3.7 版 Cisco Secure Workload 快速入门指南

首次发布日期: 2022 年 8 月 17 日

分段简介

传统上，网络安全旨在通过在网络边缘放置防火墙来阻止恶意活动进入网络。但是，您还需要保护您的组织免受已破坏您的网络或来自网络内部的威胁。分段（在此情况下也称为微分段）允许您控制网络上的工作负载和其他主机之间的流量，从而帮助保护网络上的工作负载，因此您可以仅允许您的组织出于业务目的所需的流量，并拒绝所有其他流量。

例如，您可以使用分段策略来阻止托管面向公众的 Web 应用的工作负载与数据中心内的绝密研发数据库之间的所有通信，或阻止非生产工作负载（通常为合规性较低，保护较少），以免与生产工作负载联系。

Cisco Secure Workload 使用您组织的实际流数据来建议您在实施之前评估和审批的分段策略。您还可以手动创建策略。

关于本指南

您可以将本指南与 Cisco Secure Workload 版本 3.7 配合使用。

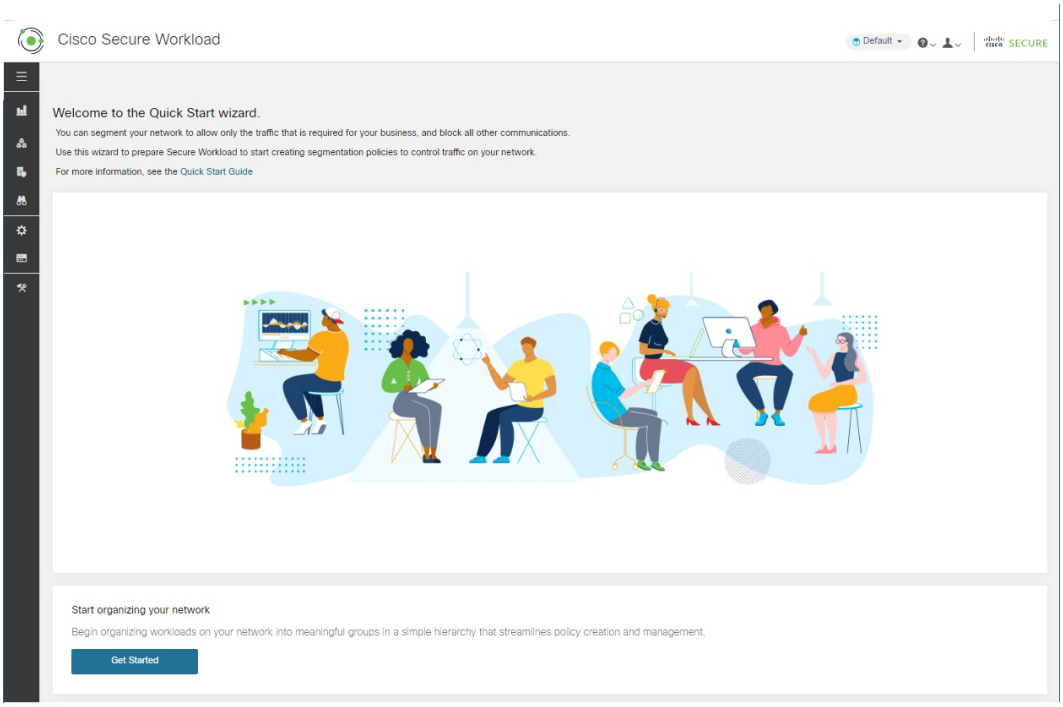
本文档：

- 向您介绍关键的 Cisco Secure Workload 概念：分段、工作负载标签、范围、分层范围树和策略发现；
- 指导您完成为单个应用创建范围树的第一个分支的过程（使用 Cisco Secure Workload 中的首次用户体验向导）；和
- 向您展示如何根据实际流量自动生成所选应用的策略。

