Configurar o Gerenciamento de Resposta para Enviar Eventos de Syslog para Splunk

Contents

Introdução

Este documento descreve como configurar o recurso Secure Analytics Response Management para enviar eventos via syslog para terceiros, como Splunk.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Secure Network Analytics Response Management (Gerenciamento de Resposta de Análise de Rede Segura).
- Syslog Splunk

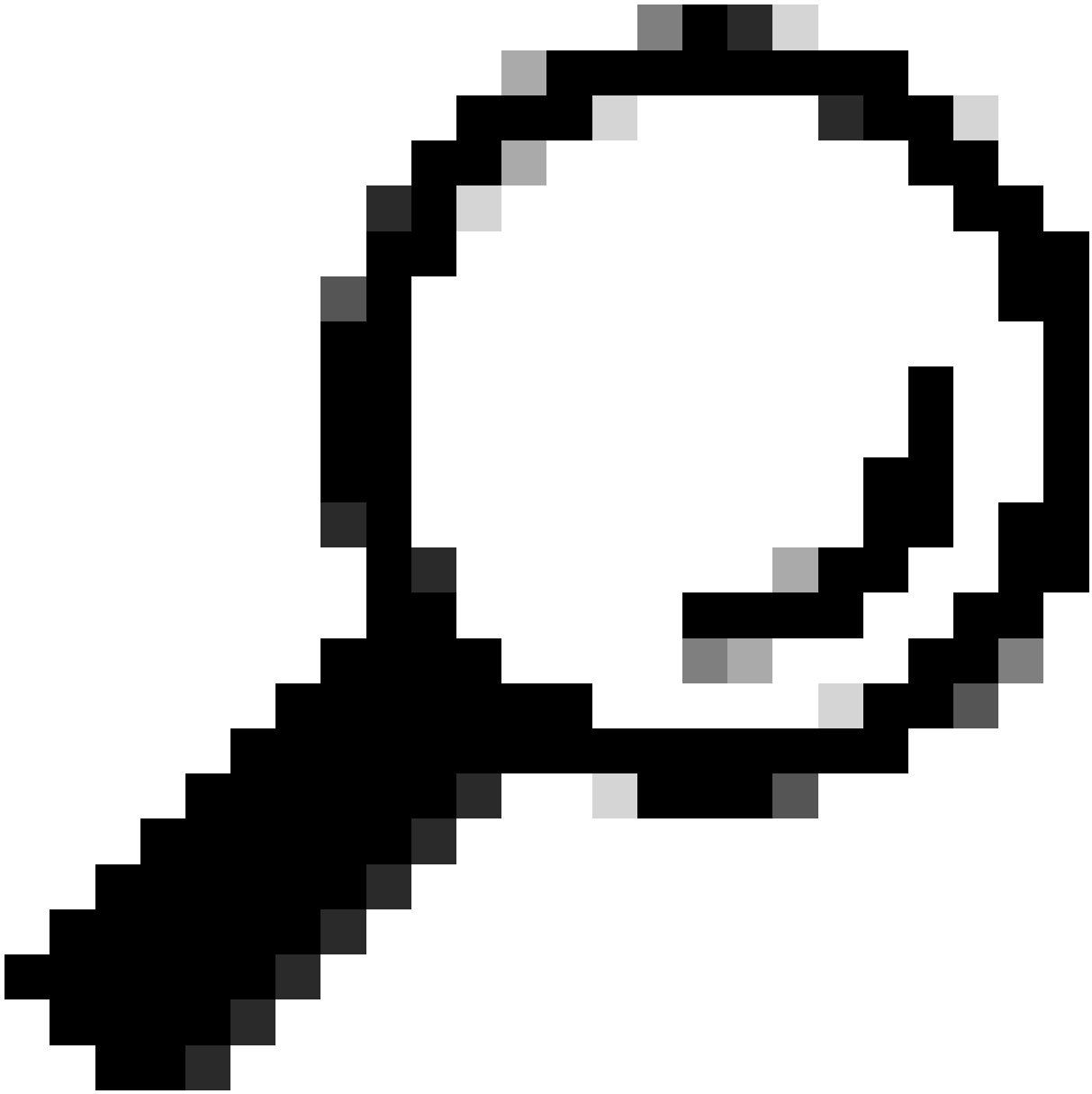
Componentes Utilizados

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

- Implantação do Secure Network Analytics (SNA) que contenha pelo menos um dispositivo Manager e um dispositivo Flow Collector.

- Servidor Splunk instalado e acessível por 443 portas.

Configurar syslog em SNA sobre UDP 514 ou porta definida personalizada



Dica:Certifique-se de que UDP/514,TCP/6514 ou qualquer porta personalizada escolhida para o syslog seja permitida em qualquer firewall ou dispositivo intermediário entre SNA e Splunk.

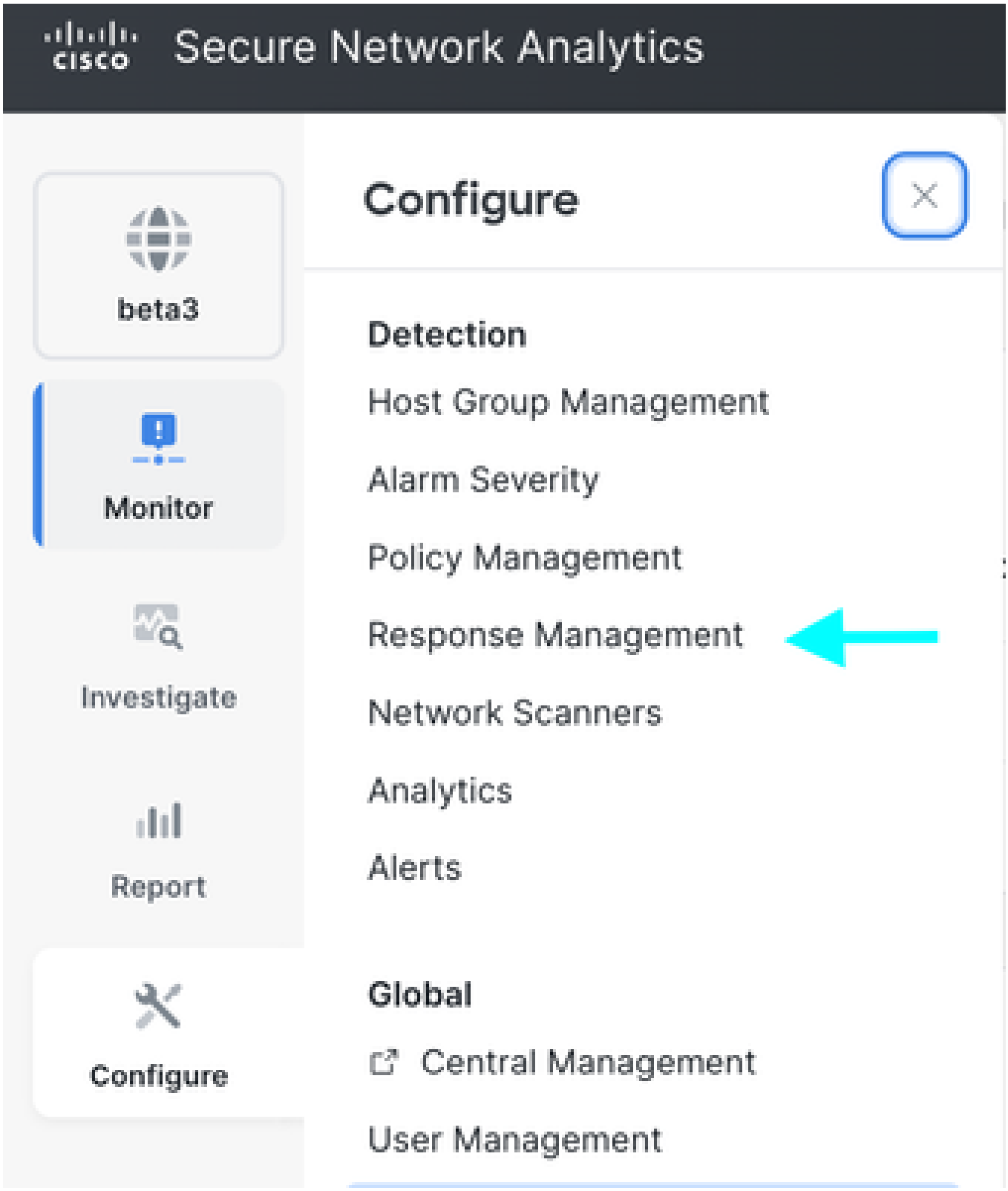
1.Gerenciamento de resposta SNA

O componente Gerenciamento de Resposta do Secure Analytics (SA) pode ser usado para

configurar Regras, Ações e Destinos de syslog.

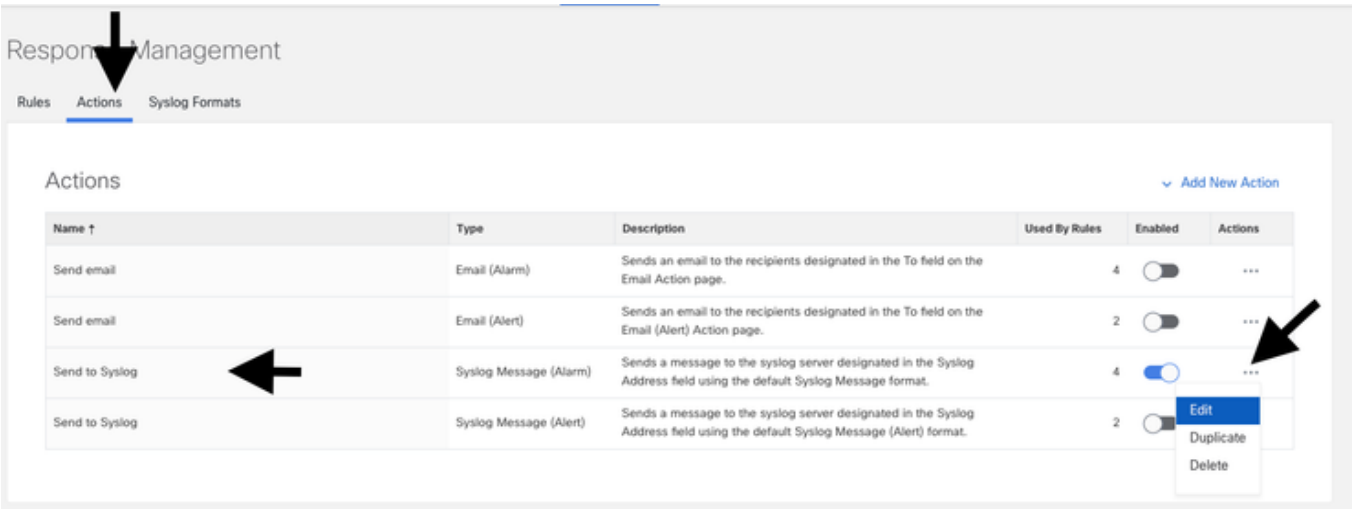
Essas opções devem ser configuradas para enviar/encaminhar alarmes do Secure Analytics para outros destinos.

Etapa1: Faça login no SA Manager e navegue para Configure > Detection Response Management.

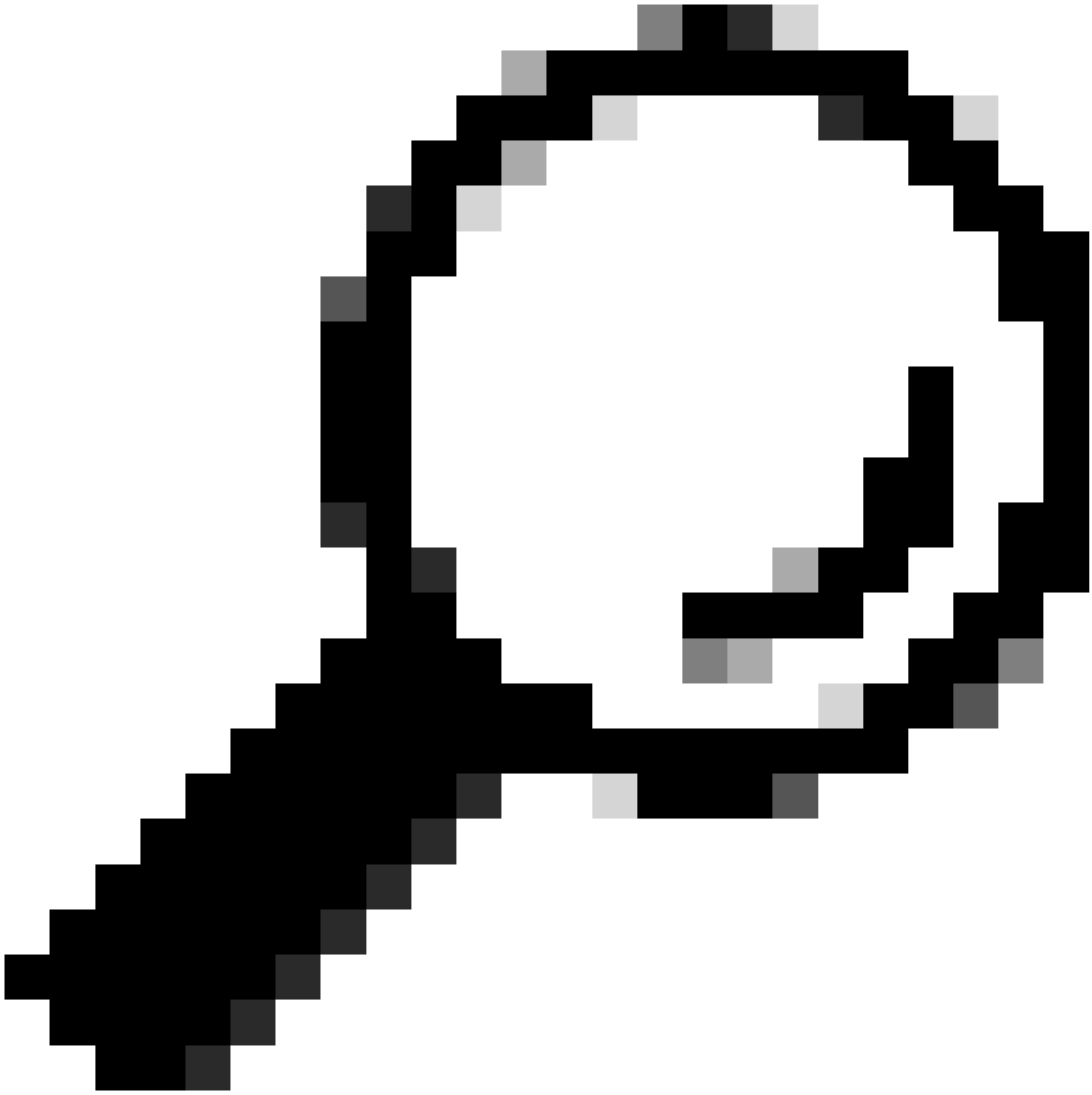


Passo 2: Na nova página, navegue até a guia Actions, localize o item de linha padrão Send to

