Respons Management configureren om Syslog Events naar Splunk te sturen

Inhoud

Inleiding

Dit document beschrijft hoe u de functie Secure Analytics Response Management kunt configureren om gebeurtenissen via syslog naar een derde partij zoals Splunk te verzenden.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

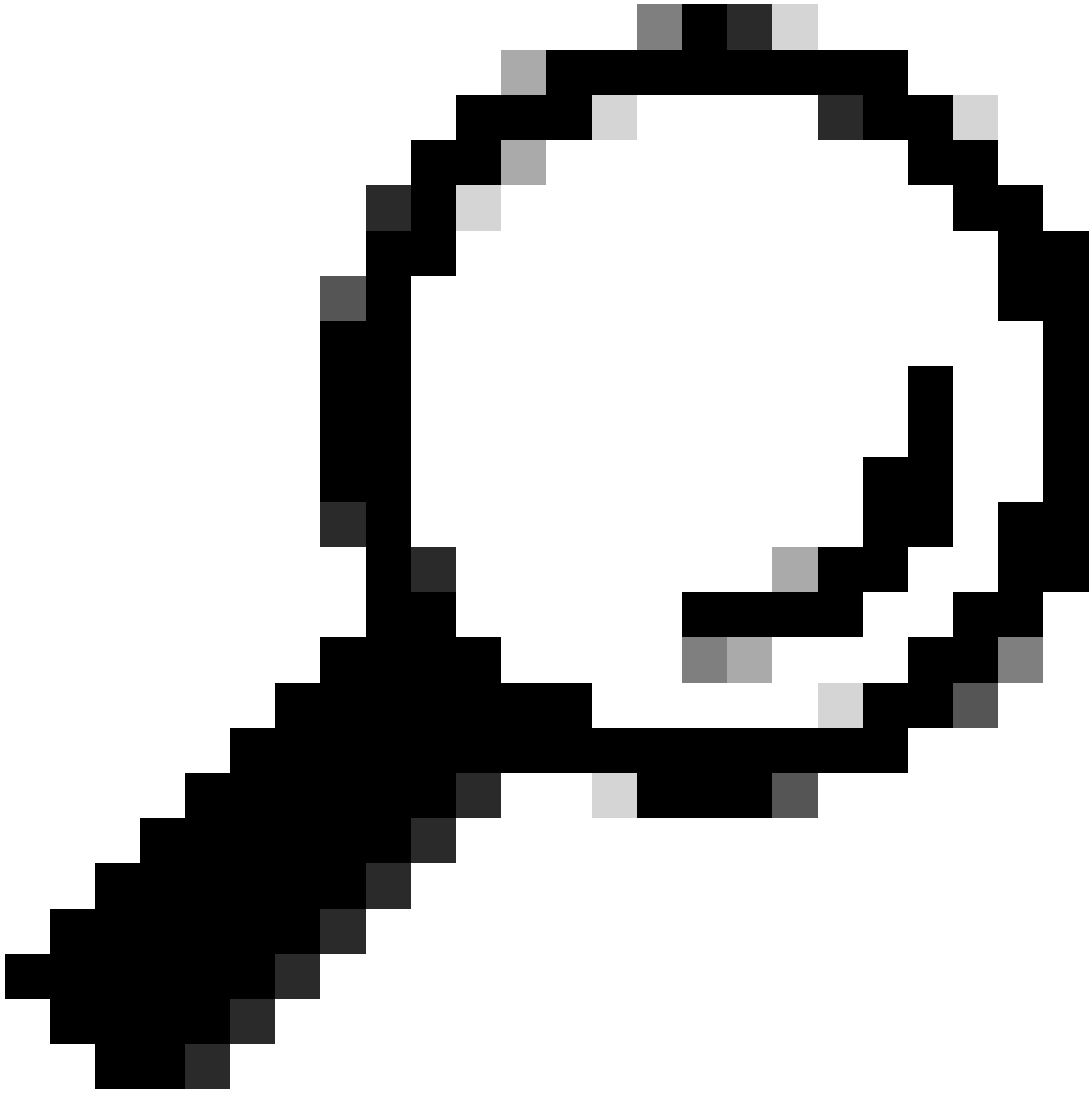
- Secure Network Analysis Response Management.
- Splunk Syslog

Gebruikte componenten

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

- Secure Network Analytics (SNA)-implementatie die ten minste één Manager-applicatie en één Flow Collector-applicatie bevat.
- Splunk-server geïnstalleerd en toegankelijk via 443-poorts.

Configureer syslog op SNA via UDP 514 of aangepaste gedefinieerde poort



Tip:Zorg ervoor dat UDP/514, TCP/6514 of een aangepaste poort die u voor syslog kiest, is toegestaan op firewalls of tussenapparaten tussen SNA en Splunk.

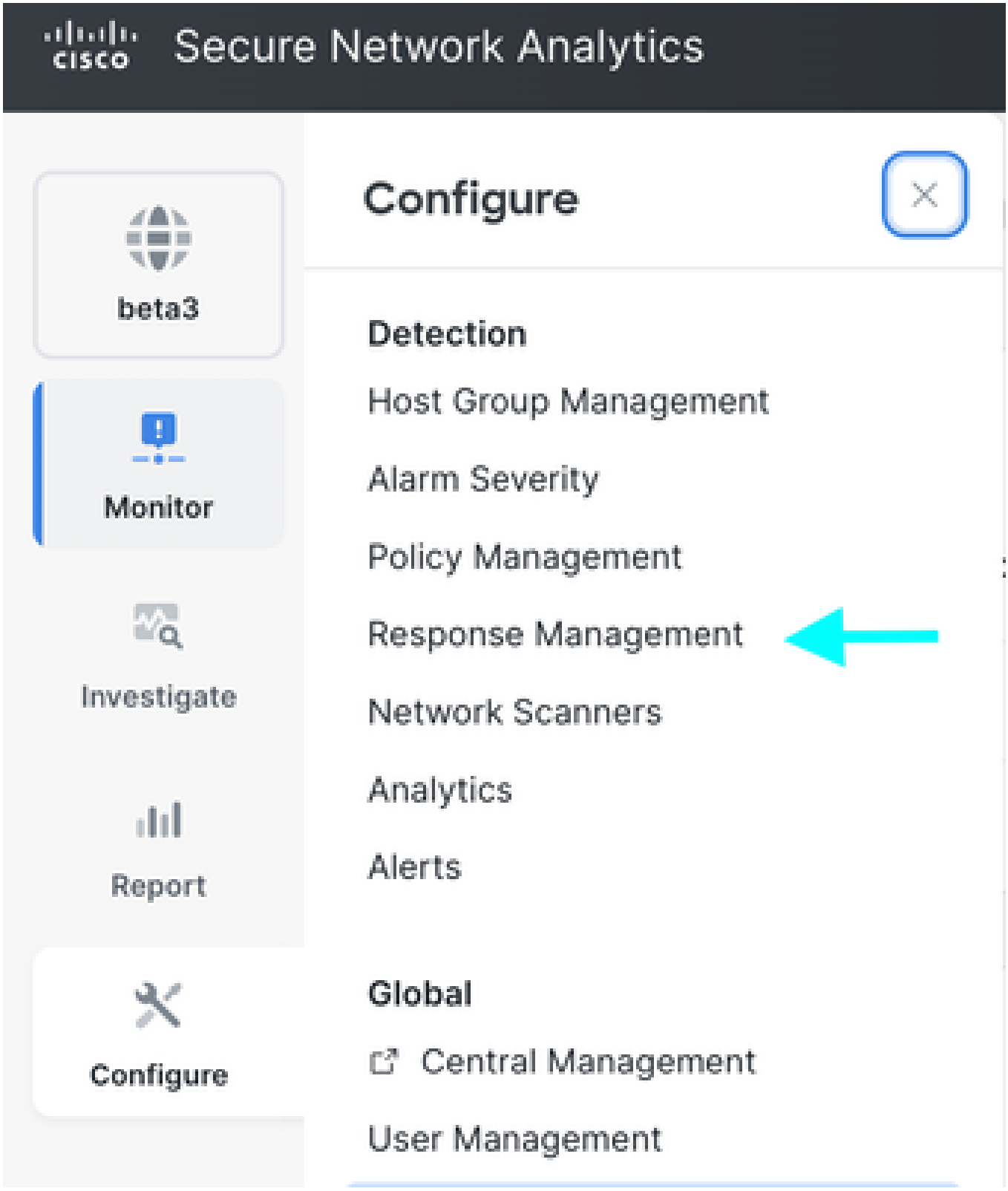
1.SNA-responsbeheer

De component Response Management van Secure Analytics (SA) kan worden gebruikt voor de configuratie van regels, acties en syslog-bestemmingen.

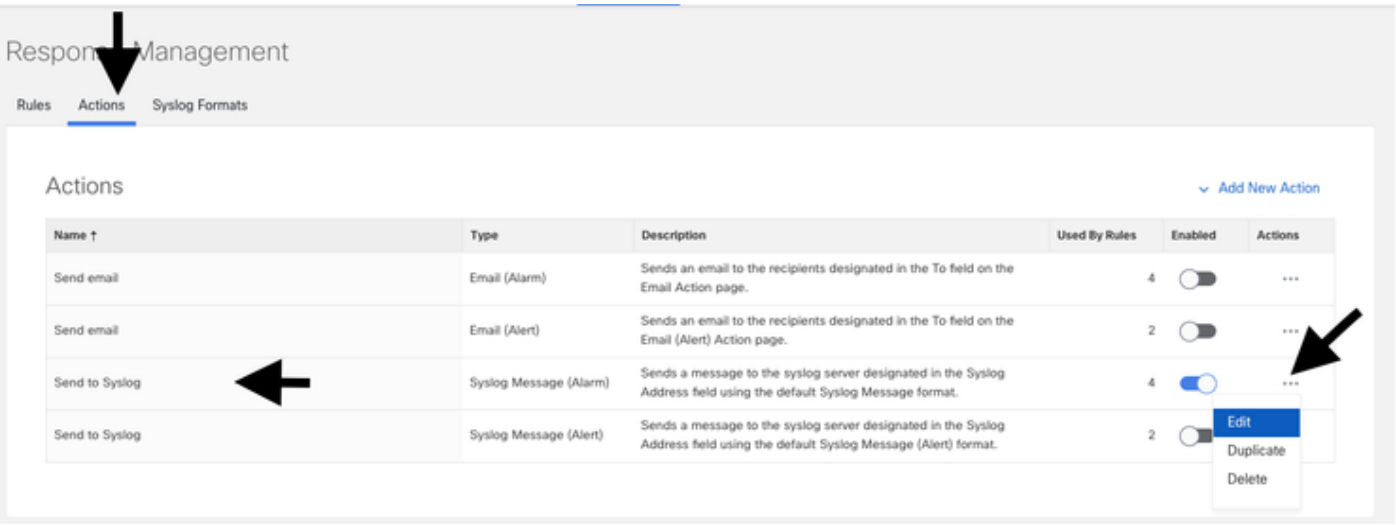
Deze opties moeten zo worden geconfigureerd dat Secure Analytics-alarmen naar andere

bestemmingen worden verzonden/doorgestuurd.

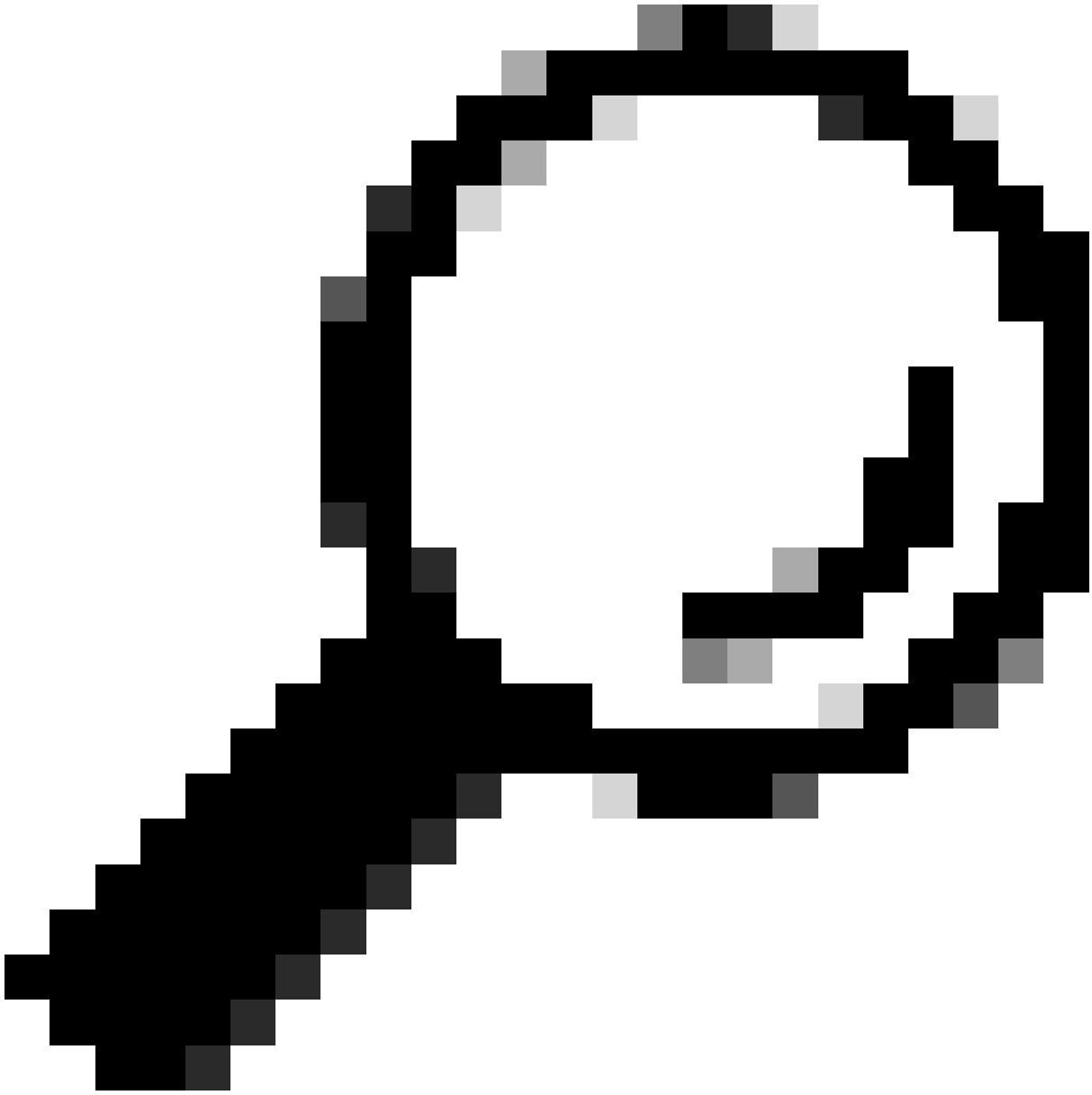
Stap 1: Log in op het SA Manager apparaat en navigeer om te configureren > Detectie Response Management.



