

Konfigurieren der Antwortverwaltung zum Senden von Syslog-Ereignissen an Splunk

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren von Syslog auf SNA über UDP 514 oder einem benutzerdefinierten Port](#)

[1.SNA-Antwortmanagement](#)

[2.Konfigurieren von Splunk zum Empfangen von SNA-Syslogs über den UDP-Port](#)

[Konfiguration von Syslog auf SNA über TCP-Port 6514 oder benutzerdefinierten Port](#)

[1.Splunk für den Empfang von SNA-Audit-Protokollen über TCP-Port konfigurieren](#)

[2.Zertifikat für Splunk generieren](#)

[3.Konfigurieren des Prüfprotokollziels auf SNA](#)

[Fehlerbehebung](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie die Funktion für das Management sicherer Analysemöglichkeiten konfigurieren, um Ereignisse per Syslog an einen Drittanbieter, z. B. Splunk, zu senden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Sicheres Reaktionsmanagement für Netzwerkanalysen:
- Splunk-Syslog

Verwendete Komponenten

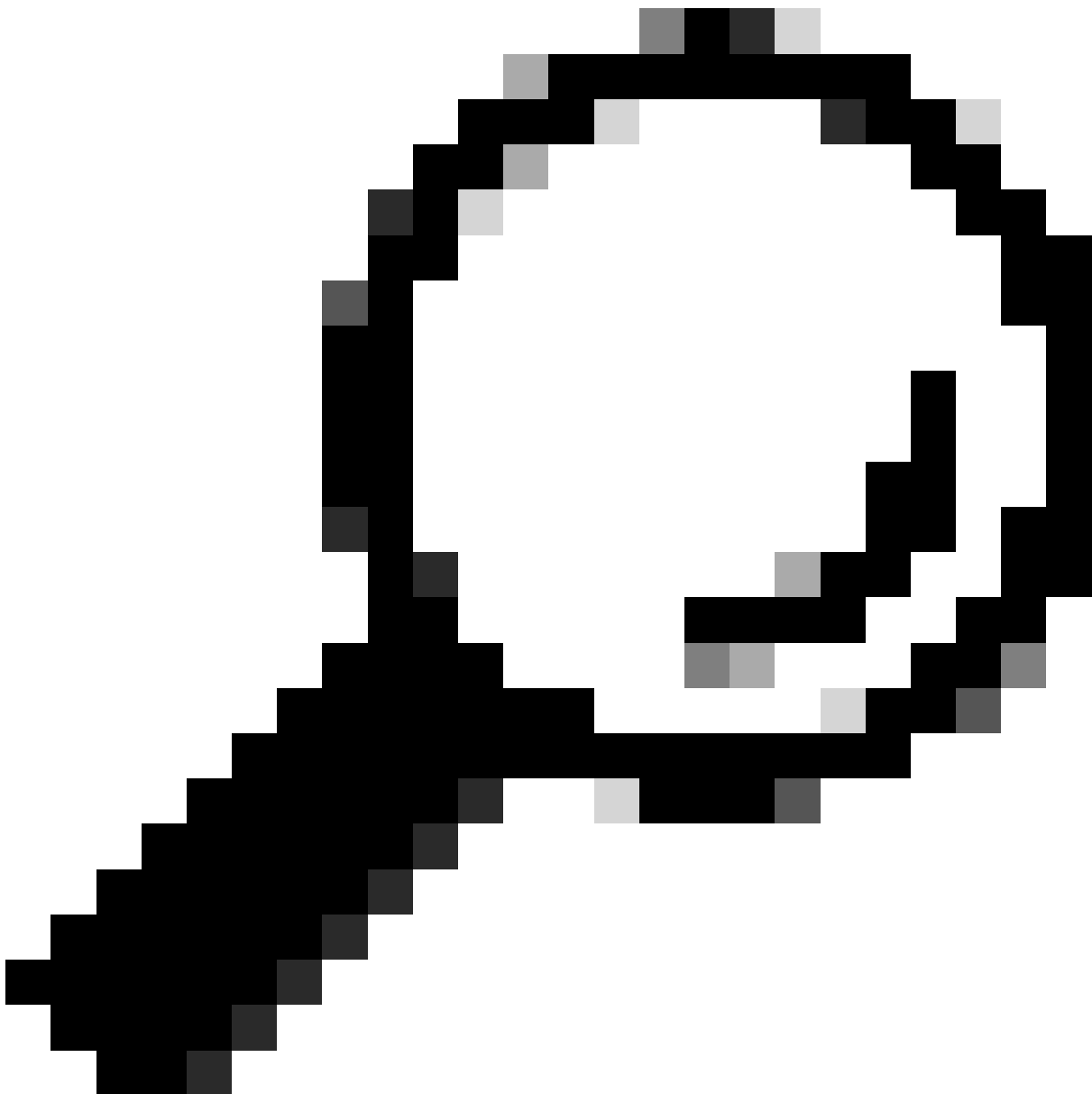
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

- Bereitstellung von Secure Network Analytics (SNA), die mindestens eine Manager-Appliance

und eine FlowCollector-Appliance enthält.

