思科遥测代理

用户指南 2.0.1

目录

简介

本指南提供思科遥测代理 管理器 Web 界面的参考。

思科遥测代理 (本文中有时将其称为 CTB) 允许您从多个输入注入网络遥测数据，转换遥测数据格式，以及将该遥测数据转发到一个或多个目标。

受众

本指南面向负责维护网络遥测流量和监控网络遥测的人员。

配置辅助功能

为了能够配置可用的网站辅助功能，在使用思科遥测代理管理器 Web 界面时必须使用 Chrome 浏览器。以下是一些使用 Chrome 以外的浏览器所无法配置的可访问性功能的示例。(这份清单并不全面。)

具备以下功能：

- 突出显示网页上的每个项目
- 在紧凑选项卡栏中显示颜色
- 指定从不使用某些字体大小

常用缩写

本指南中运用了以下缩写：

缩写	说明
DMZ	非军事区(外围网络)
DNS	域名服务器
FC	流收集器
FS	流传感器
FTP	文件传输协议
Gbps	千兆位/秒
GB	千兆字节
HTTPS	超文本传输协议(安全)
ISE	身份服务引擎

缩写	说明
Mbps	兆位/秒
NAT	网络地址转换
网卡	网络接口卡
NTP	网络时间协议
PCIe	外围组件快速互连
SNMP	简单网络管理协议
SPAN	交换端口分析器
SSH	安全外壳
TAP	测试接入端口
UDPD	UDP 导向器
UPS	不间断电源
URL	统一资源定位器
USB	通用串行总线
VLAN	虚拟局域网
虚拟机	虚拟机

常用术语

本指南中出现了以下术语：

缩写	说明
目标	思科遥测代理转发遥测的位置。思科遥测代理支持多种类型的目标。
导出程序	客户网络上将流量转发到思科遥测代理上的输入的设备。导出程序通常由 IP 地址定义。

缩写	说明
输入	思科遥测代理从客户网络收集或接收遥测的方式。思科遥测代理支持多种类型的输入。
规则	用户定义的逻辑，用于告知思科遥测代理如何将遥测从单个输入转发到单个目标。
遥测	客户生成的用于分析目的的任何类型的数据。示例包括 UDP 数据包、IPFIX、系统日志和 JSON。

警报

当实体(任何已配置的目标、输入或代理节点)存在一个或多个警报时，关联的主菜单标题旁边会显示状态指示器以及编号。

此数字反映了该实体类别中包含警报的实体数量。“输入”(Inputs)页面的状态指示器按“输入”的三个子页面进一步细分：UDP 输入、虚拟私有云 (VPC) 流日志和 Microsoft 网络安全组 (NSG) 流日志。在每个页面上，存在问题的每个实体都会显示一个状态指示器。

当实体存在多个问题时(例如，目标同时无法访问且没有任何规则，或输入没有任何目标且处于非活动状态)，则思科遥测代理会将此视作一个问题。它不会根据现有问题的数量来计算问题数量。例如，如果实体有 5 个不同的问题，思科遥测代理会将它们视作 1 个问题，而不是 5 个问题。

概述

此页面提供思科遥测代理系统的配置设置、系统运行状况、主要指标和许可信息的快照。

访问概述页面

从思科遥测代理主菜单中选择**概述 (Overview)**，或者点击思科徽标（位于页面左上角）。

查看以下组件

输入

此组件可显示过去 24 小时的遥测的以下信息：

- 思科遥测代理中已配置的输入数量。
- 从所有输入接收的遥测数量。
- 平均值是根据最近 30 天的遥测计算得出的。
- 没有为其配置规则的输入的数量。此数字由**无目标 (No Destination)** 字段中的数字表示。
- 圆环图上的每个分段显示了从每个输入接收的遥测量。将光标悬停在此图表的某个部分上可以查看以下信息：
    - 输入名称
    - 过去 24 小时内从此特定输入接收的遥测量

目标

此组件可显示过去 24 小时的遥测的以下信息：

- 已在思科遥测代理中配置的目标数量。
- 发送到所有目标的遥测数量。
- 发送到所有目标的遥测数据的平均每日速率。平均值是根据最近 30 天的遥测计算得出的。
- 不接受发送给它们的遥测数据的目标数量（由“无法接通”(Unreachable) 字段中的数字表示）。点击此数字时，系统将打开“目标”(Destinations) 页面。此处会列出无法访问的目标列表。
- 圆环图上的每个分段显示了发送到每个目标的遥测量。将光标悬停在此图表的某个部分上可以查看以下信息：
    - 目标名称
    - 过去 24 小时内发送到此特定目标的遥测量

代理节点

此部分位于关联的集群名称下并按集群分组。如果不存在高可用性集群，则所有代理节点都将被分组到“无集群”(No Cluster) 子标题下。

- 每个圆弧都显示代理节点的接收速率相对于节点理论容量的百分比。圆弧以适用的颜色来标记。有关这些圆弧颜色的说明，请参阅下表。

颜色	定义
红色 (严重)	代理节点达到的容量百分比为 100%。
橙色 (警告)	代理节点达到的容量百分比为 80% 到 99.99%。
蓝色 (参考)	代理节点达到的容量百分比 <(小于) 80%。

- 要访问代理节点的页面，请点击节点的名称。
- 如果代理节点存在任何警报，它们将显示在节点下方。它们带有红色背景的白色 *X* 标记，并附有简短说明。

警报

“警报”(Alerts) 组件会列出最近发生但仍处于活动状态或已解决的 10 个警报。红色警报仍处于活动状态，灰色警报已解决。该列表从顶部的最新警报开始，到底部的最早的警报结束。要查看其他警报，请点击列表底部的**查看更多... (See more...)** 链接。

- 思科遥测代理中的未解决的警报数量和所有警报数量都会显示在此组件的右上角。
- 默认情况下，系统会显示所有未解决警报的列表。要查看所有警报的列表，请点击此组件右上角的“全部”(All) 过滤器选项。
- 在每个警报下是关于关联实体 (例如，代理节点或目标) 的信息以及警报发生的时间。
- 当警报不再有效 (已解决) 时，警报会
  - 变暗
  - 带有复选标记，以及
  - 注明解决问题的时间。
- 点击每个警报名称下显示的链接时，系统将打开关联的“代理节点”(Broker Node) 页面或“目标”(Destinations) 页面，具体取决于警报类型。

CPU

对于管理器节点和每个代理节点，此组件会显示过去 30 天的以下信息的遥测：

- 可用的 CPU 数量。
- 可用 CPU 的使用百分比(以条形颜色表示)。
- 每个代理节点按可用 CPU 数量计算的 1 分钟平均负载(要查看此数据,请将鼠标悬停在代理节点名称上)。

有关每个条形所显示颜色的说明,请参阅下表。

颜色	定义
红色(严重)	节点达到的最大 CPU 负载百分比为 100%。
橙色(警告)	节点达到的最大 CPU 负载百分比为 80% 到 99.99%。
蓝色(参考)	节点达到的最大 CPU 负载百分比 <(小于) 80%。

许可

此组件会显示过去 14 天的遥测。

- 蓝色虚线显示过去 7 天的平均每天 GB 数。要查看此数字,请将光标悬停在虚线上。此数字是发送到智能软件许可的授权编号,用于计算许可证费用,并且它将与“遥测代理智能许可”(Telemetry Broker Smart Licensing) 页面上显示的值匹配。
- 图表中的每个条形代表不同的一天。图表最右侧的条形表示前一天,然后向左可移动到之前的每一天。
- 要查看特定日期接收的确切 GB 量,请将光标悬停在相关栏上。这样还会显示与该栏关联的日期。
- 如果产品尚未注册,则右上角会显示警告,显示试用许可证到期前的剩余天数。

遥测流

此组件会显示过去 24 小时的遥测。

- 所有输入接收的不同类型的遥测(由图表左侧的遥测表示)并发送到所有目标(由右侧的遥测表示)。
- 要显示流的确切值,请将光标悬停在流上以打开其工具提示。
- 对于 SCA 目标,此处显示的遥测统计信息表示发送到 SCA 的未压缩数据。因此,这些统计信息可能与发送的实际遥测数据不成比例(在“目标”(Destinations) 组件中显示)。

指标

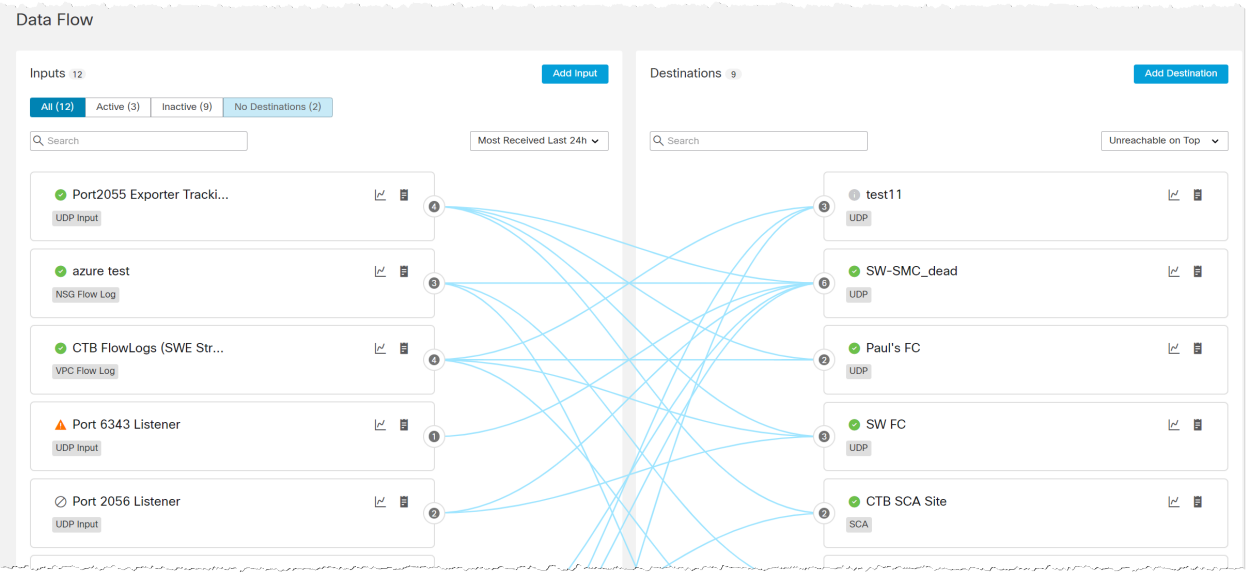
此组件中的表会显示过去 24 小时内的以下数据：

总接收速率 从所有输入接收的遥测总量。

总发送速率：发送到所有目标的遥测总量。

数据流

使用此页面可轻松查看已相互分配的输入和目标。请记住，可以将多个目标分配给 1 个输入，并且可以将 1 个目标分配给多个输入。在此页面上，您还可以查看警报、数据流信息以及与配置的输入和目标相关的其他详细信息。



查看数据流量

您看到的将各种输入连接到各种目标的线条表示这些特定输入和目标之间存在的规则。有关添加规则的信息，请参阅**目标**一章中的“为目标添加规则”部分。

您可以通过点击或将鼠标悬停在特定输入或目标的卡片上来查看该特定输入或目标的数据流。

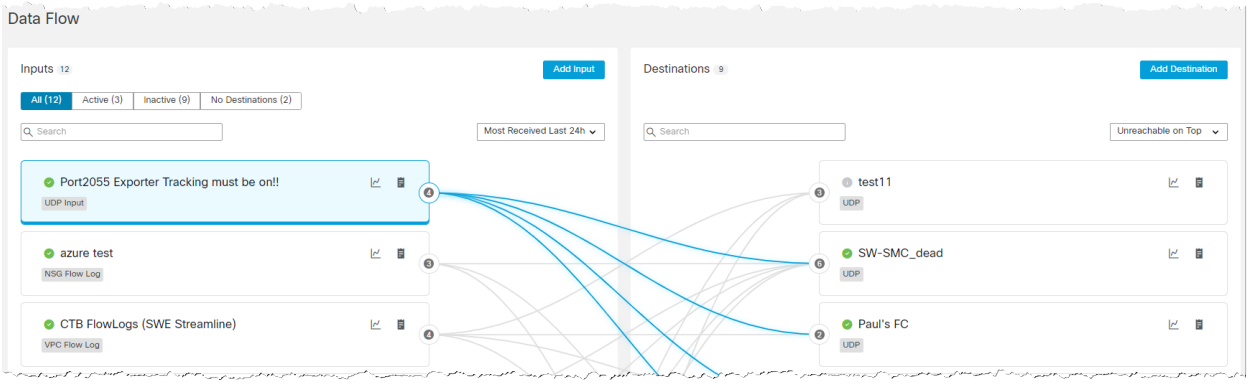
> 要取消选择某个卡片，请再次点击该卡片，或者点击该卡片外的任意位置（包括点击另一张卡片）。

请参阅下表，了解当点击与将光标悬停在卡片上时发生的视觉变化。这些视觉变化能让您更轻松地查看与所选卡片相关的信息。

点击与悬停

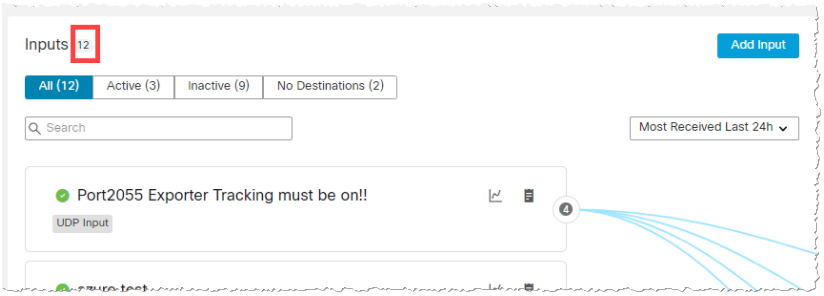
当您...	该...
点击卡片	• 卡片的边界变为深蓝色。 • 卡片内部变为浅蓝色。 • 该输入或目标的数据流行变为深蓝色。“数据流”(Data Flow) 页面上的所有其他行都变为灰色。
将光标悬停在卡片上	• 卡片的边界变为深蓝色。 • 卡片内部保持白色。 • 该输入或目标的数据流行变为深蓝色。“数据流”(Data Flow) 页面上的所有其他行保持浅蓝色。
点击卡片，然后将光标悬停在另一张卡片上	• 卡片的边界变为深蓝色。 • 卡片内部保持白色。 • 该输入或目标的数据流行变为深蓝色。“数据流”(Data Flow) 页面上的所有其他行都保持灰色。 • 您点击的卡片将保留其选定的状态。

