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

Sommario

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:

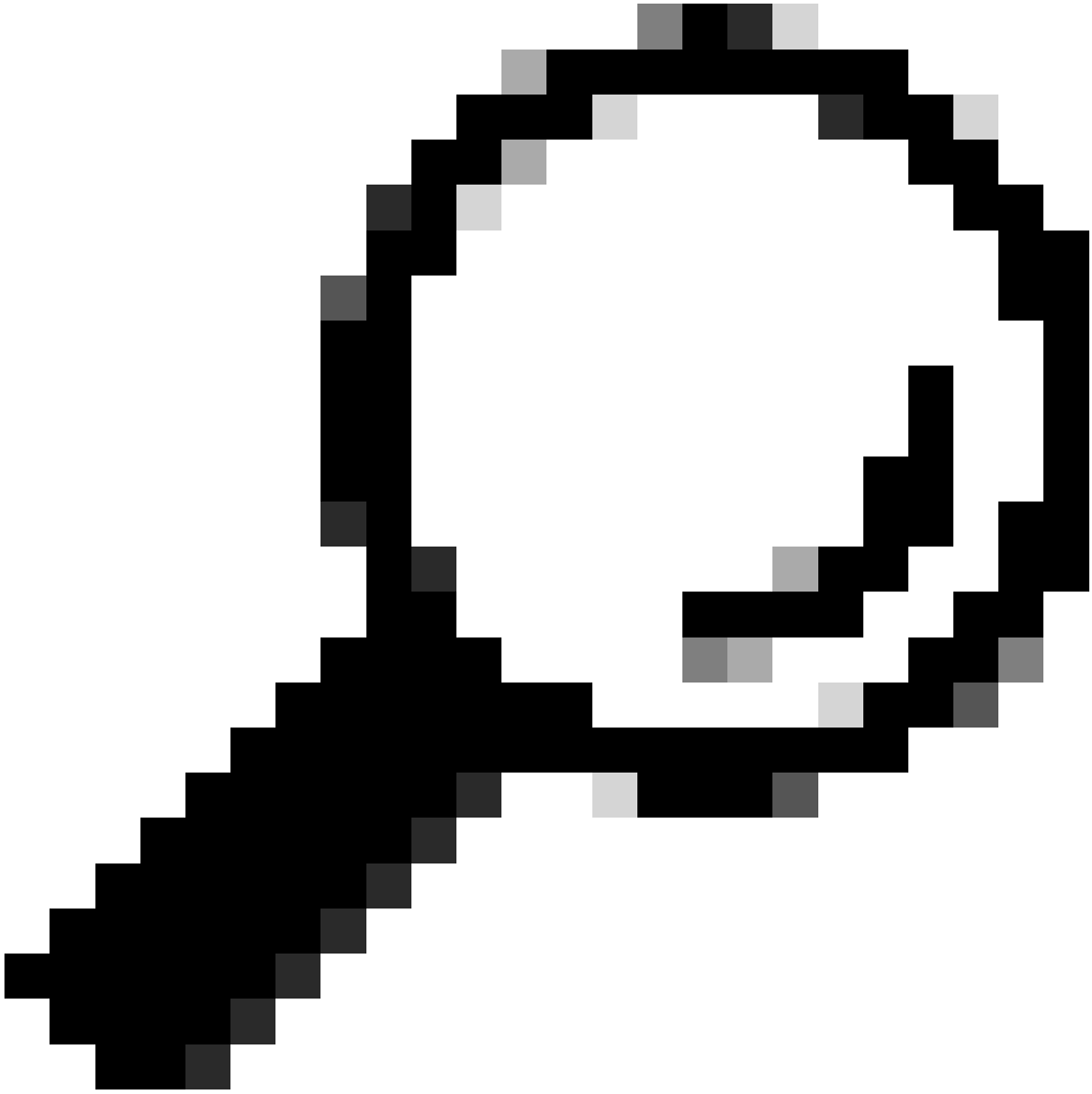
- Gestione delle risposte di Secure Network Analytics.
- Splunk Syslog

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.

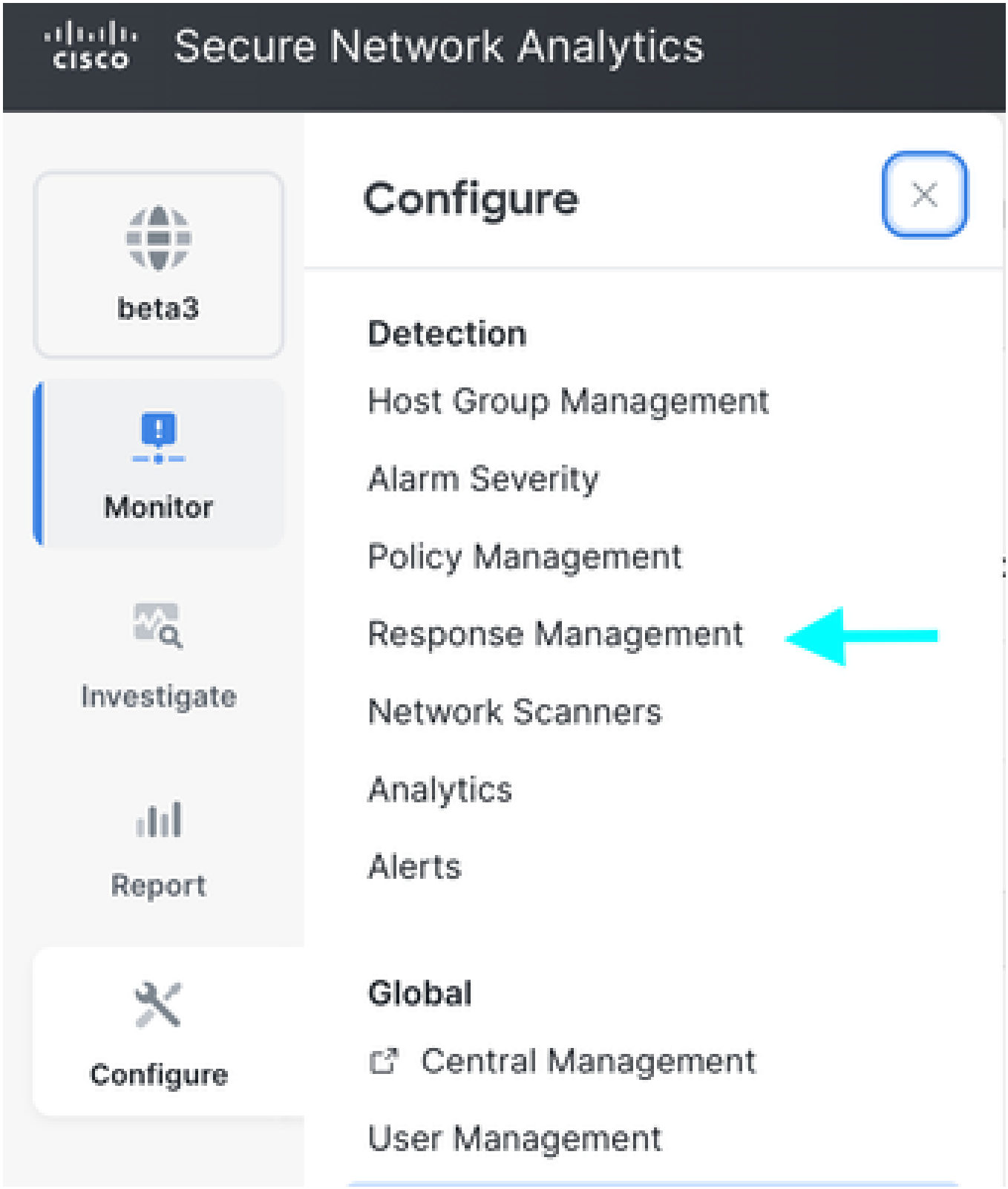
1.Gestione delle risposte SNA

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

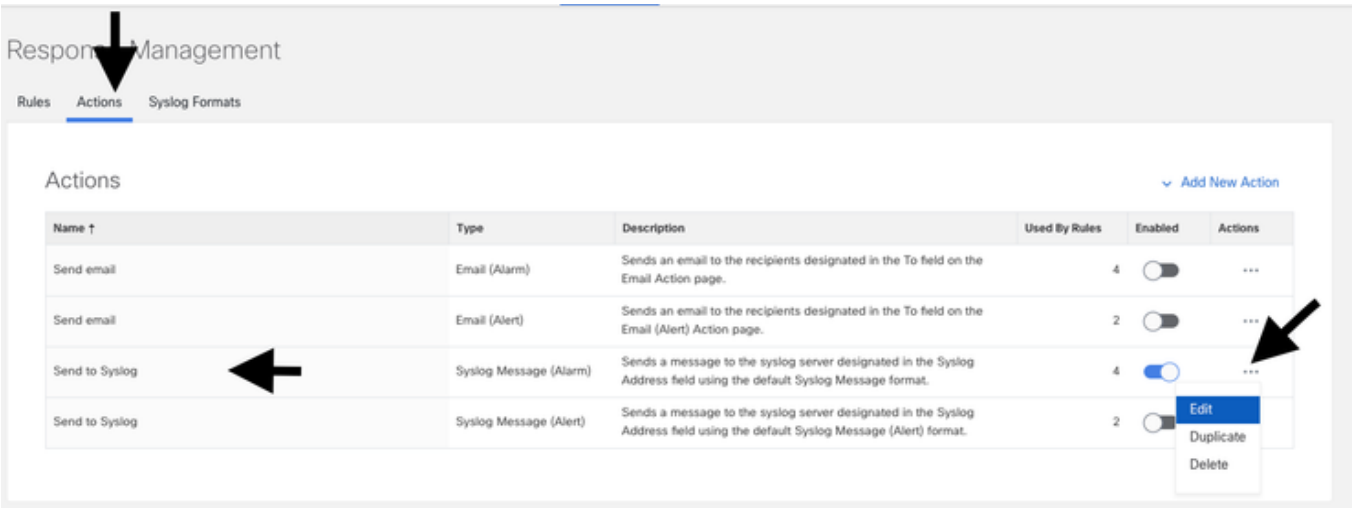
Queste opzioni devono essere configurate per inviare/inoltrare gli allarmi di Secure Analytics ad

altre destinazioni.

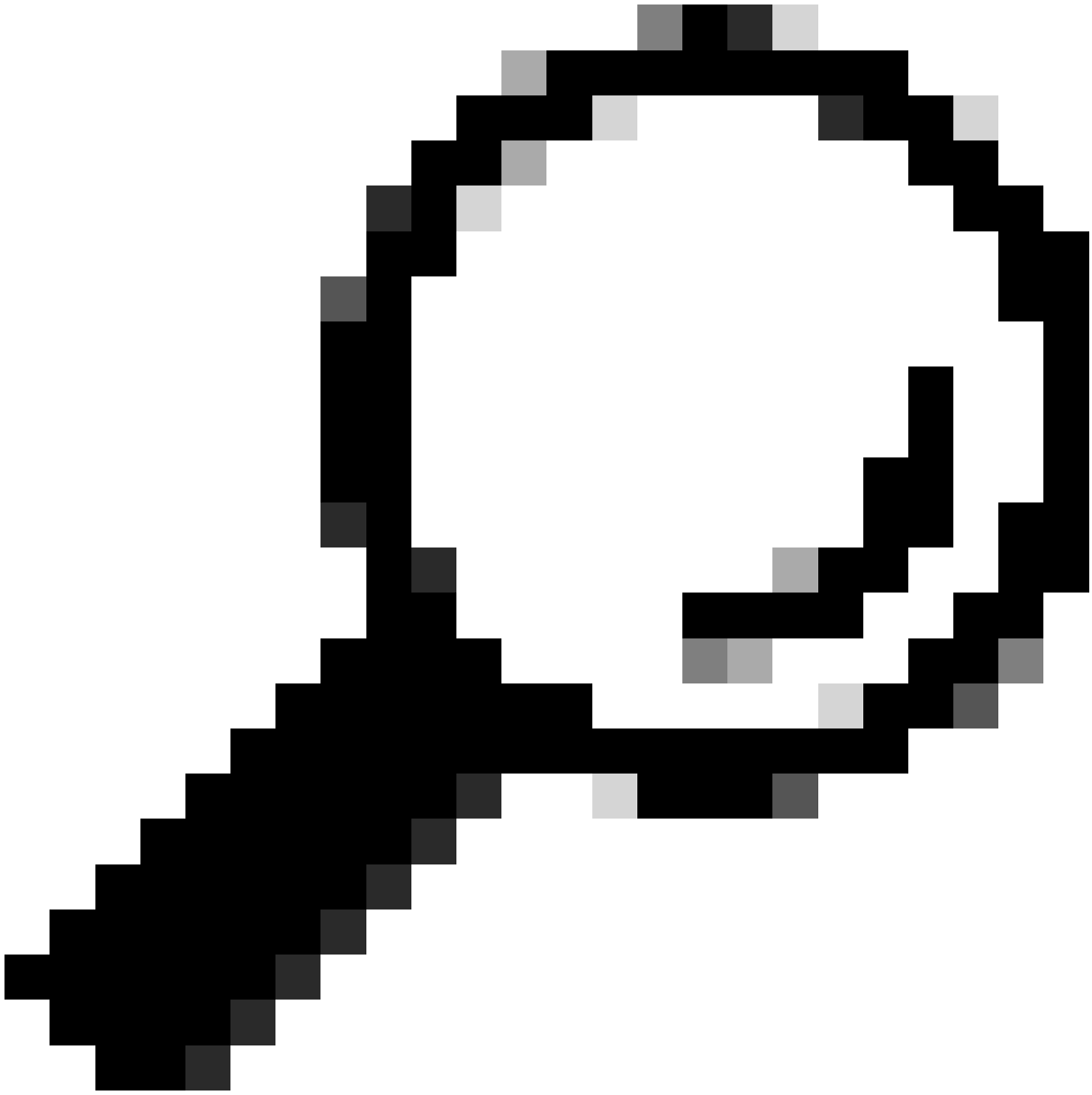
Fase 1: Accedere all'accessorio SA Manager e selezionare Configure > Detection Response Management (Configurazione > Gestione risposte rilevamento).