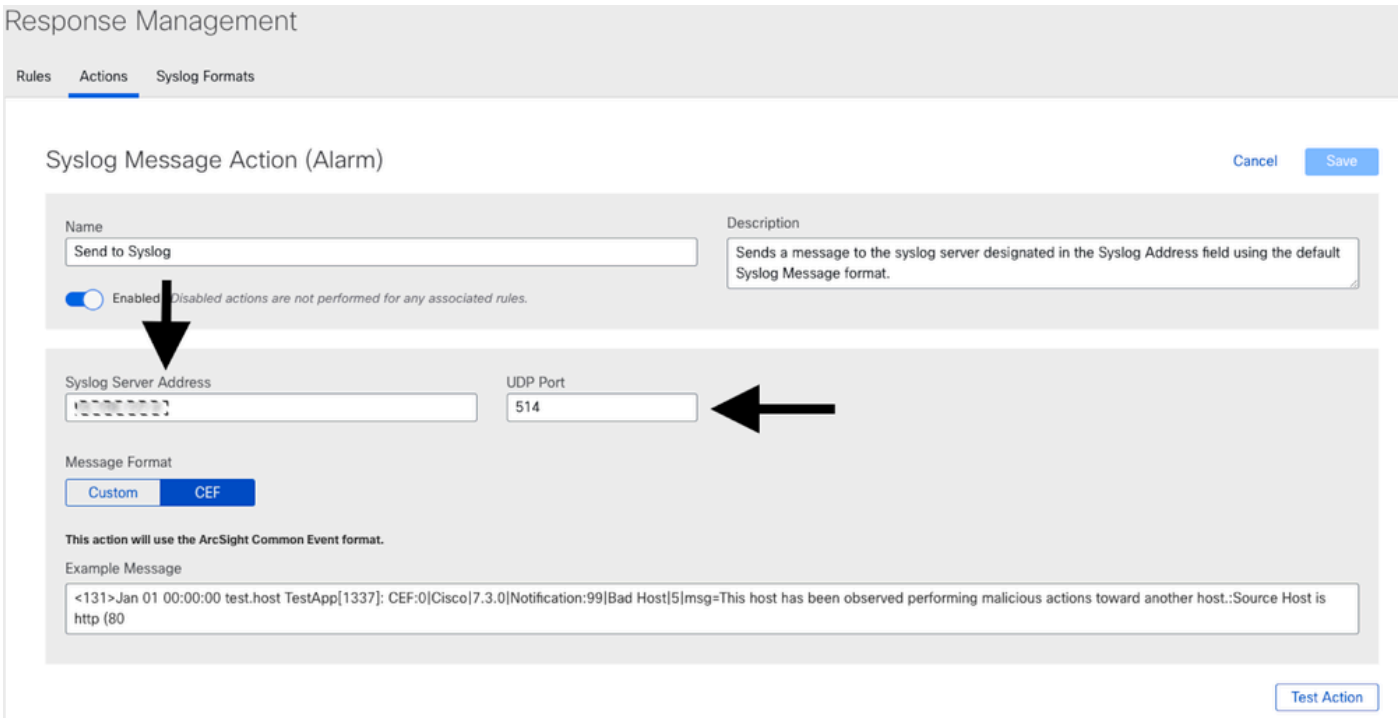
Syslog e clique nas reticências (...) na coluna Action e, em seguida, Edit.



Passo 3: Insira o endereço de destino desejado no campo Syslog Server Address e a porta de recebimento de destino desejada no campo UDP Port. No Formato da mensagem, selecione CEF.
Passo 4: Quando terminar, clique no botão azul Save no canto superior direito.



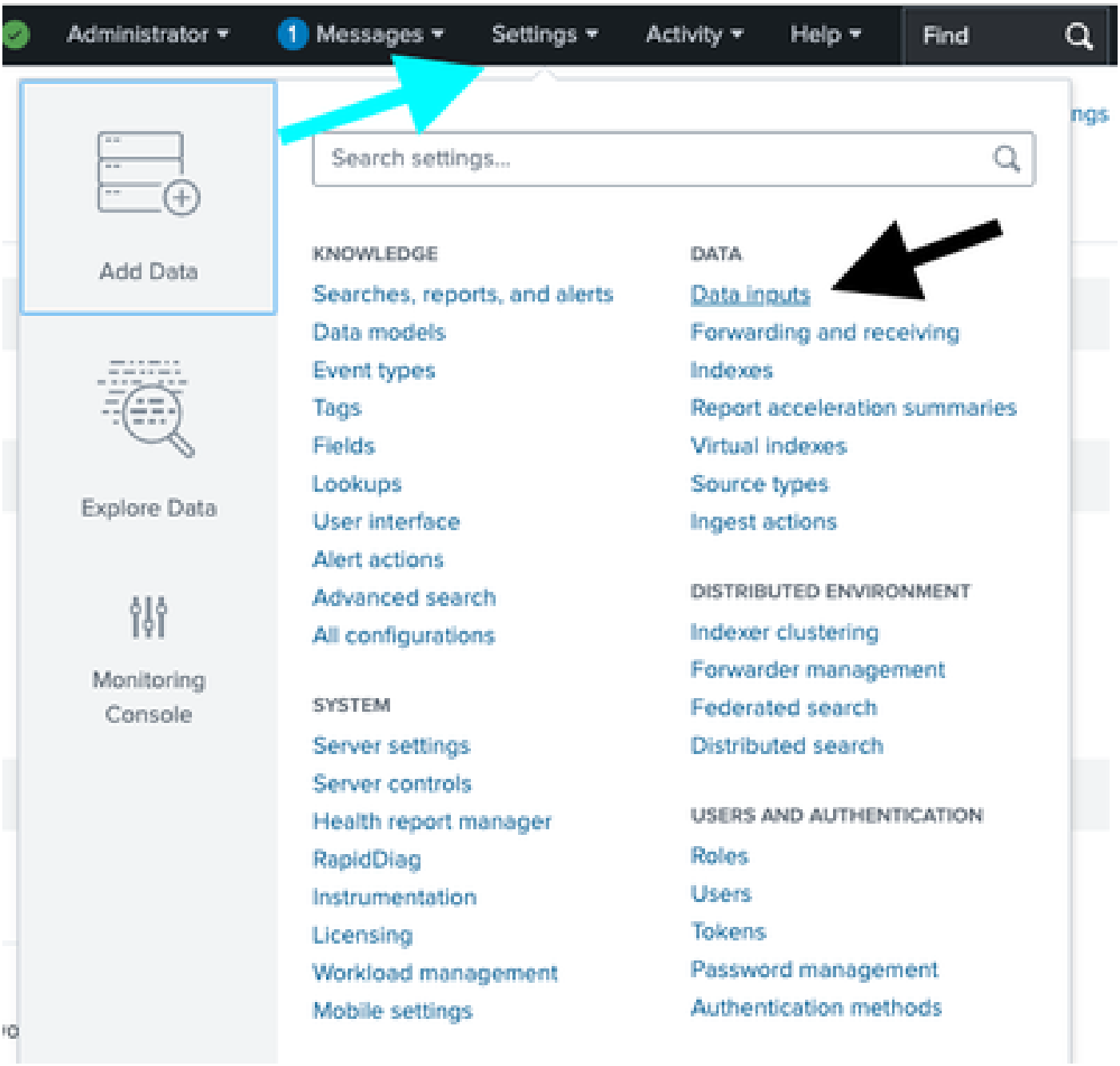
Tip: A porta UDP padrão para syslog é 514



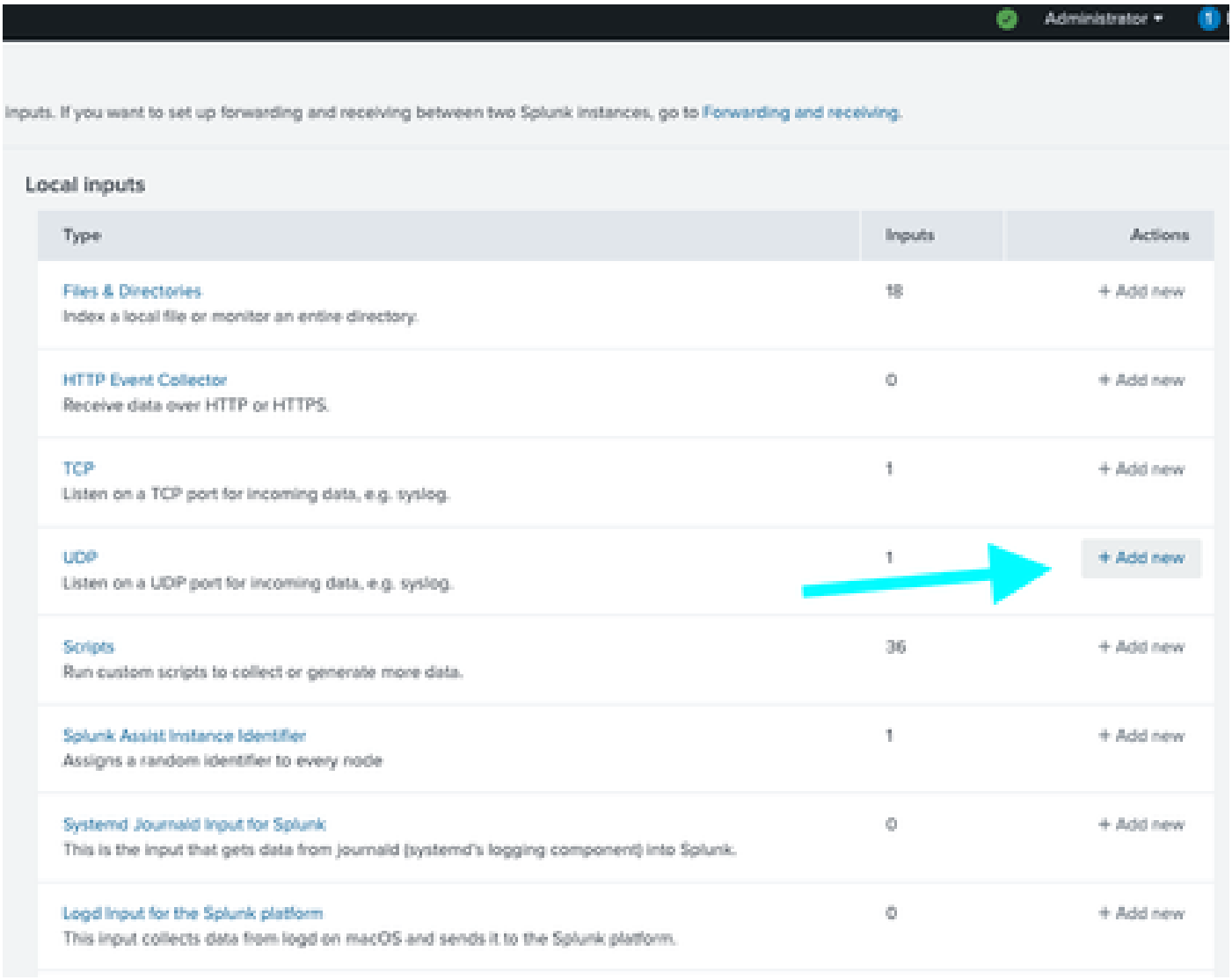
2. Configuração do Splunk para Receber Syslogs SNA pela porta UDP

Depois de aplicar suas alterações na interface do usuário da Web do Secure Network Analytics Manager , você deve configurar a entrada de dados no Splunk.

Passo 1: Faça login no Splunk e navegue até Configurações > Adicionar dados > Entradas de dados.



