Stealthwatch® 管理控制台

用户指南

（面向 Stealthwatch 系统 v6.9）

本手册中有关产品的规格和信息如有更改，恕不另行通知。本手册中的所有声明、信息和建议均准确可靠，但我们不为其提供任何明示或暗示的担保。用户必须承担使用产品的全部责任。

随附产品的软件许可和有限担保在随产品一起提供的信息包中提供，且构成本文的一部分。如果您无法找到软件许可或有限担保，请与思科代表联系获取副本。

思科所采用的 TCP 报头压缩是加州大学伯克利分校 (UCB) 开发的一个程序的改版，是 UCB 的 UNIX 操作系统公共域版本的一部分。保留所有权利。版权所有 © 1981，加州大学董事会。

无论本手册中是否有任何其他担保，这些供应商的所有文档文件和软件均按“原样”提供，可能包含缺陷。思科和上面所提及的供应商拒绝所有明示或暗示保证，包括（但不限于）适销性、特定用途适用性和无侵权保证，或者因买卖或使用以及商业惯例所引发的保证。

在任何情况下，对于任何间接、特殊、连带发生或偶发的损坏，包括（但不限于）因使用或无法使用本手册而导致的任何利润损失或数据损失或损坏，思科及其供应商概不负责，即使思科及其供应商已获知此类损坏的可能性也不例外。

本文档中使用的任何互联网协议 (IP) 地址和电话号码并非实际地址和电话号码。本文档中所含的任何示例、命令显示输出、网络拓扑图和其他图形仅供说明之用。说明性内容中用到的任何真实 IP 地址或电话号码纯属巧合，并非有意使用。

所有打印副本和软拷贝均被视为非受控副本，应以原始在线版本为最新版本。

思科在全球设有 200 多个办事处。思科网站 www.cisco.com/go/offices 上列出了各办事处的地址、电话和传真。

目录

1

关于本指南

概述

本指南提供使用 Stealthwatch 管理控制台 (SMC) 软件以最大程度减少网络性能问题和安全风险的“最佳实践”指南。鉴于网络的复杂性和多样性，本指南并非一份全面的用户指南，而旨在就使用 SMC 软件处理和/或防止网络性能问题或网络威胁，提供最佳方法指导。

本章包含以下主题：

注意：

*SMC 客户端联机帮助*包含有关使用 SMC 软件不同组件的全部有用信息。

受众

本指南的主要受众是使用 SMC 软件的任何人，从日常用户到管理员。我们假设您已经对网络概念以及以下 Stealthwatch 系统概念有了大致的了解：

- 主机数
- 流
- 服务
- 应用
- 索引
- SMC 文档和导航

关于 SMC

Stealthwatch 管理控制台 (SMC) 是一个企业级安全管理系统，它允许网络管理员从一个位置定义、配置和监控多个分布式 Stealthwatch 流收集器。此系统可在物理和虚拟环境中提供基于流的安全性、网络和应用性能监控。使用 Stealthwatch，网络运营和安全团队可以查看谁在使用网络、正在使用哪些应用和服务以及它们的执行效果如何。

通过使用表、饼图、图形和报告，管理员可以快速检测安全威胁并确定其优先级、查明网络误用和次优性能以及管理整个企业的事件响应，而且所有这些均可从单个控制中心完成。Stealthwatch 会快速放大任何异常行为，并立即向 SMC 发送警报，其中包含安全人员采取快速、果断的措施来减少任何潜在危害所需的情景信息。

SMC 用户界面

v6.5.0 之后，Stealthwatch 系统将在一段时间内使用两个用户界面（即管理控制台）来显示传感器数据并提供管理功能，例如定义策略。现有的界面将继续可用，但将逐渐被淘汰。其功能正在转移到新的 Stealthwatch Web 应用接口。在过渡期间，您需要使用这两种 UI。每个 UI 的在线帮助将在必要时提醒您需要从一个 UI 切换到另一 UI。

SMC：SMC 以图形、表和过滤器提供信息。过滤器包括单独的（有时多个）页面或对话框。

Web 应用：新格式使用更直观方法，包括您在商业网站上找到的元素，例如用于缩小查询关注范围的过滤器窗格。启动 Stealthwatch 系统时，将打开此 UI。如果需要，您可以从其访问 SMC 客户端接口。

如何使用本指南

除了此简介，我们将此指南分为以下各章，以及一个索引：

本章...	说明如何...
2 - 许可 Stealthwatch 设备	对您的 Stealthwatch 设备授权。
3 - 浏览 SMC 客户端界面	使用 SMC 中常见导航元素。
4 - 主机管理	将主机分组，以便您可以通过使用策略来控制其行为。
5 - 视图和控制面板	查看对代表 SMC 中最重要活动的数据的各种表格和图形显示。
6 - 指数：行为更改排名	使用索引来跟踪异常行为。
7 - 监控流量和网络性能	监控流量，以及服务器和网络响应时间。
8 - 分析流	分析进出主机的流以确定趋势。
9 - SLIC 威胁源服务	使用 Stealthwatch 的在线威胁情报服务。
10 - 发现原因	确认并关闭警报，使用自动缓解功能并手动阻止源。
11 - 响应警报	调整策略以减少您看到的不必要警报数量。
12 - 减少不必要的警报	找到引起警报的第一个主机以及所影响的主机。
13 - 处理文档	保存、共享和计划包含指定组件的自定义文档。
14 - 管理用户	管理与用户关联的用户访问权和角色。

文档图标

此文档使用以下图标表示重要信息：

图标	含义	包括信息...
	提示	如执行某项任务的快捷键或简便方式。
	备注	在您使用此文档或 Stealthwatch 系统时会发现十分有用。
	重要	您必须遵守以防重大后果，如软件功能故障。
	小心	您必须进行观察，防止数据丢失或硬件受损。

缩写

本指南中运用了以下缩写：

缩写	定义
AS（编号）	自治系统
CI	关注指数
CIDR	无类域间路由
CSV	逗号分隔值
DAR	磁盘存档
DHCP	动态主机配置协议
DNS	域名系统（服务或服务器）
DoS	拒绝服务
DSCP	差分服务代码点
FSI	文件共享指数
IANA	互联网编号指派机构
ID	标识符
IM	即时消息
IP	Internet 协议
MAC	介质访问控制
MPLS	多协议标签交换
PDF	便携式文档格式
P2P	点对点
RADIUS	远程身份验证拨入用户服务
RFC	征求意见
RTT	往返时间
SMC	StealthWatch 管理控制台
SNMP	简单网络管理协议
SRT	服务器响应时间
TACACS	终端访问控制器访问控制系统
TCP	传输控制协议
TI	目标指数
UDP	用户数据报协议

缩写	定义
UI	用户界面
URL	统一资源定位符
VLAN	虚拟局域网
VM	虚拟机
VPN	虚拟专用网络

其他资源

除本指南之外，如下文档和在线资源也可能很有用。

相关文档

有关 Stealthwatch 产品的附加信息，可以转至 Stealthwatch 用户社区网站查看 (community.lancope.com)。

NetFlow Ninjas 博客

Lancope 的 *NetFlow Ninjas* 博客 (http://www.lancope.com/blog) 提供有关 NetFlow、NetFlow 行业和新的 Stealthwatch 功能的重要信息，以及有关如何使用 Stealthwatch 的提示和诀窍。

Stealthwatch 视频库

Stealthwatch 在线视频库 (http://www.lancope.com/resource-center/videos) 展示 Stealthwatch 系统在网络性能和安全管理方面的优势。

联系支持人员

如果您需要技术支持，请执行以下其中一项操作：

- 联系您当地的 Lancope 合作伙伴。
- 要获得电子邮件支持，请访问 Lancope 客户社区网站 community.lancope.com。
- 致电 +1 800-838-6574。
- 使用 Lancope 客户社区网站 community.lancope.com 上的支持表提交支持请求。

您将需要提供以下信息：

- 您的姓名
- 您的公司名称
- 位置

2

许可 STEALTHWATCH 设备

概述

V6.3 之后，Stealthwatch 产品的许可要求已更改。无论您是直接从 Lancope 购买产品还是通过 Lancope 的合作伙伴购买产品，Stealthwatch 系统的所有新安装和升级都需要一个有效的许可证。

您可能需要查看库存报告，以帮助您确定您的许可需求是什么。此报告提供有关您的系统上安装的 Lancope 产品的详细信息。

注意：

有关库存报告的详细信息，请参阅“功能许可证状态”（第 28 页）和 *SMC 客户端在线帮助*。

本章包含以下主题：

激活许可证

以下 Stealthwatch 设备必须获得许可：

- SMC
- 流量收集器
- FlowSensor
- UDP 导向器（又称 FlowReplicator）

每个许可证都与设备序列号关联。如果您有多台相同类型的设备（无论是物理设备还是虚拟设备），则务必要为每台设备安装许可证。

以下 Stealthwatch 功能也必须获得许可：

- Stealthwatch 模块
- DDoS 模块
- 每秒的流数 (FPS)
- Stealthwatch 实验室情报中心 (SLIC) 威胁源
- 身份服务

有关新部署的初始许可的说明，请参阅 *下载和许可 Stealthwatch 产品*文档。使用本节中的过程向当前部署中添加新的许可证或更新现有的许可证。

要购买新的许可证或为设备或功能续订现有许可证，请执行下列操作之一：

- 联系您当地的 Lancope 合作伙伴。
- 致电 +1 888-419-1462
- 发送邮件至 sales@lancope.com。

下载和许可证中心

Lancope 下载和许可中心是一种在线软件交付服务，可帮助您管理帐户并更新您的 Stealthwatch 产品，包括许可证。当您购买设备、功能或许可证时，系统会将您定位至“下载和许可中心证中心”，如以下部分所述。我们建议您定期检查“下载和许可证中心”以获得新软件版本相关信息。您随时可以通过转至以下网址访问您的帐户：https://lancope.flexnetoperations.com。您的登录 ID 是您的邮件地址。

注意：

如果您直接从 Lancope 购买物理 Stealthwatch 设备，并且您的 SMC 具有互联网访问权限，则无需访问“下载和许可证中心”就可以激活许可证。

如果您对“下载和许可证中心”有疑问或问题，请联系 lancope@flexnetoperations.com 或致电 1-888-715-4687（美国境内）或 1-408-642-3965（美国境外）。

托管设备和非托管设备

托管设备与 SMC 直接通信，而非托管（独立）设备则不这样。以下列表指明哪些 Stealthwatch 设备是托管设备，哪些是独立设备：

- 流收集器始终是托管设备。
- FlowSensor 可以是托管设备，也可以是独立设备。
- UDP 导向器（又称 FlowReplicator）始终是独立设备。

注意：

使用设备管理 (Admin) 界面可激活独立设备的许可证。有关如何使用设备管理界面激活非托管设备的许可证的信息，请参阅*设备管理在线帮助*。

激活许可证

要为某功能或托管设备激活新的许可证或更新现有的许可证，请完成以下步骤：

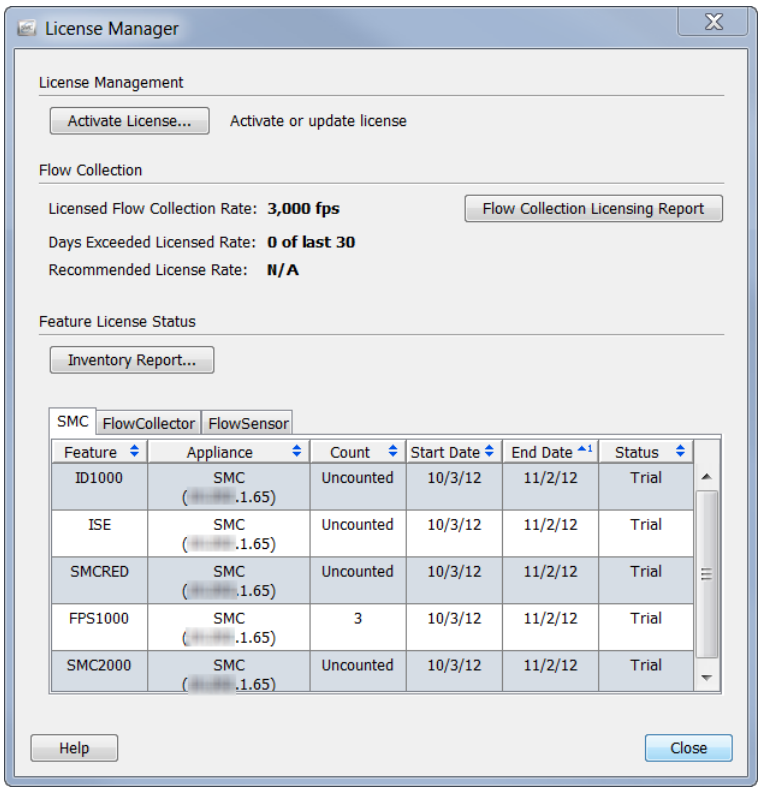
1. 您是否收到了设备或功能的任何许可证令牌？
   - 如果收到，请转到步骤 2。
   - 如果没有，请转到步骤 3。
2. 如果您收到了任何许可证令牌，请访问“下载和许可证中心”，将许可证令牌添加到您的帐户，然后注册相应的产品。有关说明，请参阅网站的“许可文档”部分。

3. 这是否是虚拟设备？
   - 如果是，请转到步骤 4。
   - 如果不是，请转到步骤 5。
4. 如果这是虚拟设备，请按照适用的 *Stealthwatch VE 安装和配置指南*中的说明安装和配置设备。
5. 此 SMC 是否连接到了互联网？
   - 如果是，请转到 “激活许可证 – 在线方法”（第 22 页）。
   - 如果不是，请转到 “激活许可证 – 离线方法”（第 24 页）。

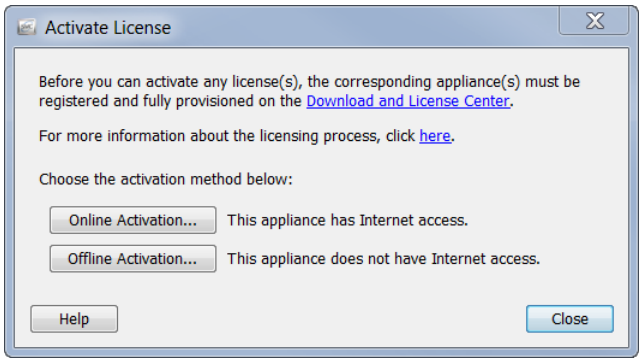
激活许可证 - 在线方法

要在 SMC 连接到互联网时激活某功能或托管设备的许可证，请完成以下步骤：

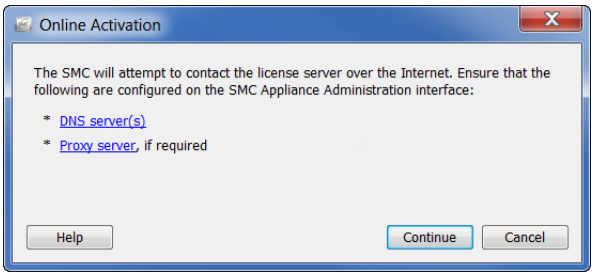
1. 访问 SMC 客户端界面。
2. 从主菜单中，选择**帮助 > 许可证管理**。系统随即会打开“许可证管理器”对话框：



3. 点击**激活许可证**。系统会打开“激活许可证”对话框：

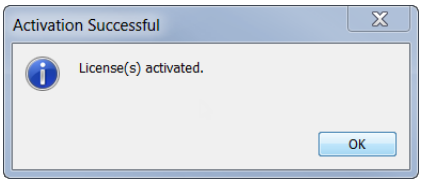


4. 点击**在线激活**。系统会打开“联机激活”对话框：

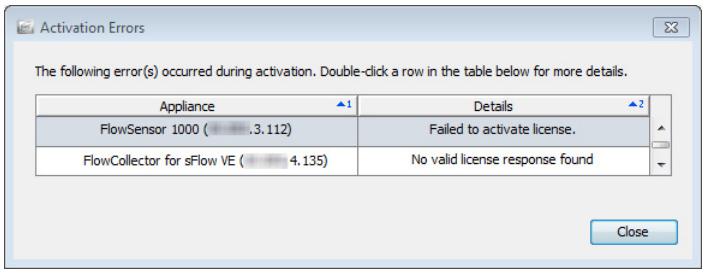


5. 点击**继续**。

- 如果此过程成功完成，系统会打开一个确认对话框。点击**确定**，关闭对话框。



- 如果激活失败，系统会打开一个错误对话框，列出此过程失败的每个设备。双击表中的行可获取更多详细信息。点击**关闭**以关闭对话框。



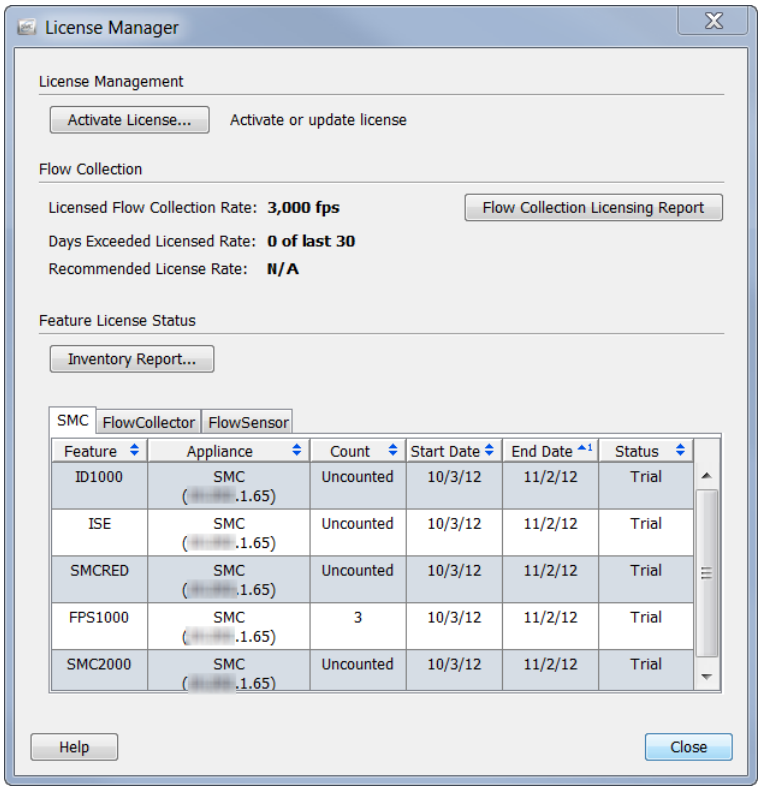
激活许可证 - 离线方法

要在 SMC 未连接到互联网时激活某功能或托管设备的许可证，请完成以下步骤：

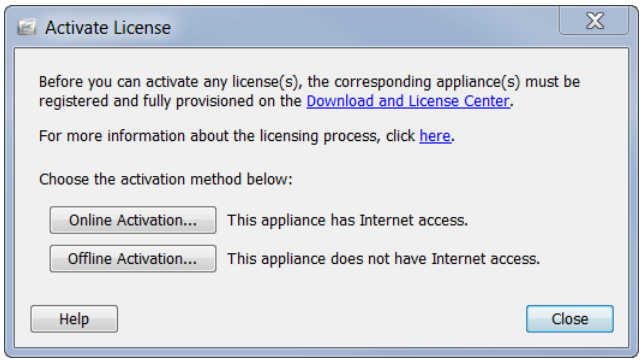
1. 转到获有互联网访问权限的计算机。
2. 访问“下载和许可证中心” (https://lancope.flexnetoperations.com) 并转至“我的设备”页面。
3. 选择适当的设备并将许可证下载到您的本地硬盘驱动器、网络位置或便携式设备（如闪存驱动器）。

   您可以下载单个许可证 (BIN) 文件，也可以下载多个许可证。如果下载多个许可证，可以将所有 BIN 文件存储在单个目录或 ZIP 文件中。
4. 转到用于访问 SMC 客户端界面的计算机。
5. 访问 SMC 客户端界面。
6. 从主菜单中，选择**帮助 > 许可证管理**。

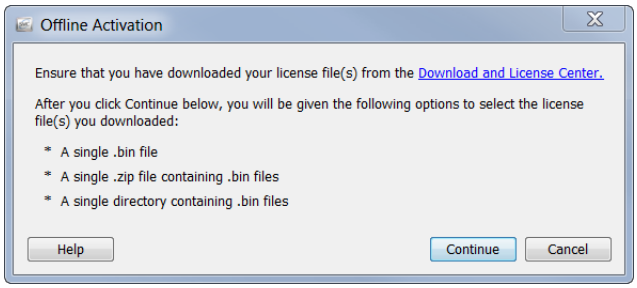
   系统随即会打开“许可证管理器”对话框：



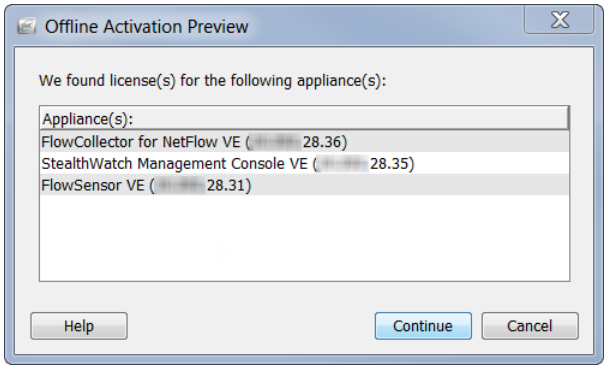
7. 点击**激活许可证**。系统会打开“激活许可证”对话框：



8. 点击**离线激活**。系统会打开“脱机激活”对话框。

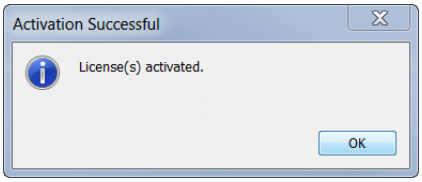


9. 点击**继续**。系统会打开一个对话框，供您选择文件。
10. 导航到在步骤 3 中下载许可证文件的位置。
11. 选择 BIN 文件、包含多个 BIN 文件的目录或包含您需要许可的功能或设备许可证的 ZIP 文件。系统会打开“脱机激活预览”对话框，其中显示了其许可证现在可用的设备。

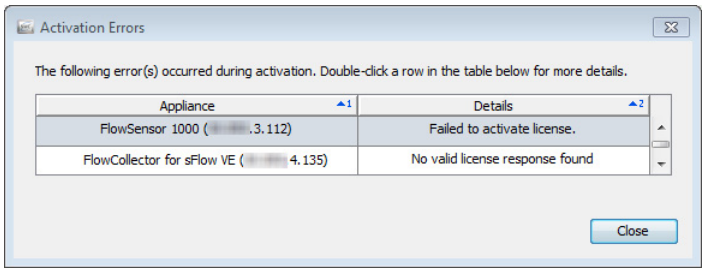


12. 点击**继续**。

- 如果此过程成功完成，系统会打开一个确认对话框。点击**确定**，关闭对话框。



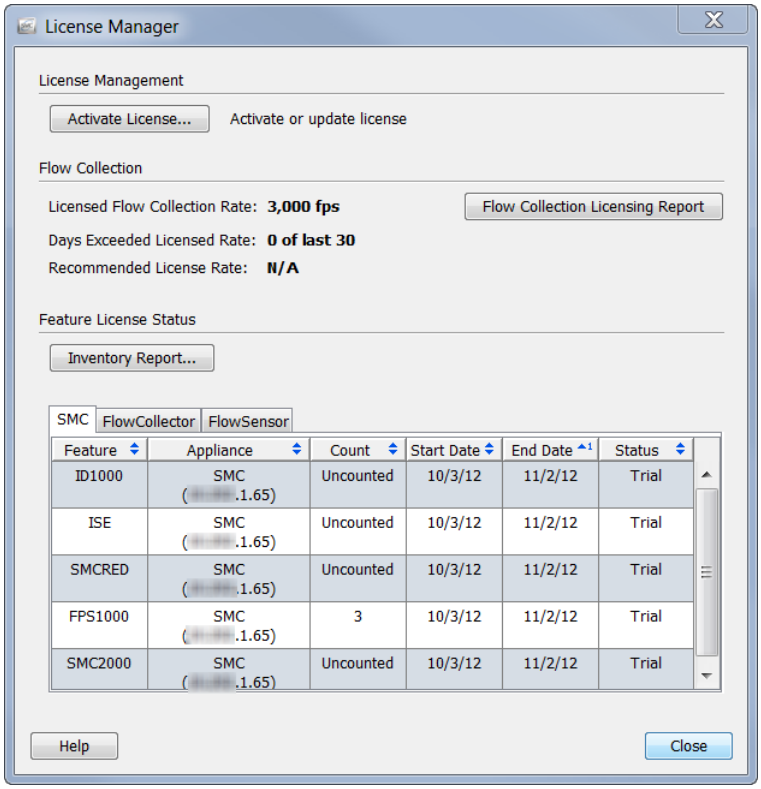
- 如果激活失败，系统会打开一个错误对话框，列出此过程失败的每个设备。双击表中的行可获取更多详细信息。点击**关闭**以关闭对话框。



许可证状态信息

如果要查看有关 SMC 和任何托管设备和功能的许可证信息，请完成以下步骤：

1. 访问 SMC 客户端界面。
2. 从主菜单中，选择**帮助 > 许可证管理**。系统随即会打开“许可证管理器”对话框：



此对话框将分为以下三部分：

- 许可证管理 - 此部分允许您激活许可证。有关如何执行此操作的信息，请参阅“激活许可证”（第 21 页）。
- 流收集 - 此部分提供有关您的流/秒 (FPS) 许可证的信息。有关详细信息，请参阅“流量收集”（第 28 页）。
- 功能许可证状态 - 此部分提供有关您的 SMC 和任何托管设备和功能的信息。有关详细信息，请参阅“功能许可证状态”（第 28 页）。

流量收集

“许可证管理器”对话框的“流收集”部分提供有关您的 FPS 许可证的信息，如下表所示：

项目	说明
许可流量收集速率	您的许可证允许的来自所有流收集器的最大流/秒数值（按第 95 个百分点）。如果此超过速率，将生成 Stealthwatch 流许可证超出警报。
超过许可速率天数	在过去 30 天中，您的系统超过许可证允许的每秒最大流量的天数。 **注意：**如果系统超过许可速率在 10 天以上，该值为红色。如果系统超过许可速率不足 10 天，该值为黄色。
建议的许可证速率	Lancope 根据过去 30 天内实际流量收集速率超过您的许可限制次数而建议对您的系统许可的 FPS 数值。
流收集许可报告	点击“流收集许可报告”按钮可查看 Stealthwatch 系统每天观察到的系统级流量速率 (FPS) 的图形和表格数据。可以使用此信息来确定您的实际使用量如何与您的许可证允许的限制对比。

功能许可证状态

“许可证管理器”对话框的“功能许可证状态”部分提供有关您的功能、SMC 和托管设备的信息：此表包含每个已许可设备的选项卡。其中每个选项卡都包含以下信息：

项目	说明
资产报告	点击“库存报告”按钮查看有关许可证的详细信息。此报告可帮助您确定实际的许可需求。
特性	许可的 Stealthwatch 产品类型，包括型号（如适用）。
设备	与许可证关联的设备的名称和 IP 地址。
计数	许可证允许的功能数。条目*未计数*表示“无限”。
- 续 -	

项目	说明
开始日期	此值取决于各种因素，如下所示： ▶ 如果这是永久的评估或预订许可证，则这是在“下载和许可中心”内提供许可证的日期。 ▶ 如果显示值*不适用*，则该功能存在于您的系统上，但未激活其许可证。 ▶ （仅限物理设备）如果这是试用许可证，则此日期是用户首次启动设备的日期。
结束日期	该许可证将到期的日期。
状态	每个许可证的状态。可能值如下： ▶ 已安装 - 此功能已安装在您的系统中并且已激活其许可证。 ▶ 未安装 - 系统具有此功能，但未激活其许可证。（“开始日期”显示状态为*不适用*。） ▶ 已过期 – 以下许可证之一已过期： • 评估许可证 • 预订许可证 • 30 天试用期许可证 ▶ 试用 -（仅限物理设备）许可证仍在其 30 天试用期内。

3

浏览 SMC 客户端界面

概述

SMC 客户端界面包含大量的文档，用于帮助您监控、保护和分析您的网络。大体熟悉这些文档的通用导航元素以及界面，可以帮助您更加熟练地使用 Stealthwatch，更高效地分析您的网络中的事件。

本章包含以下主题：

客户端内存分配

“客户端内存分配”下拉框允许您设置在您的客户端计算机上分配多少随机存取内存 (RAM) 来运行 SMC Java 客户端软件。如果您处理多个打开的文档或大数据集（例如，对超过 10 万条记录进行流查询），请考虑分配更大的内存。

您的计算机包含的 RAM 量必须至少是所选内存分配量的两倍。例如，对于具有 1024 MB 的计算机，您最多可以选择分配 512 MB；对于具有 4 GB 的计算机，您最多可以选择分配 2 GB。

您最多可以分配 2048 MB。如果您选择此数量，您必须具有 64 位 Java 功能且仅安装一个版本的 Java。

提示：

- 如果您发现 SMC 客户端接口似乎经常“挂起”，请尝试增大此值。
- 如果您收到涉及 Java 的错误消息，请尝试选择较低的内存分配。

您的视角

登录到 SMC 客户端界面后，您看到的视图将因您的登录权限而异（即，您的视角）。因此，您在办公室在 SMC 客户端界面上看到的内容与您在此指南中看到的有所不同。

您的 Stealthwatch 管理员在“用户与角色管理”对话框上定义您的登录权限。有关详细信息，请参阅第 14 章“管理用户。”

您可以创建自己的自定义控制面板，使其成为登录文档，或者选择已在 SMC 中设置的控制面板。您可以按需创建多个自定义控制面板。控制面板有许多不同的报告，包含任何带有您希望查看的数据的 SMC 组件。这可以让您关注您有兴趣查看的主要信息。

注意：

- 有关设置登录文档的信息，请参阅第 13 章“处理文档。”中的“登录文档”（第 278 页）
- 有关构建控制面板的信息，请参阅第 5 章“视图和控制面板。”

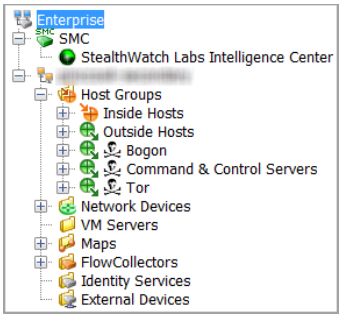
例如，域控制面板是一个您可能决定将其变成登录文档的文档，因为它可以提供有关域中的重要活动的图形和图表数据。此数据每 5 分钟从 SMC 收集一次。默认情况下，系统自动将域控制面板配置为管理员用户的登录文档。此外，它随时可用作针对新用户的计划文档；您只需启用 Stealthwatch 每日报告计划并包含此文档即可。

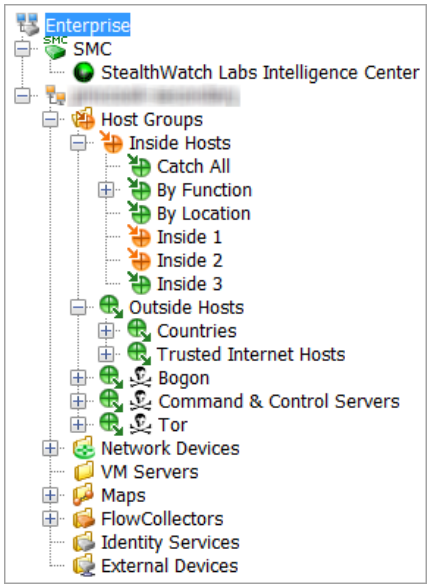
注意：

有关启用和计划文档的信息，请参阅第 14 章“管理用户。”中的“将计划文档与用户帐户关联”（第 311 页）

企业树和工具提示

SMC 客户端接口的左侧导航窗格中的项目列表通常被称为企业树。它也称为企业页面或主机组树。此树主要向您显示受监控网络的结构。





默认情况下，企业树中的选项处于折叠状态。若要同时展开树中的所有选项，请右键点击树中的任何项目，然后选择**全部展开**。若要同时折叠所有项目，请右键点击任何项目，然后选择**全部折叠**。若要完全隐藏企业树，请转至主菜单，并点击**查看 > 隐藏树**，或在键盘上按 **Ctrl+T**。SMC 将保存展开和折叠的文件夹设置。因此，在您下次登录时，企业树就会按照您离开时的方式显示。

搜索树

若要在企业树中搜索某个项目，请在企业树底部的“查找”字段中键入所需的文本 

。

注意：

“查找”字段默认处于隐藏状态。第一次打开该字段时您必须点击 **CTRL+F**，之后每次打开 SMC 时它都会显示。

您可以使用以下任何方法，在树中向前和向后搜索所需文本的其他实例：

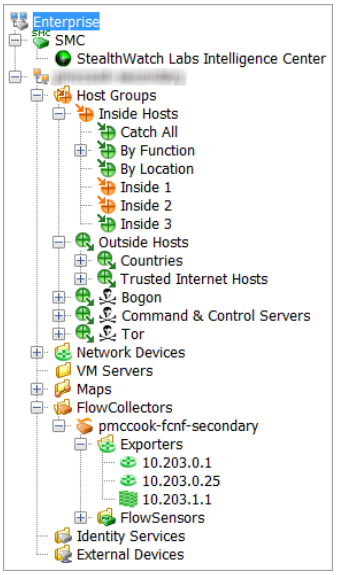
- 点击“查找”字段右侧的向下 和向上 按钮。
- 按键盘上的向下 (↓) 和向上 (↑) 箭头键。

提示：

在处理搜索时，您可以在 SMC 中继续执行其他操作。

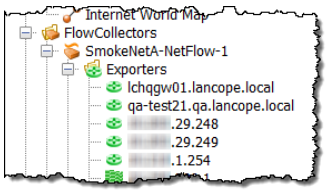
树分支

本示例中突出显示的企业树分支总是显示在企业树中。此分支代表所有 SMC 管理选项的顶级汇集点，包含由 SMC 监控的所有域。



根据您视角的不同，SMC 分支可能存在也可能不存在。此分支代表 SMC 设备自身。如果您的系统正在使用故障切换 SMC，您将同时看到主 SMC 分支和辅助 SMC 分支。

其他树分支代表 SMC 设备正在监控的域以及关联的主机组、Stealthwatch 流量收集器、Stealthwatch FlowSensor、虚拟机 (VM) 服务器（即，ESX 主机）、VM、映射、周边设备和外部设备。



要展开分支，请点击关联的加号 。您将看到的分支之一是“流量收集器”分支。若要查看在选定域上向 SMC 设备发送信息的流量收集器的列表，请通过点击关联的加号展开“流量收集器”分支。如果展开特定流量收集器的分支，可以看到其关联的 FlowSensor 设备、导出器和防火墙。

注意：

FlowSensor VE 同时显示在“FlowSensor”分支和“VM 服务器”分支下。

警报严重性级别

企业树分支使您能够立即查看网络中是否存在警报条件，因为图标会根据其指示的警报严重性级别更改颜色。SMC 自带已分配至各警报的默认严重性级别。但是，根据您的登录权限，您可以用警报配置对话框更改这些严重性级别分配，以适应网络环境的需要。下表列出了不同类型的严重性级别，每种类型由特定颜色指示：

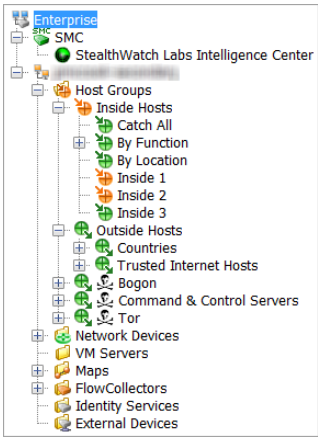
严重性级别	关联颜色
严重	红色
重大	橙色
次要	黄色
轻微	蓝色
说明性	淡蓝色
警报不存在	绿色

注意：

顶级分支图标显示任何下级分支发生的最高严重性警报的颜色。

查看菜单时，问自己以下问题：

- 有任何红色或橙色图标吗？如果是，则表明存在严重或重大警报条件。
- 您是否看到这个 图标？如果是，则表明与此图标旁边的设备的连接已丢失。
  - 您可能想要展开“内部主机”子树，以确定最重要或敏感主机组中是否存在警报。
  - 在主机组子树中，您可能需要打开一个主机组控制面板文档（本章稍后讨论）以获取更多信息。

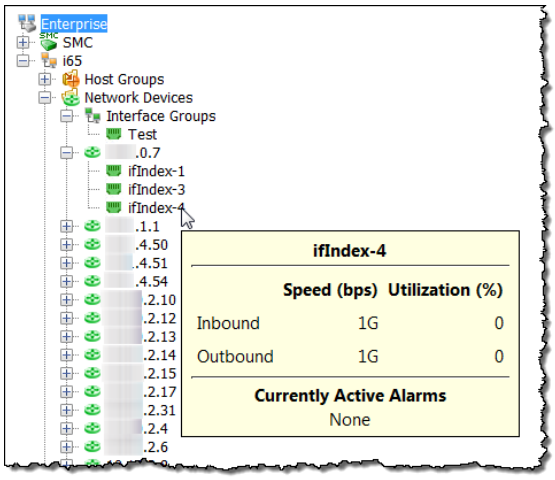


- SMC 图标是什么颜色？除绿色或灰色之外的任何颜色都表示 SMC 设备存在系统警报。

注意：

系统每分钟更新一次企业树。但您可以随时刷新以查看最新信息，方法是转到主菜单，然后依次点击**查看 > 刷新树**。您也可以右击企业树中的任意位置，然后选择**刷新树**。

企业树指示灯

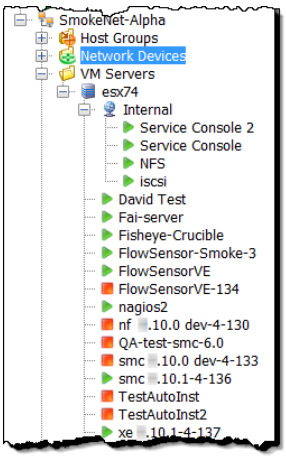


如果将光标悬停在分支上，则会出现工具提示，显示对象所经历的警报总数，包括每个警告的严重性级别。如果是“流量收集器”分支，您将看到警报信息和 Stealthwatch 设备的标识。此外，您将看到 SMC 上次尝试与设备通信、SMC 收到响应以及设备上次报告事件的时间。

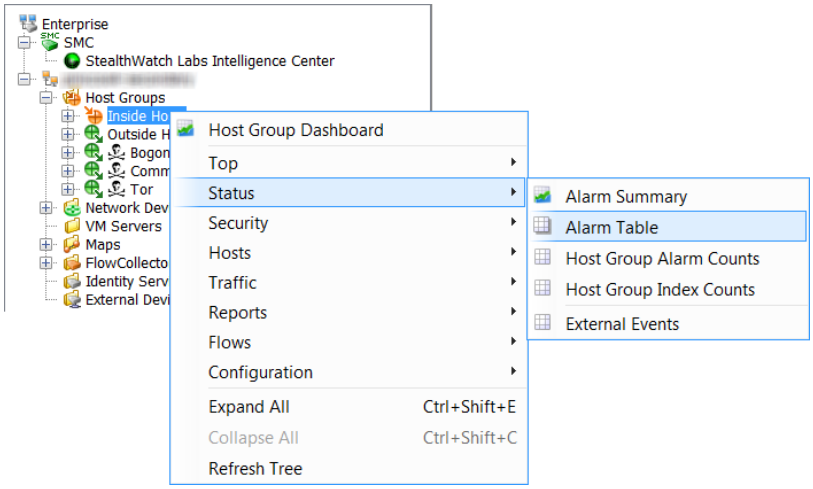
除了警报条件外，您还可以在企业树中看到 VM 的状态。以下图标指示 VM 是否已通电、已关闭或已暂停：

- – 已通电
- – 已关闭
- – 已暂停

环形图标 表示 VM 服务器资源组。地球图标 表示 VM 服务器内部的管理元素。

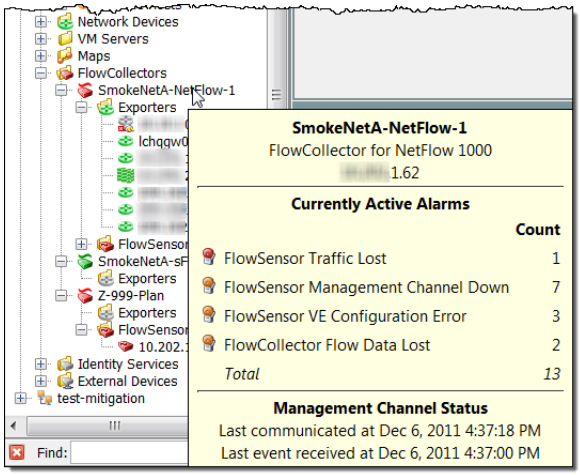


如果右键点击某个分支并选择**状态 > 警报表**，则可以查看该项目的更多警报信息。

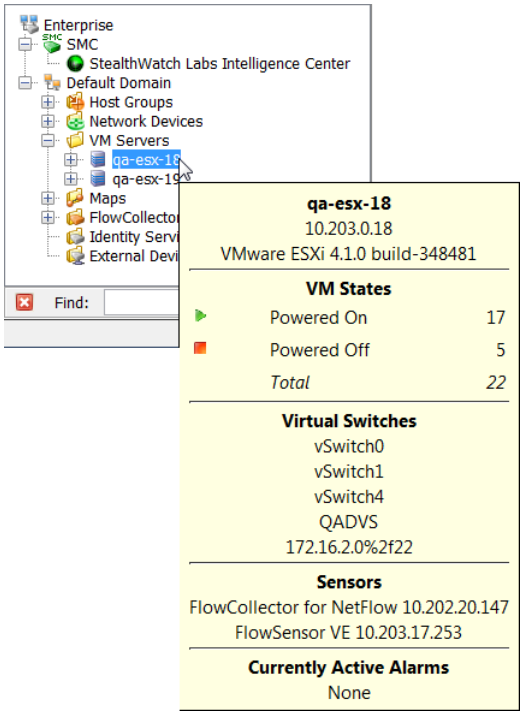


工具提示

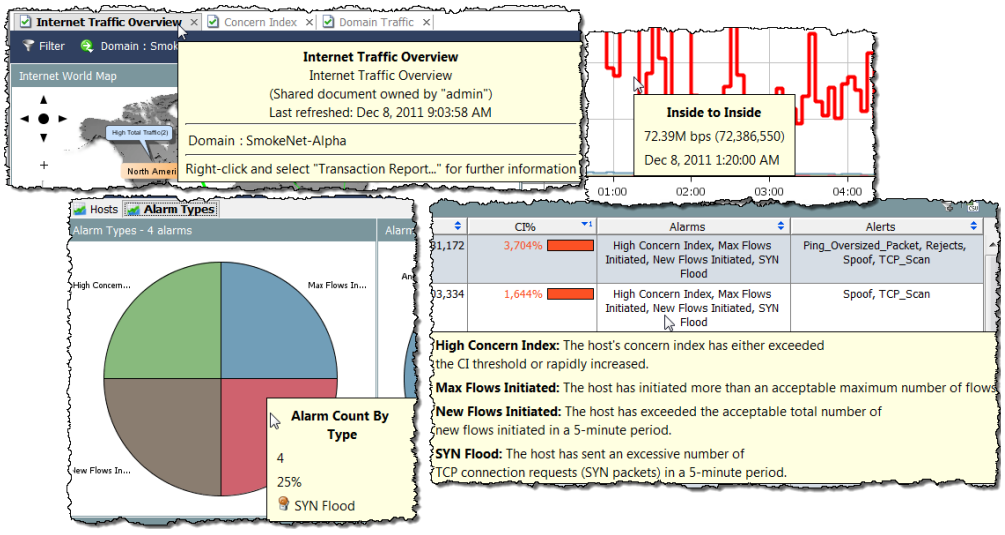
您可以将光标悬停在 SMC 客户端界面中的各个元素上，以在工具提示中显示有关该元素的摘要信息.例如，如果您将光标悬停在企业树中的流量收集器名称上，您将看到识别信息以及通信状态和流量收集器触发的任何警报。



同样，如果您的系统中具有 VM 服务器（即，ESX 主机），您将光标悬停在企业树中 VM 服务器名称上以显示工具提示，其中具有关于该 VM 服务器的名称、IP 地址和其他信息。



工具提示在 SMC 客户端界面中几乎无处不在。只需将光标悬停在某个元素（例如，选项卡、图形、图表或表单元格）上就可查看其相应的工具提示。



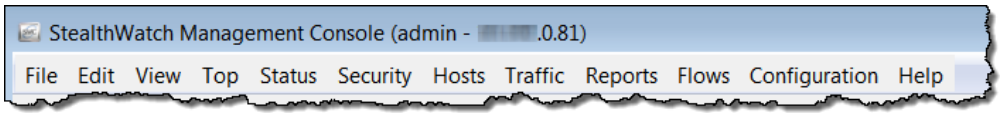
打开 SMC 文档

SMC 客户端界面允许您以多种方式打开文档，例如通过主菜单和右键点击功能。

注意：
文档也称为报告。本用户指南中存在互换使用这些术语的实例。

主菜单

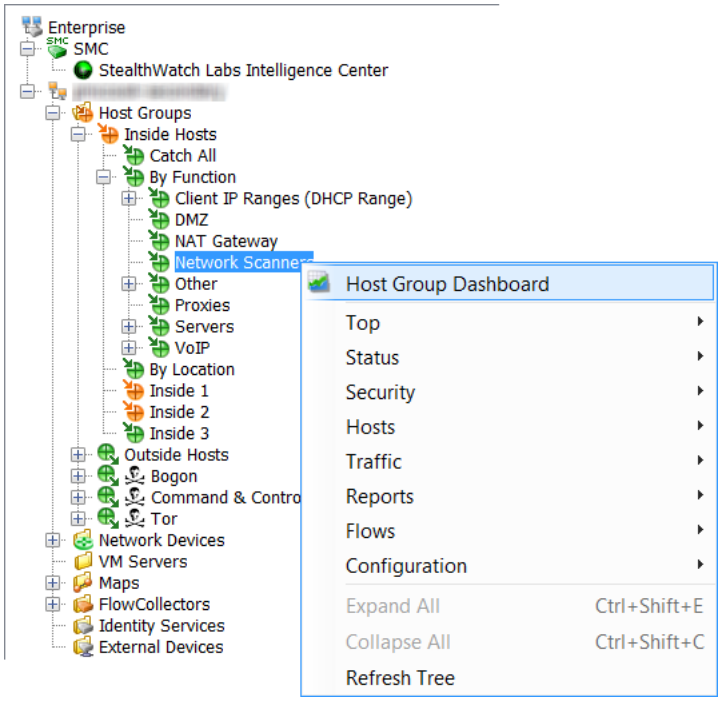
您可以从主菜单中点击菜单项来打开文档。



可用的选项将取决于以下三个主要因素：

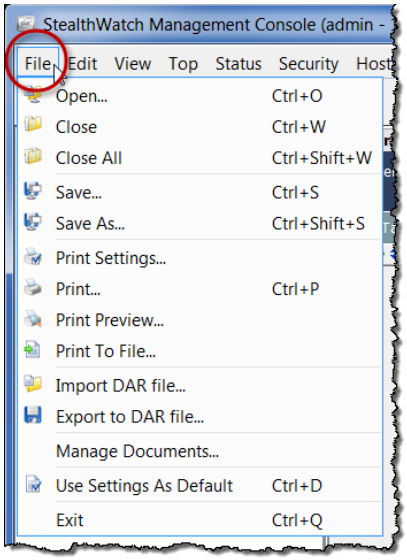
- 您在企业树中点击的内容
- 您在特定 SMC 文档中点击的内容
- 您的登录权限

例如，如果您在企业树中点击某个主机组，然后右键点击**主机组控制面板**，您将只看到该主机组的数据。



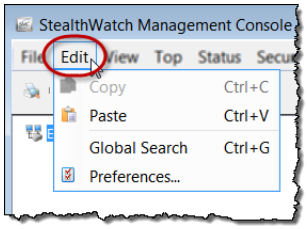
文件菜单

“文件”菜单提供处理 SMC 文档的选项，如打开、关闭、保存、打印和与其他用户共享文档。



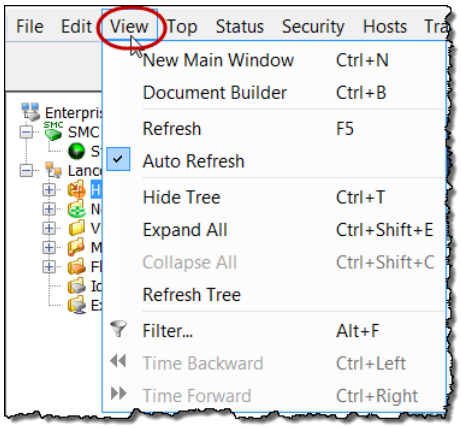
编辑菜单

“编辑”菜单提供用于复制、粘贴和搜索数据的选项，以及用于定义某些显示首选项的选项。



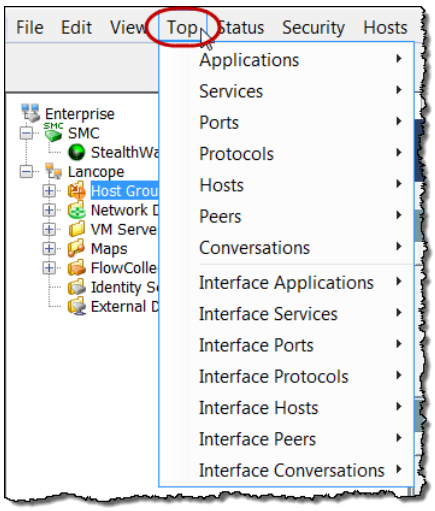
查看菜单

使用“视图”菜单，可以打开 SMC 用户界面的新实例、构建自定义控制面板、停止或启动自动刷新功能、手动刷新数据、以各种方式显示企业树或完全隐藏它、过滤数据或显示更早或更晚时间帧的数据。



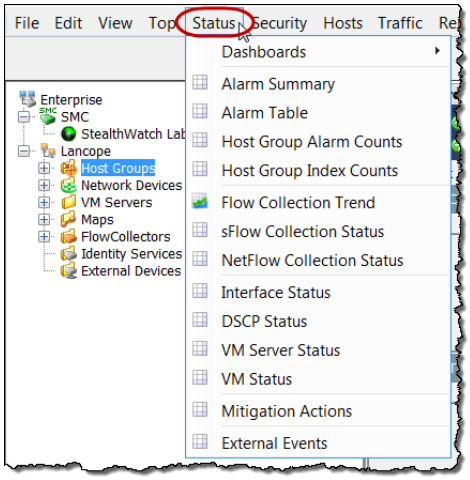
顶部菜单

“顶部”菜单允许您根据特定的条件（例如最常用的应用、最常用的服务、最常用的端口、最活跃的主机等）显示最流行的数据。您可以在整个网络中查看这些数据，也可以根据入站流量、出站流量、某个域或主机组中的流量或通过特定接口的流量将其进行细分。



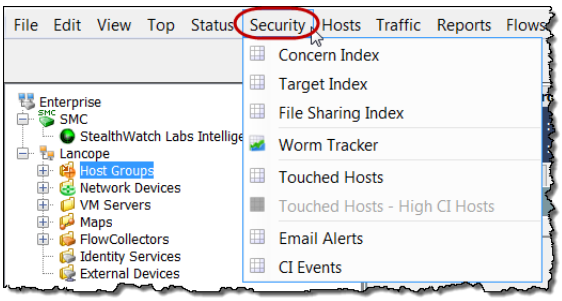
状态菜单

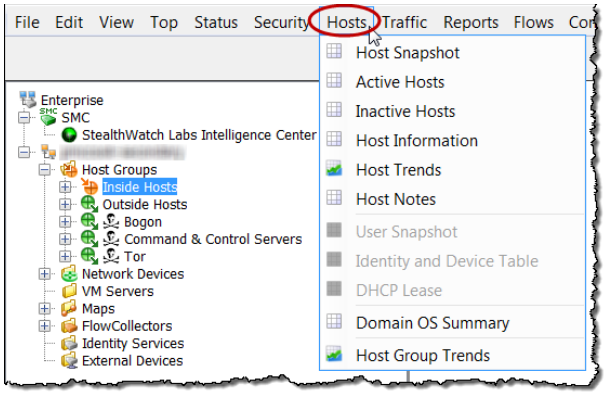
“状态”菜单提供根据特定标准（例如警报、流量、可能的数据丢失、接口、VM、外部事件等）显示网络各个部分的状态的选项。



安全菜单

使用“安全”菜单可以查看与安全问题相关的数据，如高度关注的主机、目标主机、文件共享活动、蠕虫活动和异常的邮件通信。



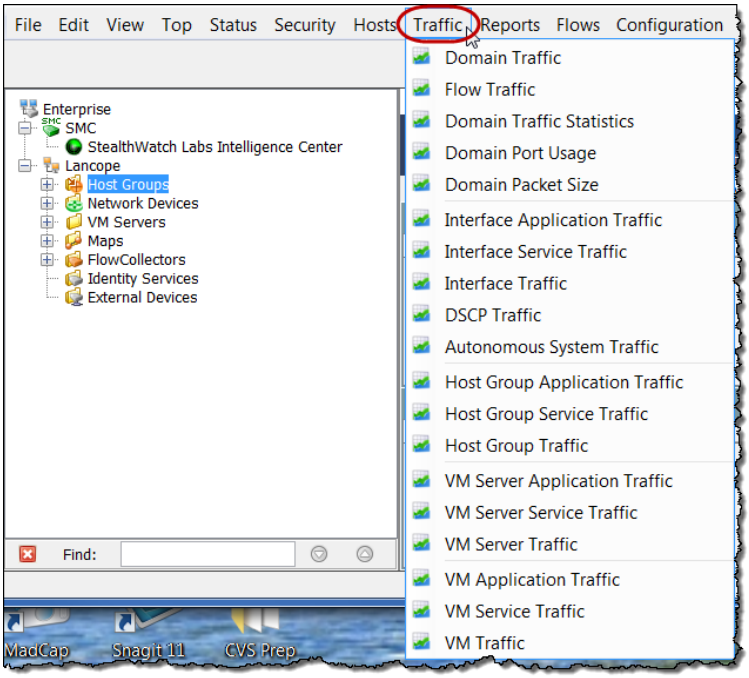


主机菜单

“主机”菜单提供显示与主机相关的数据（例如单个主机活动、主机行为趋势、活动或非活动主机、主机用户标识等）的选项。

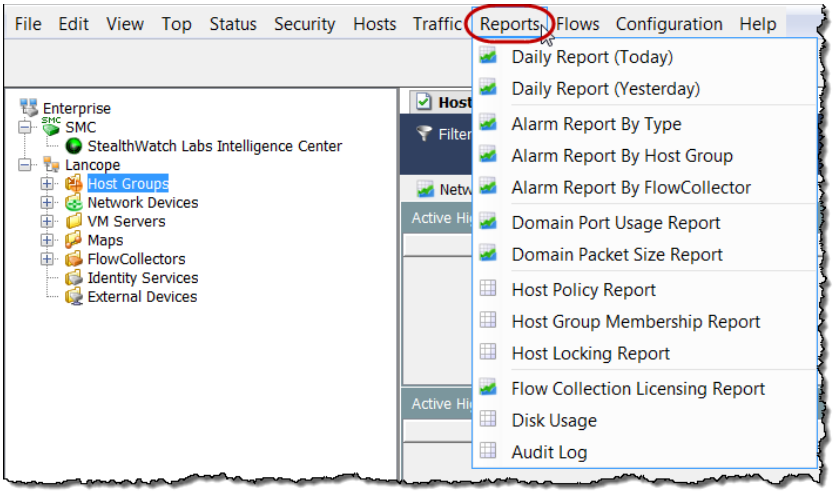
流量菜单

“流量”菜单允许您以多种方式（如按域、接口、主机组、应用、服务、端口、VM 等）细分的流量信息。



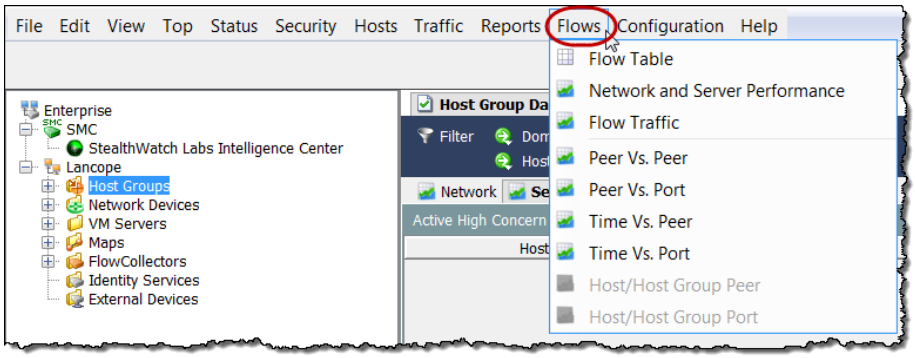
报告菜单

“报告”菜单允许您对 Stealthwatch 数据库运行查询，例如，对域活动的每日摘要或根据类型、主机组或流量收集器发生的警报报告。



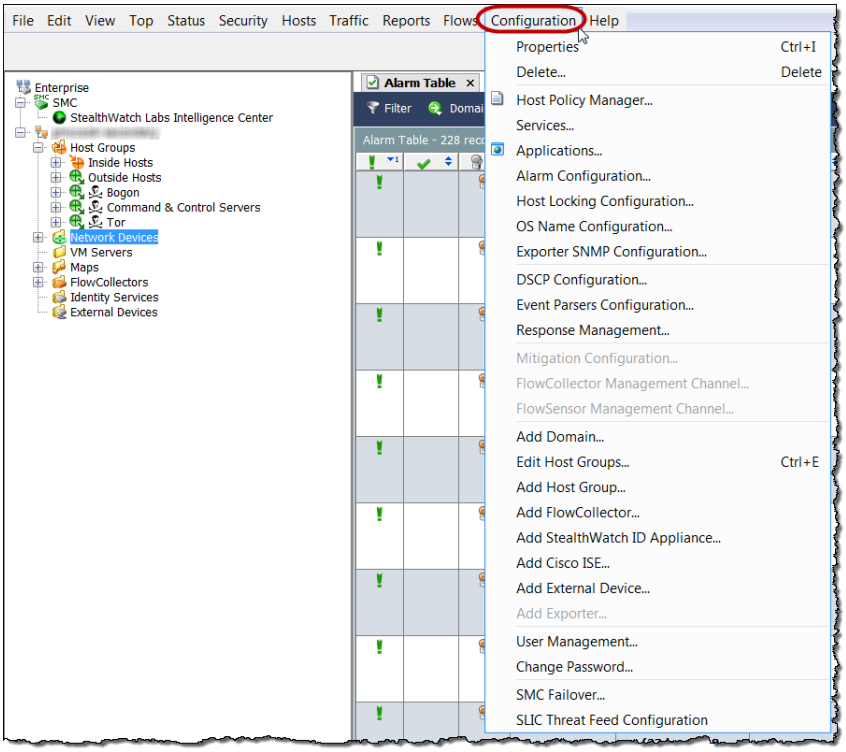
流菜单

顾名思义，“流量”菜单提供分析流量的各种方法，包括网络流量数据和服务器性能流量数据。



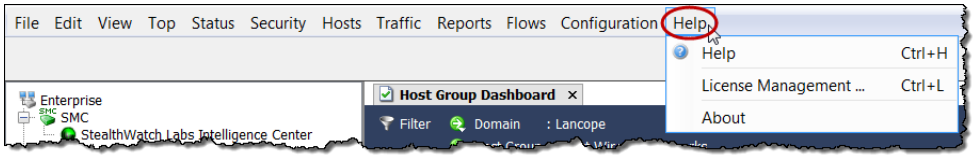
配置菜单

“配置”菜单包含 Stealthwatch 中可用的大多数配置选项。您可以通过添加、编辑或删除域、设备、主机组、策略、应用或服务定义，根据需要构造或细化所监控的网络。您也可以通过添加、编辑或删除用户及其登录权限来限制访问。Stealthwatch 系统使用一组默认的警报严重性级别。如果需要，您可以根据组织需要更改这些默认值。



帮助菜单

“帮助”菜单包含 *SMC 客户端联机帮助*以及与 SMC 客户端软件的版本、许可证和说明相关的信息。我们很快会更详细地讨论使用联机帮助的优点。

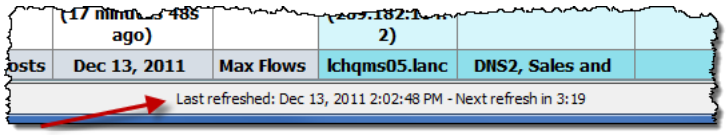


处理文档

我们来了解一下 SMC 文档中出现的一些常用导航元素。

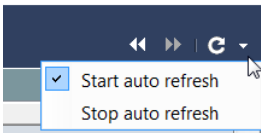
显示实时数据与静态数据

SMC 设备从 Stealthwatch 流量收集器收集数据，并自动刷新大多数 SMC 文档上的数据，因此您看到的信息始终是相对较新的信息。通过查看窗口底部的计数器，您可以看到将进行下一次自动刷新的时间。



“刷新”按钮 位于文档标题的最右侧。当您点击此按钮时，活动文档将使用最新的数据进行刷新（并变为实时文档），并重置自动刷新功能。

如果您需要在较长的时间内研究信息，则需要使文档成为静态文档。

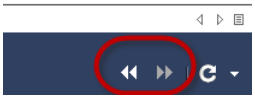


通过点击下拉菜单中的下列选项之一，可以使文档成为静态或实时文档：

- 开始自动刷新 - 文档现在是实时文档（活动状态）。当自动刷新间隔到期时，SMC 软件将使用新数据更新文档。
- 停止自动刷新 - 文档现在是静态文档（非活动状态）。

提示：

随时点击**刷新**按钮都可以触发数据更新。



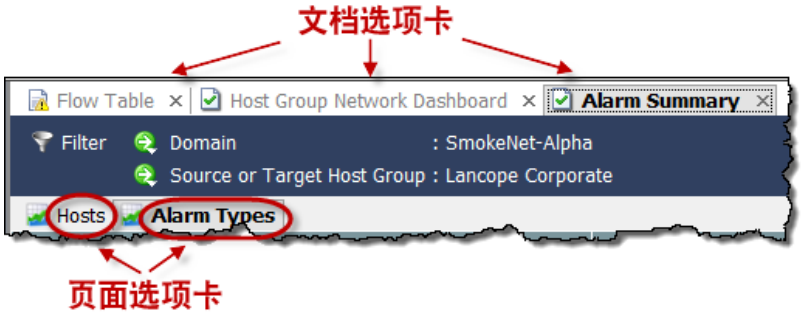
“查看较早数据”按钮 和“查看较晚数据”按钮 也位于文档标题的最右侧。点击这些按钮时，可以根据“过滤器”对话框中设置的时间增量分别向前和向后移动数据。

提示：

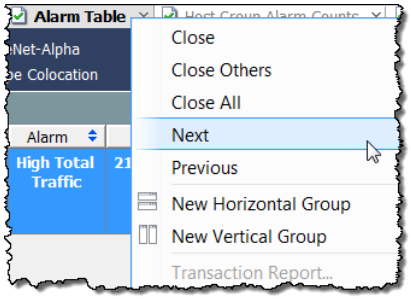
- 按 **Ctrl+左箭头键**可快速向后移动数据一段时间。
- 按 **Ctrl+右箭头键**可快速向前移动数据一段时间。

选项卡以及在文档之间移动

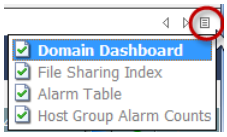
可以在 SMC 客户端界面中同时打开多个文档。每个文档都通过选项卡彼此相隔。某些文档（如下面的示例中所示的警报摘要）具有多个页面，这些页也由选项卡分隔。



您可以通过多种方式从一个文档移动到下一个文档。您可以点击所需的文档选项卡，右键点击文档选项卡并选择**下一步**或**上一页**，或者同时按下键盘上的 **Alt** 键和左 ← 或右 → 箭头键。

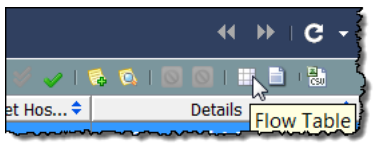


如果打开的文档太多，无法看到所有的选项卡，则可以通过点击选项卡右侧的右 ▶ 或左 ◀ 箭头从一个文档移至另一个文档。也可以点击“列表”按钮 ☰ 从下拉列表中点击打开的文档。



活动文档是您当前正在查看的文档。活动文档的标题始终为黑色、粗体。活动文档根据相应的刷新间隔自动进行刷新。非活动文档不会自动刷新。必须使非活动文档处于活动状态，然后手动刷新它。刷新开始后，您可以导航到其他文档，而无需等待刷新完成。

许多文档都包含自己的工具栏，其中带有具有该文档特定功能的按钮。您可以将光标悬停在任意按钮上以查看对该按钮做出说明的工具提示。

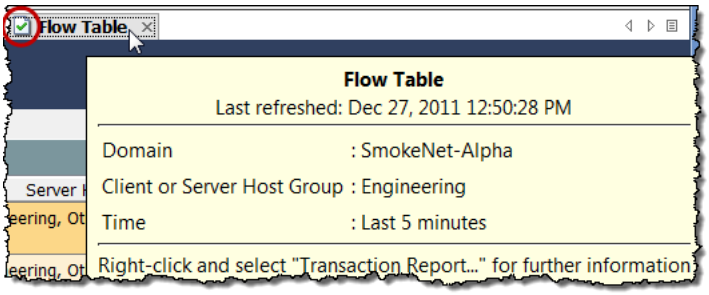


每个文档选项卡都包含一个图标，指示文档的刷新状态（请参阅下例中画圈的区域）。当非活动文档完成刷新时，选项卡文本将更改颜色以指示刷新状态。以下图标表示可用的不同刷新状态：

- 繁忙 - 文档正在刷新或执行某项操作。
- 刷新完成 - 最后一次刷新成功完成；非活动选项卡文本为绿色。

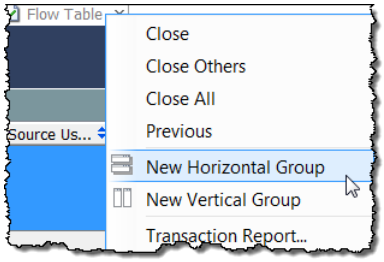
- 刷新完成(有错误) -最后一次刷新成功完成，但出现错误或有更多信息可用；非活动选项卡文本为黄色。
- 错误 - 最后一次刷新未成功完成；非活动选项卡文本为红色。

如果将光标悬停在文档选项卡上，您将看到一个工具提示，提供有关该文档的摘要信息。



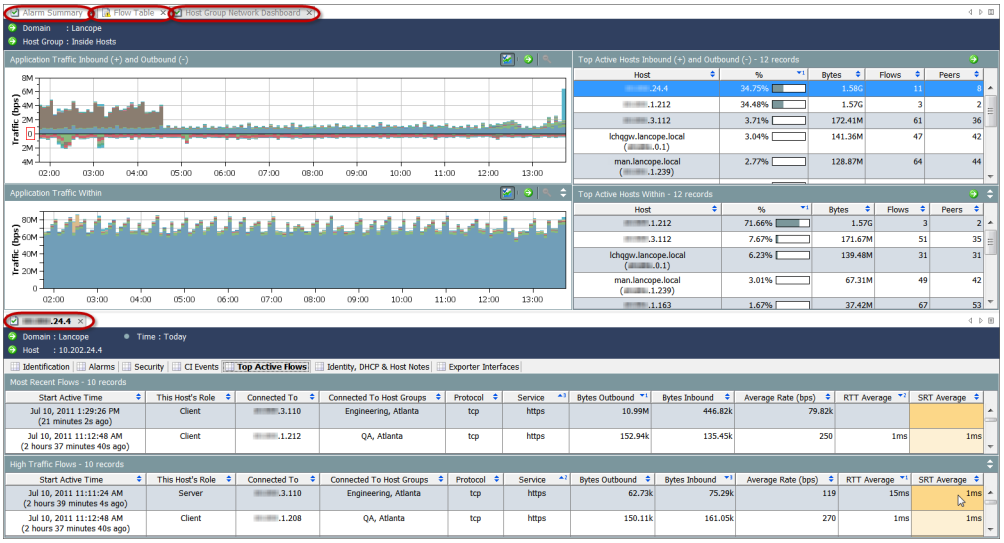
更改文档方向

默认情况下，当您打开多个文档时，这些文档会前后逐个显示，按选项卡错开。如果需要，您可以更改此方向，使其按照水平方向前后显示，或按照垂直竖直方向相邻显示。右键点击“文档”选项卡，然后点击**新建水平组**或**新建垂直组**，选择所需的方向。

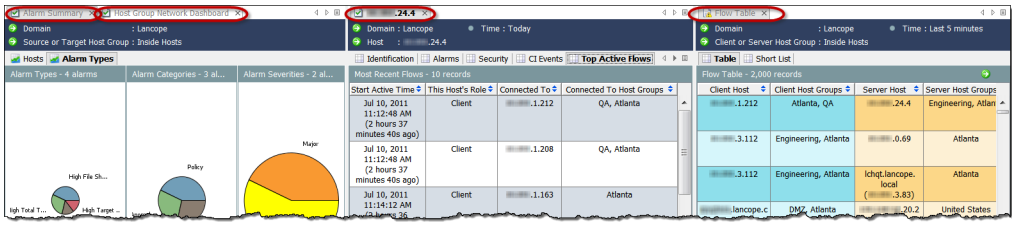


结果将类似于如下示例之一。

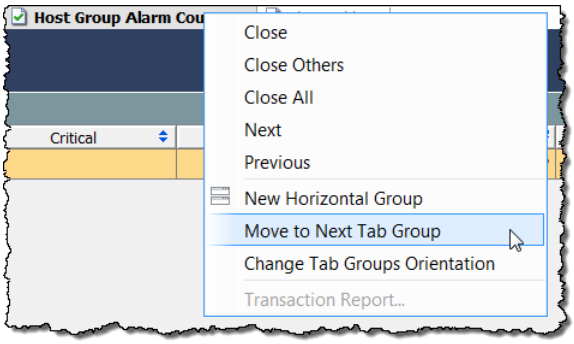
水平组



垂直组



根据当前方向，您可以通过右键点击“文档”选项卡并选择**移动到下一个选项卡组**、**移动到上一个选项卡组**或**更改选项卡组方向**将文档从一个选项卡组移动到另一个选项卡组，直到达到您预期的排列为止。您也可以点击某个文档选项卡并在打开的文档中将其从一个位置拖至另一个位置。



文档标题

文档标题包含有关文档所呈现的数据的信息。

前面的示例中显示了“流量表”标题。该标题列出涉及的主机所在的域以及主机组名称。此外，我们还会看到正在呈现的数据被捕获的时间。

因此，我们在本例中查看的数据是在 SmokeNet-Alpha 域的“内部主机”主机组中发生的流量。我们在文档中看到的数据是在过去的 12 小时内捕获的。您可以使用过滤器更改其中任一参数，这一点我们将在稍后讨论。

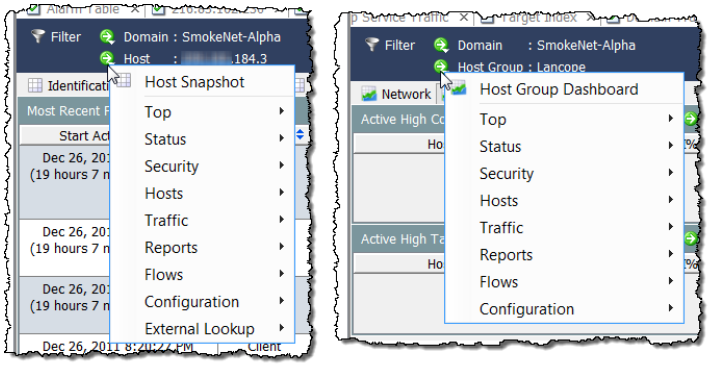
转至文档按钮

在整个 SMC 客户端界面中，“转到文档”按钮 显示在文档标题和工具栏中。点击此按钮时所看到的内容取决于与该按钮关联的对象。

在文档标题中

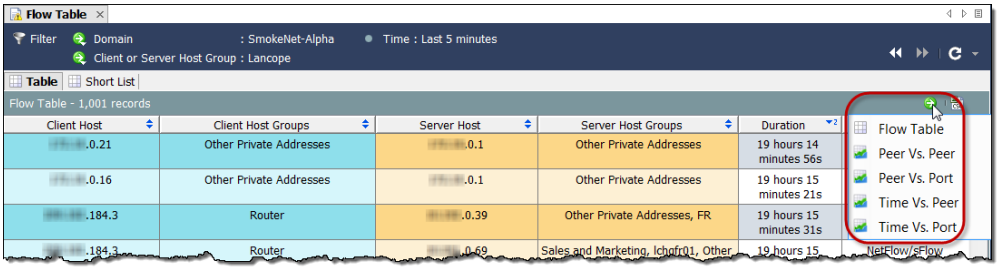
例如，如果点击文档标题中主机 IP 地址旁边的**转到文档**按钮，您将看到与主机相关的文档选项列表。如果点击其中一个选项，显示的数据将仅与该特定主机相关。

同样，如果点击标题中主机组名称旁边的**转到文档**按钮，您将看到与主机组相关的文档选项列表。如果点击其中一个选项，显示的数据将只与该特定的主机组有关。

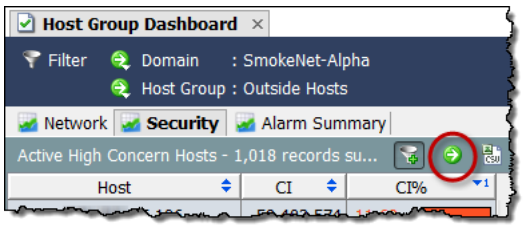


在文档工具栏中

文档工具栏中显示的“转到文档”按钮允许您以不同的方式查看正在查看的数据。例如，假设您正在查看特定主机组的流量表。如果点击“流量表”工具栏中显示的**转到文档**按钮，您会看到与流量相关的文档选项列表。如果点击其中一个选项，您会看到以其他格式显示的此流量的信息。

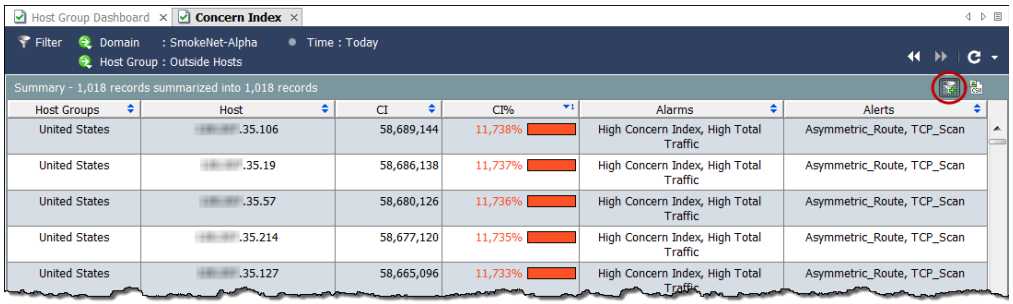


在某些情况下，只有一个文档与您正在查看的数据有关。在这种情况下，当您点击**转到文档**按钮时，该文档随即会打开。



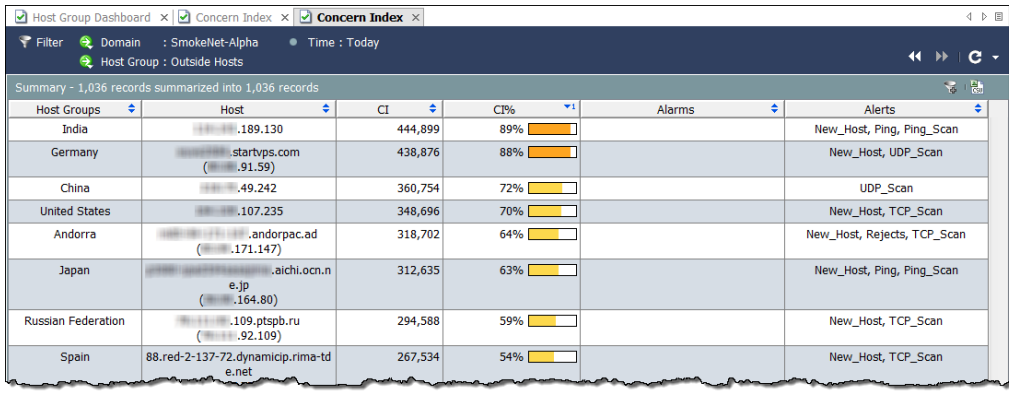
例如，主机组控制面板上的每个组件都包含自己的工具栏，工具栏上有一个“转到文档”按钮。如果您点击“活动高关注主机”组件的按钮，则 SMC 将立即打开预过滤的“关注指数”文档，以显示仅与主机组控制面板上该组件中显示的信息相关的数据。

“关注指数”文档显示自上次存档时间以来 CI 点数最高的主机的信息。



当您打开“关注指数”文档时，默认情况下，“关注指数过滤器”按钮（位于文档的右上角）处于激活状态，并且关注指数仅显示包含活动高关注指数警报的主机（即 CI 百分比高于 100% 的主机）。要查看 CI 百分比高于 50% 的主机，请点击**关注指数过滤器**按钮。

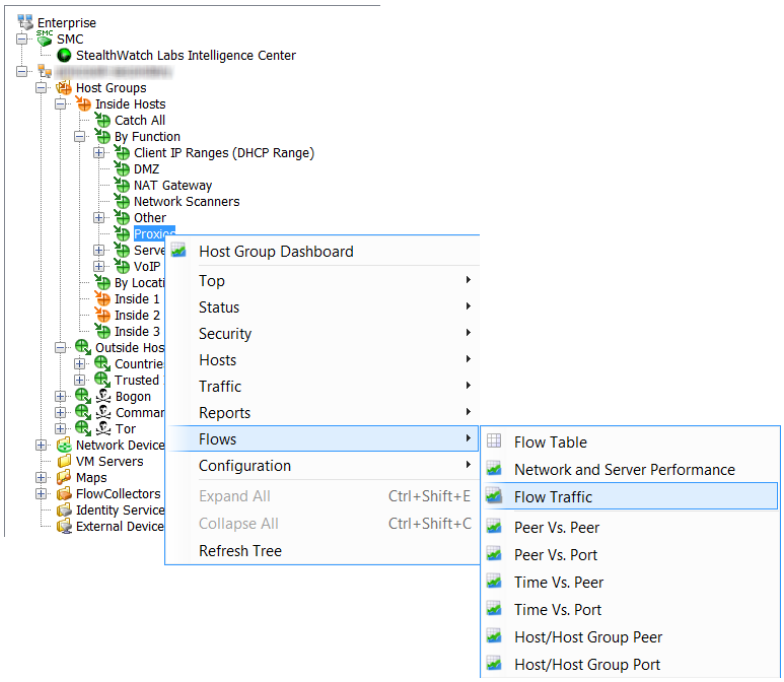
“关注指数过滤器”按钮上的加号会变为灰色，并仅显示 CI 百分比高于 50% 的主机。



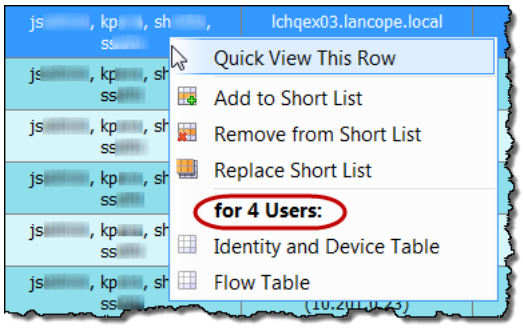
右键点击可快速聚焦

整个 SMC 客户端界面提供的右击功能可以提供打开文档的其他可选方式。通常，右键菜单可以帮助您快速查找最具体的数据，比使用主菜单快得多。

右击企业树中的某个元素，然后从弹出菜单中选择所需的文档。此时显示的数据与您点击的元素明确相关。例如，如果您右键点击企业树中的某个主机组名称，并选择**流 > 流流量**，则显示的流流量数据将与该主机组特别相关。



另一种打开文档的方式是右击文档内部，按需从显示的弹出菜单中进行选择。例如，当您右击文档中某一列里的一个用户名（或多个用户名）时，系统将显示下面的弹出菜单：



弹出菜单上的标签（上图中圈出）指示可基于其对标签下列出的文档进行过滤的用户数。如果仅点击一个名称，则该标签指示该用户的名称。

注意：

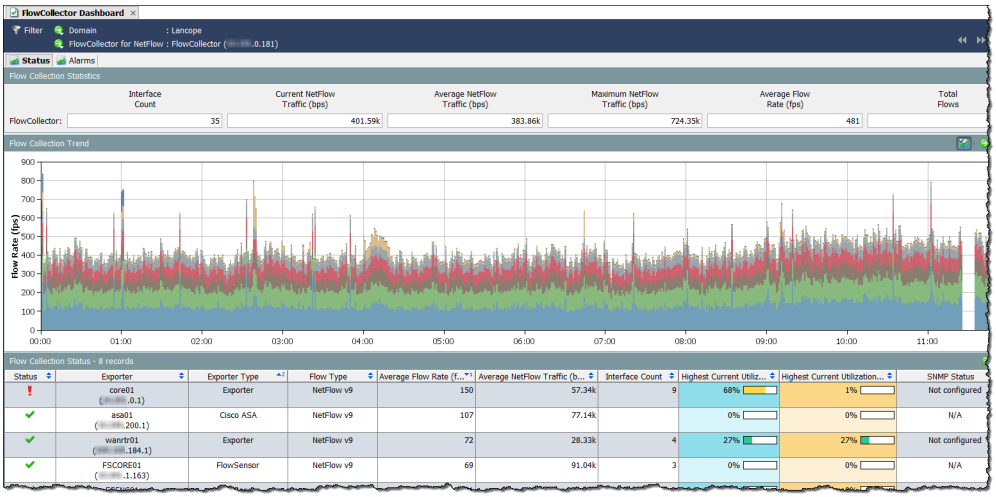
- 您也可以通过双击表单元格中的项目并使用**转到文档**按钮打开文档。

双击所选文档

双击功能提供另一种打开选定数量的文档的方法。有关可通过双击企业树中的分支打开的文档，请参阅下表：

如果在企业树中双击如下分支...	则如下文档将会打开。
“SMC”文件夹	SMC 控制面板
特定主机组	主机组控制面板
“内部/外部主机”文件夹	主机组控制面板
“网络设备”文件夹或特定网络设备	接口状态
“导出器”文件夹或特定导出器	接口状态
特定接口	接口摘要控制面板
“流量传感器”文件夹	接口状态
“VM 服务器”文件夹	VM 服务器状态
特定 VM	VM 流量
特定地图	该特定地图
特定的思科 ASA 导出器	最后五分钟的流量表，由该 ASA 进行过滤
任何不是思科 ASA 防火墙的防火墙（例如，Palo Alto 防火墙）	接口状态
防火墙接口	接口摘要控制面板
特定流量收集器	流量收集器控制面板
特定的思科 ISE	身份和设备表
特定的标识	“用户标识过滤器”对话框
特定外部设备	外部事件

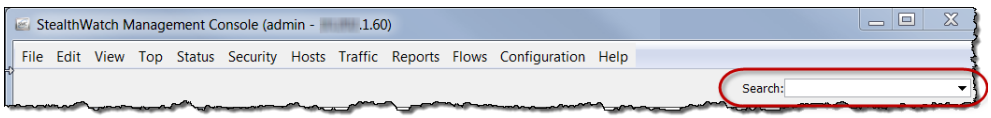
例如，如果双击流量收集器，则将打开该流量收集器的流量收集器控制面板。



搜索文档

除搜索企业树中的项目以外，SMC 还允许您在其所有文档中（跨所有域）搜索特定项目。在主工具栏上的“搜索”字段中，可以使用完整字符串、部分字符串或带有通配符 (*) 的部分字符串搜索以下项目：

- 警报 ID
- 主机或导出器 IP 地址
- 以下名称：
  - 导出器
  - 主机组
  - 服务器
  - 用户
  - VM
  - VM 服务器



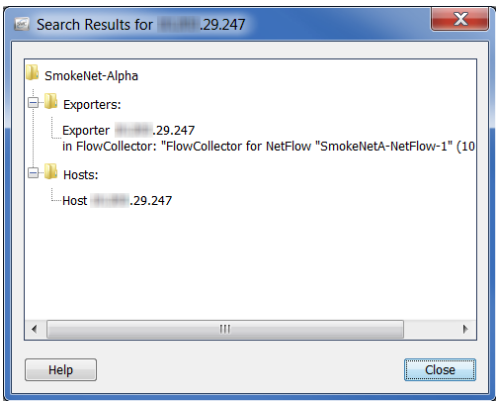
注意：

- 系统会根据与您的用户名关联的数据角色和功能角色而限制搜索结果。

提示：

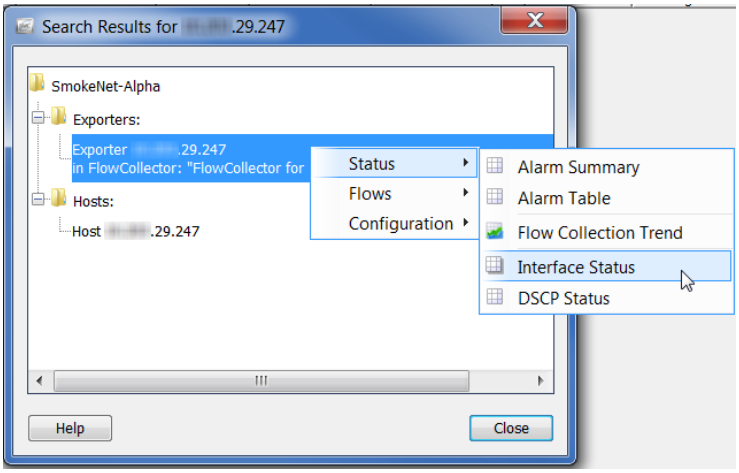
您可以使用“搜索”下拉列表框来选择先前已搜索的项目，然后按 **Enter** 键来执行搜索。

例如，如果您在“搜索”字段中键入导出器的 IP 地址，然后按键盘上的 **Enter**，则“搜索结果”对话框将显示 SMC 中出现该 IP 地址的位置的列表。

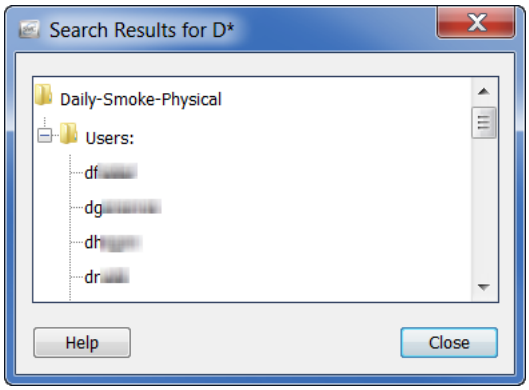


在许多情况下，可以双击列表中的 IP 地址以显示有关该项目的特定文档。例如，如果双击“主机”条目下的 IP 地址，则将显示该 IP 地址的主机快照。

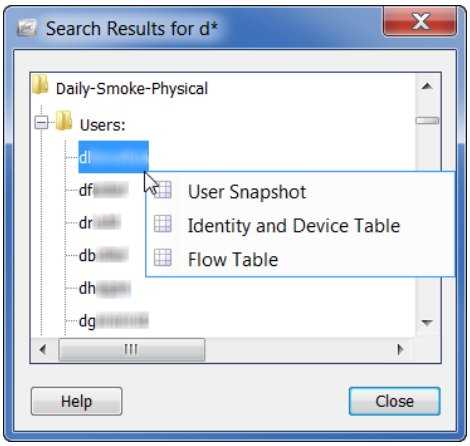
您也可以右键点击 IP 地址获取您可以访问的与该 IP 地址相关的其他参考信息列表。



执行用户名搜索时，每个用户名都会作为一个单独的项目显示在“搜索结果”对话框中一个名为“用户名”的文件夹中



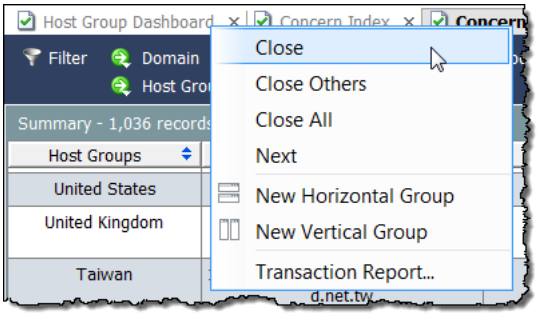
如果双击用户名，则系统将打开已按该用户进行预过滤“身份和设备表”。如果右击用户名，则会显示以下弹出菜单，您可以从中选择将为对应用户预过滤的文档。