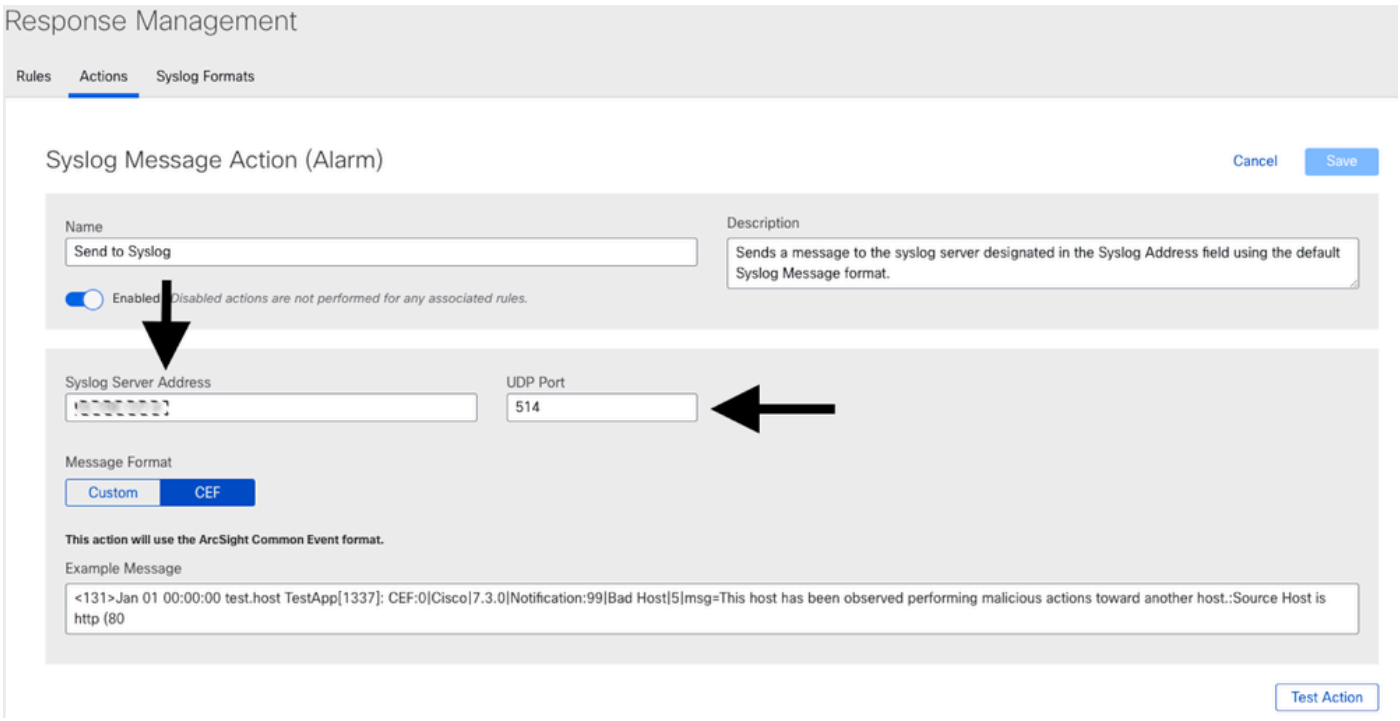
Stap 2: Op de nieuwe pagina navigeer naar het tabblad Acties, lokaliseer de standaard Verzend naar Syslog regel item en klik op de ellips (...) in de Action kolom, en vervolgens Bewerken.



Stap 3: Voer het gewenste doeladres in het veld Syslog Server Address in en de gewenste bestemmingshaven in het veld UDP Port. Selecteer CEF in het berichtenformaat.
Stap 4: Als u klaar bent, klikt u op de knop Opslaan in de rechterbovenhoek.



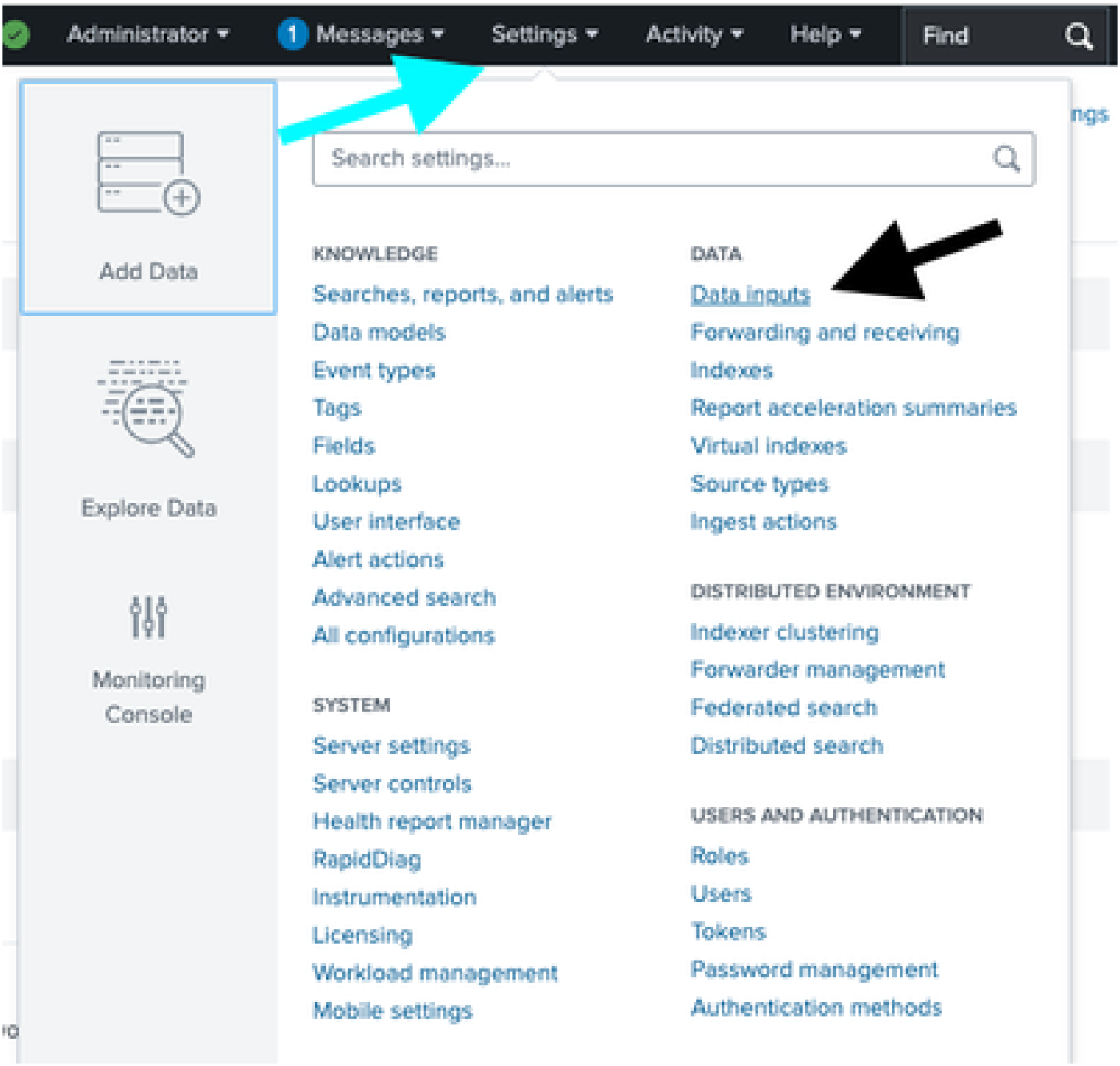
Tip: De standaard UDP-poort voor syslog is 514



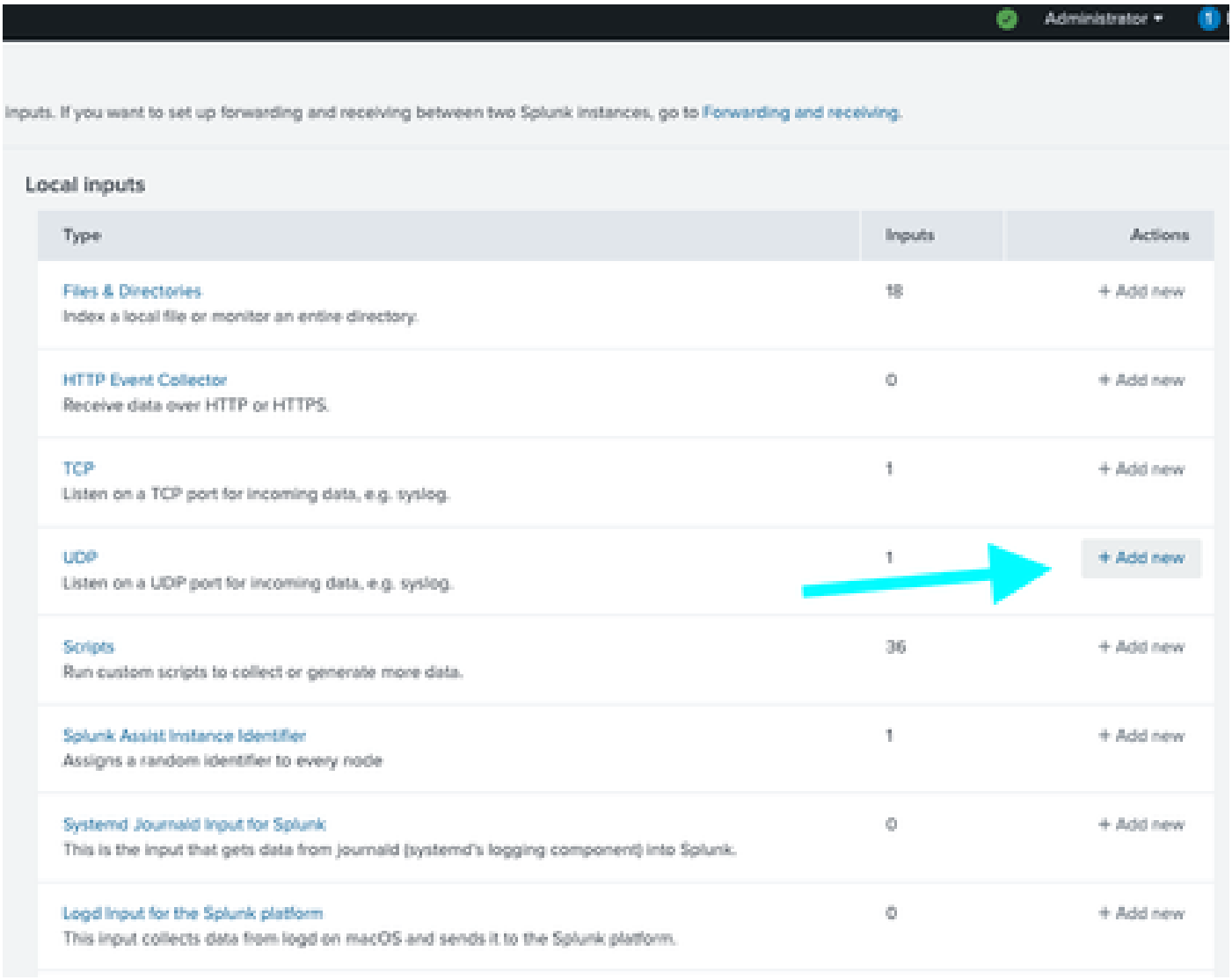
2. Splunk configureren voor ontvangst van SNA-syslogs via UDP-poort

Na het toepassen van uw veranderingen op Secure Network Analytics Manager Web UI, moet u gegevensinvoer in Splunk configureren.

Stap 1: Log in op Splunk en navigeer naar Instellingen > Gegevens toevoegen > Gegevens invoeren.