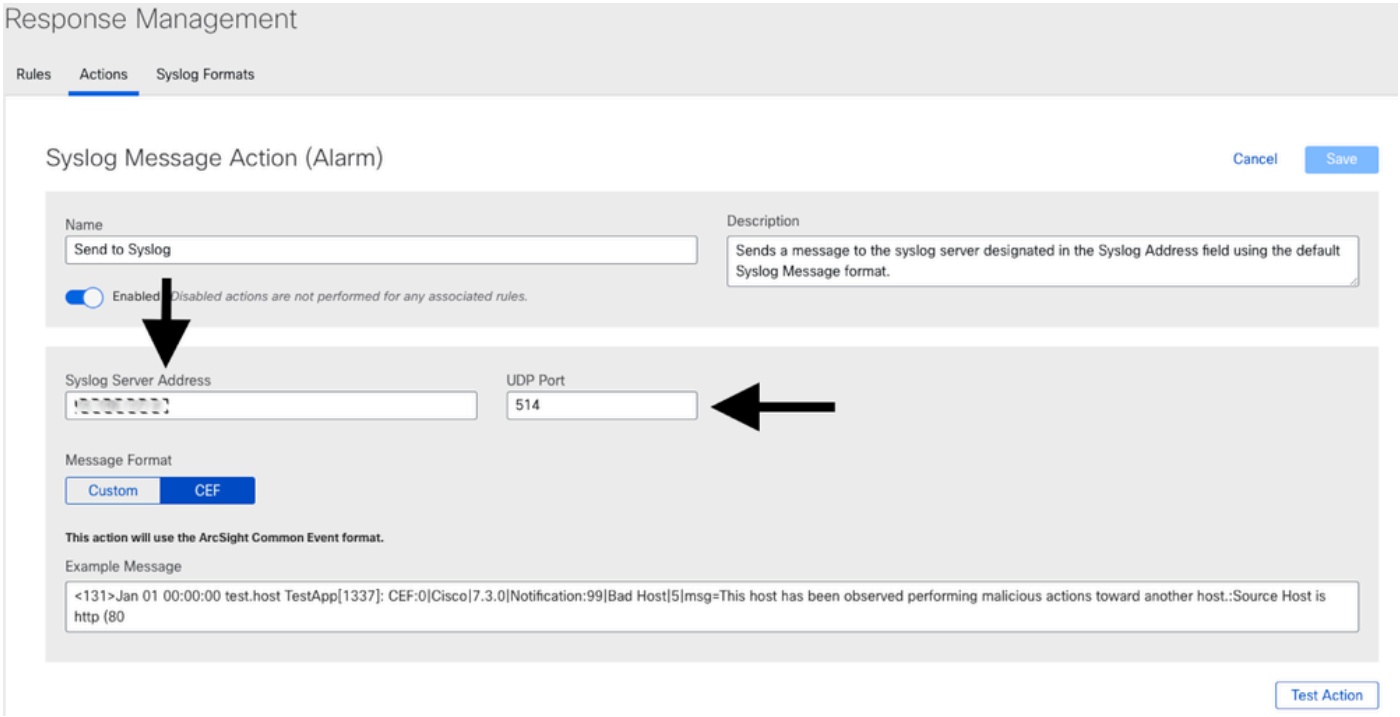
Passaggio 2: Nella nuova pagina passare alla scheda Azioni, individuare la voce di riga Invia a syslog predefinita e fare clic sui puntini di sospensione (...) nella colonna Azione, quindi fare clic su Modifica.



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.



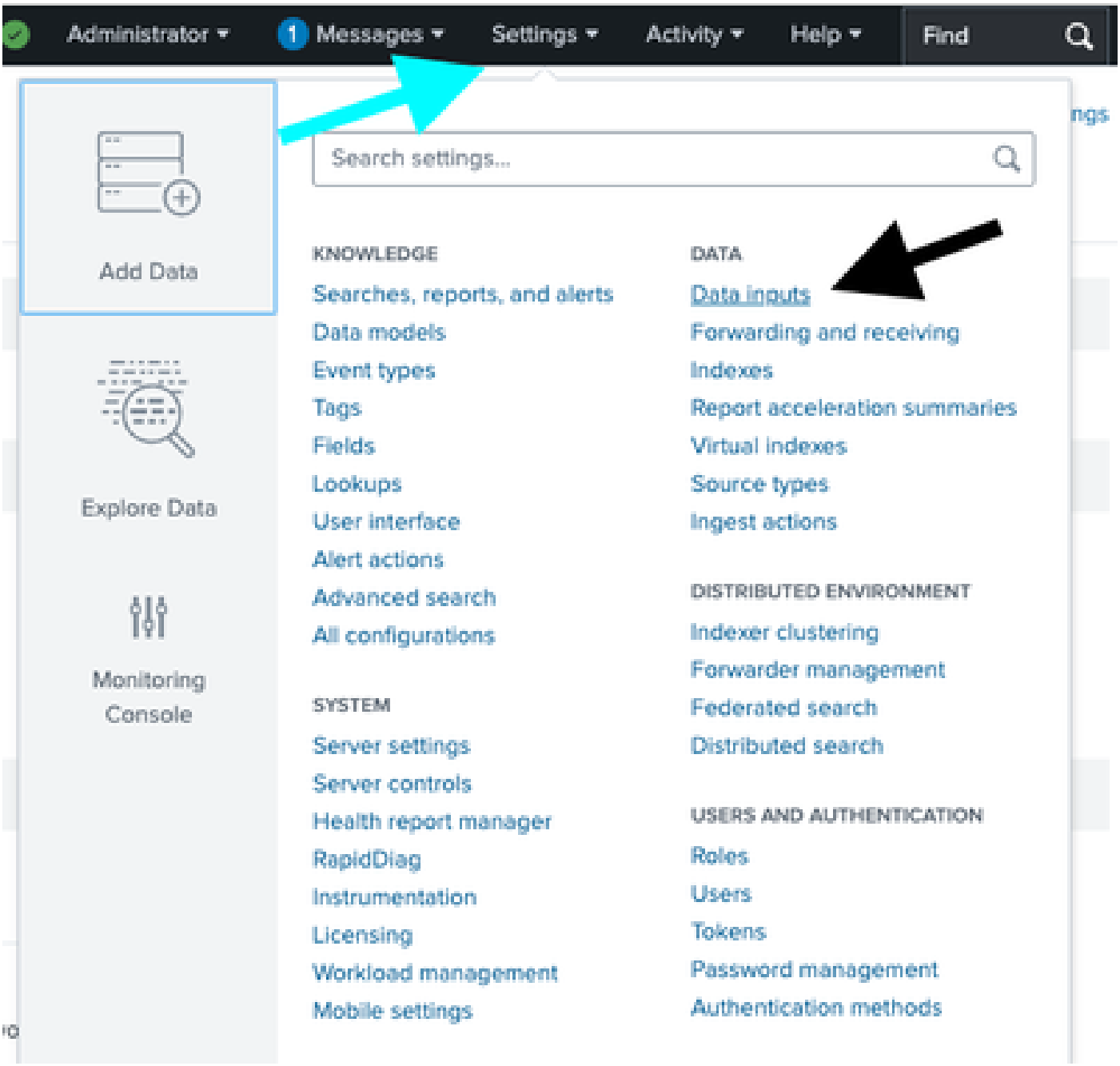
Suggerimento: La porta UDP predefinita per syslog è 514



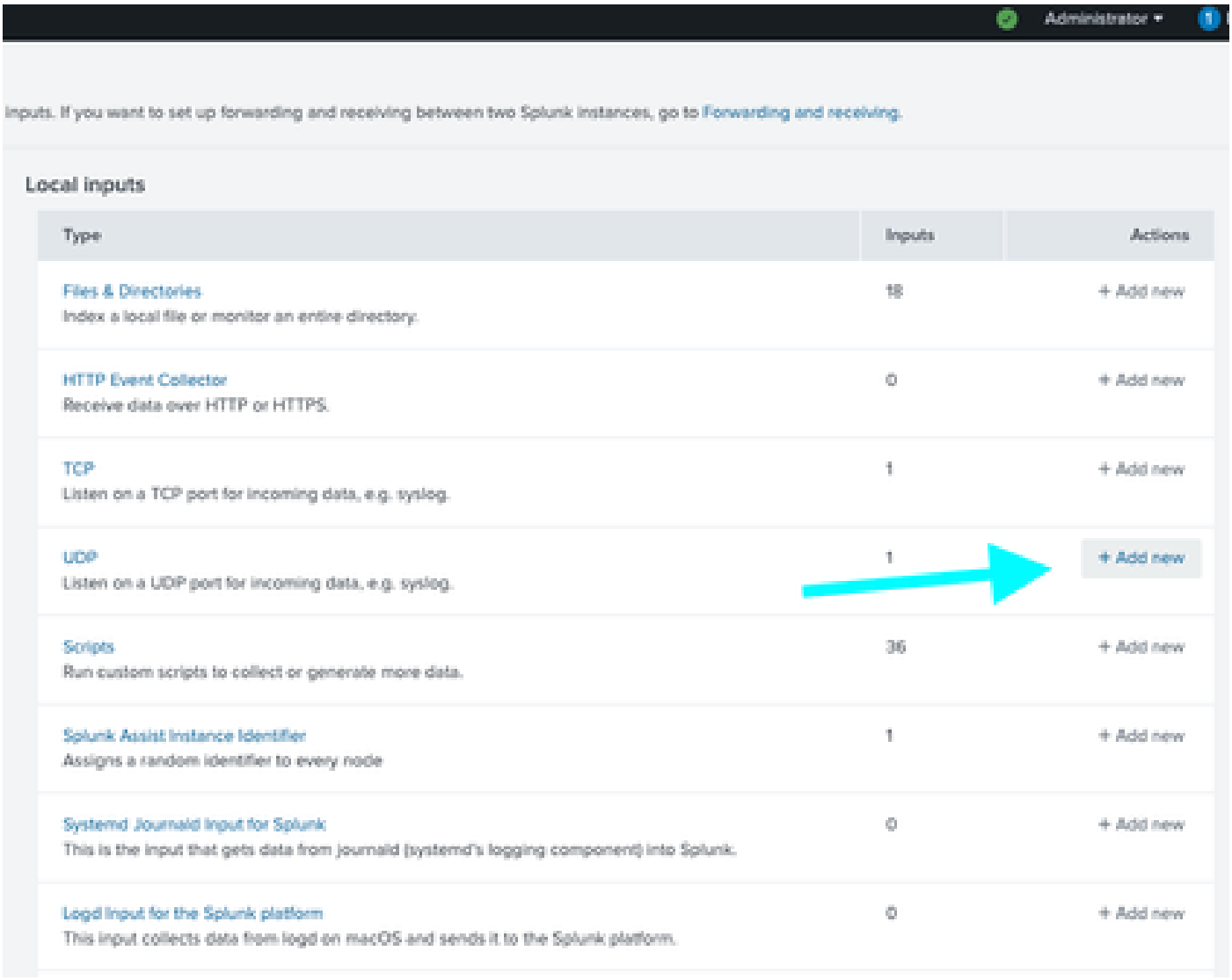
2.Configurazione di Splunk per la ricezione di syslog SNA sulla porta UDP

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.