关闭文档

正如有多种方法可以打开 SMC 文档一样，也有多种方法可以将其关闭。要关闭一个文档，只需点击“文档”选项卡右上角的 **X**。或者，在主菜单中点击**文件 > 关闭**，或在键盘上按 **Ctrl+W**。

要关闭所有文档，请从主菜单中点击**文件 > 全部关闭**。您也可以右键点击“文档”选项卡，然后从弹出菜单中选择相应的选项。

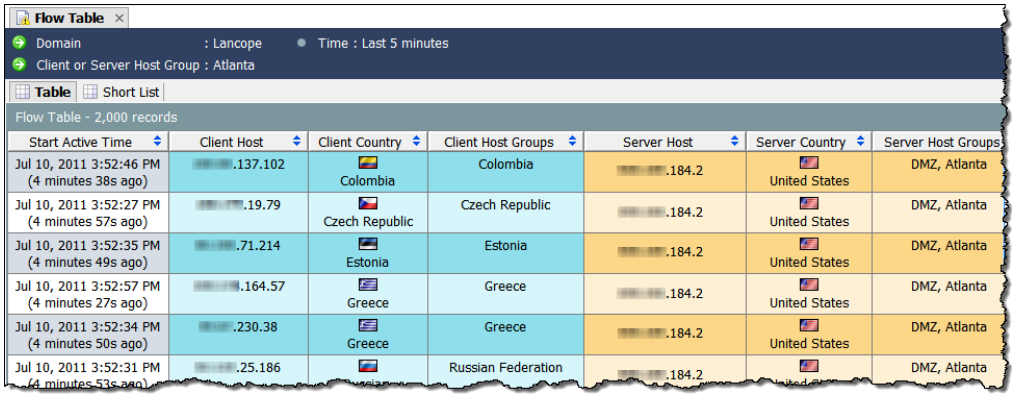


注意：

有关可与 SMC 一起使用的键盘快捷键的完整列表，请参阅“键盘快捷键”（第 85 页）。

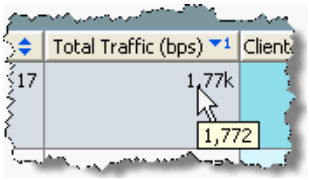
使用表

包含表的文档提供其他导航元素。一个关键的图形提示是在表行中使用颜色，如下面的流量表中所示。



- 蓝色表示客户端数据。
- 橙黄色表示服务器端数据。

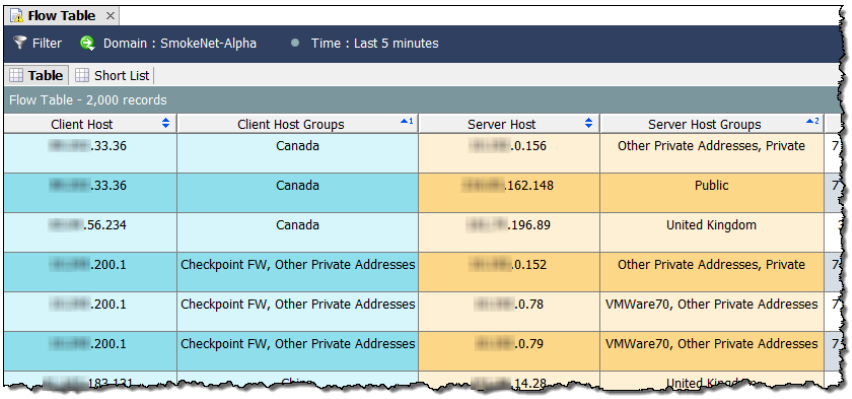
度量单位在列标题中指示，如使用 *bps* 表示位数/秒。相应单元格中的数值将进行四舍五入。但是，您可以将光标悬停在四舍五入后的值上，以在工具提示中显示确切值。



对列进行排序

要按升序或降序对列进行排序，请点击列标题中的**上/下**按钮。（此按钮可以切换以指示升序或降序。）可以按多达三个特定列对表进行排序。对单个列进行排序时，整个表将根据该列进行排序。如果对第二列进行排序，则整个表将首先根据该列进行排序，然后根据您排序所基于的第一列进行排序，以此类推。

在下面的示例中，按字母数字升序排列的第一列是“服务器主机组”列。在接下来对“客户机主机组”列按字母数字升序排列时，此列成为排序的第一列，“服务器主机组”列成为排序的第二列。

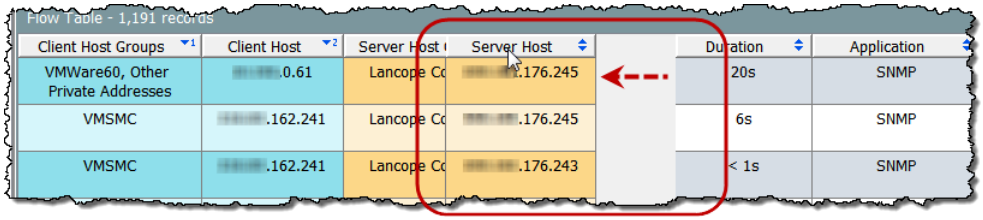


注意：

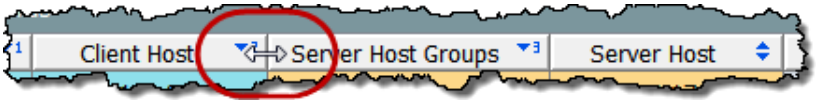
若要从列中删除排序行为，请在点击列标题时按键盘上的 **Ctrl** 键。

移动列和调整列大小

若要向左或向右移动列，只需点击列标题，并将该列拖动到所需位置。

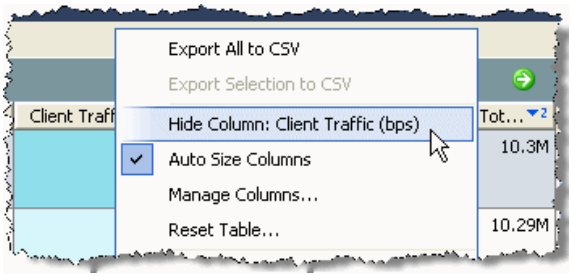


默认情况下，列宽会自动调整，以便在屏幕上尽可能显示所有列。若要手动增加或缩小列宽，请点击并将列标题的边框向左或向右拖动到所需的宽度。

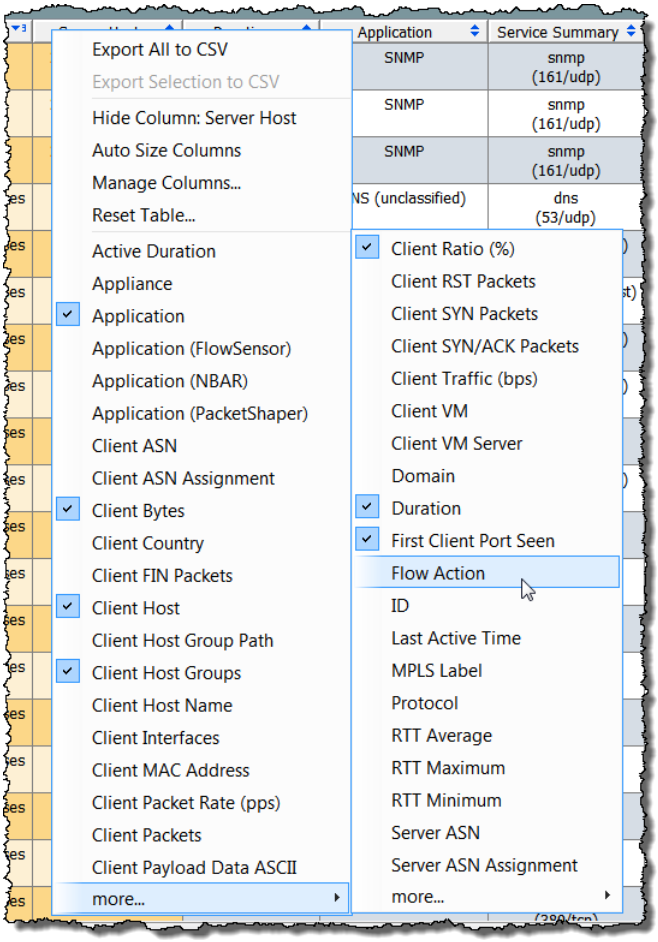


隐藏和显示列

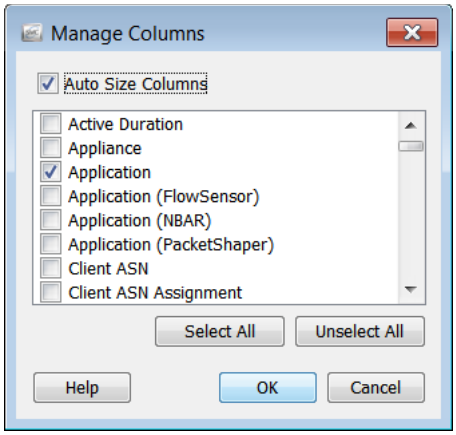
若要隐藏列，请右键点击列标题并选择**隐藏列: <名称>**。



若要显示更多列，请右键点击列标题，然后从弹出菜单中选择要查看的列。



或者，您可以转到“管理列”对话框以隐藏或显示特定的列。右键点击列标题并选择**管理列**。如果要在相应的文档上显示列，请选中其复选框以添加复选标记（如果它尚未包含复选标记）。如果不希望在相应的文档上显示列，请选中其复选框以删除复选标记（如果仍显示复选标记）。



若要使 SMC 自动调整列的大小，请确保对话框顶部的**自动调整列大小**复选框包含复选标记。SMC 将自动调整列的大小，使它们在没有水平滚动条的情况下尽可能都在屏幕上显示。若要手动调整所有列的大小，请确保**自动调整列大小**复选框不包含复选标记。

完成更改后，点击**确定**以应用更改并关闭“管理列”对话框。

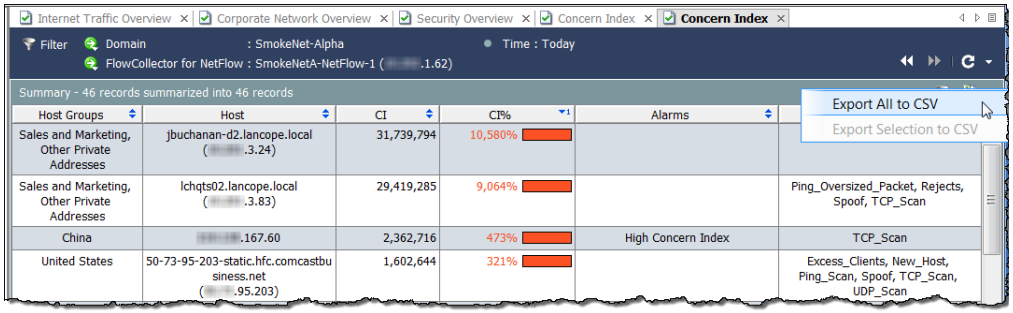
提示：

若要将表恢复默认设置，请右键点击列标题并选择**重置表**。

导出数据

可以将任何 SMC 表中显示的数据保存到逗号分隔值 (CSV) 文件。然后，您可以将 CSV 文件导入到大多数电子表格程序（如 Microsoft Excel）中，以便以后查看。您可以导出表中的所有信息，也可以只导出选定的特定信息。

若要导出表中的所有信息，请点击文档右上角的**导出到 CSV** 按钮，然后点击**全部导出为 CSV**。



注意：

如果要仅导出表中的一行数据，请点击要导出的数据行。如果要选择多行，请在进行选择时按 **Shift** 或 **Ctrl** 键，或者只需拖动光标以突出显示所需的选项。点击文档右上角的**导出为 CSV** 按钮，然后点击**将选择导出为 CSV**。

打开“保存”对话框时，导航到要保存信息的目录，然后输入文件名。（必须在文件名末尾键入 **.csv**，以便以此格式保存文件。）点击**保存**。现在，您可以在您选择的电子表格程序中打开和查看该信息。

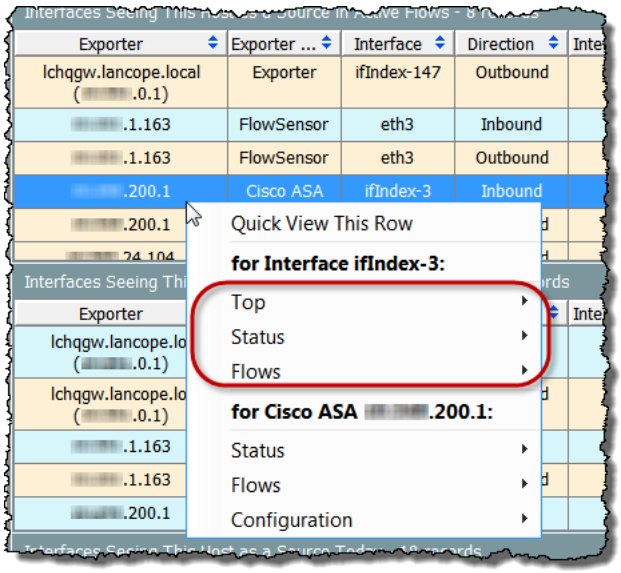
提示：

也可以右键点击表中的任何标题以访问“导出为 CSV”选项。（这些选项将显示在弹出菜单中。）

多部分弹出菜单

到目前为止，我们讨论过的表的弹出菜单是相当直观的，只有一个选项部分。但是，某些弹出菜单根据所选行的处理方式会有多个部分。

例如，要查看下面示例中显示的弹出菜单，您需要在主机快照的“导出器界面”选项卡上点击一个导出器，然后右键点击它。

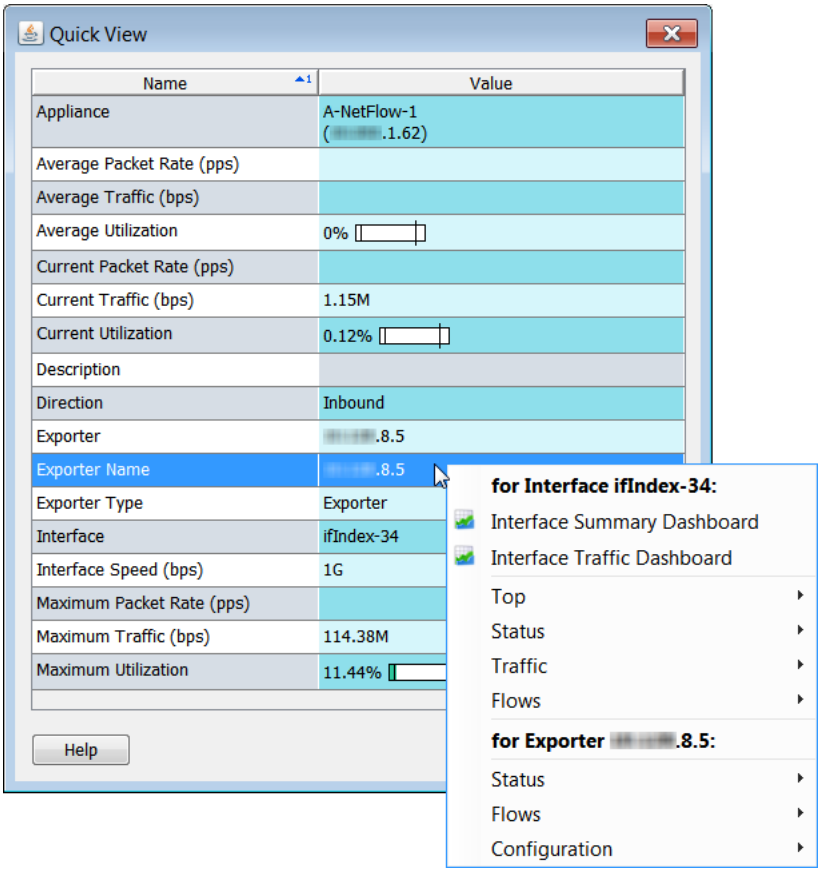


显示在弹出菜单顶部的选项将应用于整个行。弹出菜单中接下来显示的部分将应用于该行中的特定单元格。在上一个示例中，您可以查看以下类型的文档：

- 特定于 ifIndex-3 界面的文档（通过点击上一示例中的任何选项）。
- 特定于思科 ASA xxx.xxx.200.1 导出器的文件（弹出菜单上的最后三个选项）。

快速查看

“快速查看”对话框提供了一种快速简便的方法来查看表的特定行中显示的数据。只需点击所需的行，然后按键盘上的空格键即可。也可以右键点击该行并选择**快速查看此行**。



在某些情况下，通过“快速查看”可以导航到其他文档的已过滤视图。在一行中点击鼠标右键可以查看任何带有相关文档的弹出菜单，以了解该行中数据的更多详细信息。

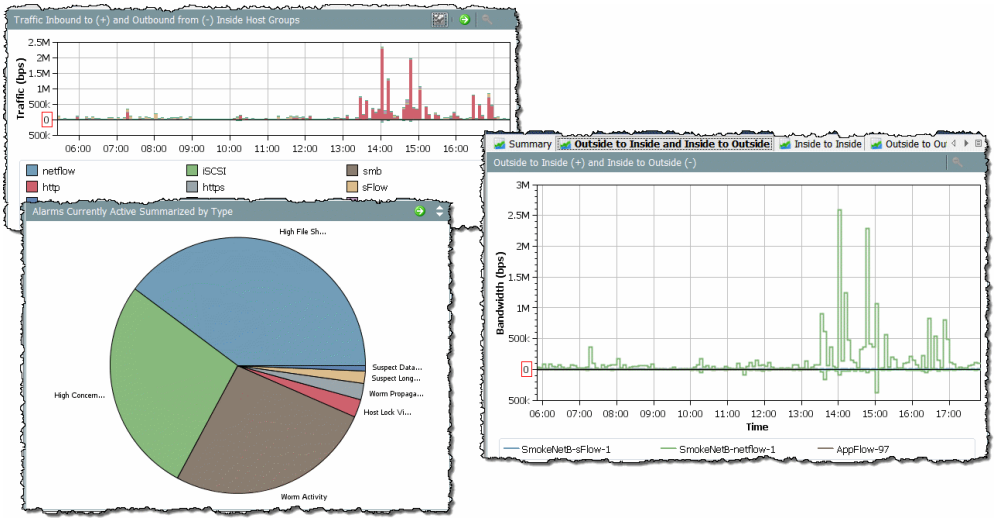
同步按键盘上的 **Alt** 键与上箭头键或下箭头键可以在关联文档中从一行导航到另一行，而不必关闭“快速查看”。

要关闭“快速视图”对话框，请执行以下其中一项操作：

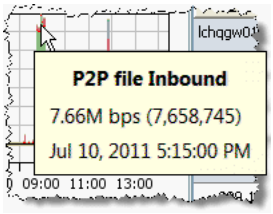
- 按键盘上的空格键。
- 按键盘上的 **Esc** 键。
- 点击右上角的 ❎ 按钮。

使用图表

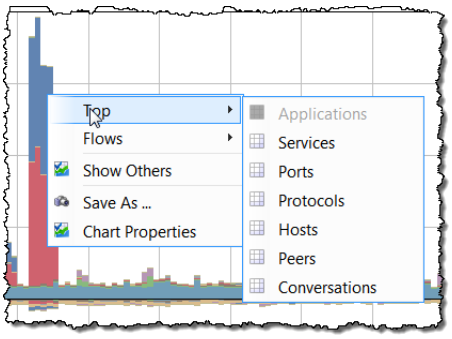
SMC 客户端界面中的某些文档包含条形图、线条形或饼状图表，如以下示例中所示。



通过右键点击图表上的任意位置并选择**另存为**，可以将任何图表保存为 JPG 或 PNG 文件。然后，您可以根据需要将图形导入另一个文档以进行分析、报告或存档。



图表中的每种颜色都表示特定的应用、服务、警报类型或设备，具体取决于您正在查看的图表。若要查看图表中特定项目的详细信息，请将光标悬停在有色区域上，以查看显示有更多信息的工具提示。



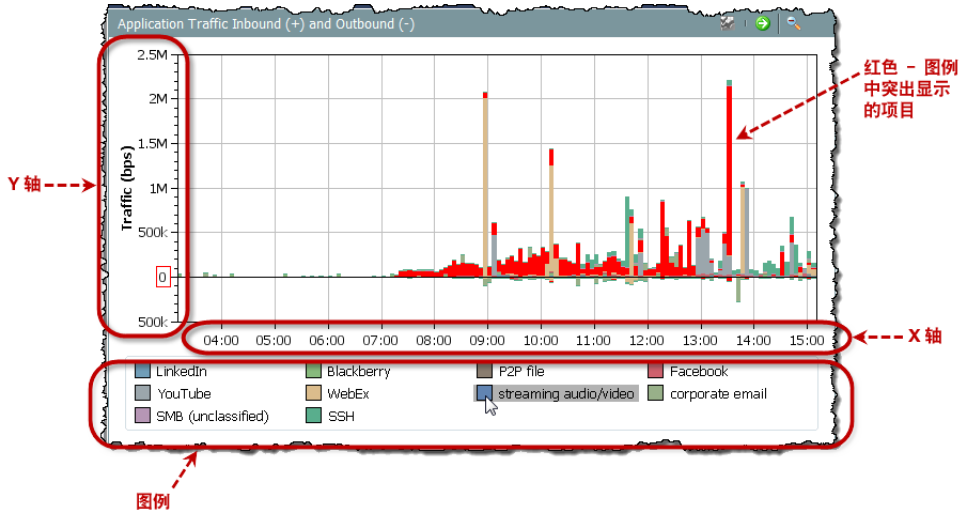
您也可以右键点击一个有色区域，然后点击出现的弹出菜单中的某个选项。打开的文档将包含特定于您在图表中点击的项目的数据。

您可以通过在感兴趣的区域按住并拖动光标来放大条形图或线条图表的区域。放大后，可以使用键盘上的箭头键在图表中向上、向下或向侧面移动，以查看不同的区域。若要返回正常放大倍数，请按键盘上的 **F** 键，或点击图表右上角的**缩小**按钮 。

注意：

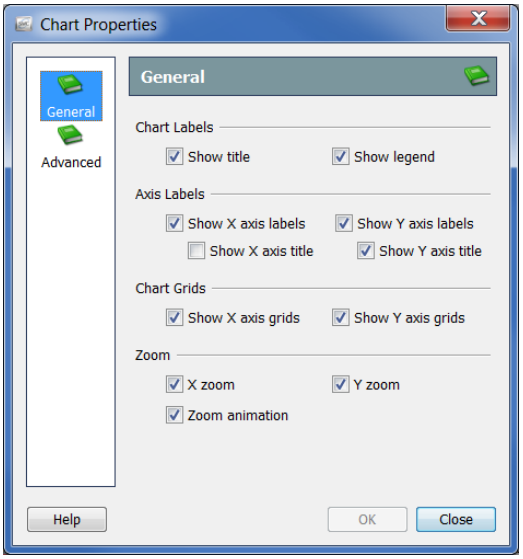
显示服务流量数据的图表在右上角包含一个“显示/隐藏”按钮 ，用于显示或隐藏通常标记为*其他*的服务流量。

条形图和折线图附带一个图例，其中列出了各种颜色及其表示的内容。将光标悬停在图例中的项目上会使图表中的关联数据点以红色突出显示。

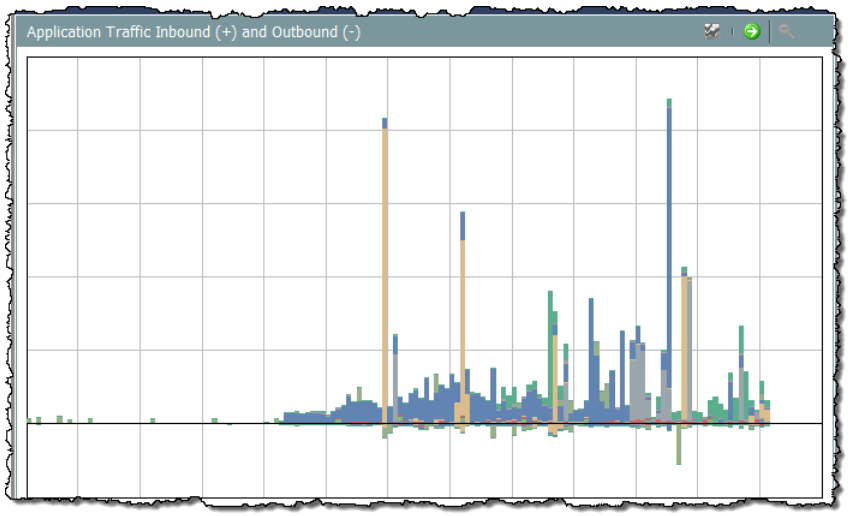


正如您所看到的，这些元素可以占用文档的大量空间。由于可以通过将光标悬停在数据点上并查看工具提示查看最适用的信息，因此您决定可能不需要查看图例和坐标轴。

若要隐藏图例或坐标轴，请右键点击图表上的任意位置，然后选择**图表属性**以打开“图表属性”对话框。对于您不希望在“图表属性”对话框中看到的任何元素，请点击相应的复选方以删除复选标记。

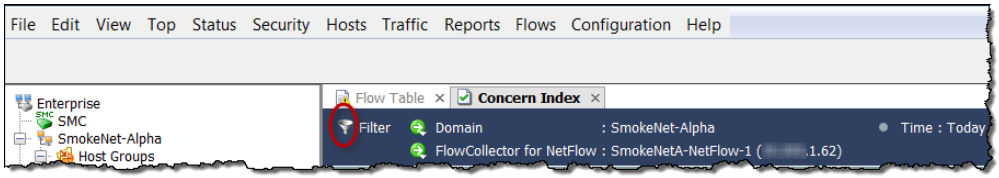


例如，如果在主机组网络控制面板上的“应用流量入站和出站”图表上隐藏图例和坐标轴标签，结果将类似于下面的示例。

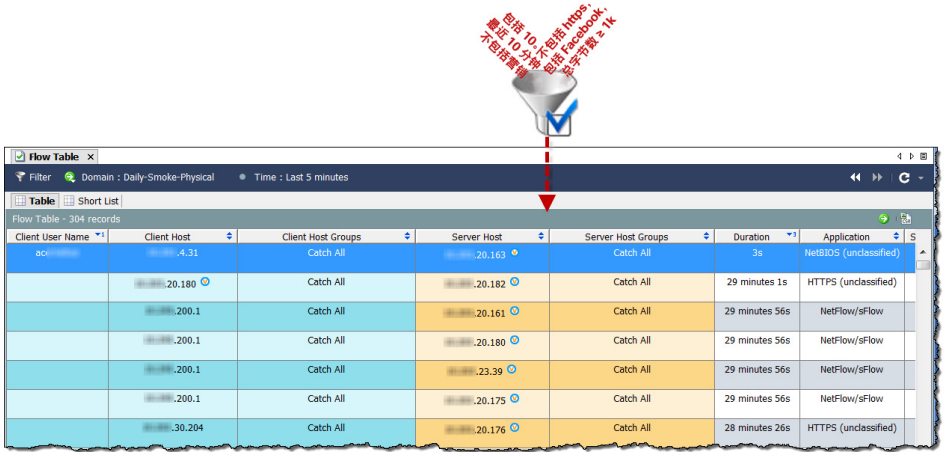


过滤文档数据

本指南中的其他信息都可以记不住，但要记住：*此过滤器可为您提供很重要的帮助！*要打开任何活动 SMC 文档的过滤器，只需点击文档标题上的**过滤器**按钮即可。



使用过滤器作为漏斗，从 Stealthwatch 系统提供的大量数据中只提取您想要的确切信息。



您可以过滤几乎任何 SMC 文档。过滤还允许您查看历史数据，从取证的角度看，这是非常有用的。

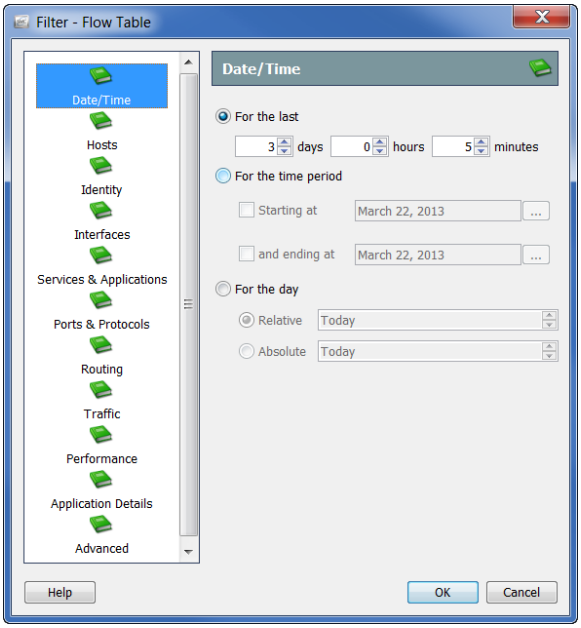
注意：

将文档另存为共享文档时，还将保存过滤器设置。有关保存文档的详细信息，请参阅“保存文档”（第 77 页）

所有 SMC 文档都有过滤器，这些过滤器的操作方式也差不多。我们来了解如何过滤在流表上看到的信息。

日期/时间

通过“日期/时间”页面，可以过滤流表，以显示在特定日期和时间（直到最后一分钟）期间发生的流的信息。



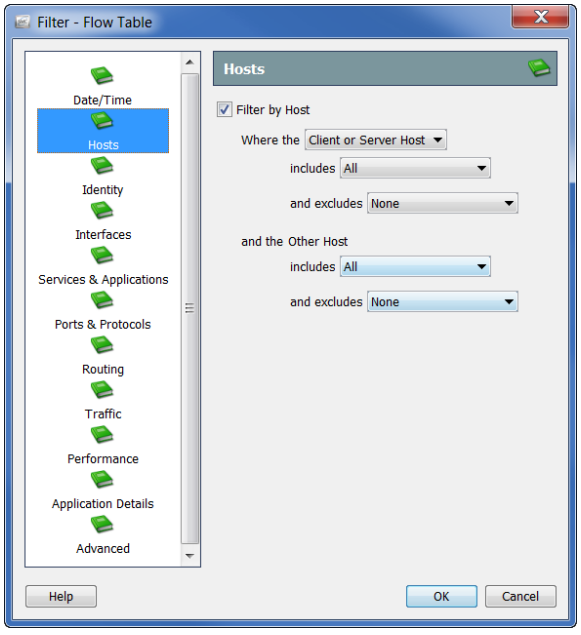
提示：

若要调查跨越多日的流，请使用“流流量”文档而不是“流表”来更快速地响应。

主机数

流表过滤器的“主机”页面允许您显示仅涉及特定主机的流的信息。

您可以对服务器主机和/或客户端主机进行过滤。您可以将焦点缩小到特定的主机组、IP 地址范围或特定的 IP 地址。您甚至可以包括 VM 和/或排除任何这些元素。



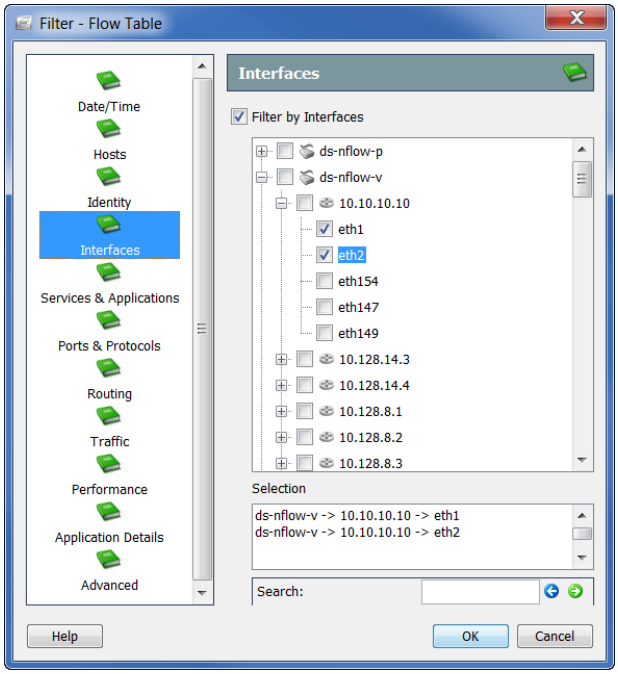
提示：

要查找涉及任何内部主机而不显示 NATed 流的流，请转到“流表过滤器: 主机”页面，并指定您的网络使用的广泛内部 IP 地址范围（例如，10.0.0.0/8）将包括在过滤过程中。

接口

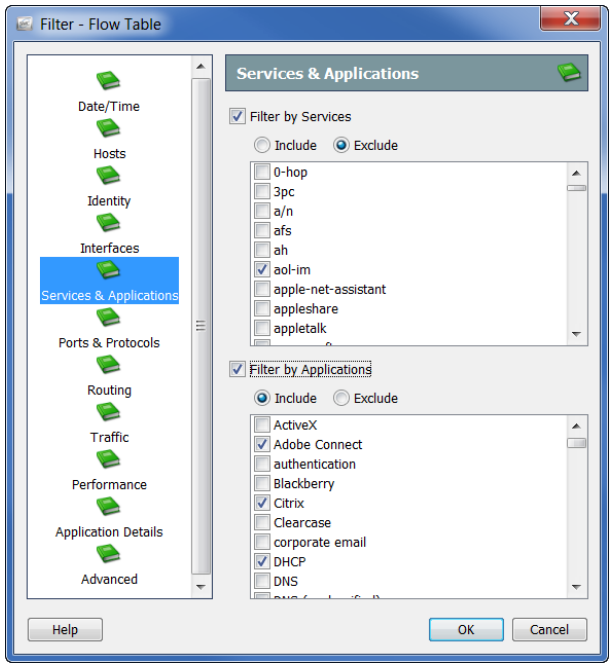
流表过滤器的“接口”页面允许您显示涉及特定流收集器、导出器和/或接口的流的信息。要选择流收集器的所有导出器，请点击该流收集器的相应复选框以添加复选标记。此操作也将为这些导出器选择所有接口。

您选择的项目将显示在过滤器的“选择”字段中。此外，如果您知道项目名称的一部分，则可以在底部的“搜索”字段中键入它，以便在接口列表中找到它。



服务和应用

流表过滤器的“服务和应用”页面允许您显示使用特定服务和/或应用的流的信息。您还可以排除使用特定服务和/或应用的流。



其他过滤器选项

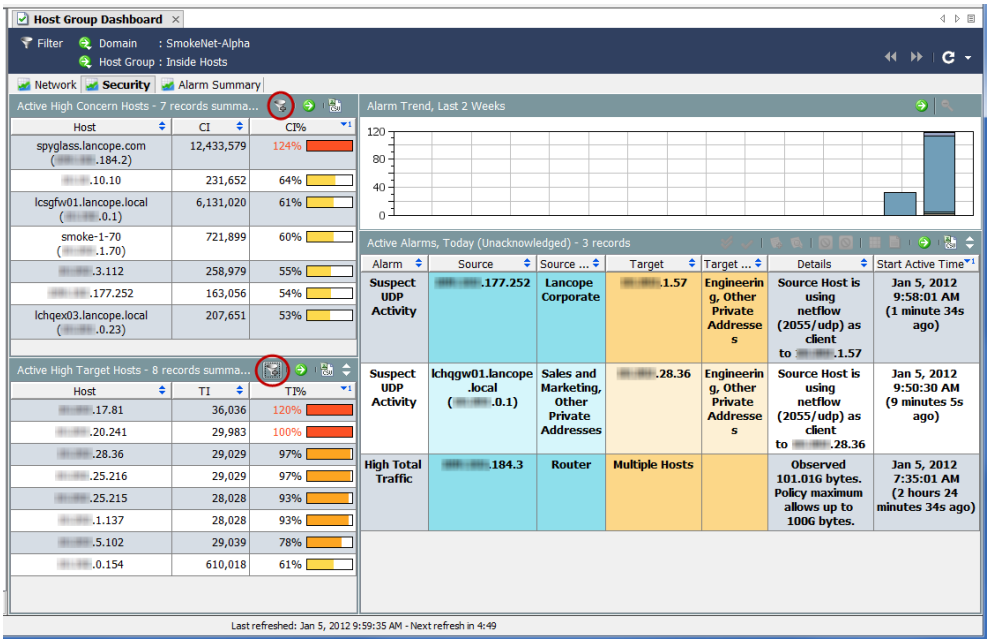
流表过滤器中的其他页面与我们刚刚介绍的过滤器页面的操作方式类似。下表提供了其余所有“流表过滤器”页面的简要说明：

此页面...	允许您根据以下条件过滤流...
身份	用户名。
端口和协议	IANA 定义的特定协议、TCP/UDP 端口和/或仅由客户端使用的端口。
路由	DSCP 点、自治系统编号、VLAN ID 和/或 MPLS 标签。
流量	如果需要，字节总数、数据包总数、客户端字节数、客户端数据包数、服务器字节数和/或服务器数据包数（包括特定值范围）。 注意：流表显示原始流量数据。
性能	TCP 总数、TCP 总重传数、最小/最大/平均 RTT和/或最小/最大/平均 SRT，包括特定值范围（如果需要）。
应用详细信息	特定应用详细信息字符串（包括或排除）。
高级	最大记录数、特定流记录字段的最高或最低值（例如，字节总数、客户端字节数等）、防火墙允许/拒绝的流操作、包括或排除的重复流和/或包括或排除的接口数据，以及更快速的查询（不进行排序或分组）。

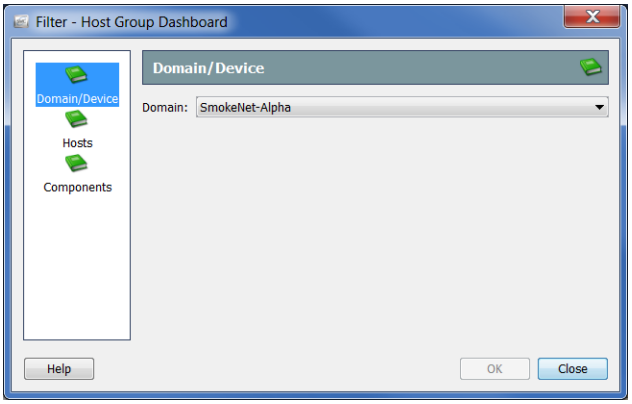
请记住，如果您对任何文档、对话框或过滤器有疑问，可以随时参考 *SMC 客户端联机帮助*。

控制面板过滤器

多数 SMC 文档的过滤器的操作都与流表过滤器非常相似。但是，控制面板的过滤器有点不同。控制面板过滤器允许您过滤关联控制面板上的每个组件。举个例子，让我们来看看如何过滤有关主机组控制面板的信息。



在主机组控制面板的文档标题中，点击**控制面板过滤器** 按钮以打开过滤器。通常，控制面板过滤器包含三个页面，如以下三个屏幕所示。

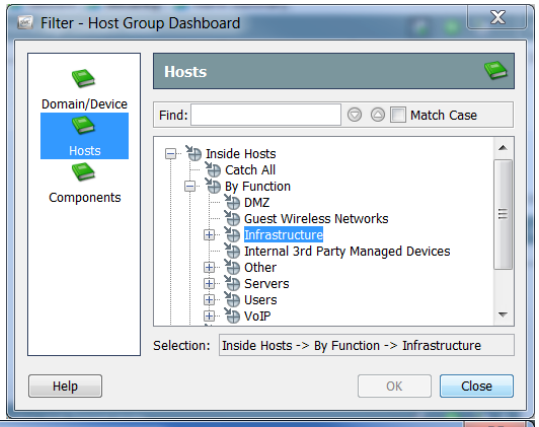


在此示例中，过滤器的“域/设备”页面允许您只更改要查看其数据的域。在上一个示例中，选择了 SmokeNet-Alpha 域。根据控制面板的不同，您可能还可以选择特定的流收集器、导出器和/或接口。

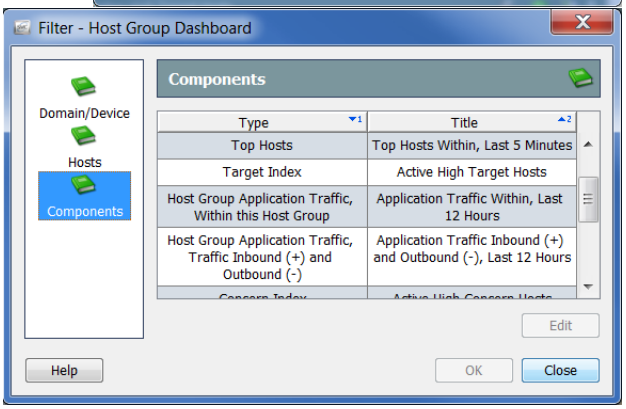
注意：

在过滤器的这三个页面上指定的任何内容都将覆盖组件过滤器上选择的内容，我们很快就会看到这一点。

若要过滤控制面板以显示不同主机组的数据，请打开“主机”页面。您可以浏览主机组列表以进行选择。或者，您可以在“查找”字段中键入主机组的全部或部分名称，以便自动搜索列表并找到所需的主机组。您点击的主机组将显示在屏幕底部的“选择”字段中。在此示例中，点击了“按功能”主机组下的“基础设施”主机组。



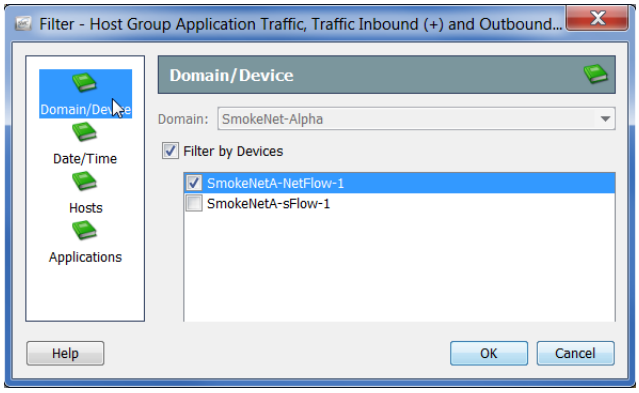
如果打开过滤器的“组件”页面，则可以过滤控制面板上的各个组件。



注意：

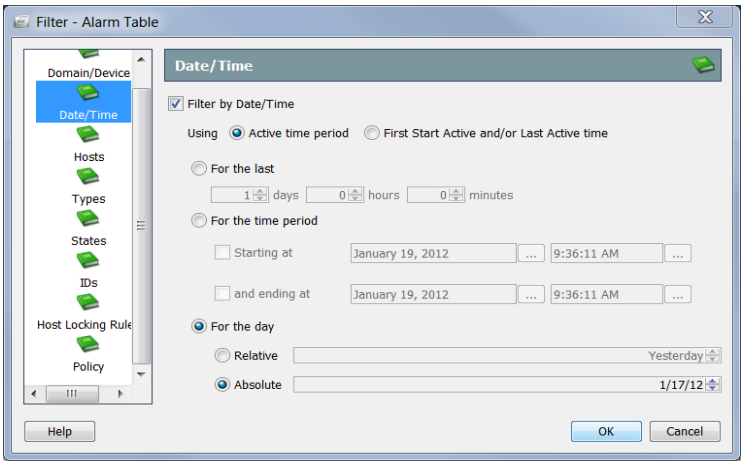
双击组件的标题，使其在控制面板上显示时重命名。

例如，假设您要查看“专用地址”主机组中的任何 Facebook 活动，就像具体时间范围内的特定流收集器所观察到的那样。在这种情况下，您可以点击“类型”列中的**主机组应用流量、流量入站 (+) 和出站 (-)**，然后点击**编辑**。



系统将打开该组件的过滤器对话框。由于您已经在控制面板过滤器中点击了 SmokeNet-Alpha 域，因此不能在此处进行更改。但是，您可以选择要查看其数据的流收集器。

若要指定要查看的时间框架，请打开过滤器的“日期/时间”页面。

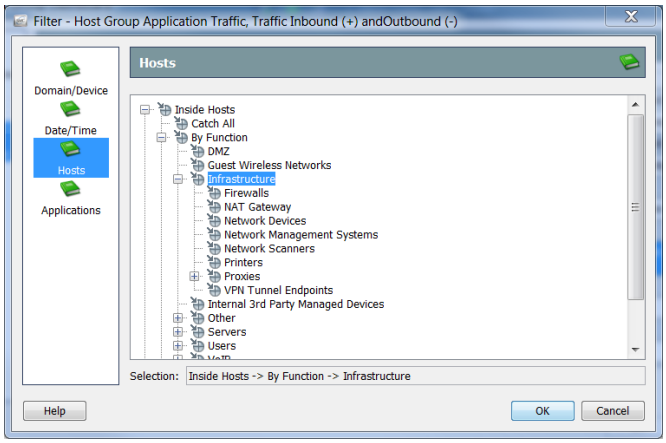


对于您希望保存以便将来使用特定的布局和/或过滤节约进行查看的文档，天设置的“相对”和“绝对”可能非常有用。

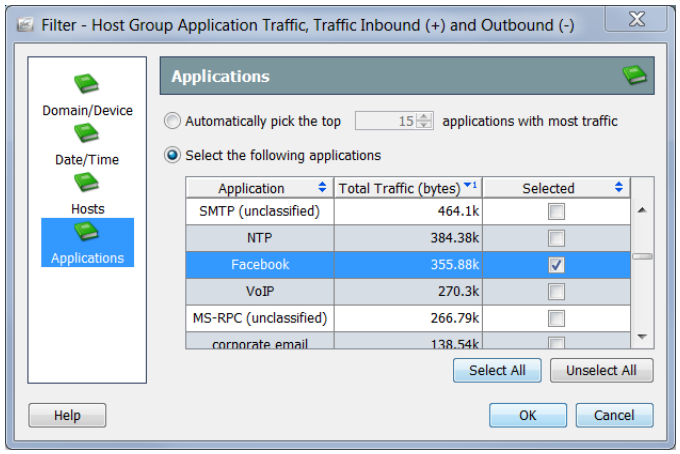
假设在“当天”部分下点击**相对**，然后从列表框中选择**昨天**。然后将文档另存为共享文档。无论何时打开该文档，它都将保留*昨天*作为所选内容。因此，本文档将始终显示当天的前一天的数据。

现在，假设在“当天”部分下点击**绝对**，然后从列表框中选择**1/17/12**。然后将文档另存为共享文档。无论何时打开该文档，它都将保留 *1/17/12* 作为所选内容。因此，此文档将始终向您显示该日期的数据。

由于您已经在控制面板过滤器中点击了“基础设施”主机组，因此不能在组件过滤器的“主机”页面上对其进行更改。您只能查看您的选择



要过滤除 Facebook 之外的所有应用，请打开组件过滤器的“应用”页面。默认情况下，此过滤器会自动选择会引发最多流量的前 10 个应用。点击**选择下列应用**选项，然后点击右下角的**取消选中所有**以清除所有选定的应用。最后，点击 **Facebook** 复选框以添加复选标记。



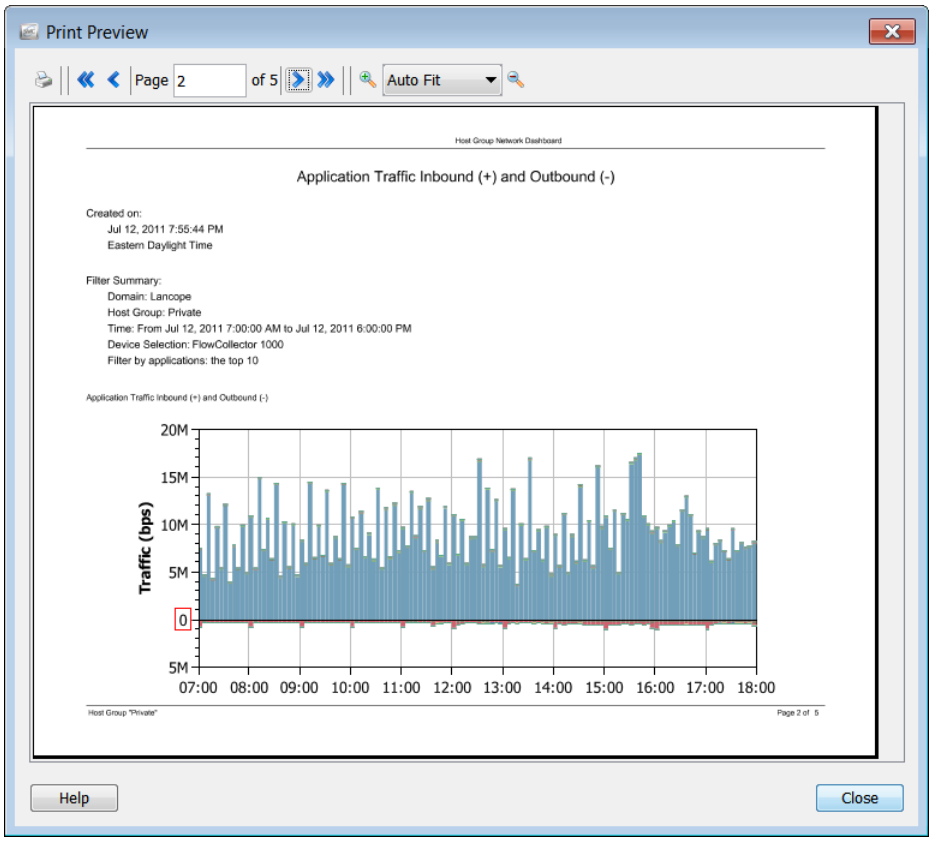
完成后，点击**确定**以关闭组件过滤器并返回到控制面板过滤器。当完成对控制面板过滤器的更改（如果有）时，点击**确定**以使用所选数据集刷新控制面板。

打印文档

您可能需要打印 SMC 文档以进行存档或报告、以备以后查看或发送给同事。SMC 允许您预览文档、自定义打印设置、打印并将文档另存为 PDF 文件。

打印预览

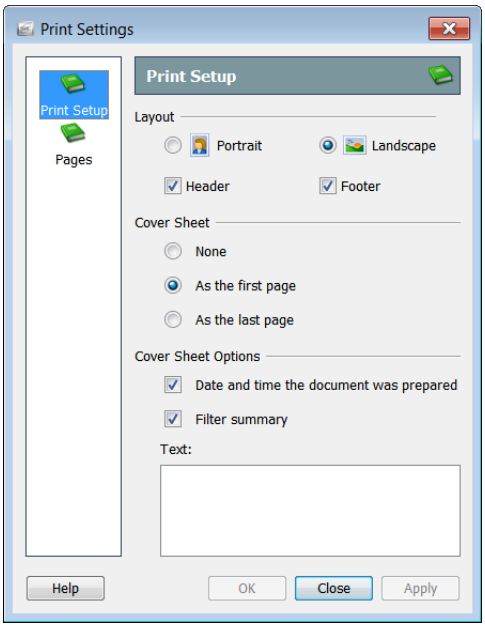
要预览文档在打印前的外观，请从主菜单中选择**文件 > 打印预览**。“打印预览”对话框随即打开。



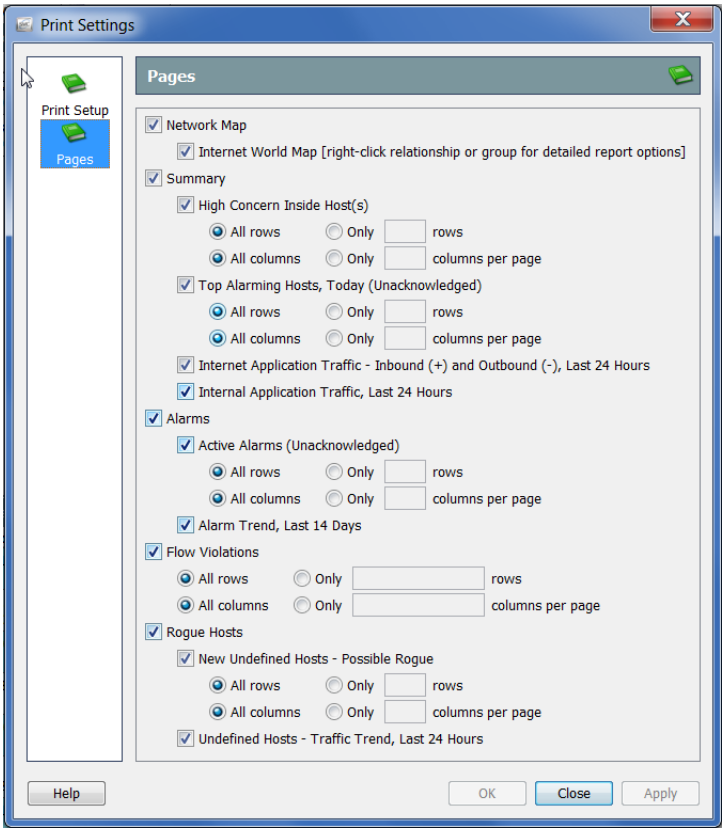
打印设置

若要在打印文档之前自定义打印外观，请使用“打印设置”功能。从主菜单中选择**文件 > 打印设置**以打开“打印设置”对话框。

在“打印设置”页面上，您可以将页面的布局定义为“纵向”或“横向”。如果需要，还可以添加页眉、页脚甚至封面。

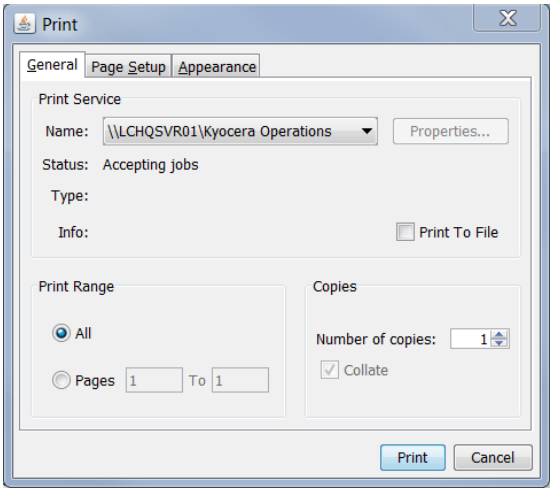


在“页面”页面上，您可以选择要打印的文档页面，以及哪些列和/或行。



打印

要打印文档，请从主菜单选择**文件中打印**。“打印”对话框随即打开。



注意：

要获得更高质量的字体，请在“首选项: PDF 查看器”对话框中设置外部 PDF 查看器（如 Adobe Acrobat 阅读器）的路径，您可以通过从主菜单中选择**编辑 > 首选项**来访问该对话框。

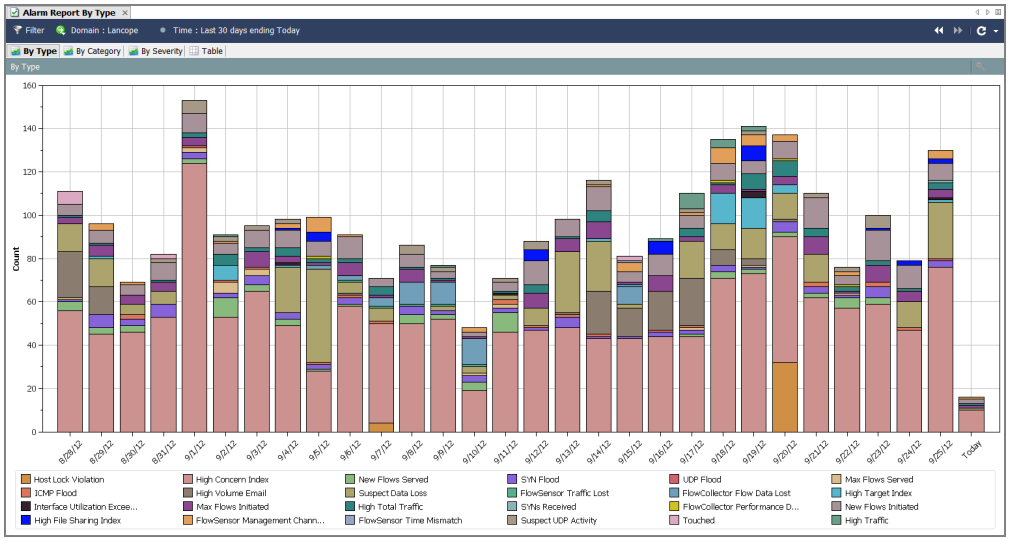
保存文档

保存文档布局供以后使用

如果您重新排列了 SMC 文档的布局，并且希望保存该布局以供以后使用，请保存该文档。保存文档时，该文档将被保存到 SMC 设备中以供随时检索。

要保存文档，请完成以下步骤：

1. 打开您想要保存的文档。例如，我们将打开“按类型的警报报告”文档。



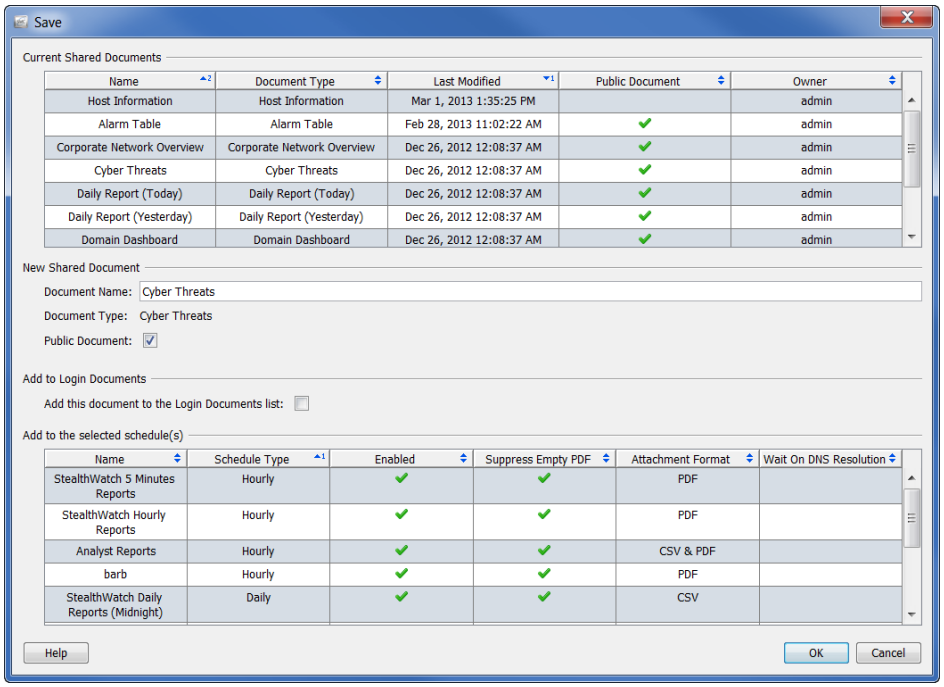
2. 对布局或过滤器设置进行任何所需的更改。
3. （可选）从 SMC 主菜单中选择**文件 > 打印设置**，并在打开的对话框中配置您希望文档在每次打印时的外观。点击**确定**保存更改。
4. （可选）若要查看文档作为 PDF 显示的方式，请选择**文件 > 打印预览**。

注意：

如果要对文档布局进行更改并保留更改（例如更改列位置或更改显示的列），请选择**文件 > 使用设置为默认值**。这些更改将在您下次打开文档时生效。

5. 执行以下操作之一：
   - 如果您只想用相同的名称替换以前的版本，请从 SMC 主菜单中选择**文件 > 保存**。
   - 如果下列任一情况适用，请从 SMC 主菜单中选择**文件 > 另存为**：
     - 如果要以新名称保存文档副本。
     - 如果您已创建了一个新文档，并且是第一次保存文档。

“保存”对话框随即打开。



6. 在“名称”字段中，为文档键入一个可以轻松识别的名称。（系统将为您建议一个名称。）
7. （可选）如果希望其他用户能够在其用户名下打开此文档，请选中**公共**复选框。

注意：

有关公共文档的详细信息，请参阅第 13 章“处理文档。”中的“公共文档”（第 283 页）

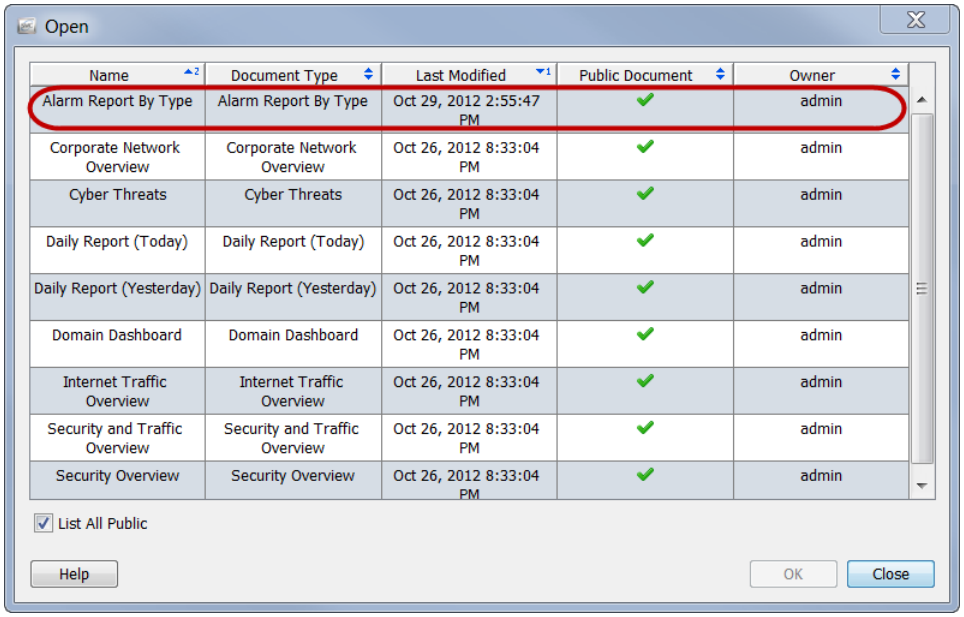
8. （可选）如果希望每次在您的用户名下登录到 SMC 客户端界面时都自动打开文档，请选中“将此文档添加到登录文档列表”复选框。

注意：

有关登录文档的详细信息，请参阅“登录文档”（第 278 页）第 13 章“处理文档。”

9. 点击**确定**。文档会被保存到 SMC 设备。现在，您可以在任何具有 SMC 访问权限的计算机上，使用您指定的布局和/或过滤器设置，在您的用户名下打开此文档。

10. 要打开此文档，请从 SMC 主菜单中选择**文件 > 打开**。“打开”对话框随即打开。



11. 选择文档并点击**确定**。

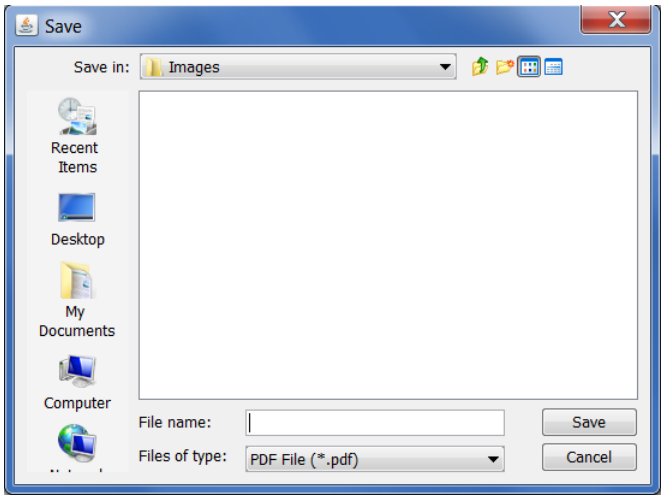
注意：

默认情况下，仅显示保存在您的用户名下的文档。若要列出所有文档（包括由其他用户创建的文档），请选中**列出所有公共文档**复选框。

将文档另存为 PDF 文件

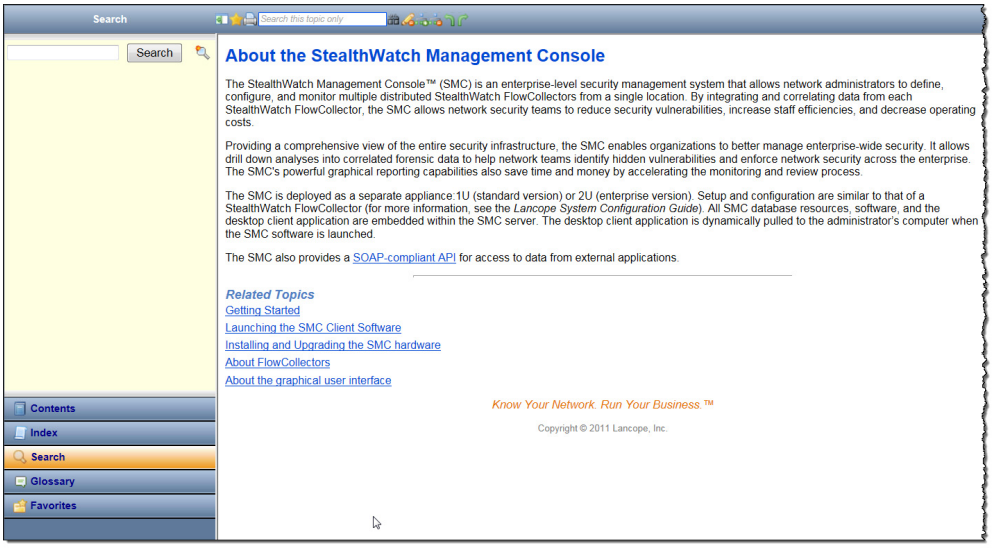
要将活动的 SMC 文档保存为 PDF 文件，请从主菜单中选择**文件 > 打印到文件**。系统将打开“保存”对话框。

打开“保存”对话框时，导航到要在其下保存文档的目录和文件名，然后点击**保存**。然后，您可以使用任何可以阅读 PDF 文件的工具打开文档。



联机帮助

如果您需要有关任何 SMC 文档的详细信息，请按键盘上的 **F1** 键或 **Ctrl+H** 以查看 *SMC 客户端联机帮助*。您还可以转到主菜单并选择**帮助 > 帮助**。



如果在文档处于活动状态时访问联机帮助，则会看到与该文档相关的帮助主题。如果没有打开的文档，您将看到介绍性的帮助主题“关于 Stealthwatch 管理控制台”。

注意：

您可能需要使用登录到 SMC 客户端界面时所使用的相同凭证登录。如果看不到活动文档的信息，请返回 SMC 客户端界面，然后再次按 **F1**。

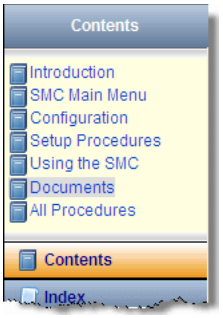
访问 *SMC 客户端联机帮助*后，有多种方法可以使用左侧导航窗格底部的以下按钮查找信息：

- 目录
- 索引
- 搜索
- 术语表
- 常用联系人

您还可以使用主题区域顶部的“快速搜索”功能来搜索打开的主题。

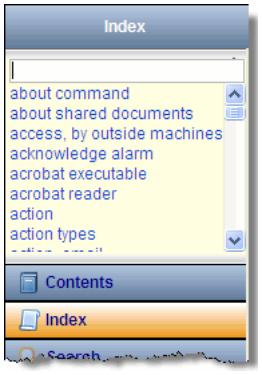
目录

“目录”窗格提供联机帮助的目录，其组织方式与书籍的目录非常类似。若要查看，请点击左侧导航窗格底部的**目录**。点击列表中的项目可查看相应的帮助主题。



索引

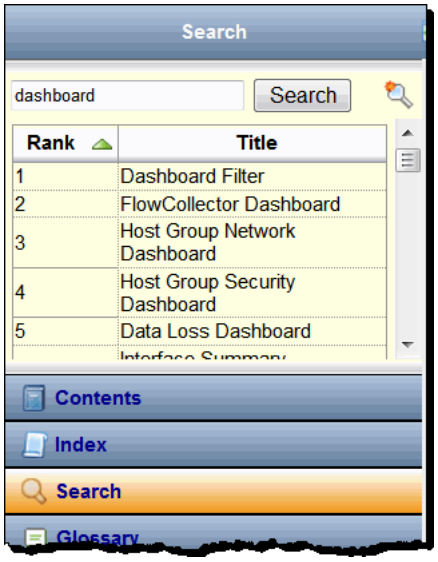
“索引”窗格提供了可对其进行搜索以查找相关主题的单词列表。若要查看，请点击左侧导航窗格底部的**索引**。点击列表中的项目可查看该帮助主题。您可以浏览列表并进行选择，也可以在顶部的字段中键入文本，以便立即转到列表中的该文本。然后，进行选择以查看所需的主题。



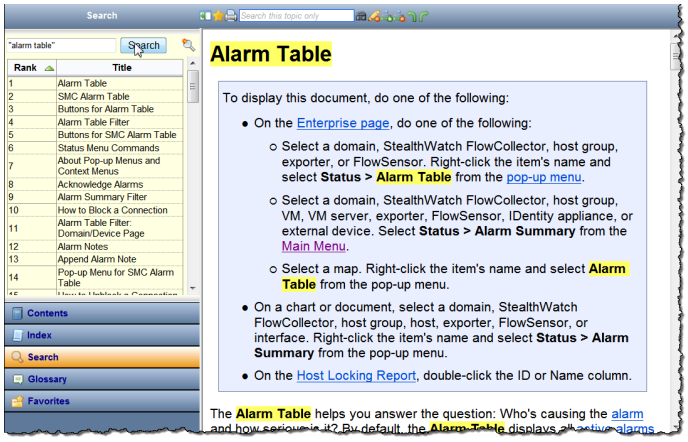
搜索

如果在访问联机帮助时没有打开任何文档，则默认会打开“搜索”窗格。在顶部的字段中键入要查找的文本，然后点击左侧导航窗格底部的**搜索**，或在键盘上按 **Enter**。主题列表将会显示，根据与您键入的文本的相关性排列。点击项目可查看该主题。

除了进行常规的信息查询，如果您需要了解如何打开特定的 SMC 文档，此功能也很方便。与特定文档相关的每个帮助主题都就如何访问该文档在第一段提供了说明。

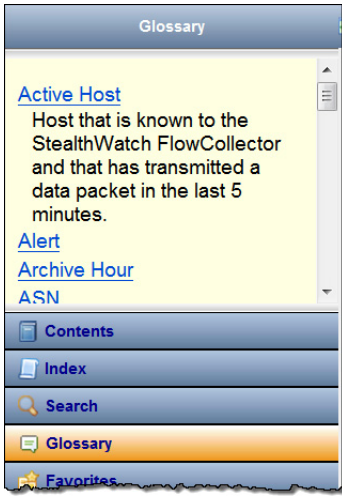


例如，假设您需要打开警报表，但您不知道或不记得如何打开。只需在“搜索”字段中键入“警报表”，然后按 **Enter** 键。当“警报表帮助”主题出现在搜索结果中时，点击主题名称。当出现“帮助”主题时，您将看到有关访问警报表的说明。



如果在联机帮助中有经常查找的项目，则可以将搜索文本添加到“收藏夹”列表中。只需在“搜索”字段中键入文本，然后点击**搜索收藏夹** 按钮。下次需要搜索该文本时，可以直接转到“收藏夹”列表并点击它。

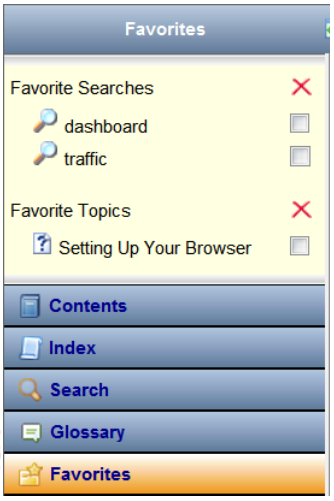
术语表



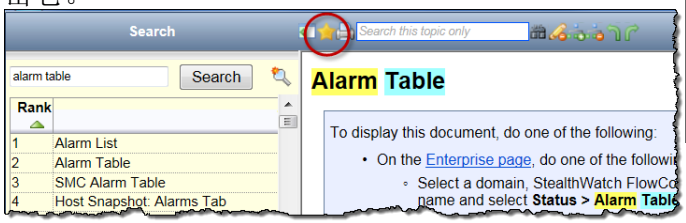
“词汇表”窗格提供了在整个 Stealthwatch 系统中常用的单词的定义。若要查看，请点击左侧导航窗格底部的**词汇表**。点击列表中的某个单词可查看其定义。

常用联系人

“收藏夹”窗格包括任何已标记为“收藏”的搜索项或主题。若要查看，请点击左侧导航窗格底部的**收藏夹**。



我们已经讨论了如何将搜索文本添加到您的“收藏夹”列表中。您也可以向列表中添加主题。如果您发现需要经常引用特定的主题，则此功能会很有用。在要添加到收藏夹列表的主题上方的“帮助”工具栏中，点击**主题收藏夹** 按钮。下次需要查看该主题时，可以直接转到“收藏夹”列表并点击它。



如果点击收藏夹搜索项，将会打开“搜索”窗格，列出与该项目相关的主题。点击列表中的项目可查看该帮助主题。

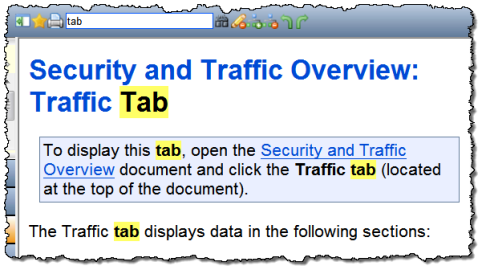
如果点击收藏夹主题项，将打开该帮助主题。

若要从“收藏夹”列表中删除项目，请点击相应的复选框 以添加复选标记，然后点击 按钮。

快速搜索

“快速搜索”字段位于“帮助”工具栏的“帮助”主题的上方。

此字段允许您在正在查看的“帮助”主题中搜索文本。只需在“快速搜索”字段中键入文本，然后点击键盘上的**搜索** 按钮或按 **Enter**。如果您键入的文本出现在主题中，它将以黄色突出显示，如下面的示例所示。若要删除突出显示，请点击**荧光笔** 按钮。



注意：

有关“帮助”工具栏中任何按钮的详细信息，请将光标悬停在按钮上以查看工具提示。

键盘快捷键

下表提供了可用来在 SMC 客户端界面中执行各种功能的键盘快捷键列表。其中许多快捷键相当于从主菜单进行选择。

注意：

我们没有讨论这份清单中提到的所有文档，但当您更加熟悉 SMC 时，这将成为您的编辑参考。

媒体	所需的操作...
←	在图表上：在放大区域向后（左）移动。
→	在图表上：在放大区域向前（右）移动。
↑	在图表上：在放大区域向上移动。 在使用树的“查找”字段时：在树中找到具有与“查找”字段中的文本相同的上一个项目。
↓	在图表上：在放大区域向下移动。 在使用树的“查找”字段时：在树中找到具有与“查找”字段中的文本相同的下一个项目。
Alt + ←	当有多个文档打开时，查看位于活动文档左侧的文档。 在流快速视图对话框上：从一个选项卡向左移动到另一个选项卡。
Alt + →	当有多个文档打开时，查看位于活动文档右侧的文档。 在流快速视图对话框上：从一个选项卡向右移动到另一个选项卡。
Alt + ↑	在快速视图对话框上：在相应文档表中向上移动一行。
Alt + ↓	在快速视图对话框上：在相应文档表中向下移动一行。
Alt + F	当企业树查找字段隐藏：显示查找字段。 当企业树查找字段显示：将光标放在查找字段中。
Ctrl	在表上，点击列标题的同时按该键，可删除此列的任何排序。

- 续 -

媒体	所需的操作...
Ctrl + ←	显示早些时候有关活动文档的数据。 此快捷键与从主菜单中选择**查看 > 时间倒流**一样。也可以点击主工具栏上的**时间倒流**按钮  。
Ctrl + →	显示晚些时候有关活动文档的数据。 此快捷键与从主菜单中选择**查看 > 时间快进**一样。也可以点击主工具栏上的**时间快进**按钮  。
Ctrl + B	打开文档生成器，以便您可以创建自己的自定义文档和布局。 此快捷键与从主菜单中选择**查看 > 文档生成器**一样。在文档生成器上，此快捷键与选择**查看 > 新文档生成器**一样。
Ctrl + C	复制选定的文本。 此快捷键与从主菜单选择**编辑 > 复制**一样。
Ctrl + D	每次打开特定 SMC 文档时，请使用相同的布局设置。 此快捷键与从主菜单选择**文件 > 使用设置作为默认值**一样。
Ctrl + E	打开主机组编辑器。 此快捷键与从主菜单中选择**配置 > 编辑主机组**一样。
Ctrl + F	当企业树查找字段隐藏：显示查找字段。
Ctrl + G	将光标置于全局搜索字段中，在所有 SMC 文档中搜索 IP 地址、警报 ID、VM 或 VM 服务器。 此快捷键与从主菜单中选择**编辑 > 全局搜索**一样。
Ctrl + H	显示适合活动对话框或文档的联机帮助。（您可能需要先登录。） 此快捷键与从文档生成器主菜单中选择**帮助 > 帮助**一样。
Ctrl + I	显示选定物体的属性。 此快捷键与从主菜单中选择**配置 > 属性**一样。
Ctrl + L	查看许可证管理器。 此快捷键与从主菜单中选择**帮助 > 许可证管理**一样。
- 续 -	

媒体	所需的操作...
Ctrl + N	打开 SMC 客户端界面的新实例。 此快捷键与从主菜单中选择**查看 > 新主窗口**一样。
Ctrl + O	打开保存为 DAR 文件的文档。 此快捷键与从主菜单中选择**文件 > 打开**一样。
Ctrl + P	打印活动文档。 此快捷键与从主菜单中选择**文件 > 打印**一样。
Ctrl + Q	关闭 SMC 客户端界面（即，退出）。 此快捷键与从主菜单中选择**文件 > 退出**一样。
Ctrl + S	将具有一组特定布局和过滤器设置的活动文档保存为 DAR 文件。 此快捷键与从主菜单中选择**文件 > 另存为**一样。
Ctrl + T	隐藏或显示企业树。 此快捷键与从主菜单中选择**查看 > 隐藏/显示树**一样。
Ctrl + V	将复制的文本插入（粘贴）到可编辑字段中。 此快捷键与从主菜单中选择**编辑 > 粘贴**一样。
Ctrl + W	关闭活动文档。 此快捷键与从主菜单中选择**文件 > 关闭**一样。
Ctrl + Shift + C	折叠树上的选定分支，如果未选择分支，则折叠树上的所有项目。 此快捷键与从文档生成器主菜单中选择**查看 > 全部折叠**一样。
Ctrl + Shift + E	展开树上的选定分支，如果未选择分支，则展开树上的所有项目。 此快捷键与从文档生成器主菜单中选择**查看 > 全部展开**一样。
Ctrl + Shift + S	用新名称将具有一套特定的布局和过滤器设置的活动文档另存为 DAR 文件。 此快捷键与从主菜单中选择**文件 > 另存为**一样。
Ctrl + Shift + W	关闭所有已打开的文档。 此快捷键与从主菜单中选择**文件 > 全部关闭**一样。
- 续 -	

媒体	所需的操作...
Delete	删除所选项目。 此快捷键与从主菜单中选择**配置 > 删除**一样。
Esc	关闭对话框窗口。
F	在图表上：返回初始缩放水平。
F1	查看适合活动对话框或文档的联机帮助。（您可能需要先登录。）
F3	在文档生成器中：在搜索树中查找与搜索字段有相同文本的下一个项目。 此快捷键与从文档生成器主菜单中选择**编辑 > 查找树中的下一项**一样。
F5	在活动文档中刷新数据。 此快捷键与从主菜单中选择**查看 > 刷新**一样。也可以点击主工具栏上的**刷新**按钮 。
Alt + ←	当一个已打开的文档包含多个选项卡时，查看活动选项卡左侧的选项卡。
Alt + →	当一个已打开的文档包含多个选项卡时，查看活动选项卡右侧的选项卡。
Shift + F3	在文档生成器中：在搜索树中查找与搜索字段有相同文本的上一个项目。 此快捷键与从文档生成器主菜单中选择**编辑 > 查找树中的上一项**。
Spacebar	在某些表上：在某一行内点击，按空格键，可显示选定项目的快速视图对话框。如果快速视图对话框已打开，可按空格键将其关闭。
Z	在图表上：在 X 轴上放大。

4

主机管理

概述

单独管理网络中的所有主机是一项艰巨的任务。不过，使用 Stealthwatch 可以将主机组织为主机组，从而帮助您大幅减少相关的工作量。

通过主机组，您可以灵活地组织主机。一般情况下，主机可以属于多个组。此外，您可以按主机组和/或主机定义策略。

在本章中，您将学习如何有条有理地将主机组织为主机组，从而监控网络的不同区域，同时更加高效地管理主机行为。

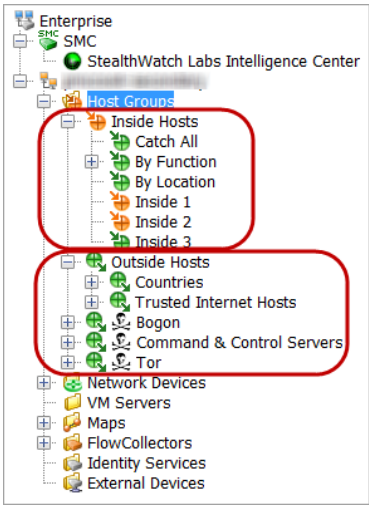
本章包含以下主题：

主机组

主机组实质上是具有类似属性（例如位置、功能或拓扑）的多个主机 IP 地址或 IP 地址范围的虚拟容器。通过将主机组合成主机组，可以控制 Stealthwatch 流量收集器如何分组（而非单独）监控和响应这些主机的行为。

管理员可以按照有益于组织的任何方式组织主机。有了这种自由度，报告和流量管理会变得无比灵活。此外，策略管理变得更加轻松，使管理员可以根据这些主机在网络中的作用来设置主机策略。

SMC 客户端界面以企业树形式显示主机组结构及网络结构，如以下示例所示。默认情况下，每个域包含以下顶级主机组，您可以向顶级主机组中添加从属主机组：



- **内部主机** - 只要主机组中包含的主机已明确定义为您网络的一部分，则属于此顶级主机组。
- **外部主机** - 只要主机组中包含的主机未明确定义为您网络的一部分，则属于此顶级主机组。

注意：
您的登录权限决定您是否可以查看企业树中的所有主机组。

根据您的登录权限，您可以按需添加任意数量的顶级主机组，每个组可包含所需的任意数量的从属主机组，而从属主机组中还可以包含从属主机组。未针对特定主机组定义的任何 IP 地址会自动进入“外部主机”主机组的“国家/地区”从属主机组。使用的主机组名称可以重复，但不能位于同一主机组级别（即，在同一父主机组下）。

注意：
虽然您可以在企业树“主机组”分支下的任意级别创建主机组，但我们建议您将它们添加到“内部主机”或“外部主机”分支之下。

默认情况下，Stealthwatch 系统不会为网络外部的主机创建策略。但是，如果需要定期跟踪产生网络流量的外部主机，可以将它们放到“外部主机”主机组中，并为该组建立策略。然后，您即可像对待内部主机一样调整设置。

注意：

如果为了实现特殊报告目的而需要创建顶级主机组（即与“内部主机”或“外部主机”位于相同级别），可以这么做。

下面是可能需要跟踪特定外部主机行为的一些情况：

- 正在使用外部 DNS 服务器时。
- 有第三方顾问或供应商定期访问您的网络时。
- 有合作伙伴公司定期访问您的网络时。

捕获所有主机组

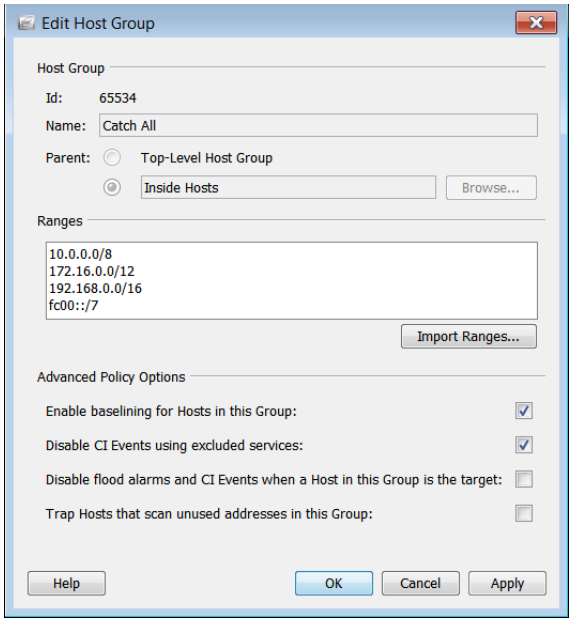
“内部主机”主机组包含默认的“全部捕获”从属主机组。管理员可以使用“全部捕获”主机组来帮助改善主机组结构。

我们建议您一开始将与网络相对应的所有大型 IP 范围放在“全部捕获”主机组中。然后，随着您创建包含更窄定义的 IP 范围或特定 IP 地址的其他主机组，这些范围/地址将自动从“全部捕获”主机组中移出。

在默认情况下，适用于 Stealthwatch 系统 v6 的新 SMC 安装将以下 IP 范围（RFC 1918 和 RFC 4193）纳入“全部捕获”主机组中：

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16
- fc00::/7

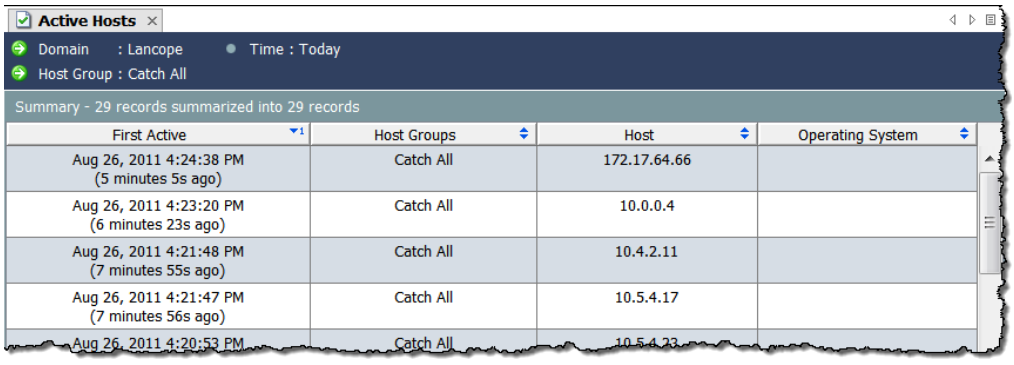
如果您已注册任何公共 IP 地址，我们建议您同时手动将这些范围放到“全部捕获”主机组中。右键点击企业树中的**全部捕获**主机组，然后选择**配置 > 主机组属性**查看“全部捕获”主机组中已定义的 IP 范围/地址（可查看的具体信息取决于您的登录权限）。



注意：

- 要编辑任何主机组，请右键点击企业树中的该主机组，然后选择**配置 > 主机组属性**。
- 主机名可以使用字母数字字符，包括以下特殊字符：< , > . ? ” ‘ : ; | { [}] + = _ - ( ) * & ^ % $ # @ ! ~ ‘ 和“空格”。

理想情况下，在完成定义主机组结构时，“全部捕获”主机组中应没有其他活动的 IP 地址。要识别任何欺诈主机 IP 地址，可以查看“全部捕获”主机组的“活动主机”文档。只需右键点击企业树中的**全部捕获**主机组，然后选择**主机 > 活动主机**即可。

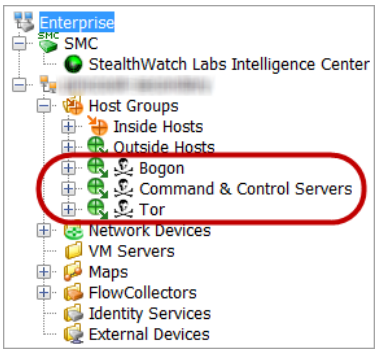


当然，每个网络不尽相同，但在向“全部捕获”主机组分配主机时需考虑下面的一些事项：

- 网络中的哪些领域相比其他领域更为敏感？
- 网络的哪些领域相比相对稳定的领域变化频繁？
- 您的关键资产在哪里？
- 哪些主机执行类似的功能？
- 您的主机执行哪些不同的功能？
- 您的任何主机是否比较古怪且时常表现“异常”？