Example: 在下图中，用户点击了“输入”(Inputs) 列表中的第一个输入卡。

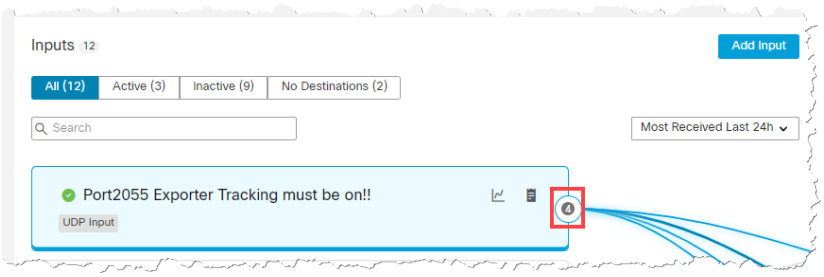


查看快照信息

已配置的输入和目标总数

要查看配置的总数...	请参阅旁边圆圈中的数字...
输入	“输入”(Inputs) 列表顶部的“输入”(Inputs) 标题。 
目标	“目标”(Destinations) 列表顶部的“目标”(Destinations) 标题。 

已分配的输入和目标总数

要查看总数...	请参阅关联的卡片上圆圈中的数字...
分配给特定输入的目标	“输入”(Input) 卡片。 
分配给特定目标的输入	目标卡片。 

数据流速率

要查看输入或目标的以下信息，请将光标悬停在 (**图表**) 图标上。系统将显示以下信息：

- 过去 24 小时内从此输入接收的所有遥测数据的接收速率。
- 过去 24 小时内发送到此目标的所有遥测数据的发送速率。

详细信息

要查看输入或目标的详细信息，请点击 (**详细信息**) 图标。

当您点击其中的**详细信息** 图标时

- 在输入卡片中点击，系统将打开该输入的输入 页面。
- 目标卡片，系统将打开该目标页面的目标页面。

警报和状态指示灯

要查看特定输入或目标的现有警报或状态指示器的说明，请将光标悬停在相关图标上。有关思科遥测代理警报列表，请参阅**附录 B: 支持的警报**。

搜索输入或目标

您可以使用以下任何实体来过滤搜索结果。

过滤按钮

您可以使用以下任何过滤器来过滤搜索结果：“全部”(All)、“活动”(Active)、“非活动”(Inactive) 和“无目标”(No Destination)(未分配给任何目标的输入)。要选择过滤器，请点击输入 列表顶部的关联按钮。

> 在使用一个或多个过滤器时，所有过滤器将用 AND 组合在一起；因此，所有返回的结果必须与所有过滤器中的搜索条件匹配。

搜索字段

在搜索字段中，键入要搜索的输入或目标的名称(取决于您所在的列表)。在您开始输入内容时，该字段会动态地进行过滤以显示包含您已输入的任何字符的条目列表。

请记住，您可以使用相同的名称来创建多个输入，反之亦然。代理节点之间的端口号也可以重复。因此，如果您搜索的输入或目标中存在多个同名输入或目标，或者搜索的端口号在两个或多个代理节点上存在重复，那么所有匹配条目都将在搜索处理完毕后显示在数据流页面上。

清除过滤器

- 如果您收到一个或多个结果，但没有看到您要搜索的任何结果，则可能是因为您配置了太多的过滤器。在这种情况下，我们建议您一次取消一个过滤器，以查看是否会显示任何预期的结果。
- 如果您没有看到任何结果，请点击**清除过滤器 (Clear Filters)** 并重新配置搜索条件。

排序方案

您可以使用这些下拉列表对输入列表和目标列表中的数据进行排序。

输入列表 在输入列表中，更改“最近 24 小时接收最多”(Most Received Last 24h) 下拉列表中的选项。其他选项如下：

- 最近查看
- 大部分目标
- 最高接收速率

目标列表：在目标列表中，可以更改位于顶部的无法访问下拉列表中的选项。其他选项如下：

- 最高发送速率
- 最近 24 小时发送最多
- 最近添加最多

添加输入

要添加输入，请点击输入列表右上角的**添加输入 (Add Input)**。

有关如何添加输入的信息，请参阅下面列出的适用主题（取决于您添加的输入类型）：

- **UDP 输入**
- **VPC 流日志**
- **NSG 流日志**

添加目标

要添加目标，请点击“目标”(Destinations) 列表右上角的**添加目标 (Add Destination)**。

有关如何添加目标的信息，请参阅**目标**。

目标

思科遥测代理 支持将遥测发送到以下类型的目标：

- **UDP 目标**：在特定 IP 地址和端口接收 UDP 数据的目标。
- **SCA 目标**：将数据指向客户拥有的 Cisco Secure Cloud Analytics 帐户的目标。

  配置 SCA 目标可能会对系统性能带来限制（就上传的 FPS 而言）。可能导致此问题的因素包括流记录的大小、这些流记录可实现的压缩，以及可用于从代理节点向Cisco Secure Cloud Analytics发送遥测的带宽。

  在大多数情况下，假设每个流记录少于 100 字节，则思科遥测代理应该能够发送：

  - 对于虚拟部署，每个代理节点为 40K FPS（假设每个代理节点有 8 个核心）。
  - 对于硬件部署 (M6)，每个代理节点为 300K FPS。

思科遥测代理 将遥测发送到目标。规则描述目标希望从特定遥测流接收的遥测。

思科遥测代理 “目标”页面显示所有目标的图形。对于每个远程目标，您可以查看以下信息：

- 目标名称
- IP 地址和端口（仅适用于 UDP 目标）
- 过去一天收到的遥测
- 如果目标正在主动接收遥测且可由管理器节点连通
- 将遥测数据发送到目标的输入和导出程序

在此页面中，您可以添加其他目标以及修改和更新它们。对于每个目标，您可以添加其他规则并从不同的遥测输入接收遥测。您可以为每个目标配置多个规则（每个规则 1 个遥测输入）。

连通性检查

“连通性检查”功能可在目标无法连通或无响应时向用户发出警报，这样用户就可以减轻因将遥测数据转发到不存在的目标而造成的任何网络破坏。

该功能生成零长度 UDP 数据包并将其发送到目标的已配置 UDP 端口。然后，代理节点侦听 ICMP 主机不可达或端口不可达响应，以确定目标是否不可达。缺少任何响应表示目标很可能正在接收遥测。

“连通性检查”功能仅适用于非 Cisco Secure Cloud Analytics 目标。您可以逐个目标禁用此功能。如果您的目标或防火墙规则配置将导致误报，请禁用此功能。

有关如何配置此设置的信息，请参阅**目标详细信息**中的以下主题：“添加 UDP 目标”或“配置连通性检查”主题。

有关如何配置思科遥测代理将遥测输入标记为非活动之前的时间量的信息，请参阅**常规**。

添加目标

添加 UDP 目标

1. 在页面的右上角，点击**添加目标 (Add Destination) > UDP 目标 (UDP Destination)**。
2. 输入目标**名称 (Name)**。
3. 输入此目标的**目标 IP 地址 (Destination IP Address)**和**目标 UDP 端口 (Destination UDP Port)**。
4. 如果要接收无法访问或无响应的目标的警报，请启用  (**连通性检查**)图标(启用后，该栏为蓝色)。有关连通性检查功能的详细信息，请参阅：
    - “连通性检查”功能仅适用于非 Cisco Secure Cloud Analytics 目标。
    - 如果您的目标或防火墙规则配置将导致误报，请禁用此功能。
5. 单击**保存 (Save)**。

添加Cisco Secure Cloud Analytics (SCA) 目标

- 在思科遥测代理中，您只能为每个系统添加 1 个 SCA 目标。
- 思科遥测代理会从 NetFlow V5、NetFlow V9 和 IPFIX 数据包中提取流数据，并将这些数据发送到Cisco Secure Cloud Analytics。
- 如果您的思科遥测代理部署包含少量遥测，则在添加 SCA 目标后，遥测最多可能需要 20 分钟才会显示在“目标”(Destinations) 页面上。

在添加 SCA 目标之前，需要获取 SCA 服务密钥和 SCA 主机 URL。Cisco Secure Cloud Analytics 会使用此密钥对思科遥测代理进行身份验证，而思科遥测代理会使用 URL 向 Cisco Secure Cloud Analytics 发送遥测。

找到密钥和 URL

1. 登录 Cisco Secure Cloud Analytics。
2. 从主菜单中，点击**设置 (Settings) > 传感器 (Sensor)**。
3. 找到并复制页面底部的服务密钥和服务主机。

添加 SCA 目标

1. 登录思科遥测代理。
2. 在页面的右上角，点击**添加目标 (Add Destination) > SCA 目标 (SCA Destination)**。
3. 输入目标**名称 (Name)**。
4. 输入 **SCA 服务密钥 (SCA Service Key)**。确保粘贴整个密钥。
5. 输入**SCA 主机 URL (SCA Host URL)**。确保粘贴整个 URL。
6. 单击**保存 (Save)**。

在将 Cisco Secure Cloud Analytics 配置为思科遥测代理目标后，您应该能够在 30 分钟内在 Cisco Secure Cloud Analytics 事件查看器中看到来自思科遥测代理的遥测。如果未显示，请联系 swatchc-support@cisco.com 并提供您的门户 URL 以获取帮助。

编辑目标

1. 在包含适用目标的行中，点击 （**编辑**）图标。
2. 在打开的“编辑目标”(Edit Destination) 对话框中，更新以下字段：
   - 对于 UDP 目标：**目标名称 (Destination Name)** 和**检查目标可用性 (Check Destination Availability)** 切换开关。您无法编辑“目标 IP 地址”(Destination IP Address) 和“目标 UDP 端口”(Destination UDP Port) 字段。
   - 对于 SCA 目标：**目标名称 (Destination Name)**、**SCA API 密钥 (SCA API Key)** 和 **SCA URL**。
3. 单击**保存 (Save)**。

删除目标

删除目标时，该目标仍会出现在指标图形中供选择，但与其关联的名称是术语“目标” (Destination)，后跟目标的 ID 和短语“已删除”(deleted)。例如，目标 (ID 10) 已删除 (Destination (ID 10) deleted)。只要该目标的数据存在，图形仍会包含该目标的数据。数据到期后，无法再从任何“按目标”(Per Destination) 下拉列表（位于“代理节点”(Broker Nodes) 页面）中选择关联的目标。

要删除目标，请完成以下步骤：

1. 在包含适用目标的行中，点击 （**删除**）图标。
2. 在打开的“删除目标”(Remove Destination) 对话框中，点击**删除 (Remove)**。

为目标添加规则

规则始终仅包含 1 个输入和 1 个目标。但请注意，输入可以将数据发送到多个特定目标。您只用创建另一个规则来执行此操作。

1. 在右下角包含适用目标的行中，点击**+ 添加规则 (+ Add Rule)**。
2. 从**选择输入 (Select Input)** 下拉列表中选择所需的输入名称。
3. （视情况而定）如果选择 UDP 输入，系统将打开**根据这些子网接收的数据 (Track data received against these subnets)** 字段。此字段用作过滤机制，用于确定将哪些流量发送到目标。仅转发来自指定子网中的导出程序 IP 的流量。输入此目标将通过其接收适用遥测的子网。使用逗号分隔条目。

   如果将**根据这些子网接收的数据 (Track data received)** 字段留空，则默认为包含所有流量的单个子网。

   - 对于 IPv4 IP 子网，CIDR IP 地址范围为 0.0.0.0/0。
   - 对于 IPv6 IP 子网，CIDR IP 地址范围为 ::/0。
4. 点击**添加规则 (Add Rule)**。

查看目标的详细信息

您可以查看有关特定目标的更多详细信息。要执行此操作，请点击位于其行左上角的所需目标名称。有关此页面的信息，请参阅下一部分**目标详细信息**。

目标详细信息

您可以在此页面上查看有关特定目标的更多详细信息。要查看目标的详细信息，请执行以下操作：

- 在“目标”(Destinations) 选项卡上，点击位于其行左上角的所需目标名称。

  系统将打开该目标的“目标详细信息”(Destination Details) 页面。

在此页面上，您可以查看以下信息：

- 目标名称、IP 地址和接收遥测的端口（仅适用于 UDP 目标）。
- 目标类型（仅适用于 SCA 目标）。
- 目标的状态及其上次接收遥测的时间。
- 此目标从其接收遥测的遥测输入数量。
- 从思科遥测代理接收的字节数及其接收速率（以位/秒为单位）。
- 为该目标配置的规则，以及每条规则的详细信息，包括为向特定输入发送数据而配置的导出程序数量，可配置为单个节点或多个节点。（此数字显示在“规则”(Rules) 表的“导出程序”(Exporters) 列中。）

  请注意，此数字不一定与“输入详细信息”(Input Details) 页面上显示的数字相对应（在“导出程序”(Exporters) 部分左上角的“导出程序”(Exporters) 标题后面的括号内）。这也是为向特定输入发送数据而配置的唯一导出程序数量。请参阅以下内容以确定这些数字是否匹配：

  - 如果已将单个导出程序配置为将数据发送到在同一输入下配置的单个节点，则这些数字将匹配。
  - 如果单个导出程序被配置为向同一输入下配置的 2 个节点发送数据，则“目标详细信息”(Destinations Details) 页面上的数字将是“输入详细信息”(Input Details) 页面上数字的两倍。
  - 如果单个导出程序被配置为向同一输入下配置的 3 个节点发送数据，则“目标详细信息”(Destinations Details) 页面上的数字将是“输入详细信息”(Input Details) 页面上数字的三倍，以此类推。

很少发生这些数字不匹配的情况。为避免此问题，我们建议您仅配置具有一个代理节点或一个集群的输入。相反，您可以创建两个单独的 UDP 输入，让它们侦听同一个 UDP 端口，但分配给不同的代理节点或集群。

指标：发送速率

在“指标”(Metrics) 部分中，您将看到“发送速率”(Sent Rate) 表。此表显示了一段时间内输入发送到此目标的遥测信息，您可以使用以下过滤器来过滤遥测信息（您可以从每个下拉列表中选择多个选项）：

对于 SCA 目标，您可以只按代理节点或按接收总量来过滤该表中的遥测数据。

- 按遥测类型
- 按输入
- 按导出程序
- 按代理节点
- 总计

您可以通过点击“指标”(Metrics) 表右上角的以下任意所需时间范围来查看多个时间范围内的这些指标：

- 最近一小时
- 过去 4 小时
- 最后一天
- 最近一周
- 最近一个月

配置连通性检查

如果要接收无法访问或无响应的目标的警报，请在页面的右上角启用 （**连通性检查**）图标（启用后，该栏为蓝色）。有关连通性检查功能的详细信息，请参阅目标中的“连通性检查”部分。

- “连通性检查”功能仅适用于非 Cisco Secure Cloud Analytics 目标。
- 如果您的目标或防火墙规则配置将导致误报，请禁用此功能。

编辑目标

1. 在页面的右上角，点击 （**编辑目标**）图标。
2. 在打开的“编辑目标”(Edit Destination) 对话框中，更新以下字段：

- 对于 UDP 目标：**目标名称 (Destination Name)** 和**检查目标可用性 (Check Destination Availability)** 切换开关。您无法编辑“目标 IP 地址”(Destination IP Address) 和“目标 UDP 端口”(Destination UDP Port) 字段。
- 对于 SCA 目标：**目标名称 (Destination Name)**、**SCA API 密钥 (SCA API Key)** 和 **SCA URL**。