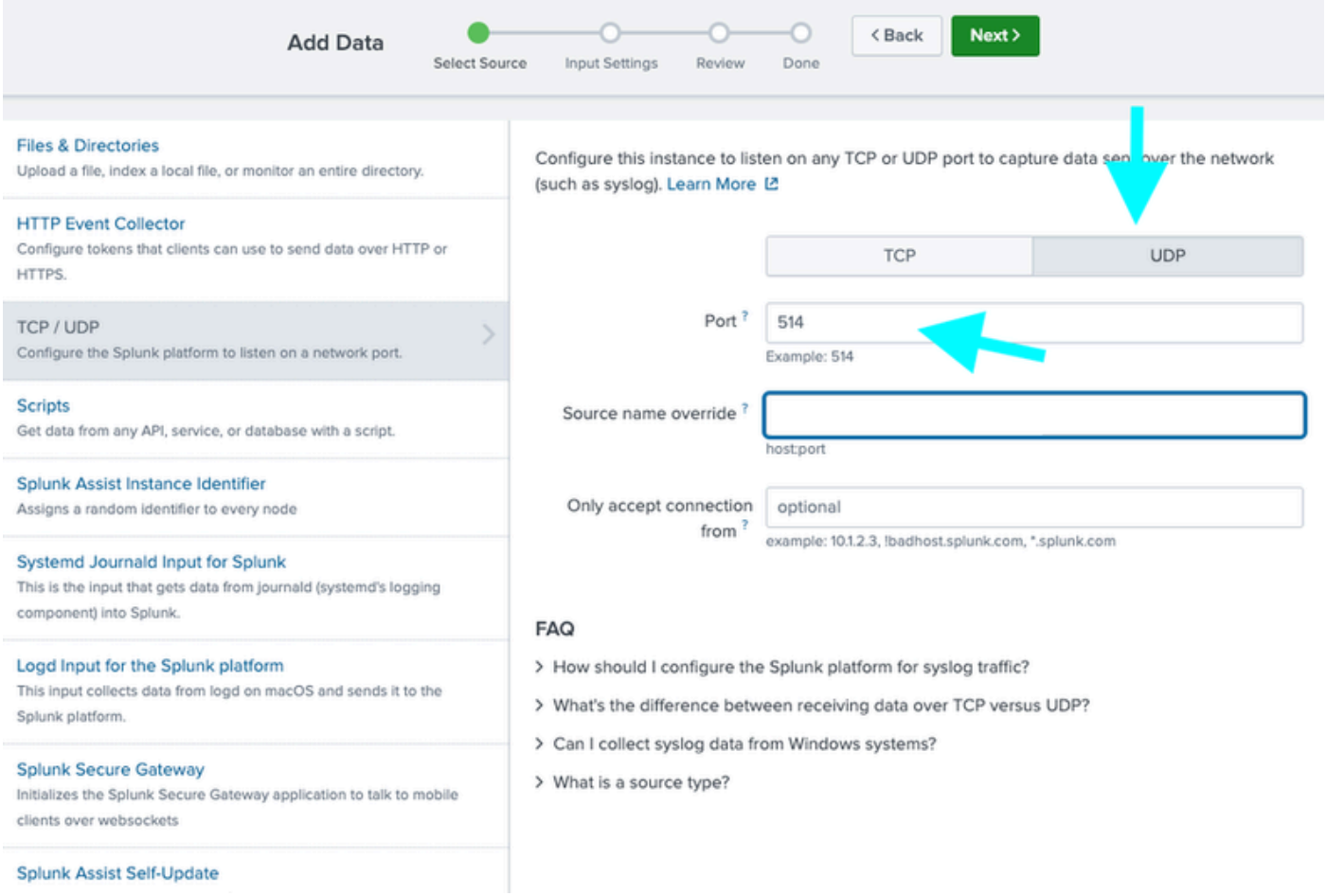


Stap 2: Zoek de UDP-lijn en selecteer +Add new.



Stap 3: Op de nieuwe pagina selecteert u UDP, voert u de ontvangende poort in, zoals 514 in het veld Port.
Stap 4: In het veld Bronnaam negeren voert u desired name of source.

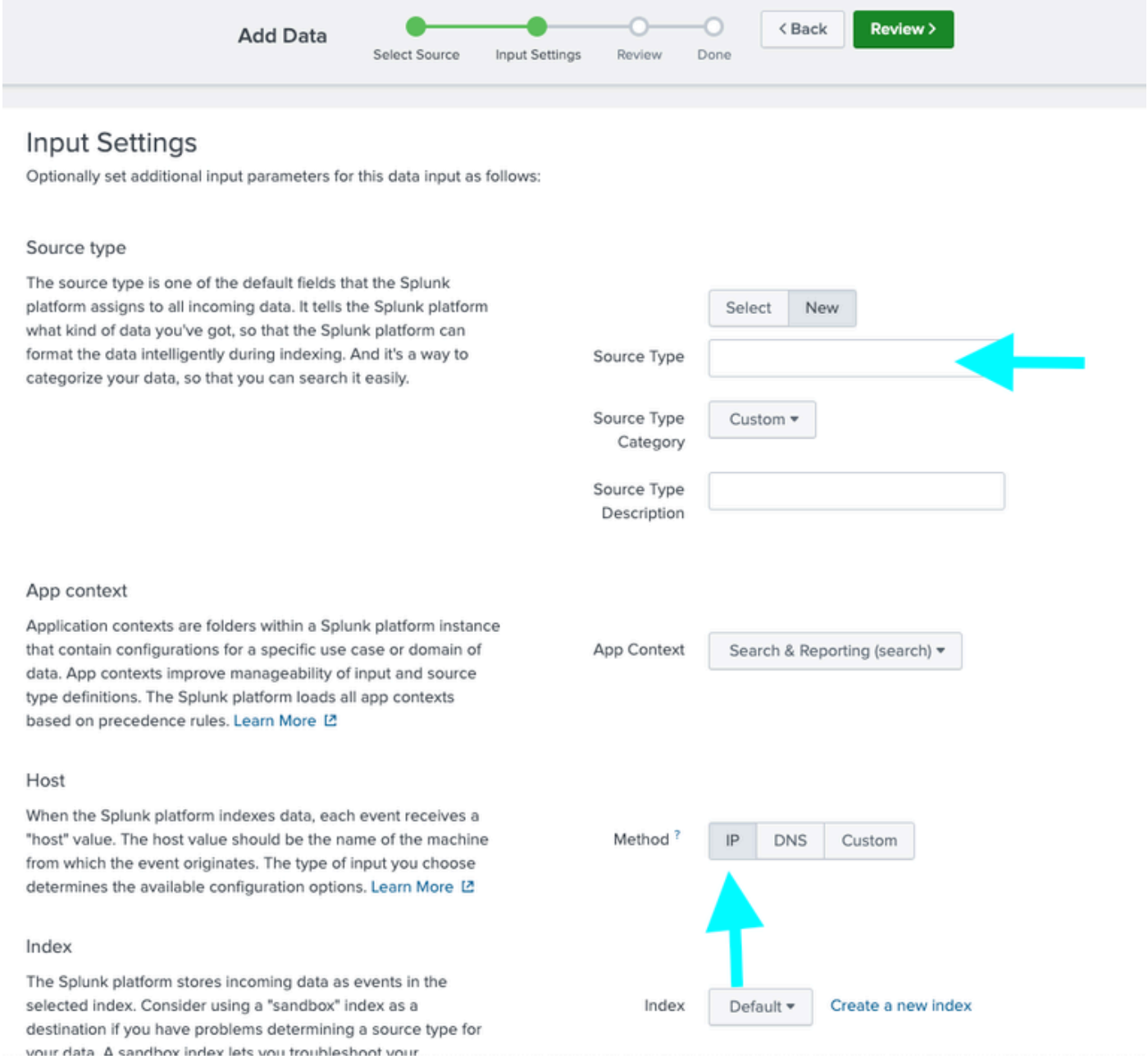
Stap 5: Als u klaar bent, klikt u op de groene knop Volgende **>** boven in het venster.



Stap 6: Op de volgende pagina zoekt switch naar Nieuwe optie het veld Brontype en voert u desired source .

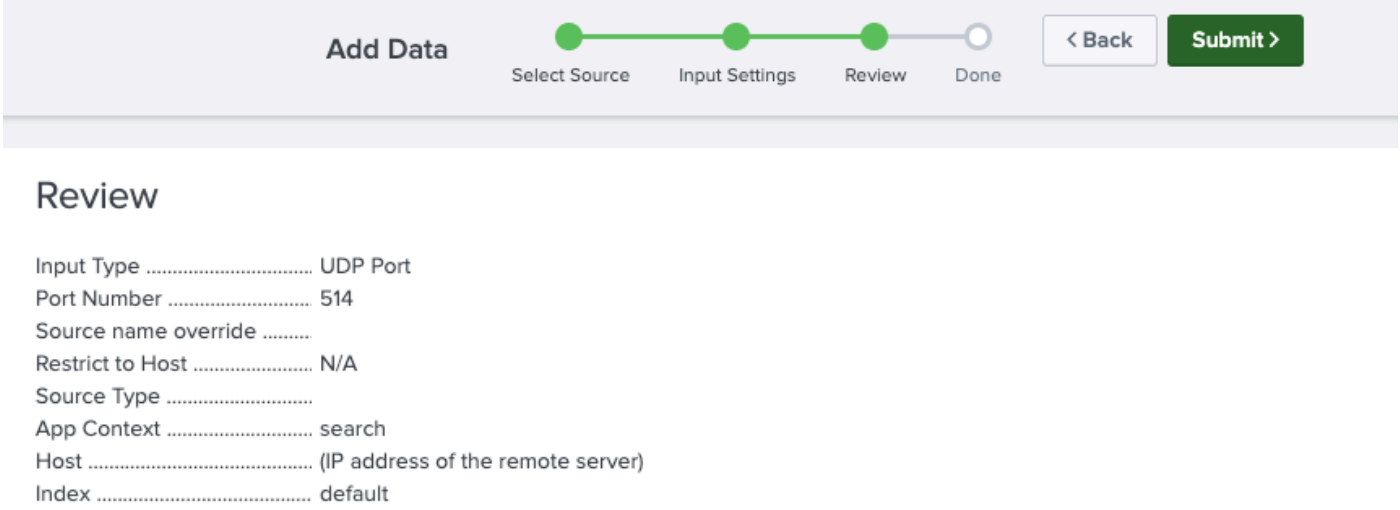
Stap 7: Selecteer IP voor de methode.

Stap 8: Klik op de groene toets Review > boven in het scherm.

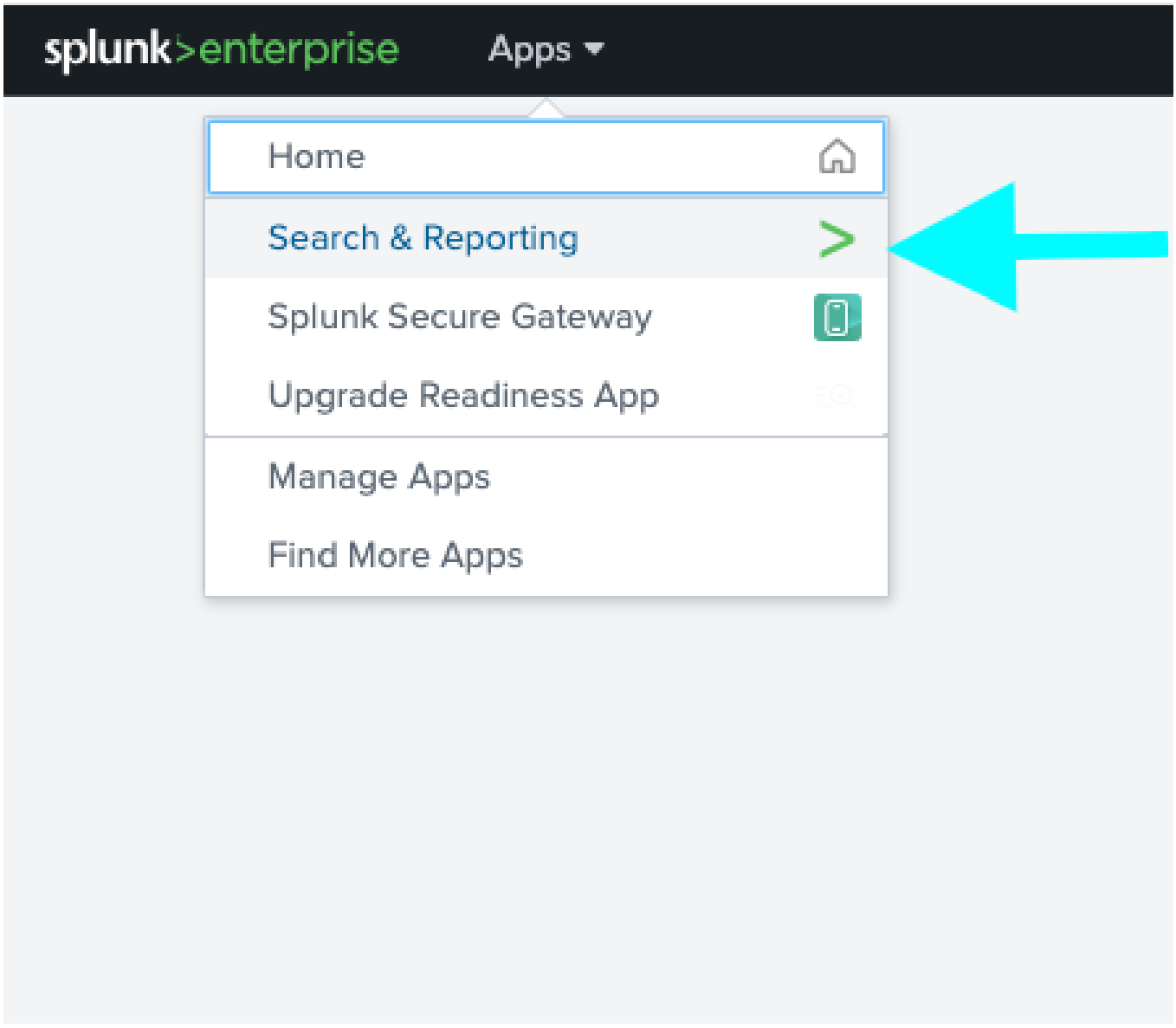


Stap 9: Controleer in het volgende venster uw instellingen en bewerk deze indien nodig.

