

# 配置響應管理以將系統日誌事件傳送到Splunk

## 目錄

---

### [簡介](#)

### [必要條件](#)

#### [需求](#)

#### [採用元件](#)

### [在通過UDP 514或自定義埠的SNA上配置syslog](#)

#### [1.SNA回應管理](#)

#### [2.配置Splunk以通過UDP埠接收SNA系統日誌](#)

### [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](#)

#### [2.生成Splunk的證書](#)

#### [3.在SNA上配置審計日誌目標](#)

### [疑難排解](#)

---

## 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：

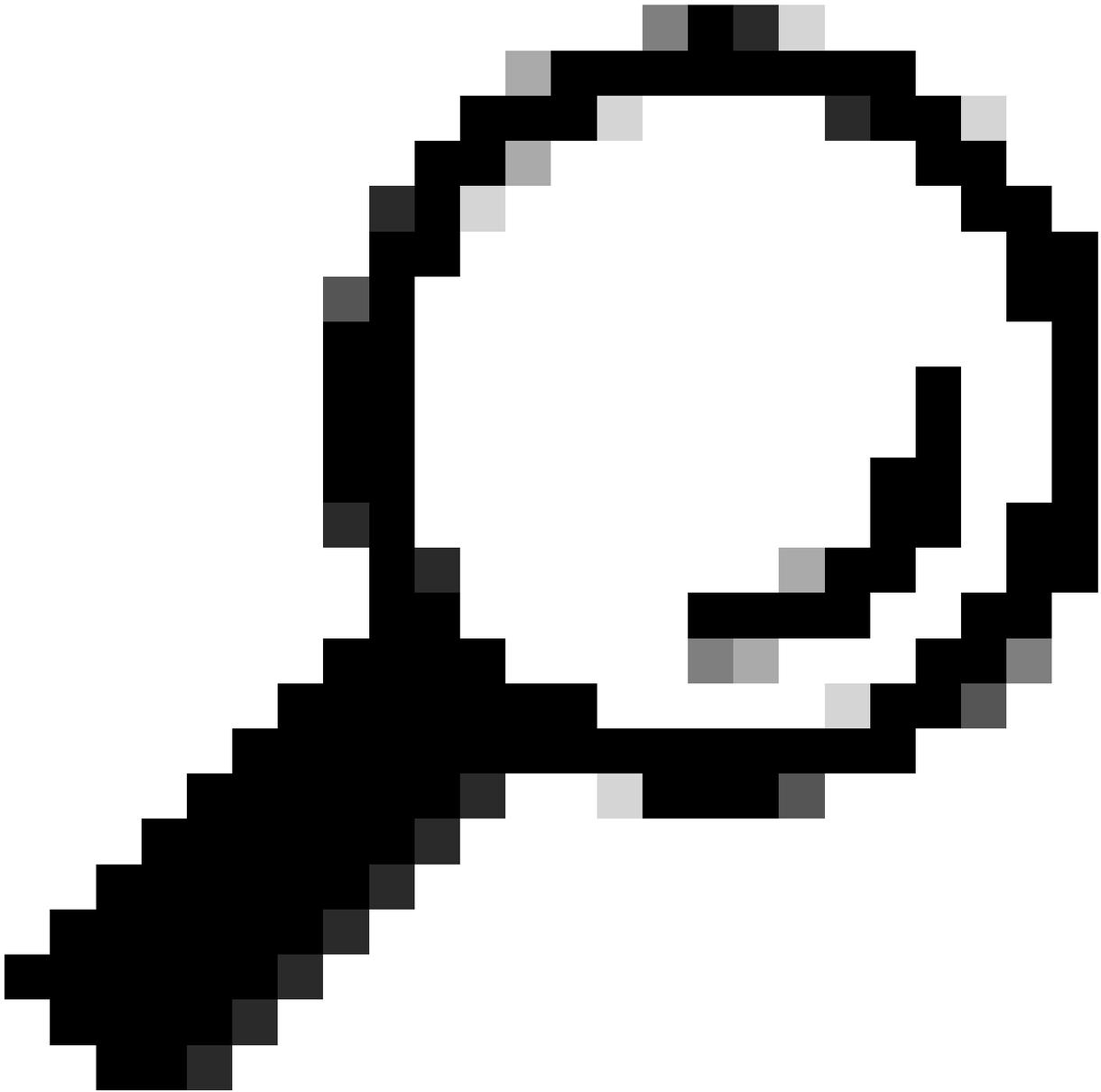
- [安全網路分析回應管理](#)。
- [Splunk系統日誌](#)