3. 单击**保存 (Save)**。

删除目标

删除目标时，该目标仍会出现在指标图形中供选择，但与其关联的名称是术语“目标”(Destination)，后跟目标的 ID 和短语“已删除”(deleted)。例如，目标 (ID 10) 已删除 (Destination (ID 10) deleted)。只要该目标的数据存在，图形仍会包含该目标的数据。数据到期后，无法再从任何“按目标”(Per Destination) 下拉列表（位于“代理节点”(Broker Nodes) 页面）中选择关联的目标。

要删除目标，请完成以下步骤：

1. 在页面的右上角，点击 **（删除目标）** 图标。
2. 在打开的“删除目标”(Remove Destination) 对话框中，点击**删除 (Remove)**。

为目标添加规则

规则始终仅包含 1 个输入和 1 个目标。但请注意，输入可以将数据发送到多个特定目标。您只用创建另一个规则来执行此操作。

1. 在规则部分中，点击 **+ 添加规则 (+ Add Rule)**。
2. 从**选择输入 (Select Input)** 下拉列表中选择所需的输入名称。
3. （视情况而定）如果选择 UDP 输入，系统将打开**根据这些子网接收的数据 (Track data received against these subnets)** 字段。此字段用作过滤机制，用于确定将哪些流量发送到目标。仅转发来自指定子网中的导出程序 IP 的流量。输入此目标将通过其接收适用遥测的子网。使用逗号分隔条目。

   如果将**根据这些子网接收的数据 (Track data received)** 字段留空，则默认为包含所有流量的单个子网。

   - 对于 IPv4 IP 子网，CIDR IP 地址范围为 0.0.0.0/0。
   - 对于 IPv6 IP 子网，CIDR IP 地址范围为 ::/0。

4. 点击**添加规则 (Add Rule)**。

输入

思科遥测代理 支持从以下类型的输入发送遥测：

- **UDP 输入 (UDP Inputs)**：使用 UDP 遥测并将其发送到目标的输入。
- **VPC 流日志 (VPC Flow Logs)**：使用 s3 存储桶中的 Amazon Web 服务 (AWS) VPC 流日志、将其转换为 IPFIX 并将 IPFIX 发送到您的目标的输入。
- **NSG 流日志 (NSG Flow Logs)**：使用来自 Azure 存储帐户的 Azure NSG 流日志的输入，将其转换为 IPFIX，并将 IPFIX 发送到您的目标。

要访问各种输入选项卡，请从思科遥测代理主菜单中选择**输入 (Inputs)**。

> ⚠ 要开始收集遥测，您首先需要在思科遥测代理中创建一个或多个输入。

您需要根据希望让思科遥测代理处理的遥测类型来配置输入。例如，如果您有兴趣在所有代理节点上的端口 2055 上收集 UDP 数据包，则应创建一个配置为在端口 2055 上侦听的 UDP 输入。或者，如果您只对处理 VPC Flowlog 遥测感兴趣，则应创建 VPC Flowlog 输入。

查看输入

1. 从思科遥测代理主菜单中选择**输入 (Inputs)**。
2. 点击适用的选项卡以查看以下任意项：
    - **UDP 输入**
    - **VPC 流日志**
    - **NSG 流日志**

UDP 输入

思科遥测代理 让您可以将 UDP 输入配置为在特定 UDP 端口上侦听传入 UDP 遥测。您可以在“输入”(Input) 选项卡上查看以下信息：

- 输入的遥测名称、输入端口和类型
- 输入的状态及其上次接收遥测的时间
- 已分配的代理节点和集群
- 为此输入配置的目标数量
- 过去 24 小时接收的字节数和速率（以每秒字节数为单位）

您可以按不同的条件过滤此遥测。只需从页面顶部的下拉菜单中选择以下条件类型之一：

- 接收最多的最近24小时
- 最近查看

- 大部分目标
- 最高接收速率

在“搜索”(Search) 字段中，占位符文本会通知您可以执行搜索的列。在您开始输入内容时，该表会动态地进行过滤以显示包含您已输入的字符的条目列表。

添加 UDP 输入

1. 在“输入”(Inputs) 选项卡上，点击 **UDP 输入 (UDP Inputs)** 选项卡。
2. 在页面的右上角，点击**添加 UDP 输入 (Add UDP Input)**。

   “添加用户”(ADD UDP Input) 对话框将打开。
3. 在“UDP 端口”(UDP Port) 字段中，输入将侦听 UDP 遥测的 UDP 端口。
4. 在 UDP 输入名称中，输入此输入的名称。
5. 思科遥测代理 跟踪将遥测发送到 UDP 输入的每个导出程序。但是，当有许多唯一的导出程序向单个 UDP 输入发送遥测时，您可能需要禁用导出程序跟踪，以确保系统不会出现性能问题。

   要禁用导出程序跟踪，请在“添加 UDP 输入”(Add UDP Input) 对话框（步骤 2 中打开的对话框）中选中**禁用导出程序跟踪 (Disable Exporters Tracking)** 复选框。如果禁用了导出程序跟踪，将不再为每个导出程序计算指标。但是，您仍然可以查看还是在由 UDP 输入处理的汇聚指标，但您的系统会受到以下限制：

   - **“输入详细信息”(Input Details) 页面** “导出程序”(Exporters) 部分不再显示每个导出程序的指标。（点击“UDP 输入”(UDP Inputs) 选项卡上的输入名称时，系统就会打开此页面。）但是，它将显示为关联输入配置的每个代理节点所看到的导出程序数量。
   - **代理节点详细信息 (Broker Nodes Details) 页面** “接收速率”(Received Rate) 图形的“按导出程序”(Per Exporter) 下拉列表不再包含来自已禁用导出程序跟踪的任何 UDP 输入的导出程序。（当您点击“代理节点”(Broker Nodes) 选项卡上的代理节点名称时，系统就会打开此页面。）

> 有关导出程序跟踪的详细信息，请参阅 **UDP 输入详细信息**中的“导出程序”部分。

5. 在“分配 HA 集群”(Assign HA Clusters) 部分中，选中要添加此输入的 HA 集群的相应复选框。
6. 在“分配代理节点”(Assign Broker Nodes) 部分中，选中要添加此输入的节点的相应复选框。

> 如果节点包含在此对话框的“分配 HA 集群”(Assign HA Cluster) 部分的“HA 集群”(HA Cluster) 选项中，则不会在“分配代理节点”(Assign Broker Nodes) 部分中列出，反之亦然。

7. 单击**保存 (Save)**。

编辑 UDP 输入

1. 在包含适用 UDP 输入的行中，点击 （**编辑**）图标。
2. 在打开的“编辑 UDP 输入”(Edit UDP Input) 对话框中，进行编辑，然后点击**保存 (Save)**。

删除 UDP 输入

删除输入时，思科遥测代理会停止在指定端口上接收遥测，同时删除与此输入关联的任何规则。

该输入仍可在指标图形中选择，但与其关联的名称是术语“输入”(Input)，后跟输入的 ID 和短语“已删除”(deleted)。例如，“输入 (ID 10) 已删除”(Input (ID 10) deleted)。只要已删除的输入的数据存在，图仍会包含该输入的数据。数据到期后，将无法再从任何“按输入”(Per Input) 下拉列表（位于“目标”(Destinations) 和“代理节点”(Broker Nodes) 页面）中选择关联的输入。

要删除 UDP 输入，请完成以下步骤：

1. 在包含适用 UDP 输入的行中，点击 （**删除**）图标。
2. 在“删除 UDP 输入”(Remove UDP Input) 对话框中，点击**删除 (Remove)**。

查看 UDP 输入的详细信息

您可以查看有关特定 UDP 输入的更多详细信息。要执行此操作，请在包含相应 UDP 输入的行中，点击输入名称。有关此页面的信息，请参阅下一部分 **UDP 输入详细信息**。

UDP 输入详细信息

在此页面上，您可以查看有关 UDP 输入的更多详细信息。要查看 UDP 输入的详细信息，请执行以下操作：

- 在“UDP 输入”(UDP Inputs) 选项卡上，在包含相应 UDP 输入的行中，点击输入名称。

  系统将打开该输入的“UDP 输入详细信息”(UDP Input Details) 页面。

在此页面上，您可以查看以下信息：

常规

- UDP 输入的显示名称、接收 UDP 端口及其分配的代理节点和集群
- UDP 输入的状态（指示此 UDP 输入的端口当前是否正在接收遥测）
- 分配给 UDP 输入的目标数量
- 过去 24 小时从思科遥测代理接收的字节数和速率（以每秒字节数为单位）

规则

分配给此 UDP 输入的规则列表，包括每个规则中目标的 IP 地址和端口。请注意，与 SCA 目标关联的规则不会列出 IP 地址。

导出程序

您可以查看有关分配给特定端口的各个导出程序的以下信息：

- 为向特定输入发送数据而配置的唯一导出程序数量。该数字显示在“导出程序”(Exporters) 部分左上角“导出程序”(Exporters) 标题后面的括号中。
- 导出程序名称。
- 接收的遥测类型。
- 导出程序的状态（指示此 UDP 输入的端口当前是否正在接收来自导出程序的遥测）。
- 分配给导出程序的目标数量。
- 过去 24 小时接收的字节数和速率（以每秒字节数为单位）

在“搜索”(Search) 字段中，占位符文本会通知您可以执行搜索的实体。在您开始输入内容时，该表会动态地进行过滤以显示包含您已输入的字符的条目列表。

思科遥测代理 跟踪将遥测发送到 UDP 输入的每个导出程序。但是，当有许多唯一的导出程序向单个 UDP 输入发送数据时，您可能需要禁用导出程序跟踪，以确保系统不会出现性能问题。

要禁用导出程序跟踪，请选中**禁用导出程序跟踪 (Disable Exporters Tracking)** 复选框。

如果禁用了导出程序跟踪，将不再为每个导出程序计算指标。但是，您仍然可以查看还是在由 UDP 输入处理的汇聚指标，但您的系统会受到限制。有关这些限制的信息，请参阅 **UDP 输入**中的添加 UDP 输入部分。

虽然不再为每个导出程序计算指标，但只要存在为保留间隔设置的时间的数据，该导出程序的数据仍会显示。

Example: 保留间隔为 8 天。导出程序在 8 月 10 日停止发送数据，因此它将保留 8 月 10 日至 18 日的数据。今天是 8 月 20 日。

- 如果您过滤 7 天或 30 天的图表，则该图表将继续显示该导出程序的数据，因为 8 月 10 日至 18 日属于 7 至 30 天前的日期。
- 如果您过滤 4 小时或 24 小时的图表，则该图表不会再显示该导出程序的数据，因为 8 月 10 日至 18 日不在过去 48 小时内。

指标：接收速率

在“指标”(Metrics) 部分中，您将看到“接收速率”(Received Rate) 表。此表显示目标在一段时间内从此 UDP 输入收到的遥测数据，您可以使用以下过滤器来过滤遥测数据。您可以从每个下拉列表中选择多个选项。

- 按导出程序
- 按代理节点

您可以通过点击“指标”(Metrics) 表右上角的以下任意所需时间范围来查看多个时间范围内的这些指标：

- 最近一小时
- 过去 4 小时
- 最后一天
- 最近一周
- 最近一个月

编辑 UDP 输入

1. 在页面的右上角，点击  (**编辑 UDP 输入**) 图标。
2. 在打开的“编辑 UDP 输入”(Edit UDP Input) 对话框中，进行编辑，然后点击**保存 (Save)**。

> 您无法编辑 UDP 端口。

删除 UDP 输入

删除输入时，思科遥测代理会停止在指定端口上接收遥测，同时删除与此输入关联的任何规则。

该输入仍可在指标图形中选择，但与其关联的名称是术语“输入”(Input)，后跟输入的 ID 和短语“已删除”(deleted)。例如，“输入 (ID 10) 已删除”(Input (ID 10) deleted)。只要已删除的输入的数据存在，图仍会包含该输入的数据。数据到期后，将无法再从任何“按输入”(Per Input) 下拉列表 (位于“目标”(Destinations) 和“代理节点”(Broker Nodes) 页面) 中选择关联的输入。

要删除 UDP 输入，请完成以下步骤：

1. 在页面的右上角，点击  (**删除 UDP 输入**) 图标。
2. 在打开的“删除 UDP 输入”(Remove UDP Input) 对话框中，点击**删除 (Remove)**。

VPC 流日志

思科遥测代理 使您能够配置 VPC 流日志输入，以使用 s3 存储桶中的 AWS VPC 流日志，将其转换为 IPFIX，并将 IPFIX 发送到您的目标。您可以从“VPC 流日志”(VPC Flow Logs) 选项卡上的表中管理这些输入，您可以在其中查看系统中的每个现有输入和相关信息，包括以下内容：

- 输入名称、IPv4 或 IPv6 地址以及 S3 存储桶名称
- 输入的状态及其上次接收遥测的时间
- 已分配的代理节点和集群
- 为此输入配置的目标数量
- 过去 24 小时接收的字节数和速率 (以每秒字节数为单位)

您可以在以下时间范围内查看此遥测。从页面右上角的下拉菜单中选择选项。

- 接收最多的最近24小时
- 最近查看
- 大部分目标
- 最高接收速率

在“搜索”(Search)字段中，占位符文本会通知您可以执行搜索的列。在您开始输入内容时，该表会动态地进行过滤以显示包含您已输入的字符的条目列表。

添加并编辑 VPC 流日志

有关如何添加和编辑 VPC Flog 日志的信息，请参阅**集成**部分。

编辑 VPC 流日志

1. 在包含适用 VPC 流日志的行中，点击 （**编辑**）图标。
2. 在打开的“编辑 VPC 流日志”(Edit VPC Flow Log) 对话框中，进行编辑，然后点击**保存 (Save)**。

删除 VPC 流日志

1. 在包含适用 NSG 流日志的行中，点击 **（删除）**图标。
2. 在“删除 VPC 流日志”(Remove VPC Flow Log) 对话框中，点击**删除 (Remove)**。

查看 VPC 流日志的详细信息

您可以查看有关特定 VPC 流日志的更多详细信息。要执行此操作，请在包含相应 VPC 流日志的行中点击流日志名称。有关此页面的信息，请参阅下一部分 **VPC 流日志详细信息**。

VPC 流日志详细信息

在此页面上，您可以查看有关 VPC 流日志的更多详细信息。要查看 VPC 流日志的详细信息，请执行以下操作：

- 在“VPC 流日志”(VPC Flow Logs) 选项卡上，在包含相应 VPC 流日志的行中点击输入名称。

  系统将打开该流的“VPC 流日志详细信息”(NSG Flow Log Details) 页面。

在此页面上，您可以查看以下信息：

常规

可以查看以下信息：

- 输入名称、S3 存储桶、区域以及用于接收遥测的已分配代理节点（如果适用）
- 输入的状态及其上次接收遥测的时间
- 为此输入配置的目标数量
- 过去 24 小时接收的字节数和速率（以每秒字节数为单位）