SLIC 威胁源主机组

SLIC 威胁源包含已知用于恶意活动的 IP 地址、端口号、协议、主机名和 URL。以下主机组包括在“SLIC 威胁源”中：



- Bogon - Bogon 是尚未正式分配到公共网络中的 IP 地址。
- 命令和控制服务器 - C&C 服务器是向僵尸网络发布命令并从被劫持计算机接收报告的中央计算机。
- Tor - Tor 是一种互联网匿名化服务。

注意：

要检测 SLIC 服务器源中可能正在与您的主机通信的 URL，您必须安装配置为导出 IPFIX（相对 NetFlow）的 FlowSensor 或路由器。（默认情况下，FlowSensor 已配置为导出 IPFIX。）

如果您希望调查已与上述某个主机组中的恶意主机通信的主机，但恶意主机不再显示于相关主机组中时，请转至“警报表”并按以下组件过滤：

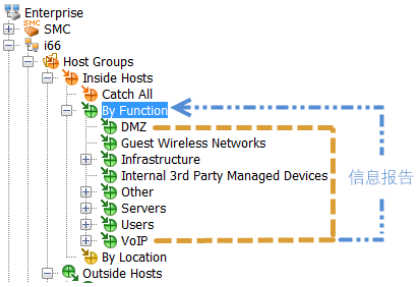
- 类型 - 根据您要过滤的恶意主机的类型，选择适用的 Bogon、命令和控制或 Tor 警报。
- 日期/时间 - 根据您要调查的时间段进行过滤。

注意：

“SLIC 威胁源”主机组分支无法重命名、更改、移动或删除。

信息报告

主机组的任何 SMC 文档都包含其从属主机组内所有主机的信息。例如，如果打开“按功能”主机组的主机信息文档（不更改任何过滤器设置），可看到该主机组下每个从属主机组内的所有主机以及直接在“按功能”主机组下定义的任何主机的相关信息。



创建主机组的策略

此时，您的主机组很可能已经定义。不过，为了帮助您了解主机组的工作方式，让我们花点时间来看看一些如何创建策略的建议。

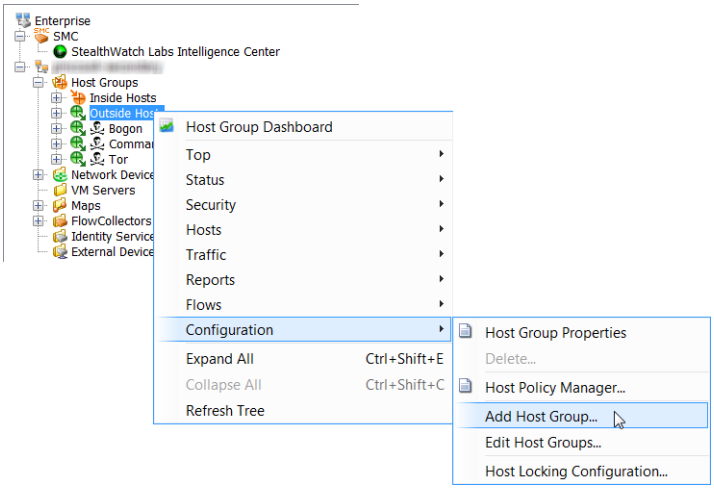
所有 Stealthwatch 流量收集器均随附默认的主机组结构。根据您的登录权限，您可以修改默认主机组以满足您的网络需要。可以创建其他主机组以及删除任何默认主机组，但以下主机组除外：内部主机、全部捕获、外部主机、国家/地区以及命令和控制服务器。

前面，我们讲到建议最初将主机放到“全部捕获”主机组中。此外，我们还建议将彼此行为类似的主机一起放到一个主机组中。不过，您可以为网络、地理区域、IP 段或对您的组织有意义的任何其他类别中的每个部门创建不同的主机组。

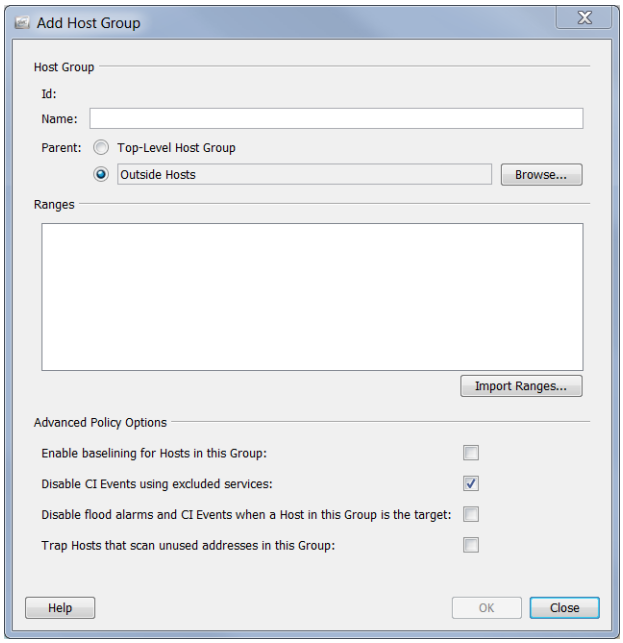
创建主机组

要创建主机组，请完成以下步骤：

1. 在“企业”页面树菜单上，点击**内部主机**或**外部主机**文件夹（要在其中添加另一主机组的文件夹）。
2. 右键点击适用的**内部主机**或**外部主机**主机组，然后选择**配置 > 添加主机组**。



系统随即会打开“添加主机组”对话框。



3. 在“名称”字段中，键入要添加的主机组的名称（例如*合作伙伴*）。
4. 在“父项”字段中，如果默认设置不正确，请点击新主机组的父项。
5. 在“范围”字段中，键入所需的 IP 地址范围。若有包含此主机组 IP 地址的现有文件，请点击**导入范围**。
6. 在**高级策略选项**部分，点击要应用于新主机组的选项。
7. 点击**确定**关闭“添加主机组”对话框。“企业”页面树菜单随即会自动更新为包括新的主机组。

IP 地址

每个主机组中包括的 IP 地址可以是 IPv4 或 IPv6 格式。如果输入 IPv4 IP 地址，则必须使用下表中描述的符号形式：

符号	示例
单一 IP 地址	**10.52.1.55** 仅包含地址为 10.52.1.55 的主机
尾部点子网	**10.52.** 包含从 10.52.0.0 到 10.52.255.255 之间的任何 IP 地址 **注意：**末尾必须包括尾随句点 (.)。

符号	示例
无类域间路由 (CIDR) 符号（例如，使用“/”表示屏蔽位）	**10.52.1.0/24** 包含从 10.52.1.0 到 10.52.1.255 之间的任何 IP 地址 **注意：**如果您希望使用“掩码”输入 IP 地址，请使用此符号。*SMC 客户端联机帮助*提供有关使用 CIDR 符号的更多信息。使用**搜索**功能来查找 **CIDR** 的引用。
网络范围	**10-11.** 包含从 10.0.0.0 到 11.255.255.255 之间的任何 IP 地址 **10.52-53.** 包含从 10.52.0.0 到 10.52.255.255 以及从 10.53.0.0 到 10.53.255.255 之间的任何 IP 地址 **10.52-55.3.** 包含从 10.52.3.0 到 10.52.3.255、从 10.53.3.0 到 10.53.3.255、从 10.54.3.0 到 10.54.3.255 以及从 10.55.3.0 到 10.55.3.255 之间的任何 IP 地址 **注意：**末尾务必包括尾随句点 (.)。
主机范围	**10.52.1.0-10** 包含从 10.52.1.0 到 10.52.1.10 之间的任何 IP 地址 **10.52.0.0-10.52.255.255** 包含从 10.52.0.0 到 10.52.255.255 之间的任何 IP 地址 **注意：**在 IPv4 地址中，最多可使用范围替换两个八位组（例如，10.52.100-255.15-255）。
多个范围	**10.52.100-255.15-255** **10.52.100-255.15-255.3** **1-2.3-4.5-6.7-8**
逗号分隔列表	**10.52.1.10、10.52.1.50、10.100.1.20** 仅包括这三个主机

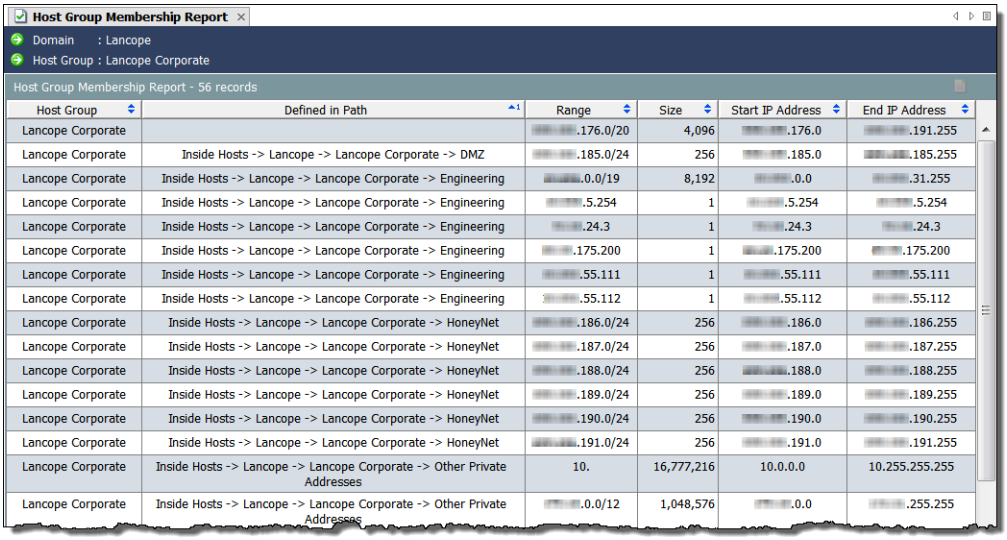
如果输入 IPv6 IP 地址，则必须使用下表中描述的符号形式。

符号	示例
单一 IP 地址	**2001:0DB8:0000:0056:0000:ABCD:EF12:3456** **2001:DB8:0:56:0:ABCD:EF12:3456** **2001:DB8::56:0:ABCD:EF12:3456** **2001:DB80:0:56::ABCD:EF12:3456** **2001:DB80:0:56::ABCD:239.18.52.86**
全局路由前缀子网	**2001:DB8:0:56::/64**

符号	示例
网络范围	**2001:DB8:0:56-58::/64**
主机范围	**2001:DB8:0:56:ABCD:EF12:3456:1-10** **2001:DB8:0:56:ABCD:EF12:3456:1-** **2001:DB8:0:56:ABCD:EF12:3456:10**
多个范围	**2001:DB8:0:56-58:ABCD:EF12:3456:1-10** **2001:DB8:0:56-58:ABCD-ABCF:EF12:3456:1-10**

主机组成员

若要查看主机组结构，请打开“主机组成员报告”。通常，可以通过右键点击企业树中的任何元素，然后选择**报告 > 主机组成员报告**来访问此报告。



Host Group Membership Report

Domain : Lancope

Host Group : Lancope Corporate

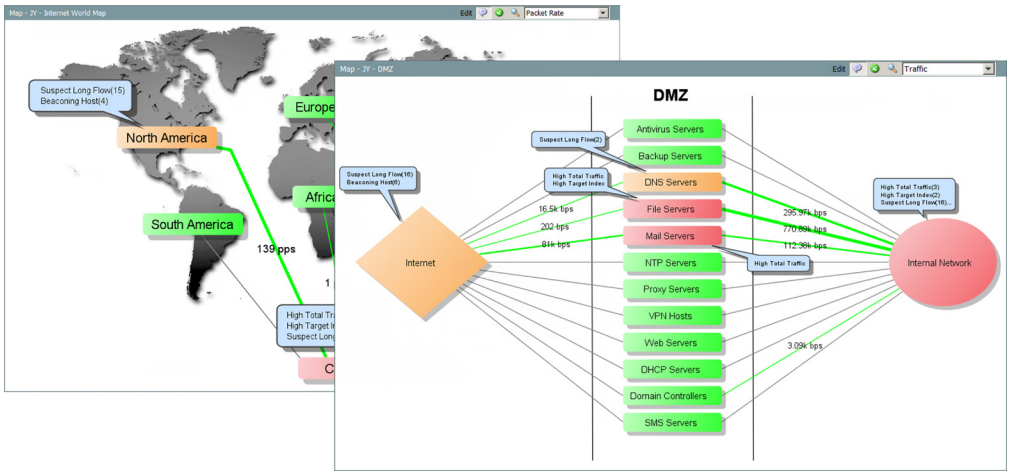
Host Group Membership Report - 56 records

Host Group	Defined in Path	Range	Size	Start IP Address	End IP Address
Lancope Corporate		.176.0/20	4,096	.176.0	.191.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> DMZ	.185.0/24	256	.185.0	.185.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> Engineering	.0.0/19	8,192	.0.0	.31.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> Engineering	.5.254	1	.5.254	.5.254
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> Engineering	.24.3	1	.24.3	.24.3
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> Engineering	.175.200	1	.175.200	.175.200
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> Engineering	.55.111	1	.55.111	.55.111
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> Engineering	.55.112	1	.55.112	.55.112
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> HoneyNet	.186.0/24	256	.186.0	.186.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> HoneyNet	.187.0/24	256	.187.0	.187.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> HoneyNet	.188.0/24	256	.188.0	.188.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> HoneyNet	.189.0/24	256	.189.0	.189.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> HoneyNet	.190.0/24	256	.190.0	.190.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> HoneyNet	.191.0/24	256	.191.0	.191.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> Other Private Addresses	10.	16,777,216	10.0.0.0	10.255.255.255
Lancope Corporate	Inside Hosts -> Lancope -> Lancope Corporate -> Other Private Addresses	.0.0/12	1,048,576	.0.0	.255.255

相关流图

相关流图提供当前网络范围内主机组之间流量状态的图形视图，由此您可以立即查明应关注何处。Stealthwatch 附带若干默认流图，管理员可以根据需要对其进行自定义。

此外，管理员可以根据任何条件（如位置、功能或虚拟环境）轻松构建新的关系图，如以下示例所示。



这些图可以帮助您解答重要问题。通过在两组主机之间创建关系，可以分析在它们之间传输的流量。双击该图中的某个主机组，可以深入探查和了解发生的状况。创建关系后，可以右键点击该关系（主机组之间的线），然后选择**关系 > 策略**启用主机组之间的基准和报警功能。

5

视图和控制面板

概述

默认情况下，SMC 中的文档会显示有关网络中发生的每一个活动的信息。但是，如果您只关心某些类型的流量或警报，应该怎么办？或者，如果您只想查看文档的某些部分而不是文档的所有内容，应该怎么办？SMC 允许您构建自己的控制面板，从而使您能够关注于想要查看的主要信息。

本章包含以下主题：

SMC 中的默认控制面板

SMC 控制台包含许多默认控制面板，以便您可在一个文档中轻松地查看不同类型的信息。要访问这些控制面板，请在主菜单中依次选择**状态 > 控制面板 > [默认控制面板名称]**。

下面是 SMC 控制台中的默认控制面板列表（按字母顺序排列）以及每个面板的说明：

控制面板名称	说明
警报控制面板	此控制面板显示所选域的警报数据。在以下部分中显示数据： ▶ 新建警报 ▶ 已确认的警报
网络威胁控制面板	此控制面板提供有关影响域的网络威胁的图形和表格数据。在以下选项卡中显示数据： ▶ 信誉 ▶ 侦测 ▶ 数据丢失 ▶ 恶意软件 ▶ 僵尸网络
数据丢失控制面板	此控制面板提供有关所选域中数据传输活动的图示。在以下部分中显示数据： ▶ 数据丢失警报（今天） ▶ 现有的数据丢失警报相关主机信息 ▶ 数据丢失报警趋势 ▶ 前 20 次上传（今天）
DDoS 警报控制面板	此控制面板提供以下信息： ▶ 可能表明即将开始发生 DDoS 威胁或 DDoS 攻击的活动 ▶ 有关您的网络上发生的警报的详细信息
DDoS 流量控制面板	此控制面板提供有关可能预示您的网络中发生 DDoS 攻击的流量高峰或流量模式变化的信息。

控制面板名称	说明
流量收集器控制面板	此控制面板提供有关 Stealthwatch 流量收集器上最重要的活动的图示。在以下部分中显示数据： ▶ 状态选项卡 • 流收集统计信息 • 流收集趋势 • 流收集状态 ▶ 警报选项卡 • 流量收集器警报趋势，前 30 天 • 流量收集器警报数，前 30 天
主机组控制面板	有关“主机组”控制面板的信息，请参阅“主机组控制面板”（第 103 页）。
接口摘要控制面板	此控制面板提供有关所选接口流量的各种图形和表格数据。在以下部分中显示数据： ▶ 流量统计信息，最近 6 个小时 ▶ 利用率入站和出站，最近 6 个小时 ▶ 应用流量入站和出站，最近 6 个小时 ▶ 排名靠前的活动通信，入站 ▶ 排名靠前的活动通信，出站
接口流量控制面板	此控制面板提供有关所选接口流量的各种图形和表格数据。在以下部分中显示数据： ▶ 接口服务流量 ▶ 接口应用流量 ▶ 接口统计信息 ▶ 接口利用率 ▶ DSCP 流量
安全概述	此控制面板提供有关系统安全的图形和表格数据。在以下部分中显示数据： ▶ 内部关注主机 ▶ 外部关注主机 ▶ 排名靠前的警报主机 ▶ 按类型生成摘要的当前活动警报
SMC 控制面板	此控制面板提供有关 SMC 控制台最重要活动的图示。在以下部分中显示数据： ▶ SMC 性能 ▶ SMC 警报 ▶ 已处理的 SMC 事件

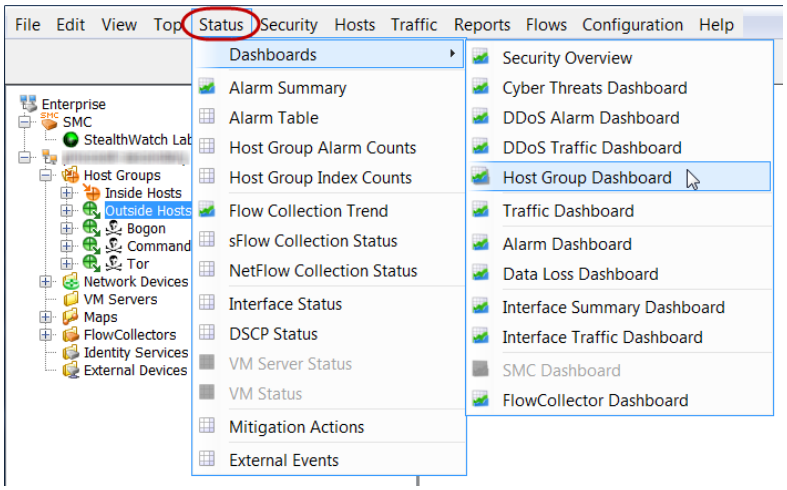
控制面板名称	说明
流量控制面板	此控制面板提供所选域的流量统计信息图示。在以下部分中显示数据： ▶ 协议，来自内部主机和外部主机的数据包 ▶ TCP 标记，来自内部主机和外部主机的数据包 ▶ 内部主机和外部主机发起的活动流数 ▶ 内部和外部的活动主机

注意：

有关这些控制面板的详细信息，请参阅 *SMC 客户端联机帮助*。

主机组控制面板

主机组控制面板提供所选主机组的重要网络、安全和警报活动的图形和表格数据。此数据每 5 分钟从 SMC 收集一次。要显示此文档，请首先点击企业树中要查看其数据的主机，然后从 SMC 主菜单中依次选择**状态 > 控制面板 > 主机组控制面板**。

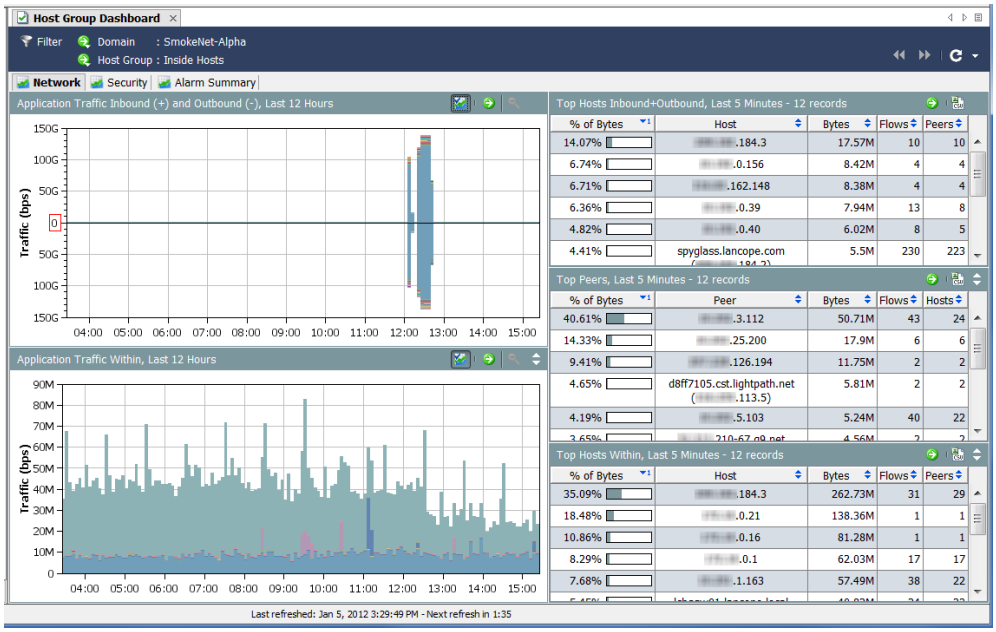


有关如何在主机组控制面板内查看以下页面的信息，请转到本章其余部分的相应章节：

- 网络页面
- 安全页面
- 警报摘要页面

主机组控制面板 - 网络页面

“主机组控制面板：网络”页面提供所选主机组重要安全相关活动的图形和表格数据。要查看此控制面板，请点击**网络**选项卡。

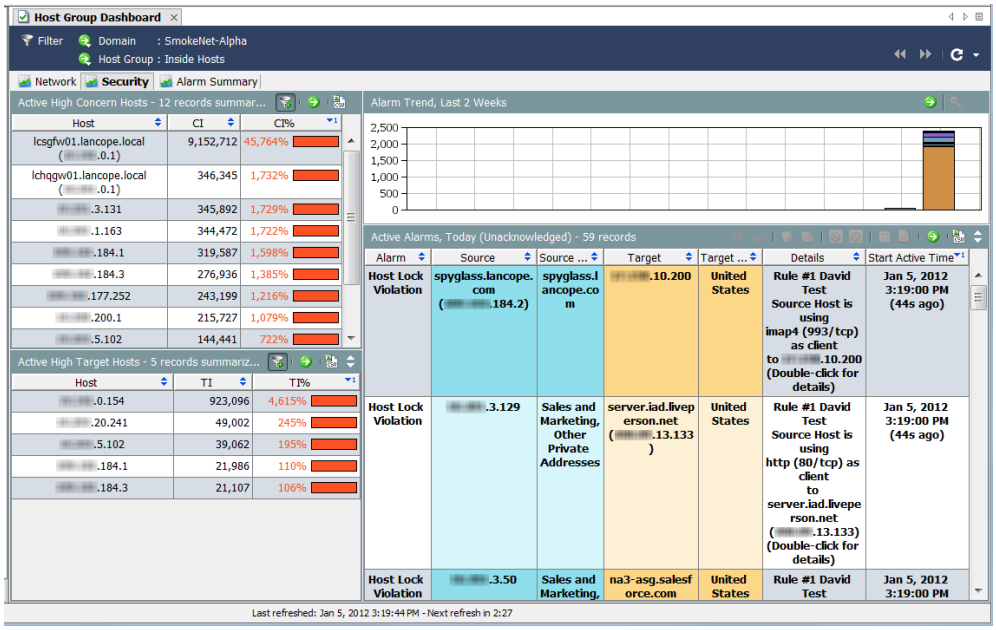


查看网络页面时，问自己以下问题：

- “应用”图中是否显示您的组织中通常不使用的应用出现大量流量？
- “应用”图中是否显示在一天当中的某些时间（例如正常办公时间之后），通常不使用的应用出现大量流量？
- “应用”图中是否显示未定义的应用或其他应用出现大量流量？如果是，则应配置更多应用定义。
- “活跃度排名靠前的主机”表是否包括通常不应出现在活跃度排名靠前的主机列表中的主机？
- “靠前的活动主机”表是否显示有少量主机占用极大比例的流量？

主机组控制面板 - 安全页面

“主机组控制面板：安全”页面是显示的第一个控制面板。此页面以文档形式提供有关所选主机组的重要安全相关活动的图形和表格数据。



注意：

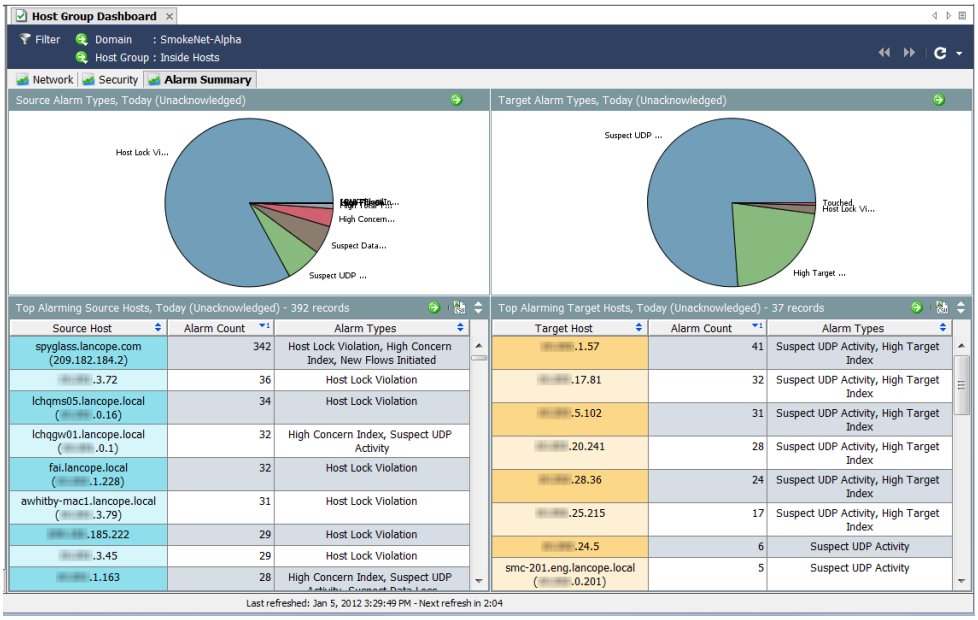
点击每个文档页眉上的**转到文档**按钮 可按单独文档形式打开每个组件。

查看安全页面时，问自己以下问题：

- “高 CI 主机”表是否显示对您的组织重要的主机出现高关注指数？
- “按主机组统计的警报报告”表是否显示敏感主机组的高关注指数警报？
- “按主机组统计的警报报告”表是否显示任意特定日的高关注指数警报高峰？
- “报警排名靠前的主机”表是否显示对您的组织重要的主机的大量警报？
- “报警排名靠前的主机”表是否显示您特别关注的警报类型？
- “热门扫描”表是否显示对您的组织十分重要的源主机或目标主机的大量 TCP/UDP 地址扫描？

主机组控制面板 - 警报摘要页面

“主机组控制面板：警报摘要”页面提供所选主机组的警报活动的图形摘要以及详细表格数据。要查看此控制面板，请点击**警报摘要**选项卡。



查看警报页面时，问自己以下问题：

- 这些表是否显示对您的组织十分重要的主机或主机组的大量警报？
- 这些表是否显示您特别关注的警报类型？

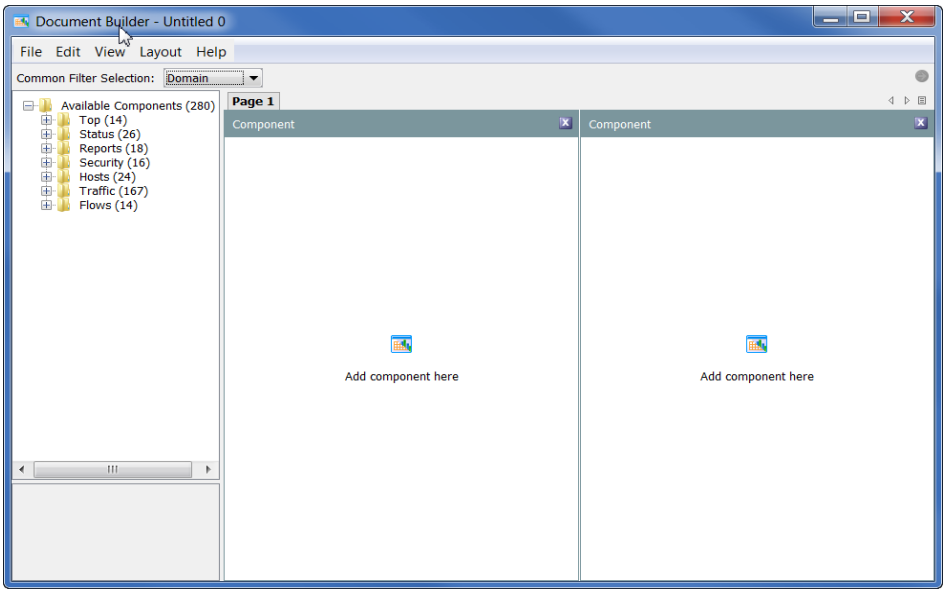
构建自己的控制面板

使用文档生成器，可创建包含所需的任何 SMC 组件以及要查看的数据的自定义控制面板（控制面板是不同报告的集合）。您甚至可以将这些组件重命名为对您而言更有意义的文本。

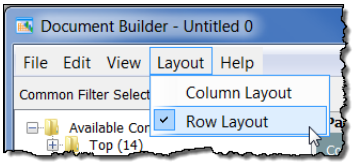
为了说明起见，我们将构建一个仅关注安全警报的“安全报告”控制面板。我们的示例将包含多个选项卡，每个选项卡包含多个组件。不过，您可以按相同的理念构建所需的任何类型的控制面板。

要构建自己的自定义控制面板，请完成以下步骤：

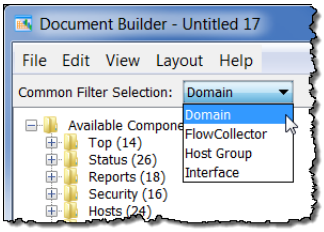
1. 从 SMC 主菜单中依次选择**查看 > 文档生成器**。此时将打开“文档生成器”对话框。



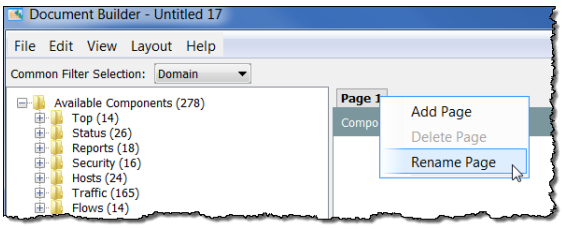
2. 如果您希望文档为行格式而不是列格式（默认），请从“文档生成器”主菜单中依次选择**布局 > 行布局**。

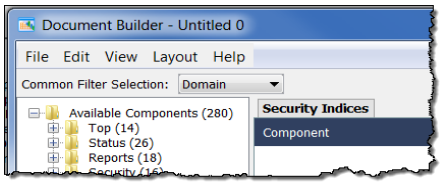


3. 点击“常用过滤选项”下拉列表中的箭头，然后点击默认要对此文档应用的过滤选项。在右侧示例中，该文档将按域进行过滤。



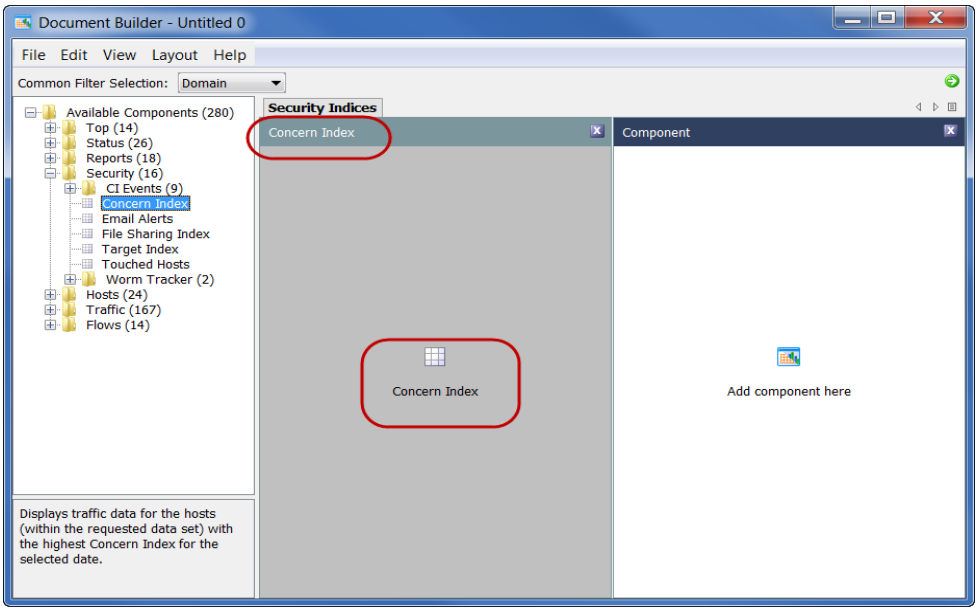
4. 如果要对某个页面重命名，请右键点击该页面的选项卡，然后选择**重命名页面**。（另外，您还可以双击选项卡，直接在该选项卡上键入新的页面名称。）





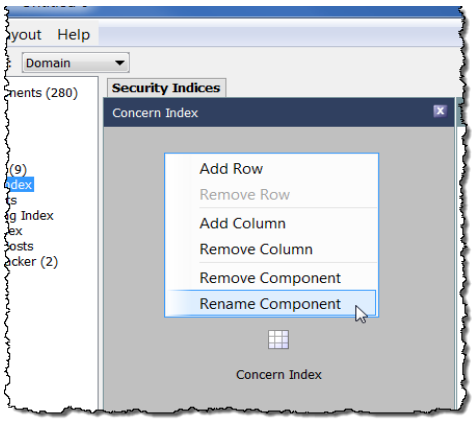
在左侧示例中，我们已将页面选项卡上的名称从*第 1 页*更改为*安全指数*。

5. 从左侧树菜单中点击要添加的组件，并将其拖到页面上要放置其的区域。在以下示例中，我们将“关注指数”组件拖到了左侧列中。

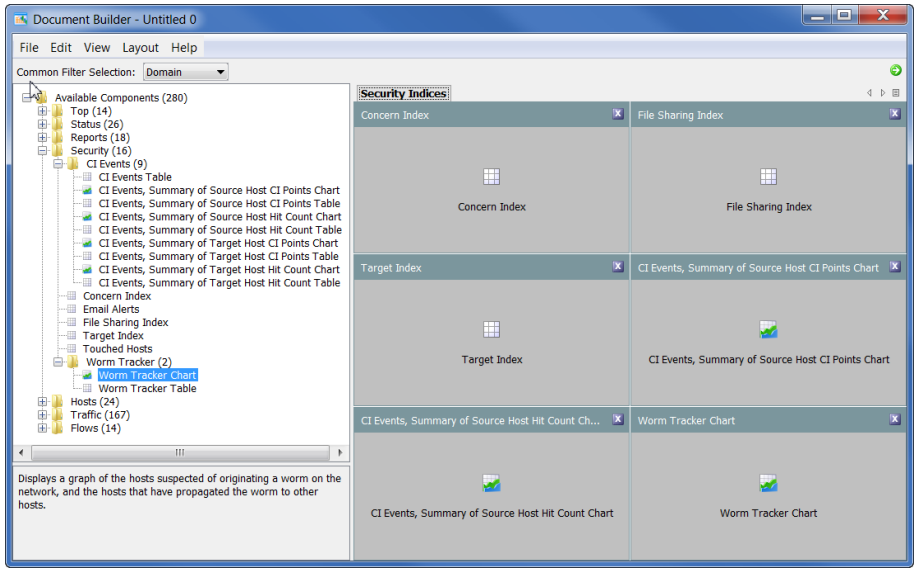


请注意，该组件的名称已从*组件*更改为*关注指数*，即我们刚才添加的组件的名称。另请注意，该列中间图标的名称也已更改为我们刚才添加的组件的名称。

6. 若要重命名该组件，请右键点击该组件的正文，然后选择**重命名组件**。



7. 继续将组件添加到此页面中，直到完成。默认页面仅显示两个组件区域。不过，如果添加的组件超过两个，它会相应地进行调整。以下示例中有六个组件。每次将新组件添加到列中时，它都会显示在该列最后一项的下面。如有必要，可以随时更改布局。

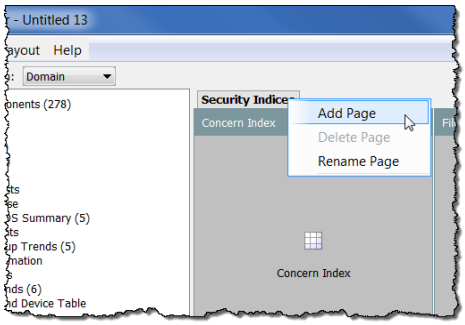


注意：

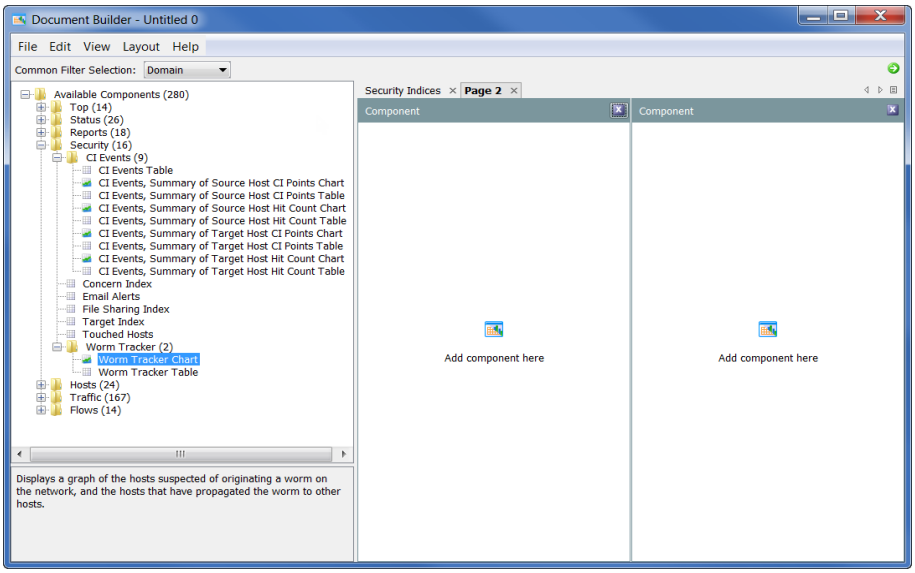
点击  按钮一次可清空组件区域。

点击  按钮两次可完全删除组件区域。

8. 如果要将其他页面（选项卡）添加到您的文档中，请右键点击现有的选项卡，然后选择**添加页面**。



系统随即会打开新的空白页。



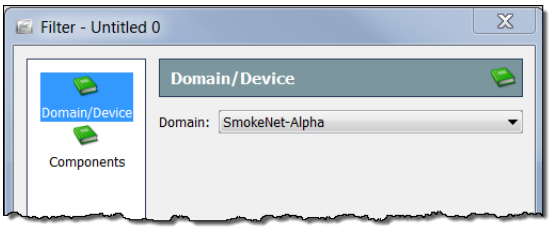
9. 将组件拖动到此页面上放置它们的位置，就像对第一页执行的操作一样。

10. 完成文档排版后，依次点击**文件 > 另存为**可将其作为 XML 模板保存到硬盘驱动器上。

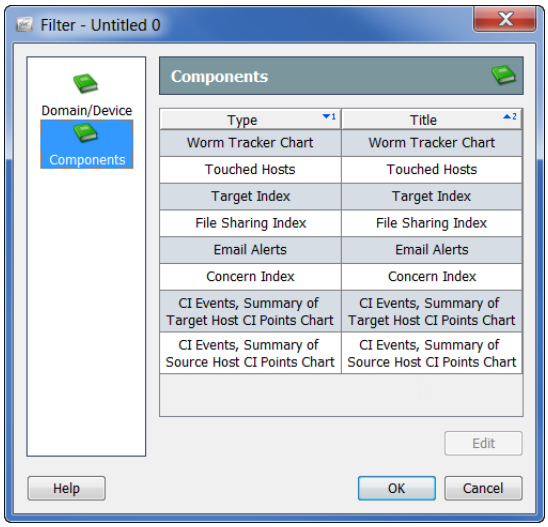
注意：

文件名是您的文档名称。例如，如果将文件名另存为 *1234*，则文档标题将为 *1234*。因此，务必要为您的文档提供一个有意义的文件名（例如*安全报告*）。

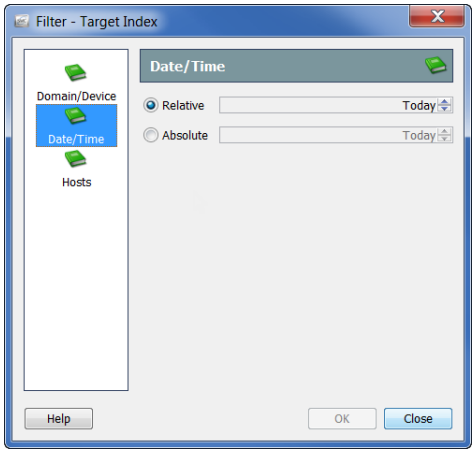
11. 启动文档，具体方法为：在 SMC 客户端界面，点击“文档生成器”对话框右上角的**转到文档**按钮 。系统随即会打开该文档的“过滤”对话框。如果未突出显示该对话框，请点击**域/设备**按钮。确保已选择您要过滤的域。



12. 点击**组件**按钮。系统随即会列出文档中包含的所有组件。

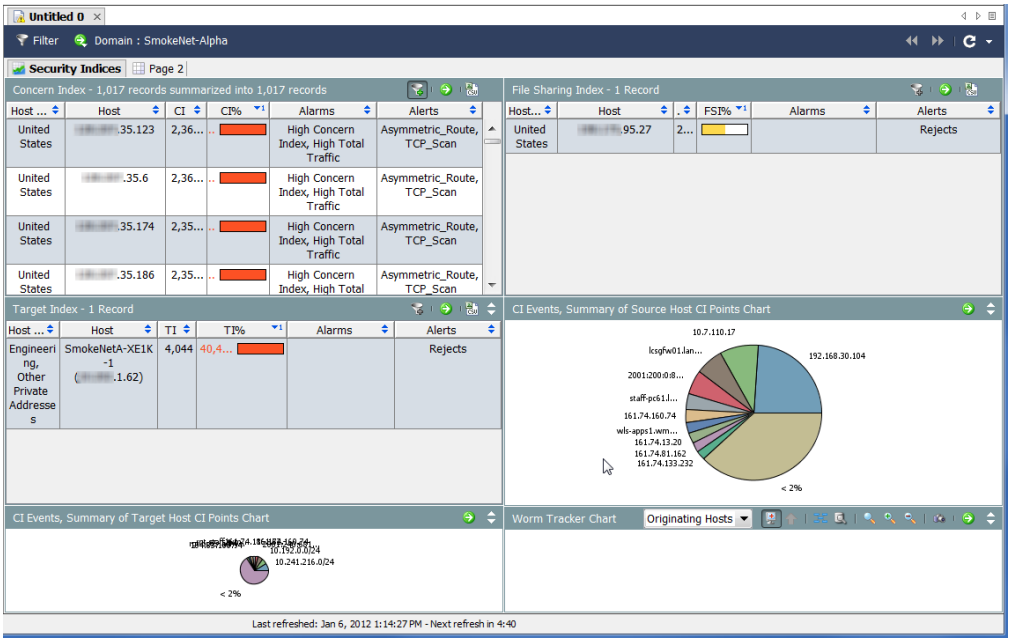


13. 点击要对其过滤的组件，然后点击**编辑**。系统随即会打开该组件的“过滤”对话框。（您可以使用的过滤选项取决于在对话框左侧点击的按钮）。



14. 完成选择后，点击**确定**。

15. 当您的新文档在 SMC GUI 中打开时，它看起来与以下示例类似。根据需要调整列和组件的大小。



16. 完成后，从 SMC 主菜单中依次选择**文件 > 另存为**将您的文档保存到 SMC 服务器，以便您可以随时在 SMC 中将其打开。

注意：

文件名是您的文档名称。例如，如果将文件名另存为 *1234*，则文档标题将为 *1234*。因此，务必为您的文档提供一个有意义的文件名（例如，*Security Reports*）。

17. 关闭“文档生成器”。

注意：

如有必要，您可以在文档生成器中打开以前保存的 XML 和 DAR 文件，对它们进行编辑。

6

指数：行为更改排名

概述

Stealthwatch 使用指数来帮助检测网络上的主机异常。使用专有启发法和算法为您的环境建立正常行为基准时，Stealthwatch 流量收集器会针对各种不可接受的主机行为将关注指数 (CI) 点添加到主机。当累积的指数点数超过可接受的阈值时，流量收集器会引发警报。

指数有助于表明行为的异常程度以及 Stealthwatch 对于该异常活动相关的自信程度。换言之，指数有助于确定调查的优先级。

例如，如果一个陌生人摇响您的前门门铃，然后说他找错了地址，您可能会认为自己没有理由报警。您的关注指数会相对较低。然而，如果该陌生人继续沿街在邻居门前做同样的事情，则他的行为会变得越来越可疑。

您的关注指数很可能会随着该陌生人每接近一扇门而上升一个点（或更多）。到他接近第三扇门时，您的关注程度就足以报警了。在这种情况下，您不担忧此行为的阈值就是两扇门。在第三扇门时，该阈值被超越，您就不得不对此采取一些措施。

Stealthwatch 指数的原理与保护网络的方式大体相同，仅在异常活动达到不可接受的水平时才会引发警报。基本上，这些指数示警的任何行为都意味着发生了重大行为变化。

例如，单个 TCP 重置不会引发警报，即便 Stealthwatch 对其分配了 CI 点。但是，根据系统中定义为可接受的水平，许多 TCP 重置就可能会引发警报。

Stealthwatch 使用以下指数来跟踪异常行为：

- 关注指数 (CI) - 跟踪其正在执行的活动可能会危及网络完整性的主机。
- 目标指数 (TI) - 跟踪似乎遭到其他主机可疑行为危害的主机。
- 文件共享指数 (FSI) - 跟踪表示点对点 (P2P) 活动的行为。

本章包含以下主题：

- 关注指数
- 目标指数
- 文件共享指数

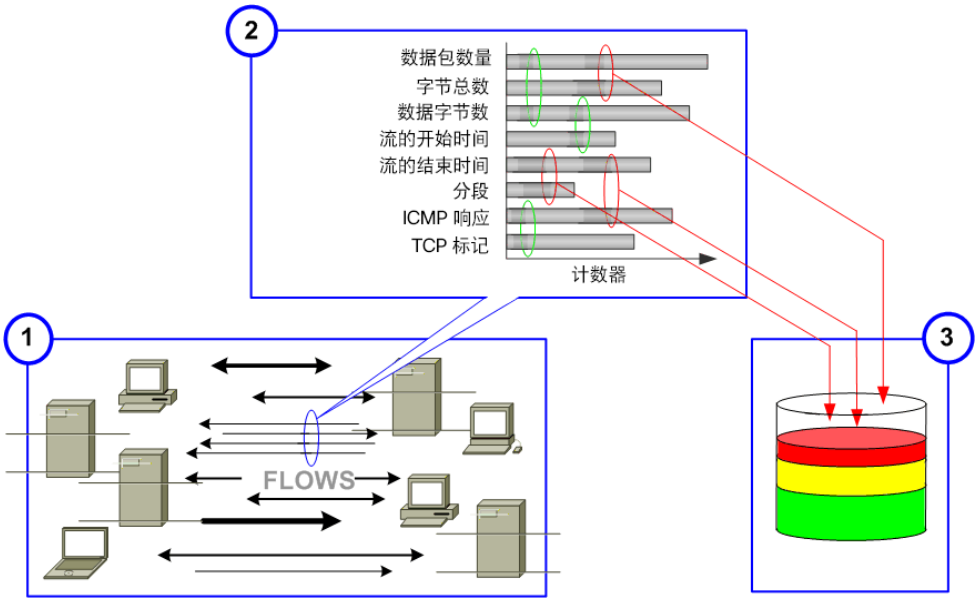
关注指数

关注指数 (CI) 是 Stealthwatch 通知您可疑流量活动的主要方式，例如在拒绝服务 (DoS) 或扫描活动期间发送数据包，旨在唤起网络主机的响应。Stealthwatch 会将这些情况标记为安全事件。

安全事件可能表示安全漏洞、错误配置的设备、发生故障的服务器或其他来源的网络问题。Stealthwatch 可跟踪与这些事件相关的信息，并增加该主机的 CI 点数。CI 越大，针对该行为的关注程度就越高。

当点数超过设置的阈值时，Stealthwatch 就会对活动来源的主机发起高 CI 警报。CI 值的范围为零点到成千上万点。

下图说明了增加 CI 涉及的三个基本阶段：



1. Stealthwatch 流量收集器可监视涉及主机的流量。
2. 流量收集器会将该活动与已配置为可接受行为的活动对比。
3. 流量收集器发现有些主机的活动不可接受，然后就会增加 CI。

内部主机出现高关注指数警报，通常表示该主机出现异常行为，应检查其是否面临潜在危害、误用或策略违规。

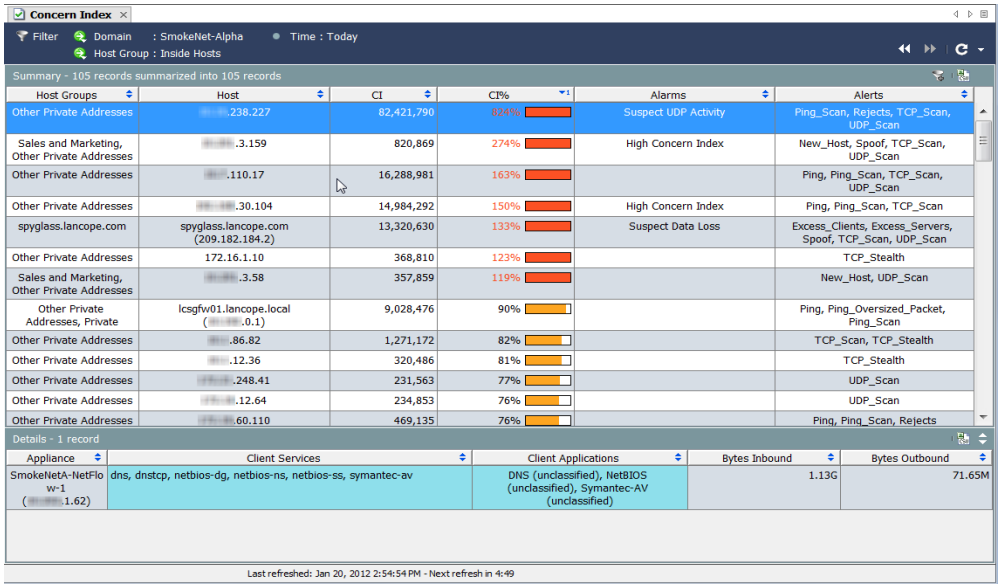
外部主机出现高关注指数警报，通常表示其正在执行“不良操作”以试图破坏网络完整性。在这两种情况下，关注指数文档都可帮助您识别哪些主机正在攻击您的网络以及哪些主机受到了攻击。

注意：

如果主机的活动超过其 CI 阈值，并且相关主机组的高关注指数警报被抑制，则流量收集器不会对该主机发出高关注指数警报。

Stealthwatch 流量收集器按用户定义的*存档时间*，每隔 24 小时清除一次所有指数计数。同时，流量收集器会保存其在之前 24 小时内收集的日志文件和 Web 文件，然后开始新一天的数据收集。

关注指数文档显示自上次存档后 CI 点数最高的主机的信息。



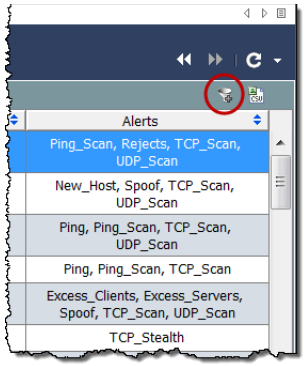
要显示关注指数文档，请右键点击域或主机组，然后依次选择**安全 > 关注指数**。

关注指数文档可帮助您确定威胁的优先级，使您关注真正重要的事件。Stealthwatch 可按严重性从高到低提供少量可行项目，让您不必再查看数以千计的每日警报。

注意：

警报是异常网络活动的信息摘要，但提示与警报不同，提示不会作为通知发送。

默认情况下，“关注指数过滤器”按钮（位于文档的右上角）处于激活状态，并且关注指数仅显示包含活动关注指数警报的主机（即 CI 百分比高于 100% 的主机）。要查看 CI 百分比高于 50% 的主机，请点击**关注指数过滤器**按钮。“关注指数过滤器”按钮上的加号将变为灰色，并显示 CI 百分比高于 50% 的主机，无论其是否存在活动的高关注指数警报。



注意：

系统将在存档时清除主机的累计 CI。

请注意，关注指数的顶部有一个“摘要”部分，底部有一个“详细信息”部分。选择“摘要”部分的某行，可在“详细信息”部分查看该行的更多相关信息。

在前面的示例中，威胁级别最高的主机为 xxx.xxx.238.227。对于此例，我们假定它是内部主机。我们可以轻松查看有关此主机的以下信息：

- 自上次存档后，此主机累计的 CI 百分比约为 824%。
- 此主机还引发了两个提示：Ping_Scan、拒绝、TCP_Scan 和 UDP_Scan。
- 已收到 1.13G 数据。
- 已发送 71.65M 数据。

结合 CI 百分比、警报、提示和数据传输，这看起来像是一个潜在的安全漏洞。应检查此主机是否面临潜在危害、误用或策略违规的情况。

双击该主机的 IP 地址，可打开作为安全事件源的主机的主机快照。

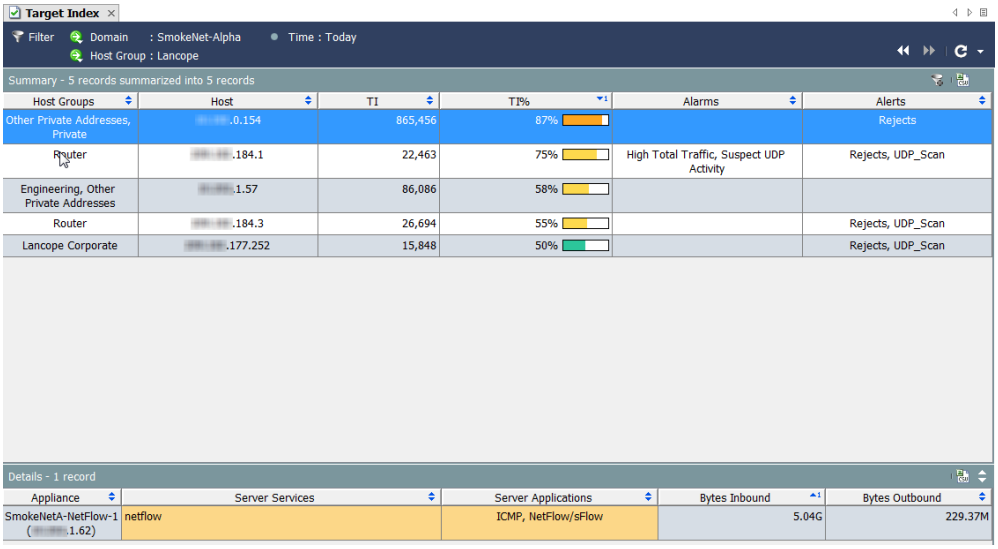
注意：

有关在关注指数文档中可查看的各列的说明，请参阅 *SMC 客户端联机帮助*。

目标指数

目标指数 (TI) 显示自 Stealthwatch 流量收集器上次存档后具有最高目标指数的（请求的数据集内）主机。当目标 IP 地址***收到***多个安全事件或其他恶意攻击并超过阈值时，Stealthwatch 流量收集器会触发高目标指数警报。目标指数的目的是提醒您许多主机可能针对单个内部主机发起了分布式攻击。

当您确定受到危害的主机及相关的服务和端口后，您可以根据您的设备和软件，在防火墙或者主机本身上阻止禁止的端口。此外，您还可以断开主机的网络，并对其进行清理。

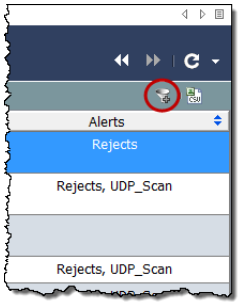


要显示目标指数，请右键点击域或主机组，然后依次选择**安全 > 目标指数**。

目标指数值的范围为零点到成千上万点。随着每个主机的目标指数点不断累积，可能会产生 TI 警报。默认情况下，数据按 TI 百分比以降序排列。此数据表示自上次存档后在域中观察到的最大数据值。例如，TI 为 158% 的主机超过了自身 TI 阈值的 58%，应对其进行更多调查。此百分比后面跟着一个图，在接近 TI 阈值时，此图会改变颜色，如下表中所示：

已配置阈值的百分比	文本颜色
占已配置阈值的 0%	空图形
占已配置阈值的 0% 到 50%	绿色
占已配置阈值的 51% 到 75%	黄色
占已配置阈值的 76% 到 99%	橙色
占已配置阈值的 100% 或以上	红色

默认情况下，“目标指数过滤器”按钮（位于文档的右上角）处于激活状态，并且目标指数仅显示包含活动目标指数警报的主机（即 TI 百分比高于 100% 的主机）。要查看 TI 百分比高于 50% 的主机，请点击**目标指数过滤器**按钮。目标指数过滤按钮上的加号会变为灰色，并显示 TI 百分比高于 50% 的主机。

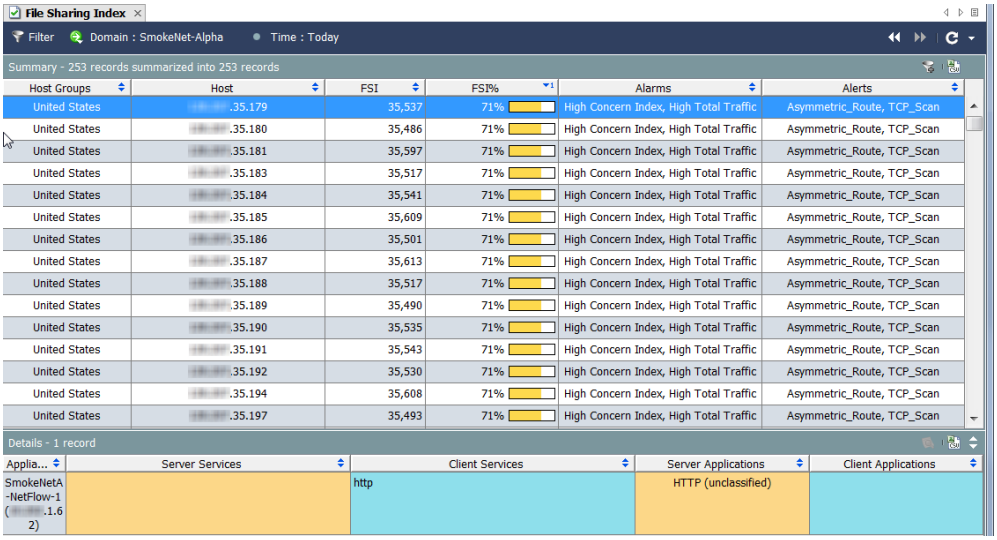


文件共享指数

文件共享指数 (FSI) 旨在检测共享文件的可疑应用，尤其是将组织置于风险之中的点对点 (P2P) 通信。传输敏感信息，或由于与网络内外其他人共享受版权保护的材料而滥用组织网络，会导致出现这一情况。

Stealthwatch 流量收集器收集有关网络中所有主机进行的连接的各种信息。通过关联某些统计信息，可得出文件共享指数，进而识别可能参与表示 P2P 活动的文件传输的主机。

使用关联技术，指数会通过添加点数来显示最活跃的主机和/或往返最常与文件共享活动关联的传感器组合的主机。此技术与确定 Stealthwatch 流量收集器用于表示扫描活动的关注指数值的技术类似。文件共享指数文档为您提供需优先调查的主机列表以及可选主机级别警报。



要显示文件共享指数，请右键点击域或主机组，然后依次选择**安全 > 文件共享指数**。

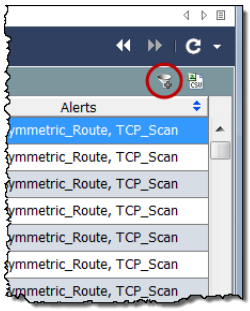
文件共享指数值的范围为零点到成千上万点不等。随着每个主机的文件共享指数点不断累积，可能会产生文件共享指数警报。默认情况下，数据按 FSI 百分比以降序排列。此数据表示自上次存档后在域中观察到的最大数据值。例如，FSI 百分比为 158% 的主机超过了自身 FSI 阈值的 58%，应对其进行更多调查。

此百分比后面跟着一个图，在接近 FSI 阈值时，此图会改变颜色，如下表中所示。

已配置阈值的百分比	文本颜色
占已配置阈值的 0%	空图形
占已配置阈值的 0% 到 50%	绿色

已配置阈值的百分比	文本颜色
占已配置阈值的 51% 到 75%	黄色
占已配置阈值的 76% 到 99%	橙色
占已配置阈值的 100% 或以上	红色

默认情况下，“文件共享指数过滤器”按钮（位于文档的右上角）处于激活状态，并且文件共享指数仅显示包含活动文件共享指数警报的主机（即 FSI 百分比高于 100% 的主机）。要查看 FSI 百分比高于 50% 的主机，请点击**文件共享指数过滤器**按钮。“文件共享指数过滤器”按钮上的加号会变为灰色，并显示 FSI 百分比高于 50% 的主机。



7

监控流量和网络性能

概述

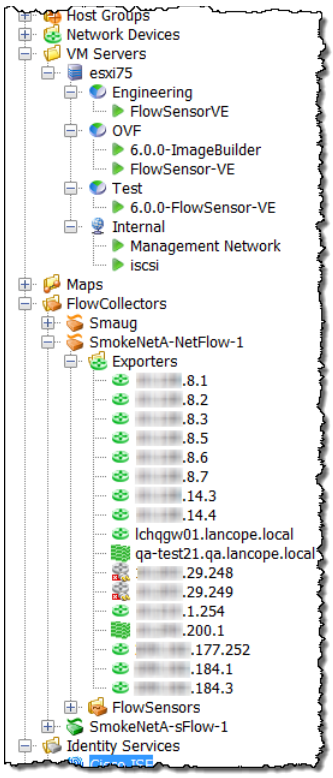
Stealthwatch 通过网络行为分析监控您的网络，并在发生可能会引发潜在问题的更改时通知您。系统会持续监视网络上的每台主机并记录行为，例如主机较为活跃和不太活跃的时间、主机之间正在传输的数据量以及涉及的流量类型。

本章介绍如何访问表示网络上流量的图形和表格数据，以便您了解主机和网络行为的变化。这样，如果确实存在任何潜在威胁，您就可以在它们对网络造成危害之前解决它们。

本章包含以下主题：

- 监控流量
- 导出器/网络设备
- 虚拟机

监控流量



企业树位于 SMC 图形用户界面左侧的框架内。此框架采用树菜单结构，使您能快速而轻松地查看系统状态和请求文档。

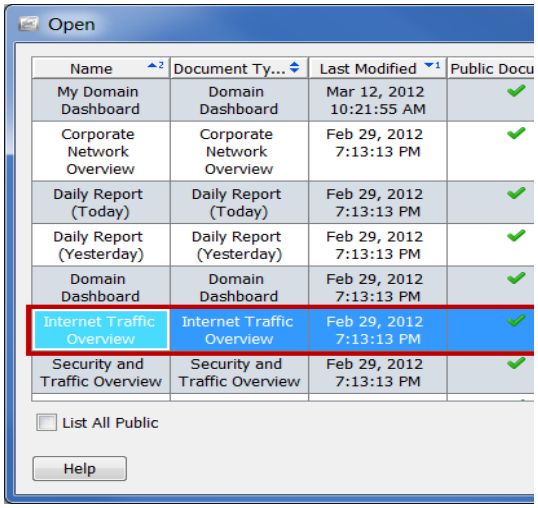
监控流量时主要有两个关注领域：

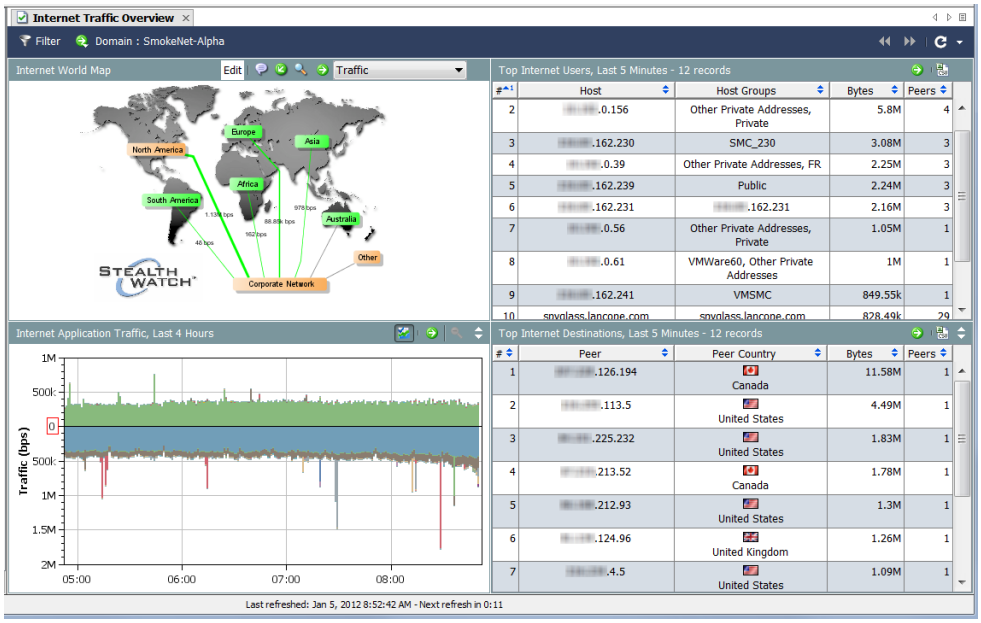
- 导出器 - 配置为向 Stealthwatch 流量收集器发送数据的路由器或交换机。
- 虚拟机 - 由 Stealthwatch FlowSensor 监控的虚拟机。

左侧示例显示了在企业树的何处可找到导出器和虚拟机。

Internet 流量概述

“互联网流量概述”提供与互联网相关的域流量的图形和表格数据。要显示此文档，请从主菜单中依次选择**文件 > 打开**。系统随即会打开以下对话框。选择“互联网流量概述”文档，然后点击**确定**。





查看互联网世界地图时，问自己以下问题：

- 是否有任何主机组或主机组关系显示严重或重要警报？颜色和标注可帮助您作出此项决定。

  如果是，右键点击报警主机组或主机组关系，然后选择**警报表**可获取更多信息。

- 点击文档标题中的下拉列表箭头，可更改显示的数据类型。是否有任何主机组关系显示异常数量的数据？线条的粗细和线条的状态文本可帮助您作出此项决定。

  如果是，右键点击主机组关系，然后选择**主机组关系控制面板**可获取更多信息。

查看互联网应用流量时，问自己以下问题：

- 该图是否显示您的组织中正在使用的应用的峰值异常？

提示：

您可以点击**隐藏其他**按钮  隐藏不在使用量排名靠前的应用的流量。此按钮可在数据的隐藏或显示之间切换。

- 该图是否显示您的组织中通常不使用的应用的大量流量？
- 该图是否显示未定义或其他应用的大量流量？

  如果是，则应配置更多应用定义。

查看排名靠前的互联网用户时，问自己以下问题：

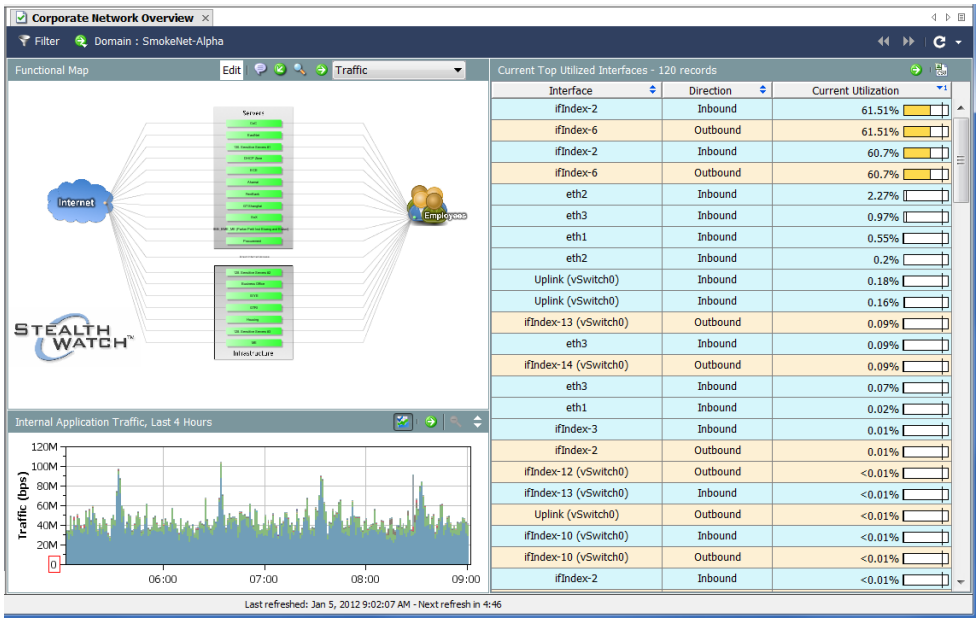
- 该表是否显示不应位于组织中排名靠前的互联网用户的主机的大量流量？
- 该表是否显示您的组织中用作服务器并发送大量流量的主机？
- 该表是否显示您的组织中与大量对等体之间发送/接收流量的主机？

查看排名靠前的互联网目标时，问自己以下问题：

- 该表是否显示不应与您的组织通信的对等体的大量流量？
- 该表是否显示用作客户端并从您组织中的主机接收大量流量的对等体？
- 该表是否显示与您组织中的大量主机之间发送/接收流量的对等体？

公司网络概述

“公司网络概述”提供与整个公司网络相关的域流量的图形和表格数据。要显示此文档，请从主菜单中依次选择**文件 > 打开**。系统随即会打开“打开”对话框。选择“公司网络概述”文档，然后点击**确定**。



查看功能映射时，问自己以下问题：

- 是否有任何主机组或主机组关系显示严重或重要警报？颜色和标注可帮助您作出此项决定。

  如果是，右键点击报警主机组或主机组关系，然后选择**警报表**可获取更多信息。

- 点击文档标题下拉列表中的箭头，可更改显示的数据类型。是否有任何主机组关系显示异常数量的数据？线条的粗细和线条的状态文本可帮助您作出此项决定。

  如果是，右键点击主机组关系，然后选择**主机组控制面板**可获取更多信息。

查看内部应用流量时，问自己以下问题：

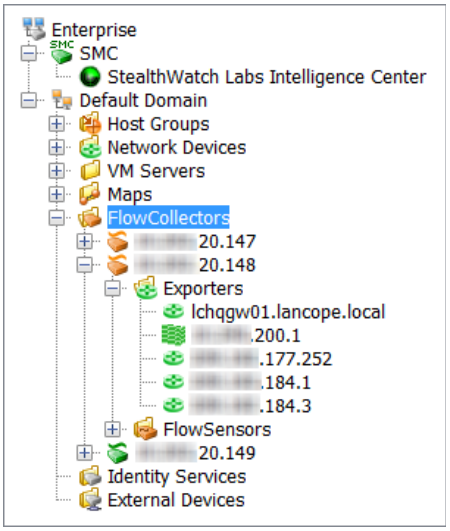
- 该图是否显示您的组织中使用的应用的峰值异常？
- 该图是否显示您的组织中通常不使用的应用的大量流量？
- 该图是否显示未定义或其他应用的大量流量？如果是，则应配置更多应用定义。

查看当前利用率排名靠前的接口时，问自己以下问题：

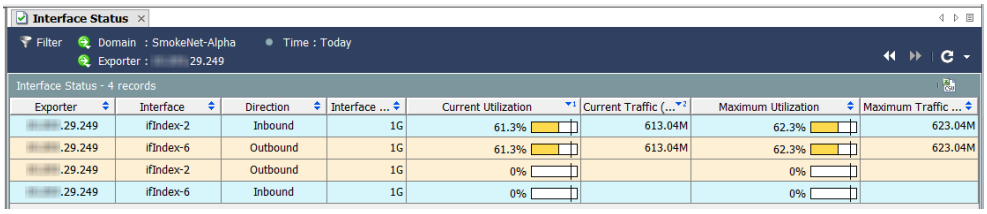
- 该表是否显示任何饱和的接口（即表示利用率百分比异常之高）？
- 该表是否显示任何不应包括在靠前用户中的接口？

导出器/网络设备

导出器位于接收其数据的 Stealthwatch 流量收集器下面的树中，如右侧示例所示。



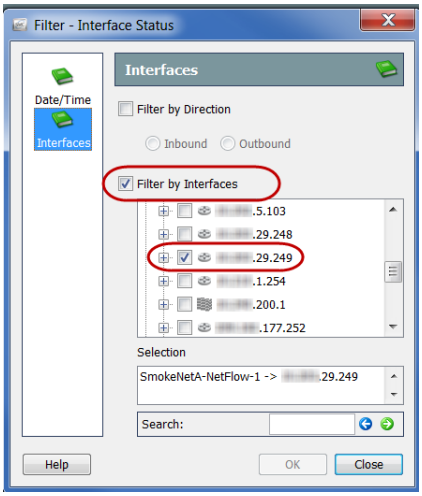
要直接导航到导出器的文档，请展开企业树中相应主机下的“网络设备”选项，然后双击导出器。系统随即会打开“接口状态”文档。本文档显示路由器或交换机上正在向面向 sFlow 的 Stealthwatch 流量收集器或面向 NetFlow 的 Stealthwatch 流量收集器发送数据的接口（即导出器）的统计信息。



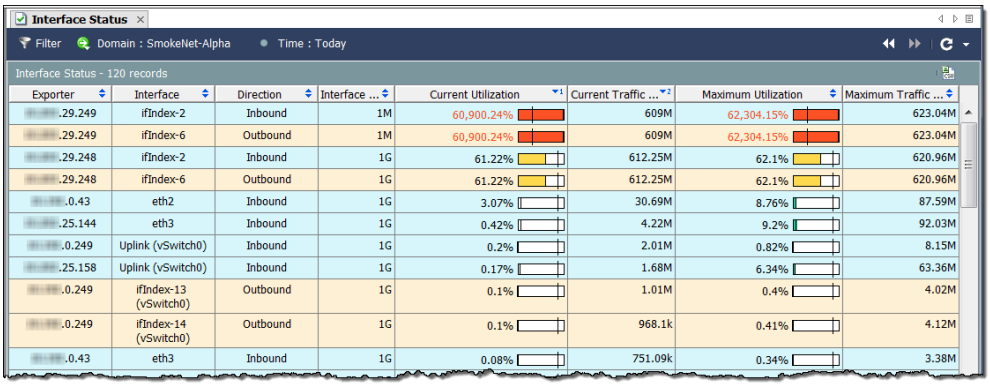
注意：

“接口状态”文档不适用于思科 ASA 导出器类型。

点击“接口状态”文档左上角的**过滤器**按钮 。在打开的“过滤器 - 接口状态”对话框中，点击**接口**按钮（如果该按钮尚未突出显示）。

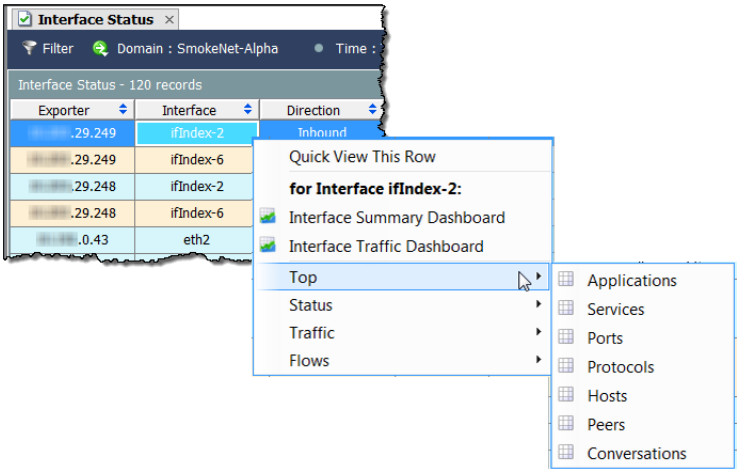


点击**按接口过滤**复选框可删除选中标记。接下来，查找当前对该文档进行过滤所依据的导出器（唯一带有复选标记的选项）。点击此导出器的复选框以删除复选标记，然后点击**确定**。现在，“接口状态”文档显示整个域的流量统计信息，如以下示例中所示。

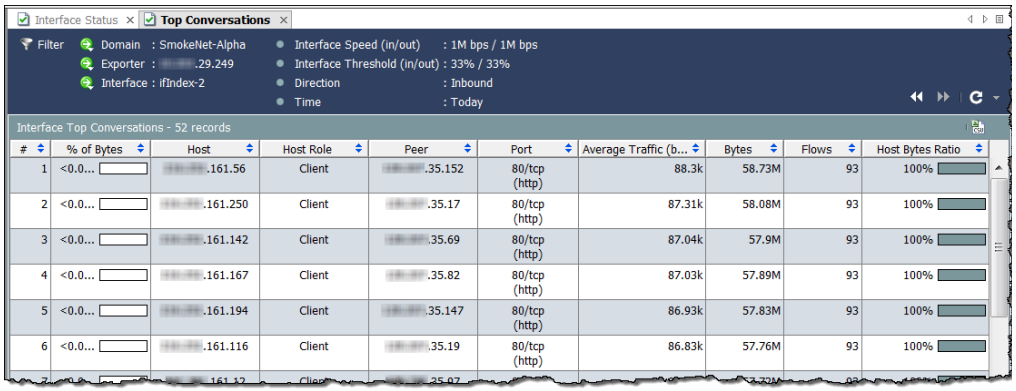


Exporter	Interface	Direction	Interface ...	Current Utilization	Current Traffic ...	Maximum Utilization	Maximum Traffic ...
.29.249	ifIndex-2	Inbound	1M	60,900.24%	609M	62,304.15%	623.04M
.29.249	ifIndex-6	Outbound	1M	60,900.24%	609M	62,304.15%	623.04M
.29.248	ifIndex-2	Inbound	1G	61.22%	612.25M	62.1%	620.96M
.29.248	ifIndex-6	Outbound	1G	61.22%	612.25M	62.1%	620.96M
.0.43	eth2	Inbound	1G	3.07%	30.69M	8.76%	87.59M
.25.144	eth3	Inbound	1G	0.42%	4.22M	9.2%	92.03M
.0.249	Uplink (vSwitch0)	Inbound	1G	0.2%	2.01M	0.82%	8.15M
.25.158	Uplink (vSwitch0)	Inbound	1G	0.17%	1.68M	6.34%	63.36M
.0.249	ifIndex-13 (vSwitch0)	Outbound	1G	0.1%	1.01M	0.4%	4.02M
.0.249	ifIndex-14 (vSwitch0)	Outbound	1G	0.1%	968.1k	0.41%	4.12M
.0.43	eth3	Inbound	1G	0.08%	751.09k	0.34%	3.38M

右键点击“接口”列中的接口，然后选择**靠前**。此时会弹出一个菜单，从中可以选择多个选项。



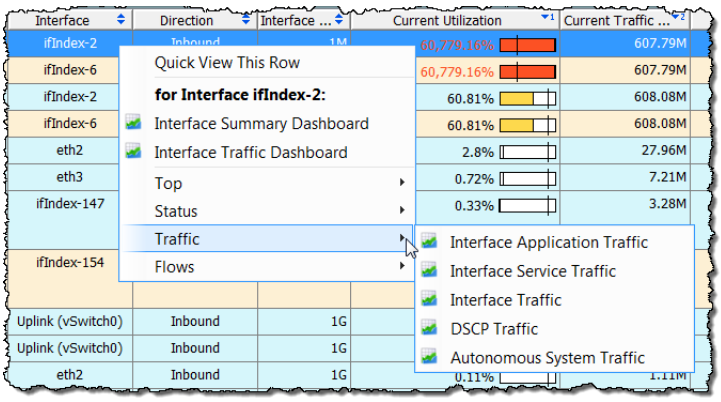
例如，如果选择**靠前 > 对话**，则显示“排名靠前的对话”文档，如以下示例所示。“排名靠前的对话”文档根据排名靠前的对话列示流数据。方向（可在过滤器中更改）表示该数据包含所有流量（即总数）、流向所选项的流量、从所选项流出的流量还是所选项内的流量。



提示：

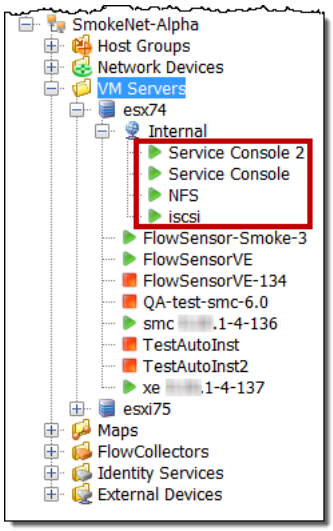
双击某个接口可打开“摘要报告”。

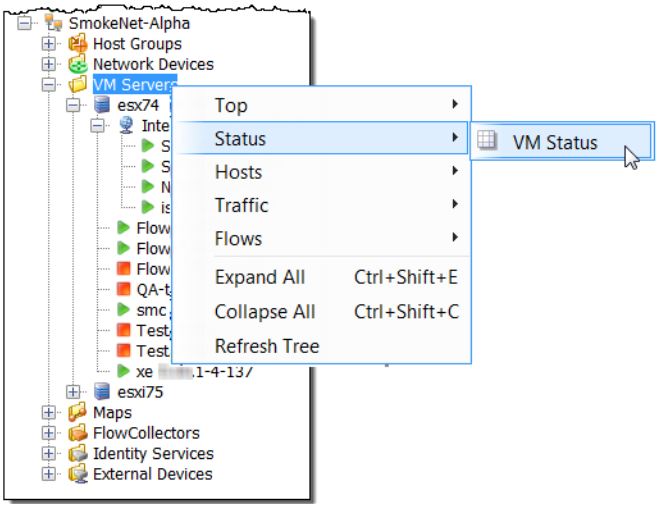
在一个列内点击鼠标右键，然后从第一个弹出菜单中选择**流量**，可以找到许多有助于监控流量的其他文档。



虚拟机

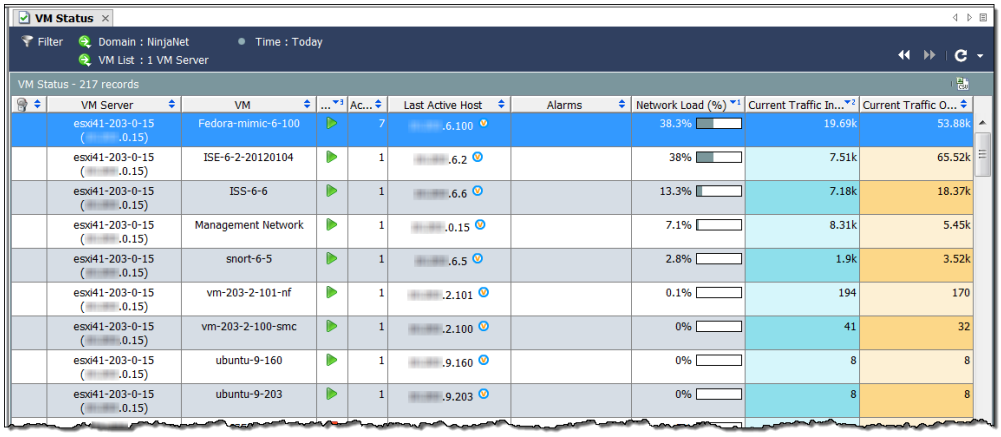
虚拟机位于其关联的虚拟机服务器（和资源组 [如果存在]）下面的企业树中，如右侧示例所示。





我们来看特定虚拟机服务器上的虚拟机状态。要执行此操作，请右键点击该虚拟机服务器，然后依次选择**状态 > 虚拟机状态**。

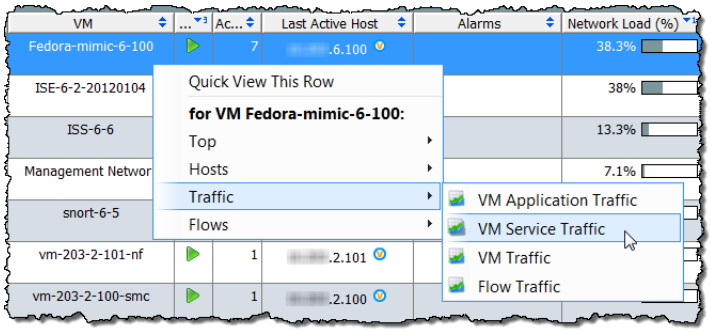
系统随即会打开“虚拟机状态”文档。此文档显示了有关同一虚拟机服务器上存在的虚拟机的有用统计信息。

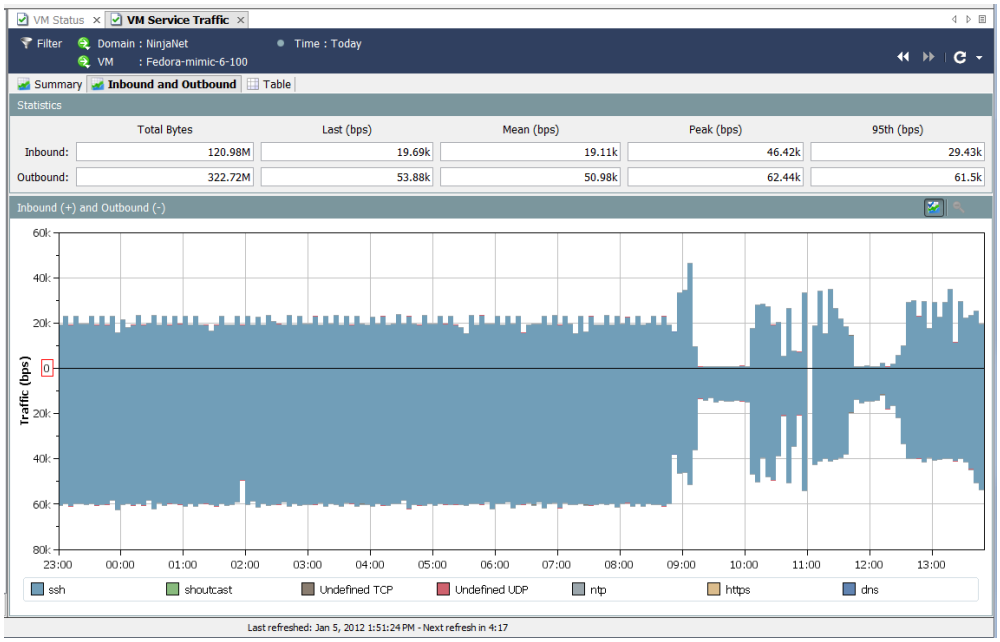


注意：

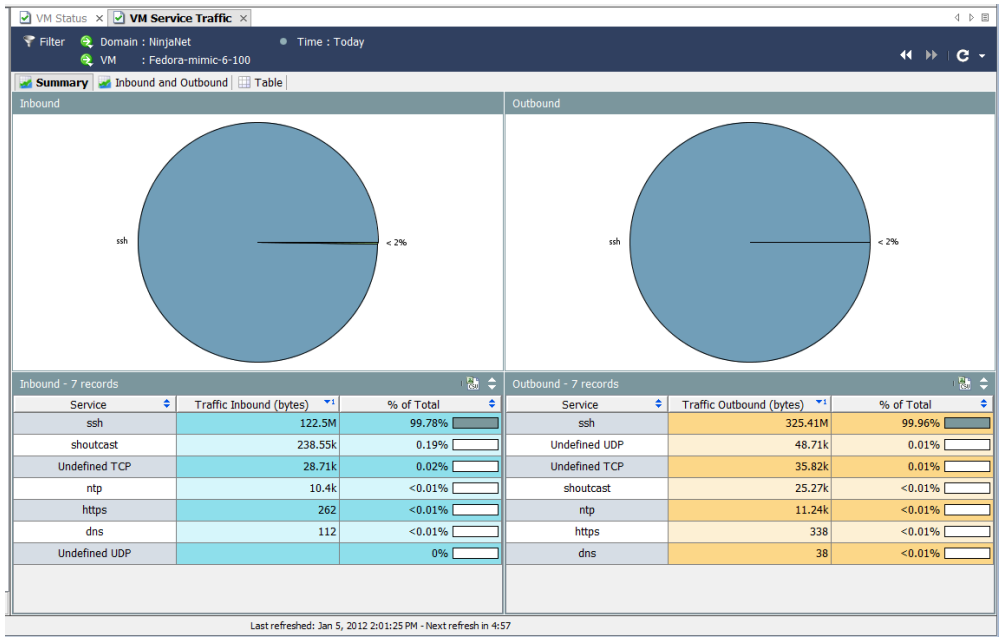
使用此文档可了解有关系统中最繁忙虚拟机的详细信息。例如，右键点击某个虚拟机可查看专门为该虚拟机过滤的其他有用文档。

