تكوين إدارة الاستجابة لإرسال أحداث syslog إلى SPLUNK

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين ميزة "إدارة إستجابة التحليلات الآمنة" لإرسال الأحداث عبر syslog إلى جهة خارجية مثل Splunk.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

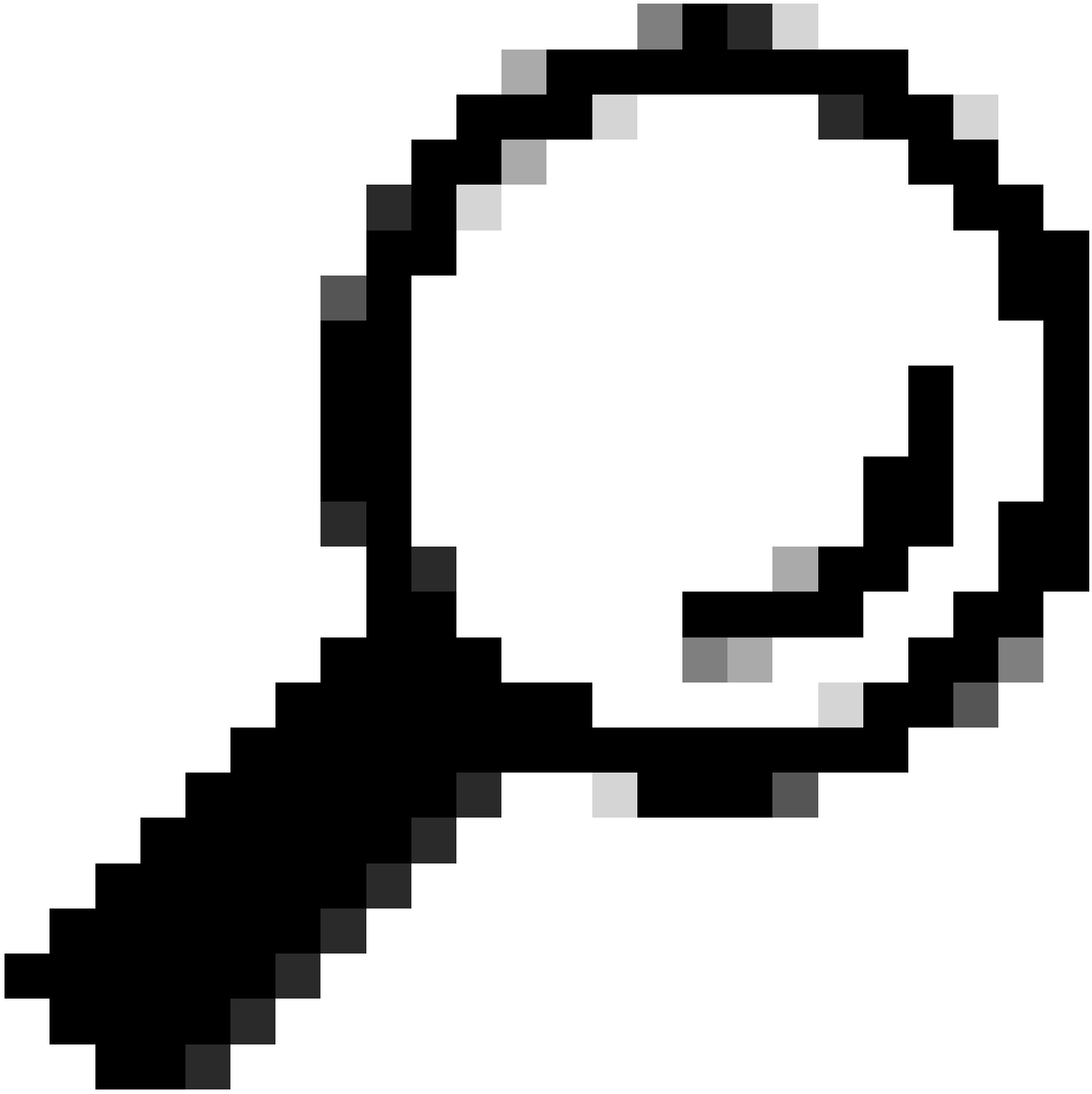
- إدارة الاستجابة لتحليلات الشبكة الآمنة.
- Splunk Syslog

المكونات المستخدمة

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

- نشر تحليلات الشبكة الآمنة (SNA) التي تحتوي على جهاز Manager واحد على الأقل وجهاز مجمع تدفق واحد.
- تم تثبيت خادم Splunk والوصول إليه عبر 443 منفذا.