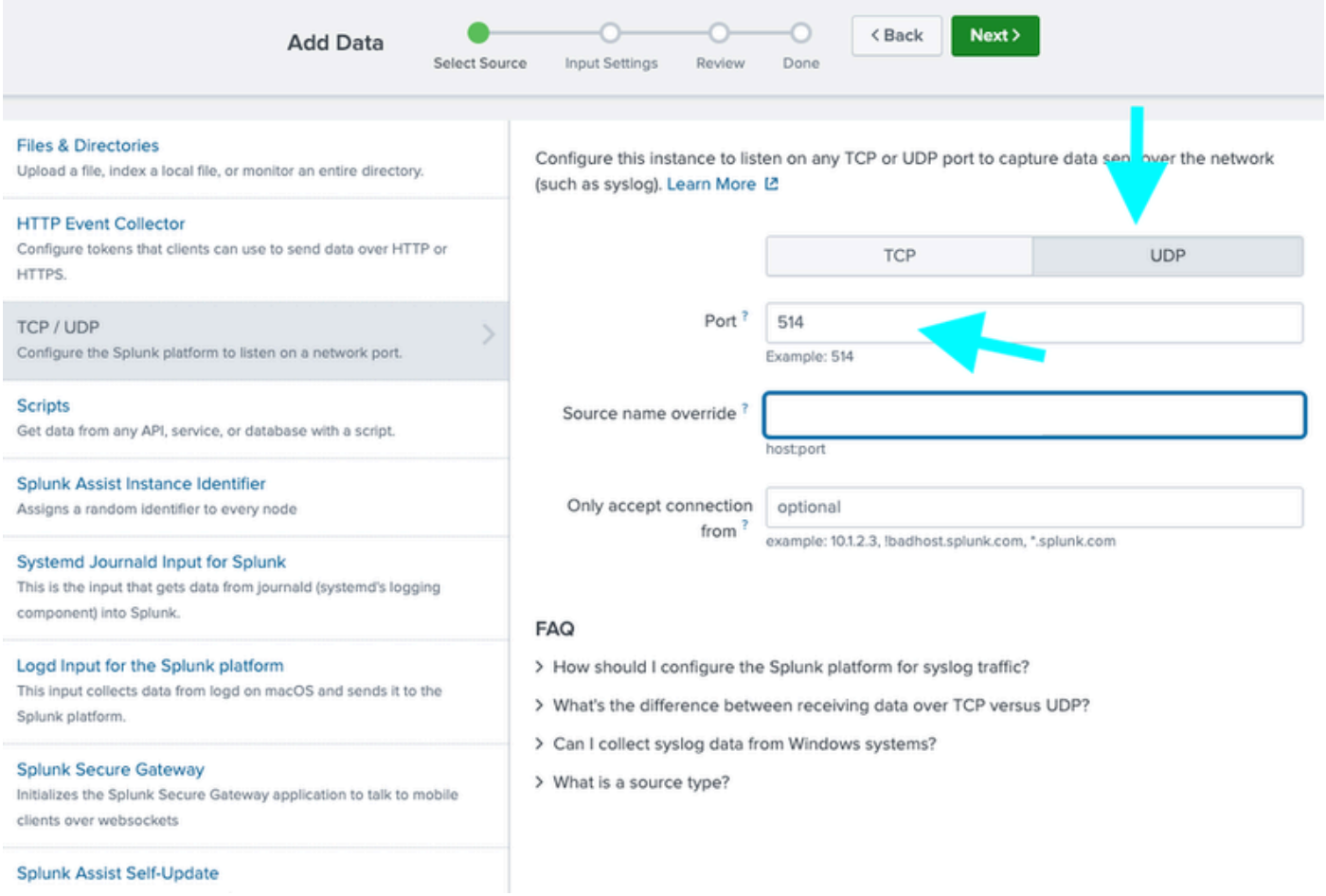
Passo 2: Localize a linha UDP e selecione +Add new.



Passo 3: Na nova página, selecione UDP, insira a porta de recebimento como 514 no campo Port.

Passo 4: No campo Sobreposição de nome de origem, insira desired name of source.

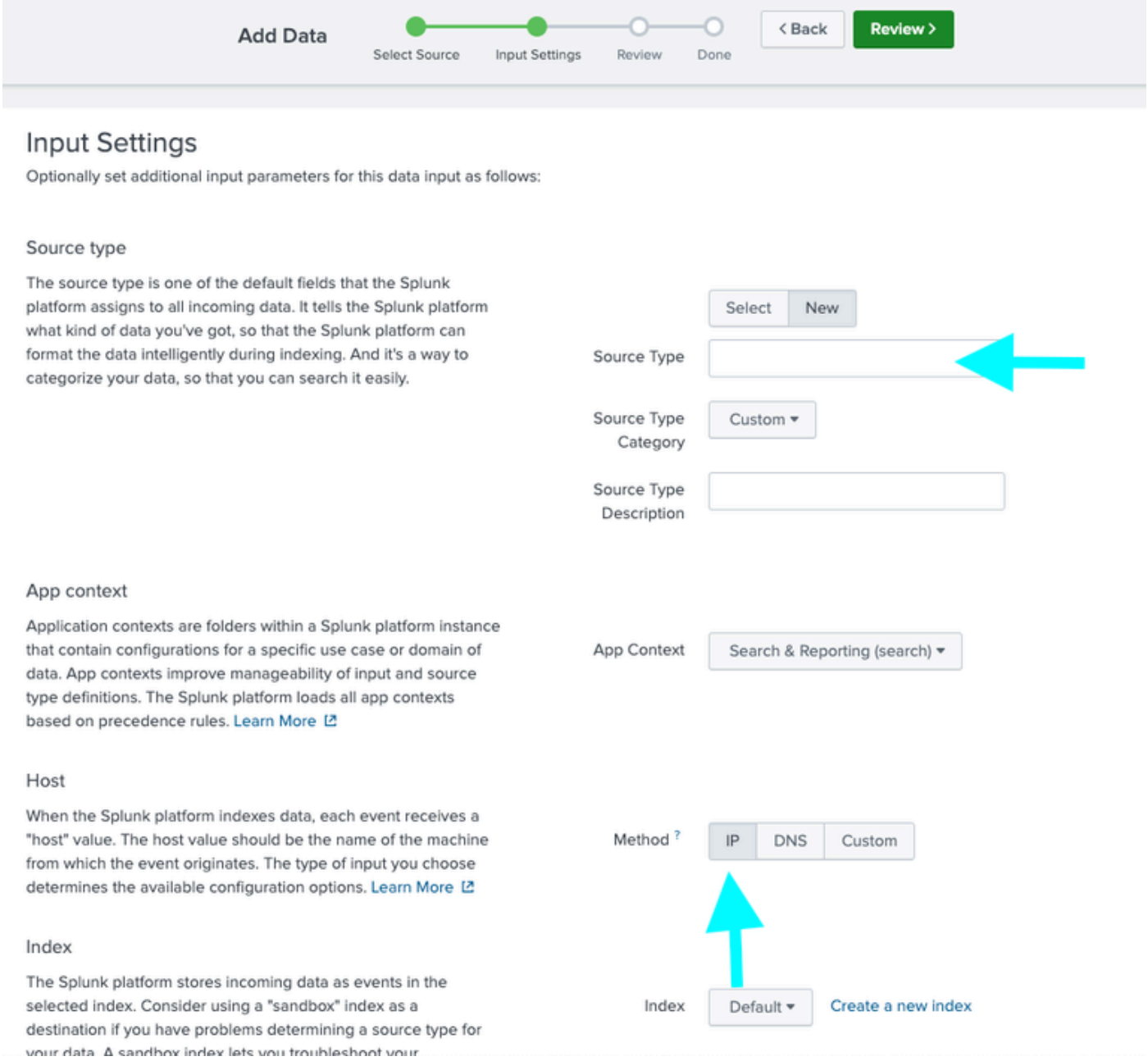
Passo 5: Ao concluir, clique no botão verde Avançar > na parte superior da janela.



Passo 6: Na próxima página, alterne para a opção New e localize o campo Source Type e insira desired source .

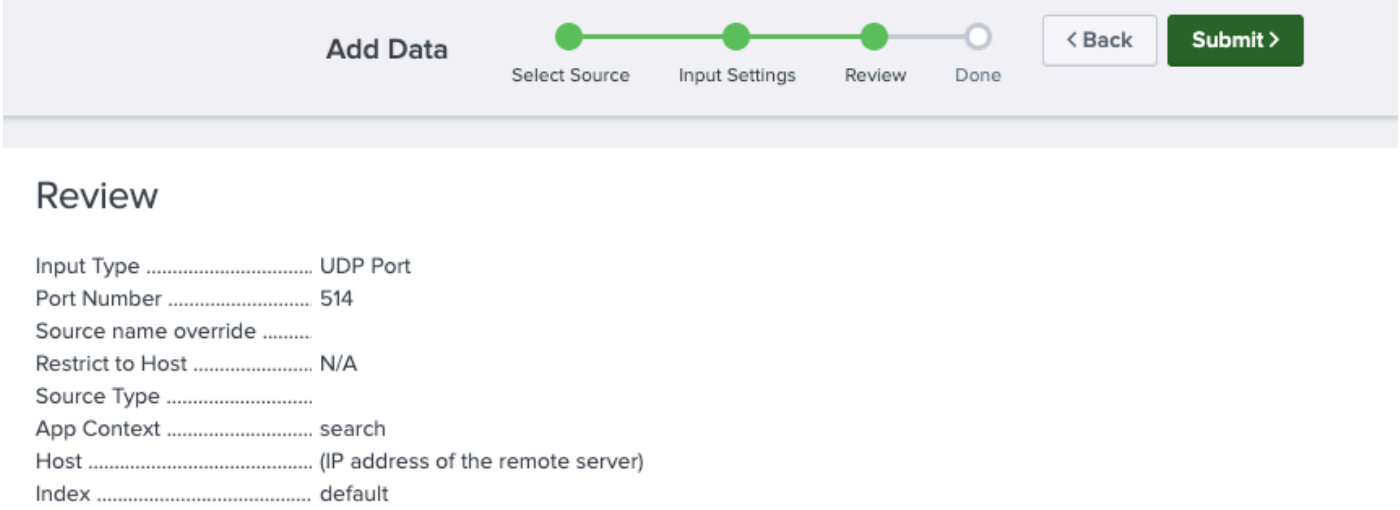
Passo 7: Selecione IP para o Método.

Passo 8: Clique no botão verde Review > na parte superior da tela.

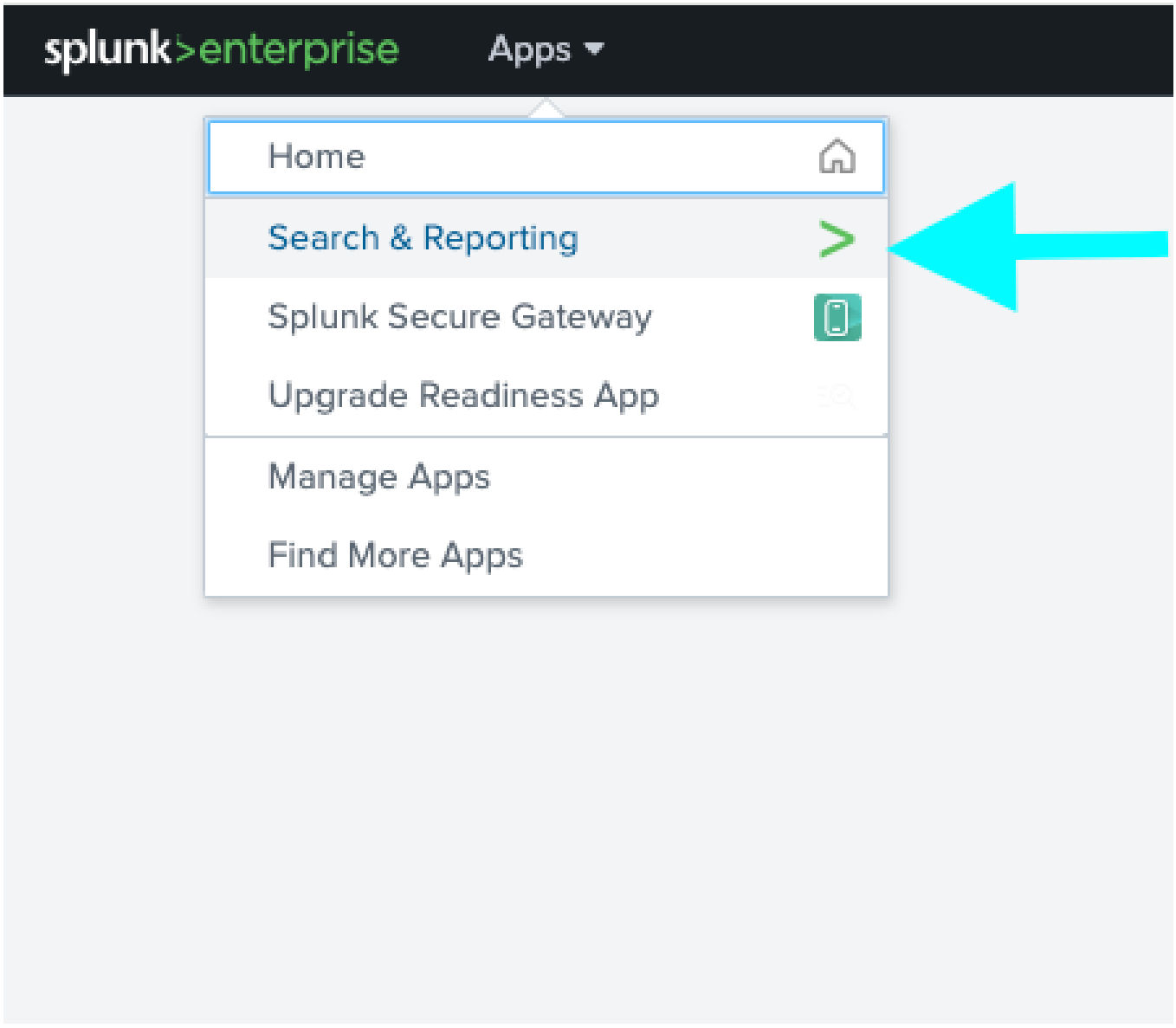


Etapa 9: Na próxima janela, revise suas configurações e edite-as, se necessário.