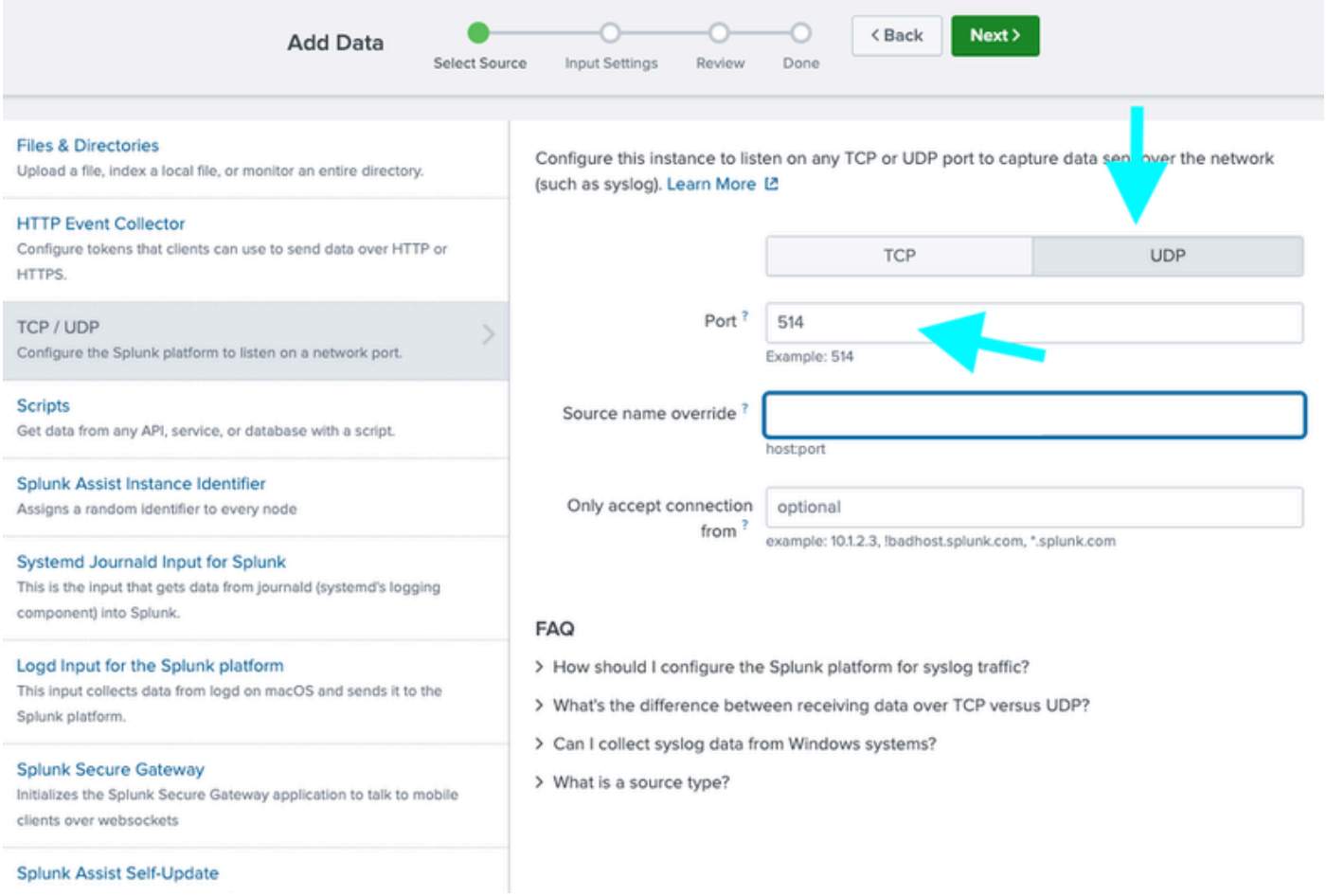


Passaggio 2: Individuare la linea UDP e selezionare +Aggiungi nuovo.



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.

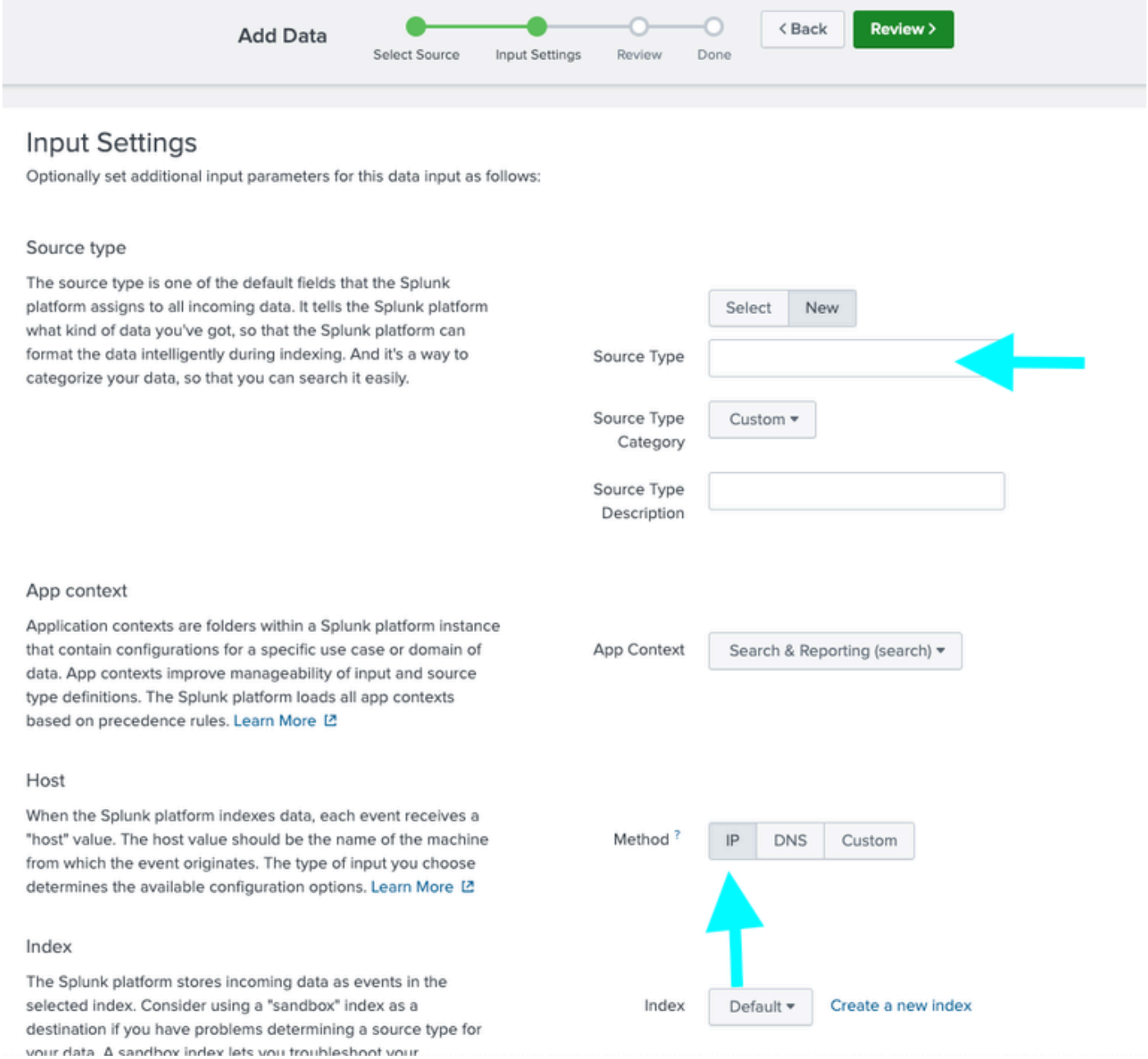
Passaggio 5: Al termine, fare clic sul pulsante verde Avanti > nella parte superiore della finestra.



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

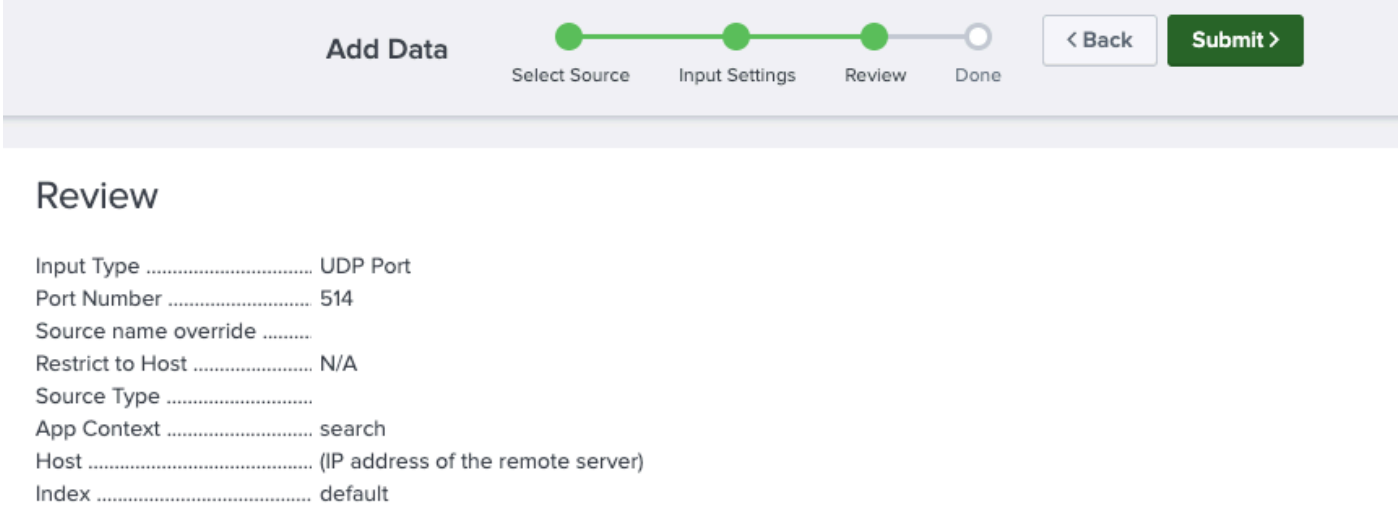
Passaggio 7: Selezionare IP come metodo.

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

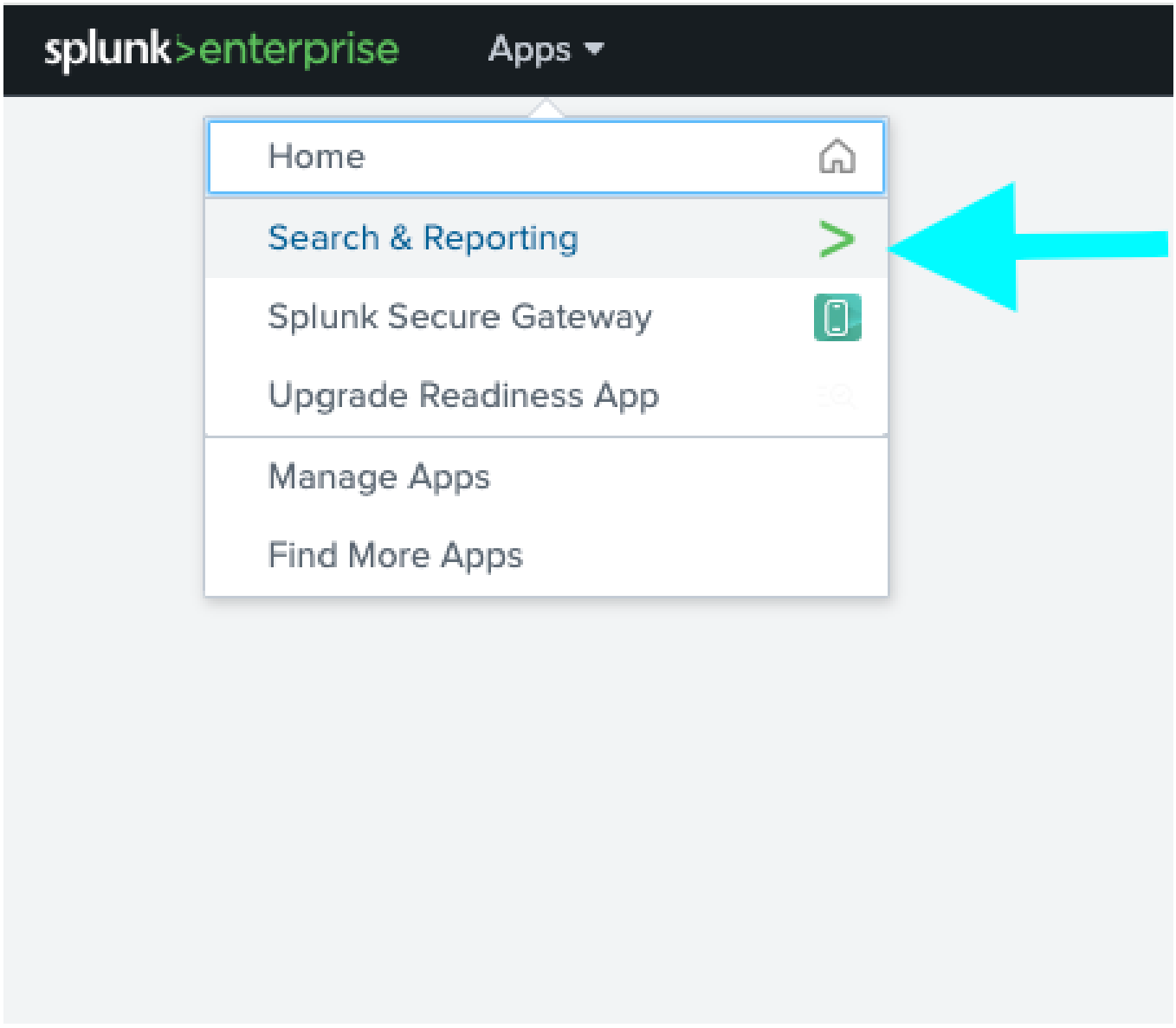


Passaggio 9: Nella finestra successiva, rivedere le impostazioni e modificarle se necessario.

