

Configuración de Response Management para enviar eventos de Syslog a Splunk

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configuración de syslog en SNA sobre UDP 514 o puerto definido personalizado](#)

[1.Gestión de respuestas SNA](#)

[2.Configuración de Splunk para Recibir los Registros del Sistema SNA sobre el puerto UDP](#)

[Configuración de syslog en SNA a través del puerto TCP 6514 o del puerto definido personalizado](#)

[1.Configuración de Splunk para Recibir Registros de Auditoría SNA sobre el Puerto TCP](#)

[2.Generar certificado para Splunk](#)

[3.Configure el destino del registro de auditoría en SNA](#)

[Troubleshoot](#)

Introducción

Este documento describe cómo configurar la función Secure Analytics Response Management para enviar eventos a través de syslog a un tercero como Splunk.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

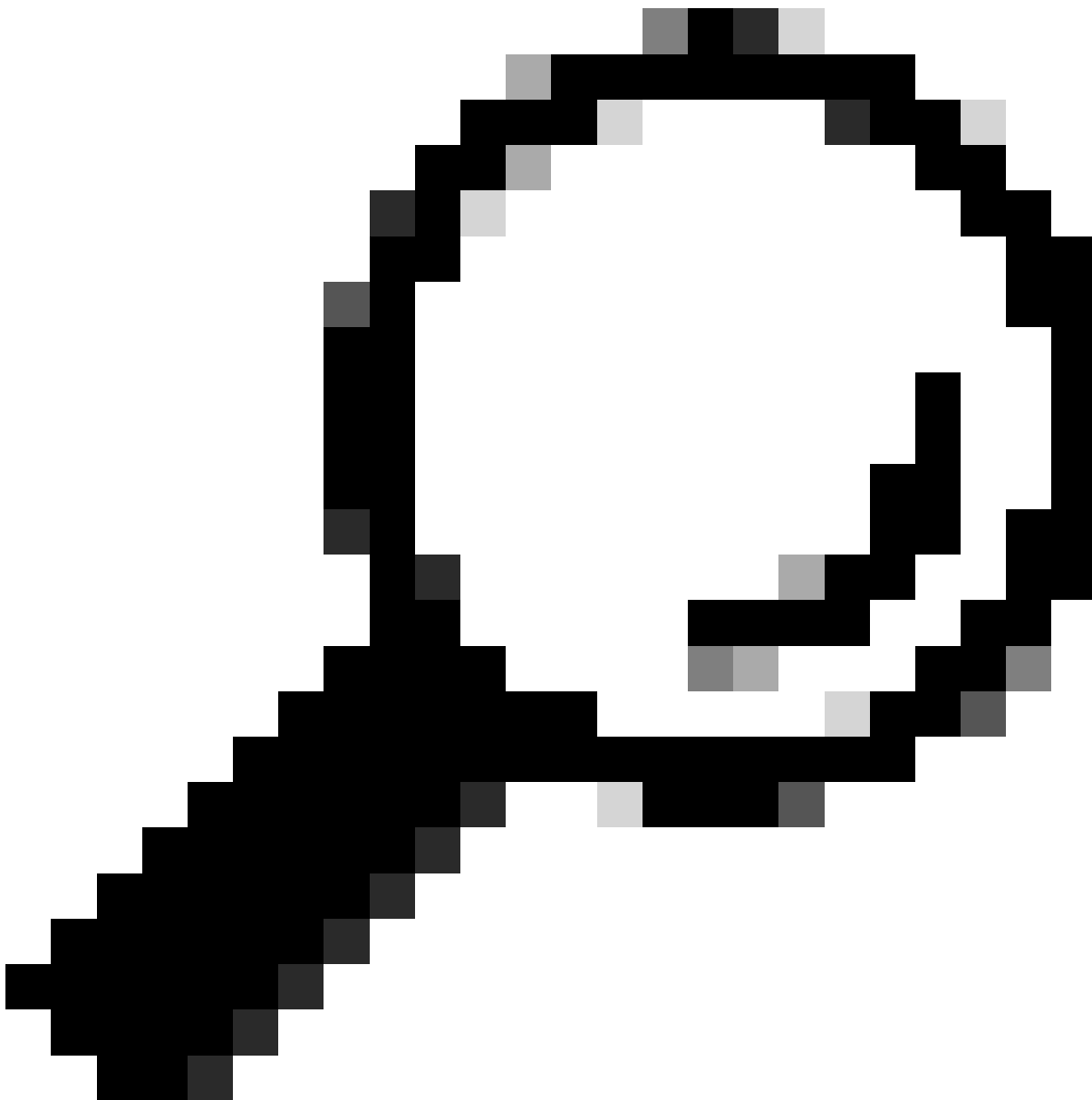
- Gestión de respuesta de Secure Network Analytics.
- Splunk Syslog

Componentes Utilizados

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

- Implementación de Secure Network Analytics (SNA) que contiene al menos un dispositivo Manager y un dispositivo Flow Collector.
- Servidor Splunk instalado y accesible a través de 443 puertos.