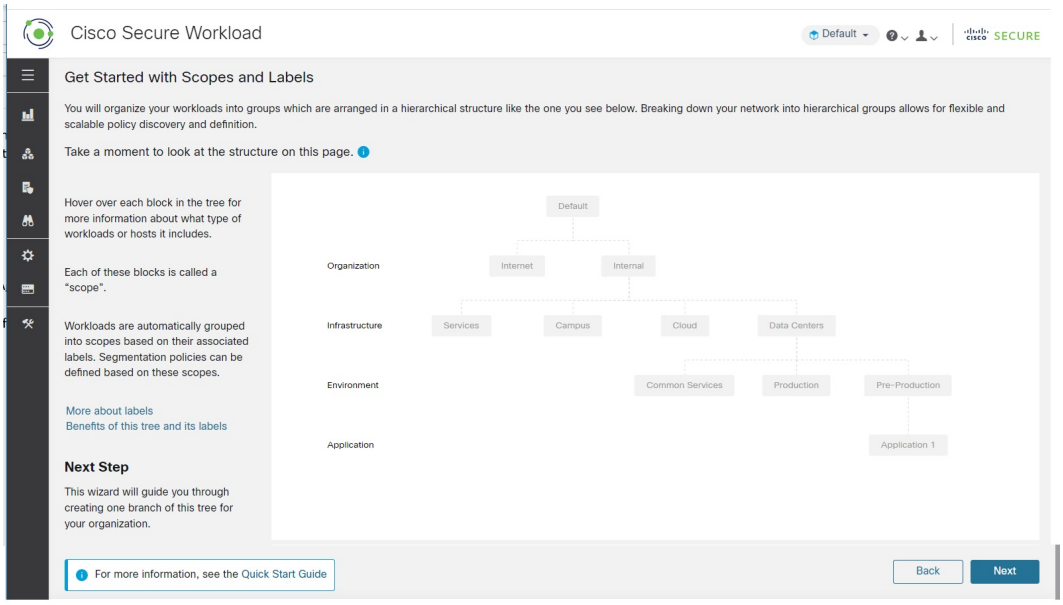
Cisco Secure Workload 快速入门向导不需要外部文档，但对于希望在使用新产品之前提前阅读的用户，本自行激活指南是可选的配套和补充信息来源。

向导之旅

起始页



范围和标签入门



本页介绍您将构建的内容。它会告诉您（并显示）什么是标签和范围，以及它们如何协同工作。

关于标签

Cisco Secure Workload 的强大功能取决于分配给工作负载的标签。

标签是描述每个工作负载的键值对。

看看上面的树。标签键显示在树的左侧。标签值是与每个键对应的灰色框中的文本。该向导可帮助您将这些标签应用于工作负载。

通过为工作负载分配标签，您可以将其分组到称为范围的组中。上面树中的每个灰色框都是一个范围。

如上图所示，属于应用 1 范围的所有工作负载（位于此树的右下角）均由以下标签集定义：

- 组织 = 内部
- 基础设施 = 数据中心
- 环境 = 预生产
- 应用 = 应用 1

标签和范围树的强大功能

标签驱动 Cisco Secure Workload 的强大功能，根据标签创建的范围树不仅仅是网络的摘要：

- 标签可让您立即了解您的策略：

  `"Deny all traffic from Pre-Production to Production"`

  将此策略与没有标签的相同策略进行比较：

  `"Deny all traffic from 172.16.0.0/12 to 192.168.0.0/16"`

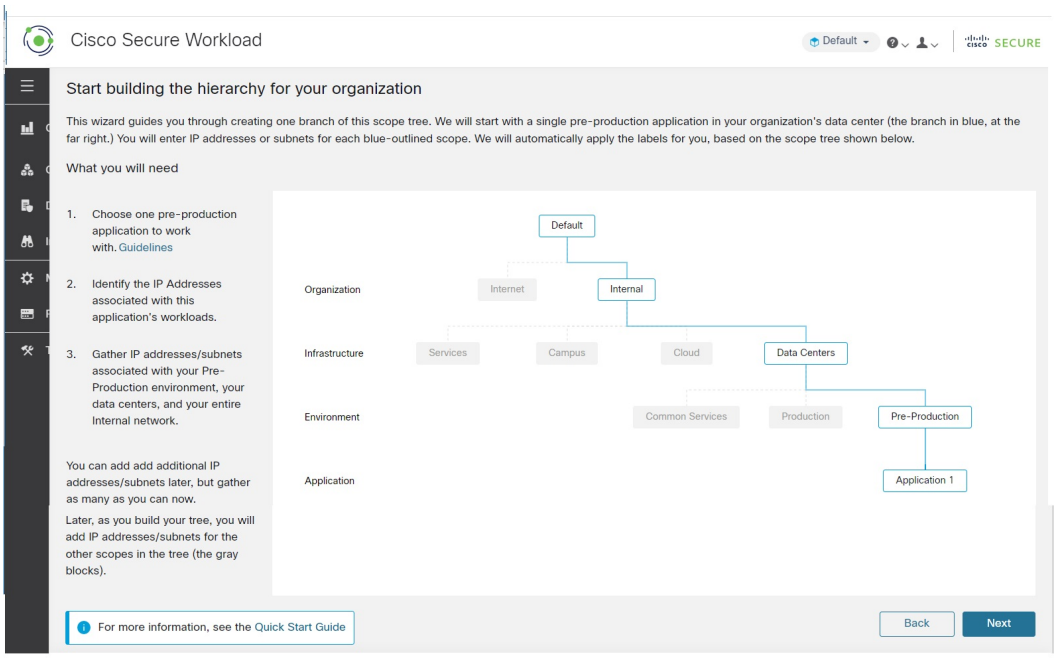
- 将标记的工作负载添加到资产中或从中删除时，基于标签的策略会自动应用（或停止应用）。随着时间的推移，这些基于标签的动态分组会大大减少维护部署所需的工作量。
- 工作负载根据其标签分组到范围中。通过这些分组，您可以轻松地将策略应用于相关工作负载。例如，您可以轻松地将策略应用于预生产范围内的所有应用。
- 在单个范围内创建的策略可以自动应用于树中后代范围内的所有工作负载，从而最大限度地减少您需要管理的策略数量。

