

配置Firesight管理中心以显示每个访问规则的命中计数

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[配置](#)

[验证](#)

[故障排除](#)

简介

本文档介绍如何配置自定义工作流程/事件查看器页面以描述每个访问规则名称的连接命中计数。配置显示与命中计数关联的规则名称字段的基本示例，以及如果需要，如何添加其他字段。

先决条件

要求

Cisco 建议您了解以下主题：

- Firepower技术知识
- 了解Firesight管理中心内的基本导航

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Firepower管理中心6.1.X及更高版本
- 适用于托管威胁防御/Firepower传感器

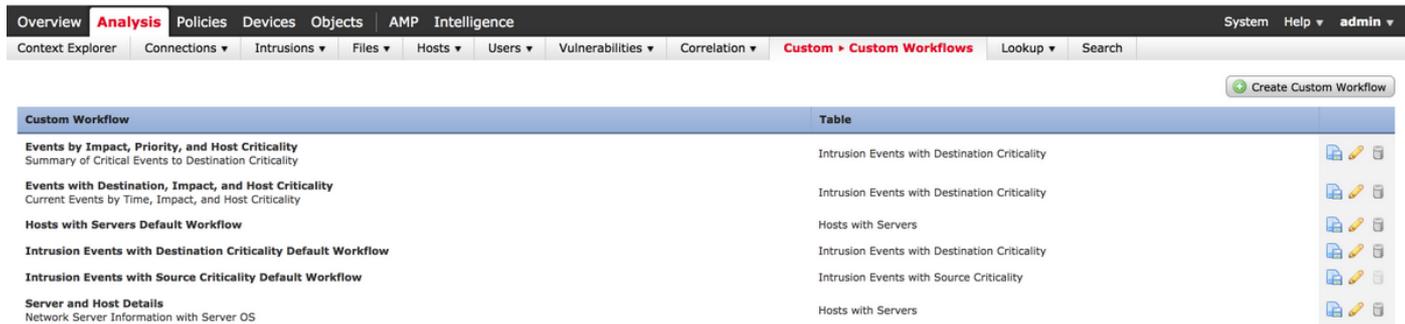
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