Configuración de syslog en SNA sobre UDP 514 o puerto definido personalizado



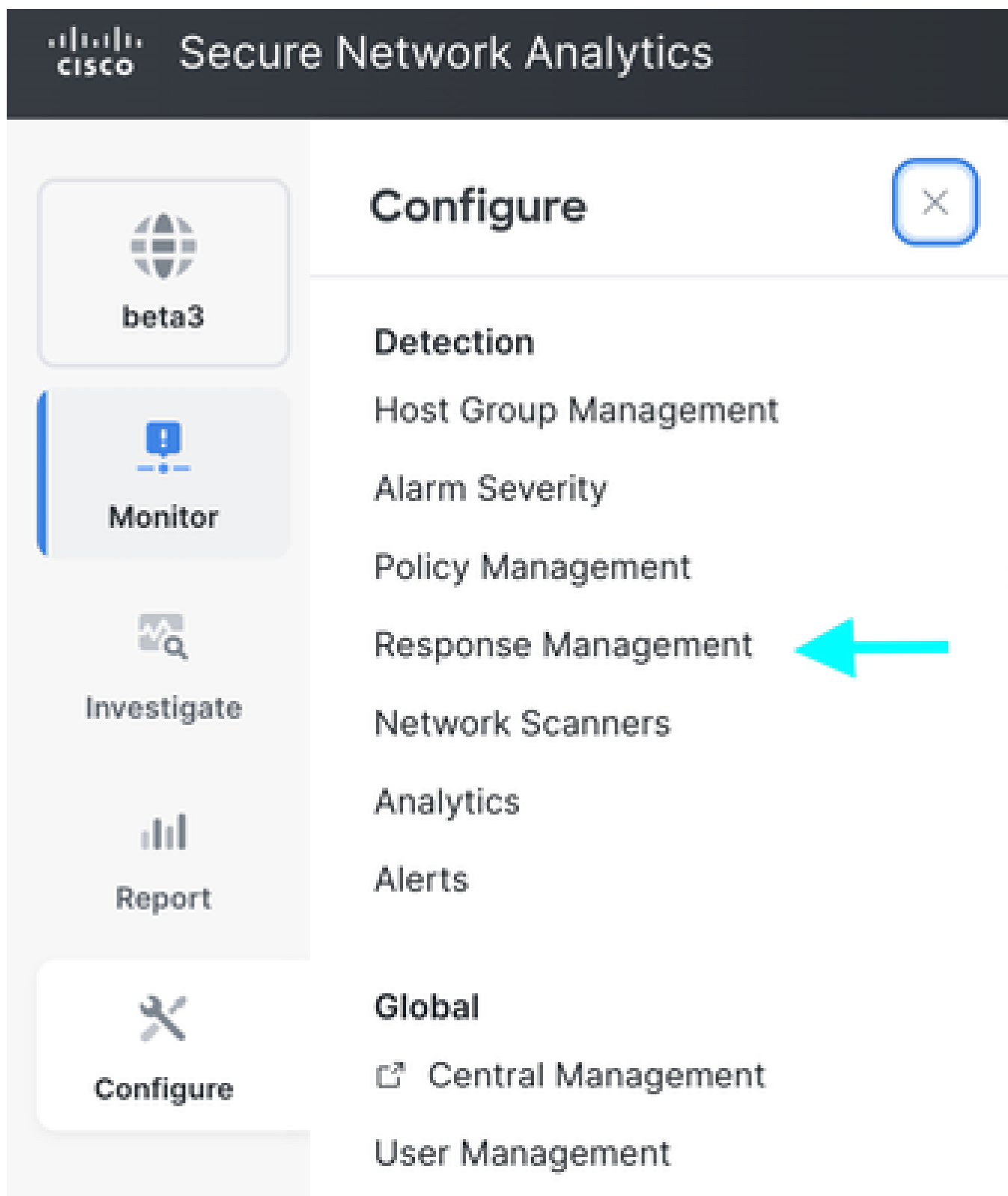
Sugerencia: asegúrese de que UDP/514, TCP/6514 o cualquier puerto personalizado que elija para syslog esté permitido en cualquier firewall o dispositivo intermedio entre SNA y Splunk.

1. Gestión de respuestas SNA

El componente Response Management de Secure Analytics (SA) se puede utilizar para configurar reglas, acciones y destinos de syslog.

Estas opciones deben configurarse para enviar/reenviar alarmas de Secure Analytics a otros destinos.

Paso 1: Inicie sesión en el dispositivo SA Manager y navegue hasta Configure > Detection Response Management.



Paso 2: En la nueva página, desplácese a la ficha Acciones, busque el elemento de línea predeterminado Enviar a Syslog y haga clic en los puntos suspensivos (...) en la columna Acción

y, a continuación, en Editar.

