

配置响应管理以将系统日志事件发送到Splunk

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[在SNA over UDP 514或自定义端口上配置系统日志](#)

[1.SNA响应管理](#)

[2.配置Splunk以通过UDP端口接收SNA系统日志](#)

[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](#)

[2.生成Splunk的证书](#)

[3.在SNA上配置审计日志目标](#)

[故障排除](#)

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：

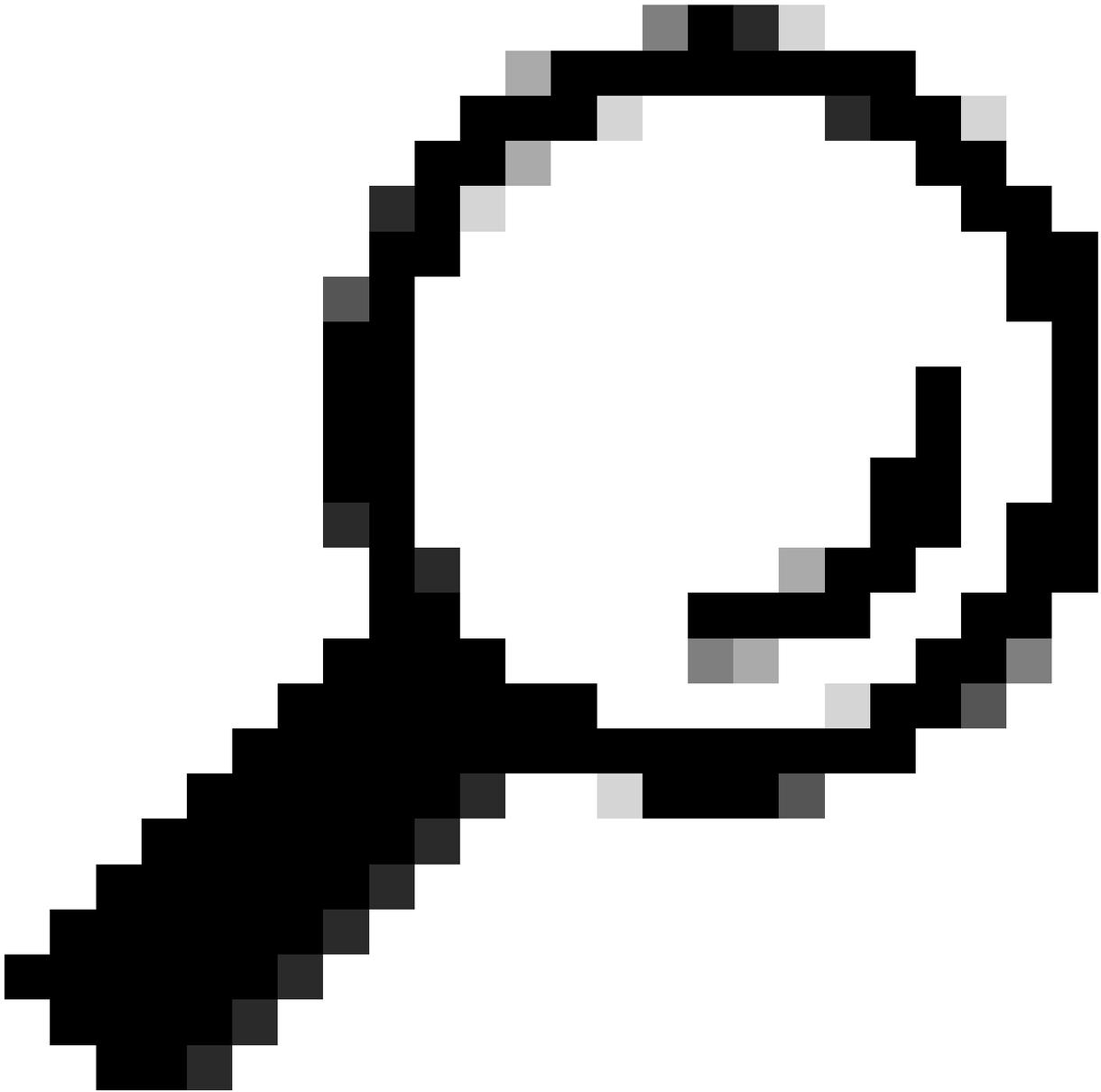
- 安全网络分析响应管理。
- Splunk系统日志

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



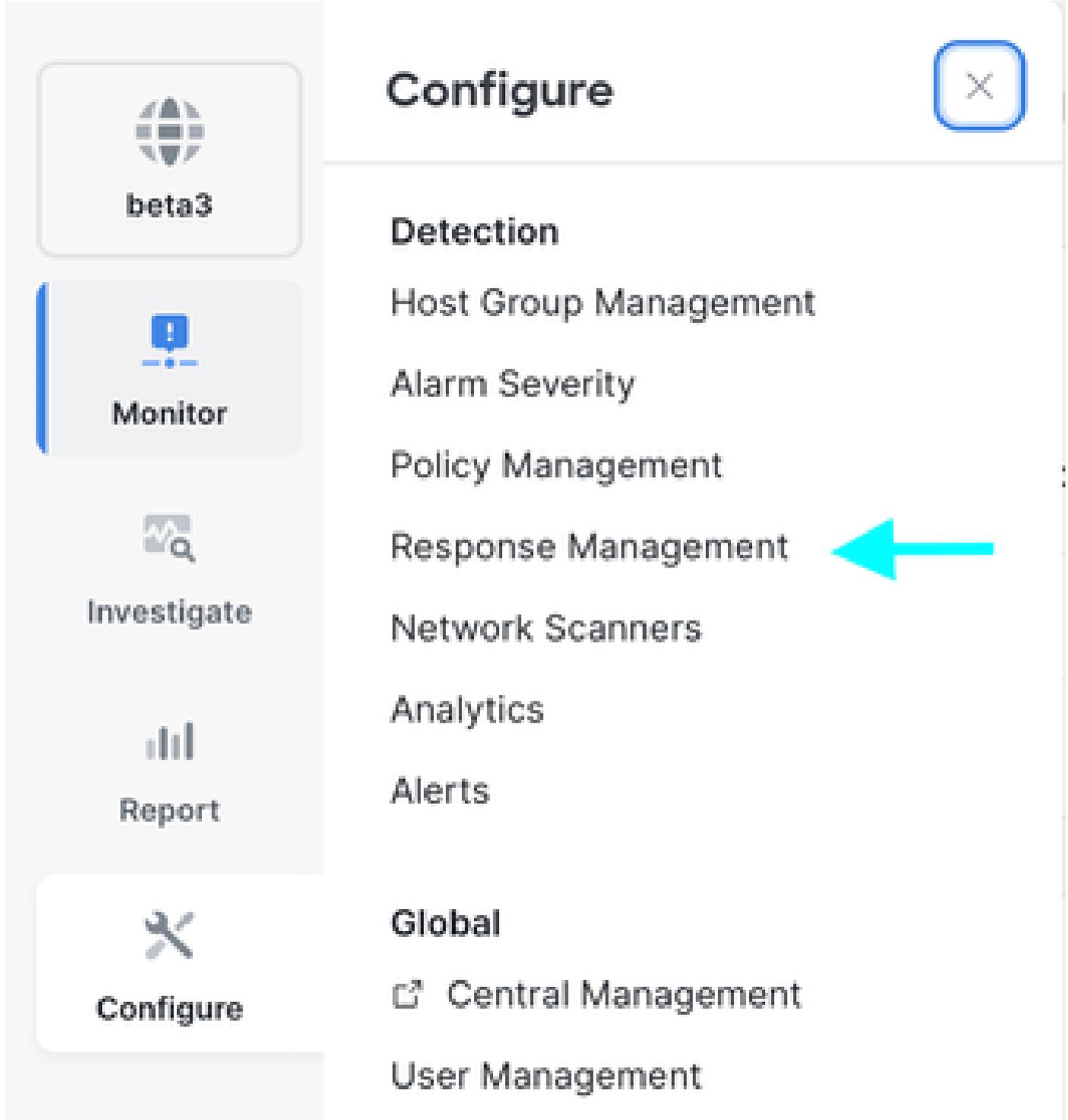
提示：确保在SNA和Splunk之间的任何防火墙或中间设备上允许UDP/514、TCP/6514或任何您为系统日志选择的自定义端口。