Etapa 10: Depois de validar, clique no botão verde Submit > na parte superior da janela.

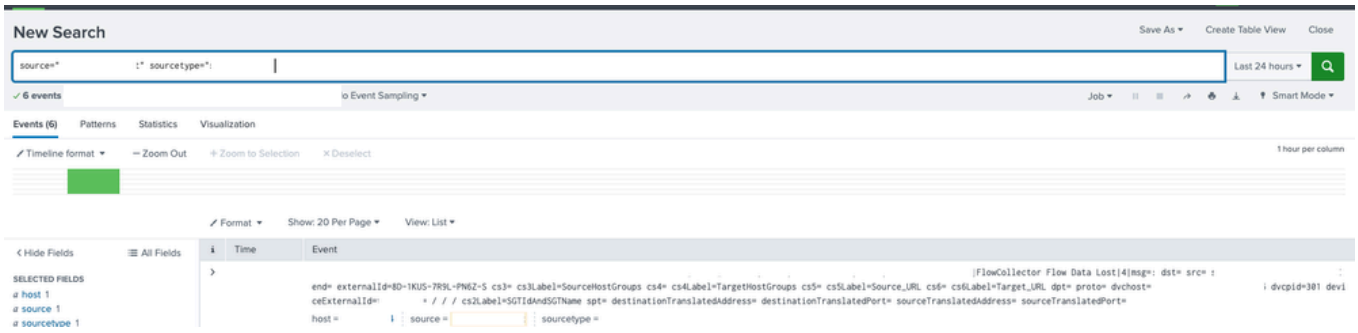


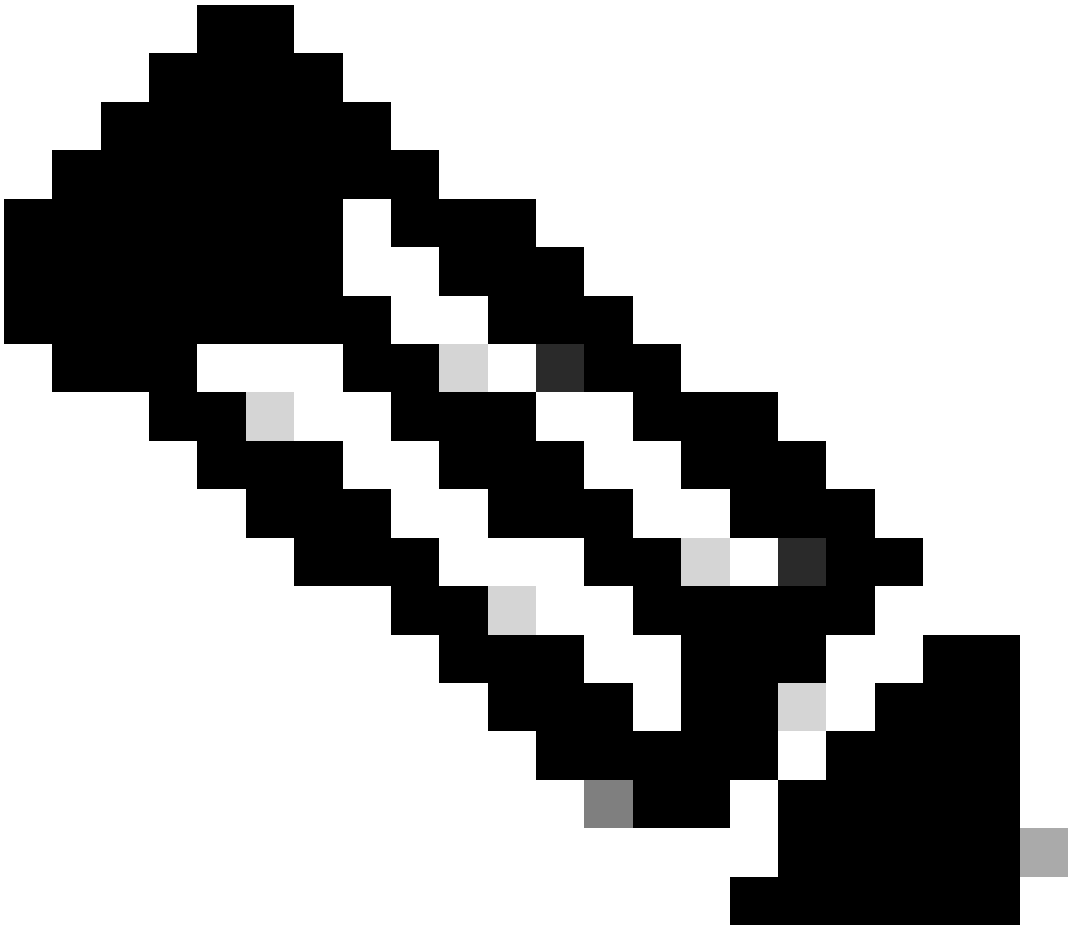
Etapa 11: Navegue até Apps > Search & Reporting na interface do usuário da Web.



Etapa 12: Na página Pesquisar, use o filtro`source="As_configured" sourcetype="As_configured"`para localizar logs

recebidos.



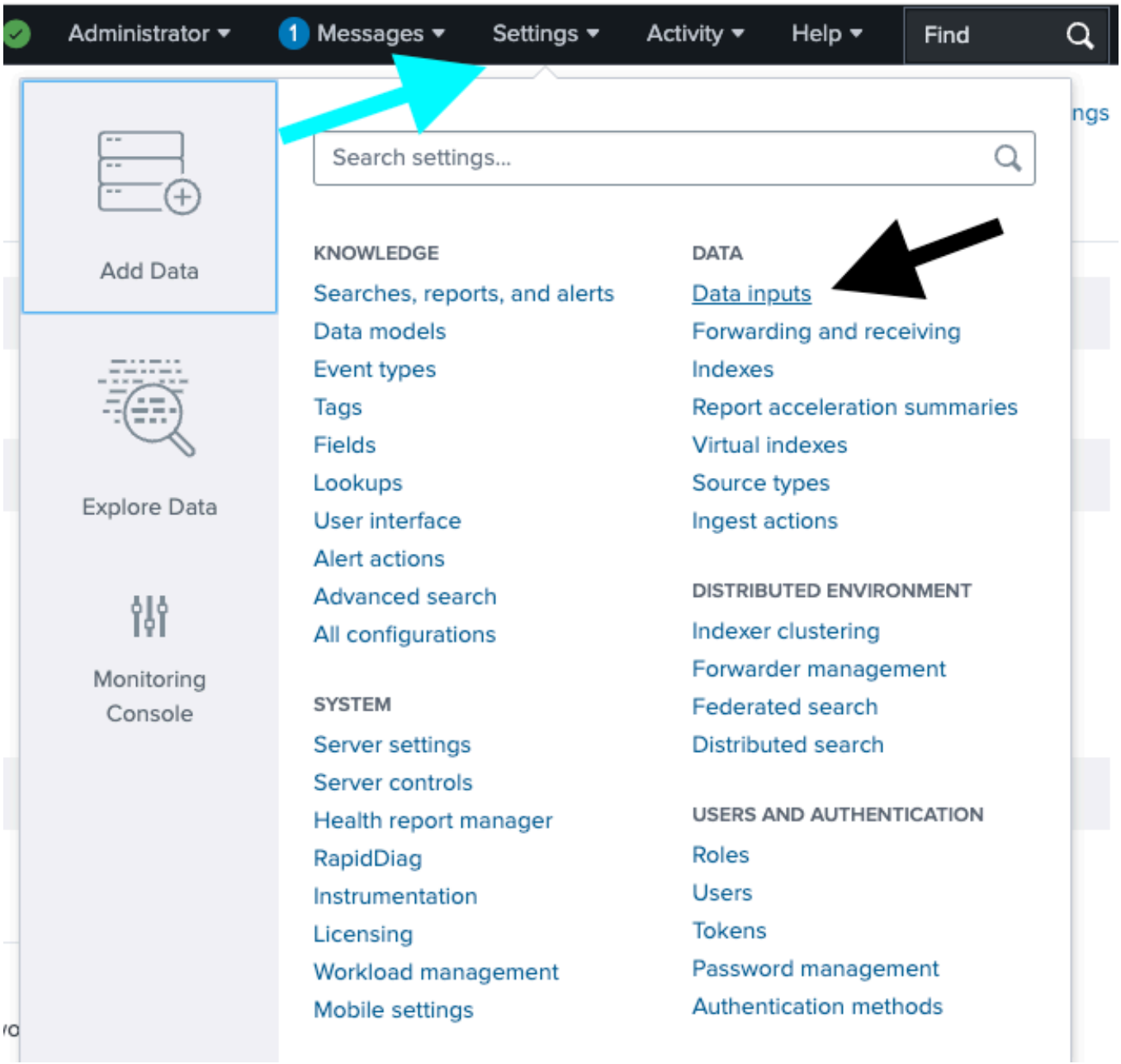


Note: Para a origem, consulte a Etapa 4
Para source_type, consulte a Etapa 6

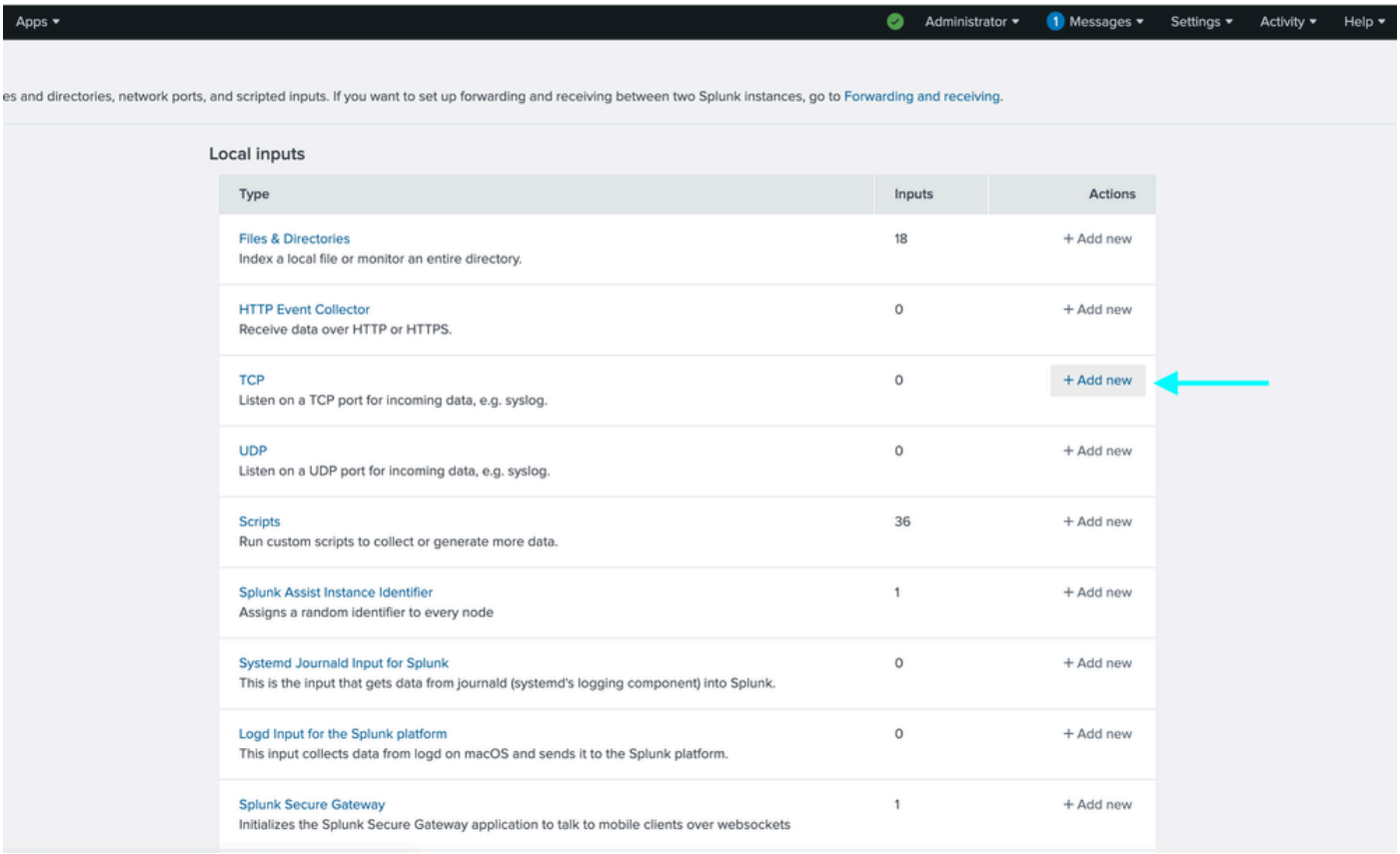
Configurar o syslog em SNA pela porta TCP 6514 ou pela porta definida personalizada

