

Configurazione di Response Management per l'invio di eventi syslog a Splunk

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurare syslog su SNA su UDP 514 o sulla porta personalizzata](#)

[1. Gestione delle risposte SNA](#)

[2. Configurazione di Splunk per la ricezione di syslog SNA sulla porta UDP](#)

[Configurare syslog su SNA sulla porta TCP 6514 o sulla porta personalizzata](#)

[1. Configurazione di Splunk per la ricezione dei log di controllo SNA sulla porta TCP](#)

[2. Genera certificato per Splunk](#)

[3. Configurare la destinazione del log di controllo sulla SNA](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come configurare la funzionalità di gestione delle risposte di Secure Analytics per inviare eventi tramite syslog a terze parti, ad esempio Splunk.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

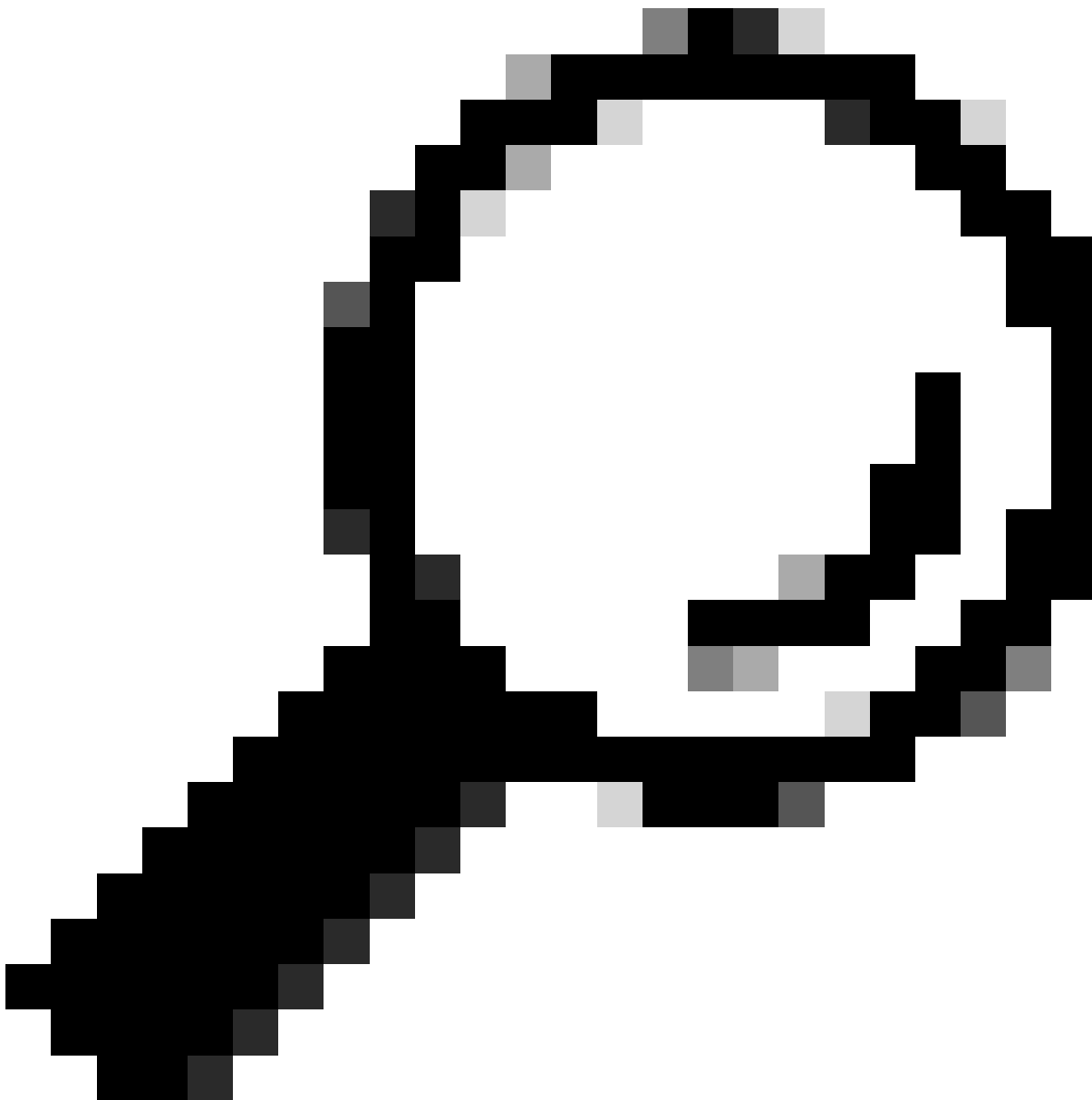
- Gestione delle risposte di Secure Network Analytics.
- Splunk Syslog

Componenti usati

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

- Distribuzione SNA (Secure Network Analytics) che contiene almeno un accessorio Manager e un accessorio Flow Collector.
- Splunk server installato e accessibile su 443 porte.