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。



Configure ✕

Detection

- Host Group Management
- Alarm Severity
- Policy Management
- Response Management** ←
- Network Scanners

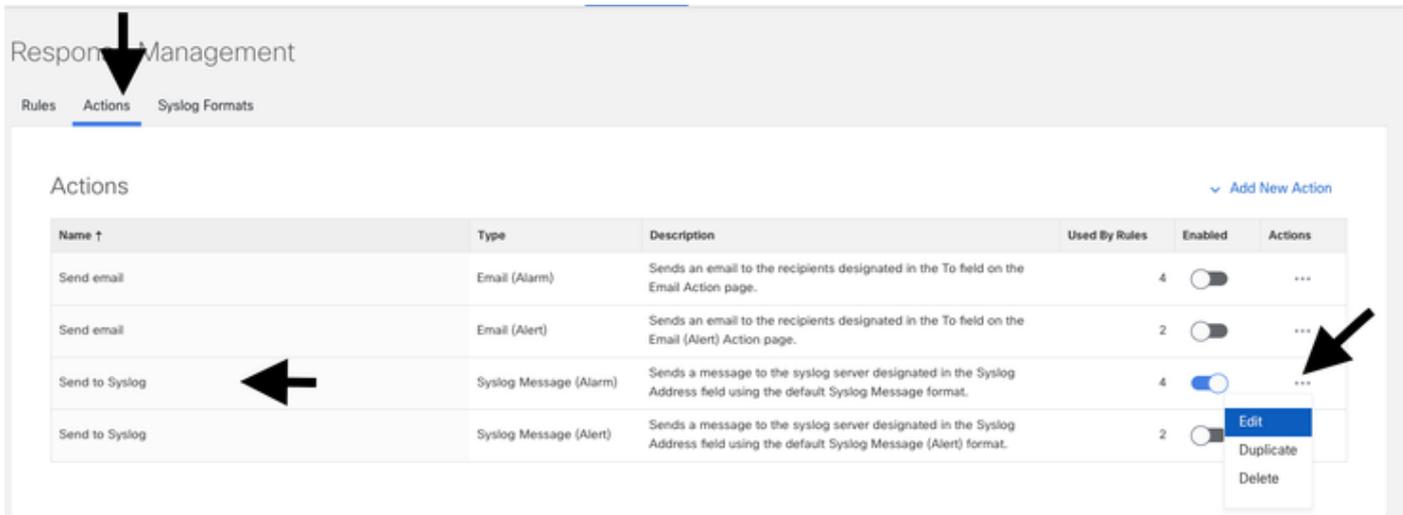
Analytics

- Alerts

Global

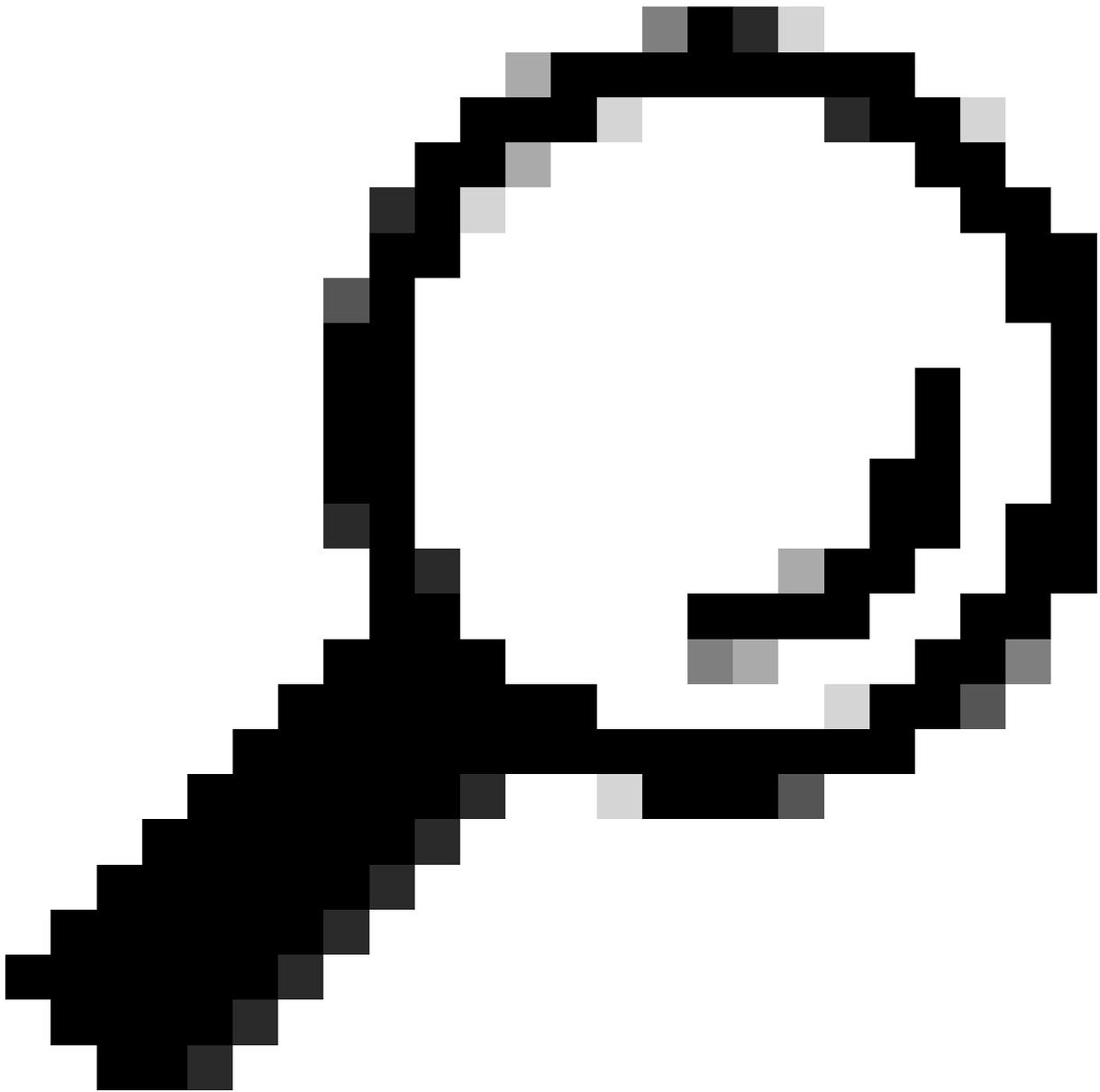
- Central Management
- User Management

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

Response Management

Rules **Actions** Syslog Formats

Syslog Message Action (Alarm)

Cancel

Save

Name

Send to Syslog

Description

Sends a message to the syslog server designated in the Syslog Address field using the default Syslog Message format.