  您可以轻松地定义和应用广泛的策略（例如，应用于组织中的所有工作负载）或狭义的策略（仅适用于属于特定应用的工作负载）或两者之间的任何级别（例如，应用于数据中的所有工作负载）中心。

- 您可以将每个范围的职责分配给不同的管理员，将策略管理委派给最熟悉网络每个部分的人员。

开始为您的组织构建分层

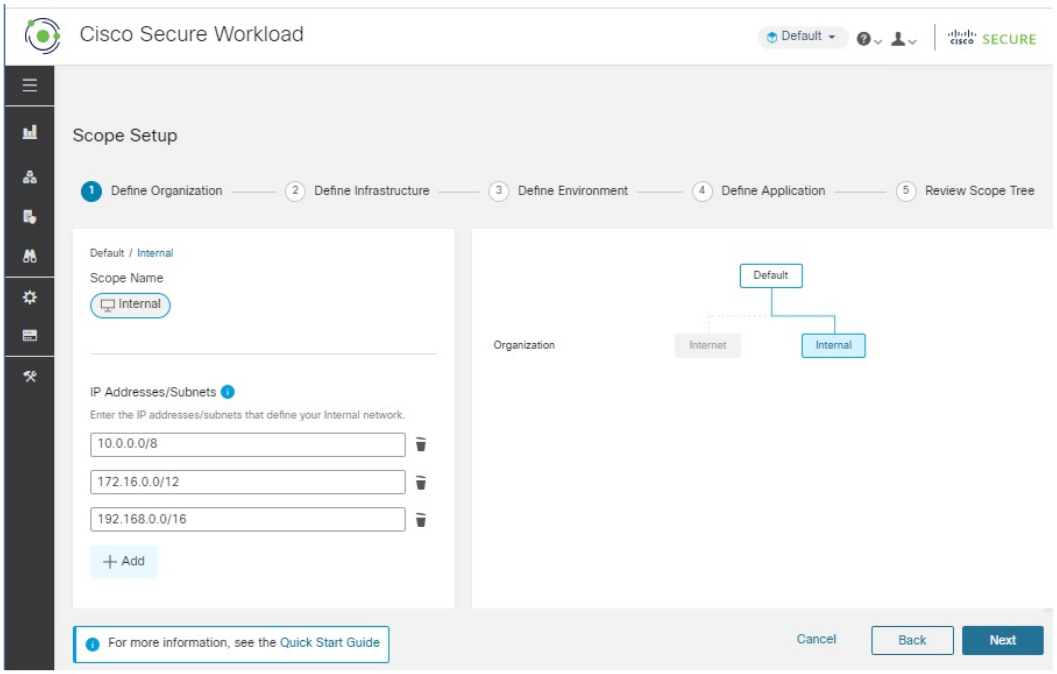
既然您知道要构建的内容以及原因，就可以开始构建自己的范围树了。



在继续之前，您需要选择要使用的应用。请参阅以下 选择此向导的应用，第 9 页的指南。请注意，运行向导时，除非重新启动向导，否则将无法返回到这些信息页面。

定义内部范围

内部范围包括定义组织内部网络的所有 IP 地址，包括公共和专用 IP 地址。



该向导将引导您向树分支机构中的每个范围添加IP地址。添加地址时，向导会为每个地址分配定义该范围的标签。

因此，在此页面上，向导会分配标签

```
Organization = Internal
```

到您输入的每个 IP 地址。