Configurare syslog su SNA su UDP 514 o sulla porta personalizzata



Suggerimento: verificare che UDP/514, TCP/6514 o qualsiasi porta personalizzata scelta per syslog sia consentita su qualsiasi firewall o dispositivo intermedio tra SNA e Splunk.

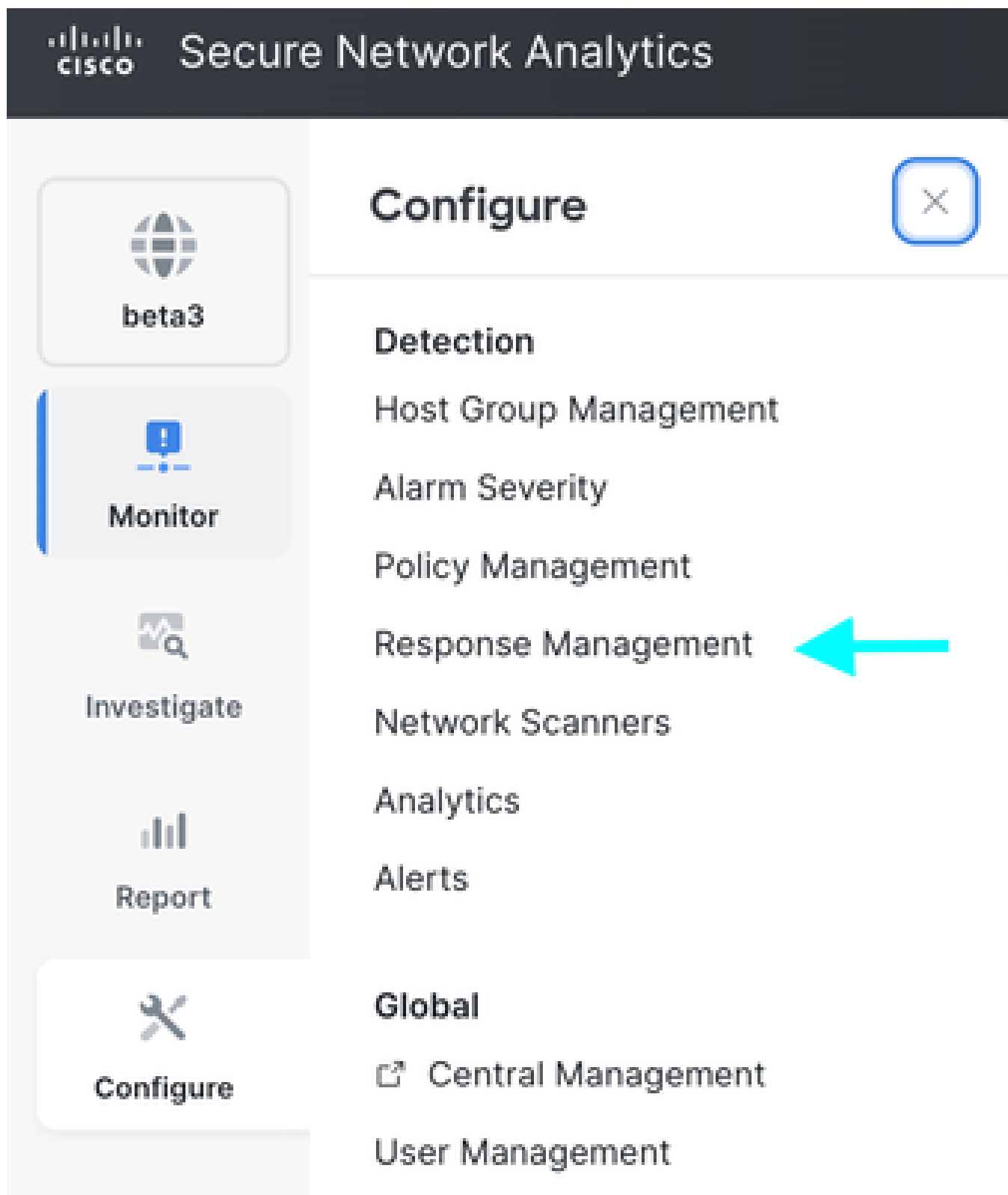
1. Gestione delle risposte SNA

Il componente Response Management di Secure Analytics (SA) può essere utilizzato per configurare regole, azioni e destinazioni syslog.

