

Respons Management configureren om Syslog Events naar Splunk te sturen

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureer syslog op SNA via UDP 514 of aangepaste gedefinieerde poort](#)

[1.SNA-responsbeheer](#)

[2. Splunk configureren voor ontvangst van SNA-syslogs via UDP-poort](#)

[Configureer syslog op SNA over TCP-poort 6514 of aangepaste gedefinieerde poort](#)

[1.Splunk configureren voor ontvangst van SNA-auditlogbestanden via TCP-poort](#)

[2. Certificaat voor Splunk genereren](#)

[3.Bestemming controlelogboek configureren op SNA](#)

[Problemen oplossen](#)

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:

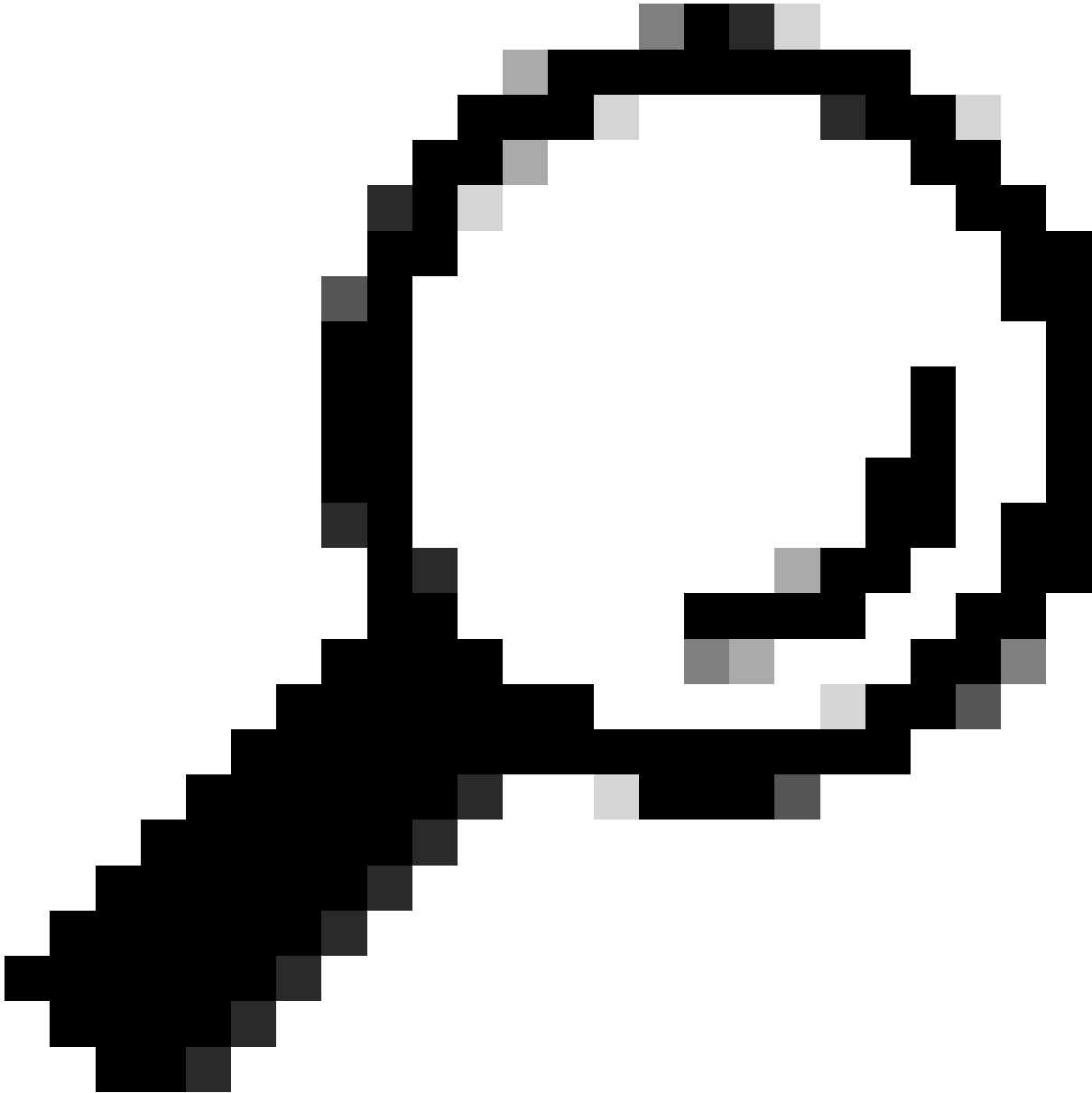
- Secure Network Analysis Response Management.
- Splunk Syslog

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.