右键点击某个虚拟机，然后依次选择**流量 > 虚拟机服务流量**。系统随即会打开“虚拟机服务流量”文档，如以下示例中所示。此文档根据使用的前十项服务显示所选虚拟机发送和接收的流量数据。

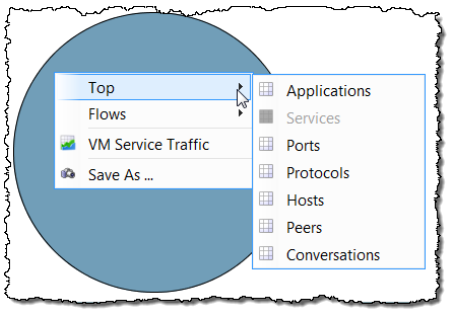




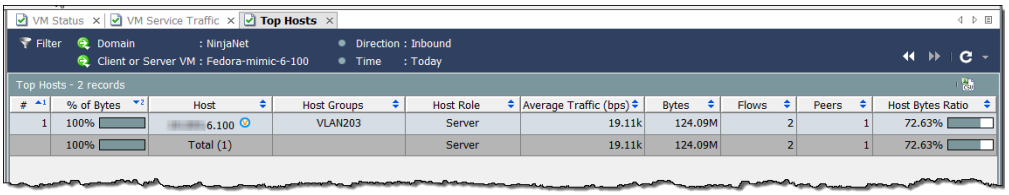
点击**摘要**选项卡，可查看饼图中汇总的数据。



在“虚拟机服务流量”文档中，您可以进一步了解更多信息。例如，如果看到特定服务的流量过多，可以右键点击该图表或表中的项目，然后选择**靠前**。系统随即会弹出一个菜单，从中可以选择多个选项。

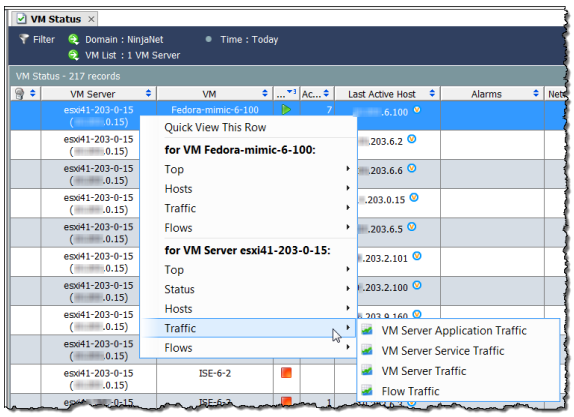


例如，如果依次选择**靠前 > 主机**，系统将显示“排名靠前的主机”文档。



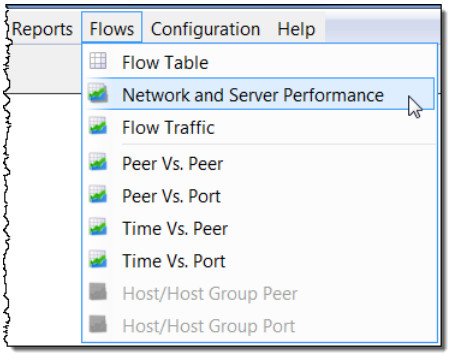
“排名靠前的主机”文档根据排名靠前的主机列出流量数据。方向（可在过滤器中更改）表示该数据包含所有流量（即总数）、流向所选项的流量、从所选项流出的流量还是所选项内的流量。

右键点击列内，然后从第一个弹出菜单中选择**流量**，可以找到许多有助于监控流量的其他文档。



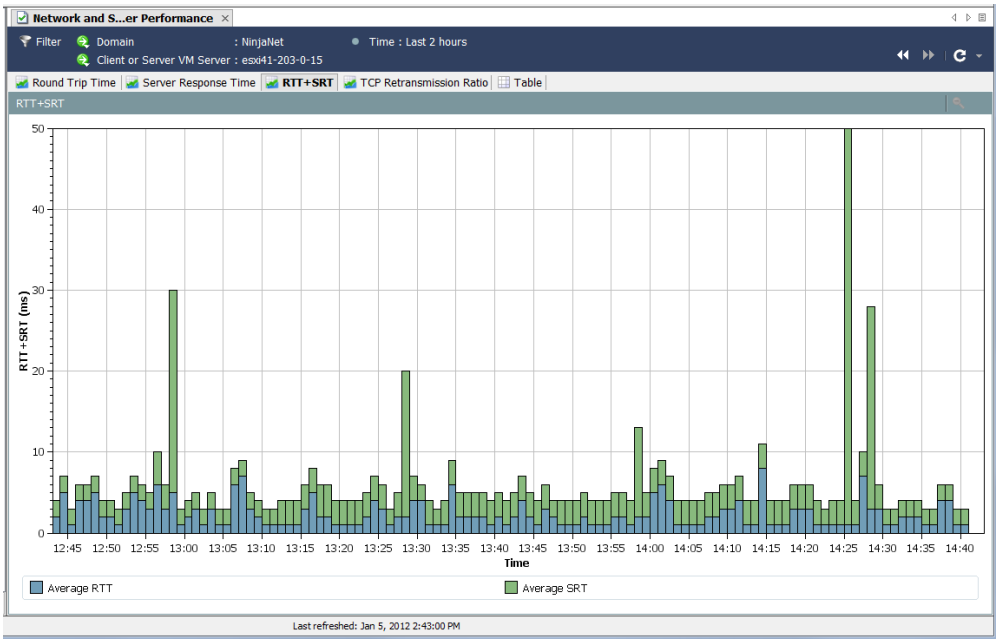
网络性能

假设您有一名员工正在抱怨“网速慢”。您可以使用“网络和服务器性能”文档来调查这些类型的问题。要访问此文档，请从主菜单中依次选择**流量 > 网络和服务器性能**。



注意：

此报告需要 Stealthwatch FlowSensor 收集特定的值来填充此报告。

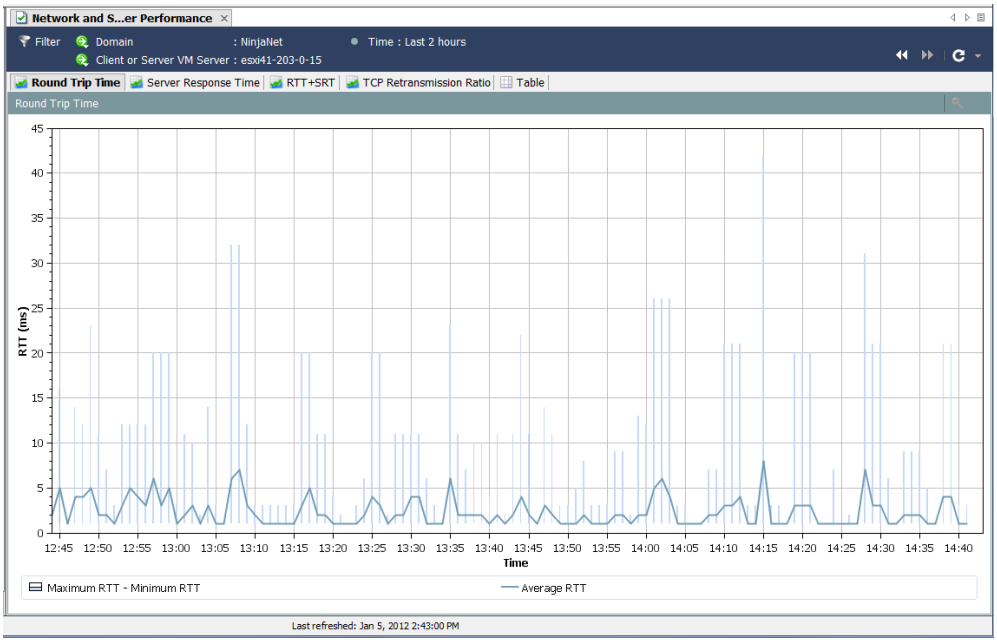


“网络和服务器性能”文档显示数据库中存储的流量的各种性能数据。访问该文档顶部的以下选项卡可查看这些数据：

- 往返时间
- 服务器响应时间
- RTT+SRT
- TCP 重新传输率
- 表

往返时间

“往返时间”选项卡以图形方式显示数据流的往返时间统计信息。

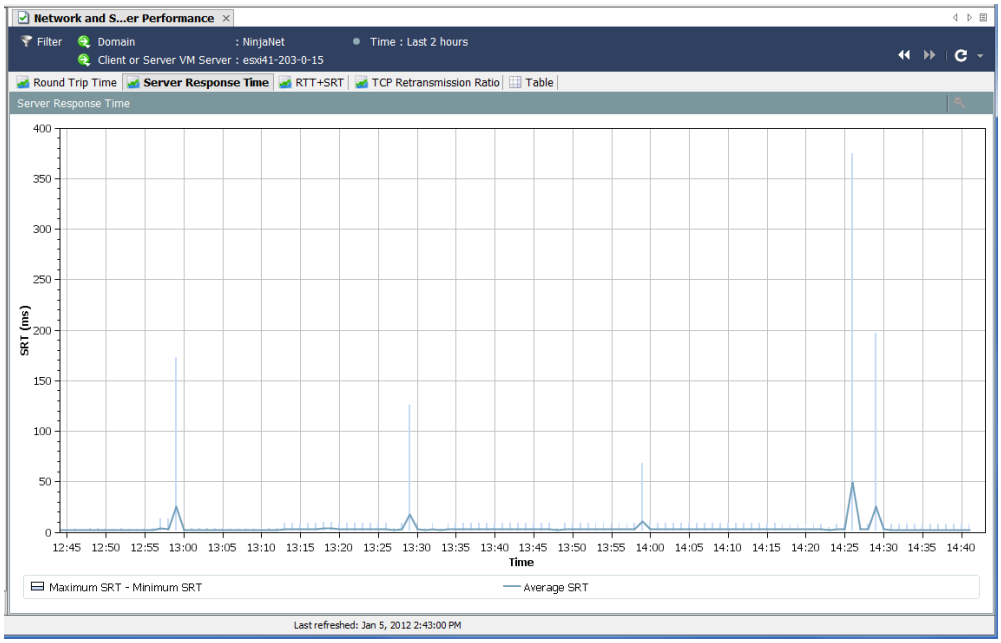


此功能有助于衡量数据流在相距较远的主机组之间完成传输所需的时间。您可以使用“过滤器”上的“主机”页面来设置此项。

图底部的深色线表示计算的平均 RTT，而又长又细的线表示计算的每分钟最小和最大 RTT 之间的分布情况。

服务器响应时间

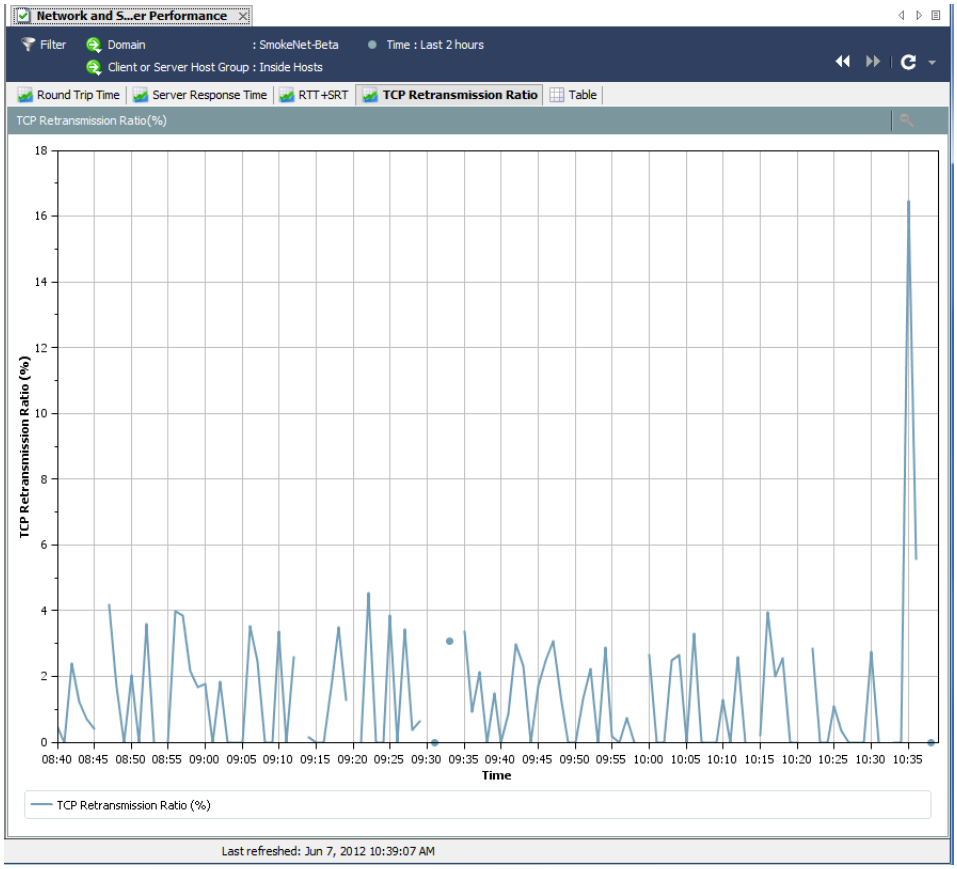
“服务器响应时间”选项卡以图形方式显示数据流的服务器响应时间 (SRT) 统计信息。



此功能有助于衡量服务器响应请求所需的时间。例如，用户抱怨他们基于 Web 的应用性能较差，因为屏幕“永远在填充”。通过此文档，您可以监控服务器的 SRT，并将平均 SRT 与服务器中用户自己的 SRT 进行比较。

TCP 重新传输率

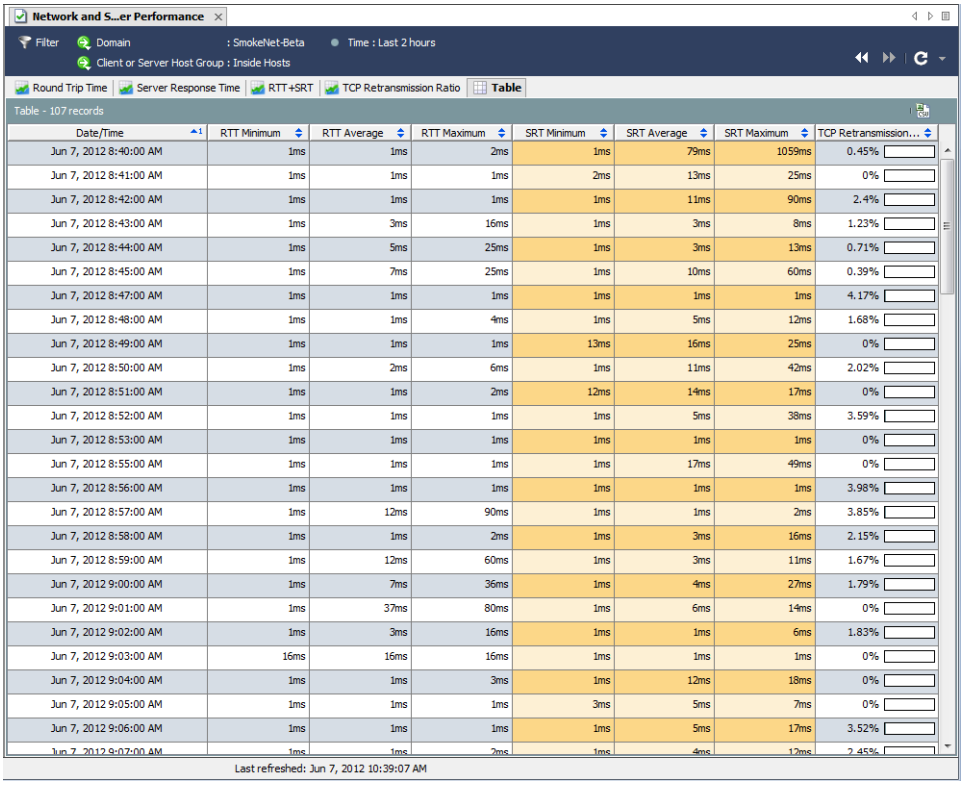
“ 网络和服务器性能 ” 文档的 “TCP 重新传输率 ” 选项卡以图形方式显示已重新传输的数据包的百分比。默认情况下，这些数据涵盖 2 小时的时间段，数据记录之间的时间间隔为 1 分钟。由于数据包损坏或丢失，通常会发生重新传输。



注意：
此文档仅对从 Stealthwatch FlowSensor 接收数据的面向 NetFlow 的 Stealthwatch 流量收集器可用。

表

“网络和服务器性能”文档的“表”选项卡列示数据流的性能数据。默认情况下，这些数据涵盖 2 小时的时间段，数据记录之间的时间间隔为 1 分钟。



Date/Time	RTT Minimum	RTT Average	RTT Maximum	SRT Minimum	SRT Average	SRT Maximum	TCP Retransmission...
Jun 7, 2012 8:40:00 AM	1ms	1ms	2ms	1ms	79ms	1059ms	0.45%
Jun 7, 2012 8:41:00 AM	1ms	1ms	1ms	2ms	13ms	25ms	0%
Jun 7, 2012 8:42:00 AM	1ms	1ms	1ms	1ms	11ms	90ms	2.4%
Jun 7, 2012 8:43:00 AM	1ms	3ms	16ms	1ms	3ms	8ms	1.23%
Jun 7, 2012 8:44:00 AM	1ms	5ms	25ms	1ms	3ms	13ms	0.71%
Jun 7, 2012 8:45:00 AM	1ms	7ms	25ms	1ms	10ms	60ms	0.39%
Jun 7, 2012 8:47:00 AM	1ms	1ms	1ms	1ms	1ms	1ms	4.17%
Jun 7, 2012 8:48:00 AM	1ms	1ms	4ms	1ms	5ms	12ms	1.68%
Jun 7, 2012 8:49:00 AM	1ms	1ms	1ms	13ms	16ms	25ms	0%
Jun 7, 2012 8:50:00 AM	1ms	2ms	6ms	1ms	11ms	42ms	2.02%
Jun 7, 2012 8:51:00 AM	1ms	1ms	2ms	12ms	14ms	17ms	0%
Jun 7, 2012 8:52:00 AM	1ms	1ms	1ms	1ms	5ms	38ms	3.59%
Jun 7, 2012 8:53:00 AM	1ms	1ms	1ms	1ms	1ms	1ms	0%
Jun 7, 2012 8:55:00 AM	1ms	1ms	1ms	1ms	17ms	49ms	0%
Jun 7, 2012 8:56:00 AM	1ms	1ms	1ms	1ms	1ms	1ms	3.98%
Jun 7, 2012 8:57:00 AM	1ms	12ms	90ms	1ms	1ms	2ms	3.85%
Jun 7, 2012 8:58:00 AM	1ms	1ms	2ms	1ms	3ms	16ms	2.15%
Jun 7, 2012 8:59:00 AM	1ms	12ms	60ms	1ms	3ms	11ms	1.67%
Jun 7, 2012 9:00:00 AM	1ms	7ms	36ms	1ms	4ms	27ms	1.79%
Jun 7, 2012 9:01:00 AM	1ms	37ms	80ms	1ms	6ms	14ms	0%
Jun 7, 2012 9:02:00 AM	1ms	3ms	16ms	1ms	1ms	6ms	1.83%
Jun 7, 2012 9:03:00 AM	16ms	16ms	16ms	1ms	1ms	1ms	0%
Jun 7, 2012 9:04:00 AM	1ms	1ms	3ms	1ms	12ms	18ms	0%
Jun 7, 2012 9:05:00 AM	1ms	1ms	1ms	3ms	5ms	7ms	0%
Jun 7, 2012 9:06:00 AM	1ms	1ms	1ms	1ms	5ms	17ms	3.52%
Jun 7, 2012 9:07:00 AM	1ms	1ms	2ms	1ms	4ms	12ms	2.45%

注意：

此文档仅对从 Stealthwatch FlowSensor 接收数据的面向 NetFlow 的 Stealthwatch 流量收集器可用。

8

分析流

概述

您已确定特定主机受到入侵。您想要“撤回”与该主机之间的对话，以便识别涉嫌导致入侵的主机。或者，您发现了流量高峰并希望分析这些数据，进而确定该高峰出现的原因。或者，系统触发了警报，您需要确定该警报是否会威胁您的网络。

流分析过程可让您确定这些情况，从而保护网络安全。本章概述流分析过程，然后介绍该过程最常用的若干场景。

本章包含以下主题：

- 流量过滤器
- 流表选项卡
- 快速视图
- 流分析场景
- 外部查找

流量过滤器

通过“流量过滤器”对话框，可选择要查看的流数据并设置不同的过滤级别来接收所需的结果。

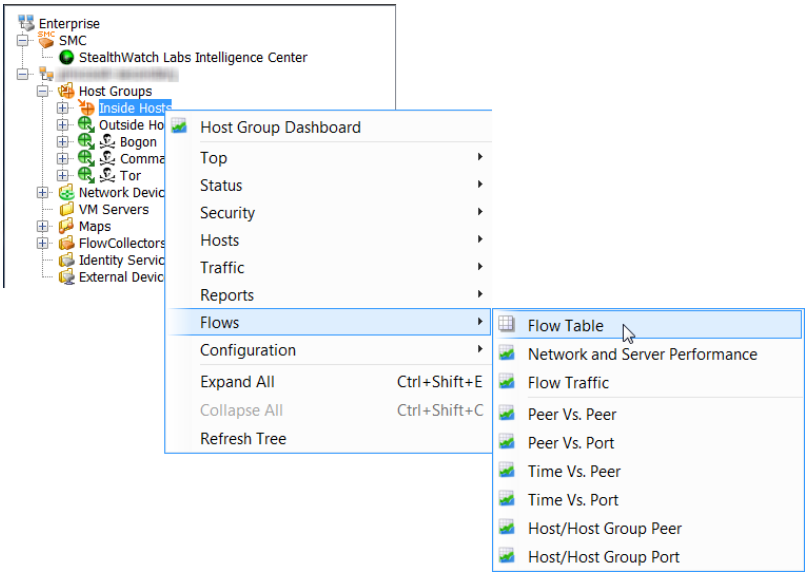
输入流查询

要查询流数据，请完成以下步骤：

注意：

无需使用以下步骤中所述的所有设置。

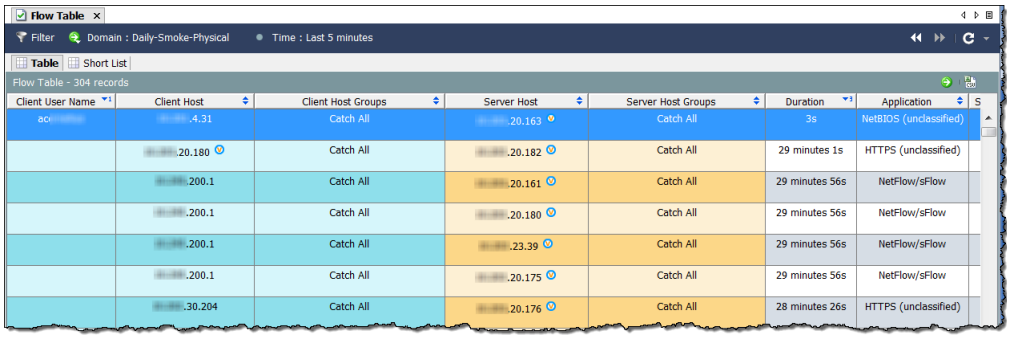
1. 右键点击域、设备、主机组或主机 IP 地址，然后依次选择**流 > 流表**。



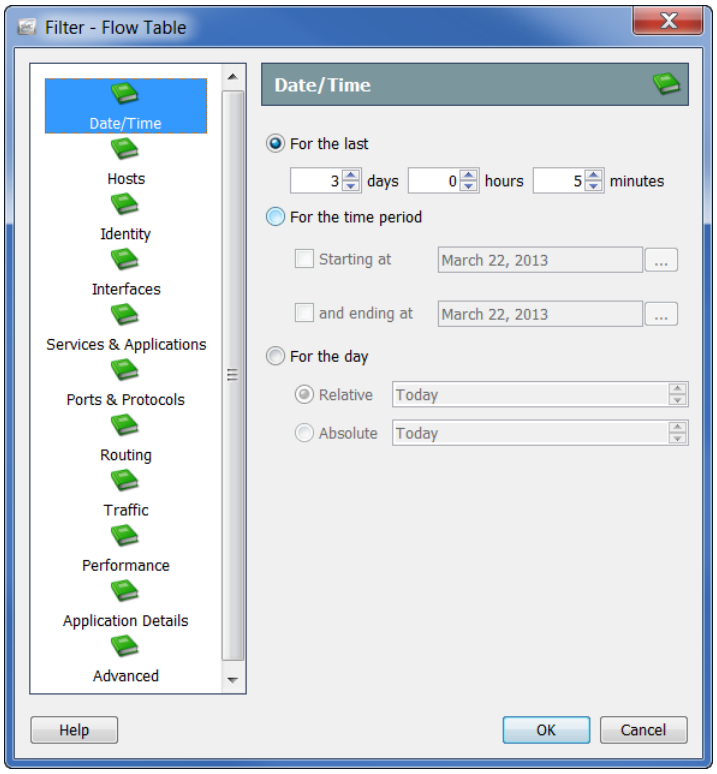
提示：

如果在点击弹出菜单中的**流表**时按下键盘上的 **Ctrl** 键，则首先显示过滤器，使您能够细化搜索条件。点击**确定**后，系统将按照您输入的搜索条件显示流表。

系统随即会打开“流表”。



2. 点击流表左上角的**过滤器**按钮，然后点击**日期/时间**图标（如果尚未突出显示）。系统会打开“日期/时间”页面。

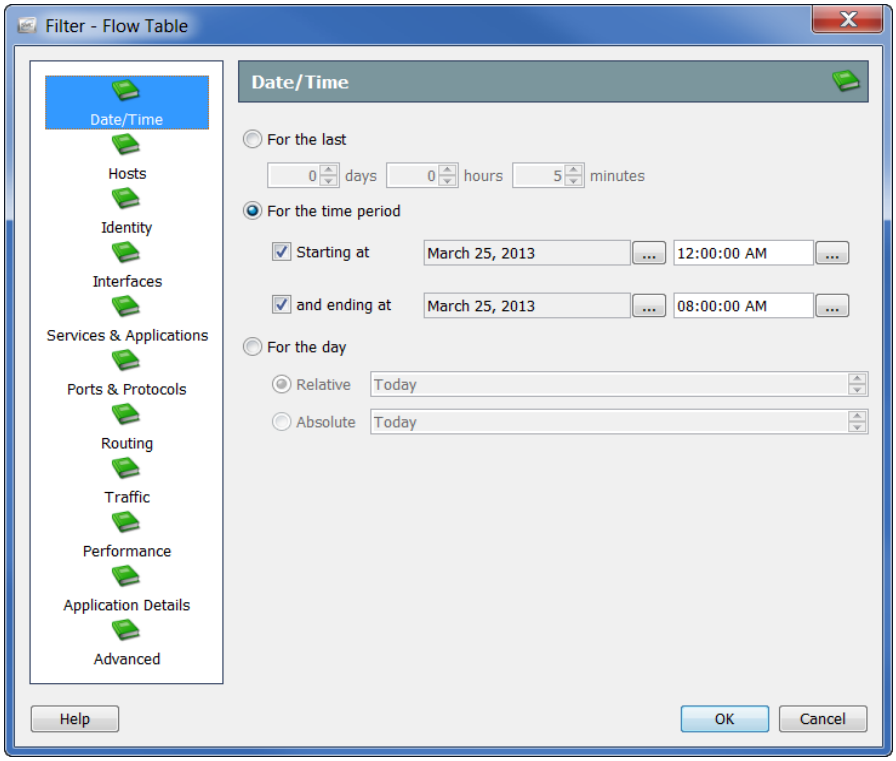


3. 指定用于过滤流数据的确切日期/时间、范围或相关设置。例如，如果要显示某一天午夜到上午 8:00 之间的所有流，您需完成以下步骤：

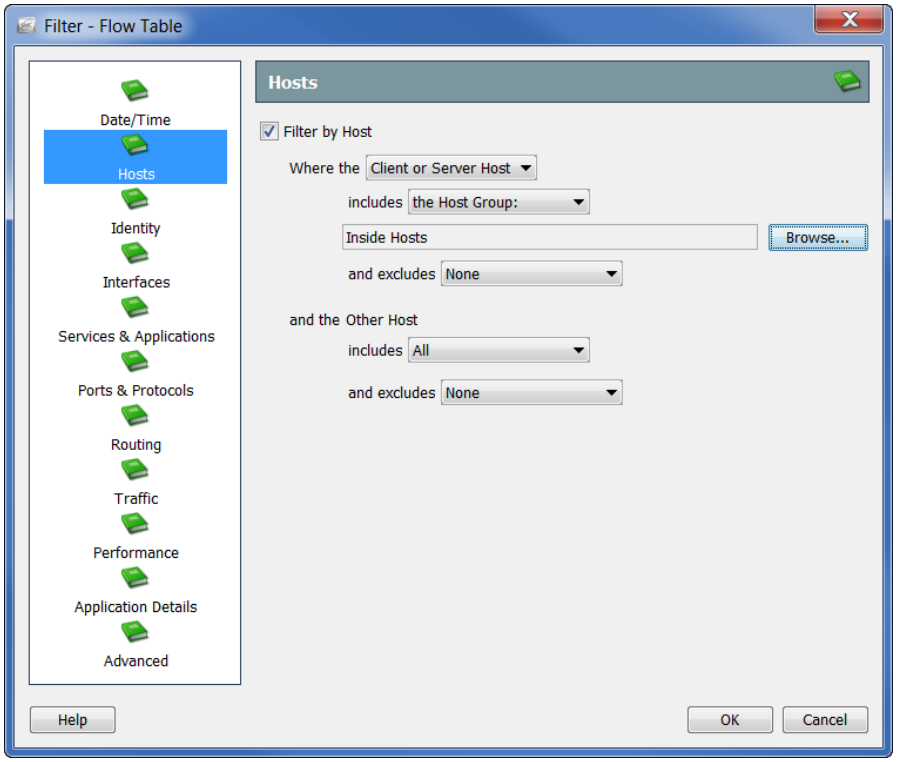
   a. 点击**时段**选项。

   b. 点击**起始时间**选项，输入要执行过滤的日期，然后在“时间”字段中输入 ***12:00:00***。

c. 点击**结束时间**选项，输入要执行过滤的日期，然后在该选项的“时间”字段中输入 ***08:00:00***。

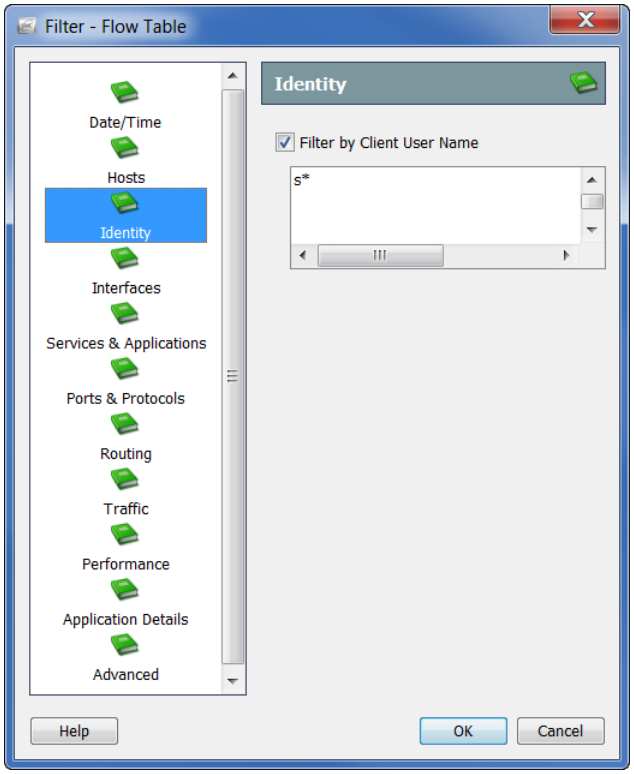


4. 点击**主机**图标。系统随即会打开“主机”页面。



指定要按其过滤流数据的主机。您可以包括/排除主机组、一个或多个虚拟机、IP 地址范围（使用 CIDR 格式）或 IP 地址列表（逗号分隔格式）。

5. 点击“身份”图标。系统随即会打开“身份”页面。



通过完成以下步骤，指定要按其过滤流数据的用户名：

1. 点击“客户端用户名”复选框以插入复选标记。
2. 在文本字段中键入以下任意内容：
   - 单个用户名，如 jdoe。
   - 多个用户名，如 jdoe、jalpha、jbeta。您可键入名称，用逗号分隔每个名称或在输入每个名称后按 **Enter**（即每行输入一个名称）。您还可从名称的逗号分隔值 (CSV) 列表复制并粘贴。
   - 带通配符的部分名称。通配符可位于任何位置，如 srh*, *doe。您可在每个名称中使用多个通配符。

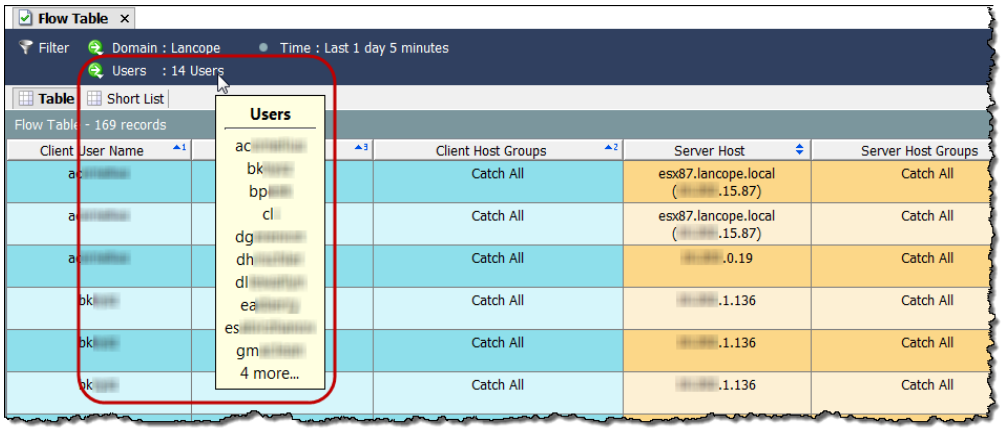
注意：

- 此字段不区分大小写。
- 用户名不能包含以下任何字符：| + = ? “ < > ( ) : ;

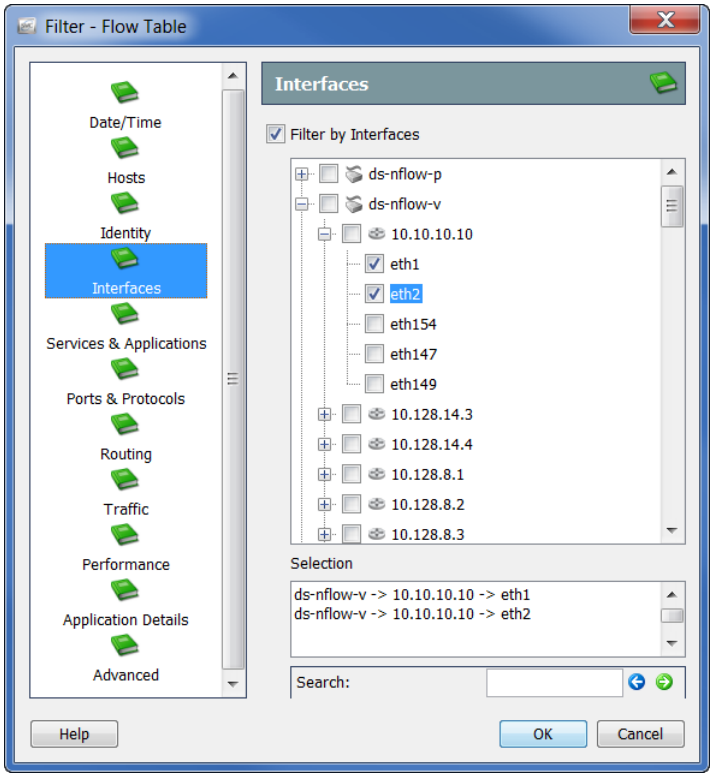
3. 点击**确定**。

结果显示在“客户端用户名”列中。如果您仅按一个用户进行过滤，该用户名将显示在顶部中。如果您按多个用户进行过滤，顶部将显示您过滤的用户名的数量。如果您将光标悬停在此条目上，将在弹出窗口中列出您已查询的前十个用户的名称（请参看以下屏幕）。

在弹出窗口底部显示超出前十个用户之外的所过滤用户名的数量。在以下示例中，已对 14 个用户名进行过滤，所以在弹出窗口的底部会显示条目*还有 4 个...*。

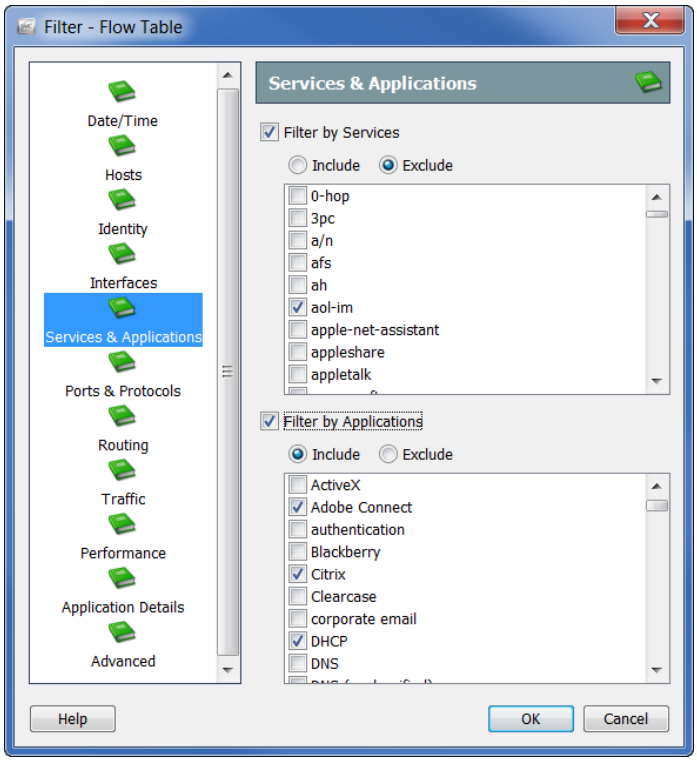


4. 点击**接口**图标。系统随即会打开“接口”页面。



指定要按其过滤流数据的接口。您可以点击单个接口、整个导出器或 Stealthwatch 设备。

5. 点击**服务和应用**图标。系统随即会打开“服务和应用”页面。

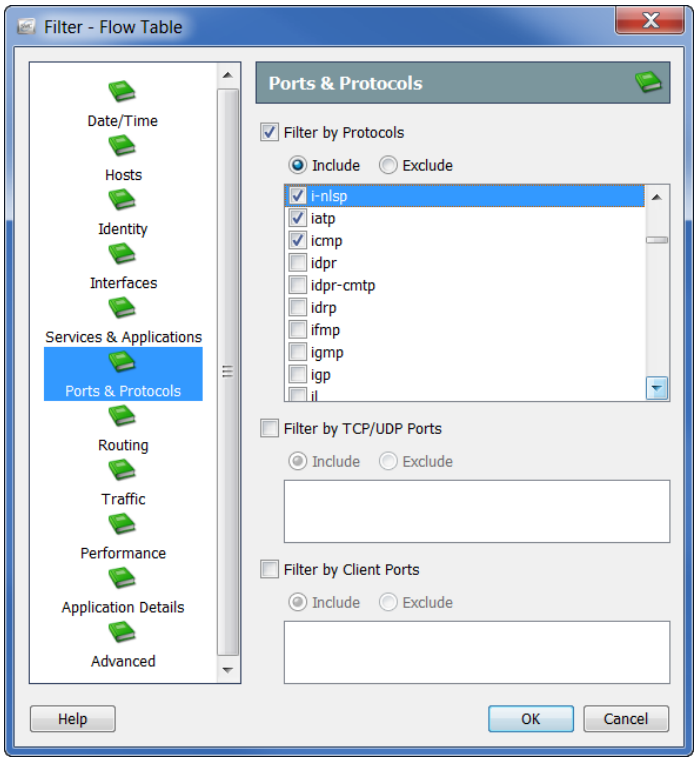


点击下列一个或两个复选框使其处于选中状态，以指定要按其过滤流数据的服务和/或应用：

- 按服务过滤
- 按应用过滤

点击**包括**或**排除**选项。例如，您可能希望将查询限制为 Facebook 之外的所有内容。在这种情况下，您可以点击**按应用过滤**复选框以添加复选标记，点击**排除**选项，然后点击 **Facebook** 复选框以添加复选标记。

6. 点击**端口和协议**图标。系统随即会打开“端口和协议”页面。

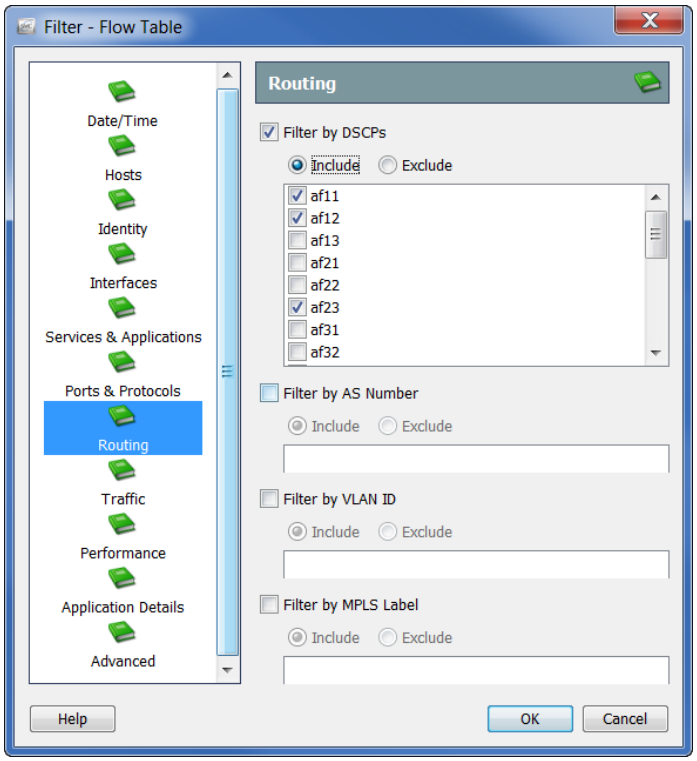


通过点击下列任意或所有复选框以添加复选标记，从而指定要按其过滤流数据的端口和协议：

- 按协议过滤
- 按 TCP/UDP 端口过滤
- 按客户端端口过滤

点击**包括**或**排除**选项，以进一步自定义查询。

7. 点击**路由**图标。系统随即会打开“路由”页面。

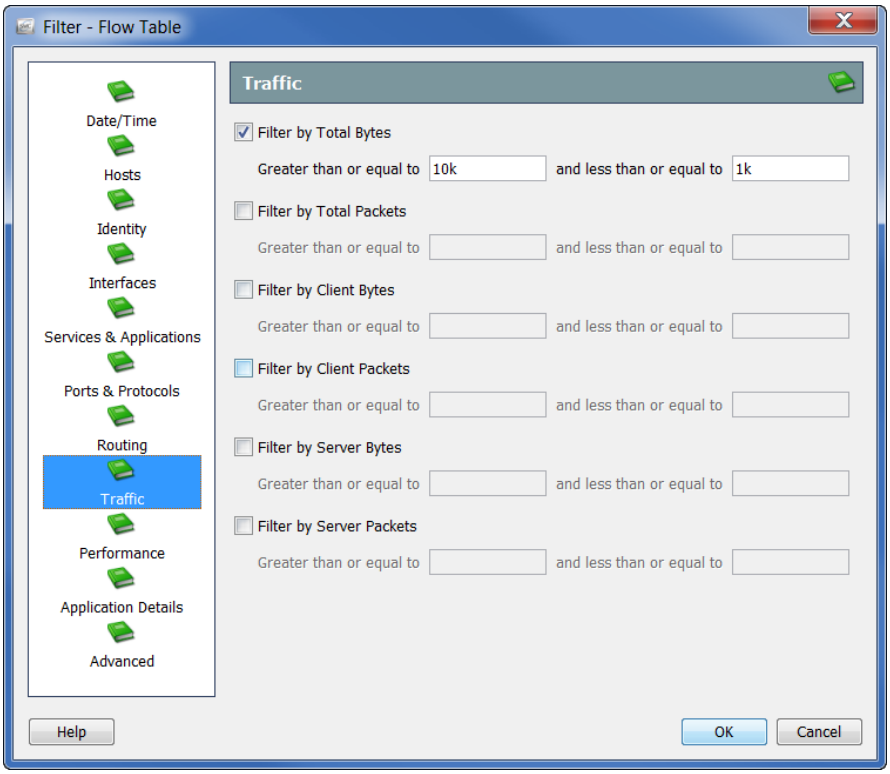


通过点击下列任意或所有复选框以添加复选标记，从而指定要按其过滤流数据的参数：

- 按 DSCP 过滤
- 按 AS 编号过滤
- 按 VLAN ID 过滤
- 按 MPLS 标签过滤

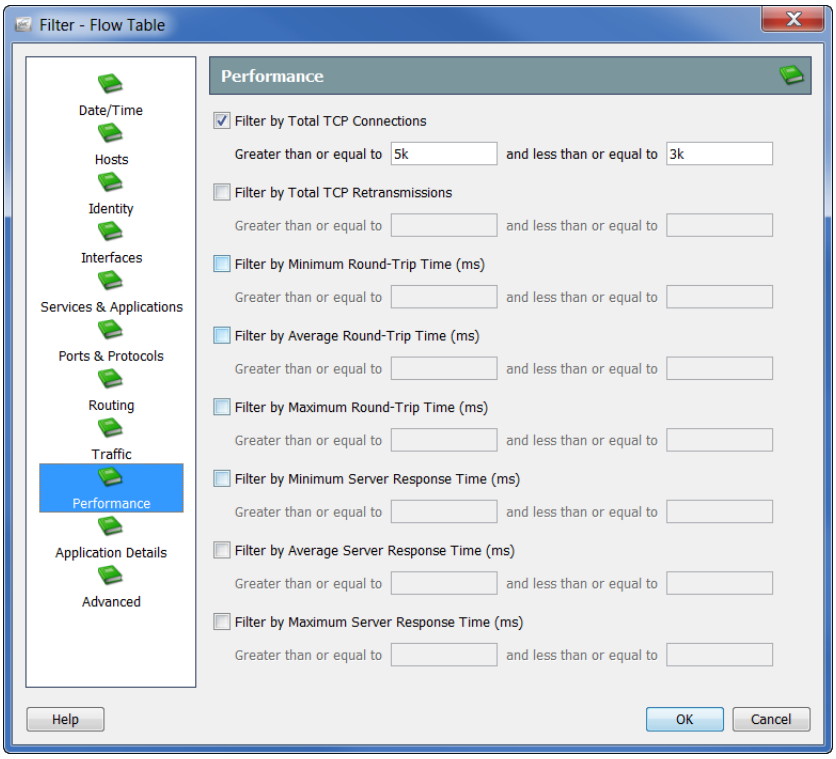
点击**包括**或**排除**选项，以进一步自定义查询。

8. 点击**流量**图标。系统随即会打开“流量”页面。



指定要按其过滤流数据的流量数据的类型和大小。

9. 点击**性能**图标。系统随即会打开“性能”页面。

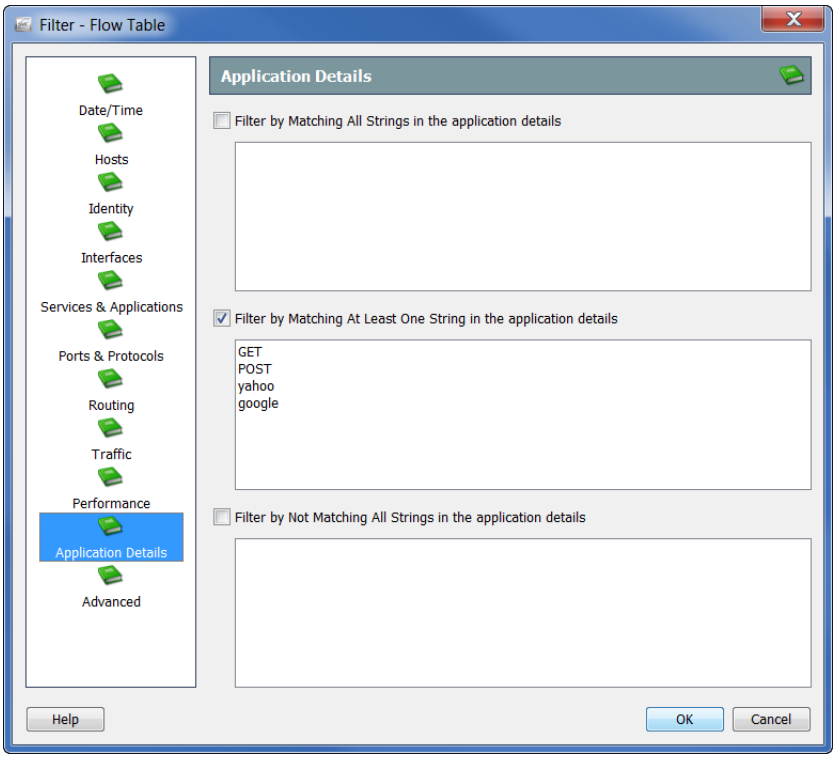


指定要按其过滤流数据的性能数据的类型和大小。

注意：

“性能”页面上的所有值需要使用 Stealthwatch FlowSensor 才能进行收集和存储。

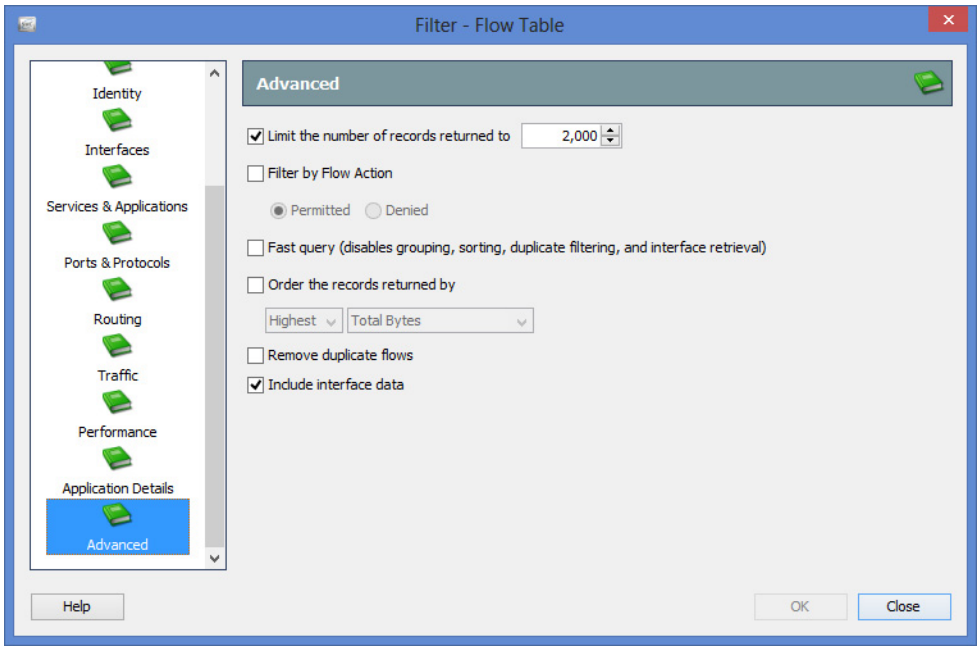
10. 点击**应用详细信息**图标。系统随即会打开“应用详细信息”页面。



指定要按其过滤流数据的负载信息。

“应用详细信息”页面上的所有值需要使用 FlowSensor 或在 Flexible NetFlow 中导出负载，以收集和存储这些信息。

11. 点击**高级**图标。系统随即会打开“高级”页面。



您可以限制查询所显示的流记录最大数量。另外，您还可以指定数据的排序方式（例如在服务器上、提取数据之前）以及是否从结果中删除重复流。

注意：

- 仅在有多个流量收集器时，才需要用到**删除重复流**选项。单一流量收集器会自动执行重复数据删除。。
- 如果不需要查看接口数据，请点击**包括接口数据**复选框以删除复选标记。这样可以更快地检索数据。

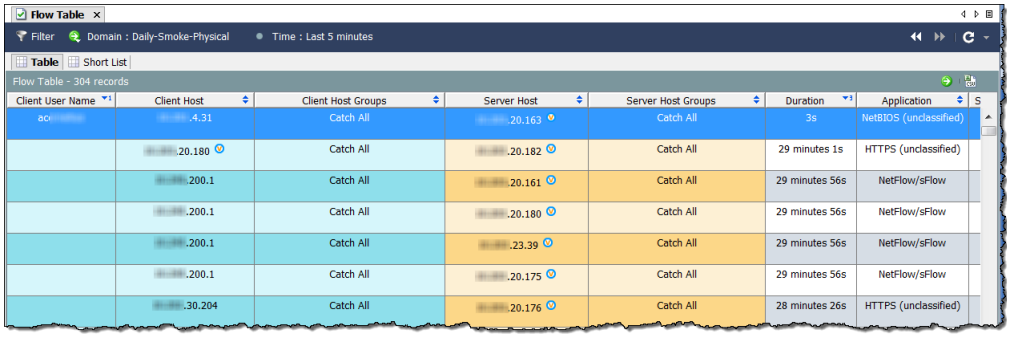
12. 当准备好执行过滤时，点击**确定**。系统随即会发送流查询，而检索到的数据将显示在“流表”文档中。

下次访问“流表”时，只有您已在“高级”页面上指定的过滤设置仍然有效。不会保留“流表”过滤器任何其他页面上的过滤设置。

流表选项卡

表选项卡

“流表”文档上的“表”选项卡根据您在“流表过滤器”上指定的选项显示流数据。



注意：

您可以点击文档右上角的**转到文档**按钮，以显示使用相同流数据的其他文档。

由于导入的流文件不包含原始设备/域信息，所以需要这些信息的弹出菜单选项对于导入的流文件不可用（以灰色显示）。

注意：

有关导入流文件的详细信息，请参阅 *SMC 客户端联机帮助*中的“如何导入流文件”主题。

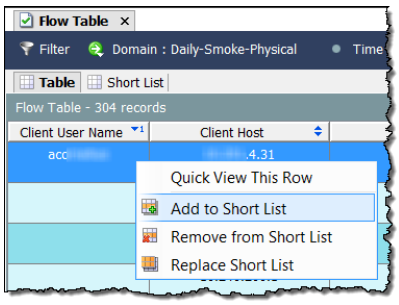
要更改表中显示的列，请右键点击某个标题，然后从弹出菜单中选择所需的列。标题旁边带有复选标记表示它将显示在文档中。

短列表选项卡

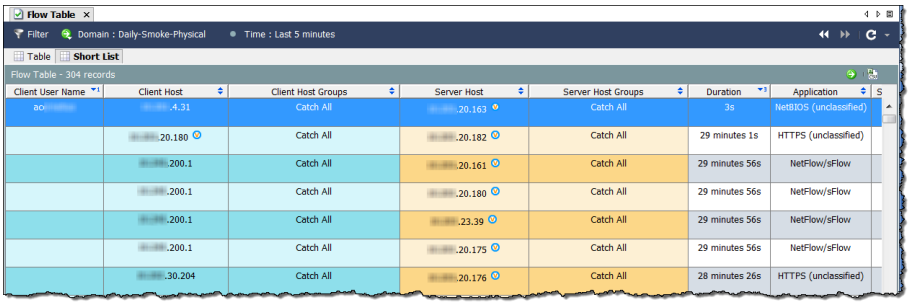
“短列表”选项卡与“表”选项卡共享相同的配置。对其中一个选项卡进行的更改会在另一个选项卡上自动反映出来。

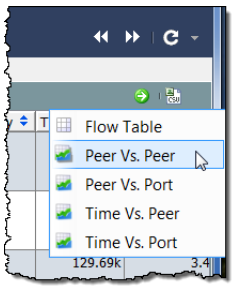
通过“流表”文档中的“短列表”选项卡，您可以显示“流表：表”页面上显示的流数据的子集。例如，“表”选项卡可能显示数千个流记录，但您可能只想查看其中少数行，以便进行更深入的分析。使用“短列表”功能可选择特定的行，从而便于查看。

右键点击“表”选项卡上的一行或多行，然后选择**添加到短列表**，如右侧示例中所示。



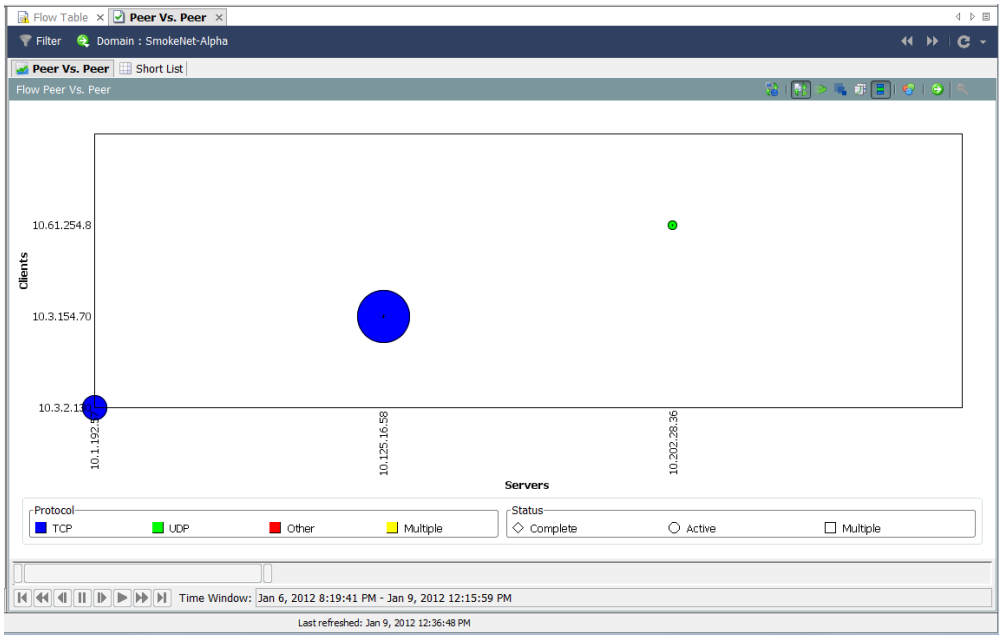
要查看流，请点击**短列表**选项卡以打开“流短列表”。所选的行随即会显示在此文档中。





若要以图形方式查看数据的子集，请点击**转到文档**按钮，然后从弹出菜单中点击所需的分析类型（例如点对点）。

仅显示短列表中主机的数据，而不是“流表”过滤器检索到的所有数据。



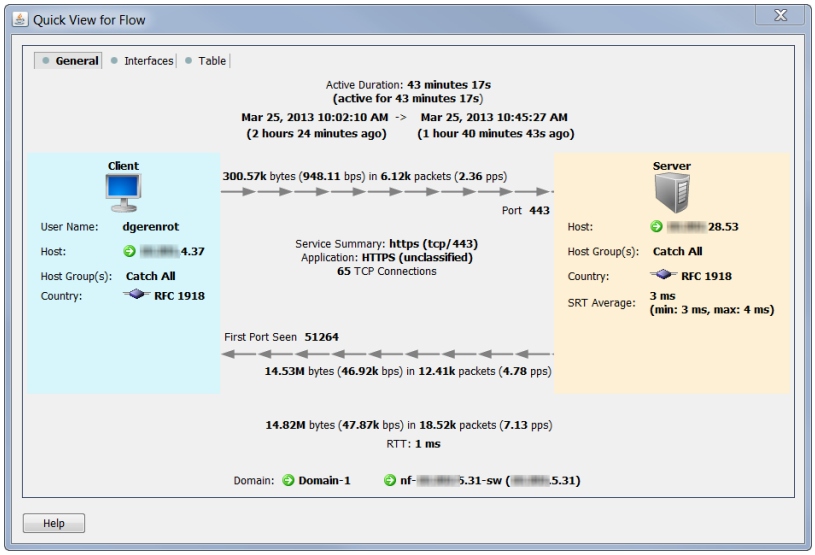
快速视图

通过“快速视图”对话框，可以图形方式快捷地查看表格数据。它也提供对其他文档已过滤视图的快速导航。

要查看“快速视图”对话框，请点击表格单元格，然后按空格键。要使对话框消失，请再次按空格键或按 Esc 键。

如下面示例中所示，“快速视图”对话框显示以下选项卡上的数据：

- 总则
- 接口
- 表



您可以同时按键盘上的 Alt 键和 ← 或 → 键在选项卡之间进行浏览。

您可以同时按键盘上的 Alt 键和 ↑ 或 ↓ 键在流之间进行浏览（同时保持打开“快速视图”对话框）。

提示：

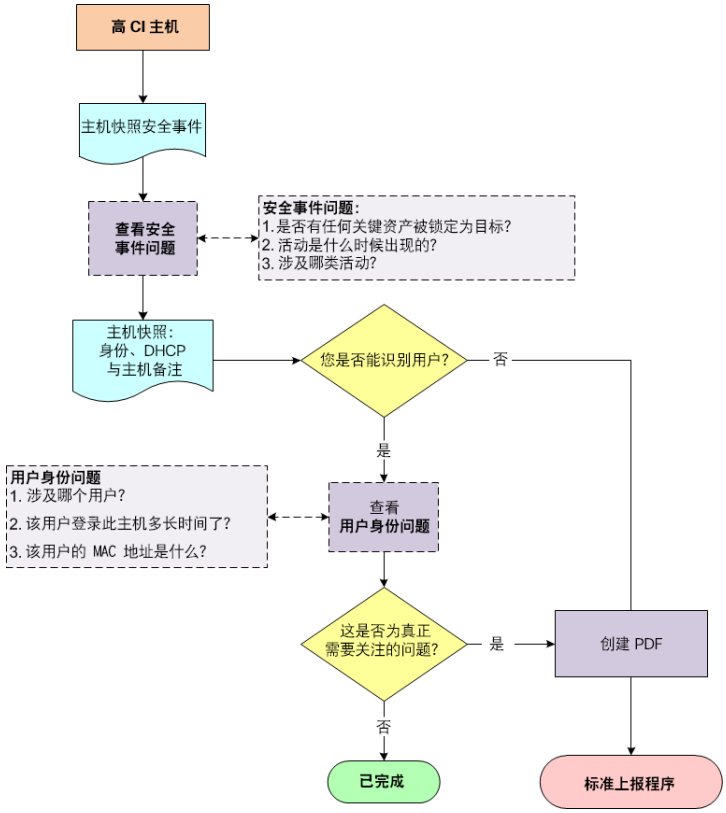
适用于其他表的相同导航功能（例如深入查看其他文档）在此处也适用。

流分析场景

现在，您已熟悉流分析过程，接下来我们将介绍几种常见情况。

高关注指数主机

高 CI 主机是指作为可疑流活动（安全事件）源的主机。下图描绘了可用来确定威胁是否真实的工作流程。



工作流程概述

以下步骤概述了前面工作流程图中描绘的程序。

1. 打开源主机的“主机快照：安全事件”页面，并查看详细信息。请参阅以下部分“检查安全事件活动（主机快照）”。
2. 点击**身份、DHCP 和主机说明**选项卡。
3. 您能否识别用户？
   - 如果是，请转至步骤 4。
   - 如果否，请转至步骤 6。

4. 查看登录到源主机的任何用户的信息。请参阅“检查用户身份信息（主机快照）”（第 159 页）。

5. 根据您收集的信息，此活动看起来是否属于真实问题？
   - 如果是或不确定，请转到步骤 6。
   - 如果否，请到此停止。

6. 创建主机快照的 PDF 文档，并根据组织的标准上报程序进行上报。

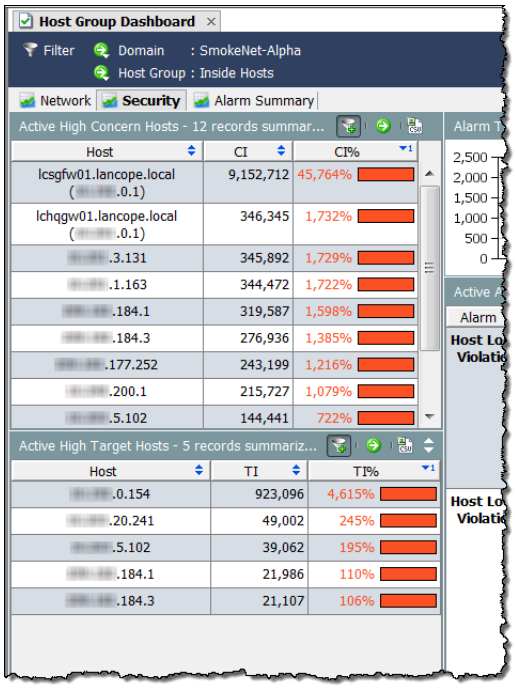
检查安全事件活动（主机快照）

高 CI 主机可能受到恶意软件感染或受到其他某些方式的入侵。通过 SMC 的某些位置（包括以下项目），您可以轻松识别高 CI 主机：

- 关注指数
- 警报表（如果触发了警报）
- 主机组控制面板：安全页面

此工作流程从“主机组控制面板：安全”页面开始调查。请完成以下步骤，以检查高 CI 主机的安全事件活动。

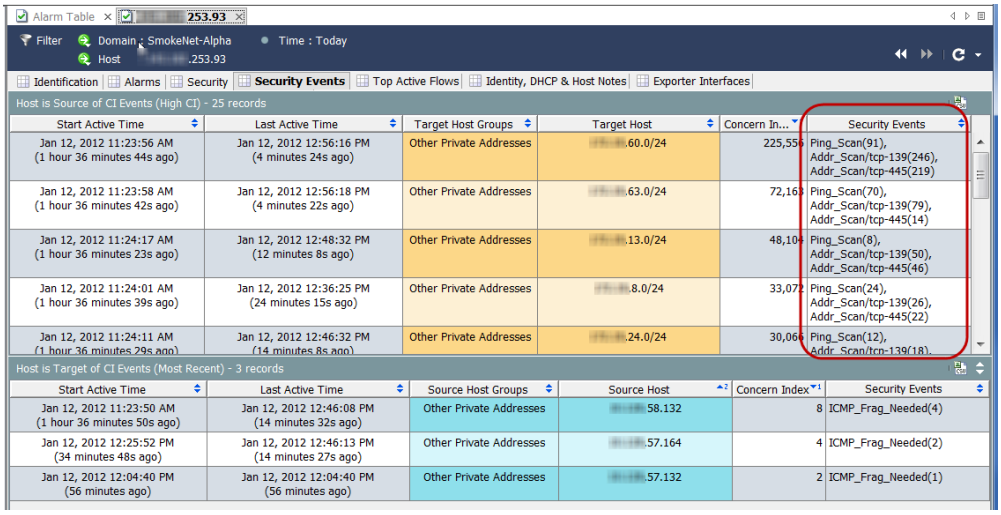
1. 在主机组控制面板上，点击**安全**选项卡。**活动高关注主机**和**活动高目标主机**部分将列出与该特定主机组控制面板关联的主机组的高 CI 主机和高 TI 主机。



2. 双击相应的主机 IP 地址打开其主机快照。

提示：
如果知道 IP 地址，还可以使用全局搜索功能查找主机快照。

3. 点击**安全事件**选项卡。
4. 在**主机是安全事件源(高 CI)** 部分，查看“安全事件”列中的条目（请参阅以下示例）。问自己以下问题：
   - 是否有任何关键资产被锁定为目标？
   - 活动是什么时候出现的？
   - 涉及哪类活动？



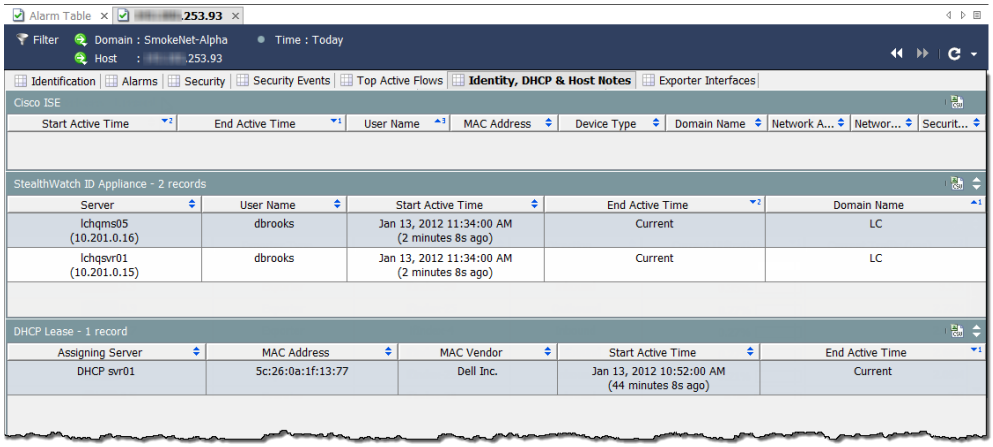
注意：
有关特定安全事件的详细说明，请参阅 *SMC 客户端联机帮助*中的“安全事件”主题。

5. 检查用户身份信息，如下一部分所述。

检查用户身份信息（主机快照）

在了解高 CI 主机的安全事件活动后，请完成以下步骤来检查已登录到该主机的用户身份。

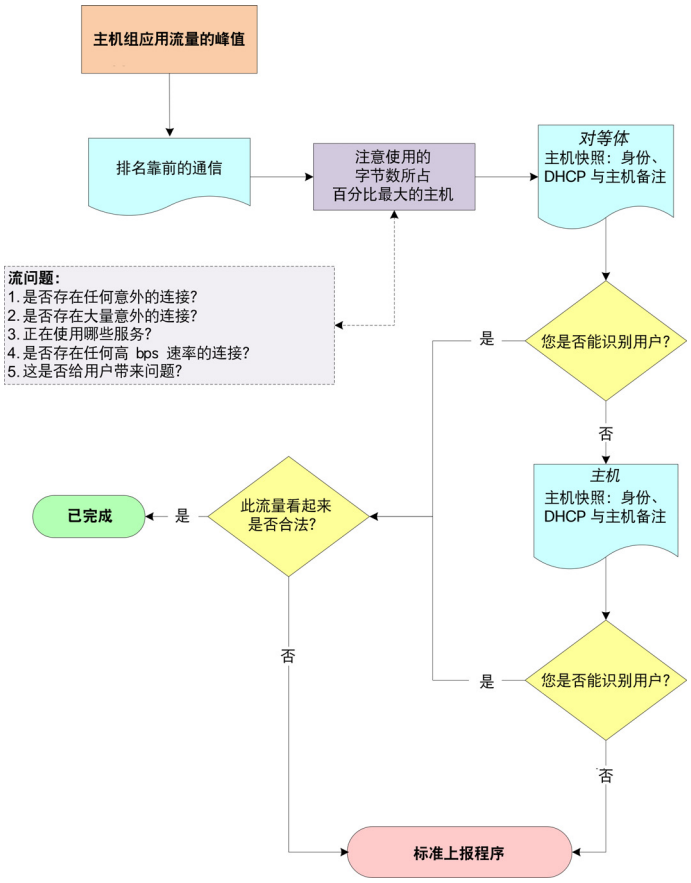
1. 在“主机快照”上，点击**身份、DHCP 和主机说明**选项卡。



2. 您是否看到任何用户信息？
   - 如果是，请转至步骤 3。
   - 如果否，请转至步骤 5。
3. 查看用户信息时，请注意以下问题：
   - 哪些用户登录了此主机？
   - 他们已登录了多久？
   - 该用户的 MAC 地址是什么？
4. 根据您收集的此主机的信息，此活动看起来是否属于真实问题？
   - 如果是或不确定，请转到步骤 5。
   - 如果否，请到此停止。
5. 创建主机快照的 PDF 文档，并根据组织的标准上报程序进行上报。

应用流量的峰值

如果您看到网络中某个区域的流量突然增加，请使用下图中描述的工作流程来帮助确定突然增加的原因，并确定是否应对此关注。



工作流程概述

通过 SMC 中的某些位置，您可以查看流量高峰，例如以下位置：

- 可以通过“流量”菜单访问的任何流量图。
- 主机组控制面板：“网络”页面

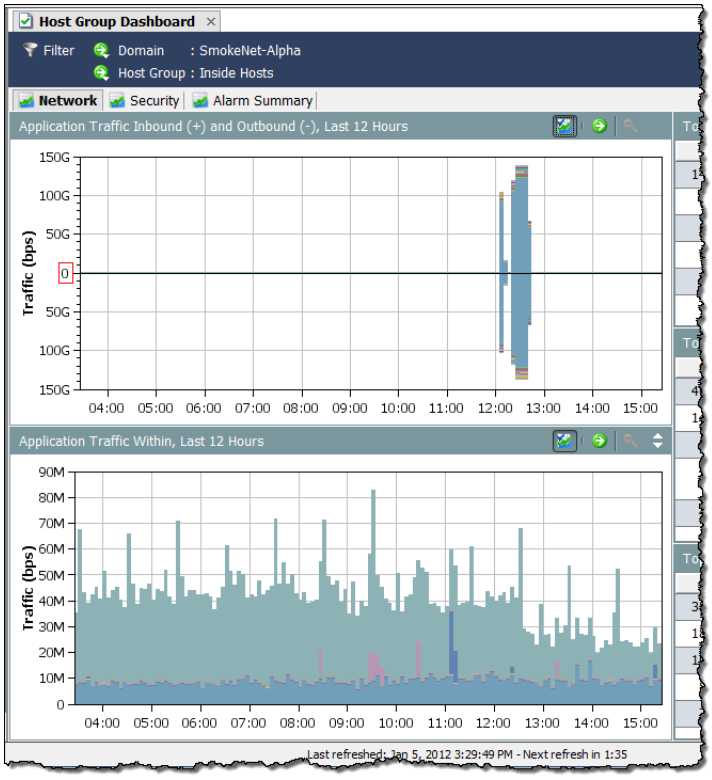
此工作流程从“网络”页面开始调查。以下步骤概述了前面工作流程图中描绘的程序。

1. 在“网络”页面上，确定流量高峰传输的方向。请参阅“确定所涉及的主机”（第 164 页）。
2. 双击该流量高峰可打开“排名靠前的对话”文档，然后即可确定哪个主机对在标注的方向占用的带宽最高。请参阅“确定所涉及的主机”（第 164 页）。

3. 针对上面识别的主机对，查看下列问题：
   - 是否有任何意外连接（例如，未经授权的主机组或服务器）？
   - 是否有大量意外连接？
   - 正在使用哪些端口？
   - 是否正在发送和/或接收大量流量？
   - 是否存在任何高 bps 速率的连接？
   - 此高峰是否与用户对网络的抱怨相关？
4. 打开对等体的“主机快照：身份、DHCP 和主机说明”页面。请参阅“识别所涉及的用户”（第 164 页）。
5. 您能否识别涉及的用户？
   - 如果是，请转至步骤 8。
   - 如果否，请转至步骤 6。
6. 打开主机的“主机快照：身份、DHCP 和主机说明”页面。请参阅“识别所涉及的用户”（第 164 页）。
7. 您能否识别涉及的用户？
   - 如果是，请转至步骤 8。
   - 如果否，请转至步骤 9。
8. 这些流量看起来是否像是合法活动？
   - 如果是或不确定，请转到步骤 9。
   - 如果否，则可以忽略该流量高峰。
9. 收集到目前为止收集到的信息，并根据组织的标准上报程序进行上报。

确定流量的方向

主机组控制面板的“网络”选项卡提供最全面的主机组应用流量视图。



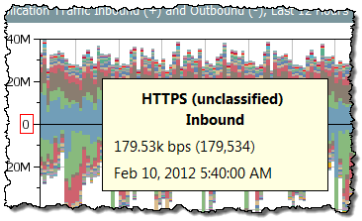
查看**应用流量入站 (+) 和出站 (-)** 和**内部应用流量**图表，可立即查看是否存在流量高峰并确定流量传输的方向。

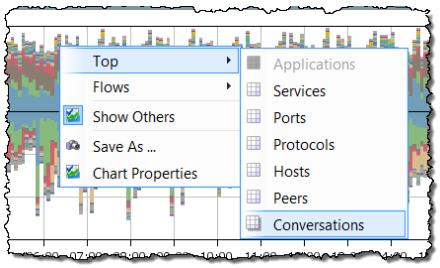
应用流量入站 (+) 和出站 (-) 图表显示从外部主机组流到内部主机组的流量，反之亦然。入站流量显示在零 (0) 行上方。出站流量显示在零行之下。

内部应用流量图表仅显示在网络（内部主机组）内从属主机组之间传输的流量。

每个图表显示在过滤器中设置的时段内使用的前 15 个应用。不同的颜色代表不同的应用。每个图表的图例按最常用到最少用的顺序列出服务。将光标悬停在图例中的应用上方，可查看图表中突出显示的应用。

将光标悬停在图表中的数据点上方会显示工具提示，其中提供有关该流量的详细信息，如右侧示例中所示。



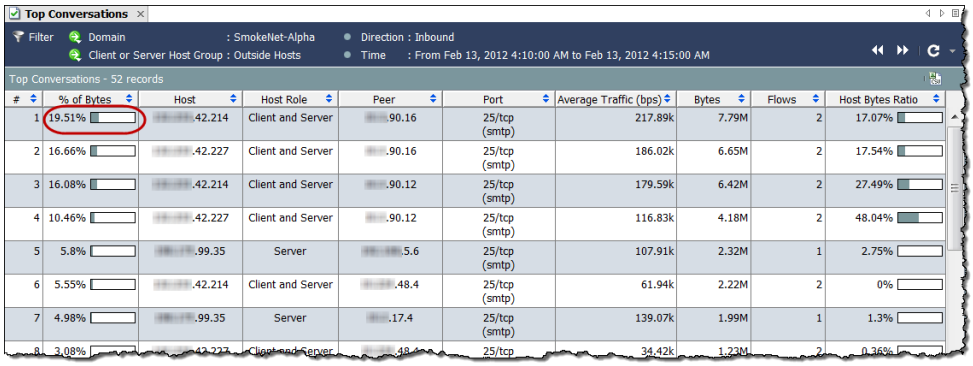


双击数据点会显示一个弹出菜单，其中提供了若干选项，选择它们可了解有关该流量的详细信息，如左侧示例中所示。

确定所涉及的主机

在知道流量传输的方向后，请完成以下步骤以确定所涉及的主机对。

1. 在“网络”选项卡上，双击流量高峰以打开“排名靠前的对话”文档。



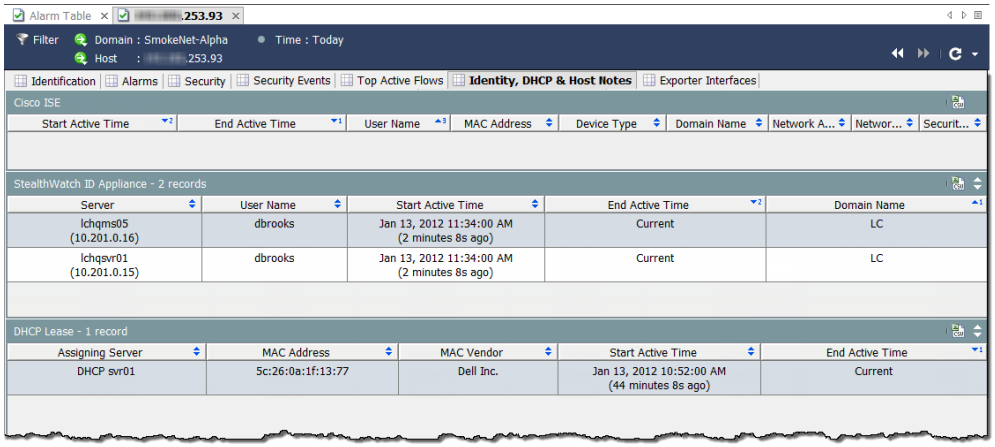
2. 确定使用字节百分比最高的主机和对等体。（默认情况下，此项会以 # 列中标记数字 **1** 来表示。）
3. 针对上面识别的主机对，查看下列问题：
   - 是否有任何意外连接（例如，未经授权的主机组或服务器）？
   - 是否有大量意外连接？
   - 正在使用哪些端口？
   - 是否正在发送和/或接收大量流量？
   - 是否存在任何高 bps 速率的连接？
   - 此高峰是否与用户对网络的抱怨相关？

识别所涉及的用户

在知道流量高峰所涉及的主机对的 IP 地址后，请完成以下步骤，以查看是否可识别所涉及的用户以及此活动是否会引起任何问题。

1. 双击相应的主机 IP 地址以打开其主机快照。

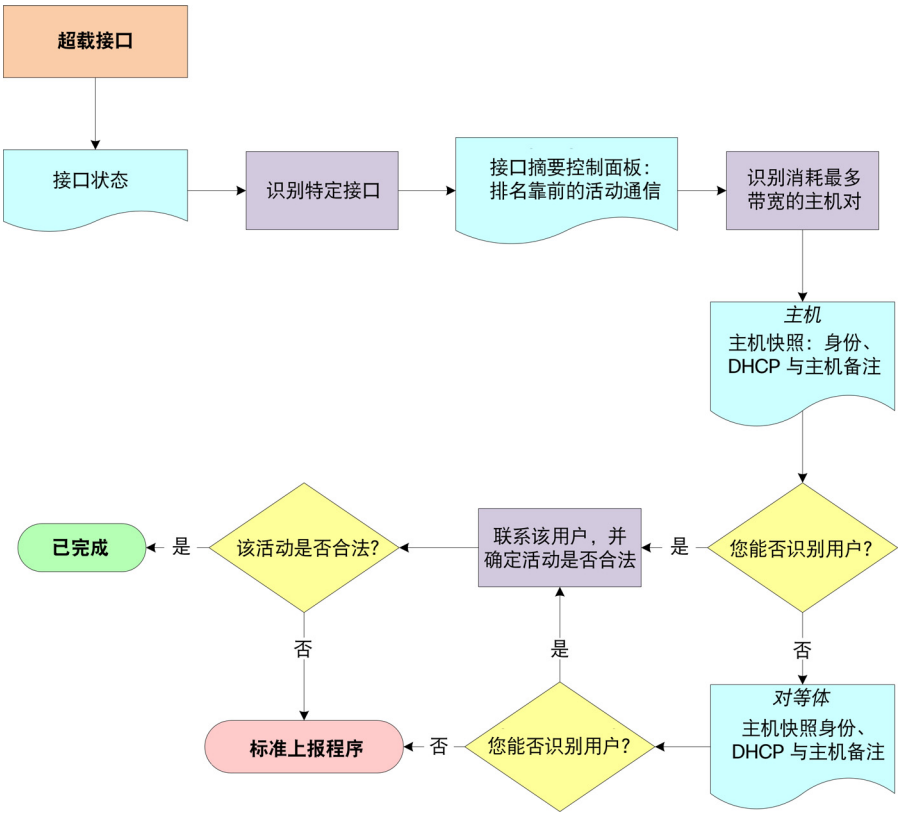
2. 点击**身份、DHCP 和主机说明**选项卡。



3. 您是否看到任何用户信息？
   - 如果是，请转至步骤 6。
   - 如果否，请转至步骤 4。
4. 双击相应对等体的 IP 地址以打开其主机快照。
5. 点击**身份、DHCP 和主机说明**选项卡。
6. 您是否看到任何用户信息？
   - 如果是，请转至步骤 6。
   - 如果否，请转至步骤 7。
7. 此活动看起来是否有任何问题？
   - 如果是或不确定，请转到步骤 7。
   - 如果否，请到此停止。
8. 收集到目前为止收集到的信息，并根据组织的标准上报程序进行上报。

过载接口

如果您知道或怀疑某个接口已过载或接近满载，可以使用下图中所示的工作流程来帮助查明问题根源。



工作流程概述

通过 SMC 的某些位置（包括以下项目），您可以轻松查看接口利用率：

- 企业树中的网络设备
- 接口状态
- 警报表（如果触发了“已超出接口利用率”警报）

此工作流程从“接口状态”文档开始调查。以下步骤概述了前面工作流程图中描绘的程序。

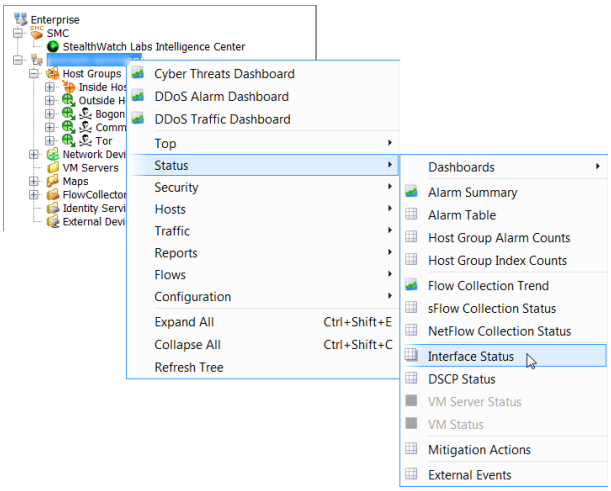
1. 打开域的“接口状态”文档以识别过载接口。请参阅以下部分“识别过载的接口（接口状态）”。
2. 打开利用过度的接口的“接口摘要”控制面板，并查看“排名靠前的活动对话”。
3. 记下占用带宽最高的主机对（主机和对等体）的 IP 地址。
4. 打开主机的“主机快照：身份、DHCP 和主机说明”页面。请参阅“识别登录高带宽主机的用户”（第 173 页）。

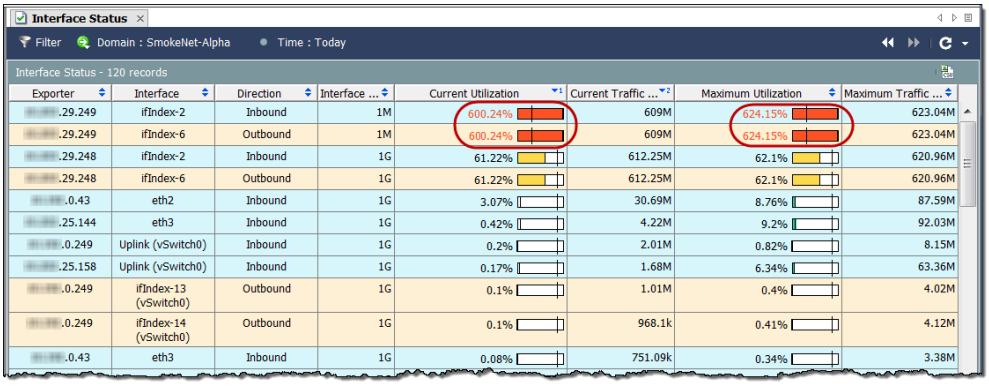
5. 您能否识别用户？
   - 如果是，请转至步骤 8。
   - 如果否，请转至步骤 6。
6. 打开对等体的“主机快照：身份、DHCP 和主机说明”页面。请参阅“识别登录高带宽主机的用户”（第 173 页）。
7. 您能否识别用户？
   - 如果是，请转至步骤 8。
   - 如果否，请转至步骤 10。
8. 联系用户并确定该用户参与的活动是否合法。
9. 该活动是否合法？
   - 如果是，请到此停止。
   - 如果否，请转至步骤 10。
10. 收集到目前为止收集到的信息，并根据组织的标准上报程序进行上报。