Enabled Disabled actions are not performed for any associated rules.

Syslog Server Address

[Redacted]

UDP Port

514

Message Format

Custom

CEF

This action will use the ArcSight Common Event format.

Example Message

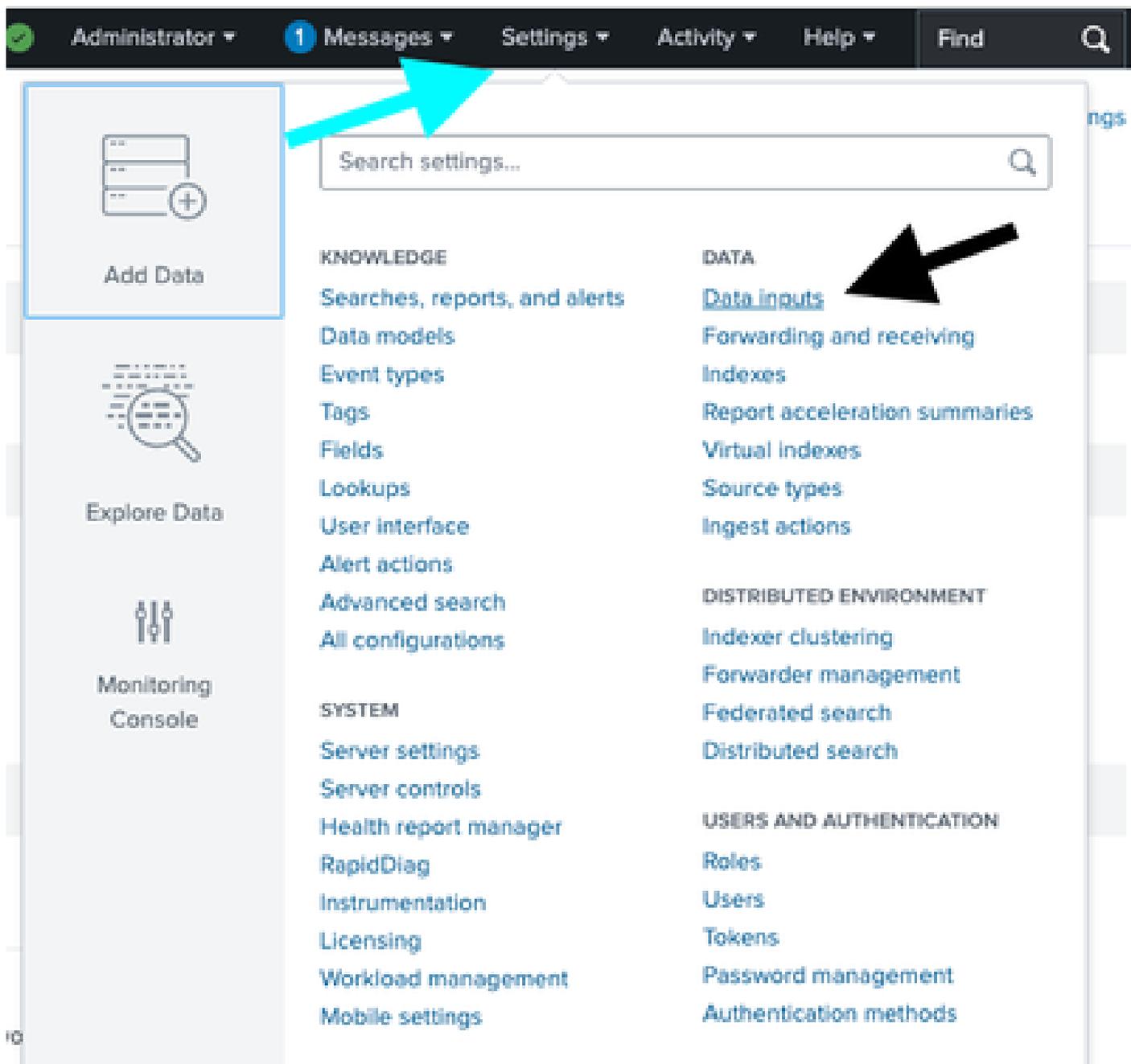
```
<131>Jan 01 00:00:00 test.host TestApp[1337]: CEF:0|Cisco|7.3.0|Notification:99|Bad Host|5|msg=This host has been observed performing malicious actions toward another host.:Source Host is http (80
```

Test Action

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。

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



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。

Add Data Select Source Input Settings Review Done < Back Next >

Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP >
Configure the Splunk platform to listen on a network port.

Scripts
Get data from any API, service, or database with a script.

Splunk Assist Instance Identifier
Assigns a random identifier to every node

Systemd Journald Input for Splunk
This is the input that gets data from journald (systemd's logging component) into Splunk.

Logd Input for the Splunk platform
This input collects data from logd on macOS and sends it to the Splunk platform.

Splunk Secure Gateway
Initializes the Splunk Secure Gateway application to talk to mobile clients over websockets

Splunk Assist Self-Update

Configure this instance to listen on any TCP or UDP port to capture data sent over the network (such as syslog). [Learn More](#)

TCP UDP

Port ?
Example: 514

Source name override ?
host:port

Only accept connection from ?
example: 10.1.2.3, lbadhost.splunk.com, *.splunk.com

FAQ

- > How should I configure the Splunk platform for syslog traffic?
- > What's the difference between receiving data over TCP versus UDP?
- > Can I collect syslog data from Windows systems?
- > What is a source type?