Stap 10: Klik na bevestiging op de groene knop Indienen > boven in het venster.

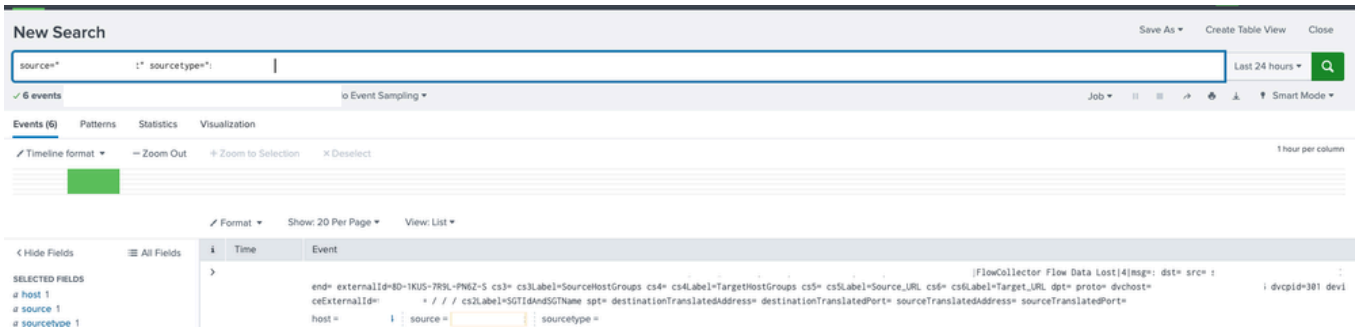


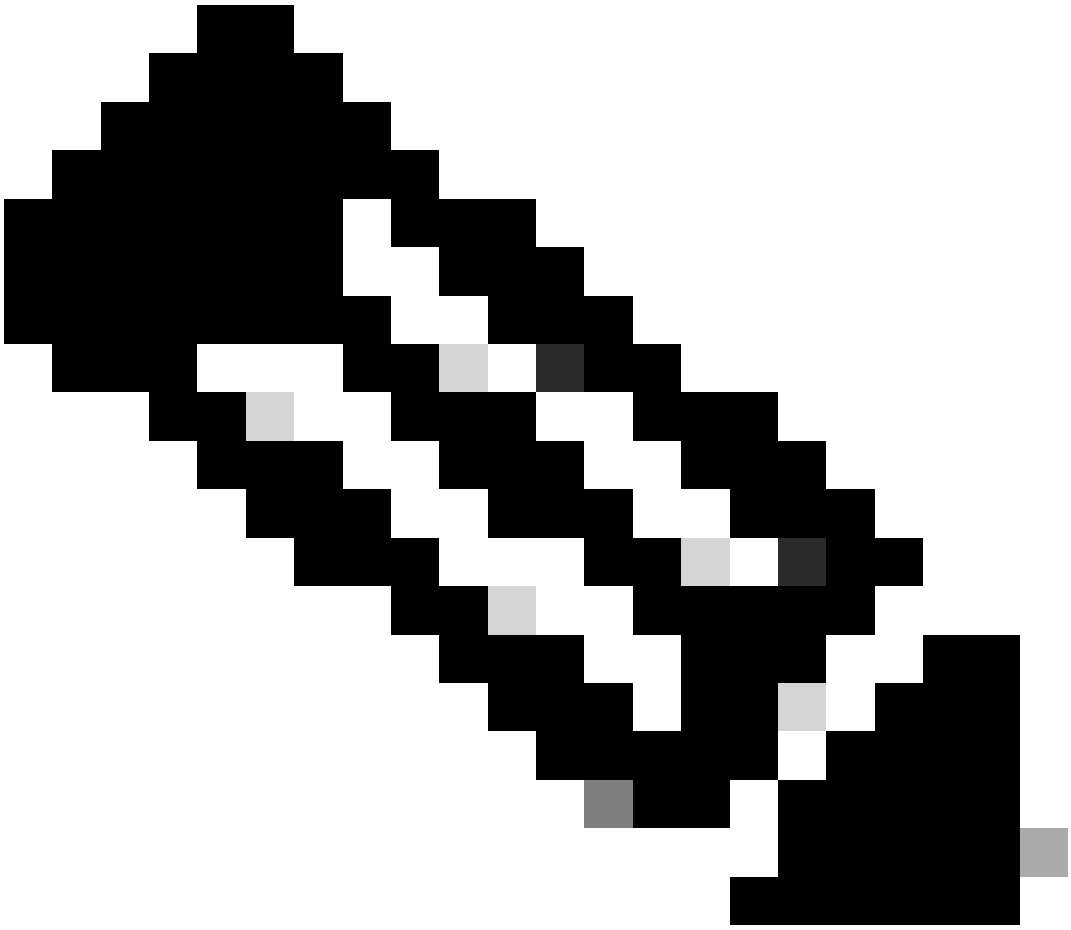
Stap 11: Ga naar Apps > Zoeken & Rapporteren in de Web UI.



Stap 12: Gebruik op de pagina Zoeken het filter`source="As_configured" sourcetype="As_configured"`om

logbestanden te vinden die zijn ontvangen.



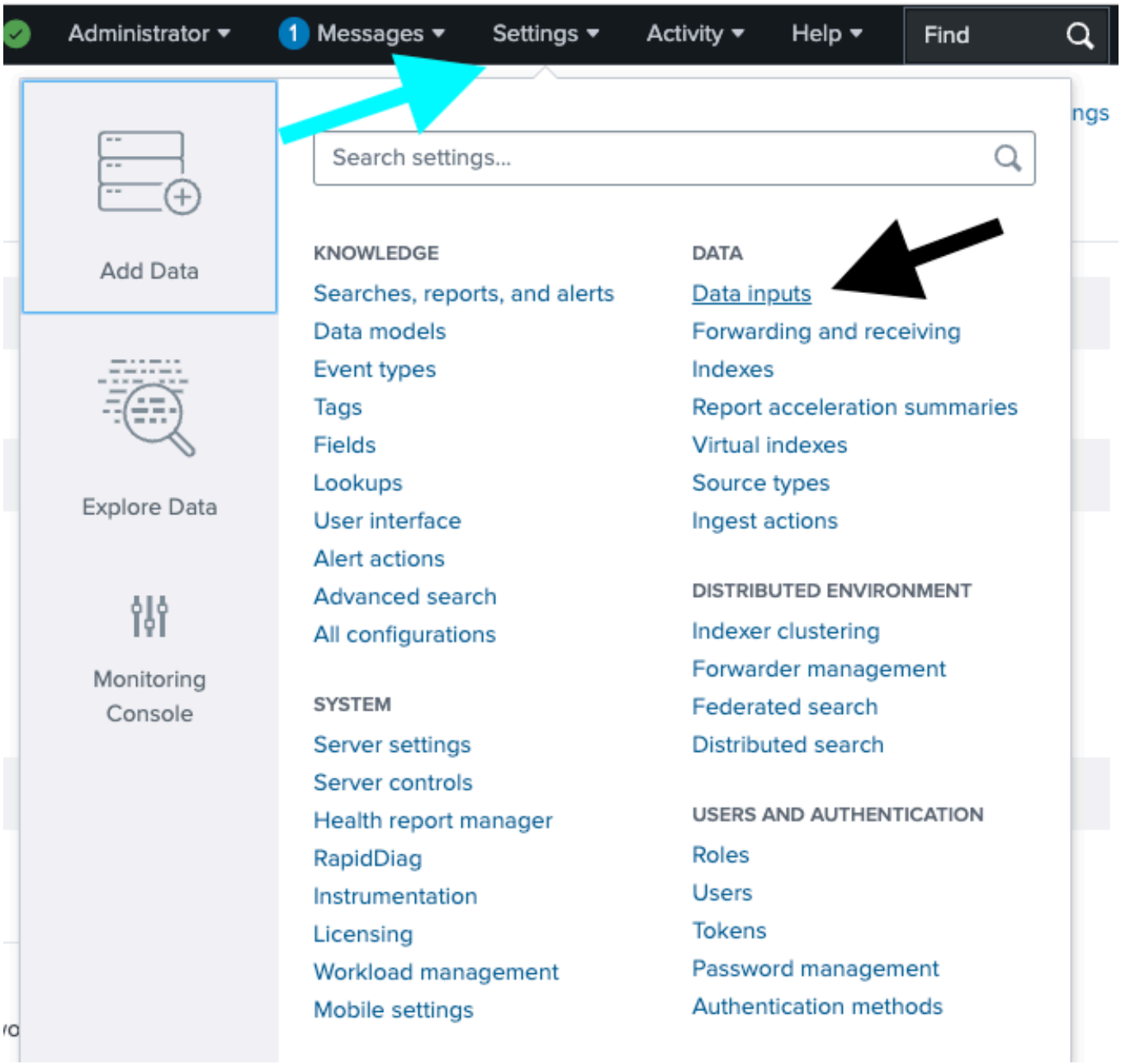


Opmerking: Zie Stap 4 voor de bron
Zie Stap 6 voor source_type

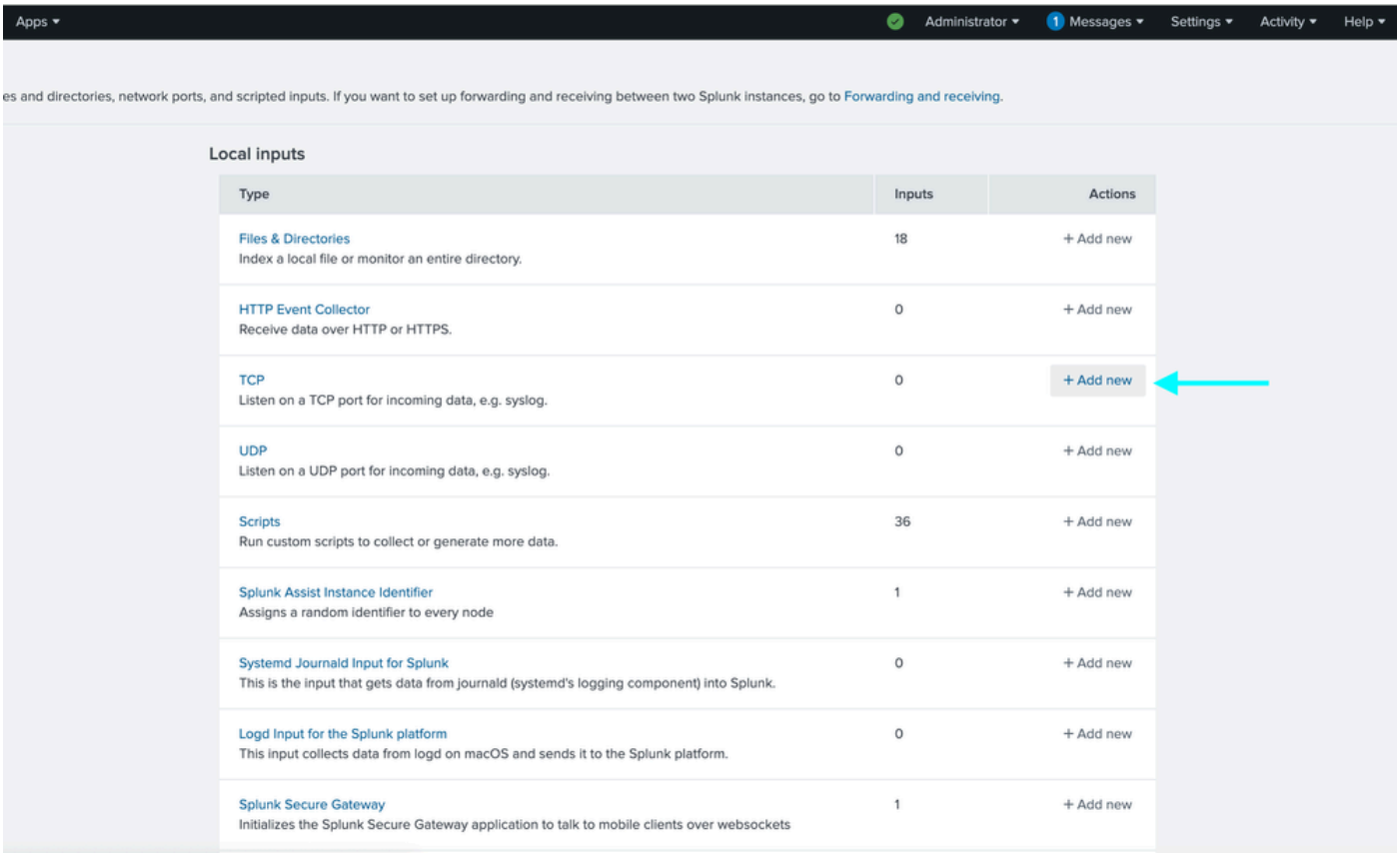
Configureer syslog op SNA over TCP-poort 6514 of aangepaste gedefinieerde poort

