配置响应管理以将系统日志事件发送到Splunk

目录

简介

本文档介绍如何配置Secure Analytics响应管理功能，以通过系统日志向第三方（如Splunk）发送事件。

先决条件

要求

Cisco 建议您了解以下主题：

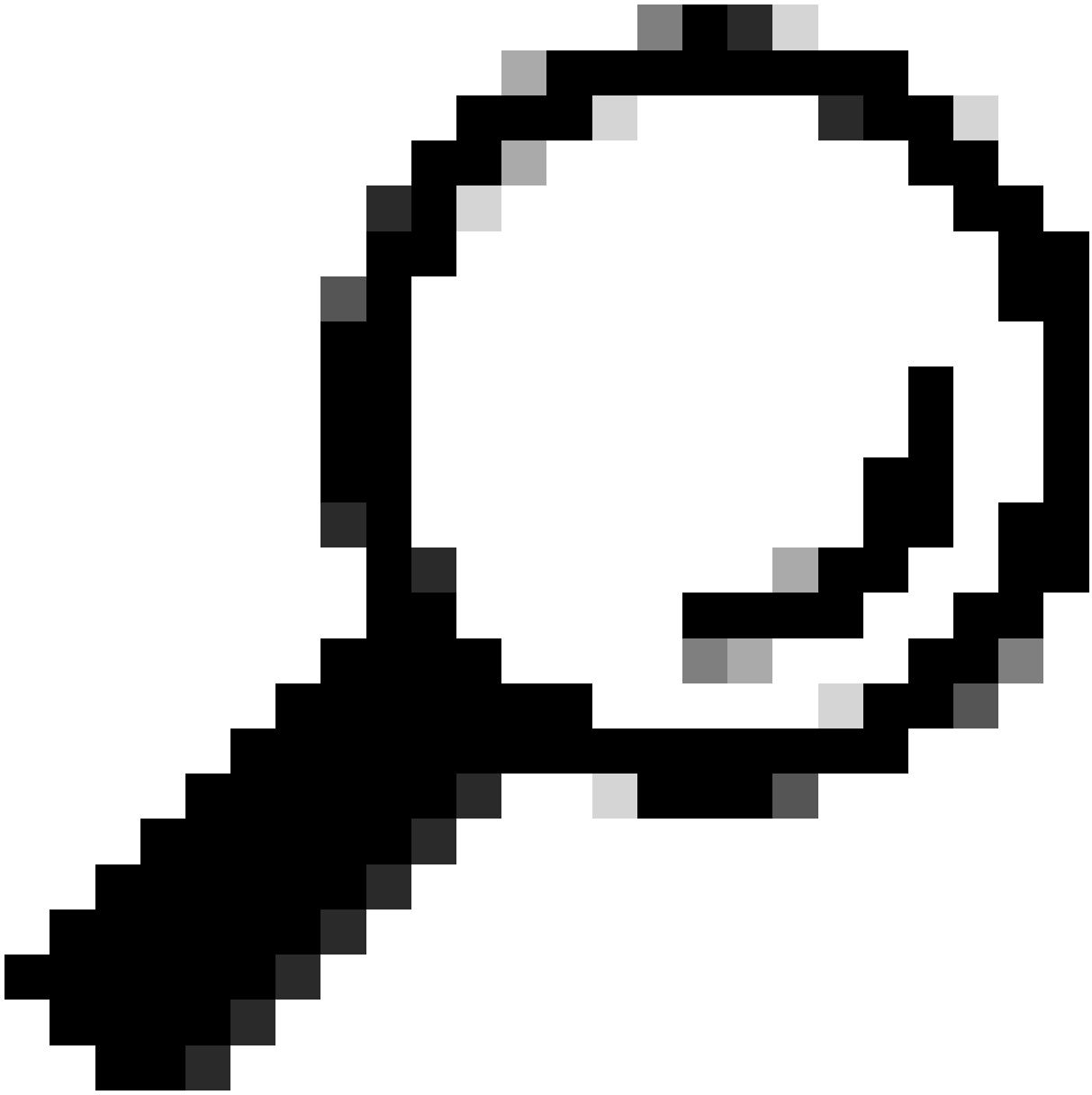
- 安全网络分析响应管理。
- Splunk系统日志

使用的组件

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

- 安全网络分析(SNA)部署，至少包含一个管理器设备和一个流量收集器设备。
- Splunk服务器已安装并可通过443端口访问。

在SNA over UDP 514或自定义端口上配置系统日志



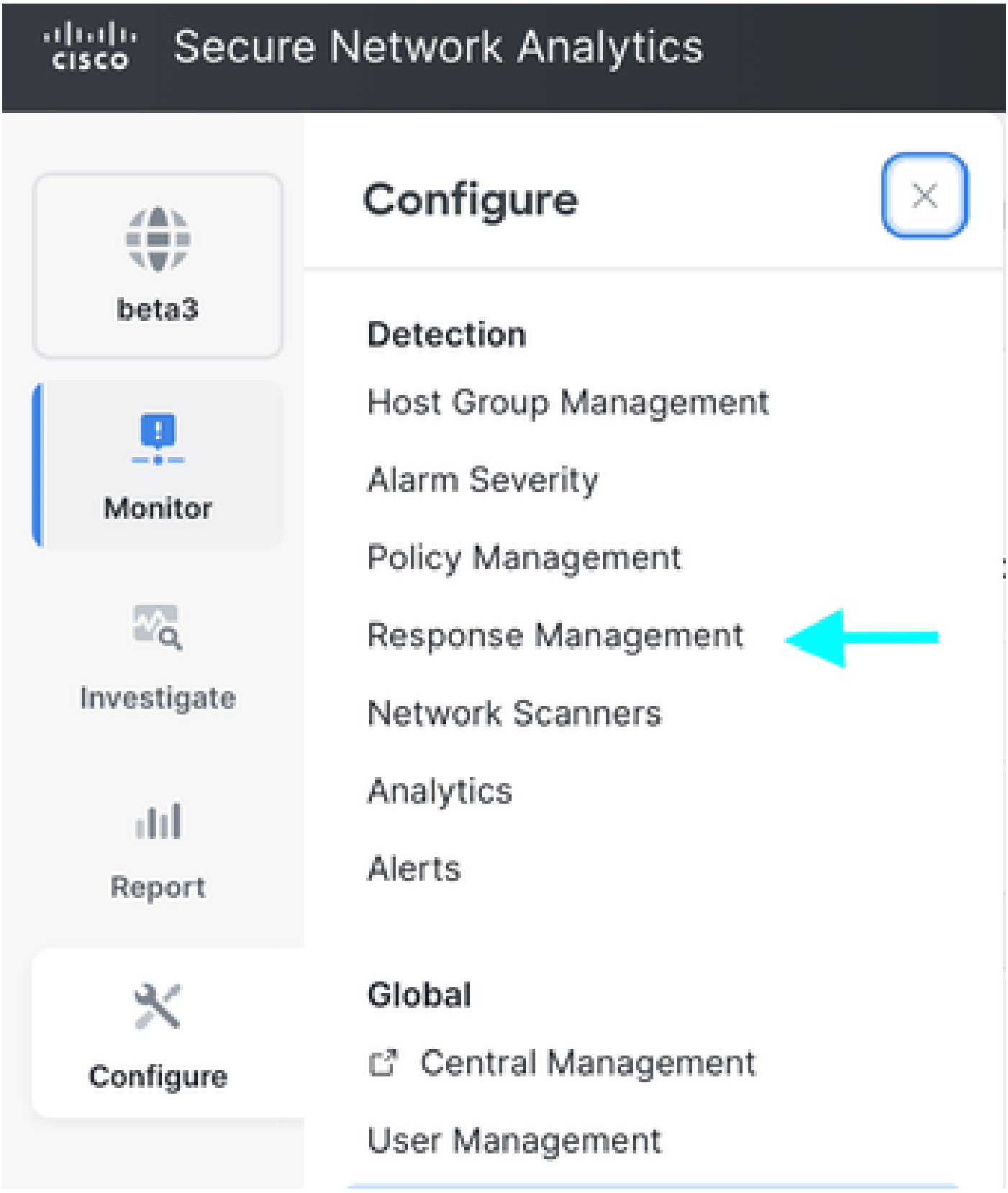
提示：确保在SNA和Splunk之间的任何防火墙或中间设备上允许UDP/514、TCP/6514或任何您为系统日志选择的自定义端口。

