

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

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar syslog em SNA sobre UDP 514 ou porta definida personalizada](#)

[1. Gerenciamento de resposta SNA](#)

[2. Configuração do Splunk para Receber Syslogs SNA pela porta UDP](#)

[Configurar o syslog em SNA pela porta TCP 6514 ou pela porta definida personalizada](#)

[1. Configuração do Splunk para Receber Logs de Auditoria SNA pela porta TCP](#)

[2. Gerar Certificado para Splunk](#)

[3. Configurar o destino do log de auditoria em redes SNA](#)

[Troubleshooting](#)

Introdução

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

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

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

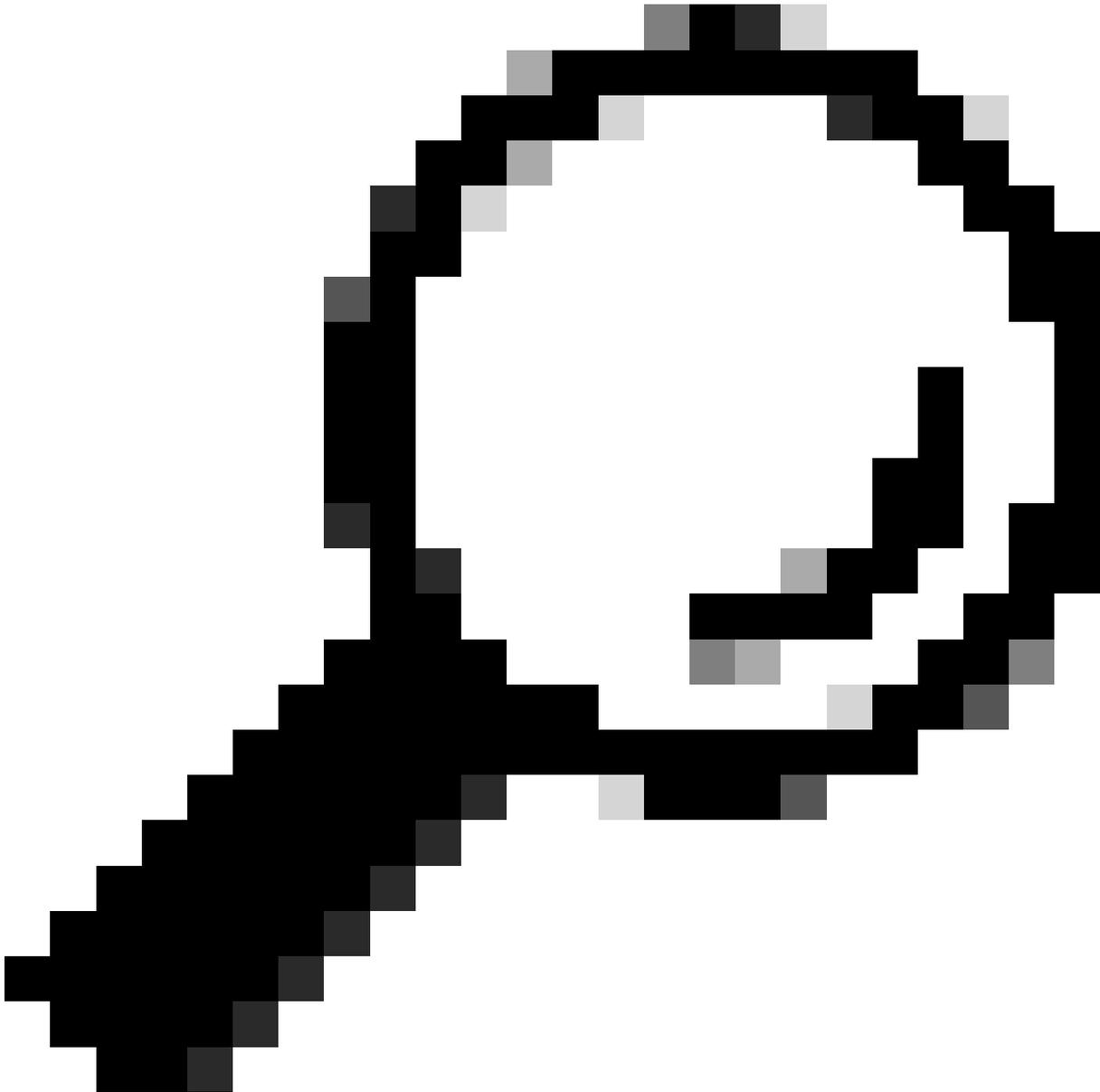
Componentes Utilizados

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

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

- Servidor Splunk instalado e acessível por 443 portas.