### 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。



beta3



Monitor



Investigate



Report



Configure

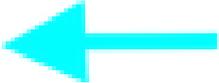
## Configure

### Detection

Host Group Management

Alarm Severity

Policy Management

Response Management 

Network Scanners

Analytics

Alerts

### Global

 Central Management

User 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列表中的省略號(...)，然後Edit。

Response Management

Rules Actions Syslog Formats

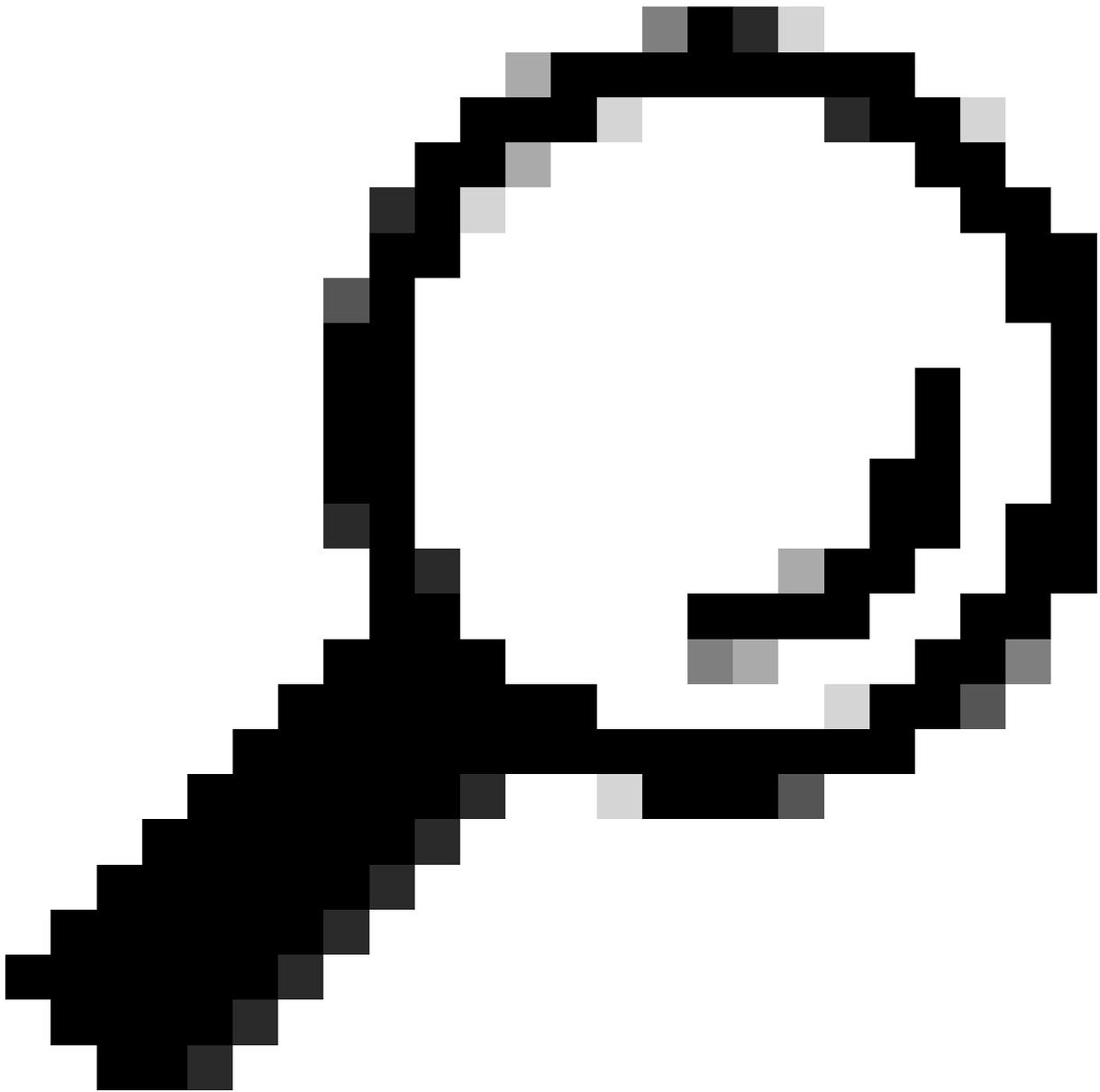
### Actions

[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"/>	<a href="#">Edit</a> <a href="#">Duplicate</a> <a href="#">Delete</a>

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

---

## 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

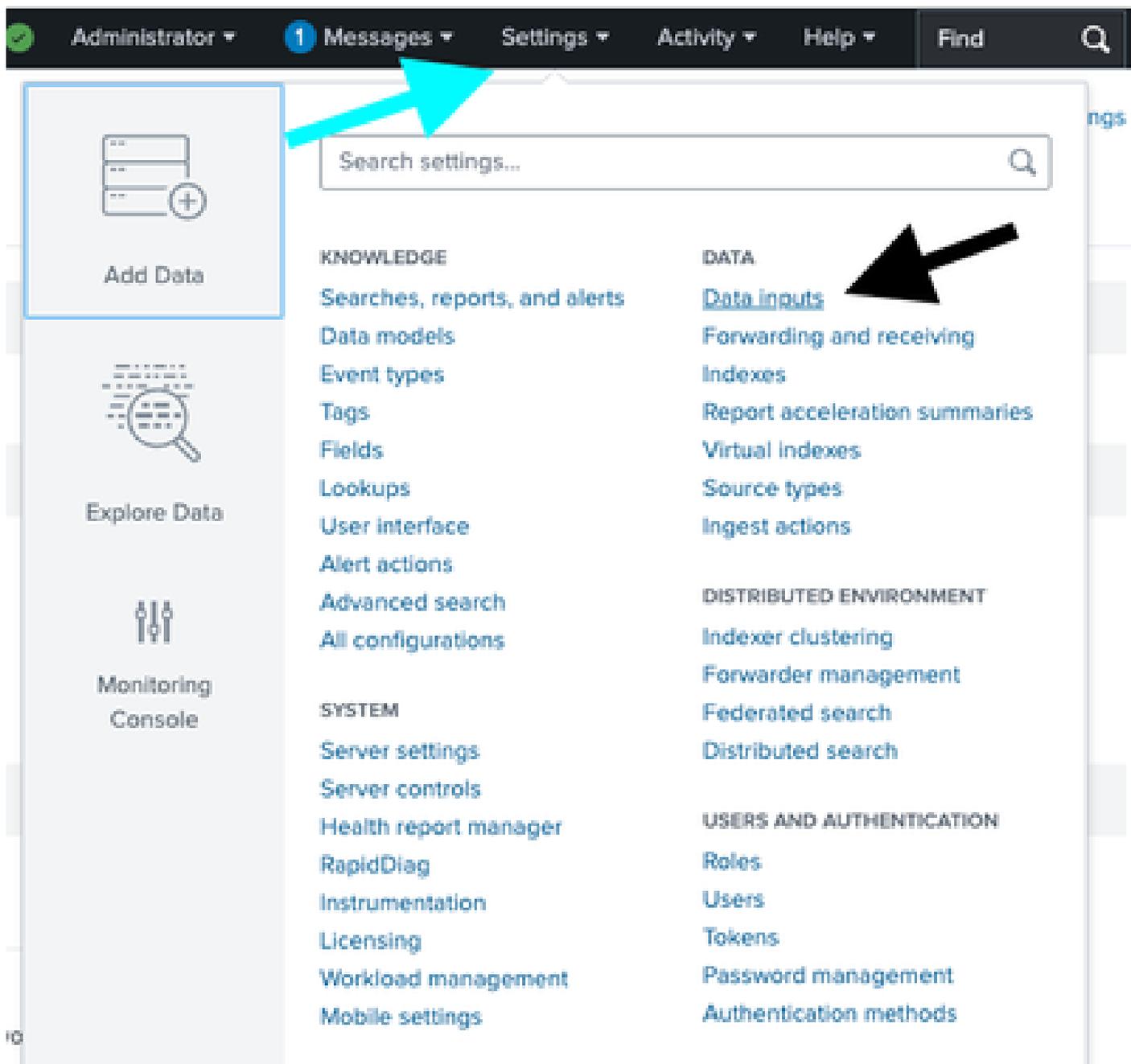
<131>Jan 01 00:00:00 test.host TestApp[1337]: CEF:0|Cisco|7.3.0|Notification:99|Bad Host|5|msg=This host has been observed performing malicious actions toward another host.:Source Host is http (80