Queste opzioni devono essere configurate per inviare/inoltare gli allarmi di Secure Analytics ad

altre destinazioni.

Fase 1: Accedere all'accessorio SA Manager e selezionare Configure > Detection Response Management (Configurazione > Gestione risposte rilevamento).



Passaggio 2: Nella nuova pagina passare alla scheda Azioni, individuare la voce di riga Invia a syslog predefinita e fare clic sui puntini di sospensione (...) nella colonna Azione, quindi fare clic su Modifica.

Response Management

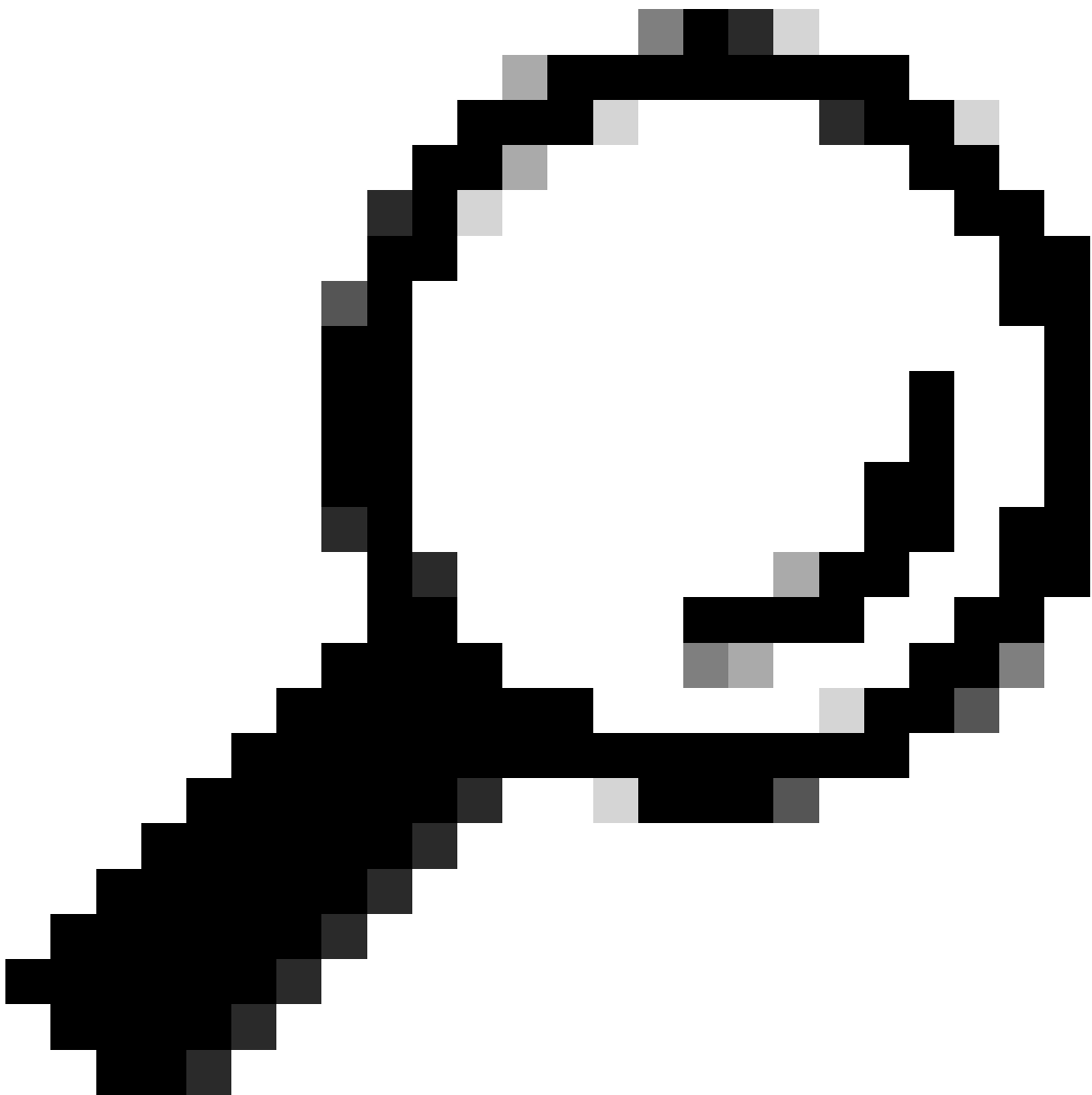
Rules Actions Syslog Formats

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

Passaggio 3: Immettere l'indirizzo di destinazione desiderato nel campo Indirizzo server syslog e la porta di ricezione desiderata nel campo Porta UDP. In Formato messaggio selezionare CEF.