规则

分配给此 VPC 流日志的规则列表，包括每个规则中目标的 IP 地址和端口。请注意，与 SCA 目标关联的规则不会列出 IP 地址。

指标：接收速率

在“指标”(Metrics) 部分中，您将看到“接收速率”(Received Rate) 表。此表显示目标在一段时间内从此 VPC 流日志收到的遥测数据，您可以使用以下过滤器来过滤遥测数据。您可以从每个下拉列表中选择多个选项。

- 按代理节点
- 以下不同时间范围内的接收速率：
  - 最近一小时
  - 过去 4 小时
  - 最后一天
  - 最近一周
  - 最近一个月

编辑 VPC 流日志

1. 在页面的右上角，点击 （**编辑 VPC 流日志**）图标。
2. 在打开的“编辑 VPC 流日志”(Edit VPC Flow Log) 对话框中，进行编辑，然后点击**保存 (Save)**。

删除 VPC 流日志

1. 在页面的右上角，点击 （**删除 VPC 流日志**）图标。
2. 在打开的“删除 VPC 流日志”(Remove VPC Flow Log) 对话框中，点击**删除 (Remove)**。

NSG 流日志

思科遥测代理 使您能够配置 NSG 流日志输入，以使用 Azure 存储帐户中的 Azure NSG 流日志，将其转换为 IPFIX，并将 IPFIX 发送到您的目标。您可以从“NSG 流日志”(NSG Flow Logs) 选项卡上的表中管理这些输入，您可以在其中查看系统中的每个现有输入和相关信息，包括以下内容：

- 输入名称、IPv4 或 IPv6 地址和 Blob 服务 SAS URL
- 输入的状态及其上次接收遥测的时间
- 已分配的代理节点和集群
- 为此输入配置的目标数量
- 过去 24 小时接收的字节数和速率（以每秒字节数为单位）

您可以在以下时间范围内查看此遥测。从页面右上角的下拉菜单中选择选项。

- 接收最多的最近24小时
- 最近查看
- 大部分目标
- 最高接收速率

在“搜索”(Search)字段中，占位符文本会通知您可以执行搜索的列。在您开始输入内容时，该表会动态地进行过滤以显示包含您已输入的字符的条目列表。

添加 NSG 流日志

> ⚠ 在本部分中，我们假设您已将 Azure 账户设置为启用 NSG 流日志。有关配置 Azure 帐户的说明，请参阅 **Azure 配置**。

1. 在“输入”(Inputs)页面上，点击 **NSG 流日志** 选项卡。
2. 在页面的右上角，点击**添加 NSG 流日志 (Add NSG Flow Log)**。
3. 在 **Blob 服务 SAS URL (Blob Service SAS URL)** 字段中，输入为 Azure 账户配置 NSG 流日志时获取的 Azure sas_url。
4. 在**输入名称 (Input Name)** 字段中，输入输入 IP 地址名称。
5. 在**输入 IP 地址 (Input IP Address)** 字段中，输入要分配给此流日志的输入 IP 地址。在发送从 NSG 流日志生成的 IPFIX 时，思科遥测代理将使用此 IP 地址作为输入地址。它应该是内部 IP 地址，并且不应与网络上的其他 IP 地址冲突。

   思科遥测代理对输入 IP 地址值设置了以下限制，以确保正确代理数据包。如果不满足以下任何条件，思科遥测代理将显示以下错误消息：

   - 输入 IP 地址不得与已分配节点的遥测接口的子网重叠。
   - 输入 IP 地址不得与系统中的任何现有输入 IP 地址冲突。
   - 输入 IP 地址不得与系统中的任何目标 IP 地址冲突。
6. 从**分配的代理节点 (Assigned Broker Node)** 下拉列表中选择分配的代理节点。此代理节点处理来自存储帐户的所有流日志遥测。
7. 选择一个或多个目标以获取流日志遥测。请注意思科遥测代理会将 NSG 流日志转换为 IPFIX。
8. 单击**保存 (Save)**。

编辑 NSG 流日志

在包含适用 NSG 流日志的行中，点击 （**编辑**）图标。

在打开的“编辑 NSG 流日志”(Edit NSG Flow Log)对话框中，进行编辑，然后点击**保存 (Save)**。

删除 NSG 流日志

在包含适用 NSG 流日志的行中，点击 **（删除）**图标。

在“删除 NSG 流日志”(Remove NSG Flow Log) 对话框中，点击**删除 (Remove)**。

查看 NSG 流日志的详细信息

您可以查看有关特定 NSG 流日志的更多详细信息。要执行此操作，请在包含相应 NSG 流日志的行中点击流日志名称。有关此页面的信息，请参阅下一部分 **NSG 流日志详细信息**。

NSG 流日志详细信息

在此页面上，您可以查看有关 NSG 流日志的更多详细信息。要查看 NSG 流日志的详细信息，请执行以下操作：

- 在“NSG 流日志”(NSG Flow Logs) 选项卡上，在包含相应 NSG 流日志的行中点击输入名称。

  系统将打开该流日志的“NSG 流日志详细信息”(NSG Flow Log Details) 页面。

在此页面上，您可以查看以下信息：

常规

可以查看以下信息：

- 输入名称、Blob 服务 SAS URL、URL 到期日期以及用于接收遥测的已分配代理节点（如果适用）
- 输入的状态及其上次接收遥测的时间
- 为此输入配置的目标数量
- 过去 24 小时接收的字节数和速率（以每秒字节数为单位）

规则

分配给此 NSG 流日志的规则列表，包括每个规则中目标的 IP 地址和端口。请注意，与 SCA 目标关联的规则不会列出 IP 地址。

指标：接收速率

在“指标”(Metrics) 部分中，您将看到“接收速率”(Received Rate) 表。此表显示目标在一段时间内从此 NSG 流日志收到的遥测数据，您可以使用以下过滤器来过滤遥测数据。您可以从每个下拉列表中选择多个选项。

- 按代理节点
- 以下不同时间范围内的接收速率：
  - 最近一小时
  - 过去 4 小时
  - 最后一天
  - 最近一周
  - 最近一个月

编辑 NSG 流日志

1. 在页面的右上角，点击  (**编辑 NSG 流日志**) 图标。
2. 在打开的“编辑 NSG 流日志”(Edit NSG Flow Log) 对话框中，进行编辑，然后点击**保存 (Save)**。

删除 NSG 流日志

1. 在页面的右上角，点击  (**删除 NSG 流日志**) 图标。
2. 在打开的“删除 NSG 流日志”(Remove NSG Flow Log) 对话框中，点击**删除 (Remove)**。

代理节点

思科遥测代理 节点概述显示有关所有代理节点的详细信息，包括以下内容：

- 代理节点名称
- 管理接口（管理网络）IPv4/IPv6 地址
- 遥测接口 IPv4/IPv6 地址
- 代理节点的容量
- 代理节点所属的高可用性集群（如有）
- 接收和发送速率（以 bps 为单位）
- 代理节点的状态以及管理器节点上次与其通信的时间

您可以按以下条件过滤此遥测。只需从页面顶部的下拉菜单中选择以下条件类型之一：

- 最高接收速率
- 最近查看

在“搜索”(Search) 字段中，占位符文本会通知您可以执行搜索的列。在您开始输入内容时，该表会动态地进行过滤以显示包含您已输入的字符的条目列表。

添加群集

有关集群相关的信息和任务，请参阅**高可用性集群**和**集群任务**。

查看代理节点的详细信息

您可以查看有关特定代理节点的更多详细信息。要执行此操作，请在相应行中点击“代理节点名称”(Broker Node Name) 列中所需的代理节点名称。有关此页面的信息，请参阅下一部分**代理节点详细信息**。

代理节点详细信息

要查看代理节点的详细信息，请执行以下操作：

- 在“代理节点”(Broker Nodes) 页面的“代理节点”(Broker Nodes) 表中，点击“代理节点名称”(Broker Node Name) 列中适用的代理节点名称。

您可以在“常规”(General) 部分中查看以下信息：

- 主机名和管理网络 IP 地址
- 输入的状态及其上次接收遥测的时间
- 过去 24 小时的接收速率（以每秒字节数为单位）
- 过去 24 小时的发送速率（以每秒字节数为单位）

“遥测接口”(Telemetry Interface) 部分包含以下信息：

- 接口索引
- 接口名称
- MAC 地址
- PCI 地址
- 容量(以 bps 为单位)
- IPv4 地址/掩码
- IPv4 网关地址
- IPv6 地址/掩码
- IPv6 网关/地址
- 接口 MTU(字节数)

编辑代理节点

要编辑代理节点,请完成以下步骤:

1. 在“遥测接口”(Telemetry Interface) 部分中,点击 **(编辑)** 图标。
2. 单击**保存 (Save)**。

删除代理节点

从管理器节点中删除代理节点时,该代理节点将从数据库中删除,并且不会再被分配给它之前被分配到的任何输入和目标。虽然代理节点仍可在指标图形中选择,但与其关联的名称会更改为术语“代理节点”(Broker Node),后跟代理节点的 ID 和短语“已删除”(deleted)。例如,“代理节点 (ID 10) 已删除”(Broker Node [ID 10] deleted)。

只要已删除的代理节点的数据存在,图仍会包含该代理节点的数据。数据到期后,将无法再从任何“按代理节点”(Per Broker Node) 下拉列表(位于“目标”(Destinations) 和“输入”(Inputs) 页面)中选择关联的代理节点。

请注意以下有关删除代理节点的规则:

- 要确保删除配置信息,必须运行 `ctb-manage` 并选择 **deactivate**。
- 如果您没有完成上一项中所述的操作,代理节点将继续使用先前保存的配置来运行,并且不会向管理器节点发送统计信息。
- 如果将先前删除的代理节点添加回同一管理器节点,则仍需要将其配置为新设备(分配遥测 IP 地址、分配输入等)。

要删除代理节点,请完成以下步骤:

1. 点击右上角的 **(删除代理节点)** 图标。
2. 在“删除”(Remove) 对话框中,点击**删除 (Remove)**。

指标

指标信息的详细信息如下所述。“指标”(Metrics) 部分会按输入和目标显示此代理节点随时间推移所接收的遥测数据。

接收速率表

此表显示此代理节点在一段时间内收到的遥测数据，您可以使用以下过滤器来过滤遥测数据。您可以从每个下拉列表中选择多个选项。

- 按输入
- 按导出程序
- 当**比较容量切换**图标被禁用( )，您可以查看从适用输入接收的遥测的当前接收速率值(以 1 分钟为间隔)。(您必须先从表格右上角的时间范围选项栏中点击**最后 1 小时 (Last 1h)**。)将光标移至 x_轴(反映时间的水平线)上方，以查找特定的分钟。
- 当启用**“与容量切换”(Compare to Capacity Toggle)** 图标时 ，您可以在与阈值进行比较时查看接收速率值。超过 90% 阈值的速率都需要进行调查，因为这些都是值得关注的问题。

您可以通过点击表右上角的以下任意所需时间范围来查看多个时间范围内的这些指标：

- 最近一小时
- 过去 4 小时
- 最后一天
- 最近一周
- 最近一个月

发送速率表

此表显示该代理节点在一段时间内向您从**按目标 (Per Destination)** 下拉列表中选择的目标发送的遥测信息。

- 当**比较容量切换**图标被禁用( )，您可以查看发送到适用目标的遥测的当前接收速率值(以 1 分钟为间隔)。(您必须先从表格右上角的时间范围选项栏中点击**最后 1 小时 (Last 1h)**。)将光标移至 x_轴(反映时间的水平线)上方，以查找特定的分钟。
- 当启用**“与容量切换”(Compare to Capacity Toggle)** 图标时 ，您可以在与阈值进行比较时查看发送速率值。超过 90% 阈值的速率都需要进行调查，因为这些都是值得关注的问题。

> 如果接收速率或发送速率超过阈值，请添加额外的代理节点以增加容量。

您可以通过点击表右上角的以下任意所需时间范围来查看多个时间范围内的这些指标：

- 最近一小时
- 过去 4 小时
- 最后一天
- 最近一周
- 最近一个月

1 分钟平均负载表

所选代理节点在 1 分钟时间间隔内的CPU 平均负载。(您必须先从表格右上角的时间范围选项栏中点击**最后 1 小时 (Last 1h)**。)将光标移至 x_轴(反映时间的水平线)上方，以查找特定的分钟。当负载平均值超过设置为 CPU 数量(由 y_轴表示的值)的阈值时，网络遥测流量速度变慢

内存使用率表

3 分钟时间间隔内的内存消耗和总可用内存。(您必须先从表格右上角的时间范围选项栏中点击**最后 1 小时 (Last 1h)**。)将光标移动到 x_轴(反映时间的水平线)上，以查找特定的 3 分钟时间间隔。超过 80% 阈值的速率都需要进行调查，因为这些都是值得关注的问题。

磁盘存储表

已用磁盘存储空间和 3 分钟时间间隔内的总可用存储空间。(您必须先从表格右上角的时间范围选项栏中点击**最后 1 小时 (Last 1h)**。)将光标移动到 x_轴(反映时间的水平线)上，以查找特定的 3 分钟时间间隔。超过 80% 阈值的速率都需要进行调查，因为这些都是值得关注的问题。

> 如果您发现平均负载，内存使用或磁盘存储超过关联的阈值，请展开 VM 的资源分配。

高可用性集群

思科遥测代理 高可用性提供高可用 IPv4 和 IPv6 虚拟 IP 地址作为输入的目标，并确保可靠地从输入向目标传输遥测数据。

要建立代理节点高可用性，您可以创建高可用性集群，并为每个集群分配多个代理节点。在每个集群中，一个代理节点被指定为 *主动*节点，这意味着它将向 思科遥测代理 传递遥测数据和提供指标，其余节点被指定为 *被动*节点，这意味着它们当前未传递遥测数据或未提供指标。如果主动代理节点停止通过遥测或以其他方式失去连接 思科遥测代理，则其中一个被动代理节点将升级为主动代理节点并开始通过遥测。

请注意以下有关集群的内容：

- 每个代理节点一次只能属于一个集群。
- 要创建集群，您至少需要为该集群分配一个代理节点。
- 请记住，如果您创建仅包含一个代理节点的集群并且该代理节点发生故障，则其他代理节点可升级为活动代理节点。同样，如果集群中的所有代理节点发生故障，则无法将任何代理节点升级为活动代理节点。如果代理节点发生故障，请尽快将其恢复在线状态。
- 您无法选择给定集群中哪个代理节点是主动节点。
- 如果虚拟 IP 地址的主动代理节点发生故障，则同一集群中的一个被动代理节点将成为虚拟 IP 地址的主动代理节点。当发生故障的代理节点再次恢复时，它仍然是被动代理节点。如果要使该节点再次处于活动状态，则需要使用提供的命令手动执行此操作。(要查看这些命令，请参阅 思科遥测代理 《虚拟设备部署和配置指南》中的“将 VIP 移至特定节点”部分。)
- 您可以为集群分配虚拟 IPv4 或虚拟 IPv6 地址，或者两个，到集群。思科遥测代理使用此虚拟 IP 地址与集群通信，并在主动代理节点失去连接时 思科遥测代理将被动代理节点升级为主动代理节点。

