在Splunk上使用来自FTD的系统日志创建自定义控制面板和警报

目录

简介

本文档介绍配置FTD以向Splunk发送系统日志以及使用这些日志构建自定义控制面板和警报的分步演练。

先决条件

要求

Cisco建议您在阅读本配置指南之前了解以下主题：

- 系统日志
- Splunk搜索处理语言(SPL)的基本知识

本文档还假设您已在服务器上安装了Splunk Enterprise实例，并且可以访问Web界面。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行在7.2.4版上的Cisco Firepower威胁防御(FTD)

- 运行在7.2.4版上的思科Firepower管理中心(FMC)
- 在Windows计算机上运行的Splunk Enterprise实例（版本9.4.3）

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。

背景信息

思科FTD设备生成详细的系统日志，涵盖入侵事件、访问控制策略、连接事件等。将这些日志与Splunk相集成，可为网络安全操作提供强大的分析和实时警报。

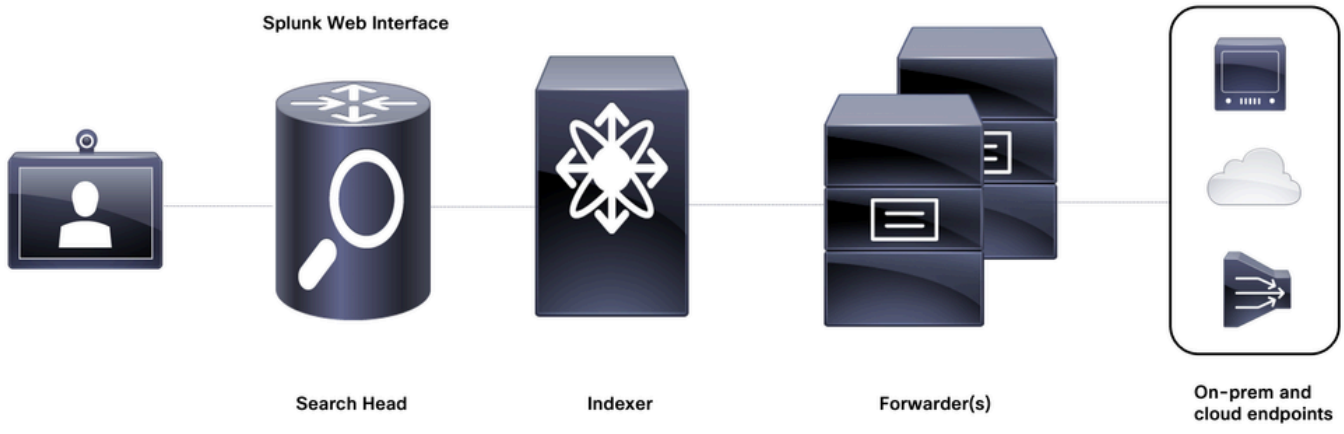
Splunk是一个实时数据分析平台，用于采集、索引、搜索和可视化机器生成的数据。Splunk作为安全信息和事件管理(SIEM)工具，在网络安全环境中特别有效，因为它能够：

- 大规模接收日志数据
- 使用SPL执行复杂搜索
- 创建控制面板和警报
- 与安全协调和事件响应系统集成

Splunk通过结构化管道处理数据，以使非结构化或半结构化机器数据变得有用且可操作。此管道的主要阶段通常称为IPIS，代表：

- 输入
- 分析
- 索引
- 搜索

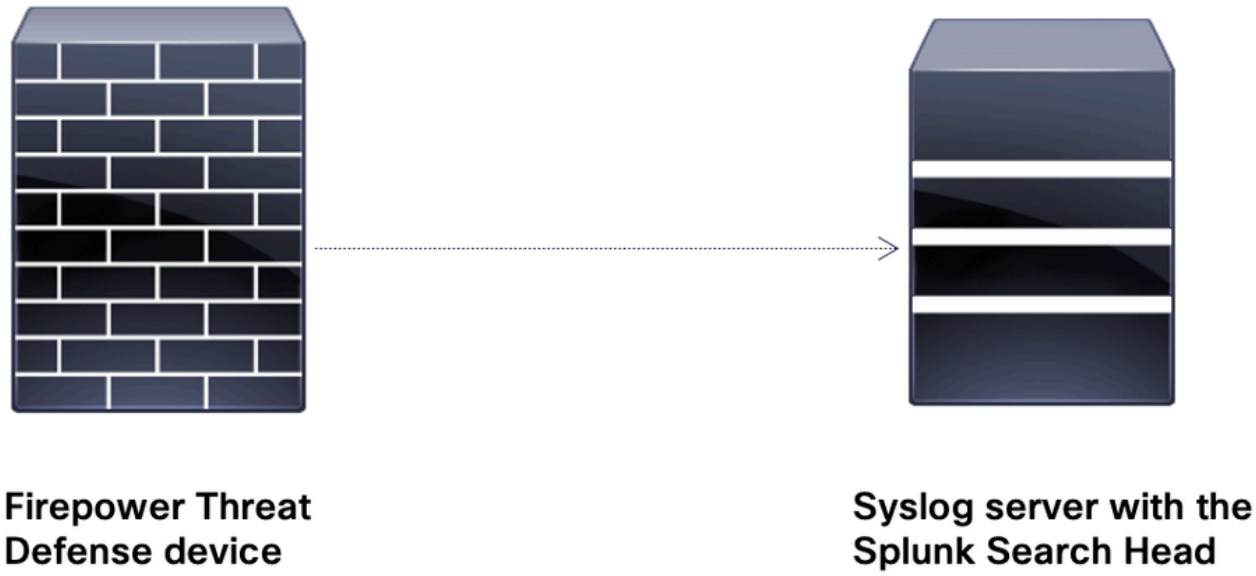
用于实现IPIS管道的底层架构的主要组件如下图所示：



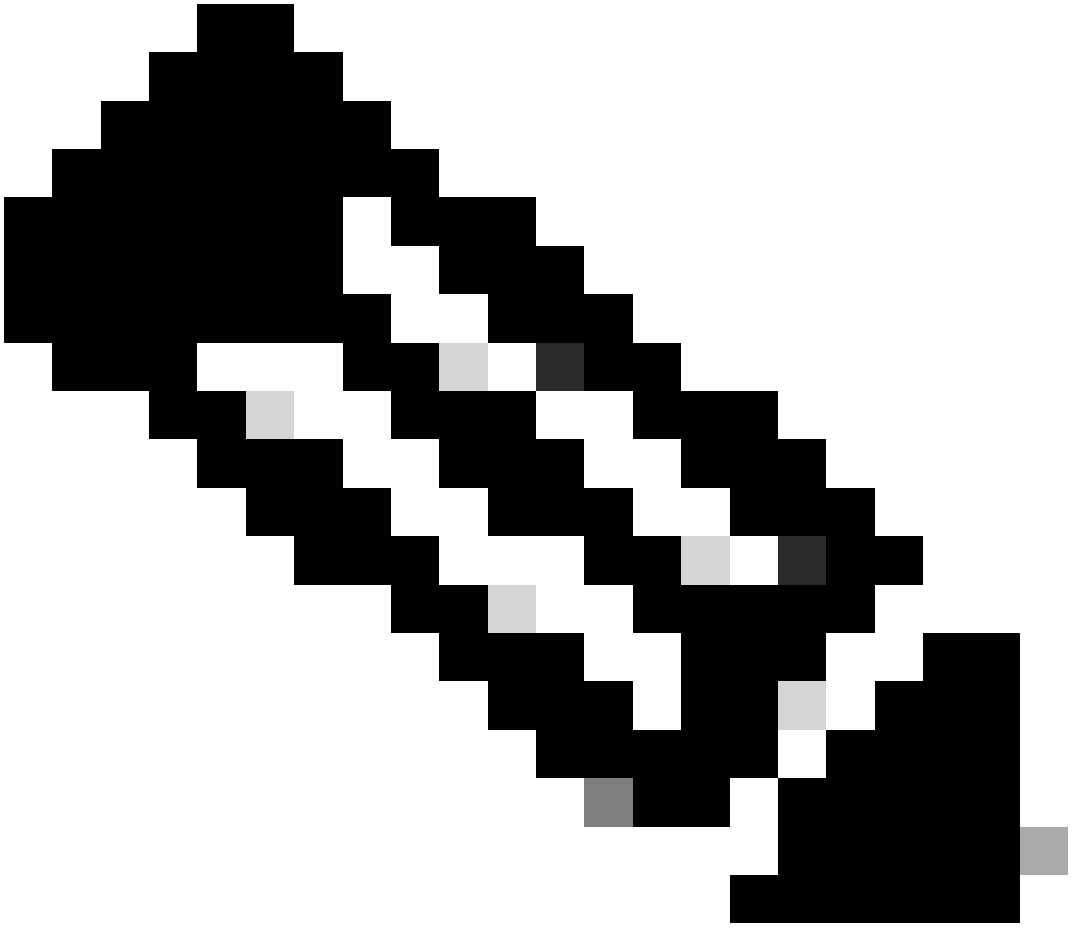
Splunk底层架构

配置

网络图


Firepower Threat Defense device
Syslog server with the Splunk Search Head

网络图

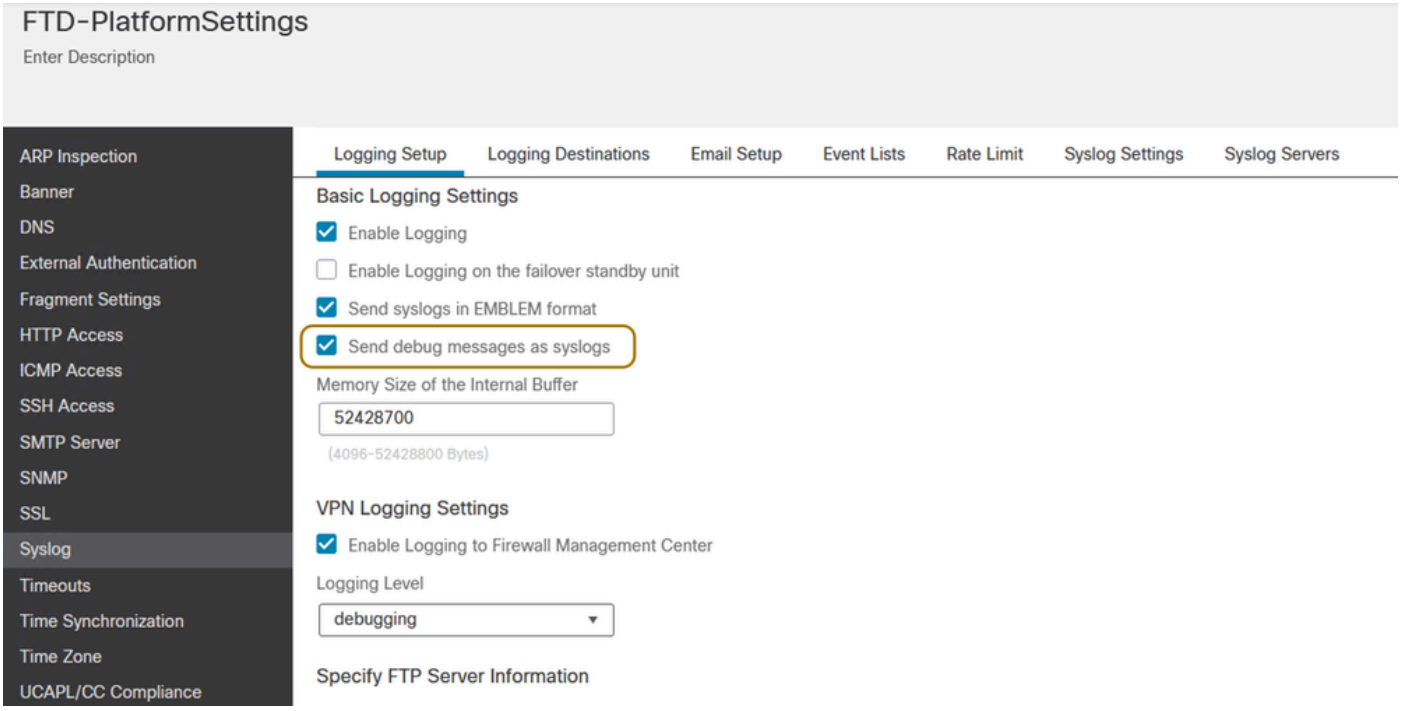


注意：本文档的实验环境不需要单独的转发器和索引器实例。安装Splunk Enterprise实例的Windows计算机（即Syslog服务器）充当索引器和搜索头。