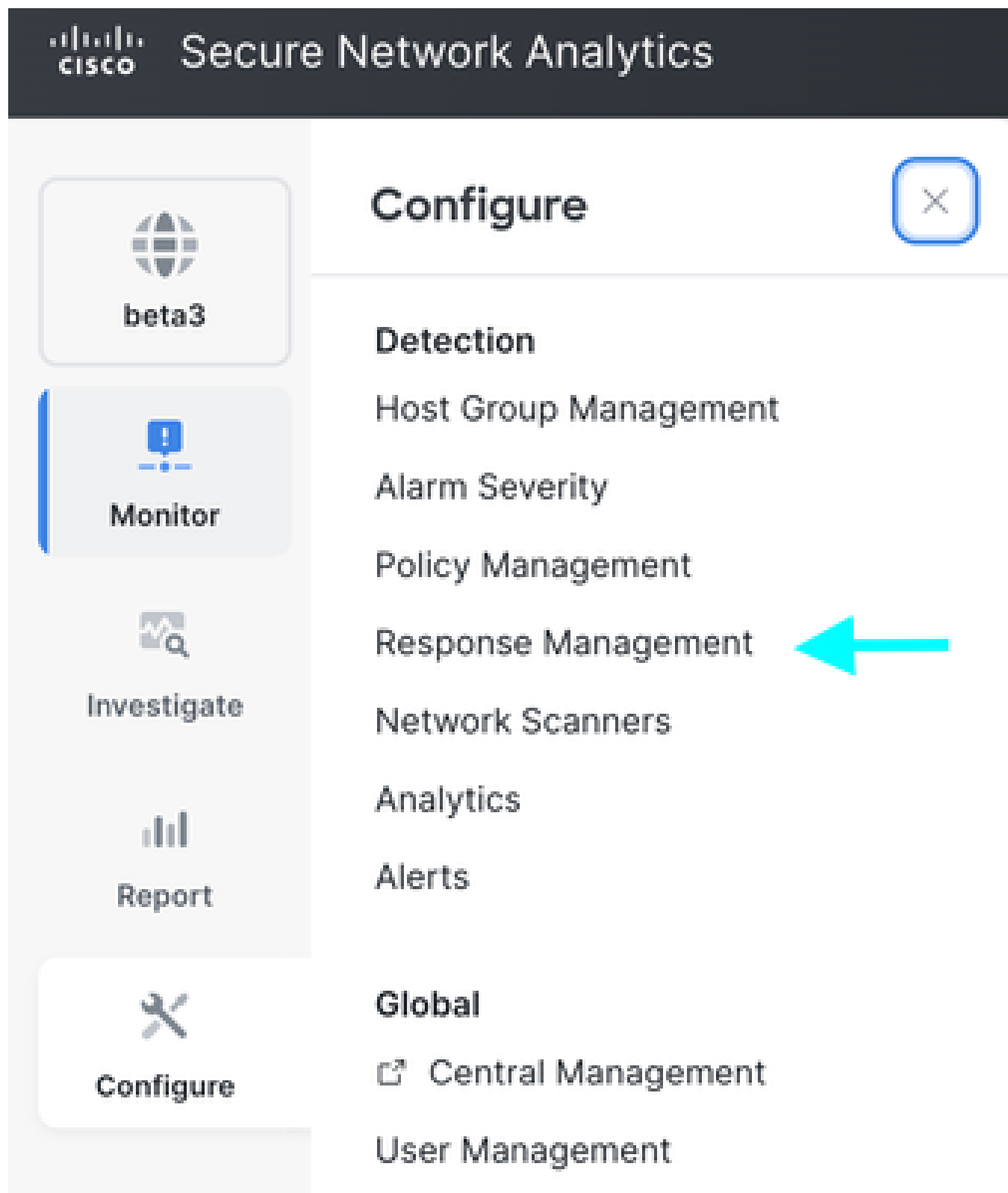
1.SNA-responsbeheer

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.