Configurar syslog em SNA sobre UDP 514 ou porta definida personalizada



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

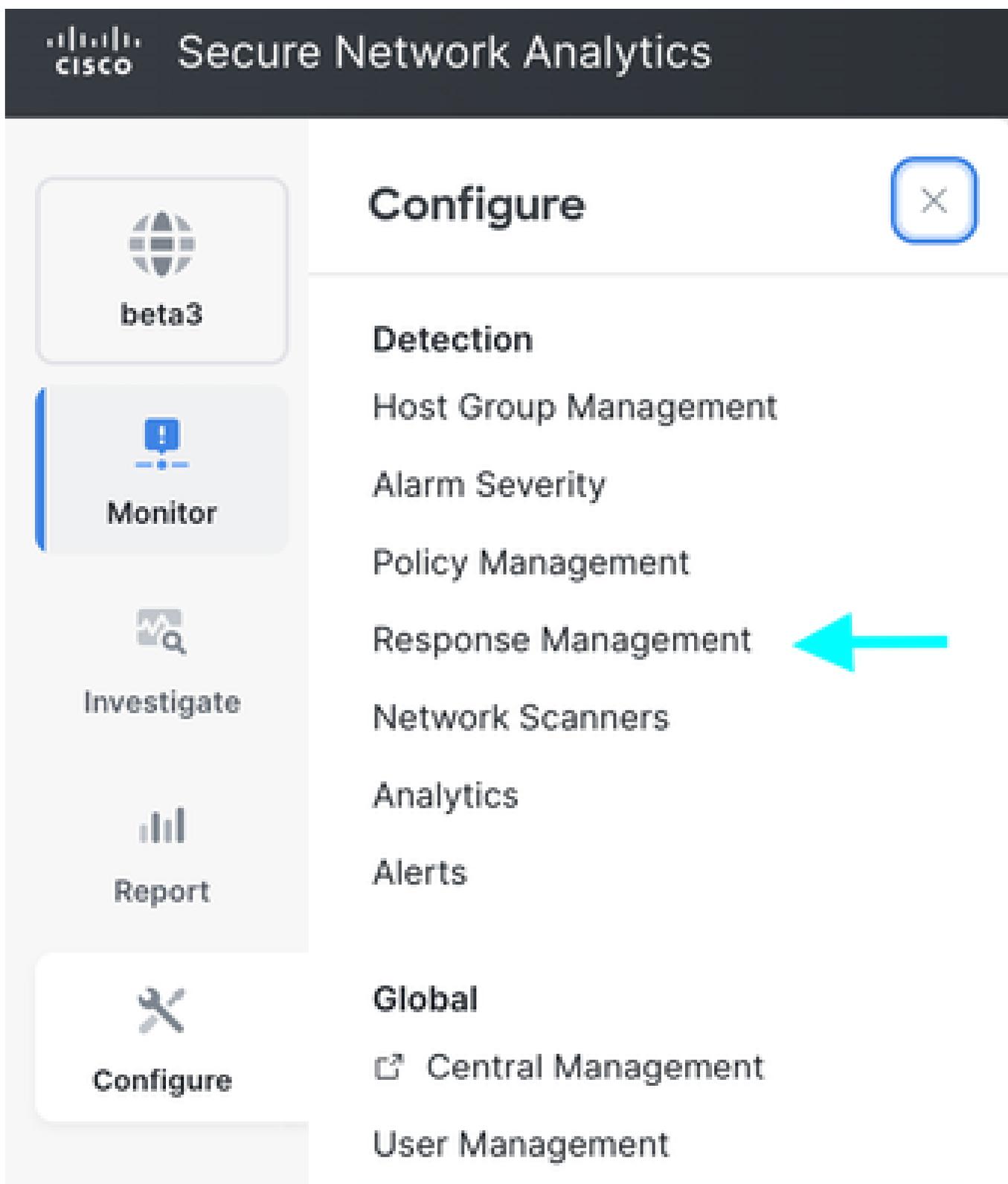
1. Gerenciamento de resposta SNA

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

configurar Regras, Ações e Destinos de syslog.