有关如何在思科遥测代理软件更新过程中更新 HA 集群的信息，请参阅**软件更新**。

集群任务

查看集群详细信息

在“代理节点”(Broker Nodes) 页面的“高可用性集群”(High Availability Clusters) 部分中，您可以查看以下数据：

- 所有配置的集群
- 每个集群的 IPv4 地址和 IPv6 地址
- 属于每个集群的代理节点

添加群集

1. 从思科遥测代理主菜单中选择**代理节点 (Broker Nodes)**
2. 在页面右侧，点击 **+ 添加集群 (+ Add Cluster)**。
3. 输入描述性集群名称。
4. 选择要包含在集群中的一个或多个代理节点。
5. 输入集群虚拟 IPv4 地址和/或 IPv6 地址。
6. 点击**添加集群 (Add Cluster)**。

    - 最多可能需要3分钟，配置才会传播，VIP 地址在网络中变为可用。
    - 当没有可分配给集群的代理节点时，**+ 添加集群 (+ Add Cluster)** 按钮将被禁用。

修改集群的配置

1. 从思科遥测代理主菜单中选择**代理节点 (Broker Nodes)**
2. 在“高可用性集群”(High Availability Clusters) 部分中，点击要编辑的集群的 **(编辑)** 图标。
3. 在打开的“编辑”(Edit) 对话框中，进行编辑，然后点击**保存 (Save)**。

删除集群

1. 从思科遥测代理主菜单中选择**代理节点 (Broker Nodes)**
2. 在“高可用性集群”(High Availability Clusters) 部分中，点击要删除的集群的 **(删除)** 图标。
3. 在打开的“删除”(Remove) 对话框中，点击**删除 (Remove)**。

有关管理集群的信息，请参阅思科遥测代理 《虚拟部署指南》中的“管理高可用性集群”部分。

管理器节点

思科遥测代理管理器视图将显示您的思科遥测代理管理器的指标。可以查看以下信息：

- 主机名和管理接口（管理网络）IPv4/IPv6 地址
- 当前内存使用情况和可用总内存
- 当前磁盘存储使用情况和可用的总磁盘存储空间

1 分钟平均负载表

所选代理节点在 1 分钟时间间隔内的CPU 平均负载。（您必须先从表格右上角的时间范围选项栏中点击**最后 1 小时 (Last 1h)**。）将光标移至 x_轴（反映时间的水平线）上方，以查找特定的分钟。当负载平均值超过设置为 CPU 数量（由 y_轴表示的值）的阈值时，网络遥测流量速度变慢

内存使用率表

1 分钟时间间隔内的内存消耗和总可用内存。（您必须先从表格右上角的时间范围选项栏中点击**最后 1 小时 (Last 1h)**。）将光标移动到 x_轴（反映时间的水平线）上，以查找特定的 3 分钟时间间隔。任何超过 80% 阈值的速率都需要被进行调查，因为这些都是值得关注的问题。

磁盘存储表

已用磁盘存储空间和 3 分钟时间间隔内的总可用存储空间。（您必须先从表格右上角的时间范围选项栏中点击**最后 1 小时 (Last 1h)**。）将光标移动到 x_轴（反映时间的水平线）上，以查找特定的 3 分钟时间间隔。任何超过 80% 阈值的速率都需要被进行调查，因为这些都是值得关注的问题。

> 如果您发现平均负载，内存使用或磁盘存储超过关联的阈值，请展开 VM 的资源分配。

您可以通过点击“指标”(Metrics) 表右上角的以下任意所需时间范围来查看多个时间范围内的这些指标：

- 最近一小时
- 过去 4 小时
- 最后一天
- 最近一周
- 最近一个月

集成

思科遥测代理 集成显示有关您的 VPC 流日志的信息。您可以将您的AWS部署配置为将 VPC 流日志导出到思科遥测代理，然后配置思科遥测代理为将 VPC 流日志转换为 IPFIX，以便按目标进行注入。

查看集成信息

从思科遥测代理主菜单中，选择**集成 (Integrations)**。

AWS 配置

AWS 配置 - 第 1 部分

启用流日志记录

要为一个或多个 VPC 启用流日志记录，然后将流日志发送到 S3 存储桶，请完成以下步骤：

1. 从 AWS VPC 主菜单中，选择**您的 VPC (Your VPCs)**。
2. 右键点击 VPC，然后选择**创建流日志 (Create Flow Log)**。
3. 从过滤器下拉列表中，选择**全部 (All)** 以记录接受和拒绝的遥测，或选择**接受 (Accept)** 以仅记录接受的遥测。
4. 选择**发送到 S3 存储桶目标 (Send to an S3 bucket destination)**。
5. 输入要在其中存储流日志遥测的 **S3 存储桶 ARN**。
6. 点击**创建 (Create)**。

创建 IAM 用户

创建有权访问 S3 存储桶的 IAM 用户，并记录访问密钥 ID 和加密访问密钥，请完成以下步骤：

1. 从 AWS IAM 主菜单中，选择**用户 (Users) > 添加用户 (Add user)**。
2. 输入**用户名 (User Name)**。
3. 选择**编程访问 (Programmatic access)**。
4. 点击 **下一步：权限 (Next: Permissions)**。
5. 点击 **下一步：标记 (Next: Tags)**。
6. 点击 **下一步：查看 (Next: Review)**。
7. 点击**创建用户 (Create User)**。
8. 对于访问密钥 ID 和秘密访问密钥，请点击**显示 (Show)**。
9. 记录访问密钥 ID 和秘密访问密钥，或点击**下载 (Download)** 并将密钥保存在安全位置。

思科遥测代理配置 - 第 1 部分

上传您的 AWS 访问

要将您的 AWS 访问密钥和秘密访问密钥上传到 思科遥测代理，请完成以下步骤：

1. 从思科遥测代理主菜单中，选择**集成 (Integrations)**。

   系统将打开 AWS 选项卡。

2. 点击**添加 AWS 凭证 (Add AWS Credentials)**（位于右上角的 AWS 凭证表上方）。
3. 输入描述性**凭证名称 (Credentials Name)**。
4. 输入 **AWS 访问密钥 ID (AWS Access Key ID)** 和 **AWS 秘密访问密钥 (AWS Secret Access Key)**。
5. 单击**保存 (Save)**。
6. 如果您有其他 S3 凭证，请重复步骤 1 到步骤 5。

配置 VPC 流日志输入

要配置 VPC 流日志输入并将存储桶策略上传到 AWS，请完成以下步骤：

1. 在思科遥测代理主菜单中，选择**输入 (Inputs) > VPC 流日志 (VPC Flow Logs)** 选项卡。
2. 点击**添加 VPC 流日志 (Add VPC Flow Log)**（位于右上角的输入表上方）。

   ***添加 VPC 流日志** 对话将打开。*

3. 在 **S3 存储桶路径 (S3 Bucket Path)** 字段中，输入 s3 存储桶名称和路径。例如，

   ［桶名称］ / ［路径］

4. 在**区域代码 (Region Code)** 字段中，输入创建 S3 存储桶的 AWS 区域。
5. 根据您上传的访问密钥和秘密访问密钥选择**凭证** 。
6. 点击下一个字段中的箭头以展开窗格。在该窗格中，复制 S3 存储桶策略并在 AWS 中将它用于 S3 存储桶配置。
7. 让此对话框保持打开并继续下一部分：“AWS 配置 - 第 2 部分”。

AWS 配置-第 2 部分

创建 S3 存储桶策略

1. 从 AWS IAM 主菜单中，选择**策略 (Policies)**。
2. 点击**创建策略 (Create policy)**。
3. 选择 JSON 选项卡。
4. 将从思科遥测代理复制的策略粘贴到 JSON 编辑器中。
5. 点击 **查看策略 (Review policy)**。

6. 在**名称 (Name)** 字段中，输入用于标识策略的唯一名称（例如，**ctb_policy**）。
7. 输入说明，例如 **Policy 以允许思科遥测代理访问 VPC 流日志**。
8. 点击**创建策略 (Create Policy)**。

创建用户组

要创建用户组，请将策略分配到 IAM 组，并将您的 IAM 用户添加到 IAM 组，请完成以下步骤：

1. 从 AWS IAM 主菜单中，选择**组 (Groups) >创建新组 (Create New Group)**。
2. 输入**组名称 (group name)**。
3. 点击**下一步 (Next Step)**。
4. 选择您创建的思科遥测代理策略。
5. 点击**下一步 (Next Step)**。
6. 点击**创建组 (Create Group)**。
7. 从 IAM 控制台，选择**组 (Groups) > [组名称] ([Group Name])**。
8. 点击**用户 (Users)** 选项卡。
9. 点击**添加用户至组 (Add Users to Group)**并选择您的**思科遥测代理用户**。
10. 点击**添加用户 (Add Users)**

思科遥测代理配置 - 第 2 部分

在思科遥测代理中注册 AWS 流登录。

要配置思科遥测代理以处理 VPC 流日志遥测并将其转换为 IPFIX，请执行以下步骤：

1. 返回到您在“思科遥测代理配置 - 第 1 部分”中部分完成的对话框（请参阅 **配置 VPC 流日志输入** 部分）。
2. 在**输入名称 (Input Name)** 字段中，输入输入 IP 地址名称。
3. 在**输入 IP 地址 (Input IP Address)** 字段中，输入要分配给此流日志的输入 IP 地址。在发送从 VPC 流日志生成的 IPFIX 时，思科遥测代理将使用此 IP 地址作为输入地址。它应该是内部 IP 地址，并且不应与网络上的其他 IP 地址冲突。

   思科遥测代理 对输入 IP 值设置以下限制，以确保正确代理数据包。如果不满足以下任何条件，思科遥测代理则显示错误消息：

   - 输入 IP 不得与已分配节点的遥测接口的子网重叠。
   - 输入 IP 不得与系统中的任何现有输入 IP 冲突。
   - 输入 IP 不得与系统中的任何目标 IP 冲突。

4. 从**分配的代理节点 (Assigned Broker Node)** 下拉列表中选择分配的代理节点。此代理节点将处理来自 S3 存储桶的所有流日志遥测。
5. 选择一个或多个目标以获取流日志遥测。请注意思科遥测代理将 VPC 流日志转换为 IPFIX。
6. 点击**添加 VPC 流日志**。
7. 如果要配置多个 VPC 流日志，请为您配置的每个 VPC 流日志按顺序完成以下步骤：
    a. 重复配置 **配置 VPC 流日志输入** 中的每个步骤。
    b. 重复 **创建 S3 存储桶策略**中的每个步骤。
    c. 重复 **创建用户组**中的每个步骤。
    d. 重复此部分中的步骤 1 至步骤 5。
8. 单击**保存 (Save)**。

> 要成功配置 VPC 流日志，请确保 AWS S3 存储桶存在流日志（已写入其中）。否则，AWS VPC 流日志配置将失败。

Azure 配置

以下说明详细介绍了如何设置从 Azure 环境收集遥测数据以进行分析的监控应用。我们建议你以分配给所有需要监控的订用的*全局管理员 AD* 和*所有者*角色的用户身份来按照以下说明进行操作。

如果无法做到这一点，请联系 Azure AD 管理员，确保要监控的每个订用的用户都能访问以下 Azure 资源：授权、网络、存储帐户和监控。为此，您必须为用户分配*用户访问管理员*和*贡献者*角色。

必备条件

在配置 NSG 流日志之前，请完成以下步骤：

1. **连接到 Azure** 访问您的 Azure 门户并按照说明进行登录。对于命令行访问，请使用搜索栏旁边的控制台图标来启动 bash 控制台。
2. **设置网络观察程序** 为具有要监控的资源组的区域设置网络观察程序服务：
    a. 从主菜单中选择**网络观察程序 (Network Watcher) > 概述 (Overview)**。
    b. 点击 ··· **（省略号）**图标，然后在订用级别或目标区域选择**启用网络观察程序 (Enable Network Watcher)**。
3. **创建存储帐户** 要存储 NSG 流日志，您需要将存储帐户置于与目标资源组相同的位置（例如美国东部）。如果目标位置还没有存储帐户，则需要创建一些具有 Blob 存储功能的帐户（StorageV2 或 BlobStorage）。

启用 NSG 流日志

对于要监控的 NSG，您需要通过完成以下步骤来启用流日志记录：

1. 从主菜单中选择**网络观察程序 (Network Watcher) > NSG 流日志 (NSG Flow Logs)**。系统将显示“网络安全组”(Network Security Groups) 列表。
2. 要显示“流日志”(Flow Logs) 设置屏幕，请从主菜单中选择 NSG。
3. 填写表单，输入以下设置：
   - **状态 (Status)：**开
   - **流日志版本 (Flow Logs version)：**版本 2
   - **存储帐户 (Storage account)：**选择您之前创建的存储帐户。
   - **保留 (Retention)：**Microsoft 当前存在流日志保留的已知问题。有关详细信息，请参阅 Microsoft 文档中“启用 NSG 流日志”部分的步骤 11 中的注释。
   - **流量分析状态 (Traffic Analytics status)：**关（或者，您可以启用此功能）
4. 点击**保存 (Save)** 并为每个 NSG 重复流日志设置。

> 您需要为创建的任何要监控的新资源组启用 NSG 流量日志。

5. 在 Azure 门户中，从主菜单中选择**存储帐户 (Storage Accounts) > 选择您的账户 (Select Your Account) > 容器 (Containers)**。验证您是否在“容器”列表中看到了 *insights-logs-networksecuritygroupflowevent* 事件条目。它可能需要几分钟才会出现。

获取 Blob 服务 SAS URL

要生成思科遥测代理所需的 Blob 服务 SAS URL，请完成以下步骤：

1. 在 Azure 门户中，从主菜单中选择**存储帐户 (Storage Accounts) > 选择您的账户 (Select Your Account) > 共享访问签名 (Shared Access Signature)**。打开的表单应包含以下条目：
   - **允许的服务 (Allowed Services)：** Blob
   - **允许的资源类型 (Allowed Resource Types)：**：服务、容器、对象
   - **允许的权限 (Allowed Permissions)：**读取、列表
   - **开始和到期时间 (Start and Expiry Times)：**：设置为允许思科遥测代理访问的间隔
2. 选择**生成 SAS (Generate SAS) > 连接字符串**。
3. 复制 Blob 服务 SAS URL。

> 在将 NSG 流日志添加到思科遥测代理时，请提供 Blob 服务 SAS URL。

注册 Azure 流登录 思科遥测代理

要配置思科遥测代理以处理 NSG 流日志遥测并将其转换为 IPFIX，请完成以下步骤：

1. 返回至 思科遥测代理。
2. 在思科遥测代理主菜单中，点击**输入 (Inputs) > NSG 流日志 (NSG Flow Logs)** 选项卡。
3. 点击**添加 NSG 流日志 (Add NSG Flow Log)**（位于右上角的“输入”(Inputs) 表上方）。