配置

配置FTD的系统日志设置

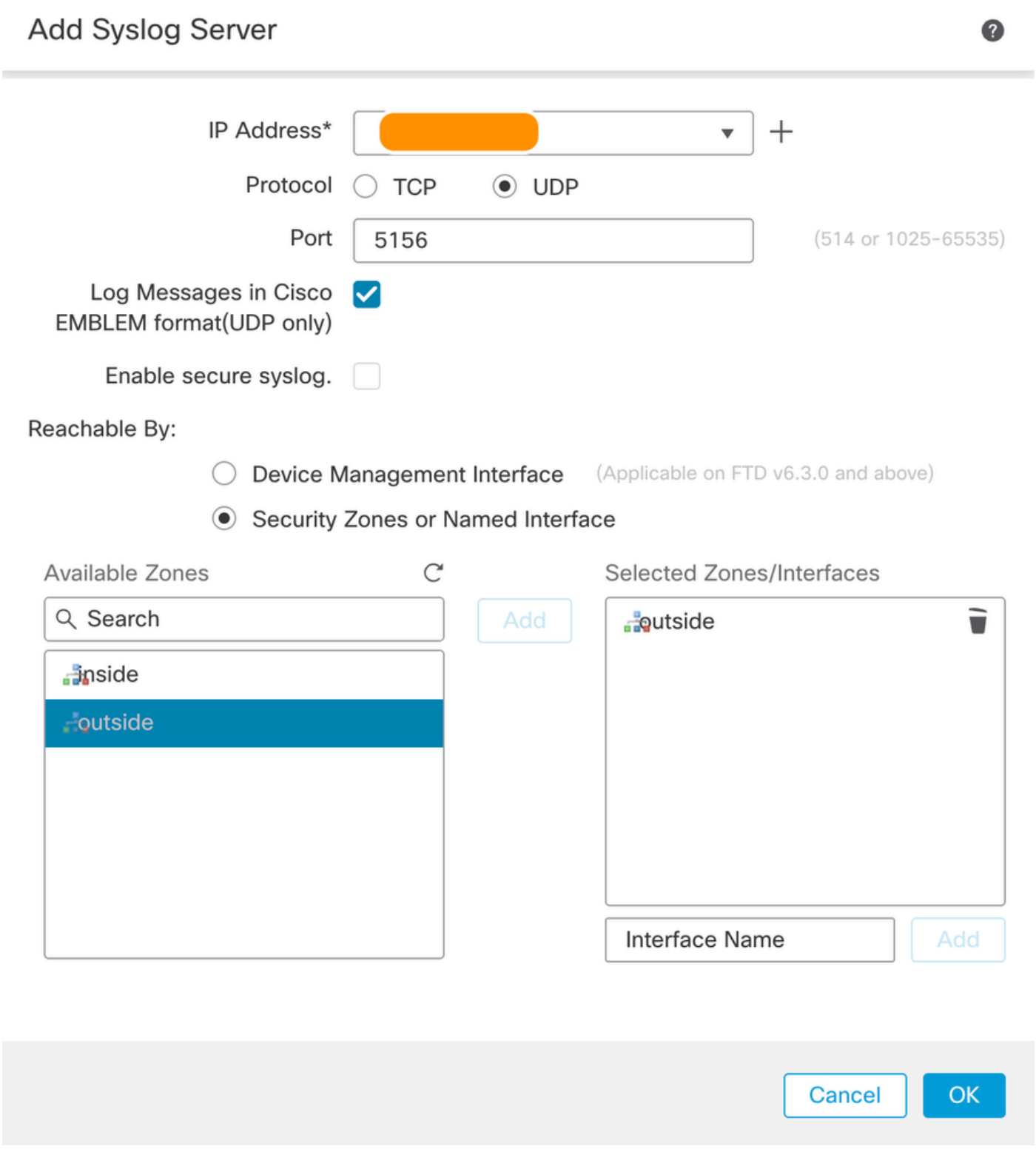
步骤1.在Devices > Platform Settings下为FTD配置FMC上的初步系统日志设置，以便将日志发送到运行Splunk实例的系统日志服务器。



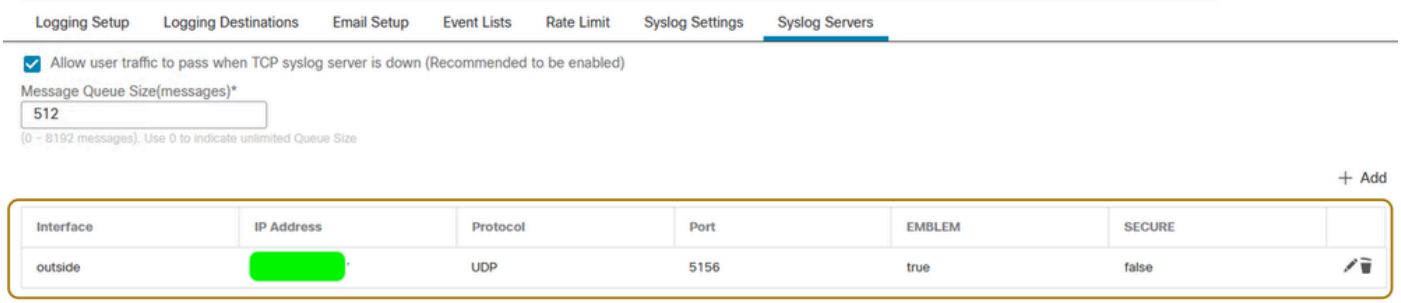
FTD上的平台设置 — 系统日志

步骤2.配置安装Splunk Enterprise实例并将其作为系统日志服务器运行的计算机的IP地址。定义上述字段。

```
IP Address: Fill in the IP address of the host acting as the syslog server
Protocol: TCP/UDP (usually UDP is preferred)
Port: You can choose any random high port. In this case 5156 is being used
Interface: Add the interface(s) through which you have connectivity to the server
```