Response Management

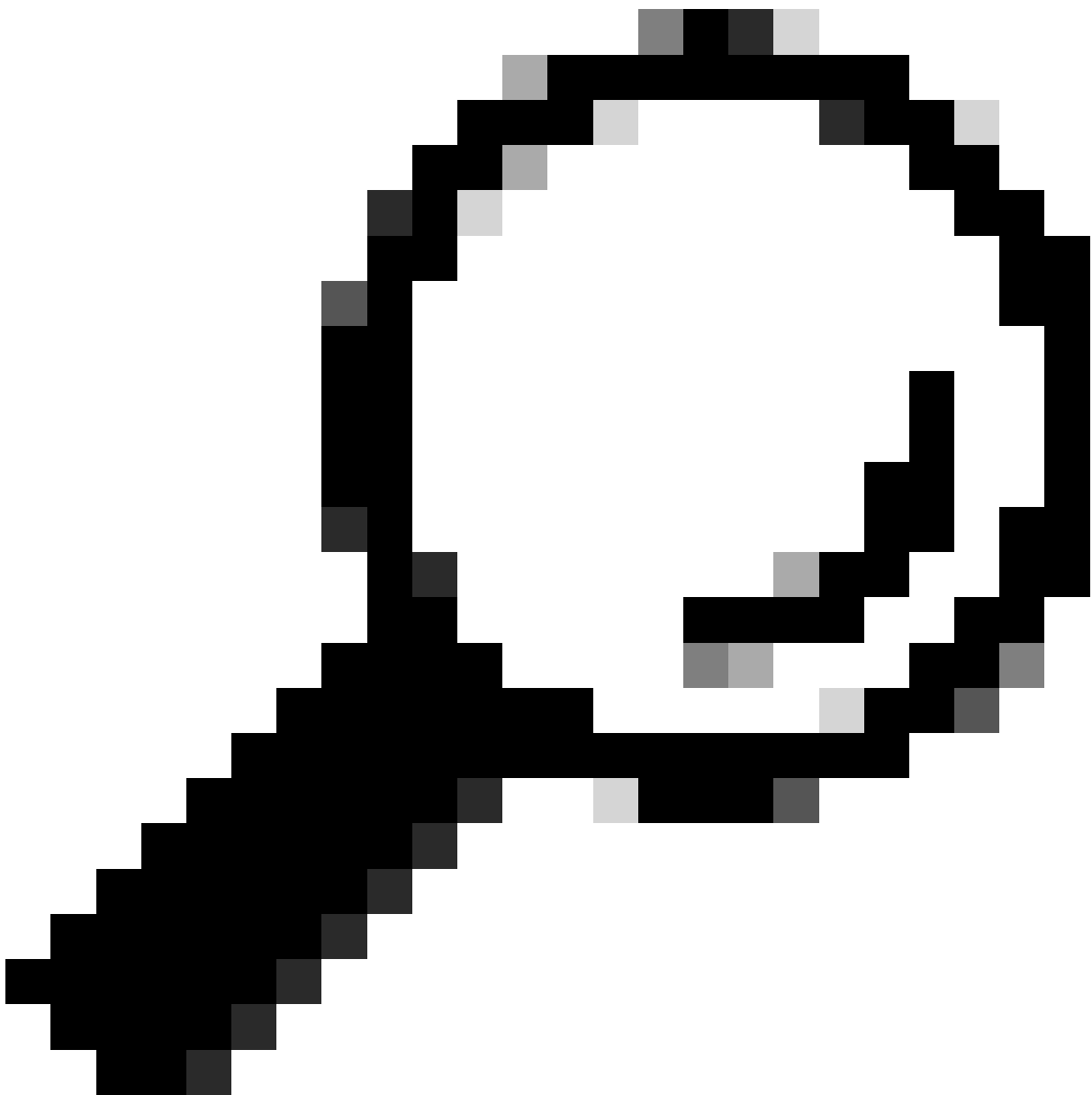
Rules Actions Syslog Formats

Actions [Add New Action](#)

Name ↑	Type	Description	Used By Rules	Enabled	Actions
Send email	Email (Alarm)	Sends an email to the recipients designated in the To field on the Email Action page.	4	☐	...
Send email	Email (Alert)	Sends an email to the recipients designated in the To field on the Email (Alert) Action page.	2	☐	...
Send to Syslog	Syslog Message (Alarm)	Sends a message to the syslog server designated in the Syslog Address field using the default Syslog Message format.	4	☒	... Edit Duplicate Delete
Send to Syslog	Syslog Message (Alert)	Sends a message to the syslog server designated in the Syslog Address field using the default Syslog Message (Alert) format.	2	☐	

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

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

UDP Port

514

Message Format

Custom

CEF

This action will use the ArcSight Common Event format.

Example Message

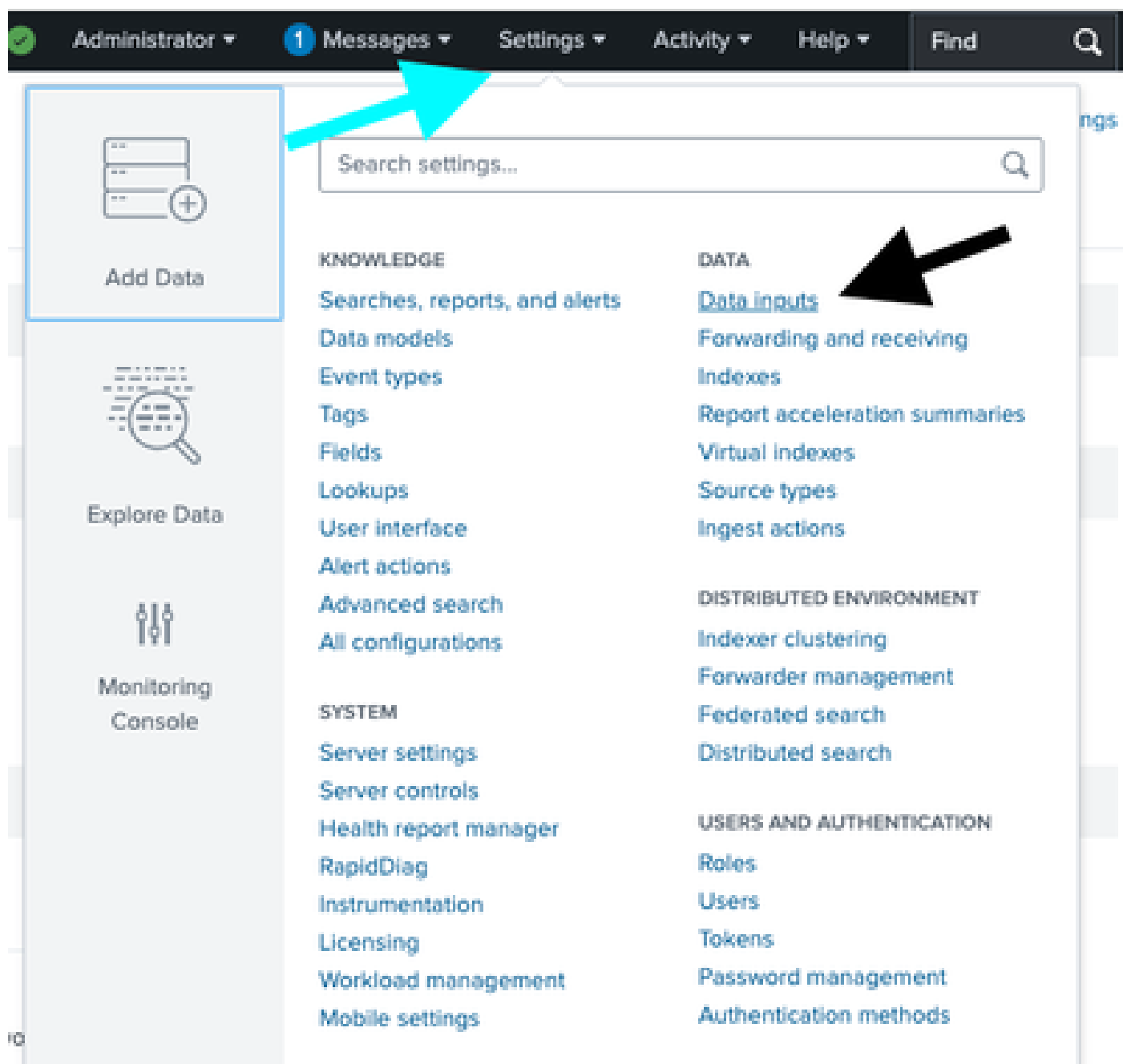
<131>Jan 01 00:00:00 test.host TestApp[1337]: CEF:0|Cisco|7.3.0|Notification:99|Bad Host|5|msg=This host has been observed performing malicious actions toward another host.:Source Host is http (80

Test Action

2. 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.