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

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



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

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

Response Management

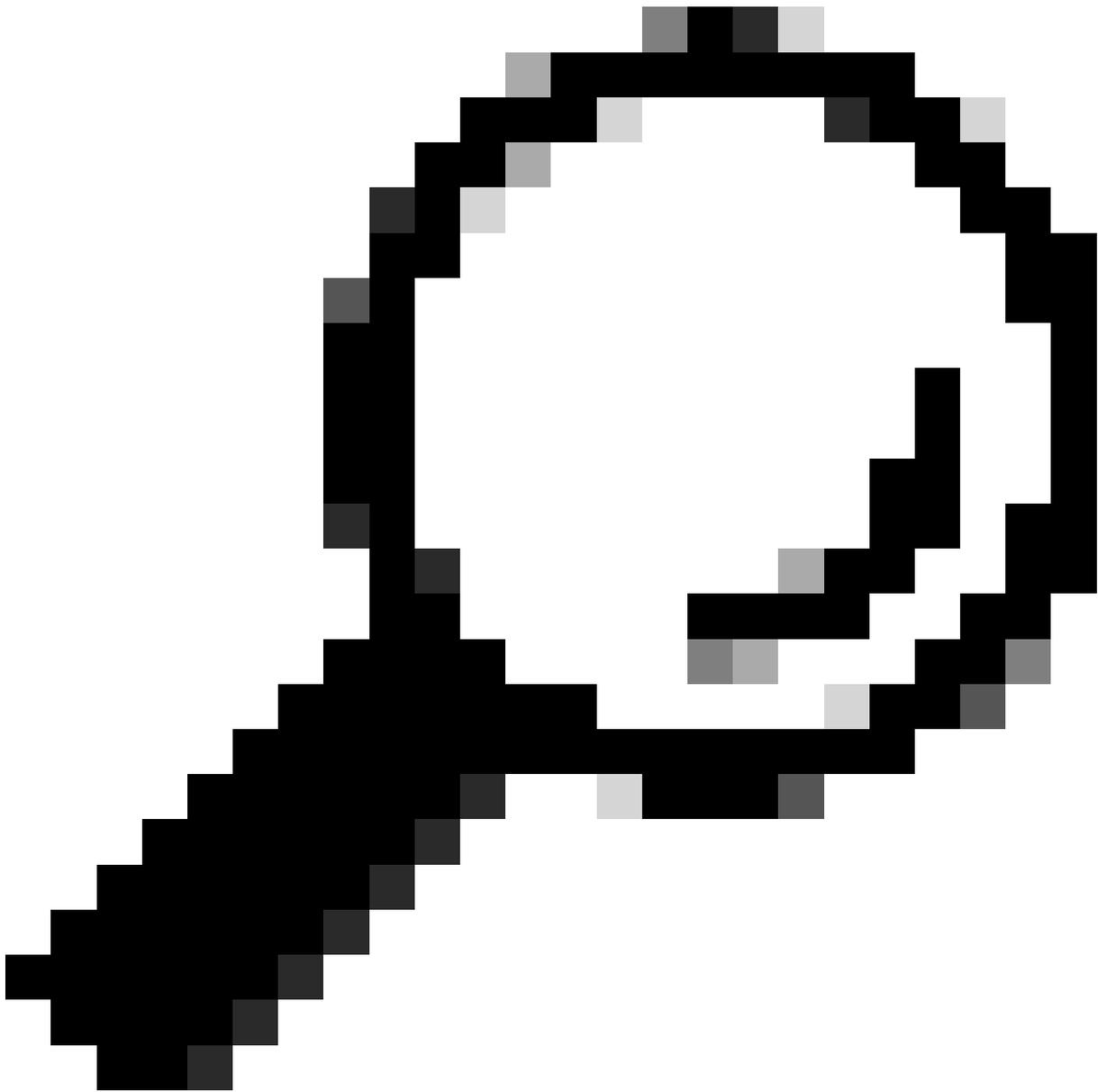
Rules Actions Syslog Formats

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	<input type="checkbox"/>	...
Send email	Email (Alert)	Sends an email to the recipients designated in the To field on the Email (Alert) Action page.	2	<input type="checkbox"/>	...
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	<input checked="" type="checkbox"/>	...
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	<input type="checkbox"/>	... Edit Duplicate Delete

Passo 3: Insira o endereço de destino desejado no campo Syslog Server Address e a porta de recebimento de destino desejada no campo UDP Port. No Formato da mensagem, selecione CEF.

Passo 4: Quando terminar, clique no botão azul Save no canto superior direito.



Tip: A porta UDP padrão para syslog é 514