Test Action

## 2. 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。

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

### Local Inputs

Type	Inputs	Actions
<b>Files &amp; Directories</b> Index a local file or monitor an entire directory.	18	+ Add new
<b>HTTP Event Collector</b> Receive data over HTTP or HTTPS.	0	+ Add new
<b>TCP</b> Listen on a TCP port for incoming data, e.g. syslog.	1	+ Add new
<b>UDP</b> Listen on a UDP port for incoming data, e.g. syslog.	1	+ Add new
<b>Scripts</b> Run custom scripts to collect or generate more data.	36	+ Add new
<b>Splunk Assist Instance Identifier</b> Assigns a random identifier to every node	1	+ Add new
<b>Systemd Journald input for Splunk</b> This is the input that gets data from journald (systemd's logging component) into Splunk.	0	+ Add new
<b>Logd input for the Splunk platform</b> This input collects data from logd on macOS and sends it to the Splunk platform.	0	+ 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。

**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?

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。

## 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](#)

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。

## Add Data



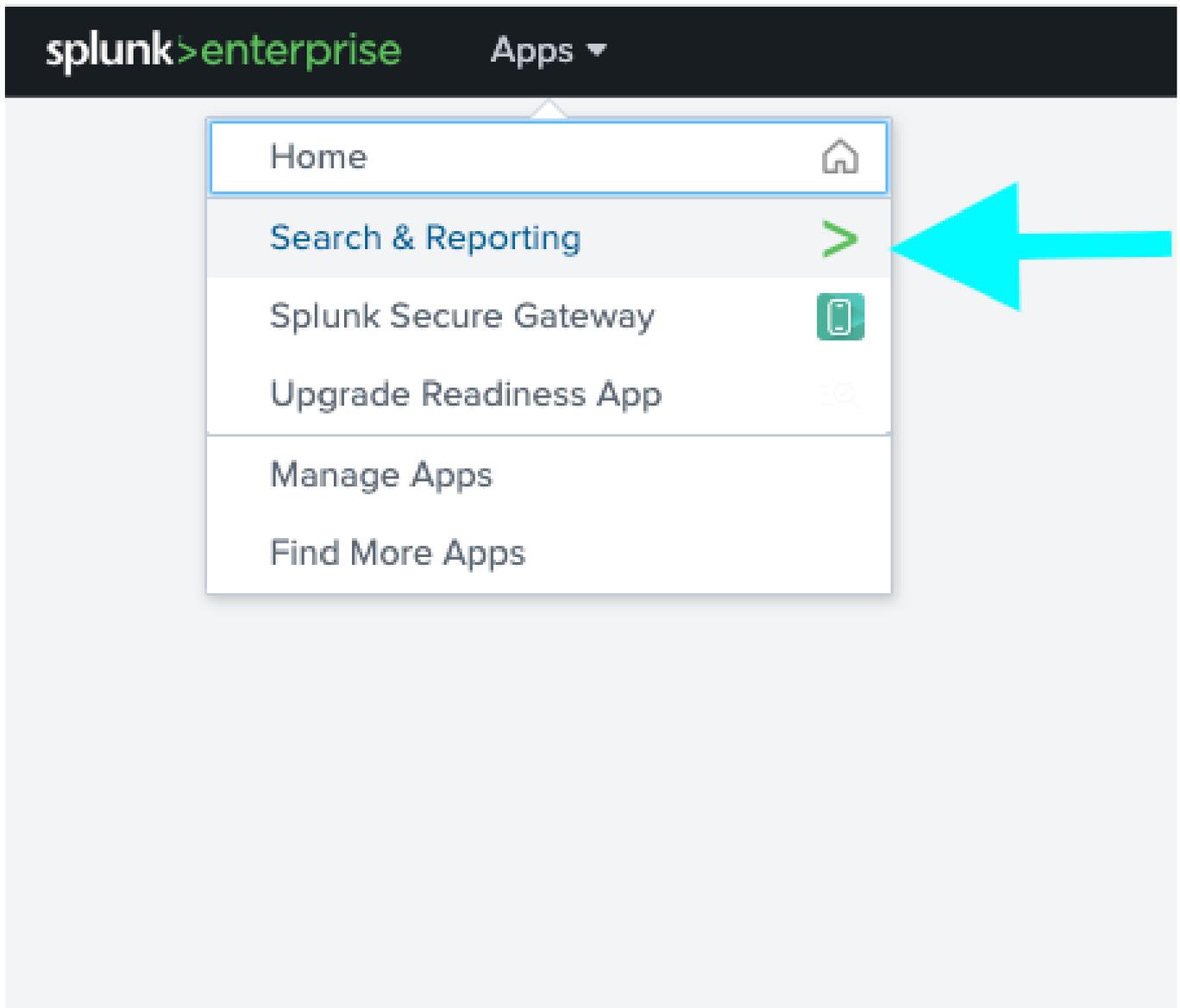
< Back

Submit >

## Review

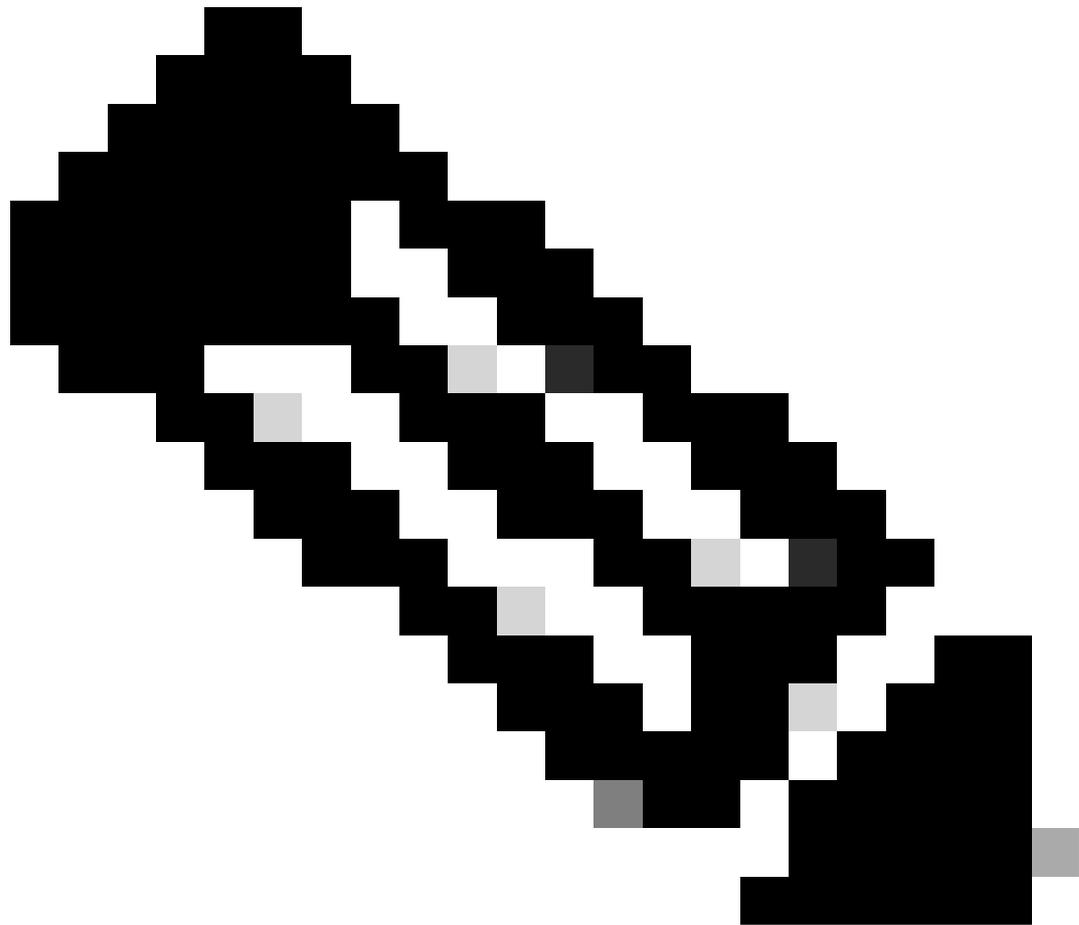
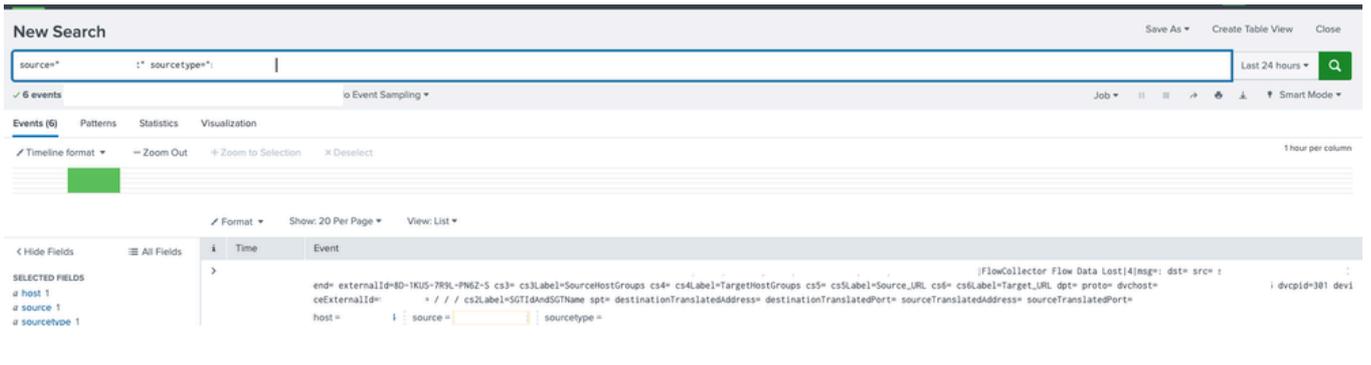
Input Type ..... UDP Port  
Port Number ..... 514  
Source name override .....  
Restrict to Host ..... N/A  
Source Type .....  
App Context ..... search  
Host ..... (IP address of the remote server)  
Index ..... default