识别过载的接口（接口状态）

请完成以下步骤以打开“接口状态”文档，并确定已过载或接近满载的特定接口。

1. 右键点击域名，然后依次选择 **状态 > 接口状态**。
2. 打开“接口状态”文档后，识别已过载或接近满载的任何接口，如以下示例中所示。（**提示：**查找“当前利用率”和“最大利用率”列中的红条、橙条或黄条。）

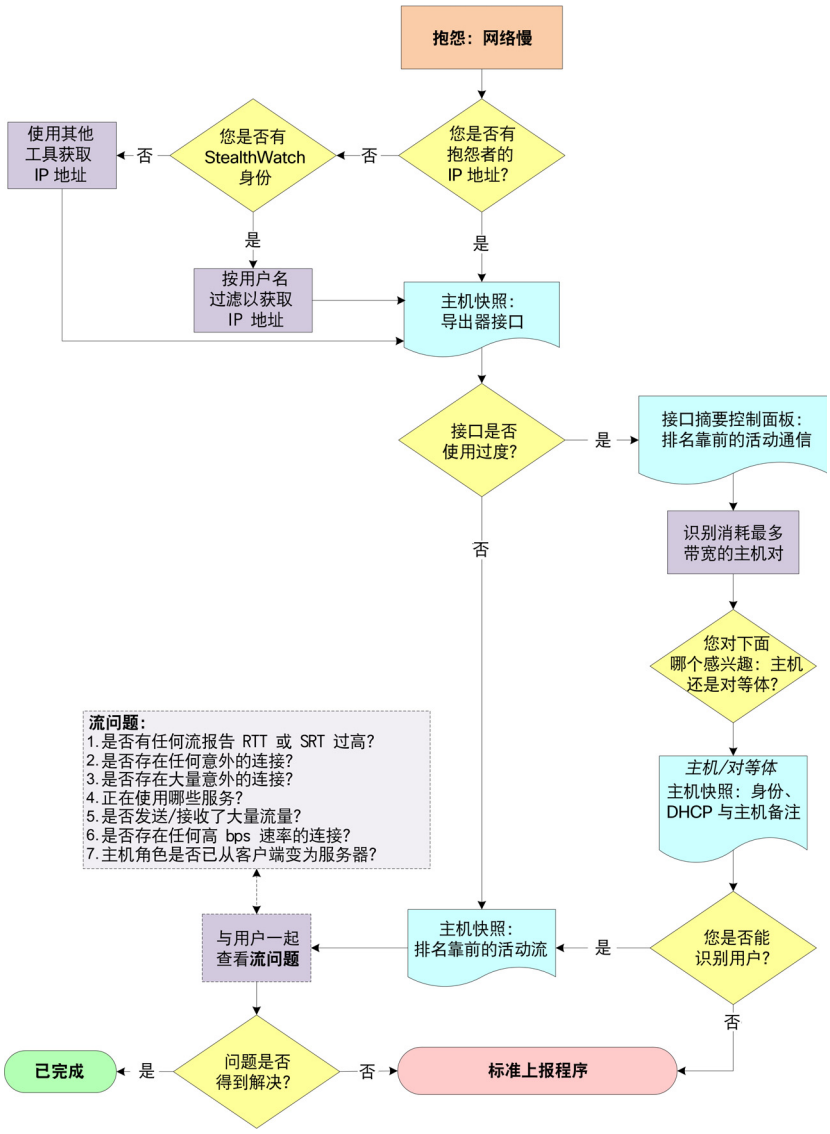




3. 双击相应的接口单元格以打开已识别接口的“接口摘要”控制面板，确定流量为什么这么多。请参阅“查找高带宽主机（接口摘要控制面板）”（第 173 页）。

网速慢

用户最常见的抱怨之一就是网速慢。下图显示了可用来帮助查明问题根源的工作流程。



工作流程概述

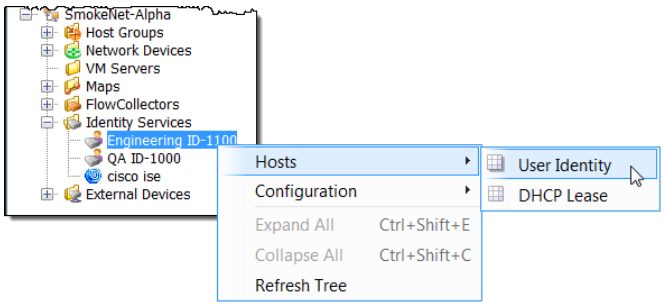
以下步骤概述了前面工作流程图中描绘的程序。

1. 您是否有抱怨用户的 IP 地址？
   - 如果是，请转至步骤 3。
   - 如果否，请转至步骤 2。
2. 您是否有 StealthWatch 身份设备？
   - 如果是，请使用用户身份过滤器来搜索该用户的 IP 地址。请参阅以下部分“使用 StealthWatch 身份查找 IP 地址”。
   - 如果否，请使用可用的任何工具（例如 ipconfig）来获取该用户的 IP 地址。
3. 打开该用户 IP 地址的“主机快照：导出器接口”页面。请参阅“检查过度利用的接口（主机快照）”（第 172 页）。
4. 是否有任何接口利用过度或接近满载？
   - 如果是，请打开利用过度的接口的“接口摘要”控制面板，并查看“排名靠前的活动对象”。请参阅“查找高带宽主机（接口摘要控制面板）”（第 173 页）。
   - 如果否，请转至步骤 8。
5. 记下占用带宽最高的主机对（主机和对等体）的 IP 地址。
6. 根据您最感兴趣的主机对，打开主机或对等体的“主机快照：身份、DHCP 和主机说明”页面，以尝试识别登录到该 IP 地址的用户。请参阅“识别登录高带宽主机的用户”（第 173 页）。
7. 您能否识别用户？
   - 如果是，请获取该用户的 IP 地址并转到步骤 8。
   - 如果否，请转至步骤 10。
8. 打开相关的“主机快照：排名靠前的活动流”页面，并查看与该用户关联的数据流的详细信息，从而确定问题的潜在原因。请参阅“检查排名靠前的活动流”（第 174 页）。
9. 您能否解决该问题？
   - 如果是，请到此停止。
   - 如果否，请转至步骤 10。
10. 收集到目前为止收集到的信息，并根据组织的标准上报程序进行上报。

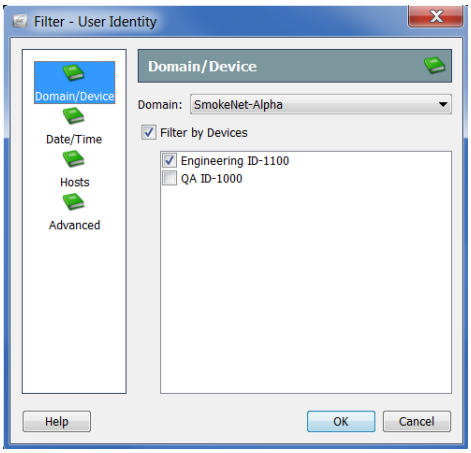
使用 StealthWatch 身份查找 IP 地址

如果您拥有 Stealthwatch 身份设备，请完成以下步骤以快速查找特定用户正在使用或使用过的 IP 地址。

1. 在企业树中，展开“身份服务”分支并查找要使用的身份设备。
2. 右键点击该身份设备，然后依次选择**主机 > 用户身份**。



系统将打开“过滤器对话框：用户身份”页面。“域/设备”页面会自动选中您所选的域和设备。

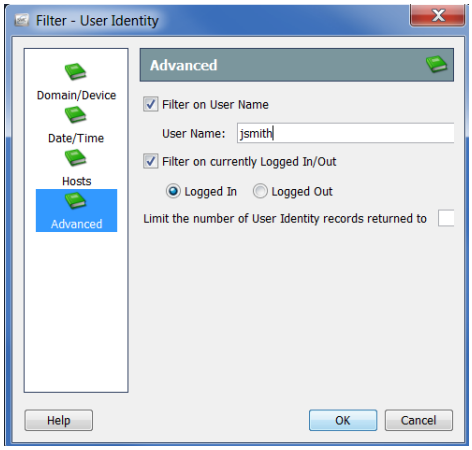


注意：

- 过滤器将打开您上次关闭过滤器时查看的最后页面。如果您从未打开过过滤器，它将打开“域/设备”页面。
- 要查看适用于用户 IP 地址的所有身份设备，请点击“域/设备”页面上的**按设备过滤**复选框以删除复选标记。

3. 点击**高级**按钮。系统将打开“高级”页面。

4. 点击**过滤用户名**复选框以添加复选标记，然后在“用户名”字段中键入用户的登录名称。



5. 默认情况下，该过滤器将按所选的**过滤当前已登录/注销用户**选项中所示，仅查找查询时已登录的用户的 IP 地址。

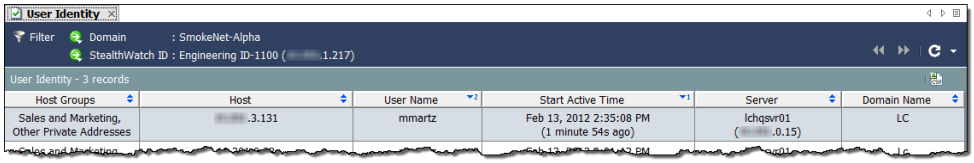
   要搜索用户在其他时间登录到的 IP 地址，请点击**过滤当前已登录/注销用户**复选框以删除复选标记，然后转到过滤器的“日期/时间”页面指定相关时间范围。

6. 如果需要，请在**限制返回的用户身份记录数**字段中键入值来更改显示的记录数。

注意：

要解决本节中所述的问题类型，通常不需要在过滤器中定义任何其他参数。如需其他帮助，请参阅 *SMC 客户端联机帮助*。

7. 点击**确定**。系统随即会打开“用户身份”文档，文档中显示与指定用户名关联的 IP 地址。



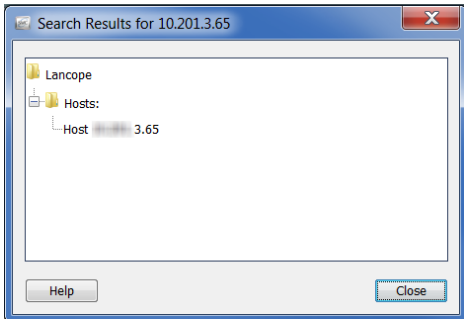
提示：

双击 IP 地址可打开相关的主机快照。

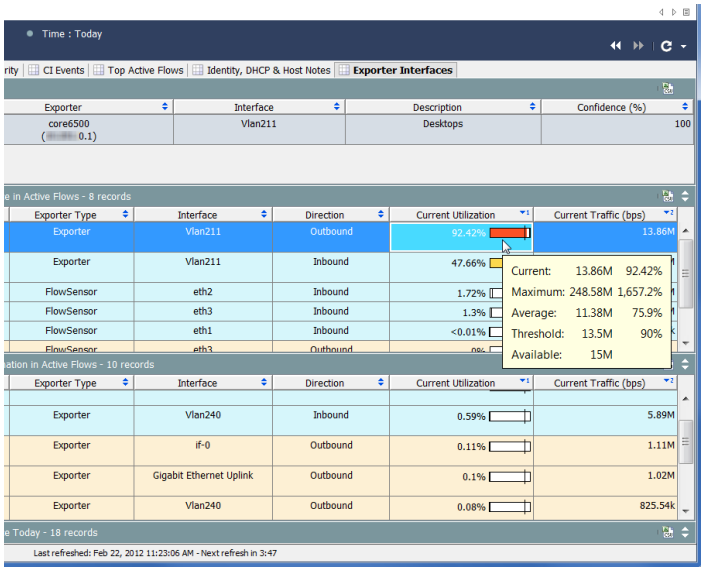
检查过度利用的接口（主机快照）

请完成以下步骤以打开特定 IP 地址的“主机快照：导出器接口”选项卡，从而查看是否有任何接口过载。

1. 您是否使用了“用户身份”文档来查找 IP 地址？
   - 如果是，请双击 IP 地址以打开主机快照，然后转到步骤 4。
   - 如果否，请转至步骤 2。
2. 在 SMC 工具栏中，在“全局搜索”字段中键入 IP 地址，然后按 **Enter**。“搜索结果”对话框将显示 SMC 中显示该地址的各个位置列表，如右侧示例中所示。



3. 双击该主机 IP 地址条目。
4. 打开主机快照后，点击**导出器接口**选项卡。



提示：

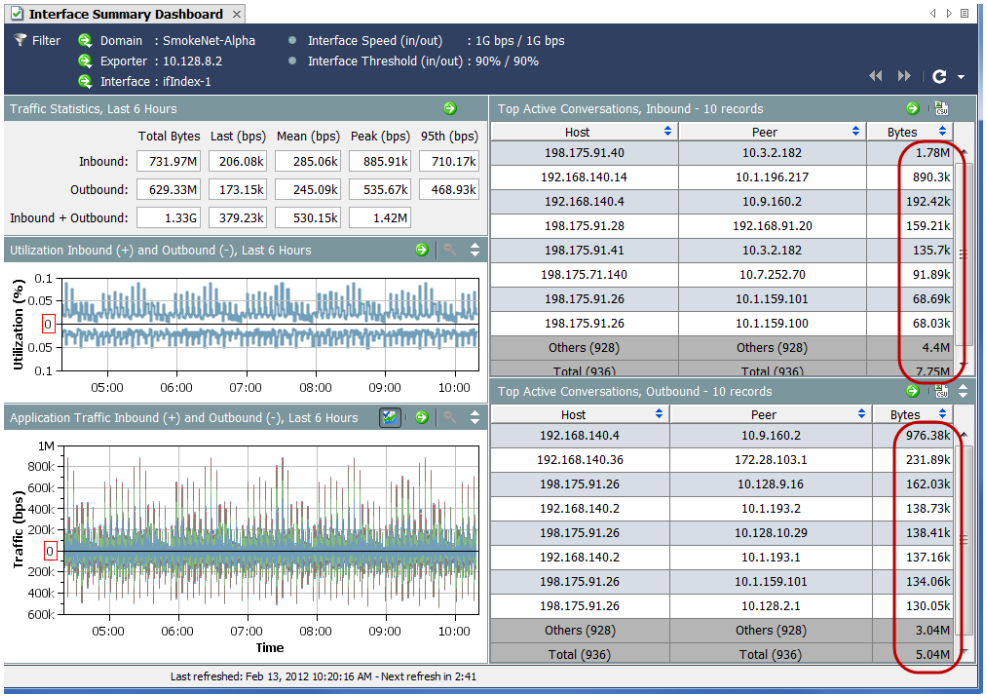
将光标悬停在“当前利用率”列的值上方，可查看相关接口的可用容量和使用详细信息。

5. 是否有任何接口过载或接近满载？（**提示：**查找“当前利用率”列中的红条、橙条或黄条。）

   - 如果是，请打开过载接口的“接口摘要”控制面板，确定流量为什么这么多。请参阅以下部分“查找高带宽主机（接口摘要控制面板）”。
   - 如果否，请点击“主机快照”上的**排名靠前的活动流**选项卡，并查看与该用户关联的数据流的详细信息，从而确定问题的潜在原因。请参阅“检查排名靠前的活动流”（第 174 页）。

查找高带宽主机（接口摘要控制面板）

在查看“接口摘要”中的“导出器接口”选项卡时，如果您看到过载或接近满载的接口（“接口”列中），请双击该接口以打开相关的“接口摘要”控制面板。



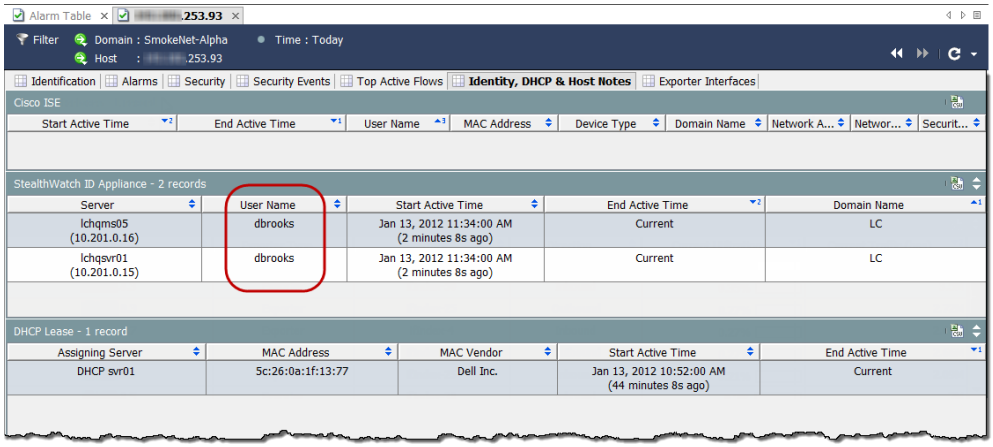
查看该控制面板的右侧，以查看排名靠前的入站和出站对话。识别每个方向占用带宽最大（详见“字节”列）的主机对（主机和对等体）。

要识别登录到其中每个 IP 地址的用户，请打开每个 IP 地址的“主机快照：身份、DHCP 和主机说明”选项卡。请参阅“识别登录高带宽主机的用户”（第 173 页）。

识别登录高带宽主机的用户

在知道使用过多带宽的主机和/或对等体的 IP 地址后，打开该地址的主机快照，然后点击**身份、DHCP 和主机说明**选项卡。

如果登录信息可用，您会看到登录到该 IP 地址的所有用户的用户名。



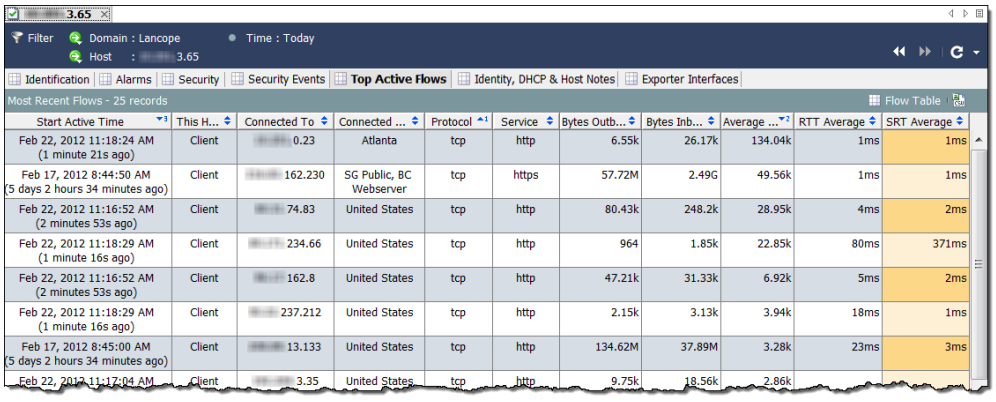
如果没有可用的用户信息，请收集您到目前为止收集到的信息，并根据组织的标准上报程序进行上报。

提示：

如果您拥有 Stealthwatch 身份设备，可以双击用户名以打开“用户身份”文档，并查看与该用户关联的 IP 地址。

检查排名靠前的活动流

主机快照的“排名靠前的活动流”选项卡提供每个 Stealthwatch 设备最近的 25 个数据流以及每个设备流量最高的 25 个数据流的详细信息。



首先，查看 RTT 和 SRT 值。如果 SRT 异常之高，则可以确定问题在于服务器，然后您即可联系服务器团队来解决问题。

如果 SRT 值正常，则问题在于网络中的某个地方，很可能与主机本身有关。在查看“排名靠前的活动流”选项卡时，检查下列问题。这些答案可帮助您确定主机是否被劫持或感染恶意软件，或者用户是否正在参与未经授权的活动。

1. 是否有任何意外连接（例如，未经授权的主机组或服务器）？
2. 是否有大量意外连接？
3. 正在使用哪些服务？
4. 是否正在发送和/或接收大量流量？
5. 是否存在任何高 bps 速率的连接？
6. 主机是否将角色从客户端更改成了服务器？如果工作站突然开始作为服务器运行，它很可能会感染恶意软件或被劫持。

如果无法根据前面问题的答案解决问题，请完成以下步骤：

1. 确保主机的防病毒程序或防火墙没有阻止对有关服务器的访问。
2. 由于主机的防病毒程序可能无法检测恶意软件且可能受到入侵，所以请在主机上使用其他防病毒程序（例如 Malwarebytes 的防恶意软件）运行病毒扫描。
3. 了解主机上是否安装或更新了任何新应用。如果是，请确认该应用的配置是否正确。您可能需要卸载该应用，再重新安装。

如果根据这些建议无法解决问题，请收集您到目前为止收集到的信息，并根据组织的标准上报程序进行上报。

外部查找

“外部查找”功能允许您启动 Web 应用（或内部资源数据库）来查看 IP 地址的更多信息。您可以直接从 Stealthwatch 管理控制台 (SMC) 客户端界面或 SMC Web 应用界面启动此 Web 应用或数据库。

您还可以使用“外部查找”功能来创建快捷方式，以从 SMC 客户端界面快速跳转到 SMC Web 应用界面。

Stealthwatch 系统包括以下默认 Web 应用（查找选项）来配合使用“外部查找”功能；您无需将它们添加到 Stealthwatch 系统：

- 思科 SenderBase
- DShield
- 主机报告

Stealthwatch 系统管理员可以添加以查看 IP 地址更多信息的 Web 应用包括：

- BigFix
- CiscoWorks
- 思科身份服务引擎 (ISE)
- Splunk
- Tripwire
- Ziften

重要：

要添加非默认查找选项，则必须使用 SMC Web 应用界面中的外部查找配置工具。有关如何执行此操作的信息，请参阅“配置外部查找”。

配置外部查找

前面提到，默认情况下包含思科 SenderBase、DShield 和主机名称，以用于外部查找功能；您不必将它们添加到 Stealthwatch 系统。要将其他任何 Web 应用与此功能一起使用，必须将其添加到 Stealthwatch 系统。要执行此操作，请使用 SMC Web 应用界面中的“外部查找配置”工具。

注意：

升级到 v6.7 时，对于先前添加的每个外部查找选项，在 v6.7 中，您将拥有两个选项。Stealthwatch 系统不再使用 webLinks.xml 文件来管理外部查找配置。

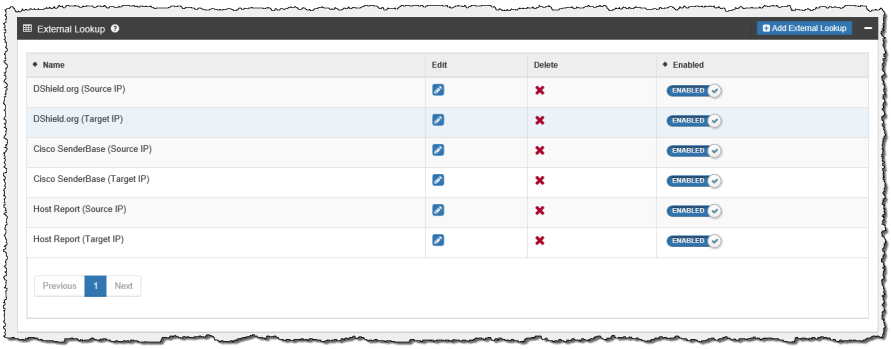
使用此工具，您还可以配置要发送到 Web 应用的特定参数。仅在您配置的参数可用于您在其中执行查找的 IP 地址时，才发送这些参数。

要添加查找选项并配置要发送到 Web 应用的参数，请完成以下步骤：

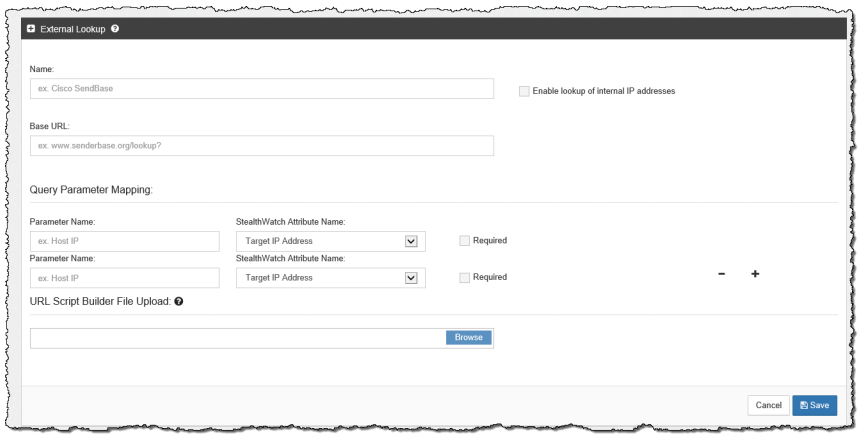
1. 在 SMC Web 应用界面左侧的“导航”窗格中，依次点击**工具 > 设置 > 外部查找配置**。系统随即会打开“外部查找配置”页面。

   要禁用查找选项以使其不可用于外部查找功能 （但保留其配置以供以后使用），请点击适用行中的**启用**。该按钮切换为显示*禁用*状态。

   要在未来启用此查找选项，请点击**禁用**。该按钮切换为显示*启用*状态。



2. 点击**添加外部查找**。系统随即会打开“外部查找”部分。



3. 在本节顶部的下列字段中，键入相应的条目：
   - 名称
   - 基本 URL

4. 要查看 Web 应用中内部 IP 地址的相关信息，请确保选中“启用内部 IP 地址查找”复选框。

5. 在“查询参数映射”部分的第一个 Stealthwatch 属性名称字段中，选择**源 IP 地址**或**目标 IP 地址**。

重要：

对于您添加的任何查找选项，必须配置源 IP 地址或目标 IP 地址。

6. 在相应的“参数名称”字段中，输入 Web 应用的参数名称，该名称用于指定您在上一步所选的 IP 地址。
7. 如果需要，对于要执行查找的 IP 地址配置要发送到 Web 应用的任何其他参数。
   - 目标 IP 地址
   - 目标端口号
   - 源 IP 地址
   - 源端口号
   - 主机名
   - 时间戳 (UTC)
   - 传输协议
   - 用户

   要添加其他参数，请点击第一个配置行末尾的加号 (+)。要删除已配置的行，请点击相应行中的减号 (-)。

注意：

您可以为每个查找选项最多映射 20 个查询参数。

8. 如果您希望在使用特定 Web 应用执行查找时需要使用参数，请选中“必需”复选框。您指定的特定 Web 应用所需的每个参数均必须可用于您在其中执行查找的 IP 地址。如果一个或多个所需参数不可用于相关 IP 地址，则不会在弹出菜单中启用此查找选项。
9. 如果您的查询参数与标准查询参数不匹配，则必须将您自定义的脚本生成器配置上传到“URL 脚本生成器文件上传”字段。

注意：

请确保使用以下脚本示例中突出显示的变量。

脚本生成器文件包含的脚本可将查询参数配置为 Web 应用运行查询所需的 URL 格式。

如果您没有上传脚本生成器文件， Stealthwatch 系统将使用如下所示的默认标准查询参数。

```
BaseURL?[ParameterName1]=[ParameterValue1]&
ParameterName2]=[ParameterValue2]&
ParameterName3]=[ParameterValue3] (and so on for
each parameter you add)
```

URL 和脚本示例

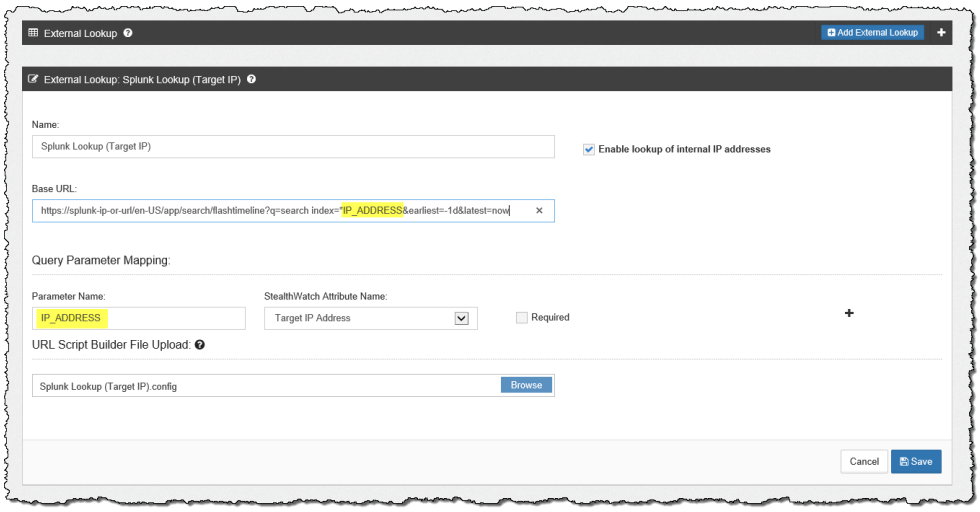
示例 1

使用以下 URL 和脚本示例的 Web 应用使用没有参数名称的值 （例如，Splunk）。

```
https://splunk-ip-or-url/en-US/app/search/flash-timeline
?q=search index=* 192.10.20.43 &earliest=-1d&latest=now
```

```
def String query = baseUrl;
def String url = baseUrl;

vendorValues.each { valueOperand ->

    if (url.indexOf(valueOperand.getName()) != -1) {
        def String convertedStr = "";
        if (valueOperand.getFromValue() instanceof String || valueOperand.getFromValue() instanceof Integer) {
            convertedStr = valueOperand.getFromValue().toString();
        } else if (valueOperand.getFromValue() instanceof Date) {
            convertedStr = new SimpleDateFormat("yyyy-MM-dd'T'HH:mm:ss").format(valueOperand.getFromValue().time);
        }
        if (query.indexOf(valueOperand.getName()) != -1) {
            String[] parts = query.split(valueOperand.getName());
            query = "";
            def int i = 0;

            parts.each { part ->
                if (i + 1 < parts.length) {
                    query = query + part + URLEncoder.encode(convertedStr,"UTF-8");
                } else {
                    query = query + part;
                }

                i += 1;
            }

            if (url.endsWith(valueOperand.getName())) {
                query += URLEncoder.encode(convertedStr,"UTF-8");
            }
            url = query;
        }
    }
};

return query;
```

为了生成脚本，从而将查询参数配置为先前在此示例中所示的 URL 格式，请使用下图中突出显示的 “ 参数名称 ” 字段条目。



注意：

您可以根据需求配置多个属性；然而，请确保配置相同数量的参数。

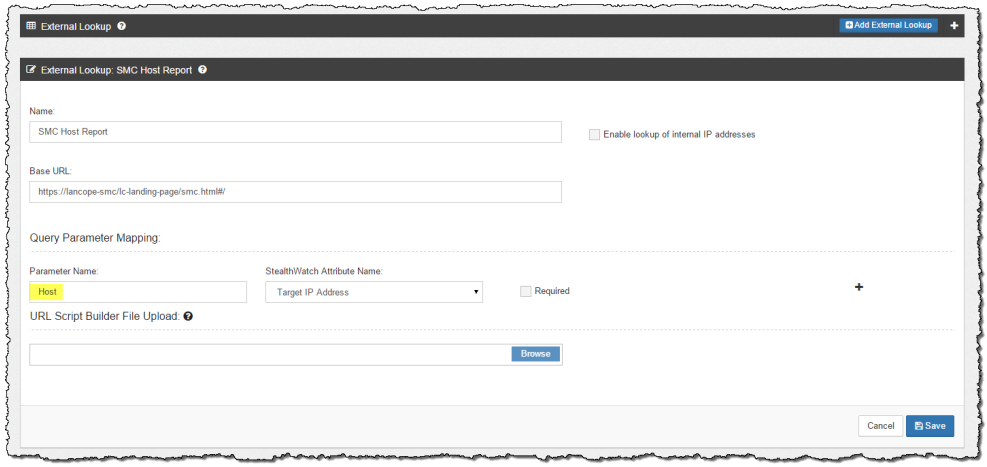
示例 2

使用以下 URL 和脚本示例的 Web 应用使用类似 REST 的路径参数 （例如， Stealthwatch 主机报告）。

```
https://lancope-smc/lc-landing-page/smc.html#/host
/172.21.114.17
```

```
def String query = "";

vendorValues.each { valueOperand ->

    query += valueOperand.getName() + "/";
    def String convertedStr = "";
    if (valueOperand.getFromValue() instanceof String || valueOperand.getFromValue() instanceof Integer) {
        convertedStr = valueOperand.getFromValue().toString();
    } else if (valueOperand.getFromValue() instanceof Date) {
        convertedStr = new SimpleDateFormat("yyyy-MM-dd'T'HH:mm:ss").format(valueOperand.getFromValue().time);
    }
    String.valueOf('java.lang.Integer');
    query += URLEncoder.encode(convertedStr,"UTF-8");
};

def char lastChar = baseUrl.charAt(baseUrl.length() - 1);
if (lastChar != '?' && lastChar != '/' && lastChar != '&') {
    baseUrl = baseUrl + "?";
};

query = baseUrl + query;
return query;
```

为了生成脚本，从而将查询参数配置为先前在此示例中所示的 URL 格式，请使用下图中突出显示的 “ 参数名称 ” 字段条目。



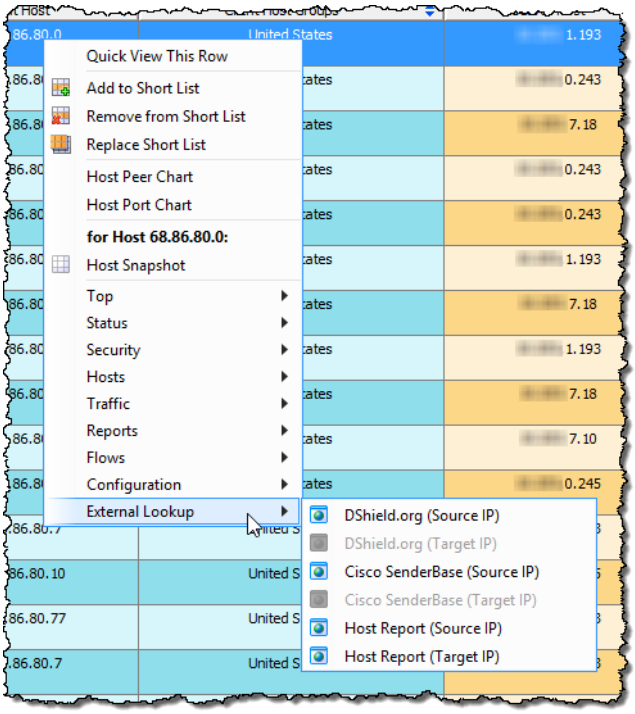
10. 完成后，点击**保存**。您将返回“外部查找”部分。您刚才添加的查找选项现在显示在列表中，默认为启用状态（它可用于外部查找功能)。

执行外部查找

要查询 Web 应用以查看有关 IP 地址的其他信息，请完成以下步骤：

1. 执行以下操作之一：
   - 如果您位于 SMC 客户端界面，请转到步骤 2。
   - 如果您位于 SMC Web 应用界面，请转到步骤 3。
2. 请完成以下步骤：
   a. 在 SMC 客户端界面中，打开包含相关 IP 地址的任何文档。
   b. 右键点击该 IP 地址。

c. 在显示的弹出菜单中，点击**外部查找**。系统将显示二级弹出菜单。

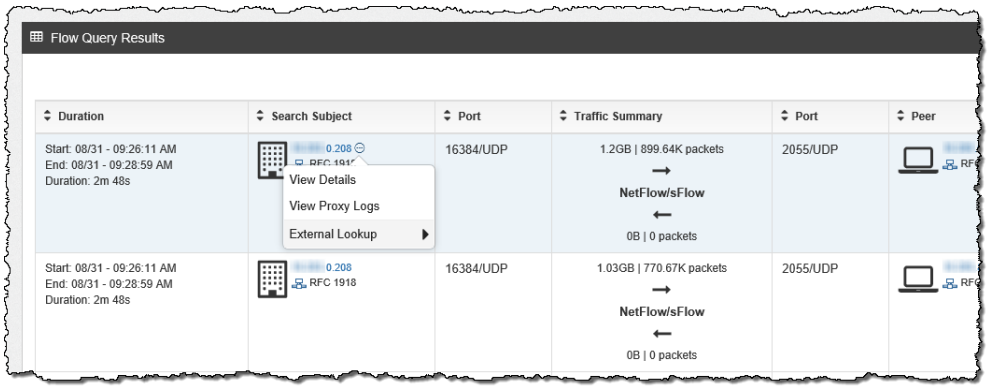


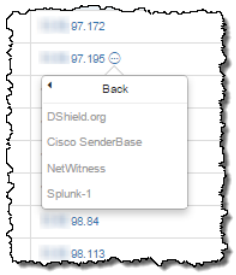
3. 请完成以下步骤：

a. 在 SMC Web 应用界面中，打开“标准流查询结果”页面或“高级流查询结果”页面。

b. 在“搜索主题”列或“对等体”列，将鼠标悬停在该 IP 地址的上方，然后点击省略号。

c. 在显示的弹出菜单中，点击**外部查找**。系统将显示二级弹出菜单。

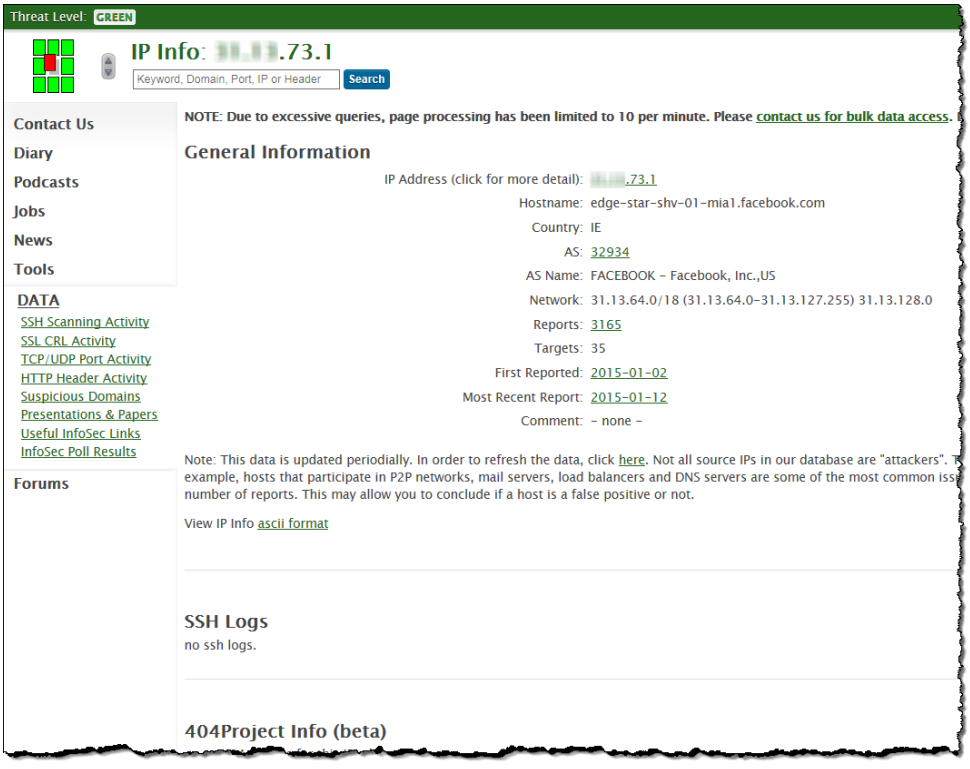




4. 从步骤 3 中显示的辅助弹出菜单中点击所需查找选项。您选择的查找选项的 Web 应用将打开（系统可能会提示您登录到 Web 应用），并且显示正在执行查找的 IP 地址的查询结果。

   您指定的特定 Web 应用所需的每个参数均必须可用于您在其中执行查找的 IP 地址。如果一个或多个所需参数不可用于相关 IP 地址，则不会在弹出菜单中启用此查找选项。有关详细信息，请参阅第 194 页上的 “ 配置供应商 ”。

   下面是对于使用 DShield Web 应用的查询返回的信息示例。



9

SLIC 威胁源服务

概述

Stealthwatch Labs Intelligence Center (SLIC) 威胁源是 Lancope 提供的一项服务，向您的网络提供有关威胁的最新信息，而且这些信息会频繁更新。SLIC 威胁源提供有关恶意软件命令和控制 (C&C) 服务器及其他感兴趣的主机（例如 bogons、Tor）的数据，Stealthwatch 用这些数据可快速、准确地识别有害网络活动。

本章包含以下主题：

关于 SLIC 威胁源

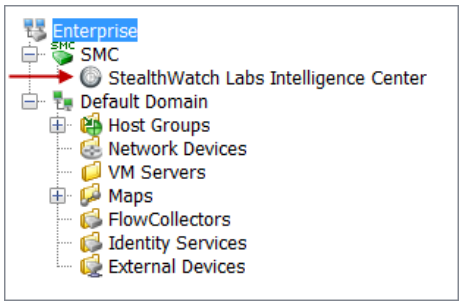
SLIC 威胁源是 Lancope 的研究活动，Lancope 通过该活动向客户及广大公众提供有关互联网热门威胁的全球情报信息。Lancope 的研究小组（称为 StealthLabs）通过内部研究，同时利用第三方专家和合作伙伴构成的广大社区，整合来自世界各地的最新威胁信息。

StealthLabs 研究团队的成员作为产品开发人员、安全研究人员、创作者及公共演讲者，拥有几十年的综合经验，走在计算机安全领域的前沿。SLIC 威胁源提供研究团队成员的演讲和网络研讨会的链接以及一个公共博客，其中讨论和解析了计算机安全威胁领域的最新发展情况。此外，您还可以查看 C&C、扫描和 DDoS 活动图，甚至可与 Lancope 代表实时聊天。

您可以访问 SLIC 网站，了解有关 SLIC 威胁源的更多信息。要访问此网站，请执行以下操作之一：

- 在浏览器中键入 http://www.lancope.com/slic。
- 右键点击企业树中的 StealthLabs Intelligence Center 分支，然后依次选择**配置 > StealthLabs Intelligence Center**。

企业树中的 SLIC 图标（由右侧图像中的箭头指示）会根据 SLIC 威胁源是否启用以及是否有活动警报而改变颜色。有关准则，请参阅以下列表：



- 如果 SLIC 威胁源被禁用，则该图标为灰色。（在右侧图像中，该图标显示为禁用模式。）
- 如果 SLIC 威胁源被启用且无活动警报，则该图标为绿色。
- 如果 SLIC 威胁源被启用且有“SLIC 通道关闭”(SLIC Channel Down) 警报，则该图标为灰色且底部显示 X。如果没有其他活动警报，则 SMC 图标的颜色会变为橙色。如果当前存在其他警报，则图标颜色与严重性最高的警报对应。

必备条件

SLIC 威胁源必须先满足以下条件方可运行：

- SMC 设备必须连接互联网，并且能够与 SLIC 服务器通信。
- 必须在 SMC 设备上配置 DNS 服务器。
- 如果您的网络使用互联网代理，则必须在 SMC 设备上配置代理服务器。

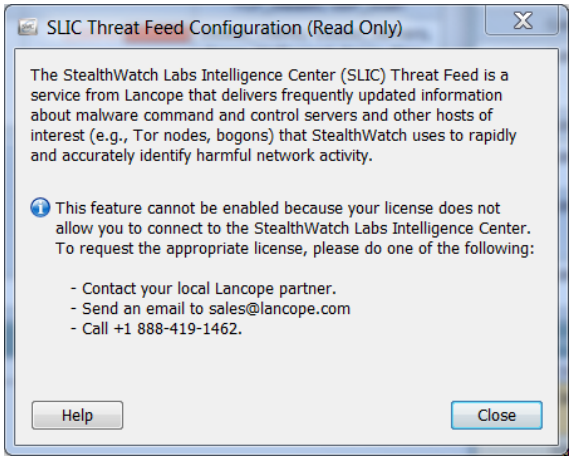
注意：

威胁源可通过代理服务器连接到互联网。如果需要通过代理服务器访问互联网，请打开“设备管理（管理员）”界面，然后依次点击**配置 > 服务**，以配置代理服务器。有关更多信息，请参阅《*Stealthwatch 系统硬件配置指南*》、适用设备的配置指南或设备管理联机帮助。

- 必须在 SMC 客户端界面中启用 SLIC 威胁源。
- SMC 许可证必须包括 SLIC 威胁源。

当许可证有效期剩余 15 天时，系统开始显示警告对话框，直到许可证过期。许可证过期后，将出现以下情况：

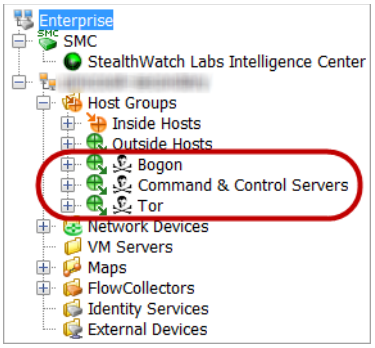
- SMC 禁用 SLIC 威胁源。
- 企业树中的 Bogon、命令和控制服务器以及 Tor 主机组分支变暗，SLIC 威胁源不再提供动态信息（源）。
- SMC 客户端界面显示一条消息，指出由于许可证不允许连接到 SLIC 威胁源，无法启用此功能。



SLIC 威胁源的运行方式

以下是启用 SLIC 威胁源时发生的事件顺序：

1. SLIC 威胁源可将已识别的威胁列表下载到 SMC。它们显示在企业树中各自的主机组分支内，如右侧图中所示。
2. SMC 会将此列表分发到系统中的每个流量收集器。
3. 流量收集器在监控网络中的主机时会使用这些信息。
4. 如果流量收集器检测到网络中的主机与 SLIC 威胁源中的威胁主机进行通信，则会触发安全事件。



注意：

有关这些安全事件可触发的警报（如果进行了相应的配置）以及引发每个警报之前必须满足的条件的信息，请参阅“SLIC 安全事件”（第 193 页）。

5. 如果在 SMC 中已启用 SLIC 威胁源，但是 SMC 服务器无法从 SLIC 威胁源检索数据，则会触发“SLIC 通道关闭”警报。企业树中的 SLIC 图标将变为灰色，并且在该图标的底部会显示 X。

   当存在以下两种情况中任意一种情况时，系统会清除此警报：

   - SMC 服务器再次开始从 SLIC 威胁源检索数据。
   - 禁用 SLIC 威胁源。

SLIC 威胁源主机组

注意：

“SLIC 威胁源”主机组分支无法重命名、更改、移动或删除。

SLIC 威胁源包含已知用于恶意活动的 IP 地址、端口号、协议、主机名和 URL。以下主机组包括在“SLIC 威胁源”中：

- Bogon - Bogon 是尚未正式分配到公共网络中的 IP 地址。
- 命令和控制服务器 - C&C 服务器是向僵尸网络发布命令并从被劫持计算机接收报告的中央计算机。
- Tor - Tor 是一种互联网匿名化服务。

注意：

要检测 SLIC 服务器源中可能正在与您的主机通信的 URL，您必须安装配置为导出 IPFIX（相对 NetFlow）的 FlowSensor 或路由器。（默认情况下，FlowSensor 已配置为导出 IPFIX。）

如果您希望调查已与上述某个主机组中的恶意主机通信的主机，但恶意主机不再显示于相关主机组中时，请转至“警报表”并按以下组件过滤：

- 类型 - 根据您要过滤的恶意主机的类型，选择适用的 Bogon、命令和控制或 Tor 警报。
- 日期/时间 - 根据您要调查的时间段进行过滤。

启用 SLIC 威胁源

在使用 SLIC 威胁源之前，必须访问“下载和许可证中心”以激活 SLIC 威胁源许可证。有关如何执行此操作的信息，请参阅第 2 章“许可 Stealthwatch 设备。”

第一次启用 SLIC 威胁源时，必须输入 SLIC 威胁源密钥。在客户购买 SLIC 威胁源功能后，Lancope 会以电子邮件形式发送 SLIC 威胁源密钥。只有具有管理员权限的用户才能输入 SLIC 威胁源密钥，以及启用或禁用 SLIC 威胁源。

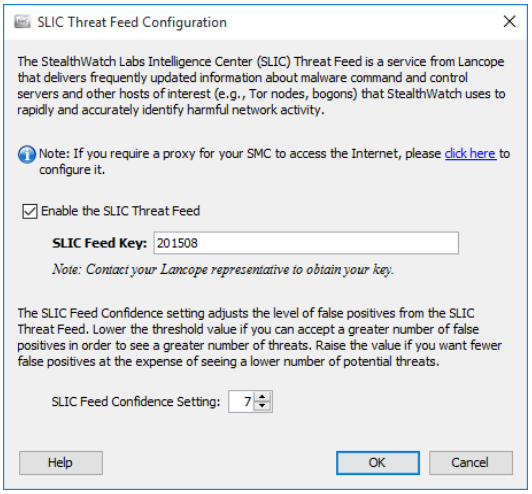
要启用 SLIC 威胁源，请完成以下步骤：

1. SMC 访问互联网是否需要使用代理？
   - 如果是，请转到“SMC 设备管理”界面并配置代理（**配置 > 服务**）。
   - 如果否，请转至步骤 2。

注意：
有关更多信息，请参阅《*Stealthwatch 系统硬件配置指南*》、适用设备的配置指南或*设备管理联机帮助*。

2. 在 SMC 客户端界面的企业树中，右键点击“StealthLabs Intelligence Center”分支，然后依次选择**配置 > SLIC 威胁源配置**。

   系统随即会打开“SLIC 威胁源配置”对话框。



注意：
如果未获得 SLIC 威胁源功能许可，则不会显示“SLIC 威胁源配置”对话框。相反，您会收到一条消息，指出您未获得此功能的许可。

3. 选中“启用 SLIC 威胁源”复选框。
4. 这是您第一次启用 SLIC 威胁源吗？

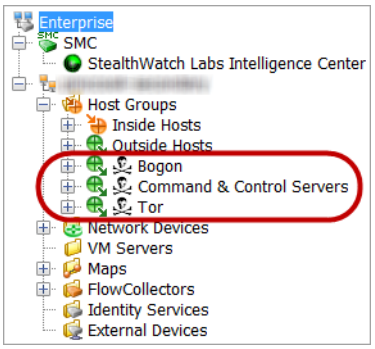
- 如果是，请在“SLIC 威胁源密钥”字段中输入您的 SLIC 威胁源密钥。
- 如果否，请转至步骤 5。

5. 如果需要，请更改 SLIC 源置信度设置。通过调整 SLIC 源置信度设置，可以选择 Stealthwatch 在与 SLIC 威胁源上的主机相匹配时将需要的置信度阈值。

   如果您可以接受更多数量的误报以查看更多数量的威胁，请降低阈值（更低的值表示更低的置信度评级）。如果您想要的更少的误报，从而查看更低数量的潜在威胁，请提高该值。默认情况下，该值设置为 7。

6. 点击**确定**。企业树中随即会显示以下主机组分支：

   - Bogon
   - 命令和控制服务器
   - Tor



注意：

点击**确定**后，这些列表可能需要一分钟才会显示在树中。

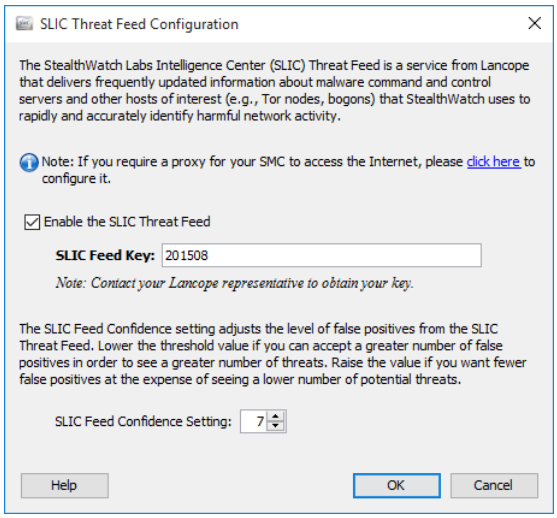
禁用 SLIC 威胁源

只有获有管理权限的用户才能禁用 SLIC 威胁源。

要禁用 SLIC 威胁源，请完成以下步骤：

1. 在企业树中，右键点击 StealthLabs Intelligence Center 分支，然后依次选择**配置 > SLIC 威胁源配置**。

   系统随即会显示“SLIC 威胁源配置”对话框。



2. 选中“启用 SLIC 威胁源”复选框将其清除。“SLIC 威胁源密钥”字段中的条目会变暗。

注意：

如果将来要选择启用 SLIC 威胁源，只需点击“启用 SLIC 威胁源”复选框即可添加选中标记。无需重新输入 SLIC 威胁源密钥。

3. 点击**确定**。

SLIC 安全事件

本节介绍 SLIC 威胁源中的威胁主机可触发的安全事件。如果进行相应配置，则这其中每个安全事件将在 SMC 客户端界面中触发警报。（可以在 SMC 客户端界面的“主机策略管理器”中进行配置。）这些事件触发后，系统会将其显示在 SMC 客户端界面的“警报表”中。

根据流量收集器检测到的内容和 SMC 的配置，以下安全事件可能触发警报：

安全事件	说明
感染僵尸病毒的主机 - 尝试执行 C&C 活动	此警报表示网络中的某个主机尝试与 C&C 服务器列表中显示的某个 C&C 服务器通信，因此现在是僵尸网络的成员。通信是单向的。 作为启动程序的内部主机会累计关注指数 (CI) 点。如果它尝试联系的 C&C 服务器也是内部主机，则该 C&C 服务器会累计目标指数 (TI) 点。有关这些指数的详细信息，请参阅第 6 章“指数：行为变化排行榜”。
感染僵尸病毒的主机 - 成功执行 C&C 活动	此警报表示网络中的某个主机尝试与 C&C 服务器列表中显示的某个 C&C 服务器通信，并已收到响应，因此现在是僵尸网络的成员。该 C&C 服务器可能在您的网络内部或外部。通信是双向的。 作为启动程序的内部主机会累计 CI 点。如果它执行通信的 C&C 服务器也是内部主机，则该 C&C 服务器会累计 TI 点。
僵尸命令和控制服务器	此警报表示网络中的某个主机正在作为僵尸网络的 C&C 服务器运行。当您的网络中的内部主机与被 SLIC 威胁源识别为 C&C 服务器的 IP 地址匹配时，会触发此警报。此警报仅识别源 IP 地址。未识别目标。
尝试从 Bogon 地址连接	查找外部 Bogon 主机尝试与网络中的主机服务器通信失败的实例。Bogon 前缀是不应在互联网路由表中出现的路由。
成功从 Bogon 地址连接	查找外部 Bogon 主机（充当客户端）成功与网络中的主机服务器通信的实例。Bogon 前缀是不应在互联网路由表中出现的路由。
尝试从 Tor 连接	有人尝试从当前 Tor 网络出口节点与您连接失败。Tor 是一种互联网匿名化服务。
从 Tor 连接成功	您网络中的一个或多个主机正在接收来自当前 Tor 网络出口节点的流量。Tor 是一种互联网匿名化服务。
尝试连接到 Bogon 地址	查找网络内部的主机尝试与外部 Bogon 通信失败的实例。Bogon 前缀是不应在互联网路由表中出现的路由。
成功连接到 Bogon 地址	查找网络内部主机与外部 Bogon IP 地址（未分配到公共网络中的 IP 地址）之间的双向流量实例，并提示已发生通信。Bogon 前缀是不应在互联网路由表中出现的路由。

安全事件	说明
尝试连接到 Tor	您的一个活动内部主机尝试连接到当前 Tor 网络入口节点失败。Tor 是一种互联网匿名化服务。
成功连接到 Tor	您网络中的一个或多个主机正在将流量发送到 Tor 网络。Tor 是一种互联网匿名化服务。
检测到从内部主机连接到 Tor 入口节点	您的一个活动内部主机正在充当 Tor 入口节点。Tor 是一种互联网匿名化服务。
检测到从 Tor 出口节点连接到内部主机	您的一个活跃的内部主机正在充当 Tor 出口节点。Tor 是一种互联网匿名化服务。

注意：

有关这些警报的其他信息，请参阅 *SMC 客户端联机帮助*中的“警报列表”主题。

10

发现原因

概述

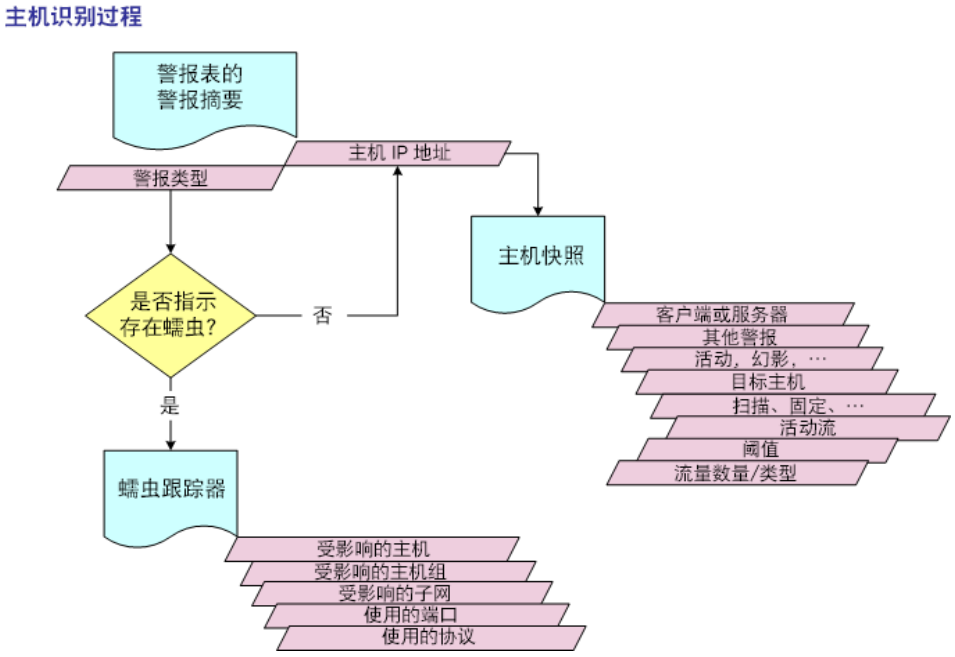
您已学过，处理威胁的第一步是找到引发警报的主机（即“源主机”）。本章介绍如何使用 SMC 收集有关源主机的信息，以便您可以对威胁处理方式作出明智的决策。

本章包含以下主题：

- 标识流程
- 警报摘要
- 警报表
- 全局搜索
- 从主机快照中获取详细信息
- 行为是否正常？
- 哪些主机有相同的特征?

标识流程

有时，评估如何处理警报条件就像定位源主机的 IP 地址一样简单。但是，在其他情况下，还需要更多有关主机和警报的信息。无论哪种情况，“警报摘要”和“警报表”对于评估都必不可少。下图说明了尝试识别可疑主机时要遵循的流程：



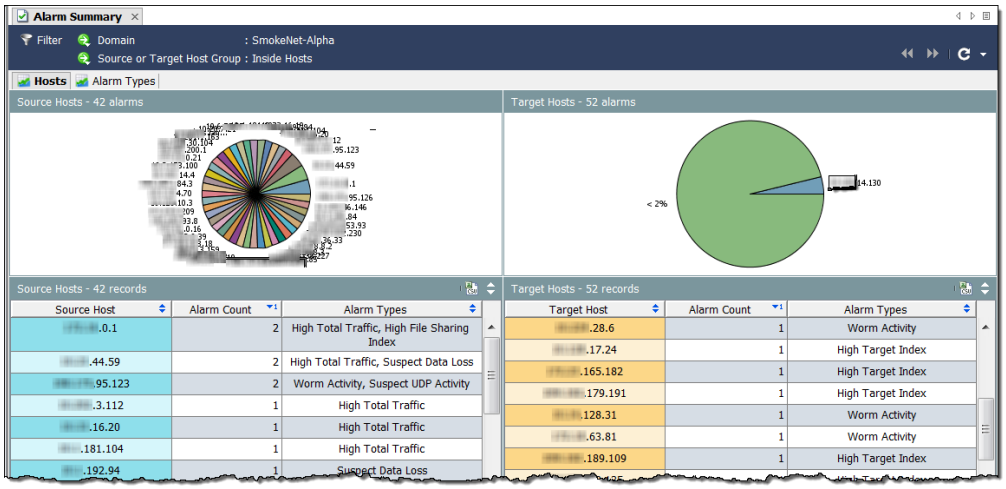
注意：

记录已引发过网络故障的主机，以便您可以轻松确定是否属于“重施故技”。

警报摘要

识别主机的最简单方法可能是使用“警报摘要”。要打开此文档，请右键点击域、导出器或 FlowSensor, 然后从弹出菜单中依次选择**状态 > 警报摘要**。

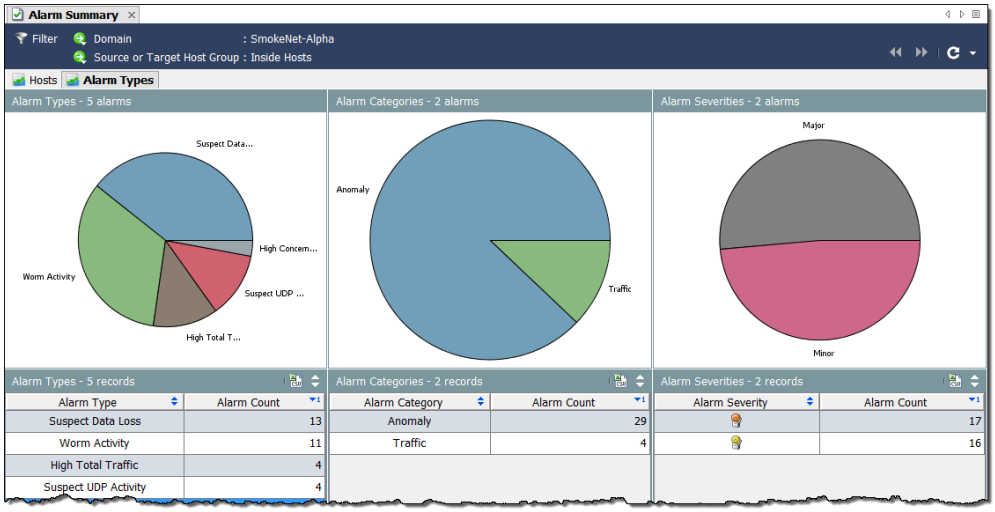
在这里，您可以看到按图形方式表示的所有网络警报，它们按类型、类别、严重性级别、源主机 IP 地址和目标主机 IP 地址进行细分。在以下示例中，您可以在“主机”选项卡上轻松查看源主机的 IP 地址。



要浏览此文档，可以执行以下任何操作：

- 要查看“主机快照”，请双击“主机”选项卡上的某个主机 IP 地址。
- 要获取“警报表”的过滤视图，请双击**警报计数**或**警报类型**列。

点击**警报类型**选项卡查看不同的视图。



要浏览此文档，可以执行以下任何操作：

- 要获取“警报表”的过滤视图，请双击“警报类型”选项卡上的某个图表或表项。
- 要显示预过滤的警报表以仅显示与该项相关的警报，请双击一列或饼图中的某项。

  例如，如果双击“警报类型”列中的**高关注指数**警报，则“警报表”仅显示“高关注指数”警报。

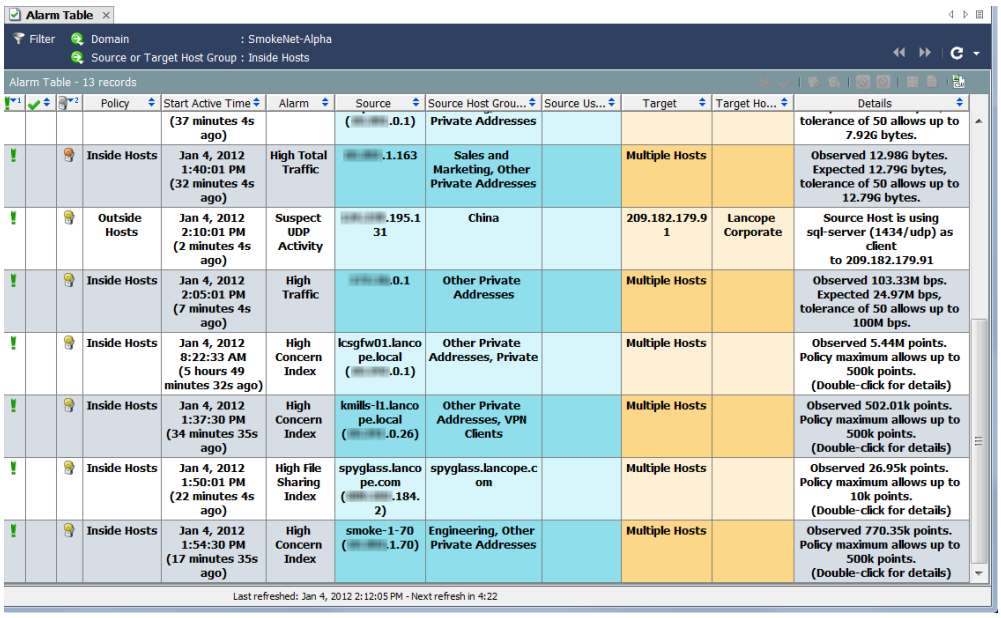
注意：

有关每个警报的说明，请参阅 *SMC 客户端联机帮助*。

警报表

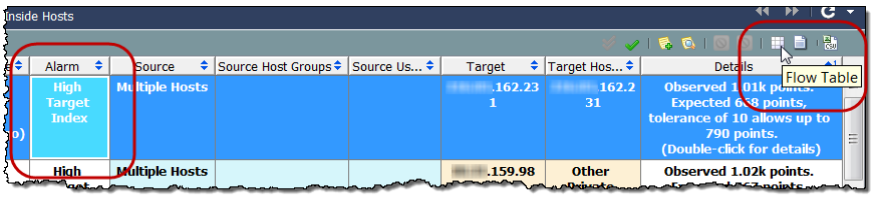
当您需要有关警报的详细信息时，请转到“警报表”。要打开此文档，请右键点击域、Stealthwatch 流量收集器、主机组、导出器或 FlowSensor, 然后从弹出菜单中依次选择**状态 > 警报表**。

“警报表”可帮助您回答以下问题：“什么问题引发了警报？”和“问题严重性如何？”默认情况下，“警报表”显示自生成警报的 Stealthwatch 流量收集器上次存档后发生的所有活动警报。



“警报表”与大多数 SMC 文档一样，显示与打开文档的级别相应的数据。例如，如果您在域级别打开“警报表”，则它显示的警报与整个域相关。如果在主机组级别打开“警报表”，则它显示的警报仅与该主机组及其从属主机组相关。

除查看警报之外，通过“警报表”还可以确认、关闭警报和添加警报注释（取决于您的登录权限）。您可以点击某个警报，然后点击**流表**按钮以显示与该警报关联的所有流的流表。

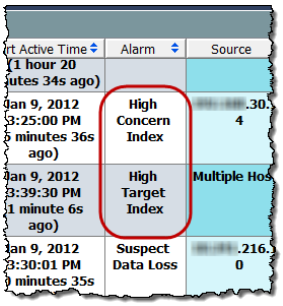


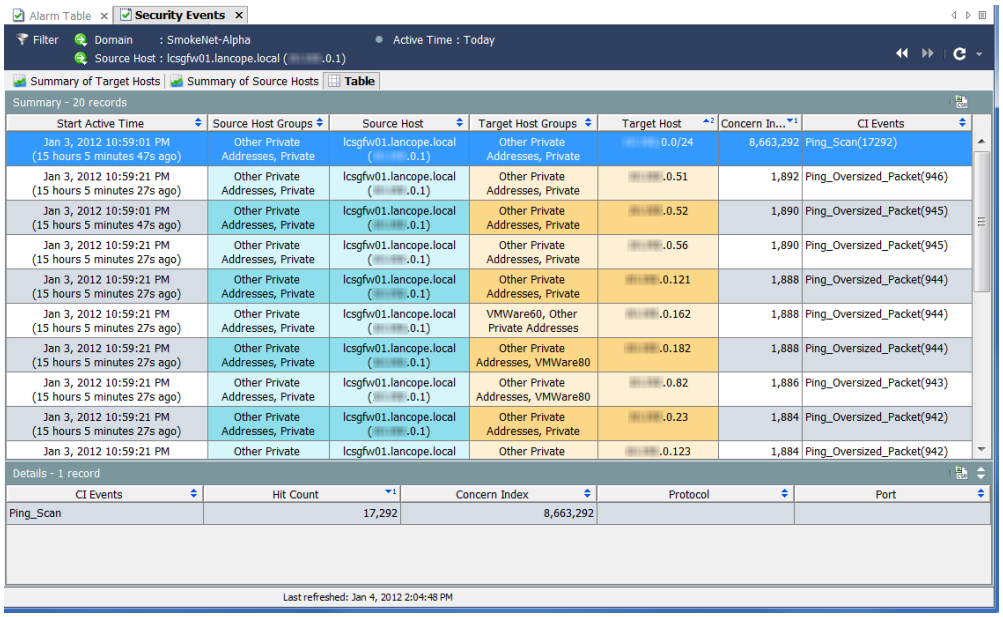
只要引起警报的条件仍然存在，该警报就保持活动状态。然后，警报变为非活动状态，这时您可以关闭该警报（如需要）。您可以确认活动警报，但不可以关闭活动警报。您只能关闭非活动警报。

“警报表”的另一优点是，允许您执行以下操作：

- 确认/取消确认警报
- 附加/查看警报注释
- 阻止或取消阻止主机（例如，警报缓解）

双击“警报表”中的某个“高关注指数”警报或“高目标指数”警报时，系统会显示“安全事件”文档，如以下示例中所示。此文档显示引发警报的安全事件数据。





注意：

有关响应警报的详细信息，请参阅第 11 章“响应警报。”

全局搜索

全局搜索功能允许您在其所有文档中（所有域范围内）搜索某些项目。在主工具栏上的“搜索”字段中，可以使用完整字符串、部分字符串或带有通配符 (*) 的部分字符串搜索以下项目：

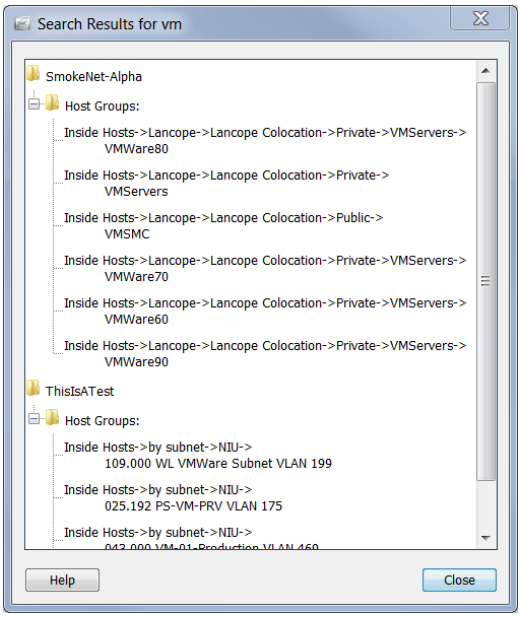
- 警报 ID
- 主机或导出器 IP 地址
- 以下名称：
  - 导出器
  - 主机组
  - 服务器
  - 用户
  - VM
  - VM 服务器

注意：
系统会根据与您的用户名关联的数据角色和功能角色而限制搜索结果。

提示：
您可以使用“搜索”下拉列表框来选择先前已搜索的项目，然后按 **Enter** 键来执行搜索。

要执行搜索，请在工具栏“全局搜索”框内点击。

键入搜索项目，然后按 **Enter**。系统随即会打开“搜索结果”对话框。

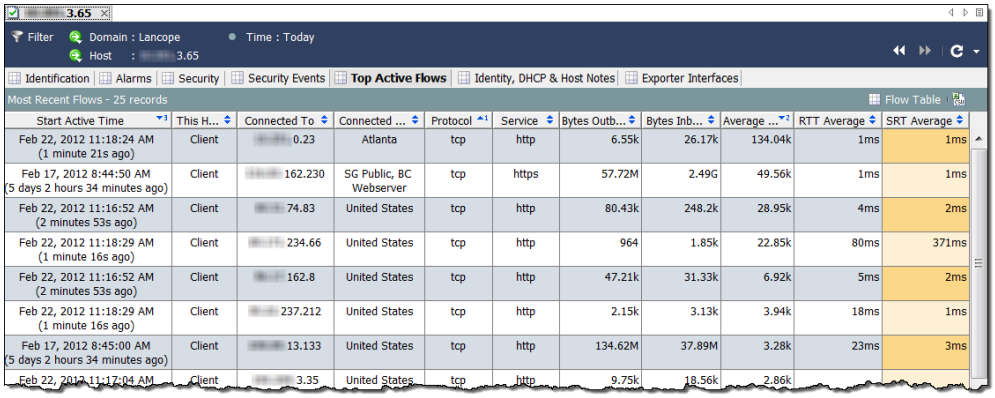


执行以下操作之一：

- 双击搜索结果。
- 右击搜索结果，然后从弹出菜单中选择所需项目。

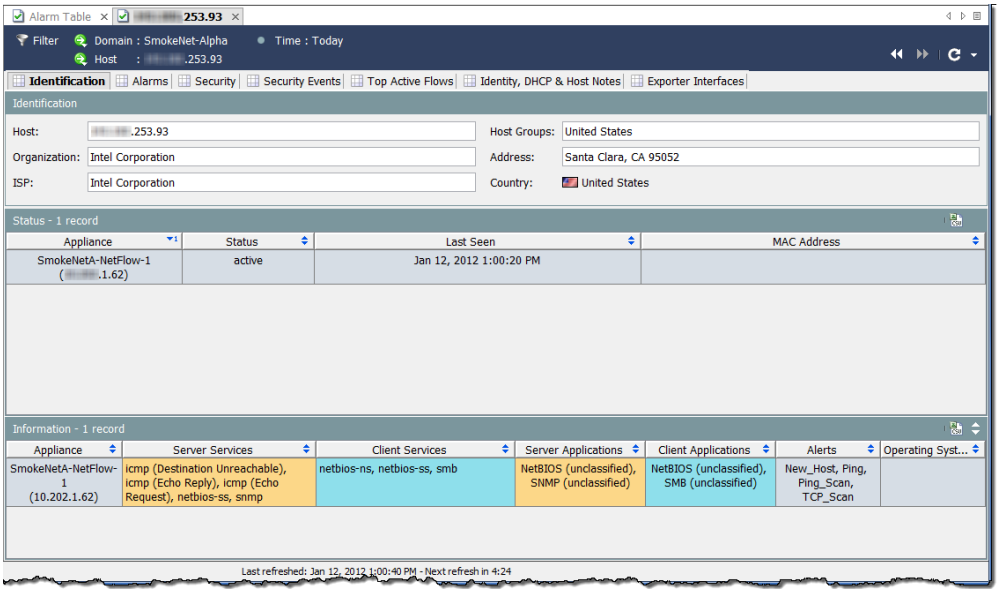
从主机快照中获取详细信息

在调查主机行为的变化时，第一站通常是查看“主机快照”文档。此文档提供网络中每个主机的最全面信息。



在大多数情况下，只需双击 SMC 客户端界面任何位置的主机 IP 地址，即可查看该主机的主机快照。“主机快照”包括以下信息：

- 与该主机相关的最近流。
- 到目前为止流量最高的流。
- 已登录到该主机的任何人的用户名。
- 与该主机相关的所有警报。
- 传输流的导出器接口。
- 该主机 IP 地址被分配到的组织以及地址和互联网服务提供商 (ISP)（如果适用）。
- 该主机的状态以及上次被看到进行网络通信的时间。
- 该主机的服务器/客户端配置文件和操作系统 (OS)，以及与该主机相关的任何风险通告。

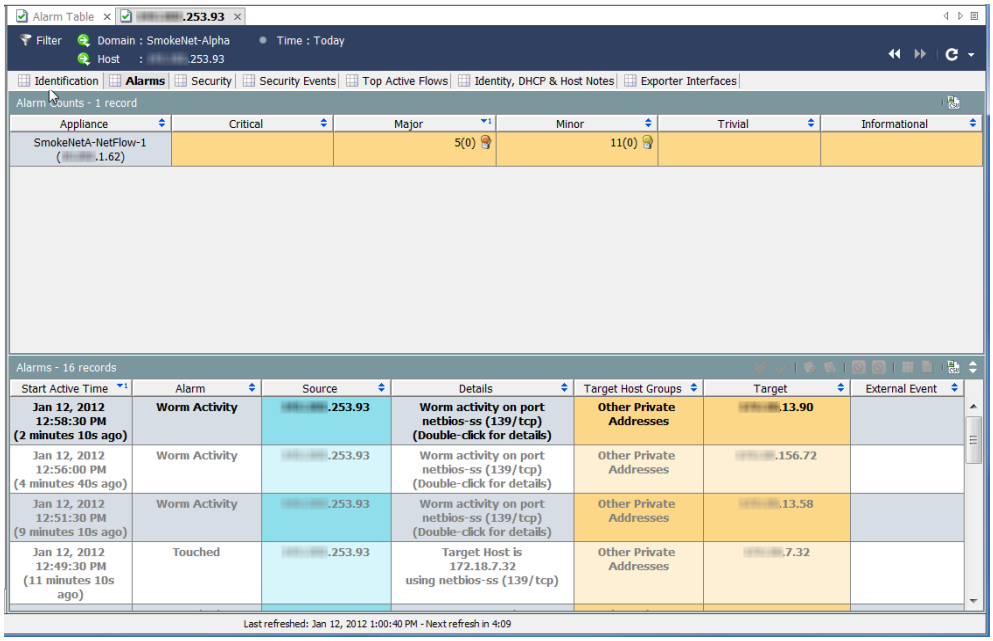


在前面示例中，我们可以在“标识”选项卡上查看有关所选主机的以下信息：

- 该主机有一个专用 IP 地址。
- 系统最后一次看到该主机活动是在 2012 年 1 月 12 日。
- 系统报告称，除许多其他服务之外，该主机还同时作为服务器和客户端发生了 netbios 流量。

主机是否引发了其他警报？

“主机快照”上的“警报”选项卡指示有关主机是否生成了其他警报以及生成的警报数量和类型（如果已生成）。



主机引发的警报越多，您的关注程度越高。请记住，严重性级别是可配置的，所以可以根据您的特定情况调整它们。

在前面示例中，我们了解了有关所选主机的以下信息：

- “警报计数”表按警报类型和类别显示由所选主机引发的警报数，具体警报由相应的 Stealthwatch 设备报告。在本例中，Stealthwatch 设备报告了 11 个轻微警报条件和 5 个重要警报条件。

注意：

可以右键点击列标题，选择要在表中显示的特定警报类型列。

- “警报”表显示自上次存档后由所选主机生成的各个警报的详细数据。在本例中，我们看到该主机生成了几个“蠕虫活动”警报。

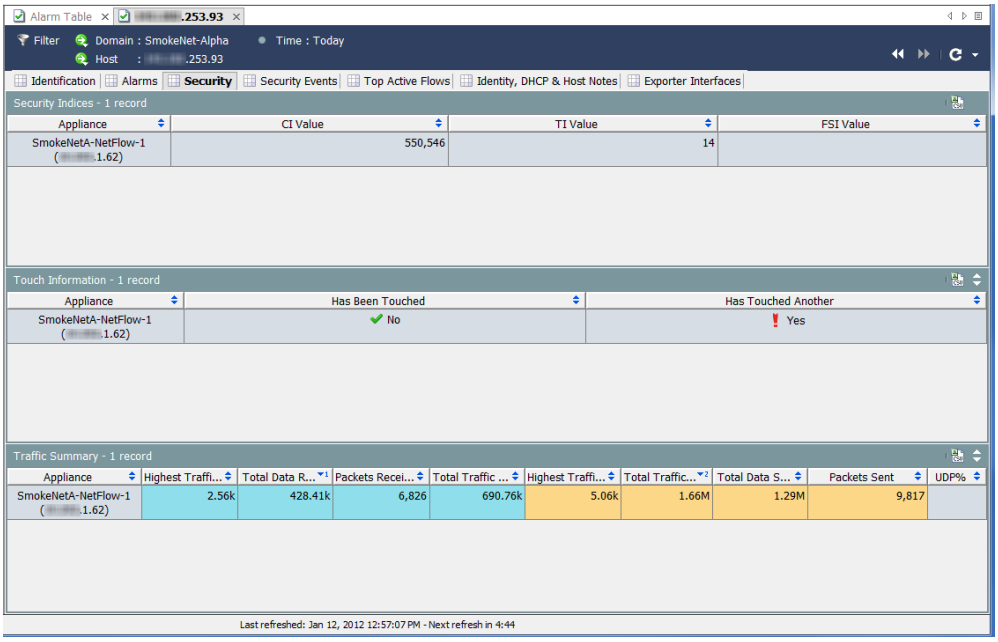
注意：

可以打开“主机策略管理器”查看和/或调整为这些值建立的策略设置。

由于我们怀疑此主机可能被感染，所以下一步就要确定感染源以及受影响的主机数。

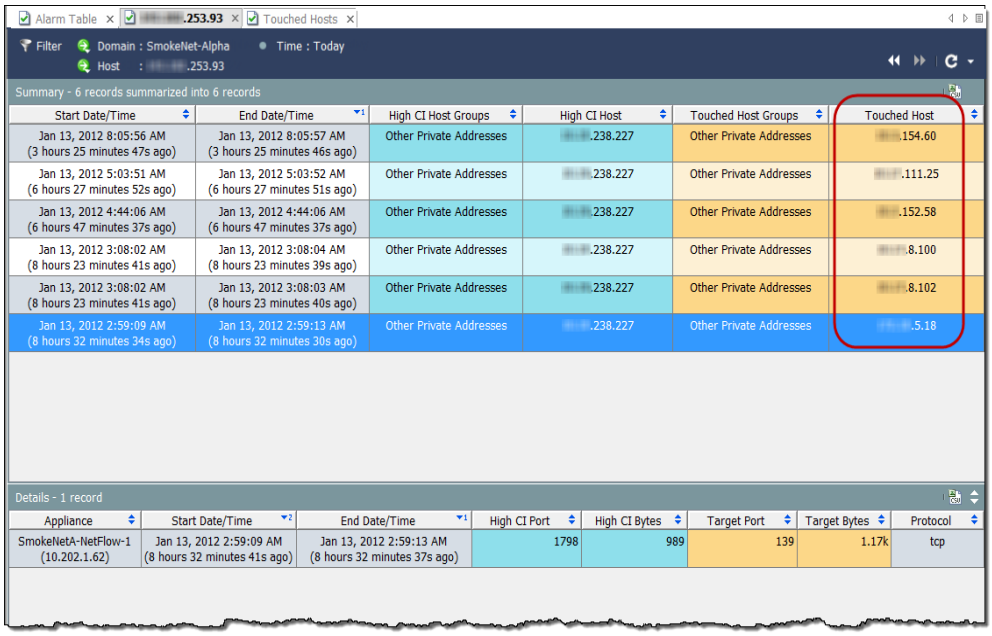
威胁的影响范围怎样？

无论是否指示蠕虫，您都可以转到“主机快照”的“安全”选项卡（如以下示例中所示），查看有关主机是否已触及其他主机或被其他主机触及。“触及信息”表可帮助您确定该主机的威胁是否源自其他地方，以及该主机是否已将威胁传播给其他主机。



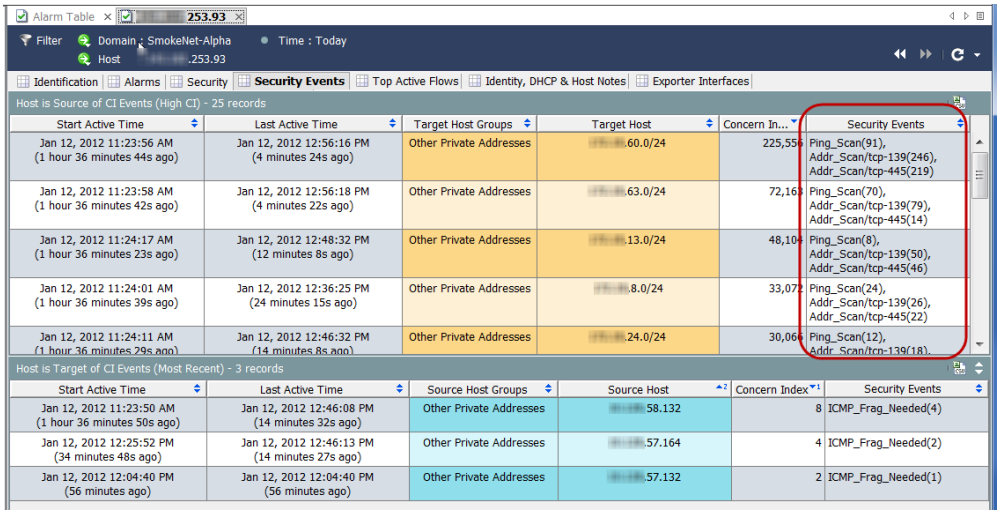
此外，“安全指数”表还显示了该主机超出每个 Stealthwatch 设备的各种指数限值的程度。“流量摘要”表显示该主机发送和/或接收的流量数量，这些信息有助于确定文件共享活动。

在前面示例中，我们需要了解该主机所触及的其他主机数。要执行此操作，我们需转到**已触及其他**列，然后双击**是**。系统随即会打开“已触及主机”文档。在“已触及主机”列中，我们可以看到该高 CI 主机至少已触及目标主机六次。

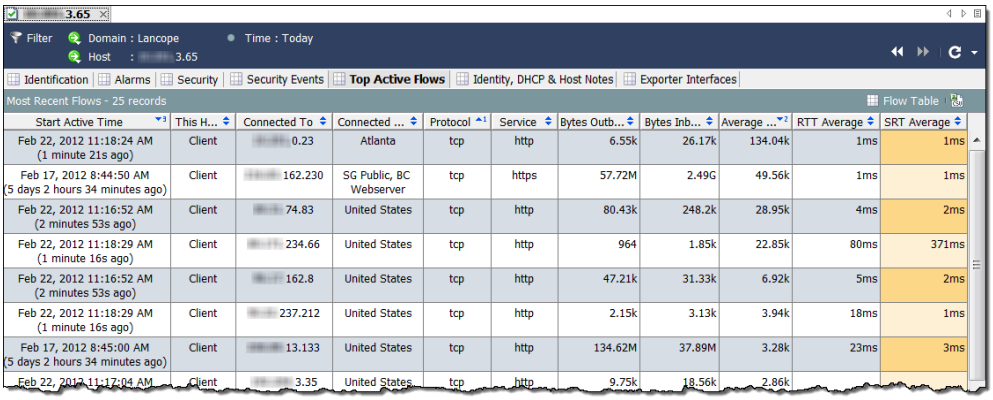


选择上表中的一行，可以在底部的“详细信息”部分看到更详细的信息，例如高 CI 端口和字节数、目标端口和字节数以及用于受影响主机的协议。

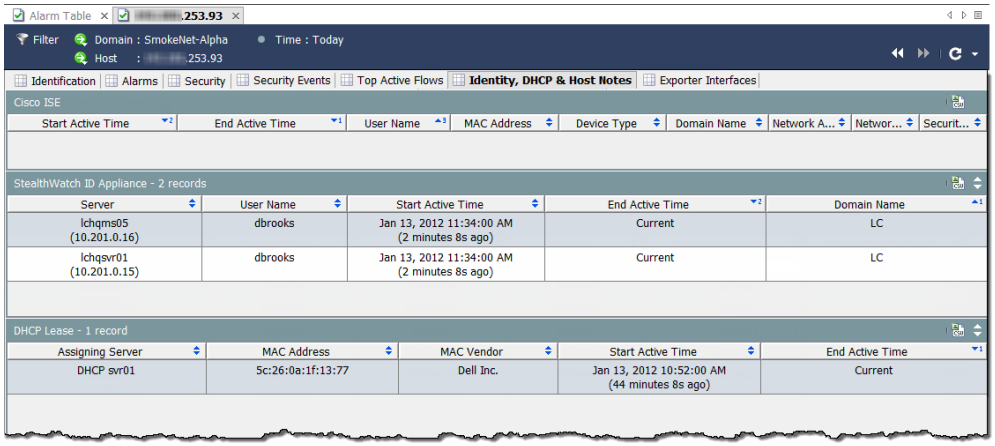
要查看安全事件的类型，请点击“主机快照”上的**安全事件**选项卡。在本例中，安全事件的类型为“地址扫描”和“Ping 扫描”。



如果要查看该主机排名靠前的活动流，请点击**排名靠前的活动流**选项卡。



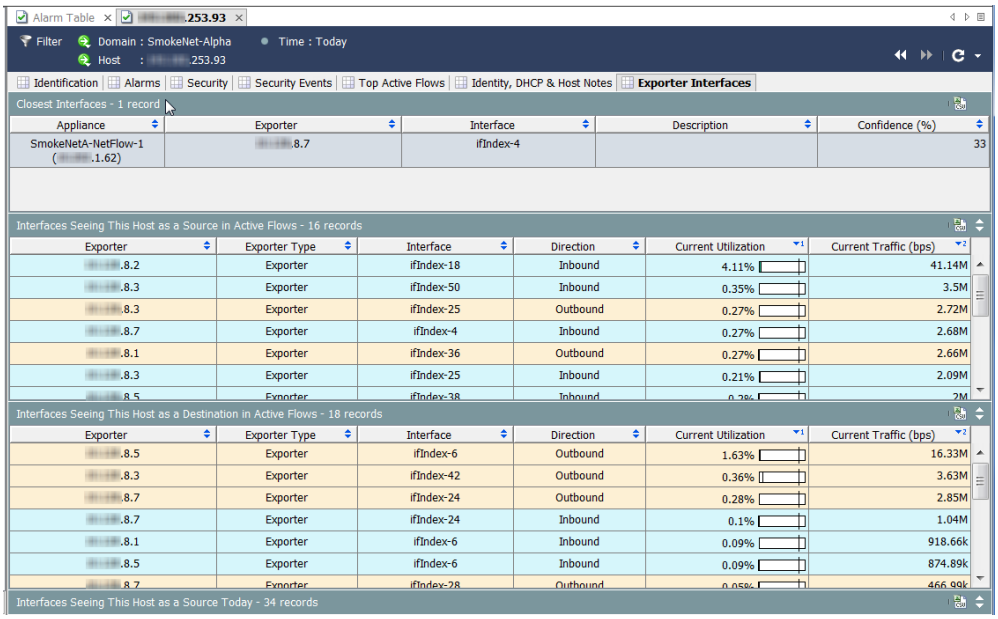
如果要查找域中与某个 IP 地址相关的用户，请点击**身份、DHCP 和主机说明**选项卡。



注意：

必须有 Stealthwatch 身份设备或思科 ISE 设备，才能获取用户身份数据。

如果要查看有关最近导出器的更多信息，并确定主机被视为活动流的源还是目标，请点击**导出器接口**选项卡。



此时，您已掌握了足够的信息来隔离源主机和目标主机。现在，您可以根据组织的策略开始执行清理。例如，您可以执行以下任何操作：

- 在每个主机上运行防病毒软件。
- 如果所有主机位于同一主机组，则可以阻止或隔离整个主机组。
- 阻止用于交换数据的端口。

行为是否正常？

到目前为止，我们一直假设的是警报条件由威胁导致。但是，如果引发警报的行为对主机来说完全正常，应该怎么办？

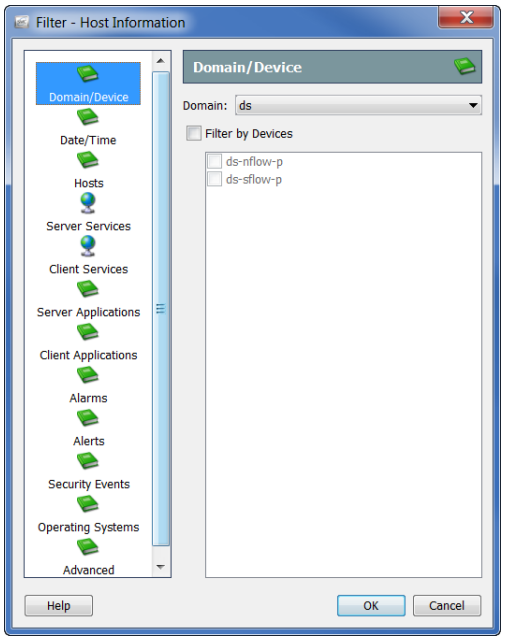
例如，邮件服务器看到大量流量，特别是邮件流量。但是，如果该服务器的参数设置得太低，您就会看到针对该服务器的多个邮件和/或流量警报。这种情况下，只需将参数设置为更高的合理限值，即可减少您看到的不必要的警报数量。在其他情况下，您可能必须编辑策略。

注意：

有关调整参数和编辑策略的信息，请参阅第 11 章“响应警报。”

哪些主机有相同的特征?

