表。
- 将光标悬停在图表上会显示在该时间戳处观察到的汇聚流的百分比。
- 点击一个时间戳，就会在下面的表格中显示所有过滤流的列表，以供进一步分析。

- 您可以通过选择或取消选择时间序列图表顶部的类型，将交互限制为三种结果类型之一。
- 右侧的“前 N 个”(Top N) 图表显示对左侧时间序列图表中显示的数据有影响的排名靠前的主机名、地址、端口等。

  您可以将时序图表限制为转义流，并在“前 N 个”(Top N) 图表中选择“端口”(Ports)，以查看导致转义流的排名靠前的端口。

示例：在其他范围内分析的策略的影响

在下面的示例中，允许的流会一直持续到中午 12 点左右。当时，策略分析是在与不同范围相关联的工作空间中启动的，影响了该范围内工作负载的流量，并导致流被标记为转义。（要知道，这一变化并不是由本工作空间中新分析的策略变化引起的，因为这会产生一个标签标记。）



无策略分析

与工作空间相关的流进、流出和范围内的流可能会受到正在分析的其他工作空间策略的影响。如果此工作空间未启用实时策略分析，则流将与系统中已启用实时策略分析的其他工作空间的流一起标记。

Note 如果没有工作空间在运行实时策略分析，则时间序列图表将为空。

策略分析详细信息

流处理结果

在策略实时分析中，要确定流是 **允许 (Permitted)**、**转义 (Escaped)** 还是**拒绝 (Rejected)** 状态，我们必须首先从网络角度确定流的**处理结果 (Disposition)** 情况。根据 Cisco Secure Workload 代理给出的信号和观察结果，每个流将收到 **ALLOWED**、 **DROPPED** 或 **PENDING** 处理结果。根据流路径和流类型的代理配置，存在多种场景。

首先，无论流类型如何，如果流路径上的任何代理报告该流已被 DROPPED，则该流量将收到 DROPPED 处理结果。

当流路径上没有任何代理报告 DROP 时，我们会分别考虑双向流和单向流的情况。观察到双向流时，我们会根据流的源、目标端口和协议以及时间成对查看流（正向和反向）。但不能对单向流执行相同的操作。

对于双向流，如果在两端都安装了代理并启用了数据平面，并且源和目标代理都报告观察到该流，则正向流将收到 ALLOWED 处理结果。否则，正向流将获得 PENDING 处理结果。如果在源或目标

工作负载上安装了代理，但未在两者上安装，则当且仅当代理在**60**秒窗口内观察到后续反向流时，正向流才会收到 ALLOWED 处理结果。否则，将为转发流分配 PENDING 状态。双向数据流反向部分的处理结果也遵循同样的逻辑，只是现在的源和目的是相反的。例如，如果只有一方有代理，反向流处理结果是PENDING还是ALLOWED，取决于基于相同逻辑的后续正向流的观察和时间安排。

请注意，我们假设防火墙会实施静默丢弃。如果在同一流上发送拒绝消息（例如，拒绝具有 RST + ACK 的 TCP SYN），则会检测反向流，并将先前的转发流标记为 ALLOWED。但是，如果在其他流上发送拒绝消息（例如，拒绝包含 ICMP 消息的 TCP SYN），则转发流将保持 PENDING 状态。

对于单向流，如果任何代理将流报告为已丢弃（与双向流的情况一样），则该流将被视为已丢弃。但是，由于没有匹配的反向流量，如果两个代理都观察到流量，则该流量的处理结果状态为 PENDING。

违规类型

根据正在分析的策略检查流处理结果，以确定最终的违规类型。

流的违规类型将被

- **允许**，如果其处理结果为 ALLOWED 或 PENDING，并且其决定性策略操作为 ALLOW，
- **转义**，如果其处理结果为 ALLOWED 且决定性策略操作为 DENY，
- **拒绝**，如果其处理结果为 DROPPED 或 PENDING，并且其决定性策略操作为 DENY，

DROPPED 状态只会被分配给其相关代理明确报告其 DROPPED 状态的流。当没有明确的代理丢弃报告时，流将处于 PENDING 状态。

当处理结果为 PENDING 时：

- 且策略操作为 DENY，则违规类型设置为“拒绝”。
- 且策略操作为 ALLOW，则违规类型设置为“允许”。

对于双向流，如果流的正向和反向部分的策略违规类型一致，则策略分析或执行分析页面只显示单一类型。否则，将单独显示正向和反向，例如 PERMITTED:REJECTED。

示例场景：

- 数据包在源端执行时被丢弃。
  - 在这种情况下，源端 Cisco Secure Workload 出口代理将报告流为 DROPPED。
- 数据包离开源。
  - 如果源端只有一个代理，而出口代理在60秒内也观察到反向数据包，则该流量将被报告为 ALLOWED。
  - 如果源端和目标端都有仅可视性代理，则当且仅当入口代理报告流已丢弃时，才会为流提供 DROPPED 处理结果状态。否则，流将报告为 ALLOWED。
  - 在目标处接收流数据包，但没有反向流量。在目标收到流数据包，但没有反向流量。

    如果没有目标端代理，则流将收到 PENDING 状态。否则，系统将为其分配 ALLOWED 状态。

调查流的建议步骤

在检查策略结果时深入了解特定流时，以下建议和过滤器可能会有所帮助：

1. 首先关注转义流 *(ESCAPED FLOWS)*：

   转义流需要特别注意，因为它们的实际流处理结果不同于基于当前分析的策略的预期操作。调查确保执行这些策略不会阻止所需的流并对您的应用产生不利影响。

   点击违规类型，例如**转义**。

   （稍后，您可以根据需要查看被拒绝和允许的流。）

   发生转义流的原因有很多，包括但不限于：

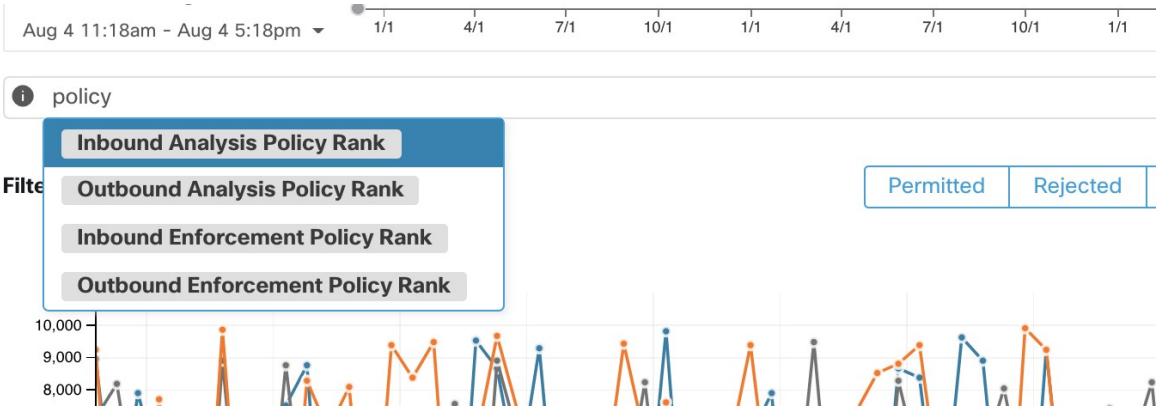
   - 另一个优先级较高的策略正在生效
   - 流量采用的路径与策略处理的路由不同，或者
   - 您期望流量命中的策略位于未分析（如果您在“策略分析”(Policy Analysis) 页面上查看转义流）或执行（如果您在“执行”(Enforcement) 页面上查看转义流）的工作空间，例如在祖先范围内，甚至在同一范围内的辅助工作空间中。

2. 识别与捕获全部策略（入站和出站）匹配的流：

   了解哪些流与捕获全部策略匹配非常重要，尤其是在允许列表策略模型中。如果这些流是合法的，但没有为其配置显式允许策略，则可能需要在相应的入站或出站范围中添加适当的显式策略。如果它们是可疑的流，则您要快速识别它们并进一步调查其详细信息。

   要关注这些流，请根据 **inbound_policy_rank** 或 **outbound_policy_rank** 的捕获全部值来应用过滤器，具体取决于您是查看入站、出站还是两端，如下所示。

   图 *61:* 用于等级的策略分析过滤选项



3. 过滤掉具有 RST 的 TCP 流： 正向标志不包含 *RST*，反向标志不包含 *RST*

   某些转义 TCP 流设置了 RST 标志。这些流由其使用者或提供者重置。它们是没有数据交换的未建立连接，但可能会报告为 ALLOWED，因为代理会看到其握手数据包。由于它们在开始时没有建立连接，因此在执行当前分析的策略时不会受到影响。过滤掉两边都有 RST 标记的 TCP

流，就能把注意力集中在更有意义和更重要的擒获流上，因为当前分析的策略会阻止这些流建立连接。

4. 如果大多数流量使用的是 IPv4，则仅关注 IPv4 流：

   使用 *address type = IPv4, address type != IPv6* 进行过滤。过滤掉 *link-local* 地址也很有帮助。

5. 通过识别转义流量中涉及的最常见主机名、端口、地址、范围等，确定下一个诊断步骤中要关注的流的优先级：

   从 TopN 功能窗格中选择主机名、端口或地址。在诊断策略时，您通常可以将这些过滤器与其他过滤器结合起来，以便深入研究特定类型的流量。

6. 搜索上一步中确定的主机名、端口、协议等流数据

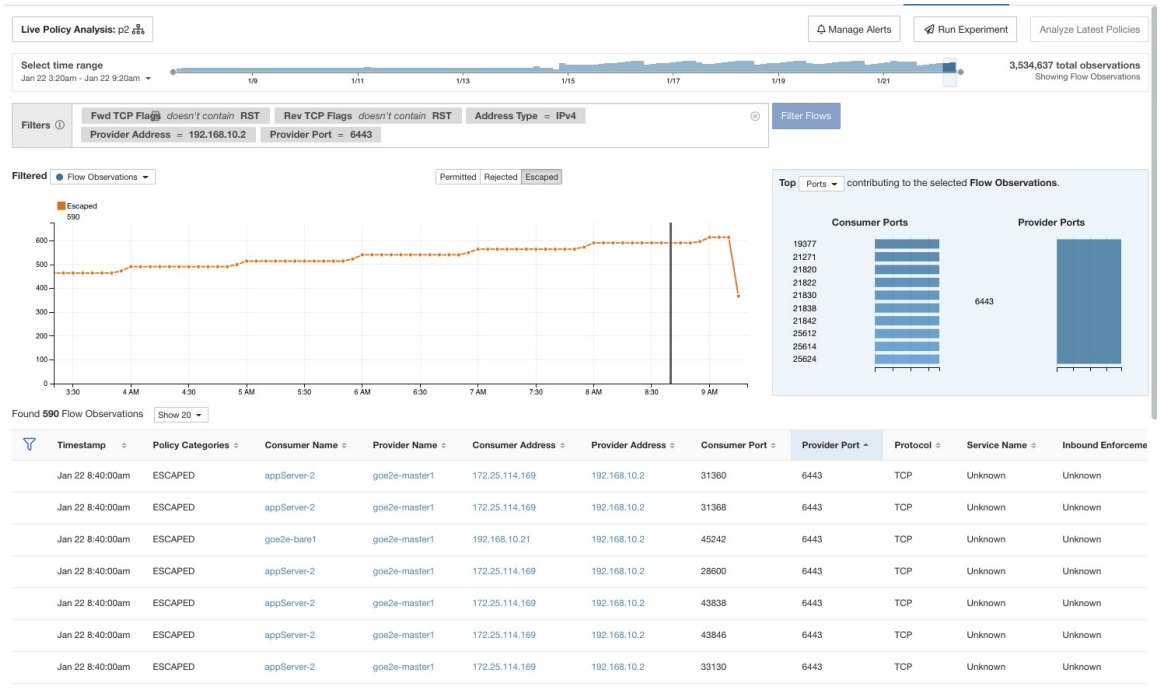
   根据目标流的主机名、端口等信息确定候选流后，您可以选择从前 N 个查询窗口中给出的值直接应用下拉过滤器，或在流搜索过滤器栏中手动输入相关过滤器，对流进行下拉过滤。例如，*Consumer Hostname contains {something}, Provider Hostname contains {something}, Provider Port = {some port number}, Protocol = TCP Protocol != ICMP*

7. 检查各个流并快速分析：

   最后，您可以通过点击与流对应的表行来关注特定流，以检查其策略结果。请注意与流匹配的策略，以及使用者和提供者地址的范围。如果策略操作与您的预期操作不匹配，则您需要在与使用者和/或提供者范围关联的工作空间中创建适当的策略，以更改策略操作。

   下图显示了使用上述部分过滤功能缩小转义流范围的工作流程示例。通过将“-”转换为范围查询，搜索输入还支持将“,”和“-”用于端口、使用者地址和提供者地址。

图 *62:* 策略分析诊断示例



运行策略试验，根据过去的流量测试当前策略

如果过去发生过已知攻击或其他重要的短期流量模式，并且您希望查看当前策略（或其他版本化策略集）如何处理该流量，则可以使用运行试验功能。

Before you begin

Tip 作为此程序的替代方法，您可以再次运行自动策略发现，包括相关的时间范围，并查看建议的不同策略。

Procedure

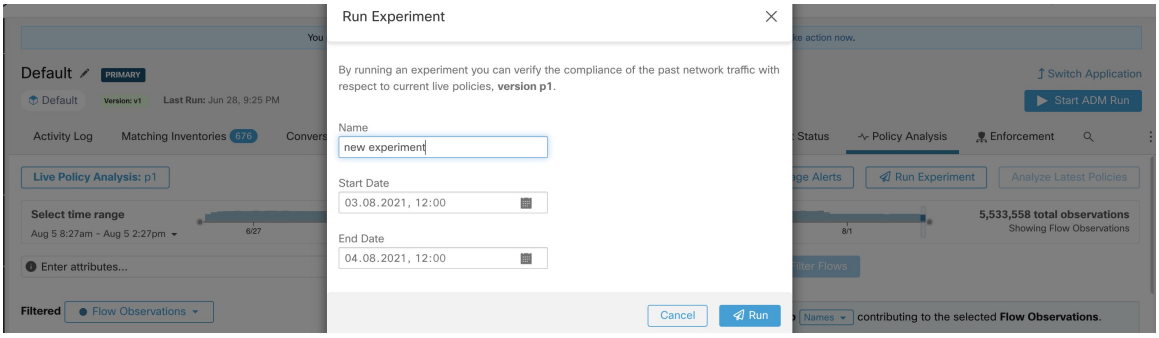
步骤 1 导航至所选工作空间的“策略分析”(Policy Analysis) 页面。