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

[Redacted]

UDP Port

514

Message Format

Custom

CEF

This action will use the ArcSight Common Event format.

Example Message

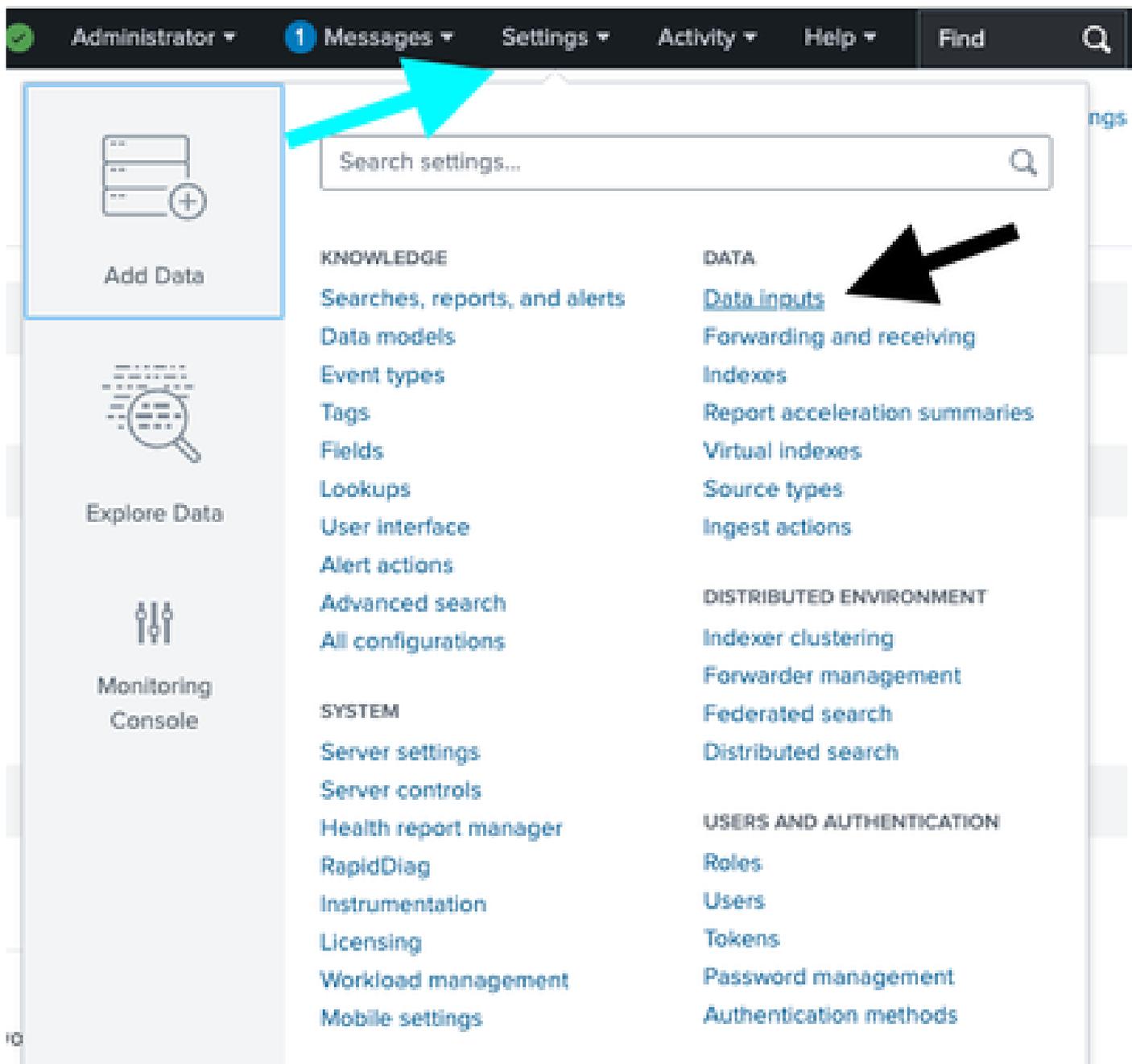
```
<131>Jan 01 00:00:00 test.host TestApp[1337]: CEF:0|Cisco|7.3.0|Notification:99|Bad Host|5|msg=This host has been observed performing malicious actions toward another host.:Source Host is http (80
```

Test Action

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

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

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



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

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

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

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

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

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

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?

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

Passo 7: Selecione IP para o Método.