1.Splunk configureren voor ontvangst van SNA-auditlogbestanden via TCP-poort

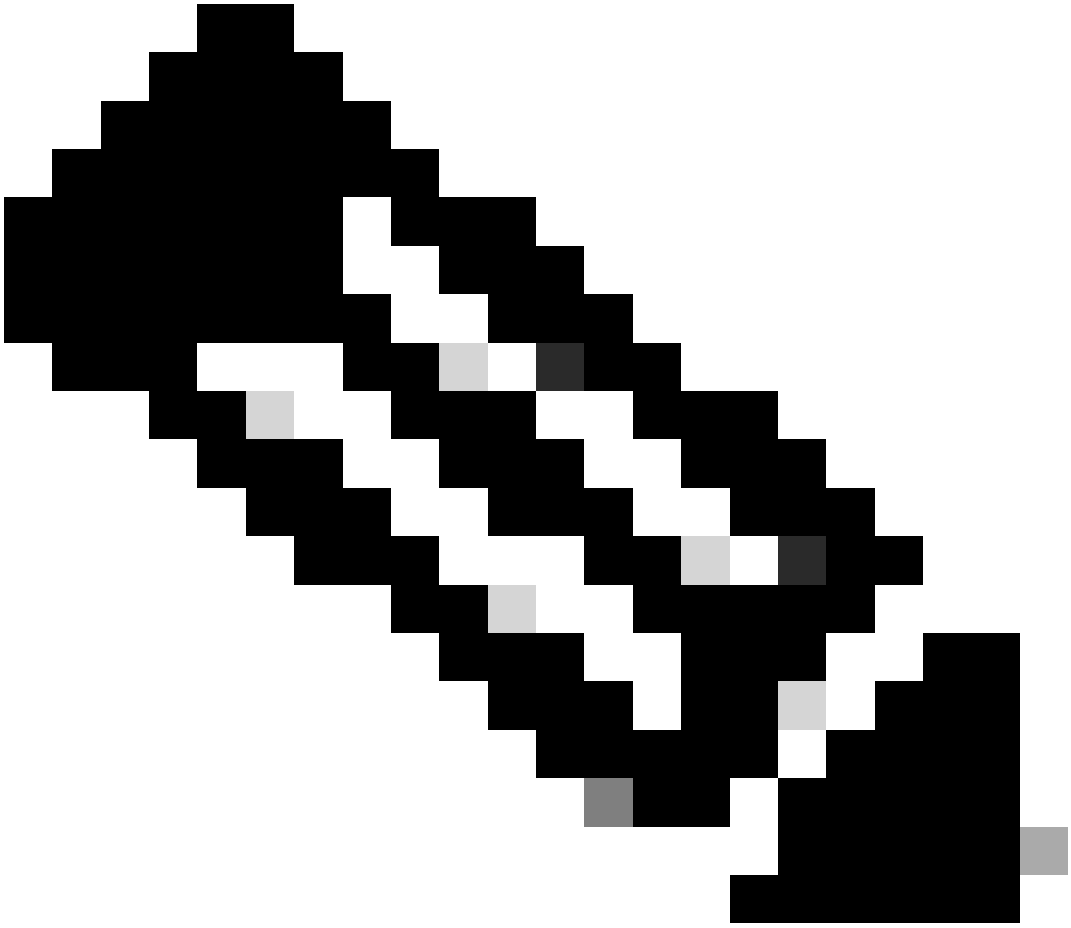
Stap 1: Ga in de Splunk UI naar Instellingen > Gegevens toevoegen > Gegevens invoeren.



Stap 2: Zoek de TCP regel en selecteer + Add new.

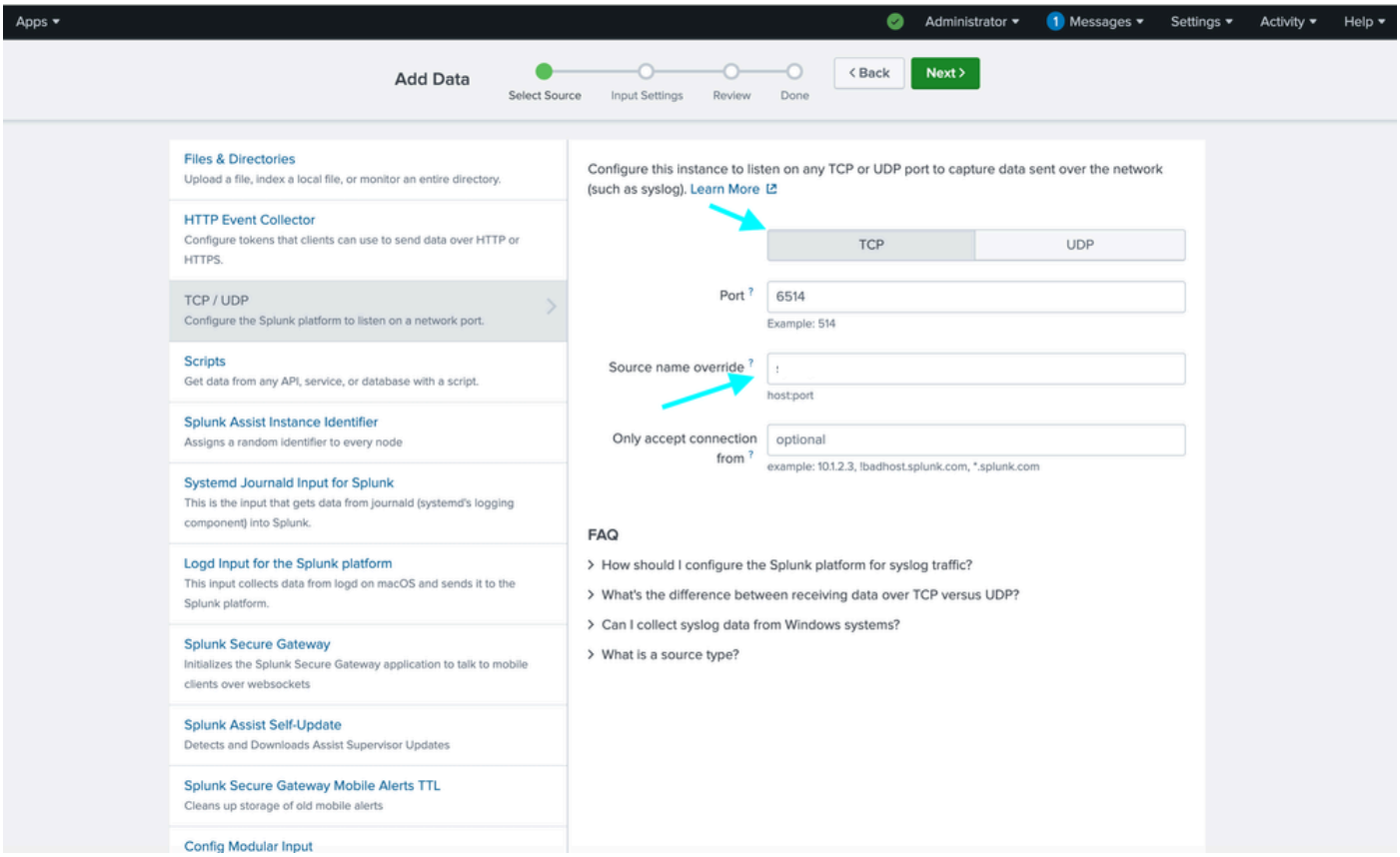


Stap 3: In het nieuwe venster selecteert u TCP, voert u de gewenste ontvangstpoort in in de voorbeeldafbeeldingspoort 6514 en voert u "gewenste naam" in het veld Bronnaam negeren in.



Opmerking: TCP 6514 is standaardpoort voor syslog over TLS

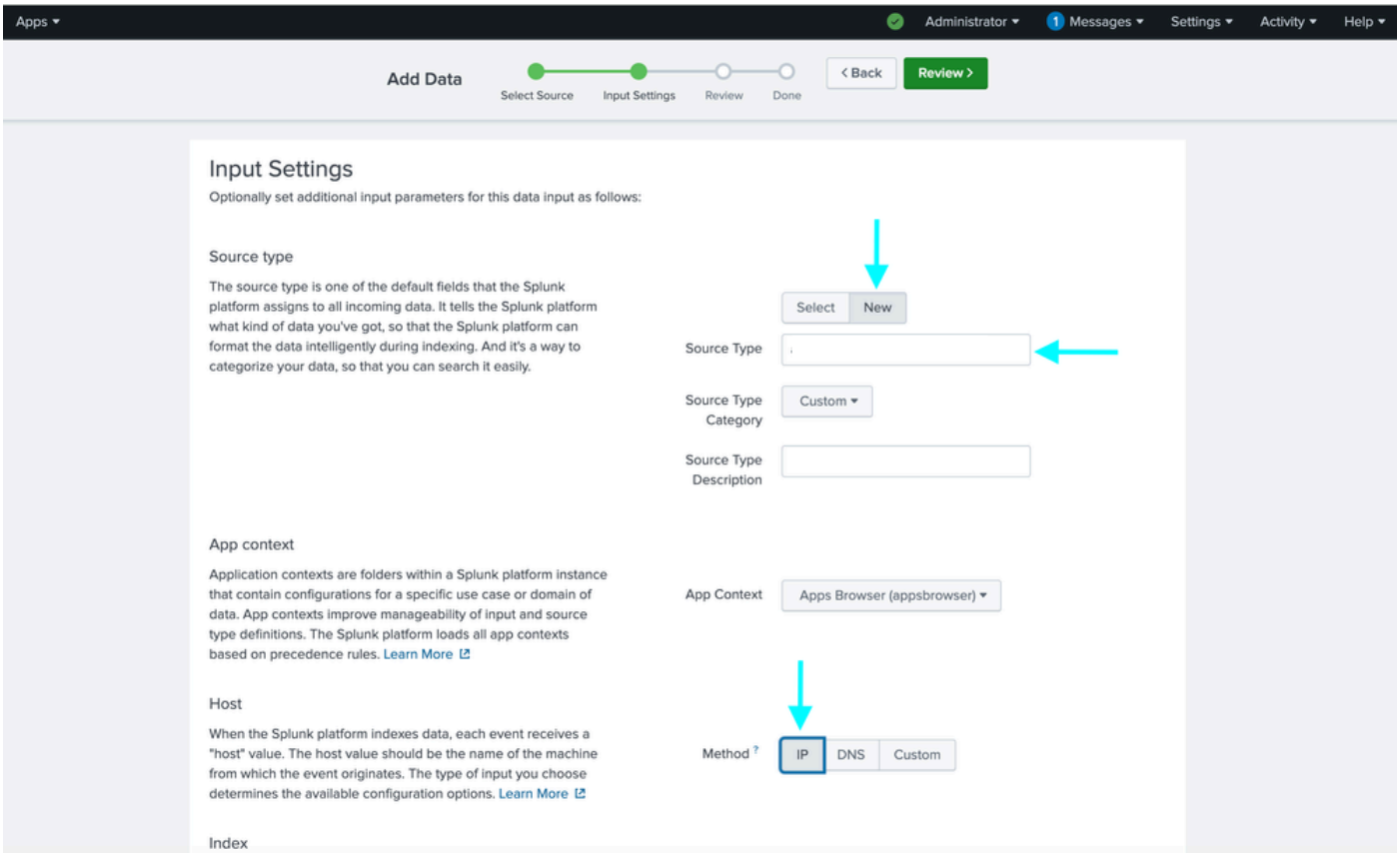
Stap 4: Als u klaar bent, klikt u op de groene knop Volgende > boven in het venster.



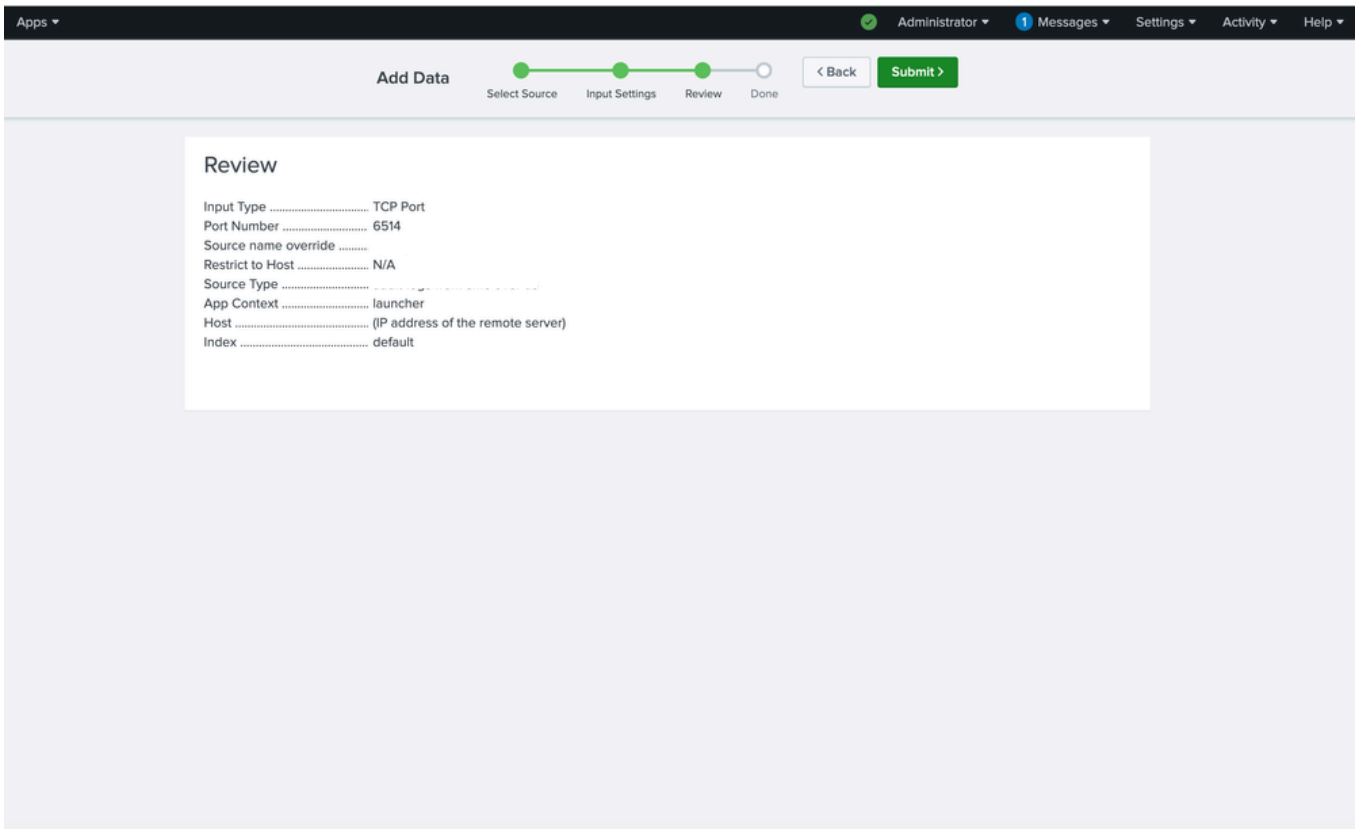
Stap 5: In het nieuwe venster selecteert u Nieuw in de sectie Brontype. Voer in het veld Brontype de gewenste naam in.