步骤 2 从页面顶部，选择要测试的策略版本。

步骤 3 点击**运行试验 (Run Experiment)**。

步骤 4 输入策略试验的名称和持续时间。

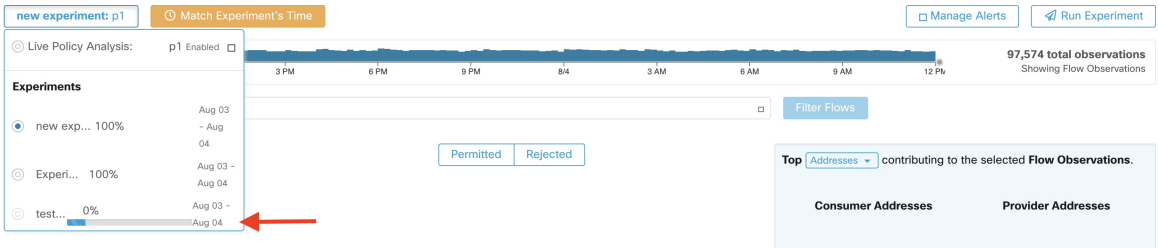
Figure 63: 运行试验表单



这将启动一项新的策略分析任务，回溯时间并根据所选版本策略重新分析所选持续时间内的所有流。

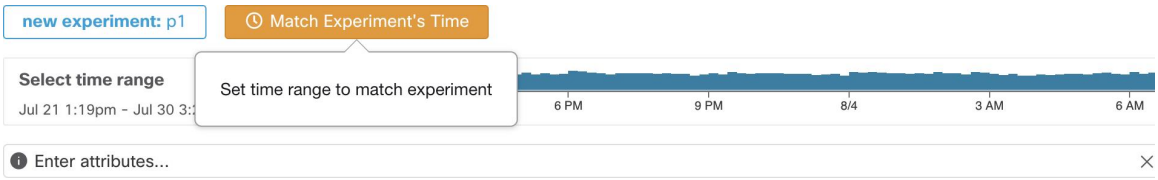
此工作可能需要几分钟，具体取决于所选的持续时间。策略选择器菜单中将显示进度。当结果准备就绪时，您应该能够像选择任何其他版本化策略一样选择策略试验，并且显示不同流类别的时间序列图表将相应更新。

Figure 64: 查看试验状态



Note 如果在选择策略试验时看不到任何流，可能是由于时间范围不匹配，例如，图表的当前时间范围是过去 1 小时，但试验持续时间是过去 6 小时。要将时间范围重置为试验的持续时间，请点击策略选择器旁边的时钟图标。

Figure 65: 匹配时间范围



在更改策略后分析最新策略

策略分析不会自动反映工作空间中的策略变化。当您准备好在进行更改后分析当前策略集时，请点击**分析最新策略 (Analyze Latest Policies)**，以便策略分析反映更改。

如果工作空间中的策略自上次启动策略分析以来未更改，或者当前未启用策略分析，则“分析最新策略”(Analyze Latest Policies) 按钮不可用。如果按钮可点击，则表示有策略更改尚未纳入到分析中。

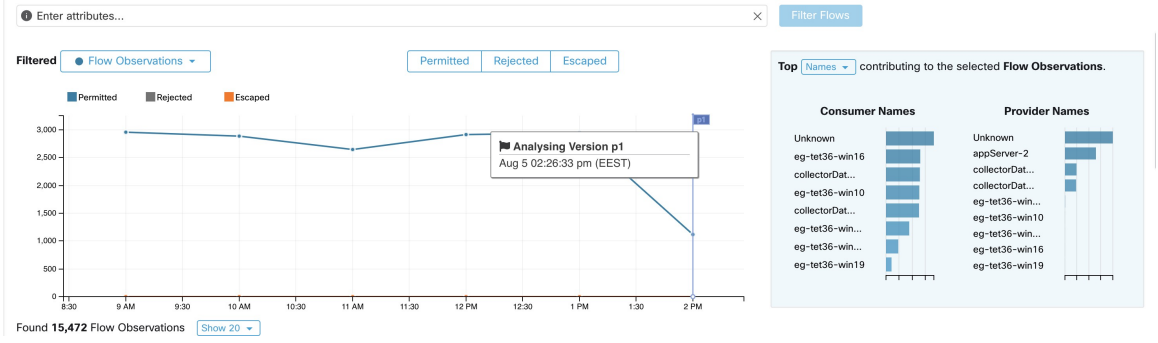
另请参阅查看、比较和管理分析的策略版本, on page 119。

策略标签标志

在策略分析时间序列图上，策略标签标志着分析开始的时间点，在每个时间点上，分析都会重新开始，以反映最新的策略和集群变化。

点击某个标志可查看与该标志关联的策略的版本：

Figure 66: 时间序列图表中的策略标签标志



点击策略标签标志可打开策略页面的相应版本，并显示该策略分析版本所分析的策略。

查看、比较和管理分析的策略版本

每次进行更改后，在工作空间中分析或重新分析策略时，都会创建一个新的分析版本 (p*)。

有关版本控制的详细信息，请参阅关于策略版本（v* 和 p*），第 137 页。

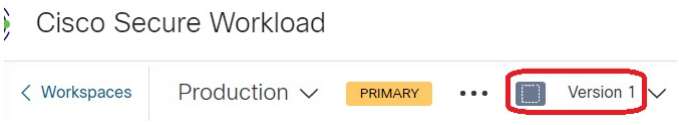
过程

步骤 1 依次点击**防御 (Defend) > 分段 (Segmentation)**。

步骤 2 导航至相关范围和主工作空间。

步骤 3 点击**管理策略 (Manage Policies)**。

步骤 4 页面顶部显示当前显示的策略版本：



显示的版本可能是策略发现版本、分析的策略版本或执行的版本。

步骤 5 您可以执行以下操作：

要显示策略的不同版本，请执行以下操作：	点击当前版本，然后选择其他版本。 有关版本的说明，请参阅关于策略版本（v* 和 p*），第 137 页。 **重要提示！**如果您选择 av* 版本，请参阅查看、比较和管理发现的策略版本，第 50 页而不是本主题，包括本主题末尾的重要警告。
要查看有关所分析版本的详细信息，请执行以下操作：	1. 点击页面顶部当前版本旁边的**查看版本历史记录 (View Version History)**。 2. 点击**发布的版本 (Published Versions)** 选项卡，查看已分析和已执行的策略的版本。 3. 要查看某个版本的日志条目，请点击版本中的链接。 浅绿色行表示分析活动。 亮绿色行表示执行活动。
要比较两个版本以查看更改内容，请执行以下操作：	1. 点击**比较修订 (Compare Revisions)**。 2. 选择要比较的版本。 您可以比较最新的草稿版本、分析版本和执行版本。 3. 有关结果详细信息，请参阅策略版本比较：策略差异，第 139 页。
要删除不需要的版本，请执行以下操作：	点击版本对应的⋮，然后选择**删除 (Delete)**。 只要不主动分析或执行已发布的策略版本（p* 版本），就可以删除该版本。

要导出版本，请执行以下操作：	点击版本对应的 ⋮，然后选择**导出... (Export...)** 。 另请参阅导出工作空间 ， 第 55 页。

下一步做什么

完成版本处理后，请在工作空间页面顶部将版本更改为最新发现的策略版本 (v*)。

这样可以避免无意中删除已发现的策略版本，还可以在工作空间中手动创建策略。

策略分析的活动日志

所有工作空间用户都可以在工作空间历史记录中查看与在策略分析页面上完成的更改相关的活动日志（请参阅活动日志和版本历史记录）。

- 启用策略分析

  Figure 67: 启用策略分析

- 禁用策略分析

  Figure 68: 禁用策略分析

- 更新策略分析

  Figure 69: 更新策略分析

执行策略

Cisco Secure Workload 可以使用以下方式执行策略：

- 在工作负载上部署软件代理 安装在单个工作负载上：
  - Linux
  - Windows 的 ISE 安全评估代理
  - Kubernetes/OpenShift

  有关代理如何在每个平台上工作的技术详细信息，请参阅使用代理的执行策略和容器上的执行, on page 129。

- 云连接器：

- AWS，通过AWS 连接器
- Azure，通过Azure 连接器

- 通过外部协调器集成负载均衡器：
  - F5 BIG-IP
  - Citrix Netscaler

- 集成Cisco Secure Firewall Management Center
- 流传输到第三方协调器以在第三方基础设施中执行

Caution 执行策略时，系统会在受影响的主机上插入新的防火墙规则，并删除相关主机上的任何现有规则。

检查代理运行状况和执行准备情况

其中一些检查可以在执行策略的前后完成。

修改代理或连接器功能可能需要权限；请参阅相关章节中的要求和前提条件。

对于不打算执行策略的任何工作负载，则无需执行这些检查。

核实：	更多信息
代理被安装在与强制工作空间关联的范围内的所有工作负载上	点击**防御 (Defend) > 分段 (Segmentation)**，然后导航至相关范围和工作空间。点击**匹配资产 (Matching Inventories)**，然后点击 **IP 地址 (IP Addresses)**。 此选项卡上的 IP 地址通常没有已安装的代理，通常必须安装代理才能执行策略。 例外情况：对“IP 地址”(IP Addresses) 选项卡上显示的以下类型的资产执行执行： • 使用云连接器执行策略的基于云的资产。（在单个工作负载上安装代理为可选。） • 如果代理安装在单个工作负载 Pod 上，则 Kubernetes 地址会出现在 IP 地址列表中；安装了代理的 Kubernetes 资产会出现在 Pod 选项卡上。
安装的代理版本为最新版本且受支持	有关已安装代理版本的概述，请点击**管理 (Manage) > 代理 (Agents)**，然后点击**分布 (Distribution)** 并查看**代理软件版本分布 (Agent Software Version Distribution)** 图表。 有关详细信息，请依次点击**管理 (Manage) > 代理 (Agents)**，然后点击**代理列表 (Agents List)**。

核实：	更多信息
已安装的代理具有执行功能	点击**管理 (Manage) > 代理 (Agents)**，然后点击**转换为执行代理 (Convert to Enforcement Agent)**。 在**过滤器 (Filter)** 框中，输入**代理类型 = 深度可视性 (Agent Type = Deep Visibility)** 转换必须执行策略的任何代理。
已为所有代理启用执行	（此要求不同于确保代理具有执行功能，也不同于在工作空间中启用执行。） **重要提示**！根据您的部署，这可能需要在执行工作空间之前或之后完成。 请参阅验证是否已为代理启用执行部分。
已为非代理执行机制启用执行	**重要信息**！！！在工作空间上执行策略之前，请勿在没有代理的云连接器上启用执行。 还必须先启用支持执行的外部协调器，然后才能执行。
代理配置文件中的**保留规则 (Preserve Rules)** 设置适用于工作负载平台	• 对于 Kubernetes/OpenShift，请参阅容器上的执行部分。 • 对于其他平台，请参阅软件代理部分中每个平台的信息。 提示：在此文档中搜索“保留规则”(Preserve Rules) 即可查找有用信息。
（执行工作空间后）所有代理均已收到工作负载的适用策略	请参阅验证已执行的策略是否被推送到代理部分。
代理运行正常	除了上述源之外，以下位置还包含有关代理运行状况的信息： • 点击**管理 (Manage) > 代理 (Agents)**，然后点击**监控 (Monitor)**。 查看**执行代理 (Enforcement Agents)**下的信息。 • 点击**管理 (Manage) > 代理 (Agents)**，然后点击**监控 (Monitor)**。 从页面顶部的菜单中选择代理类型。 • 点击**整理 (Organize) > 范围和资产 (Scopes and Inventory)**，进行过滤以查找特定的感兴趣的工作负载，然后点击 IP 地址。 系统将在单独的浏览器窗口中打开**工作负载配置文件 (Workload Profile)** 页面，其中包括“代理运行状况”(Agent Health) 面板。 有关详细信息，请参阅“工作负载配置文件”部分。

启用策略执行

Caution 执行策略会删除现有的防火墙规则，并在受此工作空间影响的范围内的每个工作负载上编写新的防火墙规则。

如果没有正确验证策略是否正常运行，执行策略可能会改变应用的工作方式，并中断业务运营。

Before you begin

- 最初，在执行策略时，请考虑将捕获全部设置为“允许”(Allow)。然后，监控流量以查看与捕获全部规则匹配的流量。当没有必要的流量与捕获全部规则匹配时，可以将捕获全部设置为“拒绝”(Deny)。
- 如果一次在多个范围中执行工作空间，则只能执行已分析的工作空间。如果使用以下程序中介绍的第二种方法执行单个工作空间，则建议但不要求在执行之前分析工作空间中的策略。

  请参阅实时策略分析以及子主题。
- 用于执行单个范围的向导比提供同时执行多个范围的选项的向导更详细。如果您需要策略执行向导, on page 127中的功能，请使用以下程序中介绍的第二种方法。
- **重要信息！**验证策略是否正确。

  任何工作空间中的策略结果都可能受到其他范围内已执行策略的影响。在工作空间上启用策略执行之前，“策略执行”(Policy Enforcement) 页面显示与其他范围关联的工作空间中执行的策略如何影响流。例如，在父范围的强制工作空间中采用宽泛的“生产主机不应与非生产主机通信”策略可能会影响属于子范围内应用的工作负载流量。

  如果“执行”(Enforcement) 图表中未显示新信息，请确保选择正确的时间范围。

  有关您在“执行”(Enforcement) 页面上看到的信息的信息，请参阅实时策略分析及其子主题。（实时分析的相同信息也适用于“策略执行”(Policy Enforcement) 页面。）

  如果实时分析结果与“执行”(Enforcement) 页面上的结果不同，请确保分析的范围、策略版本和时间范围与“执行”页面上用于生成结果的范围、策略版本和时间范围相同。
- 了解代理如何在每个平台上执行策略。请参阅：
  - 对于 Windows 和 Linux 工作负载，请参阅使用代理的执行策略及其子主题。
  - 对于 Kubernetes 和 OpenShift，请参阅

