配置響應管理以將系統日誌事件傳送到Splunk

目錄

簡介

本文檔介紹如何配置安全分析響應管理功能，以通過系統日誌將事件傳送到第三方，如Splunk。

必要條件

需求

思科建議您瞭解以下主題：

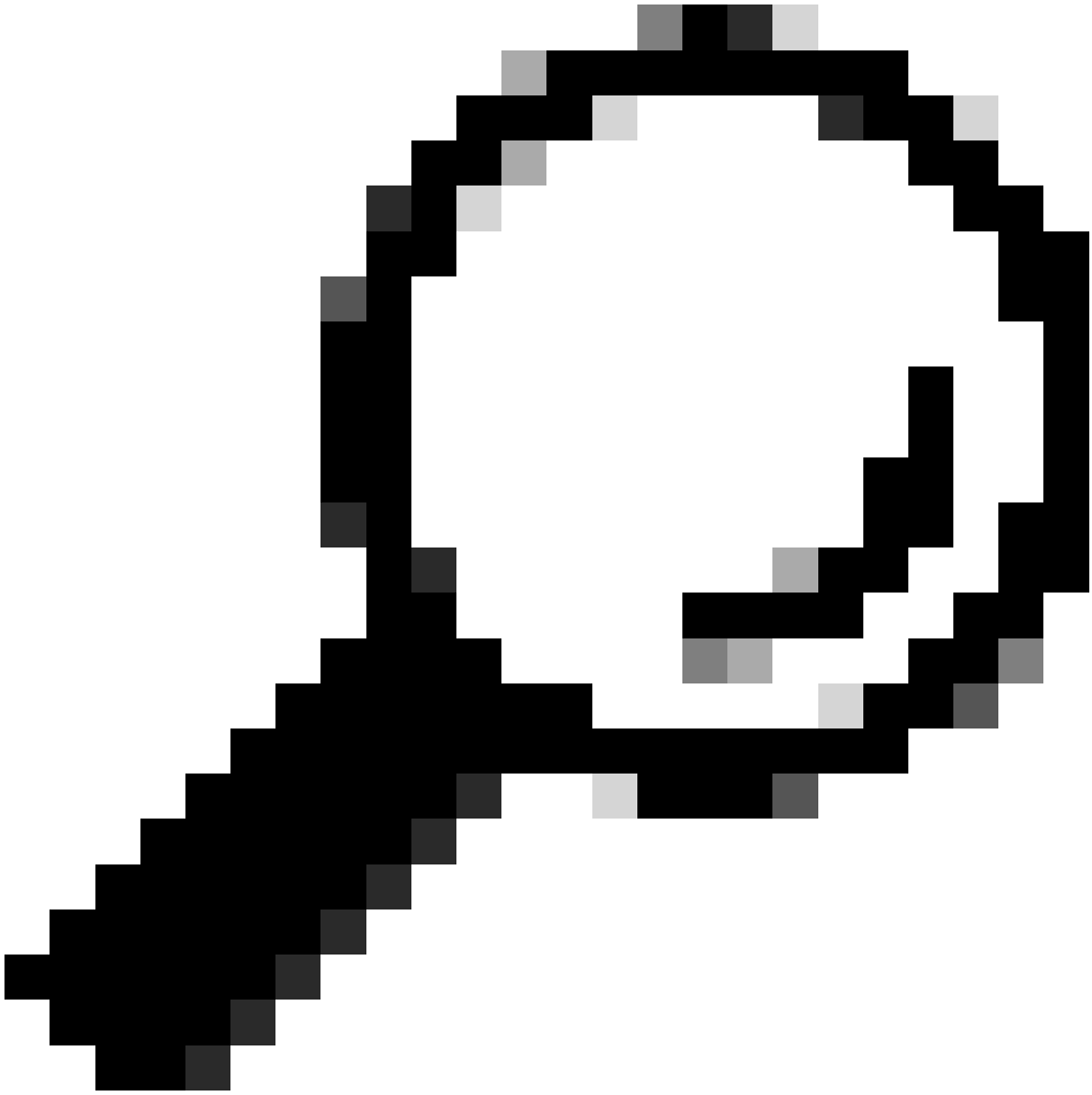
- 安全網路分析回應管理。
- Splunk系統日誌

採用元件

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

- 至少包含一個Manager裝置和一個流量收集器裝置的安全網路分析(SNA)部署。
- Splunk伺服器已安裝並可通過443埠訪問。

在通過UDP 514或自定義埠的SNA上配置syslog



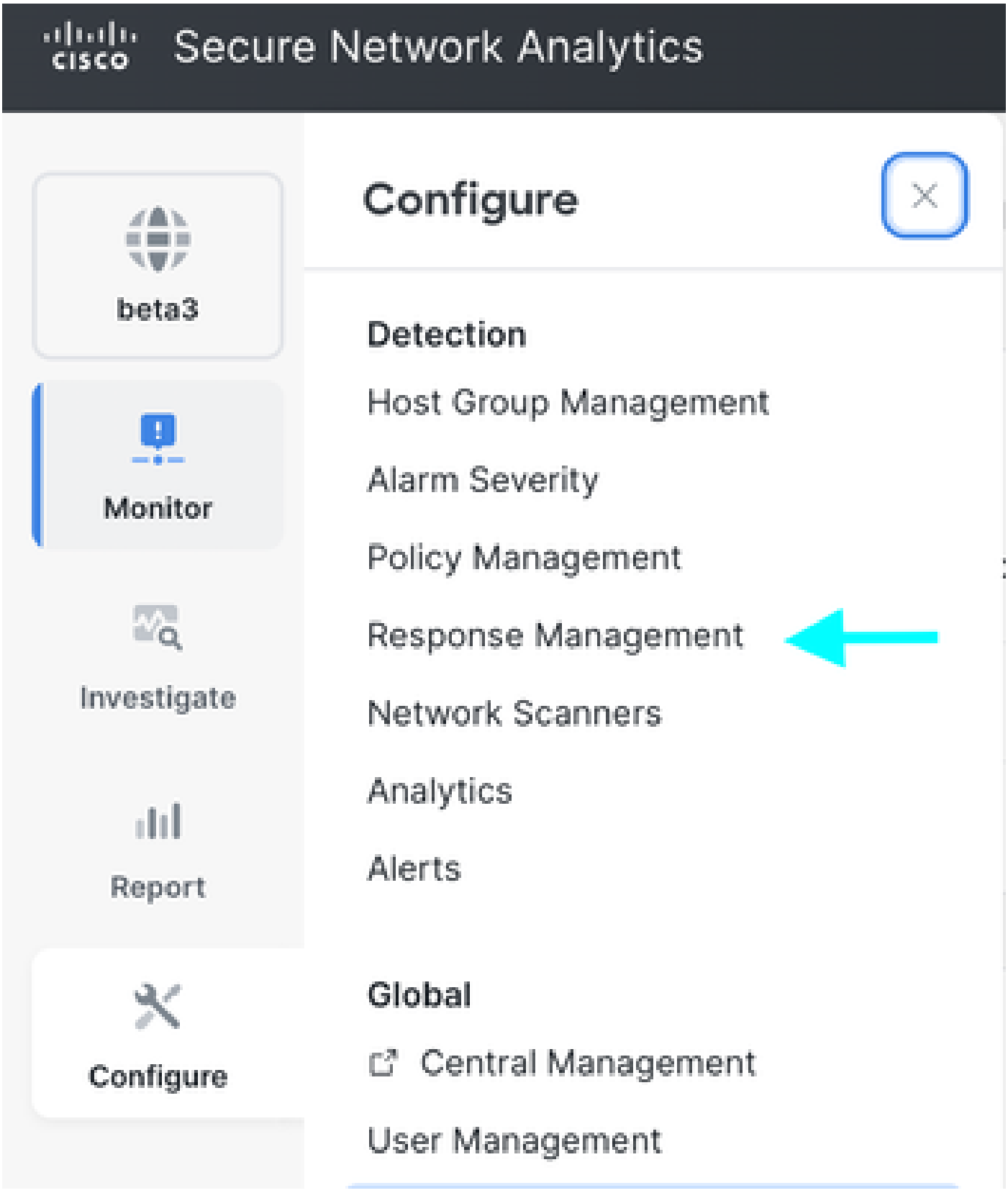
提示：確保在SNA和Splunk之間的任何防火牆或中間裝置上允許UDP/514、TCP/6514或您選擇用於系統日誌的任何自定義埠。

1.SNA回應管理

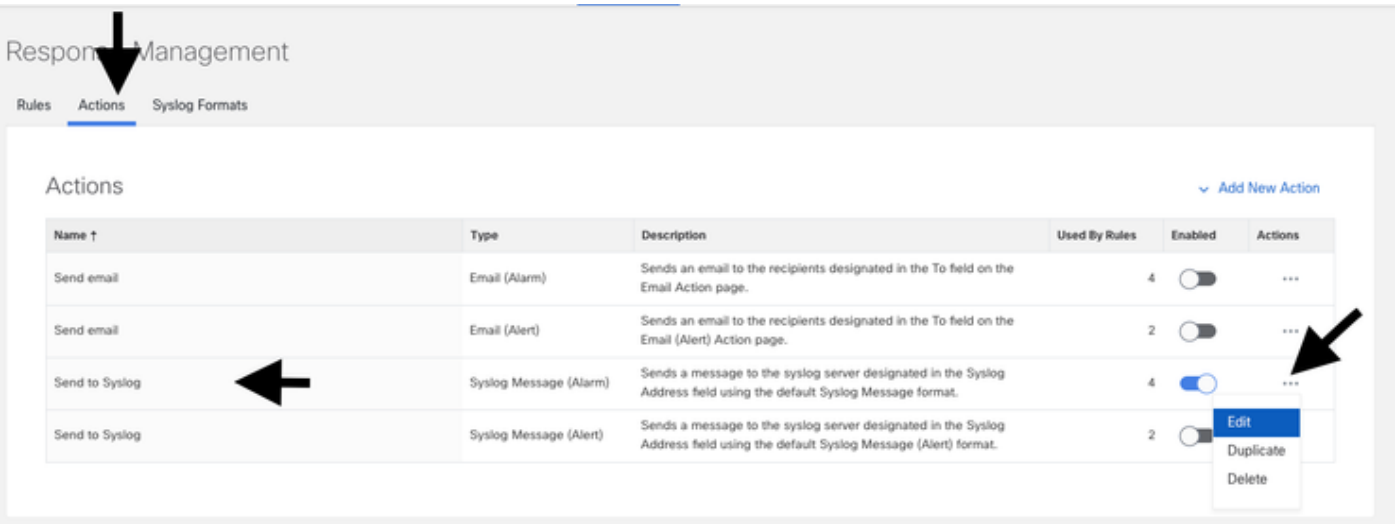
Secure Analytics(SA)的響應管理元件可用於配置規則、操作和系統日誌目標。

必須配置這些選項以將Secure Analytics警報傳送/轉發到其他目標。

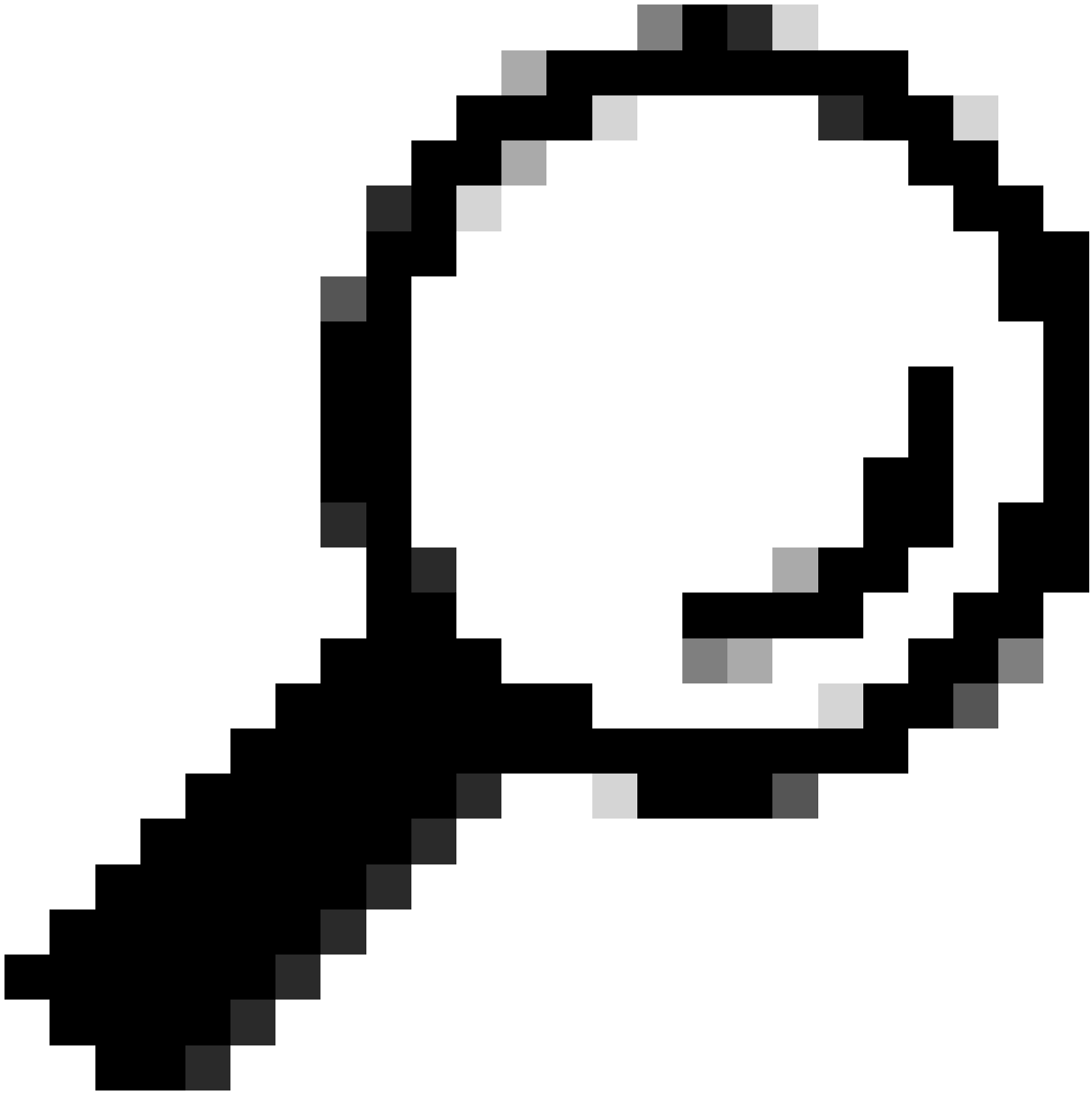
第1步：登入到SA Manager裝置，然後導航至Configure > Detection Response Management。