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。

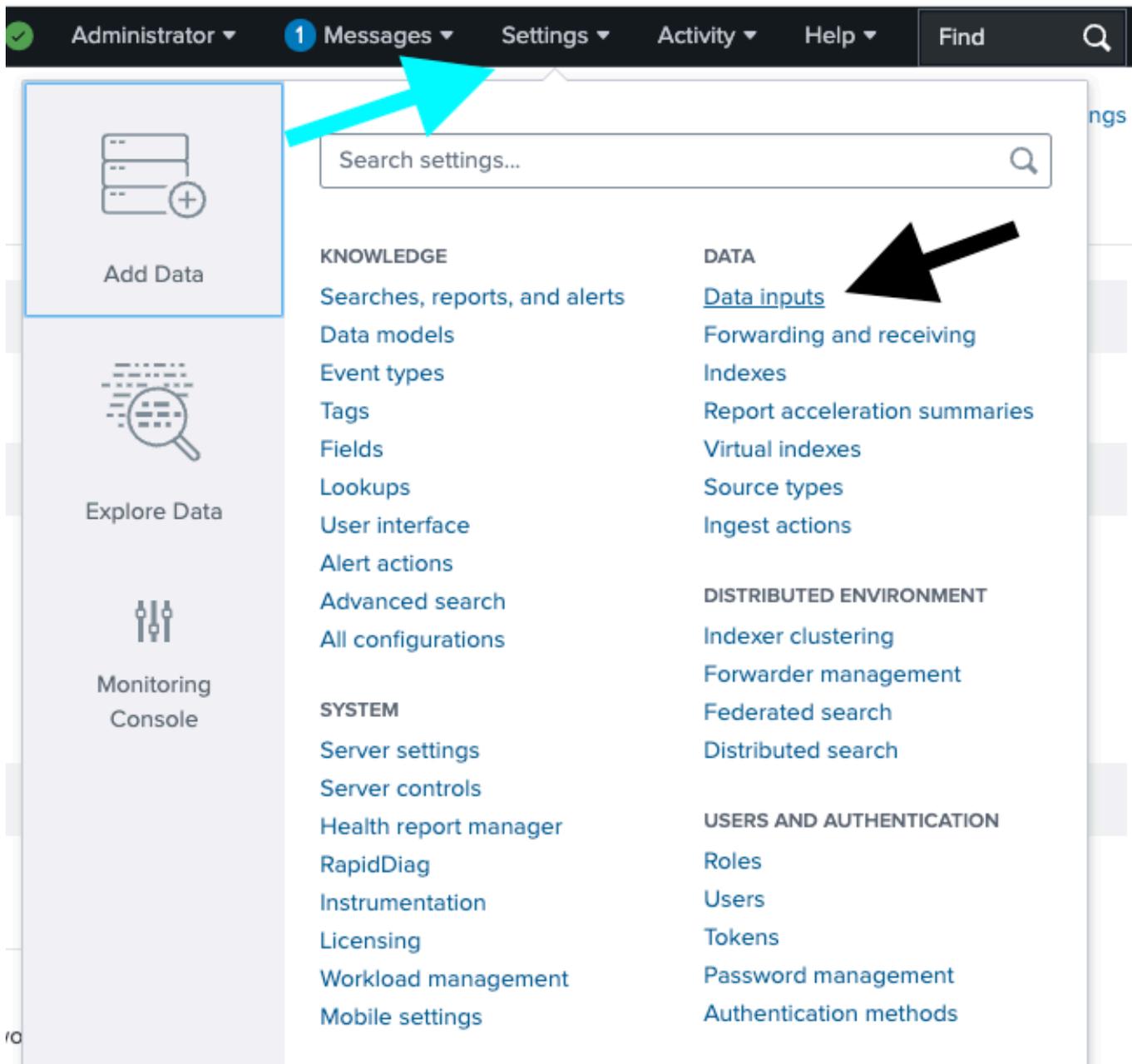


附註：有關源，請參閱步驟4  
有關source\_type的資訊，請參閱步驟6

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。

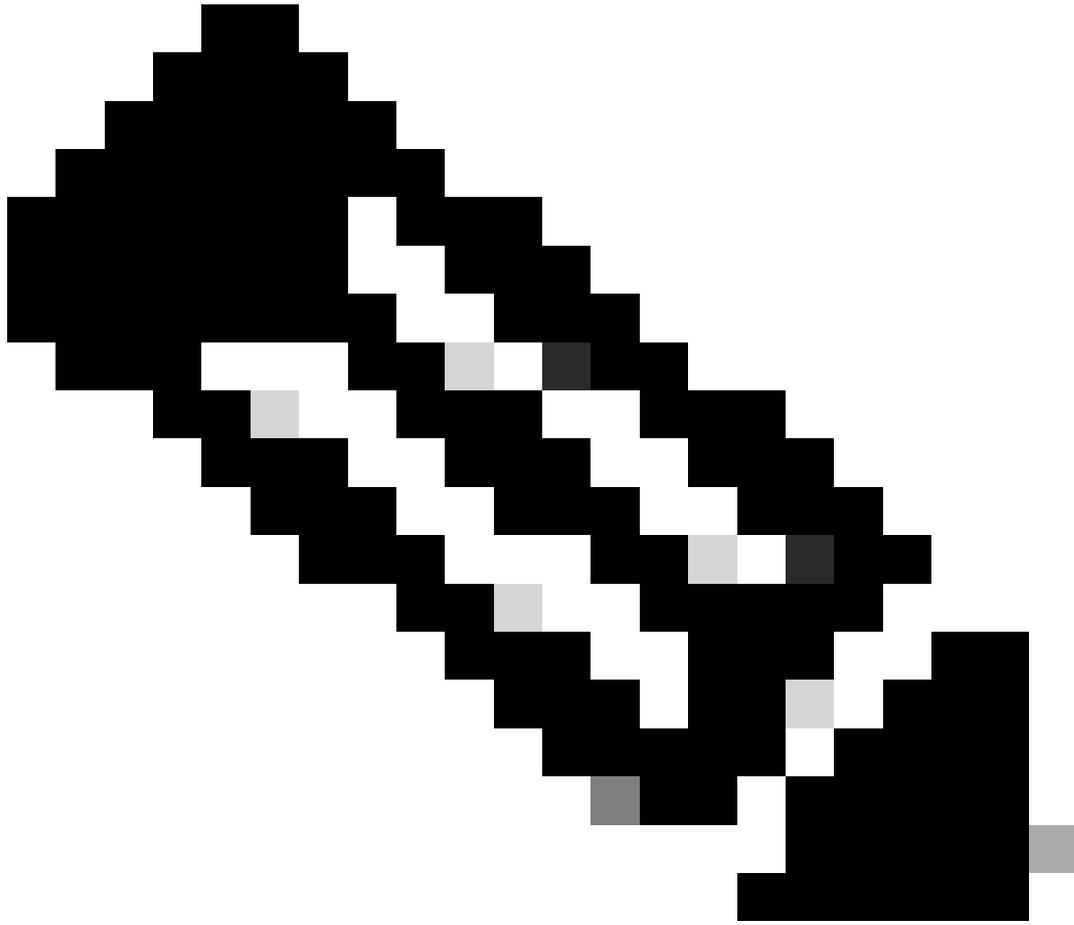
es and directories, network ports, and scripted inputs. If you want to set up forwarding and receiving between two Splunk instances, go to [Forwarding and receiving](#).