    容器上的执行, on page 129。
  - 有关负载均衡器，请参阅

    Citrix Netscaler 的策略执行，以及

    F5 BIG-IP 的策略执行。
  - 有关使用云连接器配置的基于云的工作负载，请参阅：
    - 对 AWS 资产执行分段策略时的最佳实践 和链接的主题。

- 对 Azure 资产执行分段策略时的最佳实践 和链接的主题。

- 您必须具有执行策略所需的权限：

  您必须具有范围的“执行”功能或更高级别的功能。在范围上拥有其他权限的用户仍可以查看此页面，但无法执行（或禁用）新策略。

- 验证所有已安装的相关代理和其他执行终端（例如云连接器）是否已准备好执行策略。有关代理运行状况和就绪性检查的列表，请参阅检查代理运行状况和执行准备情况, on page 122。

Note 其中一些检查必须等到执行后进行；例如，只有在工作空间中启用执行后，才应在云连接器上启用执行。对于已安装的代理，通常会在执行工作空间之前在代理配置中启用执行。

Procedure

步骤 1 从导航窗格中，选择**防御 (Defend)** > **分段 (Segmentation)**。

步骤 2 您可以为一个范围或同时为多个范围执行策略：

要同时为多个范围执行策略，请执行以下操作：

（只能使用此过程执行已分析的工作空间。）

a) 点击页面右侧的插入符号以显示“工具”(Tools) 窗格：
b) 点击**启用执行 (Enable Enforcement)**。
c) 点击**下一步 (Next)** 启动向导。
d) 选择一个要执行的工作空间。

（用于对其他范围执行工作空间的选项位于向导的最后一页。）

e) 点击**下一步 (Next)**。
f) 选择要执行的该工作空间的版本，然后点击**下一步 (Next)**。
g) 要同时为另一个范围执行策略，请点击 **+ 添加另一个工作空间 (+ Add Another Workspace)** 并完成步骤。

根据需要对其他范围重复上述操作。

h) 点击**接受并执行 (Accept and Enforce)**。

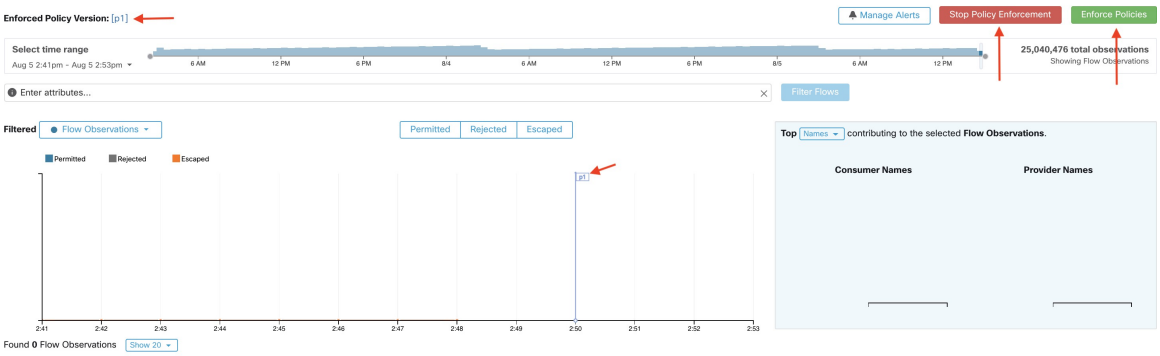
要对单个范围执行策略，请执行以下操作：

a) 导航至要执行策略的范围的主工作空间。
b) 点击**管理策略 (Manage Policies)**。
c) 点击**执行 (Enforcement)**。
d) 点击**执行策略 (Enforce Policies)**。
e) 逐步完成向导。

有关向导的详细信息，请参阅策略执行向导, on page 127。

步骤 3 在向导的最后一页上点击**接受并执行 (Accept and Enforce)**，将新的防火墙规则推送到受此工作空间中的策略影响的资产。执行时会创建一个标签标志：

Figure 70: **已启用执行的“策略执行”*(Policy Enforcement)* 页面**



您可能需要刷新页面才能看到标志。

What to do next

- 如果您为单个工作空间执行了策略，请考虑是否还必须执行其他范围的工作空间，以实现预期的执行结果。

  例如，可能还需要执行祖先范围或包含跨范围策略中涉及的工作负载的范围的工作空间。

- 在为执行策略的代理、云连接器和/或外部协调器启用执行之前，不会发生执行：
  - 对于已安装代理的工作负载，请在相关范围和资产过滤器的代理配置中执行策略。请参阅软件代理配置以及子主题。
  - 有关使用云连接器配置的基于云的工作负载，请参阅：
    - 对 AWS 资产执行分段策略时的最佳实践 和链接的主题。
    - 对 Azure 资产执行分段策略时的最佳实践 和链接的主题。
  - 对于 Kubernetes 和 OpenShift，请参阅：
    - 容器上的执行, on page 129
    - 软件代理配置
  - 有关负载均衡器，请参阅：
    - F5 BIG-IP 的策略执行

      F5 入口控制器的策略执行
    - Citrix Netscaler 的策略执行
- 检查以确保执行按预期工作。请参阅验证执行是否按预期工作, on page 130。

- 配置警报，以便您收到任何问题的通知，例如在启用执行后流被拒绝的情况。

策略执行向导

当您从工作空间的“执行”(Enforcement) 页面对单个工作空间执行策略时，策略执行向导允许您：

- 在工作负载上实施策略之前，请查看这些策略。

  这包括从祖先范围继承的策略。

- 下载策略更改以供审核。
- 比较策略版本。
- 选择要执行的工作空间的已分析版本。
- 将策略回滚到以前的版本。

策略执行向导中的步骤：

1. 选择策略更新

   您可以选择要在工作负载上执行的策略版本。

   系统将显示当前执行的策略与所选版本中的策略之间的差异。

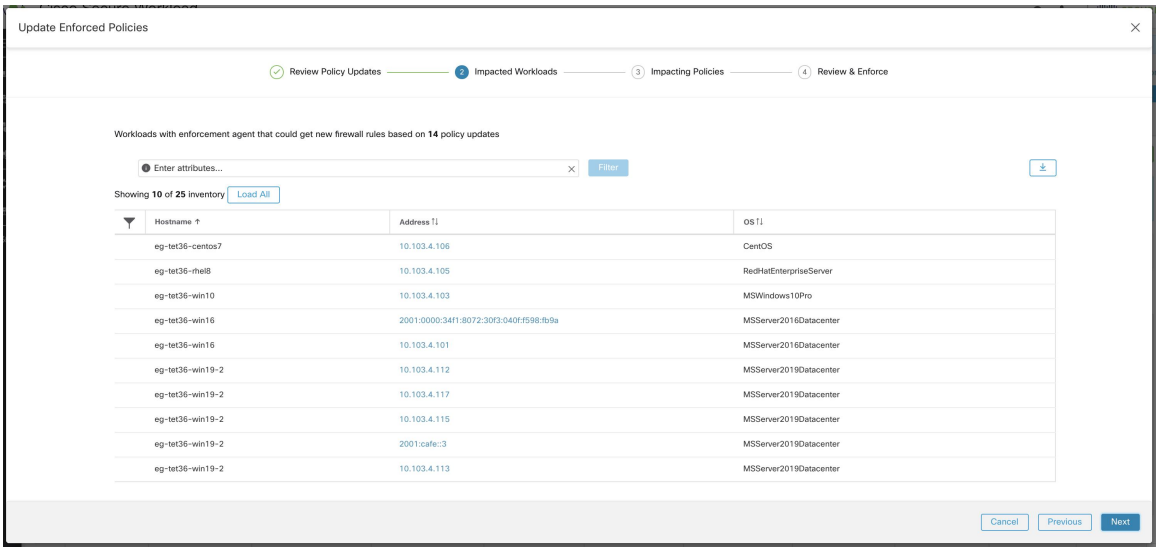
   与策略版本比较：策略差异 类似，您可以过滤和查看策略更改，并将其下载为 CSV。

2. 受影响的工作负载

   此步骤显示将受所选策略更改生成的新防火墙规则影响的工作负载。搜索结果来自于在所选策略更改的使用者/提供者联合内拥有执行代理的所有工作负载。

   可能受影响的工作负载数量不得超过范围中的工作负载总数。但是，由于代理配置意图等其他因素，实际受影响的工作负载可能会更少。

Figure 71: 受影响的工作负载列表

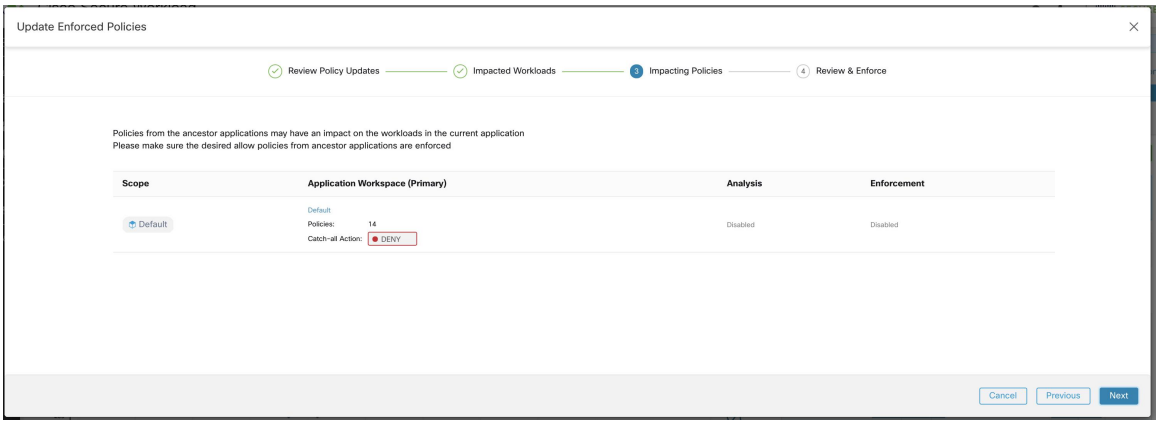


有关查看、过滤和下载资产项目的更多详细信息，请参阅管理 Cisco Secure Workload 的资产。

3. 影响策略

祖先工作空间中的策略可能会影响当前工作空间中的工作负载。因此，您应确保从祖先工作空间执行所需的允许策略。

Figure 72: 祖先工作空间和执行版本的列表

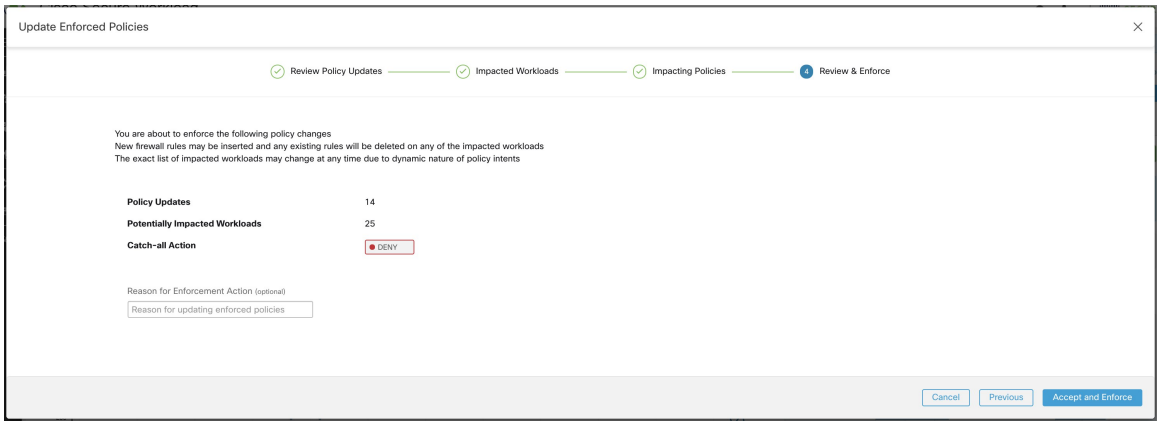


4. 审核和接受

最后一步总结了要执行的策略更改、可能受影响的工作负载的数量以及将执行的捕获全部操作。当您点击**接受并执行 (Accept and Enforce)** 时，工作空间中的策略将用于计算将在相关工作负载上配置的新防火墙规则。

您可以选择为新执行的策略提供名称、说明和操作原因，以供将来参考。如果要回滚，您可以只提供原因，因为过去版本的名称和说明无法更改。

Figure 73: 查看摘要并执行策略更改



容器上的执行

有关在由 Kubernetes 和 OpenShift 管理的基于容器的工作负载上设置分段所需步骤的概述，请参阅为基于 Kubernetes 的工作负载设置微分段。

Attention

在 Kubernetes/OpenShift 主机上运行的代理必须配置为保留现有规则。

为了防止执行干扰 Kubernetes 添加的 iptables 规则，必须使用已启用**保留规则 (Preserve Rules)** 选项的配置文件来配置代理。请参阅创建代理配置文件

在容器上执行策略时，Cisco Secure Workload 允许将 Kubernetes/OpenShift 服务抽象用作提供者。在内部，服务抽象的策略转换为提供者 Pod 及其运行所在节点的规则。这种转换取决于 Kubernetes/OpenShift 服务的类型，每当从 API 服务器收到更改时，它就会动态更新。

以下示例说明了此功能带来的灵活性。请考虑以下策略，该策略允许来自标签为 *environment = production* 的所有主机和 Pod 的流量流向类型为 *NodePort* 且名称为 *db* 的 Kubernetes 服务，这会在一组 Pod 上公开 TCP 端口 27017。

使用者	提供者	协议/端口	操作
environment = production 或 orchestrator_environment = production	orchestrator_system/service_name = db	TCP 27017	允许

此策略将产生以下防火墙规则：

- 在标记为 *environment = Production* 的主机和 Pod 上，允许到服务所属集群的所有 Kubernetes 节点的传出连接。此规则将使用 Kubernetes 分配给此服务的节点端口。

- 在标签为 *environment = production* 的 Pod 上，允许 Kubernetes 分配给此服务的 ClusterIP 的传出连接。此规则使用服务公开的端口 (TCP 27017)。
- 在服务所属的集群的 Kubernetes 节点上，允许到提供者 Pod 的传出连接。此规则使用由服务公开的目标端口 (TCP 27017)。
- 在提供服务数据库的 Pod 上，来自所有 Kubernetes 节点以及使用者主机和 Pod 的所有传入连接。此规则使用由服务公开的目标端口 (TCP 27017)。