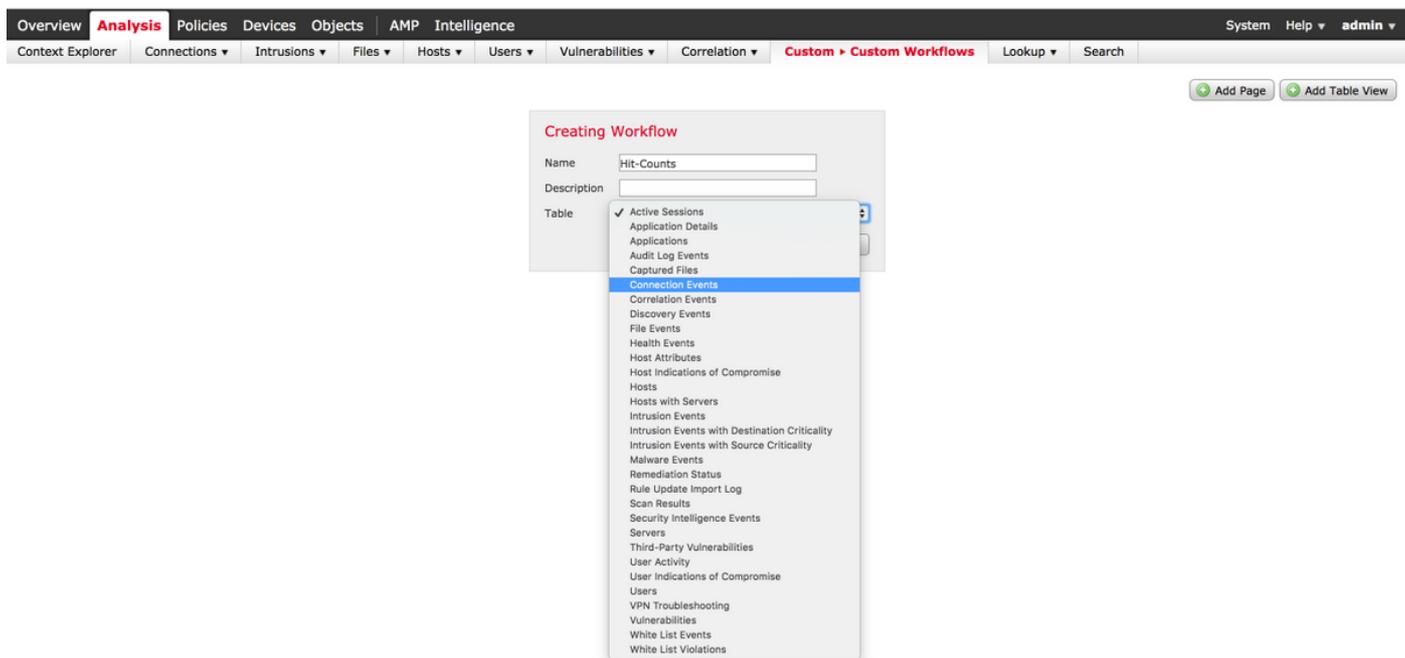
配置

步骤1.以管理员权限登录Firesight管理中心。

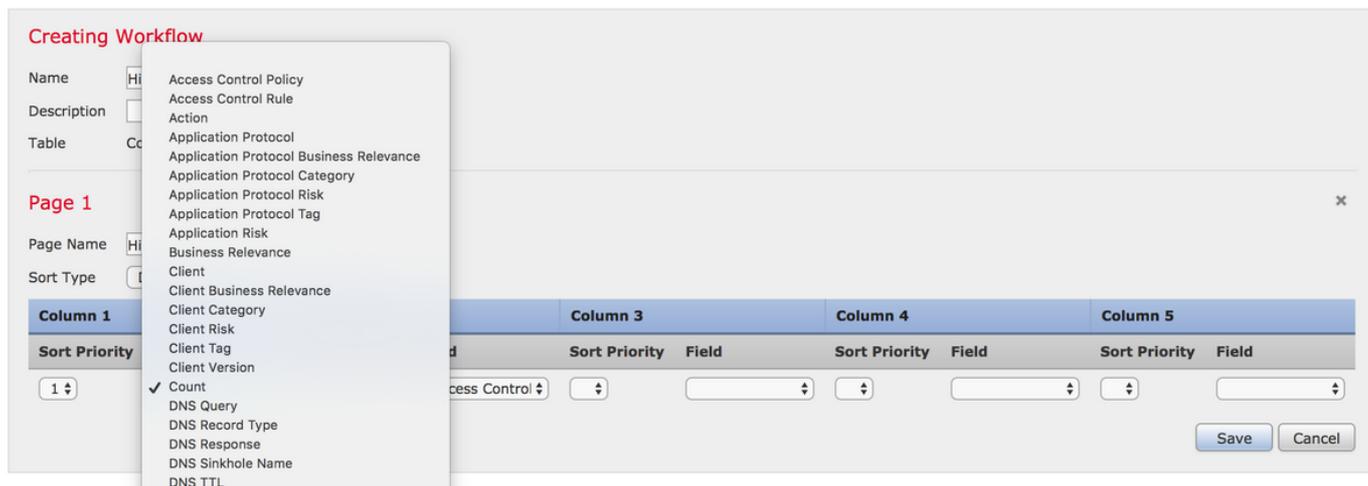
登录成功后，导航到Analysis > Custom > Custom Workflows，如图所示：



步骤2. 单击“创建自定义工作流”，然后选择如图所示的参数：



步骤3. 选择表字段作为“连接事件”并输入工作流名称，然后单击“保存”。保存工作流程后，单击“添加页”，如图所示：



注意：第一列必须是“计数”，然后在其他列中，您可以从下拉列表中选择可用字段。在这种情况下，第一列是Count，第二列是Access Control Rule。

步骤4.添加工作流程页面后，单击“保存”。

要查看命中计数，请导航至Analysis > Connections > Events，然后单击Switch Workflows，如图所示：

The screenshot shows the 'Hit-Counts' workflow configuration page. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. Under 'Analysis', 'Connections > Events' is selected. A dropdown menu is open, showing various workflow options, with 'Hit-Counts' selected. The main content area displays a table of connection events with columns: 'Last Packet', 'Action', 'Reason', 'Initiator IP', 'Initiator Country', 'Responder IP', 'Responder Country', and 'Ingress Security Zone'. The table contains several rows of event data, including timestamps, actions (all 'Allow'), initiator and responder IP addresses, and responder countries (USA).

步骤5.从下拉列表中选择您创建的自定义工作流程（在本例中为Hit-Counts），如图所示：

The screenshot shows the 'Hit-Counts' workflow configuration page. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. Under 'Analysis', 'Connections > Events' is selected. A dropdown menu is open, showing various workflow options, with 'Hit-Counts' selected. The main content area displays a table of connection events with columns: 'Last Packet', 'Action', 'Reason', 'Initiator IP', 'Initiator Country', 'Responder IP', 'Responder Country', and 'Ingress Security Zone'. The table contains several rows of event data, including timestamps, actions (all 'Allow'), initiator and responder IP addresses, and responder countries (USA).

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。