- Splunk-Server installiert und über 443 Ports zugänglich.

Konfigurieren von Syslog auf SNA über UDP 514 oder einem benutzerdefinierten Port

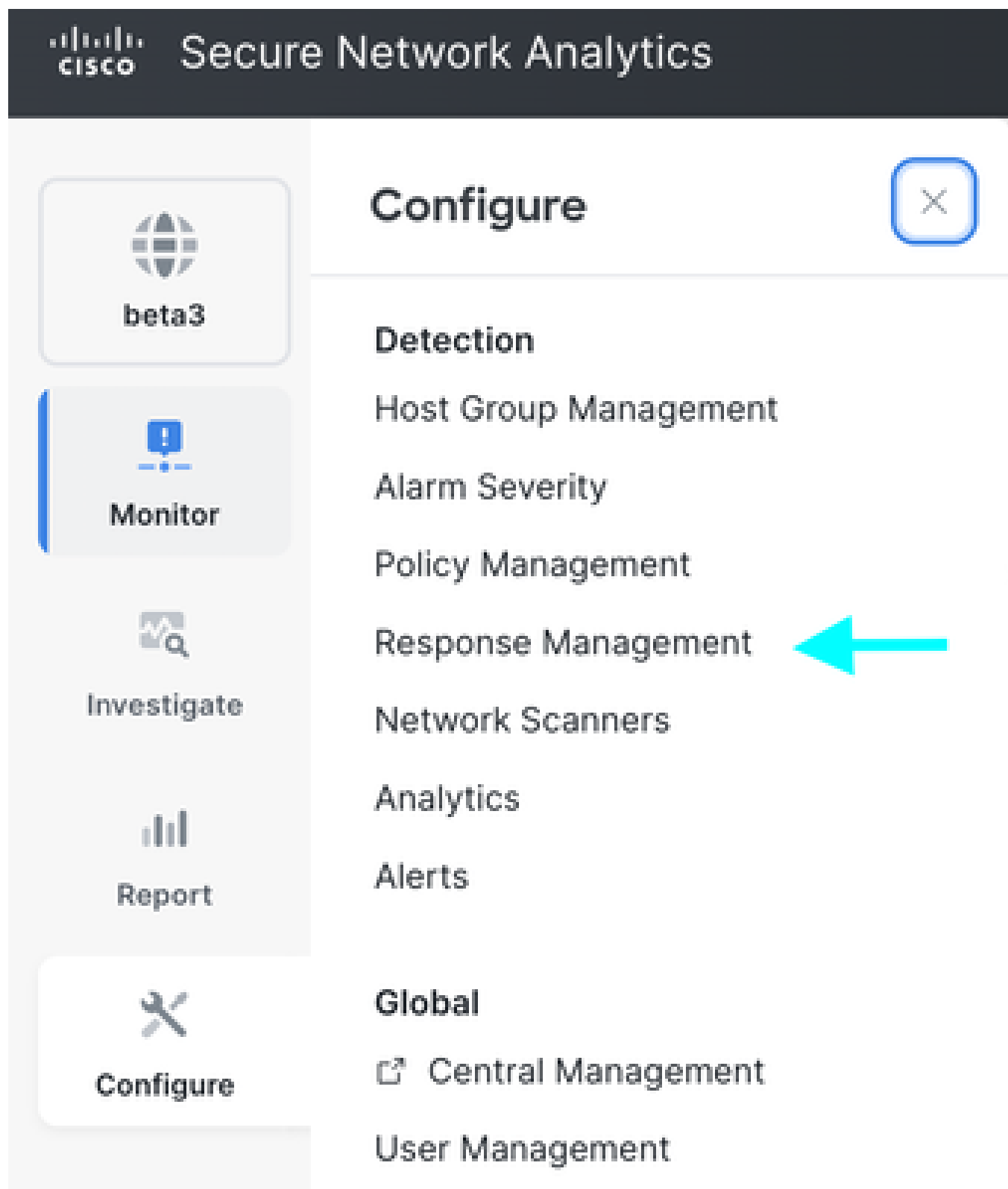


Tipp: Stellen Sie sicher, dass UDP/514, TCP/6514 oder jeder benutzerdefinierte Port, den Sie für Syslog auswählen, auf Firewalls oder zwischengeschalteten Geräten zwischen SNA und Splunk zugelassen ist.

Mit der Response Management-Komponente von Secure Analytics (SA) können Regeln, Aktionen und Syslog-Ziele konfiguriert werden.

Diese Optionen müssen konfiguriert werden, um sichere Analysen an andere Ziele zu senden/weiterzuleiten.

Schritt 1: Melden Sie sich bei der SA Manager-Appliance an, und navigieren Sie zu Configure > Detection Response Management.



Phase 2: Navigieren Sie auf der neuen Seite zur Registerkarte Aktionen, suchen Sie nach dem standardmäßigen Posten An Syslog senden, und klicken Sie in der Spalte Aktion auf die Auslassungszeichen (...) und dann auf Bearbeiten.