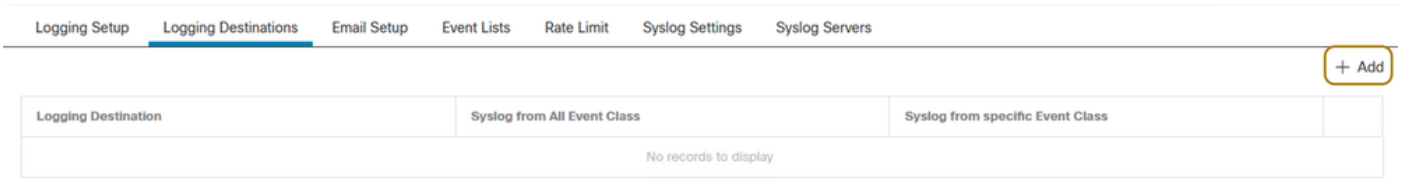


FTD上的平台设置 — 添加系统日志服务器

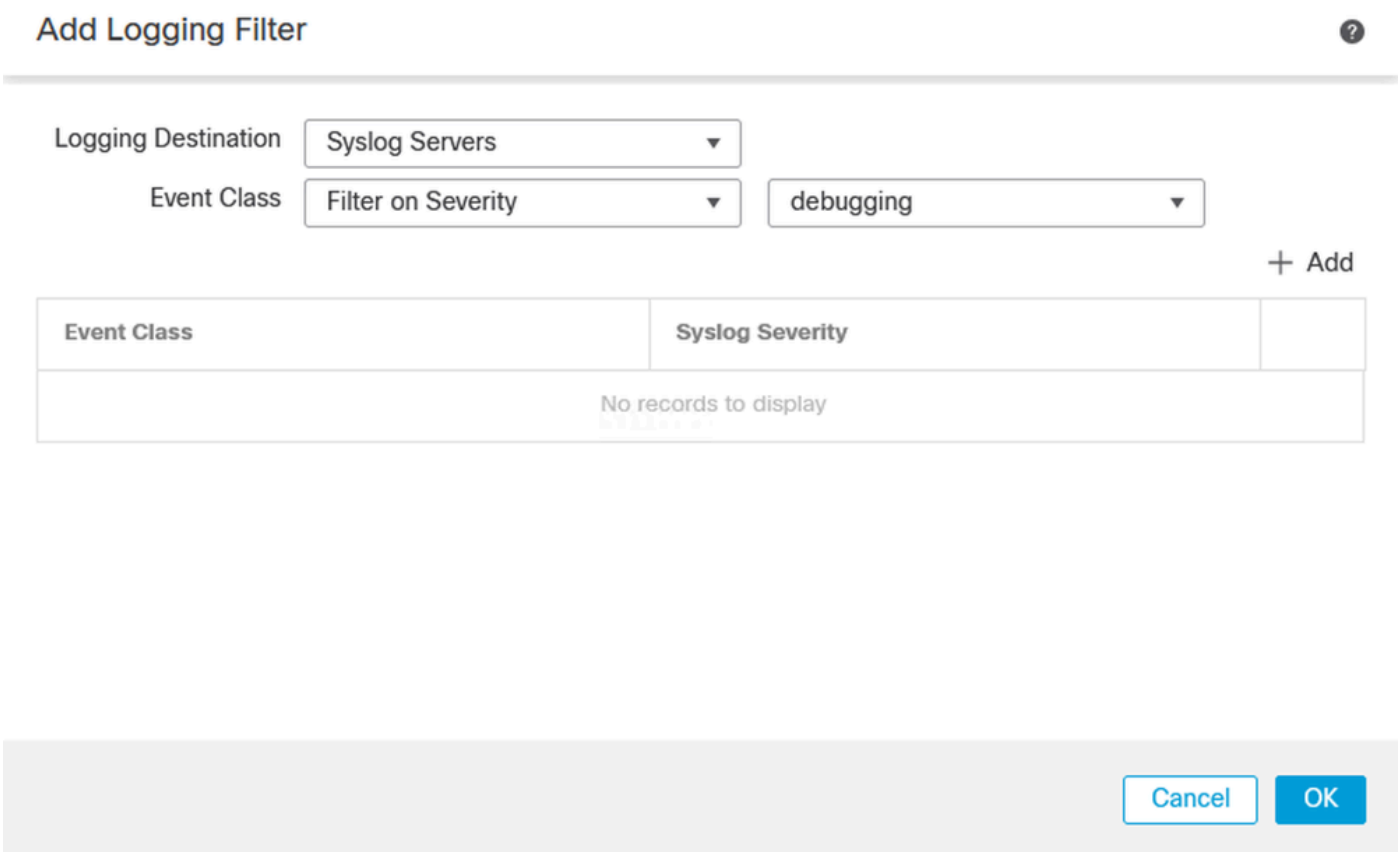


FTD上的平台设置 — 已添加系统日志服务器

步骤3.为系统日志服务器添加日志目标。可根据您的选择或使用案例设置日志级别。



FTD上的平台设置 — 添加日志记录目标



FTD上的平台设置 — 设置日志记录目标的严重性级别

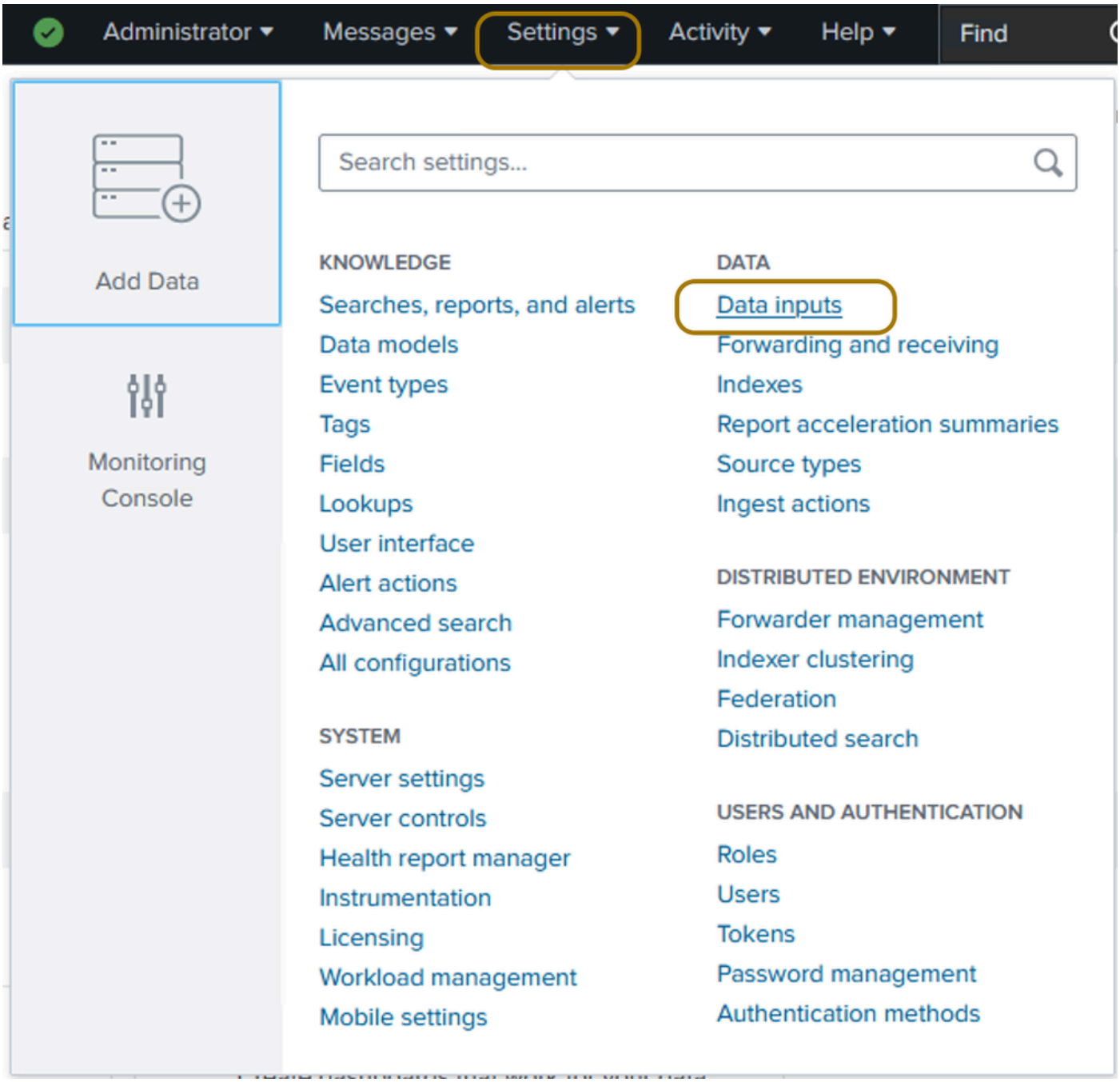
完成这些步骤后，将平台设置更改部署到FTD。

在Splunk Enterprise实例上配置数据输入

步骤1.登录到Splunk Enterprise实例Web界面。

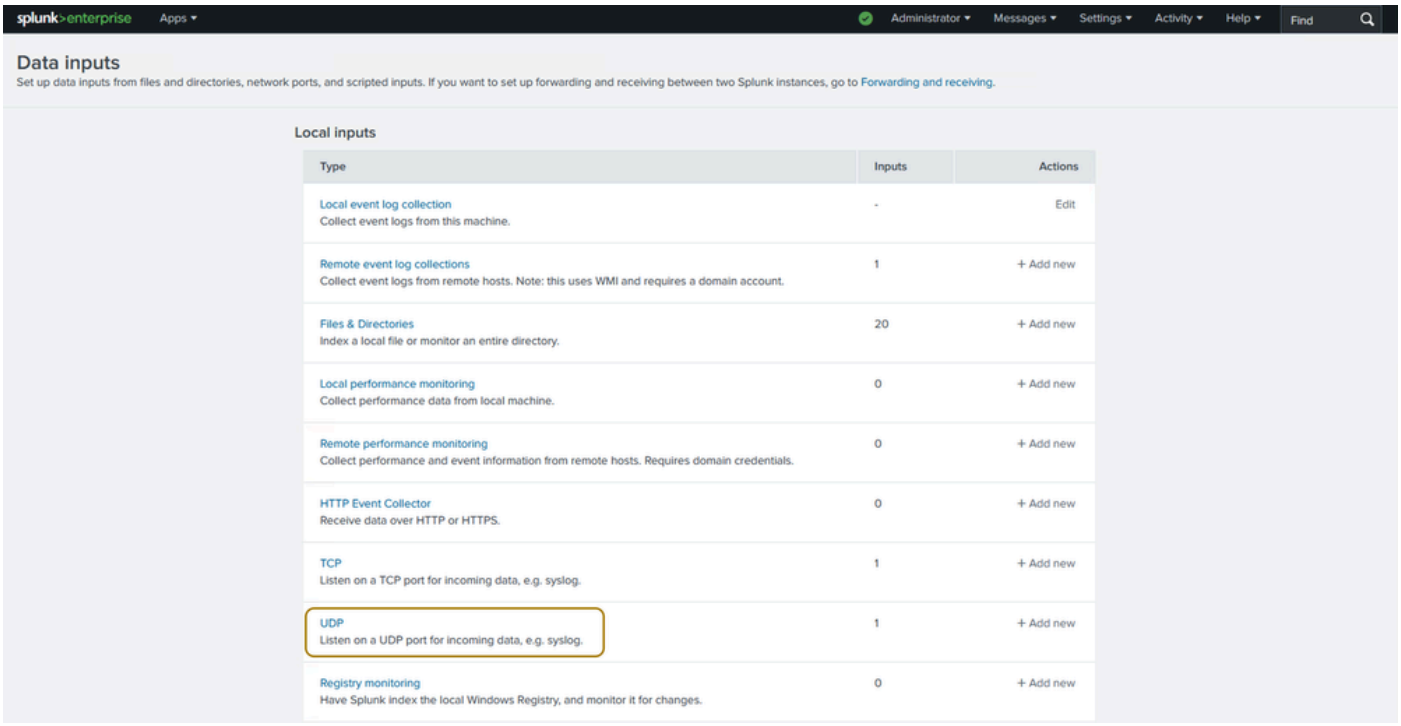
Splunk Web界面登录页

步骤2.必须定义数据输入，以便能够在Splunk上存储和索引系统日志。登录后，导航到设置>数据>数据输入。