如果要查看引发特定警报、使用特定服务或具有其他共同特征的所有主机，可以使用“主机信息”过滤器。要访问此过滤器，请从主菜单中依次选择**主机 > 主机信息**。

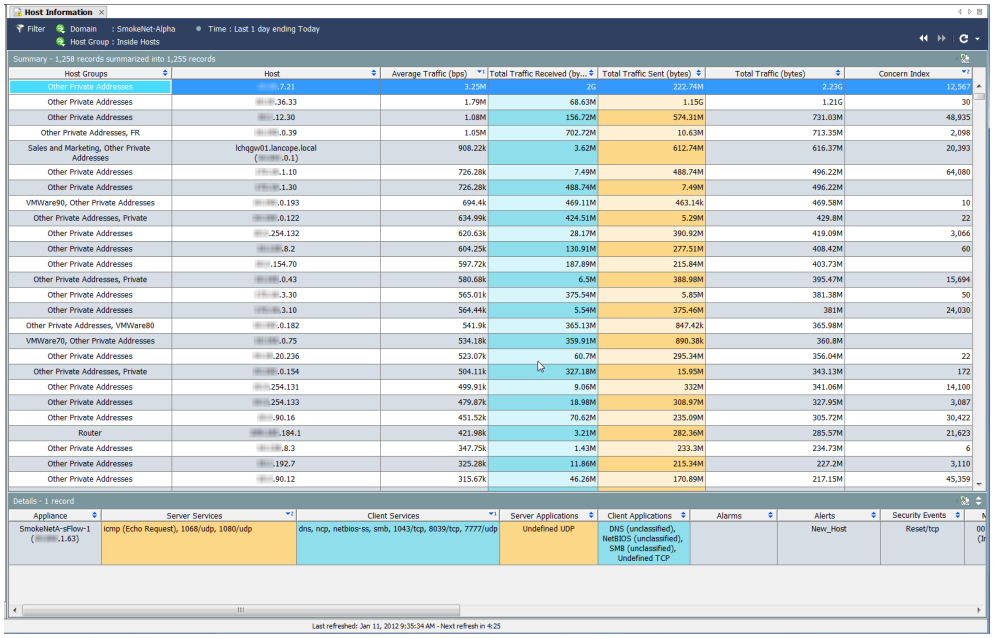


在“过滤器 - 主机信息”对话框中，您可以选择对符合这些参数的所有主机要查询的特定参数。例如，您可以过滤特定主机组中使用禁用服务或应用或引发“蠕虫活动”警报的所有主机。

注意：

由于您执行的是信息查询 (IQ)，所以此进程有时被称为“正在执行主机 IQ”。

在指定所需的参数后，点击**确定**显示包含请求数据的“主机信息”文档（例如主机 IQ）。



注意：

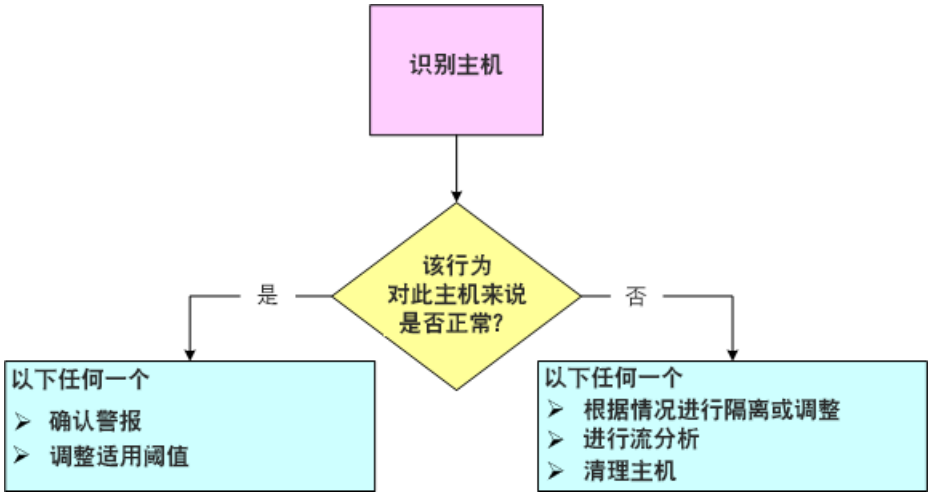
如果过滤引发“高关注指数”警报以及 TCP_Scan 风险通告的所有主机，结果将包含某些方面最可能受到感染的主机列表。

11

响应警报

概述

下图说明了解决网络威胁时要遵循的基本步骤。



如您所见，在对警报执行任何操作前，您必须回答以下三个问题：

- 哪个主机最初引发了警报？
- 对于该主机来说，引发警报的行为是否正常？
- 哪些其他主机（如有）受到了影响？

注意：

另外，您还可能会发现大量不会影响活动的不必要的警报。有关如何减少看到的不必要警报数量的详细信息，请参阅第 12 章“减少不必要的警报。”

回答前面的问题后，您就可以决定如何使用 SMC 软件来响应警报。本章介绍响应警报时最常采取的操作。

注意：

请参阅 *SMC 客户端联机帮助*，了解响应警报时可能还要执行的其他程序。

本章包含以下主题：

- 如何响应警报
- Stealthwatch 缓解功能

如何响应警报

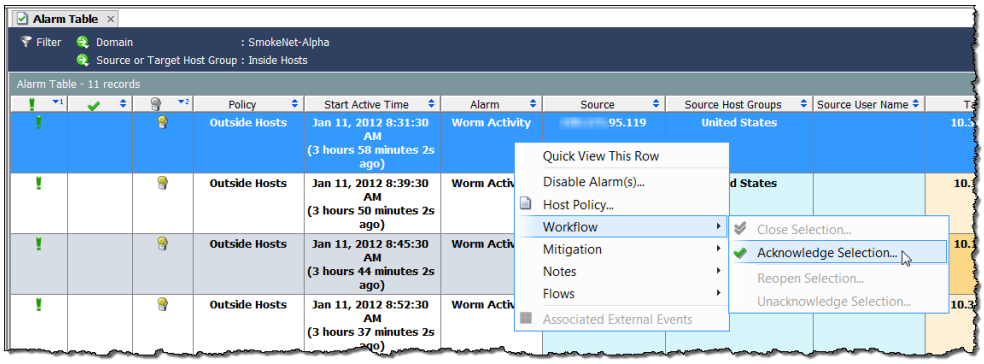
响应警报的方式有很多种。您可以确认警报、取消确认警报、关闭警报以及重新打开关闭的警报。请参阅以下部分了解相关的特定程序。

确认警报

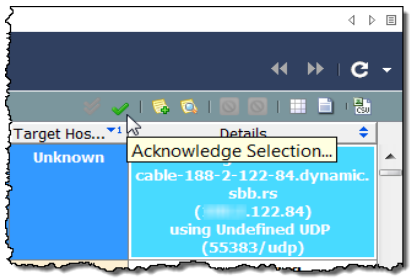
如果确认警报，即表示该警报正在予以调查。此操作对于工作流程有利，并可使其他团队成员知道该警报正在调查中。在确认警报之前，请记住，必要时可以撤消警报确认。

无论警报是活动还是非活动状态，都可以进行确认或取消确认。要使用 SMC 确认警报，请完成以下步骤：

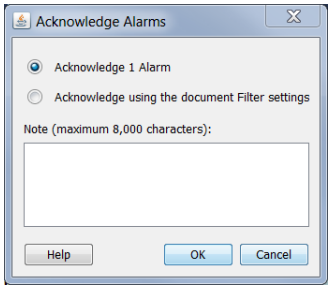
1. 在“警报表”上，右键点击警报，然后依次选择**工作流程 > 确认选择**。



另外，也可以点击警报，然后点击“警报表”工具栏上的**确认选择**按钮。



系统随即会打开“确认警报”对话框，要求您输入注释，说明为什么要关闭警报。



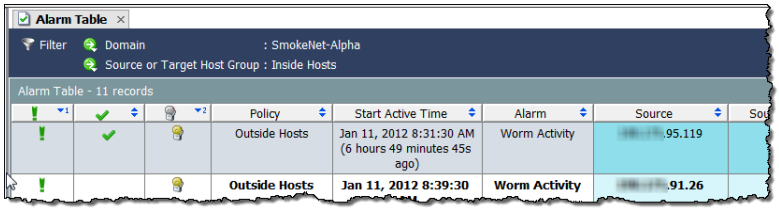
2. 指定确认警报或使用文档过滤器中的设置进行确认。请参阅以下可用选项的说明，以便了解确认警报的影响。

   - **确认 [x] 警报** - 仅确认“警报表”上当前显示的警报，其中 [x] 等于选定的警报总数。如果点击此选项，系统将逐一确认每个警报。因此，如果您有大量警报（比如 1000 个或更多），系统将需要相当长的时间才能完成此过程。
   - **使用文档过滤器设置进行确认** - 成批而不是逐个确认当前过滤器设置中包含的所有警报，*包括在确认过程中可能发生的任何新警报*。例如，假设“警报表”过滤器设置为仅显示“不重要”警报类型，且您选择基于此设置确认所有警报。系统不仅会确认您当前在“警报表”上看到的不重要警报，还会确认在确认进程执行期间可能生成的您没有看到的任何不重要警报。

注意：

由于**使用文档过滤器设置进行确认**选项成批确认警报，因此速度远远快于其他选项，尤其是在有 1000 个或更多警报的情况下。不过，您必须了解选择此选项，可能会确认您从未看到的警报。

3. 在“文本”条目字段中点击，键入关于为什么确认警报的说明，然后点击**确定**。“已确认”列中将显示一个复选标记 ✔，注释显示在“最后注释”列中（如果已选择显示这些列）。表行中关于该警报的文本不会加粗。



注意：

要查看“已确认”列和/或“最后注释”列，请右键点击列标题，然后从弹出菜单中选择相应的选项。

取消确认警报

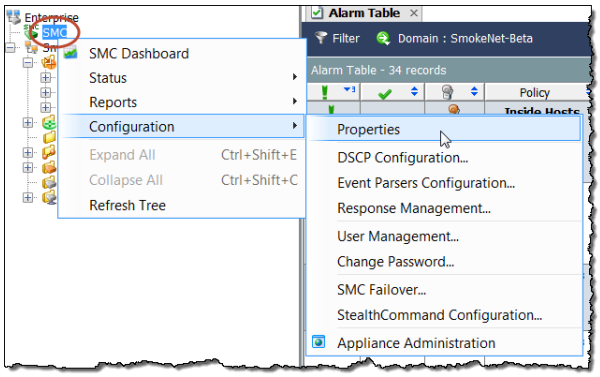
通过 SMC，您可以取消确认一个或多个已确认的警报。例如，如果您误确认了任何警报，可能希望完成以下步骤。

1. 在“警报表”上，显示要取消确认的已确认警报。必要时使用警报过滤器。
2. 右键点击要取消确认的警报，然后依次选择**工作流程 > 取消确认选择**。系统随即会打开“取消确认警报”对话框。
3. 键入警报注释，然后点击**确定**。
4. 对于要确认的每个警报，重复步骤 2 和 3。

关闭警报

如果您想表明对警报解决方式感到满意，可以关闭警报。请注意，没有必要手动关闭警报。

一旦警报变为非活动状态，当警报存在时间大于在“SMC 属性：数据保留”页面中为“警报表”指定的天数时，系统将自动从数据库中删除该警报。要访问此页面，请右键点击企业树中的 SMC 图标，然后依次点击**配置 > 属性**。



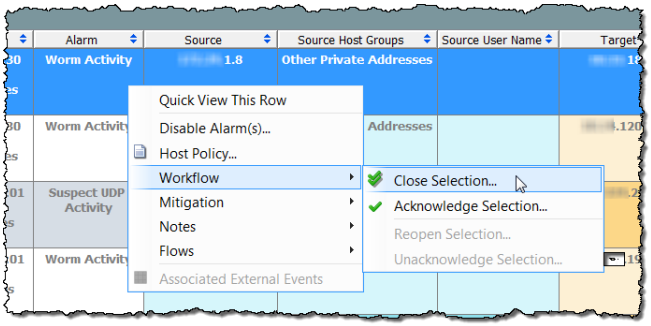
在关闭警报之前，请注意以下几点：

- 不能关闭活动警报。
- 在您关闭特定主机的警报后，该主机可能会在下次存档前再次生成该警报。
- 必要时可以撤消关闭警报。

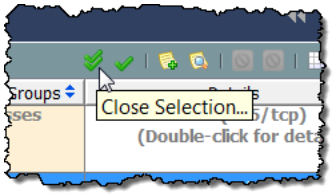
要使用 SMC 关闭警报，请完成以下步骤：

1. 更改“警报表”过滤器，以便显示非活动警报。要执行此操作，请在“警报表”过滤器对话框的“状态”页面上点击**过滤当前处于活动状态的警报**复选框以添加复选标记，然后点击**非活动**选项。

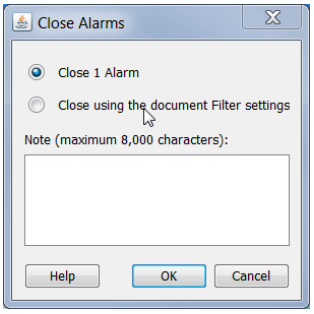
2. 在“警报表”上，右键点击警报，然后依次选择**工作流程 > 关闭选择**。



另外，也可以点击警报，然后点击“警报表”工具栏上的**关闭选择**按钮。



系统随即会打开“关闭警报”窗口，要求您输入注释，说明为什么要关闭警报。



3. 指定关闭警报或使用文档过滤器中的设置进行关闭。请参阅以下可用选项的说明，以便了解关闭警报的影响。

- **关闭 [x] 警报** - 仅确认和关闭“警报表”上当前显示的警报，其中 [x] 等于“警报表”上显示的警报总数。如果点击此选项，系统将逐一确认和关闭每个警报。因此，如果您有大量警报（比如 1000 个或更多），系统使用此选项将需要相当长的时间才能完成此进程。
- **使用文档过滤器设置进行关闭** - 成批而非逐个确认和关闭当前过滤器设置中包含的所有警报，*包括在关闭过程中可能发生的任何新警报*。例如，假设“警报表”过滤器设置为仅显示“次要”警报类型，且您选择基于此设置关闭所有警报。系统不仅会关闭您当前在“警报表”上看到的次要警报，还会关闭在关闭进程执行期间可能生成的您没有看到的任何次要警报。

注意：

由于“使用文档过滤器设置进行关闭”选项成批关闭警报，因此其速度远远快于其他选项，尤其是在有 1000 个或更多警报的情况下。不过，您必须了解选择此选项，可能会关闭您从未看到的警报。

4. 在“文本”条目字段中点击，键入关于为什么关闭警报的说明，然后点击**确定**。“已关闭”列中会显示一个复选标记 ，注释显示在“最后注释”列中（如果已选择显示这些列）。

注意：

要查看“已确认”列和/或“最后注释”列，请右键点击列标题，然后从弹出菜单中选择相应的选项。

重新打开已关闭的警报

通过 SMC，您可以重新打开一个或多个已关闭的警报。例如，如果您误关闭了任何警报，可能希望完成以下步骤：

1. 在“警报表”上，显示要重新打开的已关闭警报。如果需要，使用警报过滤器。
2. 右键点击要重新打开的警报，然后依次选择**工作流程 > 重新打开选择**。
3. 键入警报注释，然后点击**确定**。
4. 对于要确认的每个警报，重复步骤 2 和 3。

STEALTHWATCH 缓解功能

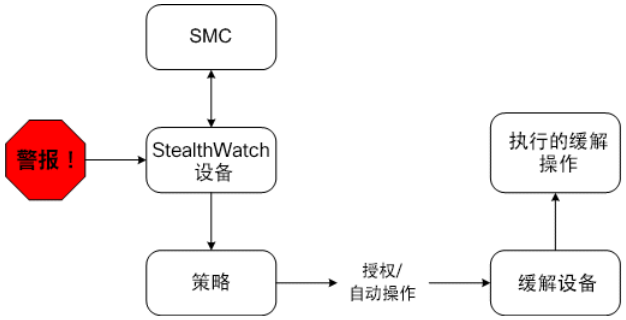
Stealthwatch 软件提供威胁缓解功能，使用该功能可使系统对各种威胁自动作出响应。通过使用此功能，您可以缩短决定如何响应某些警报所需的时间。一旦发生警报，系统将自动决定采取何种措施。

Stealthwatch 缓解功能可以帮助您在几秒钟内解决事件。如果您愿意，您可以将该功能设置为立即执行缓解（自动模式）或首先要求您授权（授权或手动模式）。

默认情况下，Stealthwatch 缓解功能处于禁用状态。要启用该功能，必须完成以下步骤（详见本节后面的内容）：

1. 为要使用缓解的每个设备配置缓解设备（例如，定义防火墙）。
2. 为要使用缓解的策略启用缓解功能。
3. 定义个别警报所需的缓解操作。

下图概述了 Stealthwatch 缓解功能的工作方式：



启用此功能后，当指定的警报发生时，Stealthwatch 系统会向缓解设备发送信号，请求此设备执行所配置的缓解操作。此设备会根据您为该警报指定的策略设置执行请求的操作。

注意：

系统不会对广播列表或缓解白名单上的主机执行缓解。有关这些列表的详细信息，请参阅 *SMC 客户端联机帮助*。

配置缓解设备

您必须配置 SMC，以便在 Stealthwatch 系统与缓解设备之间设置通信。如果您想让几个设备使用同一缓解设备，必须为该缓解设备单独配置每个设备。

注意：

您可能还需要配置缓解设备本身，才能从 Stealthwatch 设备接收信息。有关详细信息，请参阅《*缓解设备配置*指南》。您可以在 Stealthwatch 用户社区网站 (https://community.lancope.com) 中找到此文档。

对于每个设备，最多可配置以下缓解设备类型中的五种：

- Brocade INM
- 思科 ASA
- 思科 Guard
- 思科路由器（网络运营系统 11.3 及更高版本）
- 自定义
- Radware DefensePro
- Stealthwatch SNMP 缓解界面

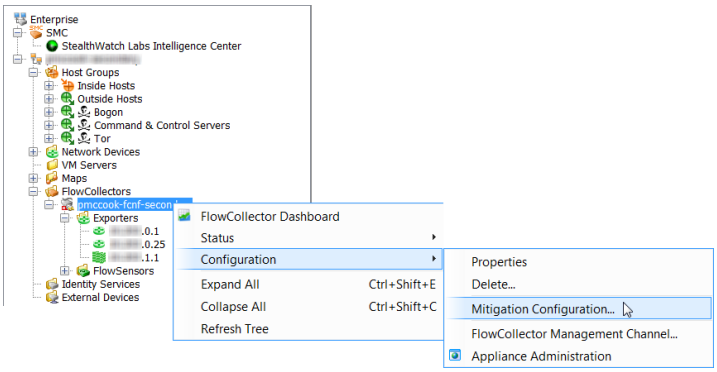
注意：

- 所有这些缓解设备类型（除 Radware DefensePro 之外）都只适用于 Stealthwatch 模块。Radware DefensePro 仅适用于 DDoS 模块。
- 如果您打算使用 expect 脚本来自定义缓解操作，请选择“自定义”选项。但是，我们建议您在尝试使用 expect 脚本之前联系 Lancope 客户支持寻求协助。

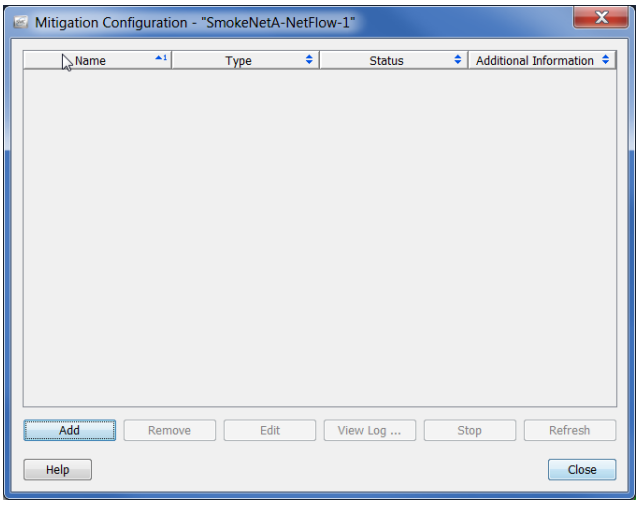
您选择的缓解设备的类型决定系统可以执行的缓解操作类型。例如，某个特定设备可能仅支持来自源 IP 地址的受阻流量。

要在 SMC 上配置缓解设备，请完成以下步骤：

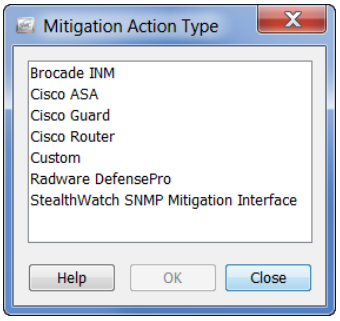
1. 右键点击设备名称，然后依次选择**配置 > 缓解配置**。



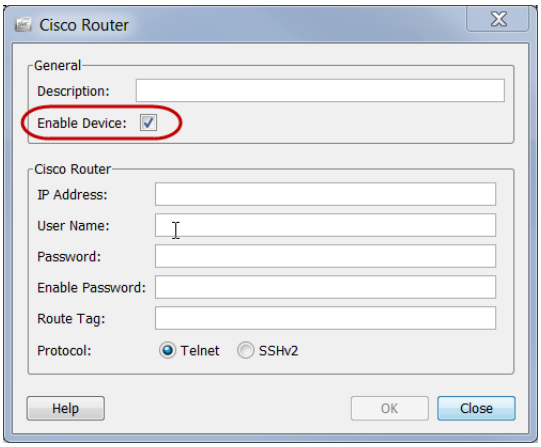
随即打开“缓解配置”对话框。



2. 点击**添加**。随即打开“缓解操作类型”对话框。

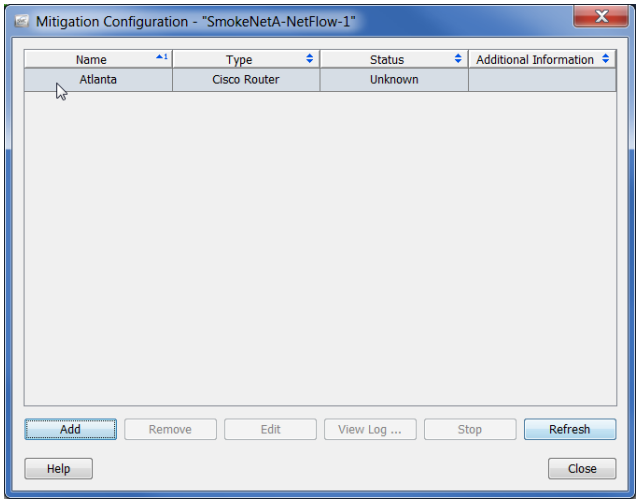


3. 点击要使用的缓解设备类型，然后点击**确定**。对于所选设备类型将打开设备信息对话框。例如，如果点击**思科路由器**，系统随即会打开“思科路由器”信息对话框。



4. 确保**启用设备**复选框包含复选标记，如前面示例中所示。如果不进行此选择，该设备将不会从 Stealthwatch 系统接收信息，并且缓解功能将不起作用。

5. 完成所选设备的所有特定识别信息，然后点击**确定**。设备信息对话框随即关闭，而您添加的设备现在已包含在“缓解配置”对话框中。



6. 重复步骤 2 至 5，直至添加需要为此设备添加的所有缓解设备。
7. 完成后，点击**关闭**以关闭“缓解配置”对话框。

现在，您即可按照下一节中所述启用每个主机组的缓解功能。

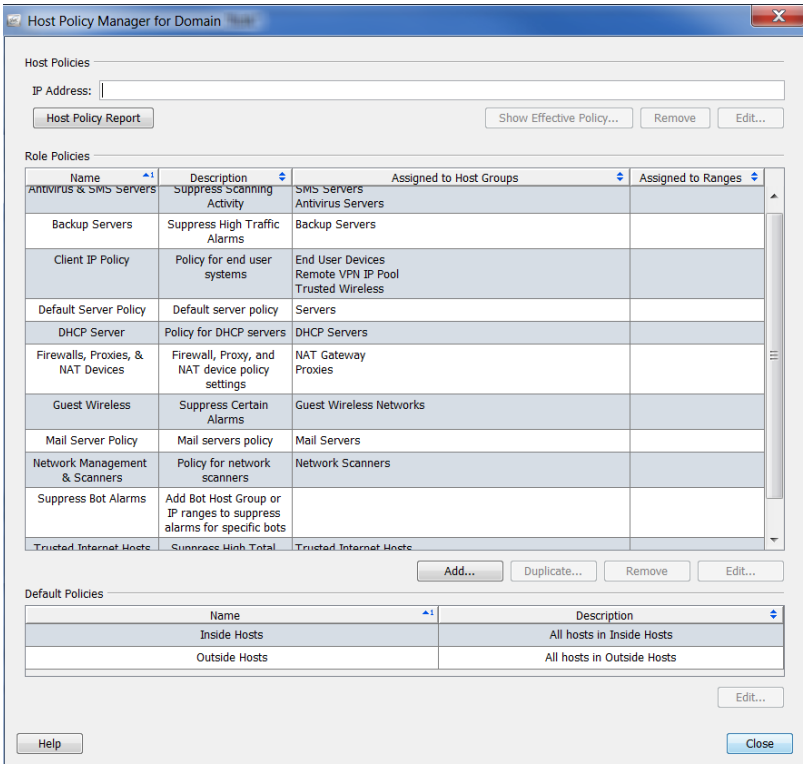
注意：
要使缓解功能起作用，必须运行缓解设备。

启用策略的缓解功能

配置缓解设备后，您可以为分配到一个或多个主机组的特定策略启用 Stealthwatch 缓解功能。例如，您可能想为“内部主机”默认策略启用缓解功能。另外，也可以只为少数主机组启用该功能，甚至可为特定主机 IP 地址启用该功能。

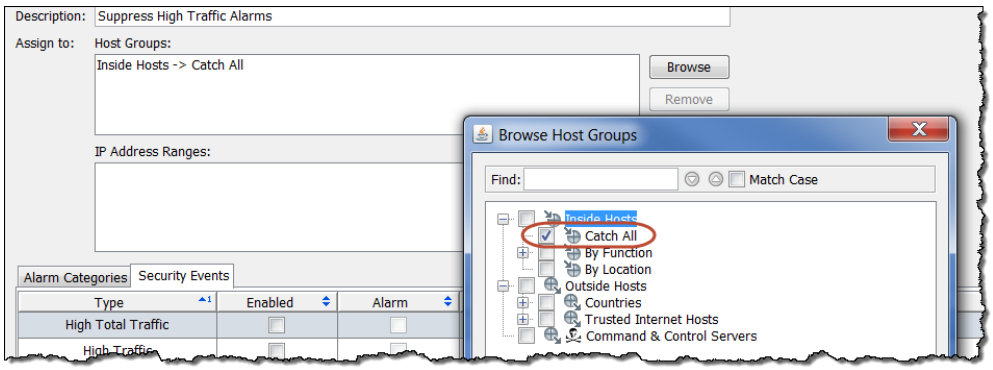
在以下示例中，我们假设要为特定角色策略启用缓解功能。为此，请执行以下操作：

1. 从主菜单中，依次选择**配置 > 主机策略管理器**。系统随即会打开“主机策略管理器”对话框。

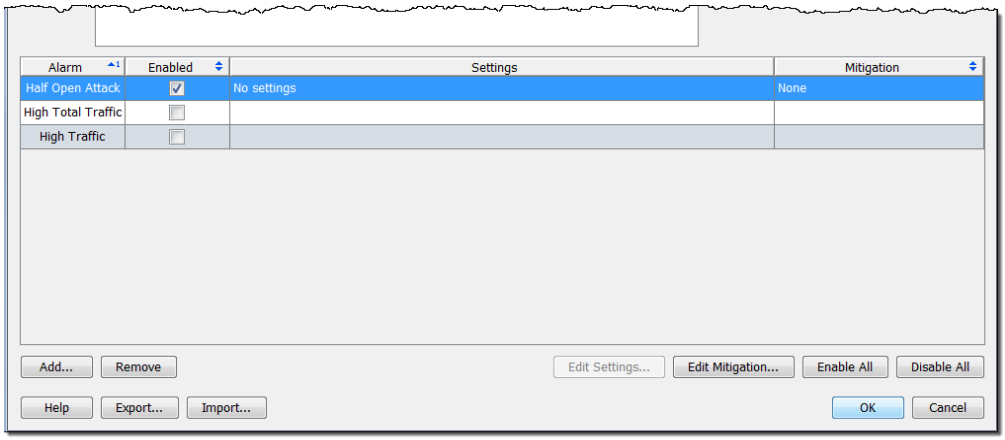


2. 在**角色策略**部分，点击所需的角色策略，然后点击**编辑**。系统会打开“编辑角色策略”对话框。

3. 在**分配给：主机组：**部分，点击**浏览**以选择要将该策略应用到的主机组，然后点击**确定**返回“编辑角色策略”对话框。（另外，您还可以在“IP 地址范围”字段中指定特定主机 IP 地址或范围。）



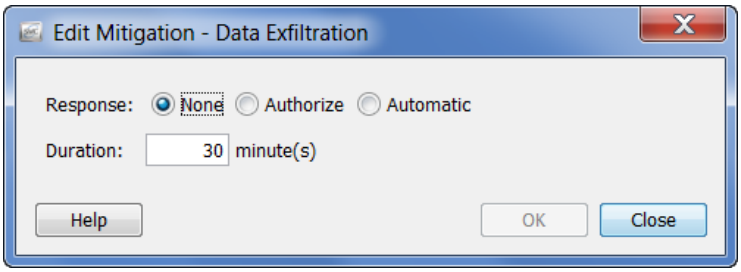
4. 在“编辑角色策略”对话框中，点击复选框以便在“启用”列中为每个要启用缓解的警报添加复选标记。（如果未列出所需的警报，请点击**添加**添加它们。）



定义警报的缓解操作

现在，您可以为所需的个别警报定义缓解操作。为此，请执行以下操作：

1. 从上一部分的步骤 4 继续，在当前打开的“编辑角色策略”对话框中选择包含要对其启用缓解的警报的行，然后点击**编辑缓解**。系统随即会打开“编辑缓解”对话框（内容可能会因警报而异）。



注意：

Lancope 为每项缓解操作提供建议的默认设置。必要时您可以根据自己的网络需求更改这些设置。

2. 根据以下说明，从弹出菜单中点击所需的缓解响应。

响应	说明
无	要禁用警报的所有缓解操作，请点击**无**。
授权	当发生警报时，要使系统在执行所选的缓解操作之前要求您授权，请点击**授权**。如果您喜欢手动阻止连接，而不允许系统自动为您阻止它们，请使用此设置。
自动	要允许系统在发生警报时立即自动执行选定的缓解操作，请点击**自动**。

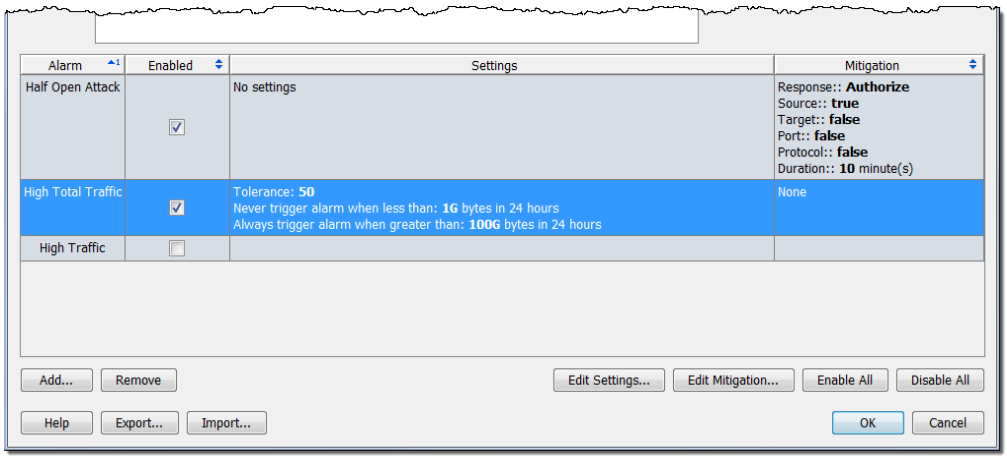
3. 指定下表中指示的其他缓解设置。您可以根据源或目标 IP 地址、协议和/或端口号的组合来自定义每个警报的缓解操作。您甚至可以指定缓解操作的运行时间。

缓解选项	目的
来源	阻止来自发起可疑活动的主机的流量。
目标	阻止流量传输到可疑活动的目标主机。
端口	阻止可疑流量经过的接口。
协议	阻止用于传输可疑流量的协议。
持续时间	您希望阻止操作保持生效的时长 （分钟）。此时间段到期后，缓解流程结束。 **注意：**持续时间为 0（零）表示无限，这意味着缓解操作会保持有效，直到手动结束缓解进程为止。

注意：

- 思科路由器不支持“端口”或“协议”缓解操作。
- OPSEC 设备要求您同时启用源和**目标**缓解操作。否则，这些设备无法阻止连接。

4. 为警报指定缓解设置后，请点击**确定**。您的设置随即会显示在“编辑角色策略”对话框中。



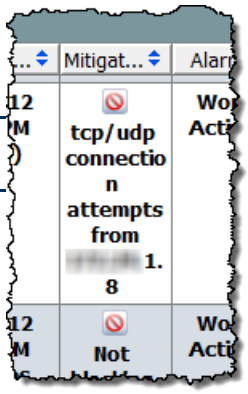
5. 对于要配置缓解设置的每个警报重复步骤 1 到 4。
6. 完成后，点击**确定**，然后点击**关闭**关闭“主机策略管理器”。

缓解和警报表

根据您是在“授权”还是在“自动”模式中启用了缓解措施，当发生相应的警报时，“警报表”会显示是否正在执行阻止操作。

授权（手动）模式

如果缓解操作处于“授权”模式，当发生警报时，“警报表”的“缓解”列中会显示红色的“不阻止”图标。



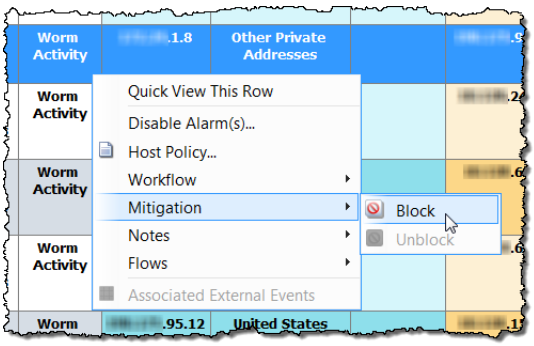
注意：

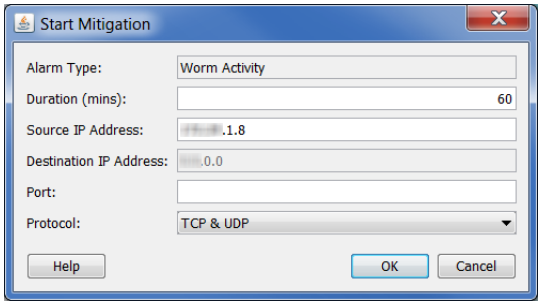
要显示“缓解”列，请右键点击列标题并选择**缓解**。

当缓解操作处于“授权”模式时，要手动对“警报表”中的特定警报执行缓解，请完成以下步骤：

1. 右键点击警报，然后依次选择**缓解 > 阻止**。

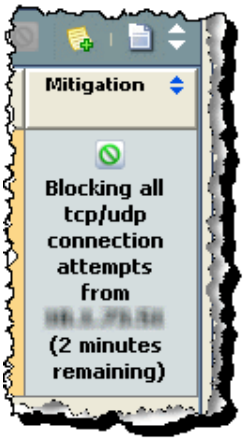
   系统随即会打开“启动缓解”对话框。





2. 如果需要，请更改缓解操作参数，然后点击**确定**。系统会关闭“启动缓解”对话框并刷新警报表。

3. 查找警报条件。红色“不阻止”图标现在将更换为绿色“阻止”图标。



注意：

如果要在缓解操作到期之前取消阻止连接，只需右键点击该警报，然后选择**缓解 > 取消阻止**即可。

自动模式

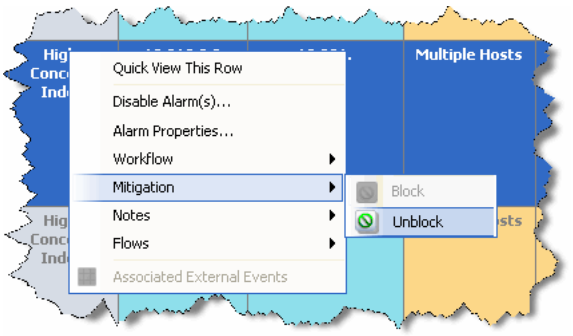
如果缓解操作处于“自动”模式，当发生警报时，“警报表”的“缓解”列中会显示绿色的“阻止”图标，如上例中所示。

注意：

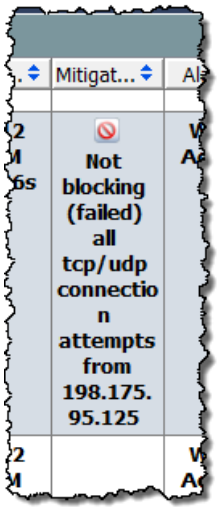
要显示“缓解”列，请右键点击列标题并选择**缓解**。

由于缓解操作处于“自动”模式，所以在警报发生时不需要执行任何操作就可以启动它。但是，如果需要停止缓解操作，请完成以下步骤：

1. 在“警报表”中，右键点击该警报，然后依次选择**缓解 > 取消阻止**。系统会刷新警报表。

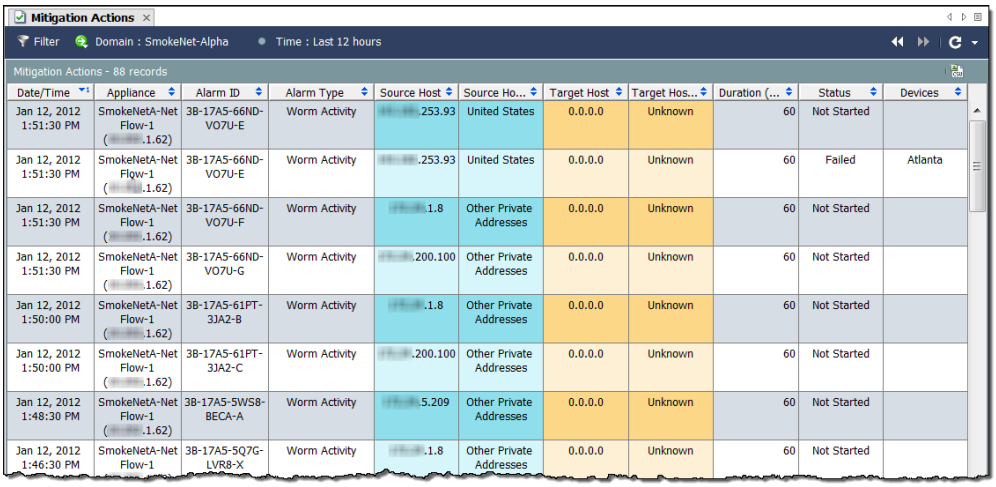


2. 再次刷新文档，然后重新选择警报条件。绿色“阻止”图标现在将更换为红色“不阻止”图标。



缓解操作文档

“缓解操作”文档允许您查看自上次存档后域中发生的所有缓解操作的状态。要访问“缓解操作”文档，请右键点击相关域，然后依次选择**状态 > 缓解操作**。系统会打开“缓解”文档。



12

减少不必要的警报

概述

如果某些策略设置的设定值太低或误禁用了特定主机组识别为正常的服务或应用，系统会由于行为被视为可疑（尽管实际上该行为正常）而引发警报。本章介绍如何减少您看到的不必要警报数量。

本章包含以下主题：

基准

基准可构建被视为正常网络行为的配置文件，所以它对于网络监控至关重要。由此，可使 Stealthwatch 在观察到异常行为时触发警报。

在网络中安装 Stealthwatch 后，它将立即开始识别网络上的每个主机。在前 7 天内，Stealthwatch 会根据大约 90 个属性建立被视为正常行为的基准，属性示例如下：

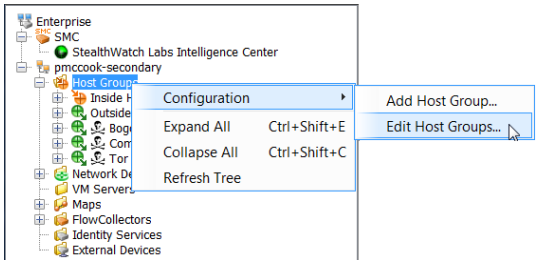
- 常规带宽使用情况。
- 与其他主机的通信。
- 并发流数量。
- 每秒数据包数。

此基准表示当天的预期行为。基准与容差一起结合使用，以计算当天使用的阈值。

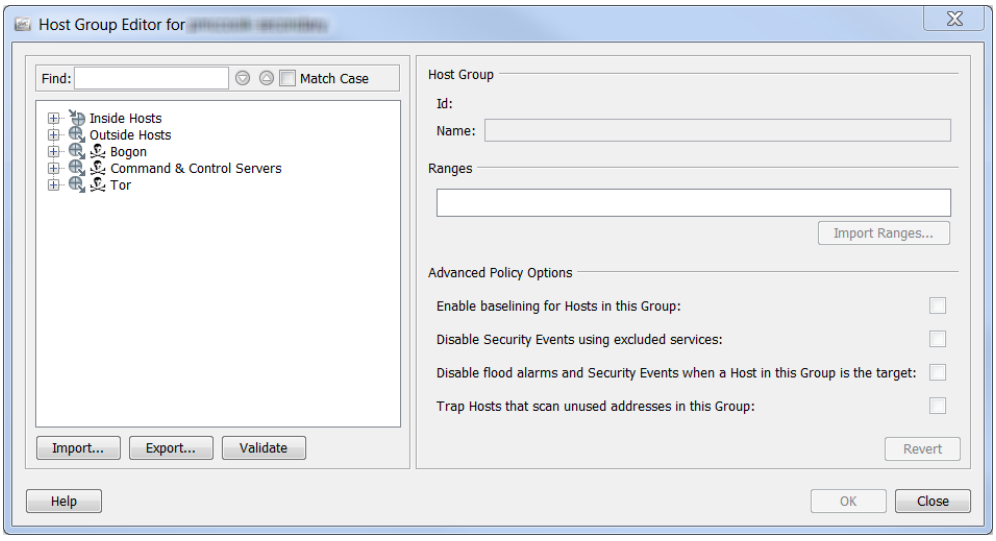
注意：

有关与警报相关的容差概念的信息，请参阅“警报”（第 261 页）。

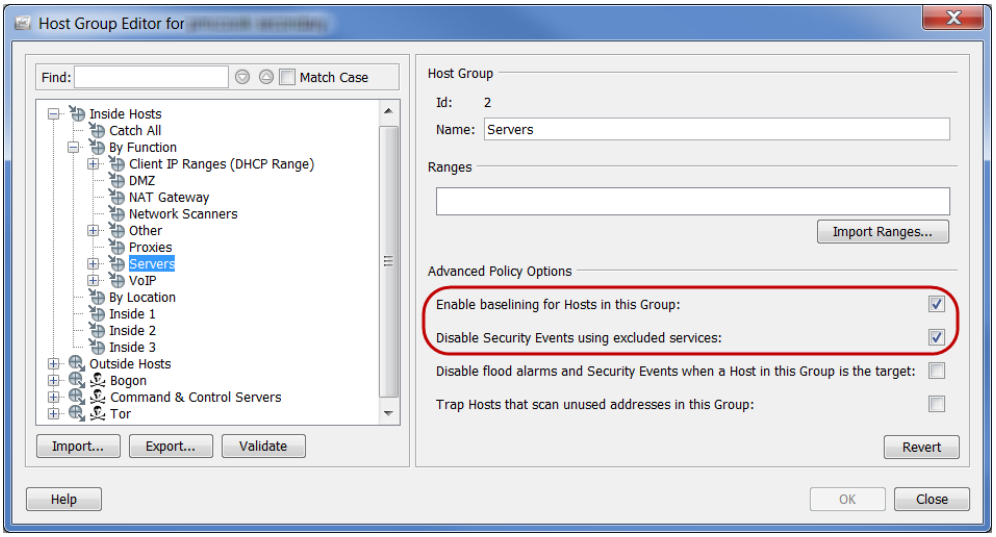
这 90 个属性属于前面提到的主机配置文件的一部分。默认情况下，Stealthwatch 为“内部主机”主机组内的每个主机建立基准。但是，对于“外部主机”主机组，Stealthwatch 仅为主机组级别的总体主机行为建立基准。您可以随时在“主机组编辑器”对话框中更改基准设置方法。



要访问此对话框，请右键点击企业树中的**主机组**，然后依次选择**配置 > 编辑主机组**。



在对话框左侧的企业树中，点击要更改其基准设置方法的主机。在“高级策略选项”部分，复选框将自动填充复选标记，以指示您所点击的主机的当前设置。



*仅当***为此组中的主机启用基准**复选框被选中时，才会为主机组的每个主机都建立唯一的主机级基准；否则 Stealthwatch 将为主机组级别的主机行为建立基准。

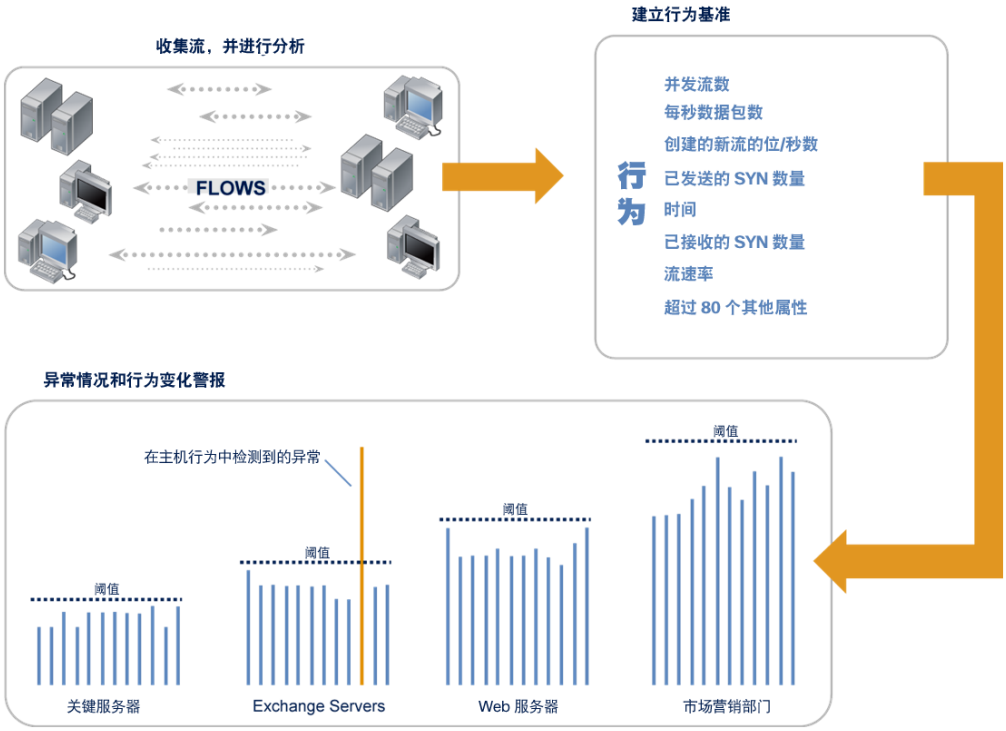
如前所述，Stealthwatch 默认为“内部主机”组内的每个主机建立基准；因此，内部主机的此选项默认为启用状态（请参阅上例中圈中的区域）。

注意：

对于频繁变化的环境，您可以禁用此功能，例如 IP 频繁变化的 DHCP 作用域。如果这样做，会使任何 DHCP 主机的预期行为基准表现同所有 DHCP 主机类似。

不过，默认情况下，Stealthwatch 对于“外部主机”组仅为主机组级别的总体主机行为建立基准；因此，外部主机的此选项默认处于禁用状态。

下图说明基准建立过程：



在最初 7 天过后，Stealthwatch 将通过跟踪 14 个关键属性来创建 28 天的滚动基准。此基准值是过去 28 天的每日属性值的平均值，着重体现过去 7 天的值。由于基准值包含过去七天，因此用于表示每周值。因此，基准值包括前一个月的值，但着重体现最近一周的值。

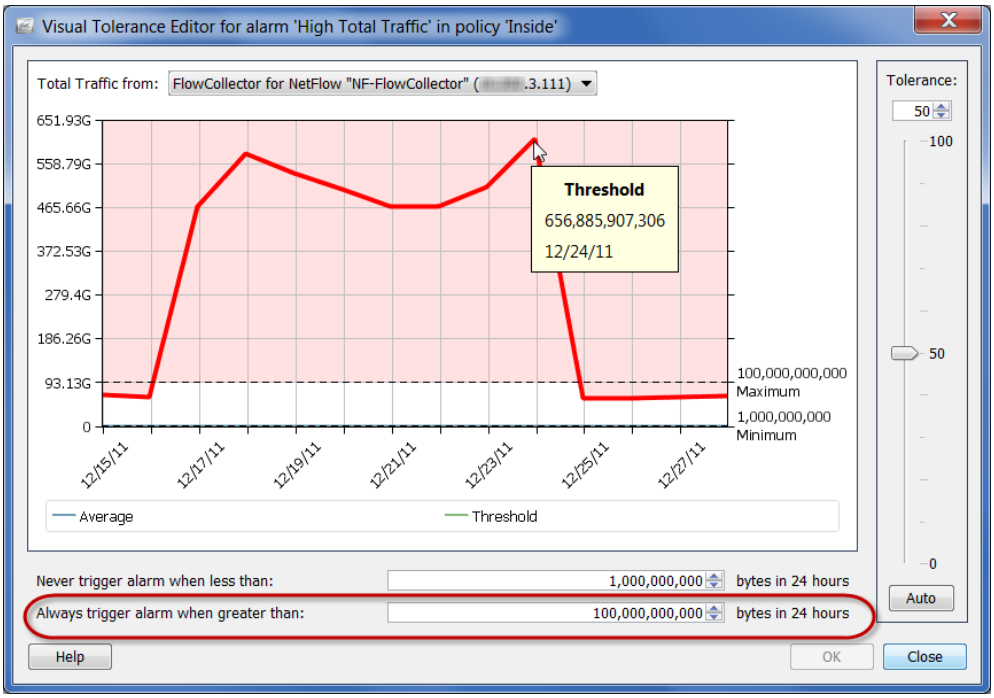
注意：

要查看作为 14 个关键属性源的 14 个警报的列表，请参阅“基于差异的警报与开/关警报”（第 261 页）中的表。

Stealthwatch 在建立基准时遵循以下准则：

- 对于主机基准，Stealthwatch 会存储每日看到的每个已启用警报（例如，“高总流量”警报）的最大值。
- 对于主机组基准，Stealthwatch 会存储组中所有主机的最大值的平均值（例如，所有主机的最大高总流量，再进行平均）。
- 如果某个主机没有每日值，它将使用其所属的主机数量最少的组的基准值。例如，如果某个主机属于两个组（组 A 定义为 10.201.0.0/16，组 B 定义为 10.201.3.0/24），则其基准值将继承自主机较少的组 B。
- 如果主机组的基准值为零 (0)，则使用最大值（例如，24 小时内的“高总流量”最大字节数）。

- 对于新安装的设备，在确立基准值前，所有主机都使用为第一天配置的策略最大值。在超出最大值之前，主机不会发出警报（请参阅以下示例中圈中的选项）。



继续，Stealthwatch 会查找并突出显示行为变化，如下所示：

- 一个主机在短时间内与大量其他主机通信（例如，P2P 应用、蠕虫）。
- 流持续时间过长（例如，隐蔽通道、VPN）。
- 使用未授权端口（例如，欺诈服务器/应用）。
- 带宽异常（例如 Warezserver、拒绝服务）。
- 未授权通信（例如，VPN 主机与记帐服务器通信）。

只要主机超过 Stealthwatch 设置为“正常”行为基准的阈值，Stealthwatch 就会触发警报。通过在发生主机行为时发现它们以及使用若干专有算法，Stealthwatch 可避免象基于签名的解决方案那样生成误报。

主机策略管理

根据您的登录权限，您可以使用策略来控制 Stealthwatch 如何监控和响应主机行为。策略包含决定 Stealthwatch 在发现特定行为时如何作出响应的设置。Stealthwatch 使用以下三种策略类型，您可以根据需要进行修改。

- *默认策略*，适用于所有“内部主机”和所有“外部主机”。
- *角色策略*，适用于服务于公共用途的主机（IP 地址）集合（例如 Web 服务器、防火墙、受信任的互联网主机等）。
- *主机策略*，适用于特定 IP 地址。

主机策略优先于所有其他策略。因此，主机策略比角色策略更具体，而角色策略比默认策略更具体。只有最具体的主机策略设置才会触发警报。

注意：

不能为一个主机分配多个主机策略。

例如，如果将警报添加到角色策略中，则无论其被禁用、启用还是警报设置被更改，它都会覆盖默认策略中的相同警报。

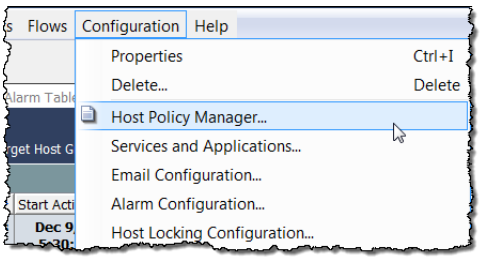
同样，如果将警报添加到特定主机的主机策略中，则无论其被禁用、启用还是警报设置被更改，它都会覆盖可能适用于该主机的任何角色策略或默认策略中的相同警报。

如果没有为主机分配主机策略，而是分配了两个或多个角色策略，则 Stealthwatch 系统将针对每个警报确定该主机的有效策略中所使用的策略设置。有关如何确定有效策略的详细信息，请参阅“有效主机策略”（第 239 页）。

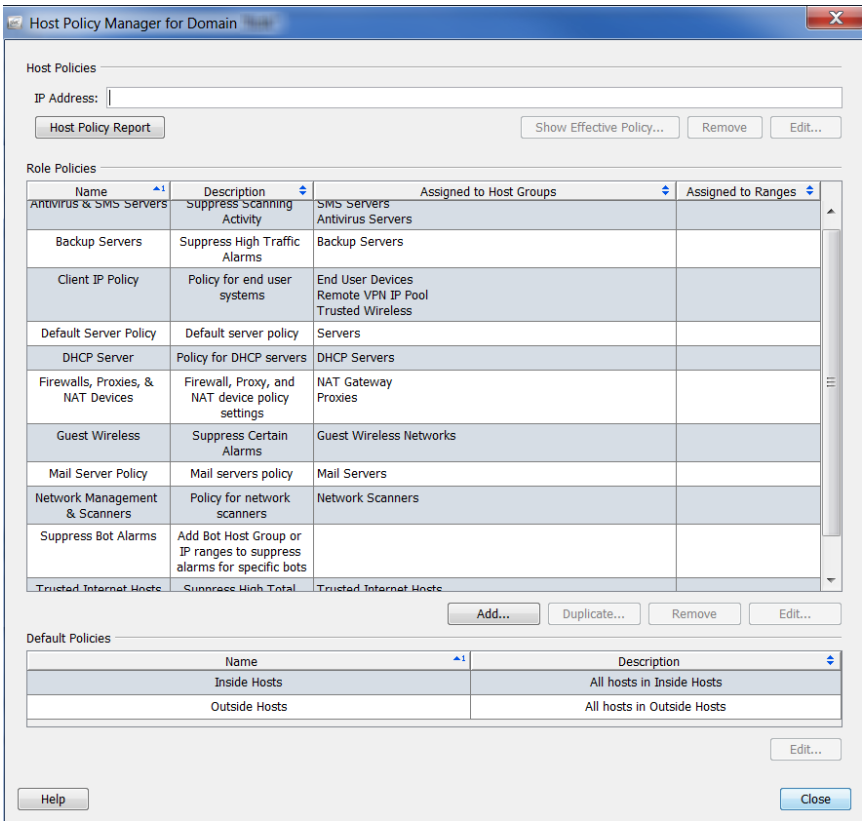
如果要更改域、主机组或特定主机所允许的行为阈值，您需要创建或编辑适当类型的策略，具体取决于您希望影响的主机组或主机数量。

Stealthwatch 系统内存在两个默认策略：“内部主机”默认策略和“外部主机”默认策略。如果尚未创建角色策略或主机策略，则应用这些设置。

您可能需要确定编辑其中一个组还是两个组的默认策略。为此，您需要访问“主机策略管理器”。要访问此对话框，请从主菜单中依次选择**配置 > 主机策略管理器**。



系统随即会打开“主机策略管理器”对话框。



在该对话框中，您可以使用以下部分配置策略：

- 主机策略 - 允许您管理单个主机的策略。
- 角色策略 - 允许您根据主机在系统中执行的角色来管理这些主机的策略。
- 默认策略 - 允许您管理内部主机或外部主机的默认策略。

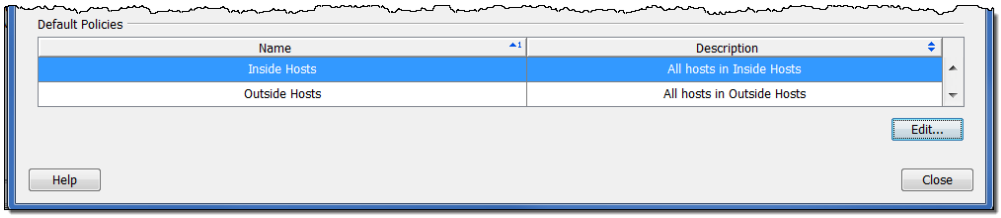
注意：
有关创建和编辑角色策略及主机策略的信息，请参阅“创建和编辑策略”（第 248 页）。

编辑内部主机/外部主机默认策略

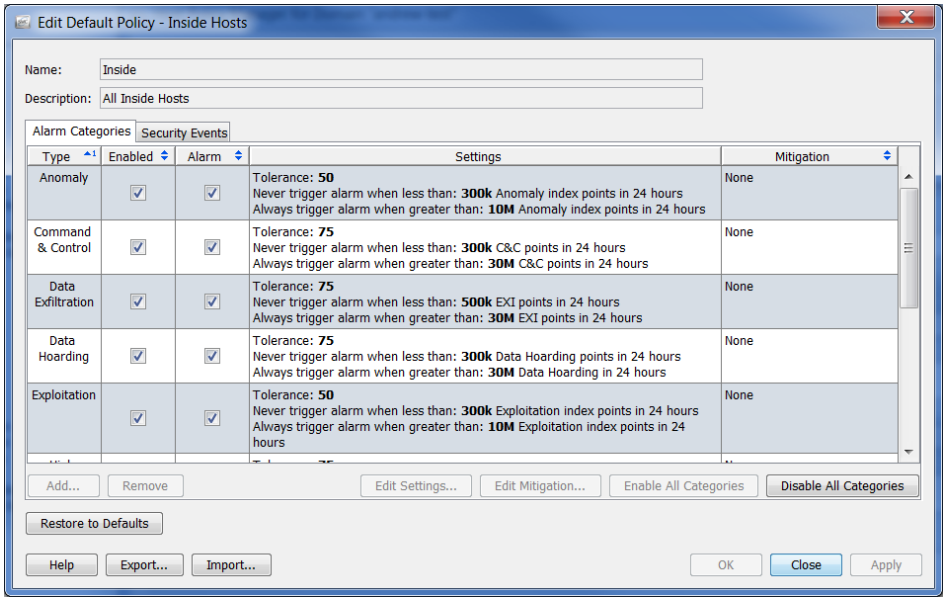
要编辑“内部主机”默认策略或“外部主机”默认策略，请完成以下步骤：

1. 从主菜单中，依次选择**配置 > 主机策略管理器**。系统将打开“主机策略管理器”对话框，如上一屏幕中所示。

2. 在**默认策略**部分，选择要编辑其默认策略的主机的名称，然后点击**编辑**。



系统随即会打开“编辑默认策略”对话框。



注意：

如果点击“恢复默认值”，则会使用出厂默认策略设置覆盖当前策略，所以使用此功能时请格外小心。

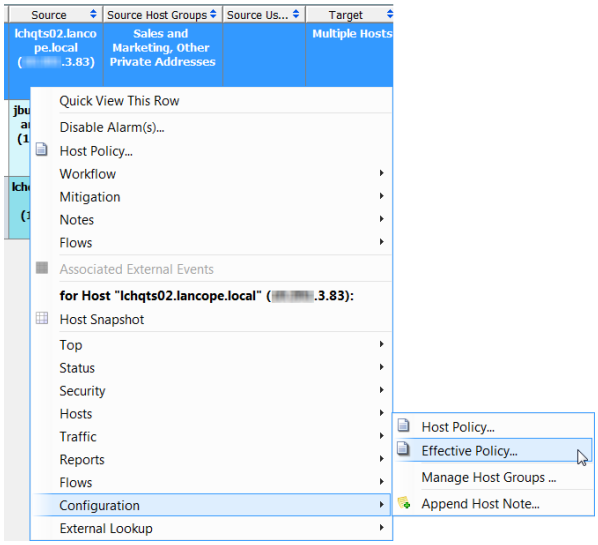
3. 如果要向策略中添加警报类别、编辑与警报类别关联的警报设置或缓解，并启用或禁用警报类别，请转到“在主机策略中配置警报类别”（第 242 页）。

4. 如果要配置策略使用的安全事件、编辑与 CI 关联的警报设置或缓解，并启用或禁用安全事件，请转到“在主机策略中配置安全事件”（第 245 页）。

有效主机策略

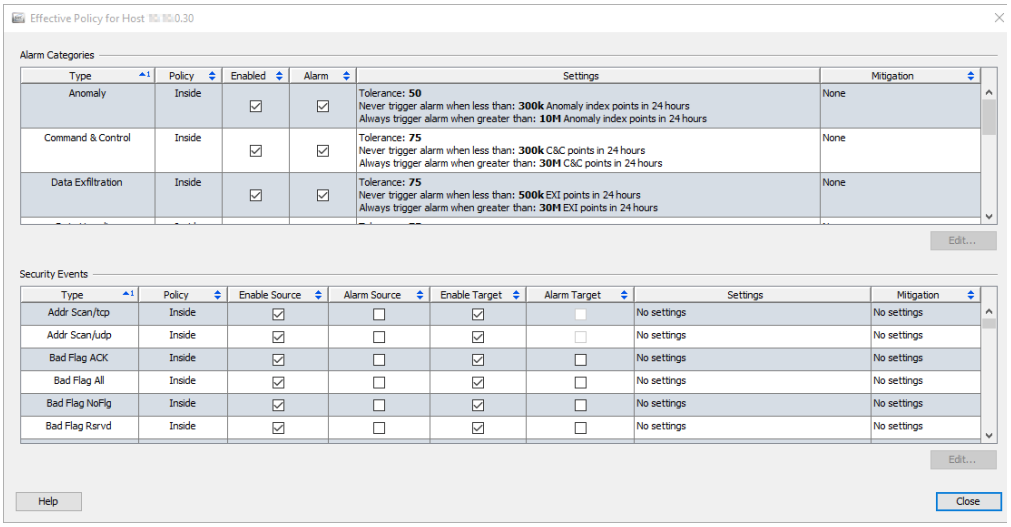
在响应警报时，您首先需要确定该特定警报由哪个策略触发。如果 IP 地址可见，可以右键点击该 IP 地址，然后依次选择**配置 > 有效策略。**

系统会打开“有效主机”对话框，如以下示例中所示。



提示：

如果您现在在“警报表”所在页面，查找控制策略的较快方法是启用“策略”列，方法为：右键点击标题内，然后从弹出菜单中选择**策略**。通过查看此列，您可以确定警报由哪个策略控制。在此，如果要查看特定策略的策略设置，请双击**策略**列中的策略名称。



您在上一示例中已看到，“高文件共享指数”警报由“服务器”角色策略控制，而“高流量”警报由“内部主机”策略控制。

在某些情况下，可能有主机未分配给一个主机策略而分配到两个或更多个不同配置的角色策略。发生此情况时，Stealthwatch 系统首先检查以发现在主机被分配到的任何角色策略中是否取消选择以下四列中的任意一个列：

- 启用源
- 警报源
- 启用目标
- 警报目标

如果甚至在任何策略中仅取消选择在上一项目符号列表中指定的四个列之一，那么在有效策略中取消选择该列。换言之，取消选择的任何列（等于“错误”设置）将覆盖该主机分配到的其他任何角色策略中的同一列，如果已选择该列（等于“真”设置）；换言之，错误设置会覆盖真设置。

在所有的分配角色策略中选择的任何列将在有效策略中保持选中状态。

示例 1

如果角色策略 1 是...			
启用源	警报源	启用目标	警报目标
真	真	错误	错误
并且角色策略 2 是... 角色策略 1 是...			
启用源	警报源	启用目标	警报目标
错误	错误	真	真
那么有效策略是... 有效策略是...			
启用源	警报源	启用目标	警报目标
错误	错误	错误	错误

示例 2

如果角色策略 1 是...			
启用源	警报源	启用目标	警报目标
真	真	真	错误
并且角色策略 2 是...			
启用源	警报源	启用目标	警报目标
真	错误	真	真
那么有效策略是...			
启用源	警报源	启用目标	警报目标
真	错误	真	错误

主机的有效策略将显示在“策略”列中，所有有效策略的名称。存在安全事件的源策略和目标策略时，“策略”列将首先列出源策略，然后列出目标策略。

注意：

有关响应警报的后续步骤，请参阅“创建和编辑策略”（第 248 页）。

警报类别

使用此部分可配置将此角色策略用于的警报类别。类别提供对特定类型的安全事件进行分组的方法。每个警报类别都可以生成警报，具体取决于发生的事件数量和事件类型。

可以执行以下操作：

- 添加或编辑警报类别设置
- 编辑与警报类别关联的警报缓解
- 启用或禁用警报类别

可用的警报类别类型包括：

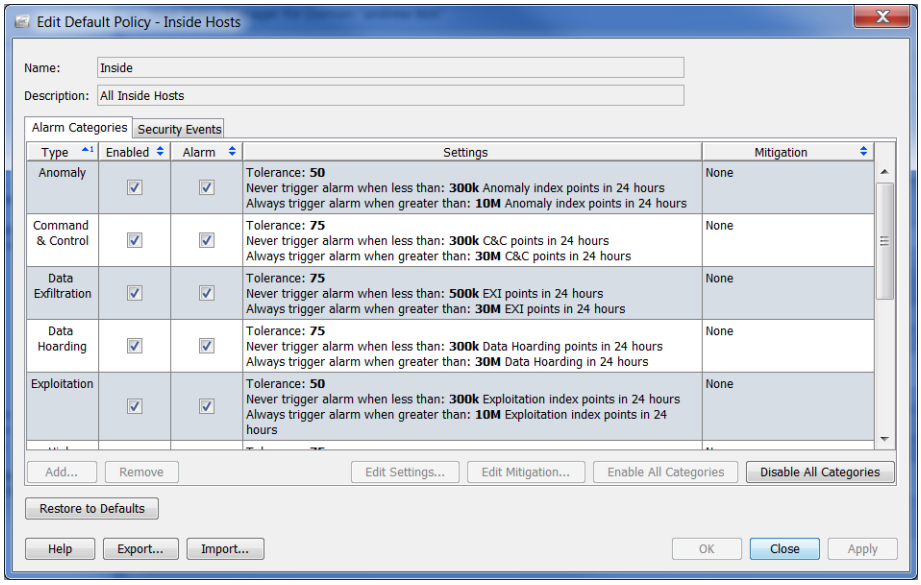
项目	说明
异常	跟踪指示主机行为异常或生成异常流量（但与其他类别的活动不一致）的事件。
C&C（命令和控制）	表示网络中存在尝试与 C&C 服务器通信的已感染僵尸病毒的服务器或主机。
数据泄露	跟踪数据传输量出现异常的内外部主机。 如果主机触发的这些事件的数量超过配置的阈值，则会导致高泄露警报。

项目	说明
数据收集	表示网络中的某个源主机或目标主机从一个或多个主机下载了异常数量的数据。
漏洞攻击	跟踪主机进行的彼此危害的直接尝试，如蠕虫传播和暴力破解密码。
高关注指数	跟踪关注指数超过 CI 阈值或快速增加的主机。 高关注指数和高目标指数类别使用相同的事件。如果事件是源主机触发的，则会导致高 CI 类别警报。如果事件是目标主机触发的，则会导致高 TI 警报。
高 DDoS 源指数	表示主机已被识别为 DDoS 攻击的源。
高 DDoS 目标指数	表示主机已被识别为 DDoS 攻击的目标。
高目标指数	跟踪所接收的扫描或其他恶意攻击已超过可接受的数量的内部主机。 高关注指数和高目标指数类别使用相同的事件。如果事件是源主机触发的，则会导致高 CI 类别警报。如果事件是目标主机触发的，则会导致高 TI 警报。
策略违规	主体表现出违反正常网络策略的行为。
侦测	表示存在使用 TCP 或 UDP 且正在您的组织主机上运行的未授权潜在恶意扫描。这些扫描（称为“侦测”）是针对您的网络发起攻击的早期信号，并且可能来自您的组织外部或内部。

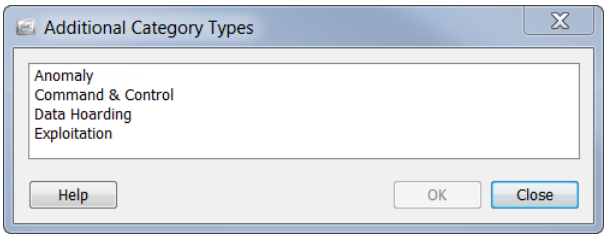
在主机策略中配置警报类别

要配置警报类别，请完成以下步骤：

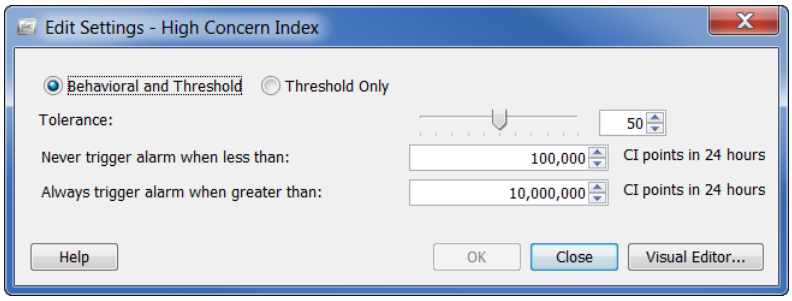
1. 在“编辑策略”对话框中，点击**警报类别**选项卡。



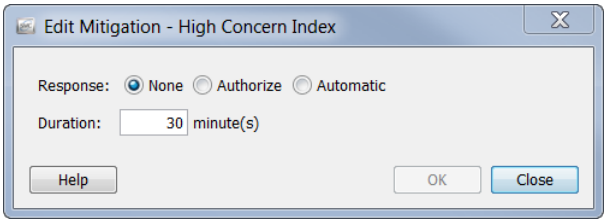
2. 执行以下操作之一：
   - 如果需要添加警报类别，请转到步骤 3。
   - 如果需要编辑警报类别，请转到步骤 5。
3. 要添加警报类别，请点击**点击**。系统随即会打开“警报类别”对话框。



4. 选择一个或多个警报类别，然后点击**确定**：
   您会返回到“编辑策略”对话框。
5. 要编辑警报类别的行为、容差或阈值设置，请选择要编辑的警报类别。
6. 点击**编辑设置**。系统会打开“编辑设置”对话框。



7. 根据需要更改设置，完成后点击**确定**。您会返回到“编辑策略”对话框。
8. 要指定应在何时以及如何执行缓解，请选择要编辑的警报类别。
9. 点击**编辑缓解**。系统将打开“编辑缓解”对话框。



10. 根据需要更改设置，完成后点击**确定**。您会返回到“编辑策略”对话框。

注意：

- 在没有为警报类别配置设置时，“设置”列中会显示*无设置*。
- 在没有为警报类别配置缓解设置时，“缓解”列中会显示*无*。

11. 要启用某个警报类别，请选中“启用”列中该警报类别的复选框。

提示：

使用“启用所有类别”或“禁用所有类别”按钮一次启用或禁用所有警报类别。

12. 要对安全事件发出警报，请选中“警报”列中的复选框。
13. 执行以下操作之一：
    - 要应用设置而不退出“编辑策略”对话框，请依次点击**应用 > 关闭**。
    - 要应用设置并退出“编辑策略”对话框，请点击**确定**。

注意：

- 有关不同类型的警报设置的信息，请参阅“警报”（第 261 页）。
- 有关特定警报的建议设置，请参阅“建议”（第 266 页）。

安全事件

使用此部分可配置策略使用的安全事件、编辑与 CI 关联的警报设置或缓解，并启用或禁用安全事件。有关“安全事件”选项卡上的复选框说明，请参阅下表。

选中此复选框 ...	执行以下操作 ...
影响源策略	如果您希望主机策略或角色策略覆盖现有有效策略中定义的源设置。 **注意：**仅当您编辑主机策略或角色策略时，才可以使用此列。
启用源	如果您希望针对源启用的安全事件可以影响任何适用的警报类别的指数点。
警报源	如果您希望针对源启用的安全事件也可以触发其关联警报。
影响源目标	如果您希望主机策略或角色策略覆盖现有有效策略中定义的源设置。 **注意：**仅当您编辑主机策略或角色策略时，才可以使用此列。
启用目标	如果您希望针对目标启用的安全事件可以影响任何适用的警报类别的指数点。
警报目标	如果您希望针对目标启用的安全事件也可以触发其关联警报。

请参阅以下相关情况，其中特定类型的安全事件不会发出警报：

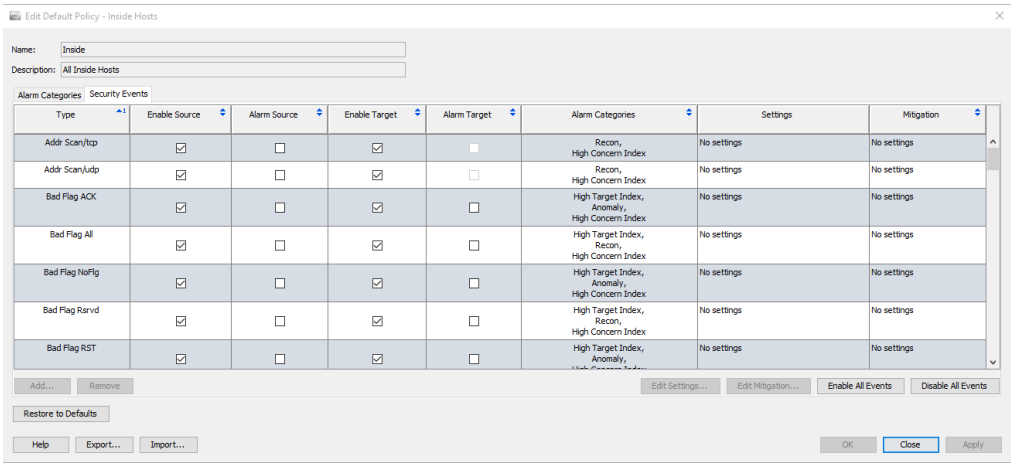
- 一对多（例如，发起的最大流数）- 此类安全事件无法对目标发出警报，因此，您无法为此类安全事件选中“警报目标”复选框。
- 多对一（例如，接收到的 SYN）- 此类安全事件无法对源发出警报，因此，您无法为此类安全事件选中“警报源”复选框。

您可以右键点击并选择“禁用警报”来禁用“警报表”中的警报。这将取消选中相应安全事件的“警报源”复选框和“警报目标”复选框；“启用源”复选框和“启用目标”复选框将保持选中状态。这将创建新的主机策略，其中“启用源”列和“启用目标”列处于选中状态，但“警报源”和“警报目标”处于取消选中状态。

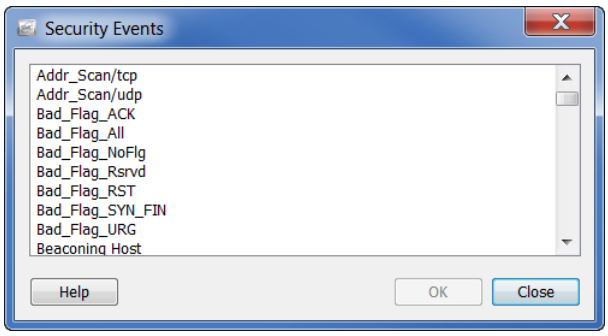
在主机策略中配置安全事件

要配置安全事件，请完成以下步骤：

1. 在“编辑策略”对话框中，点击**安全事件**选项卡。



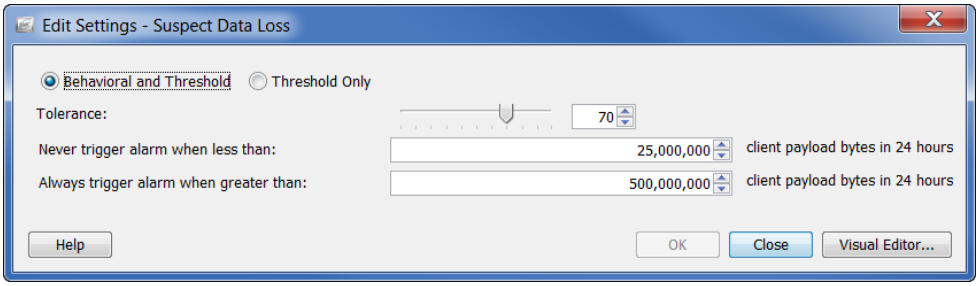
2. 执行以下操作之一：
   - 如果需要添加安全事件，请转到步骤 3。
   - 如果需要编辑安全事件，请转到步骤 5。
3. 要添加安全事件，请点击**添加**。系统随即会打开“安全事件”对话框。



4. 执行以下操作之一：
   - 要添加一个安全事件，请选择事件，然后点击**确定**。
   - 要添加按顺序列出的若干事件，请选择第一个事件，按 **Shift** 键，然后选择顺序中的最后一个事件，最后点击**确定**。
   - 要添加未按顺序列出的若干事件，请按 **Ctrl** 键，然后选择每个事件，最后点击**确定**。

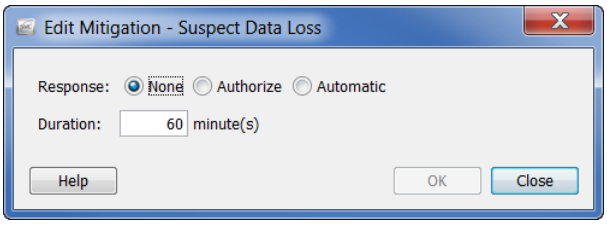
   您会返回到“安全事件”选项卡。
5. 要编辑安全事件的行为、容差或阈值设置，请选择要编辑的安全事件。
6. 点击**编辑设置**。

   系统会打开“编辑设置”对话框。



7. 根据需要更改设置，完成后点击**确定**。您会返回到“编辑策略”对话框。
8. 要指定应在何时以及如何执行缓解，请选择要编辑的安全事件。
9. 点击**编辑缓解**。

   系统将打开“编辑缓解”对话框。



10. 根据需要更改设置，完成后点击**确定**。您会返回到“编辑策略”对话框。

注意：

- 在没有为警报类别配置设置时，“设置”列中会显示*无设置*。
- 在没有为警报类别配置缓解设置时，“缓解”列中会显示*无*。

11. 根据您要启用源安全事件、目标安全事件还是同时影响任何适用警报类别的指数点，点击相应的“启用”复选框。

提示：

使用“启用所有事件”或“禁用所有事件”按钮一次启用或禁用所有事件。

12. 根据您要对源安全事件、目标安全事件还是两者发出警报，点击相应的“警报”复选框。
13. 执行以下操作之一：
    - 要应用设置而不退出“编辑策略”对话框，请依次点击**应用 > 关闭**。
    - 要应用设置并退出“编辑策略”对话框，请点击**确定**。

注意：

- 有关不同类型的警报设置的信息，请参阅“警报”（第 261 页）。
- 有关特定警报的建议设置，请参阅“建议”（第 266 页）。

创建和编辑策略

如上一节中所述，在响应警报时，您需要确定该特定警报由哪个策略触发。当准备编辑或禁用警报时，您很可能在“警报表”所在页面或“主机快照”的**警报**部分。因此，在以下示例中，我们将使用的场景是您（用户）在“警报表”所在页面准备编辑或禁用警报的情景。

当响应警报时，请完成以下步骤：

1. 确定触发主机。例如，它是服务器还是桌面等？此外，确定该行为是否正常。如果行为正常，请继续执行以下步骤。如果行为不正常，请按照标准上报程序调查警报原因。
2. 如果触发主机不是已为其创建默认角色策略的预定义组（例如备份服务器、防火墙、代理）的成员，但它在逻辑上可以属于一个预定义组，则将该主机分配到其在逻辑上适合的预定义组。（请参阅“将主机分配到预定义的组”（第 249 页）。）

   例如，如果触发主机是备份服务器，则由于存在名为“备份服务器”的预定义组，并且已经为其创建了默认角色策略。因此，您可以将此触发主机分配到该“备份服务器”组。然后，系统将自动为其分配“备份服务器”的默认角色策略。
3. 如果触发主机不是预定义组的成员，并且在逻辑上也不适合任何预定义组，但它却属于另一个角色策略，则编辑其所属的角色策略。（请参阅“编辑角色策略”（第 254 页）。）

   如果触发主机不是预定义组的成员，并且在逻辑上也不适合任何预定义组，但它却属于某个主机策略，则编辑其所属的主机策略。（请参阅“编辑主机策略”（第 259 页）。）
4. 如果触发主机不属于任何角色策略或主机策略，可以执行下列操作之一：

   - 编辑管理此主机的“内部主机”默认策略或“外部主机”默认策略（以适用者为准）。（请参阅“编辑内部主机/外部主机默认策略”（第 237 页）。）

   注意：

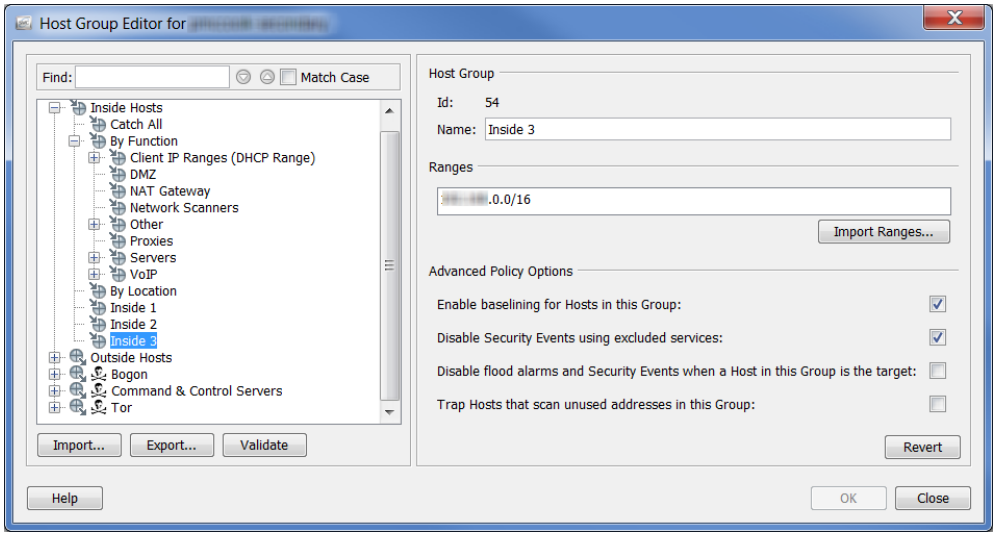
   请记住，您对“内部主机”默认策略或“外部主机”默认策略进行的任何编辑会影响全局设置。