1.SNA响应管理

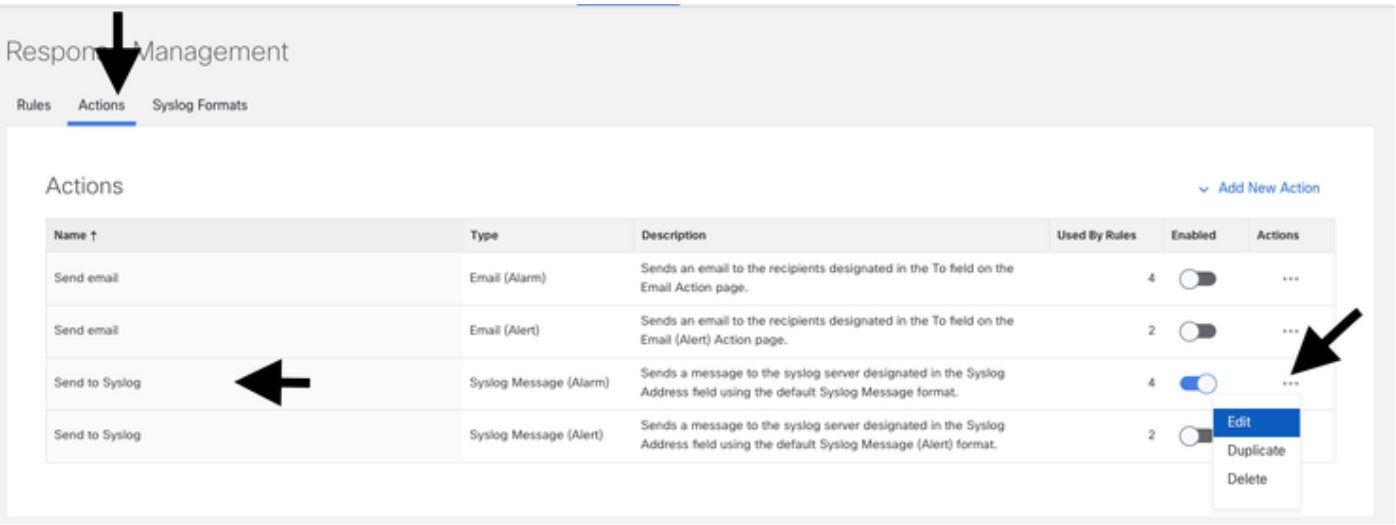
安全分析(SA)的响应管理组件可用于配置规则、操作和系统日志目标。

必须配置这些选项，才能将Secure Analytics警报发送/转发到其他目标。

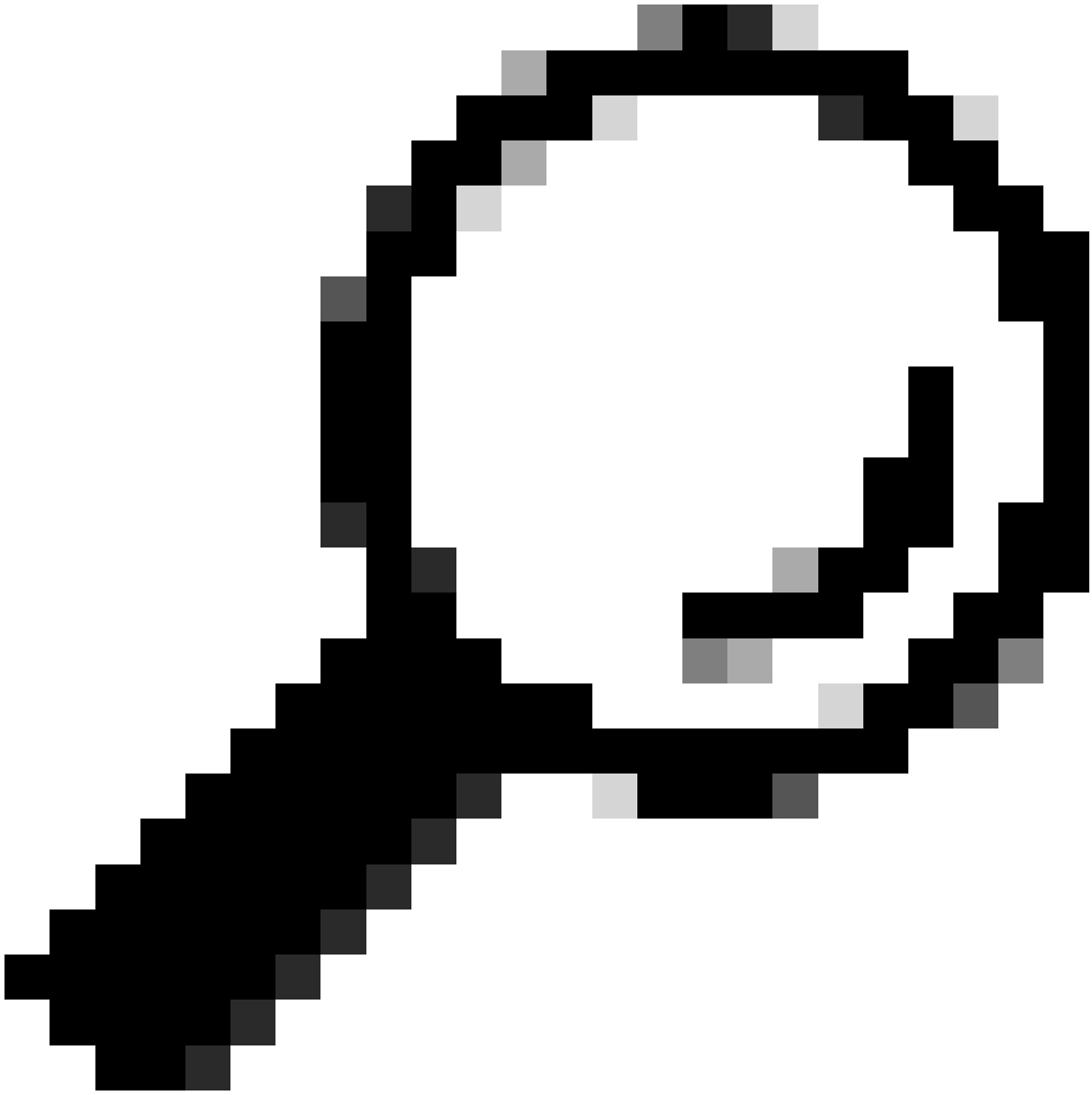
步骤1:登录到SA Manager设备，然后导航到配置 > 检测响应管理。



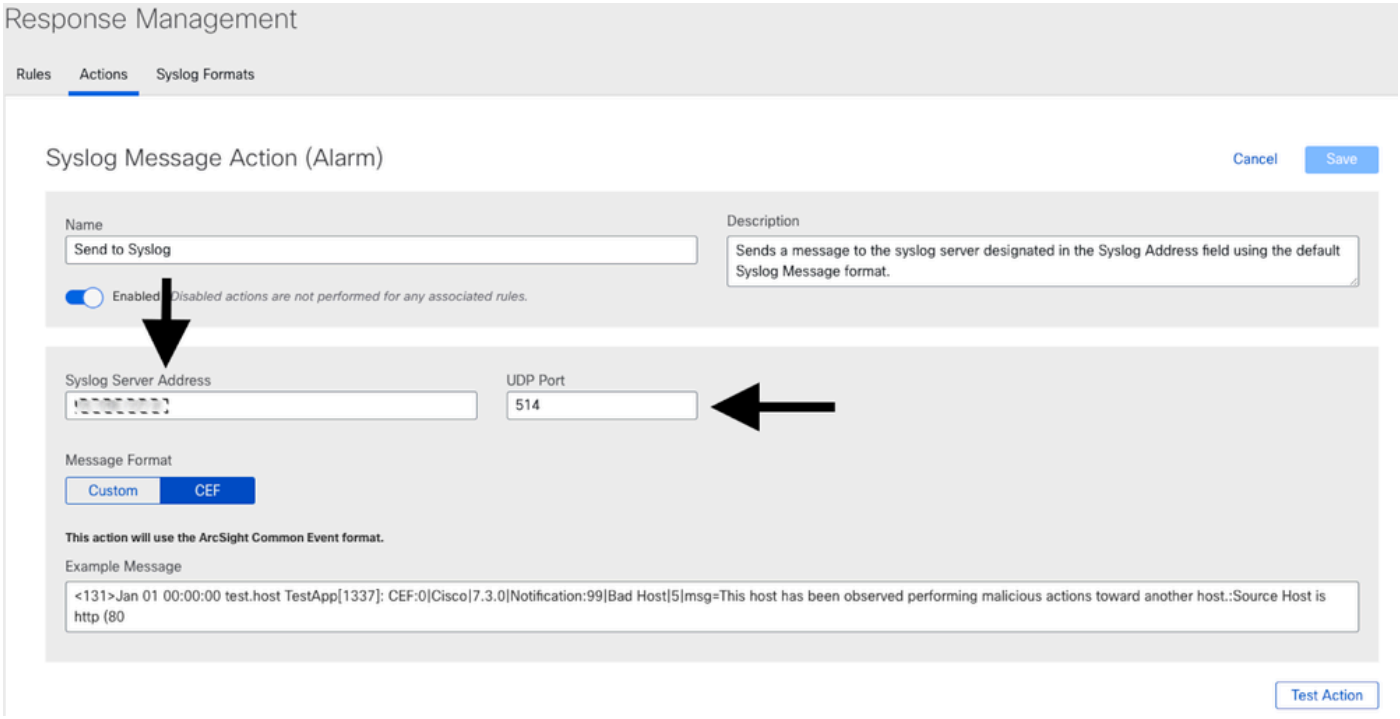
步骤 2：在新页面上，导航到操作选项卡，找到默认的发送到系统日志行项目，然后单击操作列中的省略号(...)，然后单击编辑。



步骤 3：在Syslog Server Address字段中输入所需的目标地址，在UDP Port字段中输入所需的目标接收端口。在消息格式中选择CEF。
步骤 4：完成后，单击右上角蓝色的Save按钮。