Passaggio 4: Al termine, fare clic sul pulsante blu Salva nell'angolo superiore destro.



Suggerimento: La porta UDP predefinita per syslog è 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

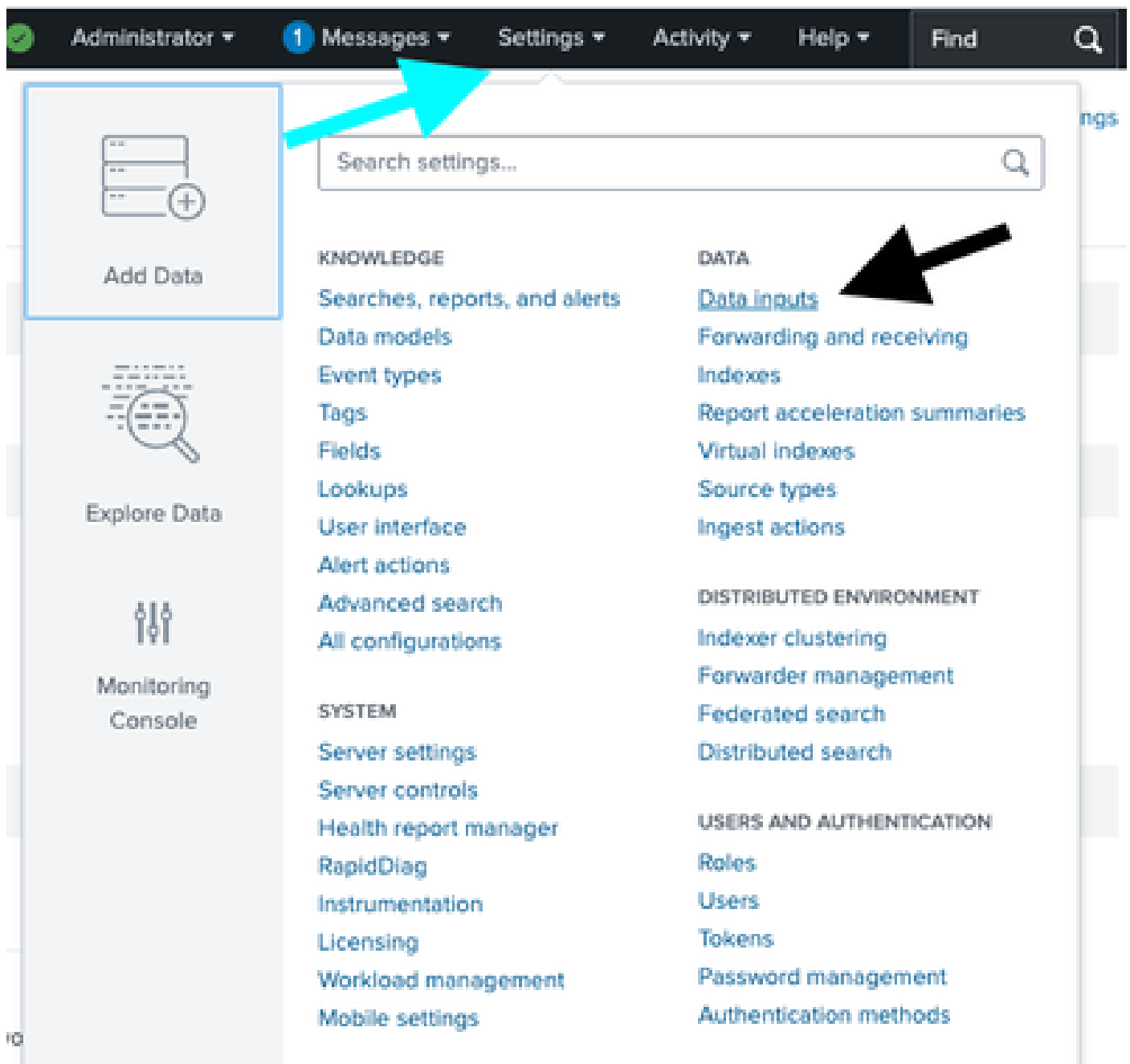
<131>Jan 01 00:00:00 test.host TestApp[1337]: CEF:0|Cisco|7.3.0|Notification:99|Bad Host|5|msg=This host has been observed performing malicious actions toward another host.:Source Host is http (80

Test Action

2. Configurazione di Splunk per la ricezione di syslog SNA sulla porta UDP

Dopo aver applicato le modifiche nell'interfaccia utente Web di Secure Network Analytics Manager, è necessario configurare l'input dei dati in Splunk.