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。

Input Settings

Optionally set additional input parameters for this data input as follows:

Source type

The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

Select New

Source Type

Source Type Category Custom ▾

Source Type Description

App context

Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. [Learn More](#)

App Context Search & Reporting (search) ▾

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

Method ? IP DNS Custom

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your

Index Default ▾ [Create a new index](#)

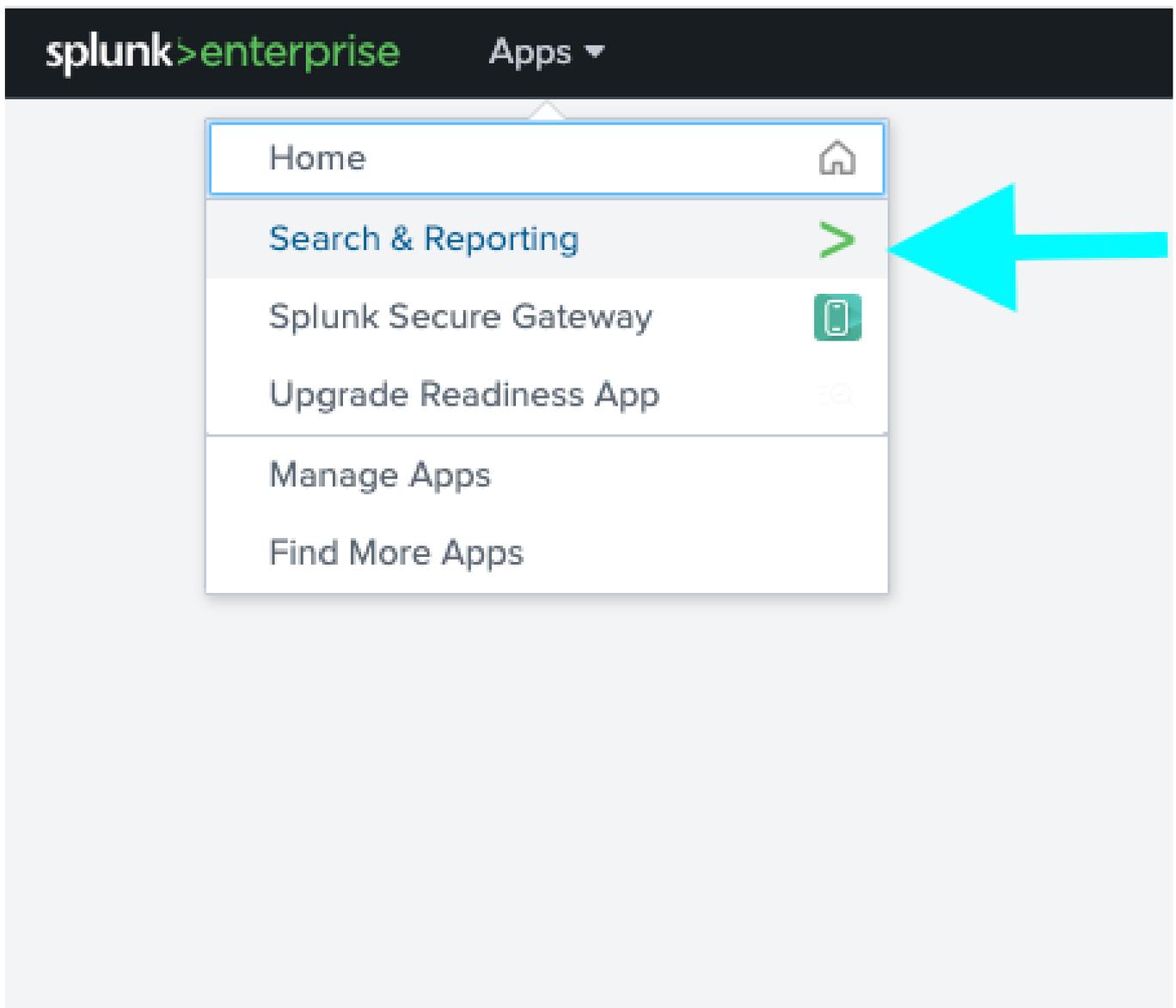
步骤 9：在下一个窗口中，检查您的设置并根据需要进行编辑。

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

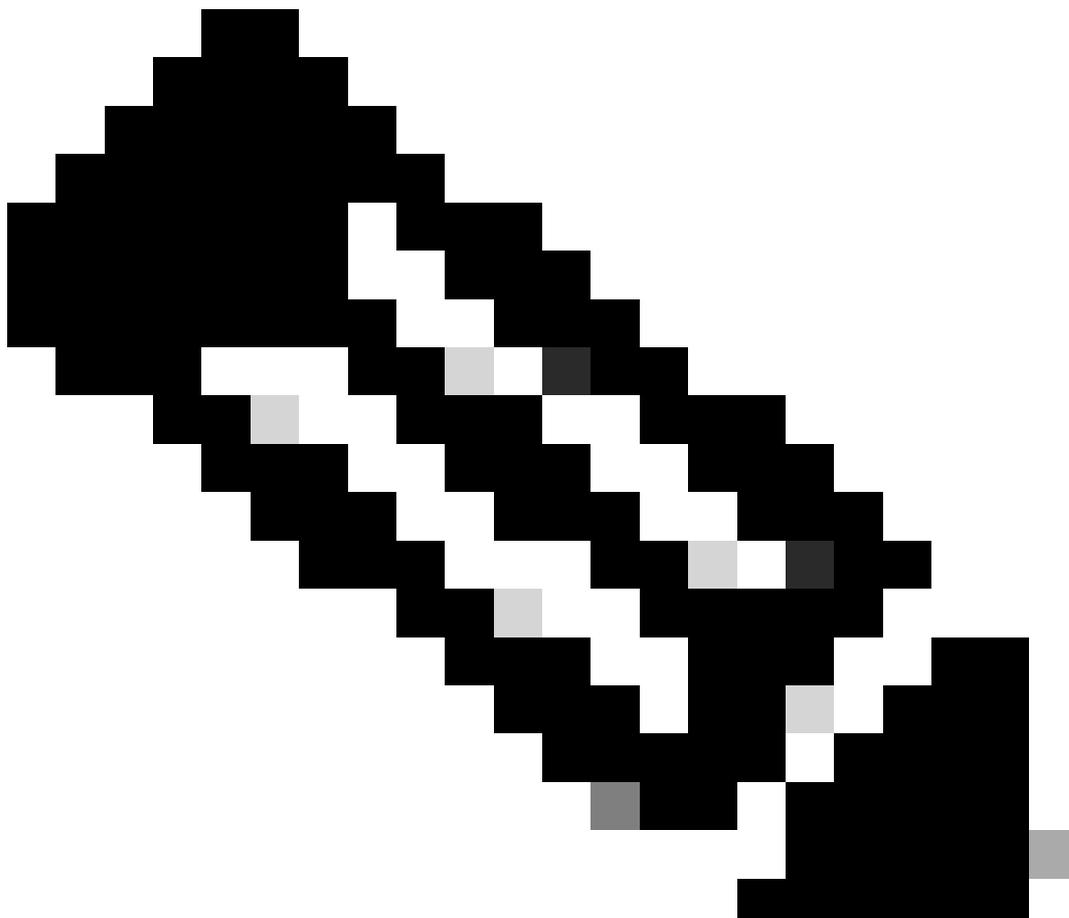
步骤 11：在Web UI中导航到应用>搜索与报告。



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。

The screenshot shows the Splunk search interface. At the top, there is a search bar with the query `source="*" : "*" sourcetype="*"`. Below the search bar, there are tabs for `Events (6)`, `Patterns`, `Statistics`, and `Visualization`. The `Events (6)` tab is active, showing a table of search results. The table has columns for `Time` and `Event`. The `Event` column contains a detailed log entry: `[FlowCollector Flow Data Lost[4]msg: dst= src= : ceExternalId= * / / cs2Label=SGTIDandSGTName spt= destinationTranslatedAddress= destinationTranslatedPort= sourceTranslatedAddress= sourceTranslatedPort= host = | source = | sourcetype =`. On the left side, there is a sidebar with `SELECTED FIELDS` including `host 1`, `source 1`, and `sourcetype 1`.