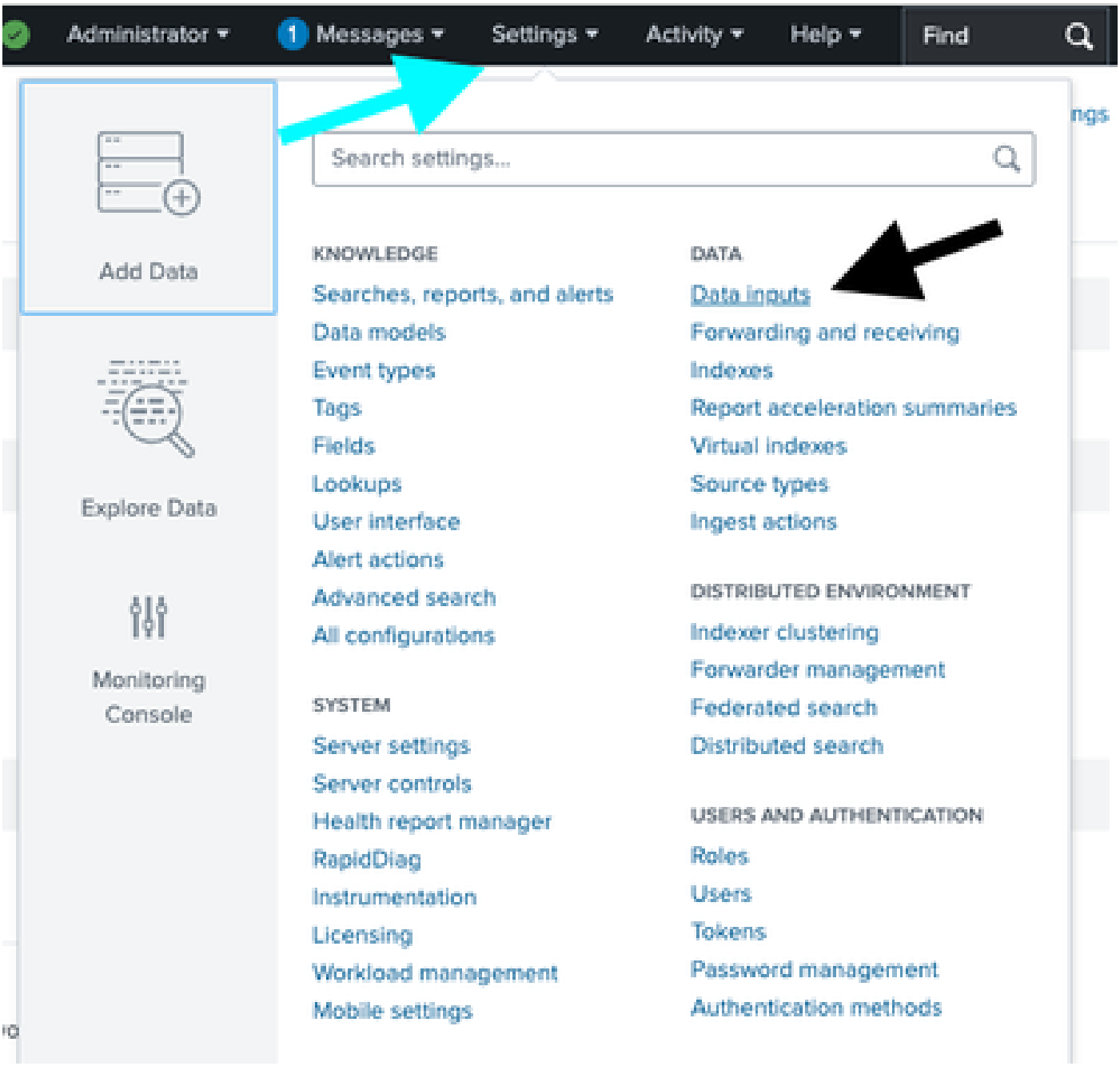
提示：系统日志的默认UDP端口是514



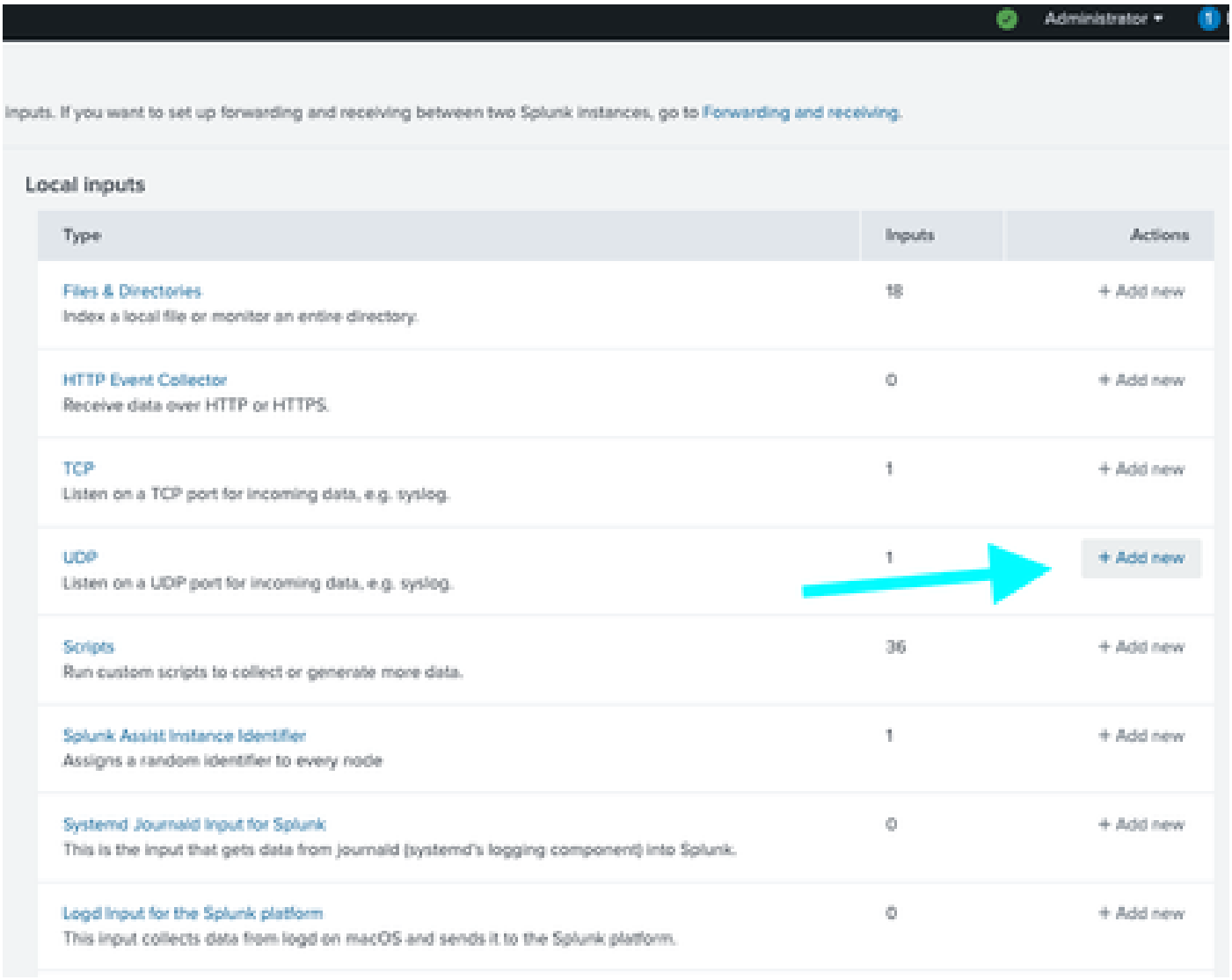
2.配置Splunk以通过UDP端口接收SNA系统日志

在Secure Network Analytics Manager Web UI上应用更改后，您必须在Splunk中配置数据输入。

步骤 1：登录Splunk并导航到设置>添加数据>数据输入。

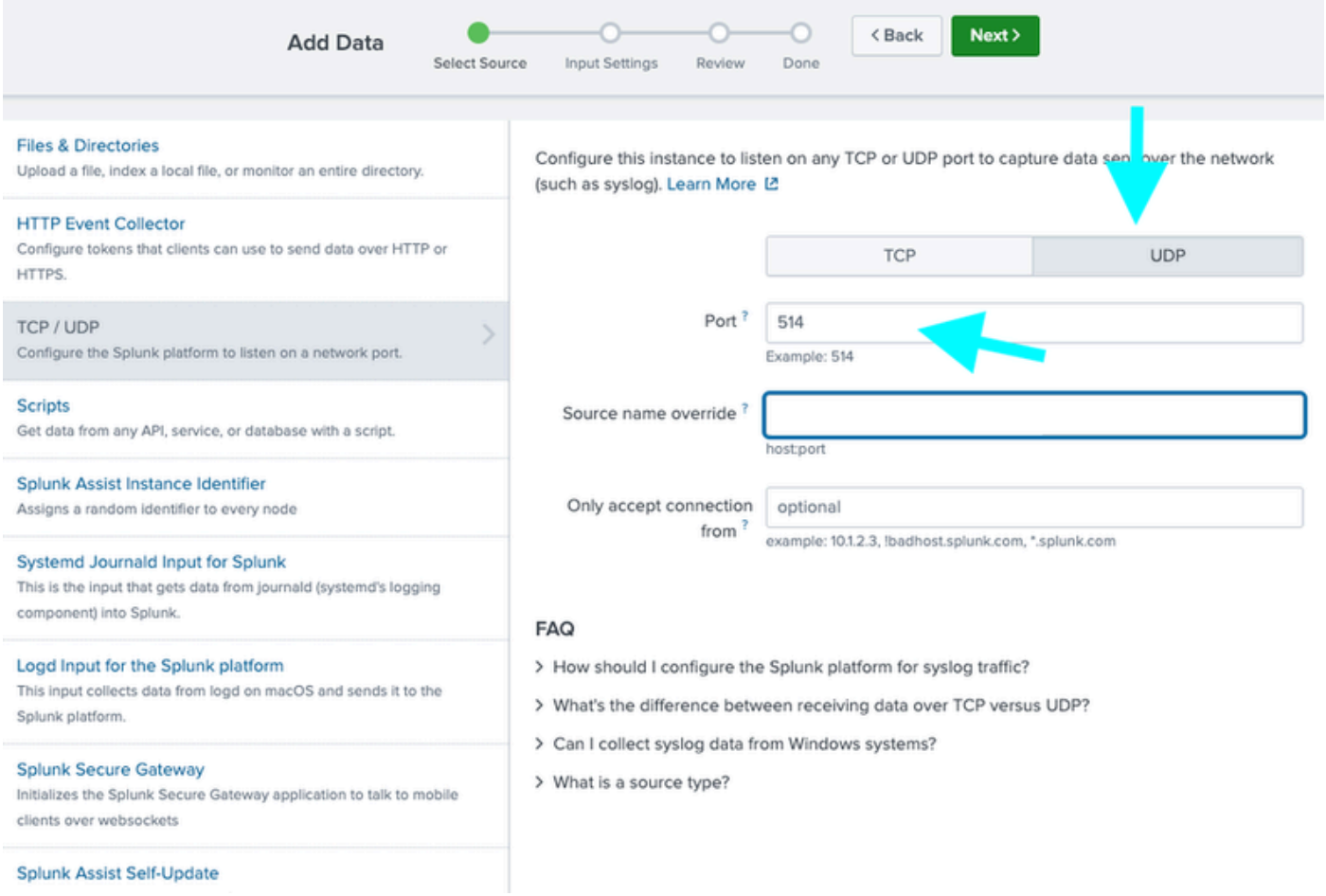


步骤 2：找到UDP行，然后选择+Add new。



步骤 3：在新页面上，选择UDP，在Port字段中输入接收端口（例如514）。
步骤 4：在Source name override字段中，输入 desired name of source.

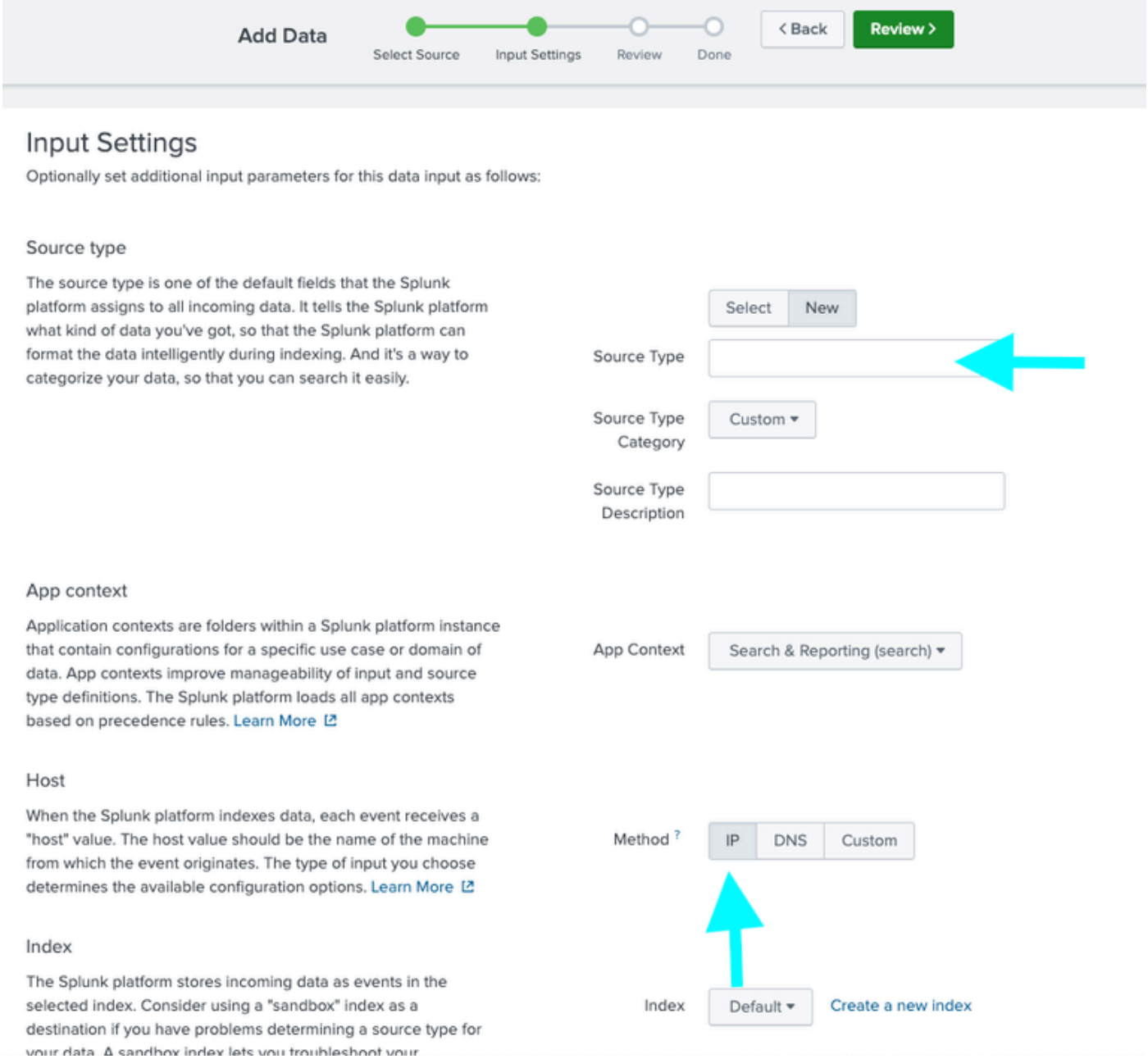
步骤 5：完成后，单击窗口顶部的绿色Next >按钮。



步骤 6：在下一页上，切换到New选项，找到Source Type字段并输入 desired source .

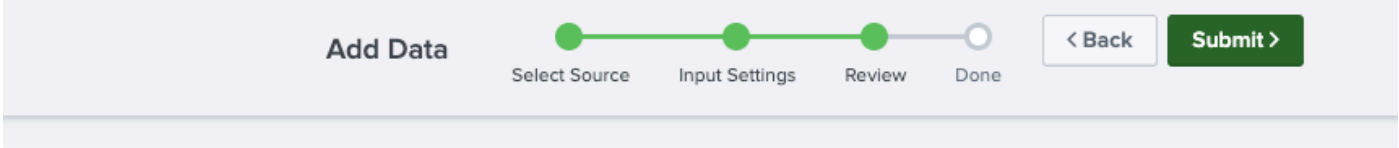
步骤 7：为Method选择IP。

步骤 8::单击屏幕顶部的绿色Review > 按钮。



步骤 9：在下一个窗口中，检查您的设置并根据需要进行编辑。

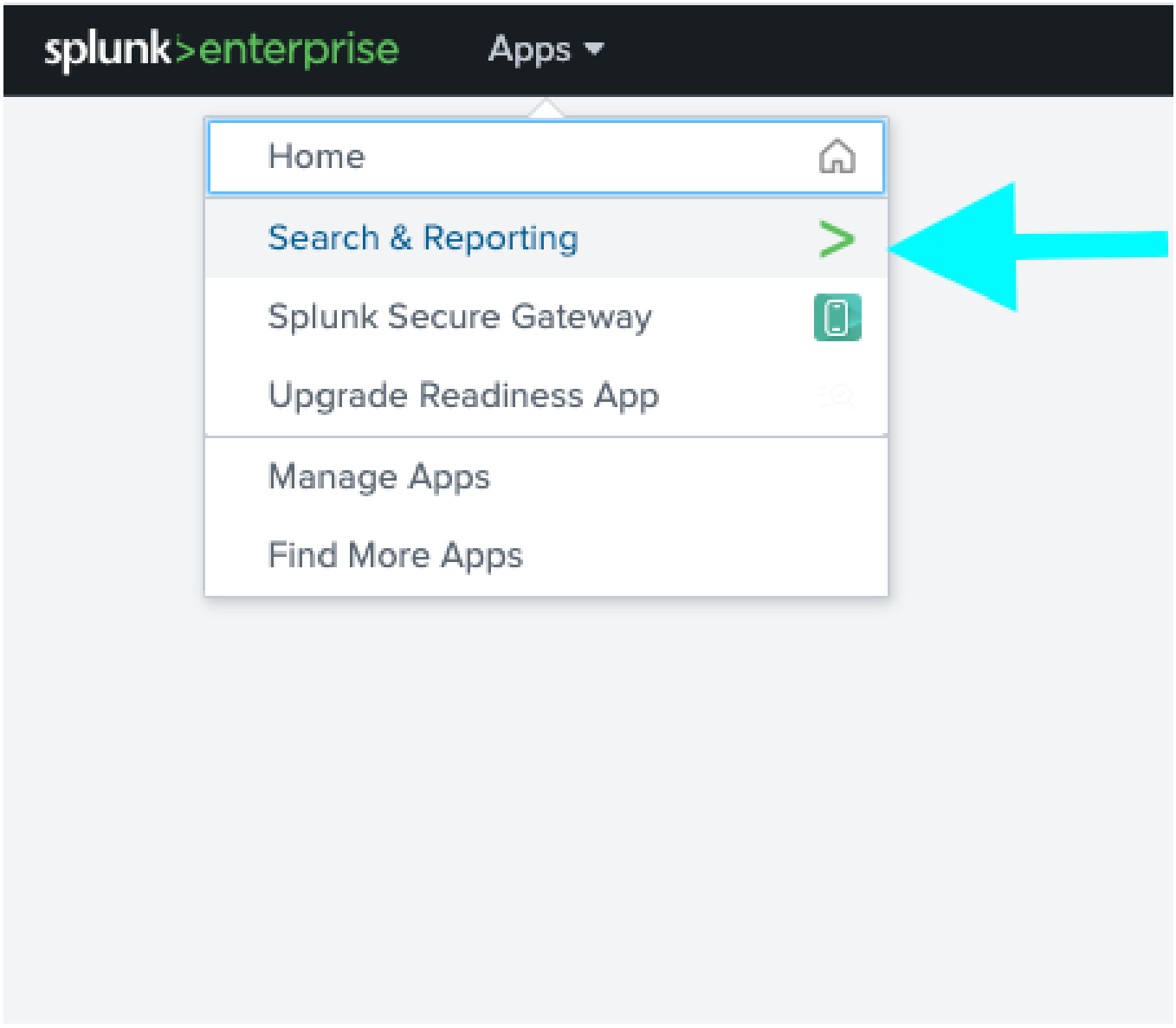
步骤 10：验证后，单击窗口顶部的Submit>按钮。



Review

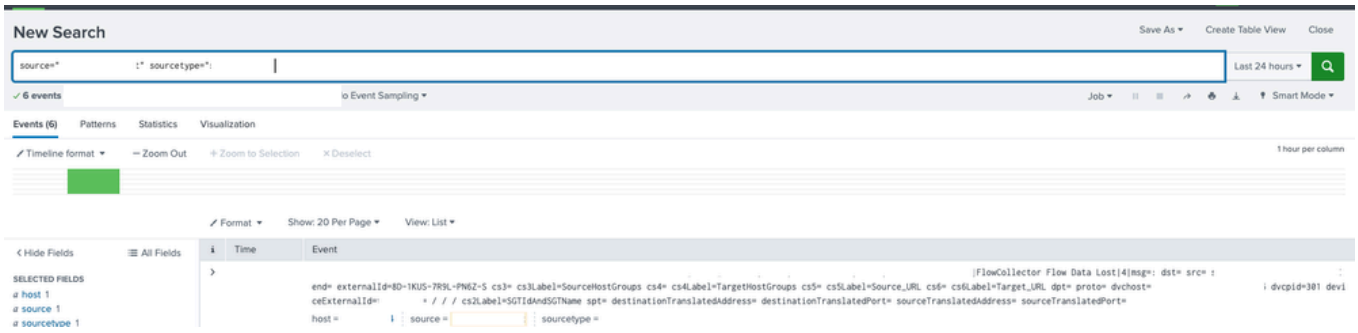
Input Type ..... UDP Port
Port Number 514
Source name override .....
Restrict to Host ..... N/A
Source Type .....
App Context ..... search
Host ..... (IP address of the remote server)
Index ..... default