Response Management

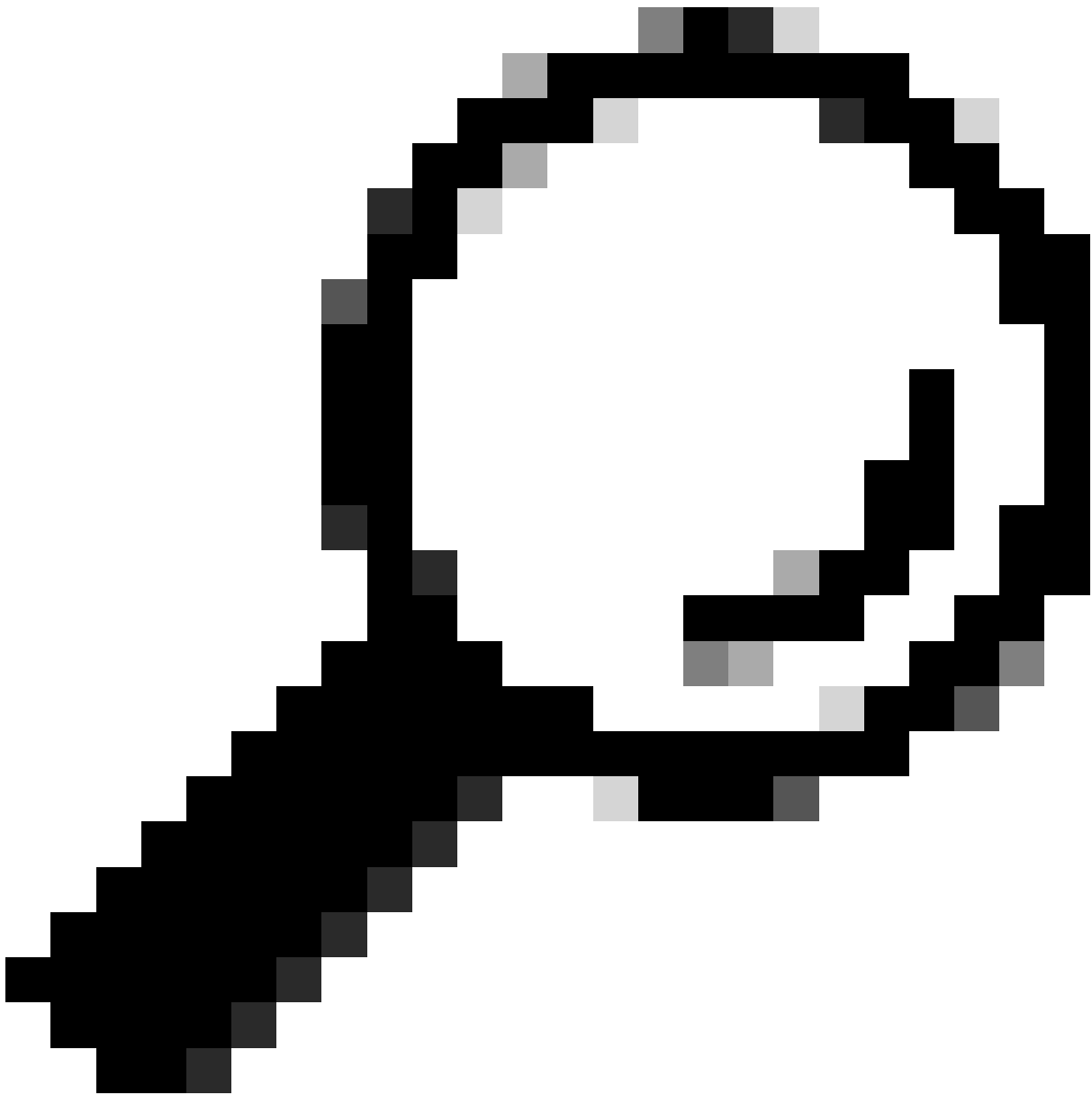
Rules Actions Syslog Formats

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	☒	...
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	☐	Edit Duplicate Delete

Schritt 3: Geben Sie die gewünschte Zieladresse in das Feld Syslog-Serveradresse und den gewünschten Ziel-Empfangsport in das Feld UDP-Port ein. Wählen Sie im Nachrichtenformat die Option CEF aus.

Schritt 4: Klicken Sie abschließend auf die blaue Schaltfläche Speichern in der rechten oberen Ecke.



Tipp: Der Standard-UDP-Port für Syslog ist 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

[Empty field]

UDP Port

514

Message Format

Custom

CEF

This action will use the ArcSight Common Event format.