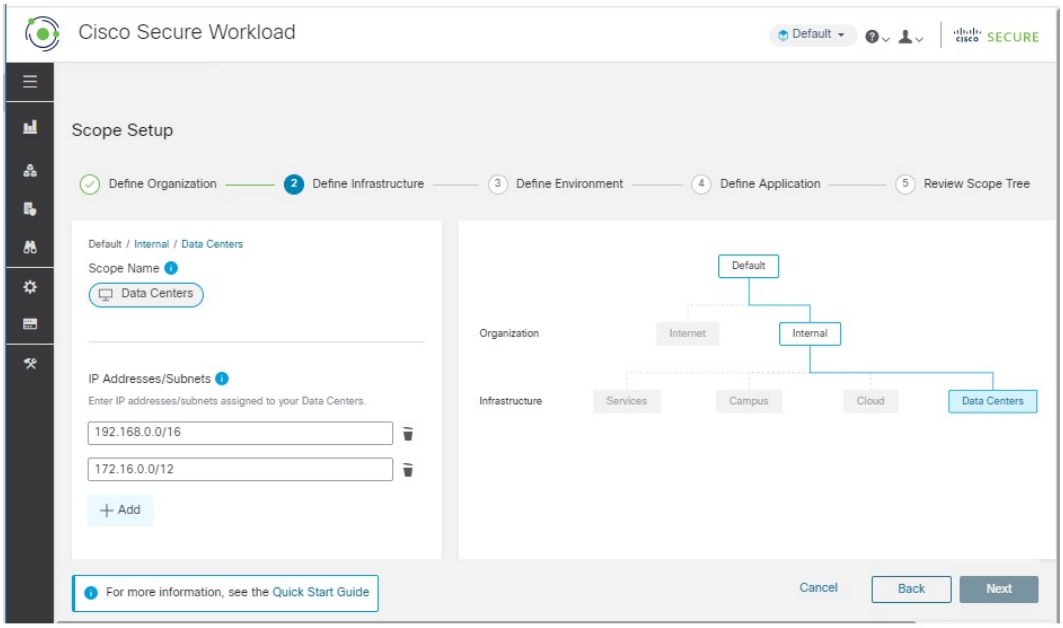
默认情况下，向导会在 RFC 1918 中定义的专用互联网地址空间中添加 IP 地址。

您现在不必添加内部网络中的所有 IP 地址，但必须包括与所选应用关联的 IP 地址，并且应尽可能多地添加其他地址。您可以稍后添加其余部分。

定义数据中心范围

此范围包括定义本地数据中心的 IP 地址。

您可以更改范围名称，但含义保持不变。范围名称应简短且有意义。



在此页面上，您输入的IP地址必须是您在上一页中输入的内部网络地址的子集。您还必须包括与所选应用关联的 IP 地址，理想情况下应包括代表数据中心工作负载的其他地址，但如果没有可用地址，也可以不使用这些地址。（如果您有多个数据中心，您会将所有这些数据中心都包括在此范围内，以便您可以定义一组策略。）您以后可以随时添加更多地址。

向导会分配标签

```
Organization = Internal
```

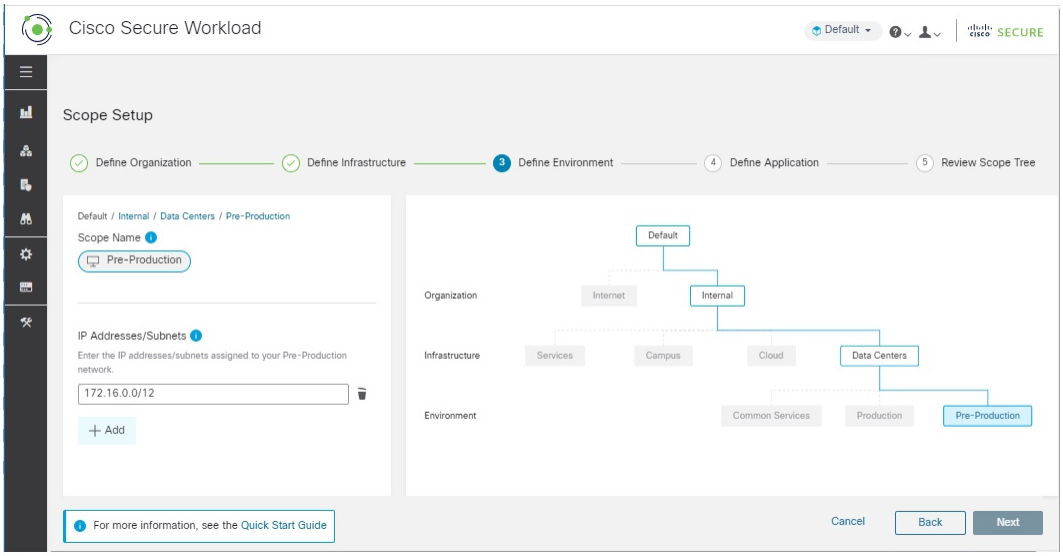
和

```
Infrastructure = Data Centers
```