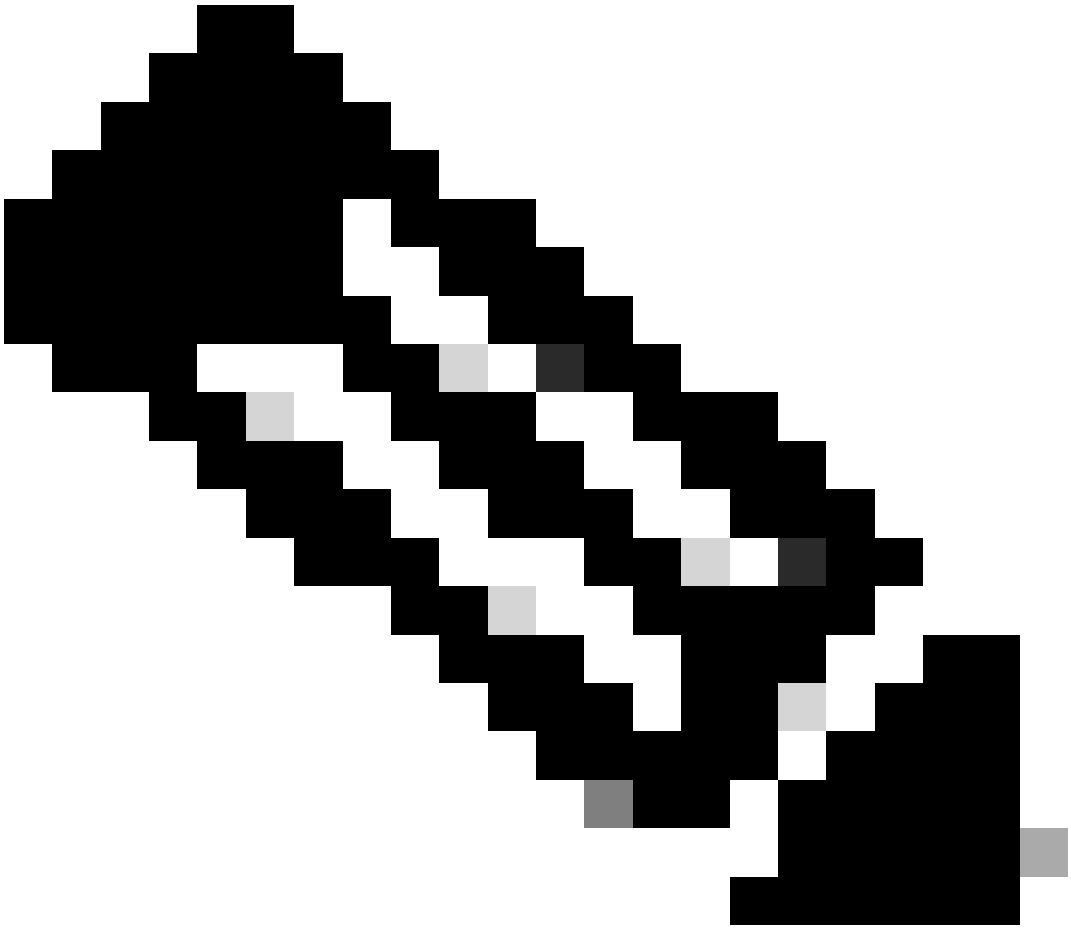
步骤 11：在Web UI中导航到应用>搜索与报告。



步骤 12：在“搜索”(Search)页面上source="As_configured" sourcetype="As_configured"，使用过滤器查找已接收的