1. Configuração do Splunk para Receber Logs de Auditoria SNA pela porta TCP

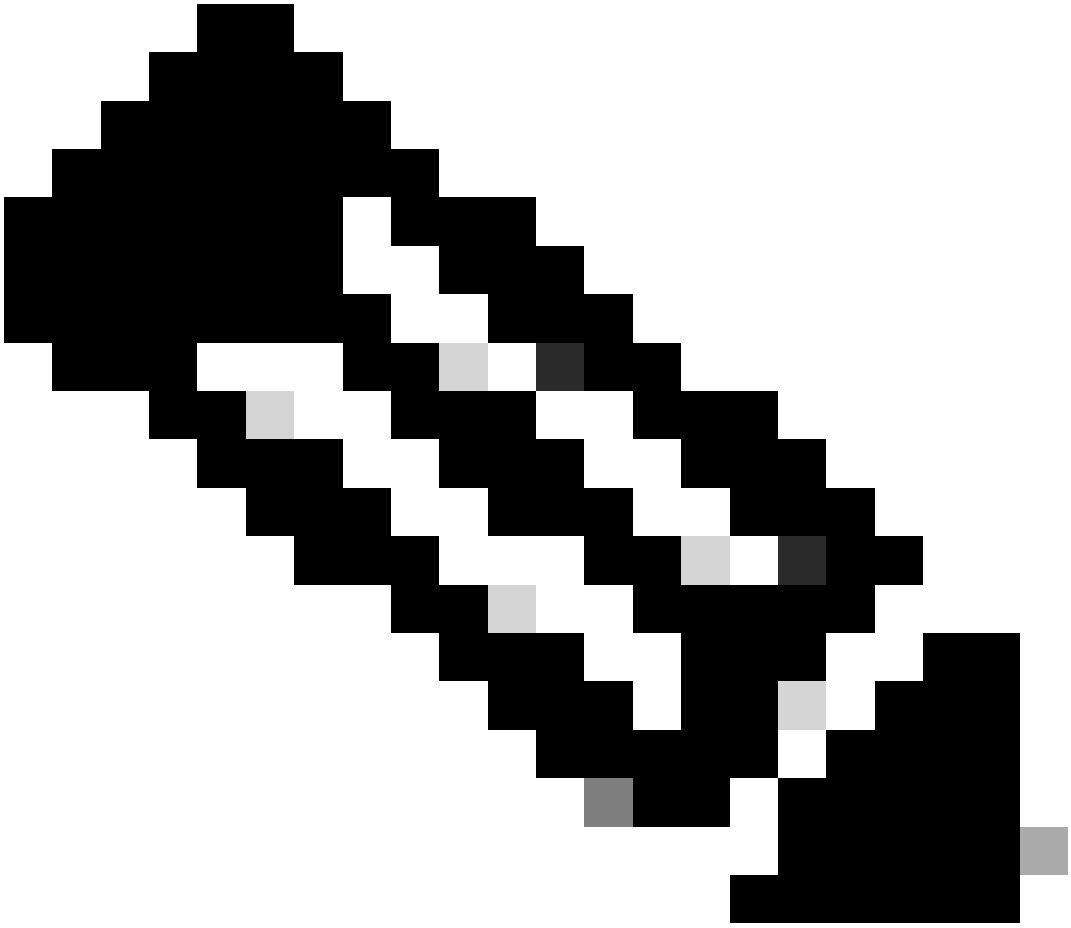
Passo 1: Na interface de usuário do Splunk, navegue para Settings > Add Data > DATA Inputs.



Passo 2: Localize a linha TCP e selecione + Adicionar novo.

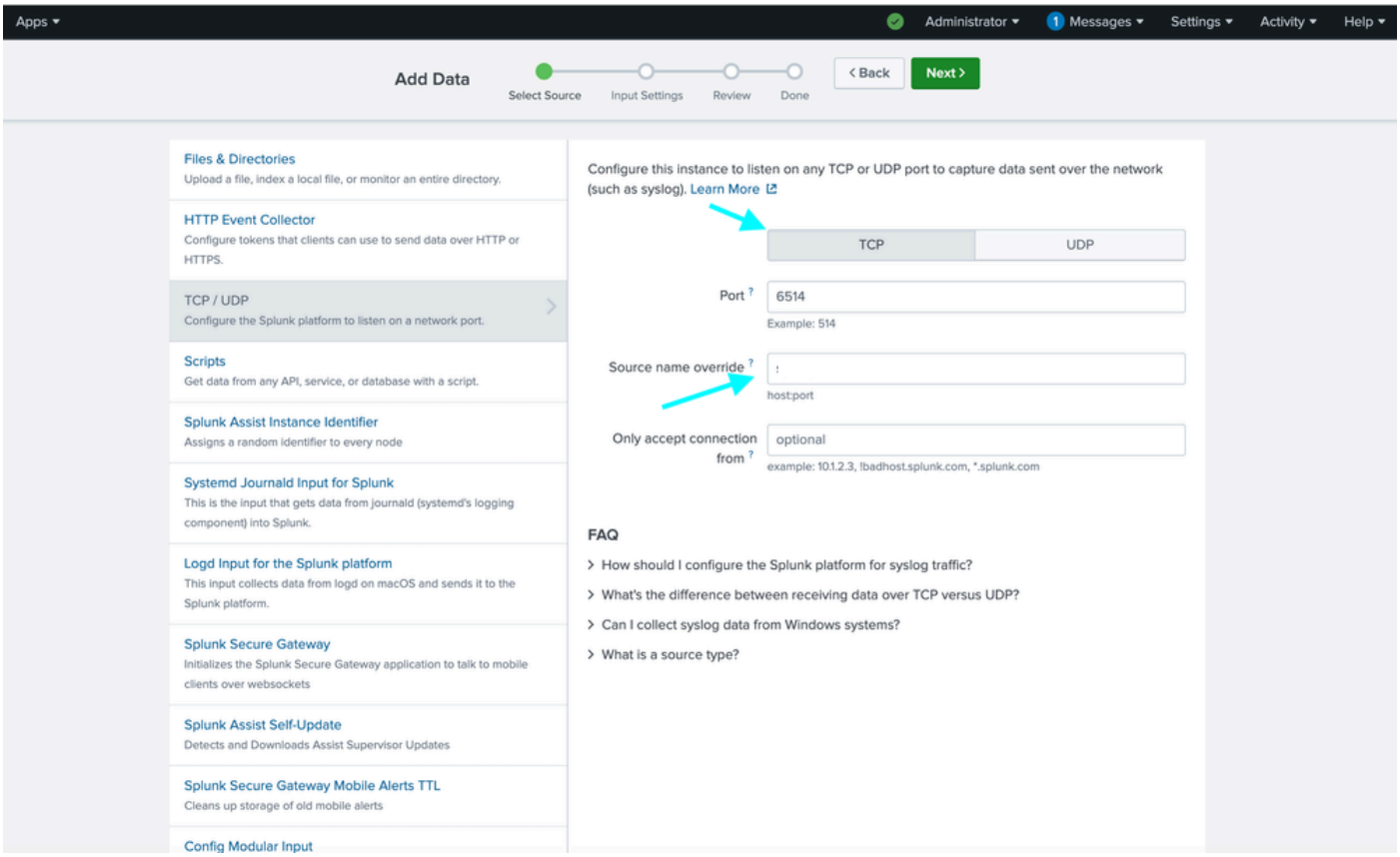


Passo 3: Na nova janela, selecione TCP, insira a porta de recebimento desejada, no exemplo de porta de imagem 6514, e insira "nome desejado" no campo Substituição do nome de origem.



Note: TCP 6514 é a porta padrão para syslog sobre TLS

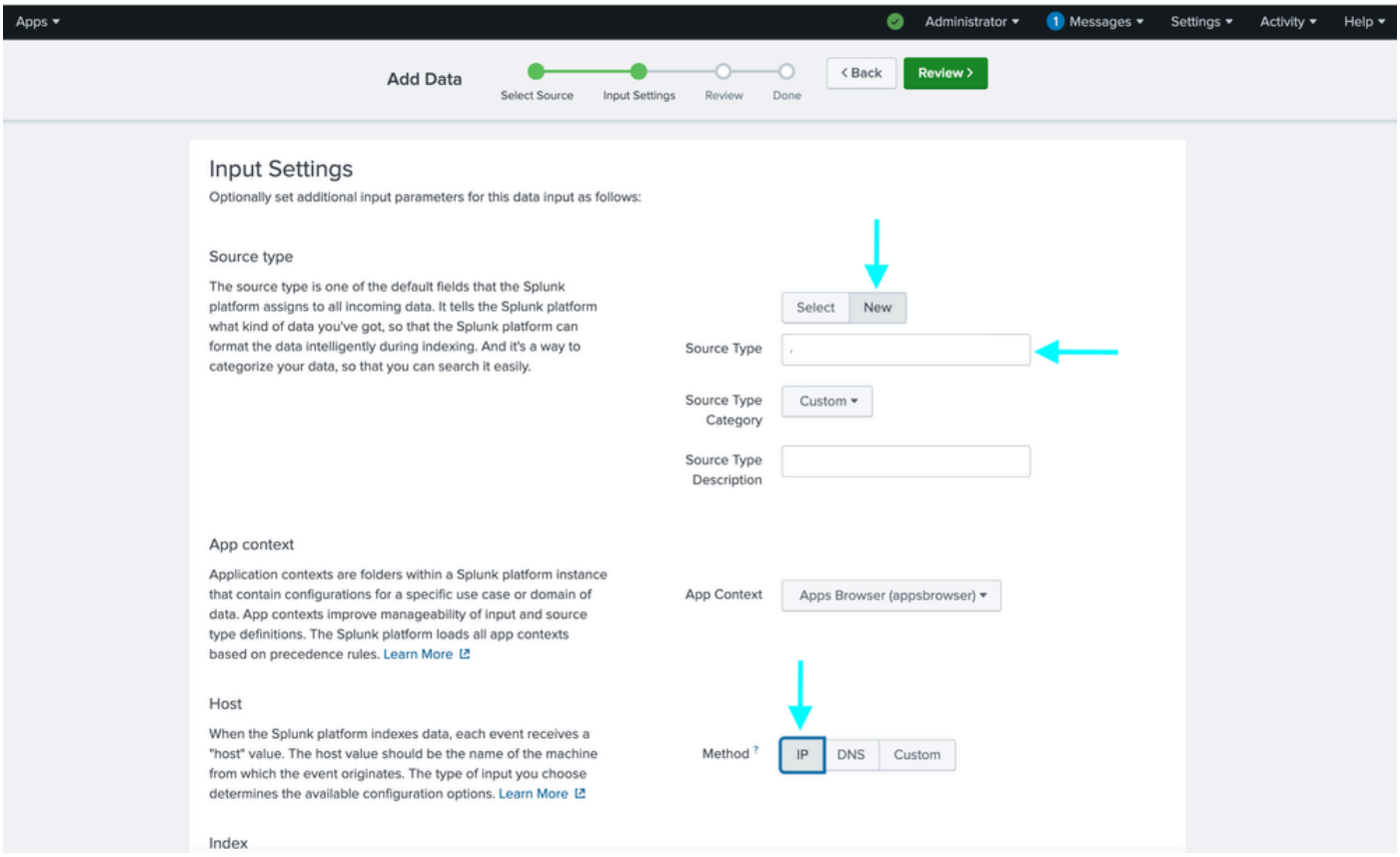
Passo 4: Ao concluir, clique no botão verde Avançar > na parte superior da janela.



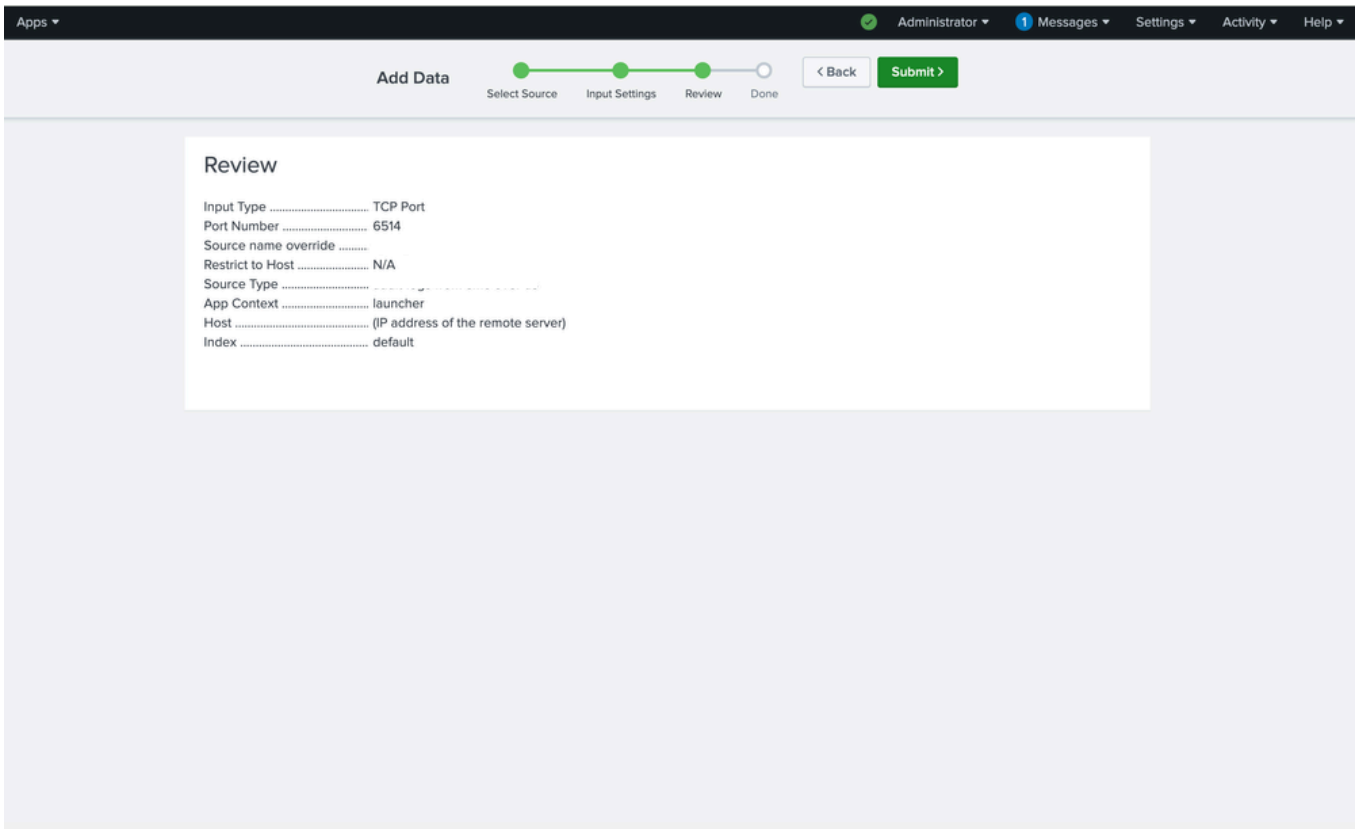
Passo 5: Na nova janela, selecione Novo na seção Tipo de origem, digite nome desejado no campo Tipo de origem.