到您输入的每个 IP 地址。

定义预生产范围

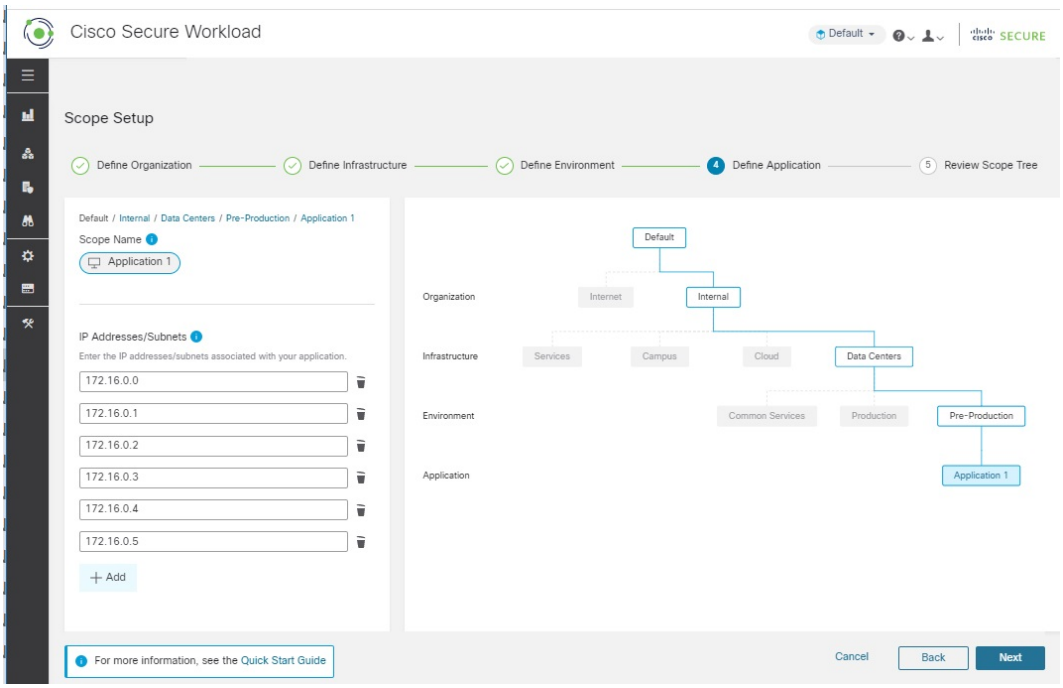
此范围包括非生产应用和主机的 IP 地址，例如开发、实验、测试或暂存系统。它不应包括您用于开展实际业务的任何应用的地址，这将是您稍后定义的生产范围的一部分。



您在此页面上输入的 IP 地址必须是您为数据中心输入的地址的子集，并且它们必须再次包含所选应用的地址。理想情况下，它们还应包括不属于所选应用的预生产地址。同样，您可以稍后添加更多地址。