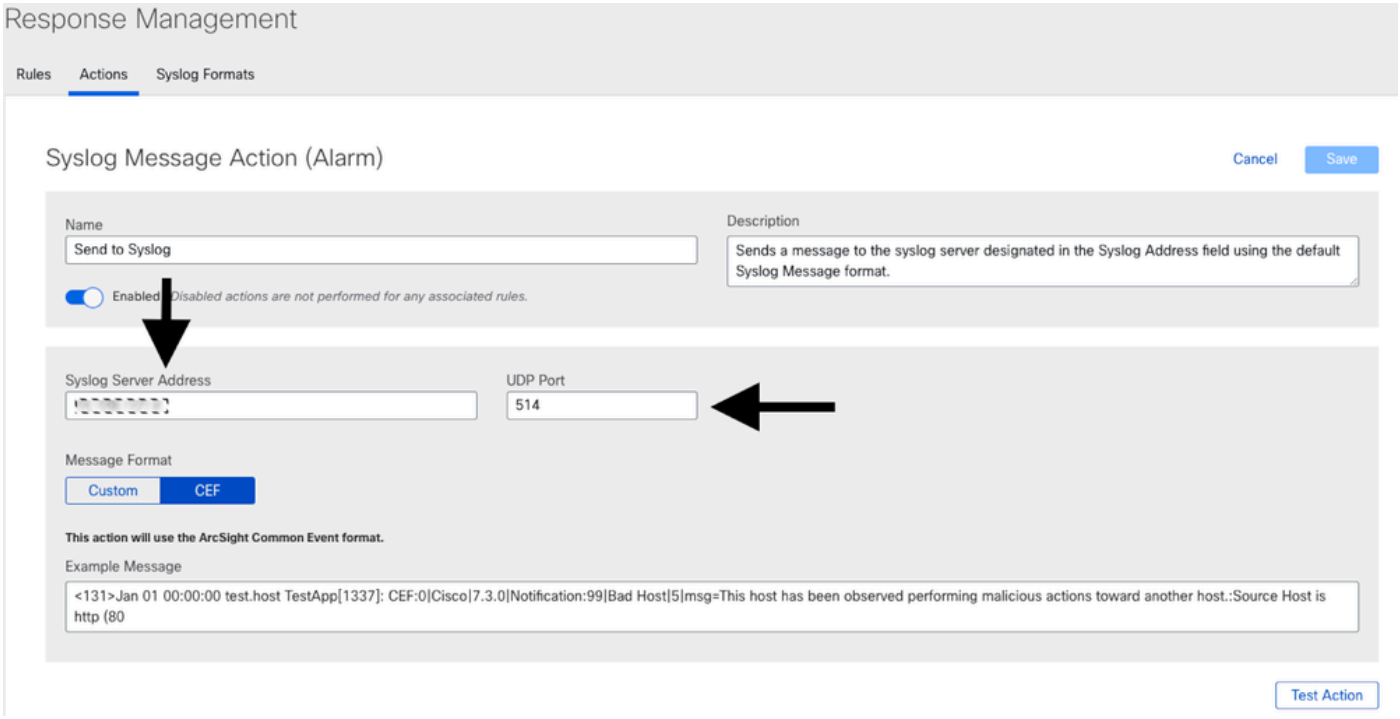
步驟 2:在新頁面上，導航到Actions頁籤，找到預設的Send to Syslog行專案，然後按一下Action列中的省略號(...)，然後Edit。



步驟 3:在Syslog Server Address欄位中輸入所需的目標地址，在UDP Port欄位中輸入所需的目標接收埠。在Message Format中選擇CEF。
步驟 4:完成後，按一下右上角的藍色Save按鈕。