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

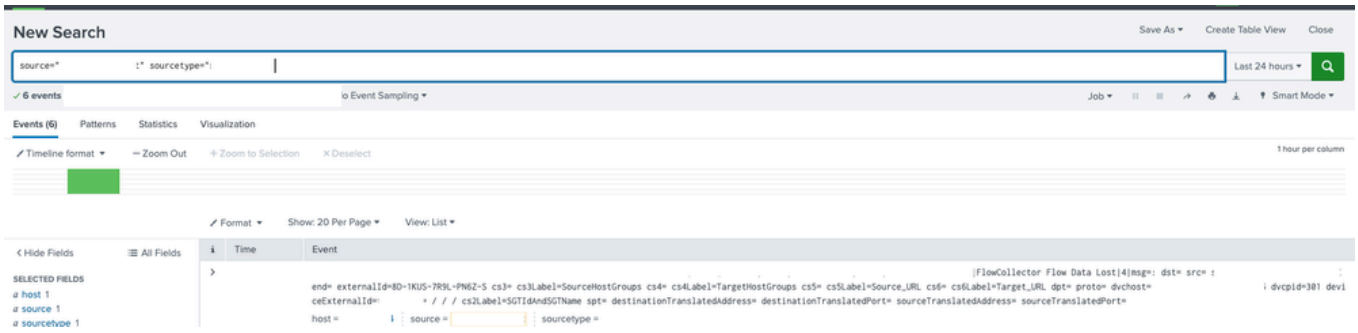


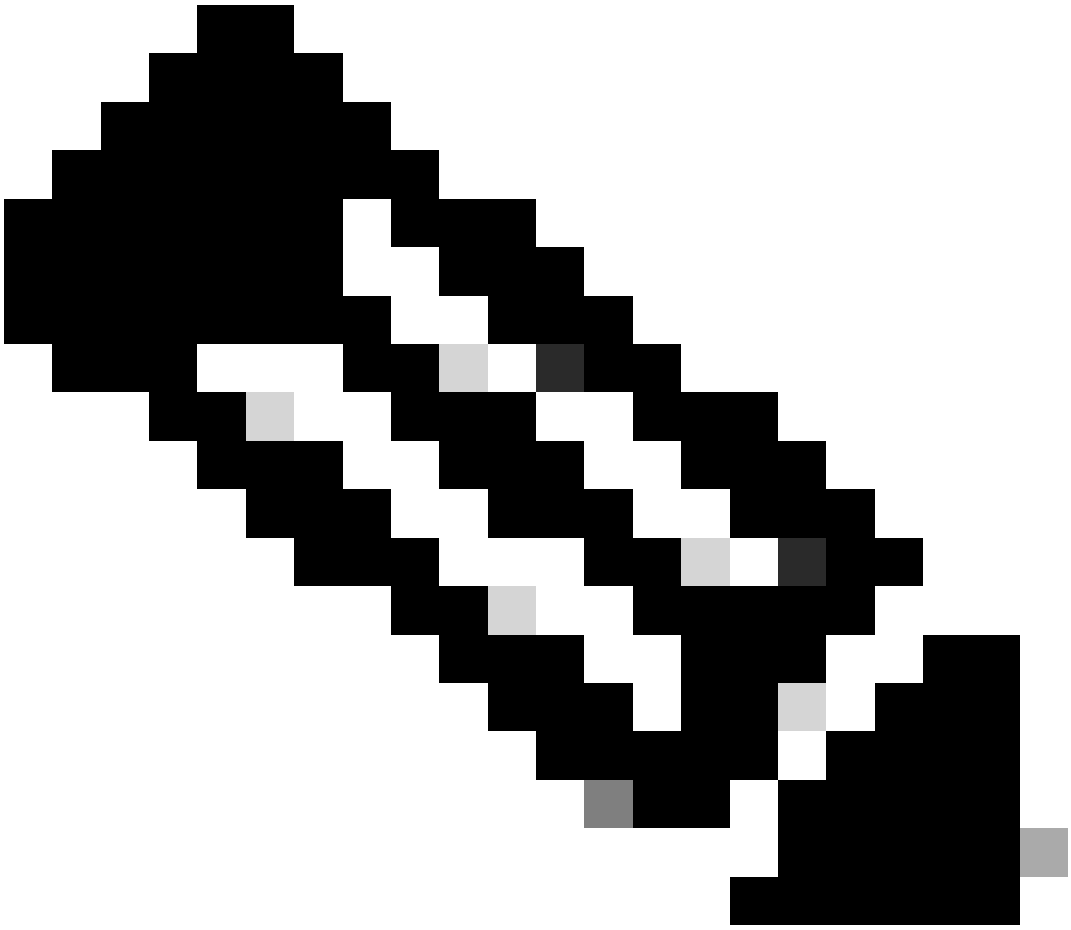
Passaggio 11: Passare ad App > Ricerca e reporting nell'interfaccia utente Web.



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

i log ricevuti.



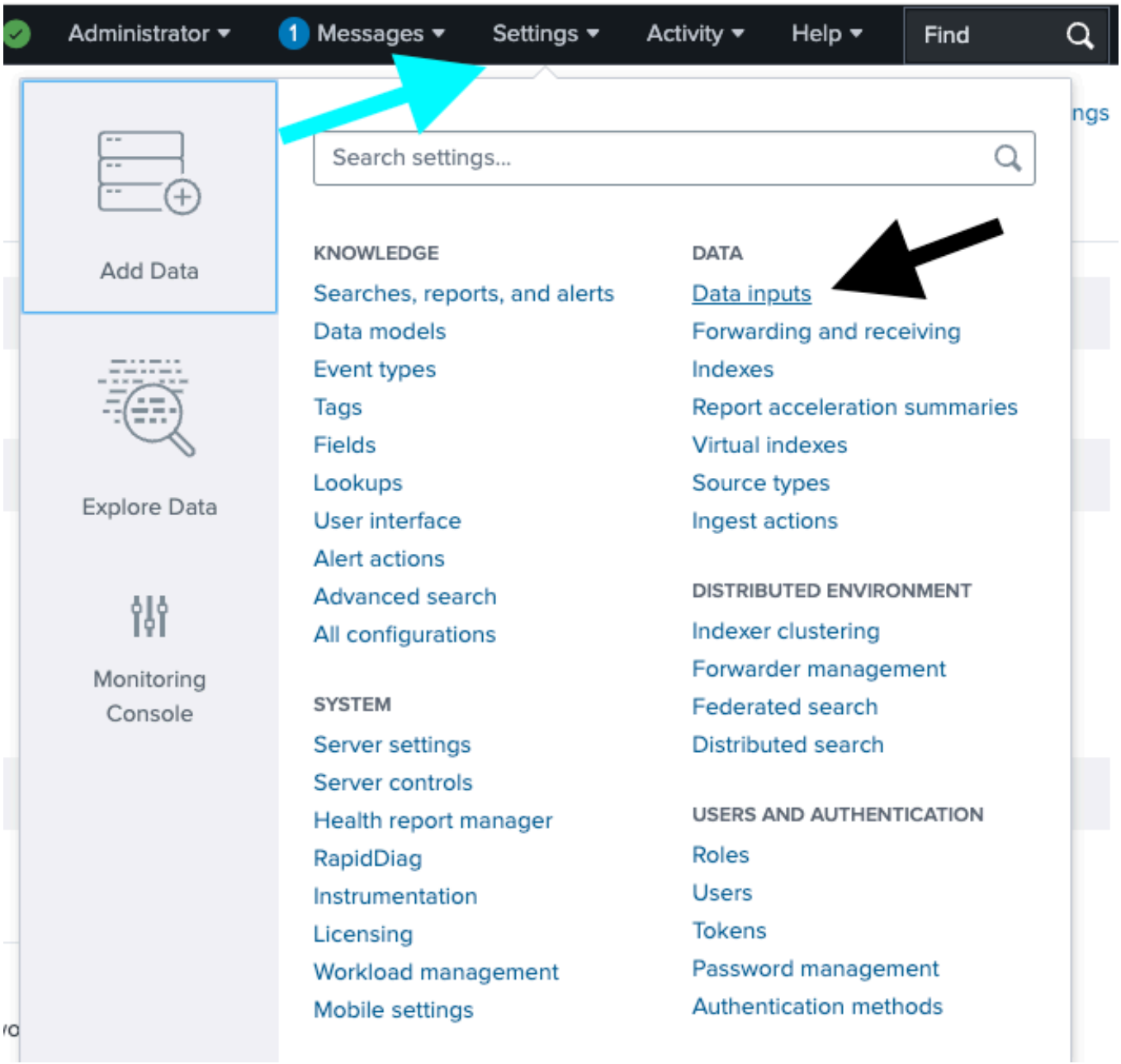


Nota: Per l'origine vedere il passo 4
Per source_type vedere il passo 6

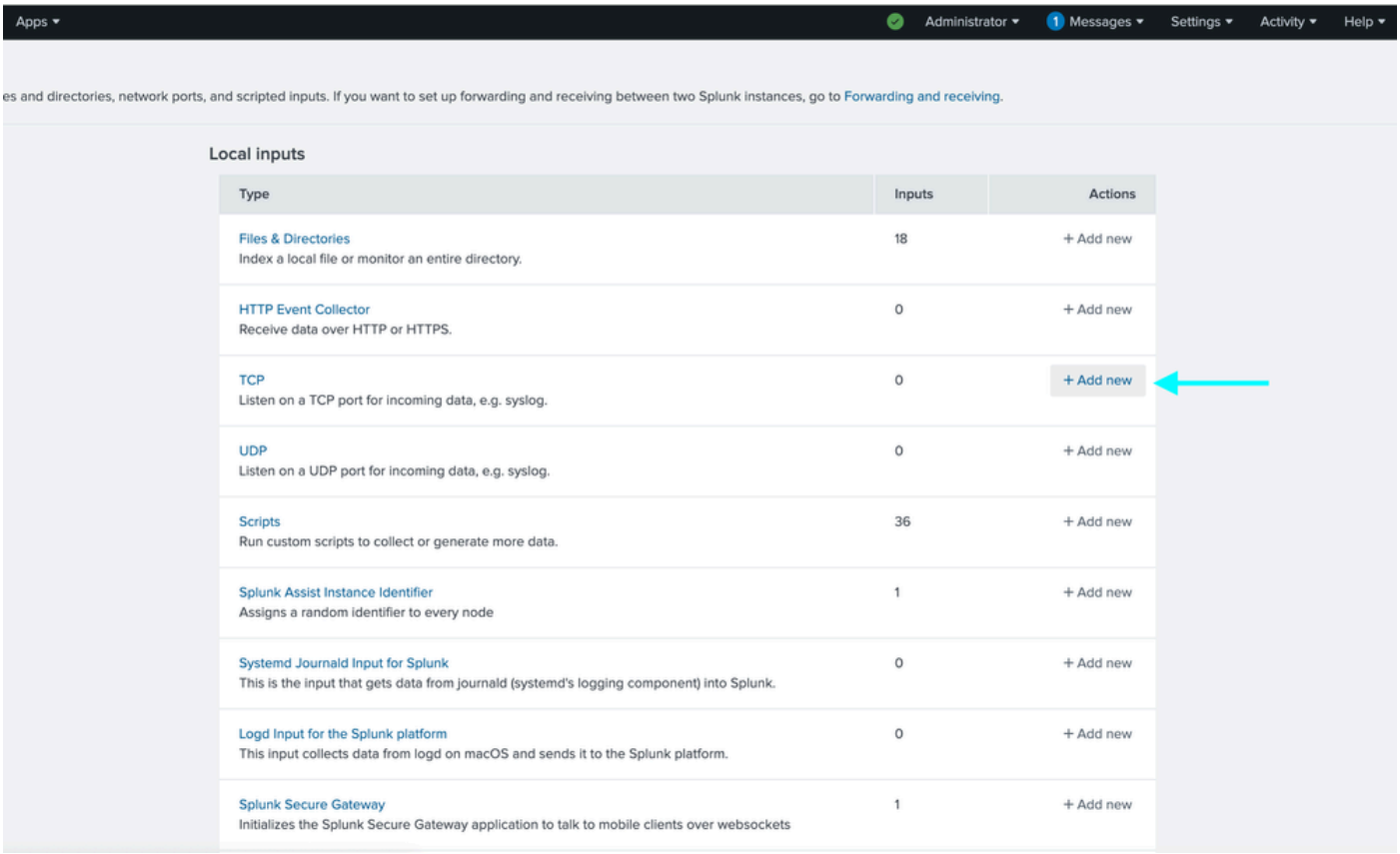
Configurare syslog su SNA sulla porta TCP 6514 o sulla porta personalizzata