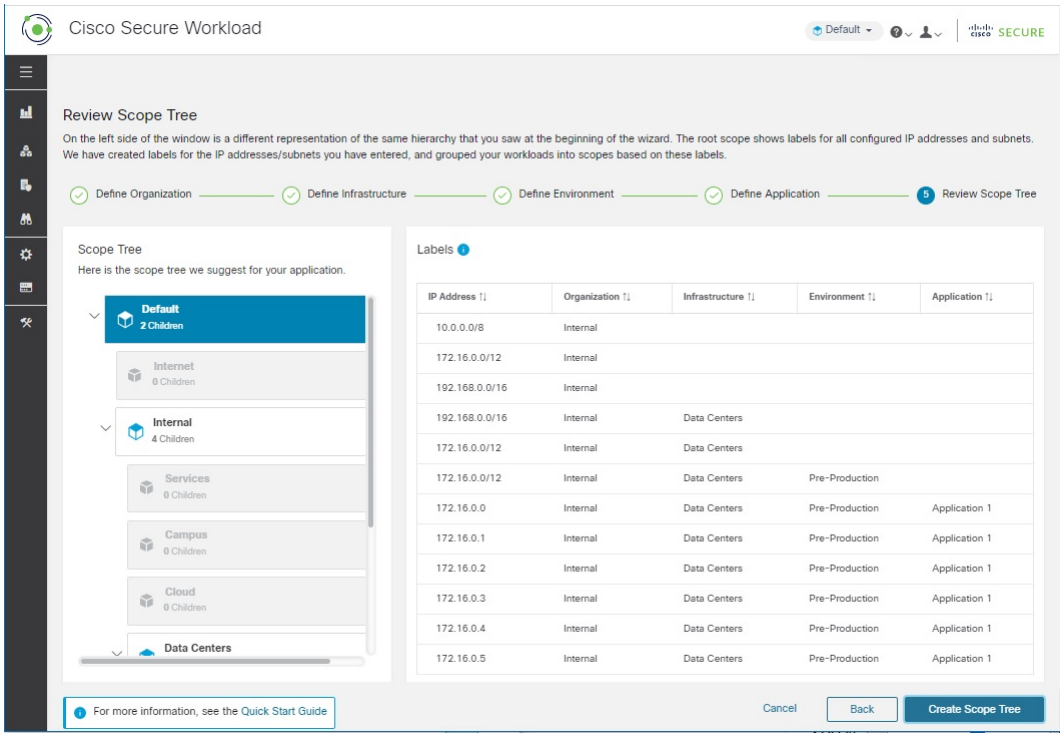
定义应用 1 的范围

“应用 1”是您选择的应用。请参阅 选择此向导的应用，第 9 页的指南。一个应用包含多个工作负载。



添加组成应用的工作负载的 IP 地址。例如，包括数据库、Web 服务、备份卷、高可用性部署中的备用实例等。您可以稍后添加更多地址，但现在应尝试包括大多数地址。

查看范围树、范围和标签



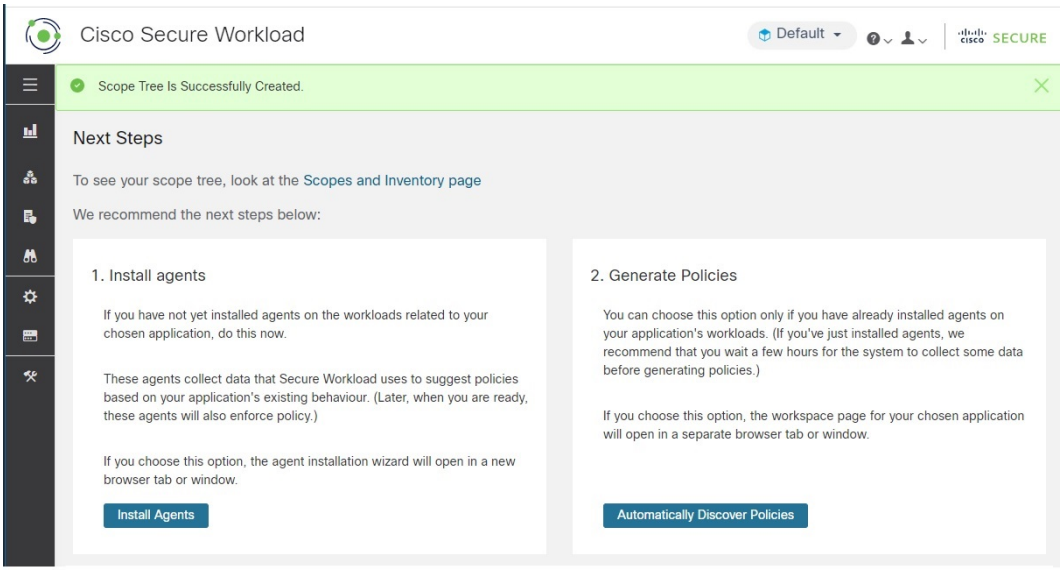
在左侧，您会看到其他页面上显示的同一范围树的不同表示。您可以展开和折叠分支，并向下滚动以点击特定范围。

在右侧，您会看到分配给您在左侧点击的范围内的工作负载的 IP 地址和标签。列标题是标签键，表格单元格显示标签值。

在上图中，选择了顶级范围，因此您可以看到在向导中指定的所有 IP 地址的数据。表中的空单元格正在等待未来标记，例如，不属于您的数据中心或属于非生产应用（所选应用除外）的工作负载。

如果要在退出向导后查看此信息，请从窗口左侧的菜单中选择 **组织 > 范围和资产** 。

“后续步骤”页面



安装席座

您应尽快在与所选应用关联的工作负载上安装 Cisco Secure Workload 席座。代理收集的数据用于根据网络上的现有流量生成建议的策略。更多的数据会产生更准确的策略。有关详细信息，请参阅在工作负载上安装席座，第 11 页。

生成策略

安装席座并允许至少几个小时的流量数据累积后，您可以告诉 C Secure Workload 根据该流量生成（“发现”）策略。有关详细信息，请参阅自动生成策略，第 12 页。

其他

如果您使用窗口左侧的导航栏，请务必在单独的窗口或选项卡中打开新页面，否则您将无法返回此页面。

快速入门工作流程

步骤	相应操作	详细信息
1	（可选）带注释的向导导览	向导之旅，第 2 页

步骤	相应操作	详细信息
2	选择要开始分段之旅的应用。	为获得最佳效果，请遵循选择此向导的应用，第 9 页中的准则。
3	收集 IP 地址	向导将请求 4 组 IP 地址。 有关详细信息，请参阅收集 IP 地址，第 9 页。
4	运行向导	要查看要求和访问向导，请参阅运行向导，第 10 页
5	在应用的工作负载上安装 Cisco Secure Workload 席座	请参阅 在工作负载上安装席座，第 11 页。
6	为席座留出时间收集流数据。	更多的数据会产生更准确的策略。 所需的最短时间取决于应用的使用情况。
7	根据实际流数据生成（“发现”）策略	请参阅 自动生成策略，第 12 页。
8	查看生成的策略	请参阅 查看生成的策略，第 13 页。