Cisco Secure Workload 规则生成器将立即获取对服务类型、端口和一组提供者 Pod 的更改，并用于更新生成的防火墙规则。

Caution **必须仔细设计包括 Kubernetes/OpenShift 资产在内的策略，以避免与 Kubernetes 集群的内部操作冲突。**

Cisco Secure Workload 导入的 Kubernetes/OpenShift 项目包括构成 Kubernetes 集群的 Pod 和服务（例如，kube-system 命名空间中的 Pod）。这样就可以定义精确的策略来确保 Kubernetes 集群本身的安全，但这也意味着设计不当的策略会影响集群的运行。

验证执行是否按预期工作

检查代理

请参阅检查代理运行状况和执行准备情况，第 122 页。

检查转义和拒绝的流

在屏幕左侧的菜单中，点击**概述 (Overview)**。

在**安全控制面板 (Security Dashboard)** 页面上，查看**分段合规性评分 (Segmentation Compliance Score)**。

如果该值小于 100，则您可能已转义或拒绝了流，其中任何一种情况都表示存在策略配置问题。

有关详细信息，请参阅分段合规性评分。

有关调查这些情况的详细信息，请参阅策略分析结果：了解基础知识，第 113 页及其子主题。（这些主题中的信息适用于“执行”(Enforcement) 选项卡上显示的已执行策略，以及“策略分析”(Policy Analysis) 选项卡上显示的已分析策略。）

添加任何缺失的策略，或修改现有策略，例如添加额外的协议/端口，以允许所需的合法流量。

然后在重新执行之前重新分析。

查看特定工作负载的已执行策略（具体策略）

使用此程序可查看特定工作负载的所有已执行策略（即该工作负载的具体策略）。此视图非常有用，因为工作空间中的所有策略可能并不适用于工作空间中的每个工作负载，而且多个 工作空间中的策略可能适用于某个特定的工作负载（例如，父范围或祖先范围中的继承策略）。

具体策略会按优先级顺序列出。有关优先级影响的详细信息，请参阅“策略优先级”部分。

开始之前

注释 具体策略仅包括强制工作空间中的策略。如果未执行工作空间，则在执行工作空间时适用于工作负载的任何策略都不会出现在列表中。

过程

步骤 1 您可以从“资产”(Inventory) 页面或工作空间导航至工作负载的“具体策略”(Concrete Policies) 页面：

要从“范围和资产”(Scopes and Inventory) 页面导航，请执行以下操作：

a) 依次选择**整理 (Organize) > 范围和资产 (Scopes and Inventory)**。
b) 搜索相关工作负载的 IP 地址，然后点击该地址。

系统将在单独的选项卡中打开工作负载配置文件。

一般来说，除了在没有代理的情况下管理的基于云的工作负载、Kubernetes 和 OpenShift 工作负载外，如果 IP 地址显示在 **IP 地址 (IP Addresses)** 选项卡中，而不显示在**工作负载 (Workloads)** 选项卡中，则意味着未在工作负载上安装代理，因此无法执行策略，并且没有具体的策略列表。

要从“分段”(Segmentation) 页面导航，请执行以下操作：

a) 依次选择**防御 (Defend) > 分段 (Segmentation)**。
b) 点击范围。
c) 点击主工作空间。
d) 点击**管理策略 (Manage Policies)**。
e) 点击**匹配资产 (Matching Inventories)** 选项卡。
f) 搜索相关工作负载的 IP 地址，然后点击该地址。
g) 在右侧打开的面板中，点击**查看工作负载配置文件 (View Workload Profile)**。

系统将在单独的选项卡中打开工作负载配置文件。

步骤 2 从“工作负载配置文件”(Workload Profile) 页面左侧的菜单中，点击**具体策略 (CONCRETE POLICIES)**。

步骤 3 点击一行可查看详细信息。

有关详细信息，请参阅“具体策略”(Concrete Policies) 选项卡。

步骤 4 要查看命中每个策略的流量，请执行以下操作：

a) 点击**获取所有统计信息 (Fetch All Stats)**。
b) 点击每个想要的策略。

步骤 5 要查看有关 Kubernetes 或 OpenShift 工作负载的信息，请点击**容器策略 (CONTAINER POLICIES)**。

下一步做什么

依次选择**监控 (Monitor) > 执行状态 (Enforcement Status)**，以查看具体策略的状态，例如查看是否已跳过任何策略。有关详细信息，请参阅“执行状态”部分。

验证是否已为代理启用执行

过程

步骤 1 点击**防御 (Defend) > 执行状态 (Enforcement Status)**。

步骤 2 要仅查看特定范围的执行状态，请切换**按范围过滤 (Filter by Scope)** 控件并选择一个范围。

步骤 3 查看**已启用代理执行 (Agent Enforcement Enabled)** 图表。

如果图表显示任何代理为**未执行 (Not Enforced)**，请继续执行此程序。

否则，请跳过此程序的其余部分，因为所有代理均已启用执行。

步骤 4 点击图表的橙色**未执行 (Not Enforced)** 部分，以在图表下方的表格中显示受影响的工作负载。

步骤 5 通过修改代理配置配置文件，在这些工作负载上启用执行。

请参阅创建代理配置文件。

验证已执行的策略是否被推送到代理

要开始执行，特定于每个工作负载的策略必须成功推送到该工作负载上安装的代理。对于由云连接器管理的策略执行，即使未安装代理，也会显示状态。

开始之前

为至少一个范围执行策略。

过程

步骤 1 点击**防御 (Defend) > 执行状态 (Enforcement Status)**。

步骤 2 要仅查看特定范围的执行状态，请切换**按范围过滤 (Filter by Scope)** 控件并选择一个范围。

步骤 3 查看**代理具体策略 (Agent Concrete Policies)** 图表。

如果图表显示任何**已跳过 (Skipped)**，请继续执行此程序。

否则，请跳过此程序的其余步骤。

步骤 4 要显示受此问题影响的工作负载列表，请点击图表的红色**已跳过 (Skipped)** 部分。

受影响的工作负载会在图表下方的表格中列出。

步骤 5 要查看导致此问题的原因，请执行以下操作：

对于搜索结果中的每个工作负载，请点击**具体策略 (Concrete Policies)** 列中**已跳过 (Skipped)** 旁边的 **(i)** 按钮。

错误消息	更多信息
代理没有安装 Windows 操作系统	至少一个仅适用于 Windows 工作负载的策略包括未运行 Windows 操作系统的使用者和/或提供者。 从这些策略中删除这些工作负载。
已达到最大策略数	请参阅用于代理的策略过多，第 133 页。

下一步做什么

（可选）配置警报，以便在将来出现这种情况时收到通知。请参阅配置告警。

用于代理的策略过多

如果无法向特定代理推送整套适用的具体策略，则不会推送最新版本的策略。

背景：每个代理上支持的策略数量都有限制。限制也适用于使用云连接器执行的策略。Cisco Secure Workload 中的配置限制 中的信息可能会对您有所帮助。

开始之前

如果验证已执行的策略是否被推送到代理，第 132 页表示代理无法容纳完整的执行策略集，请使用此程序解决此问题。

过程

步骤 1 导航至受影响范围的主工作空间。

步骤 2 修改主工作空间中的策略：

尽量减少策略的数量，并减少使用者或提供者中任何过长的 IP 地址列表。

例如，合并现有策略，和/或将策略建立在子网而不是庞大的 IP 地址列表上。

对于使用云连接器执行的策略，您还可以提高平台施加的任何限制。请参阅适用于您的云平台的文档。

步骤 3 进行更改后，执行最新版本的工作空间，并再次检查跳过的策略。

步骤 4 对出现此问题的其他范围重复此步骤。

修改已执行的策略

执行新的和修改后的策略

如果必须在执行后修改策略，通常需要在同一主工作空间中进行更改。然后，仔细查看您的更改，并再次分析工作空间，以确保达到所预期的效果。当您确信更改将产生所需的效果时，请点击页面右上角的**执行最新策略 (Enforce Latest Policies)** 按钮。

查看、比较和管理已执行的策略版本

每次进行更改后，在工作空间中执行或重新执行策略时都会创建一个新的版本 (p*)。

有关版本控制的详细信息，请参阅关于策略版本（v* 和 p*），第 137 页。

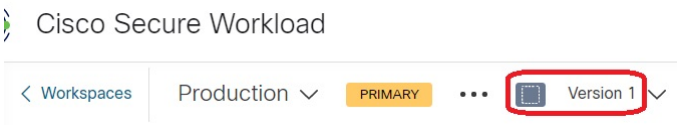
过程

步骤 1 依次点击**防御 (Defend) > 分段 (Segmentation)**。

步骤 2 导航至相关范围和主工作空间。

步骤 3 点击**管理策略 (Manage Policies)**。

步骤 4 页面顶部显示当前显示的策略版本：



显示的版本可能是策略发现版本、分析的策略版本或执行的版本。

步骤 5 执行以下操作之一：

要显示策略的不同版本，请执行以下操作：	点击当前版本，然后选择其他版本。 有关版本的说明，请参阅关于策略版本（v* 和 p*），第 137 页。 **重要提示！**如果您选择 av* 版本，请参阅查看、比较和管理发现的策略版本，第 50 页而不是本主题，包括本主题末尾的重要警告。

要查看有关所分析版本的详细信息，请执行以下操作：	1. 点击页面顶部当前版本旁边的**查看版本历史记录 (View Version History)**。 2. 点击**发布的版本 (Published Versions)** 选项卡，查看已分析和已执行的策略的版本。 3. 要查看某个版本的日志条目，请点击版本中的链接。 浅绿色行表示分析活动。 亮绿色行表示执行活动。
要比较两个版本以查看更改内容，请执行以下操作：	1. 点击**比较修订 (Compare Revisions)**。 2. 选择要比较的版本。 您可以比较最新的草稿版本、分析版本和执行版本。 3. 有关结果详细信息，请参阅策略版本比较：策略差异，第 139 页。
要删除不需要的版本，请执行以下操作：	点击版本对应的 ⋮，然后选择**删除 (Delete)**。 只要不主动分析或执行已发布的策略版本（p* 版本），就可以删除该版本。
要导出版本，请执行以下操作：	点击版本对应的 ⋮，然后选择**导出... (Export...)** 。 另请参阅导出工作空间，第 55 页。

下一步做什么

完成版本处理后，请在工作空间页面顶部将版本更改为最新发现的策略版本 (v*)。

这样可以避免无意中删除已发现的策略版本，还可以在工作空间中手动创建策略。

将已执行的策略恢复为早期版本

要将已执行的策略回滚到以前的版本，请执行 启用策略执行，第 124 页 中描述的流程之一，并选择要执行的较早版本。

禁用策略执行

- **要同时为多个范围禁用策略执行，请执行以下操作：**

  按照 启用策略执行, on page 124中所述的程序同时在多个范围内执行策略。在向导的“选择版本”(Select Version) 页面上，点击**选择版本 (Select a version)**，然后选择**禁用执行 (Disable enforcement)**。

- 要对单个范围禁用策略执行，请执行以下操作：

  导航至范围主工作空间的“策略执行”(Policy Enforcement) 页面，然后点击红色的**停止策略执行 (Stop Policy Enforcement)** 按钮。这会根据祖先工作空间中执行的策略将新的防火墙规则写入范围内的资产。将在时间序列图表上创建一个带“x”的标签标志。

暂停策略更新

Caution 此选项会暂停所有范围中所有工作负载的策略更新。

此功能需要站点管理员或客户支持权限。

要为所有范围内的所有执行终端暂停规则更新，请执行以下操作：

1. 从导航窗格中，选择**防御 (Defend)** > **执行 (Enforcement)**。
2. 点击**策略更新 (Policy Updates)** 旁边的状态。
3. 阅读并接受 EULA。

Figure 74: 防火墙规则不断更新

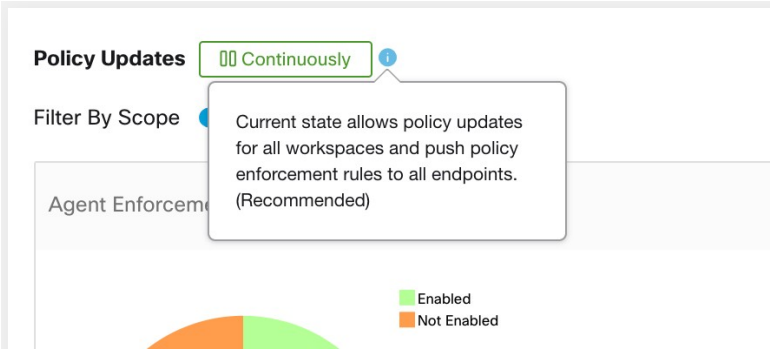
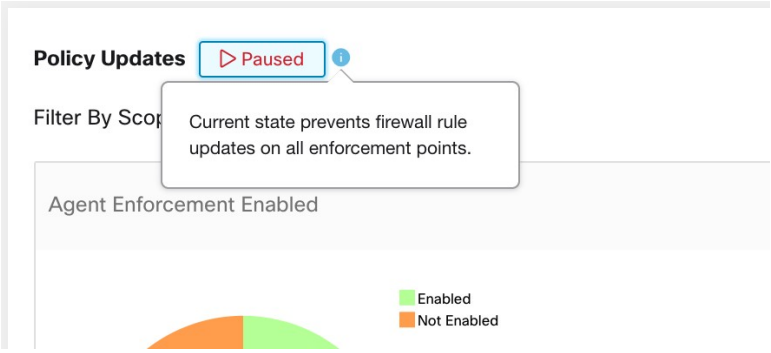