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

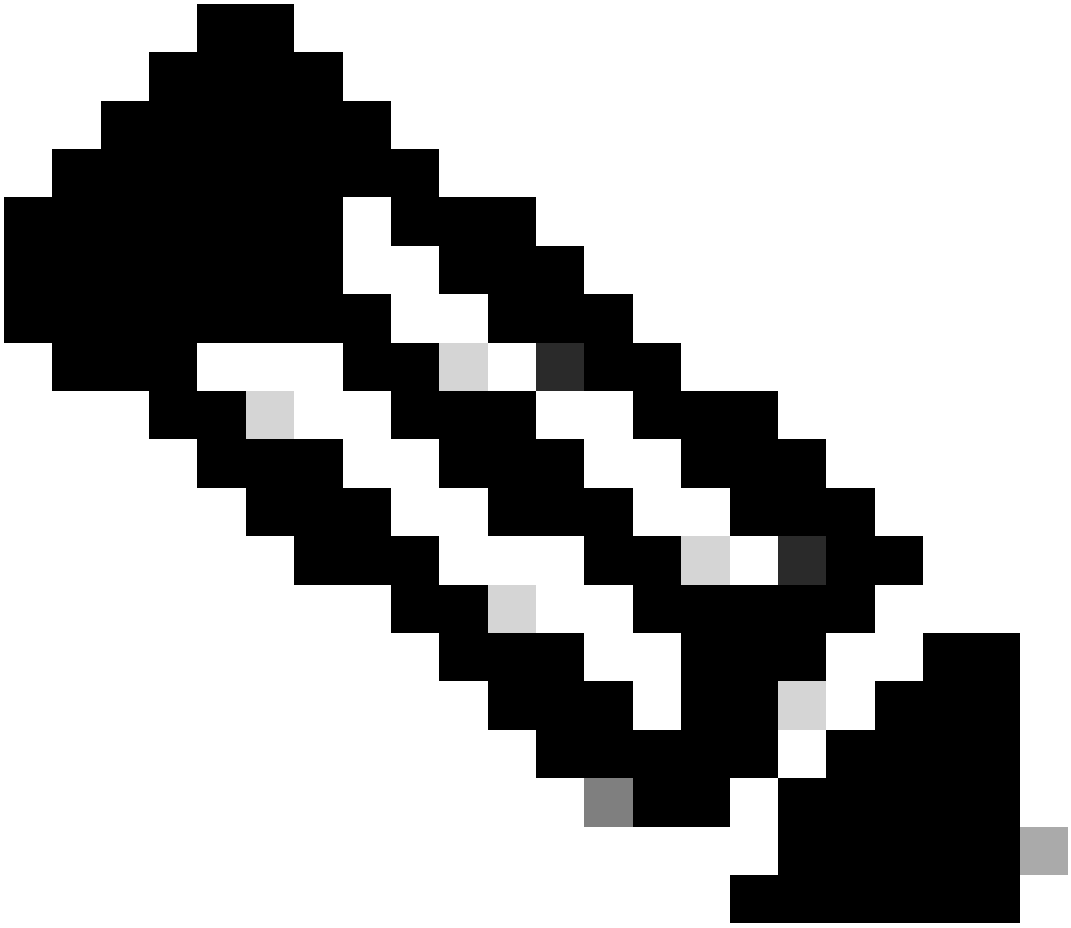
Passaggio 1: Nell'interfaccia utente Splunk, selezionare Impostazioni > Aggiungi dati > Input dati.



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

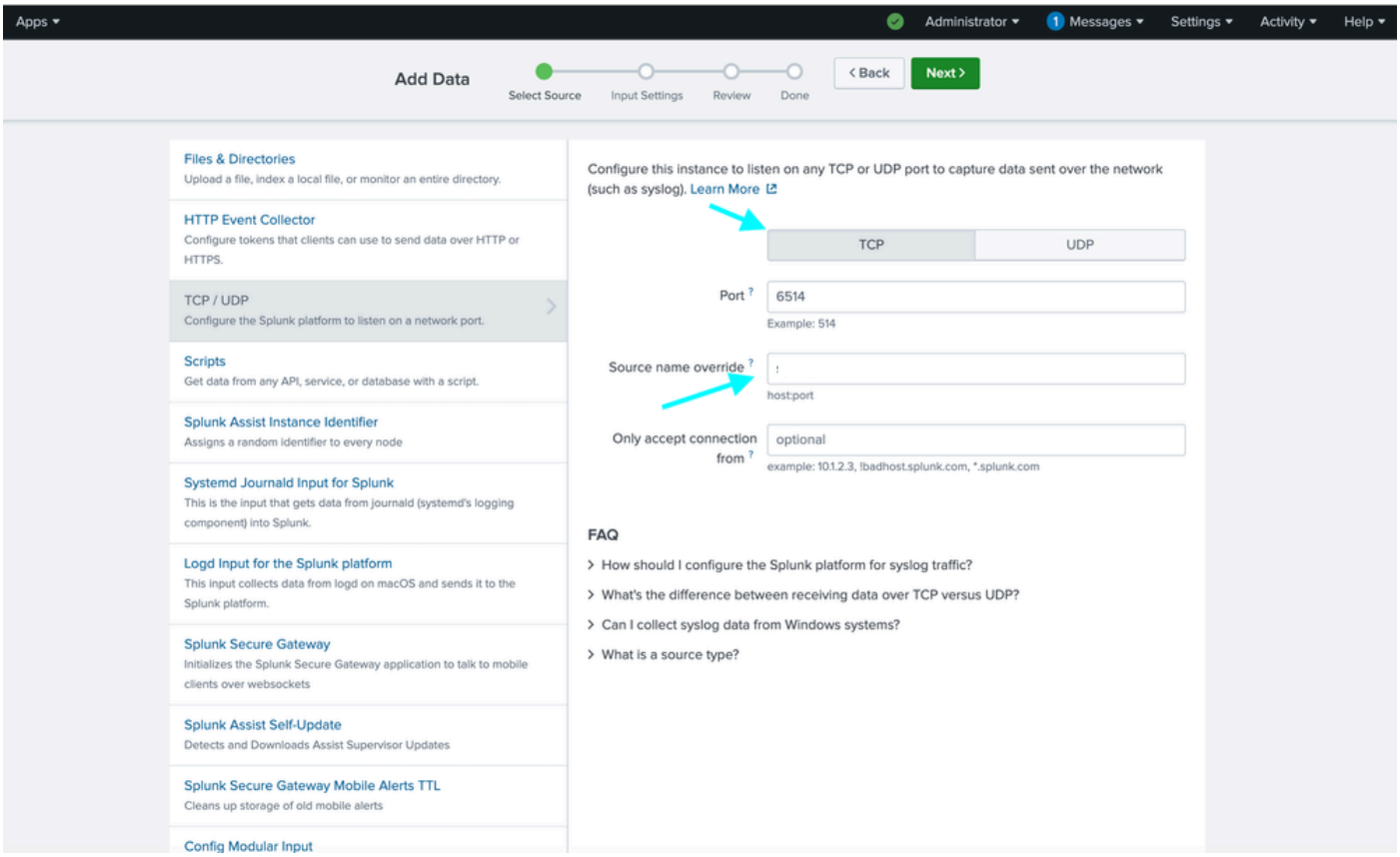


Passaggio 3: Nella nuova finestra selezionare TCP, immettere la porta di ricezione desiderata, nella porta immagine di esempio 6514, quindi immettere "nome desiderato" nel campo Sostituzione nome origine.



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

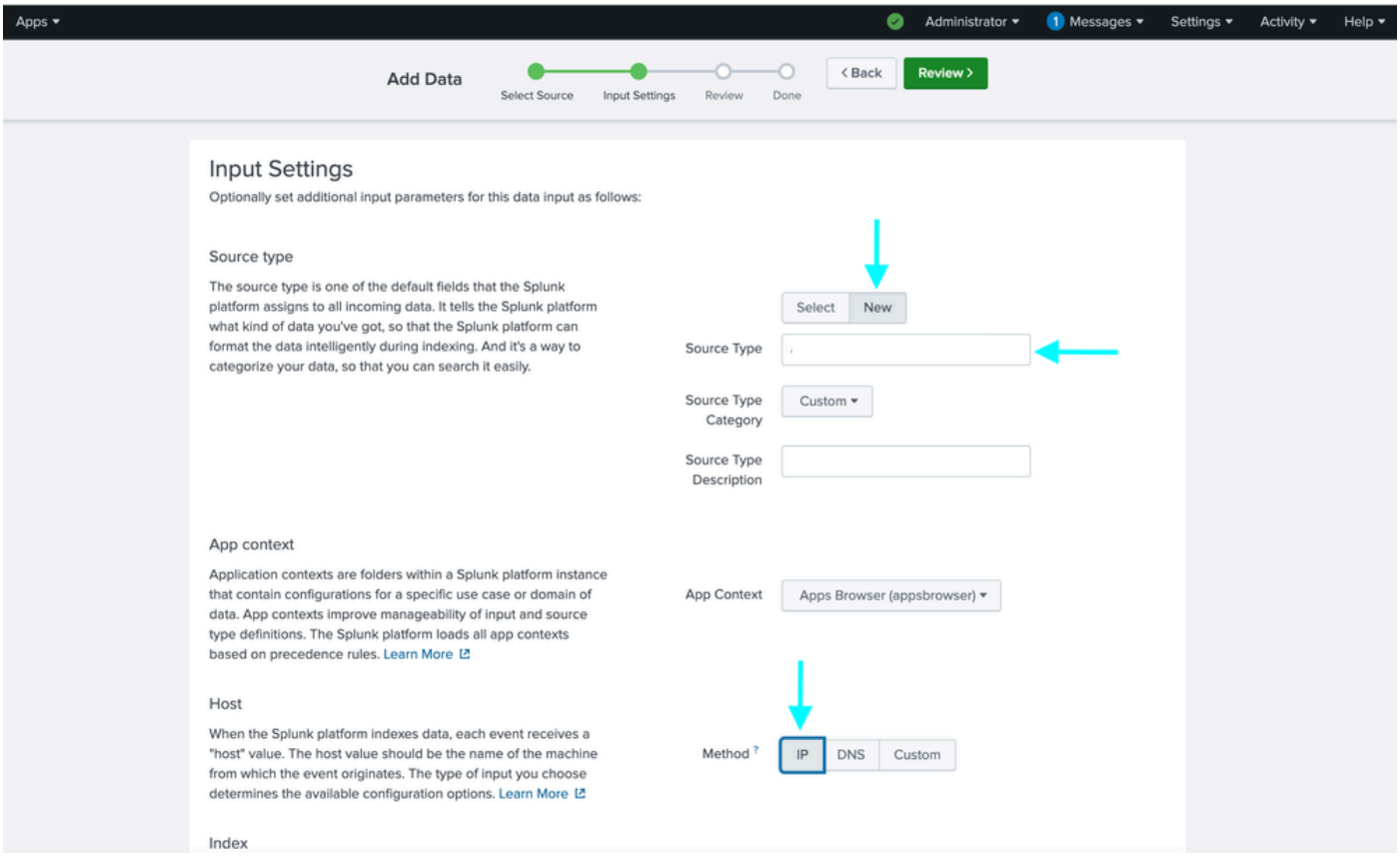
Passaggio 4: Al termine, fare clic sul pulsante verde Avanti > nella parte superiore della finestra.



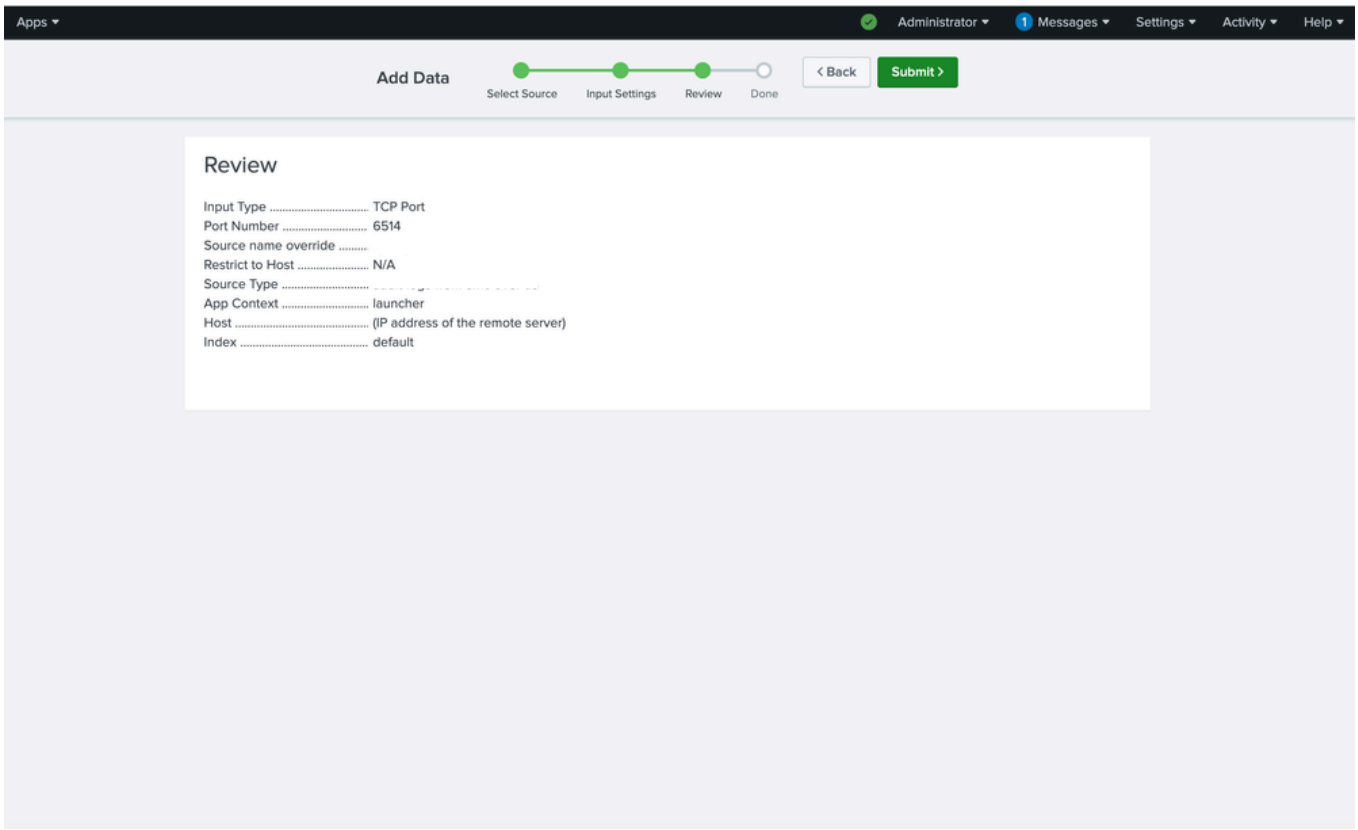
Passaggio 5: Nella nuova finestra selezionare Nuovo nella sezione Tipo di origine, immettere il nome desiderato nel campo Tipo di origine.