   *此时将打开**添加 VPC 流日志 (Add NSG Flow Log)** 对话框。*
4. 在**输入名称 (Input Name)** 字段中，输入输入 IP 地址名称。
5. 在**输入 IP 地址 (Input IP Address)** 字段中，输入要分配给此流日志的输入 IP 地址。在发送从 NSG 流日志生成的 IPFIX 时，思科遥测代理将使用此 IP 地址作为输入地址。它应该是内部 IP 地址，并且不应与网络上的其他 IP 地址冲突。

   思科遥测代理 对输入 IP 值设置以下限制，以确保正确代理数据包。如果不满足以下任何条件，思科遥测代理则显示错误消息：

   - 输入 IP 不得与已分配节点的遥测接口的子网重叠。
   - 输入 IP 不得与系统中的任何现有输入 IP 冲突。
   - 输入 IP 不得与系统中的任何目标 IP 冲突。
6. 从**分配的代理节点 (Assigned Broker Node)** 下拉列表中选择分配的代理节点。此代理节点将处理来自 S3 存储桶的所有流日志遥测。
7. 选择一个或多个目标以获取流日志遥测。请注意思科遥测代理会将 NSG 流日志转换为 IPFIX。
8. 点击**添加 VPC 流日志 (Add NSG Flow Log)**。
9. 如果要配置多个 NSG 流日志，请为您配置的每个 NSG 流日志按顺序完成以下步骤：
   a. 重复此 Azure 配置主题前面每个部分中的每个步骤。
   b. 重复此部分中的步骤 1 至步骤 7。
10. 单击**保存 (Save)**。

应用设置

应用设置控制您的 思科遥测代理 部署。以下设置可用：

常规设置

软件更新

智能许可

TLS 证书

用户管理

常规

1. 点击⚙**(设置)**图标。

   将打开应用设置页面。

2. 点击**常规 (General)**选项卡。

配置非活动间隔

遥测输入配置允许您配置将遥测输入 思科遥测代理 标记为非活动之前的时间量。

1. 在输入部分中，从非活动间隔下拉列表中选择**非活动间隔 (Inactivity Interval)**(以分钟为单位)。
2. 单击**保存 (Save)**。

配置 HTTPS 代理。

如果思科遥测代理使用 HTTPS 代理连接到互联网，则 HTTPS 代理配置允许您配置 HTTPS 代理服务器设置。

> ℹ 思科遥测代理 不支持使用 HTTP 代理服务器。

1. 在 HTTPS 代理部分中，启用**使用 HTTPS 代理**。
2. 输入 **IP 地址 (IP Address)** 和**端口 (Port)**。
3. 单击**保存 (Save)**。

软件更新

软件更新页面显示管理器节点和代理节点的当前思科遥测代理版本，并允许您升级到当前发布的版本。

更新会将您的管理器和所有托管代理节点升级到最新版本。在执行更新之前，我们建议您为您的 思科遥测代理 VM 创建 VM 快照。如果收到意外错误，您可以使用此快照恢复当前状态。

系统在更新过程中没有响应。它首先会更新管理器，然后更新代理节点。当您的管理器更新时，您可能看不到您的思科遥测代理部署的正确状态。当代理节点更新时，它们可能无法将已发送的遥测正确传递到目标。

思科遥测代理 HA 集群旨在确保在升级期间没有停机；因此，在 HA 集群中，管理器始终每次仅更新一个节点。更新 HA 集群时，管理器节点会按创建顺序来更新该集群中的节点。当节点开始更新时，它首先会将自己置于备用模式。如果这是主用节点，思科遥测代理功能将转移到备用节点。这会在之前的活动节点停止处理遥测之前进行。这样可确保在升级过程中尽可能减少遥测数据丢失。

升级您的思科遥测代理部署

下载更新文件

1. 转到 Cisco 软件中心。
2. 在“下载和升级”(Download and Upgrade) 部分中，选择**访问下载 (Access Download)**。
3. 在搜索字段中键入 **Cisco 遥测代理** 。
4. 选择**管理器节点软件 (Manager Node Software)**。
5. 下载 CTB 更新捆绑包文件。

上传更新文件

1. 在思科遥测代理管理器中，点击⚙ **(设置)** 图标。

   将打开应用设置页面。

2. 点击 **软件更新 (Software Update)** 选项卡。
3. 在页面右上角，点击 **上传更新文件 (Upload an Update File)**。
4. 选择所下载的文件。

   根据显示的时间估计，您可能需要等待几分钟才能完成上传。文件上传后，您将收到一条消息，通知您现在有软件更新可用。

5. 点击 **更新 (Update)思科遥测代理**。

   当管理器节点更新为最新版本时，您将无法在 思科遥测代理 中导航。更新过程大约需要 10 分钟。

6. 更新完成后，系统将提示您重新登录回 思科遥测代理。

   正在更新的每个代理节点旁边将显示加载指示器。

智能许可

智能软件许可页面显示您的 思科遥测代理 智能许可状态。

思科遥测代理 许可基于您的代理节点每天收集的 GB。

1. 点击 ⚙ **(设置)** 图标。

   将打开应用设置页面。

2. 点击**智能许可 (Smart Licensing)** 选项卡。

用户管理

1. 点击**设置 (Settings)** 图标。

   将打开应用设置页面。

2. 点击**用户管理 (User Management)** 选项卡。

添加用户

1. 点击**添加用户 (Add User)**。
2. 输入用户的**名字 (First Name)** 和**姓氏 (Last Name)**。
3. 输入 **用户名 (Username)**。此用户名创建后，您或用户都无法更改。
4. 在**新密码 (New Password)** 字段输入一个密码，并在**确认密码 (Confirm Password)** 字段再输入一次。确保遵守密码准则。
5. 点击 **+ 添加用户 (+ Add User)**。

编辑用户

1. 在包含要编辑的用户的行中，点击 ••• **(操作)** 图标 > **编辑配置文件 (Edit Profile)**。
2. 完成编辑。
3. 单击**保存 (Save)**。

删除用户

1. 在包含要编辑的用户的行中，点击 **操作**图标 > **删除用户 (Remove User)**。
2. 点击**删除 (Remove)**。

更改用户密码

1. 在包含要更改其密码的用户的行中，点击 **操作** 图标 > **更改密码 (Change Password)**。
2. 在**密码 (Password)** 字段输入一个新密码，并在**确认密码 (Confirm Password)** 字段再输入一次。
3. 点击**更改密码 (Change Password)**。

TLS 证书

在此页面上，您可以查看以下信息：

- 主机名
- 证书到期日期和时间
- 使用者名称和颁发者名称(在“证书详细信息”(Certificate details)下)

⚠ 证书和私钥必须采用 PEM 编码。

⚠ 私钥文件不能受密码保护。

上传 TLS 证书

1. 点击 ⚙ **(设置)** 图标。

   将打开应用设置页面。

2. 点击 **TLS 证书 (TLS Certificate)** 选项卡。
3. 要查看证书详细信息,请点击**证书详细信息 (Certificate details)** 下拉箭头。在此部分中,您可以查看使用者名称、颁发者名称和使用者备用名称。
4. 在页面右上角,点击 **上传 TLS 证书 (Upload TLS Certificate)**。
5. 在打开的“上传 TLS 证书”(Upload TLS Certificate)对话框中,点击要上传的每个证书和每个私钥的**选择文件 (Choose File)**。

   证书详细信息显示在关联文件下方,因此您可以验证所有相关信息是否正确。

6. 点击**上传 (Upload)**。

重新注册代理节点

在上传适当的 TLS 证书后,您需要通过重新注册每个代理节点来启用管理器节点和代理节点之间的连接。

1. 使用 SSH 或 VM 服务器控制台以**管理员**身份登录设备。
2. 输入以下命令:

   ```
   sudo ctb-manage
   ```

   系统将通知您管理器配置已存在。

3. 选择 **选项 C:“重新获取管理器的证书,但保留所有其他内容”(Re-fetch the manager's certificate but keep everything else)**。

系统日志通知

1. 点击 ⚙ **(设置)** 图标。

   将打开应用设置页面。

2. 点击**通知 (Notifications)** 选项卡。

要查看支持的警报列表，请点击页面顶部的**支持的警报 (Supported Alerts)** 下拉箭头。您可以指示思科遥测代理在生成任何警报时发送系统日志通知。有关这些警报的列表，请参阅**附录 B:支持的警报**。

> 目前，您无法配置自定义警报类型。

配置系统日志服务器

首先，您需要配置系统日志服务器设置。

1. 在“系统日志服务器地址”(Syslog Server Address) 字段中，点击**配置 (Configure)**。
2. 输入适用的系统日志服务器地址（可以是 IPv4 地址、IPv6 地址或 DNS 名称）以及端口号。
3. 单击**保存 (Save)**。

启用系统日志服务器以接收通知

接下来，执行以下操作：

- 启用**发送系统日志通知**切换（ ）。

在配置系统日志服务器后，您必须启用此开关，否则系统日志服务器将不会收到通知。一旦启用此开关，当思科遥测代理触发警报时，它就会立即向系统日志服务器发送系统日志通知。

发送测试系统日志通知

无论何时选择这样做，都可以手动将测试系统日志通知发送到系统日志服务器。此测试通知用于检查系统日志服务器是否已成功接收系统日志消息。

每次发送测试系统日志通知时，都会在**已发送测试 (Sent Test)** 按钮下显示该消息的副本。这让您能够将发送的消息与系统日志服务器接收的消息进行比较。

如果您注销思科遥测代理，那么再次登录时，它将不再显示消息。

> 您必须手动检查系统日志服务器，以验证是否收到测试通知。

要发送测试系统日志通知，请完成以下步骤：

1. 启用**发送系统日志通知**切换（ ）。
2. 点击**发送测试 (Send Test)**。
3. 在确认对话框中，点击**发送 (Send)**。

严重性和设施值

遥测代理会将严重性值硬编码为*警告*，并将设施值硬编码为 *local0*。

邮件通知

1. 点击⚙(**设置**)图标。

   将打开应用设置页面。

2. 点击**通知 (Notifications)**选项卡。

您可以指示思科遥测代理在生成任何警报时发送邮件通知。有关这些警报的列表，请参阅**附录 B:支持的警报**。

> ℹ 目前，您无法配置自定义警报类型。

配置 SMTP 服务器

首先，您需要配置 SMTP 服务器设置。

1. 在 SMTP 服务器字段中，点击**配置 (Configure)**。
2. 输入适用的 SMTP 服务器地址(可以是 IPv4 地址、IPv6 地址或 DNS 名称)，端口号以及发送警报的邮件地址。
3. 指定是否需要进行身份验证。如果是，请在关联字段中输入 SMTP 服务器的用户名和密码。
4. 选择加密类型。
5. 单击**保存 (Save)**。

支持用户接收电子邮件通知

在配置 SMTP 服务器后，您必须启用思科遥测代理以发送邮件通知，否则指定的用户将不会收到通知。

1. 启用 **发送邮件通知** 切换(⬭)。
2. 在“收件人”(Recipients)字段中，点击 **编辑 (Edit)**。
3. 在打开的“编辑收件人”(Edit Recipients)对话框中，选择您希望能够接收邮件通知的每个用户。

   当前用户的名称显示在列表顶部。其配置文件缺少电子邮件地址的任何用户的用户名在列表底部显示为灰色状态。

4. 单击**保存 (Save)**。

发送测试电子邮件通知

每当您选择这样做时，您都可以为所有警报手动发送测试邮件通知。此测试邮件通知会检查 SMTP 服务器是否已正确配置，并且所有适当的用户都将成功接收发生的任何警报(为其分配警报)的邮件通知。

1. 启用 **发送邮件通知** 切换( ) 。
2. 点击**发送测试 (Send Test)**。
3. 如果需要编辑将接收此测试邮件通知的用户列表，请在打开的“发送测试”(Send Test) 对话框中点击**选择 (Choose)** 并进行编辑。

   当前用户的名称显示在列表顶部。其配置文件缺少电子邮件地址的任何用户的用户名在列表底部显示为灰色状态。

4. 点击**发送 (Send)**。

文件设置

配置编辑您的个人信息

1. 点击 (**用户**) 图标。

   将打开设置页面。

2. 在个人信息部分中，点击 (**编辑**) 图标。
3. 完成编辑。
4. 单击**保存 (Save)**。

更改密码

1. 点击 (**用户**) 图标。

   将打开设置页面。

2. 在密码部分，点击**更改密码 (Change Password)**。
3. 在**密码 (Password)** 字段输入一个新密码，并在**确认密码 (Confirm Password)** 字段再输入一次。
4. 点击**更改密码 (Change Password)**。

展开思科遥测代理管理器和代理节点磁盘大小

使用思科遥测代理，您可以扩展管理器和任何代理节点的磁盘大小。

1. 备份分区表信息

登录设备并运行以下命令。

```
admin@ctb-nfik72TO:~$ sudo sgdisk -p /dev/sda > partition_table_
$(date +'%Y_%m_%d_%H_%M_%S').txt
```

这样将创建一个类似于 partition_table_2021_07_09_15_51_04.txt 的文件，其包含类似如下的内容：

```
Disk /dev/sda: 81920000 sectors, 39.1 GiB Model: Virtual disk Sector size
(logical/physical): 512/512 bytes Disk identifier (GUID): B078BED8-2BD0-4EEA-9149-
BA93FC8A299D Partition table holds up to 128 entries Main partition table begins at
sector 2 and ends at sector 33 First usable sector is 34, last usable sector is 81919966
Partitions will be aligned on 2048-sector boundaries Total free space is 4029 sectors
(2.0 MiB) Number Start (sector) End (sector) Size Code Name 1 2048 4095 1024.0 KiB EF02 2
4096 491519 238.0 MiB 8300 3 491520 3844095 1.6 GiB 8200 4 3844096 33767423 14.3 GiB 8300
5 33767424 63690751 14.3 GiB 8300 6 63690752 81917951 8.7 GiB 8300
```

磁盘的总大小(/dev/ada)为 39.1 GB，思科遥测代理应用分区的大小(/dev/sda6)为 8.7 GB。

2. 删除设备的所有现有 VM 快照

当存在快照时，无法调整 ESXi VM 磁盘的大小。为了增加磁盘大小，我们需要删除所有现有快照。

1. 登录 ESXi 控制台(vSphere 或 Web 客户端)。
2. 右键点击 VM，然后选择**快照 (Snapshots) > 管理快照 (Manage Snapshots) > 全部删除 (Delete All)**。