Response Management

Rules Actions Syslog Formats

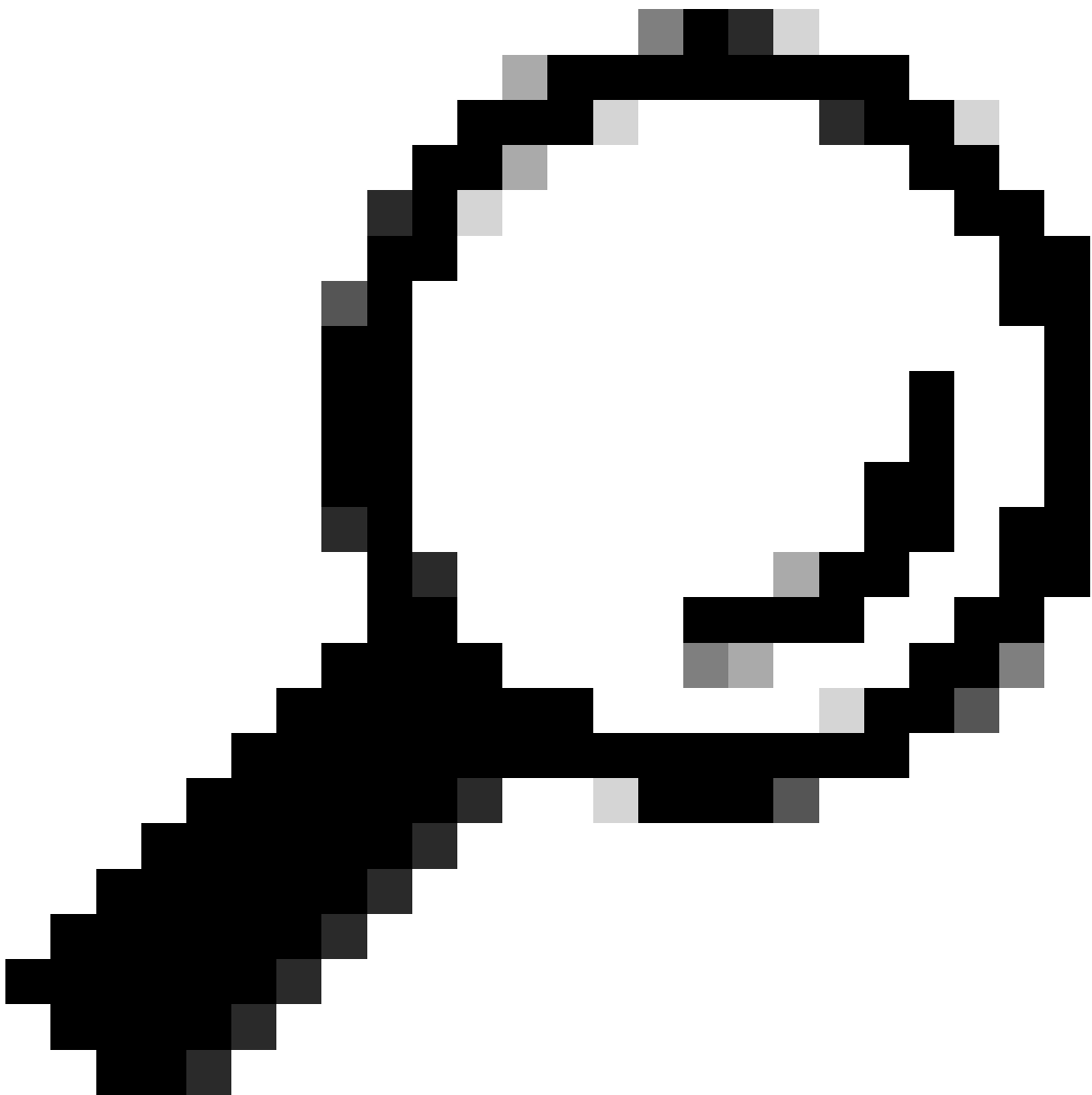
Actions [Add New Action](#)

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

Paso 3: Ingrese la dirección de destino deseada en el campo Syslog Server Address, y el puerto de recepción de destino deseado en el campo UDP Port. En Formato de mensaje, seleccione CEF.

Paso 4: Cuando haya terminado, haga clic en el botón azul Save situado en la esquina superior derecha.