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

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



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.



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.

```
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:
-----
user@examplehost:
```

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.cer
```

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.

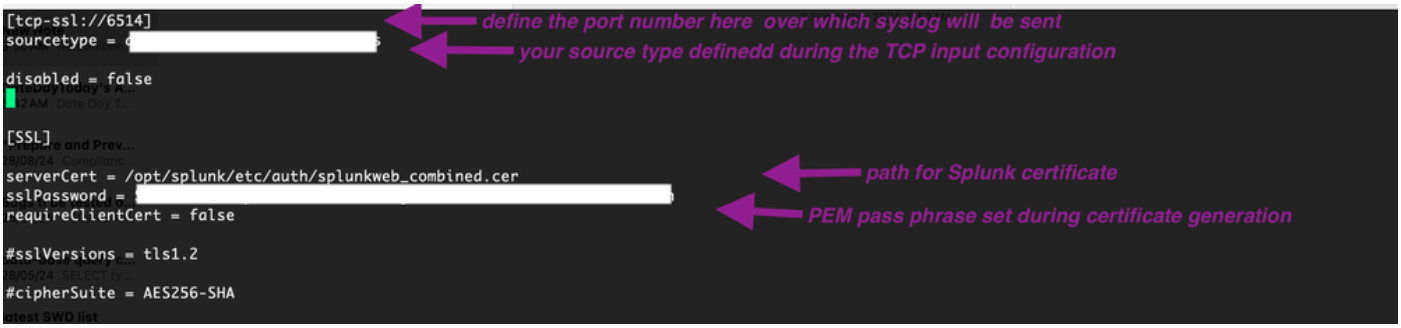
```
user@examplehost:~# chown 10777:10777/opt/splunk/etc/auth/splunkweb.cer
```

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

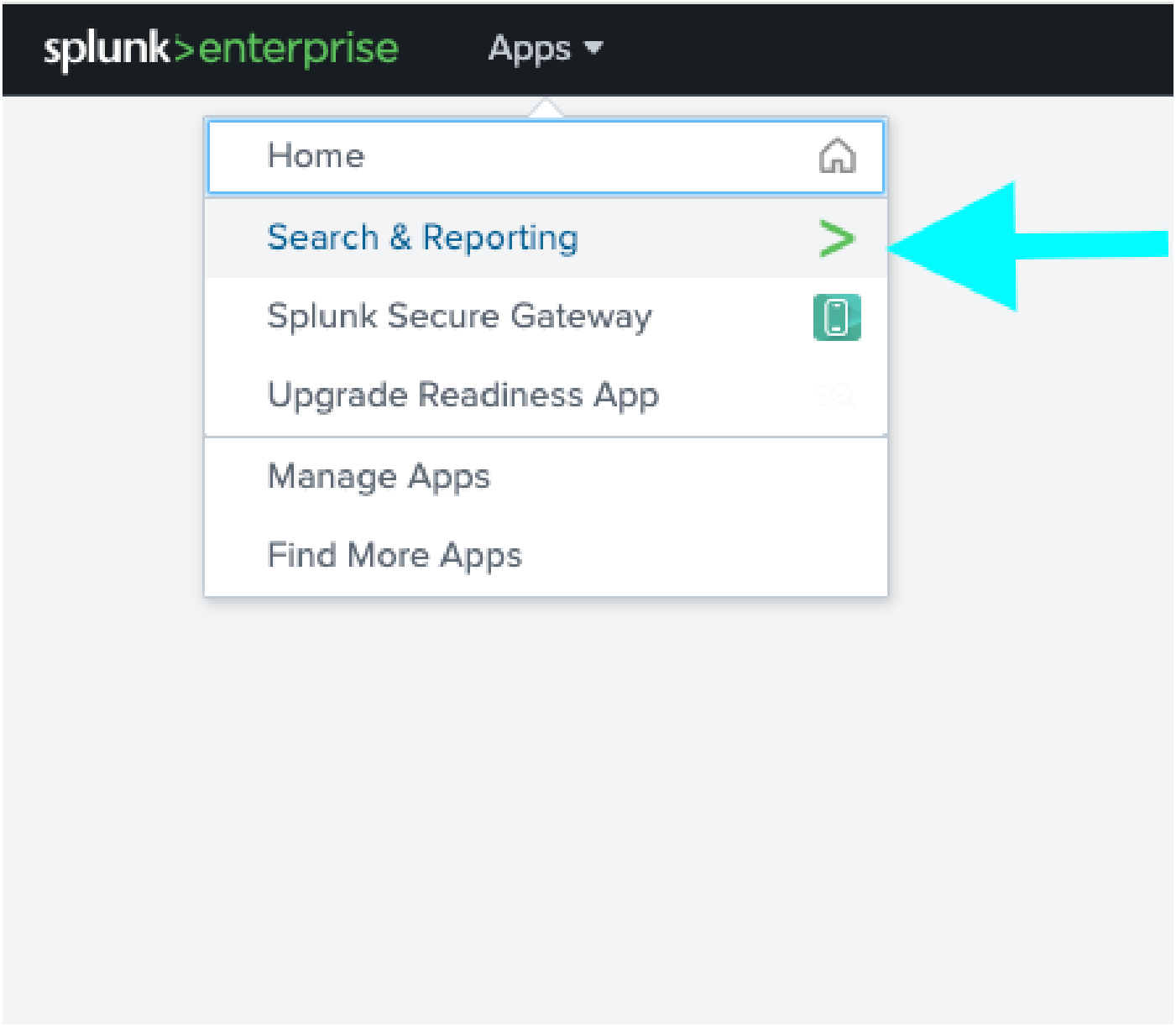
```
user@examplehost:~# chmod 600/opt/splunk/etc/auth/splunkweb.cer
```

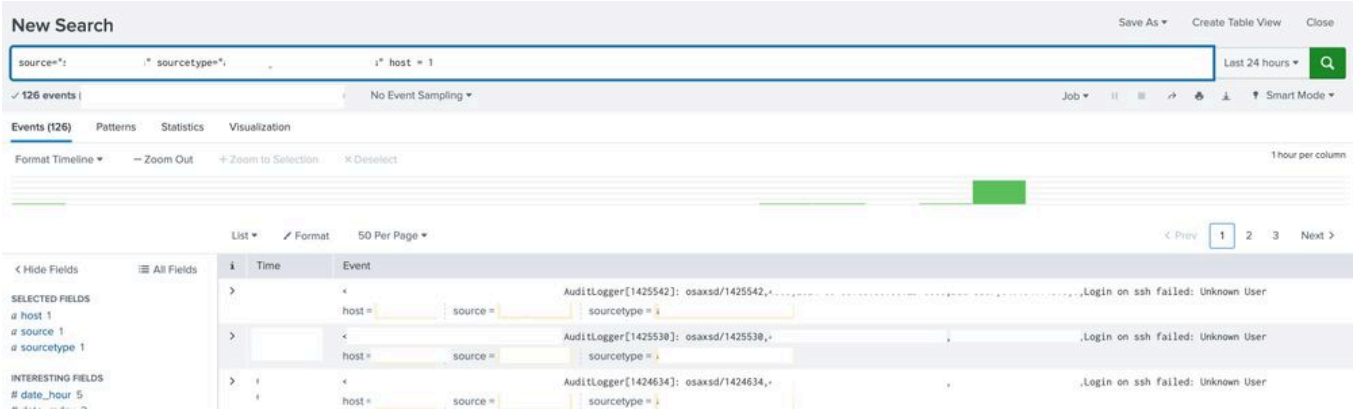
Passaggio 7: creare un nuovo file input.conf.

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