Administrator

1

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

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.

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 Journal 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 ?

514

Example: 514

Source name override ?

host:port

Only accept connection from ?

optional

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?

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.

Add Data

< Back

Review >

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.

Source Type

Select

New

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

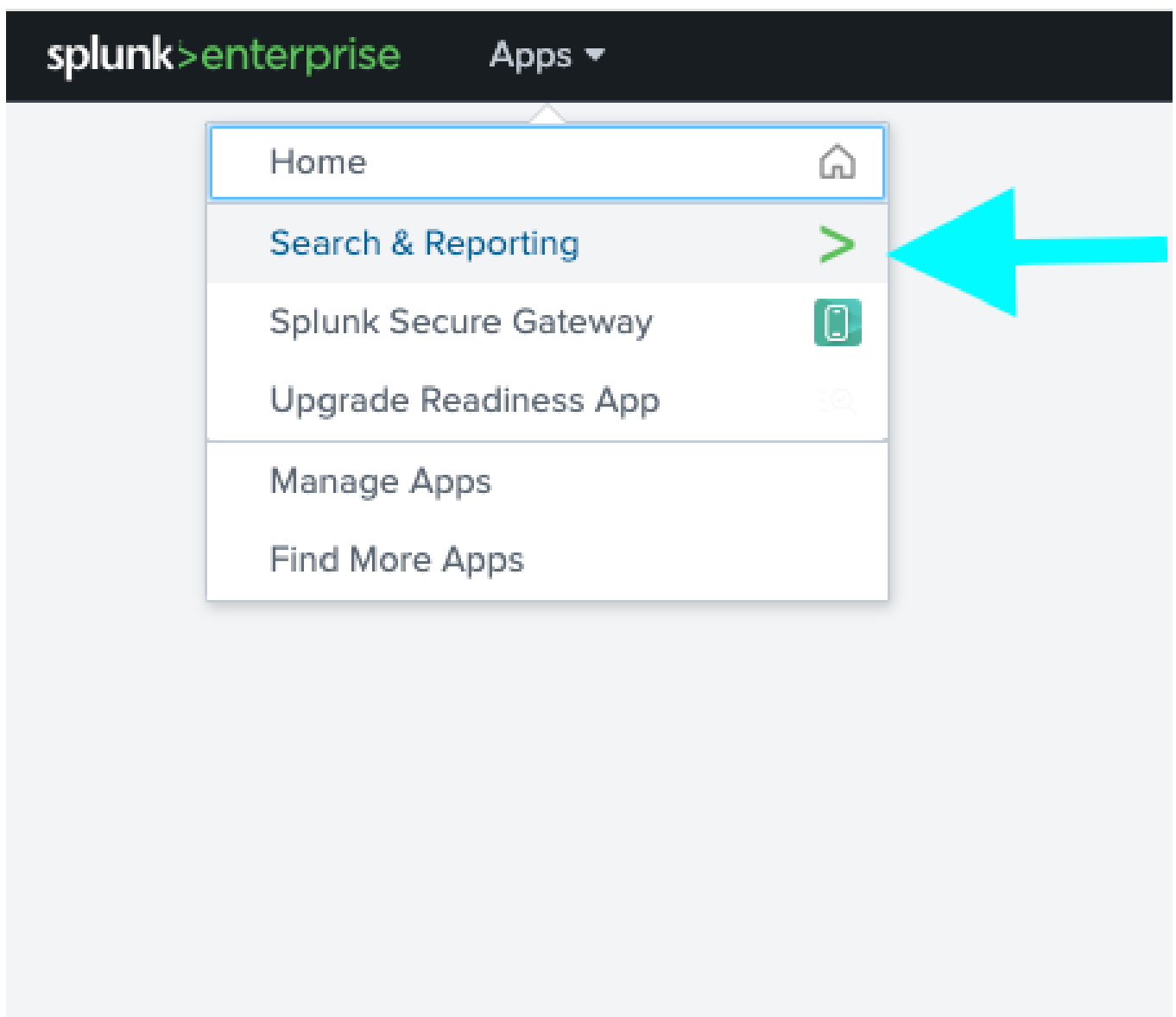
Stap 9: Controleer in het volgende venster uw instellingen en bewerk deze indien nodig.