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

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](#)

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

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

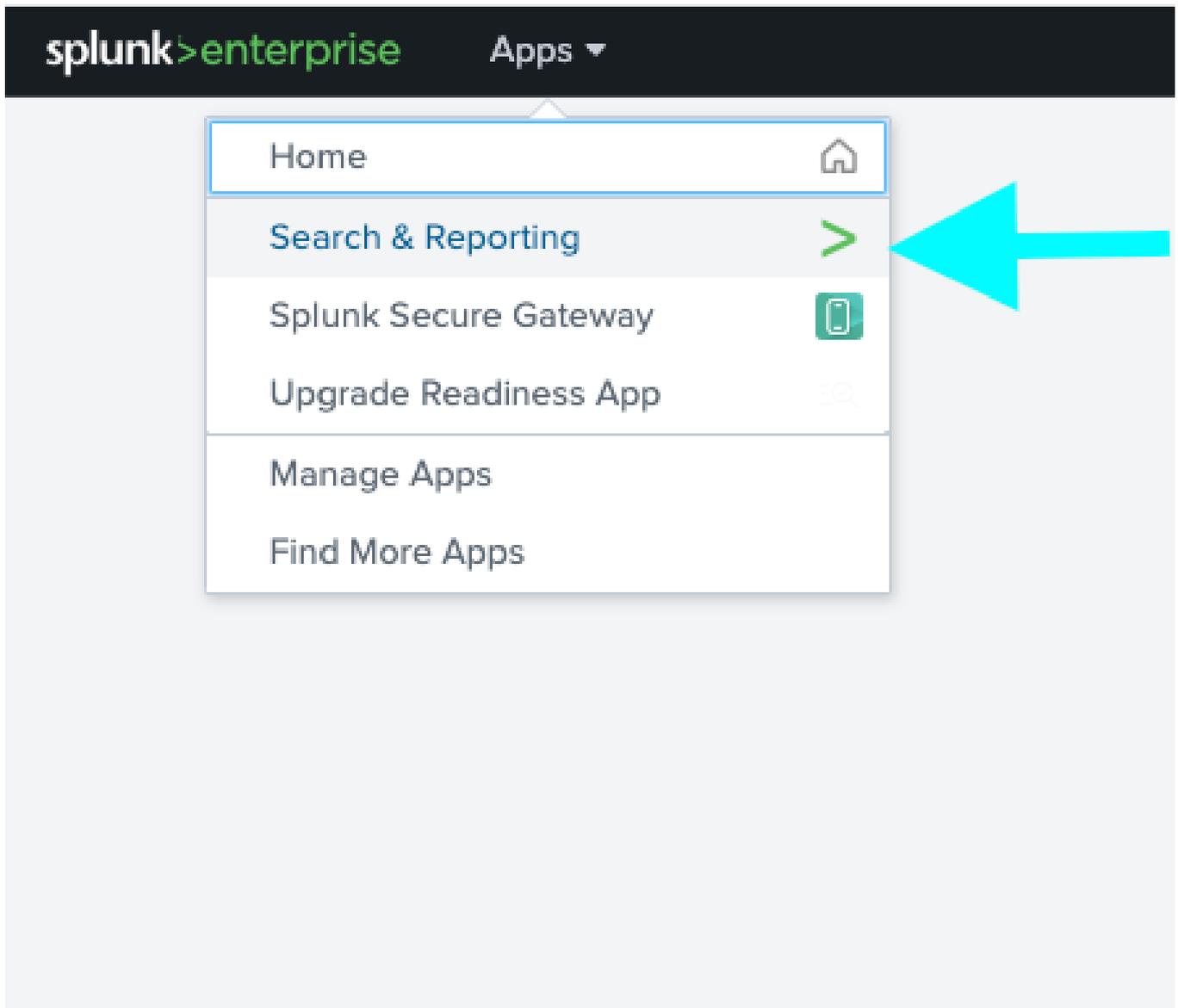
Add Data ● ——— ● ——— ● ——— ○

Select Source Input Settings Review Done

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

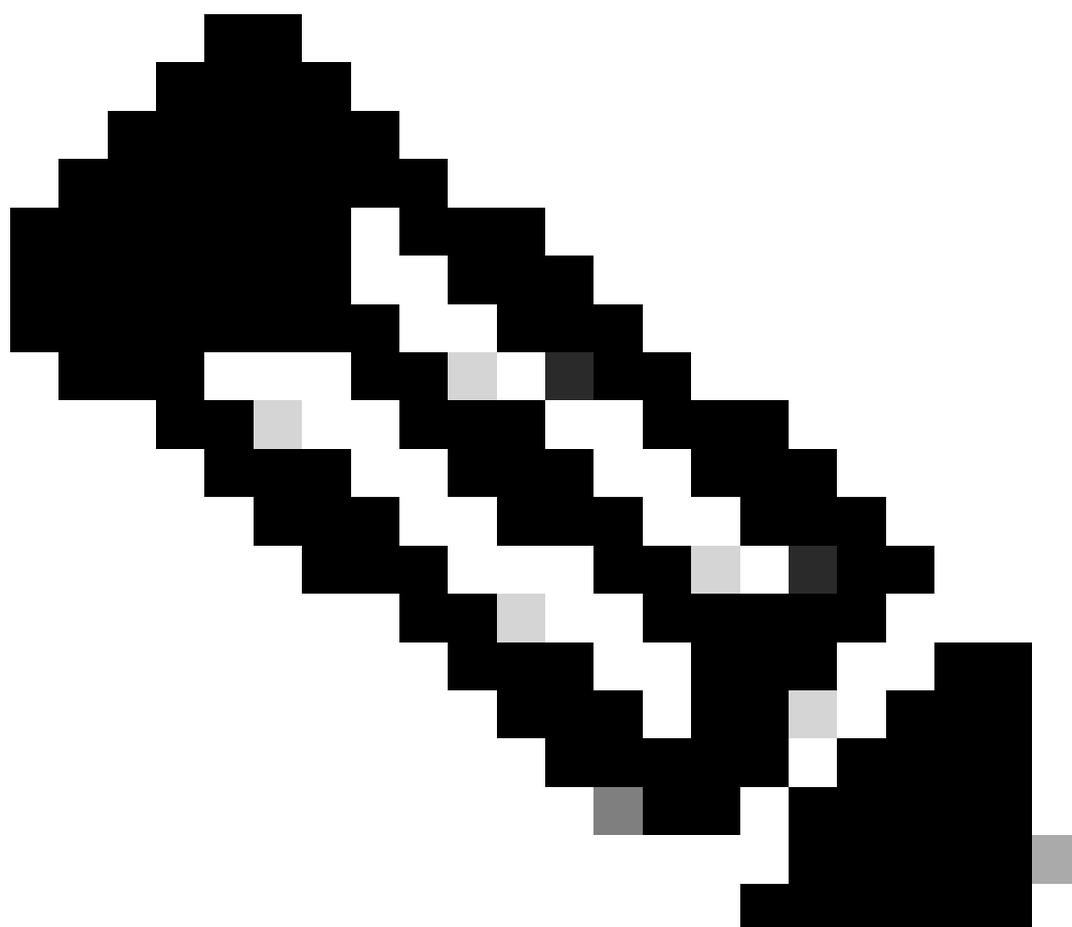
Etapa 11: Navegue até Apps > Search & Reporting na interface do usuário da Web.