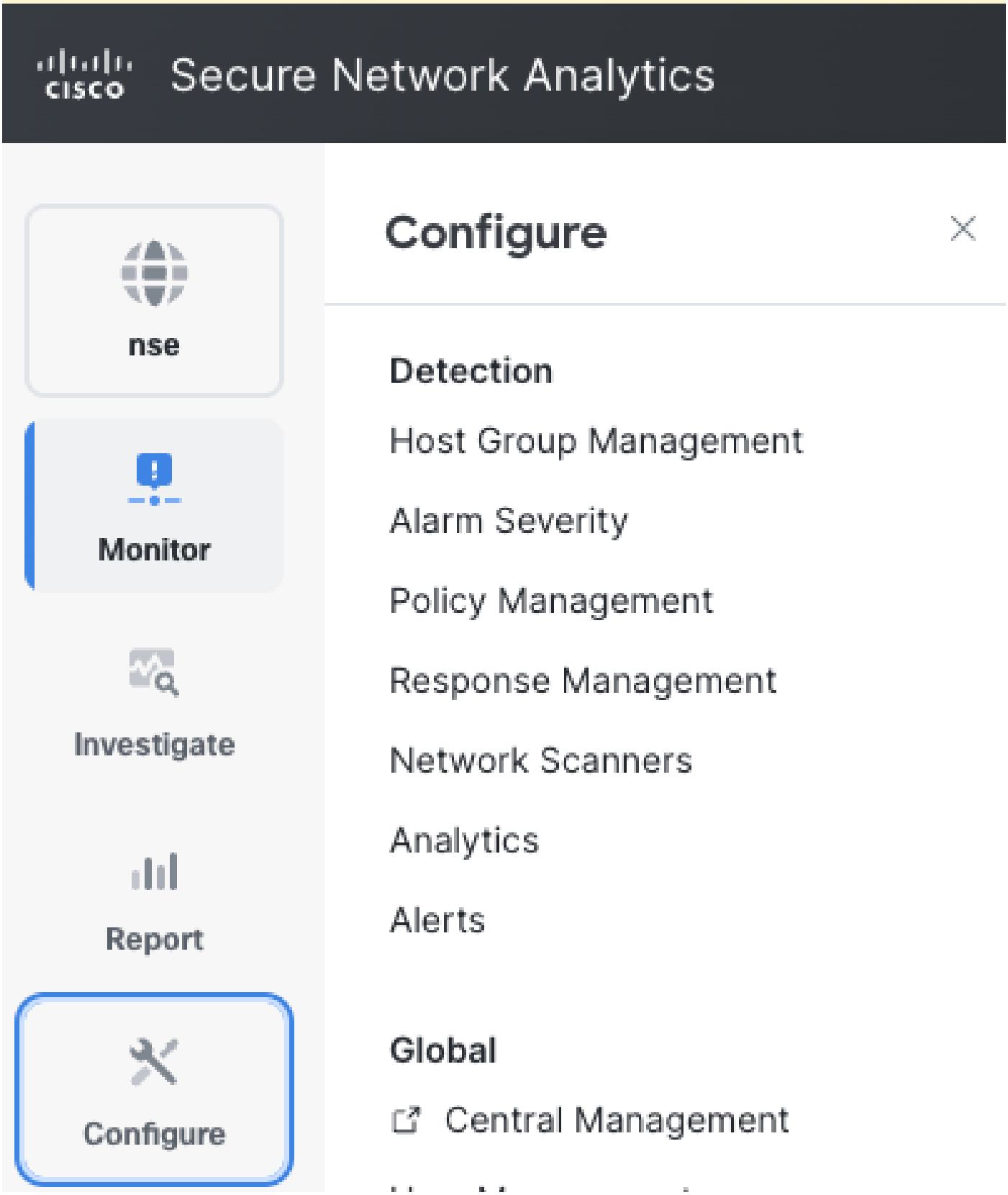
Passaggio 8: Verificare i syslog utilizzando la funzione di ricerca.



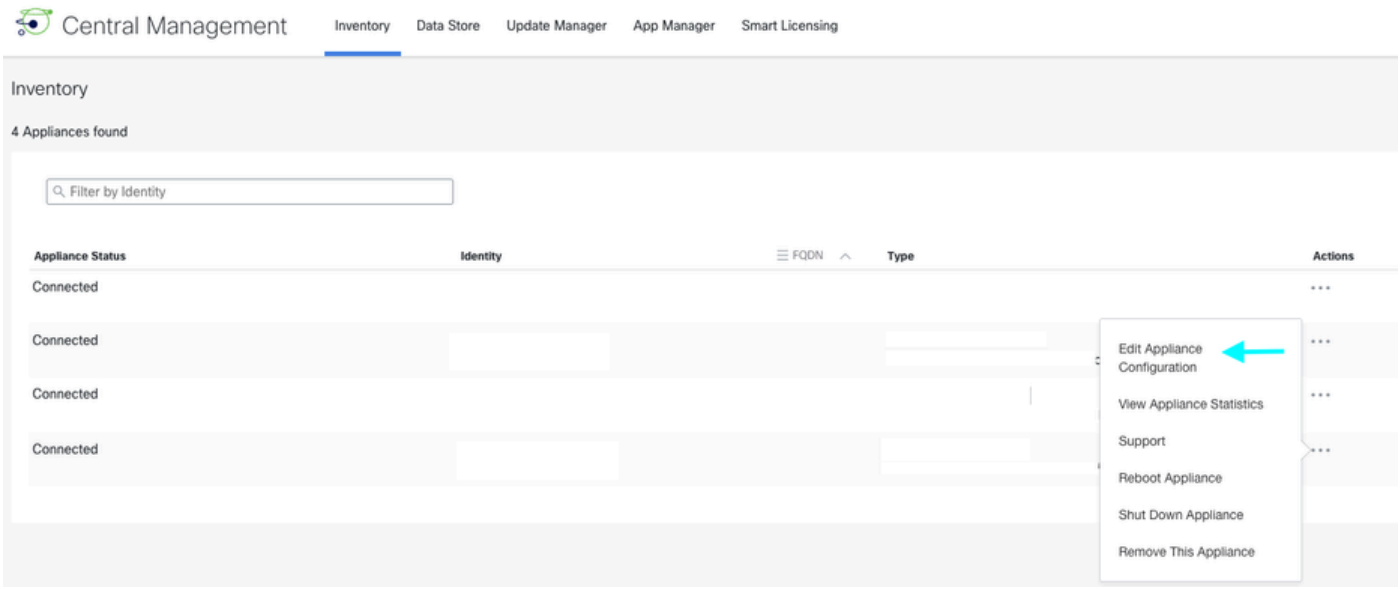


3. Configurare la destinazione del log di controllo sulla SNA

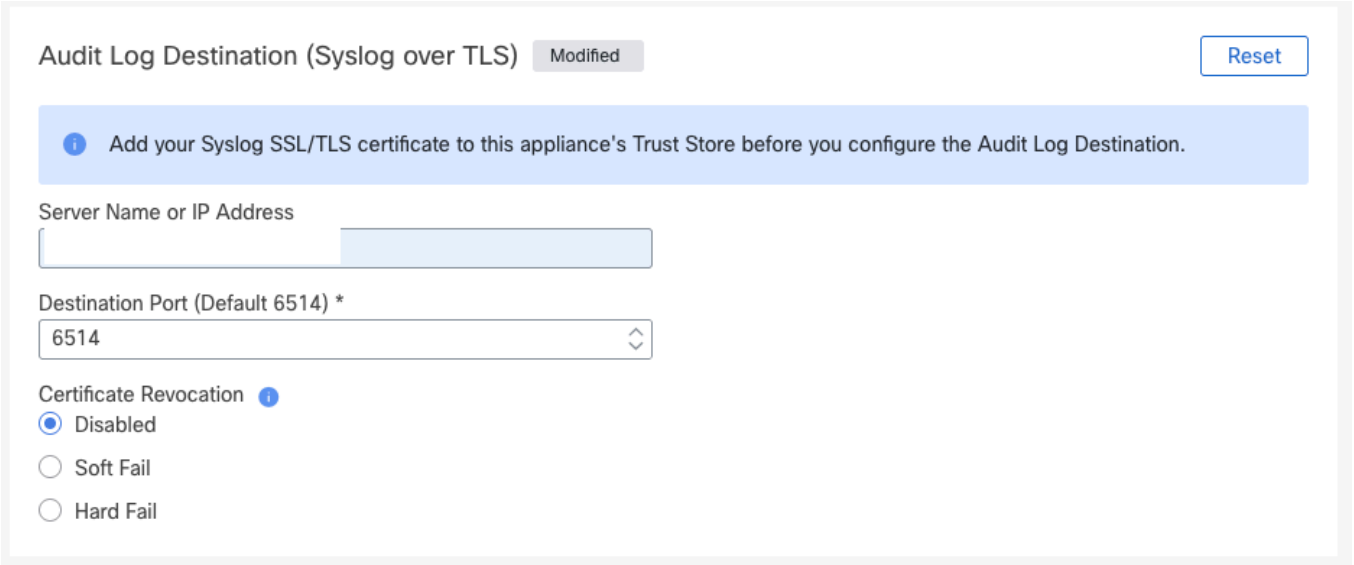
Passaggio 1: Accedere all'interfaccia utente SMC e selezionare Configure > Central Management.



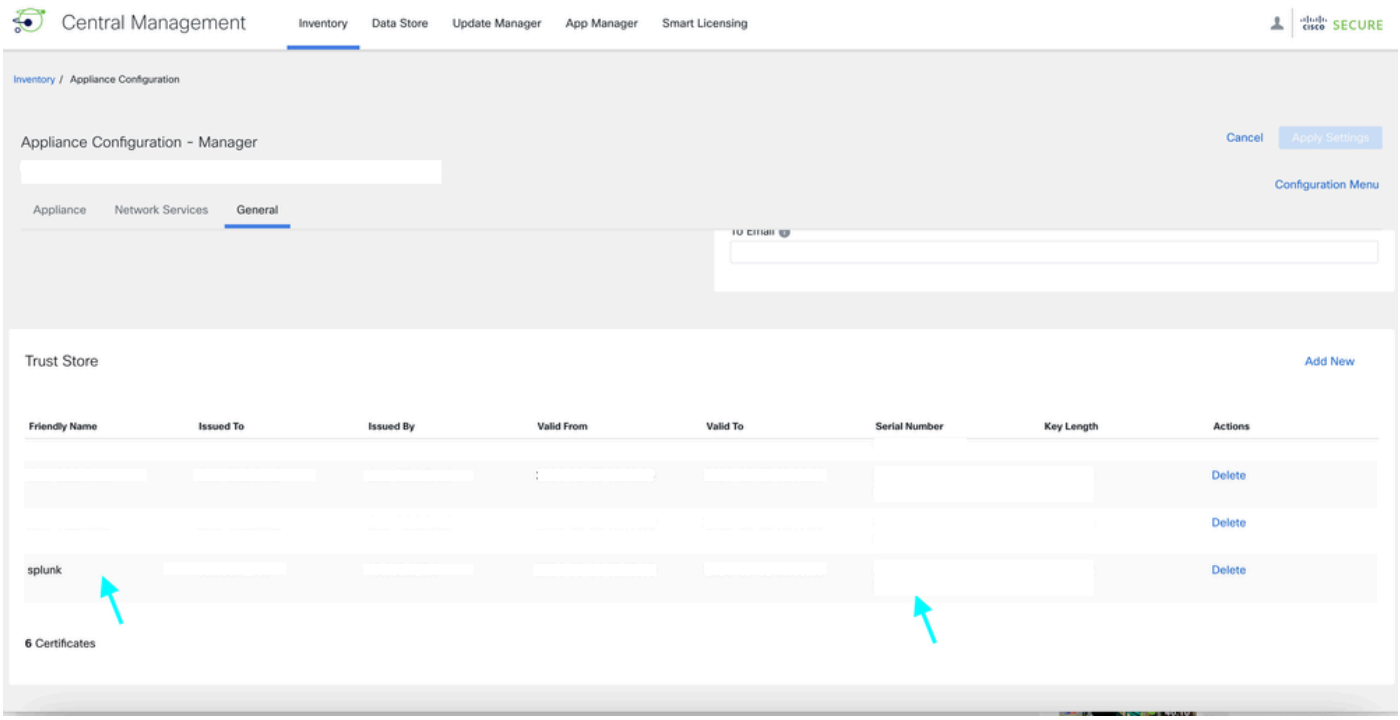
Passaggio 2: Fare clic sull'icona con i puntini di sospensione dell'accessorio SNA desiderato e selezionare Modifica configurazione accessorio.



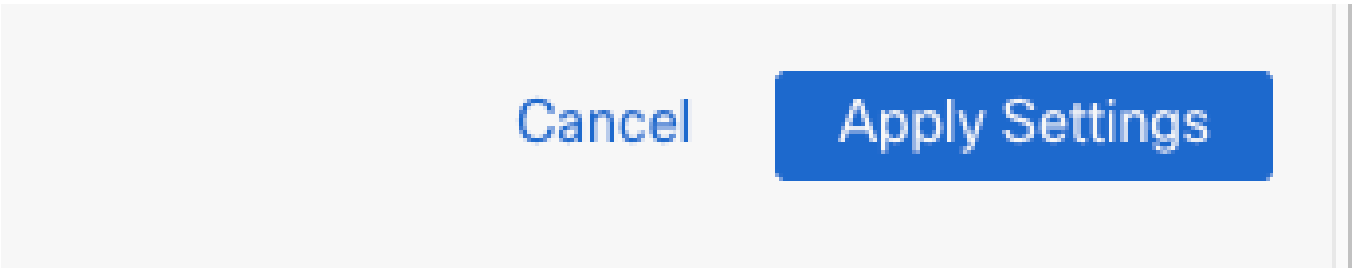
Passaggio 3: Passare alla scheda Servizi di rete e immettere i dettagli relativi alla destinazione del log di verifica (syslog over TLS).



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.

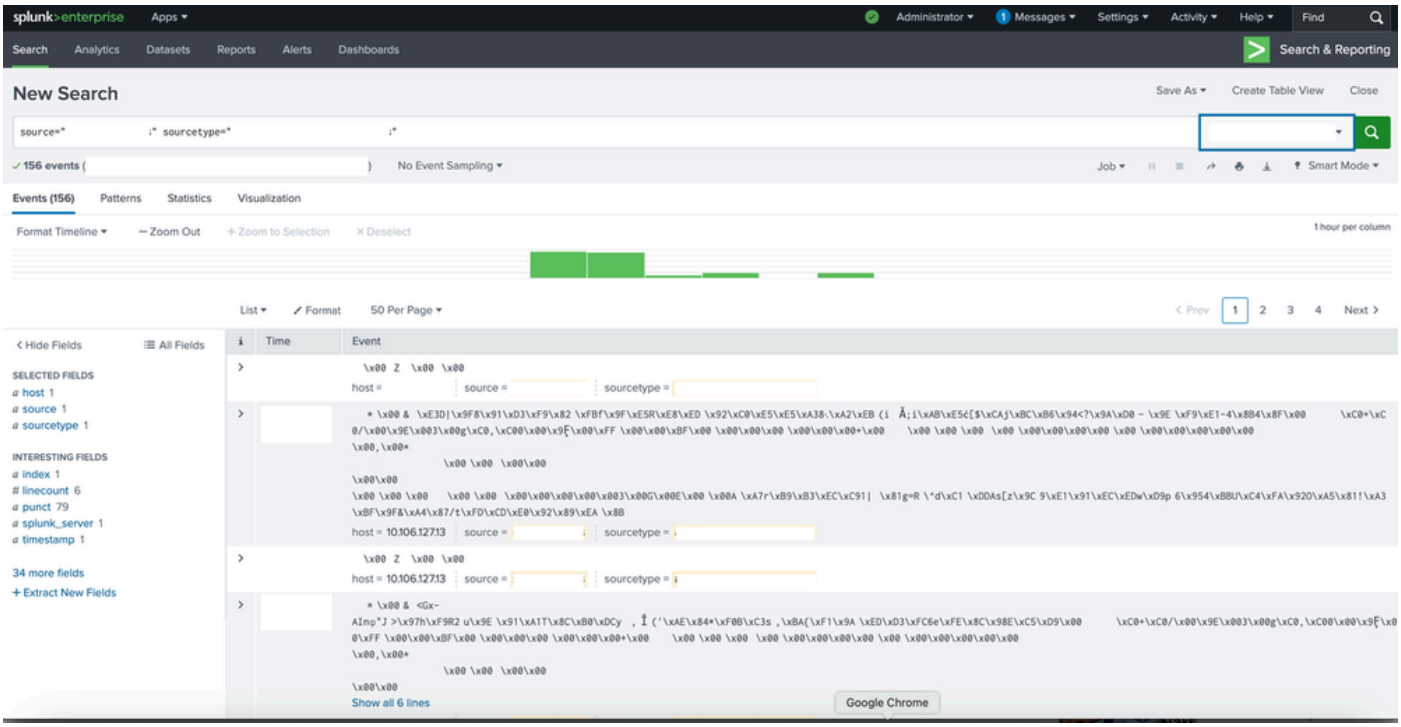


Passaggio 5: Fare clic su Applica impostazioni.