Passaggio 1: Accedere a Splunk e selezionare Impostazioni > Aggiungi dati > Input dati.



Passaggio 2: Individuare la linea UDP e selezionare +Aggiungi nuovo.

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

Passaggio 3: Nella nuova pagina selezionare UDP, immettere la porta di ricezione, ad esempio 514 nel campo Porta.

Passaggio 4: Nel campo Sostituzione nome origine immettere: desired name of source.

Passaggio 5: Al termine, fare clic sul pulsante verde Avanti > nella parte superiore della finestra.

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?

Passaggio 6: Nella pagina successiva, passare all'opzione Nuovo, individuare il campo Tipo di origine e immettere: desired source .

Passaggio 7: Selezionare IP come metodo.

Passaggio 8: Fare clic sul pulsante verde Revisione > nella parte superiore dello schermo.

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.

SelectNew

Source Type

Source Type Category

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

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 ?

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

Create a new index

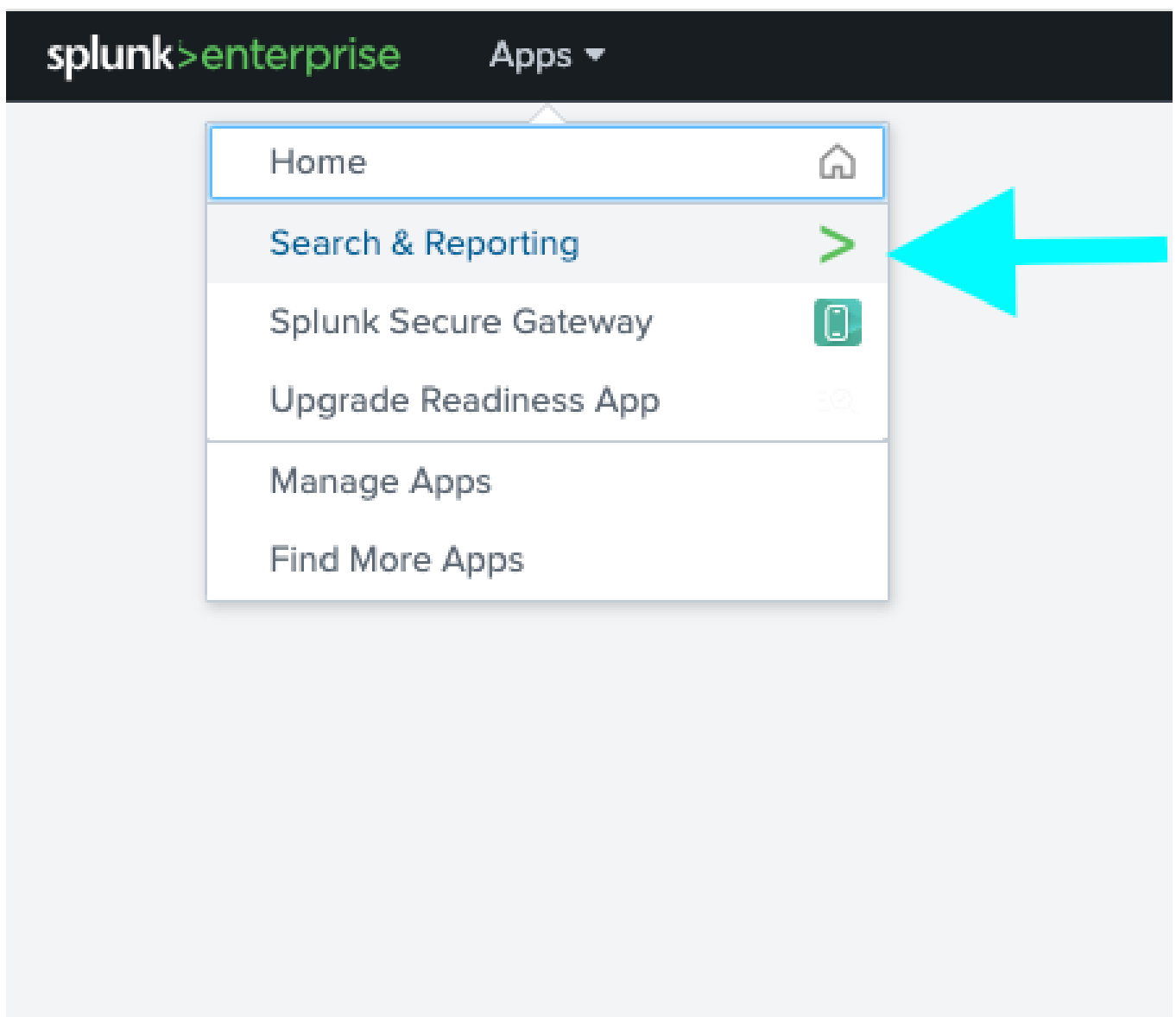
Passaggio 9: Nella finestra successiva, rivedere le impostazioni e modificarle se necessario.