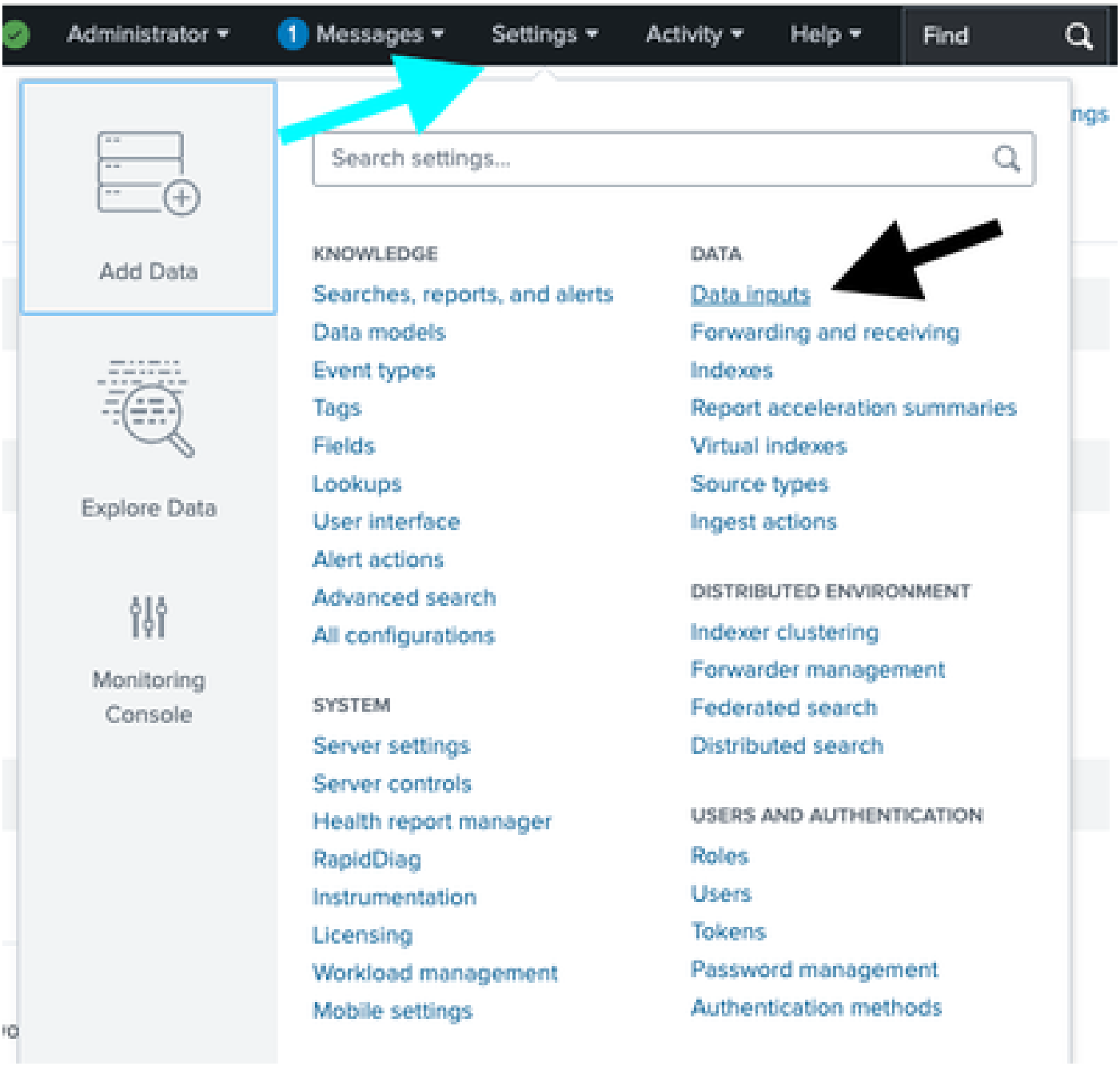
提示：系統日誌的預設UDP埠為514



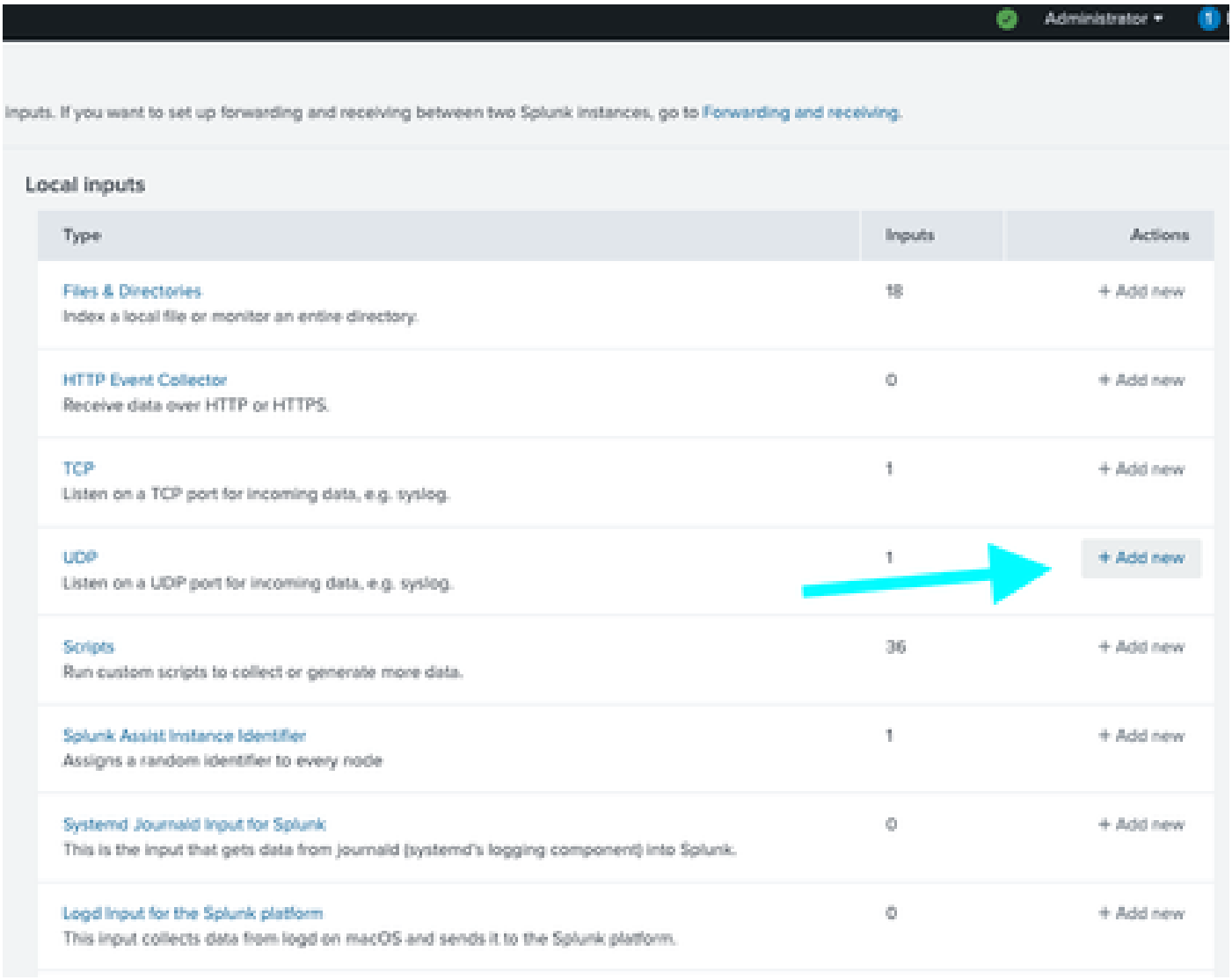
2.配置Splunk以通過UDP埠接收SNA系統日誌

在Secure Network Analytics Manager Web UI上應用更改後，必須在Splunk中配置資料輸入。

步驟 1:登入到Splunk，然後導航到設定>新增資料>資料輸入。

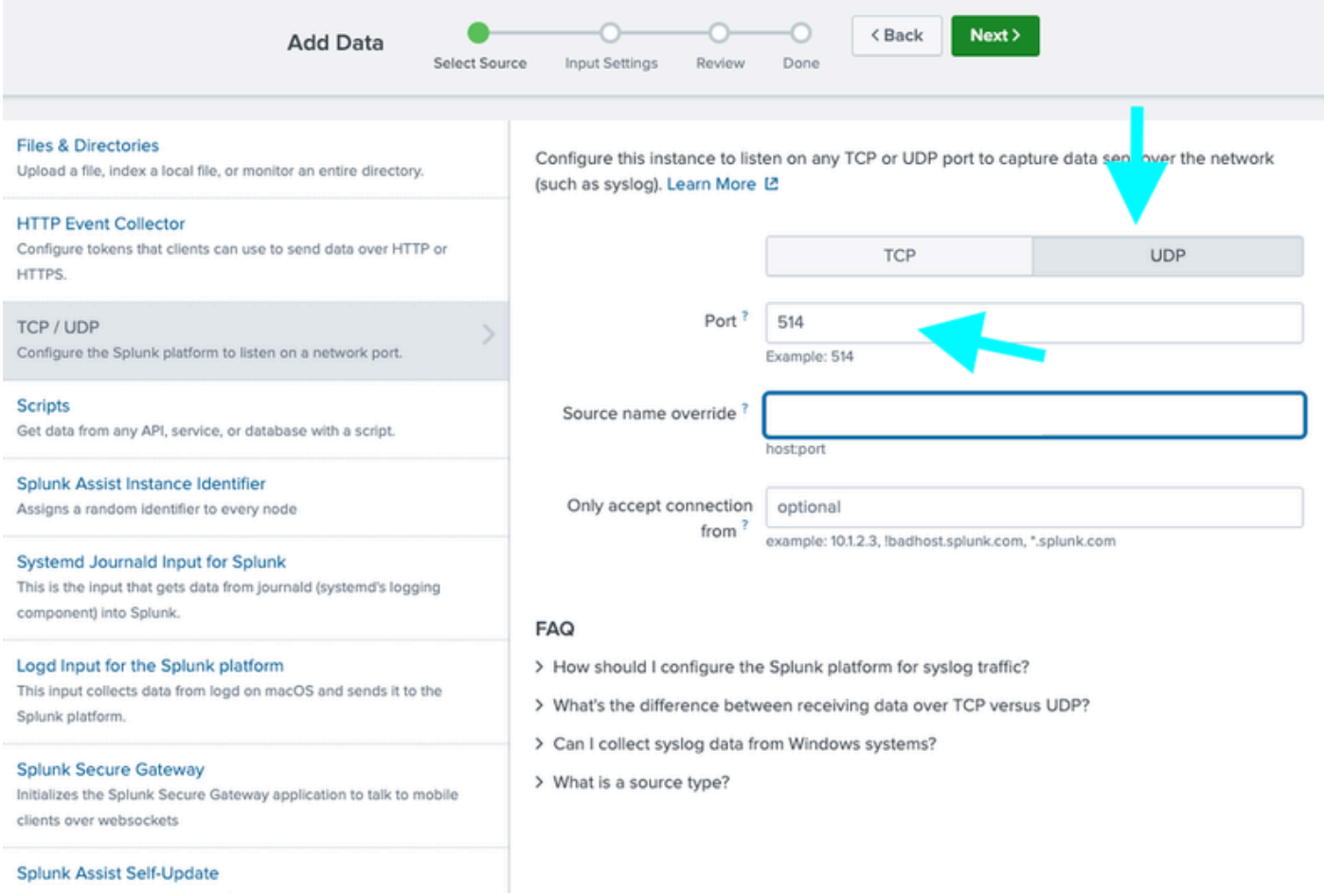


步驟 2:找到UDP行，然後選擇+Add new。



步驟 3:在新頁面上，選擇UDP，在Port欄位中輸入接收埠，例如514。
步驟 4:在Source name override欄位中，輸入 desired name of source.

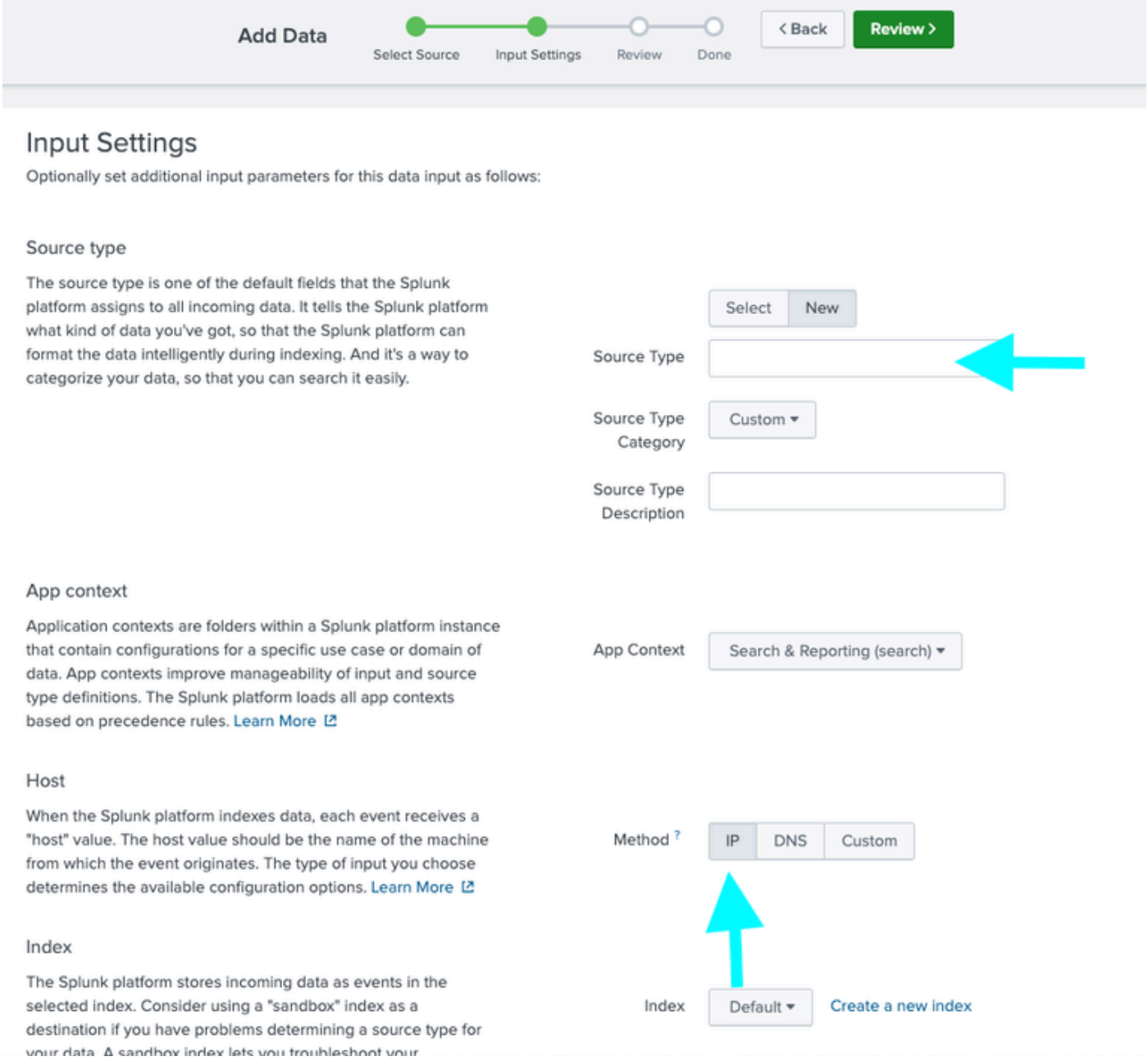
步驟 5:完成後，按一下視窗頂部的綠色「下一步」>按鈕。



步驟 6:在下一頁上，切換到New選項，找到Source Type欄位並輸入 desired source .