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

recebidos.

The screenshot shows the Splunk Search interface. At the top, there is a search bar with the query `source="*" :!* sourcetype="*"`. Below the search bar, there are tabs for `Events (6)`, `Patterns`, `Statistics`, and `Visualization`. The `Events (6)` tab is active, showing a table with columns for `Time` and `Event`. The `Event` column contains a detailed log entry: `[FlowCollector Flow Data Lost[4]msg: dst= src= : end= externalId=BD-1KUS-7R9L-PNE2-5 cs3= cs3Label=SourceHostGroups cs4= cs4Label=TargetHostGroups cs5= cs5Label=Source_URL cs6= cs6Label=Target_URL dpt= proto= dvchost= ceExternalId= * / / cs2Label=SGTIDandSGTName spt= destinationTranslatedAddress= destinationTranslatedPort= sourceTranslatedAddress= sourceTranslatedPort= host = | source = | sourcetype =`. On the left side, there is a sidebar with `SELECTED FIELDS` including `host 1`, `source 1`, and `sourcetype 1`.

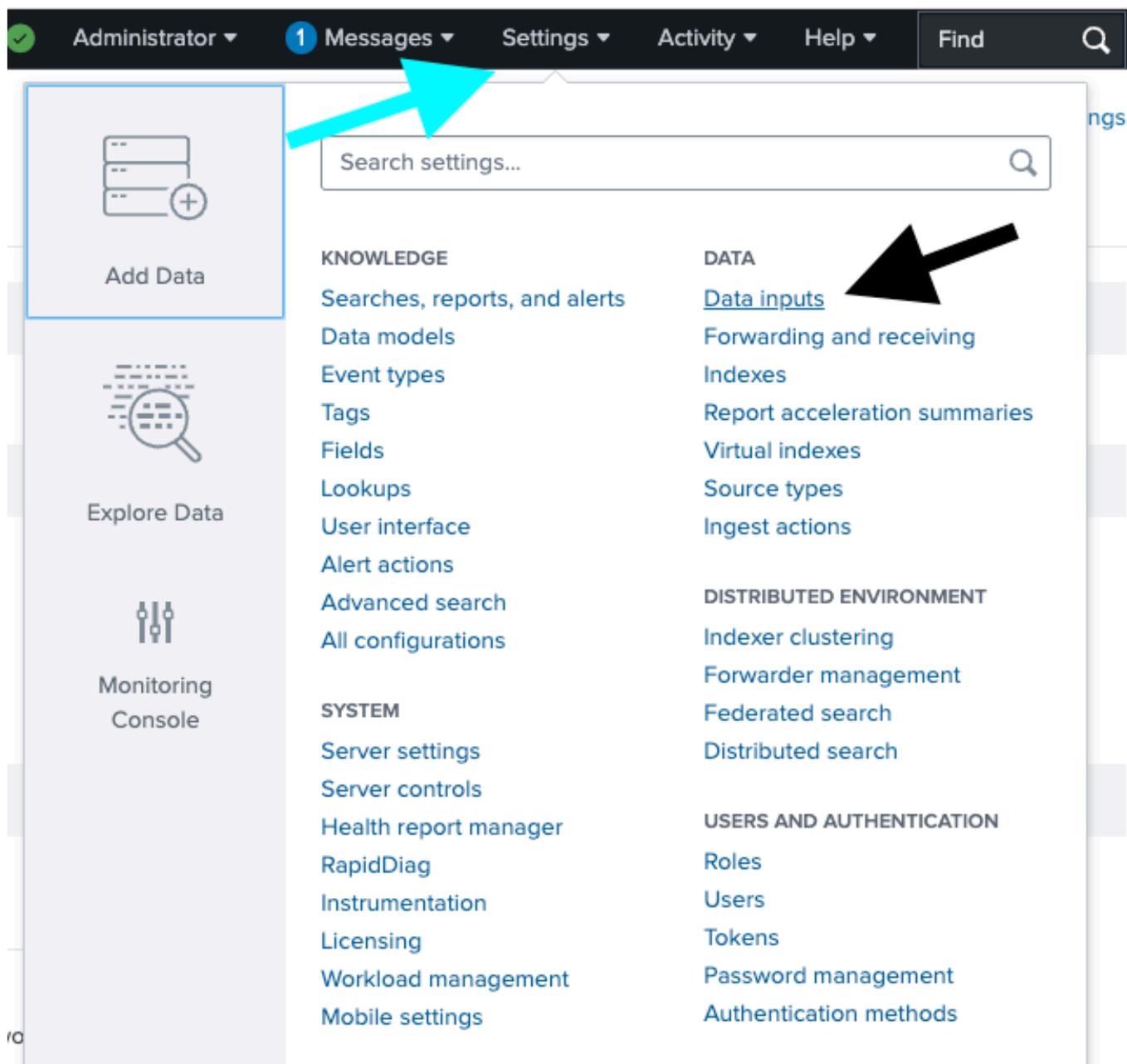


Note: Para a origem, consulte a Etapa 4
Para source_type, consulte a Etapa 6

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

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

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



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

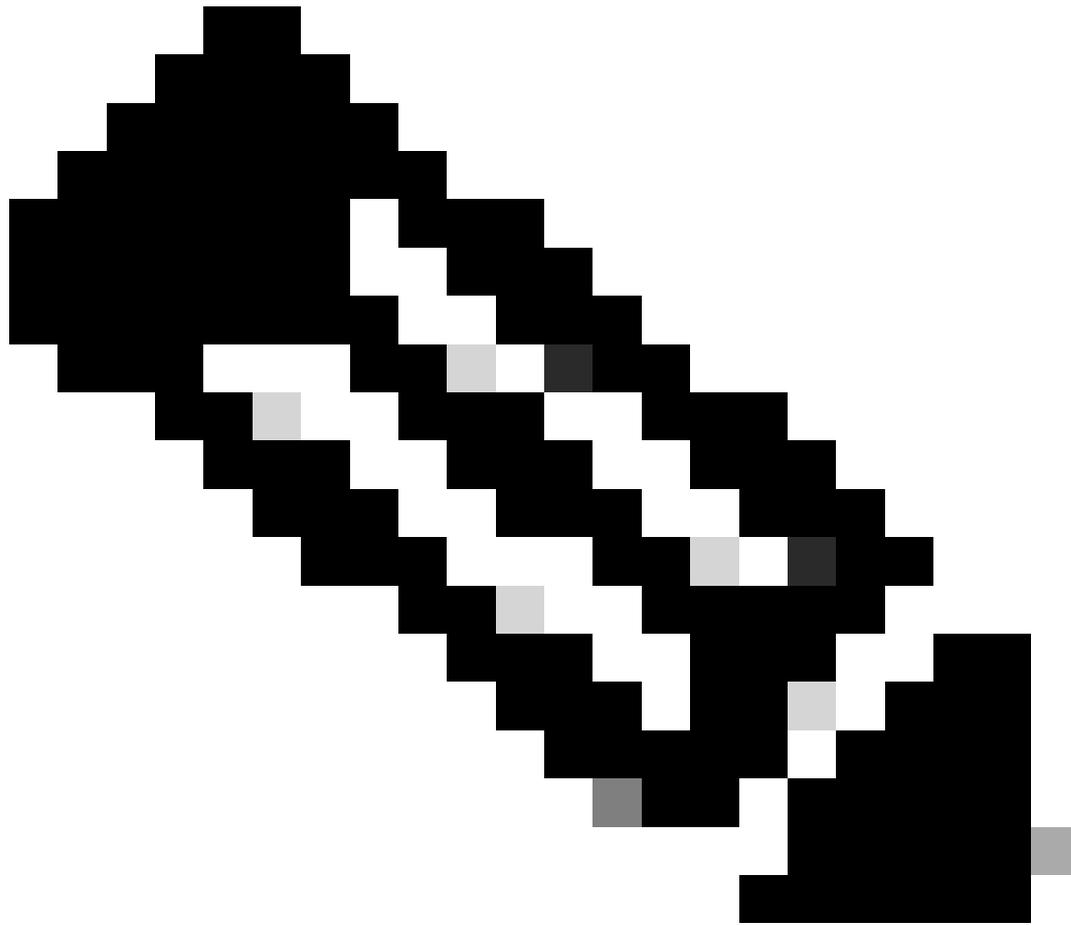
es and directories, network ports, and scripted inputs. If you want to set up forwarding and receiving between two Splunk instances, go to [Forwarding and receiving](#).