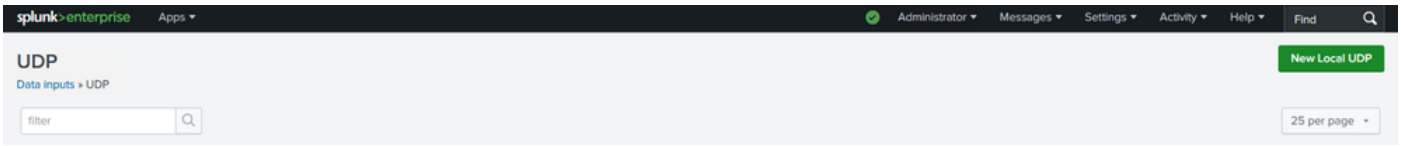


导航到Splunk上的数据输入

步骤3.选择UDP，然后在出现的下一页上单击New Local UDP。

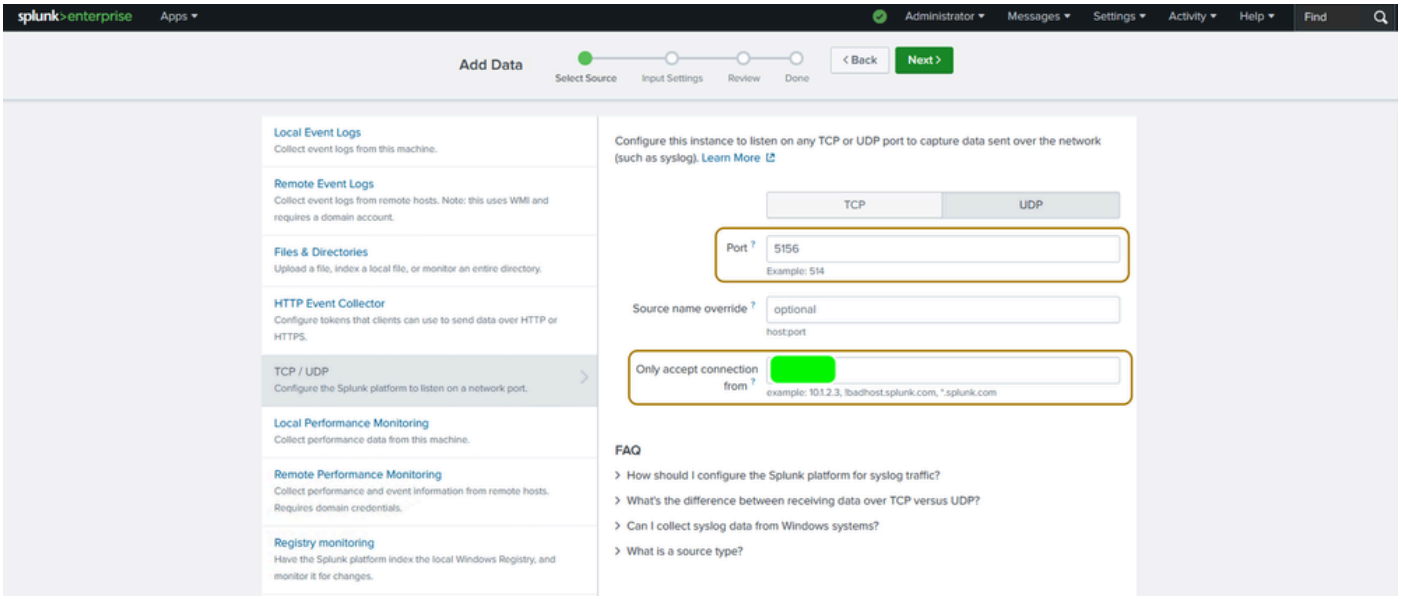


点击“UDP”以输入UDP数据



创建“新本地UDP”输入

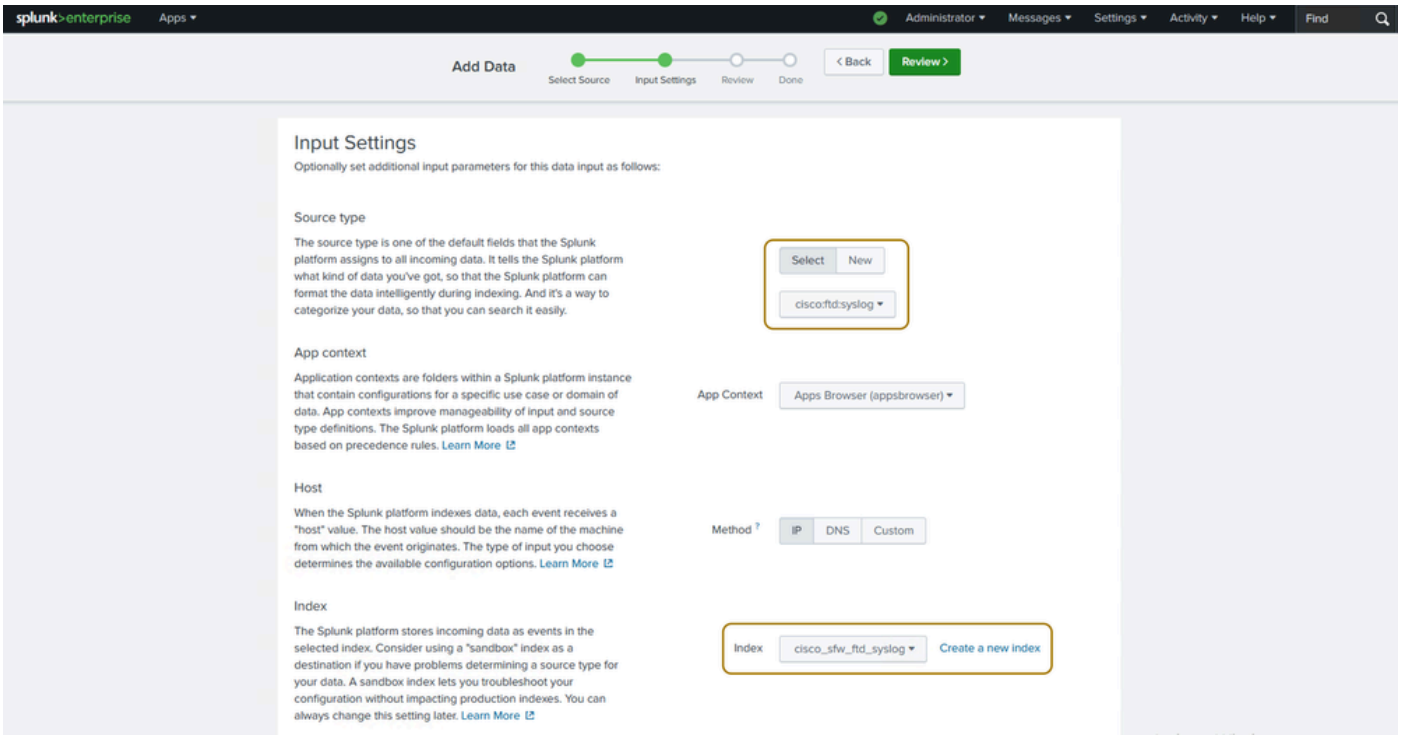
步骤4.输入发送系统日志的端口。它必须与FTD系统日志设置上配置的端口相同，在本例中为5156。要仅接受来自一个源(FTD)的系统日志，请将Only Accept Connection From字段设置为与Splunk服务器通信的FTD上接口的IP。单击 Next。



指定端口和FTD IP地址

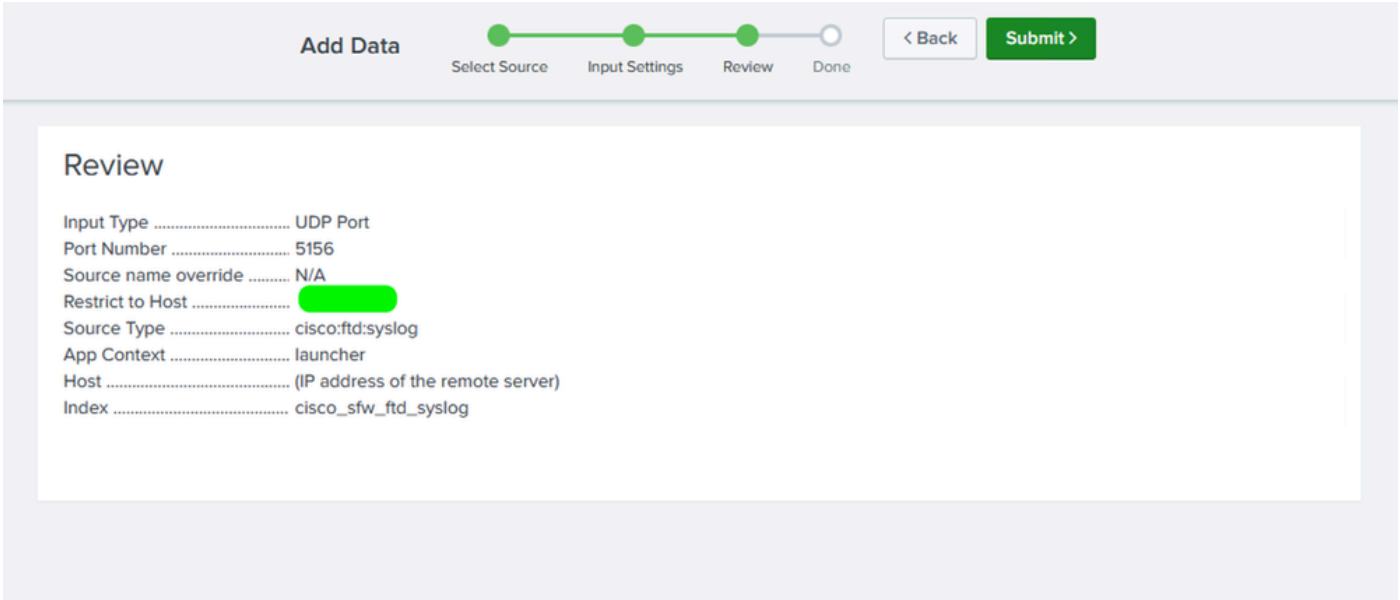
步骤5.您可以从Splunk上预定义字段值中搜索并选择源类型和索引字段值，如下一幅图像中所突出