### Local inputs

Type	Inputs	Actions
<b>Files &amp; Directories</b> Index a local file or monitor an entire directory.	18	+ Add new
<b>HTTP Event Collector</b> Receive data over HTTP or HTTPS.	0	+ Add new
<b>TCP</b> Listen on a TCP port for incoming data, e.g. syslog.	0	+ Add new
<b>UDP</b> Listen on a UDP port for incoming data, e.g. syslog.	0	+ Add new
<b>Scripts</b> Run custom scripts to collect or generate more data.	36	+ Add new
<b>Splunk Assist Instance Identifier</b> Assigns a random identifier to every node	1	+ Add new
<b>Systemd Journal Input for Splunk</b> This is the input that gets data from journald (systemd's logging component) into Splunk.	0	+ Add new
<b>Logd Input for the Splunk platform</b> This input collects data from logd on macOS and sends it to the Splunk platform.	0	+ Add new
<b>Splunk Secure Gateway</b> Initializes the Splunk Secure Gateway application to talk to mobile clients over websockets	1	+ Add new



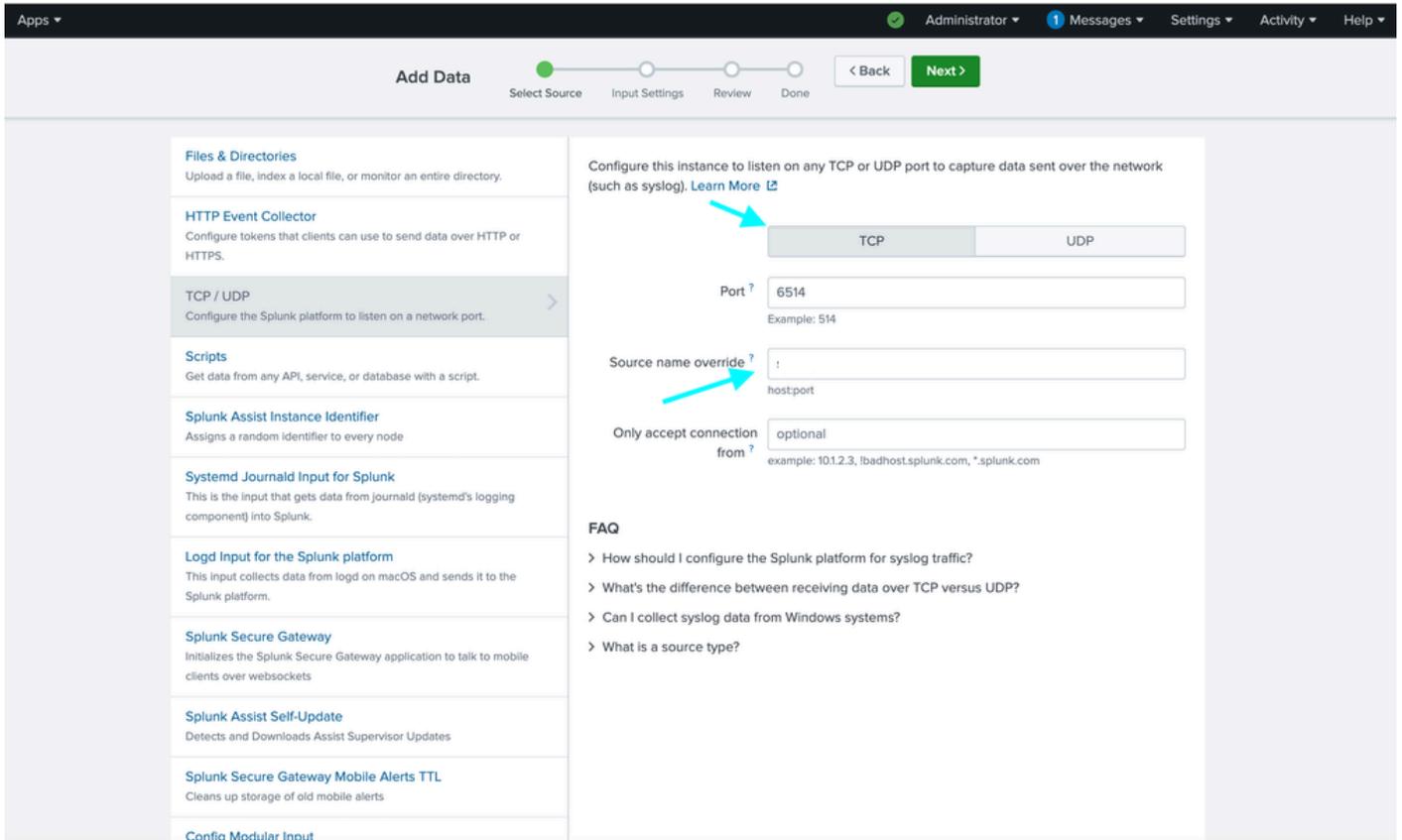
步驟 3: 在新視窗中選擇TCP，在示例影象埠6514中輸入所需的接收埠，並在源名稱覆蓋欄位中輸入「所需名稱」。



