Configurer la gestion des réponses pour envoyer les événements Syslog au Splunk

Table des matières

Introduction

Ce document décrit comment configurer la fonctionnalité Secure Analytics Response Management pour envoyer des événements via syslog à un tiers tel que Splunk.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

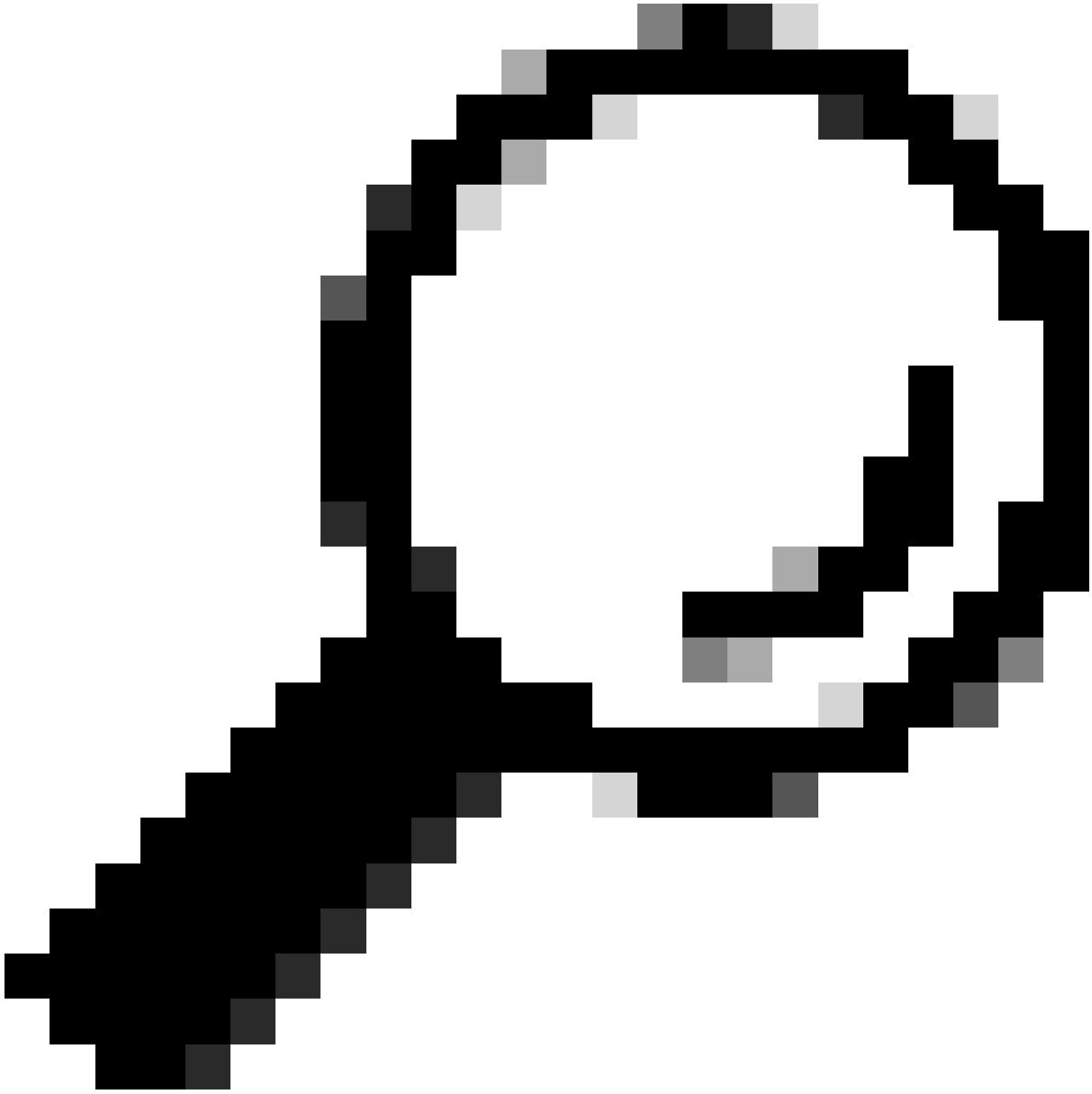
- Gestion des réponses Secure Network Analytics.
- Splunk Syslog

Composants utilisés

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

- Déploiement Secure Network Analytics (SNA) qui contient au moins une appliance Manager et une appliance Flow Collector.
- Serveur Splunk installé et accessible via le port 443.

Configurez syslog sur SNA sur UDP 514 ou sur un port personnalisé



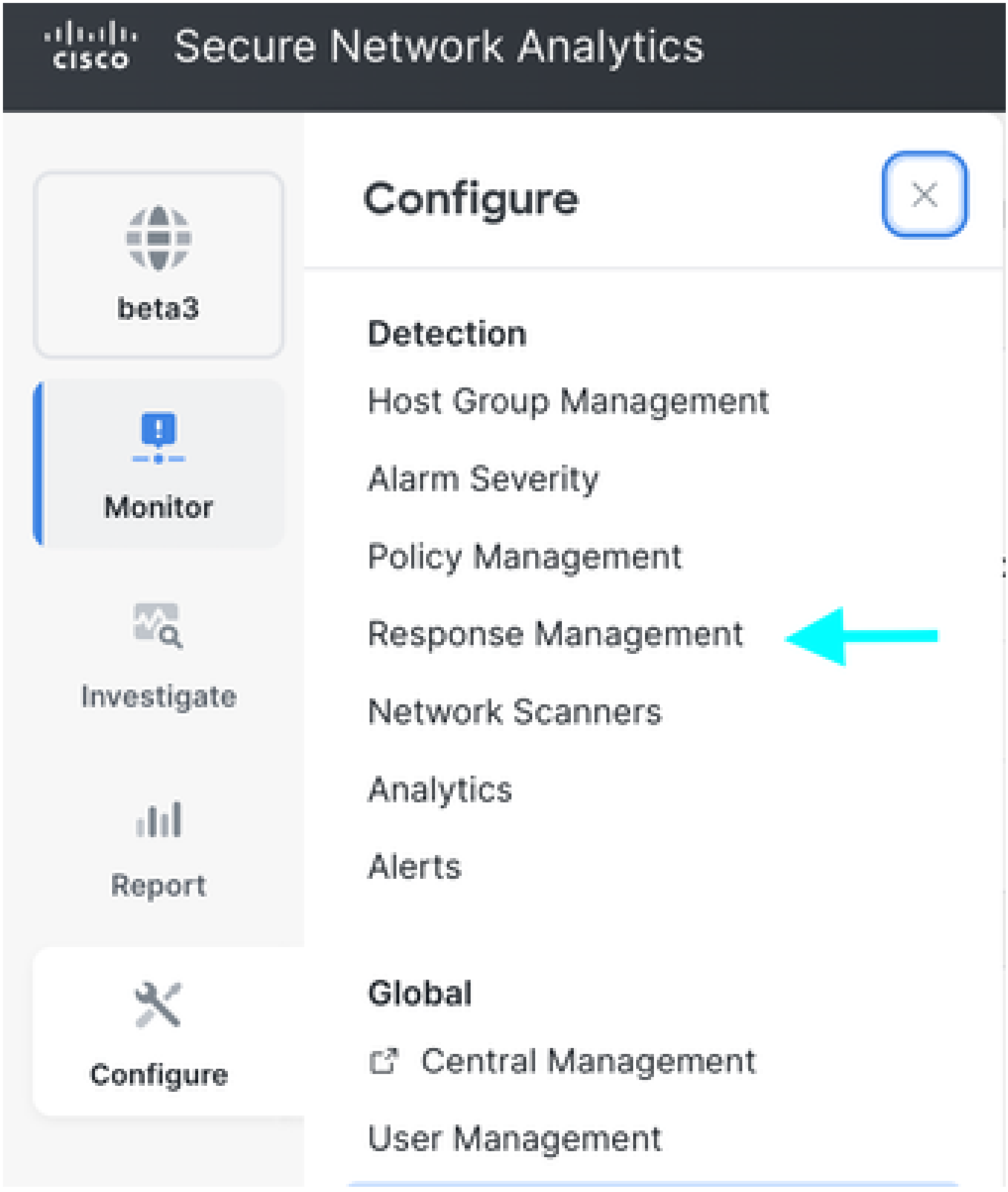
Conseil : assurez-vous que les protocoles UDP/514, TCP/6514 ou tout port personnalisé que vous choisissez pour Syslog sont autorisés sur les pare-feu ou les périphériques intermédiaires entre SNA et Splunk.

1.Gestion des réponses SNA

Le composant Response Management de Secure Analytics (SA) peut être utilisé pour configurer les règles, les actions et les destinations syslog.

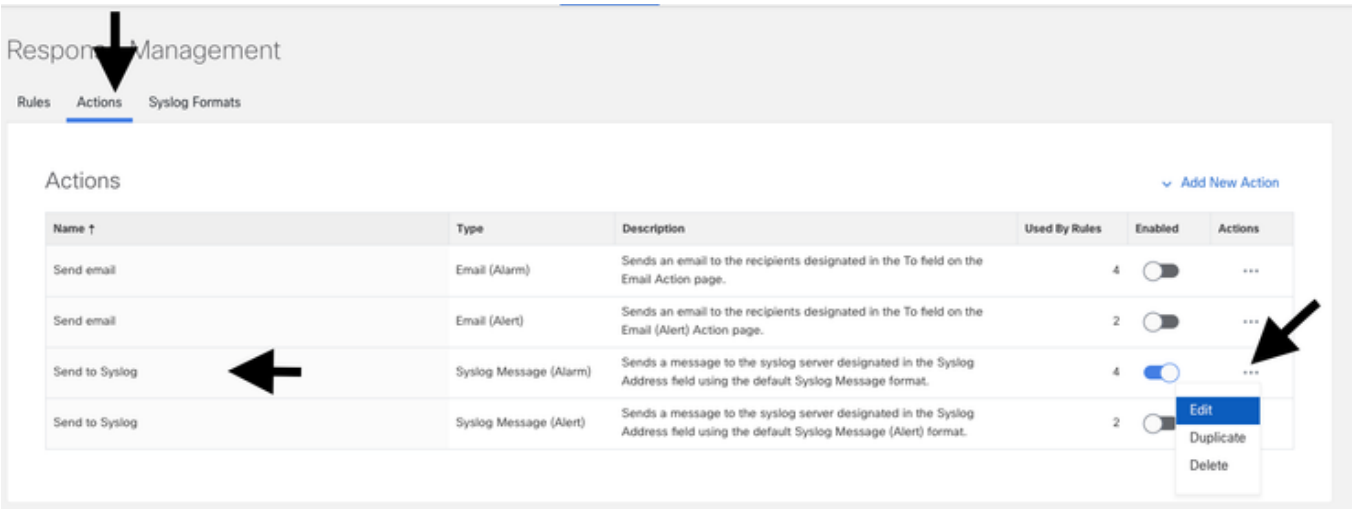
Ces options doivent être configurées pour envoyer/transférer des alarmes Secure Analytics vers d'autres destinations.

Étape 1 : Connectez-vous à l'appliance SA Manager et accédez à Configure > Detection Response Management.

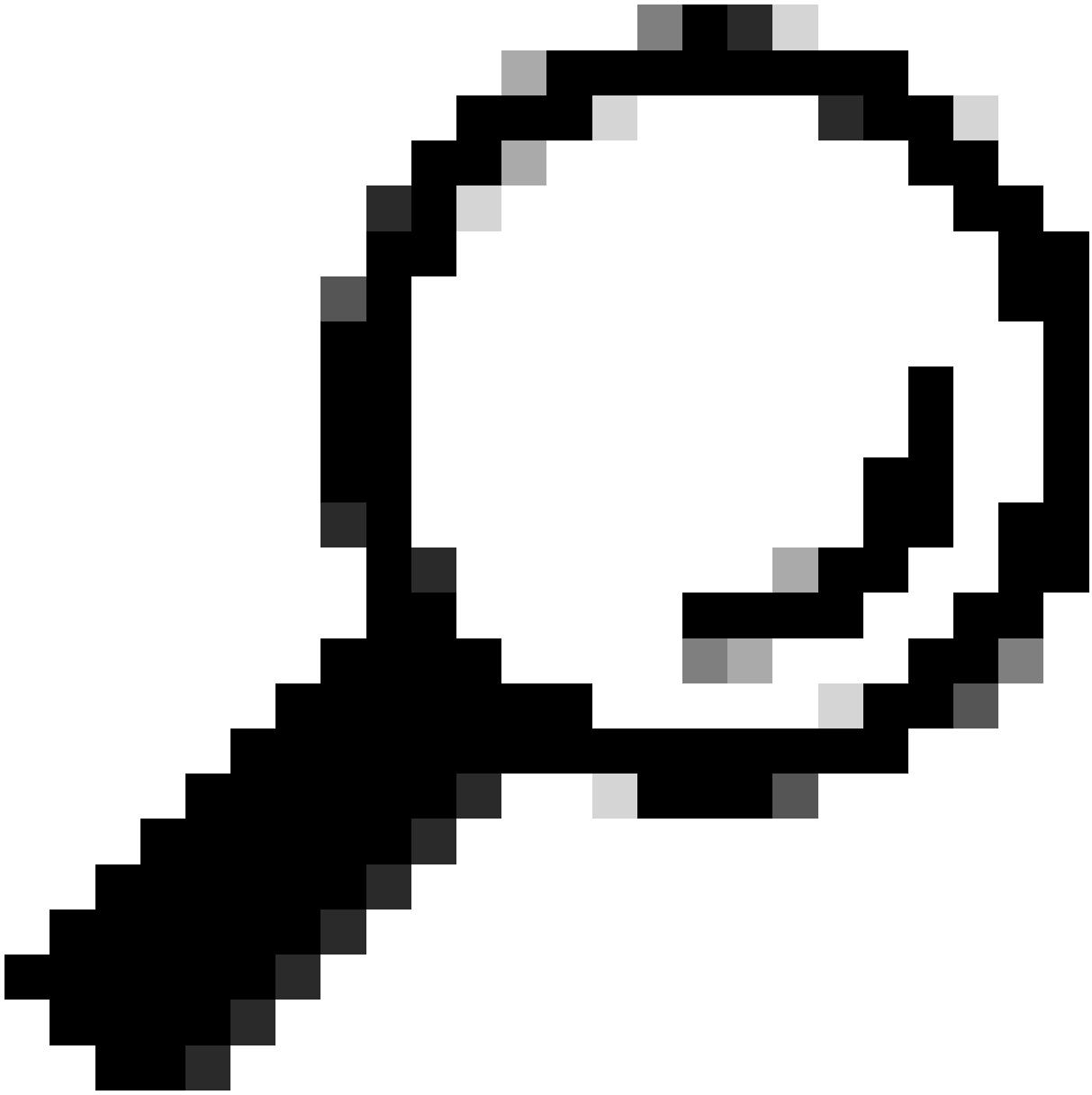


Étape 2 : Sur la nouvelle page, accédez à l'onglet Actions, localisez l'élément de ligne Send to Syslog par défaut et cliquez sur les points de suspension (...) dans la colonne Action, puis sur