显示的。默认设置可用于其余字段。



配置数据输入设置

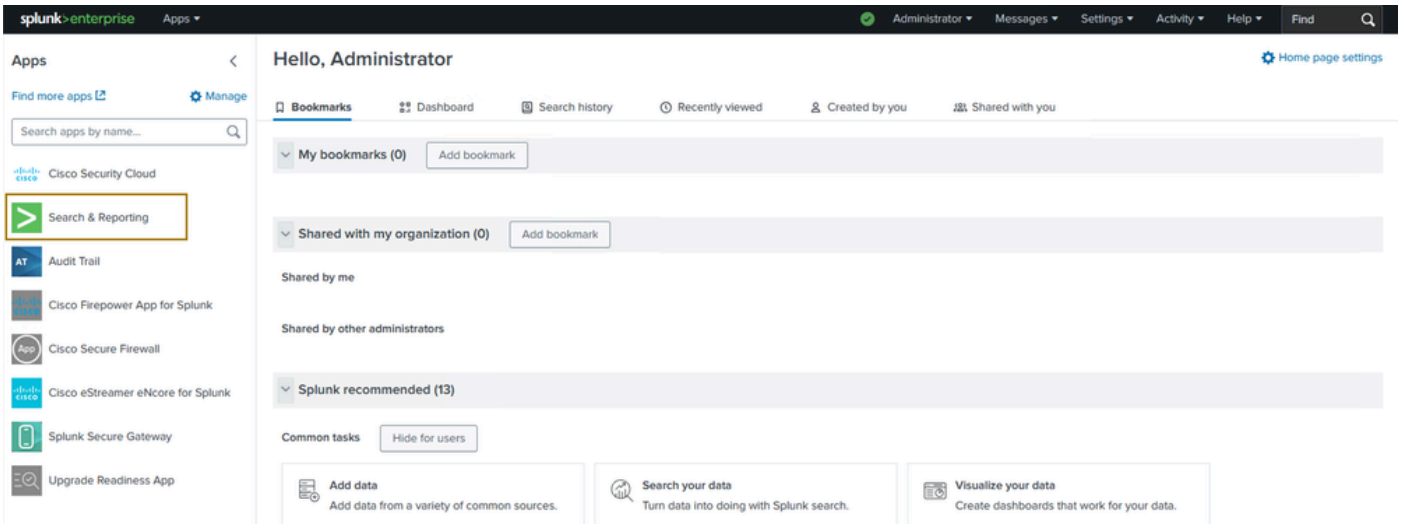
步骤6.检查设置并单击Submit。



查看数据输入设置

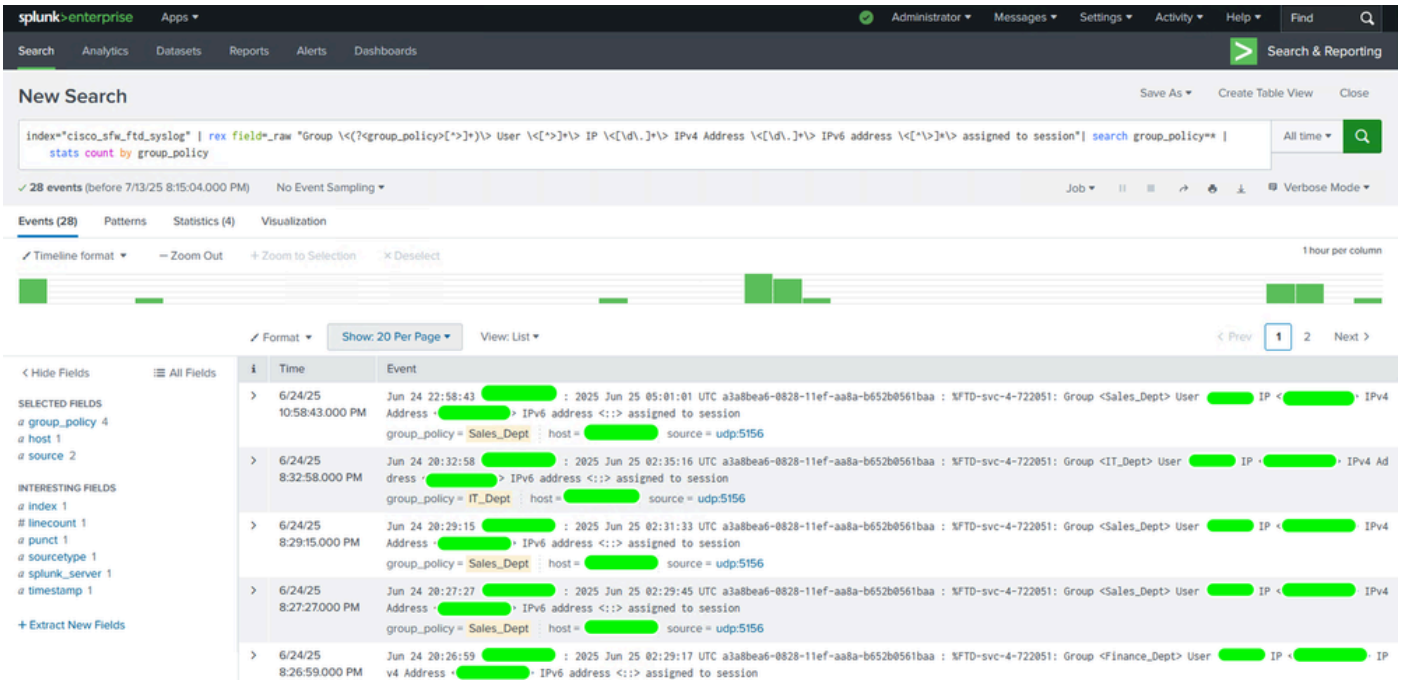
执行SPL查询和创建控制面板

第1步：导航到Splunk上的搜索和报告应用。

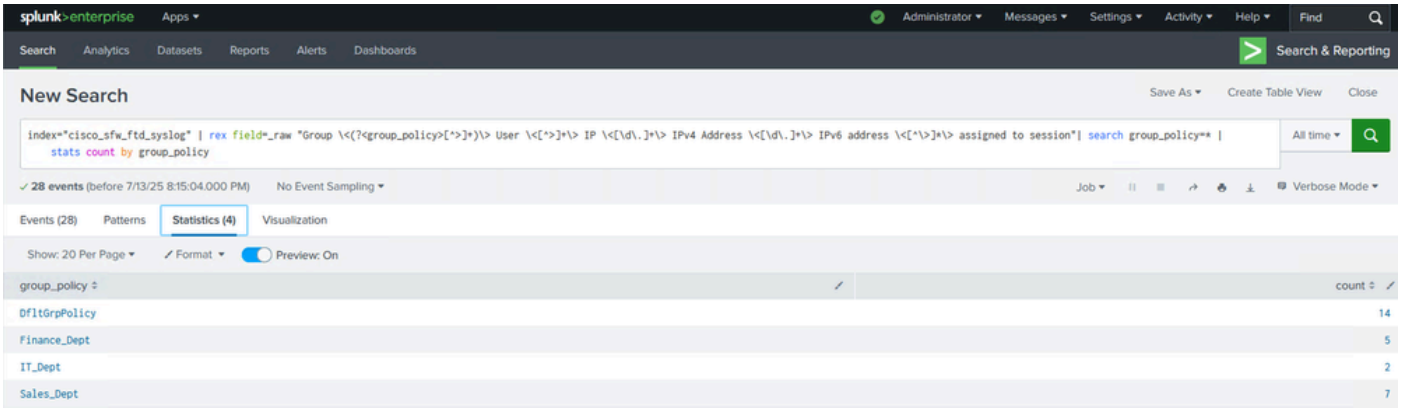


导航至搜索和报告应用

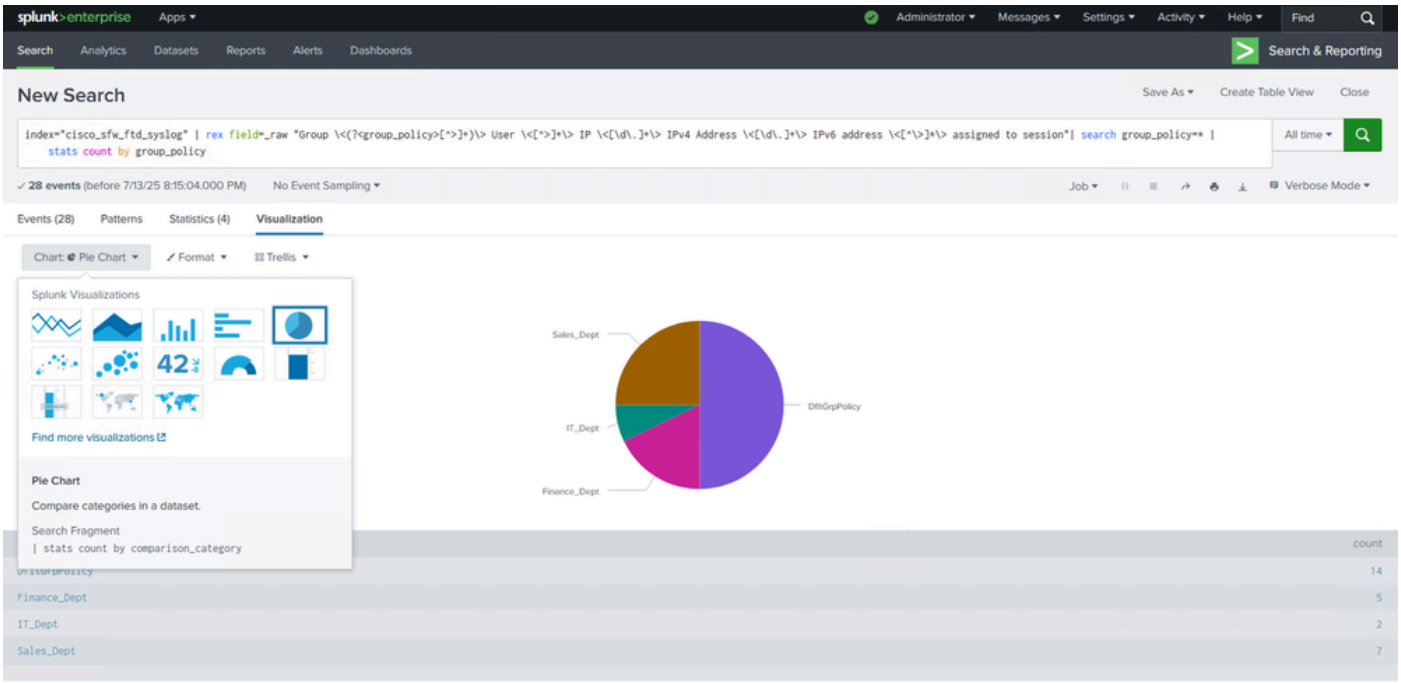
步骤2.根据要可视化的数据制定并执行SPL查询。您可以在Events选项卡下完整查看每个日志(在详细模式下)，在Statistics选项卡中查看每个组策略的连接计数，并在Visualization选项卡下使用这些统计信息查看此数据。



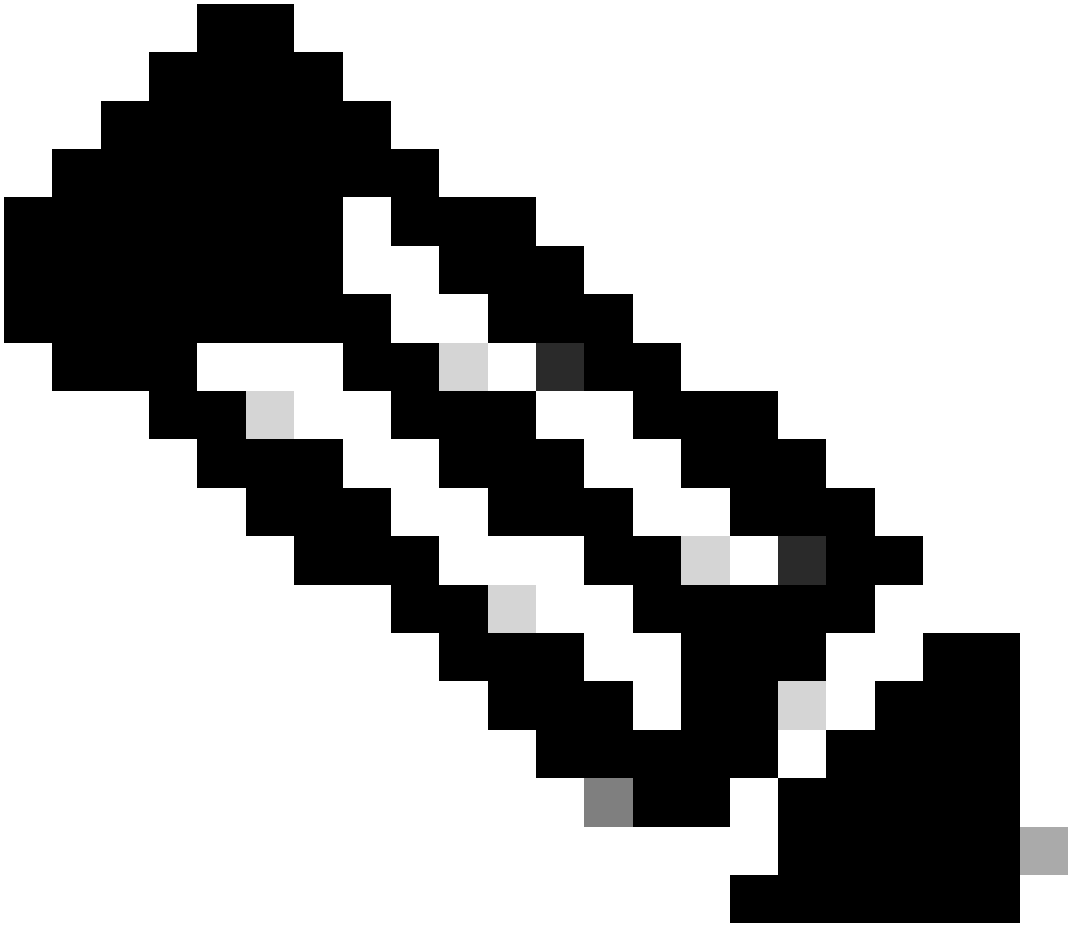
使用SPL查询搜索事件



检查统计信息选项卡

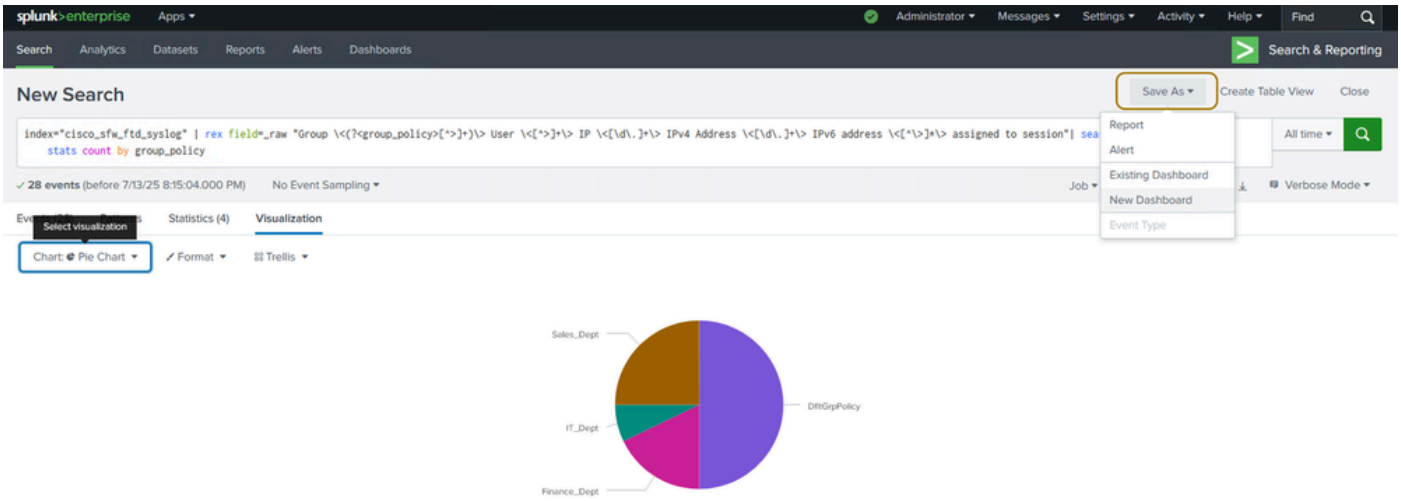


“可视化”选项卡将显示图形/图表



注意：在本示例中，查询获取不同组策略之间成功远程访问VPN连接的日志。已使用饼图来显示每个组策略成功连接的数量和百分比。根据您的要求和首选项，您也可以选择使用其他类型的可视化，如条形图。

步骤3.单击另存为，然后选择新建或现有仪表板，具体取决于您是否已具有要将此面板添加到其中的仪表板，还是要创建新仪表板。本示例显示了后者。



将面板保存到控制面板

步骤4.为正在创建的仪表板指定标题，并为将包含饼图的面板提供标题。

Save Panel to New Dashboard

Dashboard Title: FTD_Dashboard

ftd_dashboard Edit ID

Description: Optional

Permissions: Private

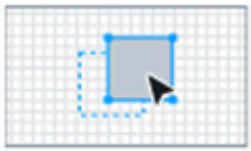
How do you want to build your dashboard? What's this?