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

Review

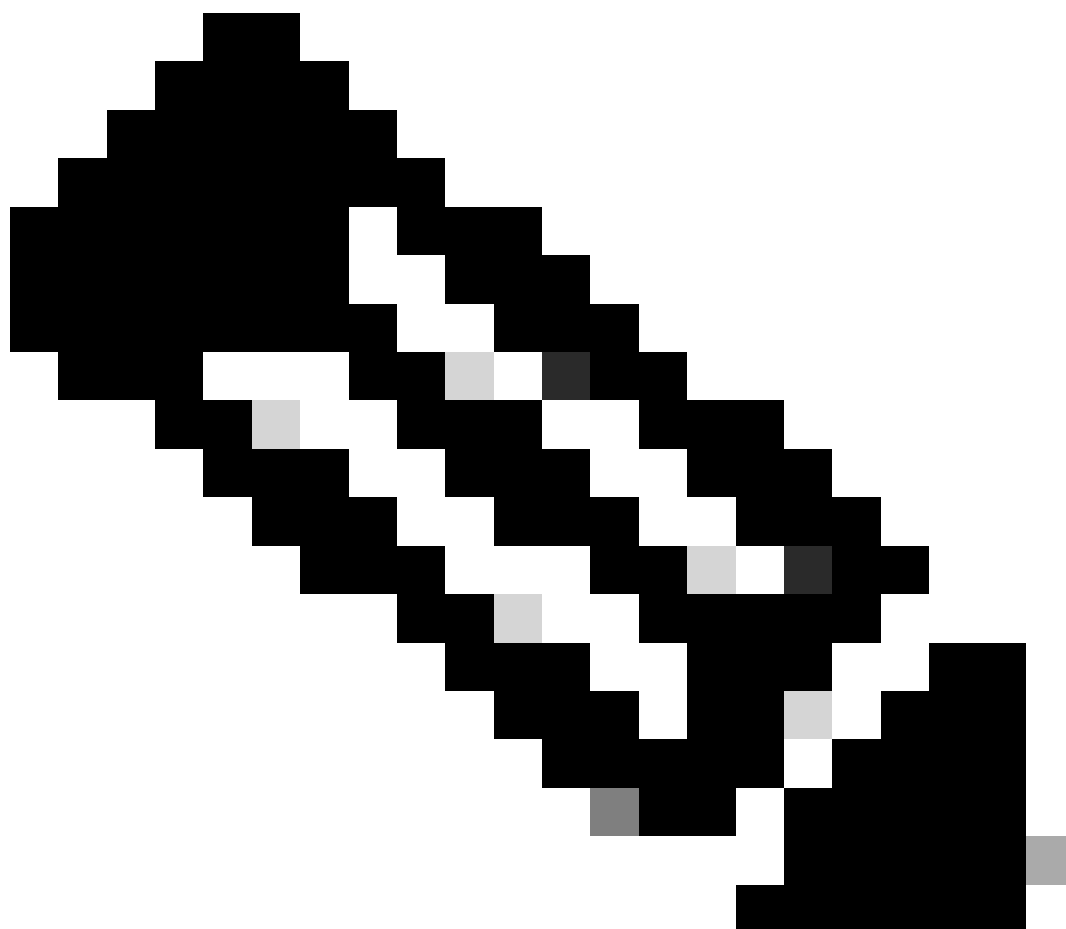
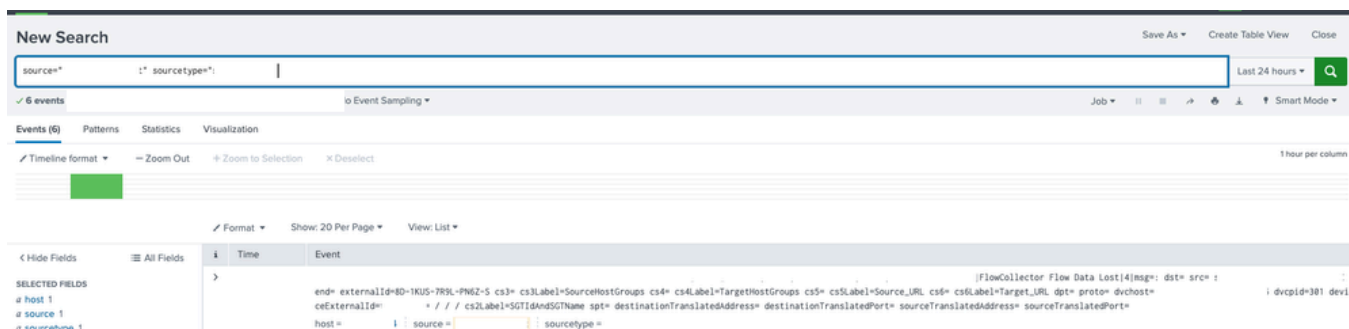
Input Type UDP Port
Port Number 514
Source name override
Restrict to Host N/A
Source Type
App Context search
Host (IP address of the remote server)
Index default

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.