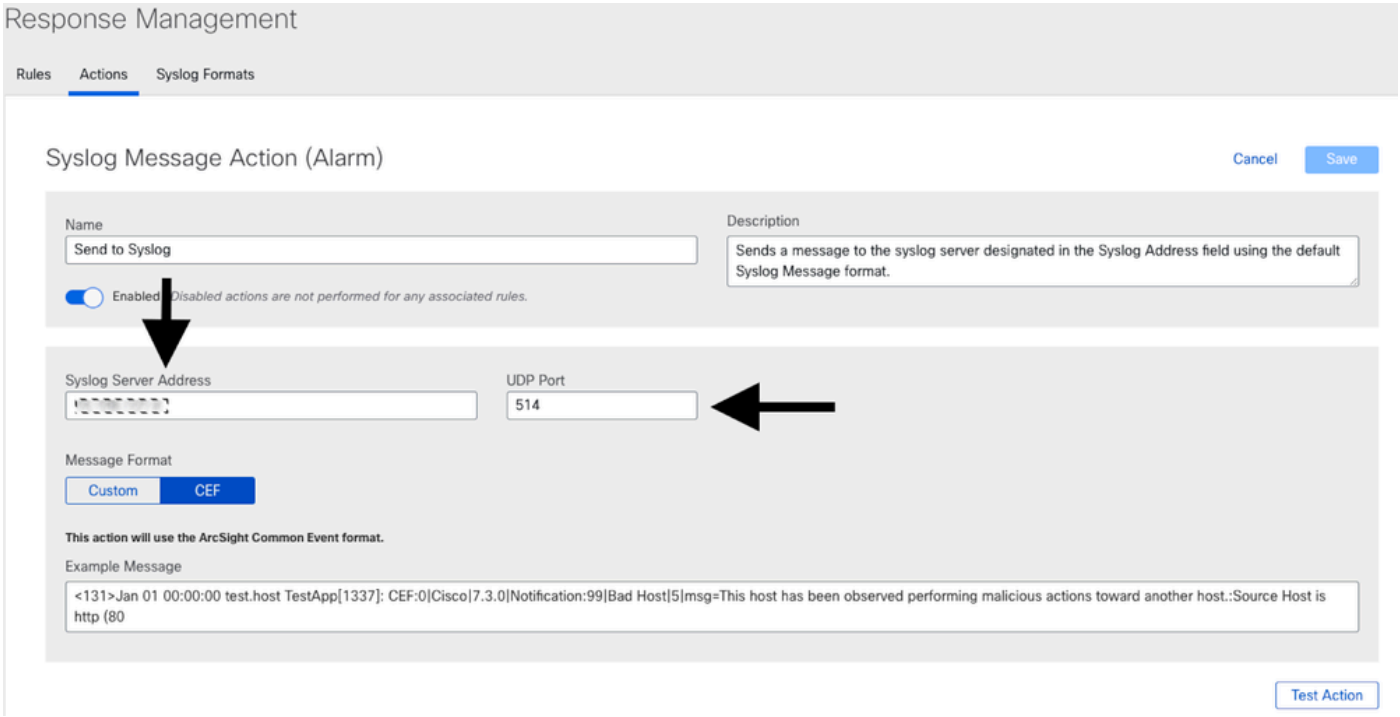
Edit.



Étape 3 : Saisissez l'adresse de destination souhaitée dans le champ Syslog Server Address et le port de réception de destination souhaité dans le champ UDP Port. Dans le champ Message Format, sélectionnez CEF.
Étape 4 : Lorsque vous avez terminé, cliquez sur le bouton bleu Enregistrer dans l'angle supérieur droit.



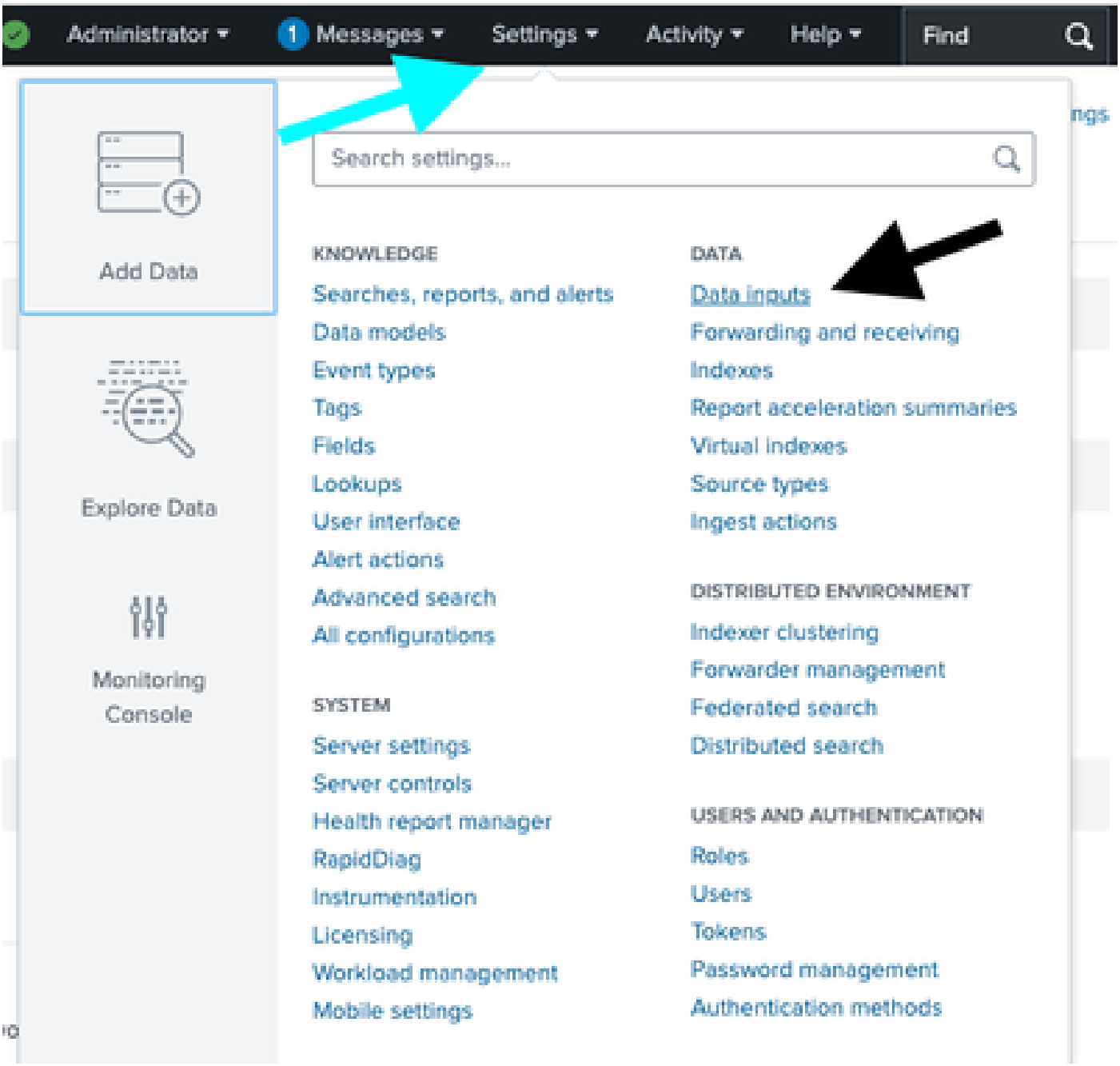
Conseil : Le port UDP par défaut pour syslog est 514



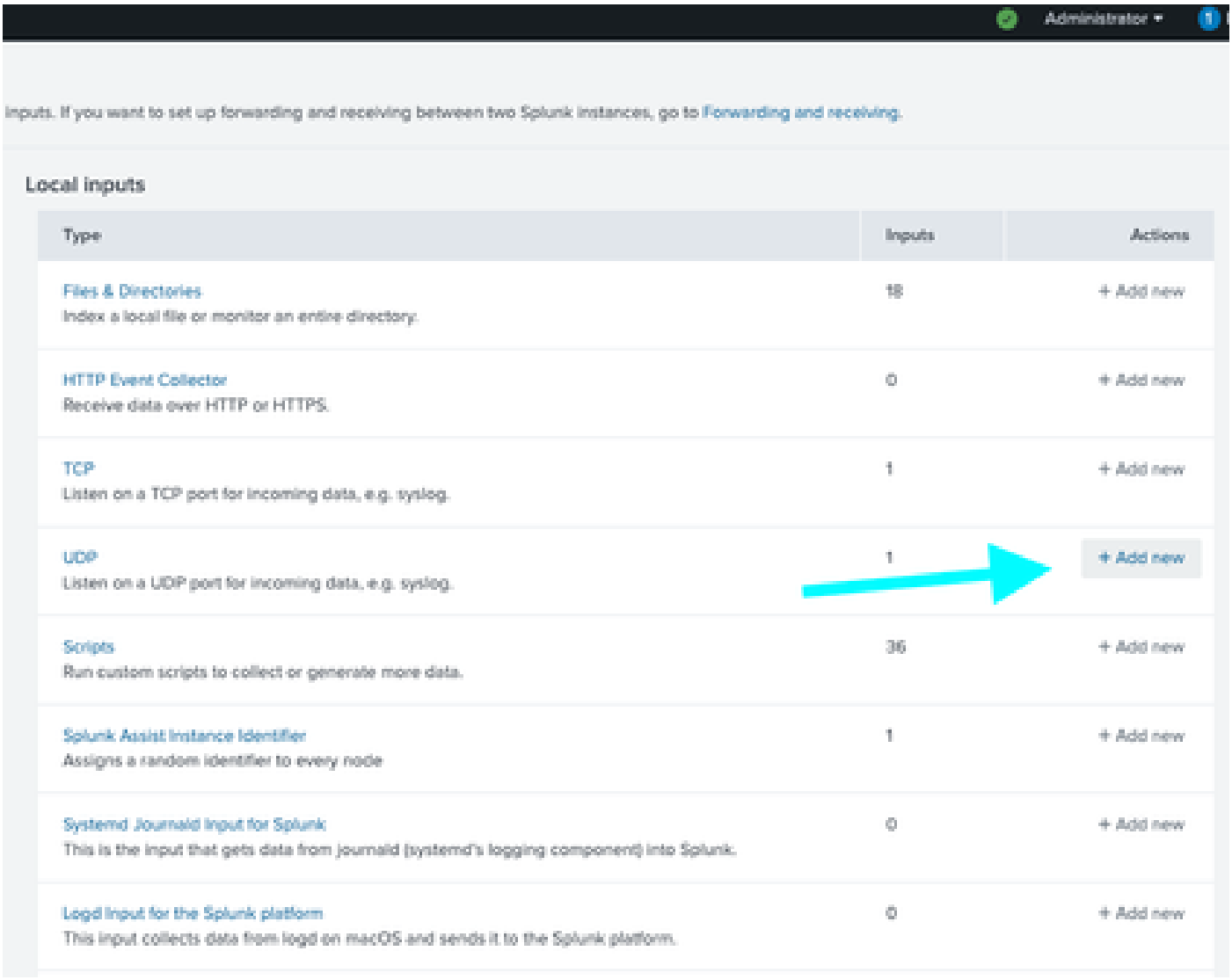
2.Configuration du Splunk pour recevoir les Syslogs SNA sur le port UDP

Après avoir appliqué vos modifications sur l'interface utilisateur Web de Secure Network Analytics Manager , vous devez configurer la saisie des données dans le Splunk.

Étape 1 : Connectez-vous à Splunk et naviguez jusqu'à Settings > Add Data > DATA Data Inputs.