Classic Dashboards
The traditional Splunk dashboard builder

Dashboard Studio NEW
A new builder to create visually-rich, customizable dashboards

Select layout mode

Absolute
Full layout control



Grid
Quick organization

Panel Title: Successful RAVPN Connections Per Group Policy

Visualization Type: Pie Chart | Statistics Table

> Advanced Panel Settings

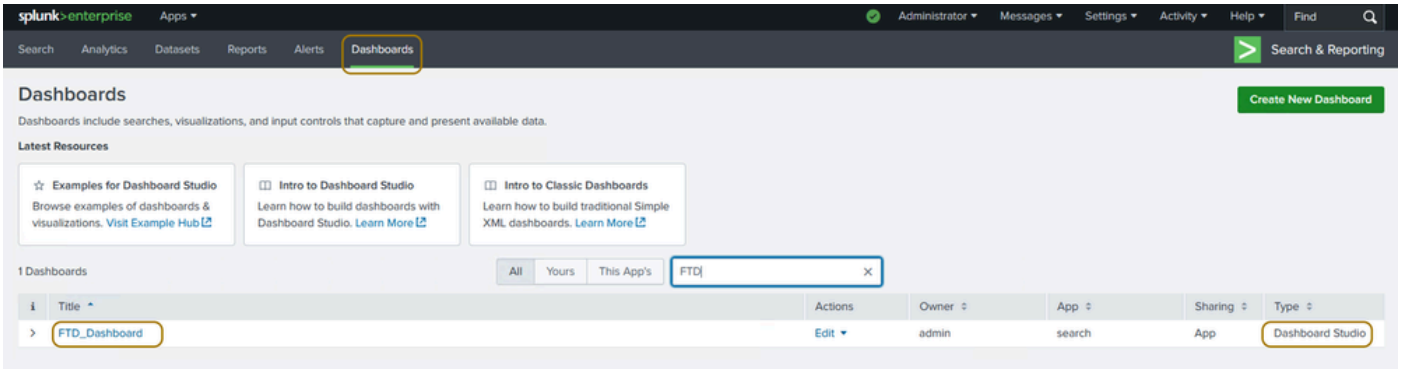
Cancel Save to Dashboard

新控制面板的设置

权限设置为。此外，根据您是否要精细控制仪表板的面板设置和布局，选择经典模式或仪表板工作室模式来构建仪表板。

第 5 步（可选）：按照您的要求，使用前面提到的步骤，执行更多SPL查询并将其保存为面板到此控制面板。

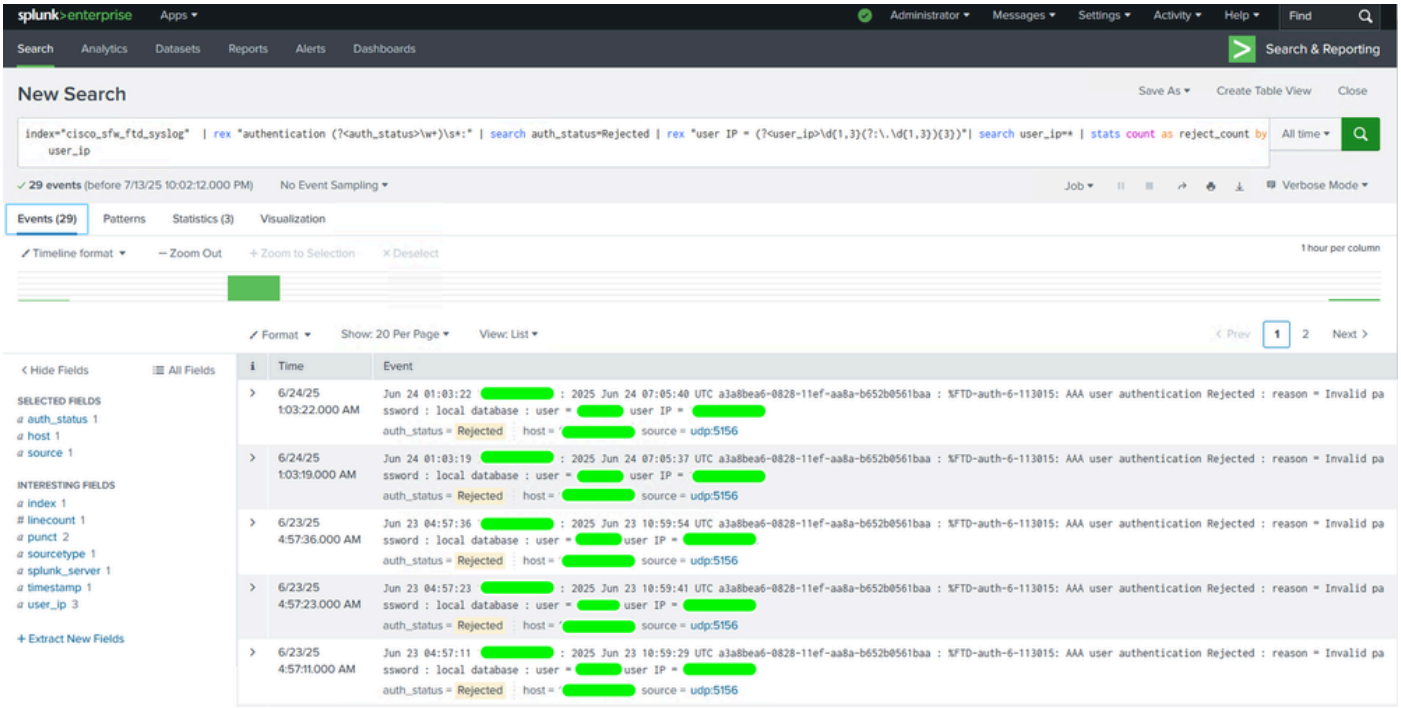
步骤6.定位至控制面板选项卡，以便搜索并选择您创建的控制面板。单击它查看、编辑或重新排列其面板。



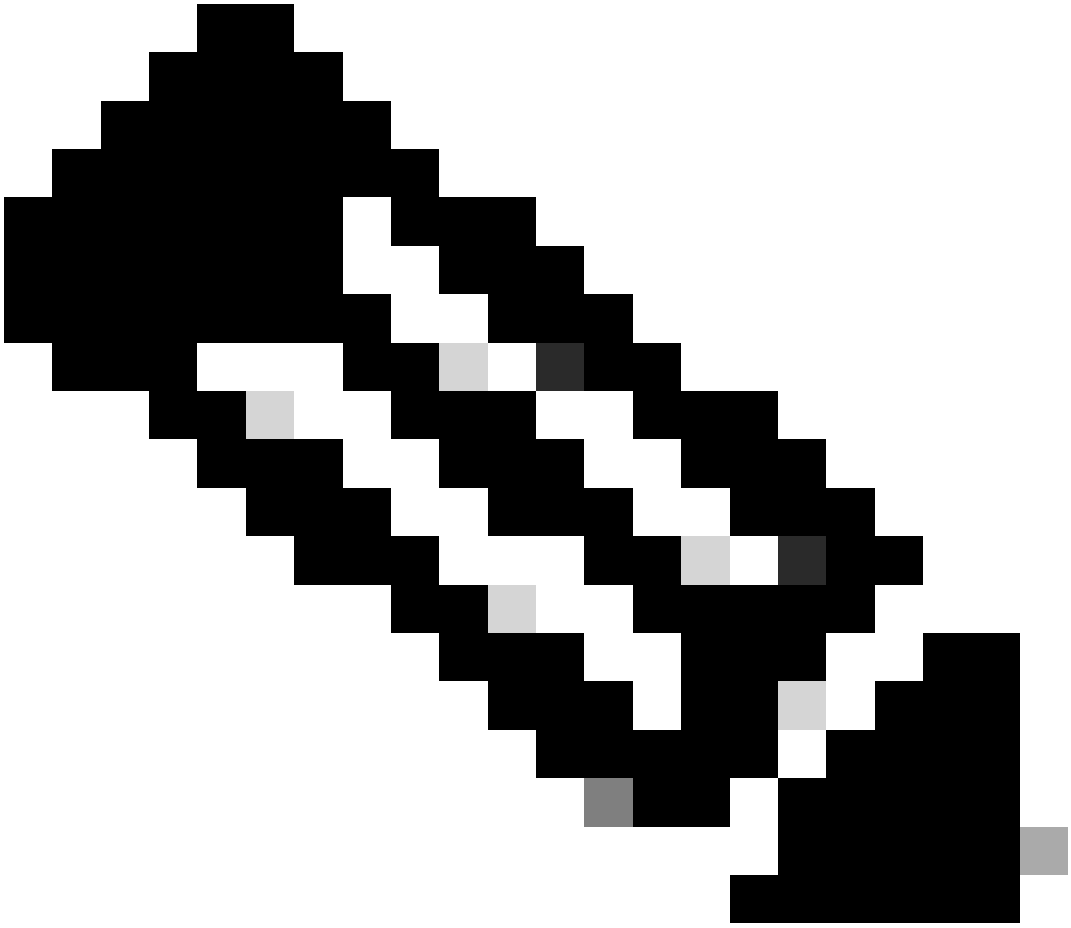
如何查看控制面板

根据SPL查询配置警报

步骤1.导航到Search and Reporting App以构建和运行SPL查询，以验证其正在获取用于触发警报的正确日志。



运行SPL查询以创建相应的警报



注意：在本示例中，查询用于获取远程访问VPN的失败身份验证日志，以便在在一定时间内失败尝试次数超过特定阈值时触发警报。

步骤3.单击另存为并选择警报。

保存警报

步骤4.为警报命名。填写配置警报所需的所有其他详细信息和参数，然后点击Save。此处已提到用于此警报的设置。

<#root>

Permissions: Shared in App.
Alert Type: Real-time (allows failed user authentications in the last 10 minutes can be tracked continu
Trigger Conditions: A