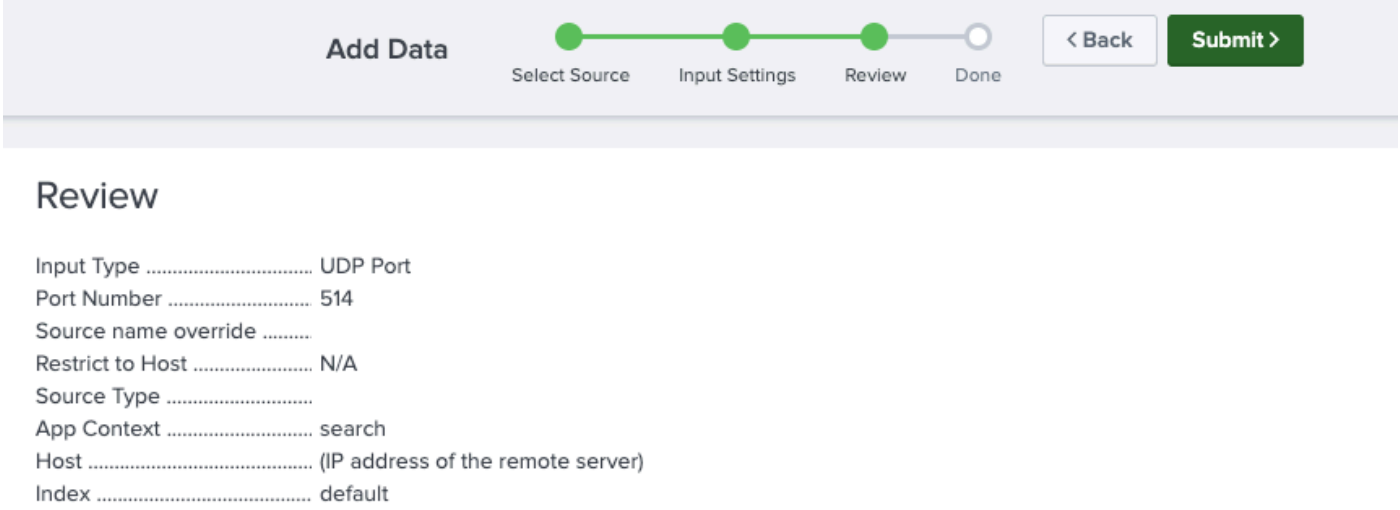
步驟 7:為Method選擇IP。

步驟 8:按一下螢幕頂部的綠色Review > 按鈕。

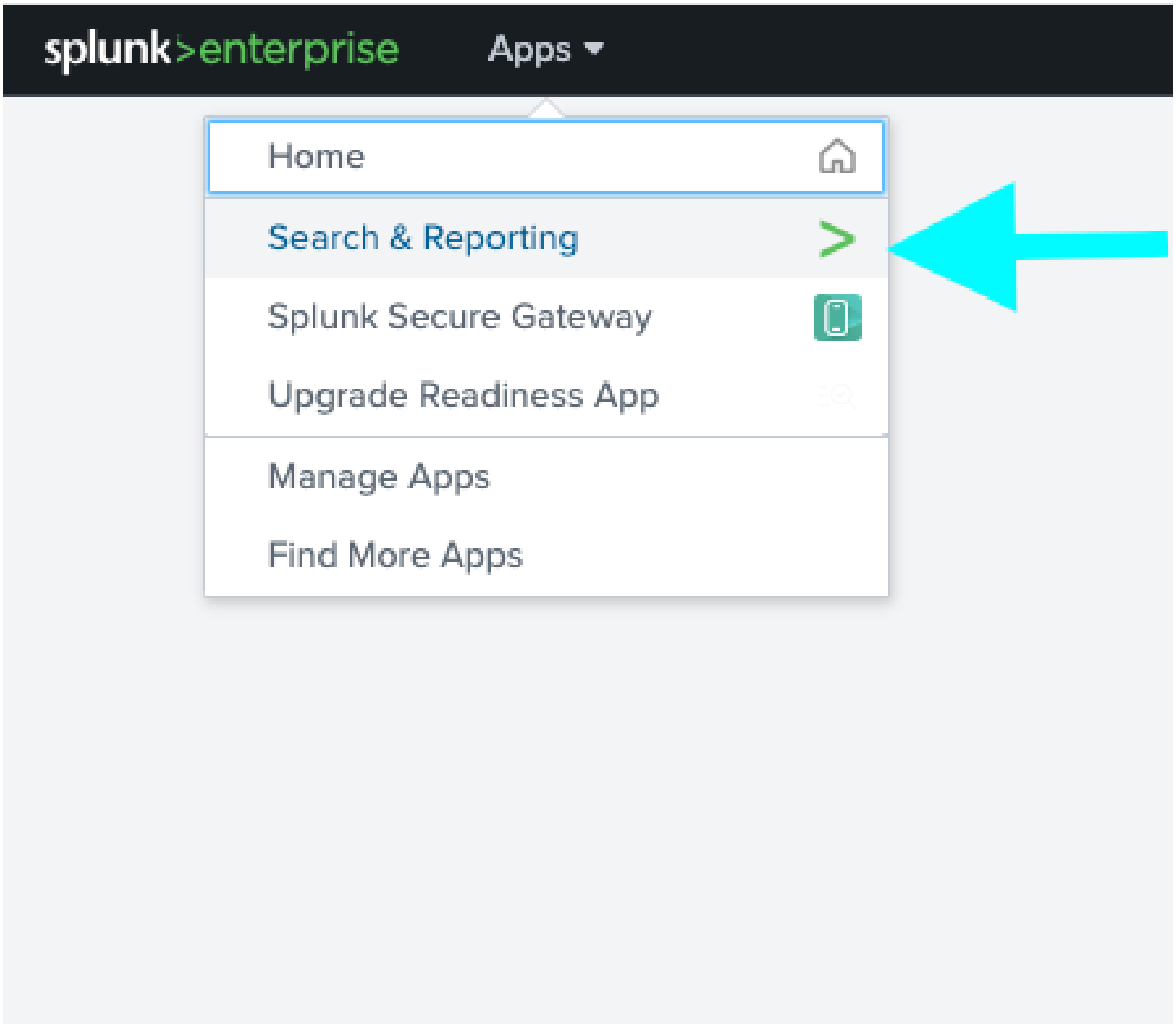


步驟 9:在下一個視窗中，檢視您的設定並根據需要進行編輯。

步驟 10:驗證後，按一下視窗頂部的Submit>綠色按鈕。

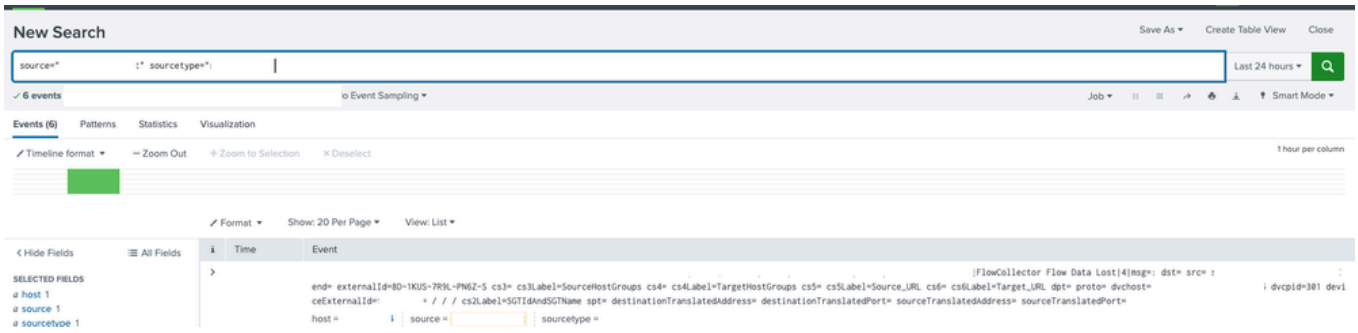


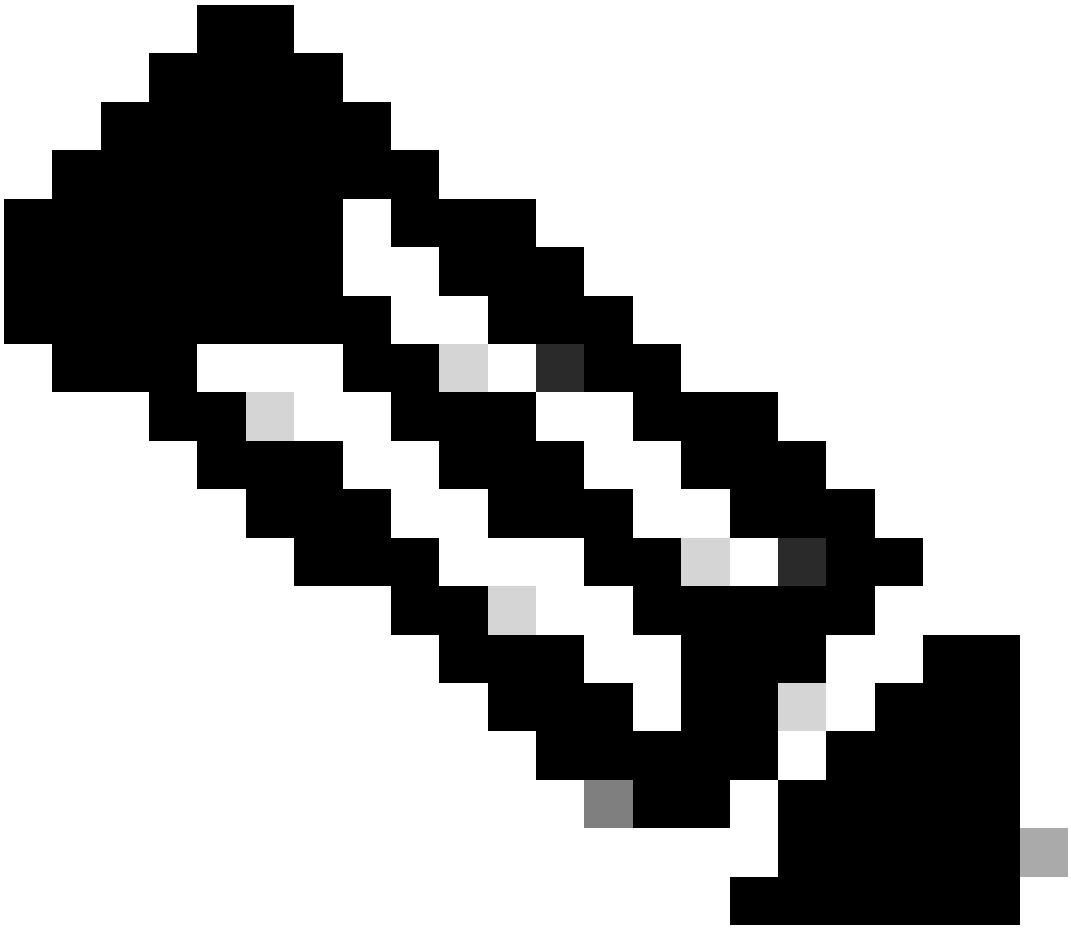
步驟 11:在Web UI中導航到Apps > Search & Reporting。