Figure 75: 防火墙规则更新已暂停



执行历史记录

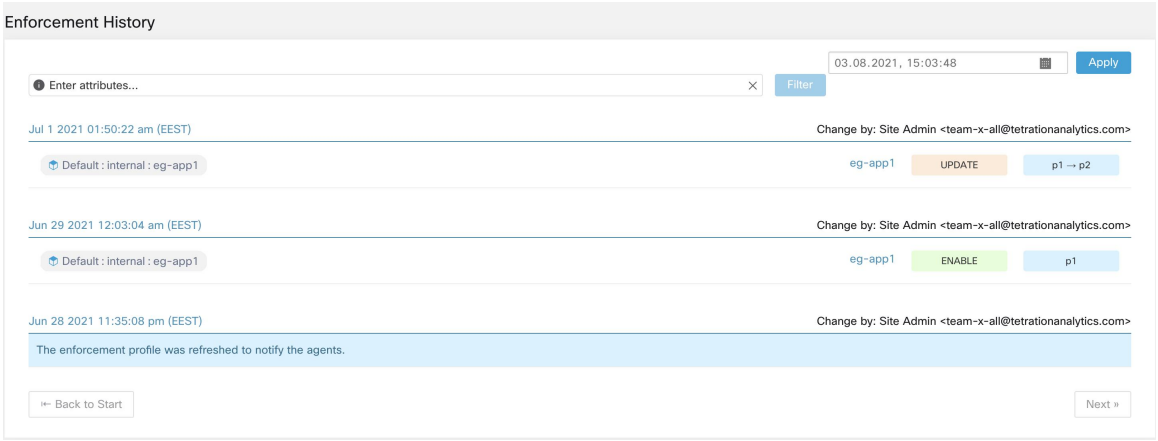
执行历史记录提供对已执行工作空间列表及其版本的更改列表。

要查看执行历史记录，请执行以下操作：

1. 点击“细分”(Segmentation) 页面右侧的插入符号以展开“工具”(Tools) 菜单。
2. 点击**执行历史记录 (Enforcement History)**。

   每个部分介绍一个事件并显示更改的摘要。
3. 点击事件，了解当时执行的所有策略的详细信息。

Figure 76: 执行历史记录视图

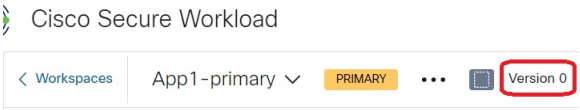


关于策略版本（v* 和 p*）

策略版本有时也被称为工作空间版本。

显示的版本

当前使用的策略（和集群）版本显示在工作空间页面顶部：



- V* 版本由自动策略发现生成

  有关详细信息，请参阅以下内容
- P* 版本为分析和/或强制版本

  有关详细信息，请参阅以下内容

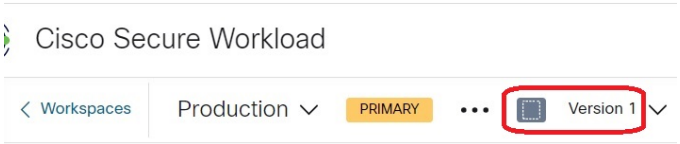
版本号旁边可能会显示以下图标：

表 6: 版本图标

	表示当前正在分析的策略的版本
	表示当前正在执行的策略的版本
	表示自动发现的策略的最新版本
（无图标）	表示版本不是其类型的最新版本

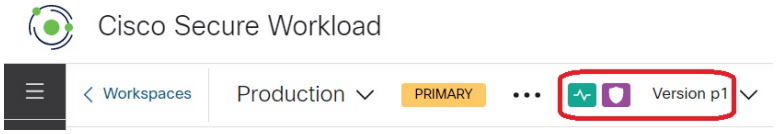
示例：

- 显示的版本是最新发现的策略版本：



- 显示的版本是当前正在分析的策略的版本：

- 显示的版本是当前正在分析和执行的策略的版本：



策略发现版本 (v*)

版本 (v*) 会在每次自动发现工作空间的策略时递增。

第一次自动发现策略时，系统会生成版本 1，并且该次运行之后的所有修改，例如编辑或批准集群（但不是重新运行），也会归入版本 1 下。当随后自动发现策略时，则会生成新版本（除非发现失败）。

如果导入策略，v* 版本也会随之递增。

要使用 v* 版本，请参阅查看、比较和管理发现的策略版本，第 50 页。

已发布的策略版本 (p*)

工作空间的术语“已发布”策略版本 (p*) 可以是指：

- 所分析策略的版本，或

- 已执行的策略版本

这是两个独立但并行的版本，具体取决于情景：

- 用于分析的策略版本：

  每次分析工作空间中的策略或在进行更改后点击**分析最新策略 (Analyze Latest Policies)** 时，系统都会为该工作空间中定义的所有集群和策略拍摄快照，并为“已发布”的策略版本 (p*) 编号分析增量。最新**实时策略分析**版本显示在页面左上角的主工作空间的“策略分析”(Policy Analysis) 选项卡上。

- 用于执行的策略版本：

  每次在工作空间中启用策略执行，或在进行更改后再次启用执行时，用于执行的“已发布”策略版本 (p*) 将成为您在执行向导中选择的分析版本号。因此，如果您执行分析版本 5，则执行版本也是版本 5，即使它是对工作空间执行策略的首次时间。当前执行的**策略版本**显示在页面左上角的主工作空间的“执行”(Enforcement) 选项卡上。

管理已发布的 (p*) 版本

无法编辑已发布的策略版本，只能完全删除。

注释 已发布的策略版本 (p*) 总数限制为 100。达到此限制后，必须删除旧版本。

要管理和删除 p* 版本，请参阅查看、比较和管理分析的策略版本，第 119 页或查看、比较和管理已执行的策略版本，第 134 页。

您还可以使用 API 来删除已发布的版本。

策略版本比较：策略差异

要比较策略，请参阅以下任何主题：查看、比较和管理发现的策略版本, on page 50、查看、比较和管理分析的策略版本, on page 119或查看、比较和管理已执行的策略版本, on page 134

策略更改将以三个类别显示：“绝对”(Absolute)、“默认”(Default) 和“全部捕获”(Catch All)。在比较表中：

- 将属于同一策略的不同服务归为一组
- 按分面或差异类型过滤策略更改
- 策略更改和服务会被分页
- 以 CSV 格式下载过滤的策略更改

Table 7: 分面过滤器属性

属性	说明
Priority	例如 100
Action	例如 ALLOW、DENY
Consumer	例如，使用者集群
Provider	例如，提供者集群
Port	例如 80
Protocol	例如 TCP

Table 8: CSV 输出列

列	说明
Rank	策略的类别。例如，ABSOLUTE、DEFAULT、CATCH_ALL
Diff	更改的差异类型。例如，ADDED、REMOVED、UNCHANGED
Priority	例如 100
Action	例如 ALLOW、DENY
Consumer Name	使用者集群的名称。
Consumer ID	使用者集群的 ID。
Provider Name	提供者集群的名称。
Provider ID	提供者集群的 ID。
Protocol	例如 TCP
Port	例如 80

下图中比较了策略版本 p1 和 v1。

Figure 77: 策略差异视图

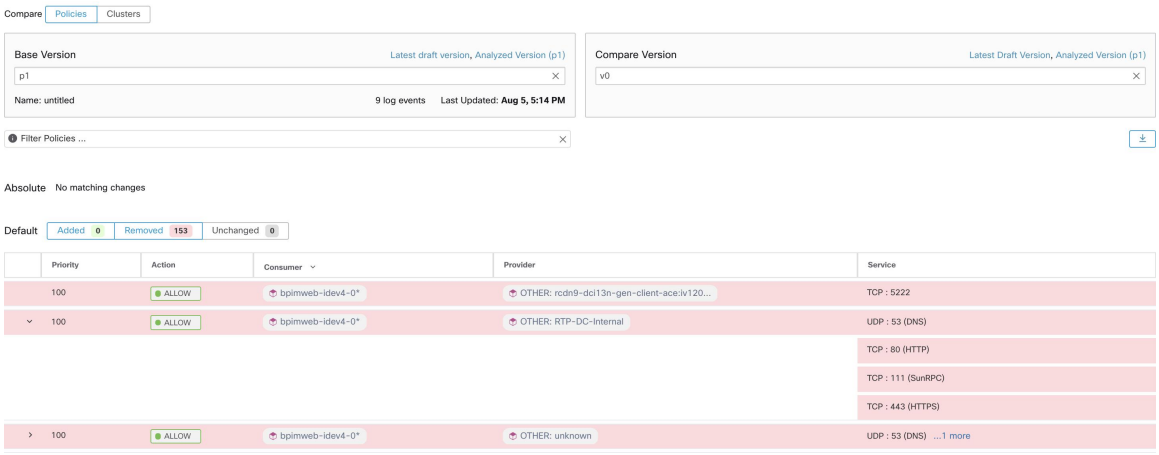


Figure 78: 策略差异视图下载按钮

Figure 79: 过滤策略差异视图

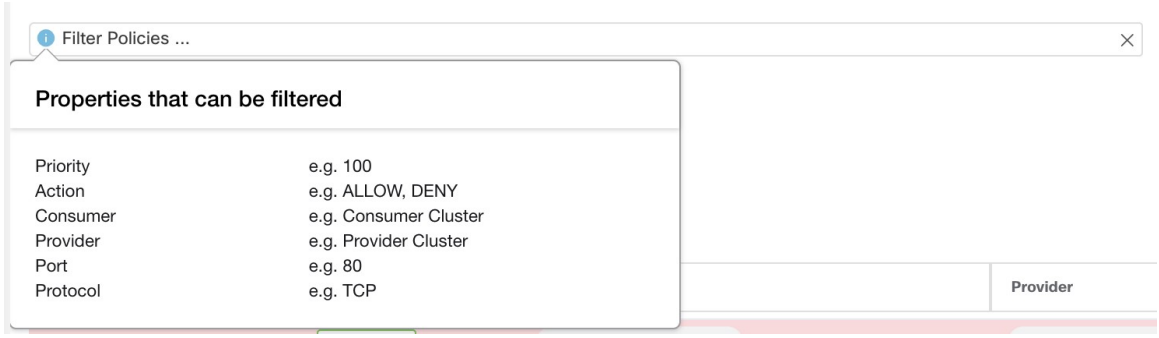


Figure 80: 策略差异视图差异类型过滤器

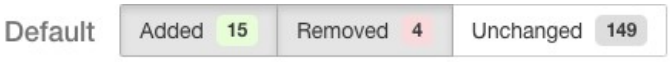


Figure 81: 策略差异视图分组

Figure 82: 策略差异视图 *CSV* 输出

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

Tip 另请参阅比较生成的集群的版本：差异视图, on page 78。

活动日志和版本历史记录

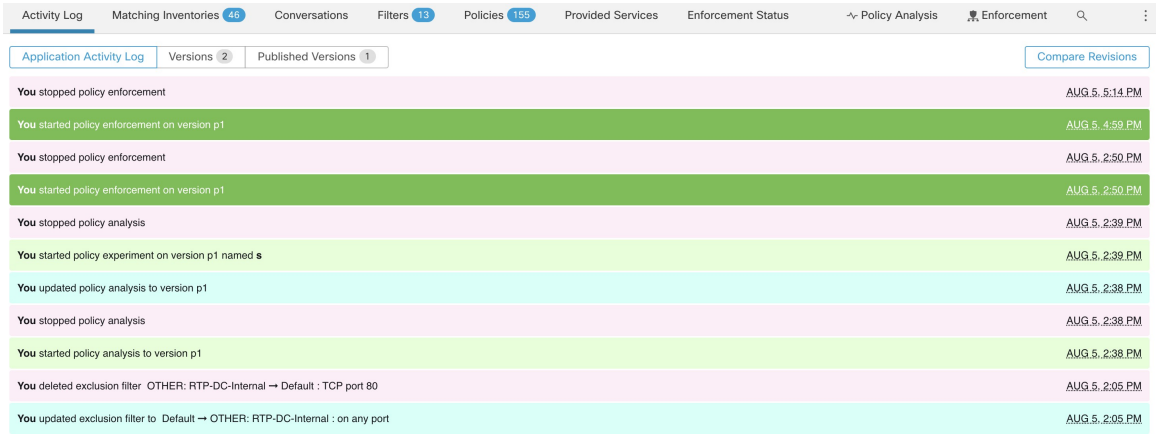
活动日志将记录您对工作空间应用的修改的历史记录。显示的事件包括添加、删除和重命名工作负载和集群，在集群之间移动工作负载，上传辅助信息，提交和中止自动策略发现等。此视图会显示进行了各项修改的用户。

要查看工作空间的修改历史记录，请点击工作空间中的任意**活动日志**链接。

例如：

1. 依次点击**防御 (Defend) > 分段 (Segmentation)**
2. 点击相关的范围和工作空间。
3. 点击**查看活动日志 (View Activity Logs)** 链接。
4. 点击**工作空间活动日志 (Workspace Activity Log)** 选项卡。

Figure 83: 适用于此工作空间版本 *v1* 的事件日志



有关页面上与版本相关的选项卡和选项的信息，请参阅：

- 关于策略版本（v* 和 p*）, on page 137

- 查看、比较和管理发现的策略版本, on page 50
- 查看、比较和管理分析的策略版本, on page 119
- 查看、比较和管理已执行的策略版本, on page 134

自动删除旧策略版本

每周自动删除以下内容： 六个月未访问的工作空间版本和过去 30 天未访问的策略试验。

对话

对话的定义是一台主机在特定端口上提供的服务被另一台主机使用。此类对话是在不同时间的多个流中实现的。自动策略发现会获取所有此类流，忽略临时/客户端端口，并对它们进行重复数据删除，以便生成对话图。对于服务器（提供者）端口 N 上主机 A 和主机 B 之间的任何给定对话，在执行自动策略发现的时间范围内，至少存在一个在端口 N 上从 A 到 B 的流观察结果。

在评估自动策略发现期间生成的集群时，利用流数据更好地了解哪些流与哪些进程相关联。

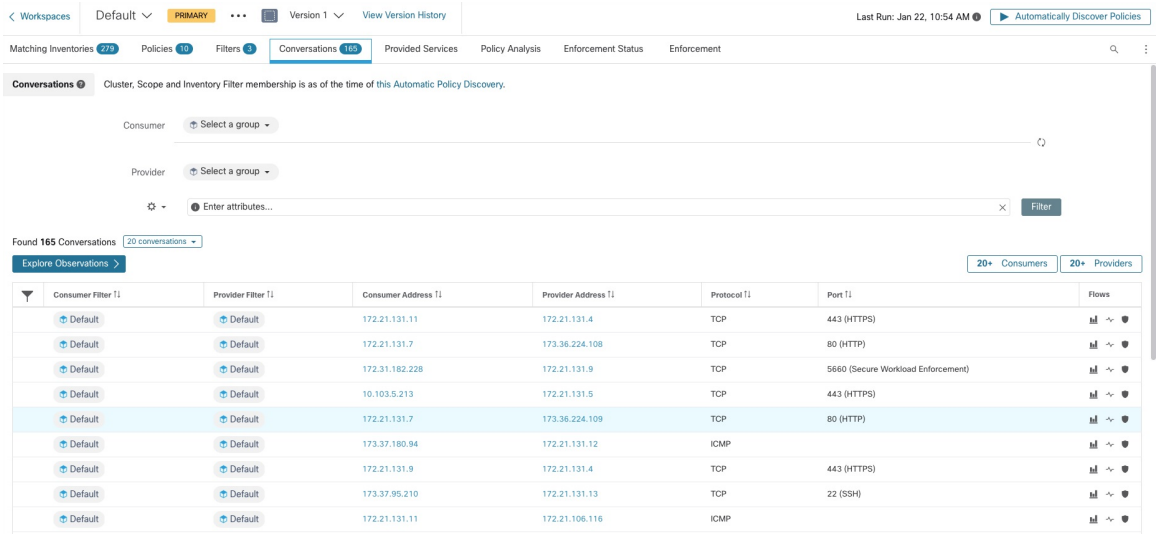
此外，通过代理收集的信息还可提供未使用的第 4 层端口的可视性。未使用的端口是指在自动策略发现所选时间间隔内没有通信的端口。此信息可用于打开这些端口上的通信策略，或者关闭与未使用端口绑定的应用，从而缩小工作负载的攻击面。