Consejo: El puerto UDP predeterminado para syslog es 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

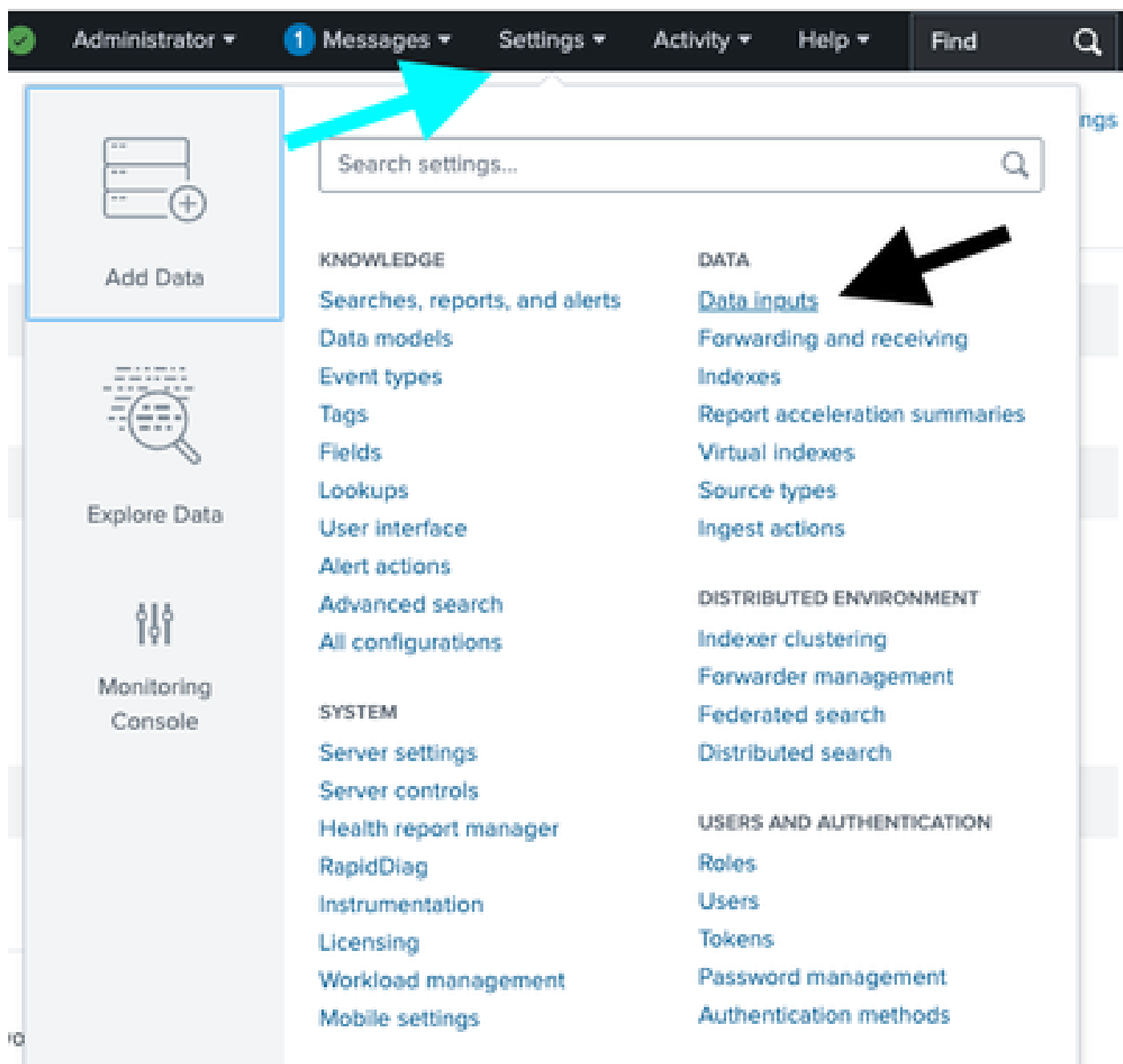
<131>Jan 01 00:00:00 test.host TestApp[1337]: CEF:0|Cisco|7.3.0|Notification:99|Bad Host|5|msg=This host has been observed performing malicious actions toward another host.:Source Host is http (80

Test Action

2. Configuración de Splunk para Recibir los Registros del Sistema SNA sobre el puerto UDP

Después de aplicar los cambios en la interfaz de usuario web de Secure Network Analytics Manager , debe configurar la entrada de datos en Splunk.

Paso 1: Inicie sesión en Splunk y navegue hasta Settings > Add Data > DATA Data Inputs.



Paso 2: Localice la línea UDP y seleccione +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

Paso 3: En la nueva página, seleccione UDP, ingrese el puerto de recepción como 514 en el campo Port.

Paso 4: En el campo Source name override, introduzca desired name of source.

Paso 5: Cuando termine, haga clic en el botón verde Next > en la parte superior de la ventana.

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?

Paso 6: En la página siguiente, cambie a la opción New, busque el campo Source Type y escriba desired source .

Paso 7: Seleccione IP para el Método.

Paso 8: Haga clic en el botón verde Review > situado en la parte superior de la pantalla.