Passo 6: Selecione IP para o Método na seção Host.

Passo 7: Ao concluir, selecione o botão verde Revisar > na parte superior da janela.



Passo 8: Na próxima janela, revise suas configurações e edite-as, se necessário. Depois de validar, clique no botão verde Submit > na parte superior da janela.



2. Gerar Certificado para Splunk

Passo 1: Usando uma máquina com o openssl instalado, execute o comando`sudo openssl req -x509 -newkey rsa:4096 -keyout server_key.pem -out server_cert.pem -sha256 -days 3650 -subj /CN=10.106.127.4`, substituindo o IP de exemplo de 10.106.127.4 pelo IP do dispositivo Splunk. Você é solicitado duas vezes a inserir uma frase secreta definida pelo usuário. Nos exemplos, os comandos estão sendo executados a partir da linha de comando da máquina de Splunk.

```
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:
```

Quando o comando é concluído, dois arquivos são gerados. Os arquivos server_cert.pem e server_key.pem.

```
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:
```

Passo 2: Alternar para usuário raiz.

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

Passo 3: Copie o certificado recém-gerado para o `/opt/splunk/etc/auth/` .

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

Etapa 4: anexe o arquivo spunkweb.cet com a chave privada.

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

Etapa 5: Alterar a propriedade do certificado de fragmento.

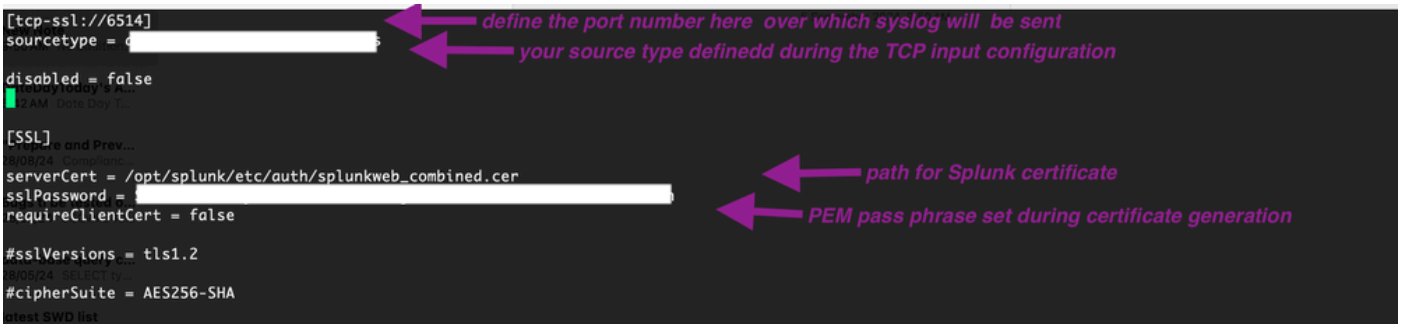
```
user@examplehost:~# chown 10777:10777/opt/splunk/etc/auth/splunkweb.cer
```

Etapa 6: Altere a permissão para o certificado de fragmento.

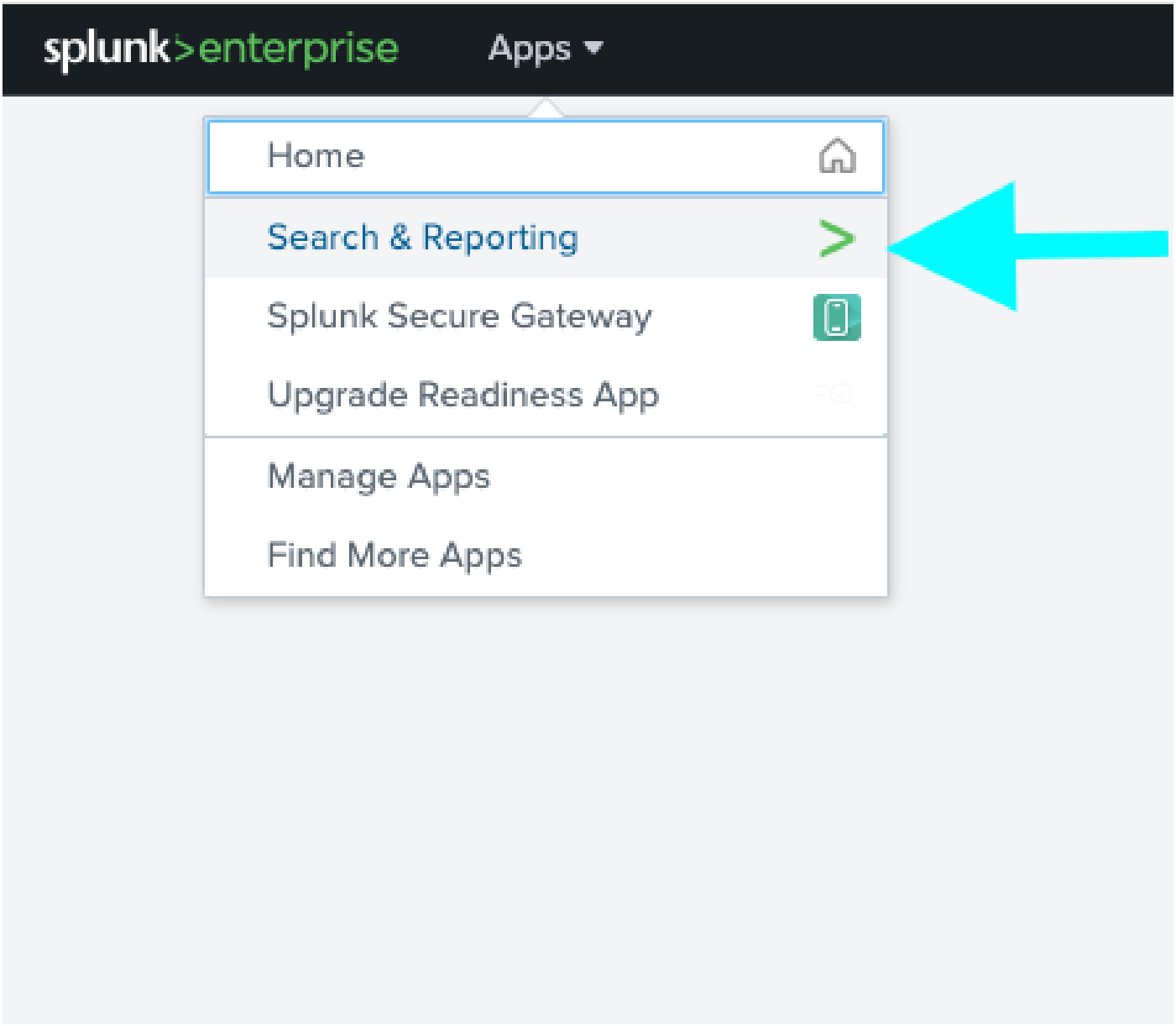
```
user@examplehost:~# chmod 600/opt/splunk/etc/auth/splunkweb.cer
```

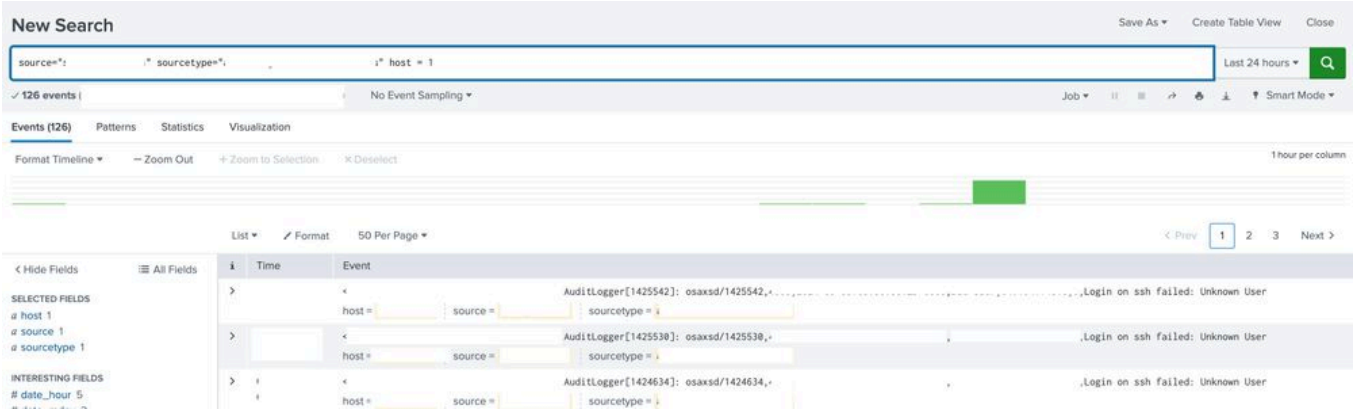
Etapa 7: crie um novo arquivo input.conf.

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



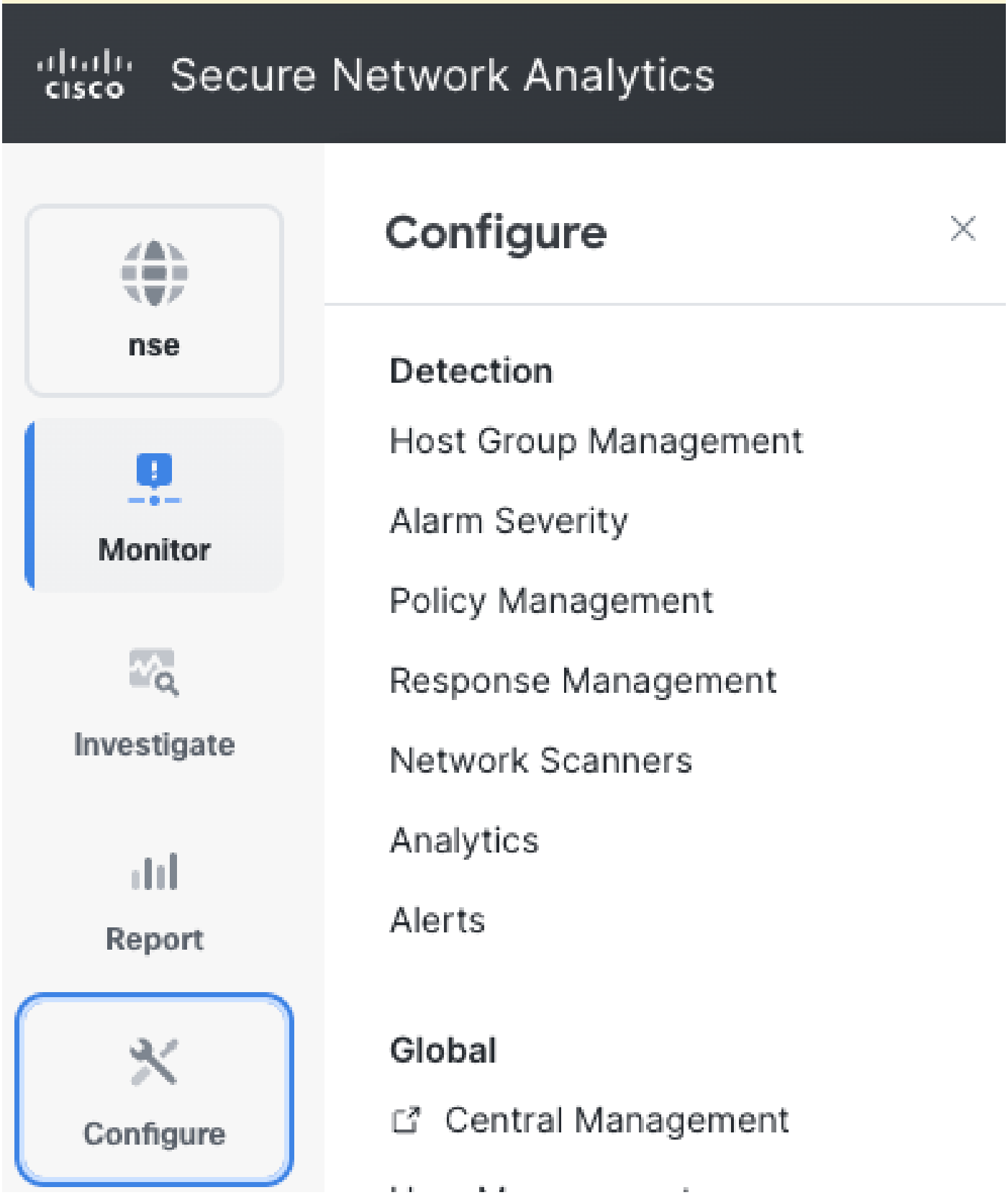
Passo 8: Verifique os syslogs usando pesquisar.