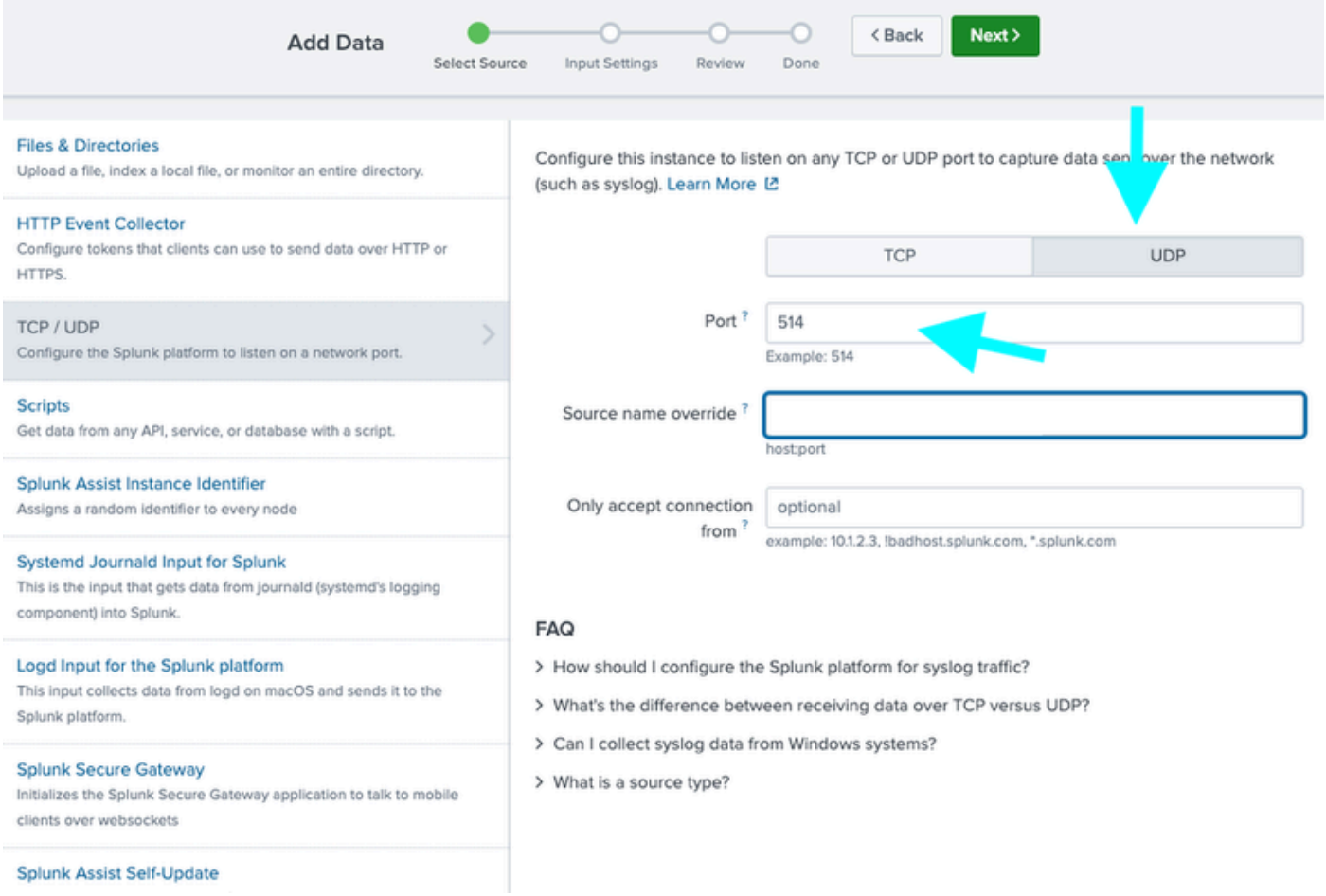


Étape 2 : Recherchez la ligne UDP et sélectionnez +Ajouter nouveau.



Étape 3 : Sur la nouvelle page, sélectionnez UDP, saisissez le port de réception tel que 514 dans le champ Port.
Étape 4 : Dans le champ Remplacement du nom de la source, saisissez desired name of source.

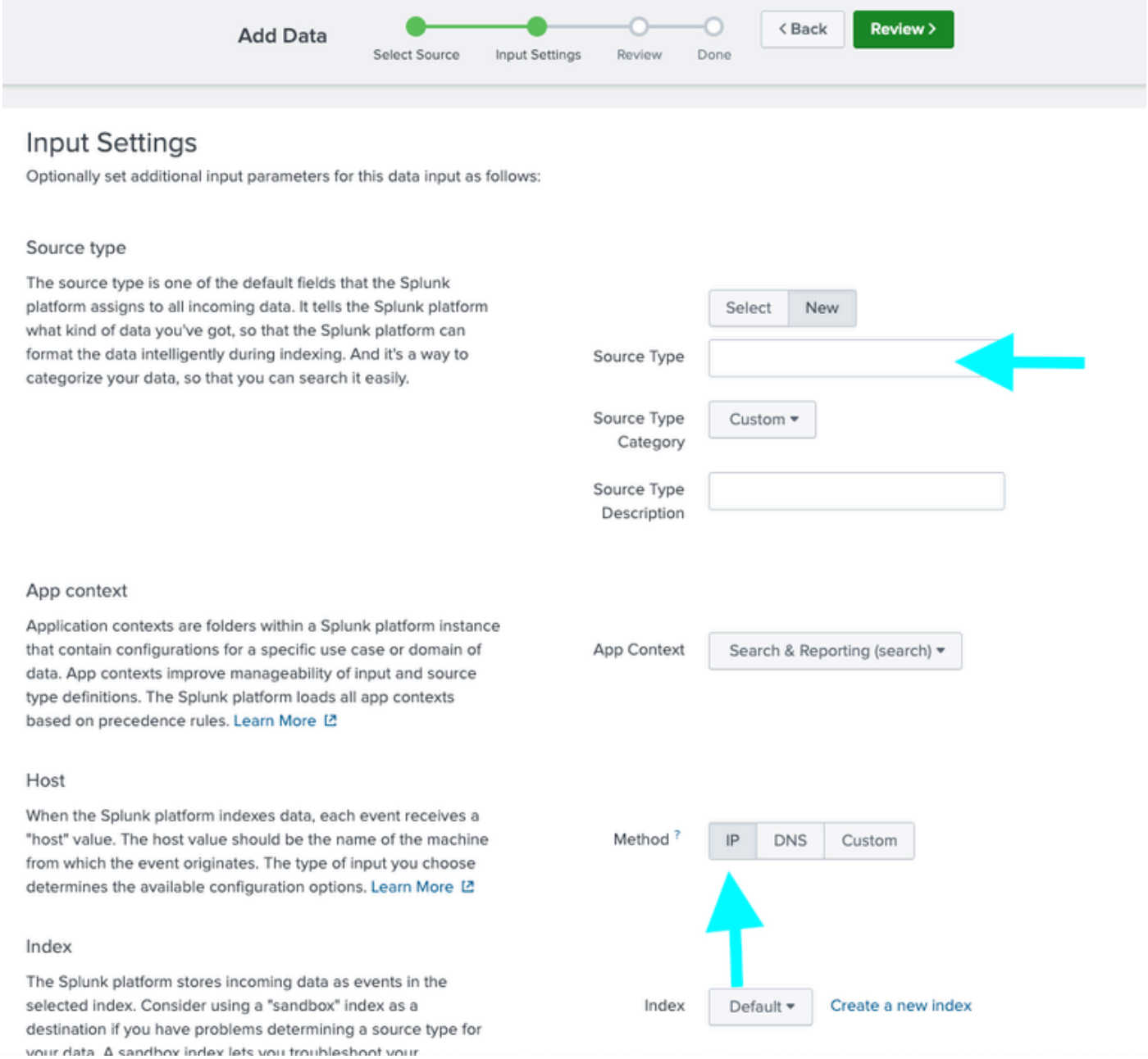
Étape 5 : Lorsque vous avez terminé, cliquez sur le bouton Suivant > vert en haut de la fenêtre.



Étape 6 : Sur la page suivante, passez à l'option New, localisez le champ Source Type et entrez desired source .

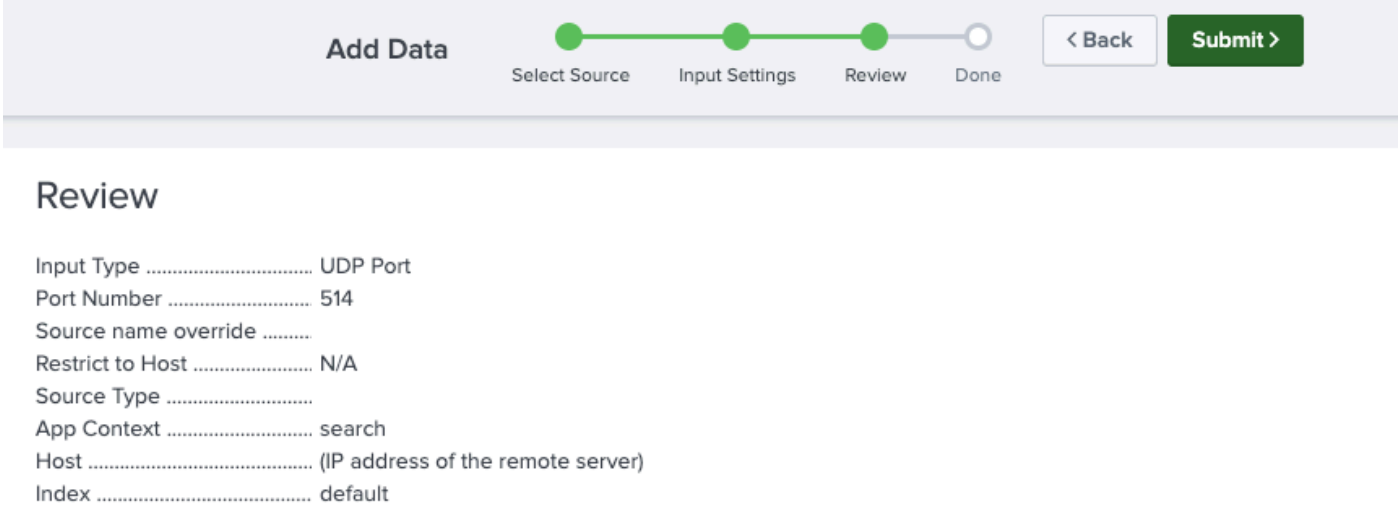
Étape 7 : Sélectionnez IP pour la méthode.

Étape 8 : Cliquez sur le bouton Review > vert en haut de l'écran.

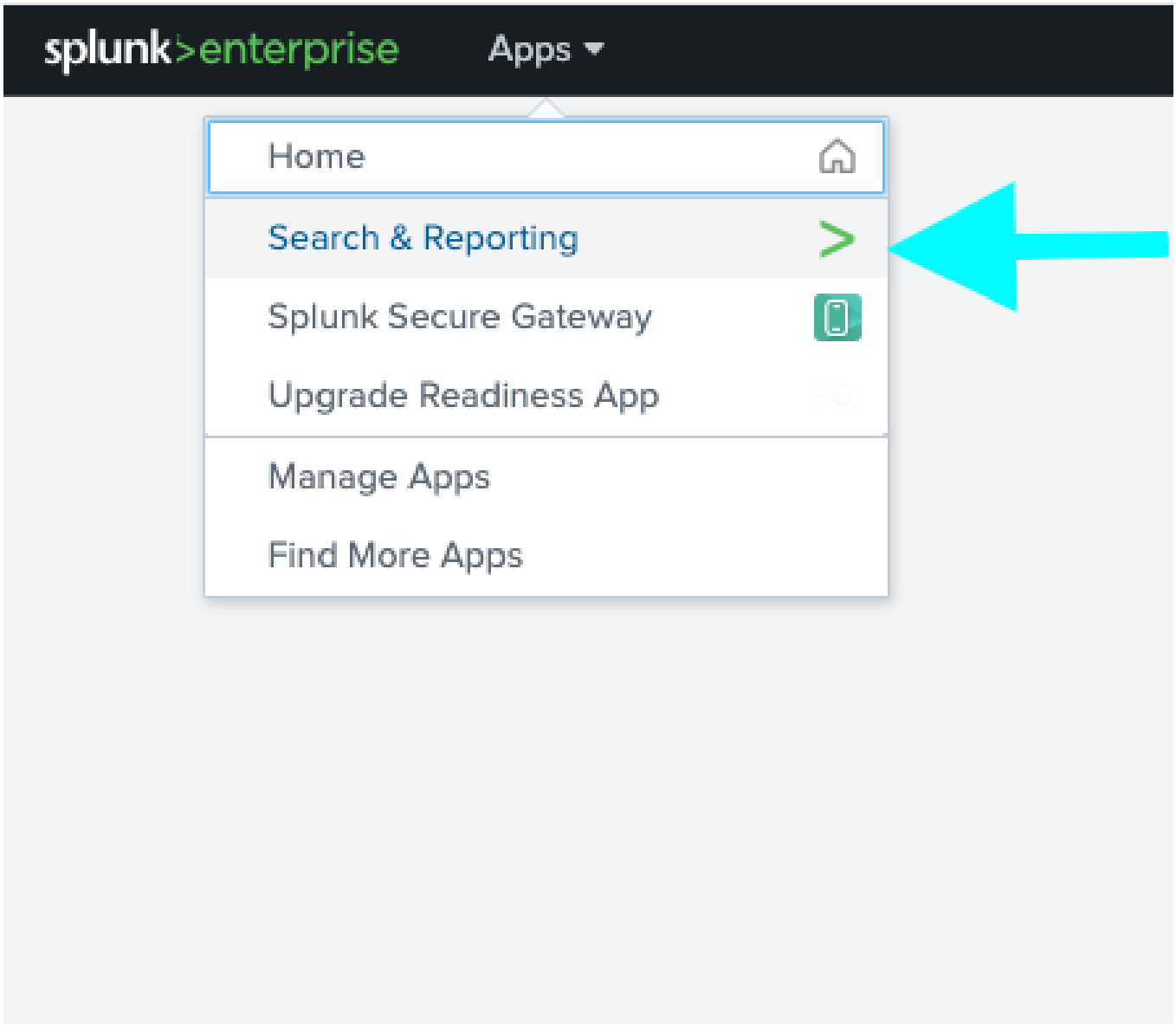


Étape 9 : Dans la fenêtre suivante, vérifiez vos paramètres et modifiez-les si nécessaire.