附註：TCP 6514是通過TLS的系統日誌的預設埠

---

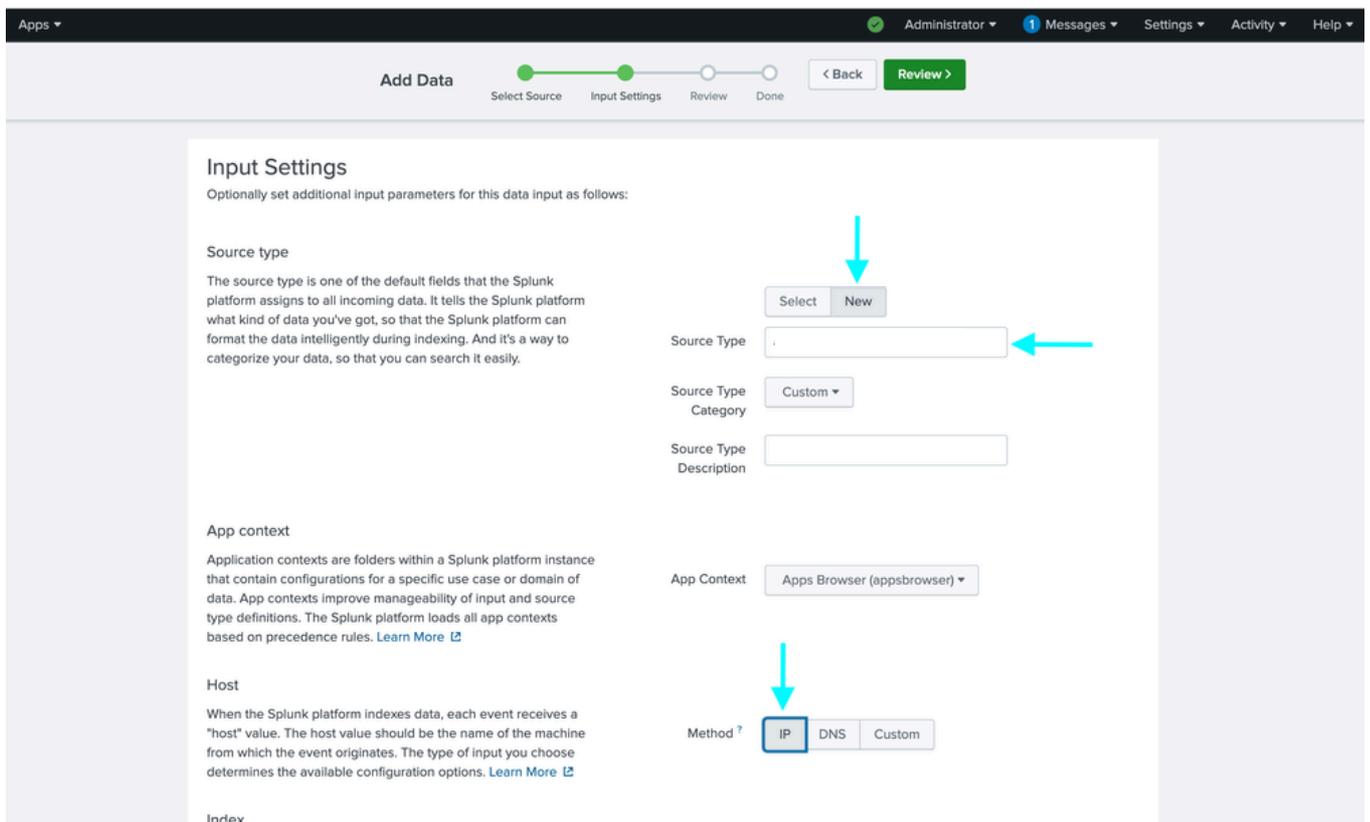
步驟 4:完成後，按一下視窗頂部的綠色「下一步」>按鈕。



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 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 splunkweb.cer 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
```

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

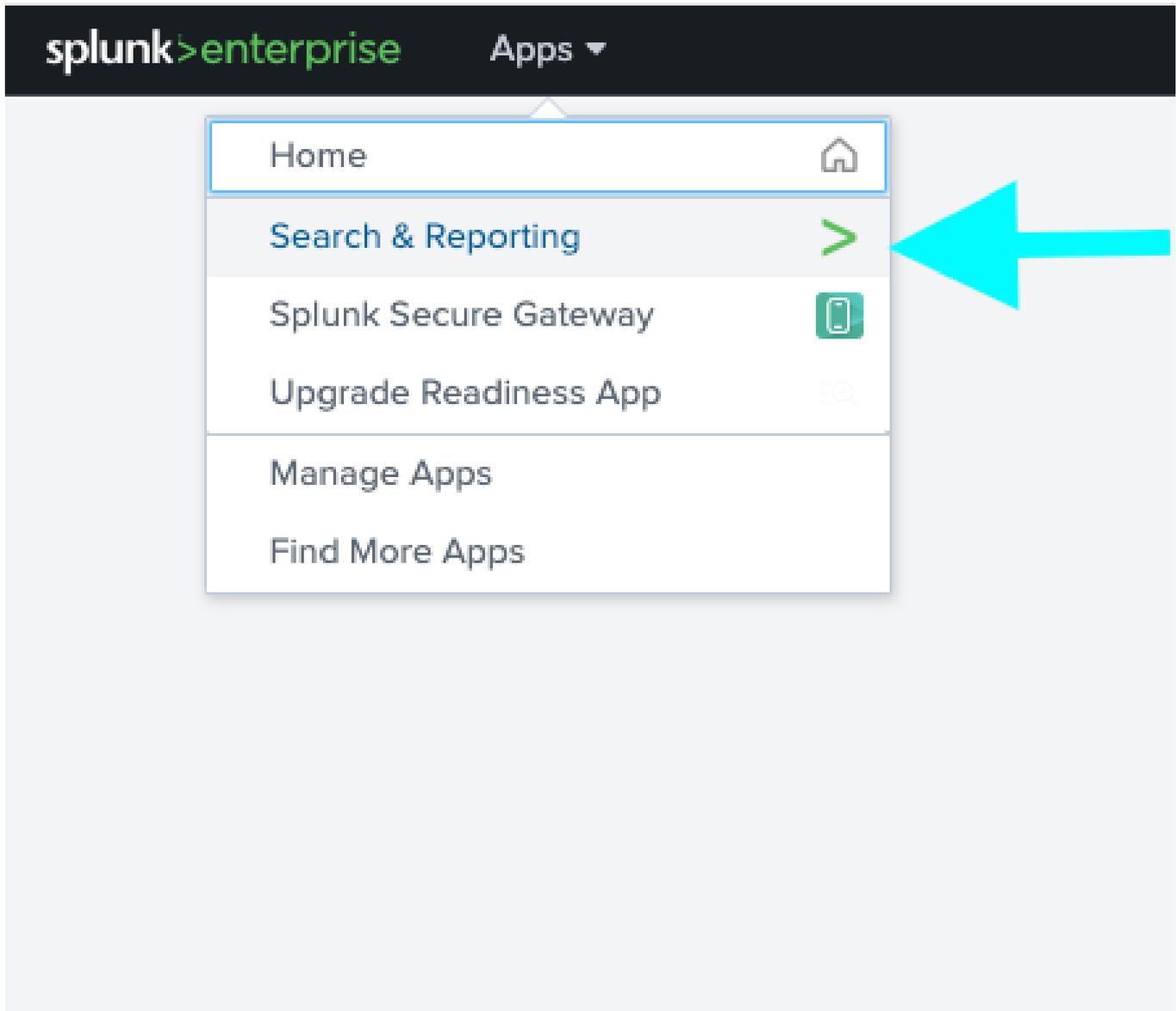
*define the port number here over which syslog will be sent*

*your source type defined during the TCP input configuration*

*path for Splunk certificate*

*PEM pass phrase set during certificate generation*

步驟 8:使用搜尋驗證系統日誌。







nse



Monitor



Investigate



Report



Configure

## Configure ×

### Detection

Host Group Management

Alarm Severity

Policy Management

Response Management

Network Scanners

Analytics

Alerts

### Global

↗ 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。

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

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

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

- Disabled
- Soft Fail
- Hard Fail

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。

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

Inventory / Appliance Configuration

Appliance Configuration - Manager Cancel Apply Settings

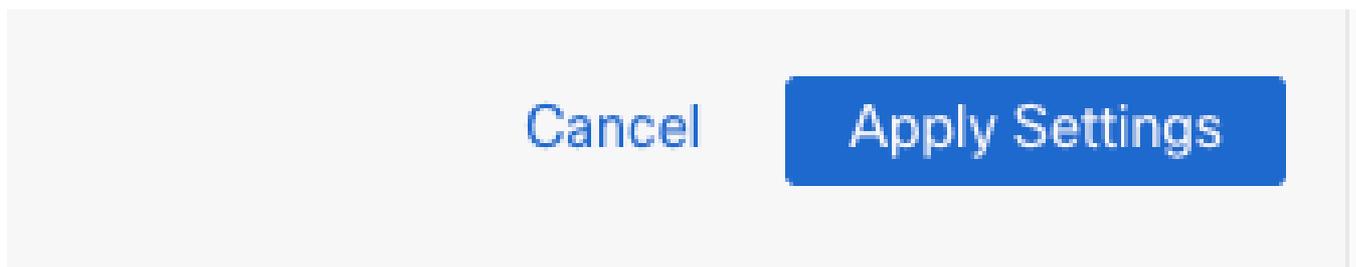
Appliance Network Services General Configuration Menu

Trust Store Add New

Friendly Name	Issued To	Issued By	Valid From	Valid To	Serial Number	Key Length	Actions