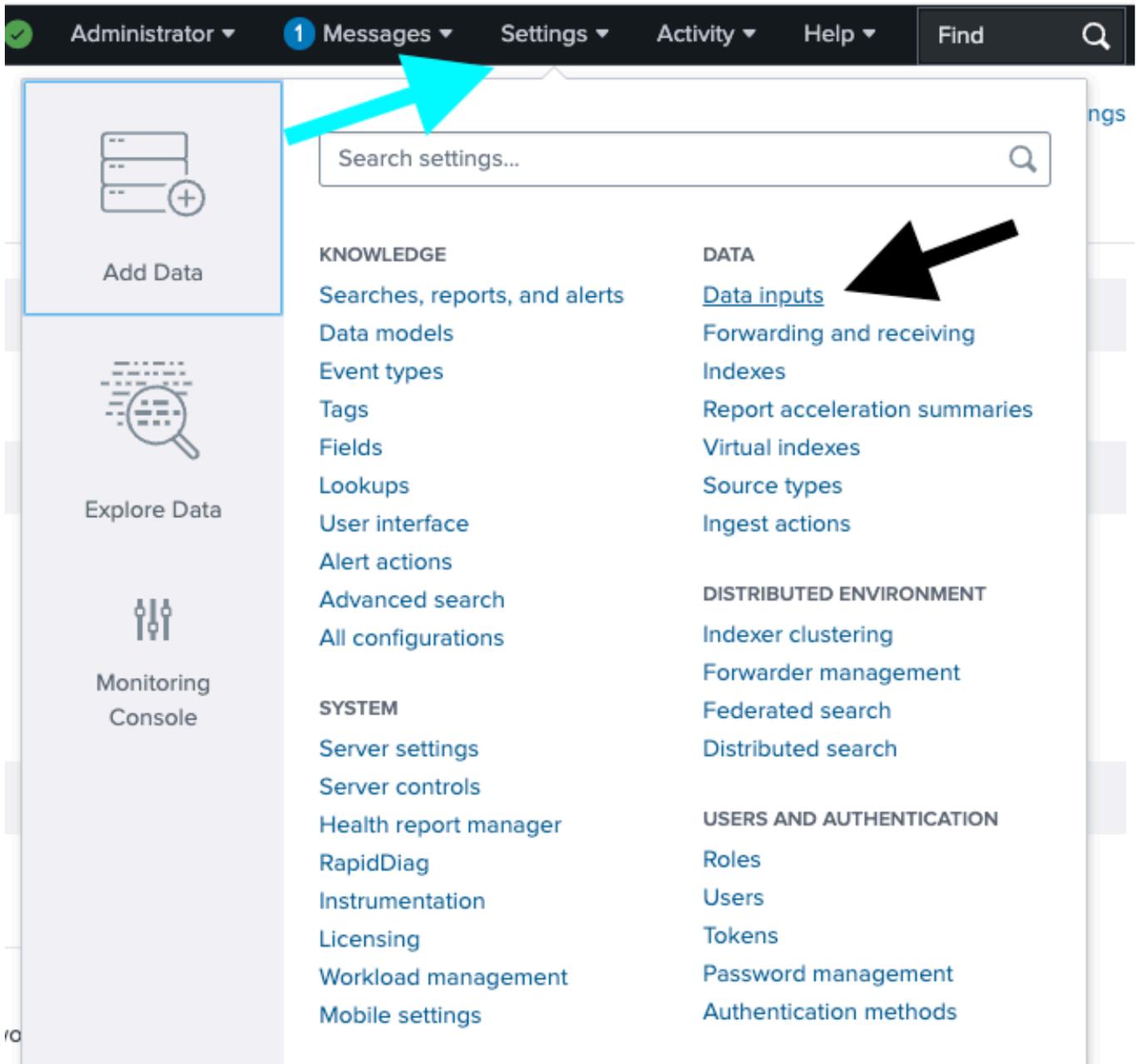


注意：有关源，请参阅步骤4
有关source_type，请参阅步骤6

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。

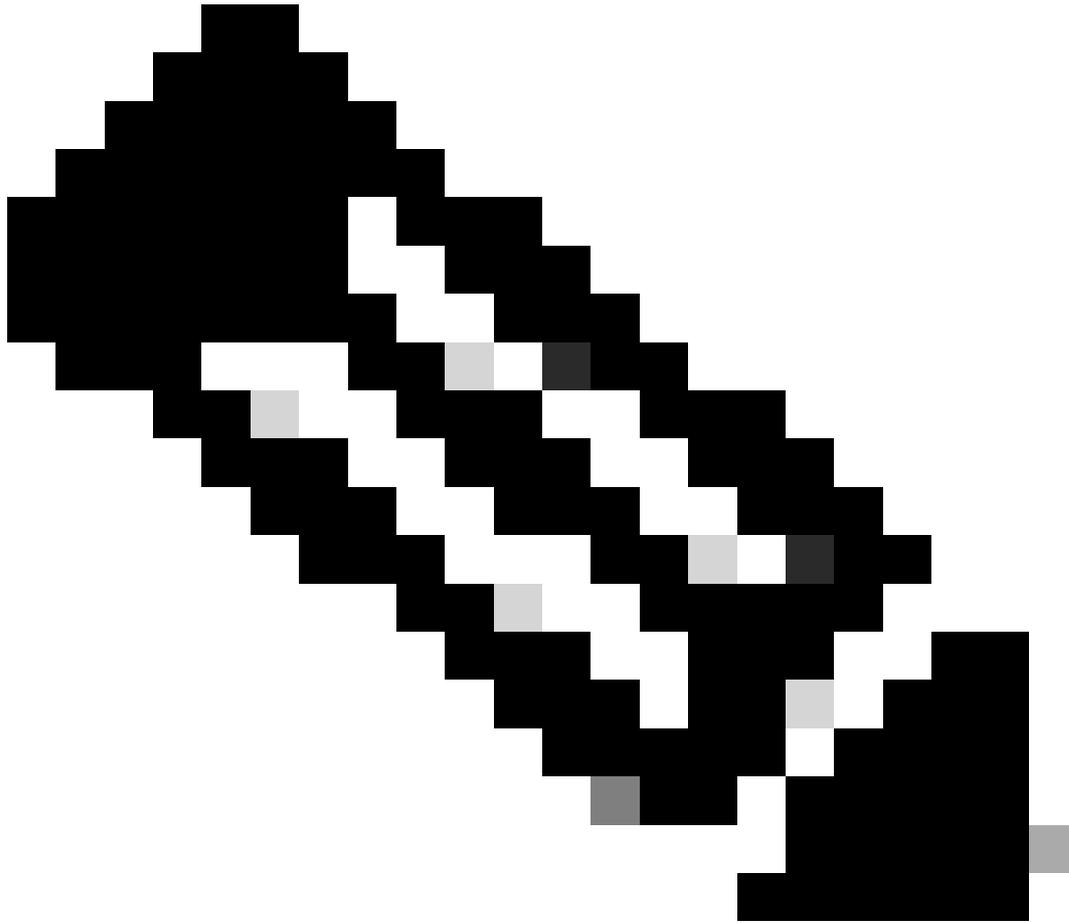
es and directories, network ports, and scripted inputs. If you want to set up forwarding and receiving between two Splunk instances, go to [Forwarding and receiving](#).