Stap 6: Selecteer IP voor de Methode in het gedeelte Host.

Stap 7: Na voltooiing selecteert u de groene knop Review > boven in het venster.



Stap 8: Controleer in het volgende venster uw instellingen en bewerk deze indien nodig. Klik na de validatie op de knop groen verzenden > boven in het venster.



2. Certificaat voor Splunk genereren

Stap 1: Gebruik een machine waarop openssl is geïnstalleerd en voer de opdracht uit`sudo openssl req -x509 -newkey rsa:4096 -keyout server_key.pem -out server_cert.pem -sha256 -days 3650 -subj /CN=10.106.127.4`. Vervang het voorbeeld IP van 10.106.127.4 door IP van het Splunk-apparaat. U wordt tweemaal gevraagd een door de gebruiker gedefinieerde wachtwoordgroep in te voeren. In de voorbeelden worden de opdrachten uitgevoerd vanaf de opdrachtregel van de Splunk-machine.

```
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:
```

Wanneer de opdracht voltooid is, worden er twee bestanden gegenereerd. De server_cert.pem en server_key.pem bestanden.

```
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:
```

Stap 2: Switch naar hoofdgebruiker.

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

Stap 3: Kopieert het nieuwe certificaat naar het `/opt/splunk/etc/auth/` .

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

Stap 4: Voeg het spunkweb.cet bestand toe met een privé-sleutel.

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

Stap 5: Verander de eigendom van splunkcertificaat.

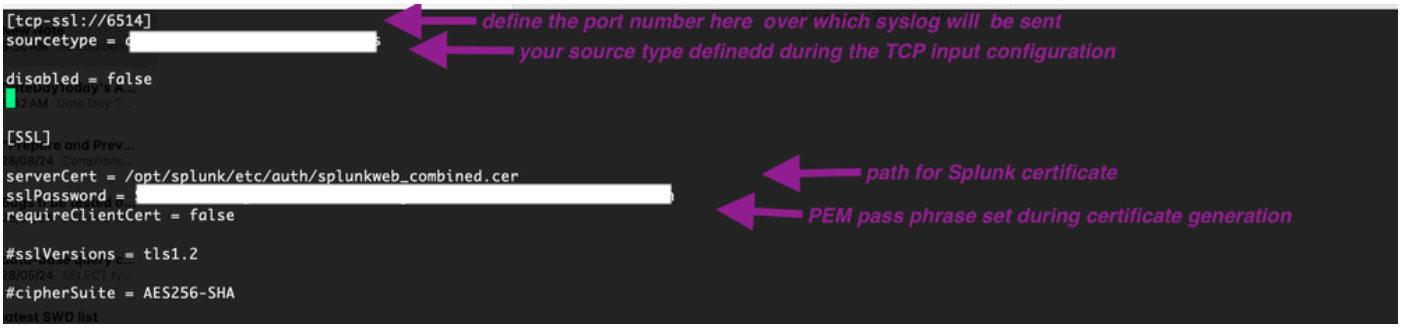
```
user@examplehost:~# chown 10777:10777/opt/splunk/etc/auth/splunkweb.cer
```

Stap 6: Verander de toestemming voor splunkcertificaat.

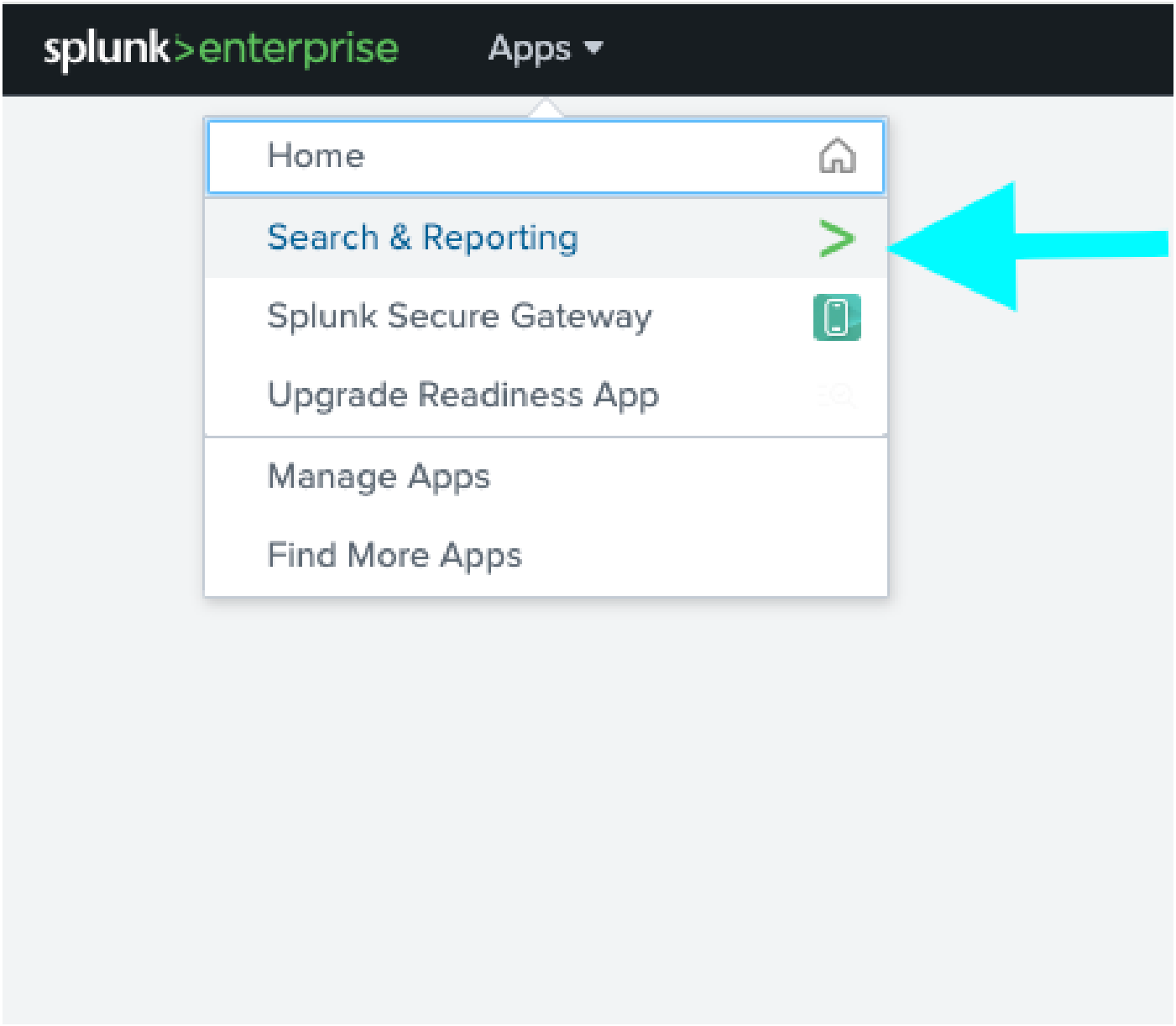
```
user@examplehost:~# chmod 600/opt/splunk/etc/auth/splunkweb.cer
```

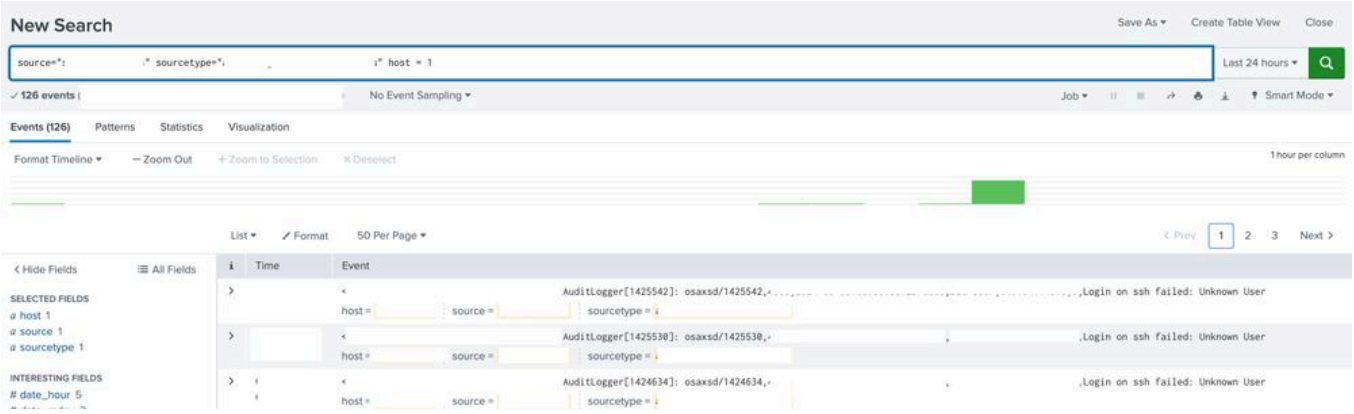
Stap 7: maak een nieuw input.conf bestand.

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



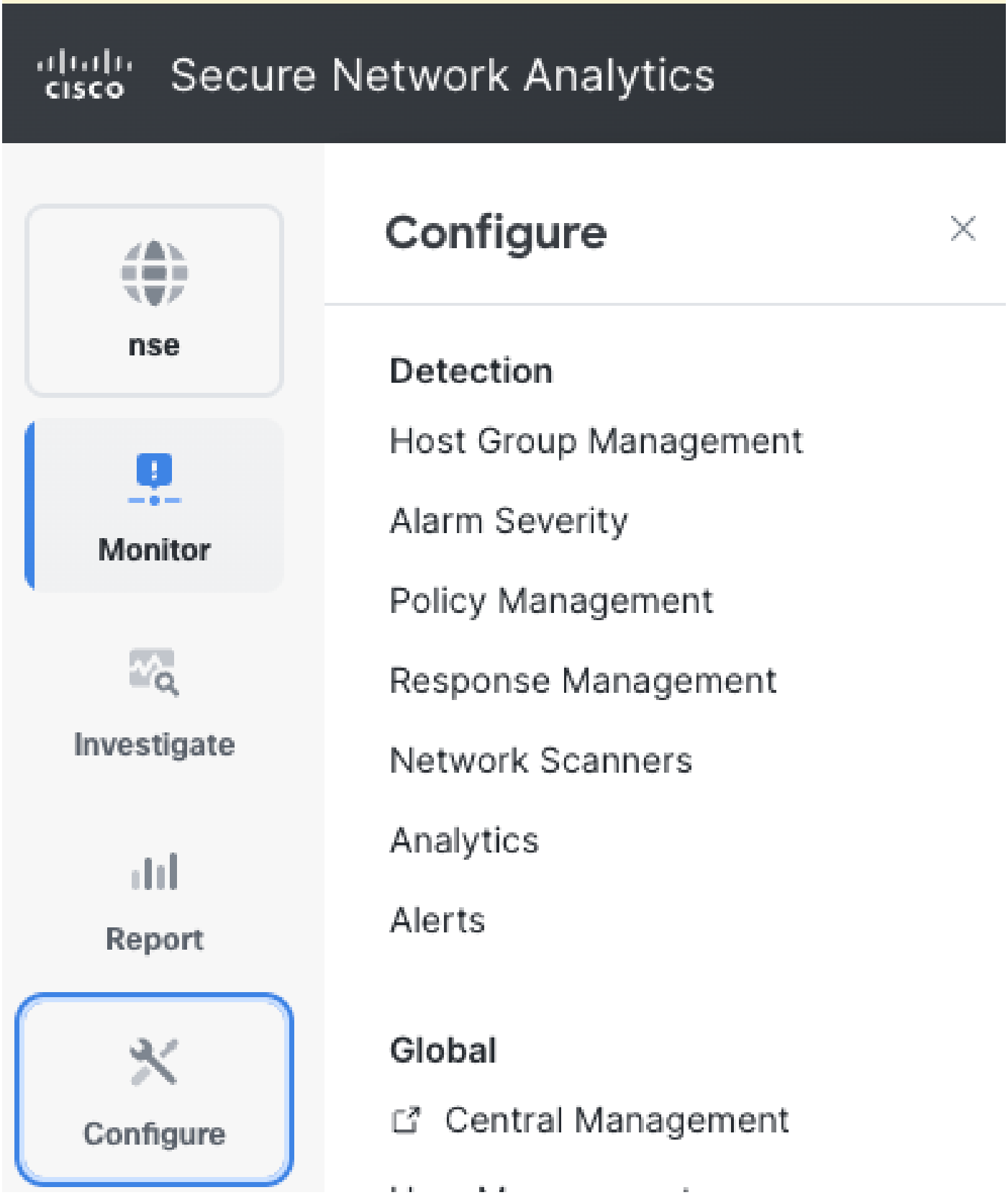
Stap 8: Controleer de syslogs met behulp van zoekactie.