日志。



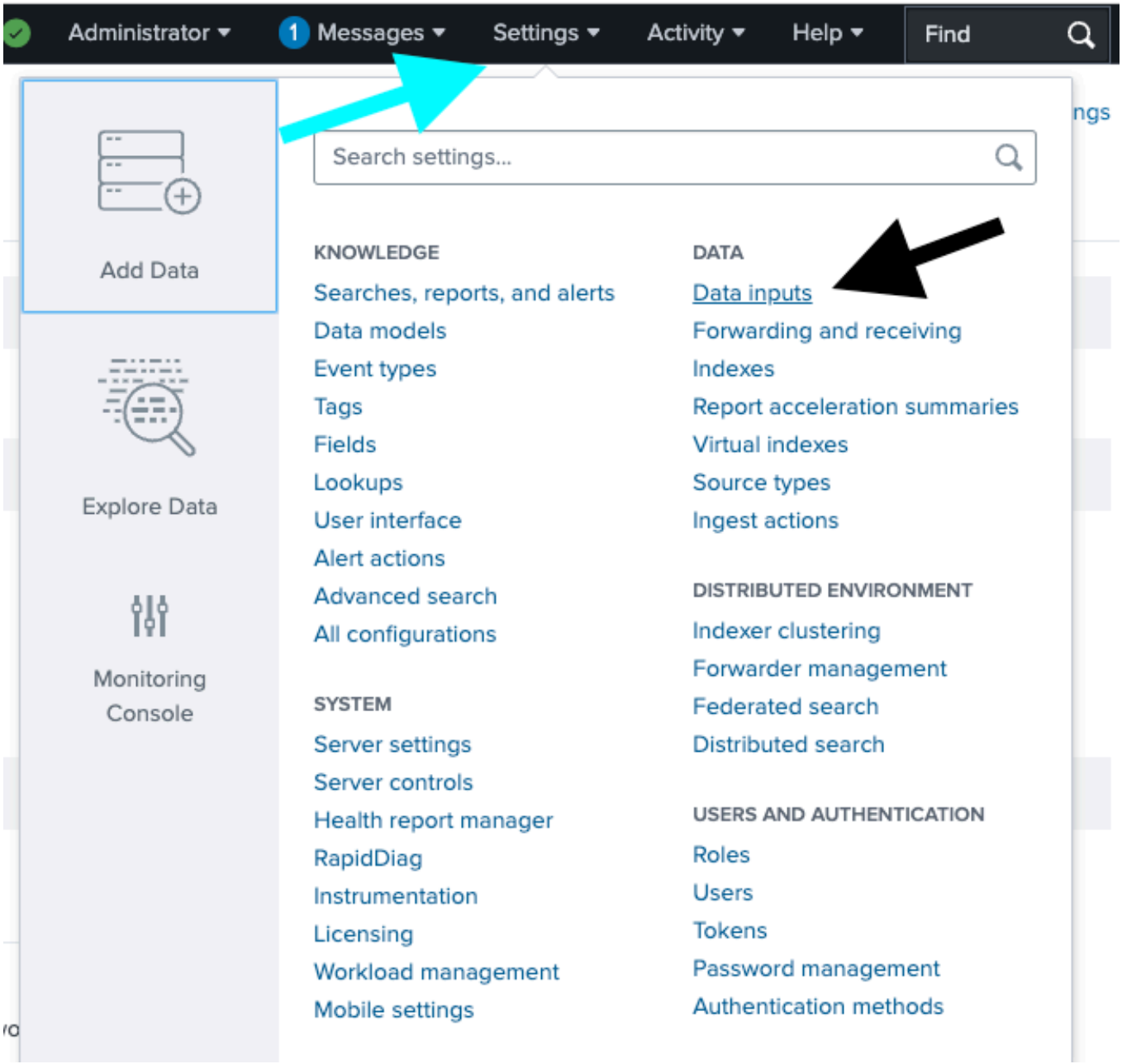


注意：有关源，请参阅步骤4
有关source_type，请参阅步骤6

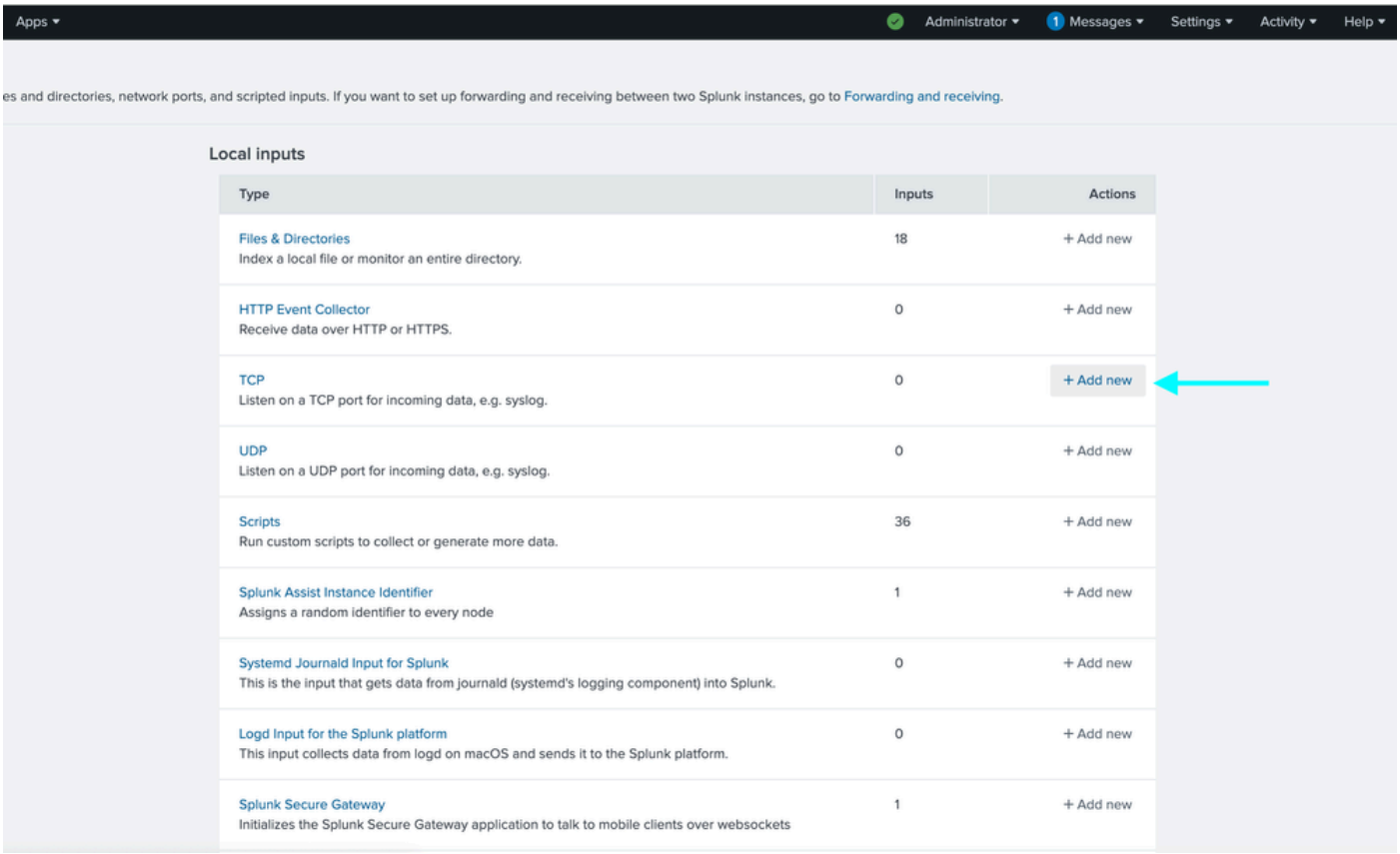
在SNA上通过TCP端口6514或自定义端口配置系统日志

1.配置Splunk以通过TCP端口接收SNA审核日志

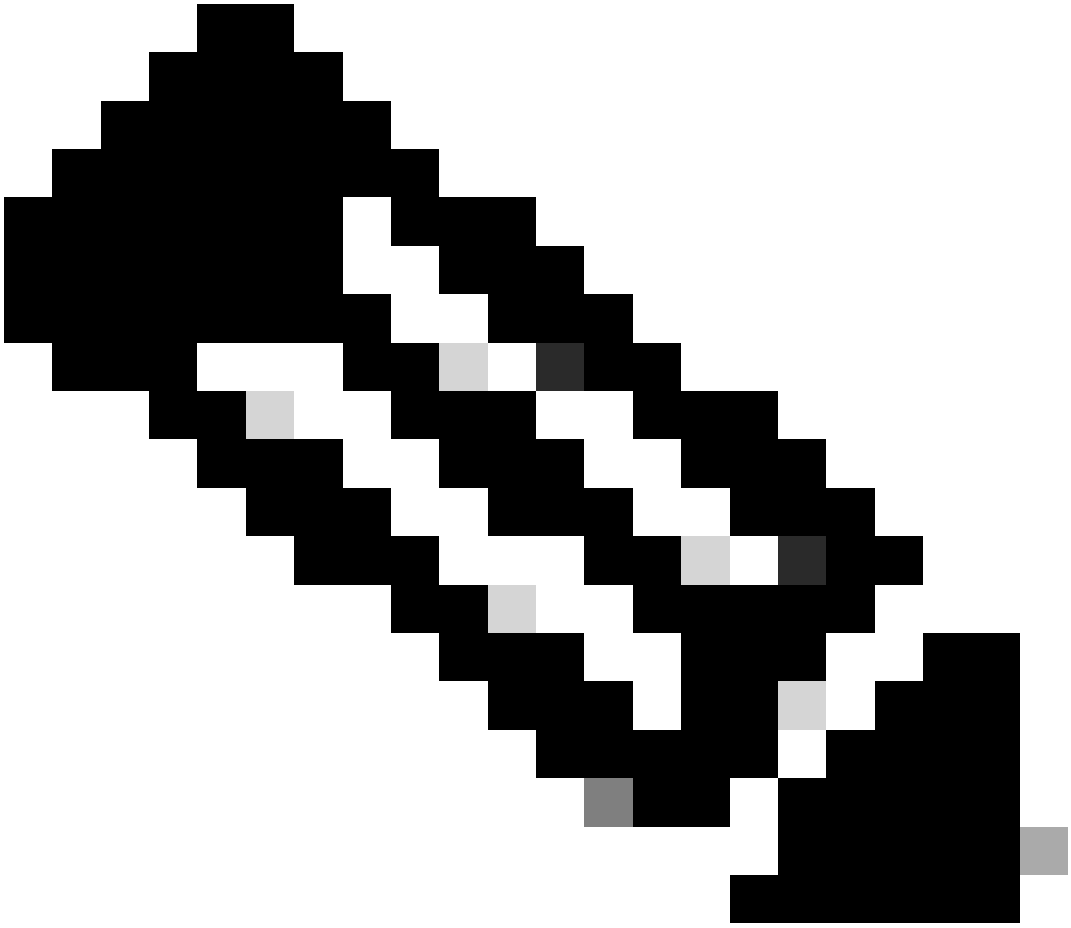
步骤 1：在Splunk UI中，导航到设置>添加数据>数据数据输入。



步骤 2：找到TCP行，然后选择+ Add new。

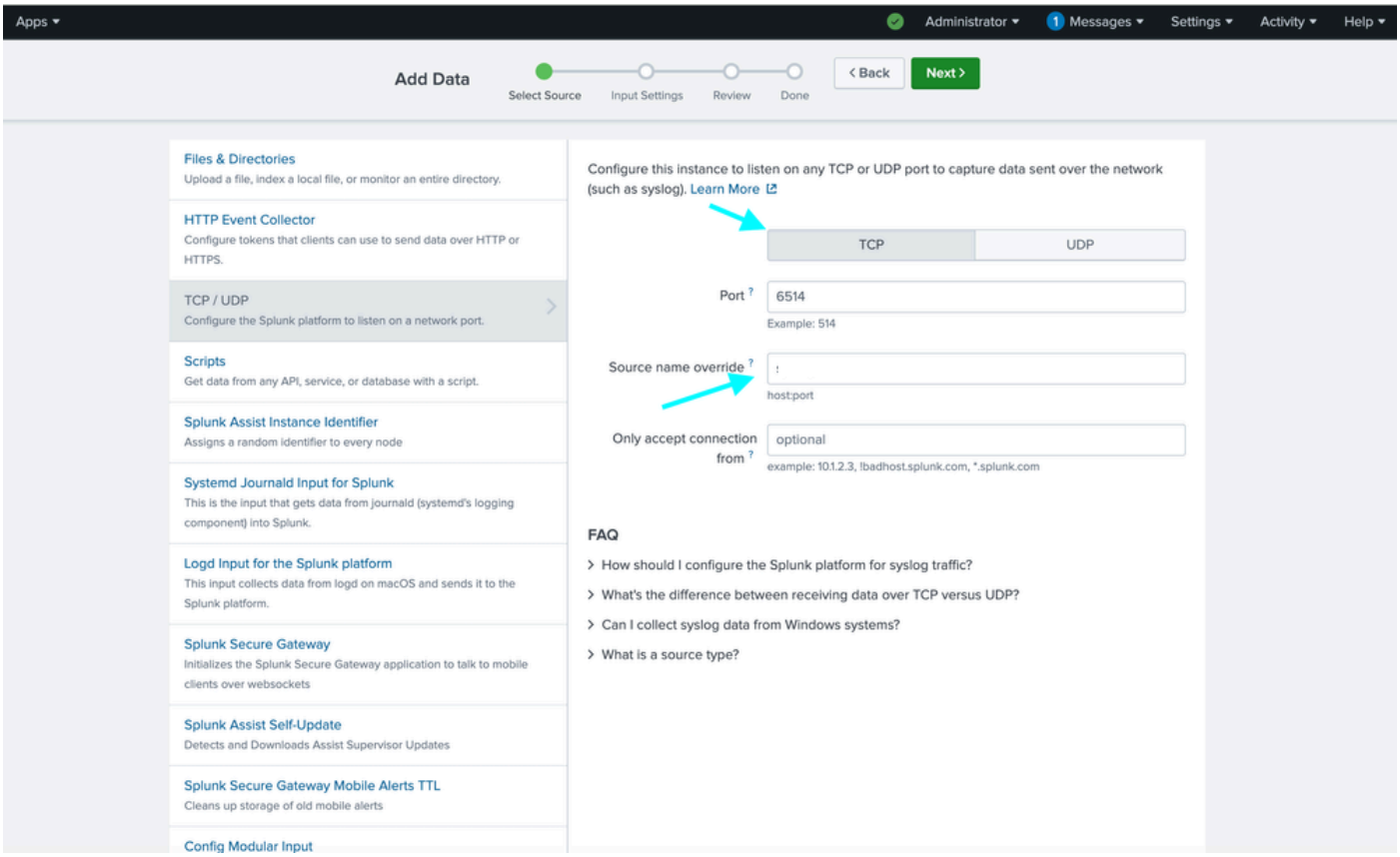


步骤 3：在新窗口中选择TCP，在示例图像端口6514中输入所需的接收端口，并在Source name override字段中输入“desired name”。



注意：TCP 6514是通过TLS的系统日志的默认端口

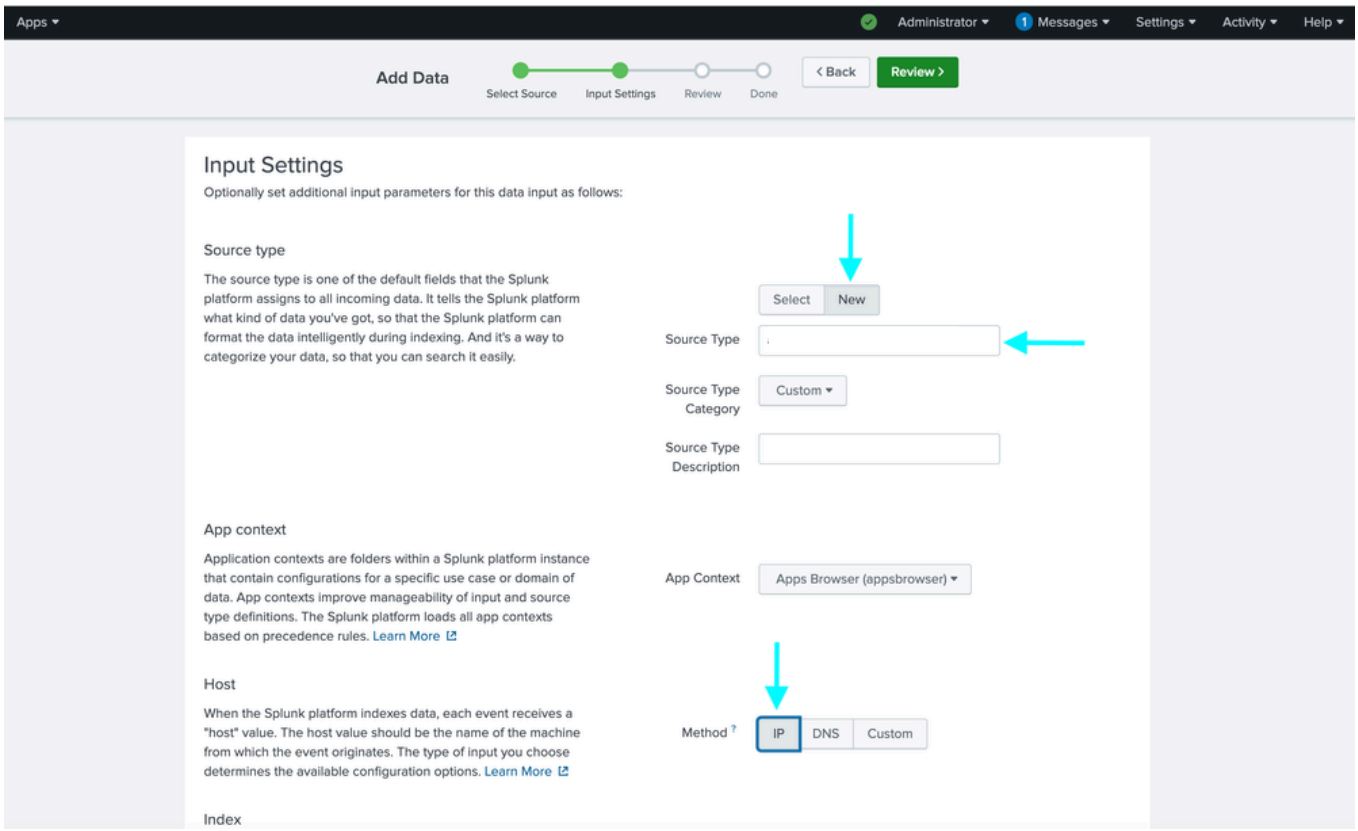
步骤 4：完成后，单击窗口顶部的绿色Next >按钮。



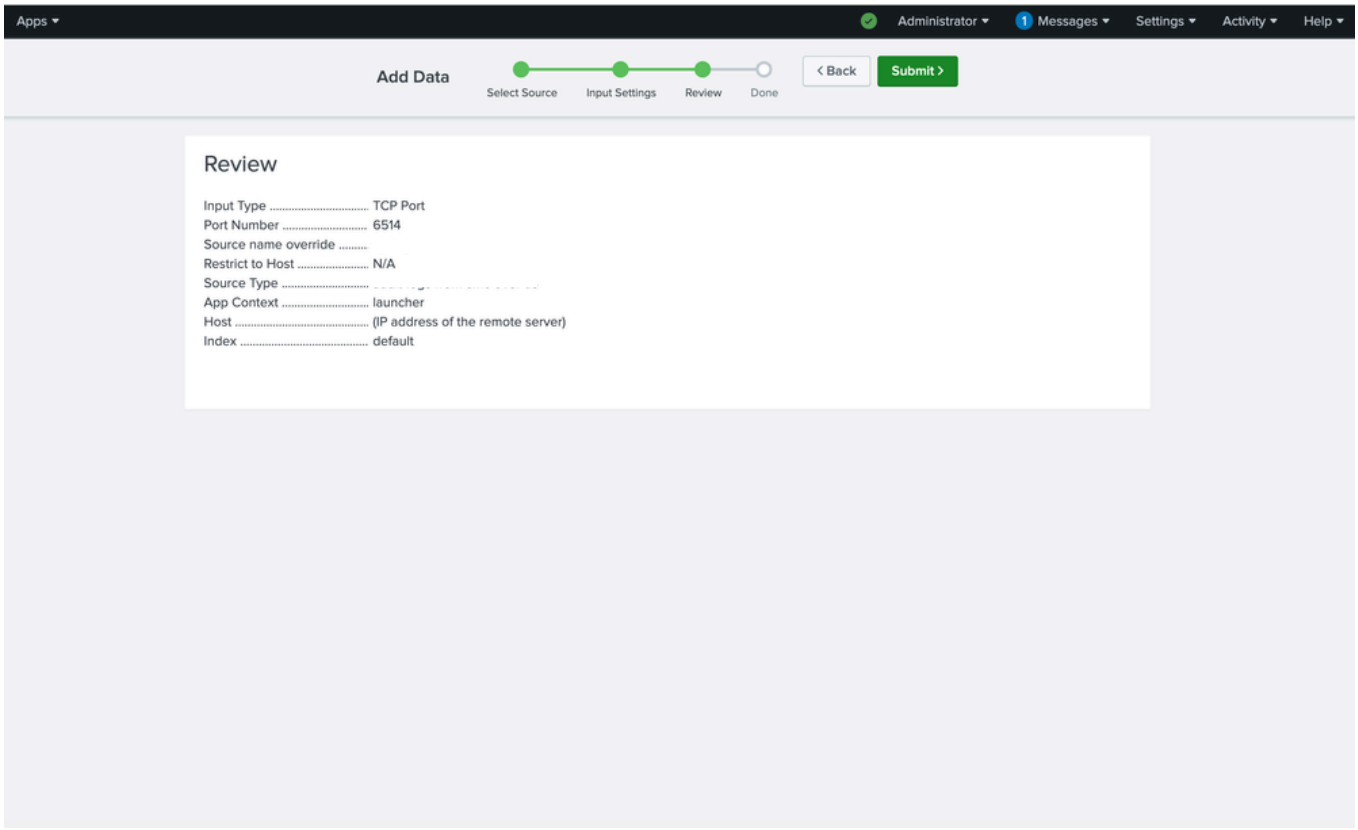
步骤 5：在新窗口中，在源类型部分中选择新建，在源类型字段中输入所需的名称。

步骤 6：在主机部分中选择方法的IP。

步骤 7：完成后，选择窗口顶部的绿色Review >按钮。



步骤 8::在下一个窗口中，检查您的设置并根据需要进行编辑。验证后，单击窗口顶部的Submit>按钮。



2.生成Splunk的证书

步骤 1：使用安装了openssl的计算机，运行sudo openssl req -x509 -newkey rsa:4096 -keyout server_key.pem -out server_cert.pem -sha256 -days 3650 -subj /CN=10.106.127.4命令，用Splunk设备的IP替换示例IP 10.106.127.4。系统会两次提示您输入用户定义的密码短语。在示例中，这些命令是从Splunk计算机的命令行运行的。

```
user@examplehost: sudo openssl req -x509 -newkey rsa:4096 -keyout server_key.pem -out server_cert.pem -
..+...+..+.+...+..+...........+.............+.+.....+.+......+..+.+..........+...++++++++++++++++++
....+.......+..+...+...+.+......+...+.........+...........+.....+....+..+...+....+...+...+.........+..
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
user@examplehost:
```

命令完成后，将生成两个文件。server_cert.pem和server_key.pem文件。

```
user@examplehost: ll server*
-rw-r--r-- 1 root root 1814 Dec 20 19:02 server_cert.pem
-rw------- 1 root root 3414 Dec 20 19:02 server_key.pem
user@examplehost:
```

步骤 2：切换到根用户。

```
user@examplehost:~$ sudo su
[sudo] password for examplehost:
```

步骤 3：将新生成的证书复制到/opt/splunk/etc/auth/。

```
user@examplehost:~# cat /home/examplehost/server_cert.pem > /opt/splunk/etc/auth/splunkweb.cer
```