步驟 12:在「搜尋」頁面上，使用source="As_configured" sourcetype="As_configured"「過濾器」查詢已接收的日

誌。



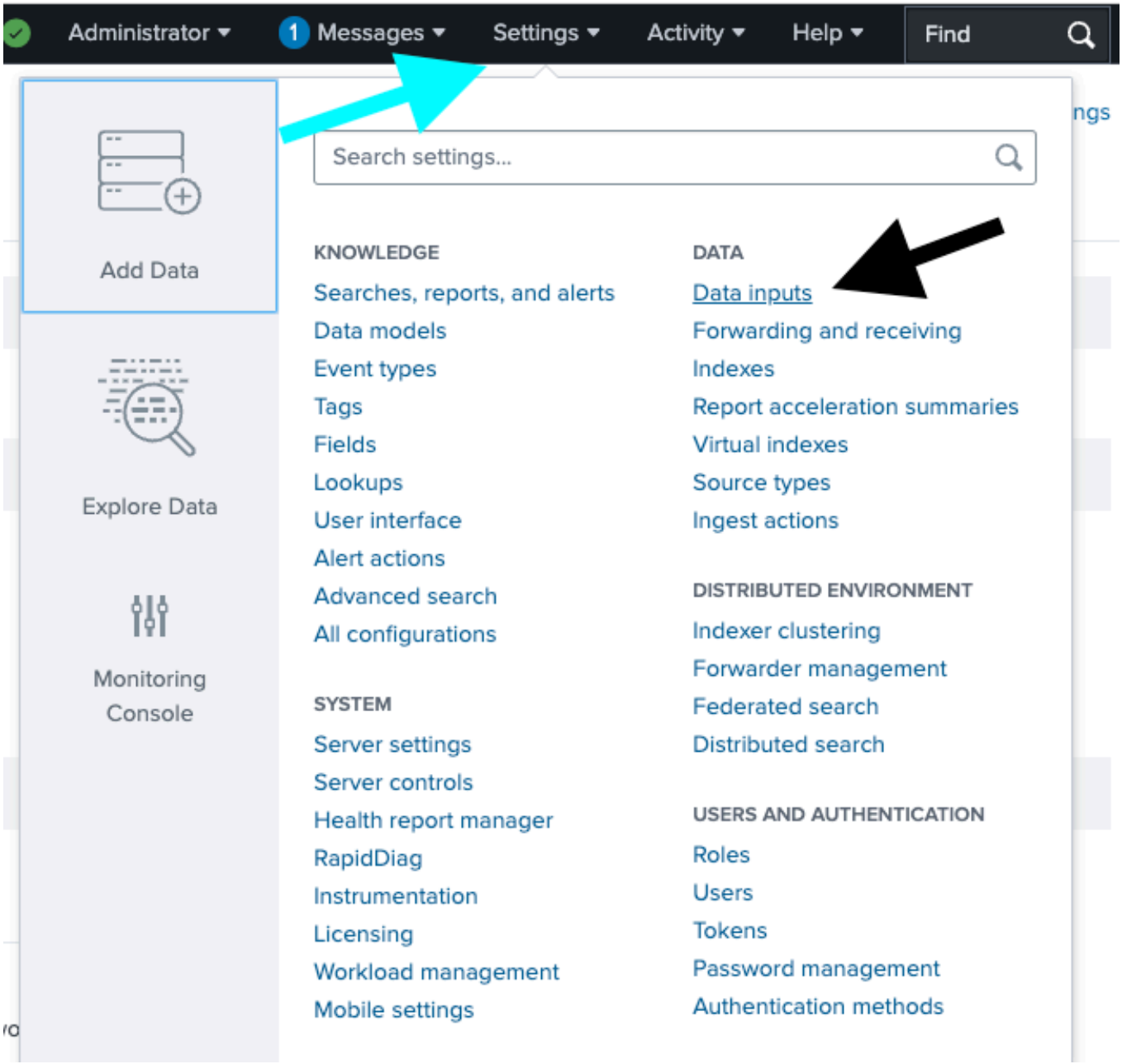


附註：有關源，請參閱步驟4
有關source_type的資訊，請參閱步驟6

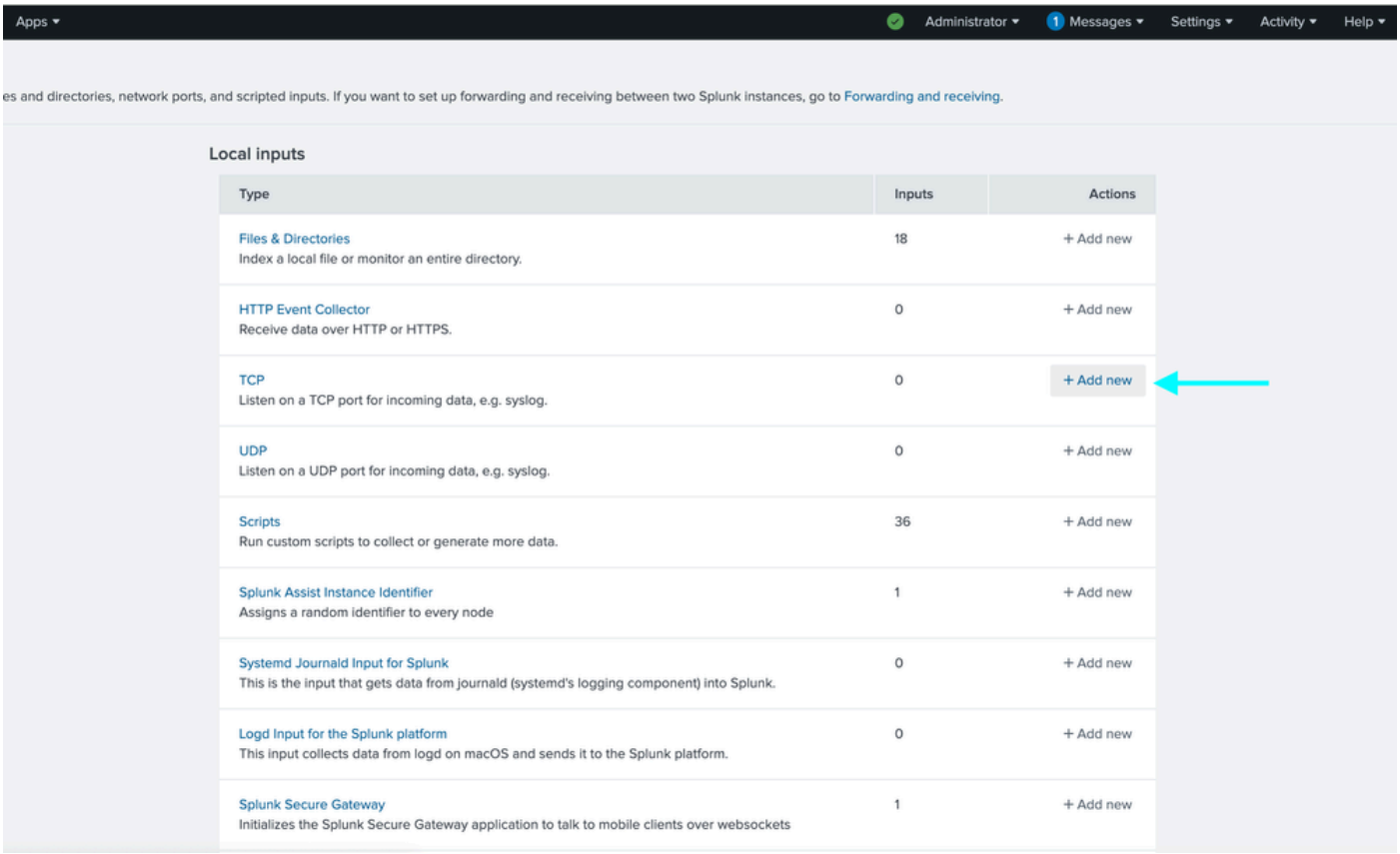
在SNA上通過TCP埠6514或自定義埠配置syslog

1.配置Splunk以通過TCP埠接收SNA稽核日誌

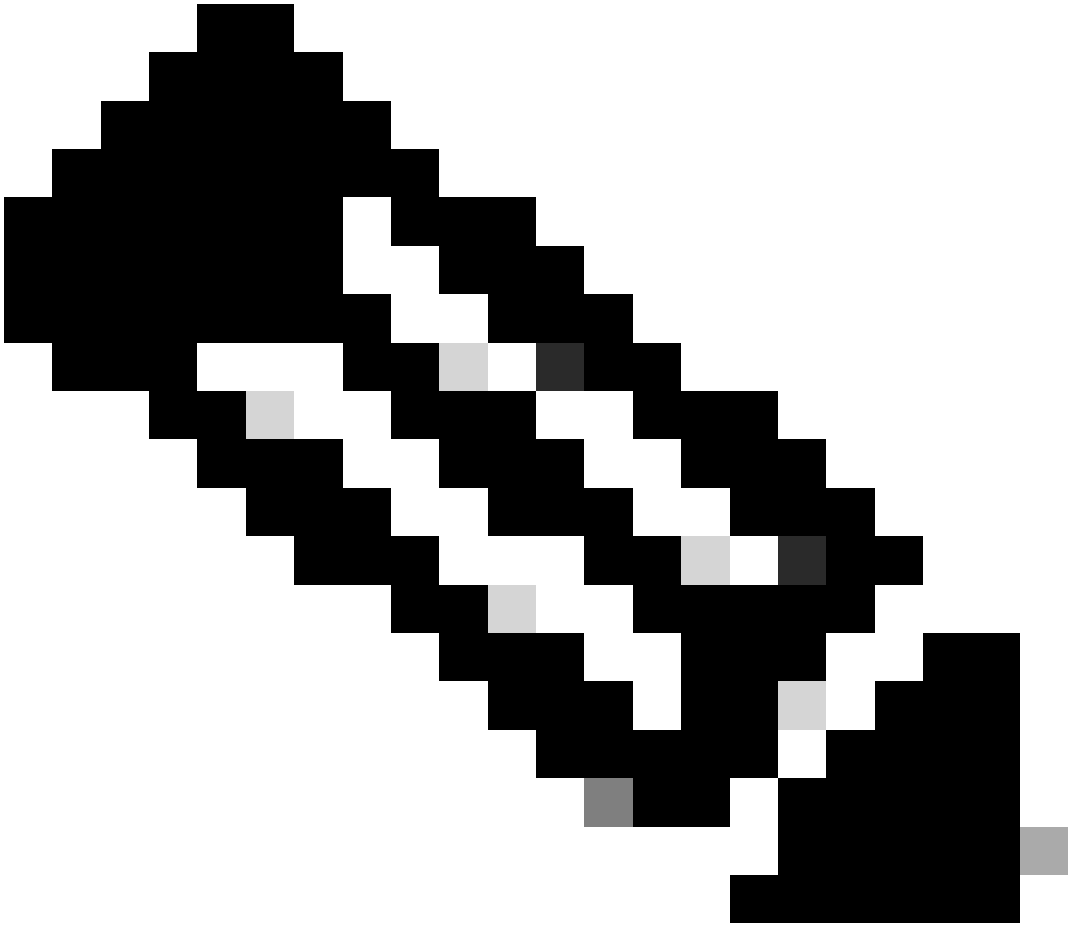
步驟 1:在Splunk UI中，導航到設定>新增資料>資料資料輸入。



步驟 2:找到TCP線路並選擇+ Add new。

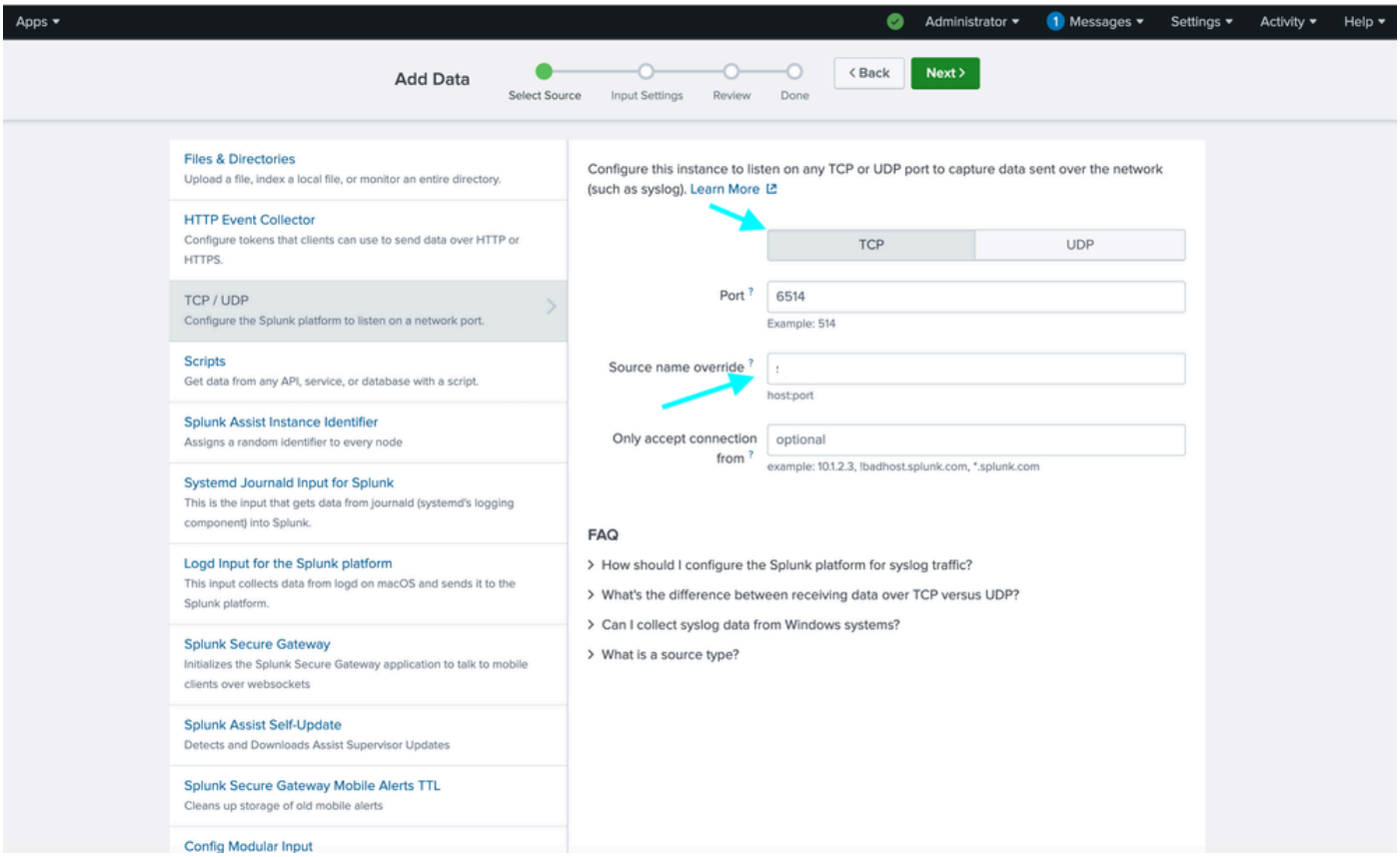


步驟 3:在新視窗中選擇TCP，在示例影象埠6514中輸入所需的接收埠，並在源名稱覆蓋欄位中輸入「所需名稱」。



附註：TCP 6514是通過TLS的系統日誌的預設埠

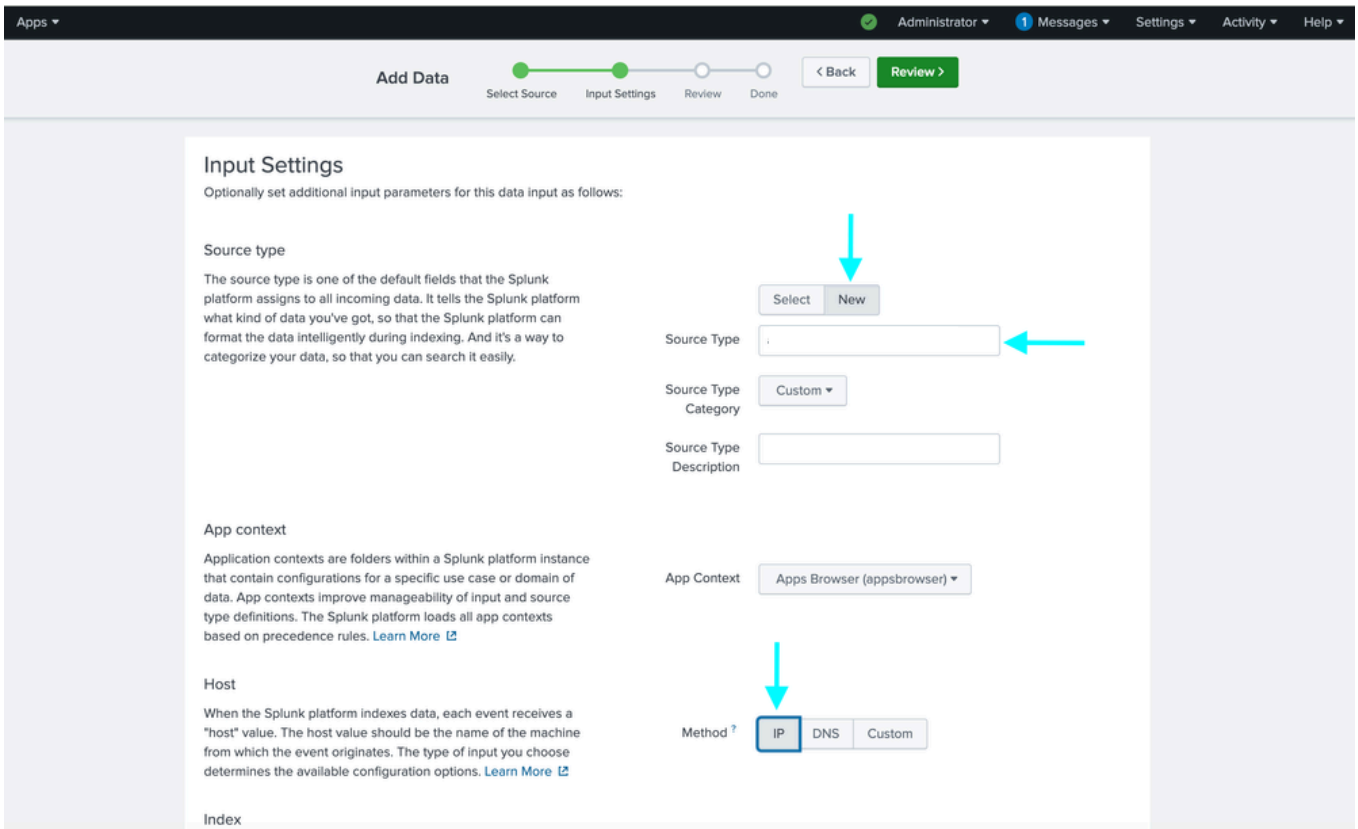
步驟 4:完成後，按一下視窗頂部的綠色「下一步」>按鈕。



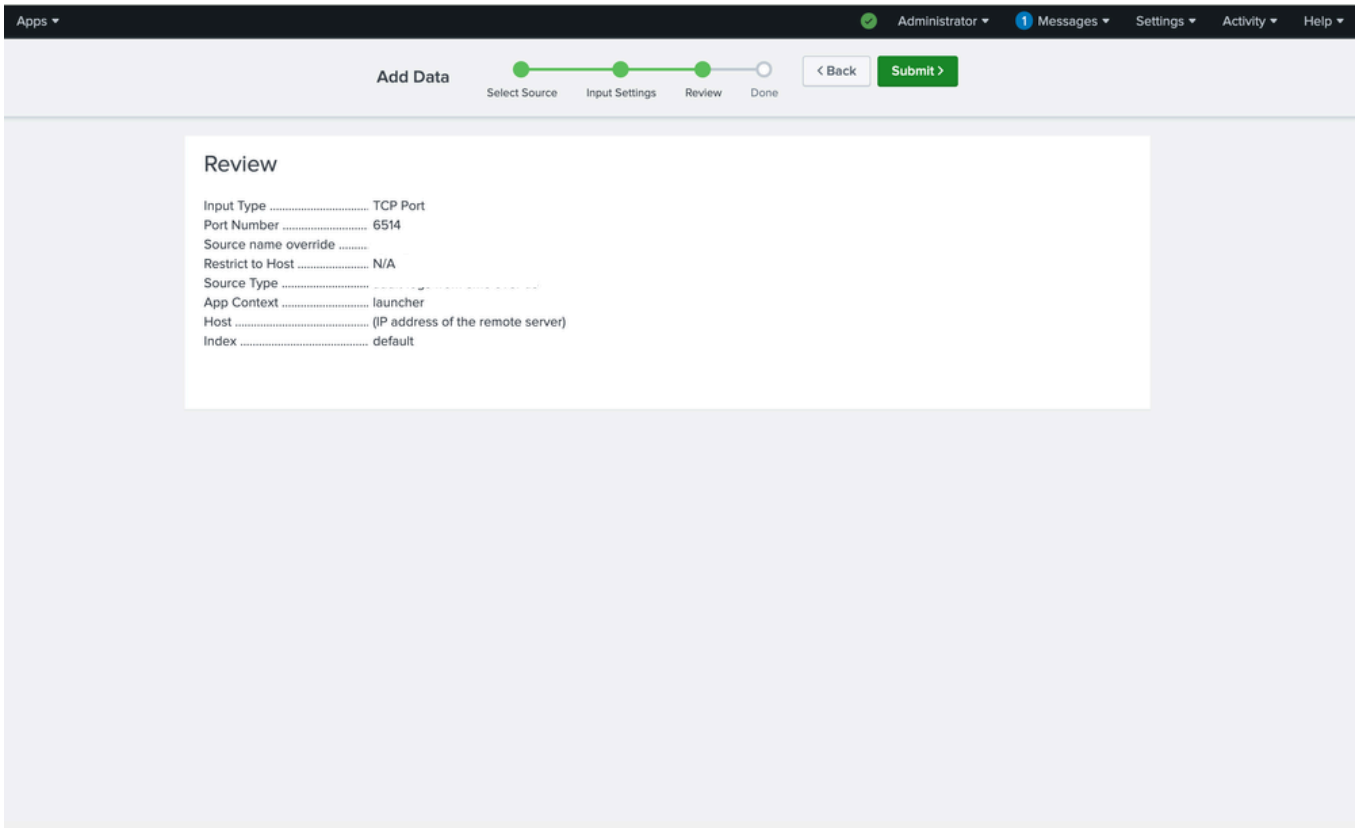
步驟 5:在新視窗的源型別部分中選擇新建，在源型別欄位中輸入所需的名稱。

步驟 6:在Host部分中選擇Method的IP。

步驟 7:完成後，選擇視窗頂部的綠色「審閱」>按鈕。



步驟 8:在下一個視窗中，檢視您的設定並根據需要進行編輯。驗證後，按一下視窗頂部的Submit>綠色按鈕。



2.生成Splunk的證書

步驟 1:使用安裝了openssl的電腦，運行sudo openssl req -x509 -newkey rsa:4096 -keyout server_key.pem -out server_cert.pem -sha256 -days 3650 -subj /CN=10.106.127.4命令，將示例IP 10.106.127.4替換為Splunk裝置的IP。系統將兩次提示您輸入使用者定義的密碼短語。在示例中，這些命令是從Splunk電腦的命令列運行的。

```
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:
```