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

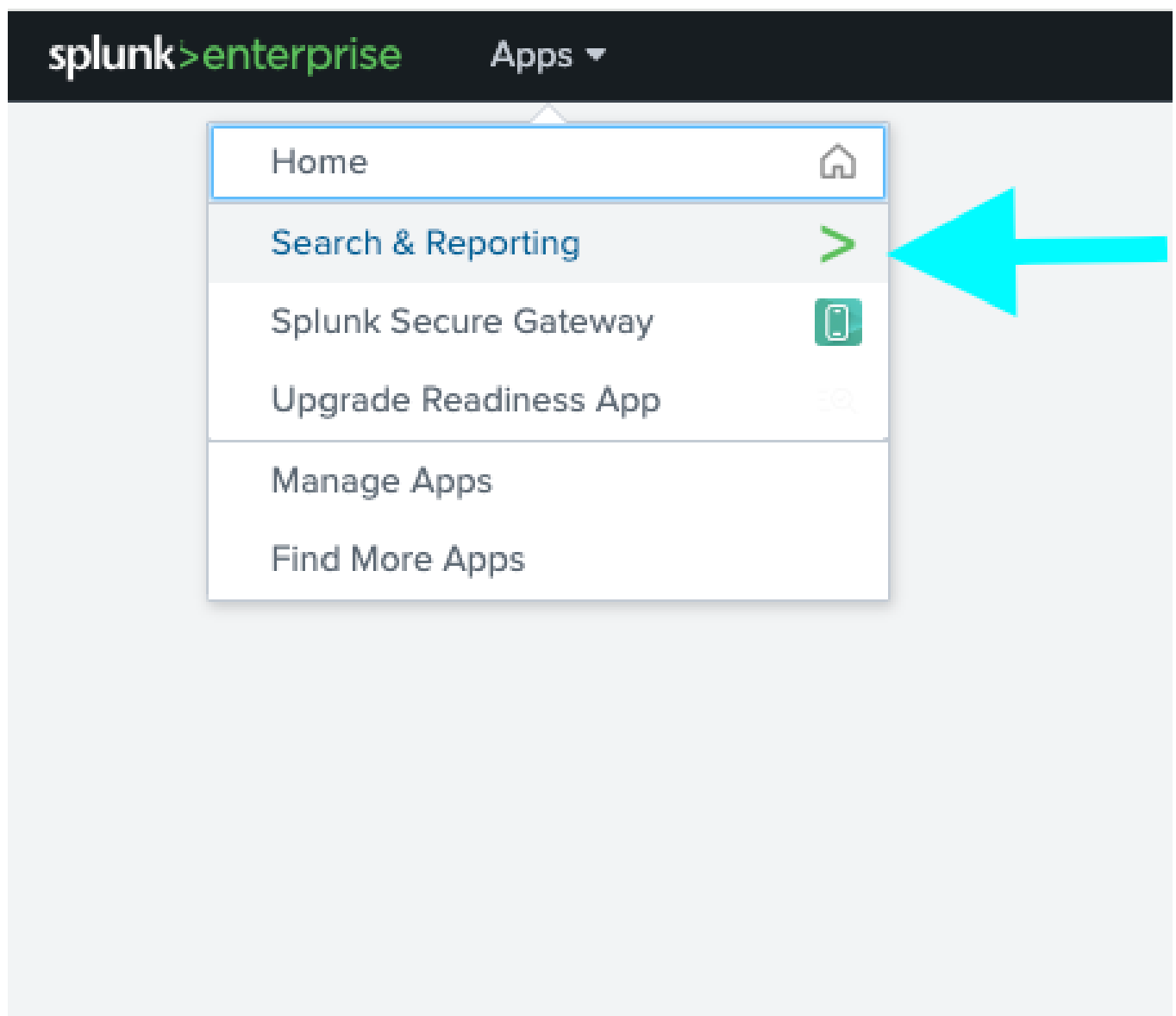
Paso 9: En la siguiente ventana, revise la configuración y edítela si es necesario.

Paso 10: Una vez validado, haga clic en el botón verde Submit > en la parte superior de la ventana.

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

Paso 11: Navegue hasta Aplicaciones > Buscar e informar en la interfaz de usuario web.



Paso 12: En la página Buscar, utilice el filtro `source="As_configured" sourcetype="As_configured"` para buscar los

registros recibidos.