第4步：使用私钥附加spunkweb.cet文件。

```
user@examplehost:~# cat /home/examplehost/server_key.pem >> /opt/splunk/etc/auth/splunkweb.cer
```

第5步：更改splunk证书的所有权。

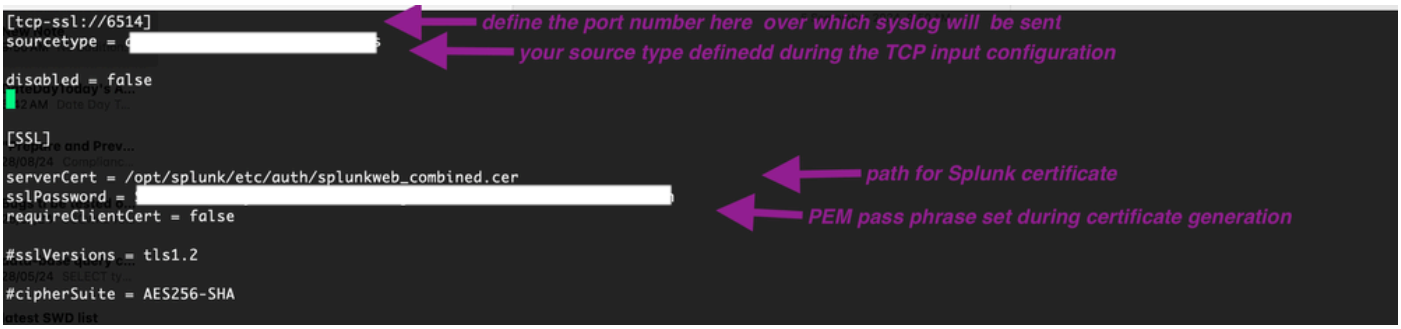
```
user@examplehost:~# chown 10777:10777/opt/splunk/etc/auth/splunkweb.cer
```

第6步：更改splunk证书的权限。

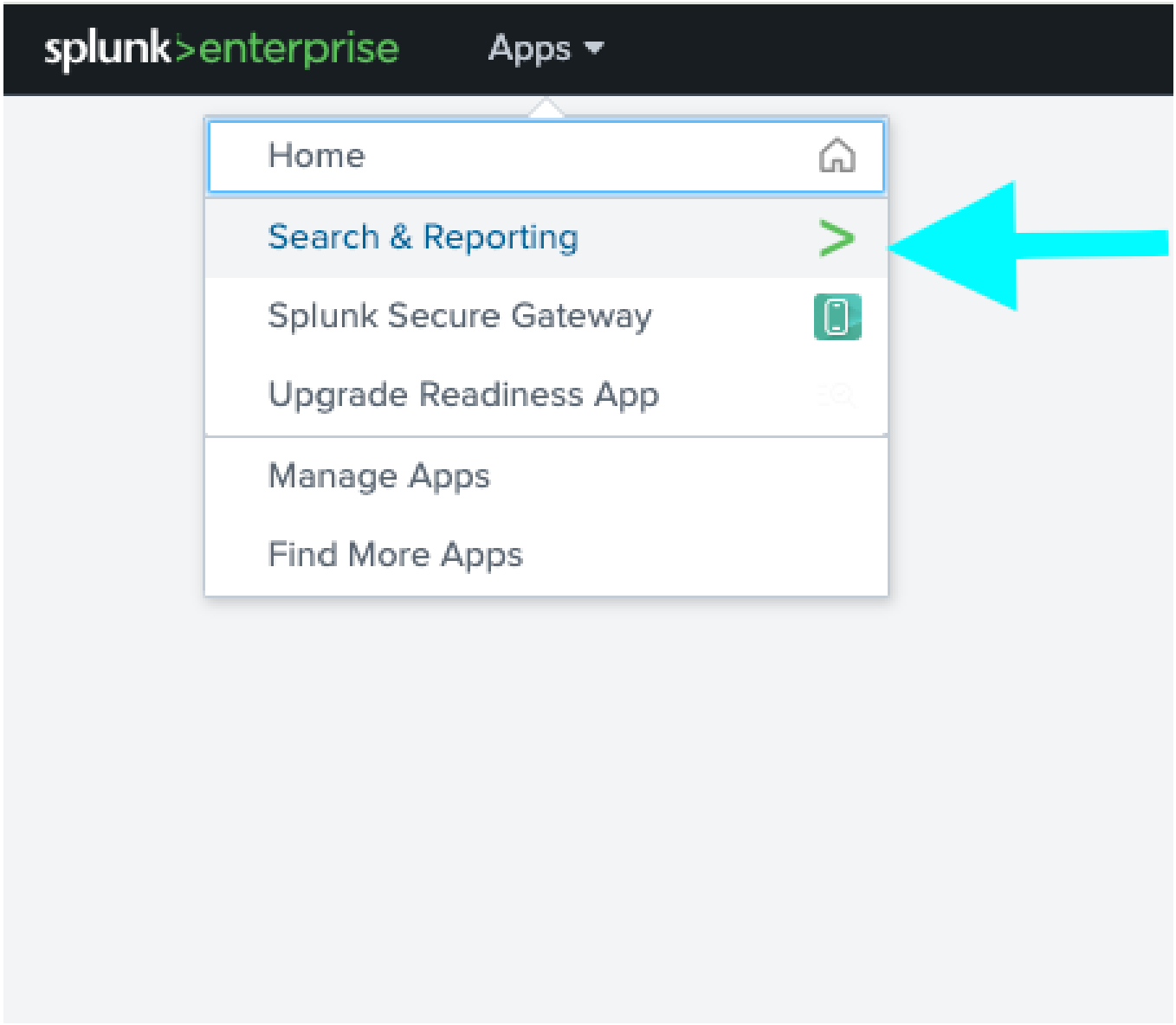
```
user@examplehost:~# chmod 600/opt/splunk/etc/auth/splunkweb.cer
```

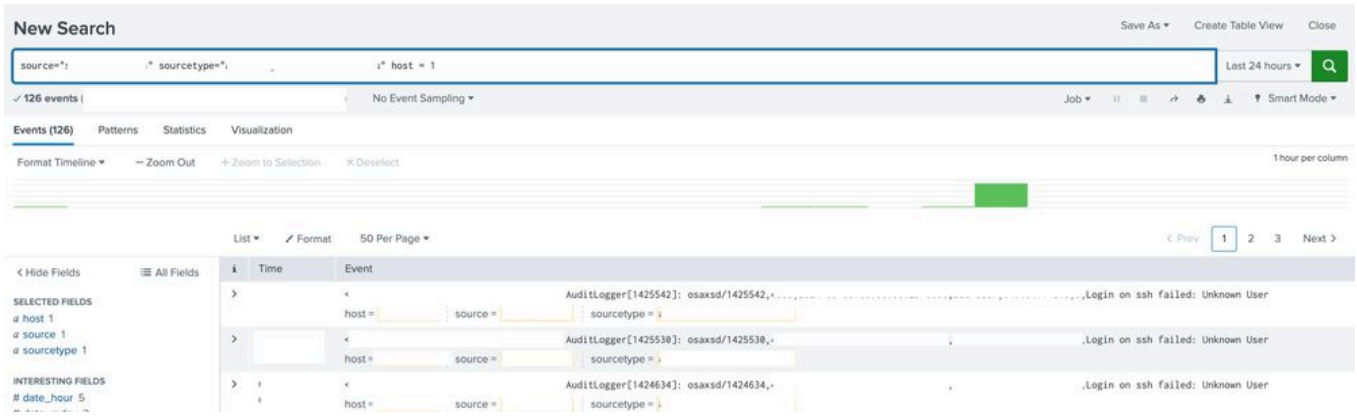
第7步：创建新的input.conf文件。

```
user@examplehost:~# vim /opt/splunk/etc/system/local/inputs
```