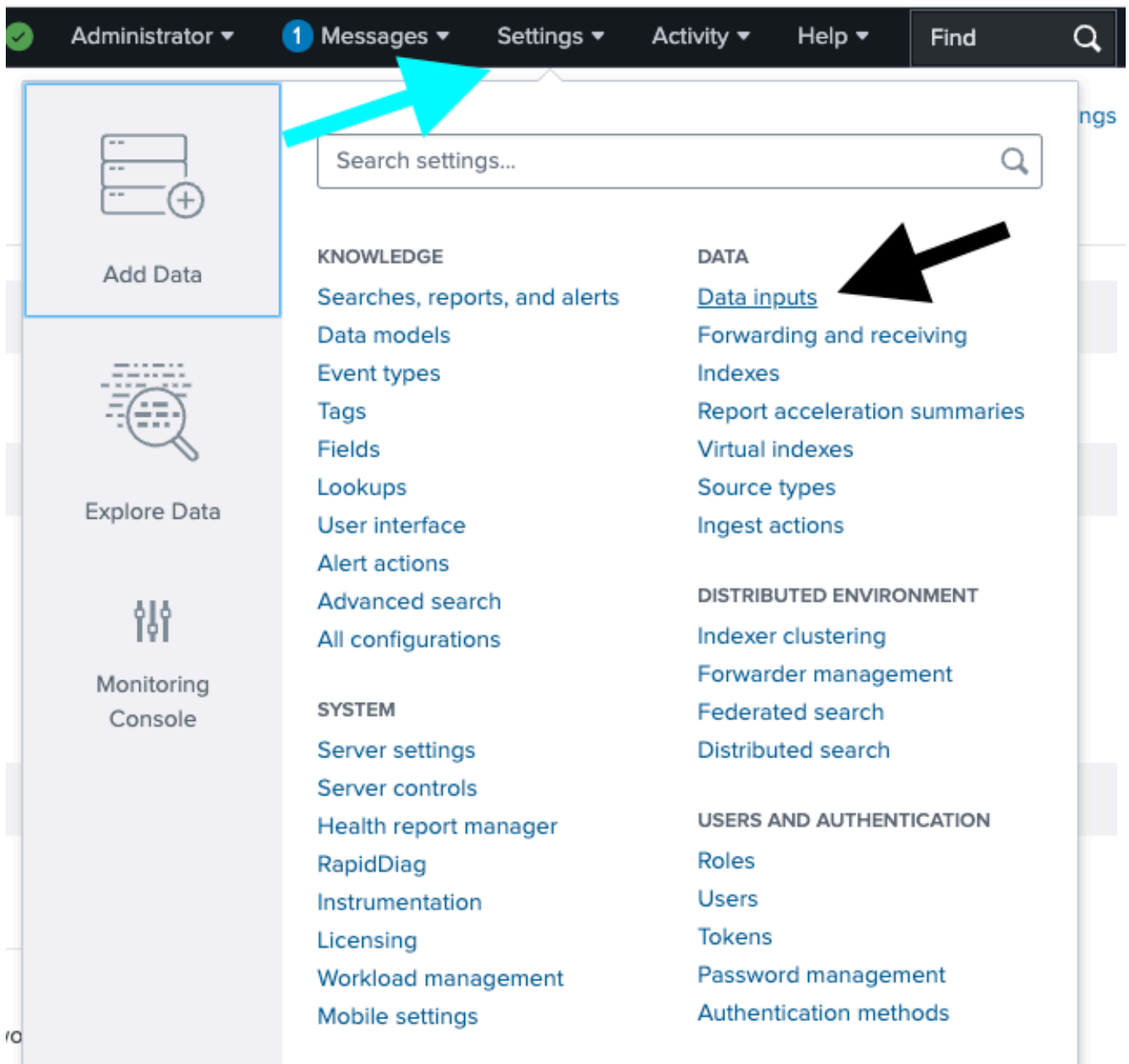


Opmerking: Zie Stap 4 voor de bron
Zie Stap 6 voor source_type

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.

Apps

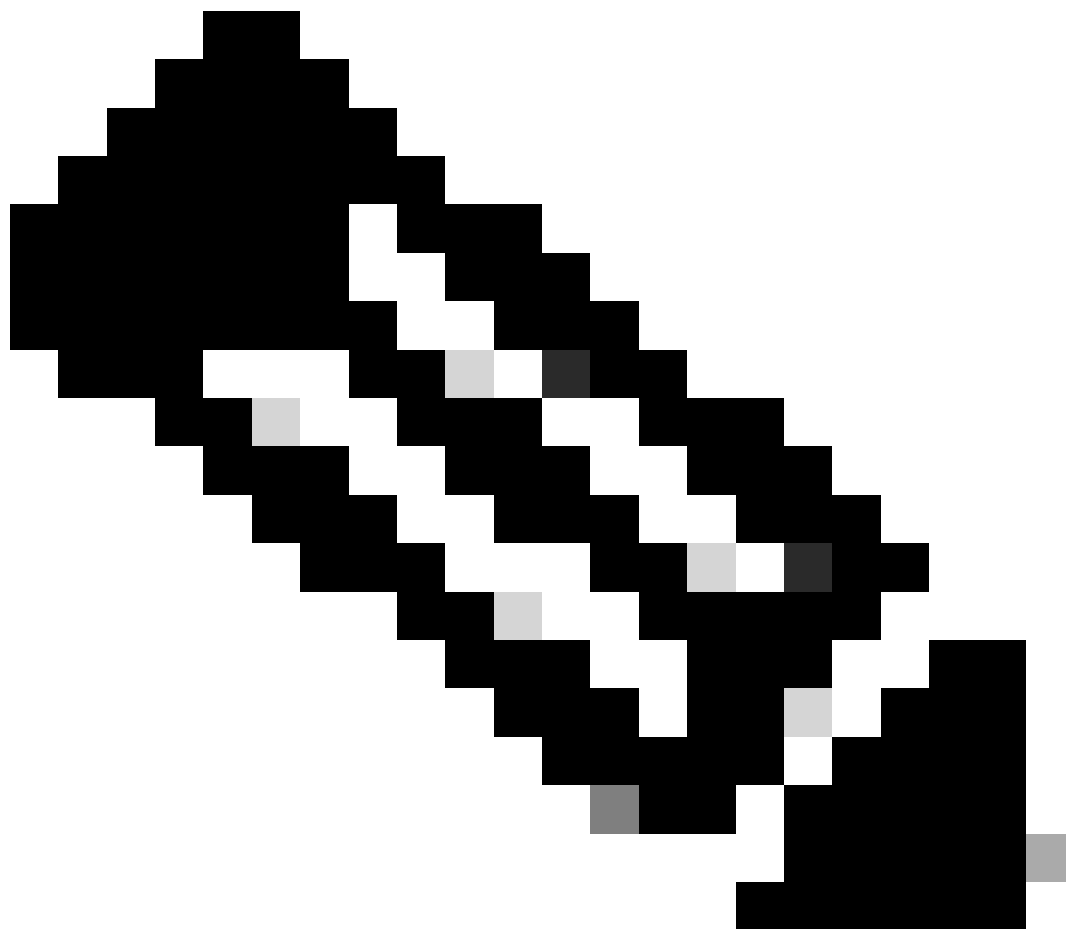
Administrator1 MessagesSettingsActivityHelp

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

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.

Apps ▾ Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾

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
Detects and Downloads Assist Supervisor Updates

Splunk Secure Gateway Mobile Alerts TTL
Cleans up storage of old mobile alerts

Config Modular Input

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?

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.

Apps ▾ Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾

Add Data ● ● ○ ○ < Back Review >

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.

Source Type 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 Apps Browser (appsbrowser) ▾

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

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.