请注意，客户端-服务器分类会影响自动策略发现对话视图 - 它将决定在汇聚中丢弃哪个端口（被视为临时端口）：请参阅客户端服务器分类。

对话表视图

“对话表”视图提供了一种简单的方法来查看自动策略发现期间的汇聚流，在自动策略发现期间，使用者端口已被移除，所有时间都只有一条记录。策略会从一个过滤器到另一个过滤器，而对话则会从一个 IP 地址到另一个 IP 地址。

Figure 84: 对话表视图

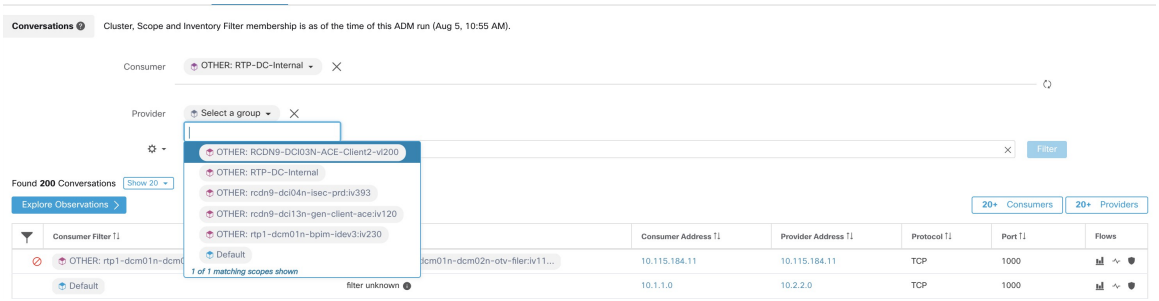


选择使用者或提供者

使用者和提供者可以通过 typeahead 下拉选择器进行选择，该选择器允许用户选择资产过滤器、范围和集群，如下例所示。系统将显示所选使用者和提供者之间的所有对话。注意：要删除现有过滤器，请点击“x”图标（清除过滤器可能不起作用）。

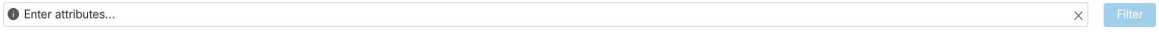
默认情况下，在自动策略发现过程中，使用者和提供者会与 IP 地址所属的所有资产过滤器进行匹配。例如，搜索“root scope”将匹配所有对话，即使某些 IP 通过更具体的范围可能会更好地匹配。要执行更具体的匹配，请从分面过滤器输入左侧的设置下拉列表中选择“将范围过滤限制为 IP 的最佳匹配”(Restrict scope filtering to an IP’s best match)。

Figure 85: 选择使用者或提供者



对话过滤器

Figure 86: 对话过滤器



在这里，您可以定义过滤器以缩小搜索结果的范围。点击“过滤器”(Filters) 一词旁边的 (?) 图标，可以找到所有可能的维度。对于任何用户标签数据，这些列也将在适当的时间间隔内可用。此输入

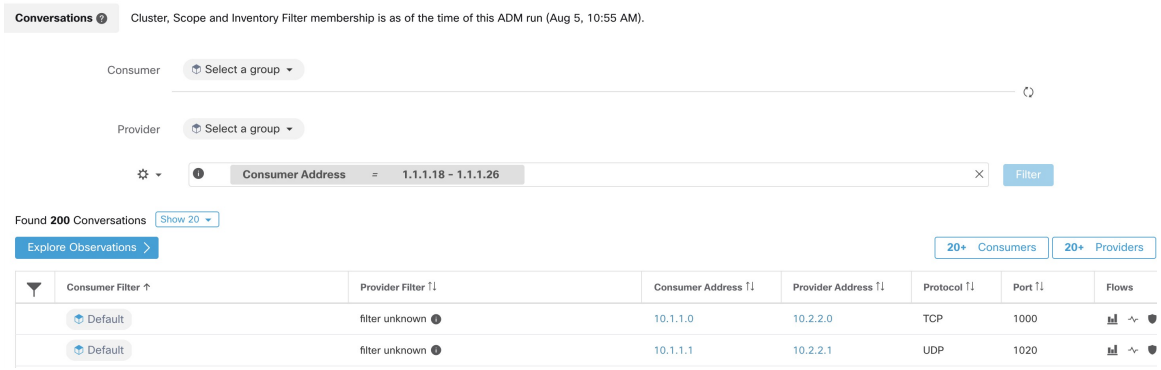
还支持 and、or、not 和括号关键字，使用这些关键字表示更复杂的过滤器。例如，IP 1.1.1.1 和 2.2.2.2 之间的方向无关过滤器可以写作：

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

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

通过将“-”转换为范围查询，过滤器输入还支持将“、”和“-”用于端口、使用者地址和提供者地址。以下是有效过滤器的示例：

Figure 87: 过滤器输入支持使用者地址的范围查询



可用过滤器：

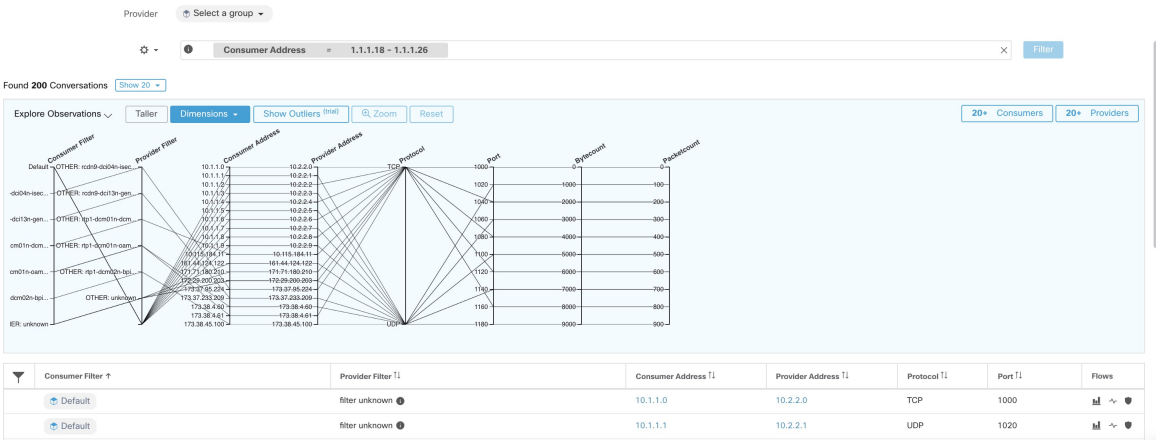
过滤器	说明
使用者地址	使用 CIDR 表示法输入子网或 IP 地址（例如，10.11.12.0/24）。匹配使用者地址与提供的 IP 地址或子网重叠的对话流观察结果。
提供者地址	使用 CIDR 表示法输入子网或 IP 地址（例如，10.11.12.0/24）匹配其提供者地址与提供的 IP 地址或子网重叠的对话流观察结果。
端口	匹配其端口与提供的端口重叠的对话流观察结果。
协议	按协议类型（TCP、UDP、ICMP）过滤对话流观察结果。
地址类型	按地址类型（IPv4、IPv6、DHCPv4）过滤对话流观察结果。
可信度	表示流方向的可信度。可能的值：高、非常高、中等。
已排除？	匹配已被排除过滤器或已批准策略排除的对话。

过滤器	说明
排除依据	匹配由特定过滤器排除的对话。可能的值：排除过滤器、策略。

探索观察结果

点击“探索观察结果”按钮可启用图表视图，允许通过“平行坐标”图表快速浏览高维数据。这个图表一开始有点令人难以理解，但在只启用您感兴趣的维度（通过取消选中“维度”(Dimensions)下拉菜单中的项目）以及重新排列维度顺序时，它还是很有用的。此图表中的单条线表示单个观察结果，该线与各个轴相交的位置表示该观察结果对于该维度的值。将鼠标悬停在图表下方的观察结果列表上，查看图表中表示该观察结果的突出显示线时，这一点会变得更清楚：

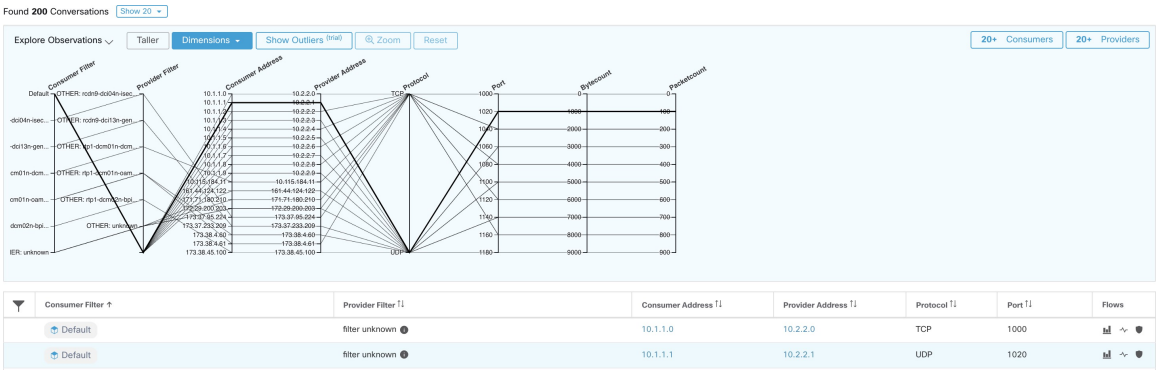
Figure 88: 探索观察结果



对话观察结果已悬停

由于对话数据的高维特性，此图表默认情况下很宽，需要向右滚动才能看到整个图表。因此，除了您感兴趣的维度外，禁用其他维度是非常有用的。在“探索对话”中提供了悬停状态，可将每个对话映射（悬停）到表格列表视图中。

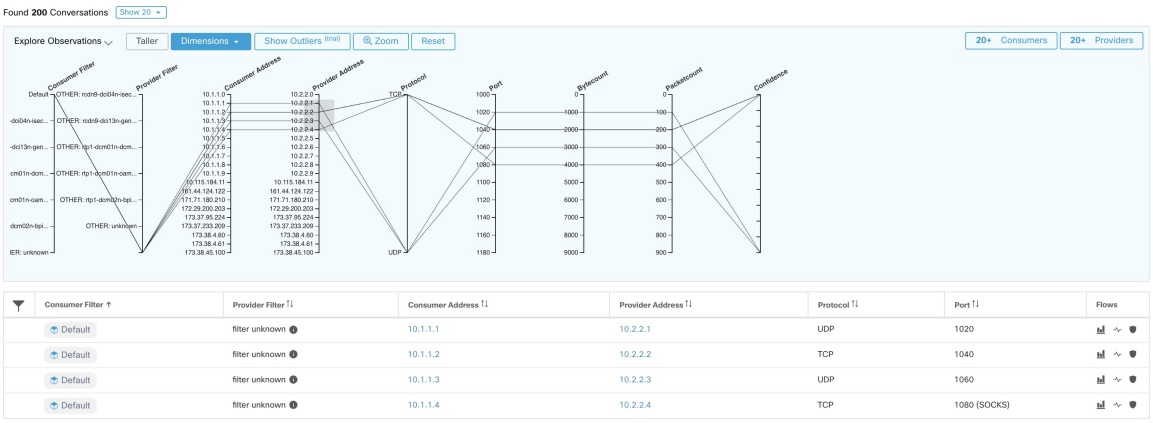
Figure 89: 对话观察结果已悬停



过滤

沿任何一个轴拖动光标都会创建一个选区，只显示与该选区匹配的观测值。再次点击轴可随时删除选择。一次可以在任意数量的轴上进行选择。观察结果列表将更新为仅显示所选对话。