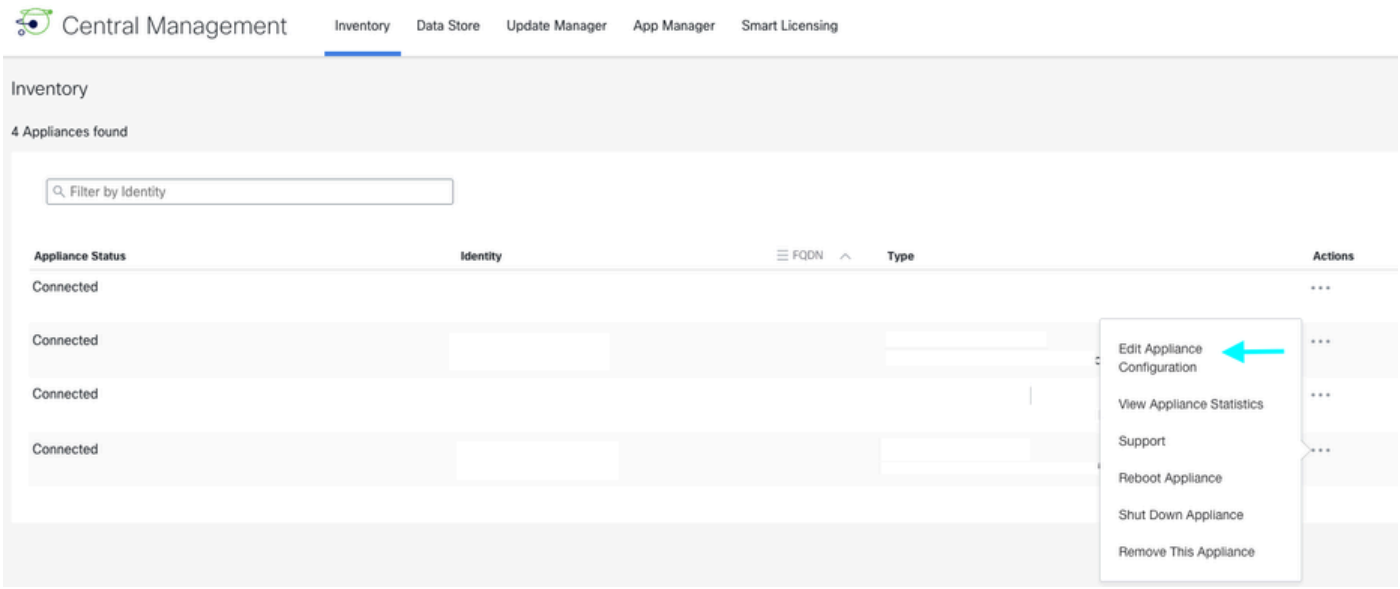


3.Bestemming controlelogboek configureren op SNA

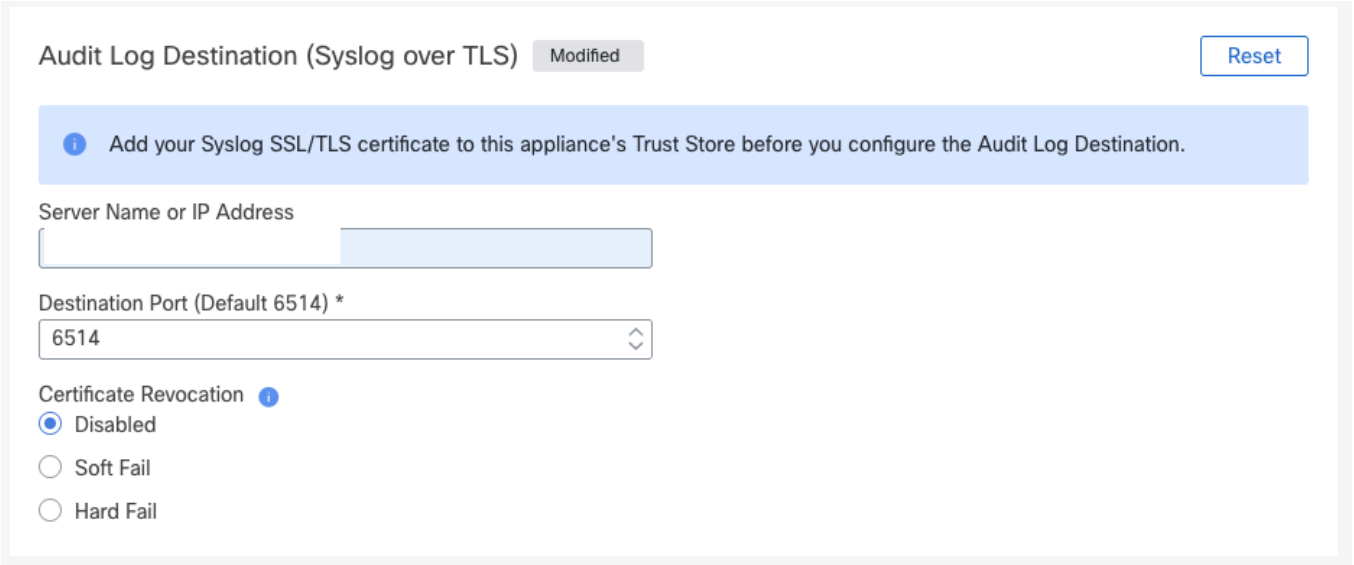
Stap 1: Log in op SMC UI navigeer om > Central Management te configureren.



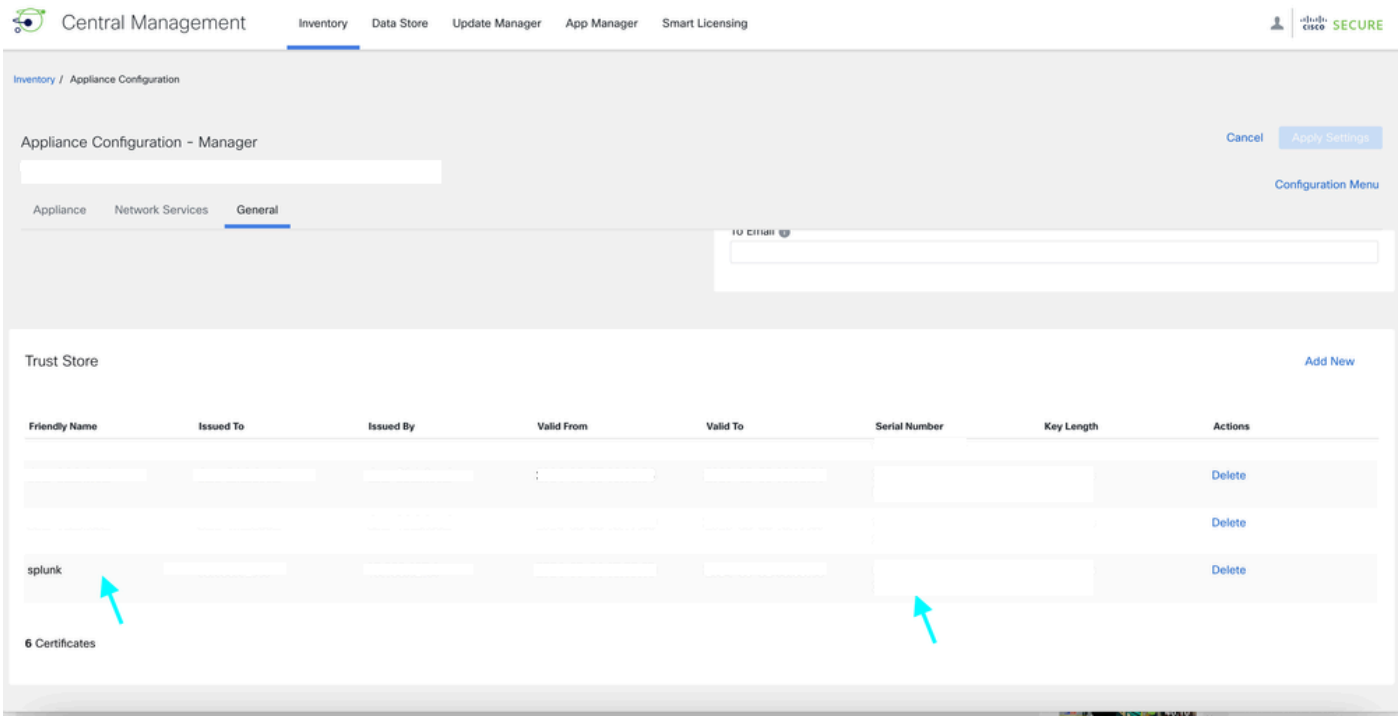
Stap 2: Klik op het pictogram ellips van uw gewenste SNA-applicatie. Selecteer Toepassingsconfiguratie bewerken.



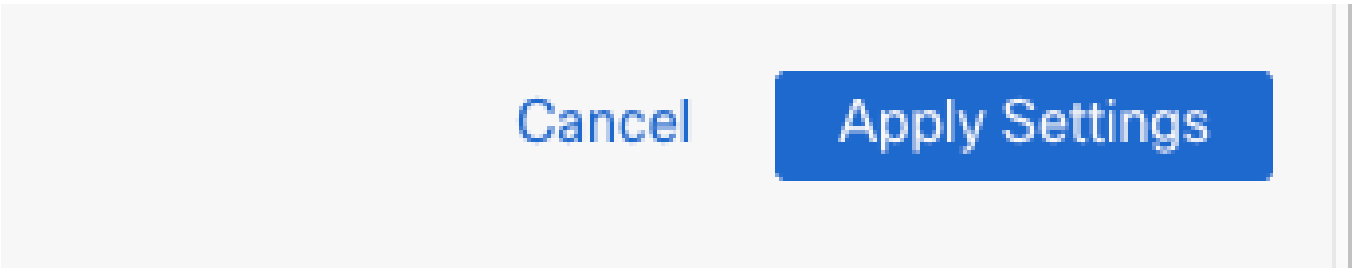
Stap 3: Navigeer naar het tabblad Network Services en voer details in van de bestemming van het auditlogboek (Syslog over TLS).



Stap 4: Navigeer naar het tabblad Algemeen, scroll naar beneden Klik op Add new om het Splunk-certificaat te uploaden dat eerder is gemaakt met de naam server_cert.pem.

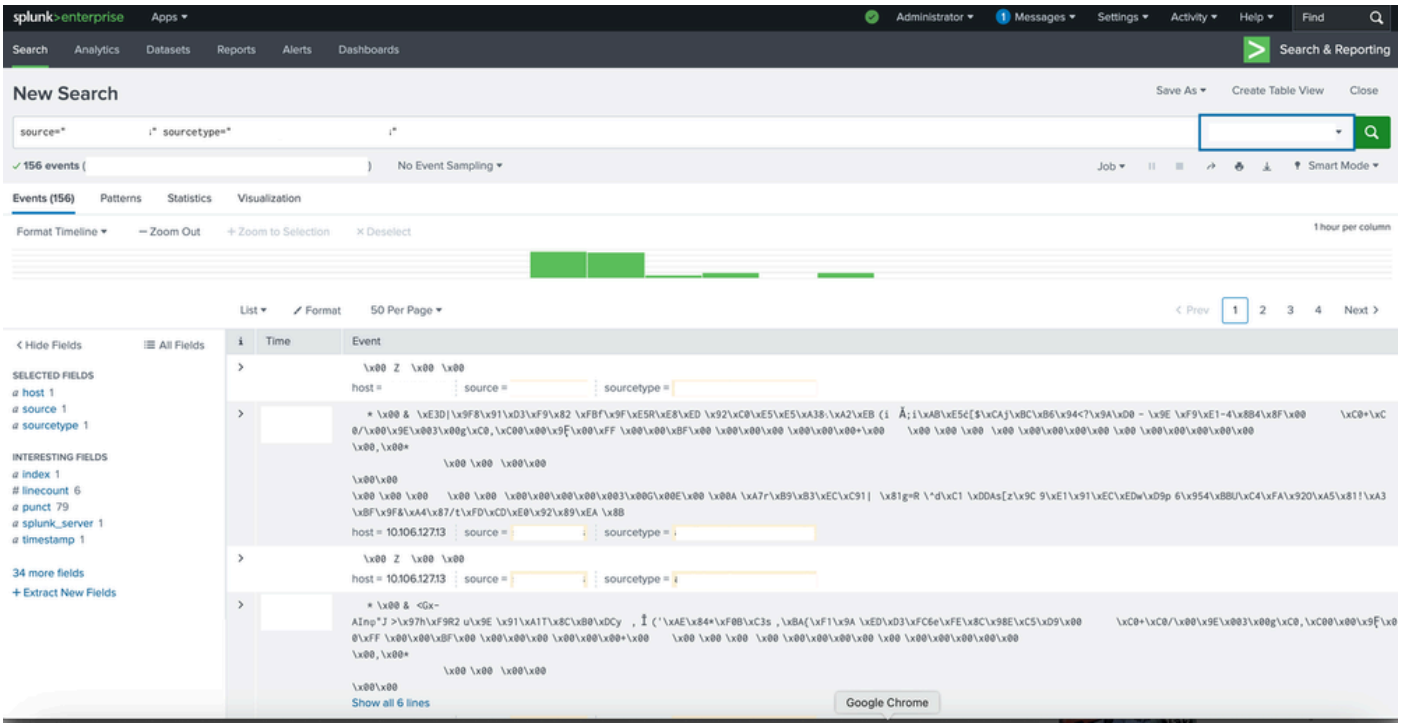


Stap 5: Klik op Instellingen toepassen.