Étape 10 : Une fois la validation effectuée, cliquez sur le bouton vert Submit > en haut de la fenêtre.

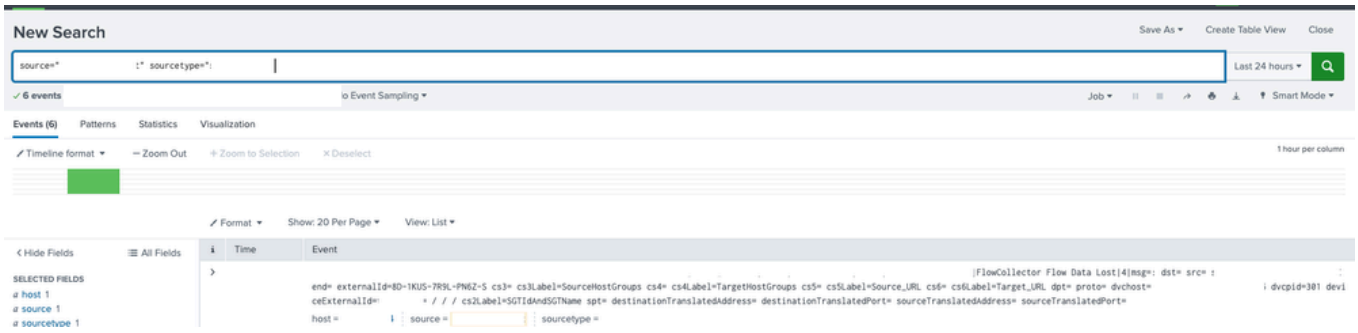


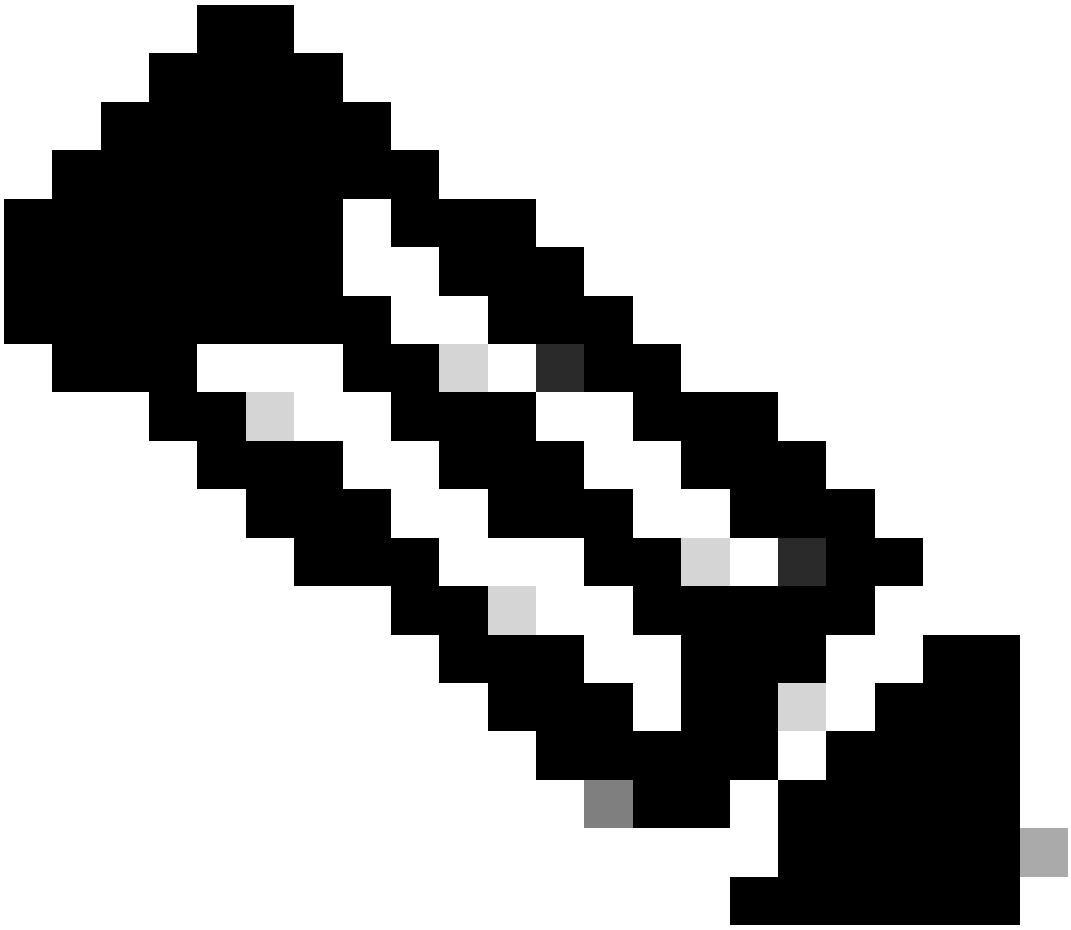
Étape 11 : Accédez à Apps > Search & Reporting dans l'interface utilisateur Web.



Étape 12: Sur la page Rechercher, utilisez le filtre`source="As_configured" sourcetype="As_configured"`pour

rechercher les journaux reçus.



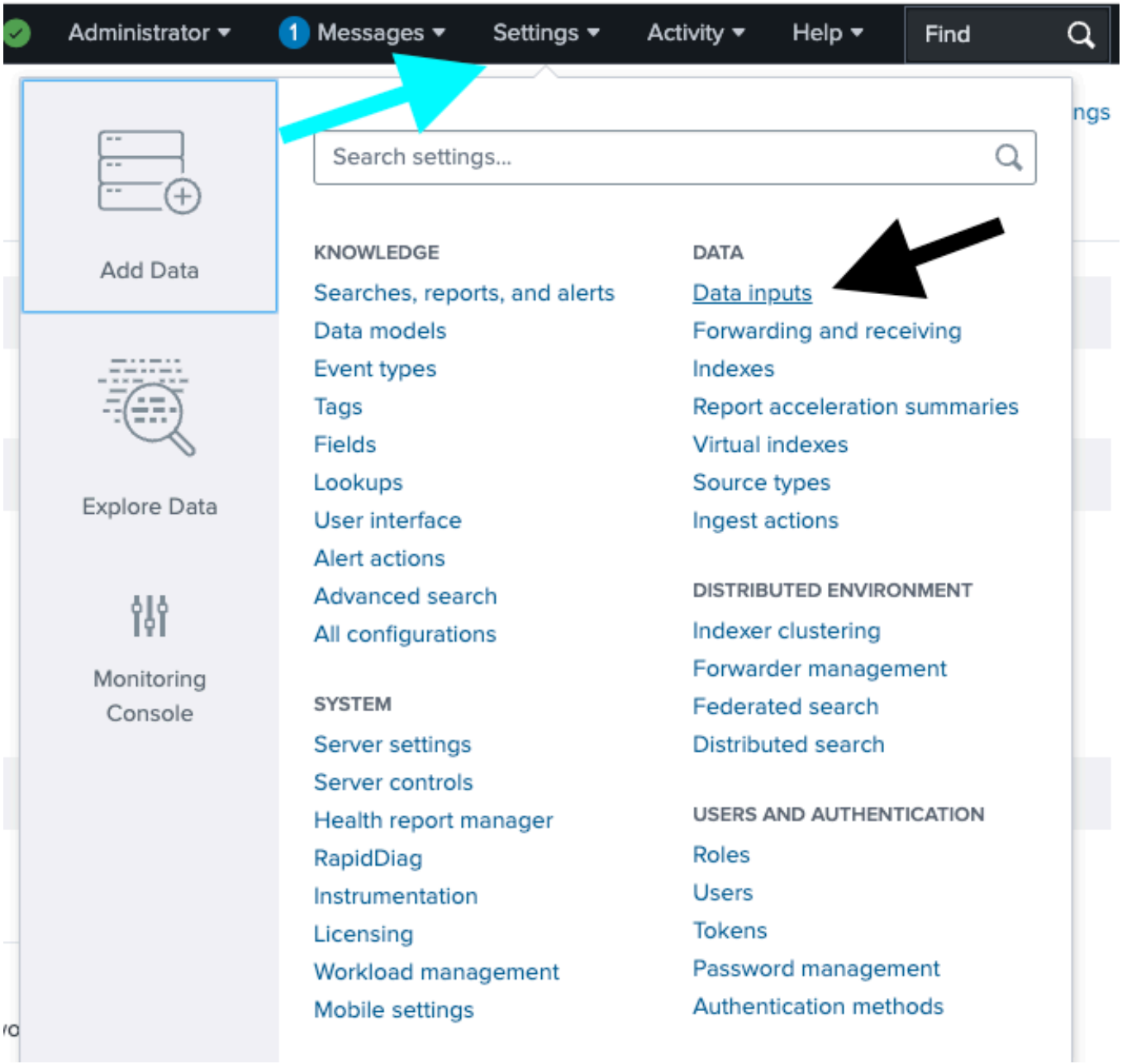


Remarque : Pour la source, voir Étape 4
Pour source_type, voir l'étape 6

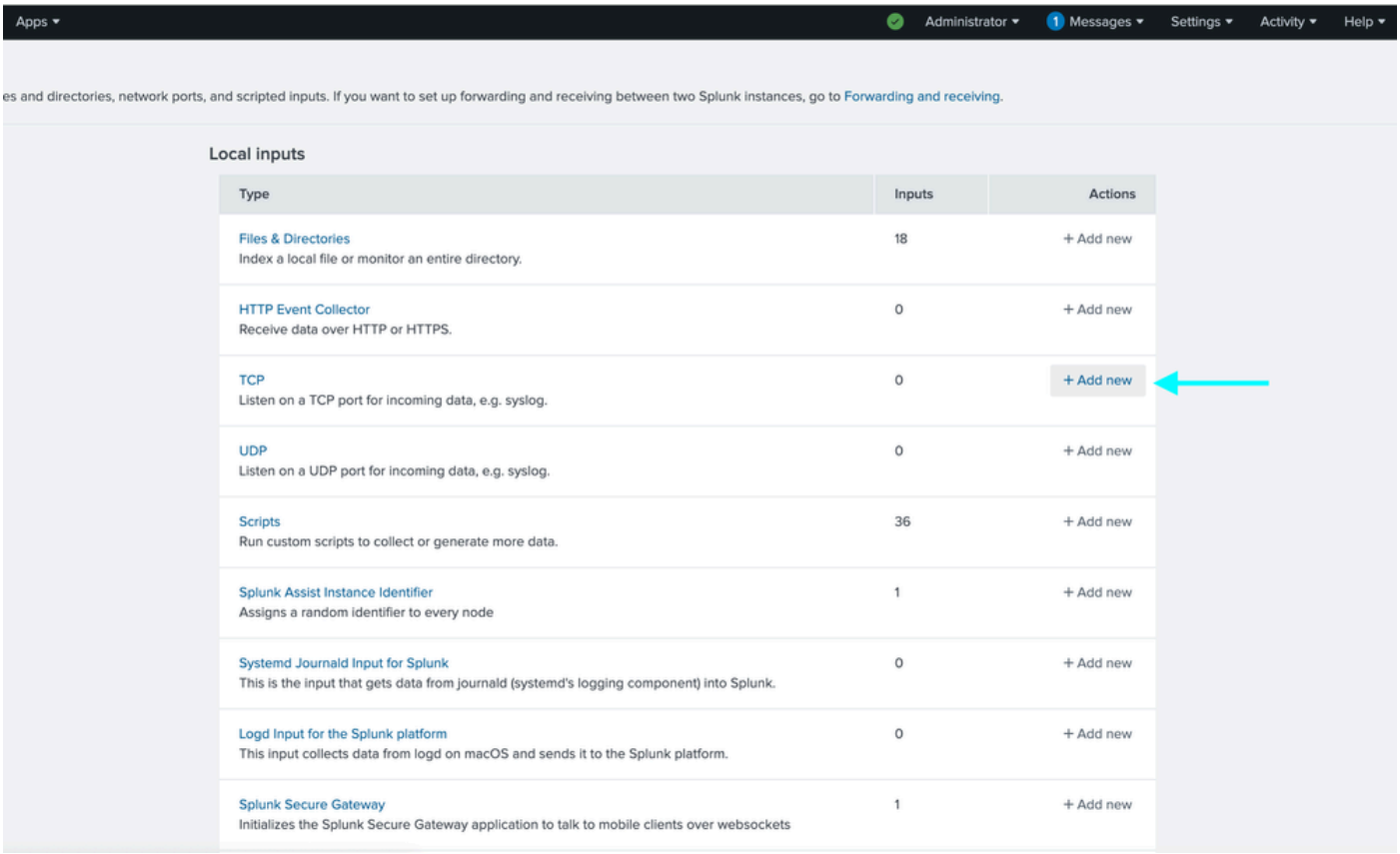
Configurez syslog sur SNA via le port TCP 6514 ou le port personnalisé défini