命令完成後，將生成兩個檔案。server_cert.pem和server_key.pem檔案。

```
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:
```

步驟 2:切換到根使用者。

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

步驟 3:將新生成的證書複製到/opt/splunk/etc/auth/。

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

第4步：使用私鑰附加spunkweb.cet檔案。

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

第5步：更改splunk證書的所有權。

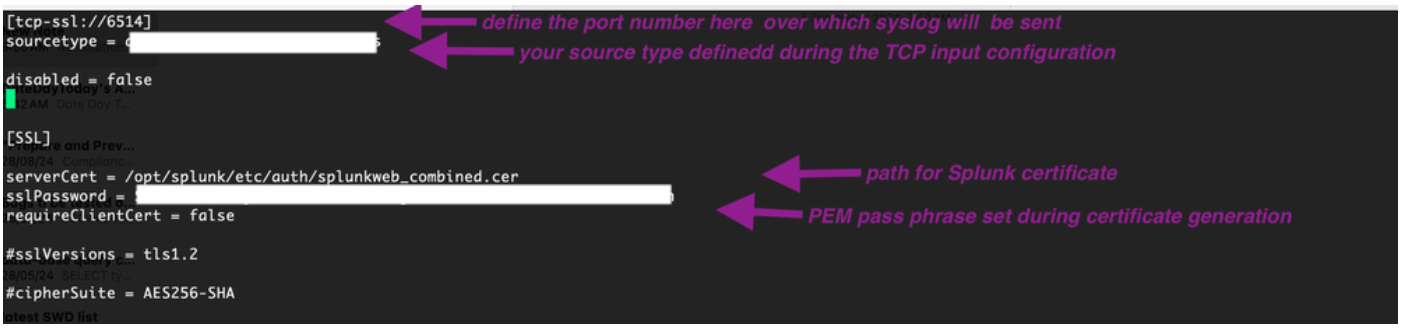
```
user@examplehost:~# chown 10777:10777/opt/splunk/etc/auth/splunkweb.cer
```

第6步：更改splunk證書的許可權。

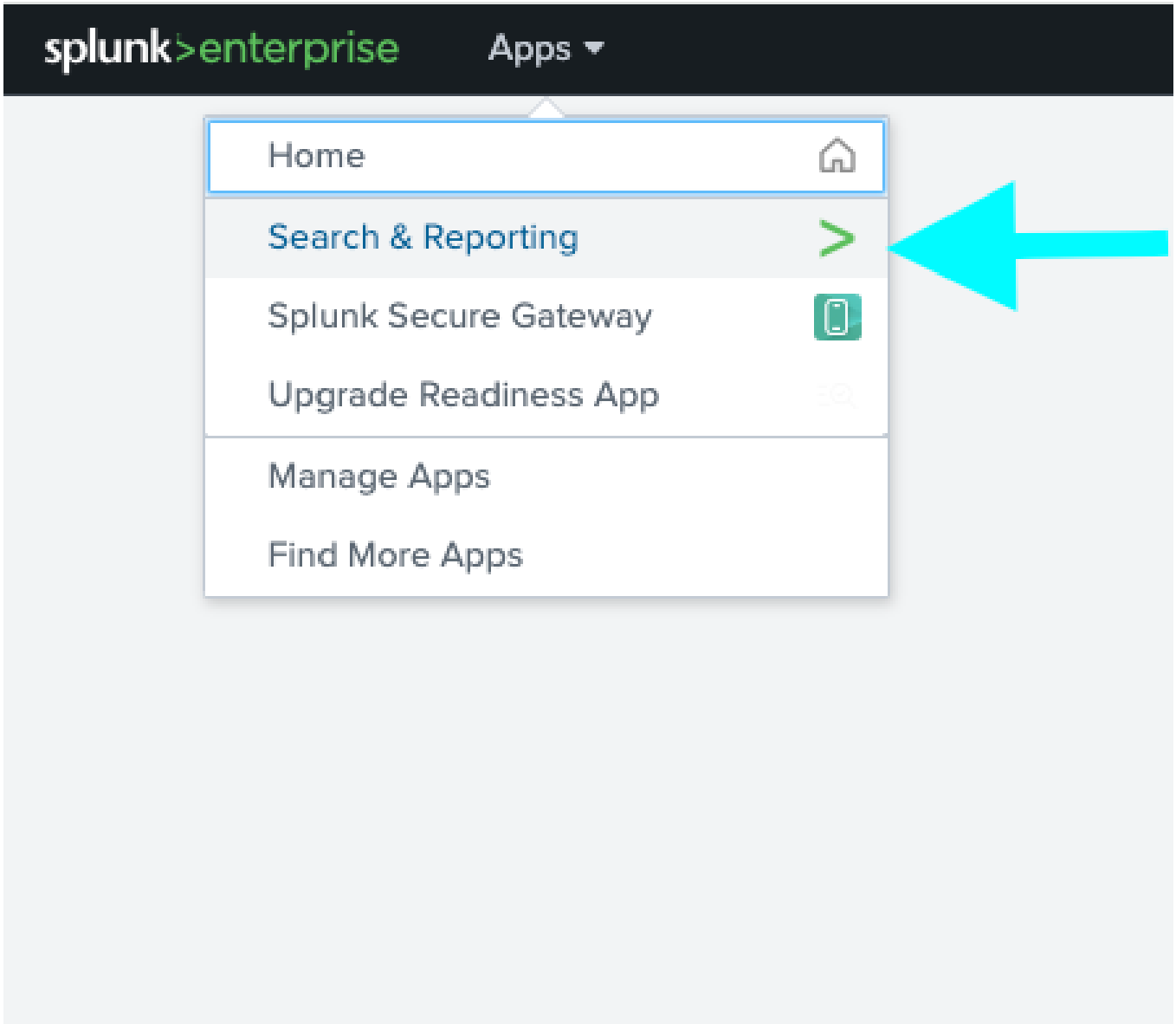
```
user@examplehost:~# chmod 600/opt/splunk/etc/auth/splunkweb.cer
```