Figure 90: 过滤

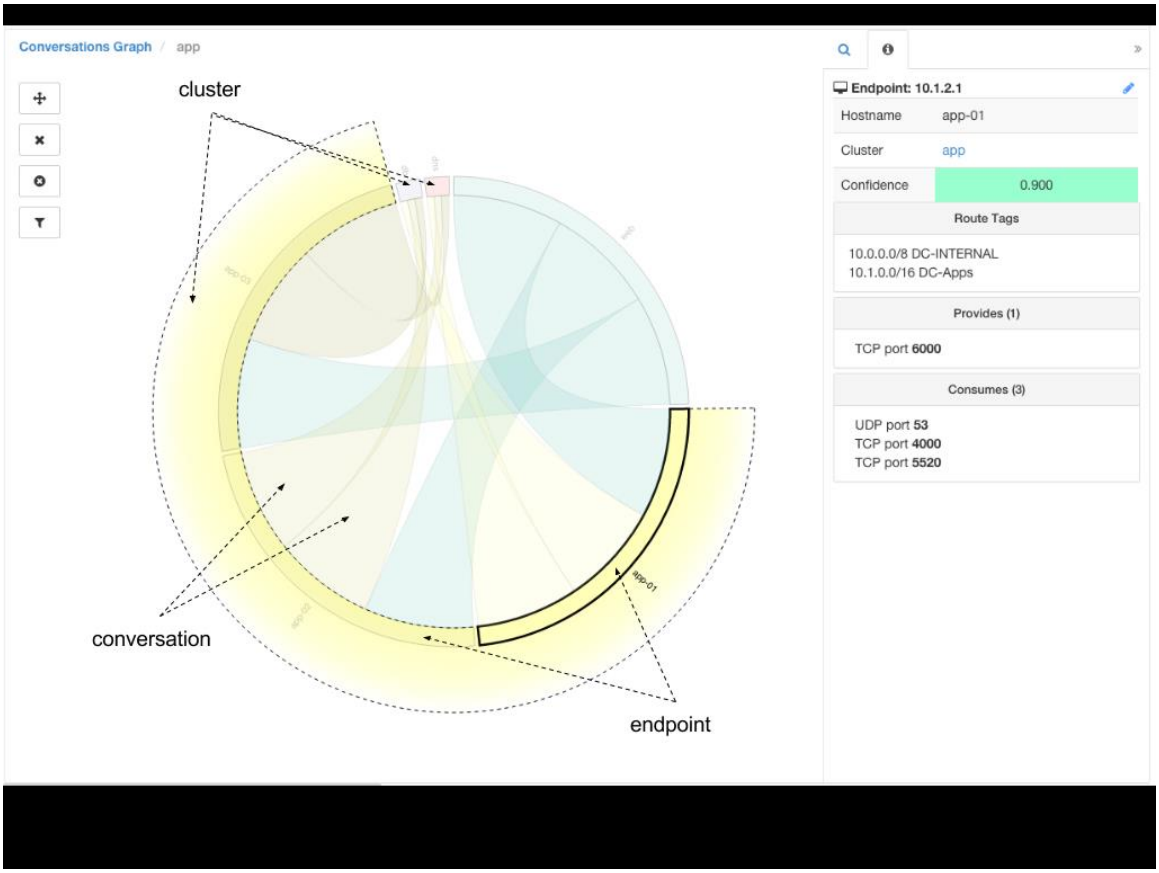


对话图表视图

对话图表视图的外观和风格与策略视图页面相似，只是它关注的不是分区/集群/策略，而是集群/工作负载/对话。如下图所示，外部弧线概括地表示集群，展开后可将成员主机/工作负载显示为内部弧线。弦线表示对话或连接。

对话视图上的控件和侧面板与策略视图的操作类似，只是侧面板信息还会显示所选工作负载的详细信息，如已使用/提供的服务，以及父集群链接和进程信息（如有）。

Figure 91: 对话图表视图



排名靠前的对话使用者/提供者

可以通过“对话”(Conversations)表顶部的两个按钮查看根据反映所选过滤器的对话总数排名靠前的使用者或提供者的数量。点击每个对话框，即可看到一个包含对话次数列、每个使用者/提供者的地址、主机名和其他用户注释列的表格。

Figure 92: 在“对话”***(Conversations)*** 表上方

Figure 93: 排名靠前的使用者模式

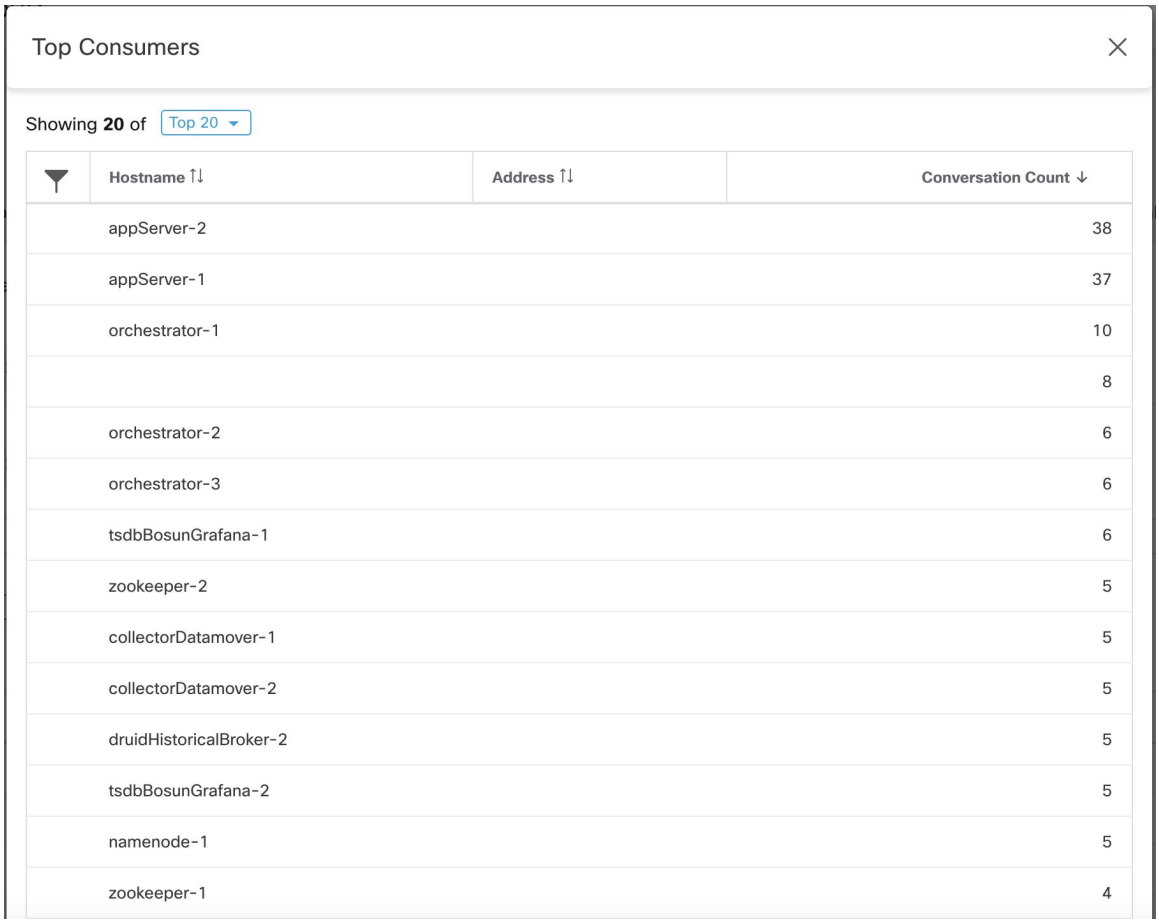
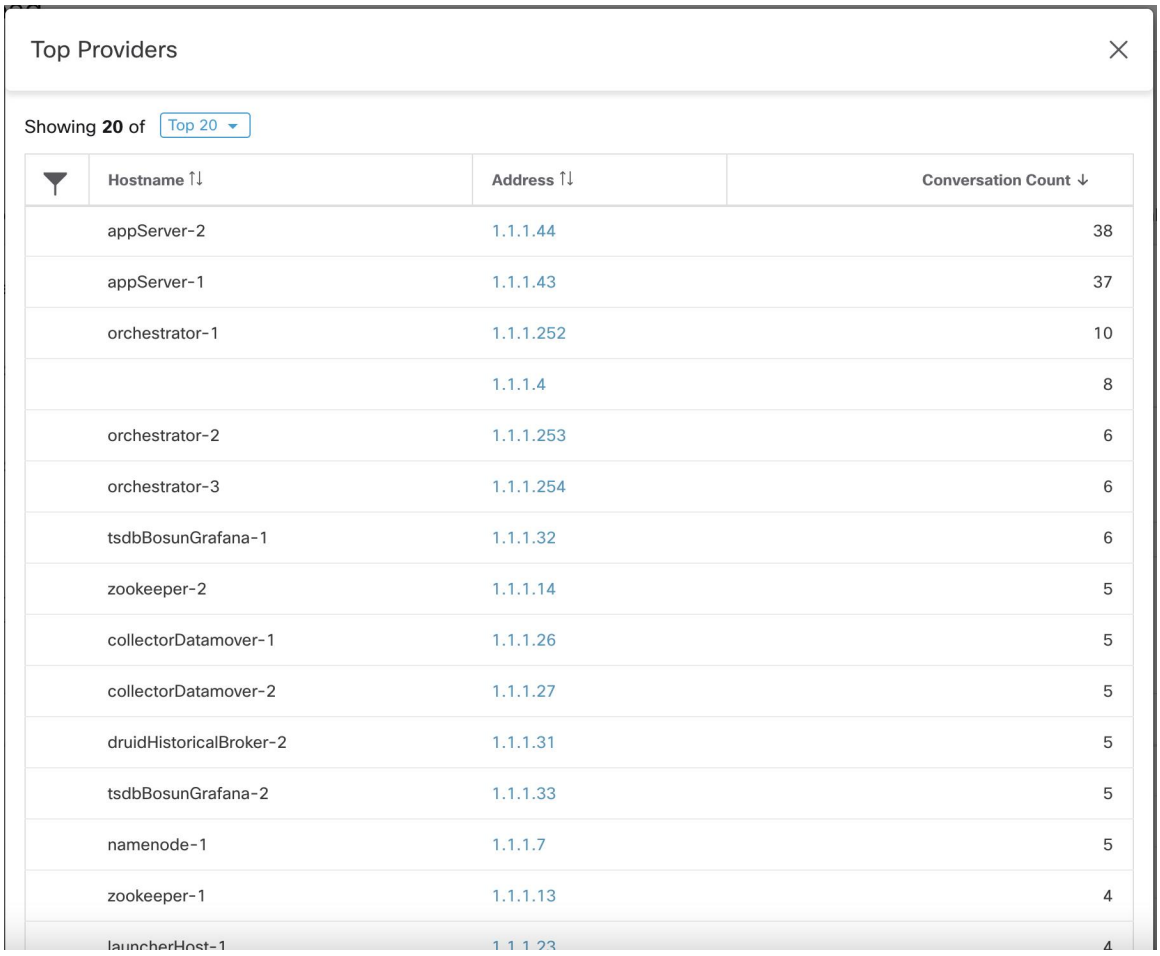


Figure 94: 排名靠前的提供者模式



自动策略发现的自动负载均衡器配置（仅限 F5）

Important 这是一个试验性功能。

此功能及其 API 位于 **ALPHA** 中，可能会在未来版本中加以更改和增强。

自动策略发现功能可为连接到外部协调器的负载均衡器从配置中生成策略。通过配置生成策略可最大限度地减少对流数据的依赖，并提高所发现的集群和策略的准确性。

它依靠客户向负载均衡器报告流量，以生成允许这些流量的策略。

术语

VIP 虚拟 IP：客户端向其发送以服务为目标的流量的 IP。

SNIP SNAT IP：负载均衡器用于向后端主机发送流量的 IP。

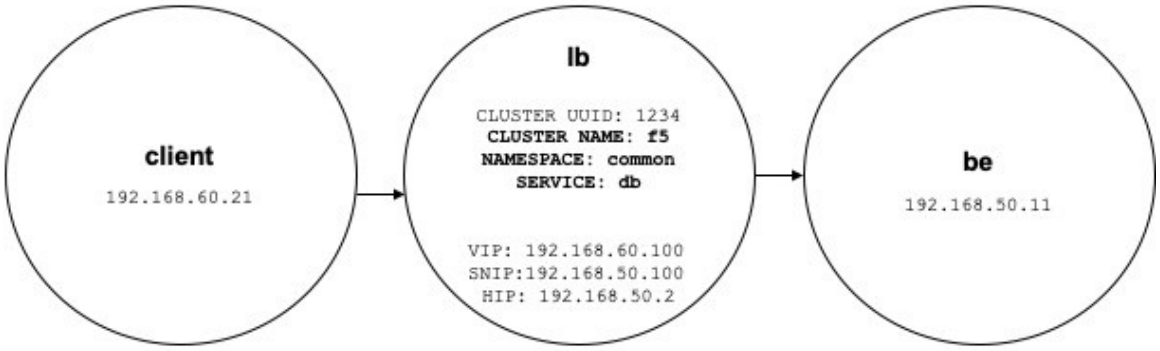
BE 后端终端：后端主机的 IP。

HIP 运行状况检查 IP：负载均衡器用于向后端主机发送运行状况检查流量的源 IP。

Note HIP 与自动映射模式下的 SNIP 相同。但在配置 SNAT 池时，HIP 和 SNIP 可能会不同。

部署

Figure 95: 部署



请考虑以下部署，其中负载均衡器 VIP、SNIP 和 HIP 属于 *lb* 范围，BE 属于 *be* 范围。范围按如下方式创建。

- 客户端

  客户端范围包括与负载均衡器通信的客户端。对于上面的示例，客户端范围查询如下：

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

- lb

  F5 外部协调器会标记负载均衡器使用的 VIP、SNIP、HIP 和 BE。这些标签可用于构建范围查询，其中 *orchestrator_system/service_name* 用于选择服务的 VIP、*orchestrator_system/service_startpoint* SNIP 和 *orchestrator_system/service_healthcheck_startpoint* HIP。对于上面的示例，包含服务 *db* 的 VIP、SNIP 和 HIP 的范围查询如下所示：

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

Note 要求 SNIP 和 VIP 属于同一范围。

- Be

user_orchestrator_system/service_endpoint 选择服务的 BE。对于上面的示例，包含服务 *db* 的 BE 的范围查询如下：

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

集群

每个服务最多可生成四个被发现的集群，其中只有服务集群对用户可见。SNIP、HIP 和 BE 集群会作为服务集群的相关集群出现。仅当 *lb* 范围中存在 HIP 和 BE 时，才会生成 HIP 和 BE 集群。

对于上面的示例，自动策略发现会在 *lb* 范围内生成一个 SNIP 集群和 HIP 集群，其中包括用于服务的 SNIP 和 HIP。由于 BE 位于 *lb* 范围之外，因此自动策略发现不会生成后端集群，而是将 *be* 范围添加到 *db* 的相关集群列表中。