1.Configuration du Splunk pour recevoir les journaux d'audit SNA sur le port TCP

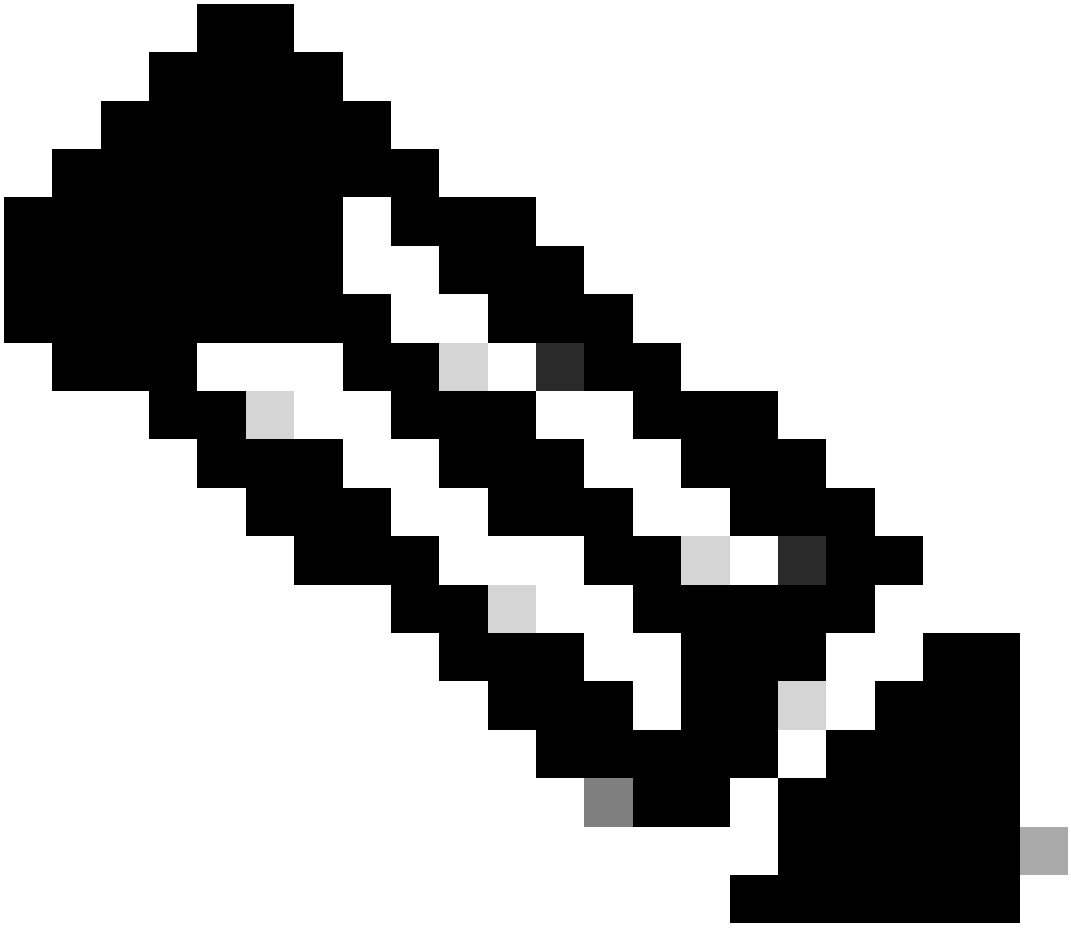
Étape 1 : Dans l'interface utilisateur du Splunk, accédez à Paramètres > Ajouter des données > Entrées de données de données.



Étape 2 : Recherchez la ligne TCP et sélectionnez + Ajouter nouveau.

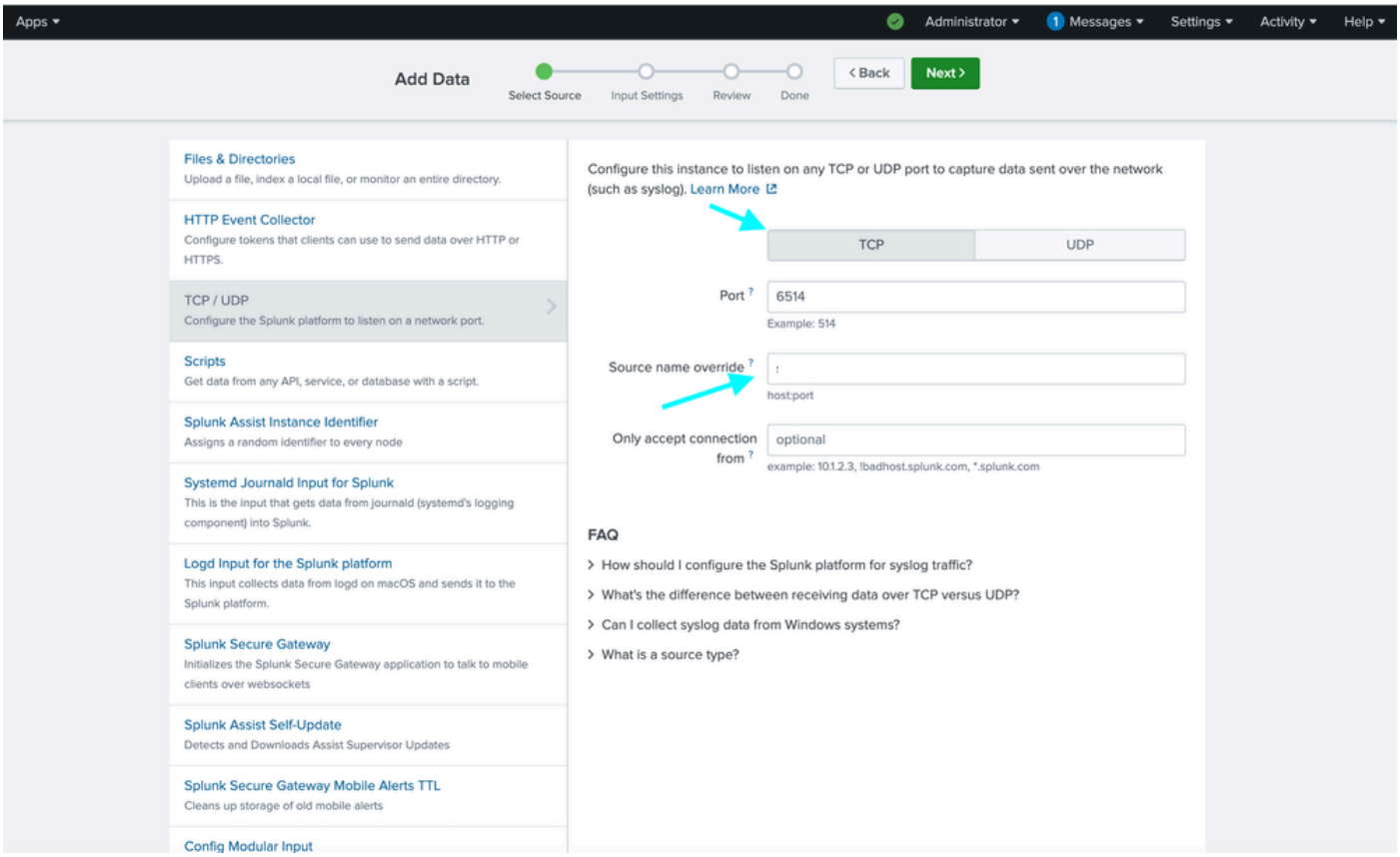


Étape 3 : Dans la nouvelle fenêtre, sélectionnez TCP, entrez le port de réception souhaité, dans l'exemple de port d'image 6514, et entrez « nom souhaité » dans le champ de remplacement du nom de source.



Remarque : TCP 6514 est le port par défaut pour Syslog sur TLS

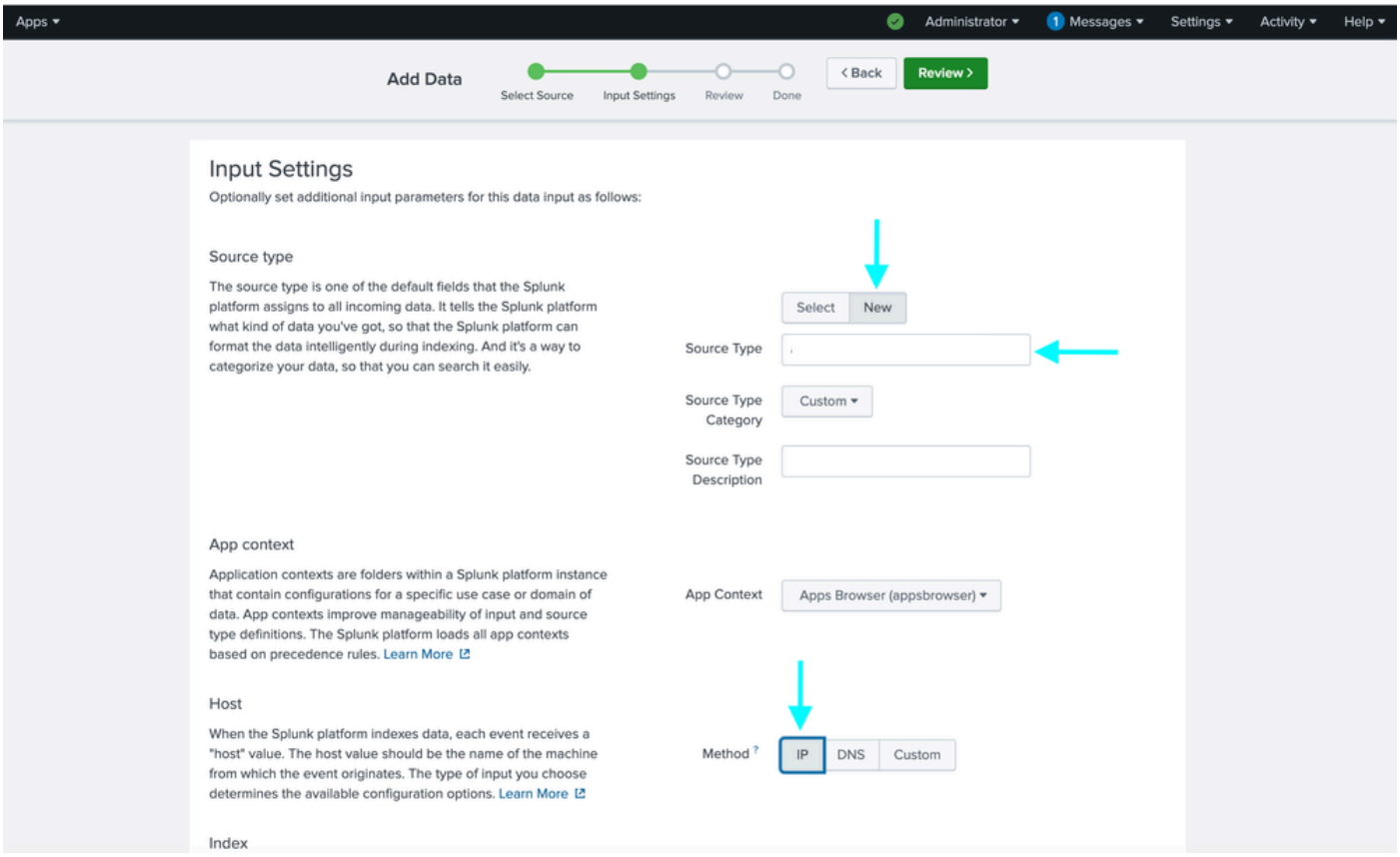
Étape 4 : Lorsque vous avez terminé, cliquez sur le bouton Suivant > vert en haut de la fenêtre.



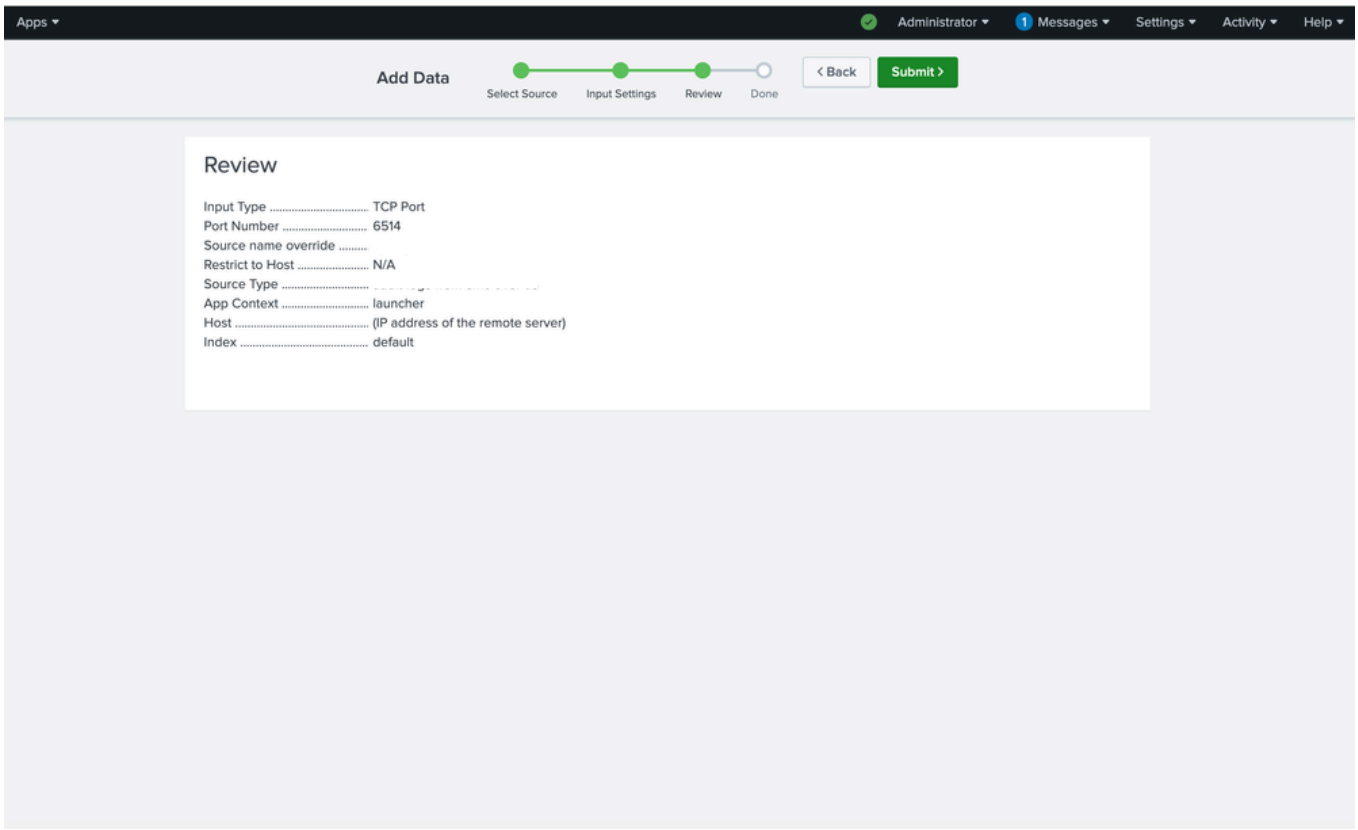
Étape 5 : Dans la nouvelle fenêtre, sélectionnez Nouveau dans la section Type de source, entrez le nom souhaité dans le champ Type de source.