收集 IP 地址

您至少需要以下每个项目符号中的一些 IP 地址：

- 定义您的内部网络的地址

  默认情况下，向导使用为专用互联网保留的标准地址。

- 为数据中心保留的地址。

  这不包括员工计算机、云或合作伙伴服务、集中式 IT 服务等使用的地址。

- 定义非生产网络的地址
- 构成所选非生产应用的工作负载的地址

现在，您不需要拥有上述每个项目符号的所有地址；您可以稍后添加更多地址。

重要事项 由于4个项目符号中的每一个都代表其上方项目符号的IP地址子集，因此每个项目符号中的每个 IP 地址也必须包含在列表中其上方项目符号的 IP 地址中。

选择此向导的应用

对于此向导，您将选择要使用的单个应用。

应用通常由提供不同服务的多个工作负载组成，例如 Web 服务或数据库、主服务器和备份服务器等。这些工作负载共同为其用户提供应用的功能。

应用选择指南

Cisco Secure Workload 支持在各种平台和操作系统上运行的工作负载，包括基于云的工作负载和容器化工作负载。但是，为简单起见，对于此向导，您应选择具有以下工作负载的应用：

- 在您的数据中心运行
- 在裸机和/或虚拟机上运行
- 在 Cisco Secure Workload 席座支持的 Windows、Linux 或 AIX 平台上运行：

  请参阅 https://www.cisco.com/go/secure-workload/requirements/agents

  （在以后的步骤中，您需要在此应用的工作负载上安装席座）
- 部署在预生产环境中

运行向导

无论您是否选择了应用和收集的 IP 地址，都可以运行向导，但不执行这些操作将无法完成向导。

重要事项 如果在注销（或超时）Cisco Secure Workload 之前未完成向导，或者如果使用左侧导航栏导航到应用的其他部分，则不会保存向导配置。

开始之前

以下用户角色可以访问该向导：

- 站点管理员
- 客户支持
- 范围所有者

过程

步骤 1 登录 Cisco Secure Workload。

步骤 2 启动向导：

如果您当前未定义任何范围，则在您登录 Cisco Secure Workload 时会自动显示该向导。

或者：

- 点击任何页面顶部蓝色横幅中的 **立即运行向导** 链接。
- 从窗口左侧的主菜单中选择 **概述** 。

如果已创建范围，则无法再次访问该向导，除非您删除所有现有范围。为此，（可选）要重新开始，请重置范围树，第 14 页。

步骤 3 向导将解释您需要了解的内容。

不要错过以下有用的元素：

- 将鼠标悬停在向导中的图形元素上可阅读其说明。
- 点击任何链接和信息按钮（ⓘ）可获取重要信息。

后续步骤

提示 完成向导后，您可以转到 **组织 > 范围和资产**，查看并使用您使用向导创建的范围树。

为应用创建范围树的分支后，请执行以下步骤：

在工作负载上安装席座

要收集用于自动生成策略建议的流数据，请在工作负载上安装席座。稍后，这些席座可以实施策略，但 **在您告知他们之前，席座不会实施策略**。

您应尽快安装席座，以开始收集数据。更多的数据会产生更准确的策略建议。

在与所选应用相关的每个工作负载上安装席座。

除非有充分的理由，否则请使用默认设置。

如果需要有关席座安装的其他信息，请参阅 Cisco Secure Workload 联机帮助或用户指南中的“部署软件席座”一章。

开始之前

- 确保您将安装席座的所有工作负载都在受支持的平台上运行。请参阅 https://www.cisco.com/go/secure-workload/requirements/agents。
- 确保您有权在每个工作负载上安装席座。如果需要，请具有所需权限的人员执行此操作。

过程

步骤 1 点击向导中的 **安装席座** 按钮。

或者，您可以通过以下方式访问席座安装程序：

a) 登录 Cisco Secure Workload Web 门户。
b) 在左侧的导航栏中，选择 **管理 > 代理**。
c) 点击 **安装程序** 选项卡。