3. 增加设备的磁盘大小

1. 登录 ESXi 控制台(vSphere 或 Web 客户端)。
2. 从左侧面板中的 VM 列表中，选择设备。
3. 从页面顶部的工具栏中，点击 (**编辑**) 图标。
4. 在硬盘 1 行中，增加到所需大小。
5. 重新启动 VM
6. 登录并通过运行以下命令验证是否已应用新的大小：

```
$ sudo sgdisk -p /dev/sda Disk /dev/sda: 125829120 sectors, 60.0 GiB Model: Virtual disk
Sector size (logical/physical): 512/512 bytes Disk identifier (GUID): B078BED8-2BD0-4EEA-
9149-BA93FC8A299D Partition table holds up to 128 entries Main partition table begins at
sector 2 and ends at sector 33 First usable sector is 34, last usable sector is 81919966
Partitions will be aligned on 2048-sector boundaries Total free space is 4029 sectors
(2.0 MiB) Number Start (sector) End (sector) Size Code Name 1 2048 4095 1024.0 KiB EF02 2
4096 491519 238.0 MiB 8300 3 491520 3844095 1.6 GiB 8200 4 3844096 33767423 14.3 GiB 8300
5 33767424 63690751 14.3 GiB 8300 6 63690752 81917951 8.7 GiB 8300
```

4. 运行 ctb-part-resize.sh 脚本

1. 拍摄 VM 快照。
2. 运行以下命令：

```
$ sudo /opt/titan/bin/ctb-part-resize.sh WARNING This program will update /dev/sda6 to use the full remain
It is HIGHLY RECOMMENDED that you take a backup of any important data/configuration before proceeding. Do
15:35:30 ctb-disk-resize: Moving the partition table header to the end of the disk(/dev/sda) Warning: The
partition table. The new table will be used at the next reboot or after you run partprobe(8) or kpartx(8)
successfully. <134>Mar 8 15:35:31 ctb-disk-resize: Deleting CTB application partition (/dev/sda6) Warning:
partition table. The new table will be used at the next reboot or after you run partprobe(8) or kpartx(8)
successfully. <134>Mar 8 15:35:32 ctb-disk-resize: Creating the CTB application partition (/dev/sda6) Warn
partition table. The new table will be used at the next reboot or after you run partprobe(8) or kpartx(8)
successfully. <134>Mar 8 15:35:33 ctb-disk-resize: Updating kernel partition tables <134>Mar 8 15:35:34 ct
resize2fs 1.44.5 (15-Dec-2018) Filesystem at /dev/sda6 is mounted on /var/lib/titan; on-line resizing requ
blocks = 2 The filesystem on /dev/sda6 is now 2412283 (4k) blocks long.
```

5. 验证是否已分配空间

运行以下命令：

```
$ df -h /dev/sda Filesystem Size Used Avail Use% Mounted on /dev/sda4 14G 5.6G 7.7G 42% /
/dev/sda2 227M 80M 132M 38% /boot /dev/sda5 14G 41M 14G 1% /mnt/alt_root /dev/sda6 8.5G
172M 7.9G 3% /var/lib/titan
```

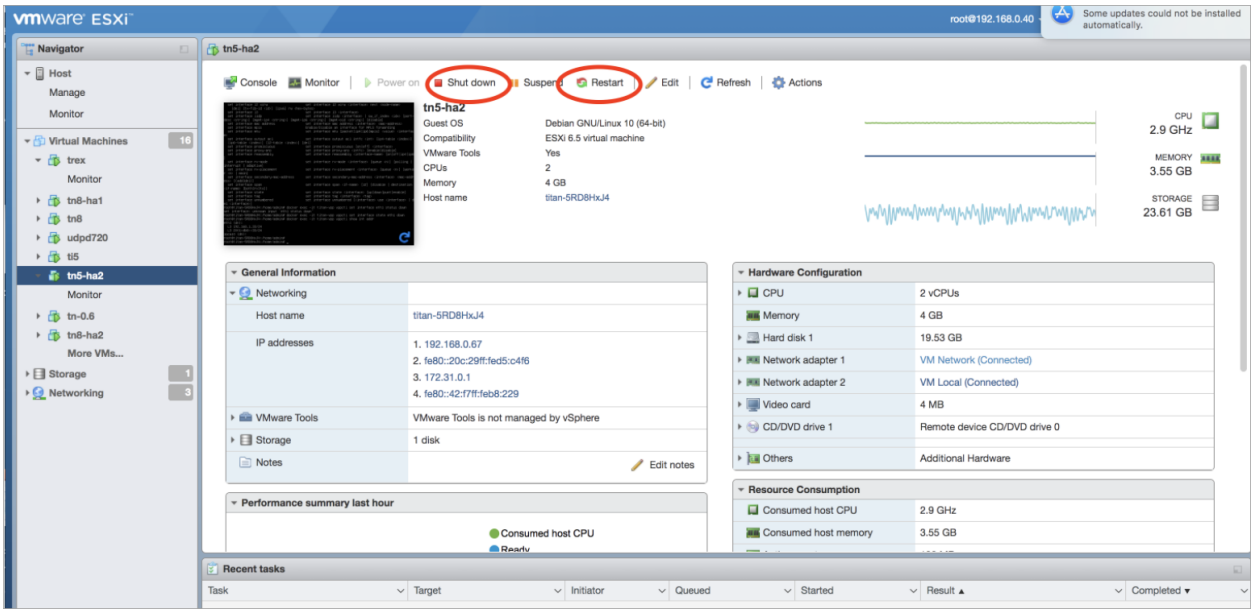
关闭或重新引导 思科遥测代理

如果在某些时候需要关闭或重新启动思科遥测代理，请完成以下步骤：

1. 使用用户名 **admin** 通过 SSH 或控制台登录到 CTB 管理器或 CTB 代理节点。
   - 若要关闭，请输入 `sudo shutdown now`
   - 若要重新引导，请输入 `sudo shutdown -r now`
2. 登录 VMWare 控制台并验证 VM 是否已正确完成关闭或重新启动。

（可选）您也可以使用 VMWare 关闭或重新引导。为此，请执行以下操作：

1. 登录到 VMWare 控制台并选择适用的 VM。
2. 请点击页面顶部显示的以下其中一个选项，具体取决于是要关闭还是要重新引导：



附录 A:支持的 IPFIX 字段 思科遥测代理

本附录中的表包含思科遥测代理支持的 IPFIX 字段的列表。

思科遥测代理 从 NetFlow 消息中的信息元素中提取数字 ID(每个数字 ID 包括一个元素 ID 和一个 PEN),并将其映射到关联的描述性名称。

> 如果思科遥测代理无法识别信息元素的数字 ID,元素信息仍会发送到 Cisco Secure Cloud Analytics,但思科遥测代理会使用以下格式为其分配名称:`unknownID_<ElementID>_<PEN>`

如果要查看任何元素 ID 的说明,请参阅《Cisco Secure Network Analytics信息元素指南》。

ElementID	PEN	Name
1	0	octetDeltaCount
2	0	packetDeltaCount
3	0	deltaFlowCount
4	0	protocolIdentifier
5	0	ipClassOfService
6	0	tcpControlBits
7	0	sourceTransportPort
8	0	sourceIPv4Address
9	0	sourceIPv4PrefixLength
10	0	ingressInterface
11	0	destinationTransportPort
12	0	destinationIPv4Address
13	0	destinationIPv4PrefixLength
14	0	egressInterface

ElementID	PEN	Name
15	0	ipNextHopIPv4Address
16	0	bgpSourceAsNumber
17	0	bgpDestinationAsNumber
18	0	bgpNextHopIPv4Address
19	0	postMCastPacketDeltaCount
20	0	postMCastOctetDeltaCount
21	0	flowEndSysUpTime
22	0	flowStartSysUpTime
23	0	postOctetDeltaCount
24	0	postPacketDeltaCount
25	0	minimumIpTotalLength
26	0	maximumIpTotalLength
27	0	sourceIPv6Address
28	0	destinationIPv6Address
29	0	sourceIPv6PrefixLength
30	0	destinationIPv6PrefixLength
31	0	flowLabelIPv6
32	0	icmpTypeCodeIPv4
33	0	igmpType
34	0	samplingInterval
35	0	samplingAlgorithm

ElementID	PEN	Name
36	0	flowActiveTimeout
37	0	flowIdleTimeout
38	0	engineType
39	0	engineId
40	0	exportedOctetTotalCount
41	0	exportedMessageTotalCount
42	0	exportedFlowRecordTotalCount
43	0	ipv4RouterSc
44	0	sourceIPv4Prefix
45	0	destinationIPv4Prefix
46	0	mplsTopLabelType
47	0	mplsTopLabelIPv4Address
48 个	0	samplerId
49	0	samplerMode
50	0	samplerRandomInterval
51	0	classId
52	0	minimumTTL
53	0	maximumTTL
54	0	fragmentIdentification
55	0	postIpClassOfService
56	0	sourceMacAddress

ElementID	PEN	Name
57	0	postDestinationMacAddress
58	0	vlanId
59	0	postVlanId
60	0	ipVersion
61	0	flowDirection
62	0	ipNextHopIPv6Address
63	0	bgpNextHopIPv6Address
64	0	ipv6ExtensionHeaders
70	0	mplsTopLabelStackSection
71	0	mplsLabelStackSection2
72	0	mplsLabelStackSection3
73	0	mplsLabelStackSection4
74	0	mplsLabelStackSection5
75	0	mplsLabelStackSection6
76	0	mplsLabelStackSection7
77	0	mplsLabelStackSection8
78	0	mplsLabelStackSection9
79	0	mplsLabelStackSection10
80	0	destinationMacAddress
81	0	postSourceMacAddress
82	0	interfaceName

ElementID	PEN	Name
83	0	interfaceDescription
84	0	samplerName
85	0	octetTotalCount
86	0	packetTotalCount
87	0	flagsAndSamplerId
88	0	fragmentOffset
89	0	forwardingStatus
90	0	mplsVpnRouteDistinguisher
91	0	mplsTopLabelPrefixLength
92	0	srcTrafficIndex
93	0	dstTrafficIndex
94	0	applicationDescription
95	0	applicationId
96	0	applicationName
98	0	postIpDiffServCodePoint
99	0	multicastReplicationFactor
100	0	className
101	0	classificationEngineId
102	0	layer2packetSectionOffset
103	0	layer2packetSectionSize
104	0	layer2packetSectionData

ElementID	PEN	Name
128	0	bgpNextAdjacentAsNumber
129	0	bgpPrevAdjacentAsNumber
130	0	exporterIPv4Address
131	0	exporterIPv6Address
132	0	droppedOctetDeltaCount
133	0	droppedPacketDeltaCount
134	0	droppedOctetTotalCount
135	0	droppedPacketTotalCount
136	0	flowEndReason
137	0	commonPropertiesId
138	0	observationPointId
139	0	icmpTypeCodeIPv6
140	0	mplsTopLabelIPv6Address
141	0	lineCardId
142	0	portId
143	0	meteringProcessId
144 个	0	exportingProcessId
145	0	templateId
146	0	wlanChannelId
147	0	wlanSSID
148	0	flowId

ElementID	PEN	Name
149	0	observationDomainId
150	0	flowStartSeconds
151	0	flowEndSeconds
152	0	flowStartMilliseconds
153	0	flowEndMilliseconds
154 种	0	flowStartMicroseconds
155	0	flowEndMicroseconds
156	0	flowStartNanoseconds
157	0	flowEndNanoseconds
158	0	flowStartDeltaMicroseconds
159	0	flowEndDeltaMicroseconds
160	0	systemInitTimeMilliseconds
161	0	flowDurationMilliseconds
162	0	flowDurationMicroseconds
163	0	observedFlowTotalCount
164	0	ignoredPacketTotalCount
165	0	ignoredOctetTotalCount
166	0	notSentFlowTotalCount
167	0	notSentPacketTotalCount
168	0	notSentOctetTotalCount
169	0	destinationIPv6Prefix

ElementID	PEN	Name
170	0	sourceIPv6Prefix
171	0	postOctetTotalCount
172	0	postPacketTotalCount
173	0	flowKeyIndicator
174	0	postMCastPacketTotalCount
175	0	postMCastOctetTotalCount
176	0	icmpTypeIPv4
177	0	icmpCodeIPv4
178	0	icmpTypeIPv6
179	0	icmpCodeIPv6
180 个	0	udpSourcePort
181	0	udpDestinationPort
182	0	tcpSourcePort
183	0	tcpDestinationPort
184	0	tcpSequenceNumber
185	0	tcpAcknowledgementNumber
186	0	tcpWindowSize
187	0	tcpUrgentPointer
188	0	tcpHeaderLength
189	0	ipHeaderLength
190	0	totalLengthIPv4

ElementID	PEN	Name
191	0	payloadLengthIPv6
192 个	0	ipTTL
193	0	nextHeaderIPv6
194	0	mplsPayloadLength
195	0	ipDiffServCodePoint
196	0	ipPrecedence
197	0	fragmentFlags
198	0	octetDeltaSumOfSquares
199	0	octetTotalSumOfSquares
200	0	mplsTopLabelTTL
201	0	mplsLabelStackLength
202	0	mplsLabelStackDepth
203	0	mplsTopLabelExp
204	0	ipPayloadLength
205	0	udpMessageLength
206	0	isMulticast
207	0	ipv4IHL
208	0	ipv4Options
209	0	tcpOptions
210	0	paddingOctets
211	0	collectorIPv4Address

ElementID	PEN	Name
212	0	collectorIPv6Address
213	0	exportInterface
214	0	exportProtocolVersion
215	0	exportTransportProtocol
216	0	collectorTransportPort
217	0	exporterTransportPort
218	0	tcpSynTotalCount
219	0	tcpFinTotalCount
220	0	tcpRstTotalCount
221	0	tcpPshTotalCount
222	0	tcpAckTotalCount
223	0	tcpUrgTotalCount
224	0	ipTotalLength
225	0	postNATSourceIPv4Address
226	0	postNATDestinationIPv4Address
227	0	postNAPTSourceTransportPort
228	0	postNAPTDestinationTransportPort
229	0	natOriginatingAddressRealm
230	0	natEvent
231	0	initiatorOctets
232	0	responderOctets

ElementID	PEN	Name
233	0	firewallEvent
234	0	ingressVRFID
235	0	egressVRFID
236	0	VRFname
237	0	postMplsTopLabelExp
238	0	tcpWindowScale
239	0	biflowDirection
240	0	ethernetHeaderLength
241	0	ethernetPayloadLength
242	0	ethernetTotalLength
243	0	dot1qVlanId
244	0	dot1qPriority
245	0	dot1qCustomerVlanId
246	0	dot1qCustomerPriority
247	0	metroEvcId
248	0	metroEvcType
249	0	pseudoWireId
250	0	pseudoWireType
251	0	pseudoWireControlWord
252	0	ingressPhysicalInterface
253	0	egressPhysicalInterface

ElementID	PEN	Name
254	0	postDot1qVlanId
255	0	postDot1qCustomerVlanId
256	0	ethernetType
257	0	postIpPrecedence
258	0	collectionTimeMilliseconds
259	0	exportSctpStreamId
260	0	maxExportSeconds
261	0	maxFlowEndSeconds
262%	0	messageMD5Checksum
263	0	messageScope
264	0	minExportSeconds
265	0	minFlowStartSeconds
266	0	opaqueOctets
267	0	sessionScope
268	0	maxFlowEndMicroseconds
269	0	maxFlowEndMilliseconds
270	0	maxFlowEndNanoseconds
271	0	minFlowStartMicroseconds
272	0	minFlowStartMilliseconds
273	0	minFlowStartNanoseconds
274	0	collectorCertificate