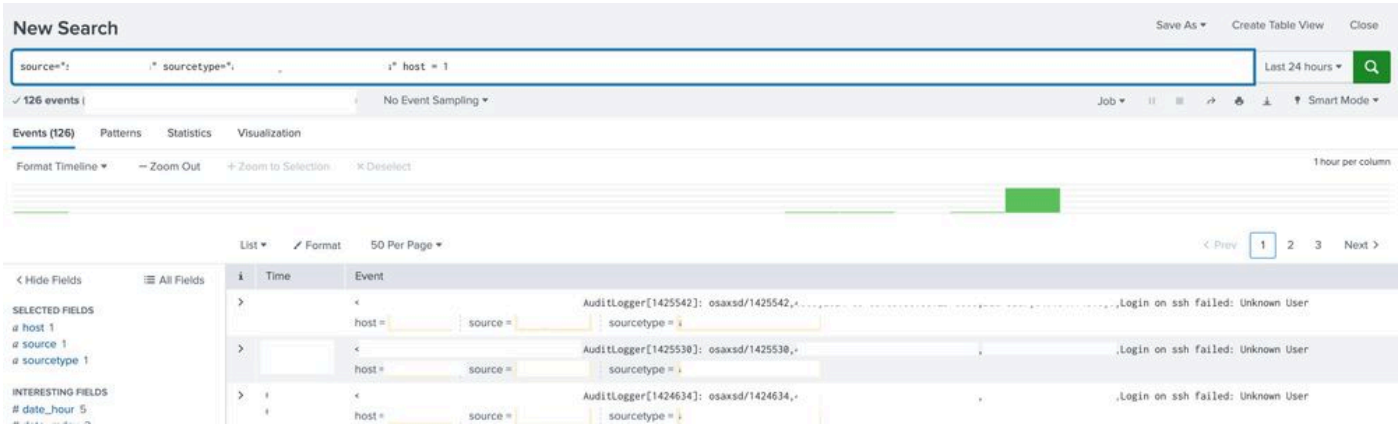
第7步：建立新的input.conf檔案。

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



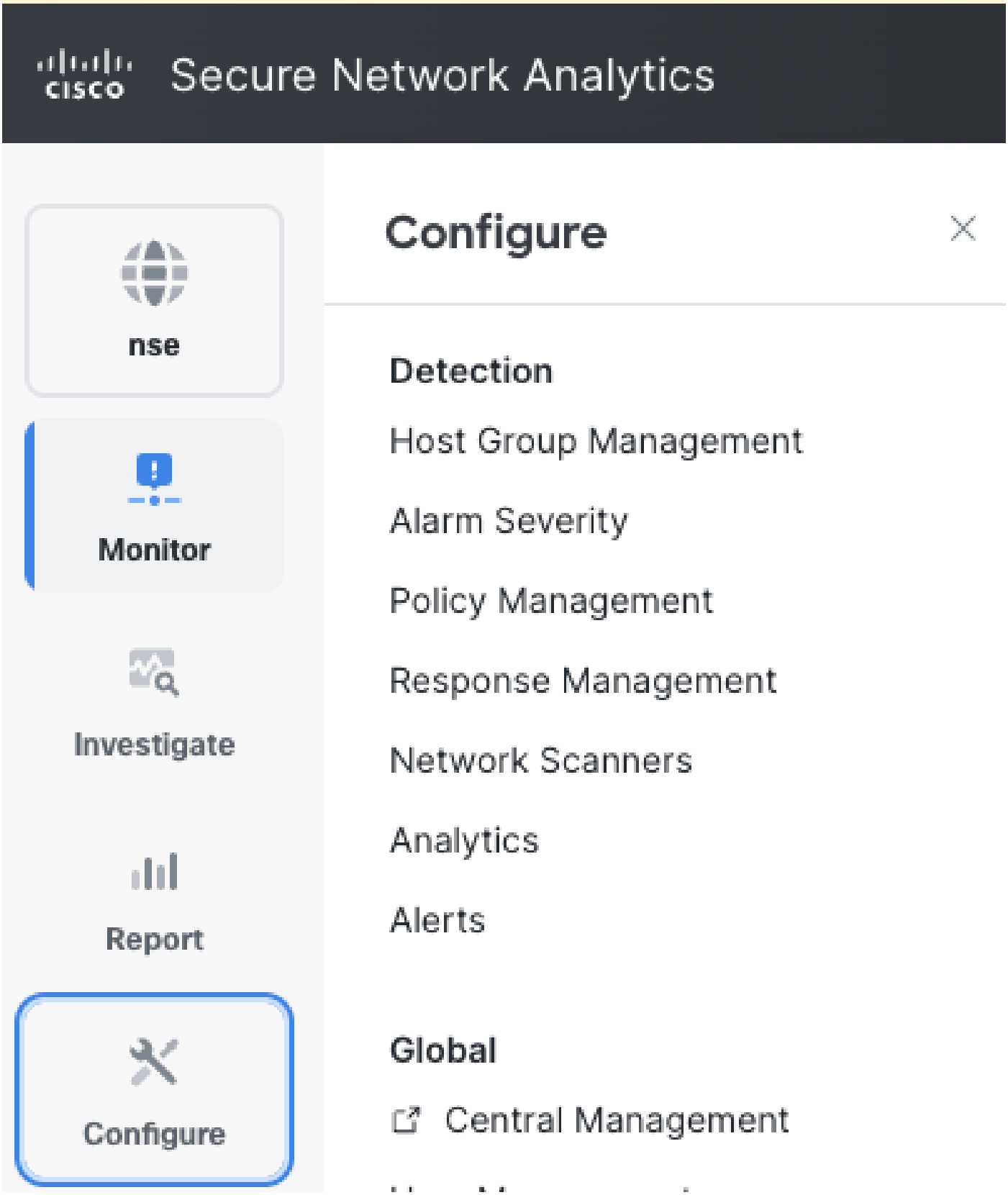
步驟 8:使用搜尋驗證系統日誌。



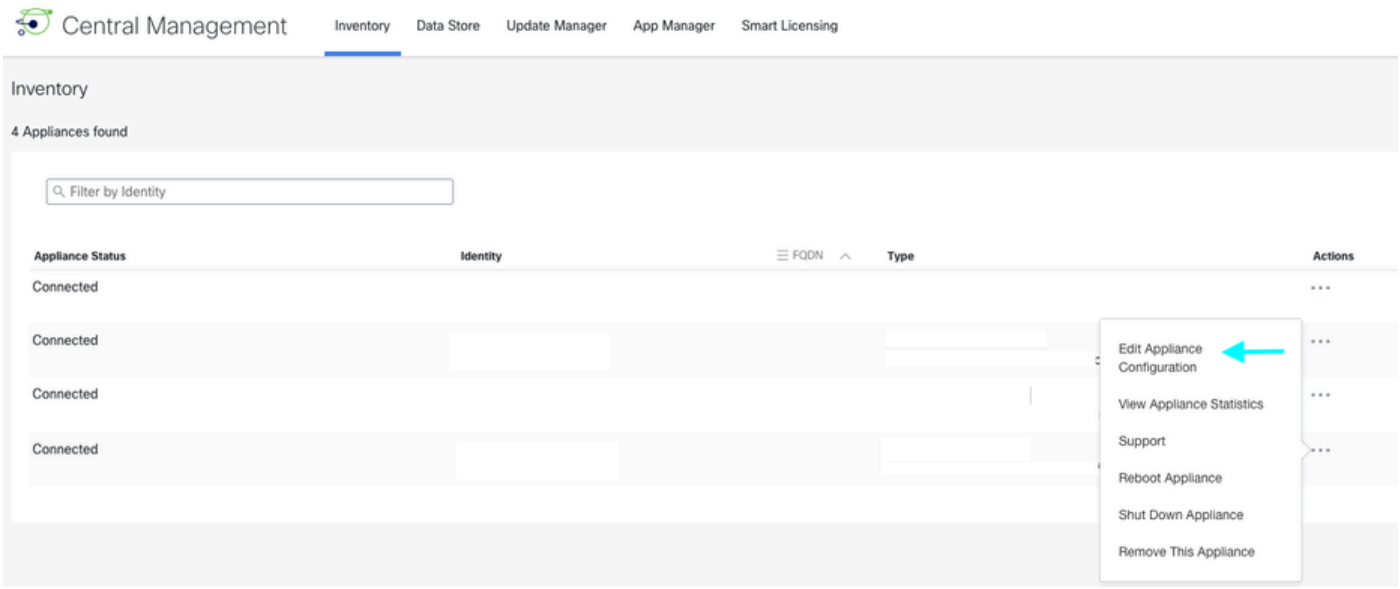


3.在SNA上配置審計日誌目標

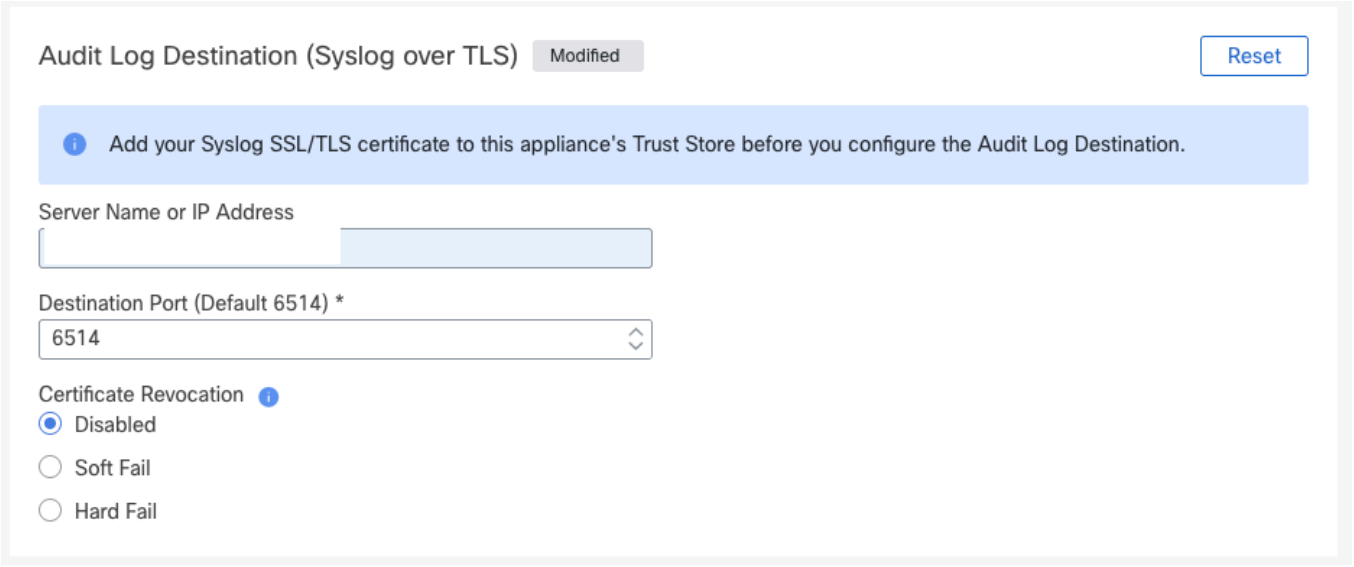
步驟 1:登入到SMC UI，導航至Configure > Central Management。



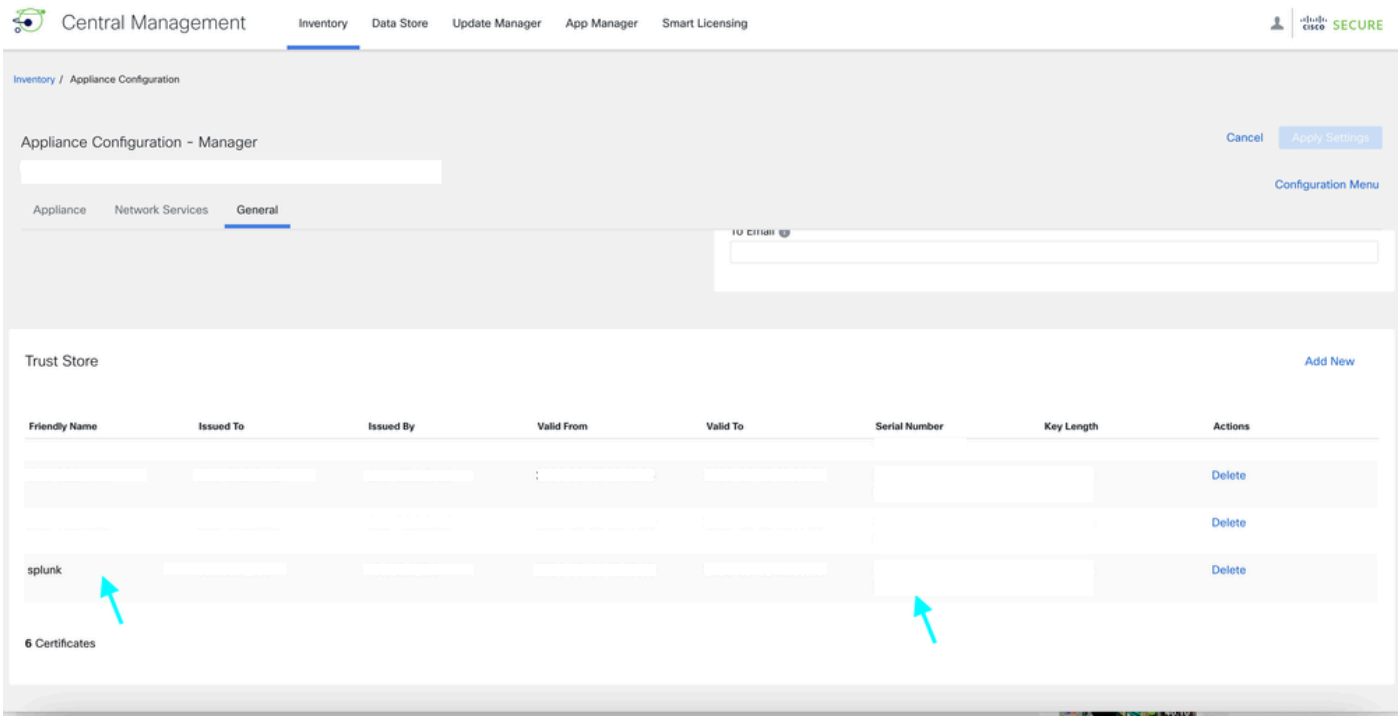
步驟 2:按一下所需SNA裝置的省略號圖示，選擇編輯裝置配置。



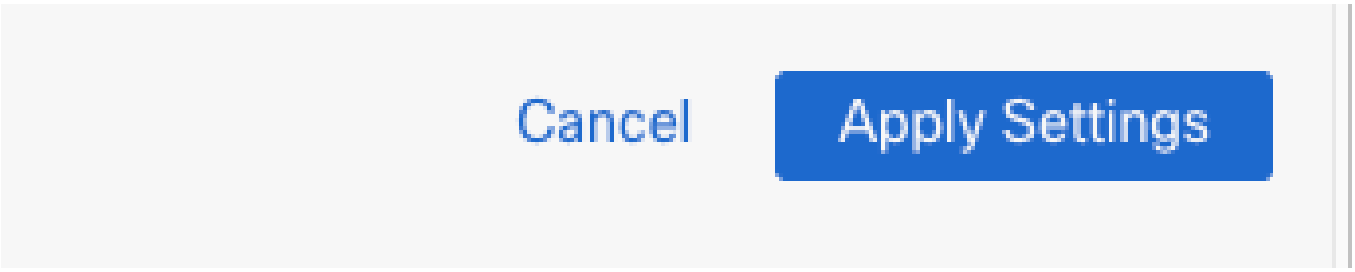
步驟 3:導航到Network Services頁籤，然後輸入Audit Log Destination(Syslog over TLS)詳細資訊。