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.	0	+ Add new
UDP Listen on a UDP port for incoming data, e.g. syslog.	0	+ 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 Journal 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

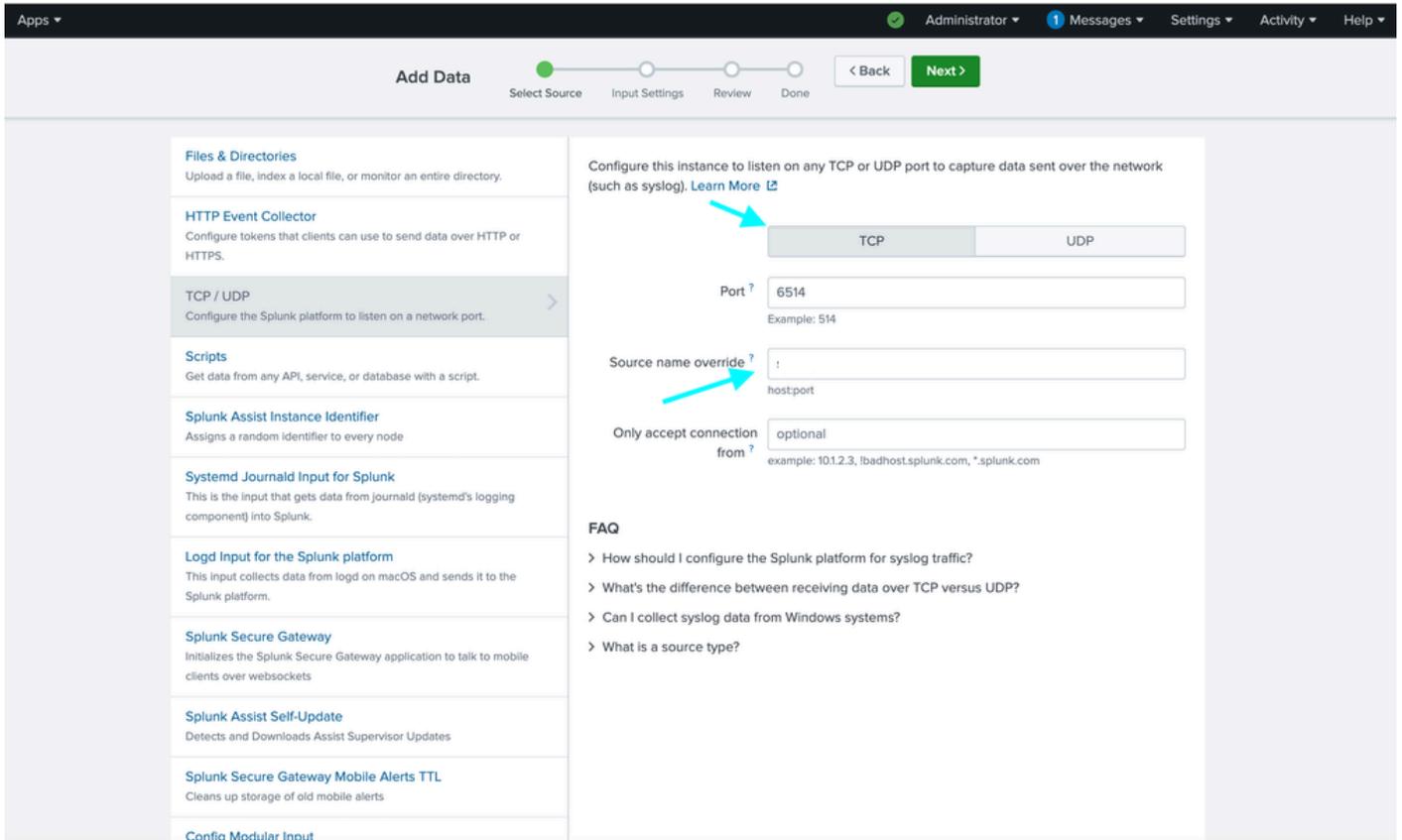


步骤 3：在新窗口中选择TCP，在示例图像端口6514中输入所需的接收端口，并在Source name override字段中输入“desired name”。



注意：TCP 6514是通过TLS的系统日志的默认端口