New Search

source="*" : " sourcetype=":

6 events

Events (6) Patterns Statistics Visualization

Timeline format Zoom Out Zoom to Selection Deselect

Format Show: 20 Per Page View: List

Time	Event
	end= externalId=80-1KUS-7R9L-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

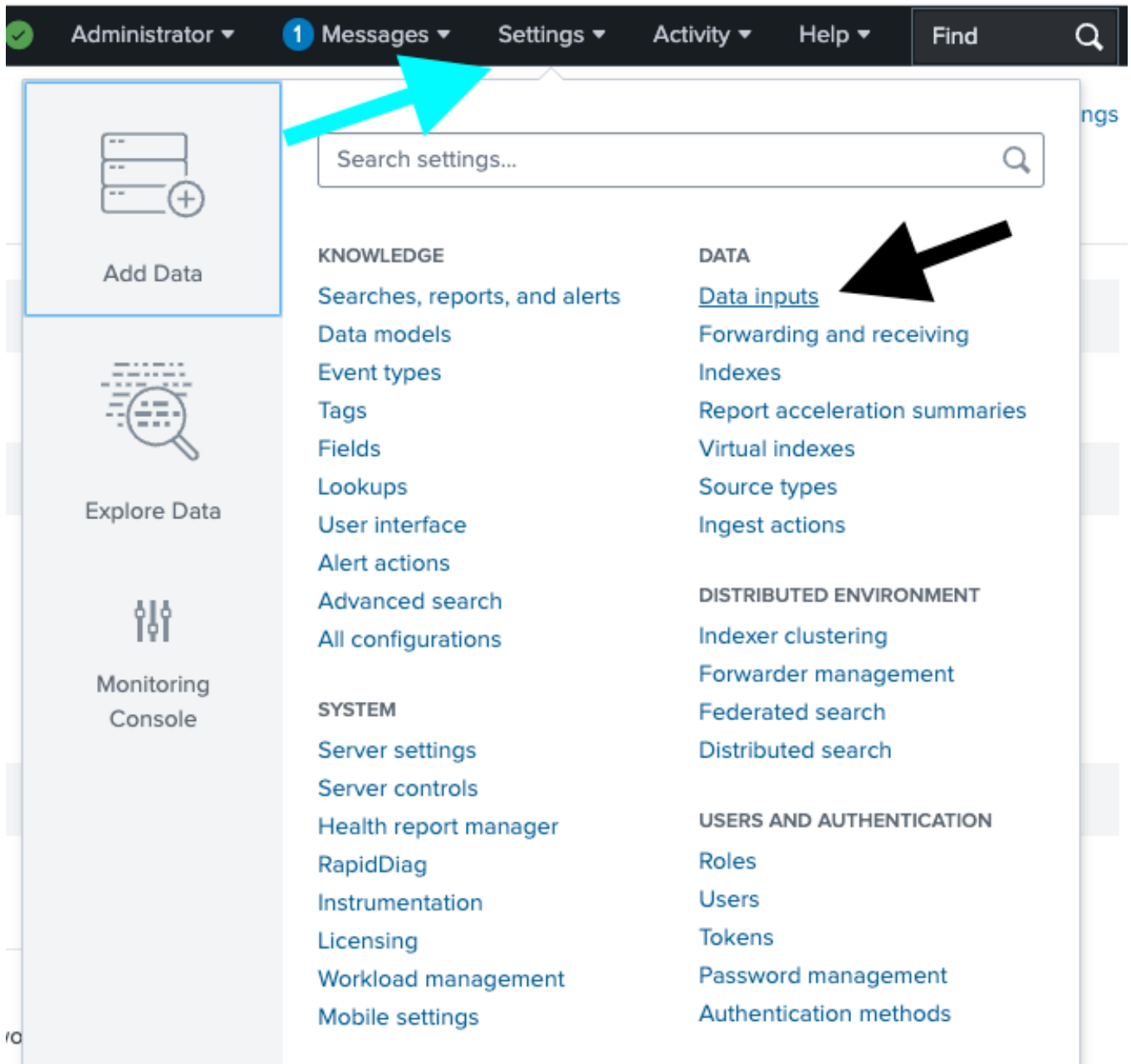
- host 1
- source 1
- sourcetype 1

Nota: Para ver el origen, consulte el paso 4
Para source_type, vea el Paso 6

Configuración de syslog en SNA a través del puerto TCP 6514 o del puerto definido personalizado

1. Configuración de Splunk para Recibir Registros de Auditoría SNA sobre el Puerto TCP

Paso 1: En la interfaz de usuario de Splunk, navegue hasta Configuraciones > Agregar datos > Entradas de datos de datos.



Paso 2: Localice la línea TCP y seleccione + 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

Paso 3: En la nueva ventana, seleccione TCP, ingrese el puerto de recepción deseado, en el puerto de imagen de ejemplo 6514, e ingrese "desired name" en el campo Source name override.



Nota: TCP 6514 es el puerto predeterminado para syslog sobre TLS

Paso 4: Cuando termine, haga clic en el botón verde Next > en la parte superior de la ventana.

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?

Paso 5: En la nueva ventana, seleccione Nuevo en la sección Tipo de origen, ingrese el nombre deseado en el campo Tipo de origen.

Paso 6: Seleccione IP para el Método en la sección Host.

Paso 7: Cuando haya terminado, seleccione el botón verde Revisar > en la parte superior de la ventana.

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

Add Data

Select Source Input Settings Review Done

< 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

Paso 8: En la siguiente ventana, revise la configuración y edítela si es necesario. Una vez validado, haga clic en el botón verde Submit > en la parte superior de la ventana.