Example Message

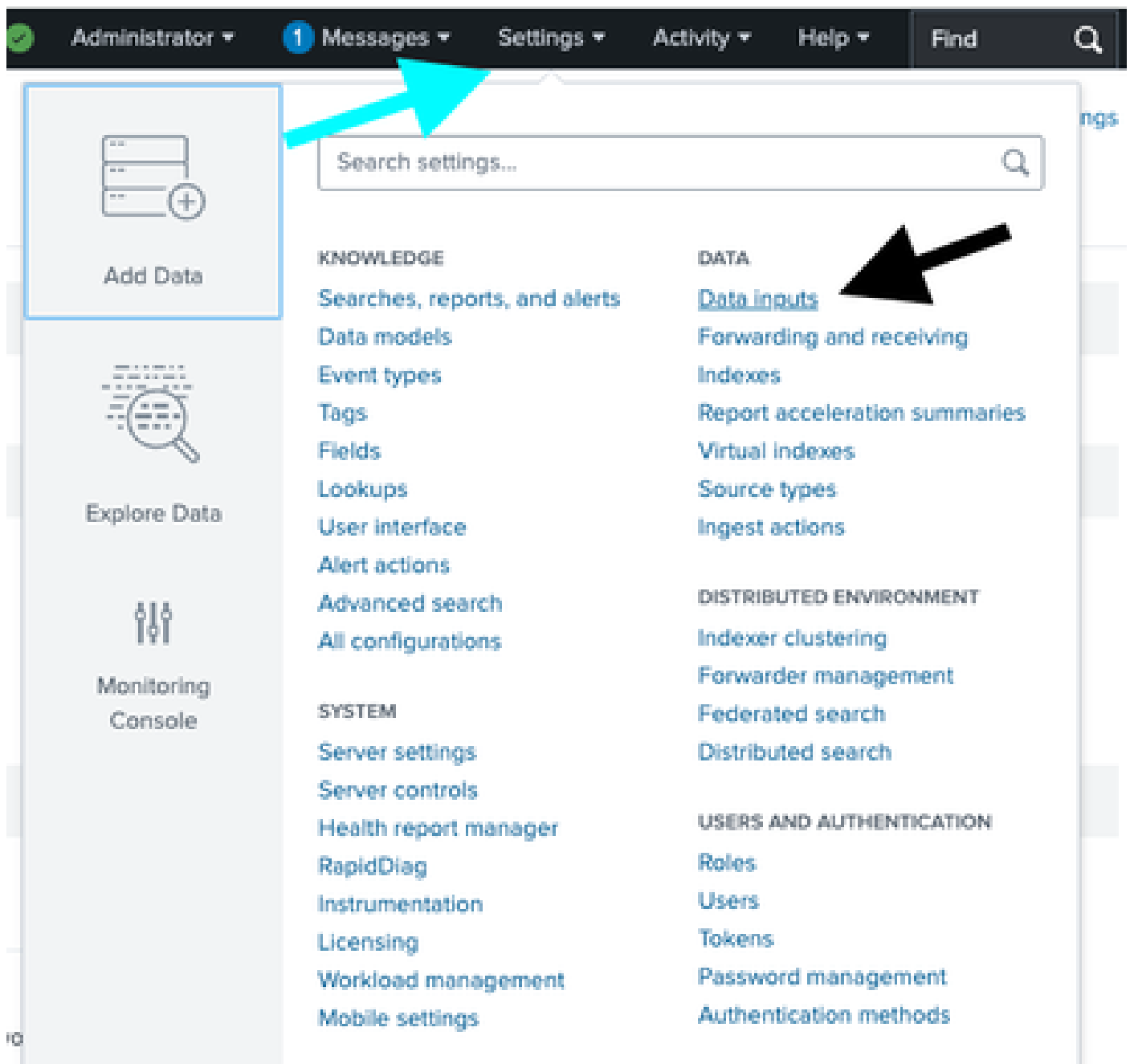
<131>Jan 01 00:00:00 test.host TestApp[1337]: CEF:0|Cisco|7.3.0|Notification:99|Bad Host|5|msg=This host has been observed performing malicious actions toward another host.:Source Host is http (80

Test Action

2. Konfigurieren von Splunk zum Empfangen von SNA-Syslogs über den UDP-Port

Nachdem Sie Ihre Änderungen auf die Webbenutzeroberfläche von Secure Network Analytics Manager angewendet haben, müssen Sie die Dateneingabe in Splunk konfigurieren.

Schritt 1: Melden Sie sich bei Splunk an, und navigieren Sie zu Einstellungen > Daten hinzufügen > DATEN-Eingaben.



Phase 2: Suchen Sie die UDP-Leitung, und wählen Sie +Neu hinzufügen aus.

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

Schritt 3: Wählen Sie auf der neuen Seite UDP aus, und geben Sie den Empfangs-Port wie 514 in das Feld Port ein.

Schritt 4: Geben Sie im Feld Überschreiben des Quellnamens Folgendes ein: desired name of source.

Schritt 5: Wenn Sie fertig sind, klicken Sie oben im Fenster auf die grüne Schaltfläche Weiter >.

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 ?

hostport

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?

Schritt 6: Wechseln Sie auf der nächsten Seite zur Option Neu, suchen Sie das Feld Quelltyp, und geben Sie desired source .

Schritt 7: Wählen Sie IP als Methode aus.

Schritt 8: Klicken Sie oben im Bildschirm auf die grüne Schaltfläche Überprüfen >.