Apps ▾ Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾

Add Data ● ● ● ○ < Back Submit >

Review

Input Type TCP Port

Port Number 6514

Source name override

Restrict to Host N/A

Source Type

App Context launcher

Host (IP address of the remote server)

Index default

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.

[illegible]

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.

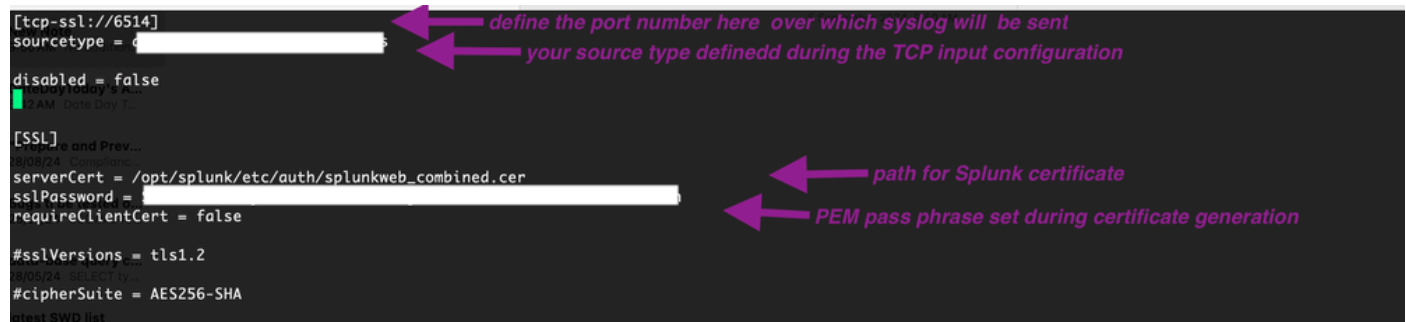
```
user@examplehost:~# chown 10777:10777/opt/splunk/etc/auth/splunkweb.cer
```