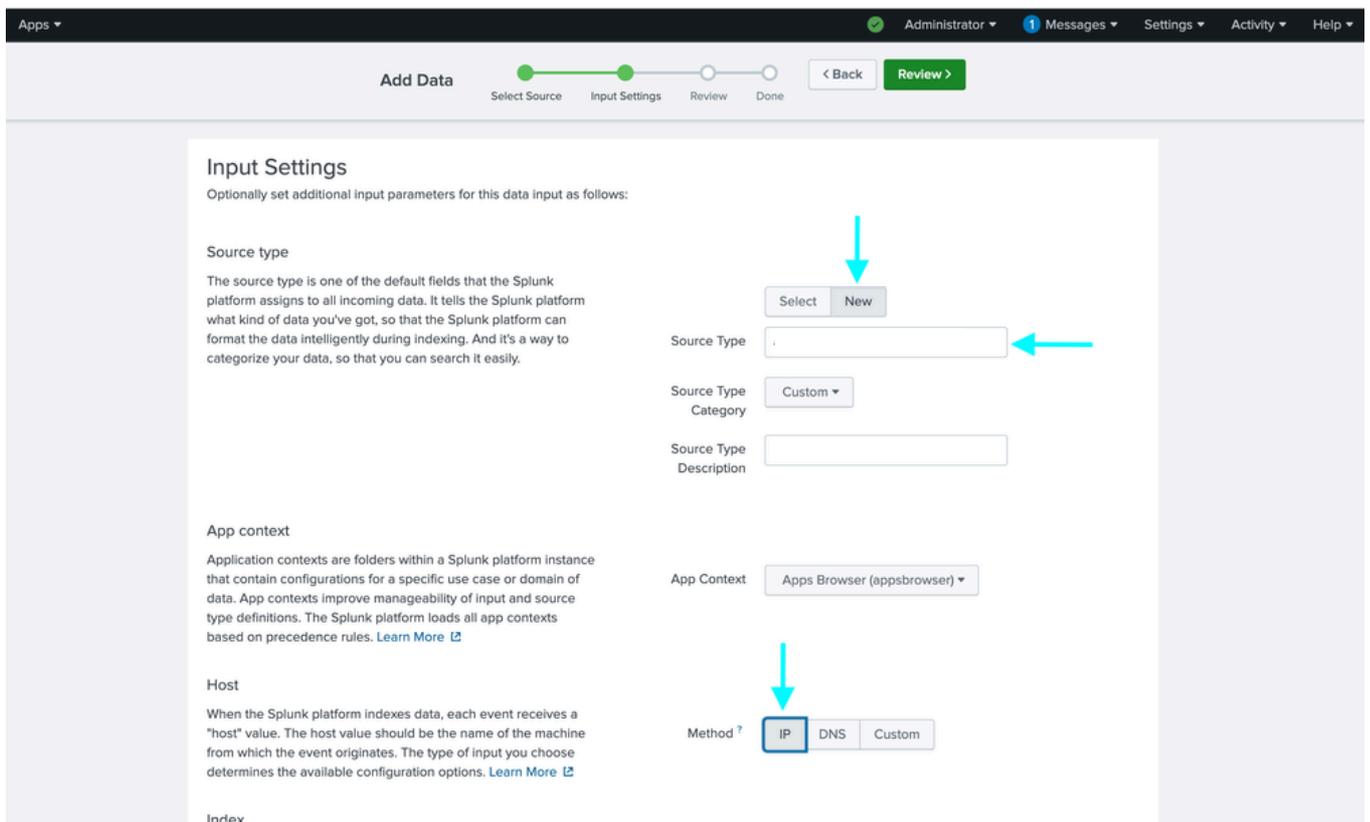
步骤 4：完成后，单击窗口顶部的绿色Next >按钮。



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 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splunkweb.cer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。

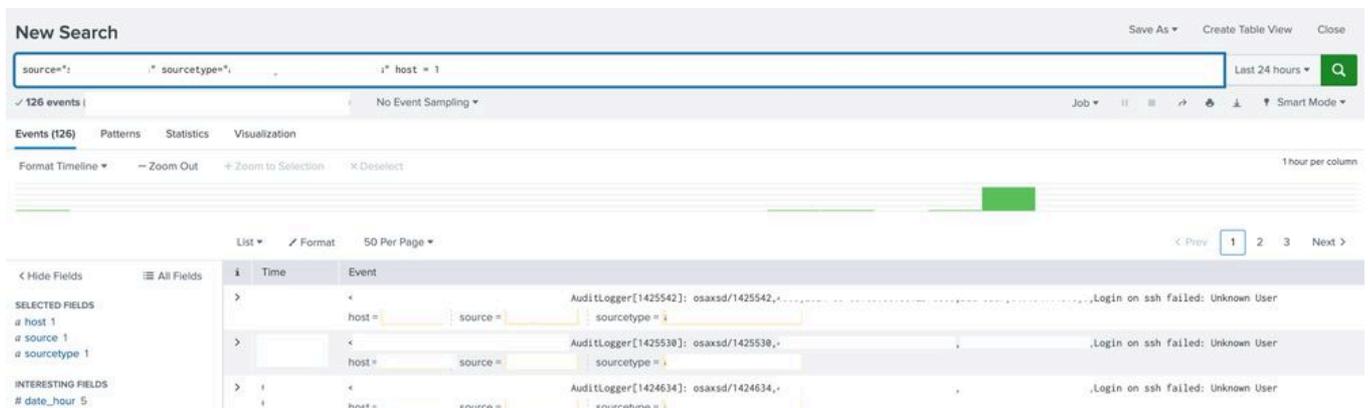
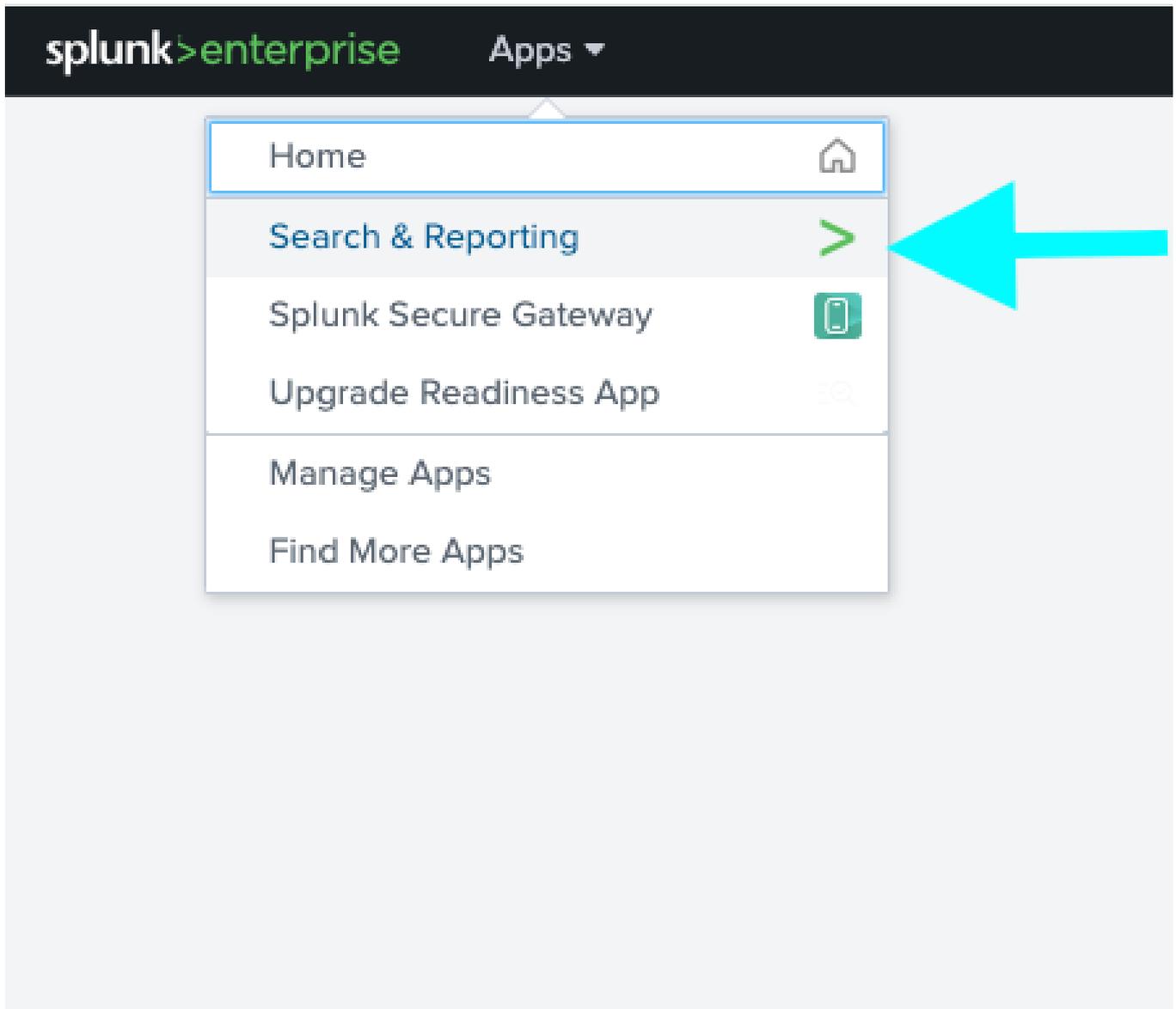
```
user@examplehost:~# chmod 600/opt/splunk/etc/auth/splunkweb.cer
```