   - 为此主机创建一个角色策略。（请参阅“创建角色策略”（第 250 页）。）
   - 为此主机创建一个主机策略。（请参阅“创建主机策略”（第 256 页）。）

将主机分配到预定义的组

要将主机分配到预定义的组，请完成以下步骤：

1. 在“企业”页面树菜单上，点击触发主机所属的域。
2. 从主菜单中，依次选择**配置 > 编辑主机组**。系统将打开您在企业树中点击的域的“主机组编辑器”对话框。
3. 在左窗口中，点击要将触发主机分配到的组。该对话框右侧的“范围”字段中显示已属于此组成员的任何主机的 IP 地址。



提示：

要将单个主机快速移到组中，请右键点击任何文档中的主机，然后依次选择**配置 > 管理主机组**。当该主机的“主机组”对话框打开时，请从对话框的顶部选择所需的组，然后点击**确定**。

4. 完成以下任何步骤，以将 IP 地址添加到步骤 3 中指定的组。
   - 在“范围”字段中，键入触发主机的 IP 地址。
   - 如果要添加多个主机并且它们位于一个范围内，则在“范围”字段中键入所需的触发主机的 IP 地址范围。
   - 如果要添加多个主机，并且您有一个包含触发主机 IP 地址的现有文件，请点击**导入范围**以导入这些 IP 地址。
5. 点击**确定**。“企业”页面树菜单会自动更新以包括添加到步骤 3 中所指定组的所有新 IP 地址。

创建角色策略

请记住，当您希望为具有共同功能或类似属性的一组主机分配相同的警报阈值时，可创建角色策略。

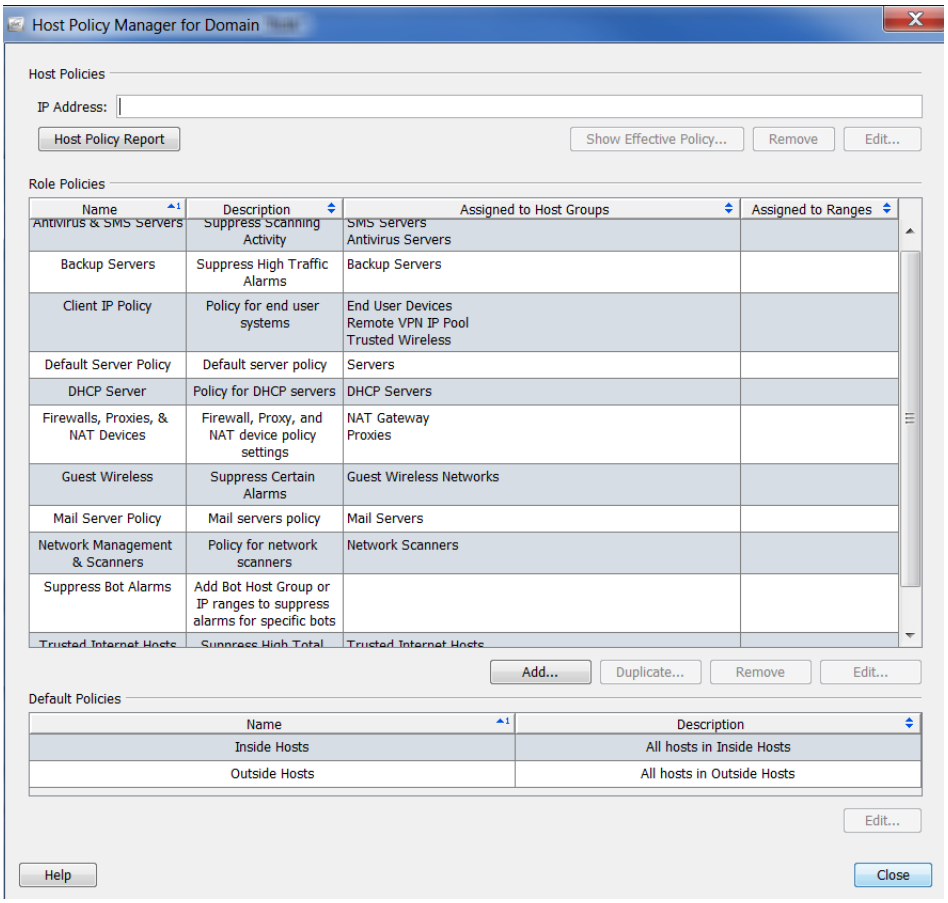
如果某个 IP 地址没有主机策略，Stealthwatch 将使用管理该主机的“角色策略”中的相应警报设置。一个主机可以位于多个“角色策略”中，并继承“角色策略”的**所有**设置。因此，由于可以为特定主机应用多个角色策略，而且每个策略的阈值设置可以不同，所以当主机行为超出每个角色策略内定义的值时，可能会触发多个警报。

注意：

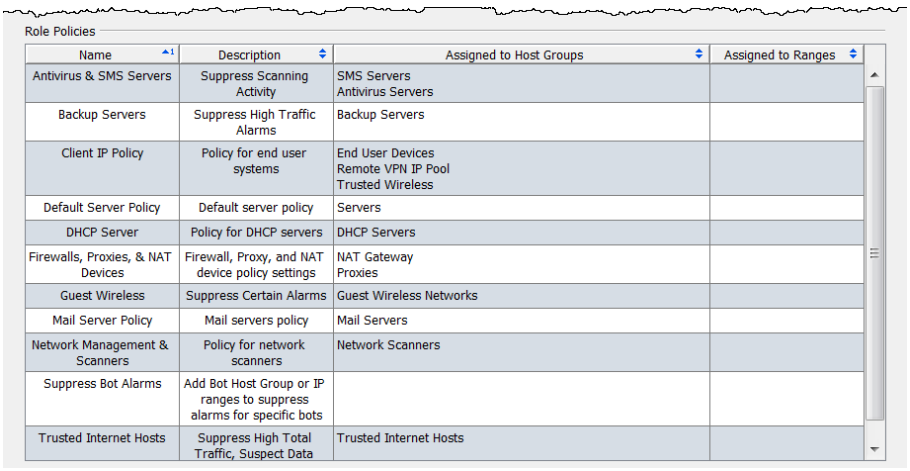
为了防止混淆，最好不要使用具有相同警报的多个角色策略，除非需要根据不同的值触发警报（例如，对于不同的团队）。

要添加角色策略，请完成以下步骤：

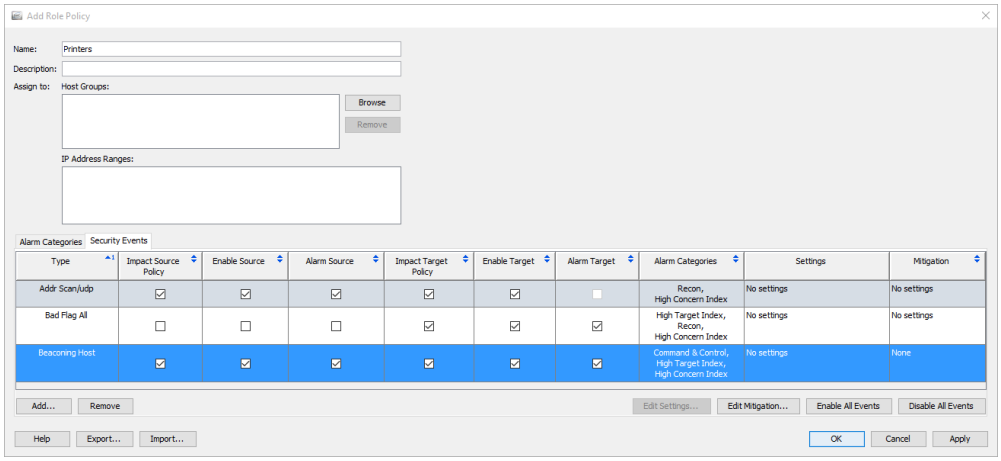
1. 从主菜单中，依次选择**配置 > 主机策略管理器**。系统将打开“主机策略管理器”对话框。



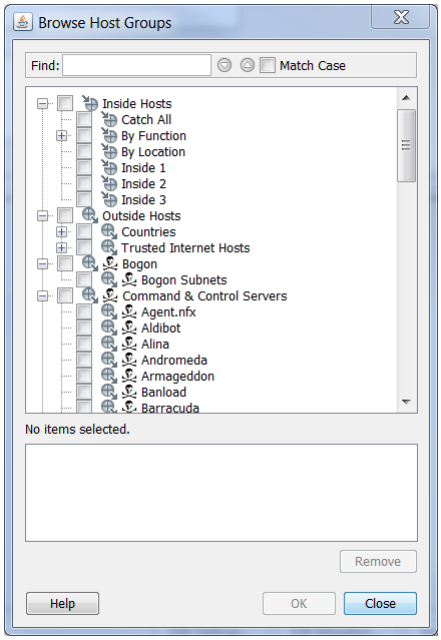
2. 在“主机策略管理器”对话框的**角色策略**部分，点击**添加**。



系统随即会打开“添加角色策略”对话框。



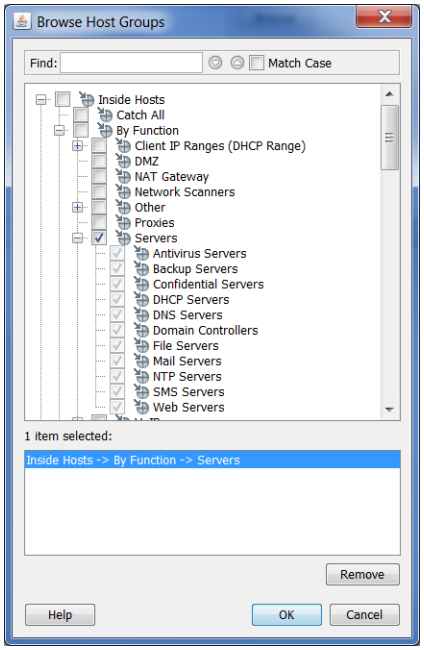
3. 在“名称”字段中，键入要添加的策略的名称（例如会计部门）。
4. 在“说明”字段中，键入说明（可选）。
5. 完成下列步骤之一：
   - 在“IP 地址范围”字段中键入特定主机 IP 地址或范围。
   - 在“分配到：主机组”字段中，点击**浏览**。系统随即会打开“浏览主机组”对话框。



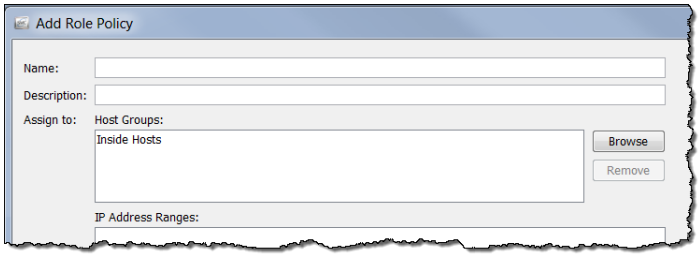
注意：

每个主机组都包含可防止某些警报的属性设置。要查看这些设置，请右键点击“企业”树菜单中的主机组，然后依次选择**配置 > 主机组属性**。系统随即会打开“编辑主机组”对话框。底部将列出“高级策略选项”。

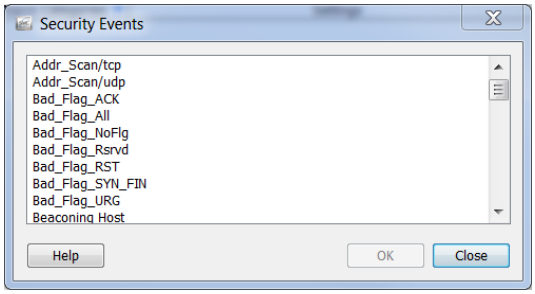
6. 点击要将该策略应用到的主机组。如果点击父主机，则会自动选择其下面的所有主机。



7. 点击**确定**。现在，这些组会显示在“添加角色策略”对话框的**分配到：主机组：**部分。



8. 点击“添加角色策略”对话框底部的**添加**。系统随即会打开“安全事件”对话框。

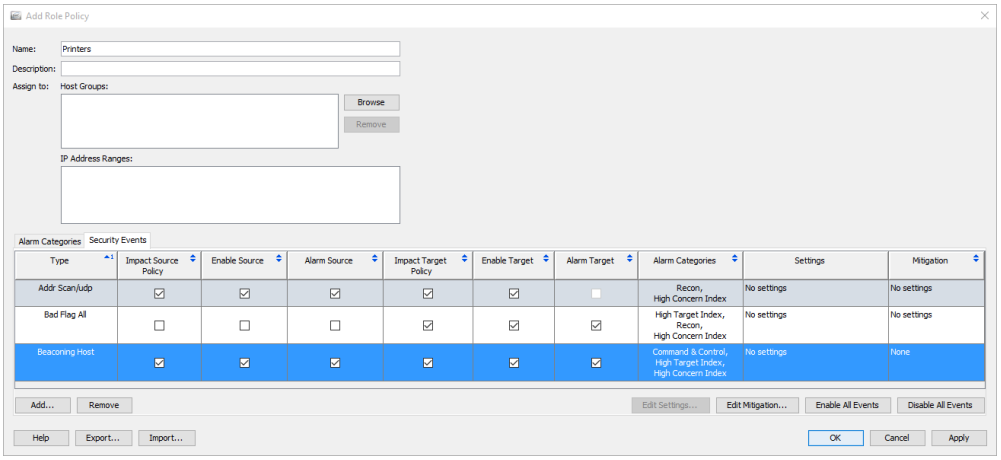


9. 点击要编辑的警报，然后点击**确定**。

注意：

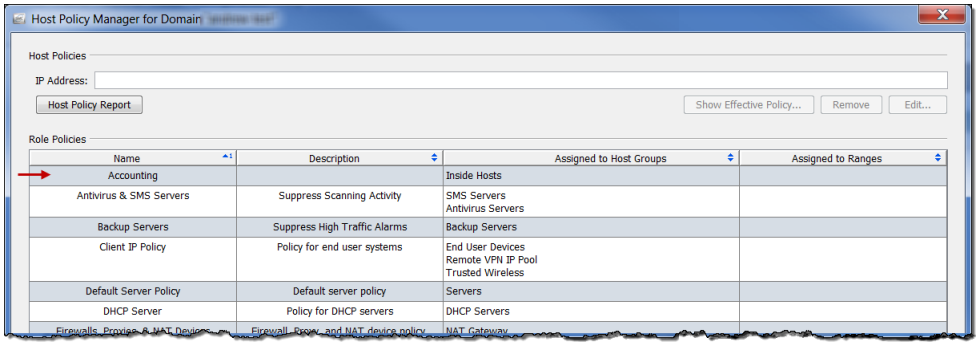
要选择多个警报，请按住 Ctrl 键并点击要添加的每个警报。要选择一系列警报，请点击要选择的范围顶部的警报，然后按住 Shift 键，再点击要选择的范围底部的警报。

这些警报将显示在“添加角色策略”对话框中。



10. 选中希望此策略触发的每个警报的复选框。

11. 依次点击**应用 > 关闭**。该策略会显示在“角色策略”部分的“主机策略管理器”对话框中。



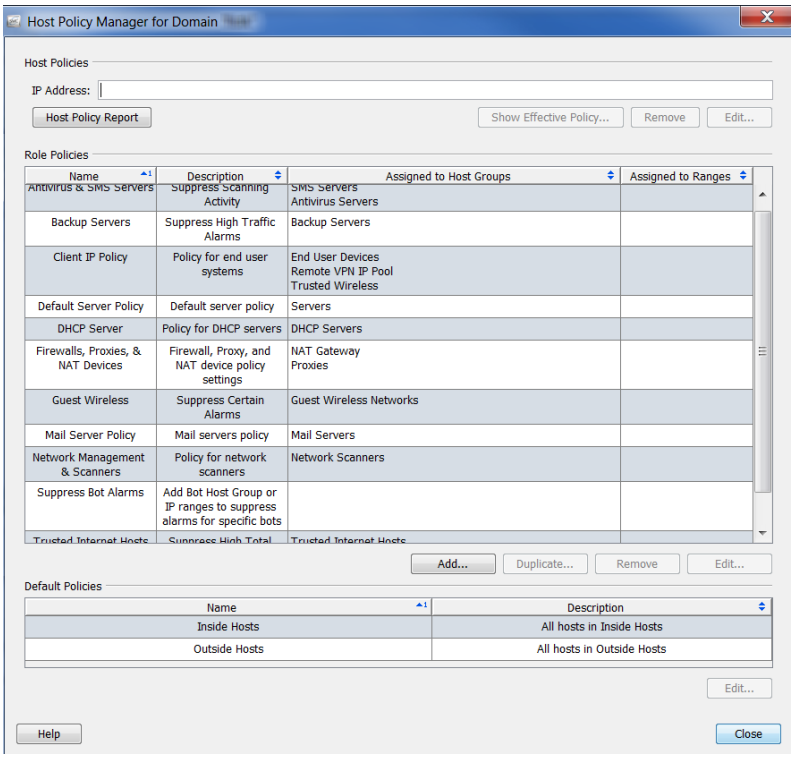
提示：

如果您发现要向一系列 IP 地址或多个 IP 地址范围分配角色策略，请为这些 IP 地址创建一个主机组，然后为此主机组分配一个角色策略。

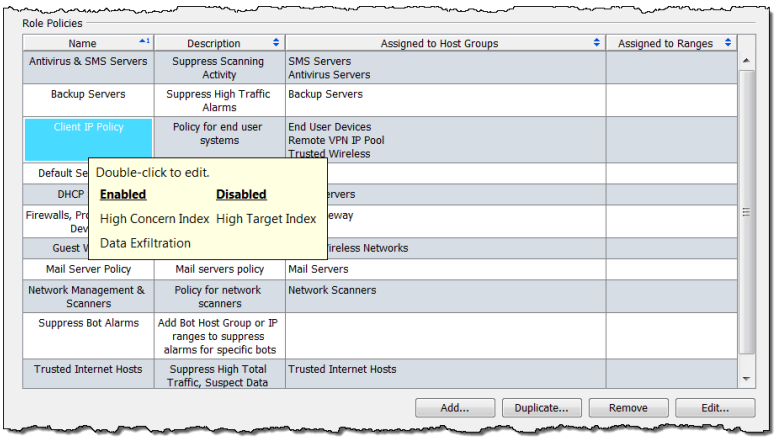
编辑角色策略

要编辑角色策略，请完成以下步骤：

1. 从主菜单中，依次选择**配置 > 主机策略管理器**。系统随即会打开“主机策略管理器”对话框。



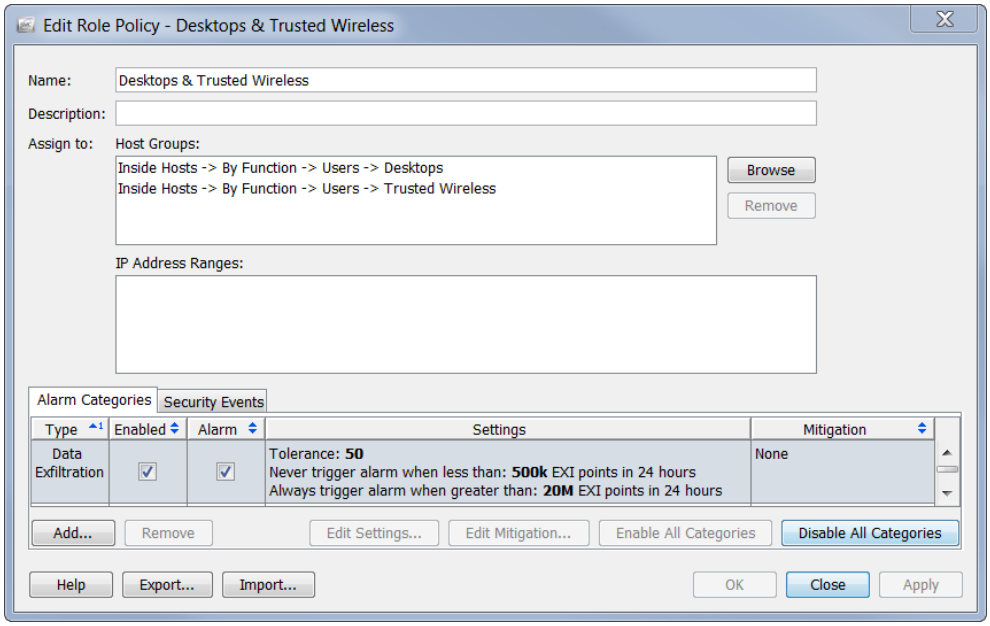
2. 在“主机策略管理器”对话框的**角色策略**部分，点击要编辑的角色策略的名称，然后点击**编辑**。



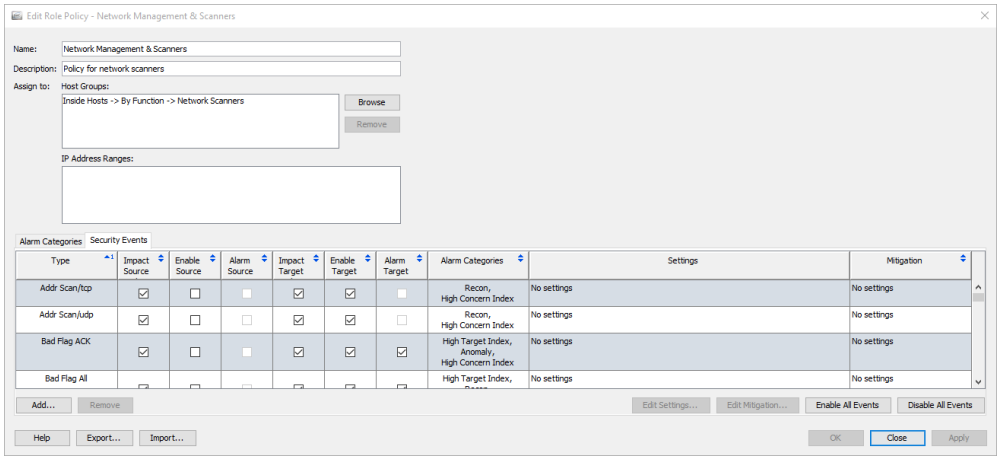
注意：

如果将光标悬停在某个条目上方，则显示所有已启用和已禁用的警报列表。上个示例中未禁用任何警报；因此，没有列出禁用的警报。

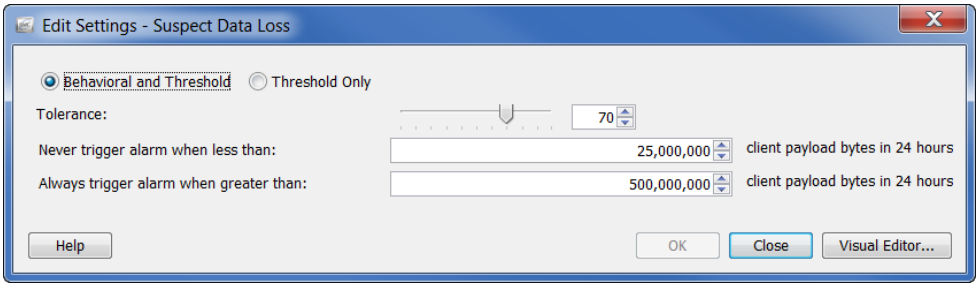
系统会打开“编辑角色策略”对话框。默认打开“警报类别”选项卡。



根据要编辑的警报，您可能需要点击“安全事件”选项卡。



3. 双击要编辑的警报（确保在“设置”列内点击）。系统会打开该警报的“编辑设置”对话框。



4. 完成编辑，完成后点击**关闭**。

注意：

- 有关不同类型的警报设置的信息，请参阅“警报”（第 261 页）。
- 有关特定警报的建议设置，请参阅“建议”（第 266 页）。

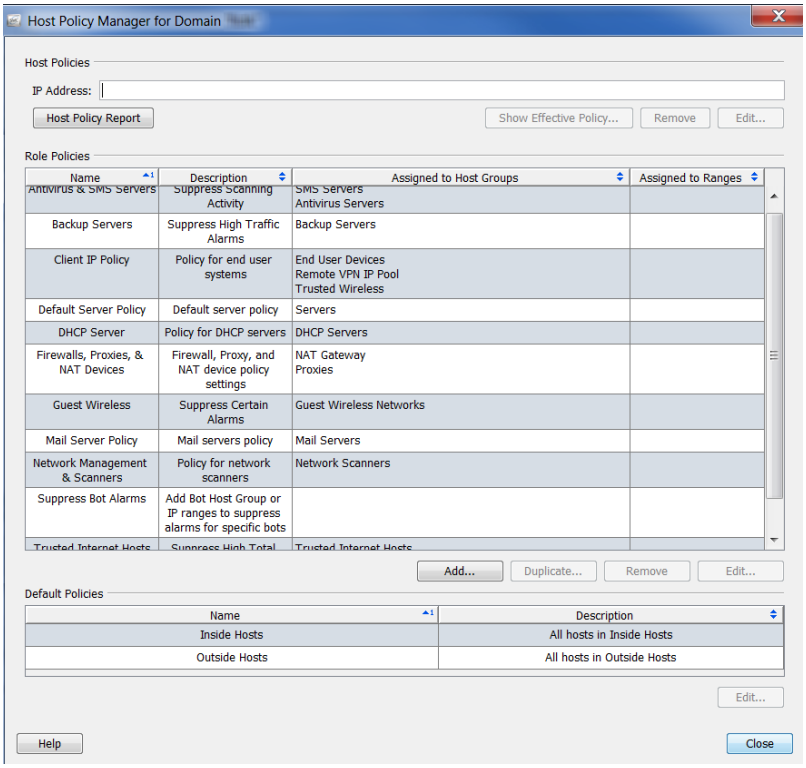
创建主机策略

您已学过，如果某个 IP 地址存在主机策略，Stealthwatch 将使用该主机策略中的相应警报类别设置来确定何时对该主机触发警报，而无论是否在角色策略或默认策略级别为此 IP 地址分配了其他警报。请记住，主机策略始终会覆盖角色策略和默认策略。

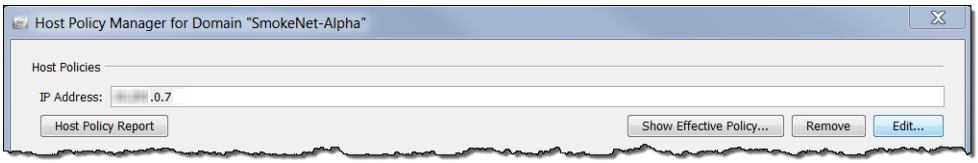
您可能希望编辑单个主机的主机策略（而不是编辑角色策略或默认策略）。如果您正在查看单个主机并发现一种情况，比如在警报表中，您看到针对特定主机触发了本不应触发或应按其他阈值触发的特定警报，您可能希望修改该特定主机的有效主机策略。

要添加主机策略，请完成以下步骤：

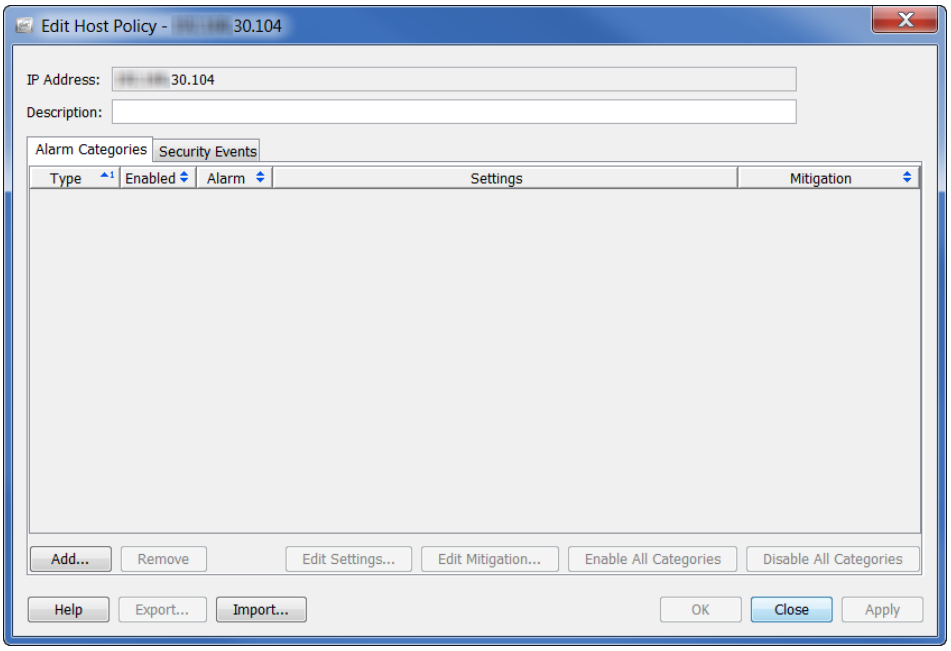
1. 从主菜单中，依次选择**配置 > 主机策略管理器**。系统将打开“主机策略管理器”对话框。



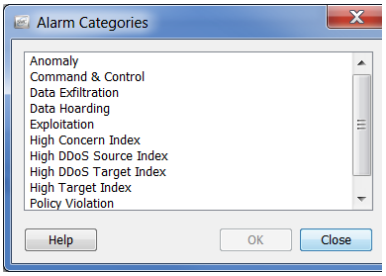
2. 在**主机策略**部分，输入要将向其添加主机策略的主机的 IP 地址。
3. 点击**编辑**。



系统会打开“编辑主机策略”对话框。默认打开“警报类别”选项卡。



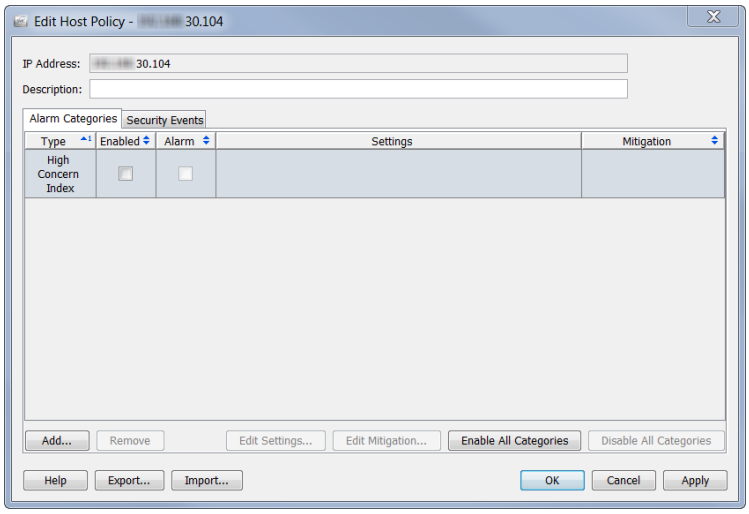
4. 点击**添加**。系统会打开“警报类别”对话框。
5. 点击要添加到此主机策略的警报类别，然后点击**确定**。



注意：

要选择多个警报，请按住 **Ctrl** 键并点击要添加的每个警报。要选择一系列警报，请点击要选择的范围顶部的警报，然后按住 **Shift** 键，再点击要选择的范围底部的警报。

这些警报类别会显示在“编辑主机策略”对话框中。



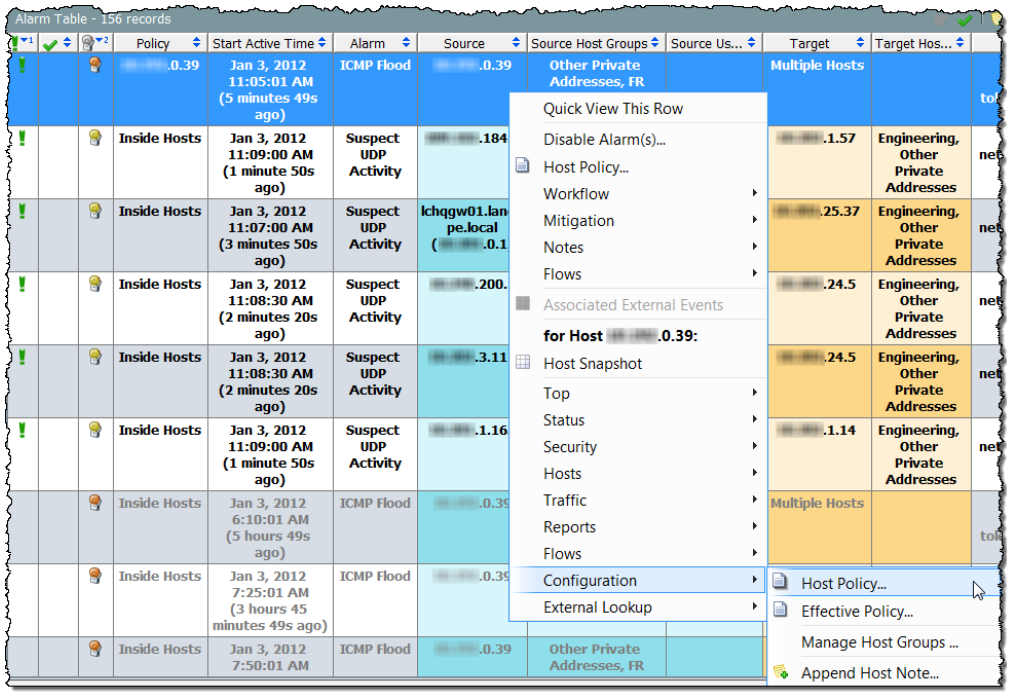
注意：

确保“启用”列中已选中您希望此策略触发的每个警报的复选框。

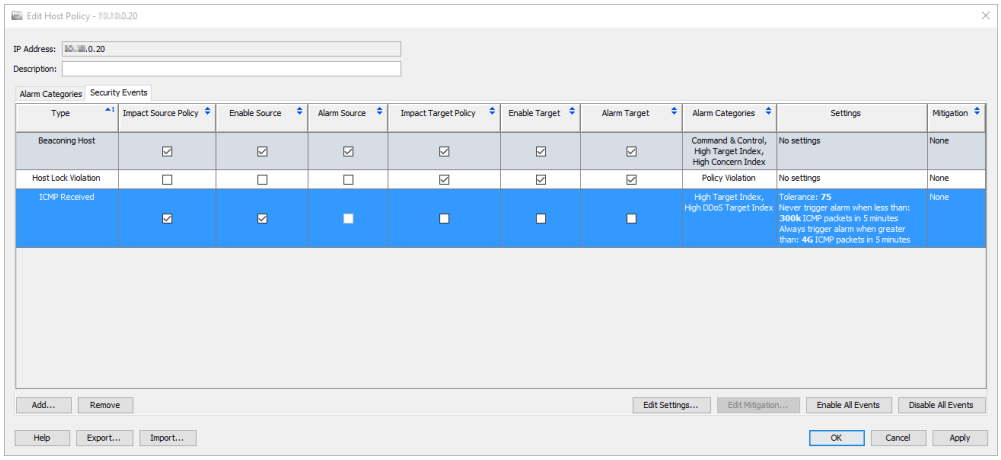
编辑主机策略

要编辑主机策略，请完成以下步骤：

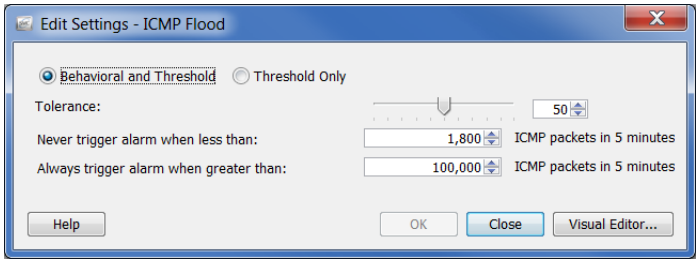
1. 右键点击主机 IP 地址，然后依次选择**配置 > 主机策略**。



系统随即会打开该主机的“主机策略”对话框。



2. 双击要修改的警报。系统会打开该警报的“编辑设置”对话框。



3. 进行更改并点击**关闭**。

注意：

- 有关不同类型的警报设置的信息，请参阅“警报”（第 261 页）。
- 有关特定警报的建议设置，请参阅“建议”（第 266 页）。

警报

基于差异的警报与开/关警报

当主机活动与过去行为相比发生重大变化时，就会触发警报。使用“主机策略管理器”可以更改这些警报类型的容差（即灵敏度）。这些警报称为基于差异的警报。下表列出了基于差异的警报：

注意：

警报类别也基于差异。

基于差异的警报	
异常	端口扫描
暴力登录	关系高总流量
命令和控制	关系型高流量
数据泄露	关系型 ICMP 泛洪
数据收集	关系型低流量
侵入漏洞	发起的最大关系型流数
高关注指数	提供的最大关系型流数
高 DDoS 源指数	关系型 SYN 泛洪
高 DDoS 目标指数	关系型 UDP 泛洪
高文件共享指数	关系往返时间
高 SMC 对等体	关系型服务器响应时间
高目标指数	关系型 TCP 重新传输率
高流量	关系高总流量
大量邮件	慢速连接泛洪
ICMP 泛洪	Span 来源
接收到的 ICMP	SSH 反向 Shell
邮件拒收	可疑的数据收集活动
邮件中继	可疑的数据丢失
启动的最大流数	SYN 泛洪
提供的最大流数	接收到的 SYN

基于差异的警报	
数据包泛洪	针对性数据收集活动
发起的新流数	已发起连接
提供的新流数	陷阱主机
策略违规	UDP 泛洪
侦测	接收到的 UDP

这种方法的主要优点是您可以调整系统，使发生的警报数量与您的组织需求相匹配。也就是说，如果您喜欢许多警报（即您只能容忍与预期行为的细微变化），可以降低相关策略中的容差设置。相反，如果您喜欢较少的警报（即您可以容忍与预期行为的重大变化），可以提高容差设置。基本上，基于差异的警报的每个设置都与数值相关，并且可以上下调整此值。

基于差异的警报中使用的阈值是系统根据最近活动的基准值和配置的容差生成的。这使得主机能够随着时间的推移而改变，而不会失去在其行为发生根本性变化时发出警报的能力。容差提供了一种控制可接受的变化程度的方法。实质上，您有能力调整警报阈值级别的灵敏度（即“将噪音调低”到所需的任何级别）。

对于基于差异的警报，主机行为与其基准必须达到一定水平的偏差，才会触发警报。例如，如果“高总流量”警报的容差级别被设置为 50，则系统将忽略超过期望值（主机的基准值）50% 以内的值，但会对高于该值的值发出警报。

注意：

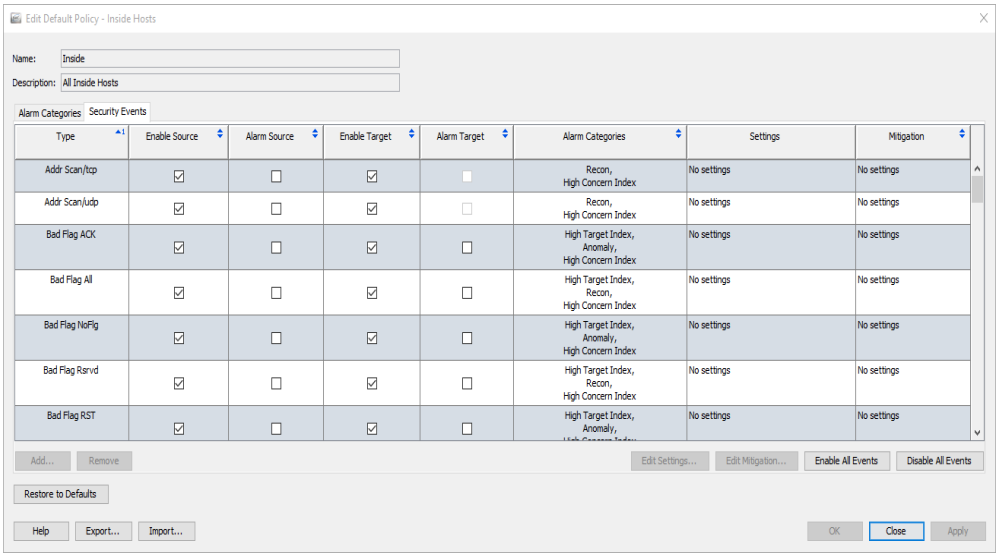
有关警报设置的详细信息，请参阅“基于差异的警报的设置”（第 263 页）。

第二种警报类型是可以打开或关闭的警报。触发此类警报的标准与基于差异的警报不同。在使用具有开/关设置的警报的情况下，主机的行为必须匹配某些条件，彼此必须完全一致，才会触发此类警报。如果所有这些条件都不存在，则不会触发该警报。例如，要触发蠕虫活动警报，则必须发生以下**所有**行为：

- 源主机已扫描多个子网。
- 至少有一个目标主机已连接到源主机。
- 此目标主机已将信息传输到源主机。

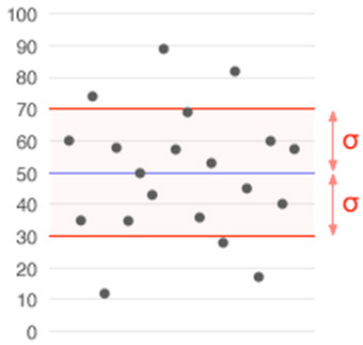
即使其中只有一个条件不存在，也不会触发警报。

通过查看“编辑默认策略”对话框的“设置”列，您可以确定哪些是基于差异的警报，哪些是开/关警报。如果是基于差异的警报，则显示为该警报指定的容差值。如果是开/关警报，则显示“无设置”条目。



基于差异的警报的设置

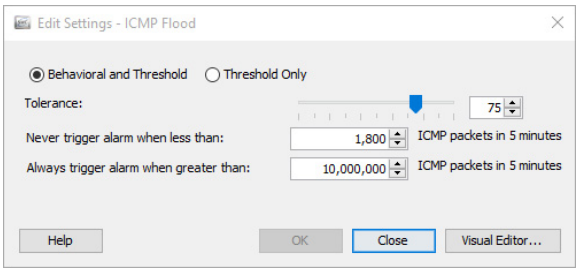
如上一节中所述，基于差异的警报中使用的阈值是系统根据最近活动的基准值和配置的容差生成的。容差是指“相比规范的标准偏差量”，为您提供了一种调整警报阈值级别灵敏度的方法。



平均值为 50（以蓝色显示）、标准偏差 (σ) 为 20 的数据集。

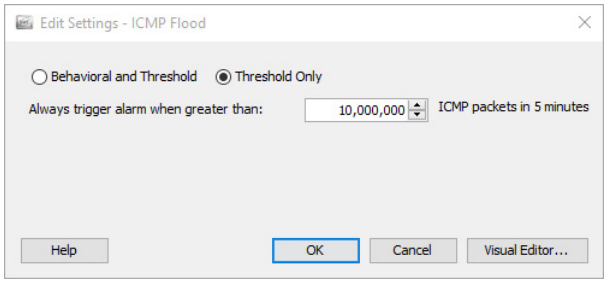
在统计学中，标准偏差广泛用来测量可变性或多样性。它显示了与平均值（即平均值或预期值）相比的变化程度。低标准偏差表示数据点往往十分接近该平均值，而高标准偏差表示数据点分布在较大的值范围内。

以下示例显示了基于差异的警报的“编辑设置”对话框。

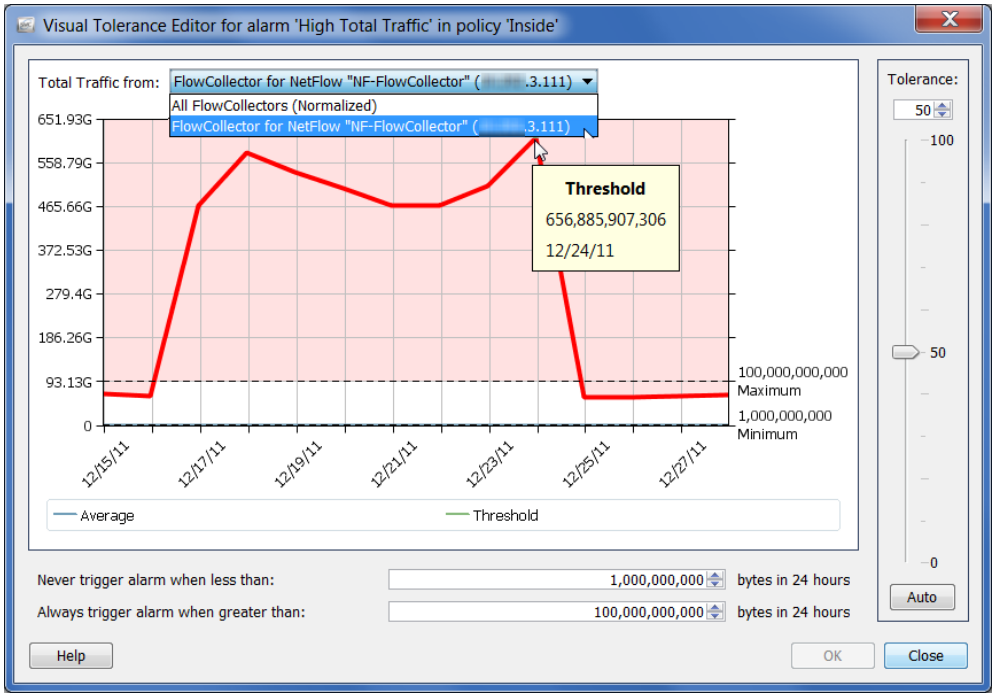


基于差异的警报包含以下可调整的设置：

- 行为和阈值 - 当选择此选项时，该对话框显示容差设置、最小阈值和最大阈值。
  - 容差 - 0 与 100 之间的一个相对数，指示在发出警报之前，在多大程度上允许实际行为超过预期行为。这让用户可以定义何为“显著差异”。
    - 容差为 0 意味着对超过预期值的任何值发出警报；这非常敏感，并将产生许多警报。
    - 100 的容差是允许警报的最高级别。这将大幅减少触发警报的次数，但单纯禁用警报将导致不会发出警报。
    - 容差为 50，表示主机将忽略超过预期值 50% 以内的值，但是会对该限制以上的值发出警报。
  - *小于其时从不触发警报：*也称为*最小阈值*，这是一个静态值，表示允许触发警报的最低值。当发现的值低于此设置时，不会触发警报。换言之，即使主机大大超过其预期值，但如果它不超过此对话框中指示的最小值，则不会触发警报。
  - *大于其时始终触发警报：*也称为*最大阈值*，这是一个静态值，表示未触发警报时允许的最高值。当发现的值超过此设置时，则触发警报。换言之，如果主机的值超过此对话框中指示的最大值，即使这是该主机的预期行为，也会触发警报。
- 仅阈值 - 当选择此选项时，该对话框仅显示最大阈值设置。



点击**可视编辑器**，可访问“可视编辑器”对话框。“可视容差编辑器”是调整特定警报的主机策略或主机组策略设置的图形方式，如以下示例中所示。



注意：

如果仅使用了一个流量收集器，则从屏幕顶部的**总流量来自**下拉列表中点击**流量收集器**选项，可查看相关警报的实际值。如果正在使用多个流量收集器，则点击**规范化**选项可规范这些值。

建议

本节提供在收到过多不必要警报时微调网络的建议。本节根据一些最常见的警报类型对这些建议进行了细分，它们将按字母顺序列出。

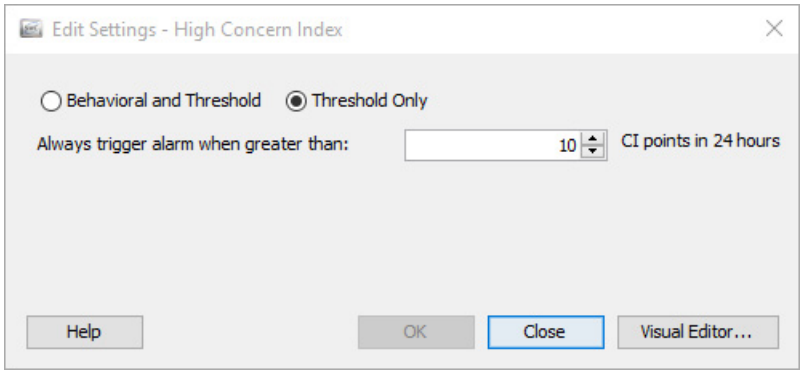
注意：

- 要了解有关这些警报和其他警报的详细说明，请参阅 *SMC 客户端联机帮助*中的“警报列表”主题。
- 有关如何调整下面列出的警报设置的详细信息，请参阅“基于差异的警报的设置”（第 263 页）。

高关注指数

“高关注指数”显示自上次存档后 CI 点数过高的主机的信息，由此帮助您确定威胁的优先级，并将重点放在真正重要的事件上。Stealthwatch 可按严重性从高到低提供少量可行项目，让您不必再查看数以千计的每日警报。

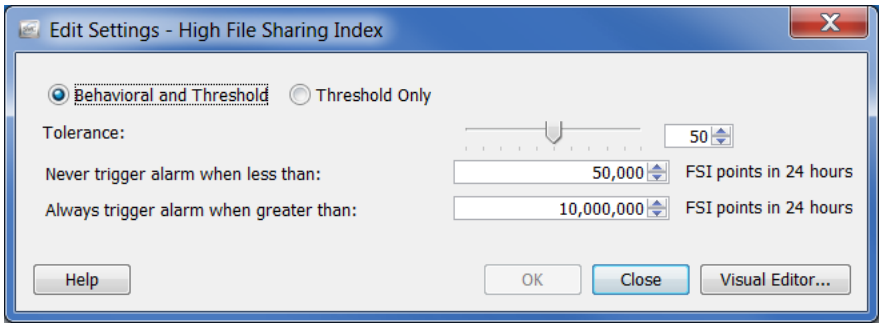
通常，当内部主机引发“高关注指数 (CI)”警报时，表示该主机不再正常工作。如果您确信所看到的高 CI 警报并非由入侵或误用导致，请调整“主机策略管理器”上的设置。此外，您还可以指定触发该警报的安全事件。



高文件共享指数

“高文件共享指数 (FSI)”警报表示，文件共享活动超出了“主机策略管理器”中定义的 FSI 阈值。如果引发高 FSI 警报的主机被用于文件共享，您可以完成以下步骤之一来减少所看到的不必要警报数量：

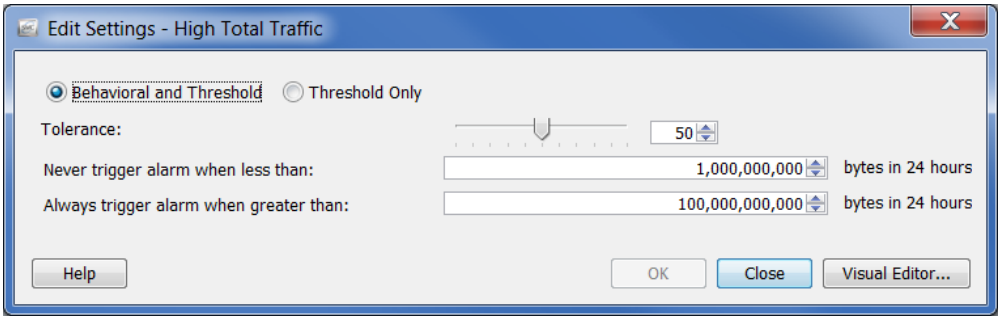
- 通过点击相应策略中的**启用**复选框来删除复选标记，可对影响相关主机/主机组的策略禁用“高文件共享指数”警报。
- 提高影响相关主机/主机组的策略的“高文件共享指数”警报阈值或容差设置。



高总流量

“高总流量”警报表示，入站总流量加上出站总流量超出了主机的策略设置。如果您对所看到的高总流量警报数量感到不满意，请在相应的策略中调整设置。

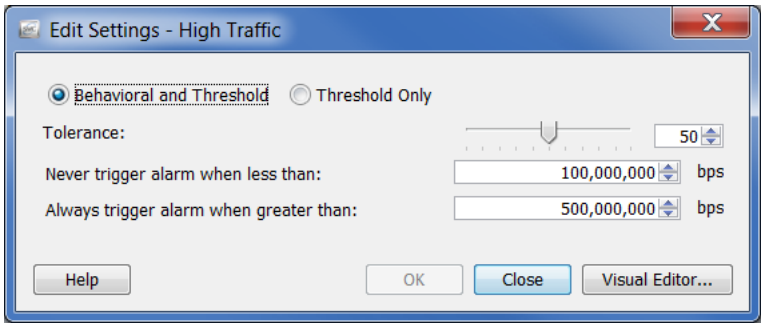
将相关主机或主机组的策略设置提高到所报告的平均字节数以上。



高流量

“高流量”警报表示，过去五分钟内的主机平均流量速率超过了可接受的流量值限制。如果您对所看到的高流量警报数量感到不满意，请调整相应策略中的设置。

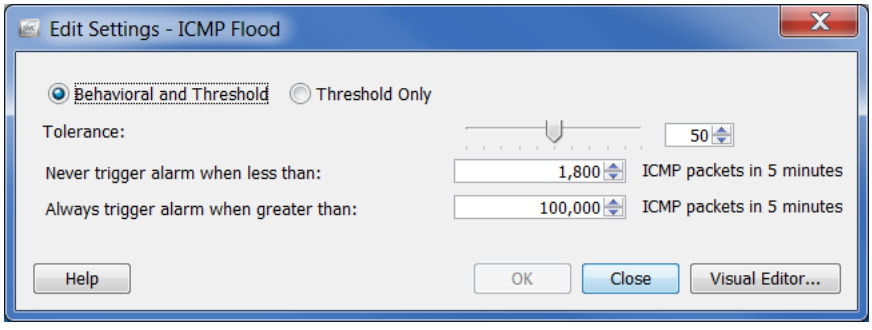
将相关主机或主机组的策略设置提高到所报告的平均字节数以上。



ICMP 泛洪

“ICMP 泛洪”警报表示，源主机在过去五分钟内发送的 ICMP 数据包数过多。这可能指示拒绝服务 (DoS) 攻击或非隐蔽的扫描活动。要解决此问题，请查明引发警报的主机类型。它可能是管理服务器，正在向网络上的主机发送大量 Ping 操作。

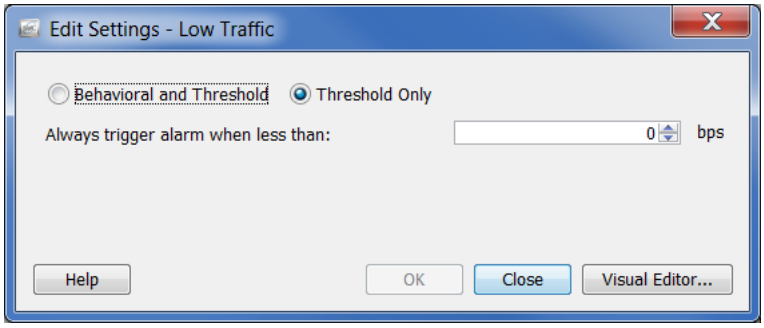
要停止警报，请点击相应策略中的**启用**复选框以删除复选标记，从而对相关主机/主机组禁用“ICMP 泛洪”警报。



低流量

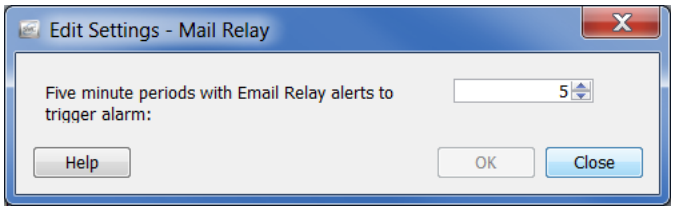
“低流量”警报表示，过去五分钟内的主机平均流量速率低于可接受的最小流量值。如果您对所看到的低流量警报数量感到不满意，请调整相应策略中的设置。

将相关主机或主机组的策略设置提高到所报告的平均字节数以上。



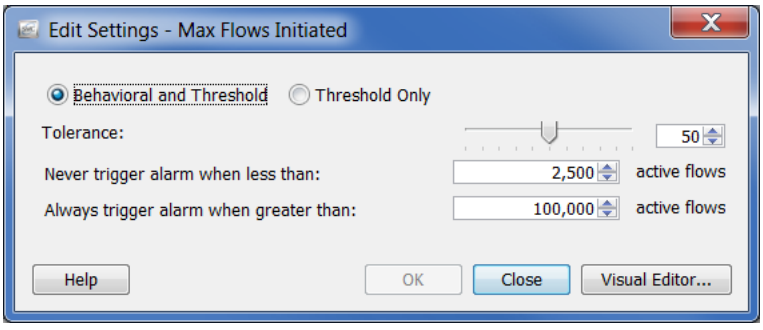
邮件中继

“邮件中继”警报表示，目标主机可能正在作为邮件中继运行。如果这些是真正的邮件服务器，可以点击相应策略中的**启用**复选框以删除复选标记，从而对相关主机/主机组禁用“邮件中继”警报。



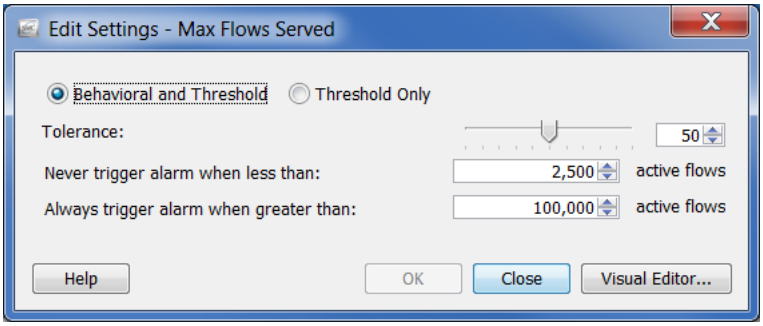
启动的最大流数

“启动的最大流数”警报表示，主机发起的流数超过了允许值，该值已在相应的*大于其时始终触发警报*策略设置中指定。请调整设置，特别是在主机属于域控制器时。



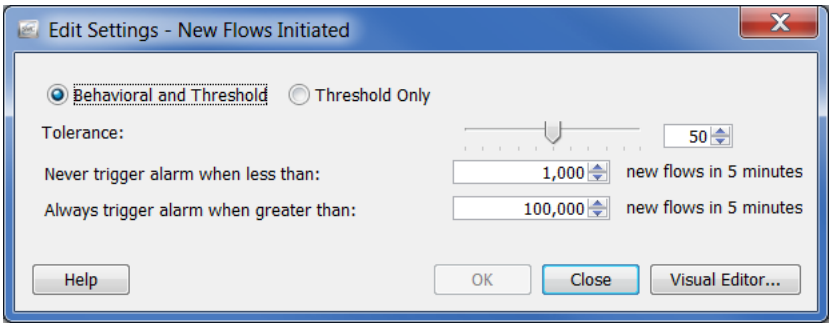
提供的最大流数

“提供的最大流数”警报表示，主机提供的流数超过了允许值，该值已在相应的*大于其时始终触发警报*策略设置中指定。请调整设置，特别是在主机属于域控制器时。



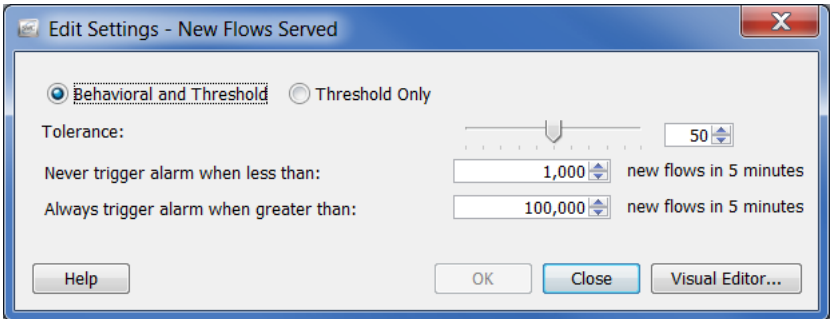
发起的新流数

“发起的新流数”警报表示，主机在五分钟内发起的新流总数超出了策略设置。请调整设置，特别是在主机属于域控制器时。



提供的新流数

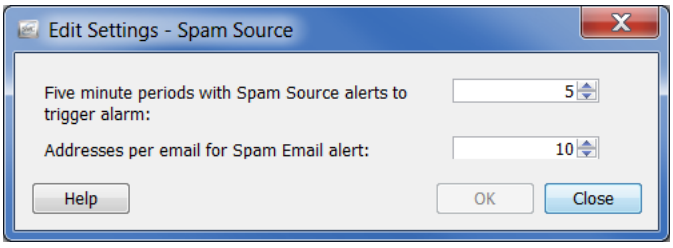
“提供的新流数”警报表示，主机在五分钟内提供的新流总数超出了策略设置。请调整设置，特别是在主机属于域控制器时。



垃圾邮件源

“垃圾邮件源”警报表示，源主机可能正在发送垃圾邮件。如果该主机是邮件服务器，可以点击相应策略中的**启用**复选框以删除复选标记，从而对相关主机/主机组禁用“垃圾邮件源”警报。

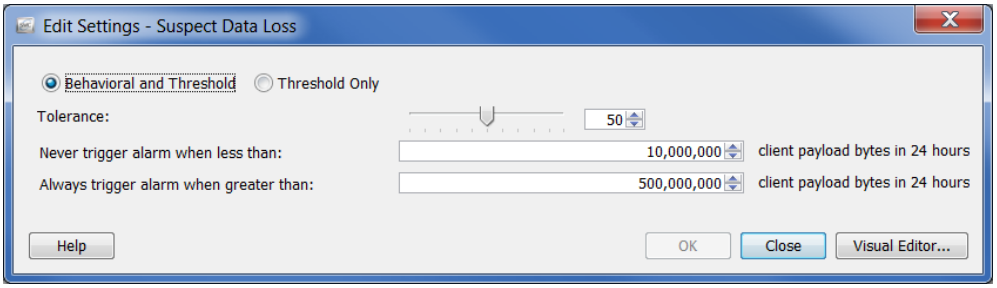
如果主机不是邮件服务器，则它可能受到感染。



可疑的数据丢失

“可疑的数据丢失”警报表示，“外部主机”组的总 TCP 和 UDP 负载数据超过了策略设置。如果您对所看到的“可疑的数据丢失”警报数量感到不满意，请对已知的高流量外部主机组（例如 YouTube、Facebook、业务合作伙伴）禁用此警报。

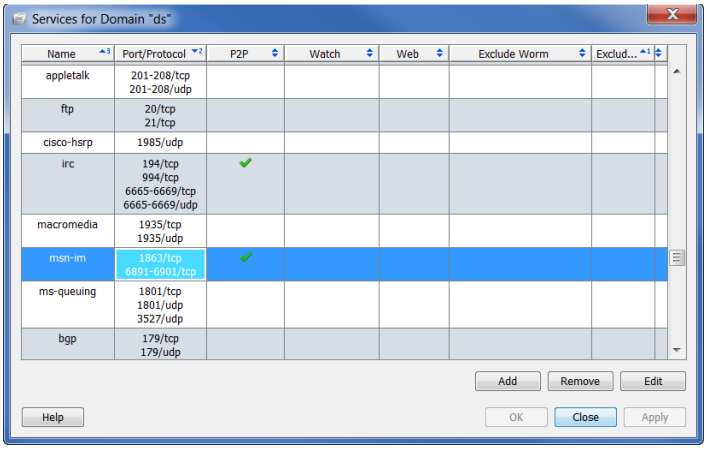
然后，针对重要主机或主机组调整策略设置。将阈值提高到所报告的平均字节数以上。

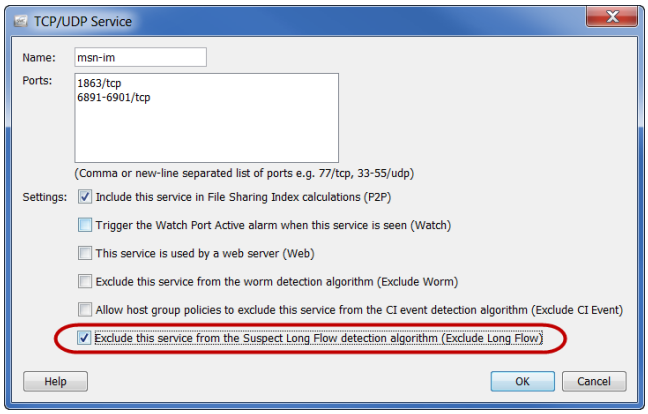


可疑的长流

“可疑的长流”警报表示，内部主机与外部主机之间的 IP 通信超过了“将流确定为持续时间过长所需的秒数”设置。此警报检测可疑的通信通道，例如间谍软件、远程桌面技术（即 gotomypc.com）、VPN、IRC 僵尸网络以及其他隐蔽的通信方式。使用 IM 技术的内部主机容易引发这种警报，因为流的持续时间超过允许的最大值（默认为 9 小时）。

您可以通过修改配置的服务从生成的“可疑的长流”警报中排除 IM 技术，例如 AOL AIM（端口 5190）、Yahoo IM（TCP 端口 5050）和 MSN Messenger（TCP 端口 1863）。从主菜单中，依次选择**配置 > 服务**。系统将打开相应域的“服务”对话框。





选择包含要编辑的服务名称的行，然后点击屏幕底部的**编辑**。点击**从“可疑的长流”检测算法中排除此服务（排除长流）**复选框以添加复选标记。

或者，您可以为授权网络（例如业务合作伙伴）创建一个“外部”主机组，然后在相应策略中禁用“可疑的长流”警报。

注意：

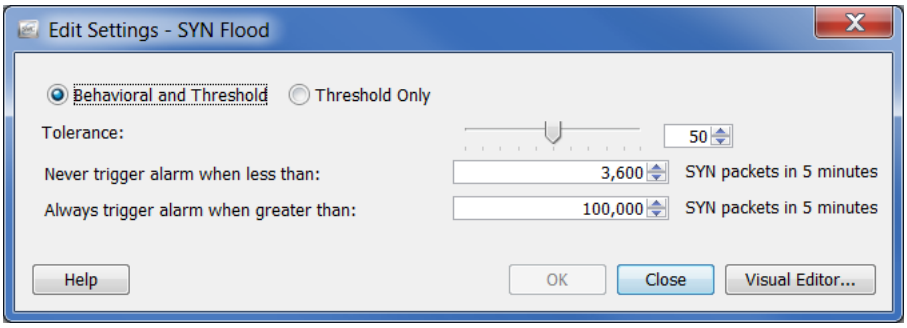
对于“内部主机”始终会引发“可疑的长流”警报，无论物理客户端/服务器关系如何。如果对“外部主机”禁用此警报，则会从此警报中排除任何与该外部主机连接的内部主机。

可疑的 UDP 活动

“可疑的 UDP 活动”警报表示，已在 UDP 端口上扫描多个主机的主机成功向另一主机发送了一个大数据包。此类行为表示多个基于 UDP 的单数据包蠕虫，例如 SQL Slammer 和 Witty。立即调查此警报。

SYN 泛洪

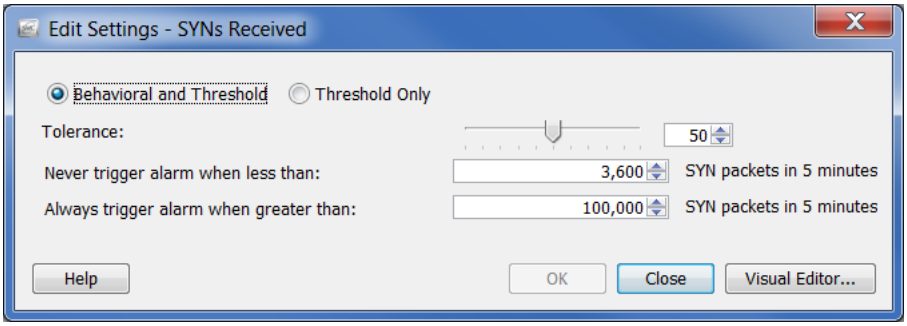
“SYN 泛洪”警报表示，主机在五分钟内发送的 TCP 连接请求（SYN 数据包）数过多。调查此警报，以查看是否正在发生 DOS 攻击或非隐蔽的扫描活动。



接收到的 SYN

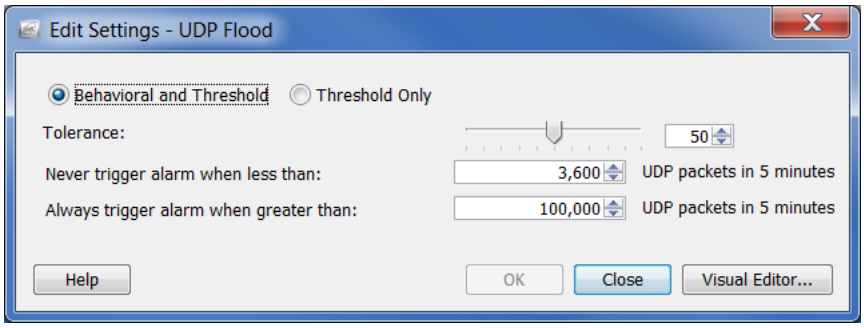
“接收到的 SYN”警报表示，主机在五分钟内收到的未应答 TCP 连接请求（SYN 数据包）数过多。此警报可能表示已分布的（多对一）DoS 攻击。

但是，服务器通常会收到大量 SYN 数据包。如果是这种情况，请将*小于其时从不触发警报*设置提高到所看到的平均警报数以上。您可能希望将比其他服务器收到更多 SYN 数据包的服务器隔离到单独的主机组中，例如 Web 服务器与应用服务器。



UDP 泛洪

“UDP 泛洪”警报表示，源 IP 在过去五分钟内发送的 UDP 数据包数过多。调查此警报，以查看是否正在发生 DOS 攻击或非隐蔽的扫描活动。



蠕虫活动

“蠕虫活动”警报表示，主机在特定端口上扫描和连接了多个子网。此警报的详细信息部分指定用于观察该活动的端口。

对于域控制器，在 UDP 端口上执行地址扫描及 ping 扫描是正常的。如果“蠕虫活动”警报发生在具有域控制器的主机组中，在相应策略中删除“高关注指数”警报“安全事件”选项卡上 **Addr_Scan/udp** 和 **Ping** 复选框中的复选标记有助于防止这些警报。

13

处理文档

概述

本章介绍了一些过程，例如，如何使用一组特定的布局设置和过滤器设置保存 SMC 文档、将文档添加到登录文档列表、创建 DAR 文件、共享文档、定期生成文档以及通过邮件向他人发送文档。

本章包含以下主题：

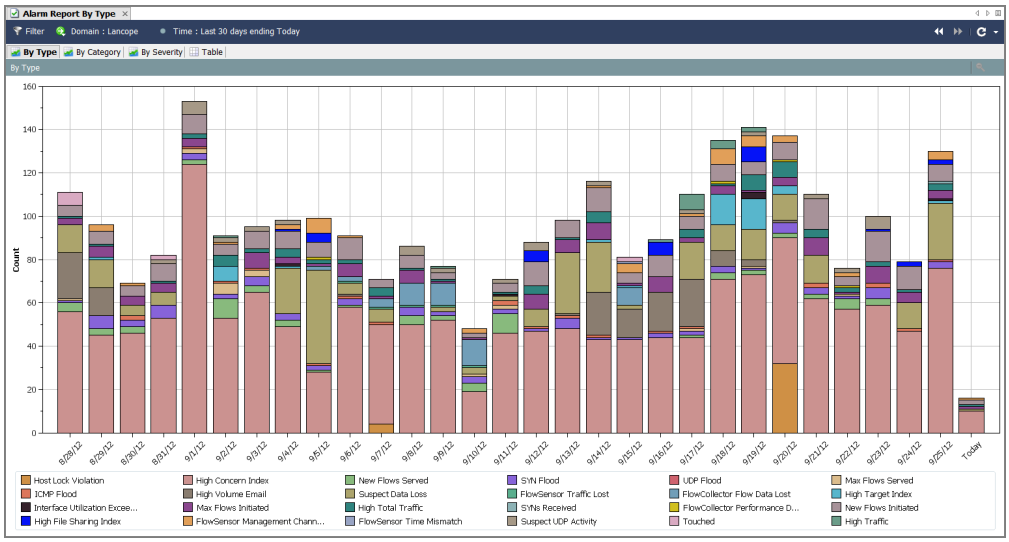
- 保存文档
- 共享文档
- 计划文档

保存文档

如果您重新排列了 SMC 文档的布局，并且希望保存该布局以供以后使用，请保存该文档。保存文档时，该文档将被保存到 SMC 设备中以供随时检索。

要保存文档，请完成以下步骤：

1. 打开您想要保存的文档。例如，我们将打开“按类型的警报报告”文档。



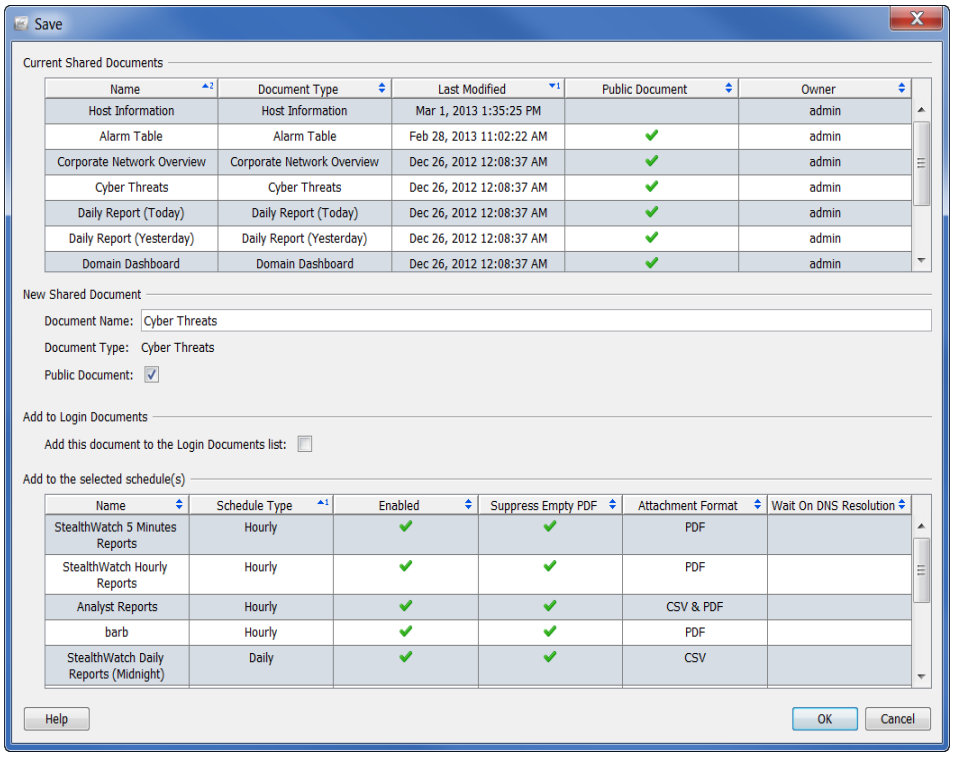
2. 对布局或过滤器设置进行任何所需的更改。
3. （可选）从 SMC 主菜单中选择**文件 > 打印设置**，并在打开的对话框中配置您希望文档在每次打印时的外观。点击**确定**保存更改。
4. （可选）若要查看文档作为 PDF 显示的方式，请选择**文件 > 打印预览**。

注意：

如果要对文档布局进行更改并保留更改（例如更改列位置或更改显示的列），请选择文件 > 使用设置为默认值。这些更改将在您下次打开文档时生效。

5. 执行以下操作之一：
   - 如果您只想用相同的名称替换以前的版本，请从 SMC 主菜单中选择**文件 > 保存**。
   - 如果下列任一情况适用，请从 SMC 主菜单中选择**文件 > 另存为**：
     - 如果要以新名称保存文档副本。
     - 如果您已创建了一个新文档，并且是第一次保存文档。

“保存”对话框随即打开。



6. 在“名称”字段中，为文档键入一个可以轻松识别的名称。（系统会为您建议一个名称。）
7. （可选）如果希望其他用户能够在其用户名下打开此文档，请选中**公共**复选框。

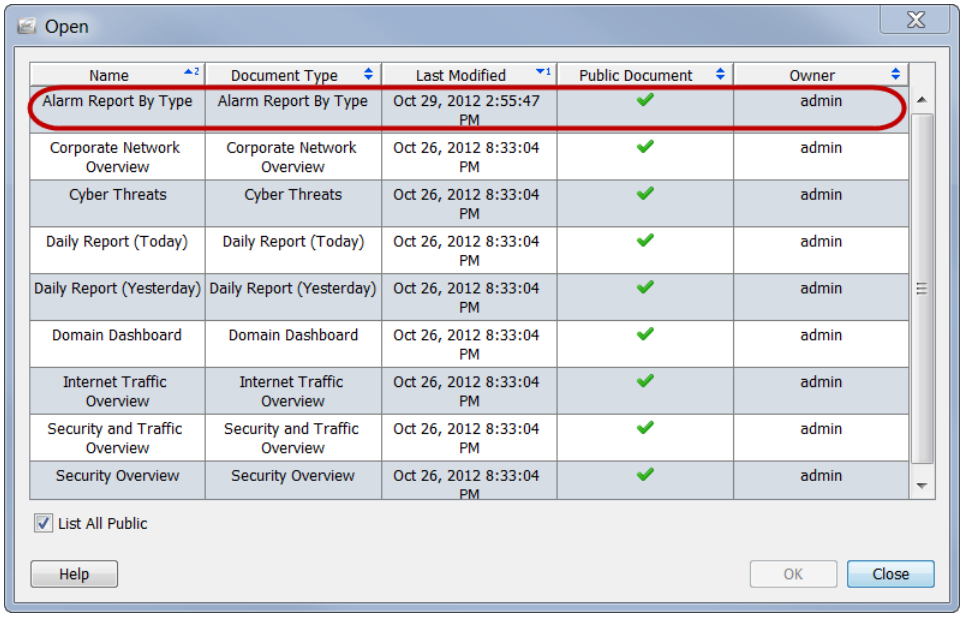
注意：
有关公共文档的详细信息，请参阅“公共文档”（第 283 页）。

8. （可选）如果希望每次在您的用户名下登录到 SMC 客户端界面时都自动打开文档，请选中“将此文档添加到登录文档列表”复选框。

注意：
有关登录文档的详细信息，请参阅“登录文档”（第 278 页）。

9. 点击**确定**。文档会被保存到 SMC 设备。现在，您可以在任何具有 SMC 访问权限的计算机上，使用您指定的布局和/或过滤器设置，在您的用户名下打开此文档。

10. 要打开此文档，请从 SMC 主菜单中选择**文件 > 打开**。“打开”对话框随即打开。



11. 选择文档并点击**确定**。

注意：

默认情况下，仅显示保存在您的用户名下的文档。若要列出所有文档（包括由其他用户创建的文档），请选中列出所有公共文档复选框。

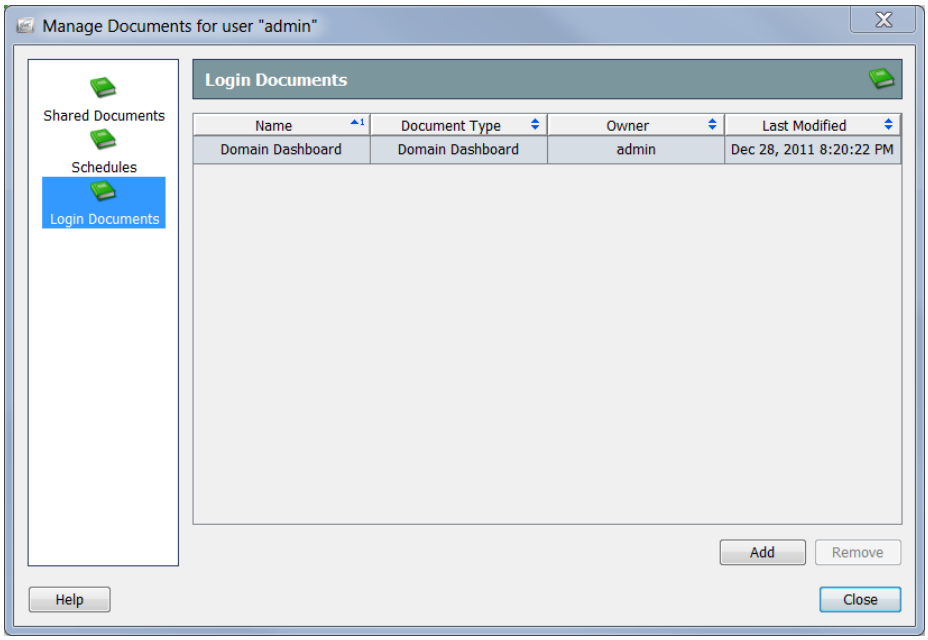
登录文档

您可以将任何文档添加到您的登录文档列表中。每次登录 SMC 客户端界面时，登录文档都会自动打开。此功能对于查看您将定期手动打开的文档非常有用。

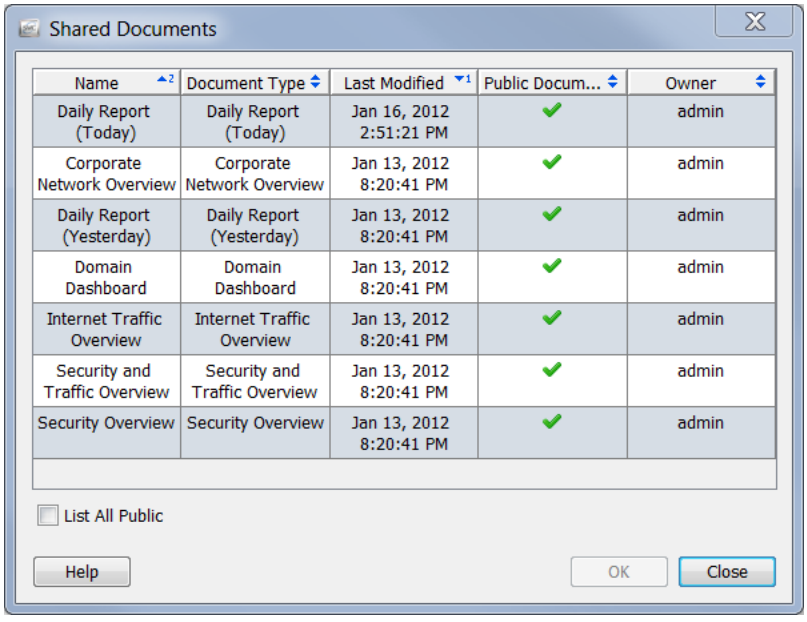
要使文档成为登录文档，请完成以下步骤：

1. 从 SMC 主菜单中，选择**文件 > 管理文档**。“管理文档”对话框随即打开。

2. 点击**登录文档**图标。“登录文档”页面随即打开。



3. 点击**添加**。“共享文档”对话框随即打开。



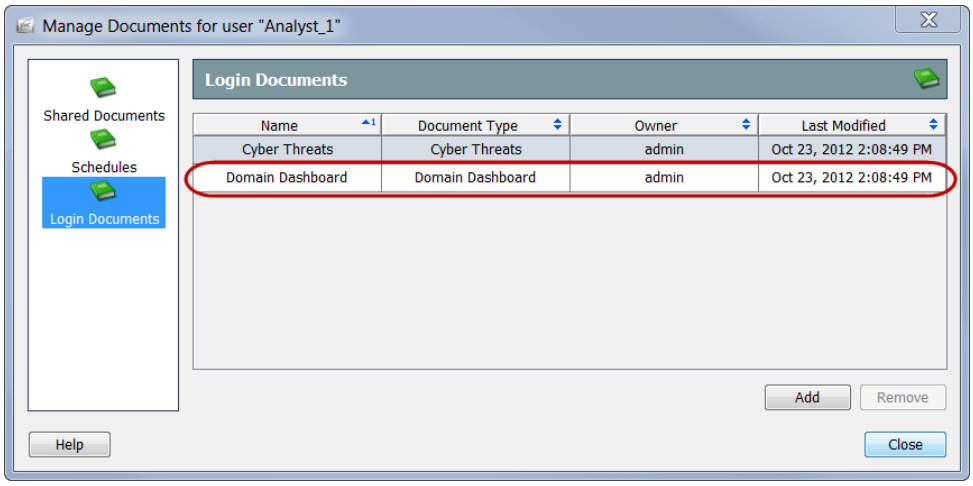
4. 选中**列出所有公共文档**复选框以查看其他用户保存的所有公共文档。

5. 选择要添加到用户的登录文档列表的文档。对于本示例，我们将选择“域控制面板”文档。

注意：

要选择多个文档，请按住 **Ctrl** 键并点击要添加的每个文档。要选择文档范围，请点击要选择的范围顶部的文档，按住 **Shift** 键，然后点击要选择的范围底部的文档。

6. 点击**确定**。“共享文档”对话框随即关闭。您选择的文档将显示在用户的登录文档列表中。



7. 点击**关闭**退出“管理文档”对话框。

共享文档

与其他用户共享文档的两种方法是：

- 将文档导出为 DAR 文件
- 使文档公开

DAR 文件

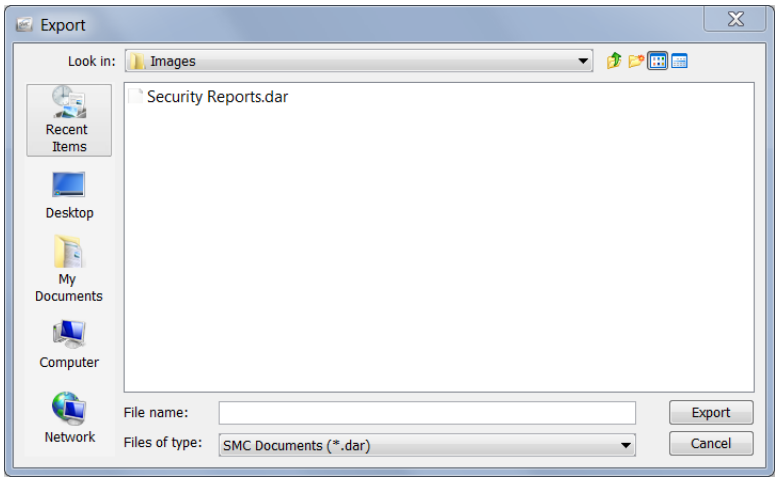
将文档导出为 DAR 文件允许您对文档执行以下操作：

- 将其复制到计算机的硬盘驱动器。
- 将其复制到闪存驱动器，以便在可访问 SMC 设备的另一台计算机上使用。
- 与他人分享。

导出 DAR 文件

要将文档导出为 DAR 文件，请完成以下步骤：

1. 打开要导出的文档。
2. 对布局或过滤器设置进行任何所需的更改。
3. 从 SMC 主菜单中，选择**文件 > 导出为 DAR 文件**。系统随即会打开“导出”对话框。



4. 导航到要导出文档的位置。
5. 在“文件名”字段中，为文档键入一个名称。

6. 点击**导出**。该文档在您选择的位置中另存为 DAR 文件。此外，“文档”选项卡将采用新名称。

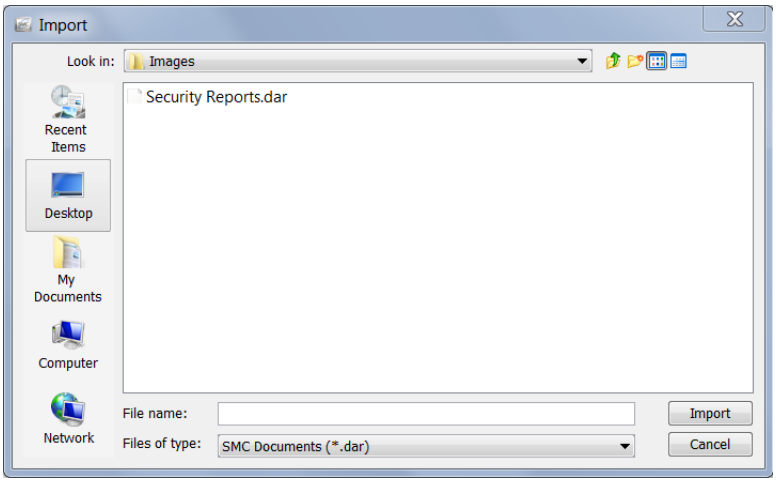
注意：

如果将光标悬停在“文档”选项卡上，屏幕上会出现一个工具提示，其中显示有关文档的详细信息，如原始文档名称和文档创建人（“拥有者”）。

导入 DAR 文件

如果有人将文档导出为 DAR 文件并将其提供给您，您随时可以通过导入它在 SMC 客户端界面中打开它。为此，请执行以下操作：

1. 从 SMC 主菜单中，选择**文件 > 导入 DAR 文件**。系统随即会打开“导入”对话框。



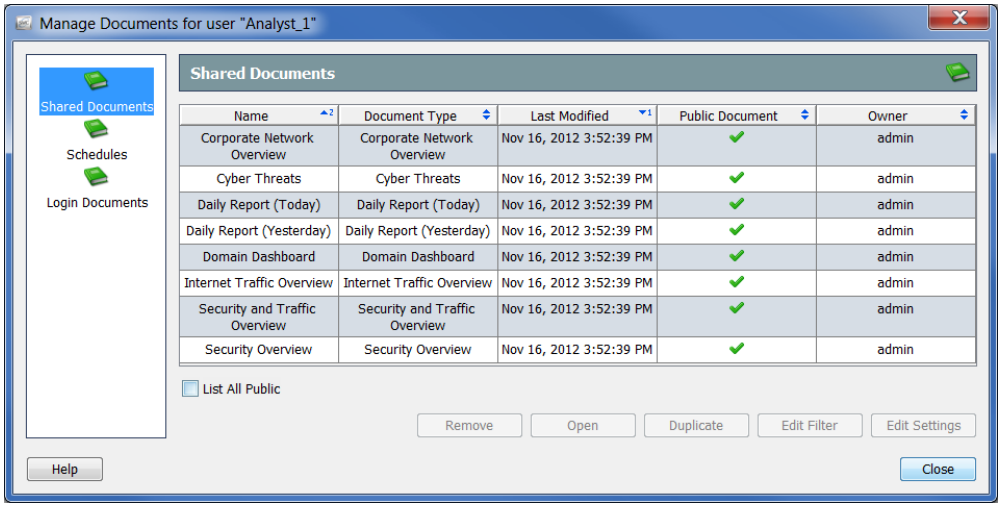
2. 导航到 DAR 文件所在的位置。
3. 选择 DAR 文件。
4. 点击**导入**。文档会在 SMC 客户端界面打开。