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
```



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

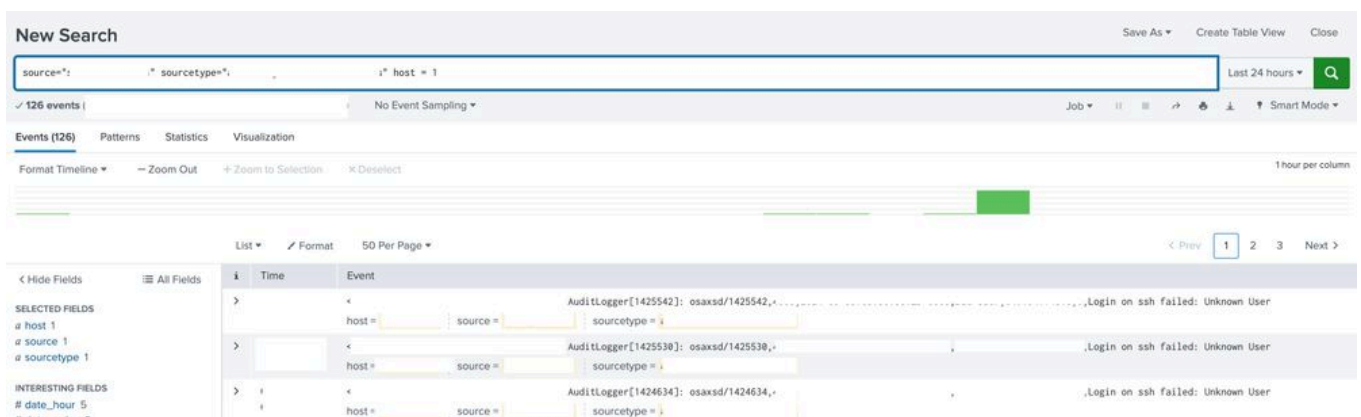
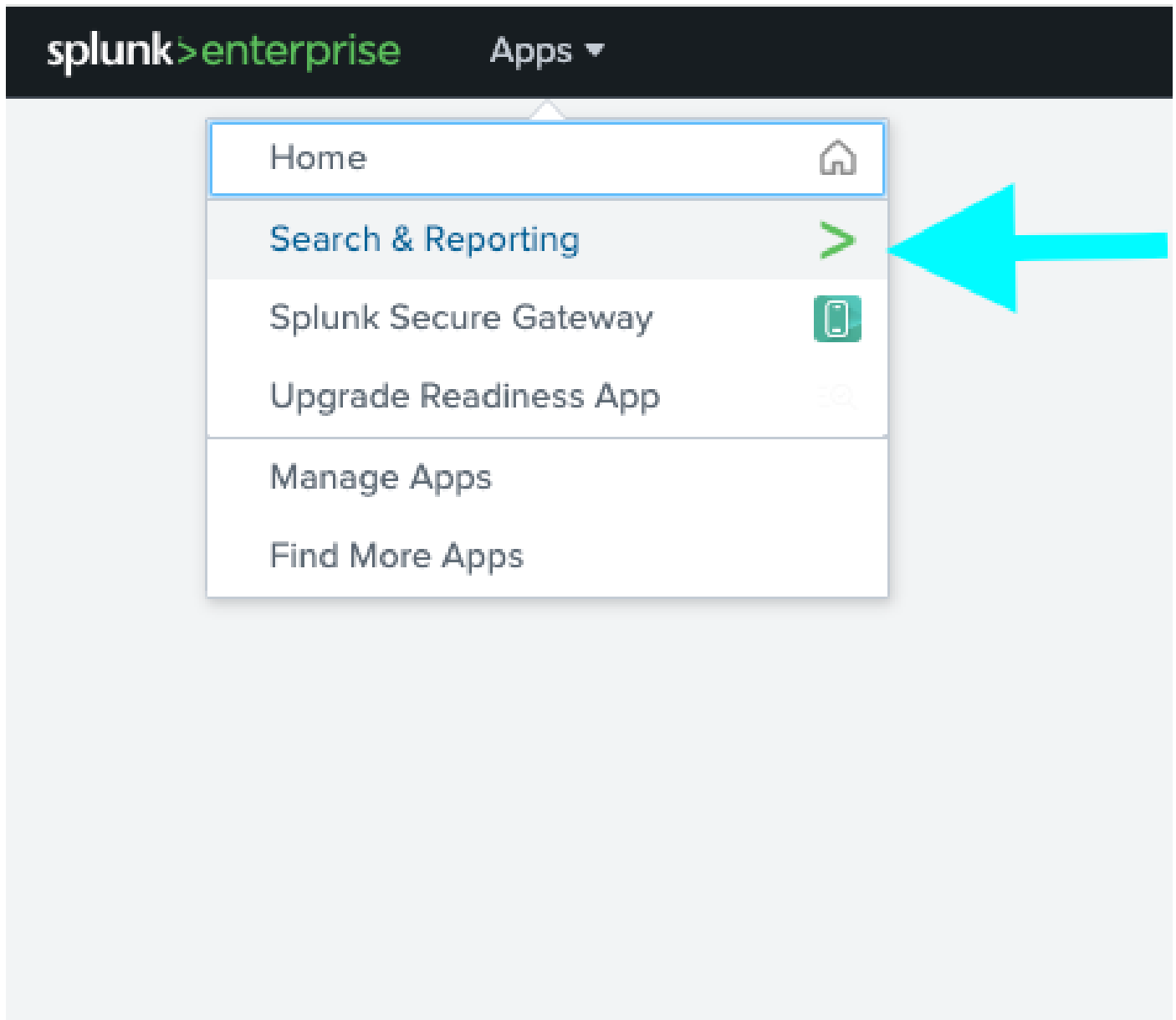
define the port number here over which syslog will be sent

your source type defined during the TCP input configuration

path for Splunk certificate

PEM pass phrase set during certificate generation

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.



nse



Monitor



Investigate



Report



Configure

Configure



Detection

Host Group Management

Alarm Severity

Policy Management

Response Management

Network Scanners

Analytics

Alerts

Global

 Central Management

... ..

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

Inventory

4 Appliances found

Filter by Identity

Appliance Status	Identity	FQDN	Type	Actions
Connected				...
Connected				- Edit Appliance Configuration - View Appliance Statistics - Support - Reboot Appliance - Shut Down Appliance - Remove This Appliance
Connected				...
Connected				...

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

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) *

6514

Certificate Revocation

☒ Disabled

☐ Soft Fail

☐ Hard Fail

Step 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.

Central Management

Inventory Data Store Update Manager App Manager Smart Licensing

Inventory / Appliance Configuration

Appliance Configuration - Manager

Cancel Apply Settings

Configuration Menu

Appliance Network Services General

TO ENRIG

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

Stap 5: Klik op Instellingen toepassen.

Cancel Apply Settings

Problemen oplossen

Er kan volledige onzin worden weergegeven op de zoektocht.

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search

Save As Create Table View Close

source=* :* sourcetype=* *

156 events () No Event Sampling Job II Smart Mode

Events (156) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 hour per column

List Format 50 Per Page Prev 1 2 3 4 Next

	i	Time	Event
>			<pre>\x00 Z \x00 \x00 host = source = sourcetype =</pre>
>			<pre>* \x00 & \xE3D \x9F8\x91\xD3 \x9F9\x82 \xF8F\x9F\xE5R\xE8\xED \x92\xC0\xE5\xE5\xA38:\xA2\xEB (i Ä;1\xAB\xE5C[\$\xC4J\xBC\xB6\x94C7\x9A\xD0 - \x9E \xF9\xE1-4\x884\x8F\x00 \xC0+\xC 0/\x00\x9E\x00J\x00g\xC0,\xC00\x00\x9F\x00\xFF \x00\x00\xBF\x00 \x00\x00\x00 \x00\x00\x00+\x00 \x00 \x00 \x00 \x00 \x00\x00\x00 \x00 \x00\x00\x00\x00 \x00 \x00\x00\x00\x00\x00 \x00,\x00* \x00 \x00 \x00 \x00\x00 \x00 \x00 \x00 \x00 \x00 \x00\x00\x00\x00\x00\x00\x00\x00 \x00A \xA7\xB9\xB3\xEC\xC91 \xB81g=R \xD0As[z\x9C 9\xE1\x91\xEC\xEDw\xD9p 6\x954\x88U\xC4\xFA\x920\xA5\x81!\xA3 \xBF\x9F&\xA4\x87/t\xFD\xCD\xE0\x92\x89\xEA \x88 host = 10106.12713 source = sourcetype =</pre>
>			<pre>\x00 Z \x00 \x00 host = 10106.12713 source = sourcetype =</pre>
>			<pre>* \x00 & <GK- AInp"J >\x97h\xF9R2 u\x9E \x91\xATT\x8C\xB0\xDCY , Î (' \xAE\x84+\xF0B\xC3s , \xBA(\xF1\x9A \xED\xD3\xFC6\xFE\x8E\xC5\xD9\x00 \xC0+\xC0/\x00\x9E\x00J\x00g\xC0,\xC00\x00\x9F\x00 0\xFF \x00\x00\xBF\x00 \x00\x00\x00 \x00\x00\x00+\x00 \x00 \x00 \x00 \x00\x00\x00\x00 \x00 \x00\x00\x00\x00\x00 \x00,\x00* \x00 \x00 \x00 \x00\x00 \x00 \x00</pre>

Show all 6 lines Google Chrome

Oplossing:

Breng de input aan zijn correct brontype in kaart.



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

Showing 1-1 of 1 item

25 per page

New Local TCP

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

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.