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

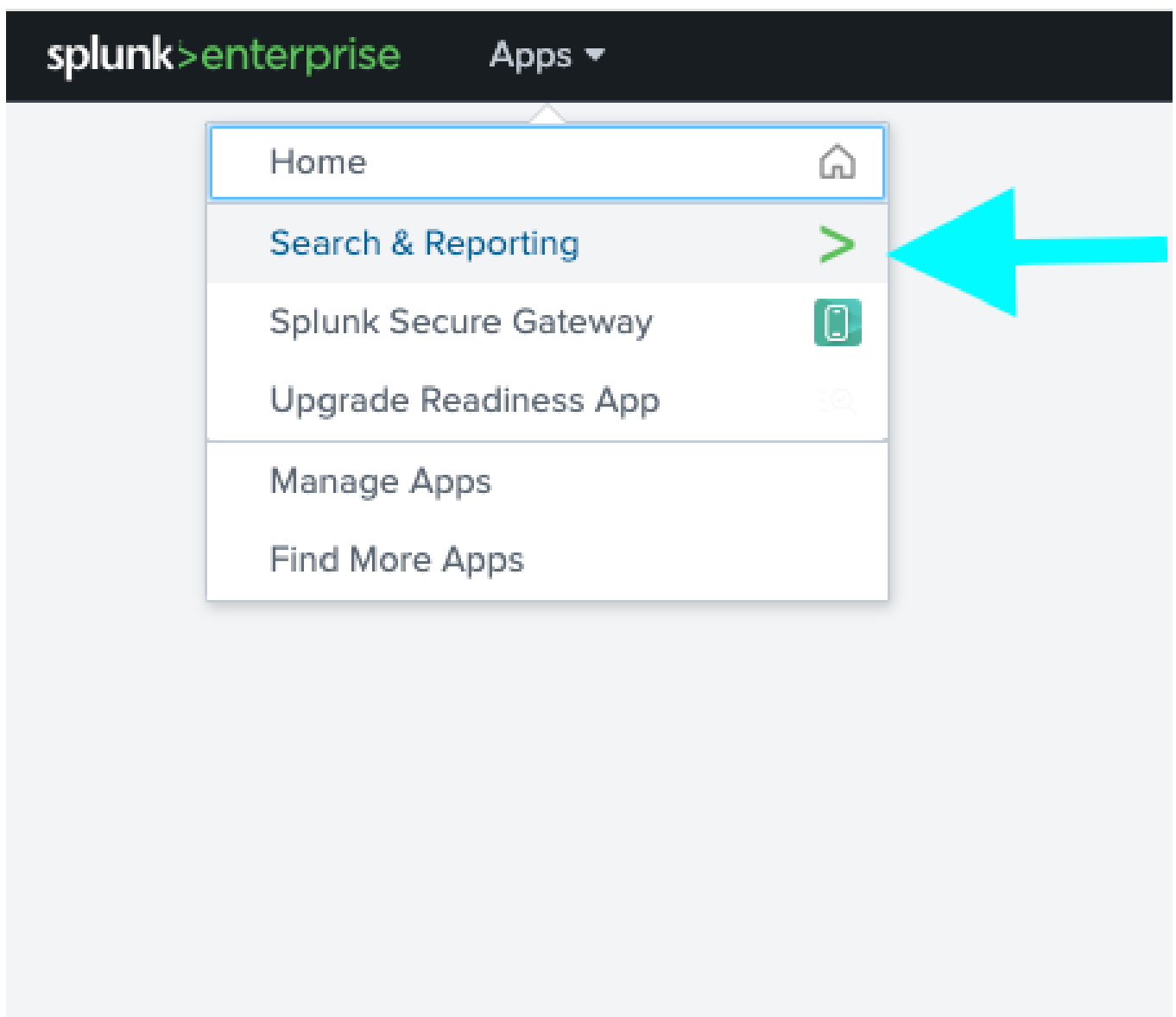
Schritt 9: Überprüfen Sie im nächsten Fenster Ihre Einstellungen, und bearbeiten Sie sie gegebenenfalls.

Phase 10: Klicken Sie nach der Validierung oben im Fenster auf die grüne Schaltfläche Submit > (Senden).

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

Phase 11: Navigieren Sie in der Webbenutzeroberfläche zu Apps > Search & Reporting.



Phase 12: Verwenden Sie auf der Seite "Suchen" den Filter `source="As_configured" sourcetype="As_configured"`,

um nach empfangenen Protokollen zu suchen.

New Search

source="*" :* sourcetype="*" Last 24 hours

6 events Event Sampling

Events (6) Patterns Statistics Visualization

Timeline format Zoom Out Zoom to Selection Deselect

Format Show: 20 Per Page View: List

Time	Event
	[FlowCollector Flow Data Lost[4]msg=; dst= src= ;
	end= externalId=80-1KUS-789L-PN6Z-5 cs3= cs3Label=SourceHostGroups cs4= cs4Label=TargetHostGroups cs5= cs5Label=Source_URL cs6= cs6Label=Target_URL dpt= proto= dvchost= i dvcpid=381 devl=
	ceExternalId= * / / cs2Label=SGTIDAndSGTName spt= destinationTranslatedAddress= destinationTranslatedPort= sourceTranslatedAddress= sourceTranslatedPort=
	host = source = sourcetype =