custom

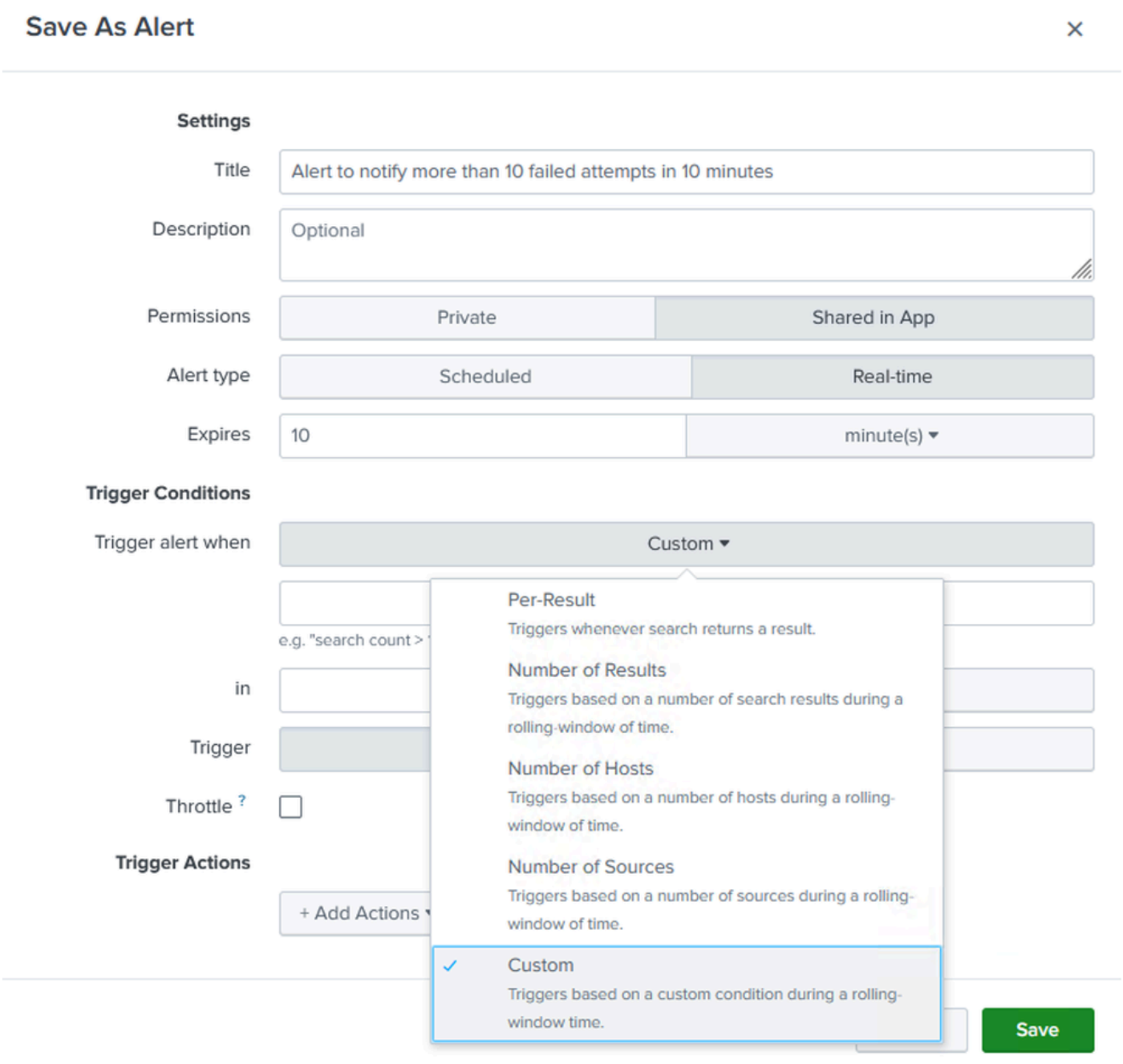
condition is used to search if the

reject_count

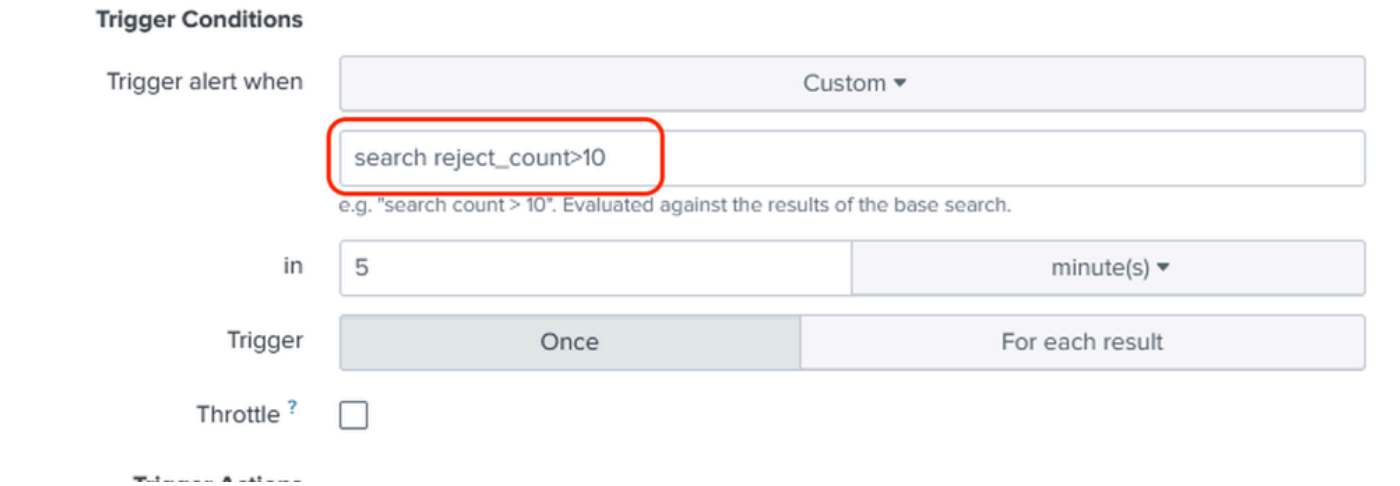
counter from the SPL query has exceeded 10 in the last 5 minutes for any IP address.
Trigger Actions: Set a trigger action such as

Add to Triggered Alerts, Send email, etc.

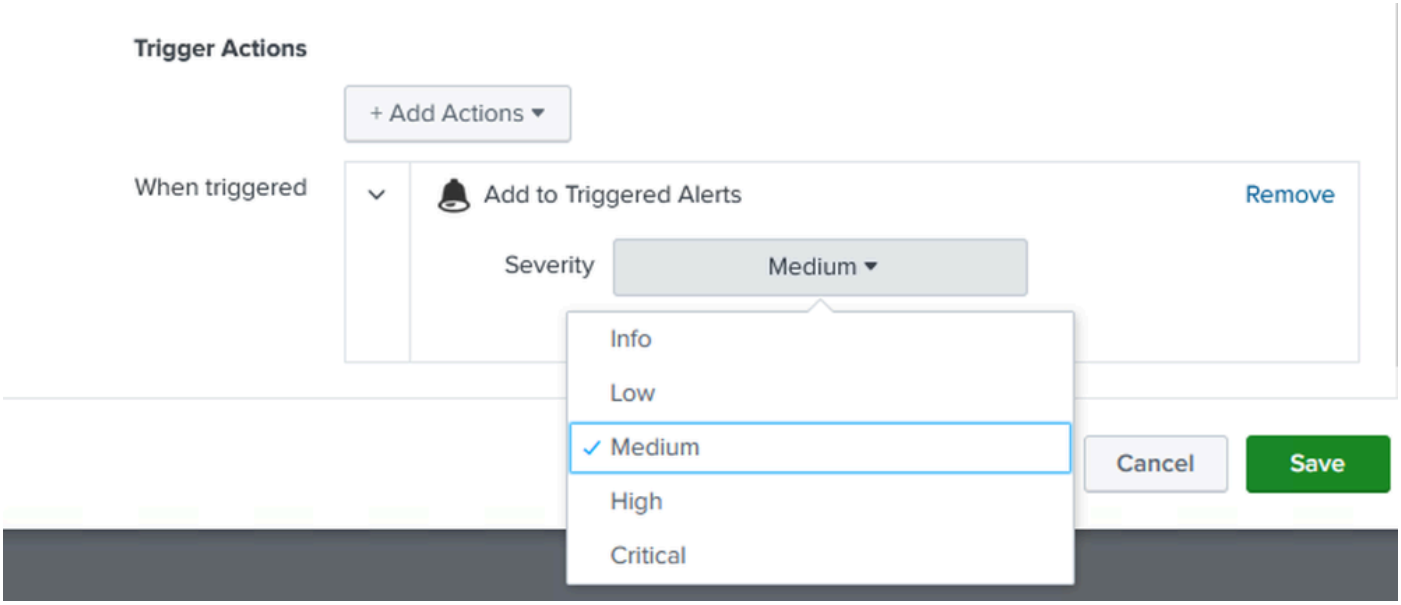
and set the alert severity as per your requirement.