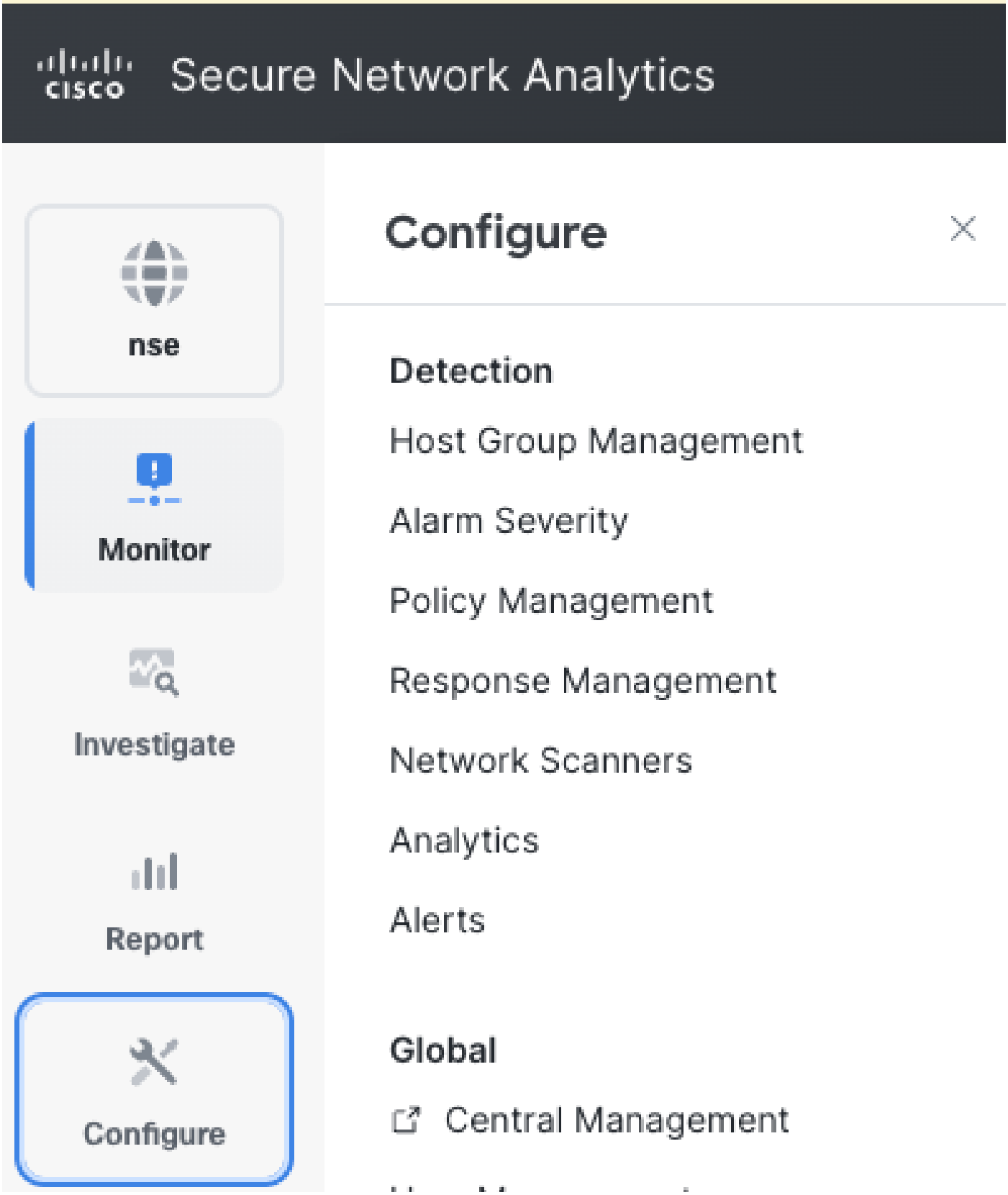
步骤 8::使用搜索验证系统日志。



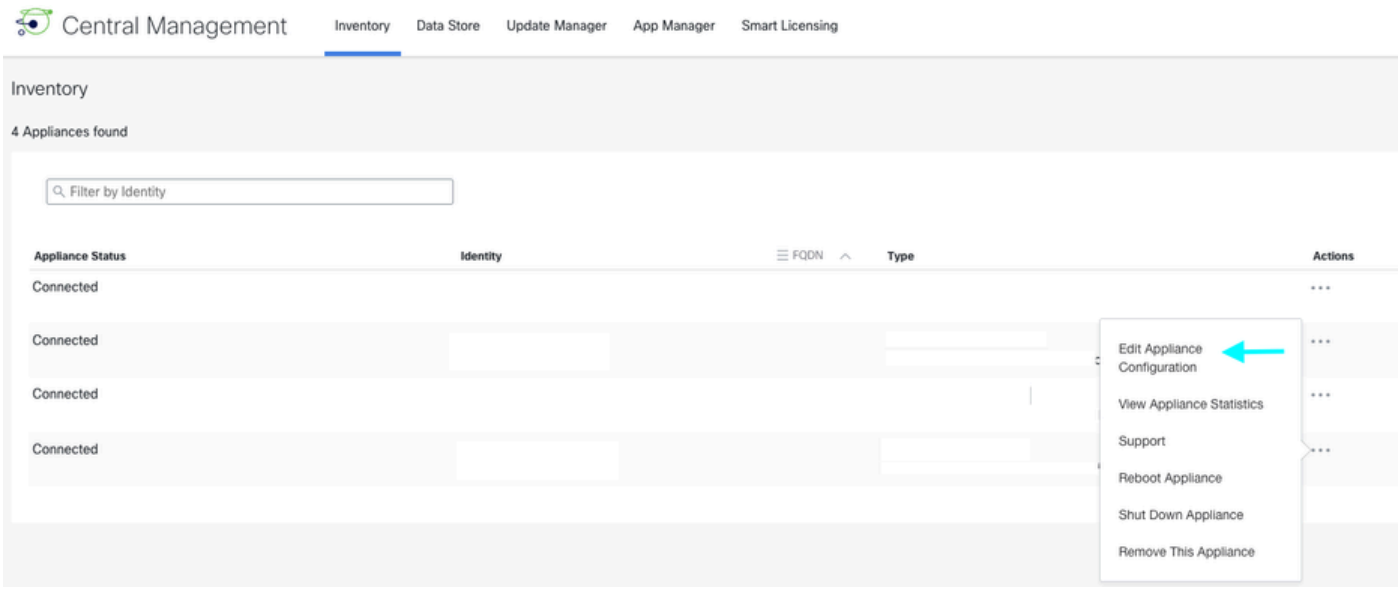


3.在SNA上配置审计日志目标

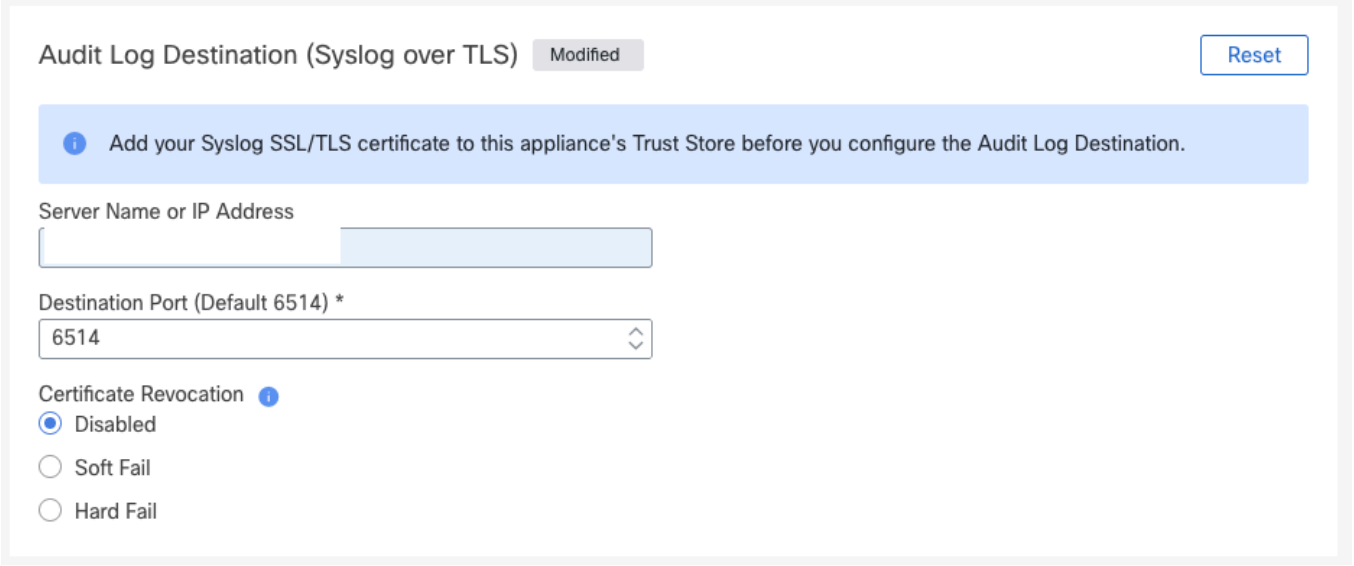
步骤 1：登录到SMC UI，导航至配置 >中央管理。



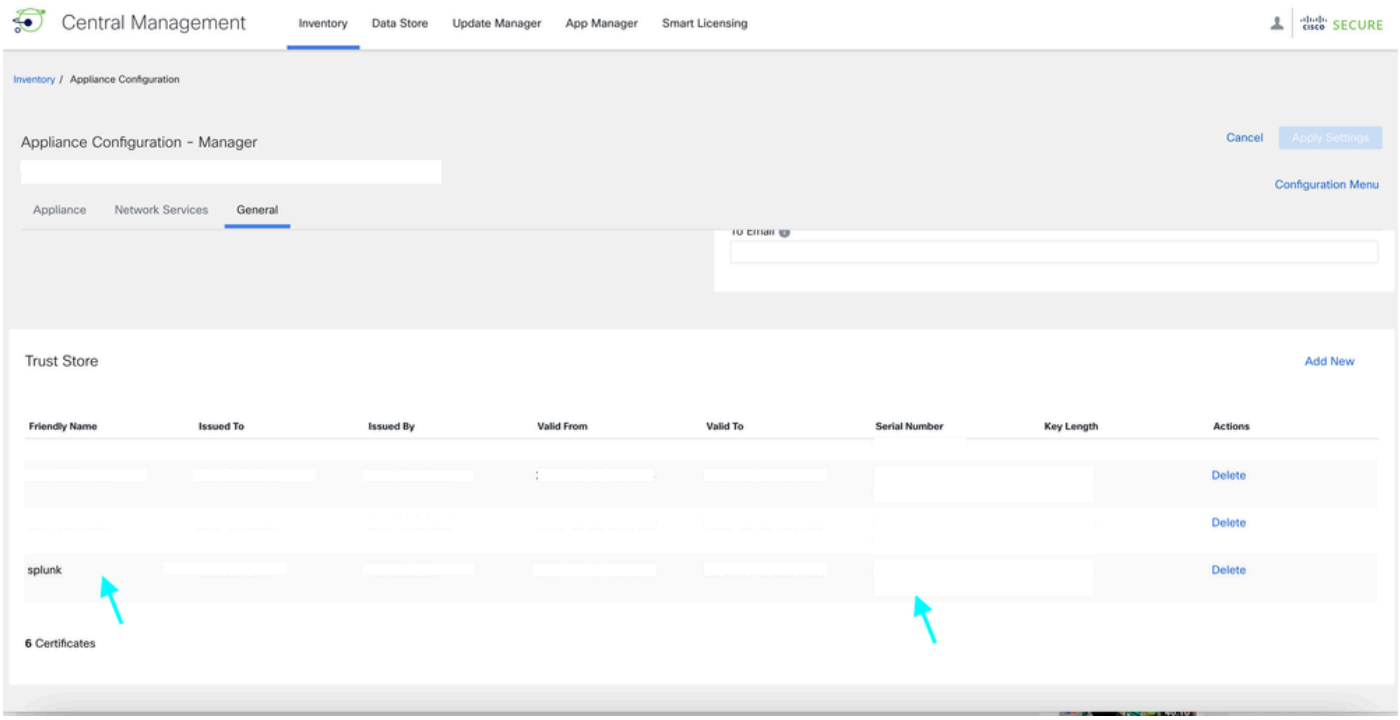
步骤 2：单击所需SNA设备的省略号图标，选择编辑设备配置。



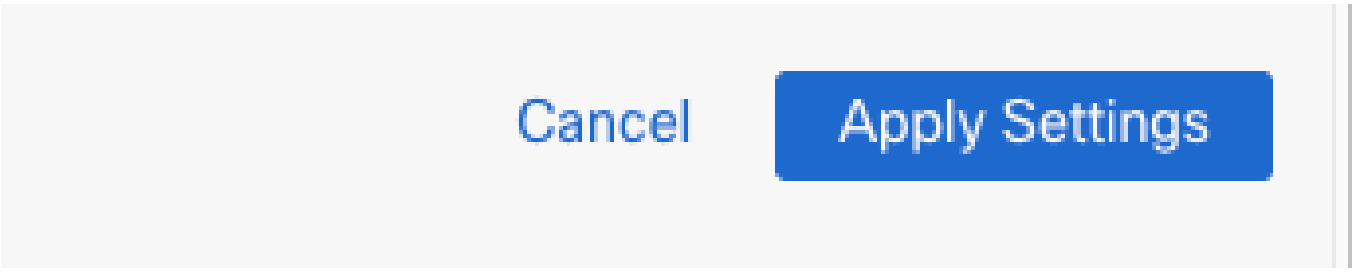
步骤 3：导航到网络服务选项卡并输入审核日志目标（基于TLS的系统日志）详细信息。