Passaggio 10: Dopo la convalida, fare clic sul pulsante verde Invia > nella parte superiore della finestra.

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

Passaggio 11: Passare ad App > Ricerca e reporting nell'interfaccia utente Web.



Passaggio 12: Nella pagina Cerca utilizzare il filtro `source="As_configured" sourcetype="As_configured"` per trovare

i log ricevuti.

New Search

source="*" :*" sourcetype="*"

6 events

Events (6) Patterns Statistics Visualization

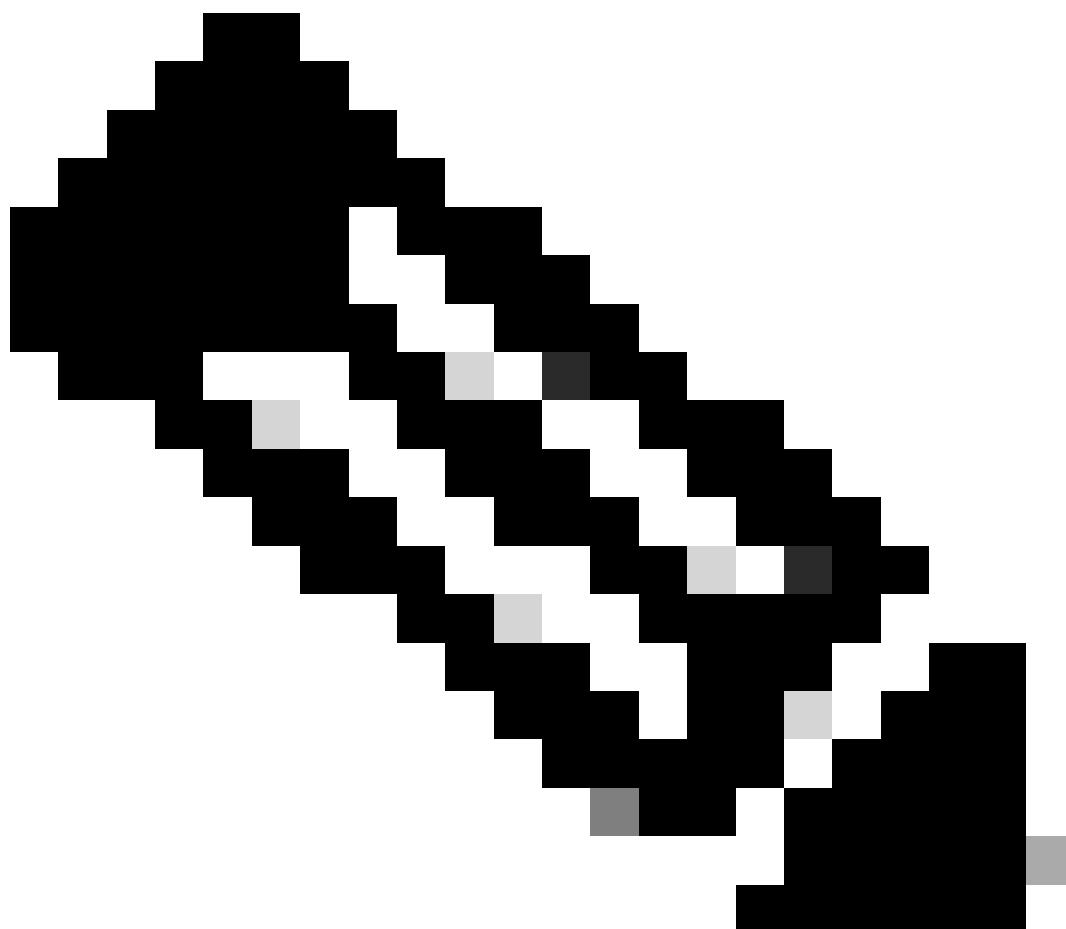
Timeline format Zoom Out Zoom to Selection Deselect

Format Show: 20 Per Page View: List

	Time	Event
		[FlowCollector Flow Data Lost(4)msg=; dst= src= ;
		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