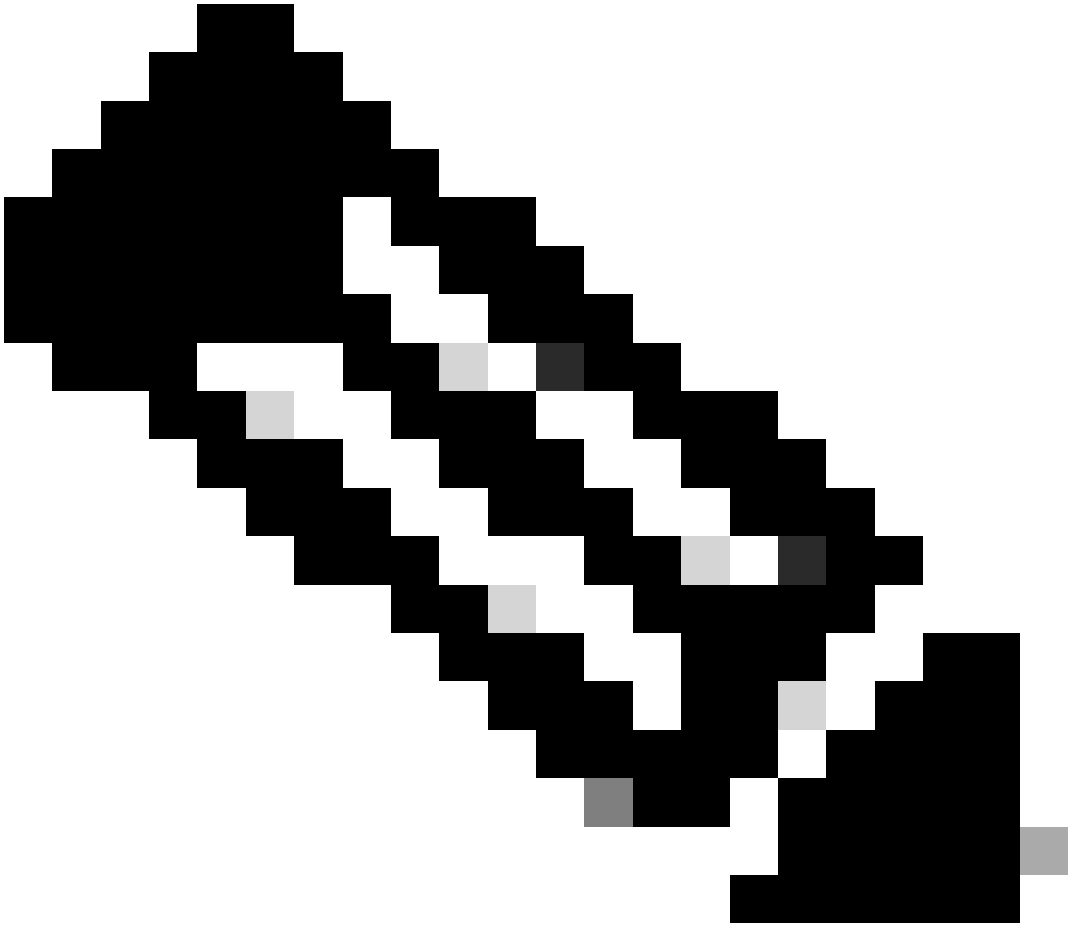
创建警报的其他设置



创建警报的其他设置



创建警报的其他设置



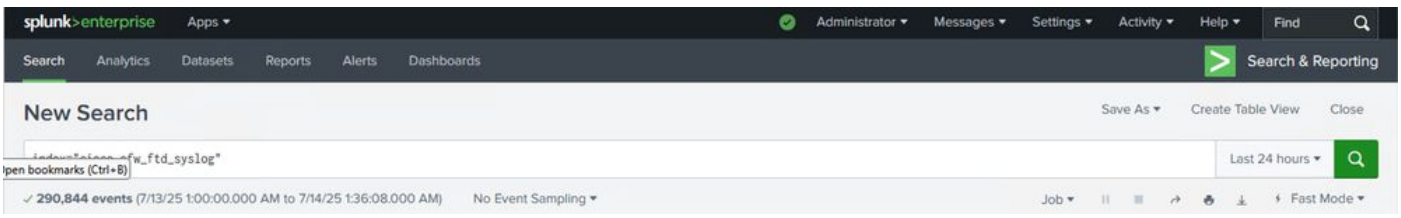
注意：如果要触发每个结果的警报，还必须相应地定义限制设置。

验证

创建控制面板和警报后，您可以按照本节提供的说明验证配置、数据流、控制面板和实时警报。

查看日志

您可以使用搜索应用来确认是否收到防火墙发送的日志，并且这些日志是否可以显示在splunk搜索头中。可以通过检查索引的最新日志(搜索索引= "cisco_sfw_ftd_syslog")以及与其关联的时间戳来验证这一点。

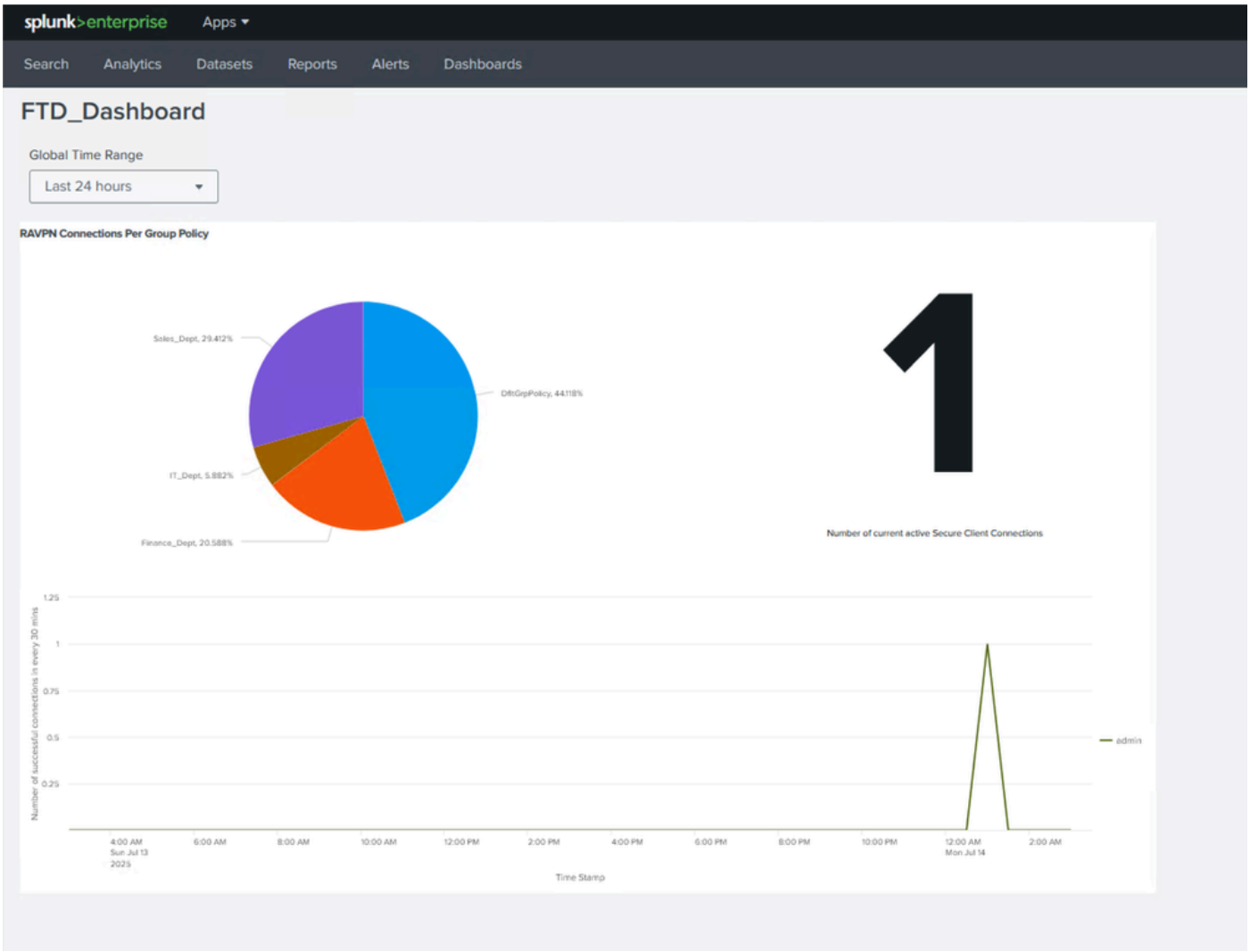


检查并查看日志

检查并查看日志

查看实时控制面板

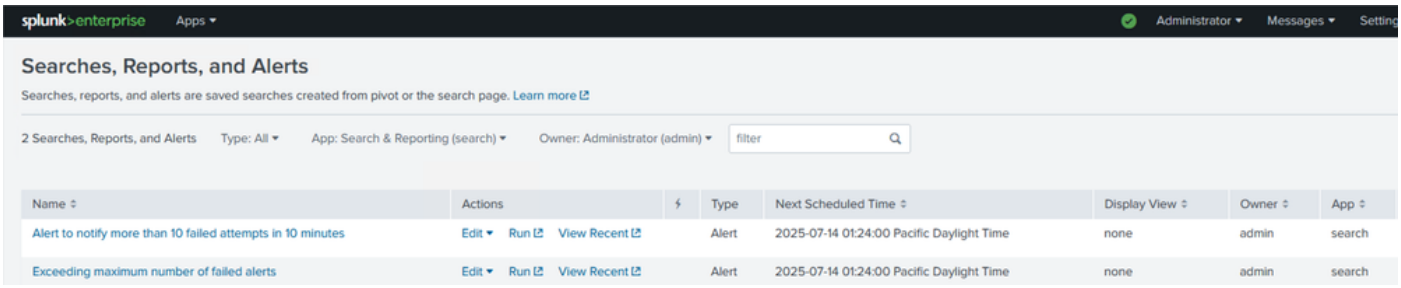
您可以导航到已创建的自定义控制面板，并在从FTD生成新数据和日志时，查看每个面板上的更改。



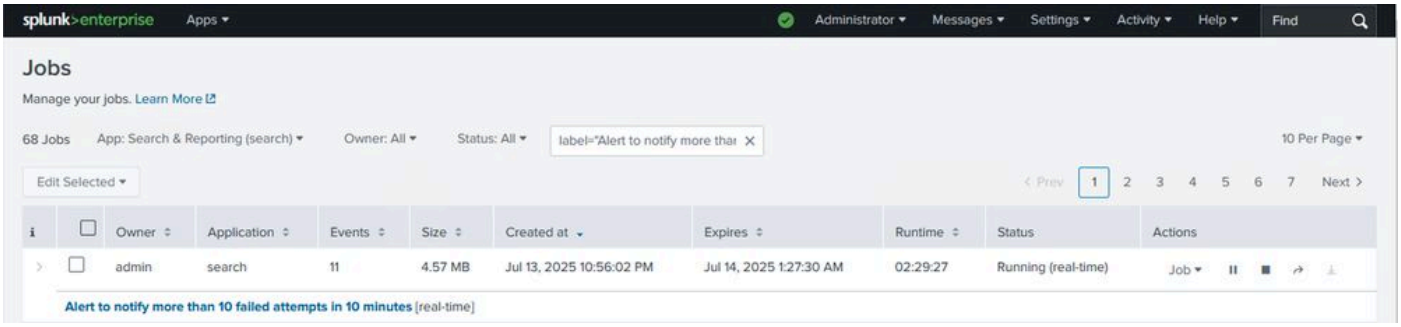
查看控制面板

检查是否已触发任何警报

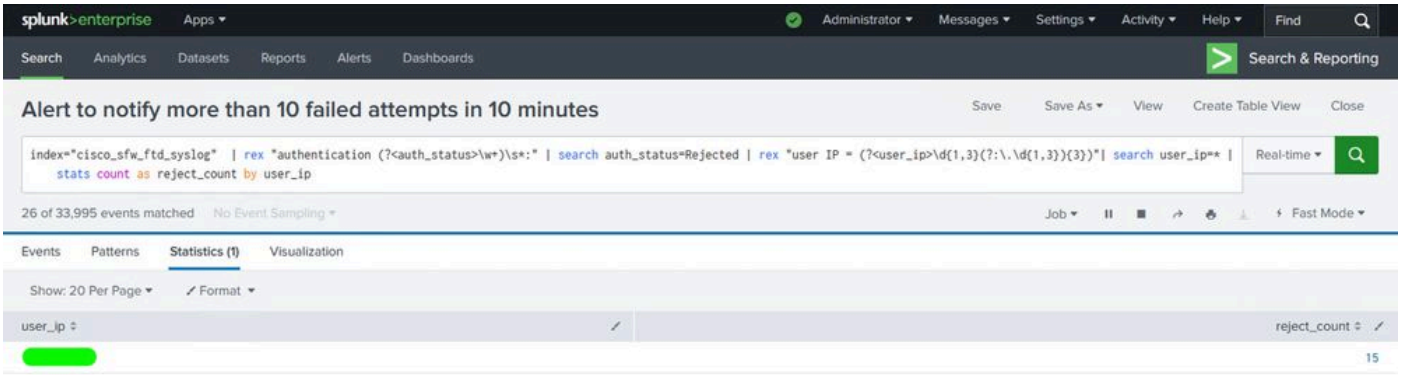
为了验证有关警报的信息，您可以导航到搜索、报告和警报部分，查看最近的警报信息。单击View Recent以进一步检查作业和搜索。



检查并查看警报



检查并查看警报



检查触发警报的统计信息

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。