SELECTED FIELDS

- host 1
- source 1
- sourcetype 1

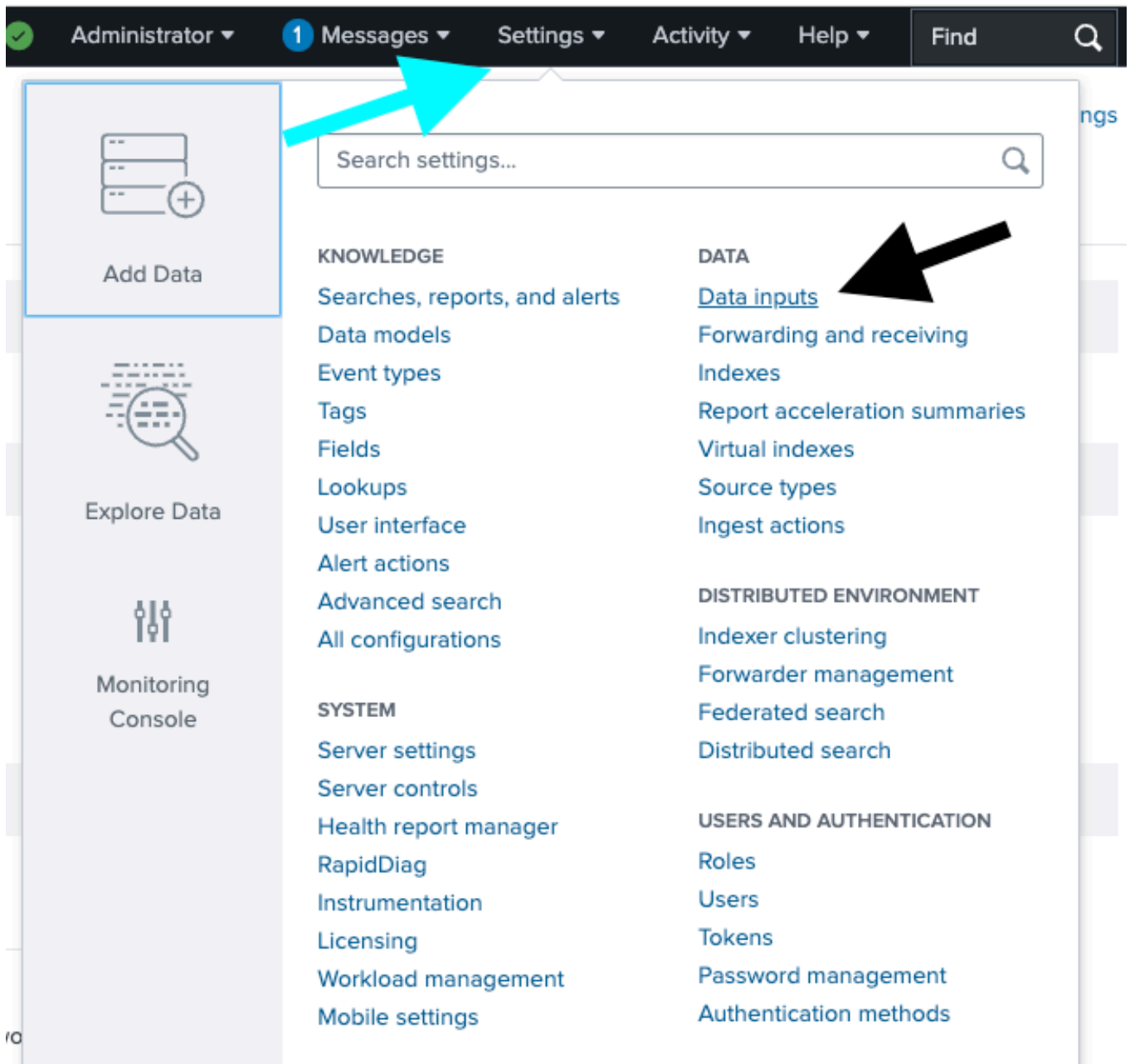
Anmerkung: Zur Quelle siehe Schritt 4

Informationen zu source_type finden Sie in Schritt 6.

Konfiguration von Syslog auf SNA über TCP-Port 6514 oder benutzerdefinierten Port

1. Splunk für den Empfang von SNA-Audit-Protokollen über TCP-Port konfigurieren

Schritt 1: Navigieren Sie in der Splunk-Benutzeroberfläche zu Einstellungen > Daten hinzufügen > Dateneingaben von DATEN.



Phase 2: Suchen Sie die TCP-Zeile, und wählen Sie + Neu hinzufügen aus.