第7步：创建新的input.conf文件。

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

```
[tcp-ssl://6514]  
sourcecetype =   
disabled = false  
[SSL]  
serverCert = /opt/splunk/etc/auth/splunkweb_combined.cer  
sslPassword =   
requireClientCert = false  
#sslVersions = tls1.2  
#cipherSuite = AES256-SHA
```

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。



nse



Monitor



Investigate



Report



Configure

Configure ×

Detection

Host Group Management

Alarm Severity

Policy Management

Response Management

Network Scanners

Analytics

Alerts

Global

 Central Management

步骤 2：单击所需SNA设备的省略号图标，选择编辑设备配置。

Inventory

4 Appliances found

Filter by Identity

Appliance Status	Identity	FQDN	Type	Actions
Connected				...

- Edit Appliance Configuration
- View Appliance Statistics
- Support
- Reboot Appliance
- Shut Down Appliance
- Remove This Appliance

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。

Audit Log Destination (Syslog over TLS) Modified Reset

Add your Syslog SSL/TLS certificate to this appliance's Trust Store before you configure the Audit Log Destination.

Server Name or IP Address

Destination Port (Default 6514) *

Certificate Revocation **i**

Disabled

Soft Fail

Hard Fail

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。

Central Management Inventory Data Store Update Manager App Manager Smart Licensing SECURE

Inventory / Appliance Configuration

Appliance Configuration - Manager Cancel [Apply Settings](#)

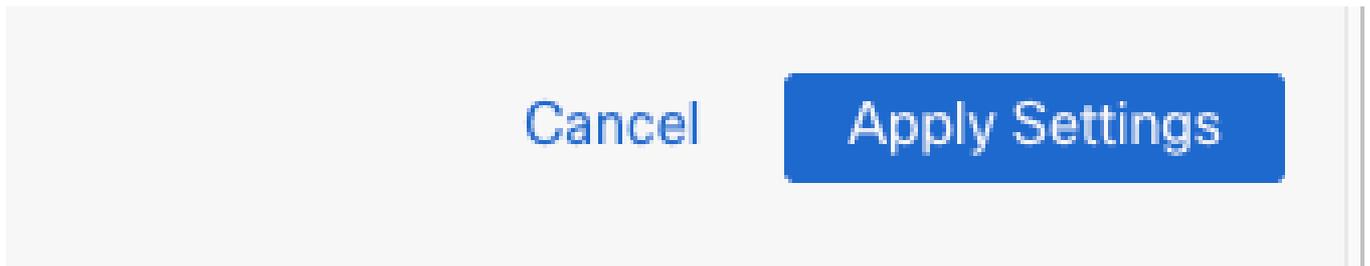
Appliance Network Services General Configuration Menu

Trust Store Add New

Friendly Name	Issued To	Issued By	Valid From	Valid To	Serial Number	Key Length	Actions
							Delete
							Delete
splunk							Delete

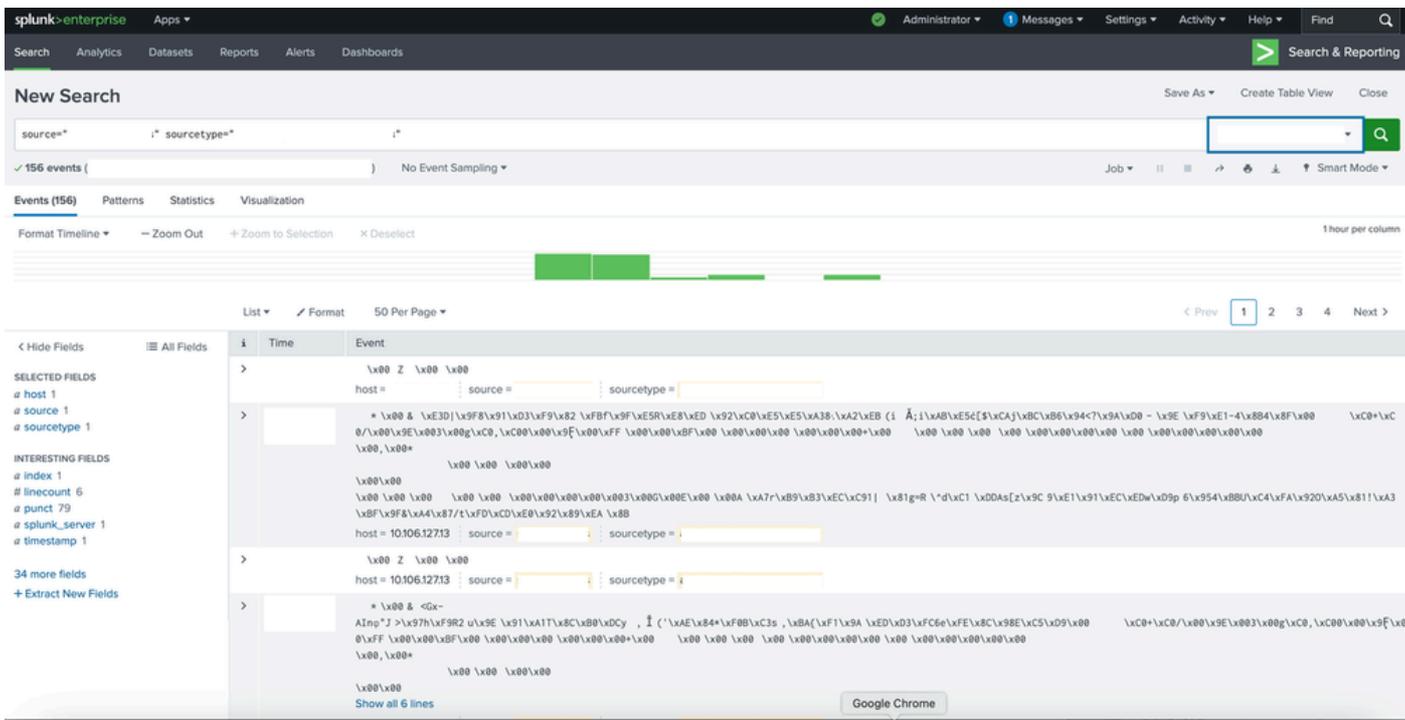
6 Certificates

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。


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



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

TCP

Data inputs > TCP

New Local TCP

Showing 1-1 of 1 item

25 per page

TCP port	Host Restriction	Source type	Status	Actions
6514			Enabled Disable	Clone Delete

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

Select source type from list *

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）。