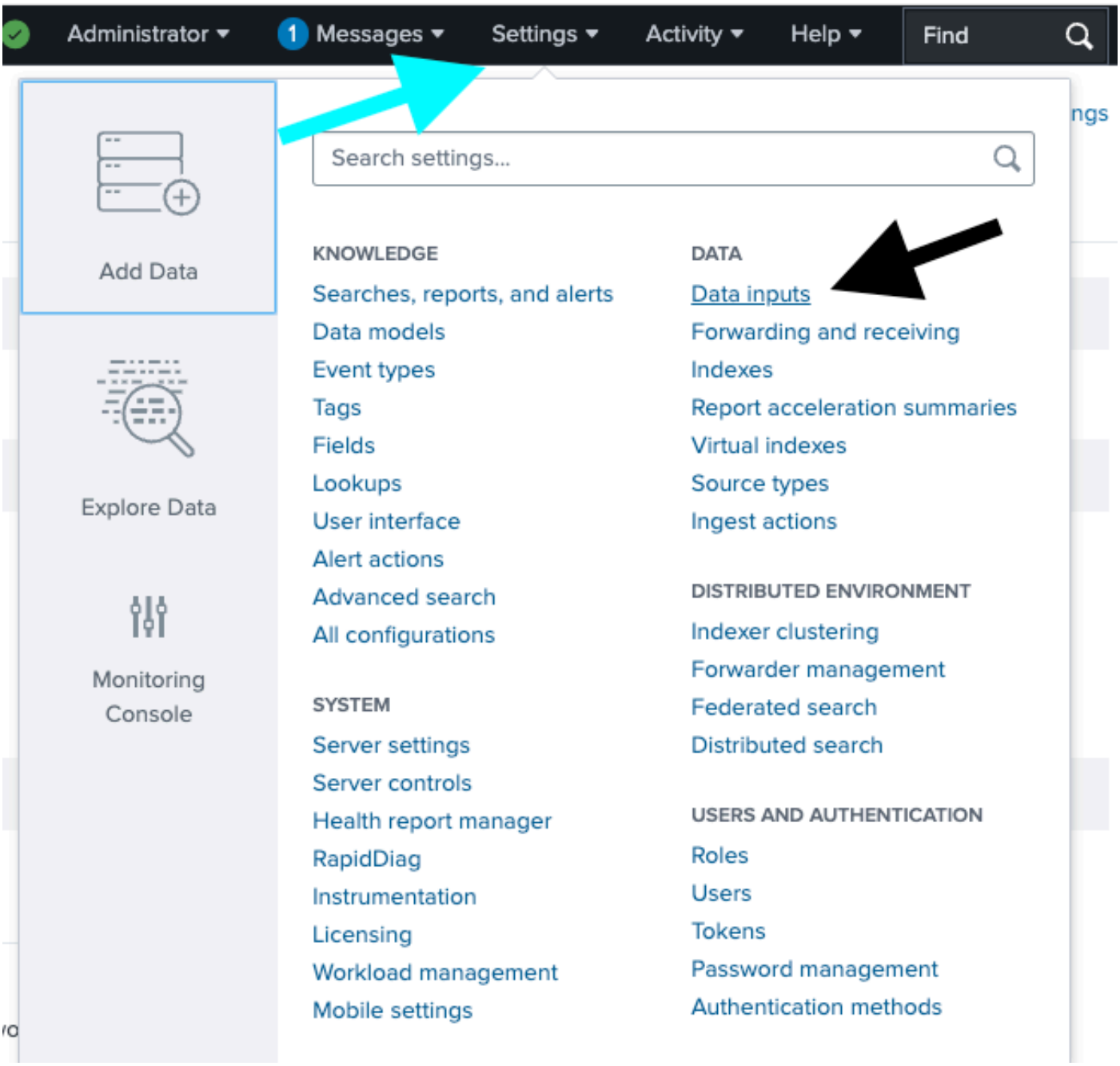
Risoluzione dei problemi

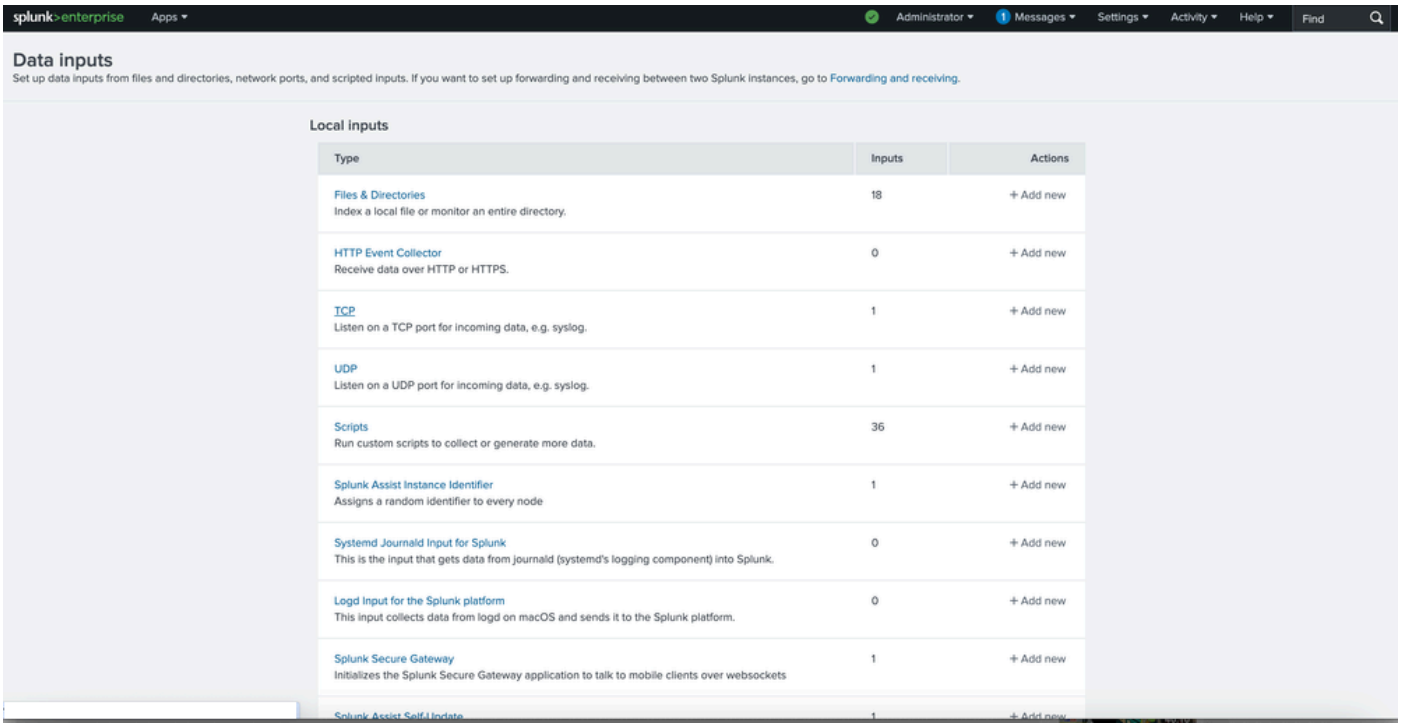
Potrebbero esserci degli scherzi completi che si presentano durante le ricerche.

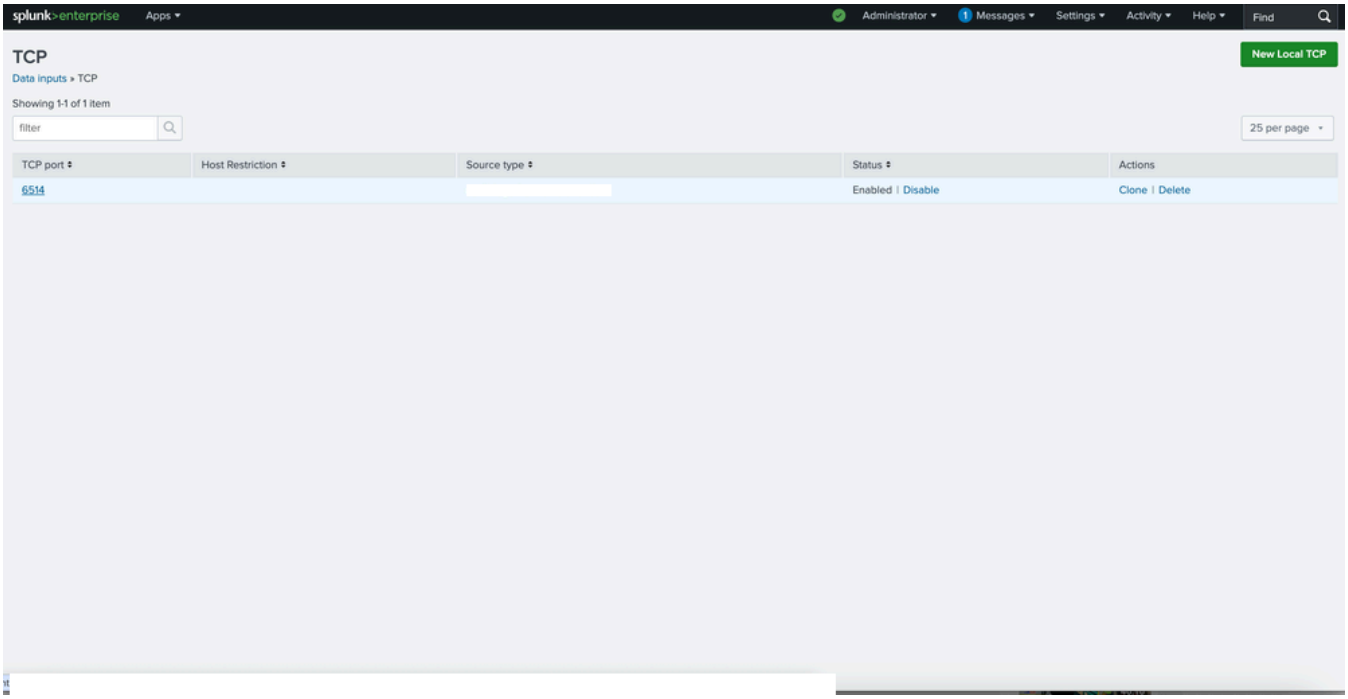


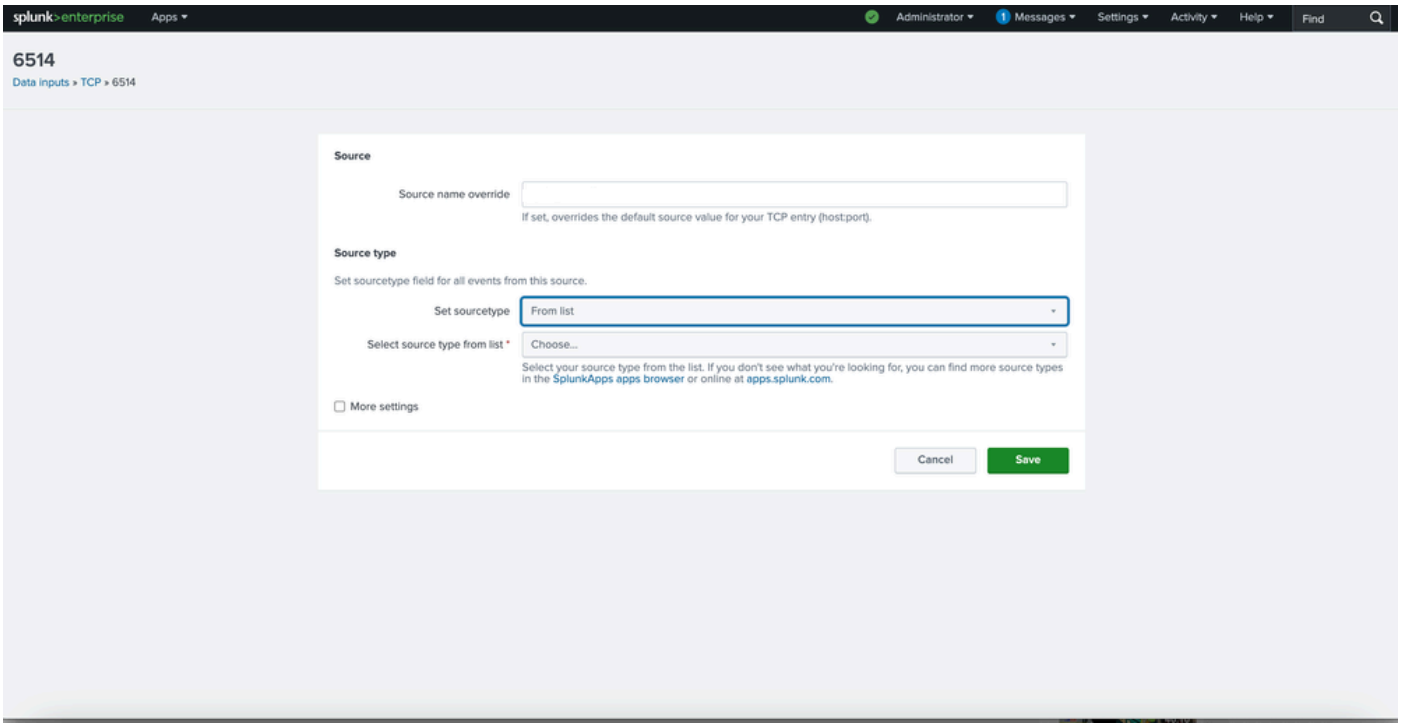
Soluzione:

Mappare l'input al tipo di origine corretto.


Administrator
1 Messages
Settings
Activity
Help
Find
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


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
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


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
TCP
New Local 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


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
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
From list
Select source type from list *
Choose...
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).