ElementID	PEN	Name
275	0	exporterCertificate
276	0	dataRecordsReliability
277	0	observationPointType
278	0	newConnectionDeltaCount
279	0	connectionSumDurationSeconds
280	0	connectionTransactionId
281	0	postNATSourceIPv6Address
282	0	postNATDestinationIPv6Address
283	0	natPoolId
284	0	natPoolName
285	0	anonymizationFlags
286	0	anonymizationTechnique
287	0	informationElementIndex
288	0	p2pTechnology
289	0	tunnelTechnology
290	0	encryptedTechnology
291	0	basicList
292	0	subTemplateList
293	0	subTemplateMultiList
294	0	bgpValidityState
295	0	IPSecSPI

ElementID	PEN	Name
296	0	greKey
297	0	natType
298	0	initiatorPackets
299	0	responderPackets
300	0	observationDomainName
301	0	selectionSequenceId
302	0	selectorId
303	0	informationElementId
304	0	selectorAlgorithm
305	0	samplingPacketInterval
306	0	samplingPacketSpace
307	0	samplingTimeInterval
308	0	samplingTimeSpace
309	0	samplingSize
310	0	samplingPopulation
311	0	samplingProbability
312	0	dataLinkFrameSize
313	0	ipHeaderPacketSection
314	0	ipPayloadPacketSection
315	0	dataLinkFrameSection
316	0	mplsLabelStackSection

ElementID	PEN	Name
317	0	mplsPayloadPacketSection
318	0	selectorIdTotalPktsObserved
319	0	selectorIdTotalPktsSelected
320	0	absoluteError
321	0	relativeError
322	0	observationTimeSeconds
323	0	observationTimeMilliseconds
324	0	observationTimeMicroseconds
325	0	observationTimeNanoseconds
326	0	digestHashValue
327	0	hashIPPayloadOffset
328	0	hashIPPayloadSize
329	0	hashOutputRangeMin
330	0	hashOutputRangeMax
331	0	hashSelectedRangeMin
332	0	hashSelectedRangeMax
333	0	hashDigestOutput
334	0	hashInitialiserValue
335	0	selectorName
336	0	upperCILimit
337	0	lowerCILimit

ElementID	PEN	Name
338	0	confidenceLevel
339	0	informationElementDataType
340	0	informationElementDescription
341	0	informationElementName
342	0	informationElementRangeBegin
343	0	informationElementRangeEnd
344	0	informationElementSemantics
345	0	informationElementUnits
346	0	privateEnterpriseNumber
347	0	virtualStationInterfaceId
348	0	virtualStationInterfaceName
349	0	virtualStationUUID
350	0	virtualStationName
351	0	layer2SegmentId
352	0	layer2OctetDeltaCount
353	0	layer2OctetTotalCount
354	0	ingressUnicastPacketTotalCount
355	0	ingressMulticastPacketTotalCount
356 家	0	ingressBroadcastPacketTotalCount
357	0	egressUnicastPacketTotalCount
358	0	egressBroadcastPacketTotalCount

ElementID	PEN	Name
359	0	monitoringIntervalStartMilliSeconds
360	0	monitoringIntervalEndMilliSeconds
361	0	portRangeStart
362	0	portRangeEnd
363	0	portRangeStepSize
364	0	portRangeNumPorts
365	0	staMacAddress
366	0	staIPv4Address
367	0	wtpMacAddress
368	0	ingressInterfaceType
369	0	egressInterfaceType
370	0	rtpSequenceNumber
371	0	userName
372	0	applicationCategoryName
373	0	applicationSubCategoryName
374	0	applicationGroupName
375	0	originalFlowsPresent
376	0	originalFlowsInitiated
377	0	originalFlowsCompleted
378	0	distinctCountOfSourceIPAddress
379	0	distinctCountOfDestinationIPAddress

ElementID	PEN	Name
380	0	distinctCountOfSourceIPv4Address
381	0	distinctCountOfDestinationIPv4Address
382	0	distinctCountOfSourceIPv6Address
383	0	distinctCountOfDestinationIPv6Address
384	0	valueDistributionMethod
385	0	rfc3550JitterMilliseconds
386	0	rfc3550JitterMicroseconds
387	0	rfc3550JitterNanoseconds
388	0	dot1qDEI
389	0	dot1qCustomerDEI
390	0	flowSelectorAlgorithm
391	0	flowSelectedOctetDeltaCount
392	0	flowSelectedPacketDeltaCount
393	0	flowSelectedFlowDeltaCount
394	0	selectorIDTotalFlowsObserved
395	0	selectorIDTotalFlowsSelected
396	0	samplingFlowInterval
397	0	samplingFlowSpacing
398	0	flowSamplingTimeInterval
399	0	flowSamplingTimeSpacing
400	0	hashFlowDomain

ElementID	PEN	Name
401	0	transportOctetDeltaCount
402	0	transportPacketDeltaCount
403	0	originalExporterIPv4Address
404	0	originalExporterIPv6Address
405	0	originalObservationDomainId
406	0	intermediateProcessId
407 个	0	ignoredDataRecordTotalCount
408	0	dataLinkFrameType
409	0	sectionOffset
410	0	sectionExportedOctets
411	0	dot1qServiceInstanceTag
412	0	dot1qServiceInstanceId
413	0	dot1qServiceInstancePriority
414	0	dot1qCustomerSourceMacAddress
415	0	dot1qCustomerDestinationMacAddress
417	0	postLayer2OctetDeltaCount
418	0	postMCastLayer2OctetDeltaCount
420	0	postLayer2OctetTotalCount
421	0	postMCastLayer2OctetTotalCount
422	0	minimumLayer2TotalLength
423	0	maximumLayer2TotalLength

ElementID	PEN	Name
424	0	droppedLayer2OctetDeltaCount
425	0	droppedLayer2OctetTotalCount
426	0	ignoredLayer2OctetTotalCount
427	0	notSentLayer2OctetTotalCount
428	0	layer2OctetDeltaSumOfSquares
429	0	layer2OctetTotalSumOfSquares
430	0	layer2FrameDeltaCount
431	0	layer2FrameTotalCount
432	0	pseudoWireDestinationIPv4Address
433	0	ignoredLayer2FrameTotalCount
434	0	mibObjectValueInteger
435	0	mibObjectValueOctetString
436	0	mibObjectValueOID
437	0	mibObjectValueBits
438	0	mibObjectValueIPAddress
439	0	mibObjectValueCounter
440	0	mibObjectValueGauge
441	0	mibObjectValueTimeTicks
442	0	mibObjectValueUnsigned
443	0	mibObjectValueTable
444	0	mibObjectValueRow

ElementID	PEN	Name
445	0	mibObjectIdentifier
446	0	mibSubIdentifier
447	0	mibIndexIndicator
448	0	mibCaptureTimeSemantics
449	0	mibContextEngineID
450	0	mibContextName
451	0	mibObjectName
452	0	mibObjectDescription
453	0	mibObjectSyntax
454	0	mibModuleName
455	0	mobileIMSI
456	0	mobileMSISDN
457	0	httpStatusCode
458	0	sourceTransportPortsLimit
459	0	httpRequestMethod
460	0	httpRequestHost
461	0	httpRequestTarget
462	0	httpMessageVersion
463	0	natInstanceID
464	0	internalAddressRealm
465	0	externalAddressRealm

ElementID	PEN	Name
466	0	natQuotaExceededEvent
467	0	natThresholdEvent
468	0	httpUserAgent
469	0	httpContentType
470	0	httpReasonPhrase
471	0	maxSessionEntries
472	0	maxBIBEntries
473	0	maxEntriesPerUser
474	0	maxSubscribers
475	0	maxFragmentsPendingReassembly
476	0	addressPoolHighThreshold
477	0	addressPoolLowThreshold
478	0	addressPortMappingHighThreshold
479	0	addressPortMappingLowThreshold
480	0	addressPortMappingPerUserHighThreshold
481	0	globalAddressMappingHighThreshold
482	0	vpnIdentifier
483	0	bgpCommunity
484	0	bgpSourceCommunityList
485	0	bgpDestinationCommunityList
486	0	bgpExtendedCommunity

ElementID	PEN	Name
487	0	bgpSourceExtendedCommunityList
488	0	bgpDestinationExtendedCommunityList
489	0	bgpLargeCommunity
490	0	bgpSourceLargeCommunityList
491	0	bgpDestinationLargeCommunityList
33002	0	ASAFirewallExtendedEvent
34000	0	TrustSecSourceIdentifier
34001	0	TrustSecDestinationIdentifier
34002	0	TrustSecSourceName
34003	0	TrustSecDestinationName
1232	9	SGTSourceId_9
1233	9	SGTDestinationId_9
9292	9	AVCRespsCountDelta_9
9303	9	AVCSumRespTime_9
9306	9	AVCSumServerRespTime_9
12172	9	ETAInitialDataPacket_9
12173	9	ETASequenceOfPacketLengthsAndTimes_9
12184	9	ETASequenceOfPacketLengths_9
12185	9	ETASequenceOfPacketTimes_9
12235	9	AVCSubApplicationValueIPFIX_9
12332	9	NVMUdid_9

ElementID	PEN	Name
12333	9	NVMLoggedInUser_9
12334	9	NVMOsName_9
12335	9	NVMOsVersion_9
12336	9	NVMSystemManufacturer_9
12337	9	NVMSystemType_9
12338	9	NVMProcessAccount_9
12339	9	NVMParentProcessAccount_9
12340	9	NVMProcessName_9
12341	9	NVMProcessHash_9
12342	9	NVMParentProcessName_9
12343	9	NVMParentProcessHash_9
12344	9	NVMDnsSuffix_9
12345	9	NVMDestinationHostname_9
12346	9	NVML4ByteCountIn_9
12347	9	NVML4ByteCountOut_9
12351	9	NVMOsEdition_9
12352	9	NVMModuleNameList_9
12353	9	NVMModuleHashList_9
12355	9	NVMInterfaceInfoUid_9
12356	9	NVMInterfaceIndex_9
12357	9	NVMInterfaceType_9

ElementID	PEN	Name
12358	9	NVMInterfaceName_9
12359	9	NVMInterfaceDetailsList_9
12360	9	NVMInterfaceMacAddress_9
12361	9	NVMUserAccountType_9
12362	9	NVMProcessAccountType_9
12363	9	NVMParentProcessAccountType_9
12364	9	NVMAgentVersion_9
12365	9	NVMProcessId_9
12366	9	NVMParentProcessId_9
12367	9	NVMProcessPath_9
12368	9	NVMParentProcessPath_9
12369	9	NVMProcessArgs_9
12370	9	NVMParentProcessArgs_9
12371	9	NVMFlowStartMsec_9
12372	9	NVMFlowEndMsec_9
12172	8712	FlowSensorEtaInitialDataPacket_8712
12173	8712	FlowSensorEtaSequenceOfPacketLengthsAndTimes_8712
29794	8712	FlowSensorInitiator_8712
29795	8712	FlowSensorTcpSynAckTotalCount_8712
29796	8712	FlowSensorTcpSrsTotalCount_8712

ElementID	PEN	Name
29797	8712	FlowSensorRoundTripTime_8712
29798	8712	FlowSensorServerResponseTime_8712
29799	8712	FlowSensorRetransmits_8712
29800	8712	FlowSensorTcpBadTotalCount_8712
29801	8712	FlowSensorTcpFragTotalCount_8712
29802	8712	FlowSensorSourceEmailIn_8712
29803	8712	FlowSensorSourceEmailOut_8712
29804	8712	FlowSensorSourceEmailInMess_8712
29805	8712	FlowSensorSourceEmailOutMess_8712
29806	8712	FlowSensorSourceEmailInTrys_8712
29807	8712	FlowSensorSourceEmailOutTrys_8712
29808	8712	FlowSensorDestinationEmailIn_8712
29809	8712	FlowSensorDestinationEmailOut_8712
29810	8712	FlowSensorDestinationEmailInMess_8712
29811	8712	FlowSensorDestinationEmailOutMess_8712
29812	8712	FlowSensorDestinationEmailInTrys_8712
29813	8712	FlowSensorDestinationEmailOutTrys_8712
29814	8712	FlowSensorTraces_8712
29817	8712	FlowSensorEmbIcmpProtocol_8712
29818	8712	FlowSensorEmbIcmpType_8712
29819	8712	FlowSensorEmbIcmpCode_8712

ElementID	PEN	Name
29820	8712	FlowSensorApplicationIdentifier_8712
29821	8712	FlowSensorBadFlagXmas_8712
29822	8712	FlowSensorBadFlagSynFin_8712
29823	8712	FlowSensorBadFlagBadRst_8712
29824	8712	FlowSensorBadFlagNoAck_8712
29825	8712	FlowSensorBadFlagUrg_8712
29826	8712	FlowSensorBadFlagNoflag_8712
29828	8712	FlowSensorShortFragAttack_8712
29829	8712	FlowSensorFragPktTooShort_8712
29830	8712	FlowSensorFragPktTooLong_8712
29831	8712	FlowSensorFragDifferentSizes_8712
29832	8712	FlowSensorApplicationDetails_8712
29833	8712	FlowSensorSrcSgt_8712
56701	25461	PaloAltoApplicationIdentifier_25461
56702	25461	PaloAltoUserIdentifier_25461

附录 B:支持的警报

下表包含思科遥测代理警报的列表。

Alert	说明
设备磁盘空间严重不足	设备磁盘的可用空间不足 1G。系统运行降级。
设备磁盘空间不足	此设备的磁盘使用率已达到其容量的 80%。
代理节点丢弃数据包	此节点正在丢弃数据包。请确保代理节点未过载或配置错误。
未发现代理节点	此节点已有 [x] 分钟未与管理器通信。
目标无法接通	此目标已发送“目标无法接通”ICMP 消息。
分配的 CPU 不足	尚未为此设备分配建议数量的 CPU。
分配的内存不足	尚未为此设备分配建议的内存量。
TLS 证书即将到期	管理器的 TLS 证书即将到期。请安装新的证书。
TLS 证书已过期	管理器的 TLS 证书已过期。请安装新的证书。

联系支持团队

如果需要技术支持人员，请执行以下操作之一：

- 联系您当地的思科遥测代理合作伙伴
- 联系思科遥测代理支持
- 通过以下网址反映问题：http://www.cisco.com/c/en/us/support/index.html
- 通过以下邮箱反映问题：tac@cisco.com
- 美国支持电话：1-800-553-2447
- 全球支持电话：https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

更改历史记录

文档版本	发布日期 (Published Date)	说明
1_0	2023 年 4 月	初始版本
1_1	2023 年 6 月	对“Azure 配置”部分进行了一些编辑。

版权信息