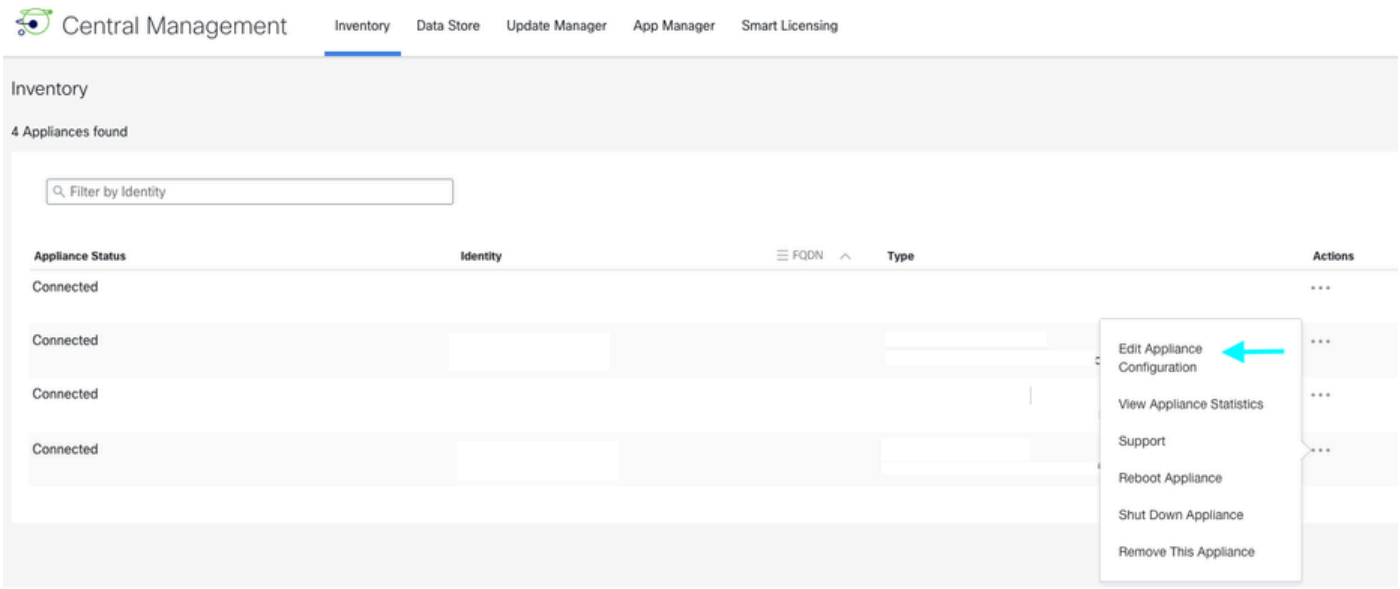


3. Configurar o destino do log de auditoria em redes SNA

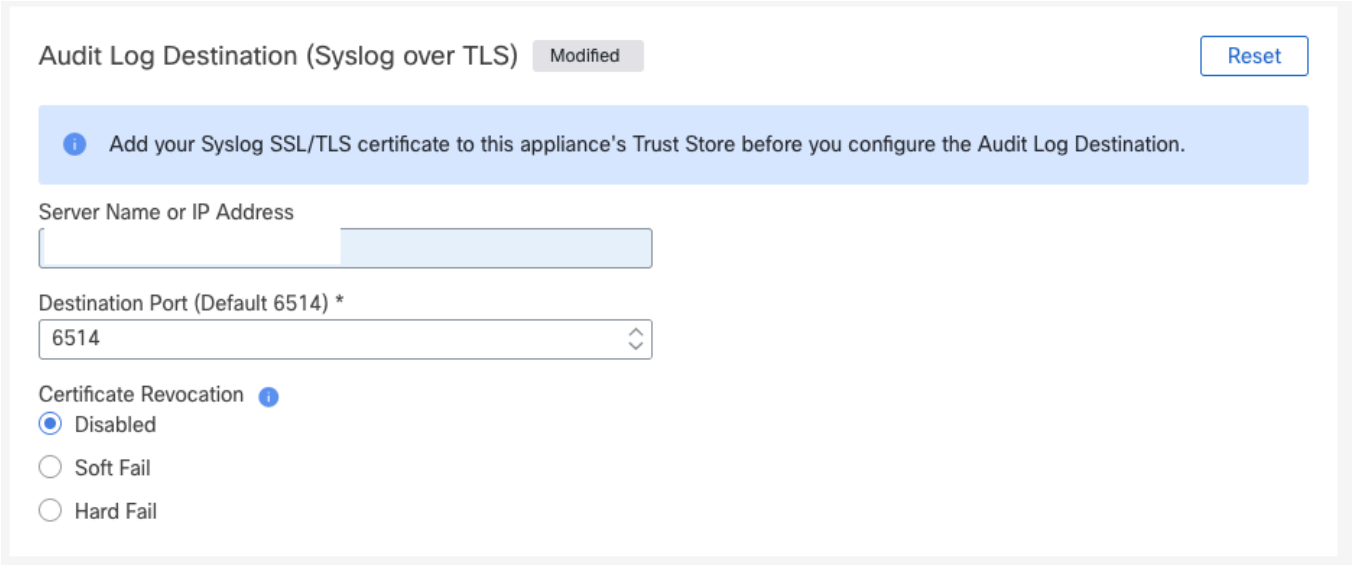
Passo 1: Faça login na interface do usuário do SMC e navegue para Configure > Central Management.



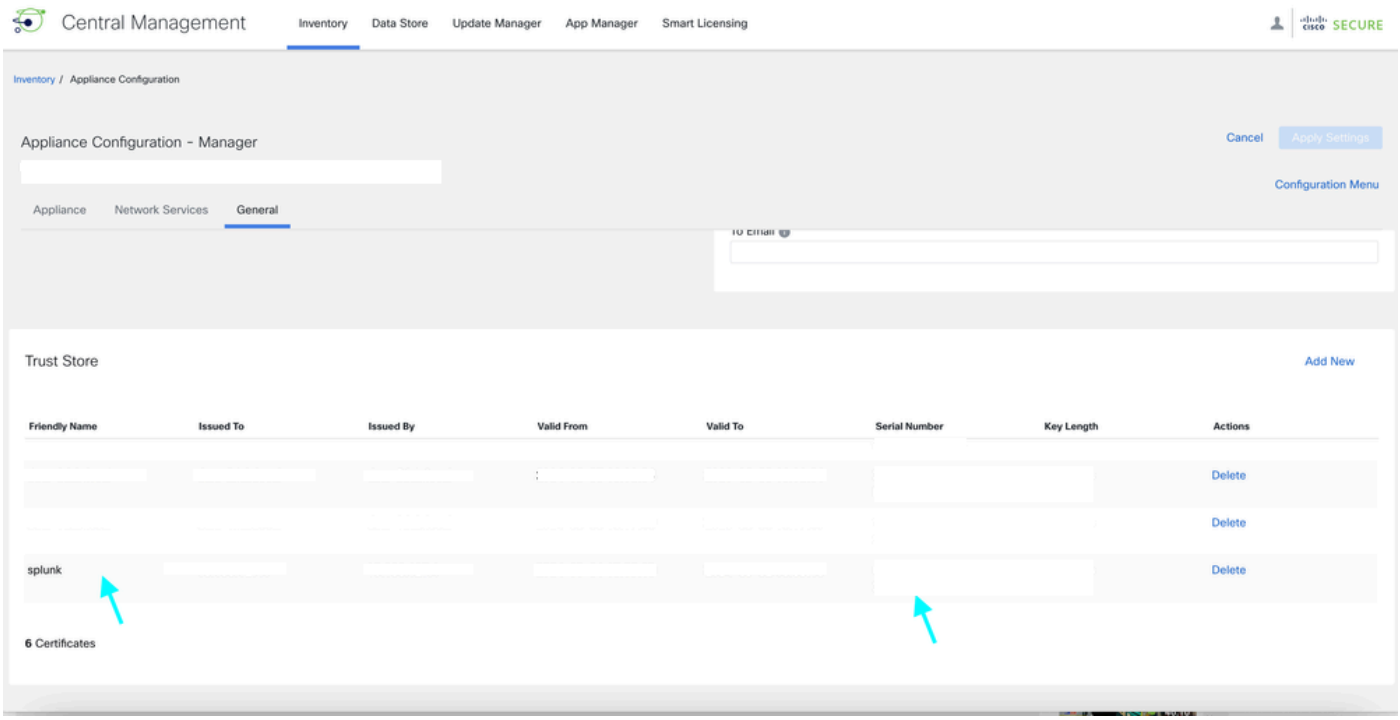
Passo 2: Clique no ícone de reticências do dispositivo SNA desejado e selecione Editar configuração do dispositivo.



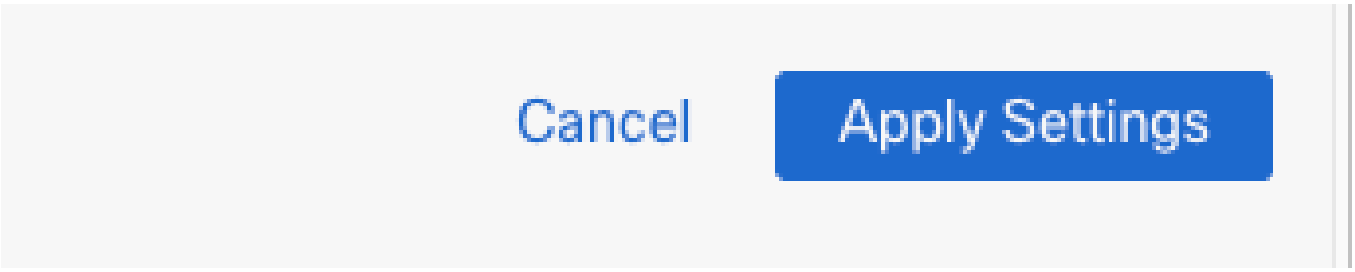
Passo 3: Navegue até a guia Network Services e insira os detalhes de Audit Log Destination (Syslog over TLS).



Passo 4: Navegue até a guia Geral, role para baixo até a parte inferior Clique em Adicionar novo para carregar o certificado Splunk criado anteriormente chamado server_cert.pem.

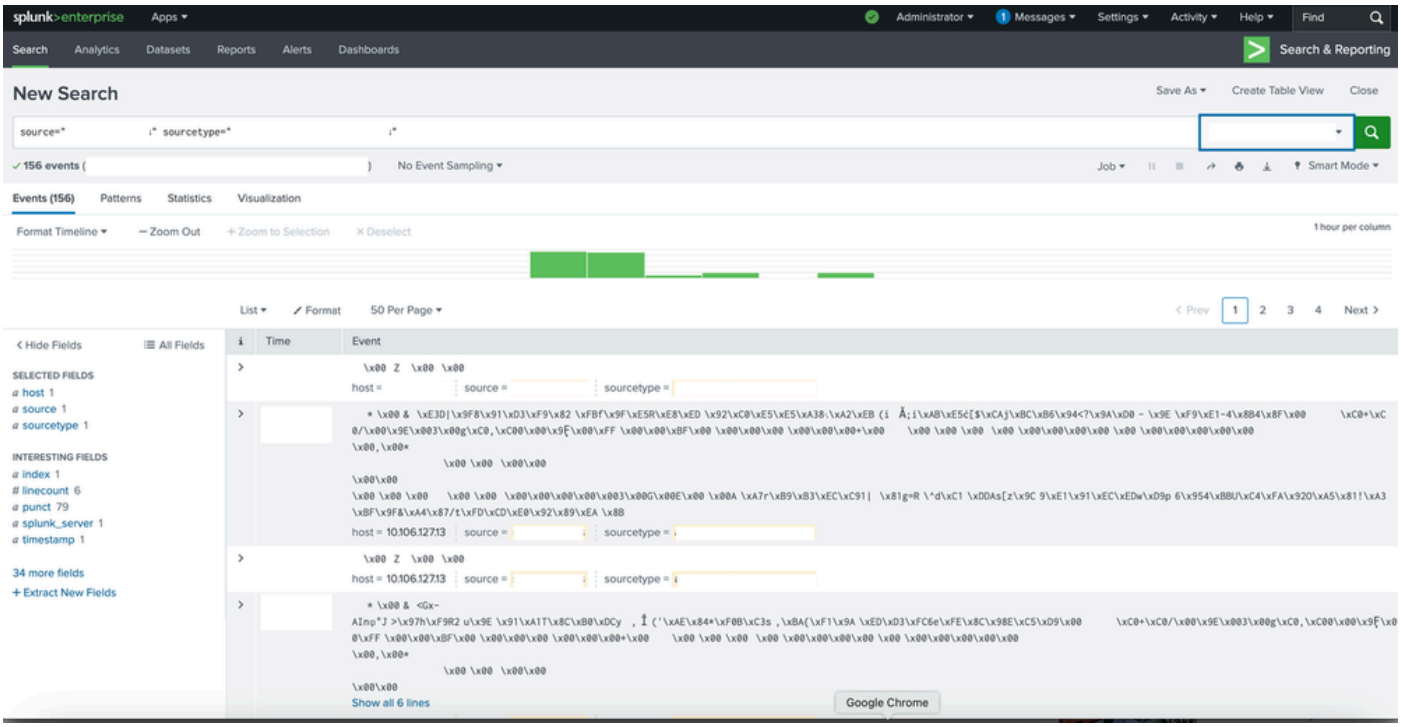


Passo 5: Clique em Aplicar configurações.