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



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



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

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

Apps Administrator 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

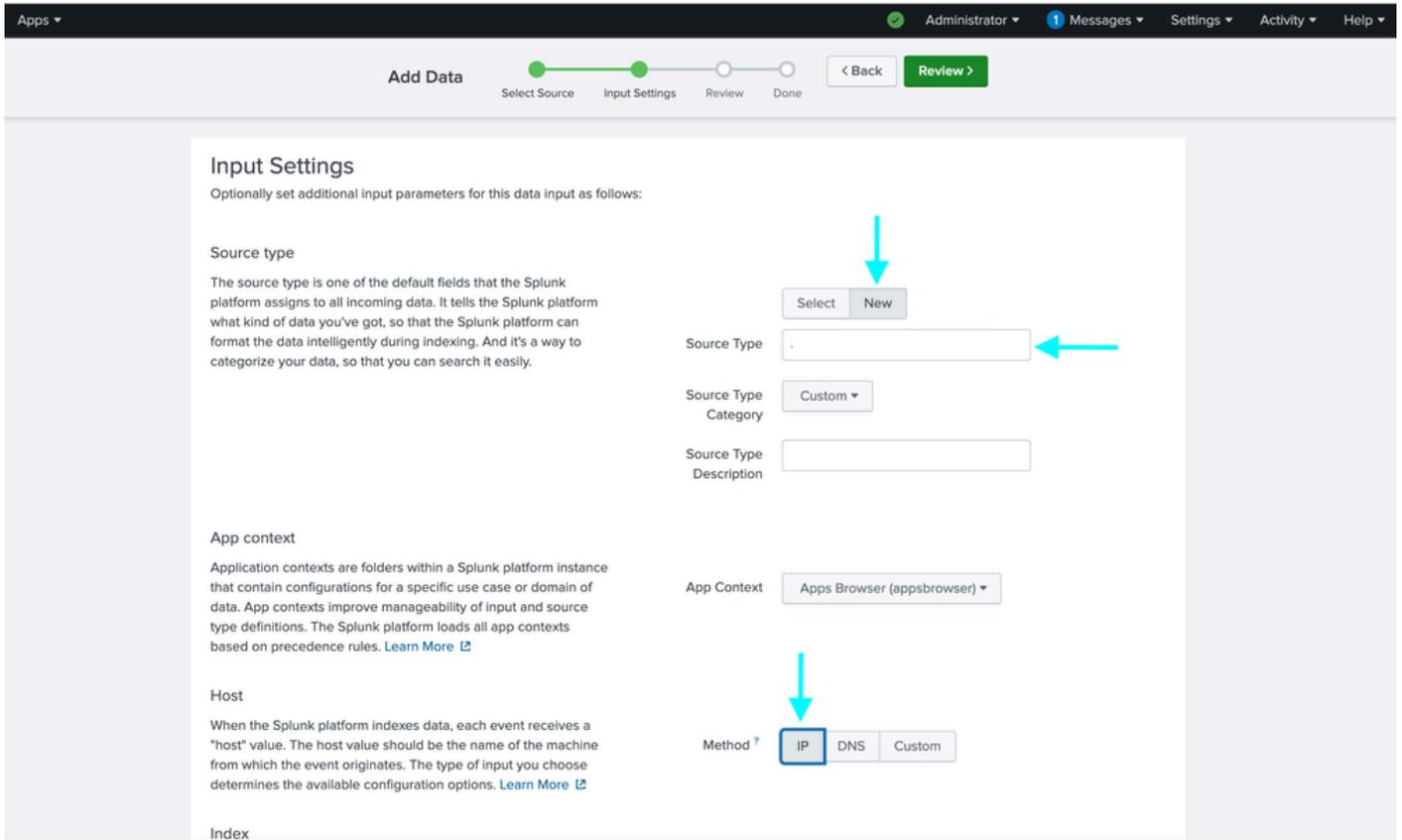
FAQ

- > 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?

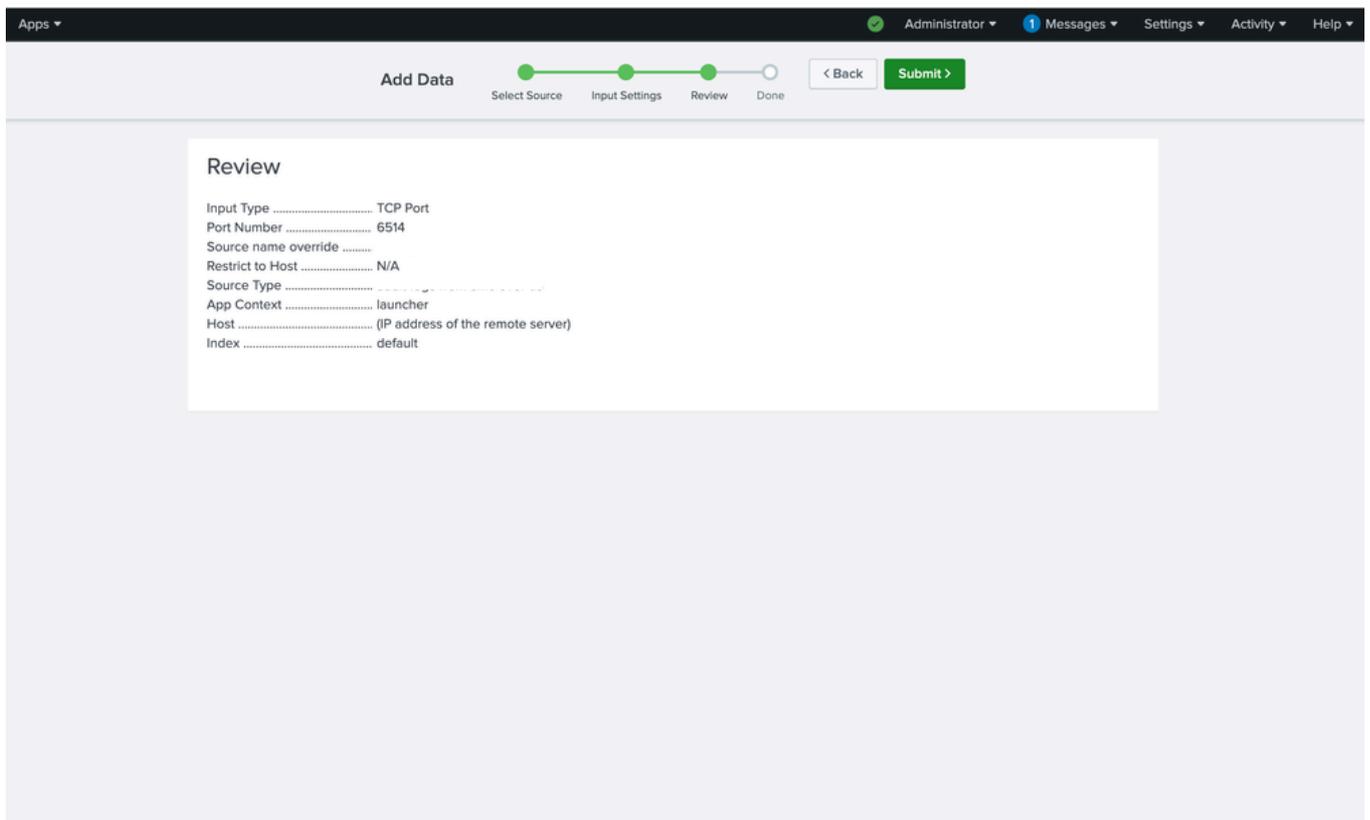
Passo 5: Na nova janela, selecione Novo na seção Tipo de origem, digite nome desejado no campo Tipo de origem.

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

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



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



2. Gerar Certificado para Splunk


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

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

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

Etapa 7: crie um novo arquivo input.conf.