步驟 4:導航到General頁籤，向下滾動到底部按一下Add new以上傳之前建立的Splunk證書，該證書名為server_cert.pem。

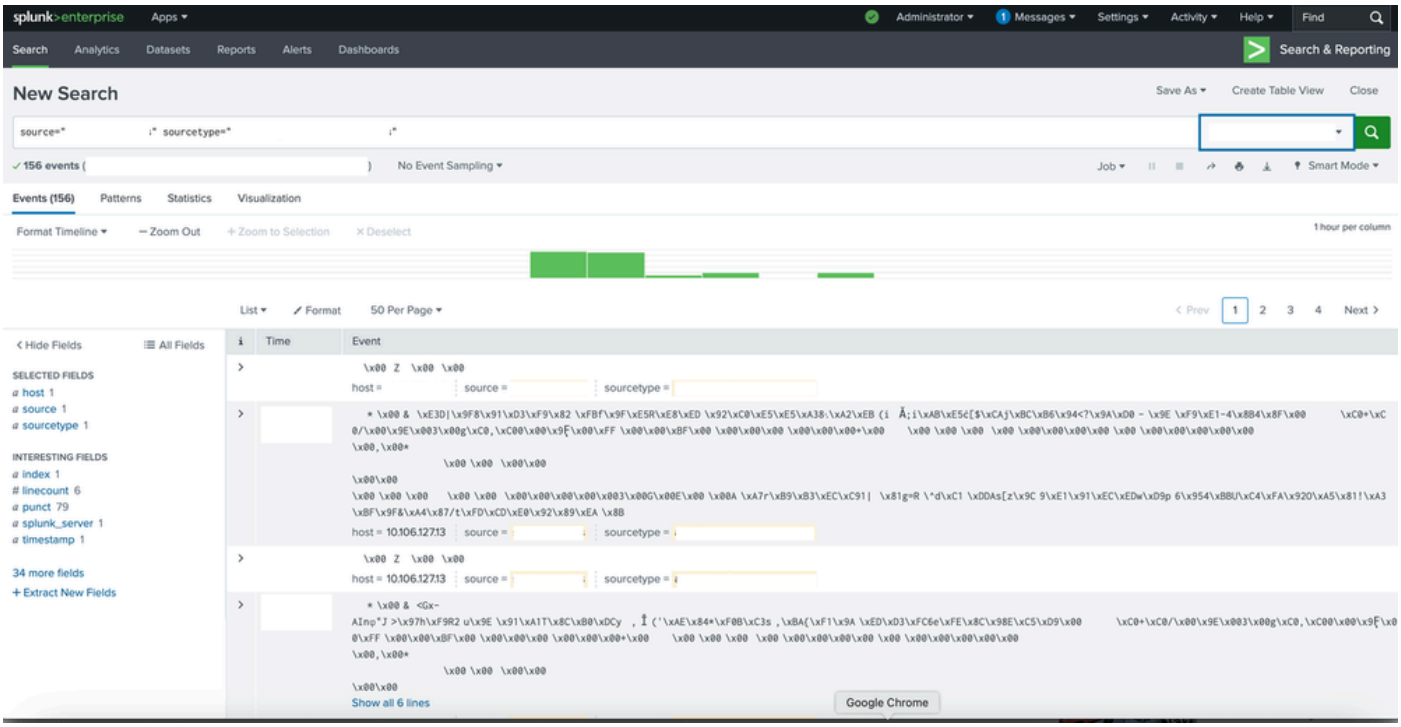


步驟 5:按一下「Apply settings」。



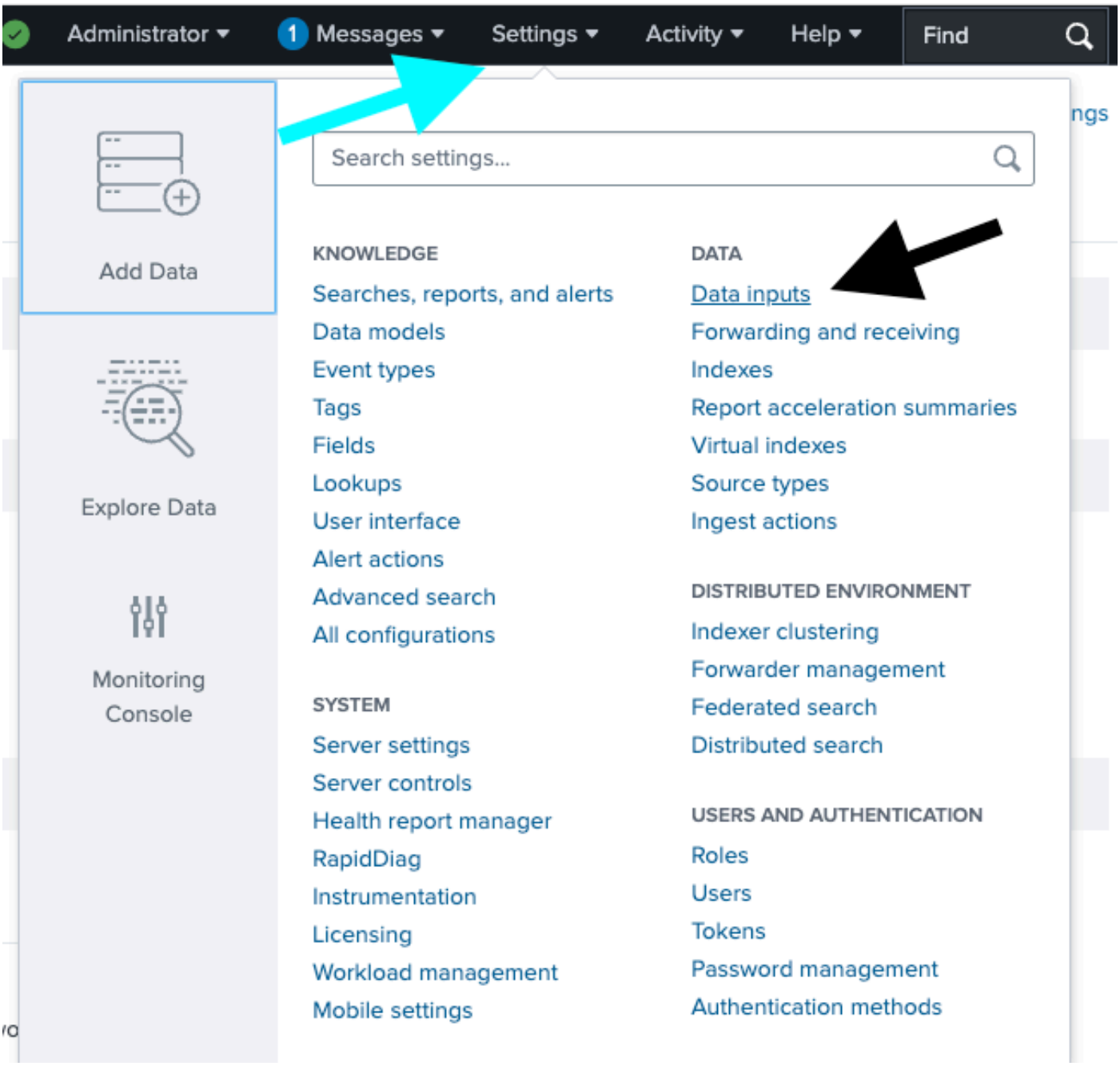
疑難排解

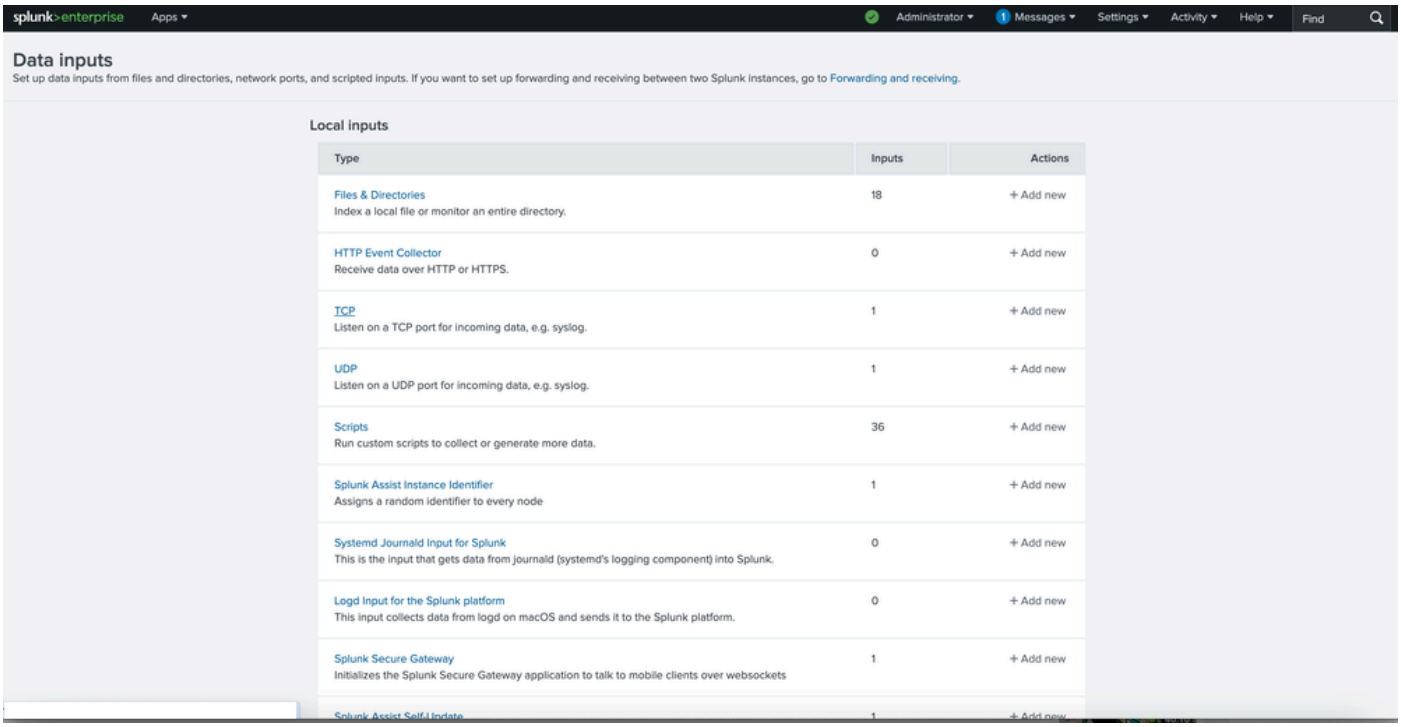
搜尋中可能會出現完全胡說八道的內容。

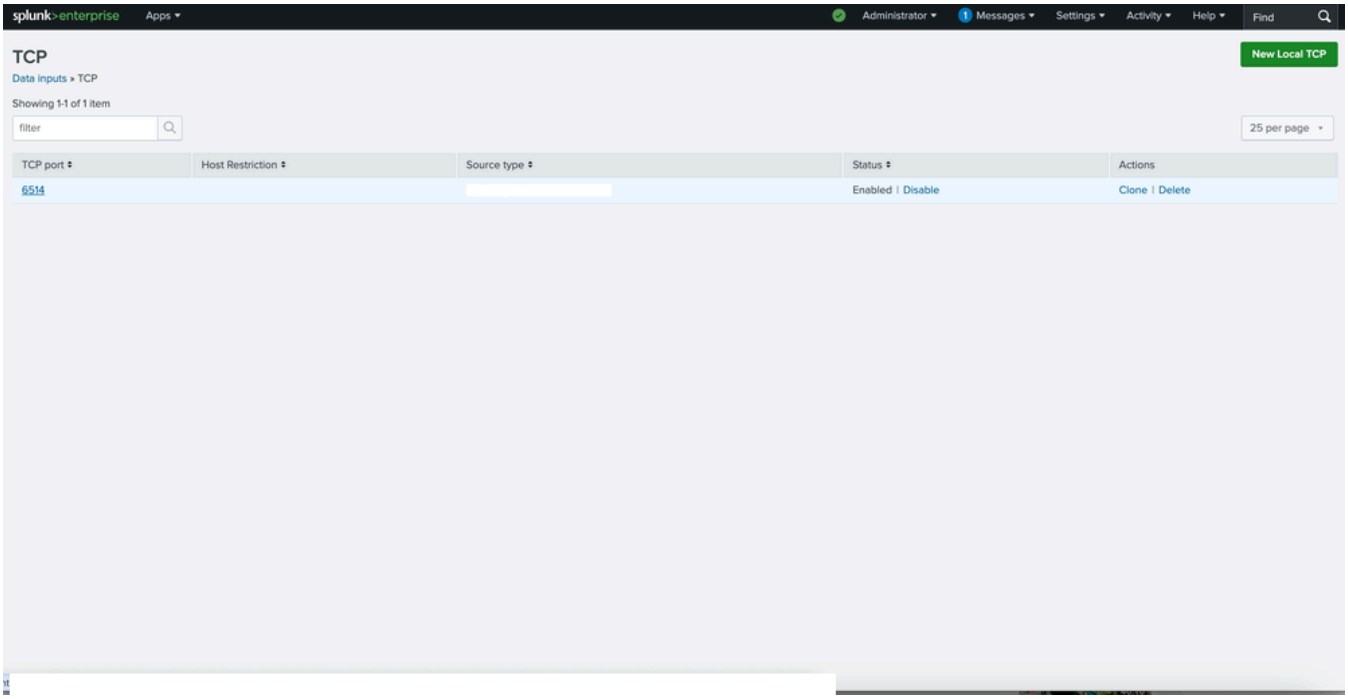


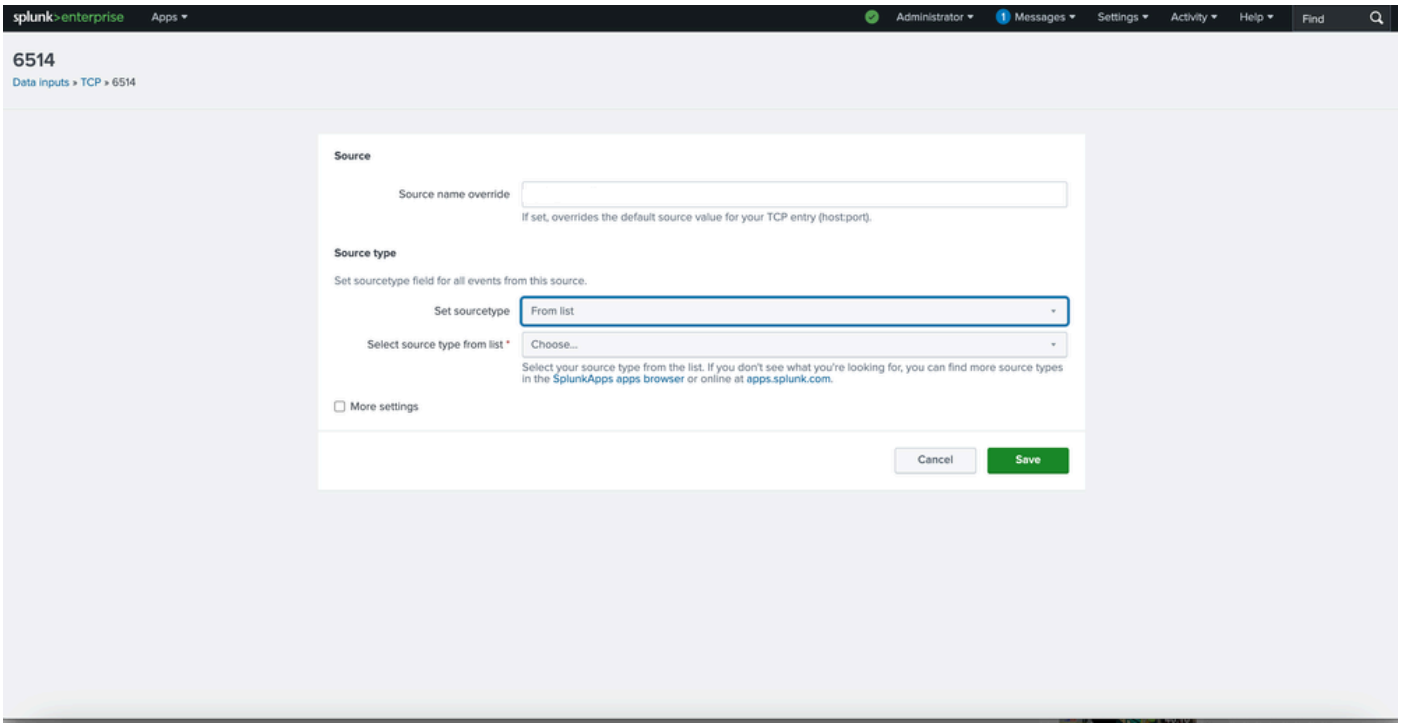
解決方案：

將輸入對映到其正確的源型別。


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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。