Étape 6 : Sélectionnez IP comme méthode dans la section Host.

Étape 7 : Lorsque vous avez terminé, cliquez sur le bouton vert Review > en haut de la fenêtre.



Étape 8 : Dans la fenêtre suivante, vérifiez vos paramètres et modifiez-les si nécessaire. Une fois la validation effectuée, cliquez sur le bouton vert Submit> en haut de la fenêtre.



2.Generate Certificat pour le Splunk

Étape 1 : À l’aide d’une machine sur laquelle openssl est installé, exécutez la`sudo openssl req -x509 -newkey rsa:4096 -keyout server_key.pem -out server_cert.pem -sha256 -days 3650 -subj /CN=10.106.127.4`commande en remplaçant l’exemple d’adresse IP 10.106.127.4 par l’adresse IP du périphérique Splunk. Vous êtes invité deux fois à saisir une phrase de passe définie par l'utilisateur. Dans les exemples, les commandes sont exécutées à partir de la ligne de commande de la machine 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:
```

Lorsque la commande est terminée, deux fichiers sont générés. Les fichiers server_cert.pem et 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:
```

Étape 2 : Passer à l'utilisateur racine.

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

Étape 3 : Copiez le certificat nouvellement généré dans le `/opt/splunk/etc/auth/` .

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

Étape 4 : Ajoutez le fichier spunkweb.cet avec une clé privée.

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

Étape 5 : Modifiez la propriété du certificat splunk.

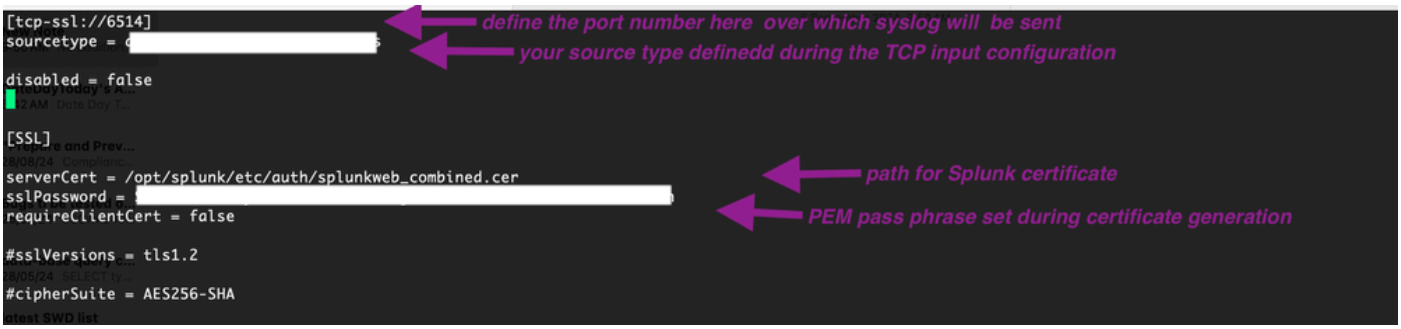
```
user@examplehost:~# chown 10777:10777/opt/splunk/etc/auth/splunkweb.cer
```

Étape 6 : Modifiez l'autorisation pour le certificat splunk.

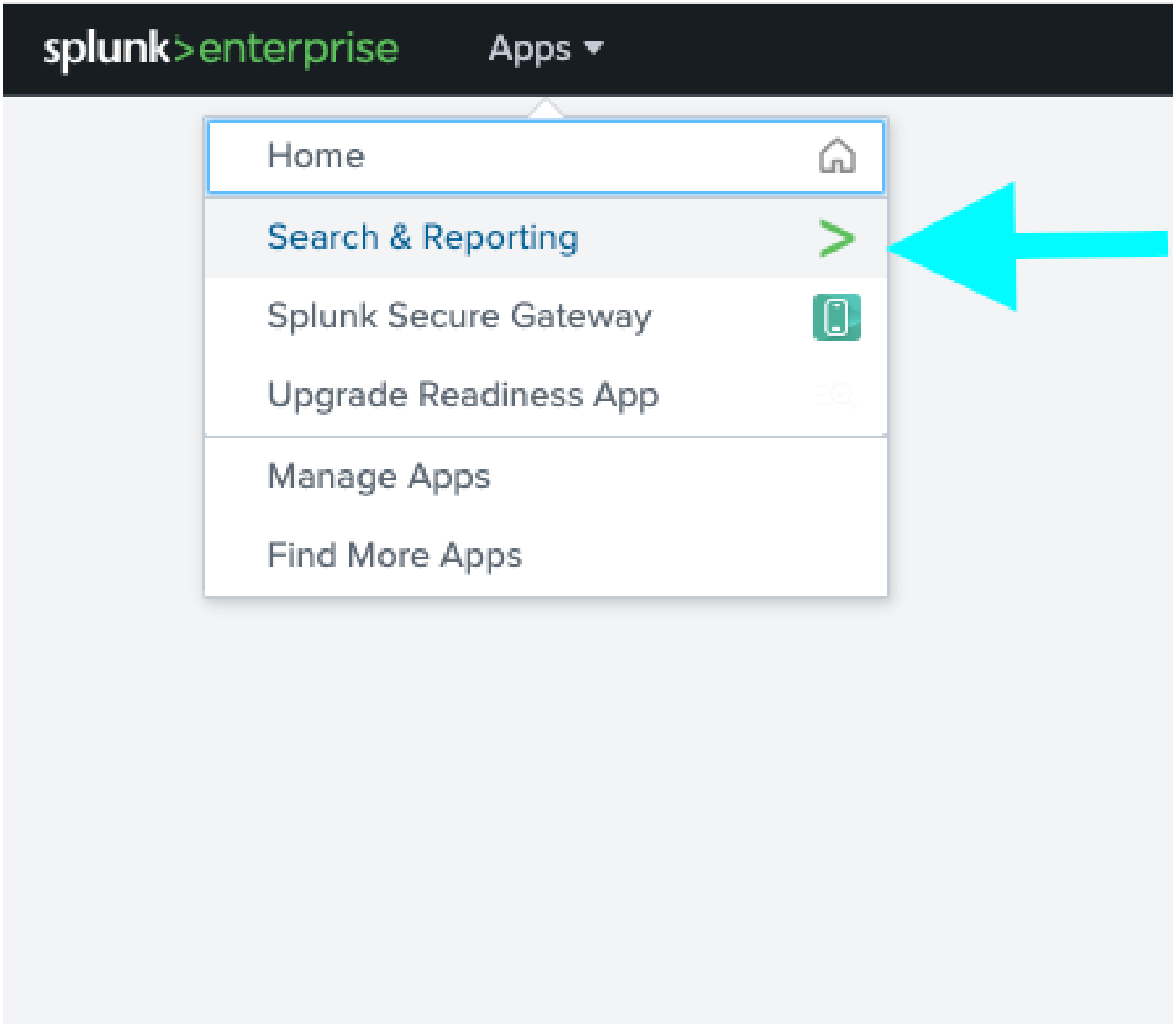
```
user@examplehost:~# chmod 600/opt/splunk/etc/auth/splunkweb.cer
```

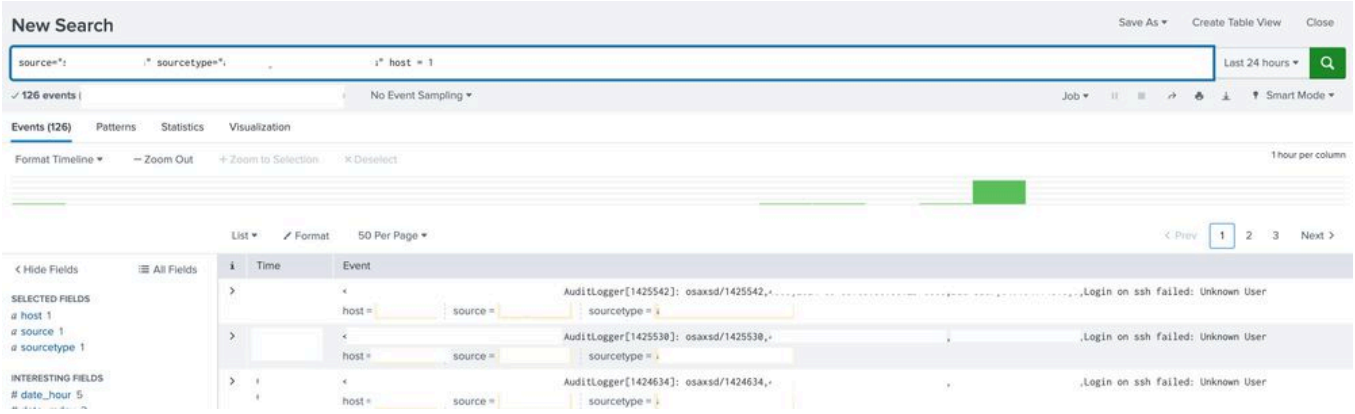
Étape 7 : créez un nouveau fichier input.conf.

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



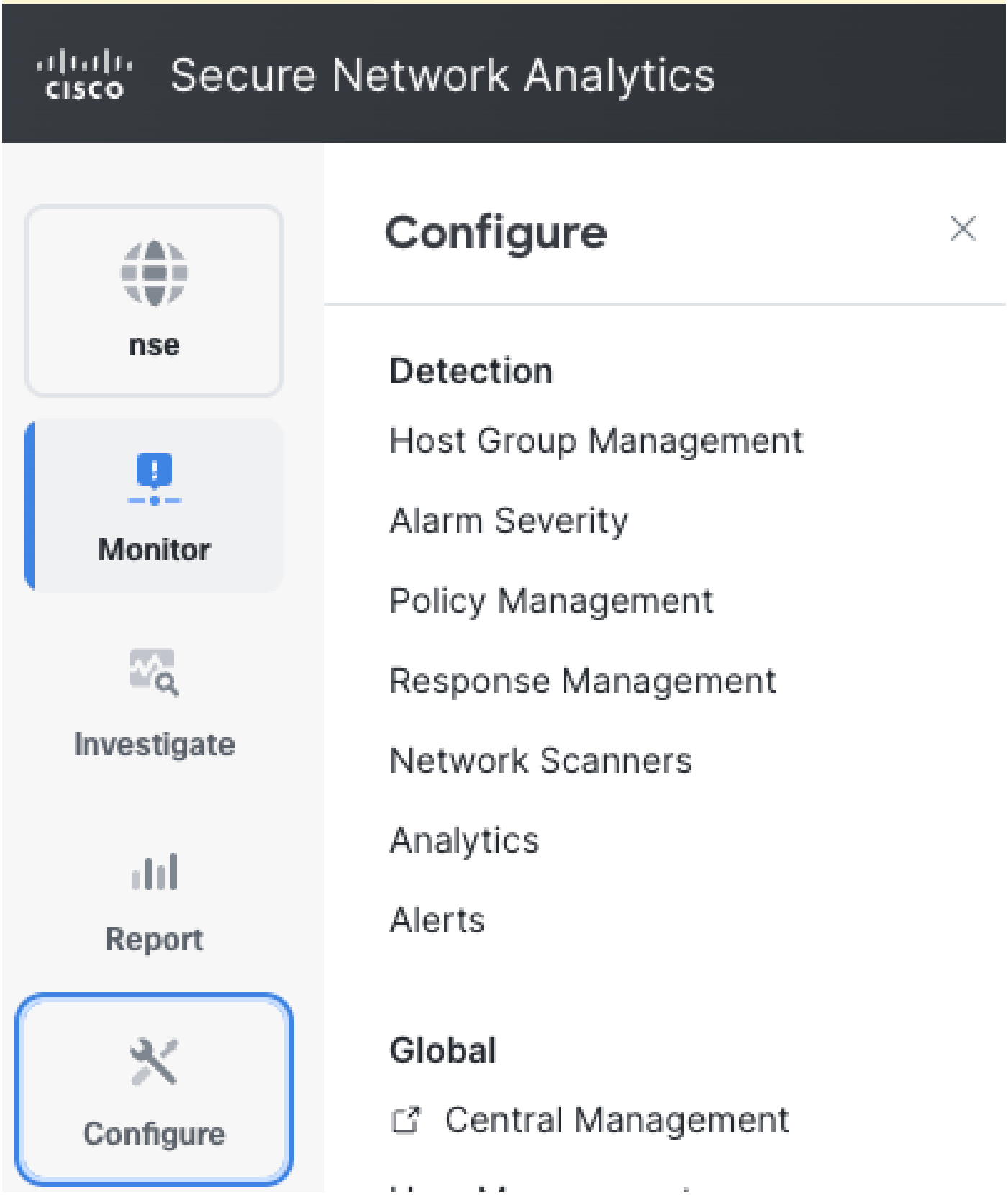
Étape 8 : Vérifiez les syslogs à l'aide de la recherche.