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

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

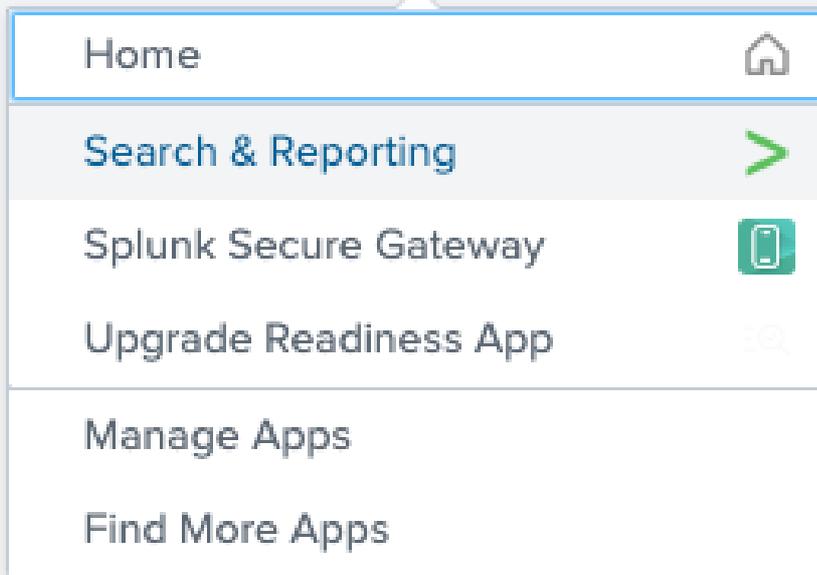
define the port number here over which syslog will be sent

your source type defined during the TCP input configuration

path for Splunk certificate

PEM pass phrase set during certificate generation

Passo 8: Verifique os syslogs usando pesquisar.



New Search

source="*" " sourcetype="* " host = 1

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

- host 1
- source 1
- sourcetype 1

INTERESTING FIELDS

- # date_hour 5

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

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

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



nse



Monitor



Investigate



Report



Configure

Configure ×

Detection

Host Group Management

Alarm Severity

Policy Management

Response Management

Network Scanners

Analytics

Alerts

Global

[↗ Central Management](#)

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

Inventory

4 Appliances found

Filter by Identity

Appliance Status	Identity	FQDN	Type	Actions
Connected				...

- Edit Appliance Configuration
- View Appliance Statistics
- Support
- Reboot Appliance
- Shut Down Appliance
- Remove This Appliance

Passo 3: Navegue até a guia Network Services e insira os detalhes de Audit Log Destination (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) *

Certificate Revocation *i*

- Disabled
- Soft Fail
- Hard Fail

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

Central Management Inventory Data Store Update Manager App Manager Smart Licensing SECURE

Inventory / Appliance Configuration

Appliance Configuration - Manager Cancel Apply Settings

Configuration Menu

Appliance Network Services General

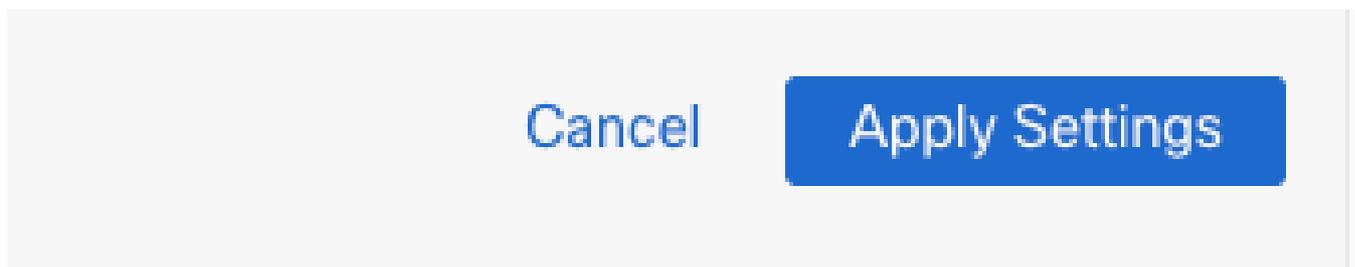
TO ENTER

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

Passo 5: Clique em Aplicar configurações.



Troubleshooting

Pode haver toda a confusão aparecendo na pesquisa.

splunk>enterprise Apps Administrator Messages Settings Activity Help Find Search & Reporting

Search Analytics Datasets Reports Alerts Dashboards

New Search

source* * sourcetype* 156 events () No Event Sampling

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 # host 1 # source 1 # sourcetype 1		>		\x00 Z \x00 \x00 host = source = sourcetype =
INTERESTING FIELDS # index 1 # linecount 6 # punct 79 # splunk_server 1 # timestamp 1		>		* \x00 & \xE3D \x9F8\x91\xD3 \x99\x82 \xF8F\x9F\xE5R\xE8\xED \x92\xC0\xE5\xE5\xA38:\xA2\xEB (i ;\x00\xE5C[\x00\x00\x94C7]\x9A\x00 - \x9E \xF9\xE1-4\x884\x8F\x00 \xC0+\xC0/\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* \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 \xBF\x9F&\xA4\x87/t\xFD\xCD\xE0\x92\x89\xEA \x88 host = 10.106.127.13 source = sourcetype =
34 more fields + Extract New Fields		>		\x00 Z \x00 \x00 host = 10.106.127.13 source = sourcetype =
		>		* \x00 & <Gk- AInp*?>\x97h\xF9R2 u\x9E \x91\xA1T\x8C\xB0\xDCy , \x00(\x00\x84+\x00\xC3s , \xBA(\x00\x9A \x00\x03\xFC6\xFE\x8C\x98E\xC5\xD9\x00 \xC0+\xC0/\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,\x00* \x00 \x00 \x00\x00 \x00\x00 Show all 6 lines

Solução:

Mapeie a entrada para o tipo de origem correto.

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

New Local 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

Sobre esta tradução

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

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

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