集群按如下方式生成：

- 服务

  服务集群包括用于服务的 VIP。服务集群的查询如下：

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

- SNIP

  服务的 SNIP 包含在 SNIP 集群中。SNIP 集群的查询如下：

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

- HIP

  服务的 HIP 包含在 HIP 集群中。HIP 集群的查询如下：

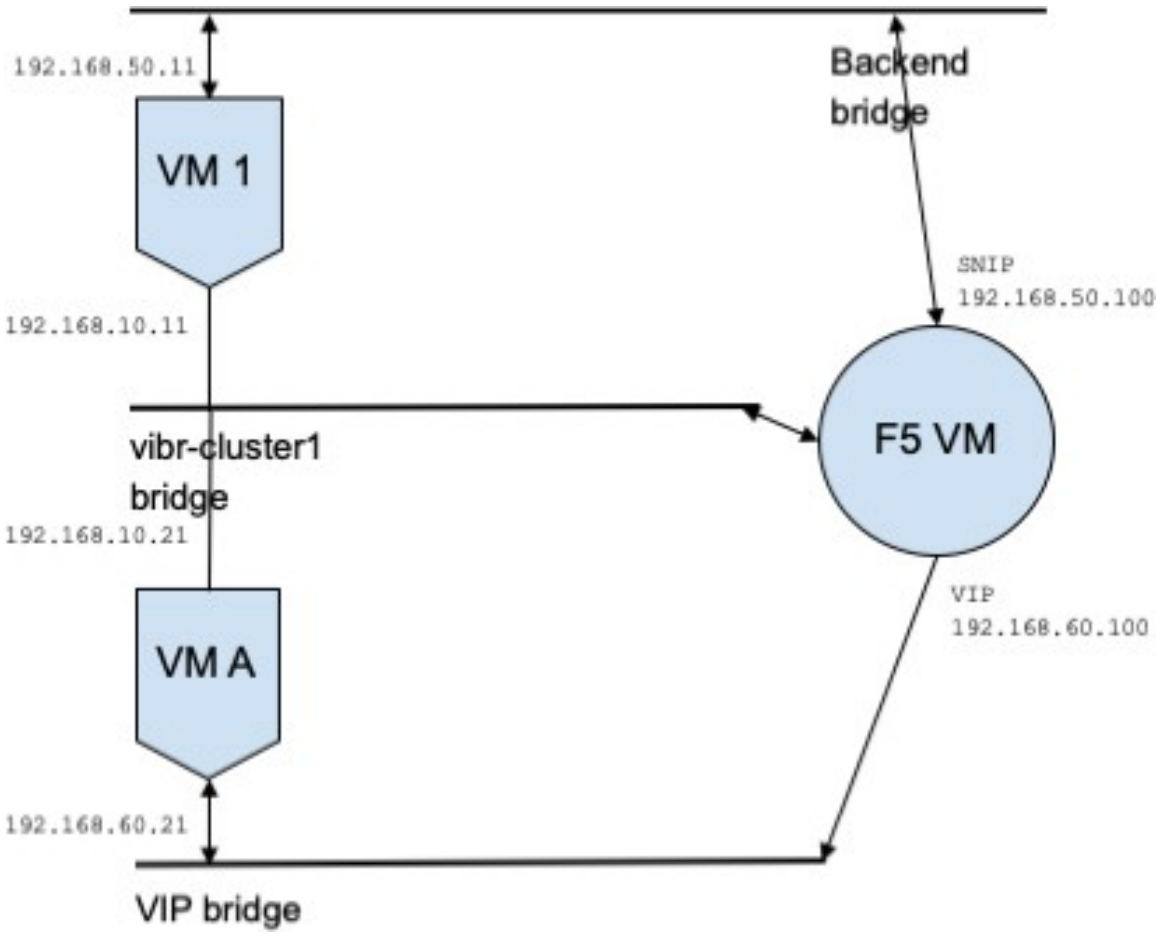
  ```
  user_orchestrator_system/cluster_id eq 1234 and
  user_orchestrator_system/service_healthcheck_startpoint eq db
  ```

- 后端

  当一个或多个 BE 属于 *lb* 范围时，将生成服务的后端集群。这不适用于上面的示例，导致不会在 *lb* 范围内生成后端集群。

策略

Figure 96: 策略生成



假设我们有一个 VIP 为 *192.168.60.100* 、SNIP 为 *192.168.50.100* 的服务 *db*，一个 IP 为 *192.168.50.11* 的后端虚拟机在端口 10000 上侦听。从客户端虚拟机 *192.168.60.21* 到 *db* 的流量会产生以下策略：

- 从客户端到 VIP 的策略

  以下策略允许从客户端虚拟机为 *db* 提供服务。

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

- 从 SNIP 到 BE 的策略。

  从配置中自动生成允许从 SNIP 到 BE 的流量的策略，并显示为 *db* 的相关策略。

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

  从 *lb* 范围到 *be* 范围的策略连接器会向其推送以下策略。

使用者	提供者	端口	协议	行动
SNIP	be	10000	TCP	允许

  这会在 BE 主机 192.168.50.11 上生成防火墙规则，从而允许端口 10000 上来自 LB SNIP 192.168.50.100 的传入流量。

- 从 HIP 到 BE 的策略。

  系统会从配置中自动生成允许从 HIP 到 BE 的流量的策略，并显示为 *db* 的相关策略。

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

  从 *lb* 范围到 *be* 范围的策略连接器会向其推送以下策略。

使用者	提供者	端口	协议	行动
HIP	be	0	ICMP	允许

  这会在 BE 主机 *192.168.50.11* 上生成防火墙规则，从而允许来自 LB HIP *192.168.50.2* 的传入 ICMP 流量。

警告

- 当同一负载均衡器实例中的多个服务具有相同名称时，为其中任何一个服务生成的后端规则都将包括所有服务的后端池，也就是说，规则的许可性将超出需要。

策略发布者

策略发布服务器是思科 Cisco Secure Workload 的一项高级功能，它允许第三方供应商实施自己的执行算法，这些执行算法已针对负载均衡器或防火墙等网络设备进行了优化。通过将已定义的策略发布到驻留在 Cisco Secure Workload 集群中的 Kafka 实例，并向客户提供 Kafka 客户端证书，即可实现此功能，从而允许第三方供应商代码从Kafka检索策略，并将其适当地转换到其网络设备配置中。

本部分旨在介绍第三方供应商（下文简称为用户）在 Linux 上通过 Java 利用策略发布服务器功能而必须执行的程序。

前提条件

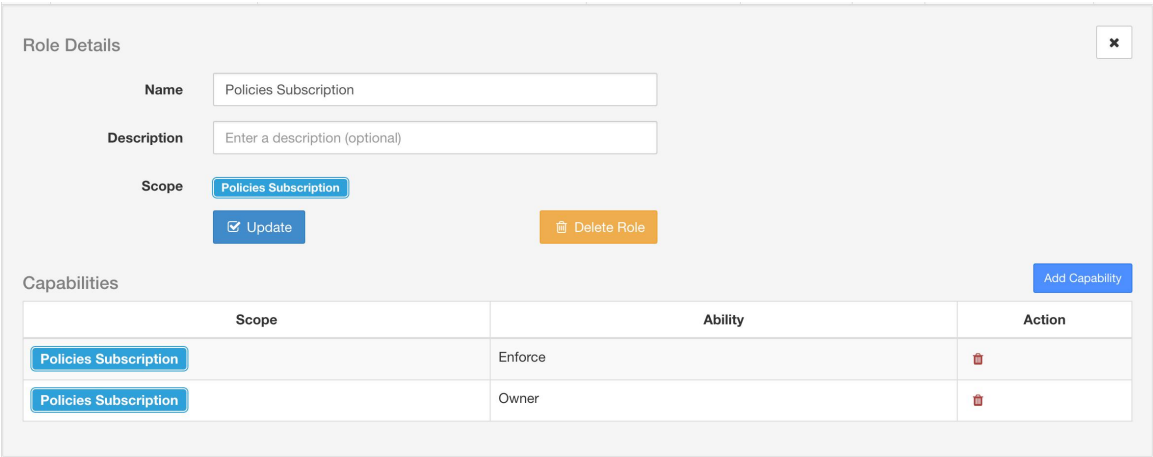
在 Linux 系统（如 Ubuntu 16.04）上安装以下软件包。

- Java 8 JDK
- Apache Kafka 客户端：kafka-clients-1.0.0.jar
- 协议缓冲区核心：protobuf- java-3.4.1.jar
- Apache Log4j：log4j-1.2.17.jar
- 适用于 Java 的简单日志记录外观：slf4j-api-1.7.25.jar、slf4j-log4j12-1.7.25.jar
- 适用于 Java 的 Snappy 压缩器/解压缩器：snappy- java-1.1.4.jar

获取 Kafka 客户端证书

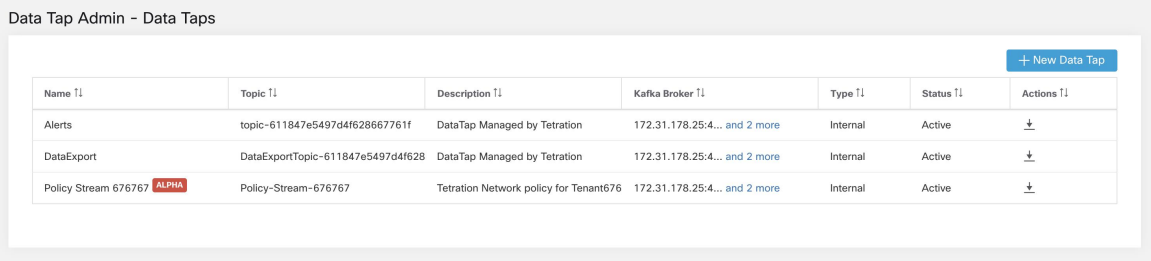
- 创建具有“所有者”功能的用户角色，并将其分配给选择的用户帐户：

Figure 97: 用于从 ***Kafka*** 接收策略的用户角色配置



- 按照执行策略中的说明执行策略执行。第一步必不可少，因为它会创建与活动范围关联的Kafka主题。
- 导航至**管理 (Manage)** > **数据分流管理员 (Data Tap Admin)**
- 选择数据分流 *(Data Taps)* 选项卡，然后通过点击操作 *(Actions)* 列下的下载按钮来下载 Kafka 客户端证书。确保在下载对话框中选择 *Java* 密钥库 *(Java Keystore)* 格式。

Figure 98: 数据分流视图



- 下载的客户端证书文件通常具有类似 *Policy-Stream-10-Policies-Subscription.jks.tar.gz* 的名称。创建一个目录并在创建的目录下将其解压，如下所示：

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

Protobuf 定义文件

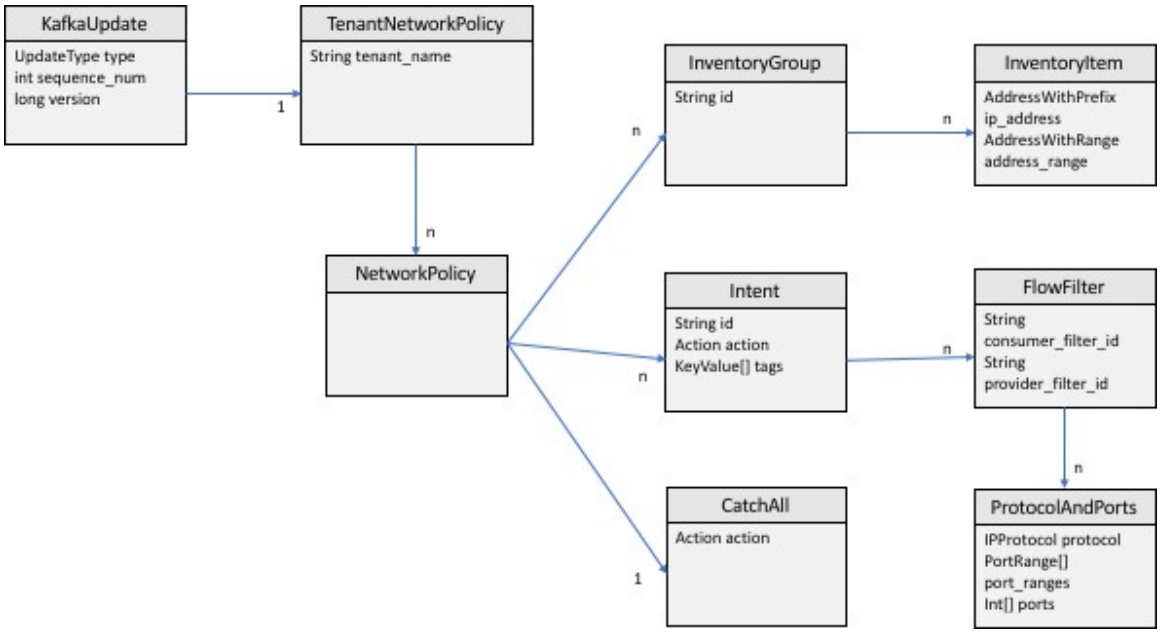
由 Cisco Secure Workload 后端向 Kafka 公开的网络策略将以 Google Protocol Buffers 格式进行编码。有关如何在 Linux 系统上下载并安装它的说明，请参阅本指南。

Cisco Secure Workload 网络策略的原始文件可在此处下载。

Cisco Secure Workload 网络策略的数据模型

下图显示了向 Kafka 公开的 Cisco Secure Workload 实体的简化 UML 图：

Figure 99: Cisco Secure Workload 网络策略的数据模型



在 protobuf 中建模的 *Cisco Secure Workload* 网络策略包含 *InventoryGroup*列表、意图列表和 *CatchAll* 策略。每个策略包含属于一个根范围的所有项目。*InventoryGroup* 包含 InventoryItem 列表，这些 *InventoryItem* 通过指定网络地址（可以是单个网络地址、子网或地址范围）来表示 Cisco Secure Workload 实体，例如服务器或设备。意图描述当网络流与给定使用者的 *InventoryGroup*、提供者的 *InventoryGroup* 以及网络协议和端口匹配时要采取的操作（允许或拒绝）。*CatchAll* 表示为 Cisco Secure Workload 内部的根范围定义的捕获全部操作。如果不存在已为根范围启用执行的工作空间，则会将默认策略 *ALLOW* 写入生成的策略中。

当用户或资产组更改触发执行时，Cisco Secure Workload 后端将已定义网络策略的完整快照作为表示为 *KafkaUpdates* 的消息序列发送到 Kafka。有关如何将这些消息重建为完整快照以及如何处理错误情况的详细信息，请参阅 *tetration_network_policy.proto* 文件中 *KafkaUpdate* 的注释。

如果 *KafkaUpdate* 消息大小大于 10MB，则 Cisco Secure Workload 后端会将此消息拆分为多个片段，每个片段的大小为 10MB。如果有多个分段，则仅第一个分段具有 *TenantNetworkPolicy* 的 *ScopeInfo* 字段。在 *KafkaUpdate* 消息的其余片段中，*ScopeInfo* 将被设置为 nil。

Cisco Secure Workload 网络策略客户端的参考实施

有关如何编译和运行演示客户端的执行和说明，请参阅 Java 版本的 tnp-enforcement-client。

此实施提供通用代码，用于仅通过 Kafka 从 Cisco Secure Workload 策略流读取网络策略。通过执行所需的接口 PolicyEnforcementClient，可以插入用于将实际策略编程到网络设备的供应商特定代码。

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。