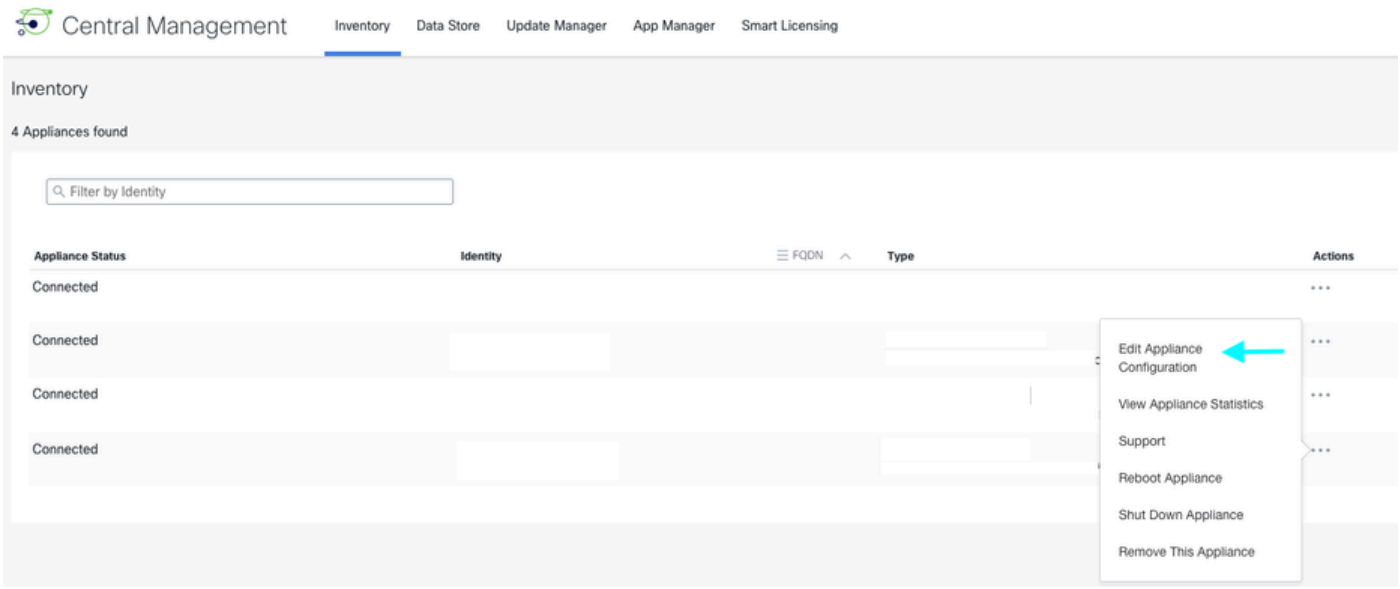


3.Configurez la destination du journal d'audit sur SNA

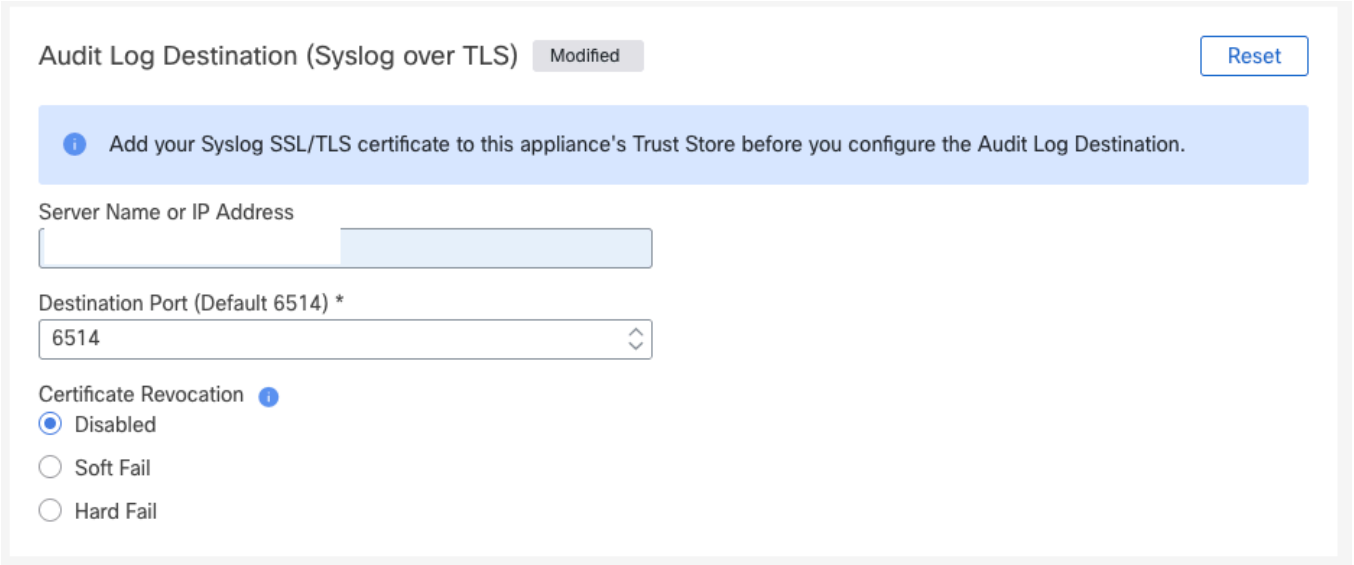
Étape 1 : Connectez-vous à l'interface utilisateur de SMC. Naviguez jusqu'à Configure > Central Management.



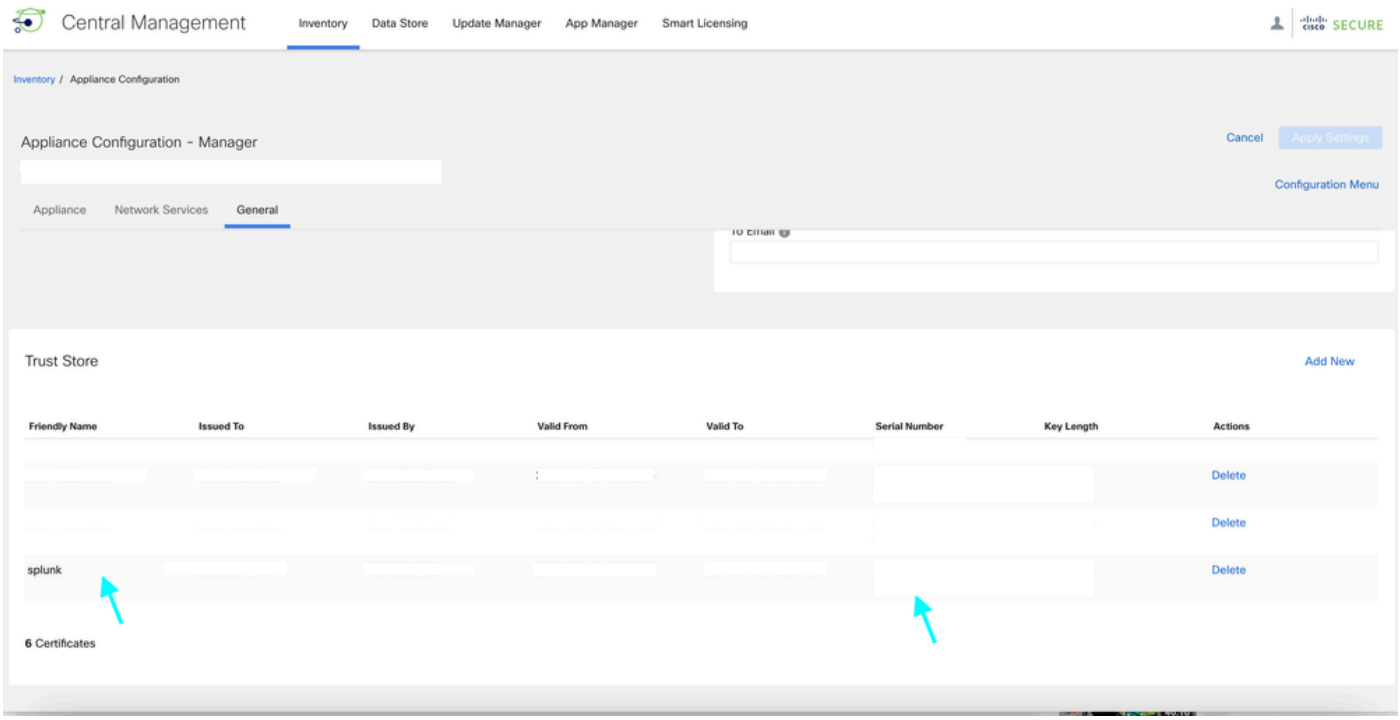
Étape 2 : Cliquez sur l'icône de points de suspension de l'appliance SNA souhaitée et sélectionnez Modifier la configuration de l'appliance.



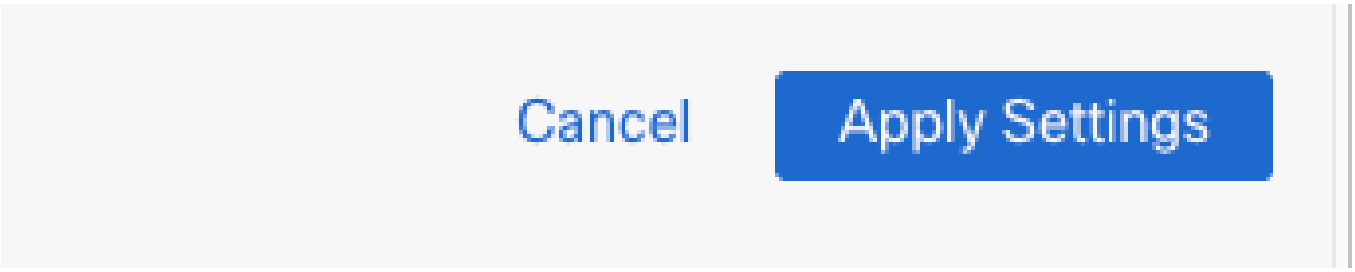
Étape 3 : Accédez à l'onglet Services réseau et entrez les détails de la destination du journal d'audit (Syslog sur TLS).



Étape 4 : Accédez à l'onglet Général, faites défiler jusqu'en bas. Cliquez sur Ajouter nouveau pour télécharger le certificat Splunk créé précédemment nommé server_cert.pem.

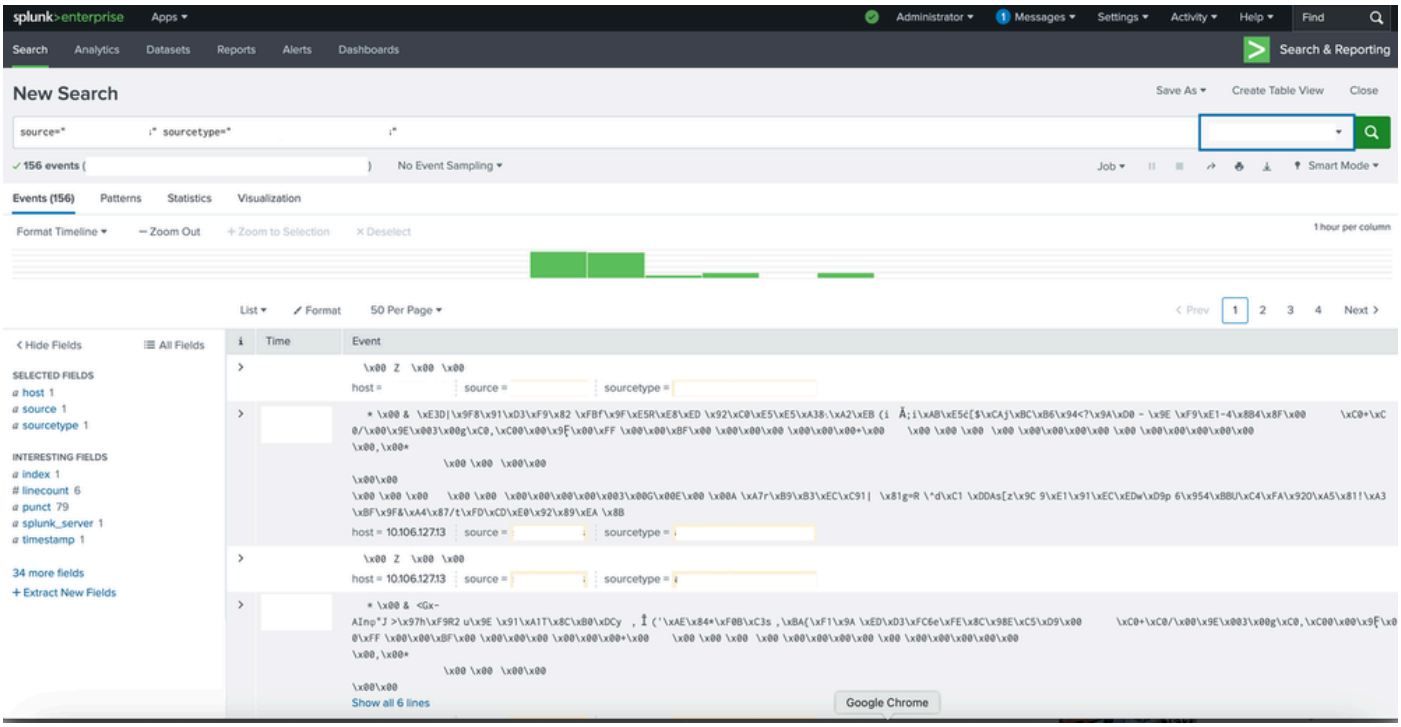


Étape 5 : Cliquez sur Apply settings.