步骤 2 点击 **使用安装程序自动安装席座**，然后点击 **下一步**。

步骤 3 如果您在本地使用 Cisco Secure Workload：

如果您看到此选项：**您的席座将安装在哪个租户下？**：选择默认值，除非您有理由选择其他选项。

（仅当您使用本地 Cisco Secure Workload 时，才会看到此选项。）

步骤 4 跳过此选项：**您希望我们为此工作负载应用哪些标签？（可选）**。

步骤 5 选择运行应用的平台。

步骤 6 如果需要，请输入您的环境的 HTTP 代理。

步骤 7 如果需要，选择安装程序到期选项。

步骤 8 点击**下载设置**。

步骤 9 点击**下一步**。

步骤 10 按照安装前检查说明进行操作，然后点击 **下一步**。

步骤 11 按照安装说明进行操作。

除非有充分的理由去更改它们，否则请使用默认设置。

您不需要更改为安装程序脚本列出的任何标志。

步骤 12 点击**下一步**。

步骤 13 按照屏幕上的说明验证席座是否已成功安装。

步骤 14 在与您的应用关联的每个工作负载上安装席座。

自动生成策略

Cisco Secure Workload 根据您的工作负载与其他主机之间的现有流量生成（“发现”）策略。（策略发现功能以前称为“ADM”，因此您可能会看到或听到它的称呼。）准备就绪后，您可以修改、补充、分析并最终批准和实施这些策略。

注释 在您实施策略之前，不会实施策略。

开始之前

- 在应用的工作负载上安装席座
- 安装席座后，请留出一些时间来累积流数据。

过程

步骤 1 在快速启动向导的 **下一步** 页面上，点击 **自动生成策略**。

或者，您可以随时执行以下操作：

a) 从 Cisco Secure Workload 窗口的左侧选择 **防御 > 分段** 。

b) 在左侧窗格的范围树或范围列表中，向下滚动到应用的范围。

c) 点击该范围内的 **主** 。

（向导已为您的应用创建主工作空间。）

步骤 2 点击 **管理策略**。

步骤 3 点击 **发现发现策略**。

步骤 4 选择要包括的流数据的时间范围。

通常，数据越多，策略越准确。

步骤 5 点击 **发现策略**。

生成的策略将显示在此页面上。

下一步做什么

查看生成的策略，第 13 页。

查看生成的策略

查看已发现的策略。（如果您已离开该页面，可以按照 查看策略，第 13 页中的步骤返回该页面。）

这些策略是否有意义？标签应帮助您了解每个工作负载与之通信的主机类型。

您看到任何奥秘了吗？看看您是否可以找出神秘的工作负载或通信。

您可以请熟悉此应用的同事评估建议的策略。

随着流数据的积累，您应根据需要扩展配置的时间范围并再次发现策略，以生成处理流量的策略。

查看策略

如果您在启动策略发现后（或在任何其他时间）离开了策略页面，则可以通过转至与范围关联的应用工作区来查看生成的（“已发现的”）策略。

开始之前

发现策略。请参阅 自动生成策略，第 12 页。

过程

步骤 1 在左侧的导航栏中，选择 **防御 > 分段**。

步骤 2 在窗口左侧的范围列表中，滚动到要查看其策略的范围并点击。

步骤 3 点击要在其中查看策略的工作空间。

这可能是主工作空间或辅助工作空间，具体取决于您在启动策略发现时所在的工作空间。

步骤 4 点击 **管理策略**。

步骤 5 如果您没有看到策略建议列表，请点击 **绝对和默认策略**。

步骤 6 （可选）要查看不同工作空间版本（主要或辅助）中的策略，请使用页面顶部的下拉列表。

步骤 7 （可选）要查看其他范围的策略，请点击页面顶部的**工作空间**，然后点击左侧列表中的其他范围。

下一步做什么

有关要查找的内容，请参阅 查看生成的策略，第 13 页。

（可选）要重新开始，请重置范围树

您可以删除使用向导创建的范围、标签和范围树，也可以选择再次运行向导。

提示 如果您只想删除一些已创建的范围，并且不想再次运行向导，则可以删除单个范围，而不是重置整个树：点击要删除的范围，然后点击 **删除**。

开始之前

需要具有根范围的范围所有者权限。

如果您创建了其他工作空间、策略或其他依赖关系，请参阅 Cisco Secure Workload 中的用户指南，了解有关重置范围树的完整信息。

过程

步骤 1 从左侧的导航菜单中，选择 **组织 > 范围和资产** 。

步骤 2 点击树顶部的范围。

步骤 3 点击**重置**。

步骤 4 确认您的选择。

步骤 5 如果重置按钮更改为销毁待处理，您可能需要刷新浏览器页面。

更多信息

有关向导中概念的详细信息，请参阅：

- Cisco Secure Workload 中的联机帮助
- 适用于您的版本的 *Cisco Secure Workload* 用户指南 PDF，可从 https://www.cisco.com/c/en/us/support/security/tetration-analytics-g1/model.html获取：

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。