公共文档

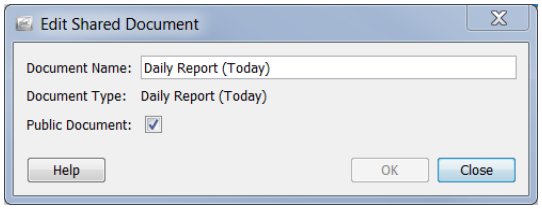
当您使文档公开时，可以使其他用户能够访问 SMC 设备，以在其用户名下查看文档。

正如“保存文档”（第 276 页）中所述，您可以使文档成为公共文档。通过完成以下步骤，可以使以前保存的文档成为公共文档：

1. 从主菜单中，选择**文件 > 管理文档**。“管理文档”对话框随即打开。



2. 点击**共享文档**图标。系统随即会打开“共享文档”页面。
3. 选择所需文档。
4. 点击**编辑设置**。系统将打开“编辑设置”对话框。



5. 选中**公共文档**复选框。
6. 点击**确定**退出“编辑”对话框。
7. 点击**关闭**退出“管理文档”对话框。

任何有权访问 SMC 客户端界面的用户都可以查看此文档以及已成为公共文档的其他所有文档。

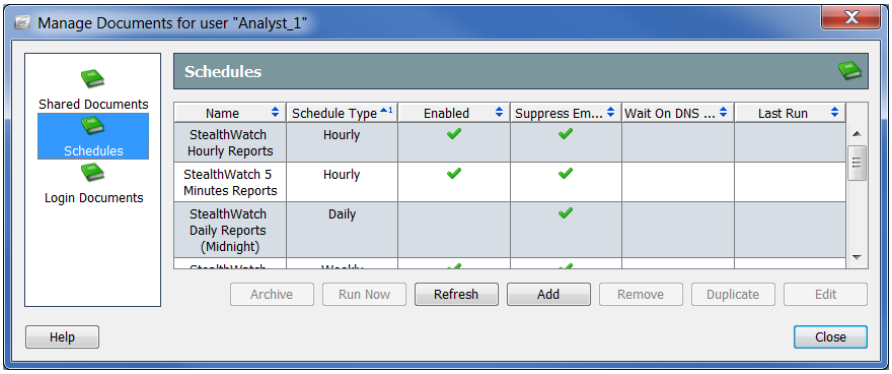
计划文档

在某些情况下，您可能希望每次使用相同的设置（例如，过滤器、布局、时间间隔）自动生成文档。为此，需要将文档添加到包含所需设置的计划中。

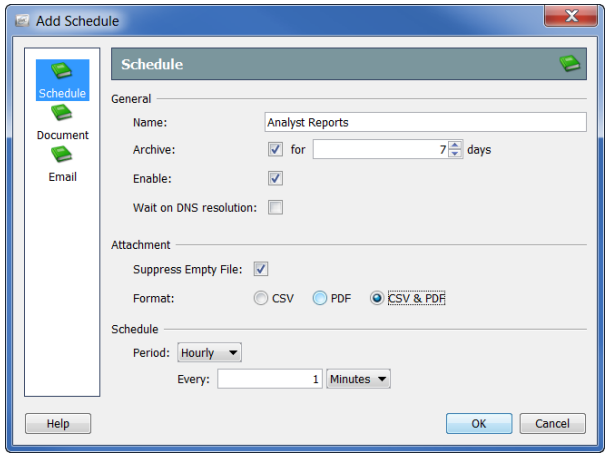
添加新计划

要为您的帐户添加新计划，请完成以下步骤：

1. 从 SMC 主菜单中，选择**文件 > 管理文档**。“管理文档”对话框随即打开。



2. 点击**计划**图标。“计划”页面随即打开。
3. 点击**添加**。“添加计划”对话框随即打开。



4. 点击**计划**图标。“计划”页面随即打开。
5. 在“名称”字段中，为计划键入一个名称。本例中，我们将计划命名为“分析师报告”。

6. 定义“常规”部分中的参数，如下表所示：

如果您希望 ...	则选中 ...
将此计划生成的文档存储在 SMC 数据库中	**存档**复选框。然后，点击相应的下拉列表，并选择要存储文档的天数。
在创建此计划后立即将其激活	**启用**复选框。
如果希望系统等到计划文档中引用的 IP 地址解析至名称后再生成该文档	“等待 DNS 解析”复选框。 **注意：**启用此功能可能会延迟文档生成。每个 IP 地址解析可能最多需要 2 秒。如果系统未能在 2 秒钟内解析 IP 地址，则系统在显示该 IP 地址时不显示 DNS 名称。
防止SMC存档或通过电子邮件发送无数据的生成文档	“抑制空 PDF”复选框。
指定要打印的数据类型	▶ CSV（逗号分隔值）- 如果您仅想打印已生成文档中包含的表数据，则选择此选项。 • 每个表都放置在 CSV 文件中。 • 所有其他类型的数据（例如，映射、图形、图表）都不打印。 • 每个文档的所有 CSV 文件都压缩在一个文件中（即，每个文档一个压缩文件）。 • 对于所选计划生成的文档，系统将通过邮件将其所有压缩文件发送给指定接收这些文档的邮件副本的每位用户。
	▶ PDF - 如果您想要打印已生成文档中包含的所有数据，则选择此选项。 • 每个已生成文档都放置在 PDF 文件中。 • 每个 PDF 文件都压缩在一个文件中。 • 对于所选计划生成的文档，系统将通过邮件将其所有压缩文件发送给指定接收这些文档的邮件副本的每位用户。
- 续 -	

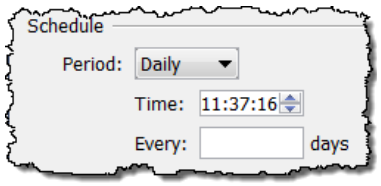
如果您希望 ...	则选中 ...
指定要打印的数据类型	▶ CSV & PDF - 如果您想要打印 CSV 格式的表数据和 PDF 格式的所有其他数据，则选择此选项。 • 每个表都放置在 CSV 文件中。 • 每个已生成文档中的所有其他类型的数据都放置在 PDF 文件中（即，每个文档一个 PDF 文件）。 • 属于文档的所有文件都压缩在一个文件中（即，每个文档一个压缩文件）。 • 对于所选计划生成的文档，系统将通过邮件将其所有压缩文件发送给指定接收这些文档的邮件副本的每位用户。

注意：

- 如果您未在“打印设置”对话框的“页面”页面上启用表，则即使计划已配置为创建 CSV 文件，计划也不会为该表创建 CSV 文件。
- 如果您在“打印设置”对话框的“打印设置”页面指定在生成的文档中包括过滤器摘要，则过滤器摘要将包括在其中。请注意，您必须（在“封面页”部分中）选择“作为第一页”选项或“作为最后一页”选项以启用“过滤器摘要”复选框（在“封面页选项”部分），这样您才能选择它。

7. 点击“期间”下拉列表，并选择您希望 SMC 生成与此计划相关联的任何文档的频率。您可以选择按小时、按天、按周或按月生成计划文档。根据您选择的选项，将显示不同的字段供您指定更多详细信息。

   例如，如果选择**按天**，则会出现两个字段，用于指定希望计划在当天的什么时间运行，以及希望每天、每隔一天、每隔三天运行计划。

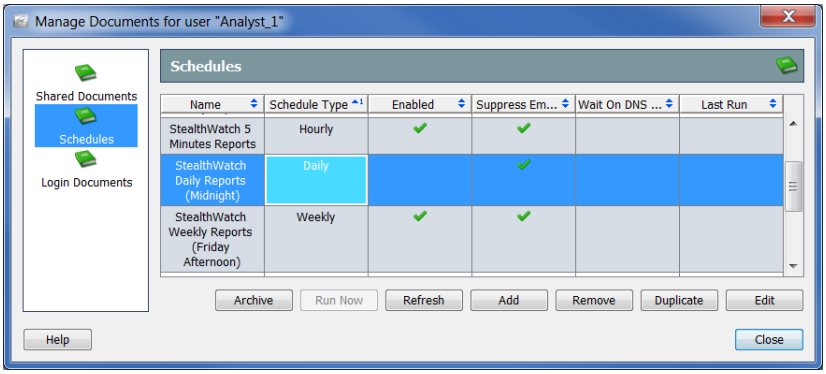


8. 请继续“将文档添加到计划”（第 288 页）。

编辑现有计划

如果要与您的帐户关联的计划已存在，请完成以下步骤以相应地编辑计划：

1. 从 SMC 主菜单中，选择**文件 > 管理文档**。“管理文档”对话框随即打开。

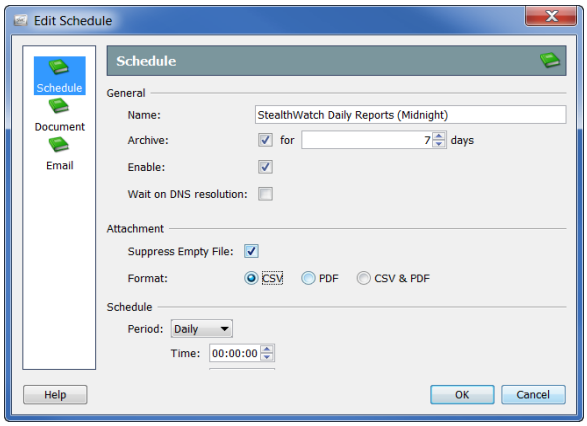


2. 点击**计划**图标。“计划”页面随即打开。
3. 选择要编辑的计划。

注意：

在上面的示例中，选择了“Stealthwatch 按天报告(午夜)”计划。请注意，“启用”列中没有复选标记，表示尚未为您的帐户启用此计划。如果计划未启用，则不会生成计划中的任何文档。

4. 点击**编辑**。“编辑计划”对话框随即打开。

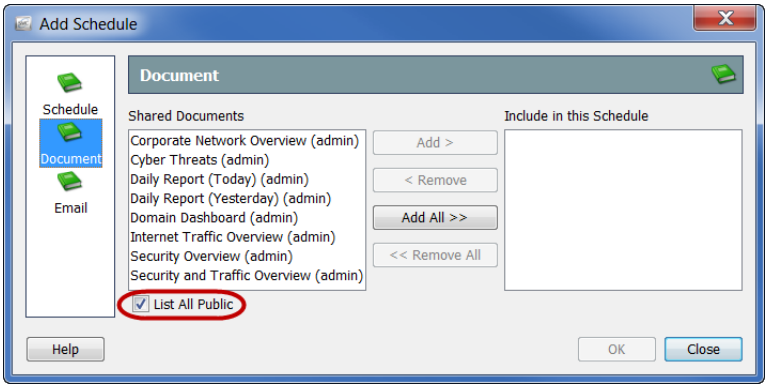


5. 点击**计划**图标。“计划”页面随即打开。
6. 根据需要更改设置。有关任何选项的详细信息，请点击**帮助**。
7. 继续本章中的下一部分“将文档添加到计划”。

将文档添加到计划

要将一个或多个文档添加到计划中，请完成以下步骤：

1. 在“添加(或编辑)计划”对话框中，点击**文档**图标。“文档”页面随即打开。



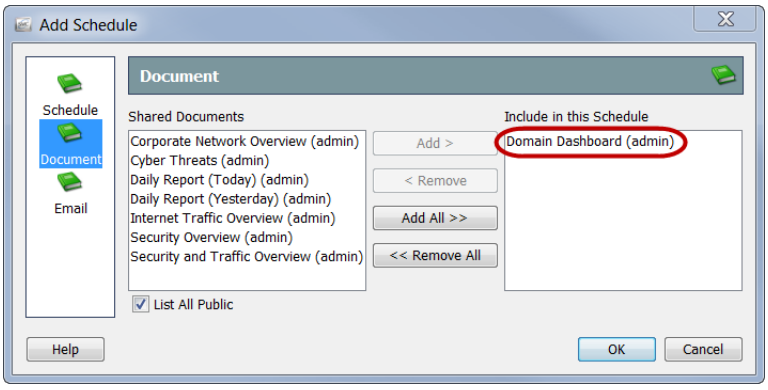
2. 选中**列出所有公共文档**复选框（如果尚未选中）。（有关详细信息，请参阅 “公共文档”（第 283 页））

3. 选择要添加至计划的文档。在本示例中，我们将选择“域控制面板”文档。

注意：

若要选择多个文档，请按住 **Ctrl** 键并点击要添加的每个文档。若要选择文档范围，请点击要选择的范围顶部的文档，按住 **Shift** 键，然后点击要选择的范围底部的文档。

4. 点击**添加**。文档随即会显示在“包含在此计划中”字段中。



5. 您是否希望 SMC 自动通过邮件将计划文档发送给您？
   - 如果是，请继续执行“将用户的邮件地址添加到计划”（第 290 页）
   - 如果不是，请点击**确定**保存信息，退出“添加(或编辑)计划”对话框，然后返回“管理文档”对话框。

6. 关闭其余对话框。

通过邮件发送计划文档

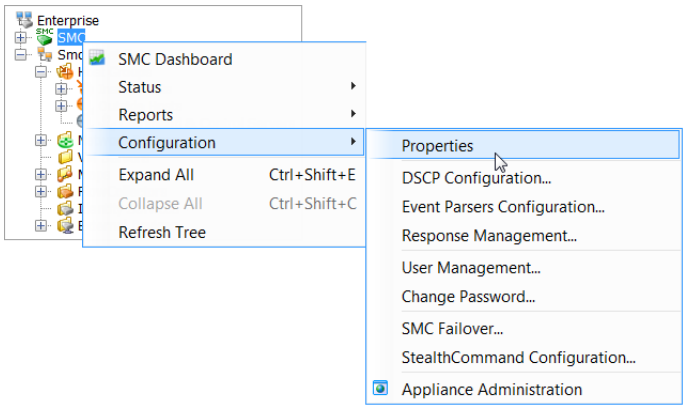
如果您希望 SMC 自动将计划文档通过邮件发送给您，则必须完成以下两个过程：

1. 将邮件服务器的 IP 地址添加到 SMC。（请参阅下一部分，“将邮件服务器添加到 SMC”。）
2. 将用户的邮件地址添加到计划中。（请参阅“将用户的邮件地址添加到计划”（第 290 页）。）

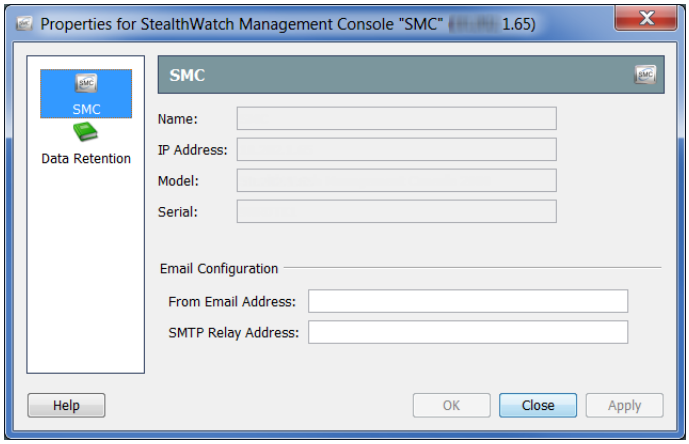
将邮件服务器添加到 SMC

如果之前没有添加，则必须将邮件服务器的 IP 地址添加到 SMC，然后 SMC 才能通过邮件发送任何计划文档。为此，请执行以下操作：

1. 在企业树中右键点击 **SMC** 分支，然后从弹出菜单中选择**配置 > 属性**。系统随即会打开“属性”对话框。



2. 点击 **SMC** 图标。系统会打开“SMC”页面。



3. （可选）在“发件地址”字段中，使用以下格式键入地址：

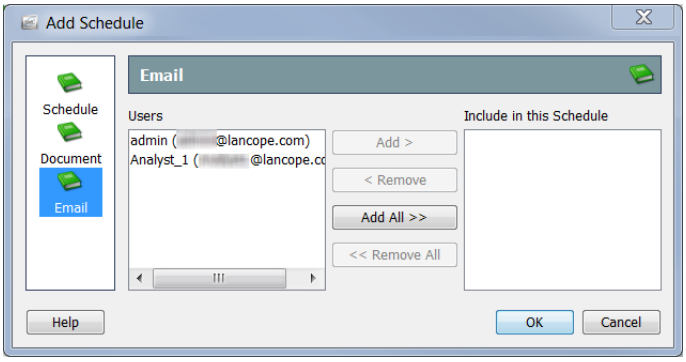
   [FromUser]@[hostname].[domain]

4. 在“SMTP 中继地址”字段中，键入邮件服务器的 IP 地址。
5. 点击**确定**保存信息并关闭“属性”页面。

将用户的邮件地址添加到计划

如果您希望 SMC 自动通过邮件将计划文档发送给您，您必须通过完成以下步骤将您的邮件地址添加到计划中：

1. 在“添加(或编辑)计划”对话框中，点击**邮件**图标。“邮件”页面随即打开。



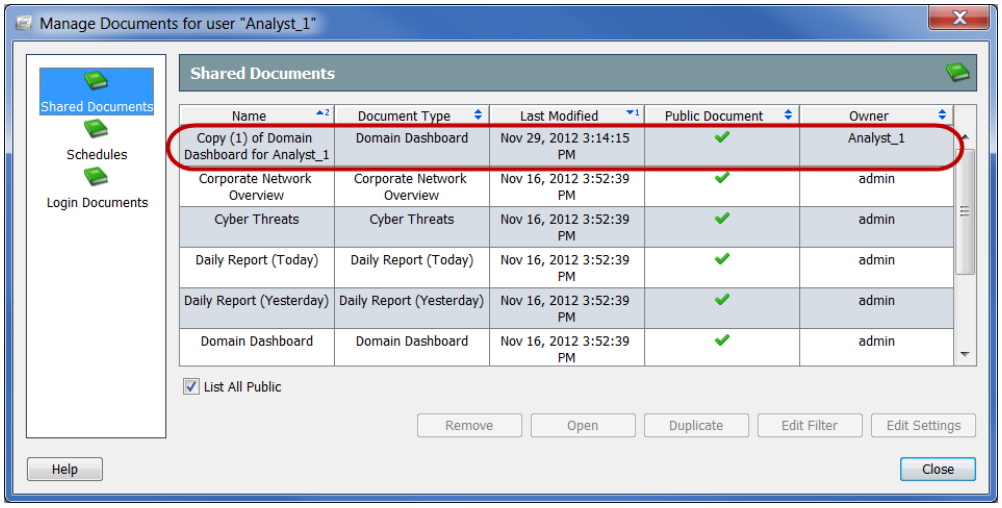
2. 在“用户”字段中，选择您的邮件地址。
3. 点击**添加**。您的邮件地址随即会显示在“包含在此计划中”字段中。
4. 点击**确定**保存信息，关闭“添加(或编辑)计划”对话框，然后返回“管理文档”对话框。
5. 关闭其余对话框。

预过滤共享文档

您可以编辑任何共享文档的过滤器设置，这样，在按计划生成共享文档时，它都将自动使用这些过滤器设置。

这些编辑按以下方式之一保存：

- 如果您不是文档的所有者，则不会修改原始文档，而是使用新过滤器设置创建一个复制文档。仅此复制文档包含新过滤器设置。



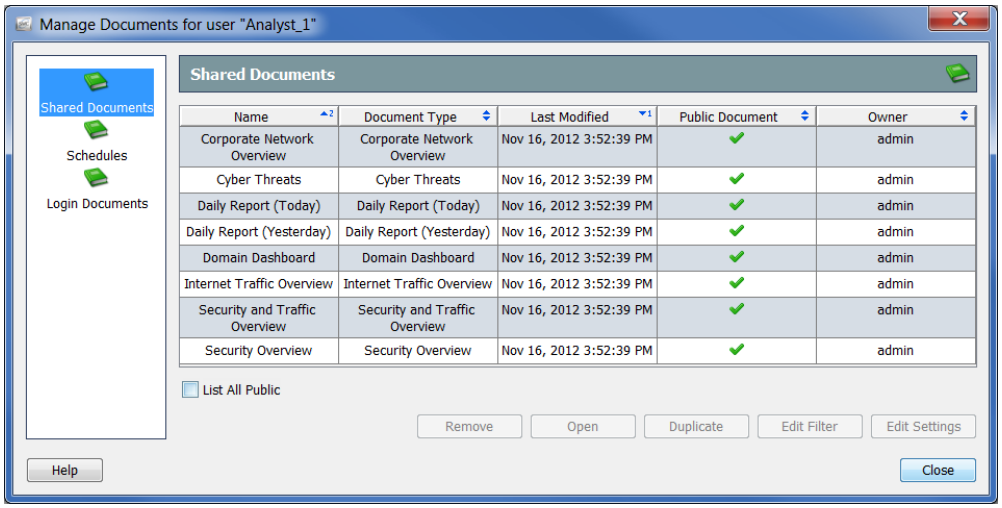
- 如果您是文档所有者，新过滤器设置会在原始文档中生效。此后，任何有权访问此文档的人员无论何时生成或打开此文档，新过滤器设置都将有效。

您可以编辑共享文档的过滤器设置，以便在根据计划生成该文档时，将自动使用这些过滤器设置。为此，请执行以下操作：

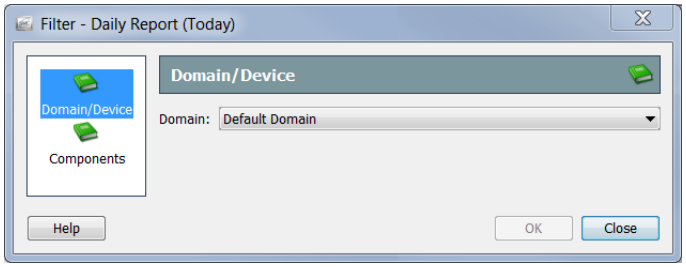
注意：

有关过滤文档的详细信息，请参阅第 3 章“浏览 SMC 客户端界面。”中的“过滤文档数据”

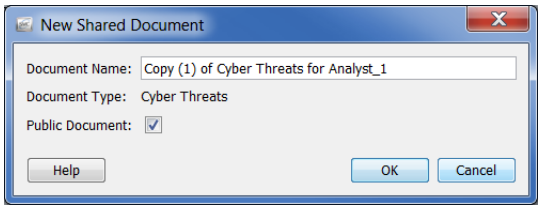
1. 从主菜单中，选择**文件 > 管理文档**。“管理文档”对话框随即打开。



2. 点击**共享文档**图标。系统随即会打开“共享文档”页面。
3. 选择所需文档。
4. 点击**编辑过滤器**。系统会打开“过滤器”对话框。



5. 对过滤器设置进行任何所需更改。如果您正在编辑其他人拥有的文档的过滤器设置，系统则会打开“新建共享文档”对话框，如下面的示例所示。



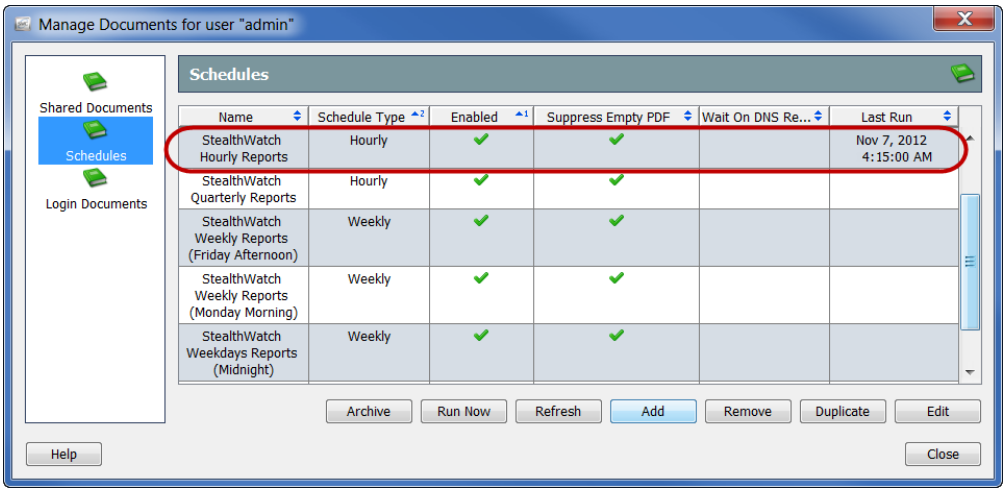
6. 执行以下操作之一：
   - 点击**确定**接受“文档名称”字段中的默认名称，然后退出“新建共享文档”对话框。
   - 更改“文档名称”字段中的名称，然后点击**确定**退出“新建共享文档”对话框。
7. 点击**确定**退出“管理文档”对话框。

删除已存档的文档

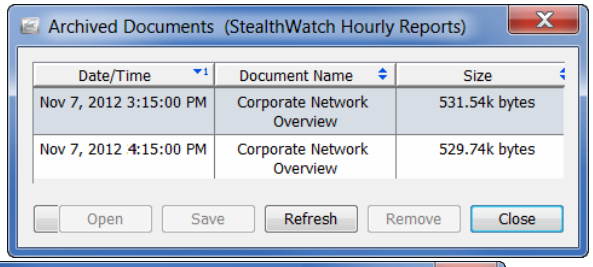
如果您不希望 SMC 自动通过邮件将计划文档发送给您，或者您没有能力从 SMC 接收邮件，那么您可以选择在方便时检索计划文档。

要检索生成的文档，请完成以下步骤：

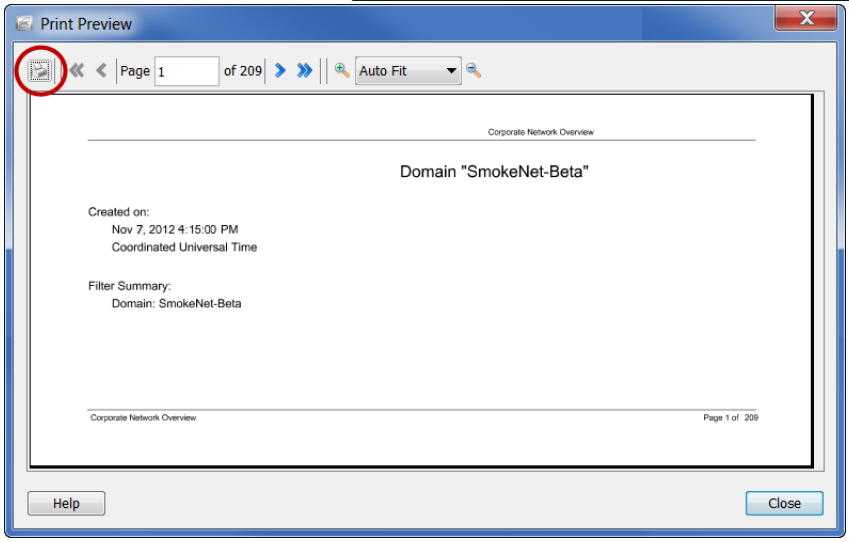
1. 从 SMC 主菜单中，选择**文件 > 管理文档**。“管理文档”对话框随即打开。



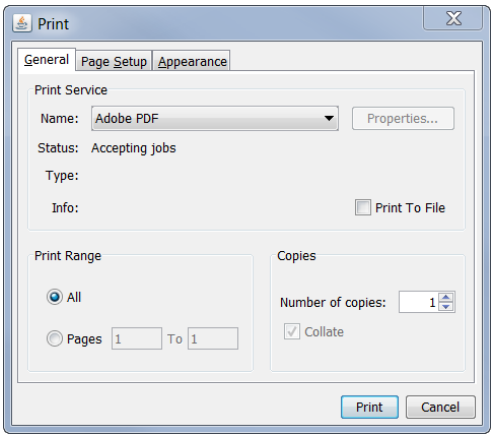
2. 点击**计划**图标。“计划”页面随即打开。
3. 点击包含要查看的生成文档的计划。请注意，“上次运行”列包含上次运行计划的日期和时间。
4. 点击**存档**。系统随即会打开“存档文档”对话框，如右图所示。



5. 点击要查看的文档。
6. 点击**打开**。系统会显示“打印预览”对话框。



7. 点击**打印**图标（在上图中圈出）。“打印”对话框随即打开。



您可以打印文档的硬拷贝，也可以将其下载到本地硬盘驱动器。

14

管理用户

概述

注意：
只有具有管理员权限的用户才能执行本章所述的过程。

SMC 在设置具有不同权限级别的用户方面可提供很大的灵活性。例如，您可以允许一个用户查看和修改网络的每个区域，您也可以限制某些用户，使其只能查看网络中的特定区域，但无法执行其他任何操作。

本章包含以下主题：

流程概述

通常，要在 SMC 中管理用户，需要完成本章中详细介绍的以下过程：

1. 如果您希望 SMC 自动将计划文档发送给用户，则将邮件服务器信息添加到 SMC 中，如第 13 章“处理文档。”的“将邮件服务器添加到 SMC”（第 289 页）中所述
2. 添加您的网络使用的身份验证服务。
3. 确定每个用户所能查看和配置的数据。
4. 为用户添加数据角色。
5. 确定每个用户所能访问的 SMC 功能（即菜单选项）。
6. 为用户添加功能角色。
7. 添加具有适当数据和功能角色的用户。

注意：

具有管理员权限的用户可以访问所有 SMC 功能，也可以查看和配置所有数据。

8. 如果需要，可以将计划文档与用户帐户相关联。

注意：

只有在用户登录后，更改才会生效。因此，如果在受影响的用户登录时修改任何设置元素，那么在用户注销并重新登录之前，他们不会看到这些更改。

添加身份验证服务

注意：

- 如果选择使用本地身份验证，则不需要执行此过程。
- 如果您的网络不使用 RADIUS 或 TACACS 服务器，则必须在本地进行身份验证。

管理用户的第一步是确定在本地进行身份验证（内部验证），还是使用身份验证服务（外部验证）。默认情况下，Stealthwatch 系统使用本地身份验证。

身份验证是服务器或主机对客户端或用户的身份进行验证的过程。此过程可采取多种形式，但通常涉及客户端向服务器提供密码进行验证以获取访问权限。

如果您具有下列身份验证服务之一，则可以将 SMC 配置为利用其中一项服务实现系统访问功能。Stealthwatch 支持以下身份验证服务：

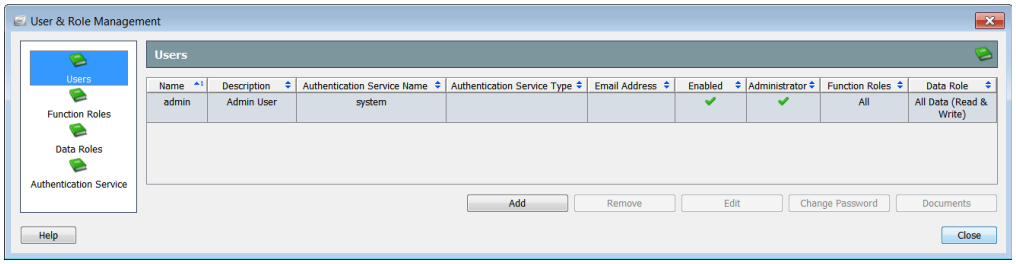
- RADIUS（远程身份验证拨入用户服务）
- TACACS+（终端访问控制器访问控制系统）

重要：

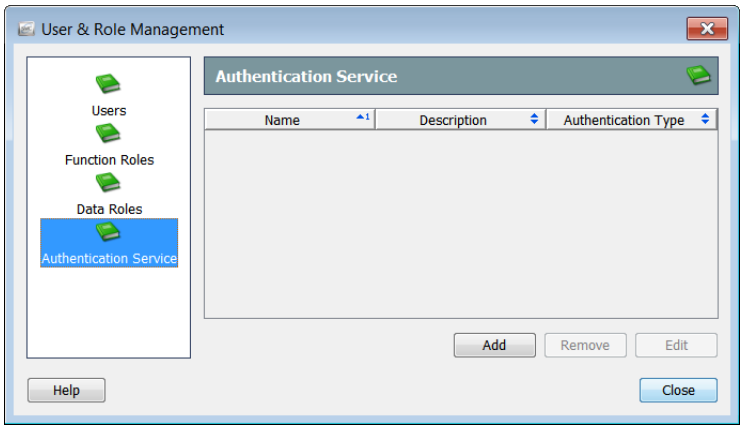
如果您的系统将 Windows Internet 身份验证服务用作您的 RADIUS 身份验证服务器，则用户的 Active Directory 用户帐户必须启用“拨入”访问。否则，用户将无法登录到 SMC

如果需要添加身份验证服务，请完成以下步骤：

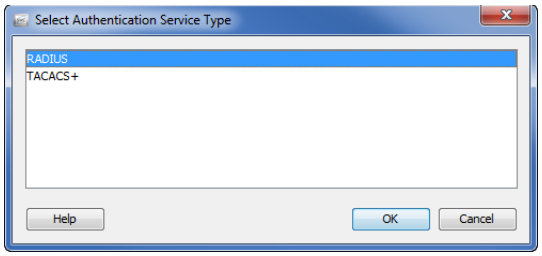
1. 从 SMC 主菜单中，选择**配置 > 用户管理**。“用户和角色管理”对话框随即打开。



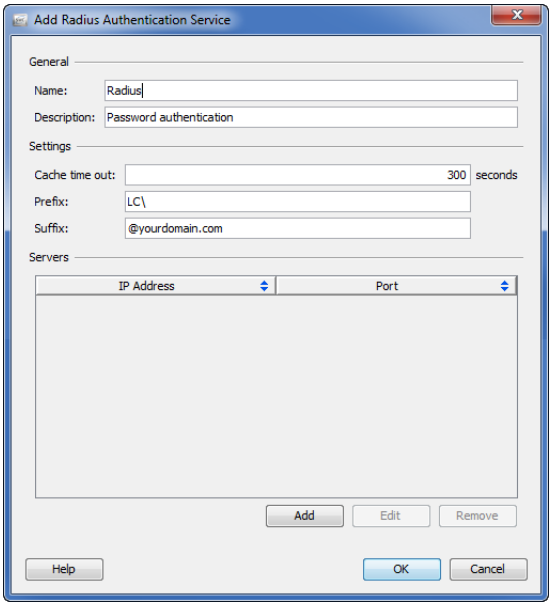
2. 点击**身份验证服务**图标。“身份验证服务”页面随即打开。



3. 点击**添加**。系统随即会显示“选择身份验证服务类型”对话框。



4. 选择所需的服务，然后点击**确定**。“添加身份验证服务”对话框随即打开。

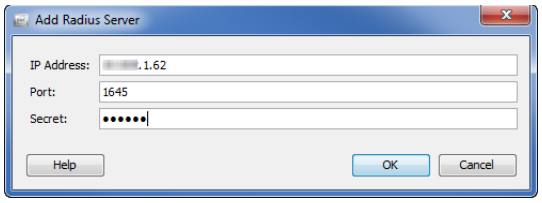


5. 在相应的字段中，键入以下信息：
   - 身份验证服务的名称
   - 服务的描述（可选）
   - 在缓存超时并且系统需要身份验证服务器之前用户/密码有效的秒数。

注意：
需要为用户和分配的角色验证每个 SMC 文档以及 SMC 文档中的每个单元格。SMC 会缓存身份验证长达缓存超时秒，以便用户不用为每个 SMC 文档都登录一次。

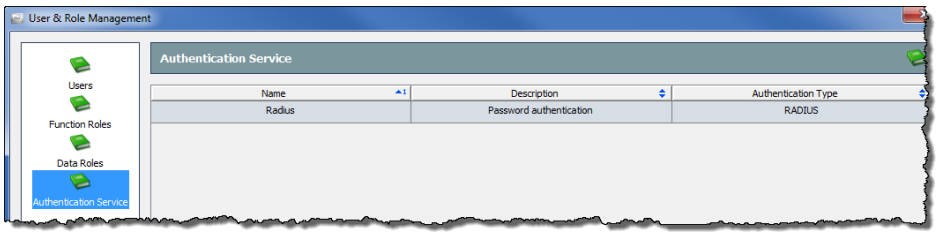
   - 服务所需的任何前缀（例如 `rowspan="1" colspan="1"` 或 `[domain]\`）
   - 服务所需的任何后缀（例如 `@yourdomain.com`）

6. 点击**添加**添加身份验证服务器信息。“添加 [服务名称] 服务器”对话框随即打开。



7. 在相应的字段中，为身份验证服务器键入以下信息：
   - IP 地址
   - 与身份验证服务关联的端口号
     - RADIUS 默认值 = 1645
     - TACACS+ 默认值 = 49
   - 域管理员为用户提供的密码 (RADIUS) 或密钥 (TACACS+)

8. 点击**确定**。“添加服务器”对话框随即关闭。“添加身份验证服务”对话框中的“服务器”表将根据新增服务器相应更新。
9. 点击**确定**。“添加身份验证服务”对话框随即关闭。新服务会显示在“身份验证服务”页面上。



10. 点击**关闭**以关闭“用户和角色管理”对话框，或继续完成下一部分。

控制哪些用户可以查看和配置（数据角色）

SMC 允许您为用户定义*数据角色*。数据角色将决定用户可以查看（读取）和配置（写入）的信息，包括以下内容：

- 域
- 主机组
- VM 服务器
- 虚拟机
- 流收集器
- 导出设备
- FlowSensor
- 外部设备
- 身份识别设备

数据角色还提供隐藏不希望用户看到的数据的有效方法。例如，如果您的系统使用冗余（故障切换）流收集器，就会向 SMC 报告重复数据：主流收集器中的数据与来自故障切换的数据相同。但是，您可以创建一个数据角色来隐藏故障转移流收集器中的数据。然后，分配了此数据角色的用户将只看到主流收集器中的数据。

注意：

有关上述方案的更多详细信息，请参阅“添加数据角色以隐藏冗余的流收集器数据”（第 302 页）。

SMC 附带以下默认数据角色：

- 所有数据(读写)- 具有此数据角色的用户可以查看和配置任何 Stealthwatch 数据。
- 所有数据(只读)- 具有此数据角色的用户可以查看任何 Stealthwatch 数据，但不能配置任何数据。

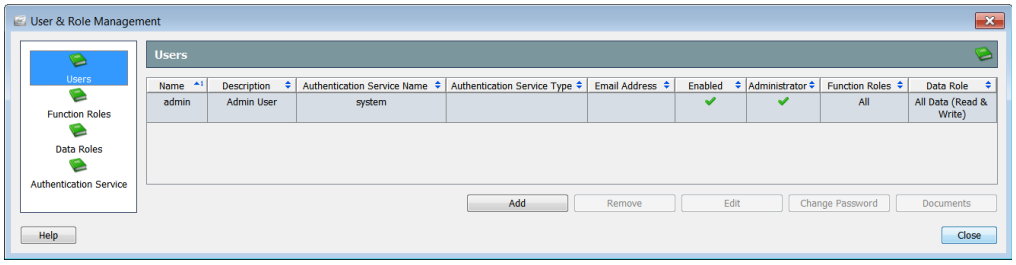
注意：

您必须对添加的每个用户分配数据角色。

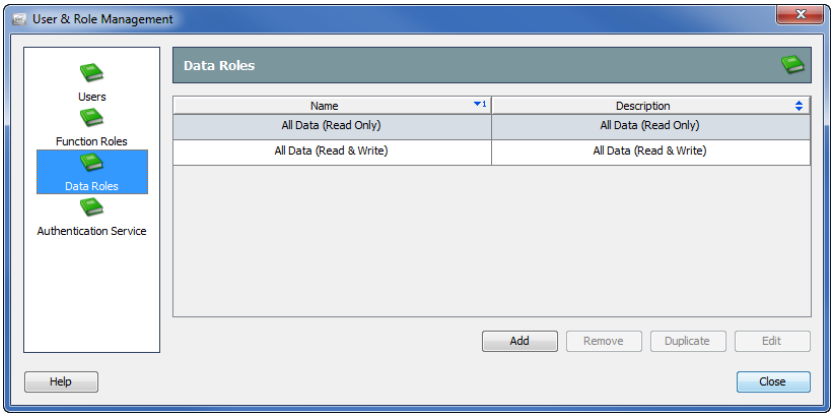
您可以根据需要创建新数据角色。您可以修改或删除您创建的任何数据角色。但是，您不能修改或删除默认的数据角色。

要添加数据角色，请完成以下步骤：

1. 从 SMC 主菜单中，选择**配置 > 用户管理**。“用户和角色管理”对话框随即打开。

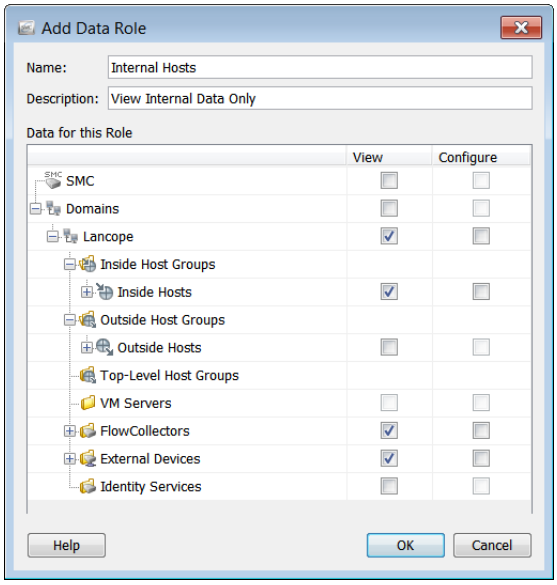


2. 点击**数据角色**图标。“数据角色”页面随即打开。



3. 点击**添加**。

“添加数据角色”对话框随即打开。



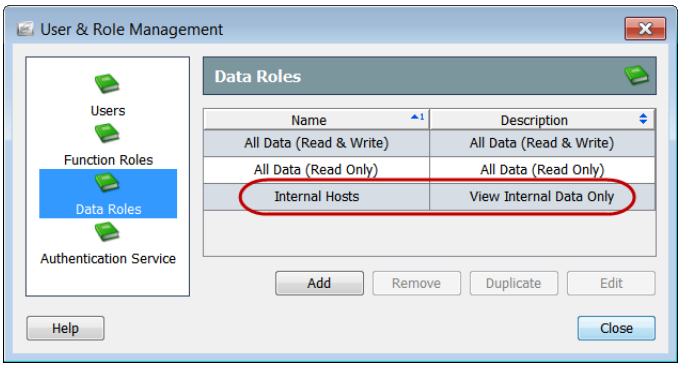
4. 在“名称”字段中，为数据角色键入一个名称。
5. （可选）在“说明”字段中，为数据角色键入说明。

6. 选中您希望具有此数据角色的用户可以查看和/或配置的项目的复选框。

注意：

要面向用户隐藏数据，请不要选中与该数据关联的项目的“查看”复选框（例如冗余流收集器）。

7. 点击**确定**。“添加数据角色”对话框随即关闭。新数据角色会显示在“数据角色”页面上。



8. 点击**关闭**以关闭“用户和角色管理”对话框，或继续完成下一部分。

添加数据角色以隐藏冗余的流收集器数据

如果您使用的是冗余流收集器，并且希望用户仅查看主流收集器中的数据，请按以下顺序完成本部分的如下四个步骤：

1. 为主流收集器添加数据角色。（请参阅第 303 页。）
2. 为冗余流收集器添加数据角色。（请参阅第 304 页。）
3. 添加用户帐户并将主流收集器数据角色分配给它。（请参阅第 307 页。）
4. 必要时编辑用户帐户，将冗余流收集器数据角色分配给它。（请参阅第 309 页。）

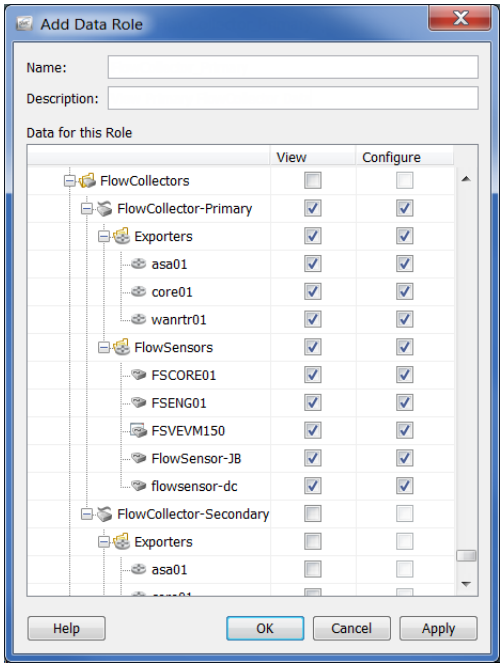
重要：

如果主流收集器出现故障，并且用户的数据角色隐藏了冗余流收集器，则用户将看不到任何数据。若要解决此问题，请编辑用户帐户，分配一个用于显示冗余流收集器的数据角色。

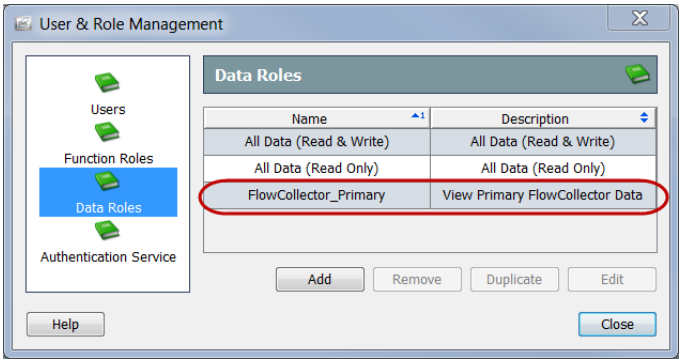
为主流收集器添加数据角色

要为主流收集器添加数据角色，请完成以下步骤：

1. 从 SMC 主菜单中，选择**配置 > 用户管理**。“用户和角色管理”对话框随即打开。
2. 点击**数据角色**图标。“数据角色”页面随即打开。
3. 点击**添加**。“添加数据角色”对话框随即打开。



4. 在“名称”字段中，为数据角色键入一个名称，例如 Flow Collector_Primary。
5. （可选）在“说明”字段中，为数据角色键入说明。
6. 向下滚动到主流收集器，然后选中您希望具有此数据角色的用户可以查看和/或配置的项目的复选框。
7. 点击**确定**。“添加数据角色”对话框随即关闭。新数据角色会显示在“数据角色”页面上。

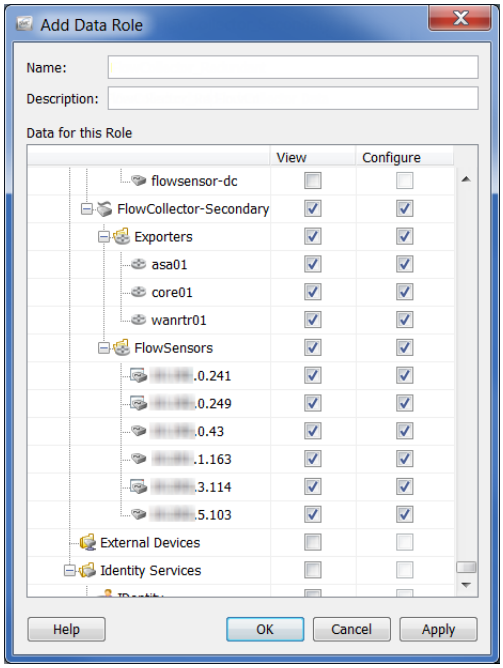


8. 继续下一部分。

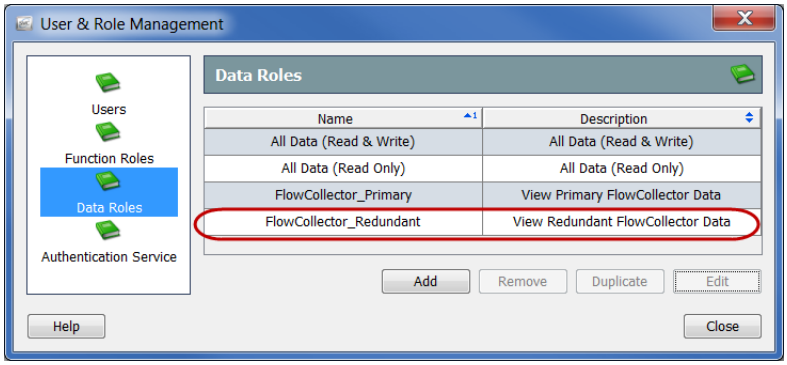
为冗余流收集器添加数据角色

要为冗余流收集器添加数据角色，请完成以下步骤：

1. 在“用户和角色管理”对话框的“数据角色”页面上，点击**添加**。“添加数据角色”对话框随即打开。



2. 在“名称”字段中，为数据角色键入一个名称，例如 Flow Collector _Secondary。
3. （可选）在“说明”字段中，为数据角色键入说明。
4. 向下滚动到冗余流收集器，然后选中您希望具有此数据角色的用户可以查看和/或配置的项目的复选框。
5. 点击**确定**。“添加数据角色”对话框随即关闭。新数据角色会显示在“数据角色”页面上。



现在，您有了主流收集器和冗余流收集器的数据角色，并且可以按照“添加用户帐户”（第 307 页）中的描述将它们分配给用户。

6. 点击**关闭**以关闭“用户和角色管理”对话框，或继续完成下一部分。

控制哪些用户可以执行（功能角色）

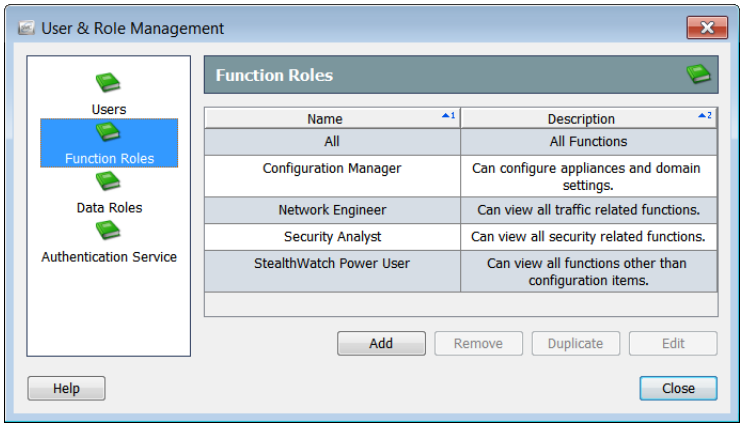
创建所需的数据角色后，定义用户的下一步是创建*功能角色*。功能角色控制用户可以访问的 SMC 菜单项以及可以执行的活动。SMC 附带以下默认功能角色：

- 全部 - 允许用户查看所有菜单项和更改 SMC 客户端界面中的任何内容。
- 配置管理员 - 允许用户查看所有菜单项以及配置所有设备和域设置。
- 网络工程师 - 允许用户查看 SMC 客户端界面中所有与流量相关的菜单项，附加警报和主机说明，以及执行除缓解措施之外的所有警报操作。
- 安全分析员 - 允许用户查看所有与安全相关的菜单项，附加警报和主机说明，以及执行包括缓解措施在内的所有警报操作。
- Stealthwatch 超级用户 - 允许用户查看所有菜单项，确认警报，以及附加警报和主机说明，但不能更改任何内容。

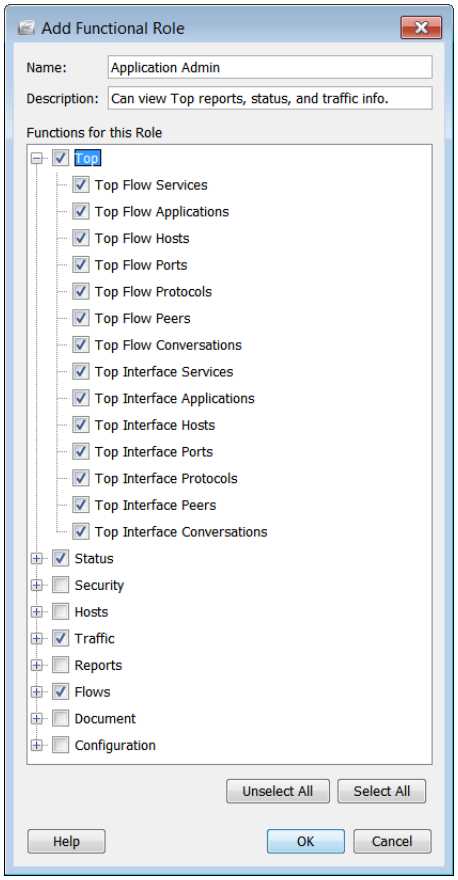
您可以根据需要创建其他功能角色。您还可以修改或删除任何功能角色（包括默认角色）。

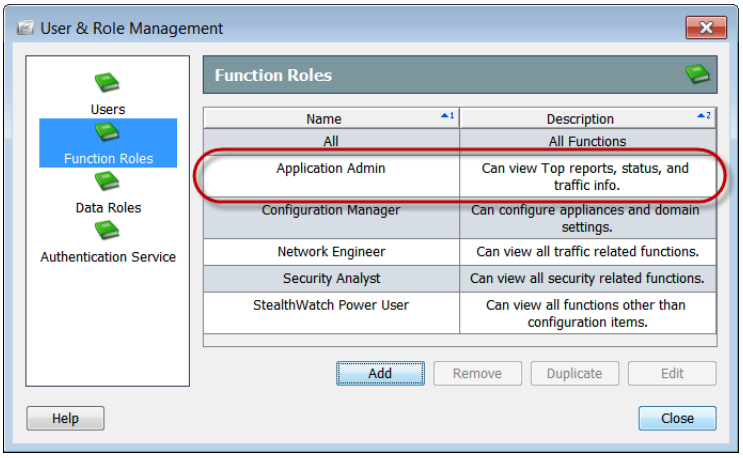
要添加功能角色，请完成以下步骤：

1. 从 SMC 主菜单中，选择**配置 > 用户管理**。“用户和角色管理”对话框随即打开。
2. 点击**功能角色**图标。“功能角色”页面随即打开。



3. 点击**添加**。“添加功能角色”对话框随即打开。
4. 在“名称”字段中，为功能角色键入一个名称。
5. （可选）在“说明”字段中，为功能角色键入说明。
6. 选中您希望具有此功能角色的用户可以查看和/或执行的项目的复选框。
7. 点击**确定**。“添加功能角色”对话框随即关闭。新功能角色会显示在“功能角色”页面上。





8. 点击**关闭**以关闭“用户和角色管理”对话框，或继续完成下一部分。

添加用户帐户

添加所需的数据角色和功能角色后，可以添加用户并为其分配相应的角色。SMC 附带已定义的管理员用户。您可以修改任何用户，包括默认的管理员用户。您可以删除任何用户，但管理员用户*除外*。

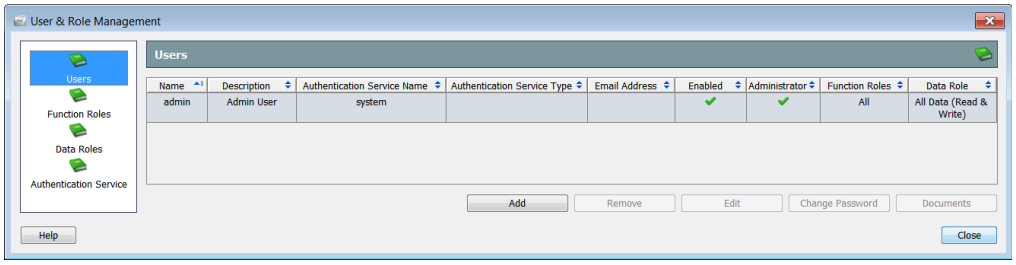
注意：
您必须为您希望 SMC 自动通过邮件发送计划文档的任何人添加用户帐户。

添加用户时，请考虑以下准则：

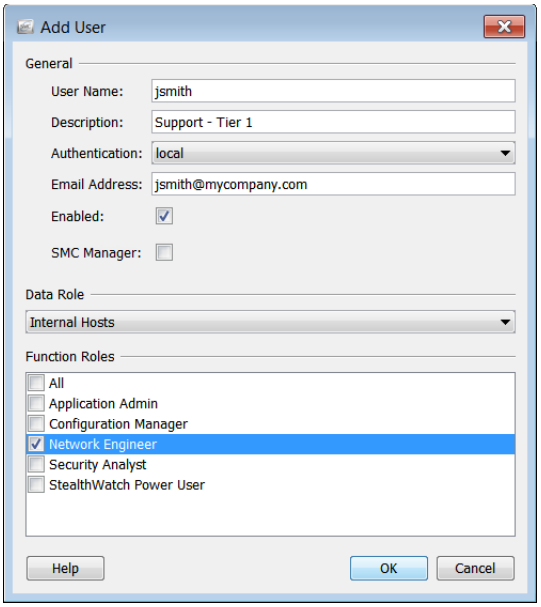
- 不能将名称 *admin* 提供给任何其他用户。
- 只有管理员用户才能登录到设备管理 Web 界面。
- 如果选中**管理员**复选框（在第 9 步中），则添加的用户将具有管理员权限，这样，此用户将可以执行以下操作：
  - 查看和配置所有数据
  - 访问所有菜单项和执行所有功能
  - 创建和管理其他用户

要添加新用户，请完成以下步骤：

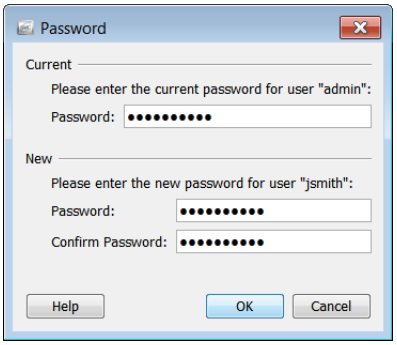
1. 从 SMC 主菜单中，选择**配置 > 用户管理**。“用户和角色管理”对话框随即打开。
2. 点击**用户**图标。“用户”页面随即打开。



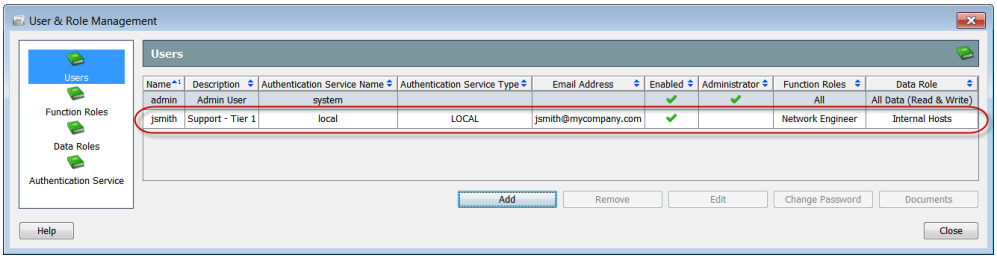
3. 点击**添加**。“添加用户”对话框随即打开。



4. 在“名称”字段中，键入用户的登录名（区分大小写）。
5. （可选）在“说明”字段中，为用户键入说明。
6. 选择将用于验证用户身份的身份验证服务。
7. 如果您希望 SMC 向该用户发送邮件报告和警报，请输入用户的邮件地址。
8. 选中**已启用**复选框以允许此用户登录到 SMC 客户端界面，并通过邮件接收计划文档。
9. 用户是否需要管理员权限？
   - 如果需要，请选中 **SMC 管理员**复选框。然后转至步骤 12。
   - 如果不需要，则转至下一步。
10. 在“数据角色”部分中，点击下拉框并选择要分配给该用户的数据角色（例如，Flow Collector_Primary）。
11. 在“功能角色”部分中，选择要分配给该用户的功能角色。
12. 点击**确定**。“添加用户”对话框随即关闭，“密码”对话框随即打开。



13. 在“当前用户”部分中，键入管理员用户的密码。
14. 如果适用，请执行以下角色：
    - 在“新用户”部分中，为新用户键入密码（区分大小写）。
    - 在“确认密码”字段中， 重新键入密码。
15. 点击**确定**。“密码”对话框随即关闭。新用户显示在“用户”页面上。



16. 您是否要将任何计划文档与此用户的帐户关联？
    - 如果是，请继续执行“将计划文档与用户帐户关联”（第 311 页）
    - 如果不是，请转至步骤 17。

17. 您是否要将任何登录文档添加到此用户的帐户？
    - 如果是，请转到步骤 “登录文档”（第 319 页）。
    - 如果不是，请点击**关闭**退出“用户和角色管理”对话框。

编辑用户帐户

如果需要更改用户的帐户信息，请完成本部分中的步骤。例如，如果为用户分配了一个隐藏冗余流收集器的数据角色，并且主流收集器出现故障，您可以使用此过程为用户分配一个显示冗余流收集器的数据角色。

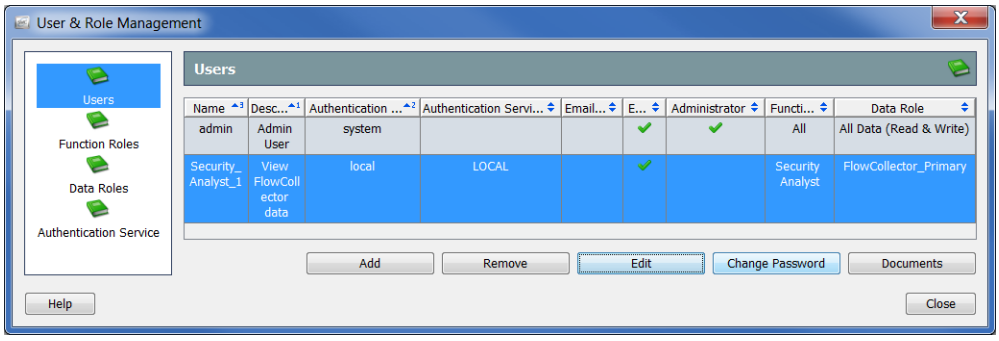
重要：

如果主流收集器出现故障，并且用户的数据角色隐藏了冗余流收集器，则用户将看不到任何数据。

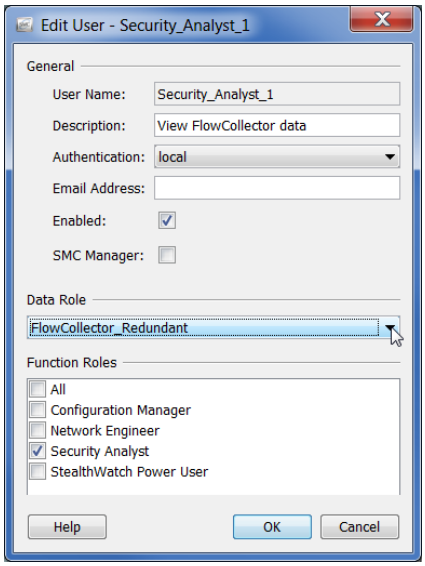
注意：

只有在用户登录后，更改才会生效。因此，如果在受影响的用户登录时修改任何设置元素，那么在用户注销并重新登录之前，他们不会看到这些更改。

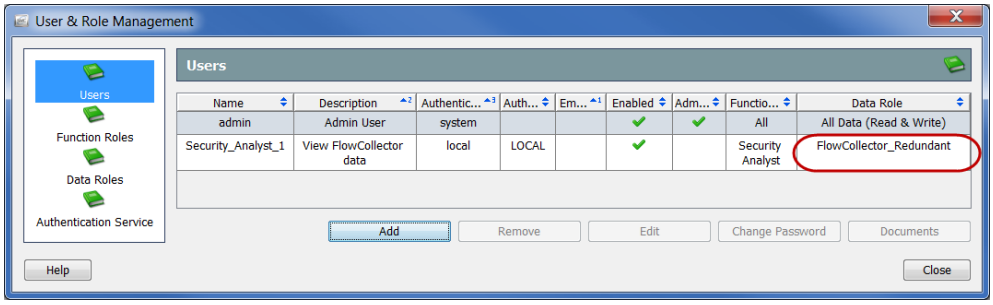
1. 从 SMC 主菜单中，选择**配置 > 用户管理**。“用户和角色管理”对话框随即打开。
2. 点击“用户”图标。“用户”页面随即打开。
3. 选择要编辑的用户帐户。



4. 点击**编辑**。该用户的“编辑用户”对话框随即打开。



5. 若要更改数据角色，请在“数据角色”部分中，点击下拉框并选择数据角色，如显示冗余流收集器的数据角色。
6. 根据需要更改此帐户的任何其他设置。
7. 点击**确定**。“编辑用户”对话框随即关闭。用户的新信息会显示在“用户”页面上。这些更改将在用户下次登录时生效。



8. 您是否要将任何计划文档与此用户的帐户关联？
   - 如果是，请继续执行“将计划文档与用户帐户关联”（第 311 页）
   - 如果不是，请转至步骤 9。
9. 您是否要将任何登录文档添加到此用户的帐户？
   - 如果是，请转到步骤“登录文档”（第 319 页）。
   - 如果不是，请点击**关闭**退出“用户和角色管理”对话框。

将计划文档与用户帐户关联

在某些情况下，您可能希望每次使用相同的设置（例如，过滤器、布局、时间间隔）自动生成文档。为此，需要将文档添加到包含所需设置的计划中。

Stealthwatch 提供两种将计划文档与用户帐户相关联的方法。如果您是管理员用户，可以使用本部分描述的“用户和角色管理”对话框，在创建/编辑用户帐户时执行此操作。

单个用户可以使用“管理文档”对话框为自己的帐户完成此任务，如第 13 章“处理文档。”中所述

注意：

本部分假定所需的文档已保存在 SMC 设备上。有关保存文档的详细信息，请参阅第 13 章“处理文档。”

文档计划仅设置有关一个或多个文档运行的频率和存档时间的参数。SMC 附带了一组默认计划，它们与所有用户帐户自动关联。并非所有默认计划都已启用。但是，它们都可供每个用户使用。

此外，用户还可以为自己创建自定义计划。最后，作为管理员用户，您可以在创建帐户时将自定义计划与本部分描述的用户帐户相关联。

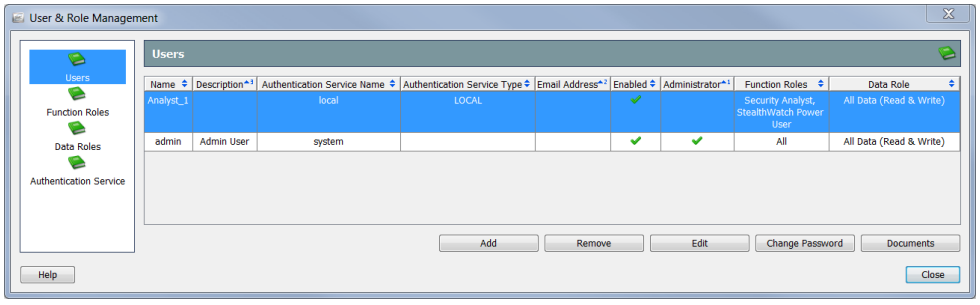
将计划与用户帐户关联的流程涉及完成以下过程：

1. 添加新计划或编辑现有计划。
2. 向计划中添加一个或多个文档。
3. （可选）如果您希望 SMC 在创建计划文档时通过邮件将这些文档发送给用户，请将该用户的邮件地址添加到计划中。

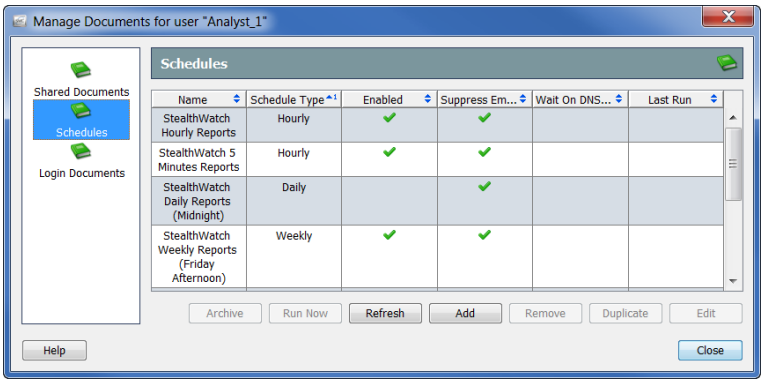
添加新计划

要向用户帐户添加新计划，请完成以下步骤：

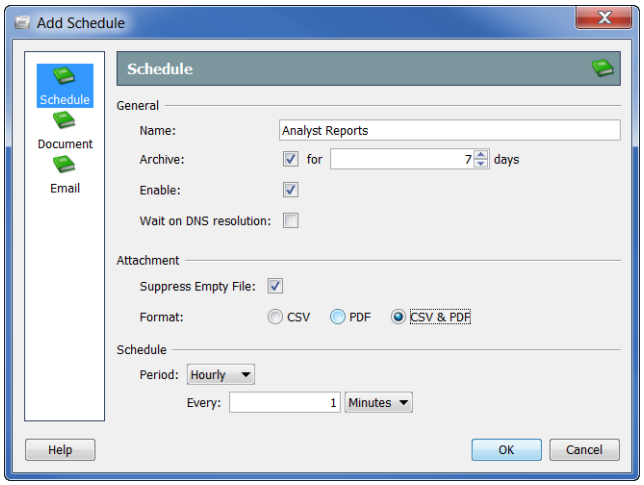
1. 从 SMC 主菜单中，选择**配置 > 用户管理**。“用户和角色管理”对话框随即打开。



2. 点击**用户**图标。“用户”页面随即打开。
3. 选择所需的用户。
4. 点击**文档**。系统会打开管理文档对话框。



5. 点击**计划**图标。“计划”页面随即打开。
6. 点击**添加**。“添加计划”对话框随即打开。



7. 点击**计划**图标。“计划”页面随即打开。
8. 在“名称”字段中，为计划键入一个名称。本例中，我们将计划命名为“分析师报告”。
9. 定义“常规”部分中的参数，如下表所示：

如果您希望 ...	那么 ...
将此计划生成的文档存储在 SMC 数据库中	选中**存档**复选框。然后，点击相应的下拉列表，并选择要存储文档的天数。
在创建此计划后立即将其激活	选择**启用**复选框。
如果希望系统等到计划文档中引用的 IP 地址解析至名称后再生成该文档	选中“等待 DNS 解析”复选框。 **注意：**启用此功能可能会延迟文档生成。每个 IP 地址解析可能最多需要 2 秒。如果系统未能在 2 秒钟内解析 IP 地址，则系统在显示该 IP 地址时不显示 DNS 名称。
防止 SMC 存档或通过邮件发送没有数据的生成文档	选中“抑制空 PDF”复选框。
- 续 -	

如果您希望 ...	那么 ...
指定要打印的数据类型	▶ CSV（逗号分隔值）- 如果您仅想打印已生成文档中包含的表数据，则选择此选项。 • 每个表都放置在 CSV 文件中。 • 所有其他类型的数据（例如，映射、图形、图表）都不打印。 • 每个文档的所有 CSV 文件都压缩在一个文件中（即，每个文档一个压缩文件）。 • 对于所选计划生成的文档，系统将通过邮件将其所有压缩文件发送给指定接收这些文档的邮件副本的每位用户。 ▶ PDF - 如果您想要打印已生成文档中包含的所有数据，则选择此选项。 • 每个已生成文档都放置在 PDF 文件中。 • 每个 PDF 文件都压缩在一个文件中。 • 对于所选计划生成的文档，系统将通过邮件将其所有压缩文件发送给指定接收这些文档的邮件副本的每位用户。 ▶ CSV & PDF - 如果您想要打印 CSV 格式的表数据和 PDF 格式的所有其他数据，则选择此选项。 • 每个表都放置在 CSV 文件中。 • 每个已生成文档中的所有其他类型的数据都放置在 PDF 文件中（即，每个文档一个 PDF 文件）。 • 属于文档的所有文件都压缩在一个文件中（即，每个文档一个压缩文件）。 • 对于所选计划生成的文档，系统将通过邮件将其所有压缩文件发送给指定接收这些文档的邮件副本的每位用户。

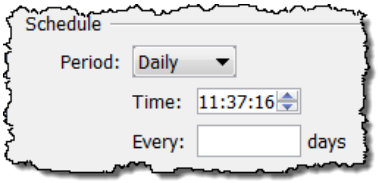
注意：

▶ 如果您未在“打印设置”对话框的“页面”页面上启用表，则即使计划已配置为创建 CSV 文件，计划也不会为该表创建 CSV 文件。

▶ 如果您在“打印设置”对话框的“打印设置”页面指定在生成的文档中包括过滤器摘要，则过滤器摘要将包括在其中。请注意，您必须（在“封面页”部分中）选择“作为第一页”选项或“作为最后一页”选项以启用“过滤器摘要”复选框（在“封面页选项”部分），这样您才能选择它。

10. 点击“期间”下拉列表，并选择您希望 SMC 生成与此计划相关联的任何文档的频率。您可以选择按小时、按天、按周或按月生成计划文档。根据您选择的选项，将显示不同的字段供您指定更多详细信息。

    例如，如果选择**按天**，则会出现两个字段，用于指定希望计划在当天的什么时间运行，以及希望每天、每隔一天、每隔三天运行计划。

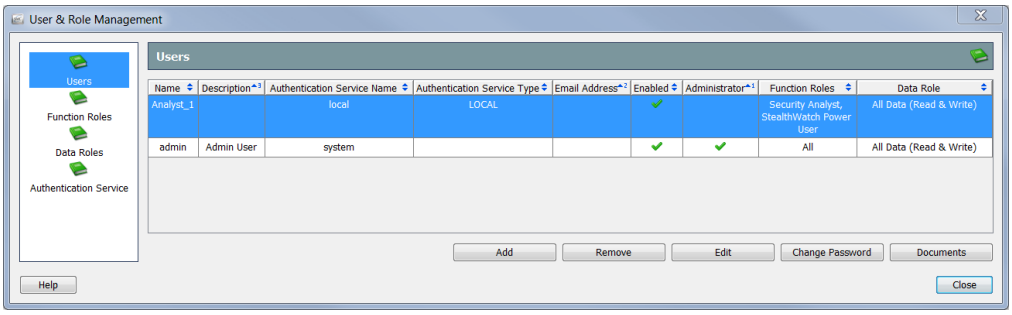


11. 请继续“将文档添加到计划”（第 316 页）。

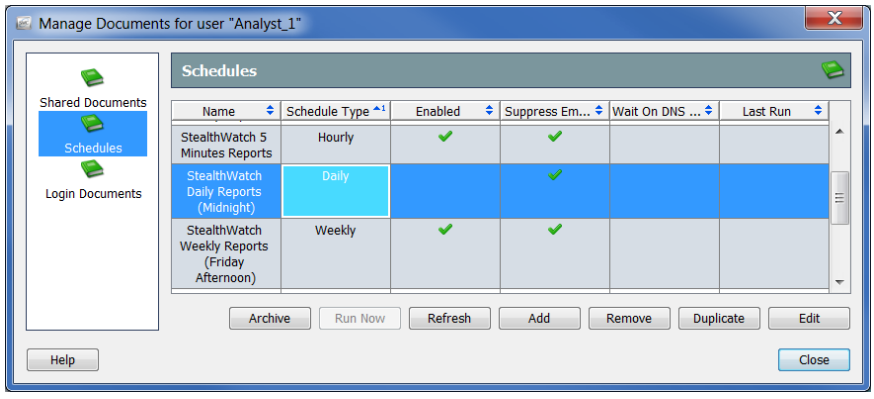
编辑现有计划

如果要与用户帐户关联的计划已存在，请完成以下步骤以相应地编辑计划：

1. 从主菜单中选择**配置 > 用户管理**。“用户和角色管理”对话框随即打开。



2. 点击**用户**图标。“用户”页面随即打开。
3. 选择所需的用户。
4. 点击**文档**。“管理文档”对话框随即打开。



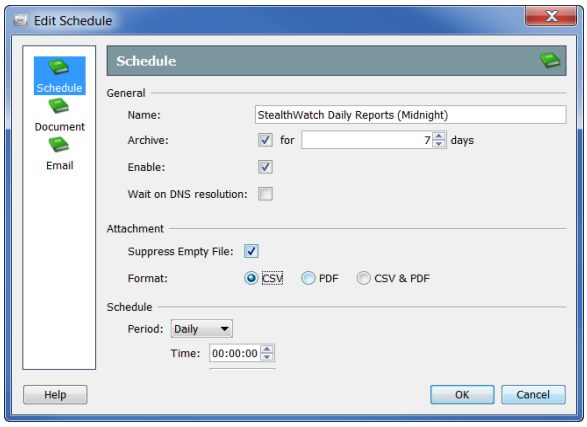
5. 点击**计划**图标。“计划”页面随即打开。

6. 选择要编辑的计划。

注意：

在上面的示例中，选择了“Stealthwatch 按天报告(午夜)”计划。请注意，“启用”列中没有复选标记，表示尚未为用户帐户启用此计划。如果计划未启用，则不会生成计划中的任何文档。

7. 点击**编辑**。“编辑计划”对话框随即打开。

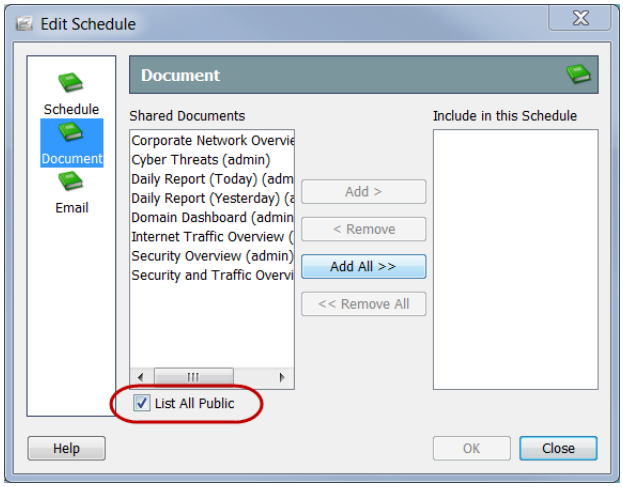


8. 点击**计划**图标。“计划”页面随即打开。
9. 根据需要更改设置。有关任何选项的详细信息，请点击**帮助**。
10. 继续本章中的下一部分“将文档添加到计划”。

将文档添加到计划

要将一个或多个文档添加到计划中，请完成以下步骤：

1. 在“添加(或编辑)计划”对话框中，点击**文档**图标。“文档”页面随即打开。



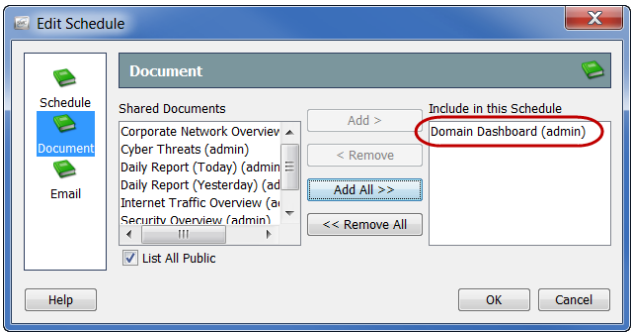
2. 选中**列出所有公共文档**复选框（如果尚未选中）。（有关详细信息，请参阅“公共文档”（第 283 页） 的第 13 章“处理文档。”

3. 选择要添加至计划的文档。对于本示例，我们将选择“域控制面板”文档。

注意：

若要选择多个文档，请按住 **Ctrl** 键并点击要添加的每个文档。若要选择文档范围，请点击要选择的范围顶部的文档，按住 **Shift** 键，然后点击要选择的范围底部的文档。

4. 点击**添加**。文档将显示在“包含在此计划中”字段中。



5. 您是否希望 SMC 自动通过邮件将计划文档发送给该用户？

   - 如果是，请继续本章中的下一部分“将用户的邮件地址添加到计划”。
   - 如果不是，请点击**确定**保存信息，退出“添加(或编辑)计划”对话框，然后返回“管理文档”对话框。

6. 关闭其余对话框。

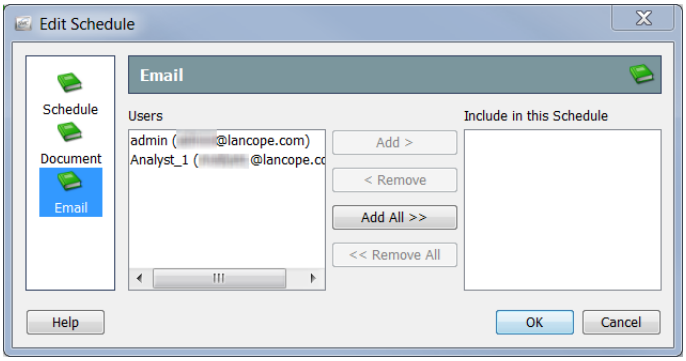
将用户的邮件地址添加到计划

注意：

如果之前没有添加，则必须将邮件服务器的 IP 地址添加到 SMC，然后 SMC 才能通过邮件发送任何计划文档。（有关详细信息，请参阅“将邮件服务器添加到 SMC”（第 289 页）的第 13 章“处理文档。”

如果您希望 SMC 自动通过邮件将计划文档发送给某人，您必须通过完成以下步骤将其邮件地址添加到计划中：

1. 在“添加(或编辑)计划”对话框中，点击**邮件**图标。“邮件”页面随即打开。



2. 在“用户”字段中，选择用户的邮件地址。
3. 点击**添加**。邮件地址将显示在“包含在此计划中”字段中。

注意：

若要选择多个邮件地址，请按住 **Ctrl** 键并点击要添加的每个邮件地址。若要选择邮件地址范围，请点击要选择的范围顶部的邮件地址，按住 **Shift** 键，然后点击要选择的范围底部的邮件地址。

4. 点击**确定**保存信息，关闭“添加(或编辑)计划”对话框，然后返回“管理文档”对话框。
5. 您是否要将任何登录文档添加到此部分？
   - 如果是，请继续本章中的下一部分“登录文档”。
   - 如果不是，请关闭其余对话框。

登录文档

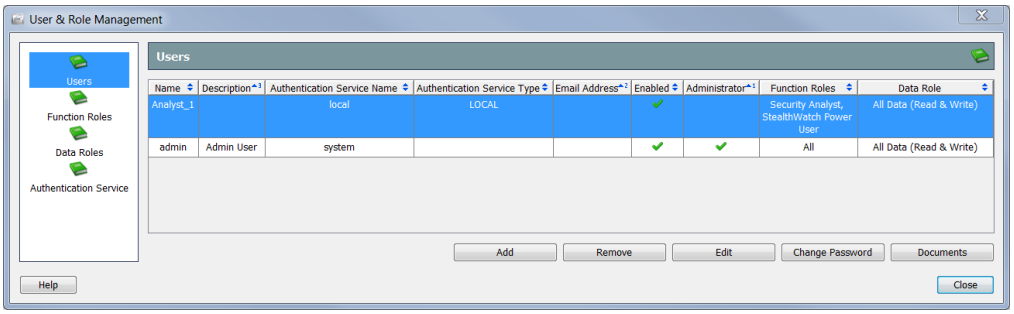
您可以将任何文档添加到您的登录文档列表中。每次登录 SMC 客户端界面时，登录文档都会自动打开。此功能对于查看您将定期手动打开的文档非常有用。

注意：

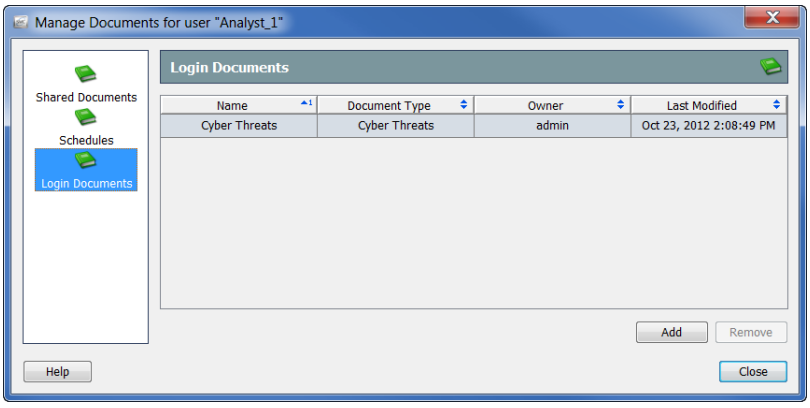
本部分假定已创建所需的共享文档。有关创建共享文档的详细信息，请参阅第 13 章“处理文档。”

要使文档成为用户帐户的登录文档，请完成以下步骤：

1. 从 SMC 主菜单中，选择**配置 > 用户管理**。“用户和角色管理”对话框随即打开。

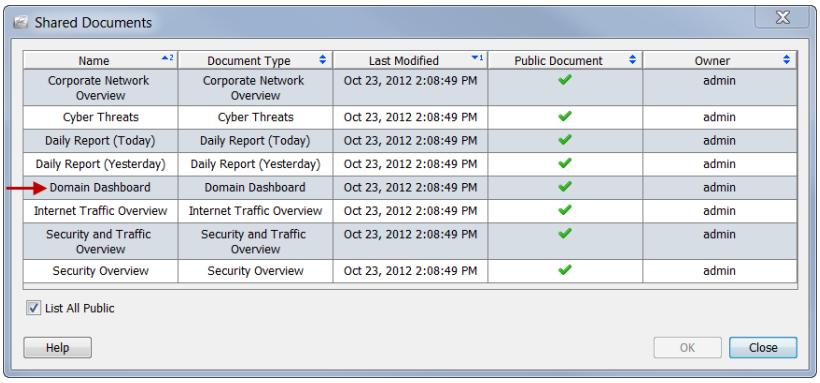


2. 点击**用户**图标。“用户”页面随即打开。
3. 选择您要向其添加登录文档的用户帐户。
4. 点击**文档**。所选用户的“管理文档”对话框随即打开。



5. 点击**登录文档**图标。“登录文档”页面随即打开。

6. 点击**添加**。“共享文档”对话框将会打开，其中显示您保存的所有文档。

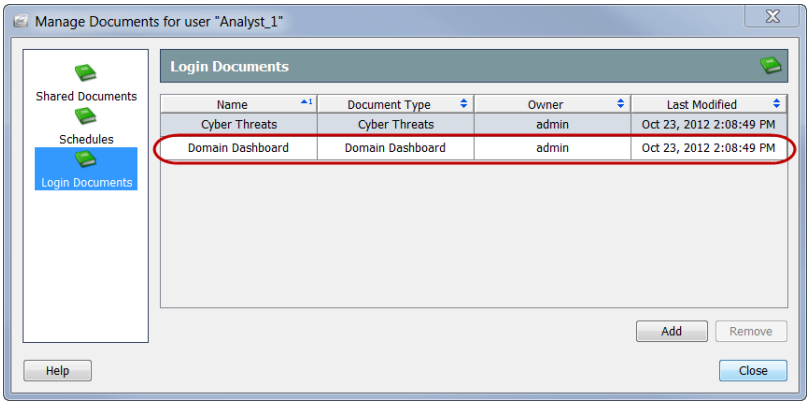


7. 选中**列出所有公共文档**复选框以查看其他用户保存的所有公共文档。
8. 选择要添加到用户的登录文档列表的文档。对于本示例，我们将选择“域控制面板”文档。

注意：

若要选择多个文档，请按住 **Ctrl** 键并点击要添加的每个文档。若要选择文档范围，请点击要选择的范围顶部的文档，按住 **Shift** 键，然后点击要选择的范围底部的文档。

9. 点击**确定**。“共享文档”对话框随即关闭。您选择的文档将显示在用户的登录文档列表中。



10. 点击**关闭**退出“管理文档”对话框。
11. 点击**关闭**退出“用户和角色管理”对话框。

索引

符号

英文

A

B

C

D

F

G

H

J

K

L

M

X

Y

Z