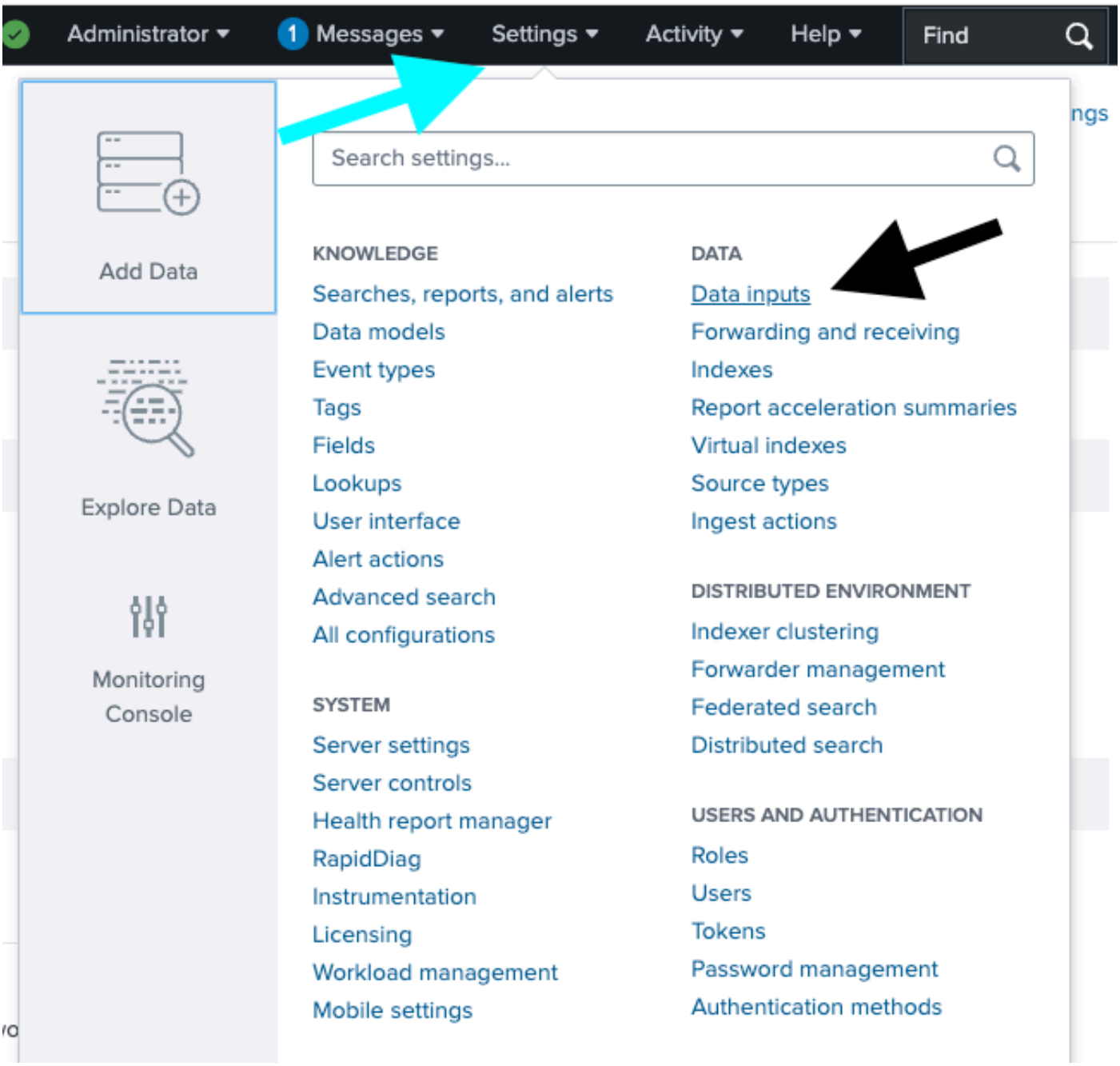
Troubleshooting

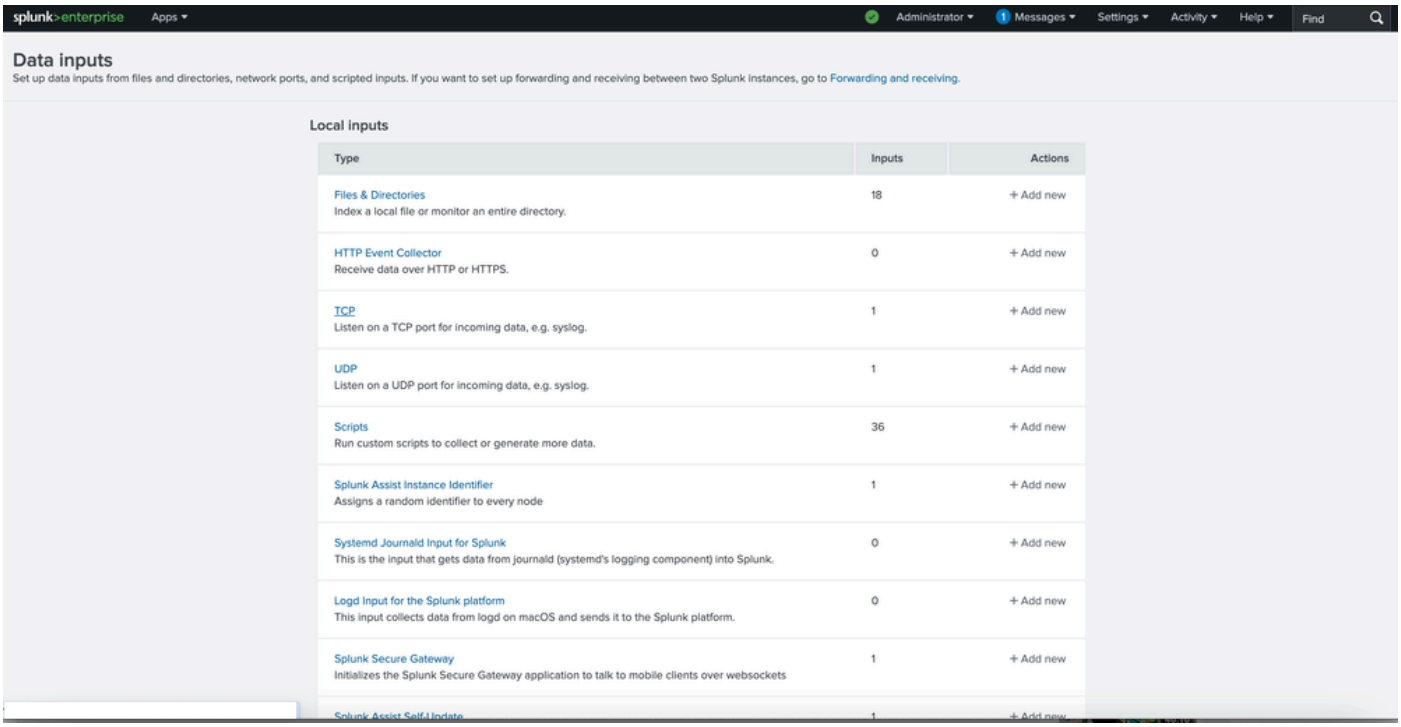
Pode haver toda a confusão aparecendo na pesquisa.

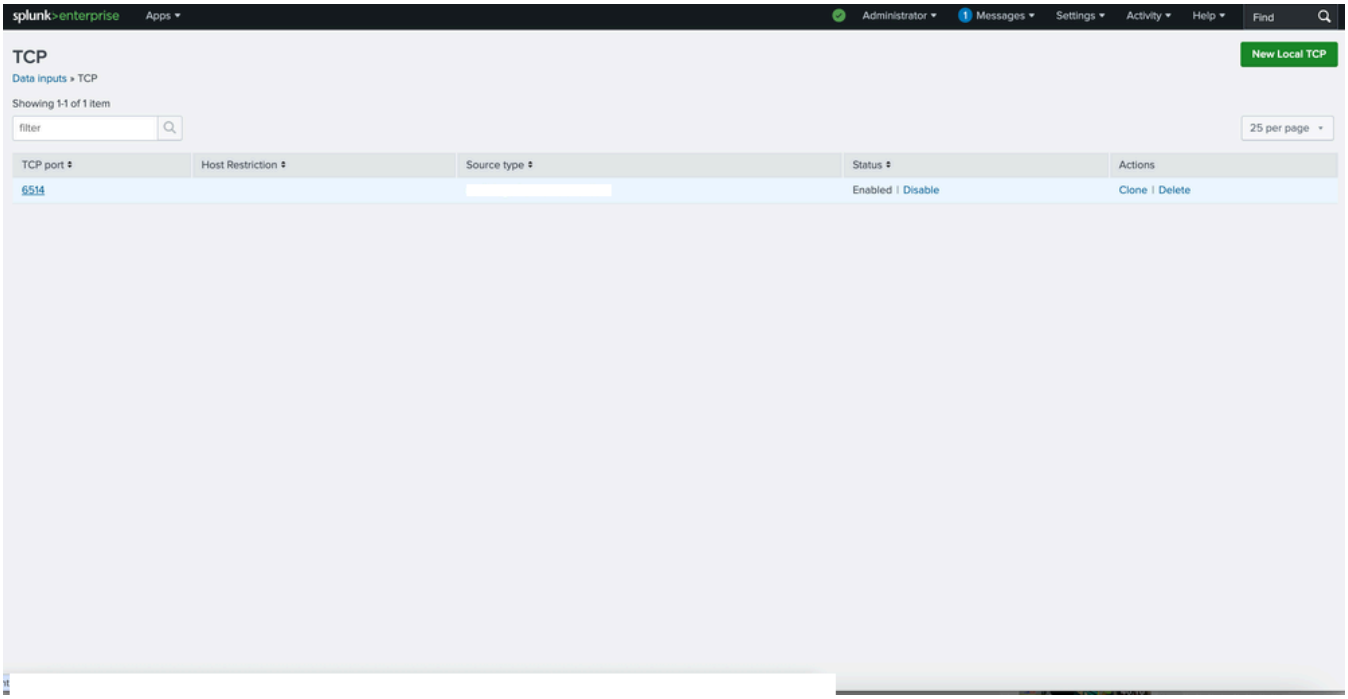


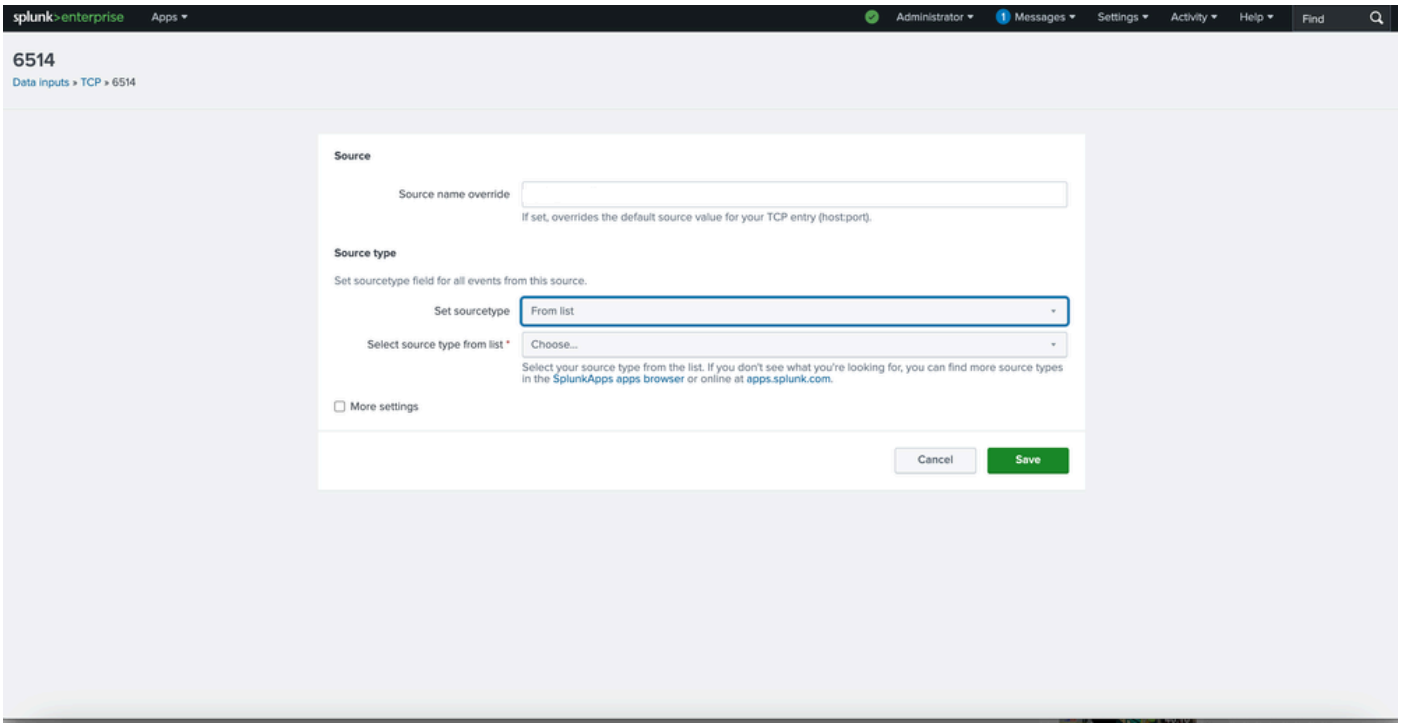
Solução:

Mapeie a entrada para o tipo de origem correto.


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

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.