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

Add Data

Select Source Input Settings Review Done

< 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. Generar certificado para Splunk

Paso 1: Con una máquina que tenga instalado openssl, ejecute el 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`, reemplazando la IP de ejemplo de 10.106.127.4 con la IP del dispositivo Splunk. Se le pedirá dos veces que introduzca una frase de paso definida por el usuario. En los ejemplos, los comandos se ejecutan desde la línea de comandos de la máquina Splunk.

[illegible]

Cuando se completa el comando, se generan dos archivos. Los archivos `server_cert.pem` y `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:
```

Paso 2: Cambiar al usuario raíz.

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

Paso 3: Copie el certificado recién generado en el `/opt/splunk/etc/auth/`.

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

Paso 4: Añada el archivo spunkweb.cet con clave privada.

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

Paso 5: Cambiar la propiedad del certificado splunk.

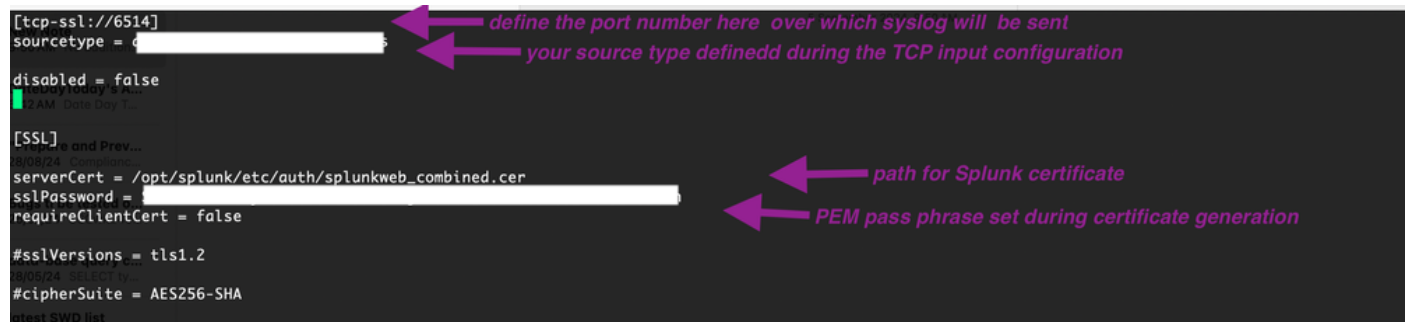
```
user@examplehost:~# chown 10777:10777/opt/splunk/etc/auth/splunkweb.cer
```

Paso 6: Cambie el permiso para el certificado de splunk.

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

Paso 7: cree un nuevo archivo 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
```