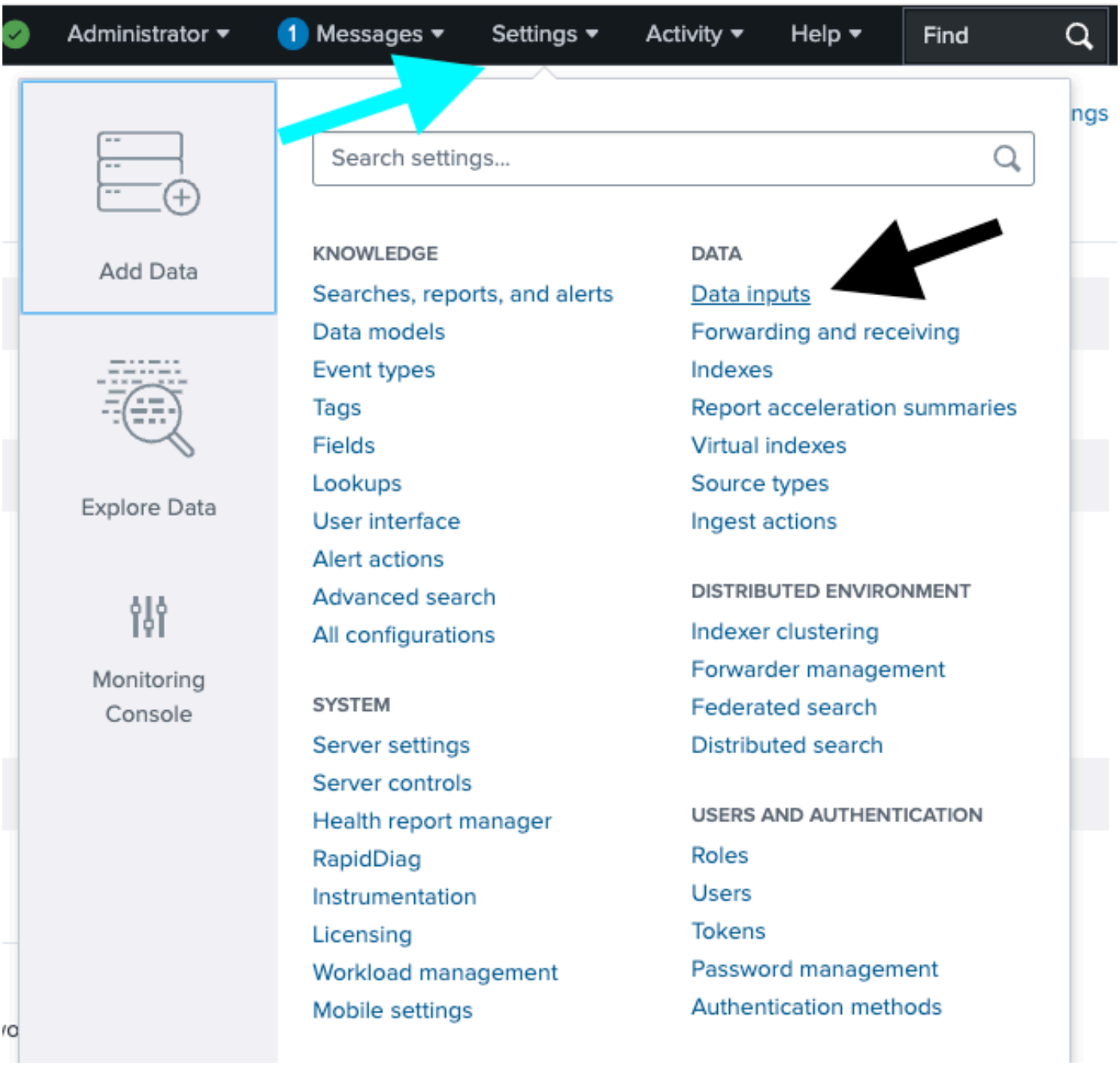
Problemen oplossen

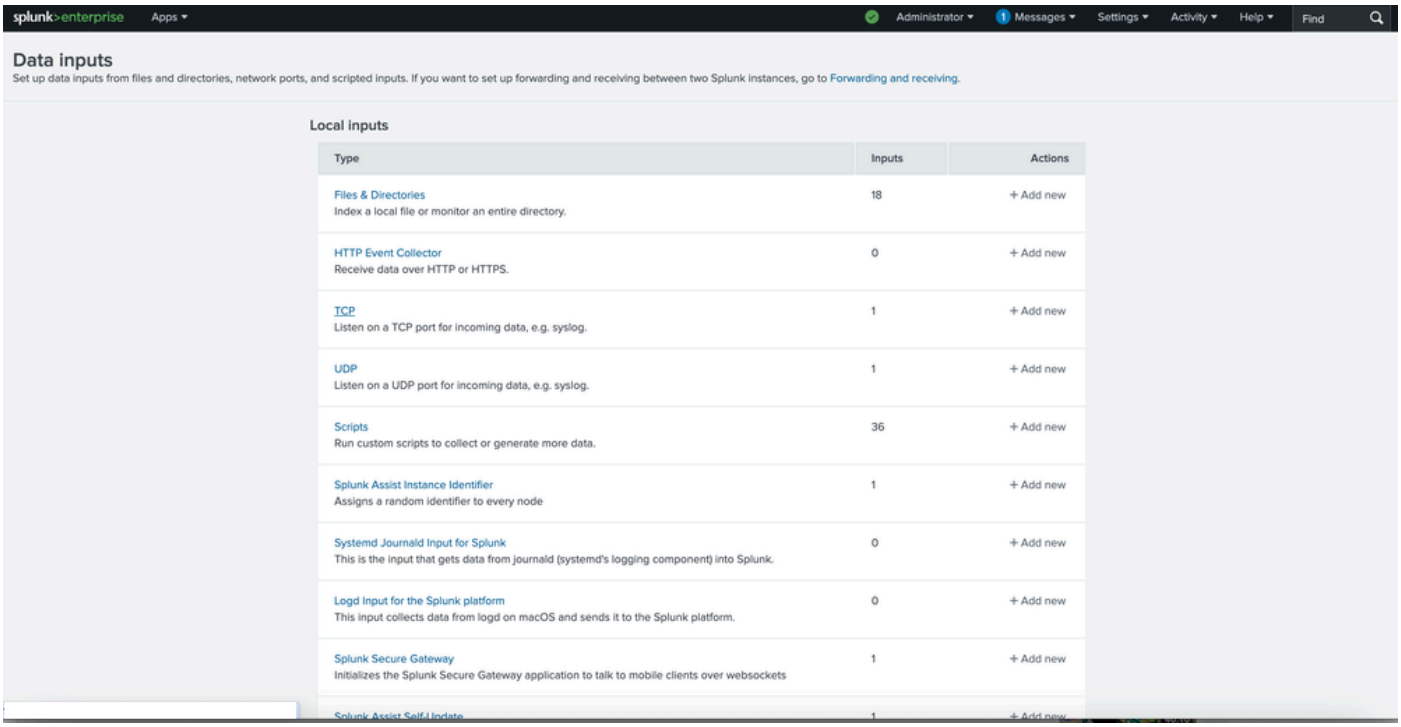
Er kan volledige onzin worden weergegeven op de zoektocht.

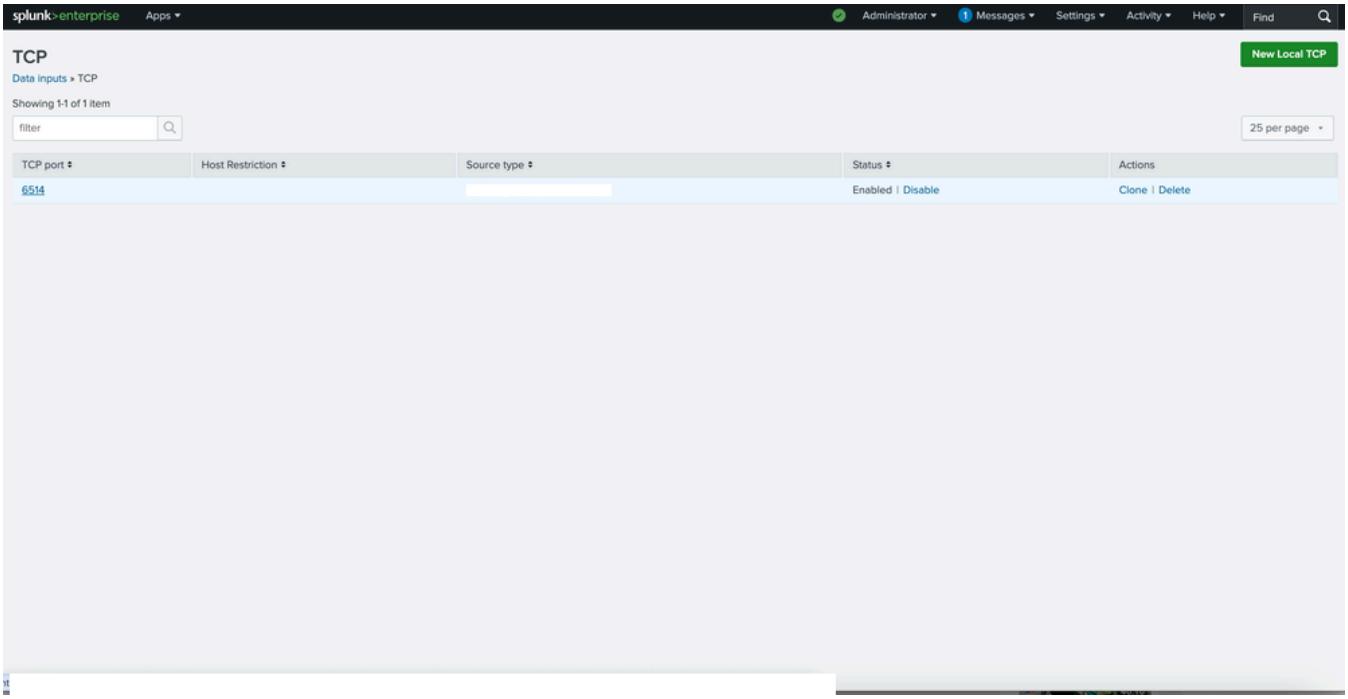


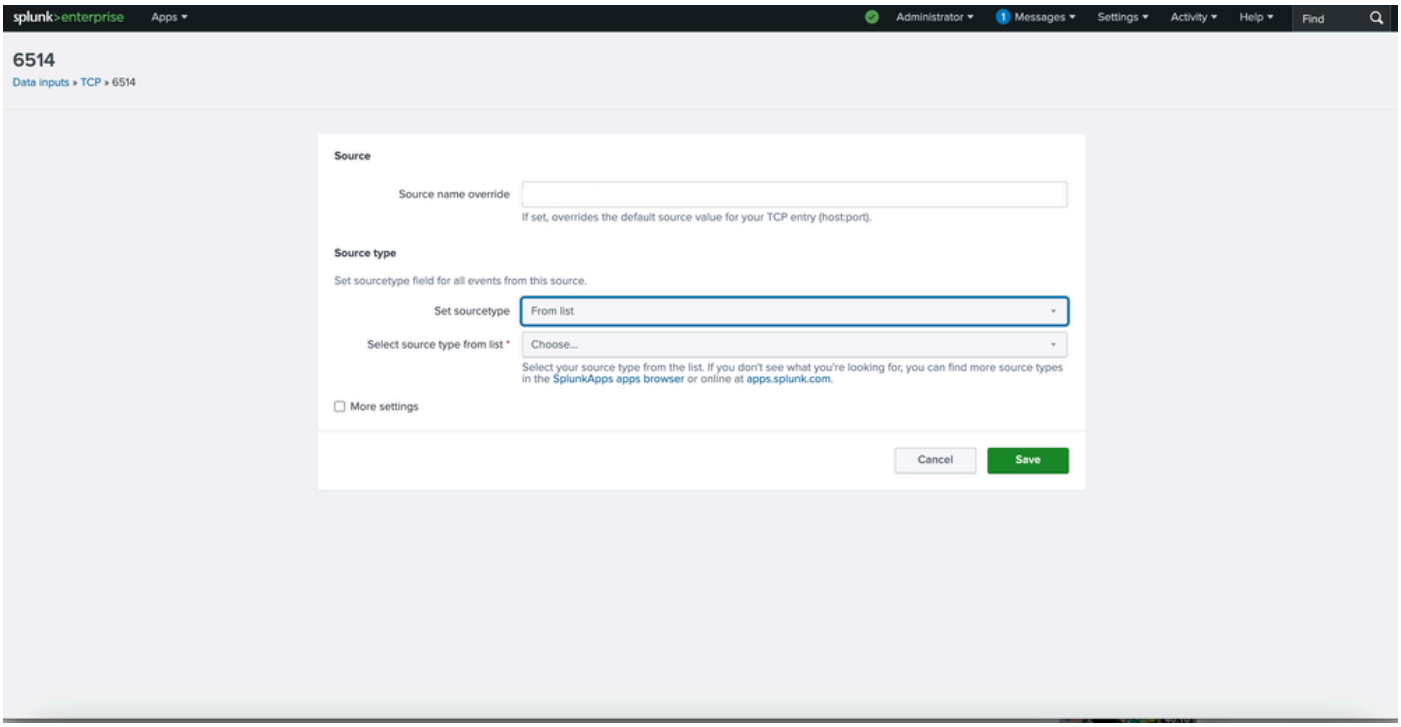
Oplossing:

Breng de input aan zijn correct brontype in kaart.


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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.