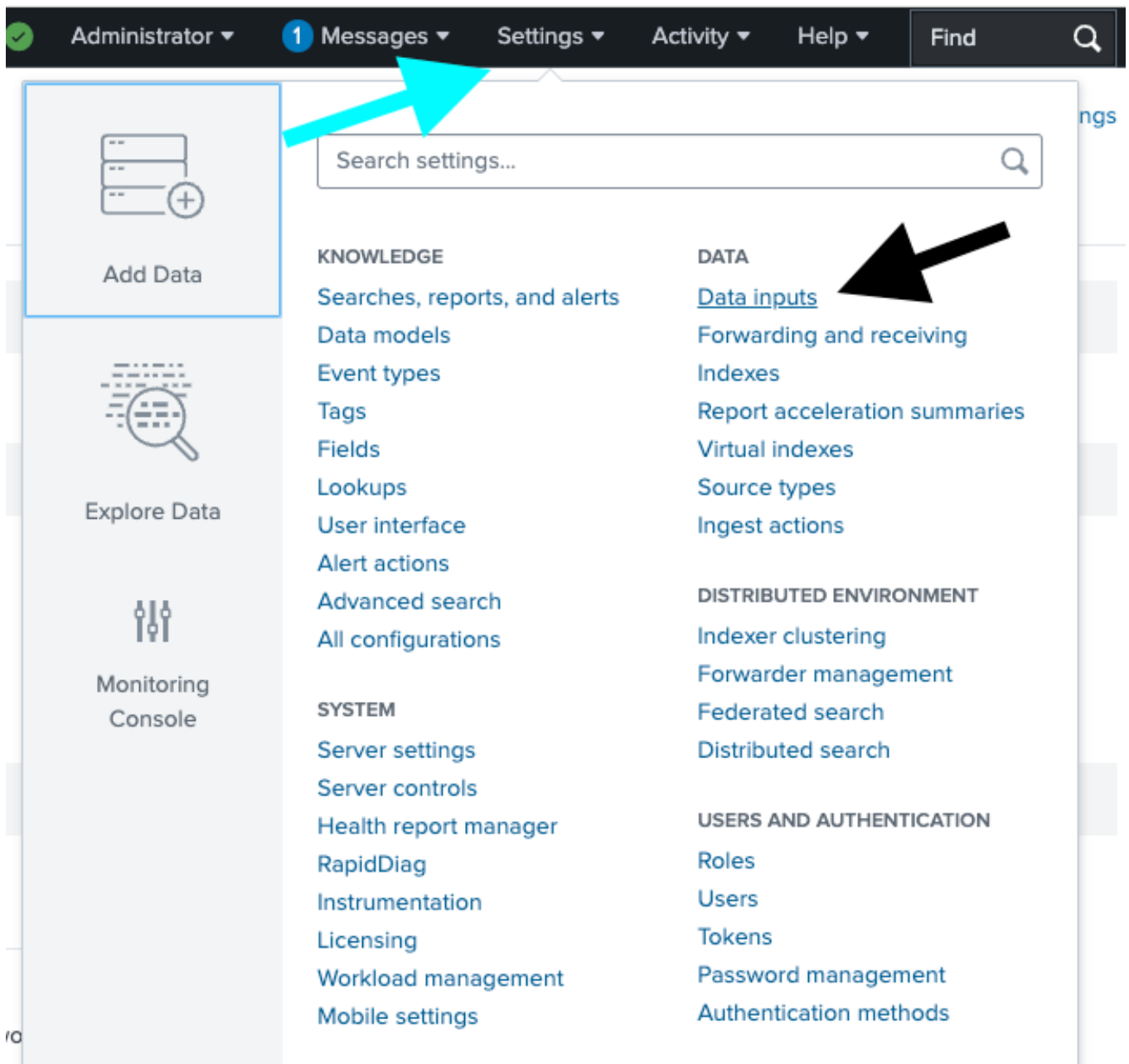


Nota: Per l'origine vedere il passo 4
Per source_type vedere il passo 6

Configurare syslog su SNA sulla porta TCP 6514 o sulla porta personalizzata

1. Configurazione di Splunk per la ricezione dei log di controllo SNA sulla porta TCP

Passaggio 1: Nell'interfaccia utente Splunk, selezionare Impostazioni > Aggiungi dati > Input dati.



Passaggio 2: Individuare la linea TCP e selezionare + Aggiungi nuovo.

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

Passaggio 3: Nella nuova finestra selezionare TCP, immettere la porta di ricezione desiderata, nella porta immagine di esempio 6514, quindi immettere "nome desiderato" nel campo Sostituzione nome origine.



Nota: TCP 6514 è la porta predefinita per syslog su TLS

Passaggio 4: Al termine, fare clic sul pulsante verde Avanti > nella parte superiore della finestra.