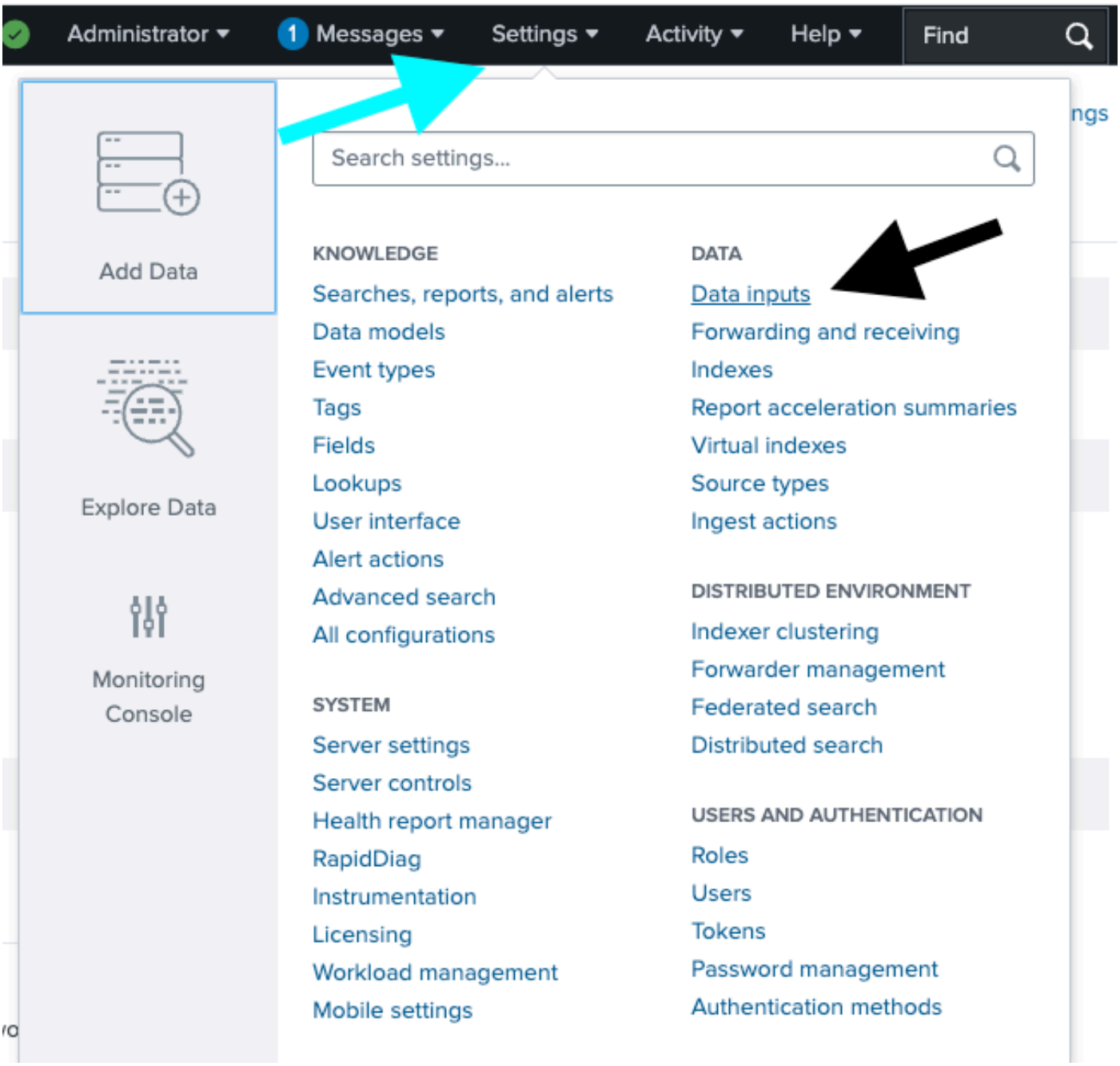
Dépannage

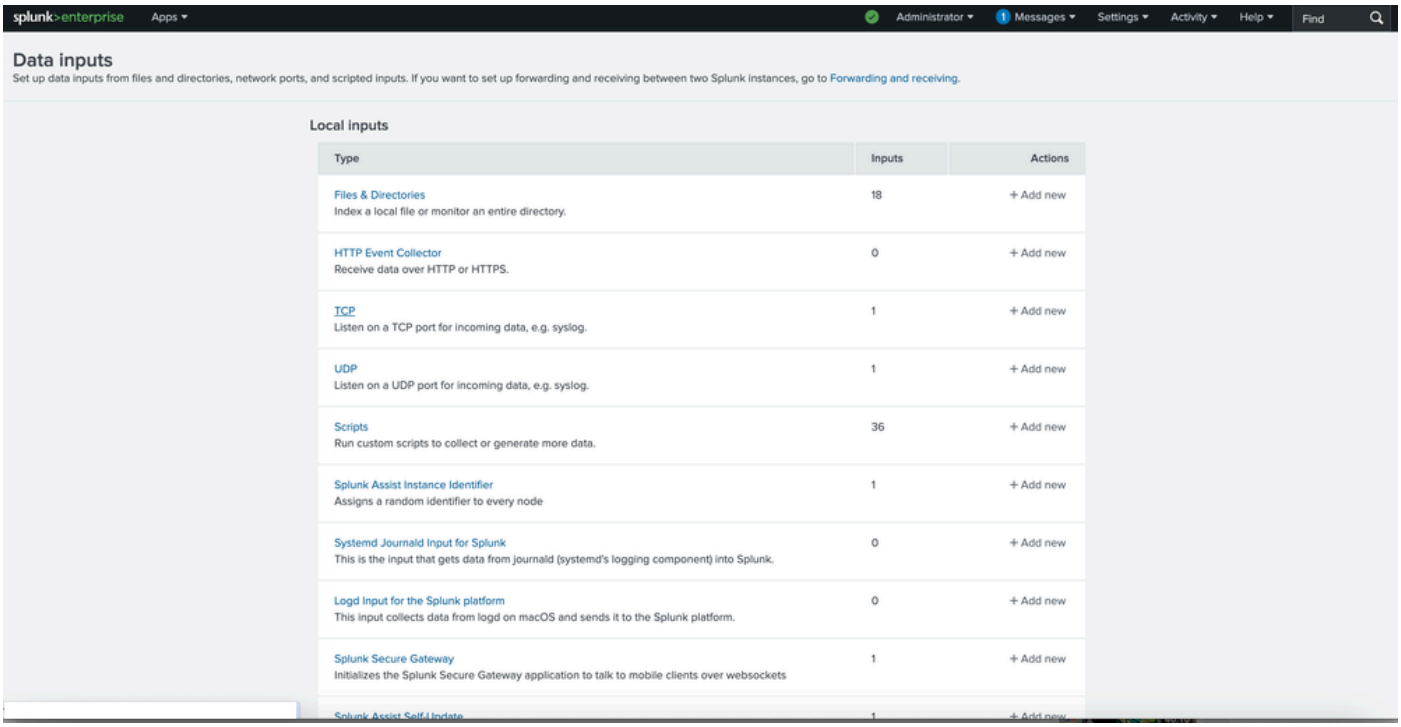
Il pourrait y avoir du charabia complet qui s'affiche lors d'une recherche.

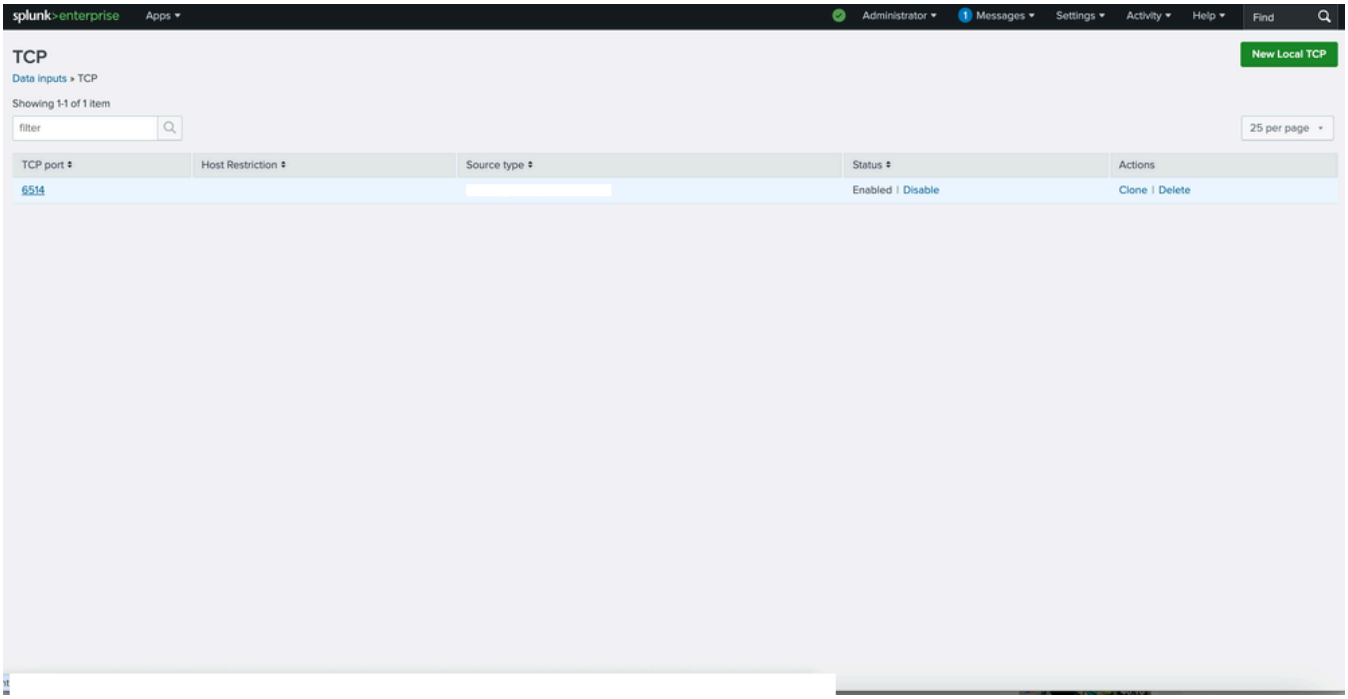


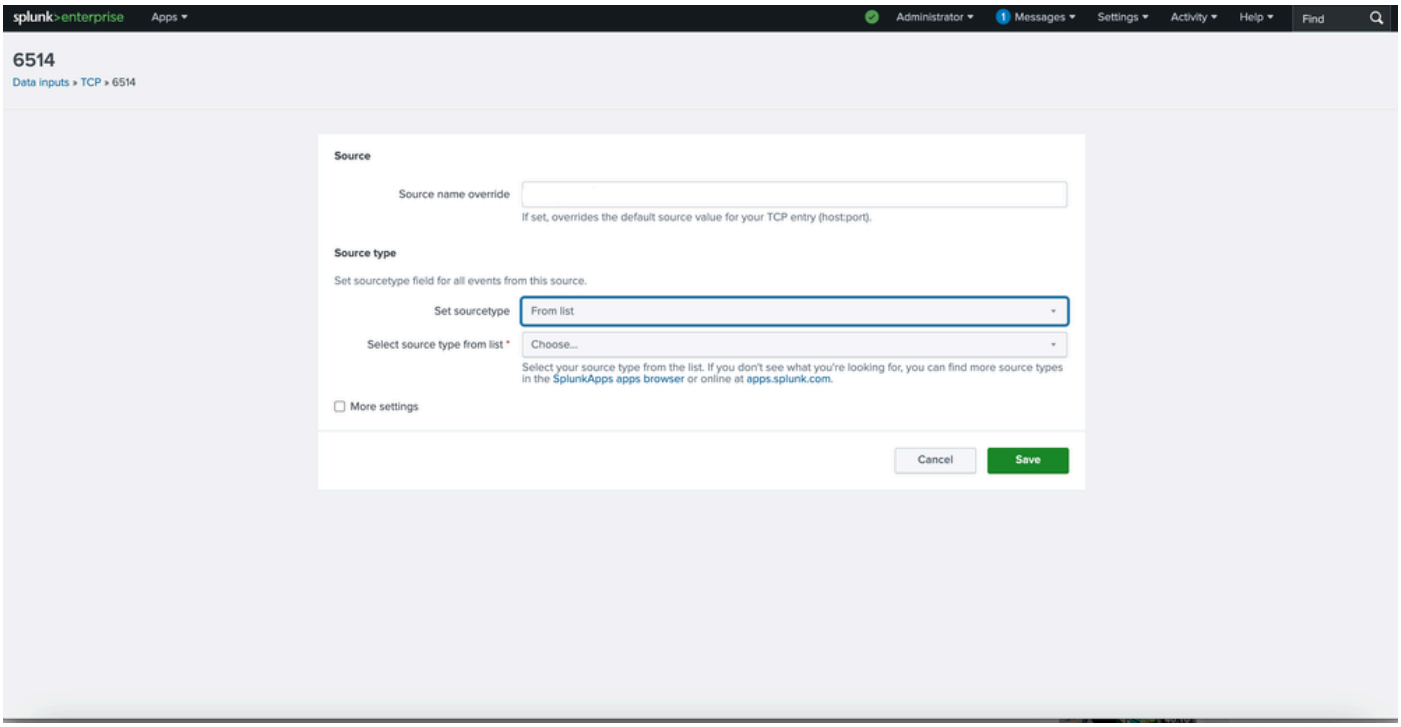
Solution :

Mappez l'entrée à son type de source correct.


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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.