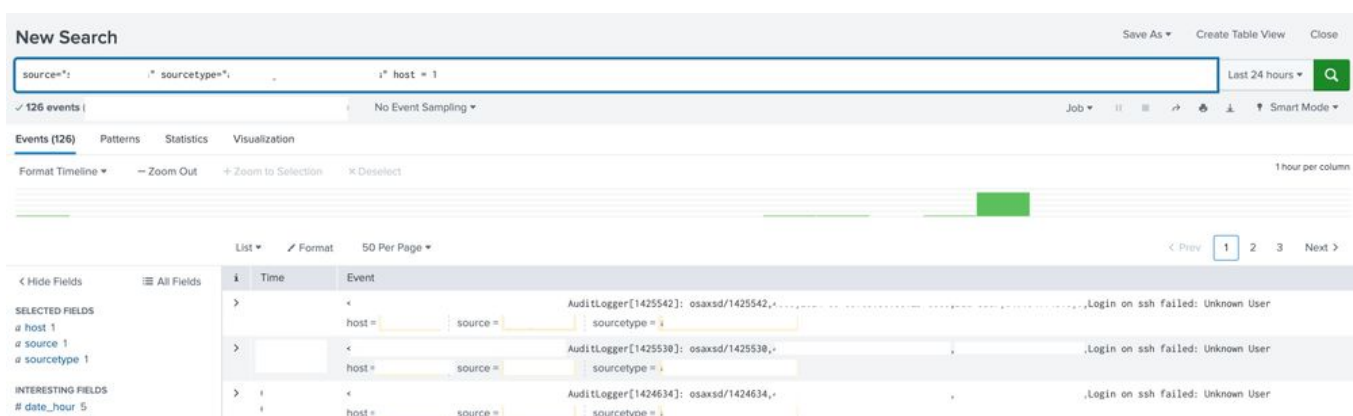
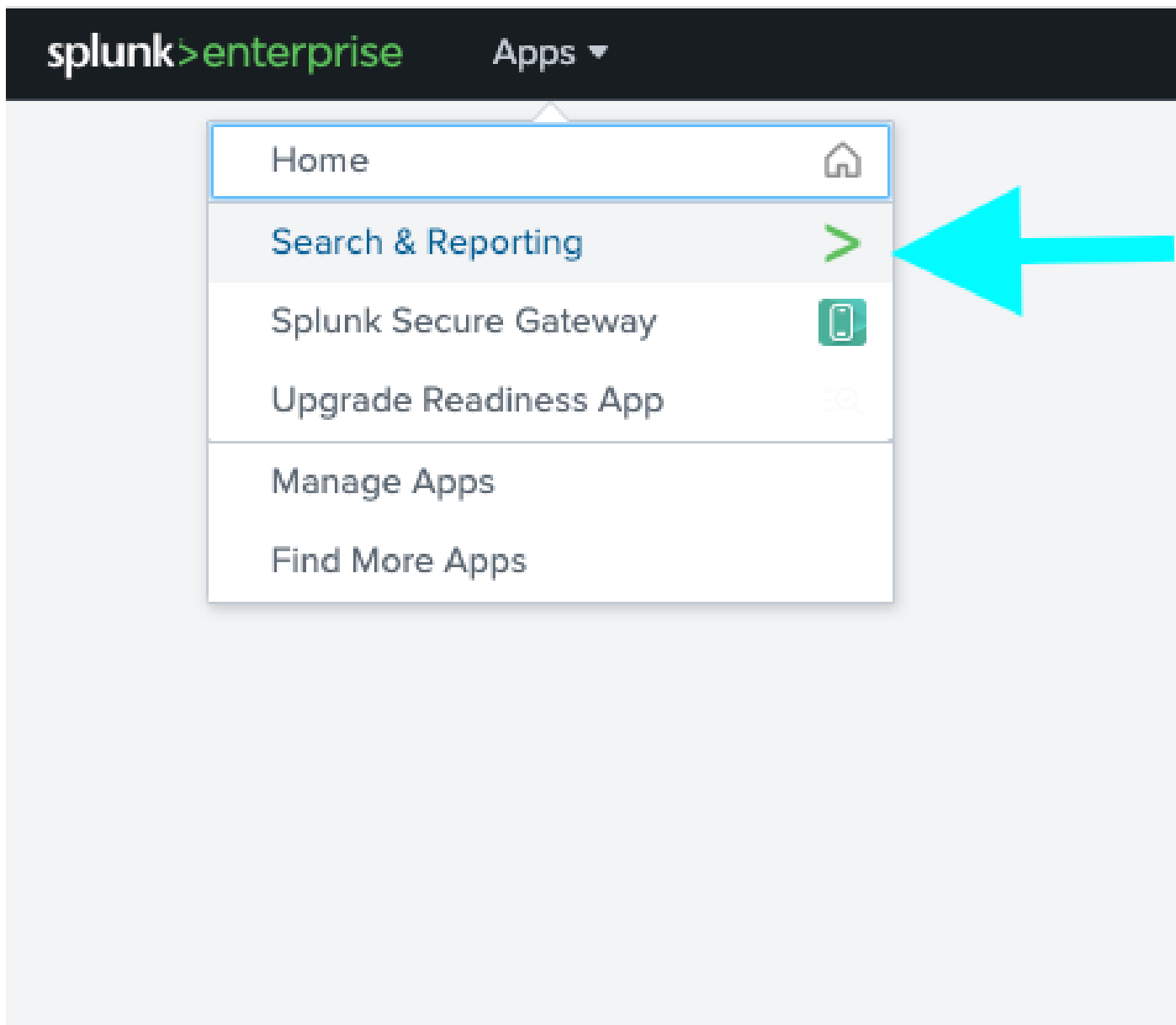
define the port number here over which syslog will be sent

your source type defined during the TCP input configuration

path for Splunk certificate

PEM pass phrase set during certificate generation

Paso 8: Verifique los registros del sistema mediante la búsqueda.



3. Configure el destino del registro de auditoría en SNA

Paso 1: Inicie sesión en la interfaz de usuario de SMC y navegue hasta Configurar > Administración central.



nse



Monitor



Investigate



Report



Configure

Configure



Detection

Host Group Management

Alarm Severity

Policy Management

Response Management

Network Scanners

Analytics

Alerts

Global

 Central Management

... ..

Paso 2: Haga clic en el icono de puntos suspensivos del dispositivo SNA que desee y seleccione Editar configuración del dispositivo.

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				...

Paso 3: Navegue hasta la pestaña Servicios de red e ingrese los detalles de Destino de registro de auditoría (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

Paso 4: Navegue hasta la ficha General, desplácese hacia abajo y haga clic en Add new para cargar el certificado Splunk creado anteriormente denominado 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 EMAIL

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

Paso 5: Haga clic en Aplicar configuración.

Cancel Apply Settings

Troubleshoot

Podría haber un completo galimatías apareciendo en la búsqueda.



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

filter

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

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).