Apps

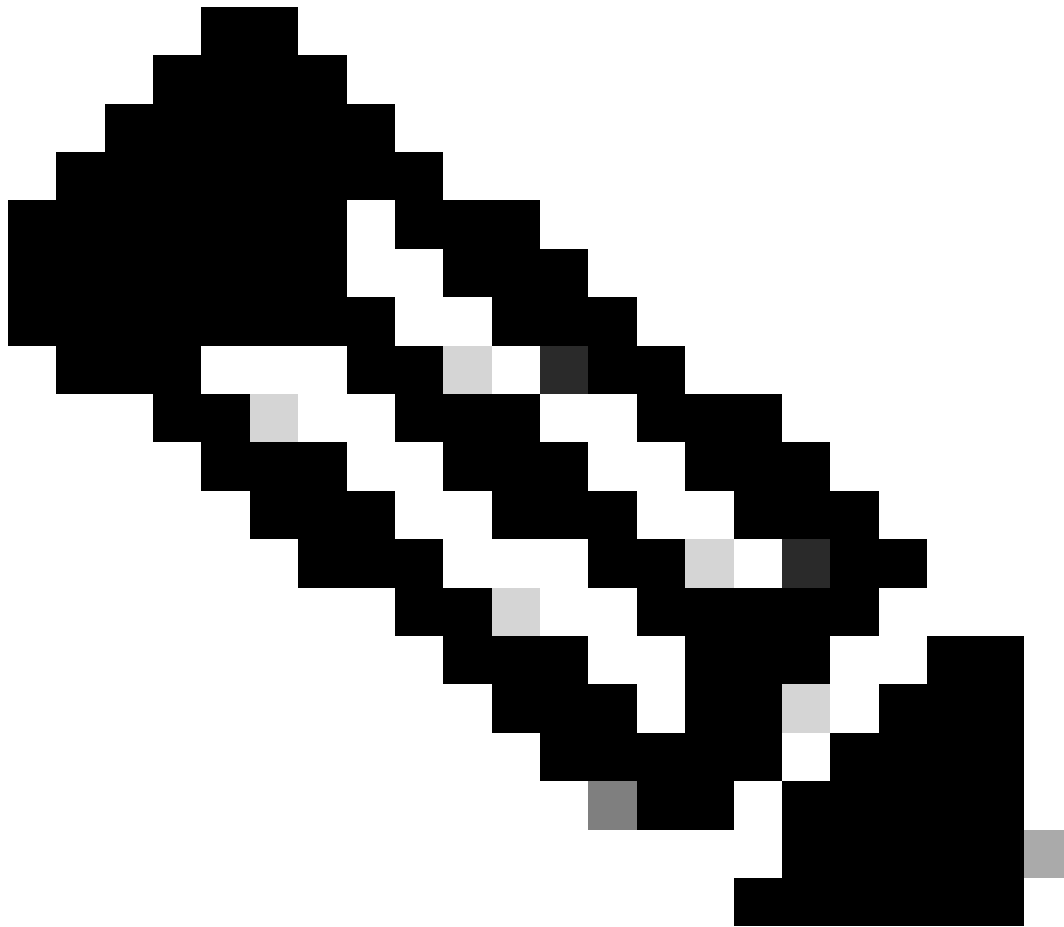
Administrator1 MessagesSettingsActivityHelp

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

Schritt 3: Wählen Sie im neuen Fenster die Option TCP aus, geben Sie den gewünschten Empfangs-Port in das Beispielfeld für den Port 6514 ein, und geben Sie im Feld Source name override (Quellname außer Kraft setzen) den gewünschten Namen ein.



Anmerkung: TCP 6514 ist der Standardport für Syslog über TLS

Schritt 4: Wenn Sie fertig sind, klicken Sie oben im Fenster auf die grüne Schaltfläche Weiter >.

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 ?

6514

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?

Schritt 5: Wählen Sie im Abschnitt Quellentyp im neuen Fenster die Option Neu aus, und geben Sie im Feld Quelltyp den gewünschten Namen ein.

Schritt 6: Wählen Sie im Host-Abschnitt IP als Methode aus.

Schritt 7: Wenn Sie fertig sind, klicken Sie oben im Fenster auf die grüne Schaltfläche Prüfen >.

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

Schritt 8: Überprüfen Sie im nächsten Fenster Ihre Einstellungen, und bearbeiten Sie sie gegebenenfalls. Klicken Sie nach der Validierung oben im Fenster auf die grüne Schaltfläche Submit > (Senden).

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.Zertifikat für Splunk generieren

Schritt 1: Führen Sie auf einem Computer, auf dem OpenSSL installiert ist, den `sudo openssl req -x509 -newkey rsa:4096 -keyout server_key.pem -out server_cert.pem -sha256 -days 3650 -subj /CN=10.106.127.4` Befehl aus, und ersetzen

```
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:  
-----
```