Apps

Administrator1 MessagesSettingsActivityHelp

Add Data

Select Source

Input Settings

Review

Done

< BackNext >

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](#)

TCPUDP

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?

Passaggio 5: Nella nuova finestra selezionare Nuovo nella sezione Tipo di origine, immettere il nome desiderato nel campo Tipo di origine.

Passaggio 6: Selezionare IP per il metodo nella sezione Host.

Passaggio 7: Al termine, selezionare il pulsante verde Revisione > nella parte superiore della finestra.

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.

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](#)

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](#)

Index

Method ? IP DNS Custom

Source Type Select New

Source Type Category Custom ▾

App Context Apps Browser (appsbrowser) ▾

Passaggio 8: Nella finestra successiva, rivedere le impostazioni e modificarle se necessario. Una volta convalidato, fare clic sul pulsante verde Invia > nella parte superiore della finestra.

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. Genera certificato per Splunk

Passaggio 1: Usando un computer su cui è installato openssl, eseguire il 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`, sostituendo l'IP di esempio 10.106.127.4 con l'IP del dispositivo Splunk. Viene richiesto due volte di immettere una passphrase definita dall'utente. Negli esempi, i comandi vengono eseguiti dalla riga di comando della macchina Splunk.

[illegible]

Al completamento del comando, vengono generati due file. I file `server_cert.pem` e `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:
```

Passaggio 2: Passare all'utente root.

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

Passaggio 3: Copiare il certificato appena generato in `/opt/splunk/etc/auth/`.

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

Passaggio 4: aggiungere il file spunkweb.cet con la chiave privata.

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

Passaggio 5: modificare la proprietà del certificato di splunk.

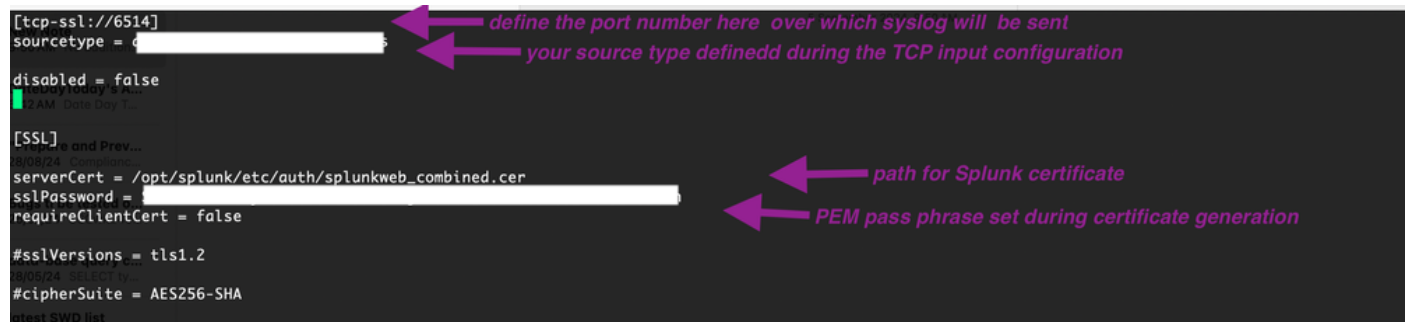
```
user@examplehost:~# chown 10777:10777/opt/splunk/etc/auth/splunkweb.cer
```

Passaggio 6: modificare l'autorizzazione per il certificato splunk.

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

Passaggio 7: creare un nuovo file 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

Passaggio 8: Verificare i syslog utilizzando la funzione di ricerca.

Home



Search & Reporting



Splunk Secure Gateway

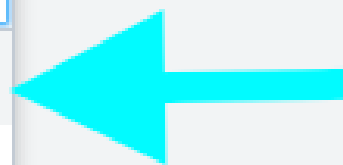


Upgrade Readiness App



Manage Apps

Find More Apps



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

- 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. Configurare la destinazione del log di controllo sulla SNA

Passaggio 1: Accedere all'interfaccia utente SMC e selezionare 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

... ..

Passaggio 2: Fare clic sull'icona con i puntini di sospensione dell'accessorio SNA desiderato e selezionare Modifica configurazione accessorio.

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				...

Passaggio 3: Passare alla scheda Servizi di rete e immettere i dettagli relativi alla destinazione del log di verifica (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

Passaggio 4: Passare alla scheda Generale, scorrere verso il basso Fare clic su Aggiungi nuovo per caricare il certificato Splunk creato in precedenza con il nome 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

Passaggio 5: Fare clic su Applica impostazioni.

Cancel Apply Settings

Risoluzione dei problemi

Potrebbero esserci degli scherzi completi che si presentano durante le ricerche.



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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).