步骤 4：导航到General选项卡，向下滚动到底部单击Add new以上传之前创建的Splunk证书，该证书名为server_cert.pem。

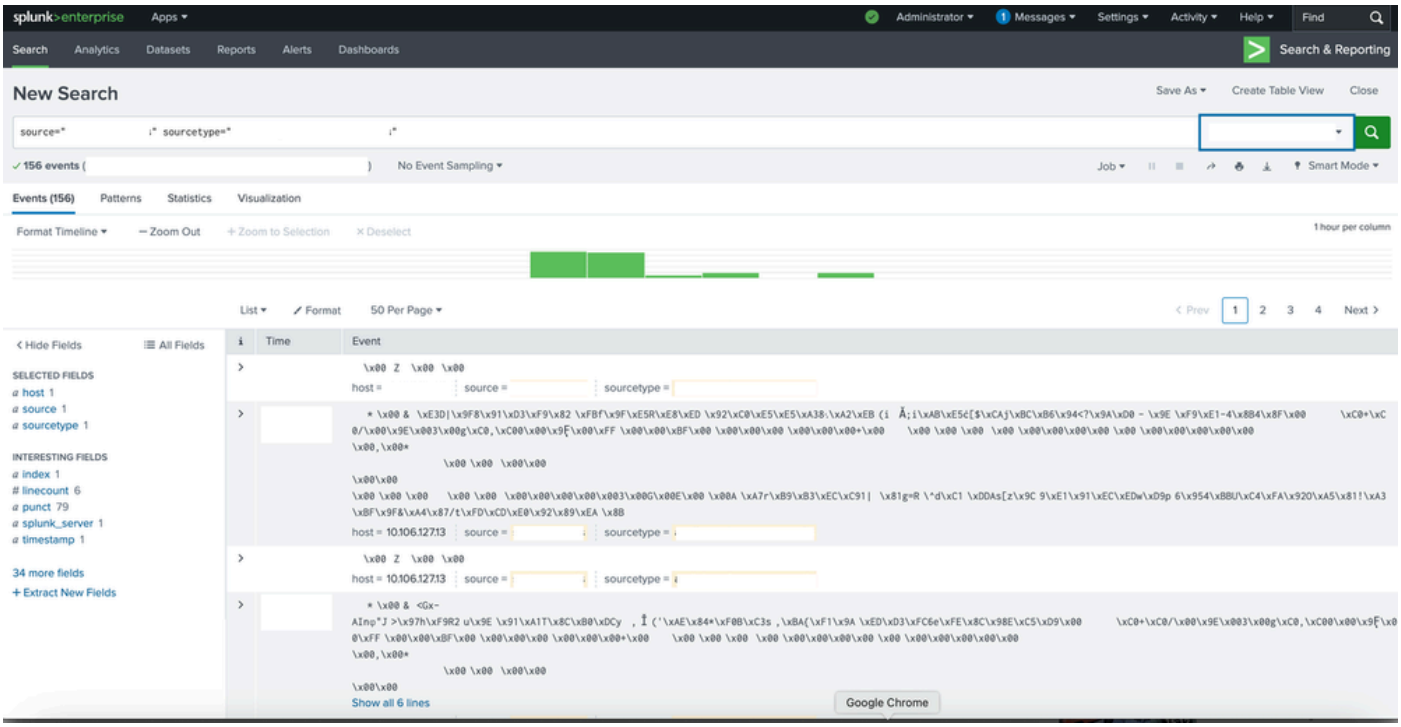


步骤 5：单击Apply settings。



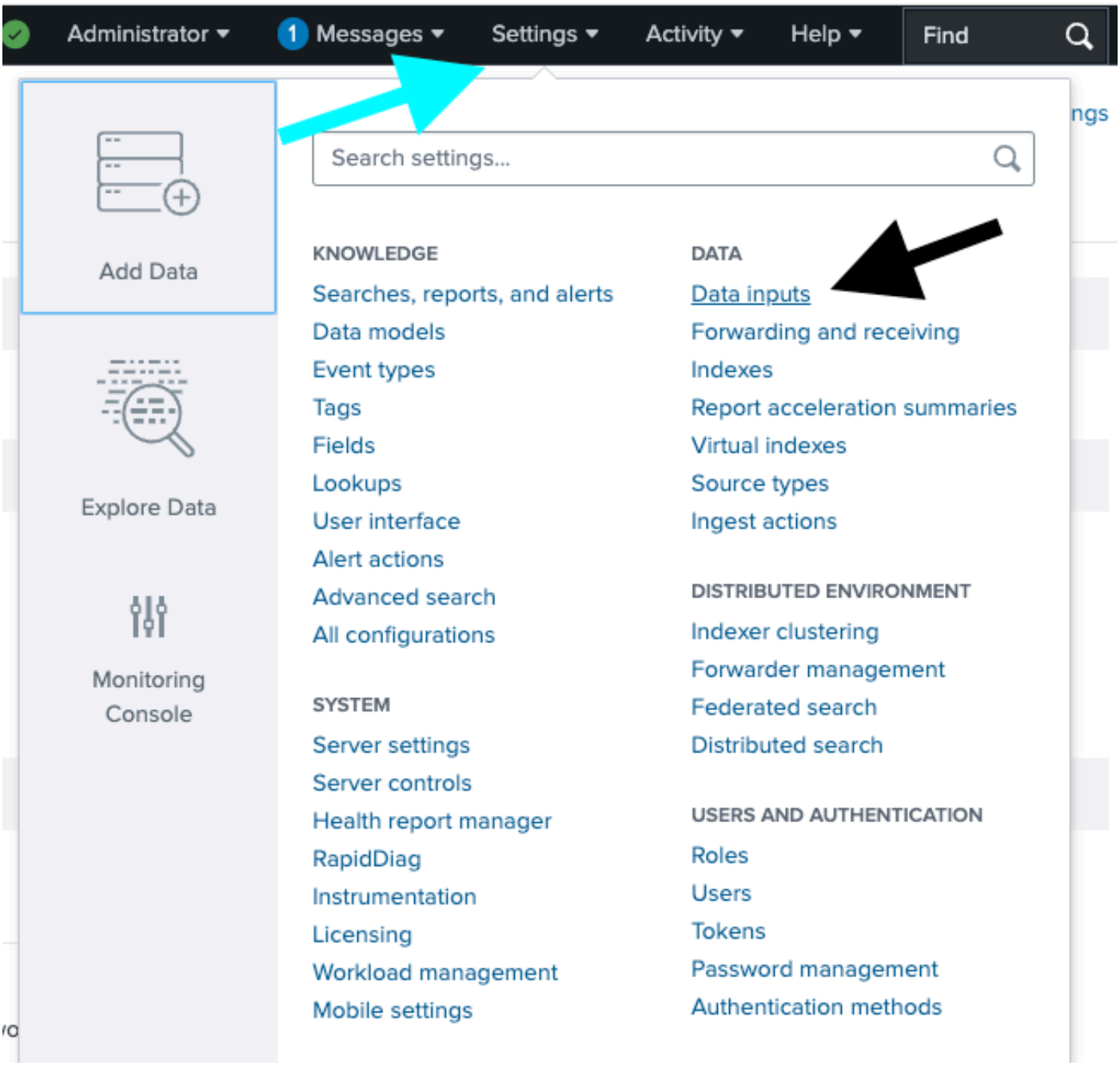
故障排除

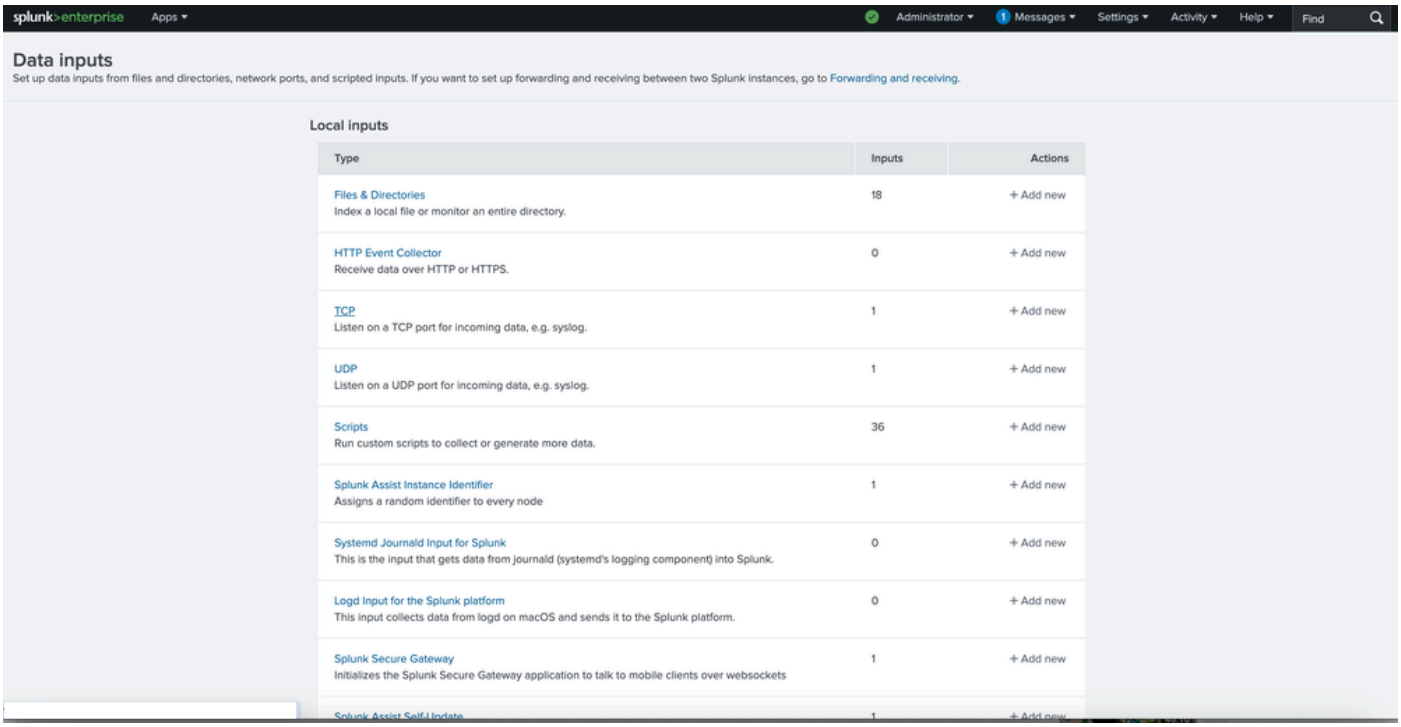
搜索时可能会出现完全的胡言乱语。

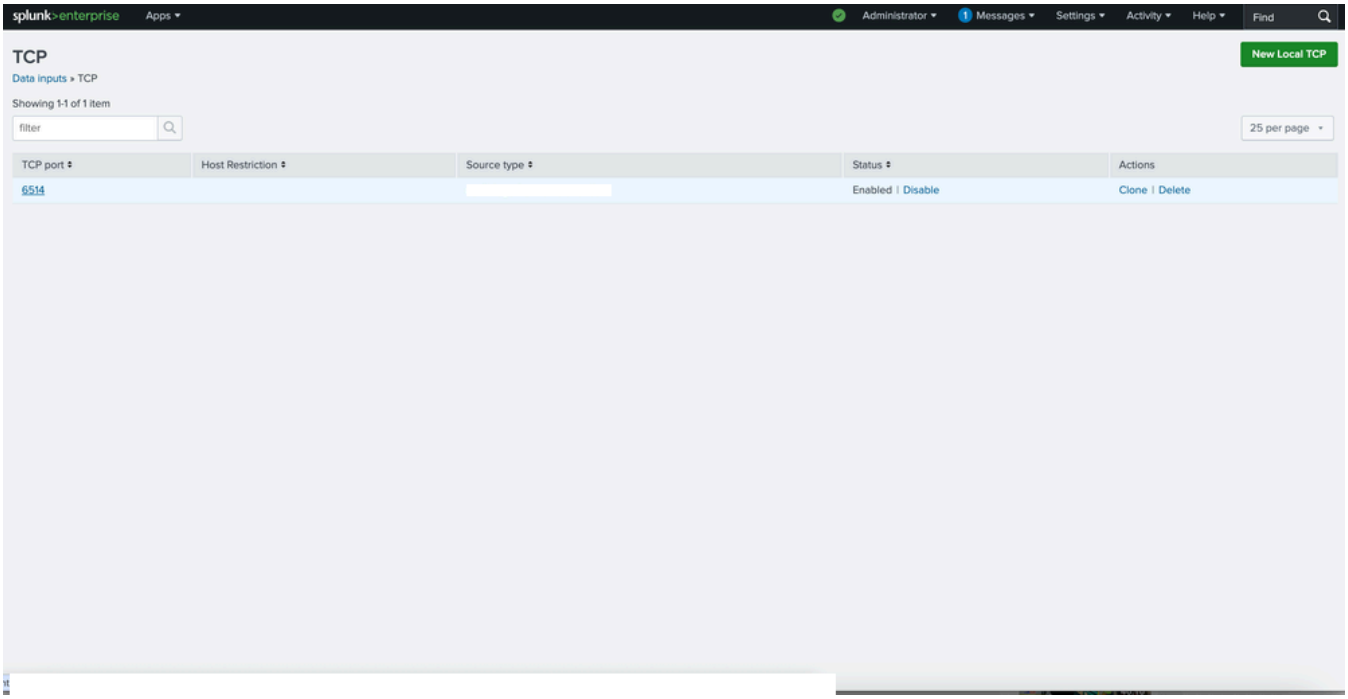


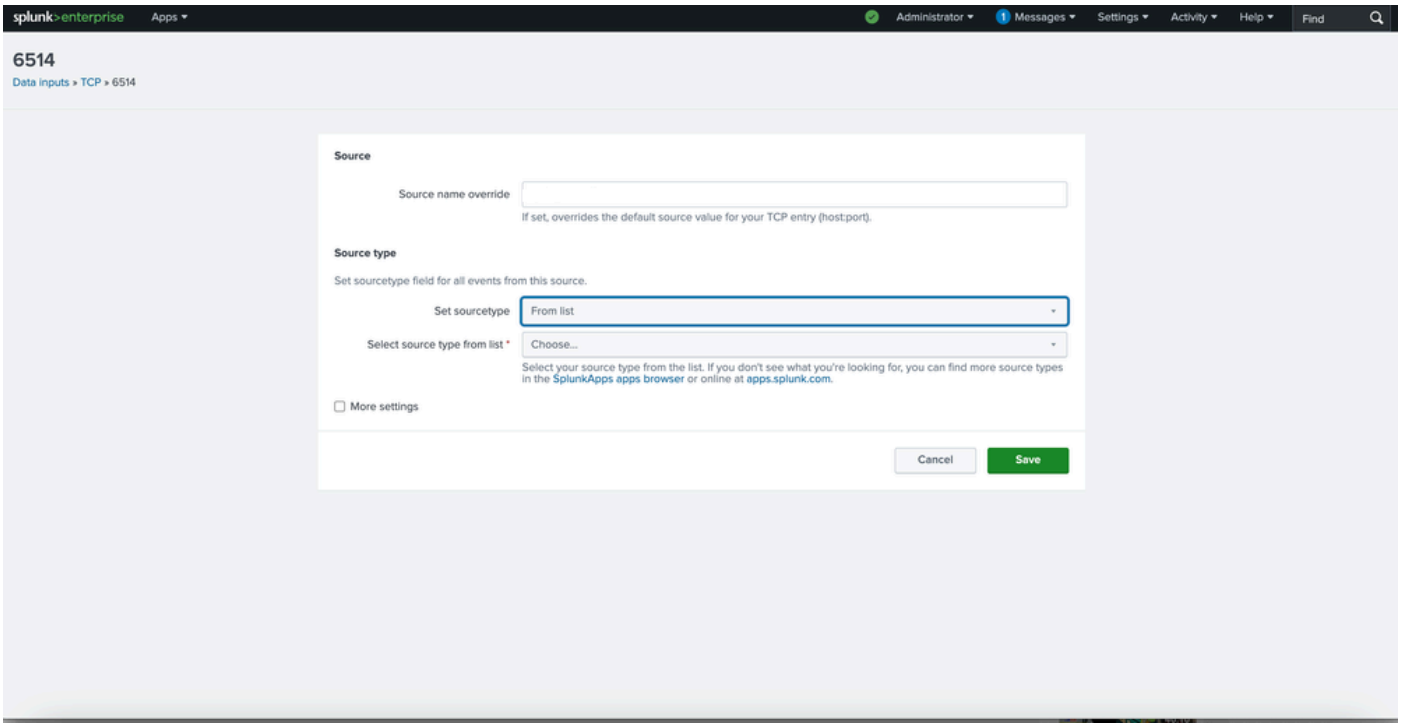
解决方案：

将输入映射到正确的源类型。


Administrator
1 Messages
Settings
Activity
Help
Find
Add Data
Explore Data
Monitoring Console
Search settings...
KNOWLEDGE
Searches, reports, and alerts
Data models
Event types
Tags
Fields
Lookups
User interface
Alert actions
Advanced search
All configurations
SYSTEM
Server settings
Server controls
Health report manager
RapidDiag
Instrumentation
Licensing
Workload management
Mobile settings
DATA
Data inputs
Forwarding and receiving
Indexes
Report acceleration summaries
Virtual indexes
Source types
Ingest actions
DISTRIBUTED ENVIRONMENT
Indexer clustering
Forwarder management
Federated search
Distributed search
USERS AND AUTHENTICATION
Roles
Users
Tokens
Password management
Authentication methods


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Data inputs
Set up data inputs from files and directories, network ports, and scripted inputs. If you want to set up forwarding and receiving between two Splunk instances, go to Forwarding and receiving.
Local inputs
Type
Inputs
Actions
Files & Directories
Index a local file or monitor an entire directory.
18
+ Add new
HTTP Event Collector
Receive data over HTTP or HTTPS.
0
+ Add new
TCP
Listen on a TCP port for incoming data, e.g. syslog.
1
+ Add new
UDP
Listen on a UDP port for incoming data, e.g. syslog.
1
+ Add new
Scripts
Run custom scripts to collect or generate more data.
36
+ Add new
Splunk Assist Instance Identifier
Assigns a random identifier to every node
1
+ Add new
Systemd Journald Input for Splunk
This is the input that gets data from journald (systemd's logging component) into Splunk.
0
+ Add new
Logd Input for the Splunk platform
This input collects data from logd on macOS and sends it to the Splunk platform.
0
+ Add new
Splunk Secure Gateway
Initializes the Splunk Secure Gateway application to talk to mobile clients over websockets
1
+ Add new
Splunk Assist Self-Update
1
+ Add new


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
TCP
New Local TCP
Data inputs › TCP
Showing 1-1 of 1 item
filter
25 per page
TCP port
Host Restriction
Source type
Status
Actions
6514
Enabled | Disable
Clone | Delete


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
6514
Data inputs » TCP » 6514
Source
Source name override
If set, overrides the default source value for your TCP entry (host:port).
Source type
Set sourcetype field for all events from this source.
Set sourcetype
From list
Select source type from list *
Choose...
Select your source type from the list. If you don't see what you're looking for, you can find more source types in the SplunkApps apps browser or online at apps.splunk.com.
More settings
Cancel
Save

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）。