Nach Abschluss des Befehls werden zwei Dateien generiert. Die Dateien `server_cert.pem` und `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:
```

Phase 2: Wechseln Sie zum Root-Benutzer.

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

Schritt 3: Kopieren Sie das neu generierte Zertifikat in den `/opt/splunk/etc/auth/`.

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

Schritt 4: Anhängen der Datei "punkweb.cet" mit einem privaten Schlüssel.

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

Schritt 5: Ändern des Besitzes des Splunk-Zertifikats

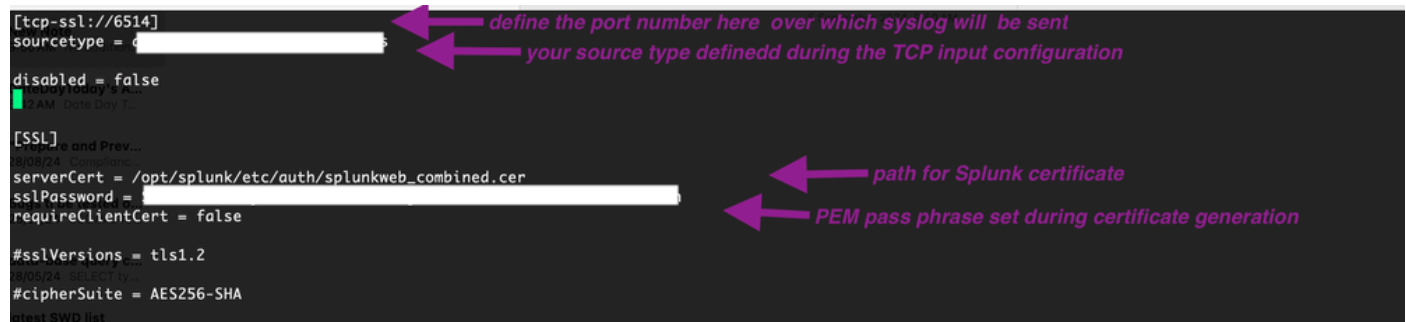
```
user@examplehost:~# chown 10777:10777/opt/splunk/etc/auth/splunkweb.cer
```

Schritt 6: Ändern der Berechtigung für das Splunk-Zertifikat

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

Schritt 7: Erstellen Sie eine neue Datei input.conf.

```
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

Schritt 8: Überprüfen Sie die Syslogs mithilfe der Suchfunktion.

Home



Search & Reporting



Splunk Secure Gateway

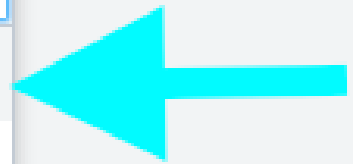


Upgrade Readiness App



Manage Apps

Find More Apps



New Search

source="*" "sourcetype=" " host = 1 Last 24 hours

✓ 126 events | No Event Sampling

Events (126) Patterns Statistics Visualization

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

List Format 50 Per Page

< Hide Fields All Fields

SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1

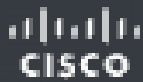
INTERESTING FIELDS

- # date_hour 5

Time	Event
>	< AuditLogger[1425542]: osaxsd/1425542, Login on ssh failed: Unknown User
host =	source = sourcetype =
>	< AuditLogger[1425538]: osaxsd/1425538, Login on ssh failed: Unknown User
host =	source = sourcetype =
>	< AuditLogger[1424634]: osaxsd/1424634, Login on ssh failed: Unknown User
host =	source = sourcetype =

3. Konfigurieren des Prüfprotokollziels auf SNA

Schritt 1: Melden Sie sich bei der SMC-Benutzeroberfläche an, und navigieren Sie zu Configure > Central Management.



nse



Monitor



Investigate



Report



Configure

Configure



Detection

Host Group Management

Alarm Severity

Policy Management

Response Management

Network Scanners

Analytics

Alerts

Global

 Central Management

Phase 2: Klicken Sie auf das Auslassungszeichen-Symbol der gewünschten SNA-Appliance, und wählen Sie Einheit-Konfiguration bearbeiten aus.

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				...

Schritt 3: Navigieren Sie zur Registerkarte Network Services (Netzwerkdienste), und geben Sie Details zum Ziel des Überwachungsprotokolls (Syslog über TLS) ein.

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

Schritt 4: Navigieren Sie zur Registerkarte General (Allgemein), scrollen Sie nach unten, und klicken Sie auf Add new (Neu hinzufügen), um das zuvor erstellte Splunk-Zertifikat mit dem Namen server_cert.pem hochzuladen.

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 ENROLL

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

Schritt 5: Klicken Sie auf Einstellungen übernehmen.

Cancel Apply Settings

Fehlerbehebung

Es könnte komplettes Kauderwelsch auf der Suche sein.

splunk>enterprise Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find 🔍

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search

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 >

< Hide Fields	≡ All Fields	i	Time	Event
SELECTED FIELDS				
a host 1				
a source 1				
a sourcetype 1				
INTERESTING FIELDS				
a index 1				
# linecount 6				
a punct 79				
a splunk_server 1				
a timestamp 1				
34 more fields				
+ Extract New Fields				
		>		<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 0/\x00\x9E\x003\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\x003\x00G\x00E\x00 \x00A \xA7\xB9\xB3\xEC\xC91 \x81g=R \^d\xC1 \xD0As[z\x9C 9\xE1\x91\xEC\xEDw\xD9p 6\x954\x88U\xC4\xFA\x920\xA5\x81!\xA3 \x00\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\xA1T\x8C\xB0\xDCY , I (' \xAE\x84+\xF0B\xC3s , \xBA(\xF1\x9A \xED\xD3\xFC6\xFE\x8E\xC5\xD9\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 </pre>

Show all 6 lines Google Chrome

Lösung:

Ordnen Sie die Eingabe dem richtigen Quelltyp zu.



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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.