							Delete
							Delete
splunk							Delete

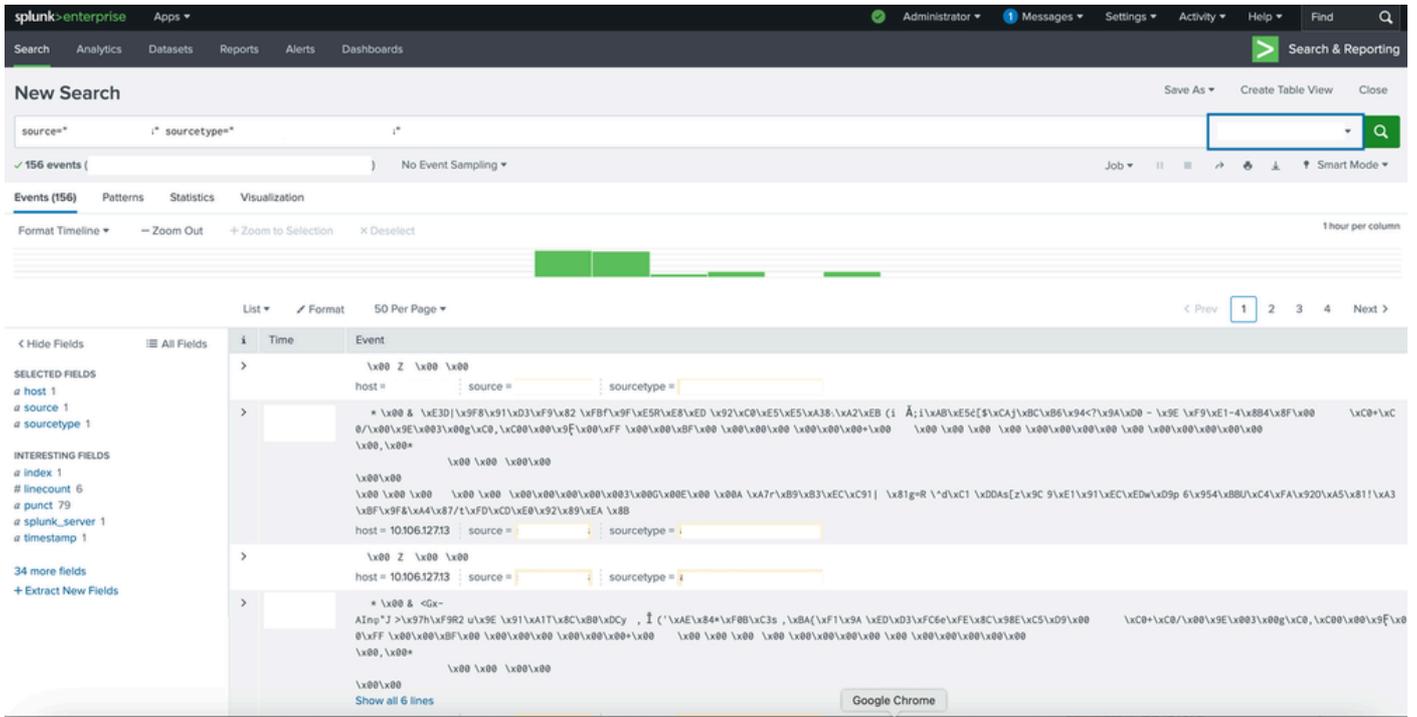
6 Certificates

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。

  
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
<a href="#">Files &amp; Directories</a> Index a local file or monitor an entire directory.	18	+ Add new
<a href="#">HTTP Event Collector</a> Receive data over HTTP or HTTPS.	0	+ Add new
<a href="#">TCP</a> Listen on a TCP port for incoming data, e.g. syslog.	1	+ Add new
<a href="#">UDP</a> Listen on a UDP port for incoming data, e.g. syslog.	1	+ Add new
<a href="#">Scripts</a> Run custom scripts to collect or generate more data.	36	+ Add new
<a href="#">Splunk Assist Instance Identifier</a> Assigns a random identifier to every node	1	+ Add new
<a href="#">Systemd Journald Input for Splunk</a> This is the input that gets data from journald (systemd's logging component) into Splunk.	0	+ Add new
<a href="#">Logd Input for the Splunk platform</a> This input collects data from logd on macOS and sends it to the Splunk platform.	0	+ Add new
<a href="#">Splunk Secure Gateway</a> Initializes the Splunk Secure Gateway application to talk to mobile clients over websockets	1	+ Add new
<a href="#">Splunk Assist Self Update</a>	1	+ Add new

## TCP

Data inputs > TCP

New Local TCP

Showing 1-1 of 1 item

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

## 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）。