تكوين syslog على SNA عبر UDP 514 أو المنفذ المحدد المخصص



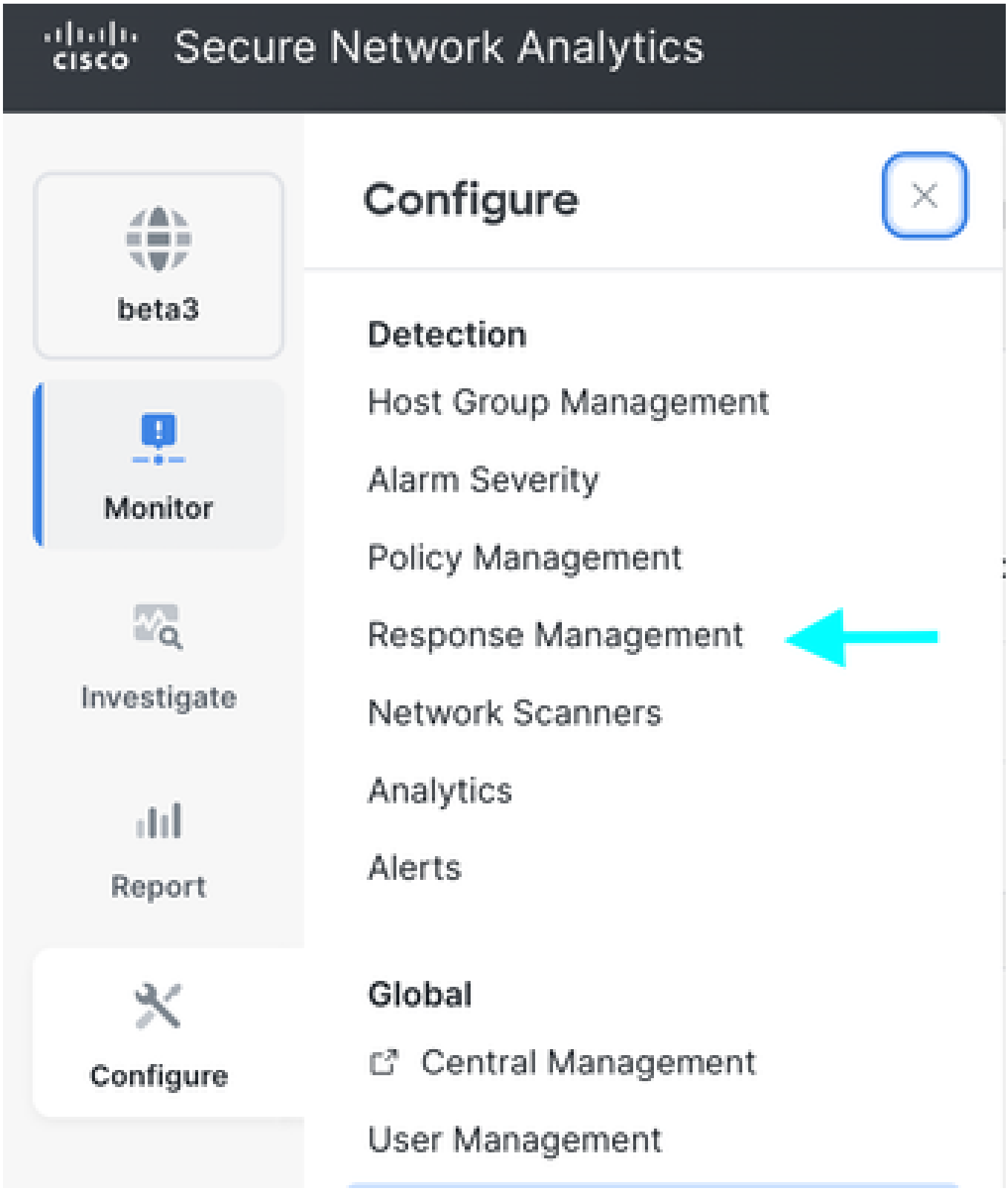
تلميح:تأكد من أن UDP/514،TCP/6514 أو أي منفذ مخصص تختاره لـ syslog مسموح به على أي جدران حماية أو أجهزة وسيطة بين SNA و Splunk.

إدارة الاستجابة عبر نظام SNA الإصدار 1.SNA

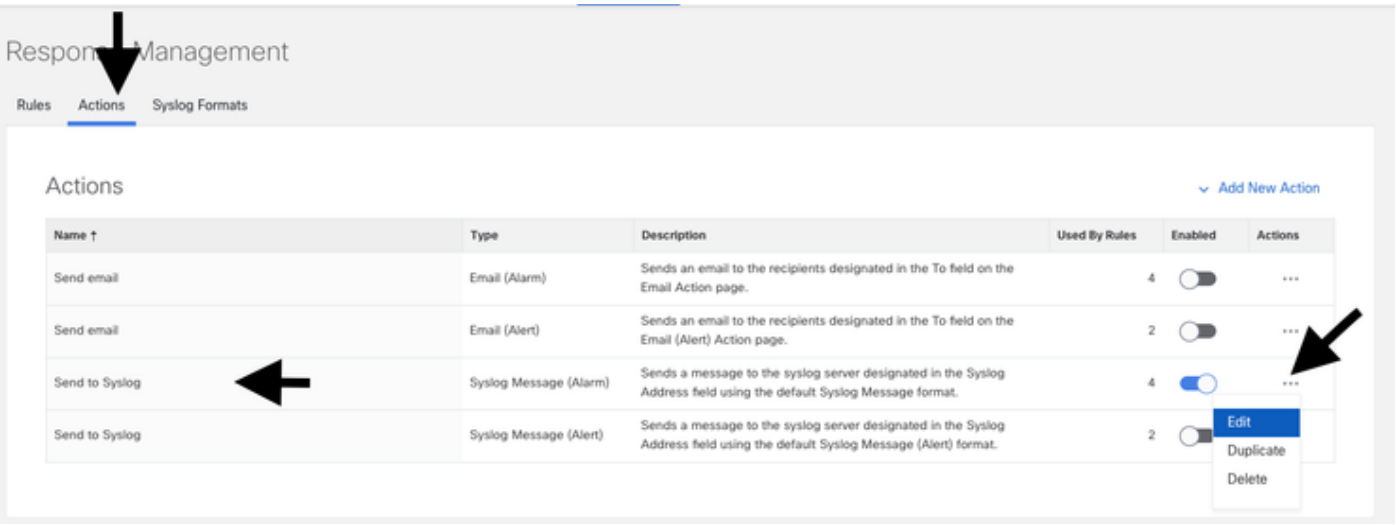
يمكن إستخدام مكون إدارة الاستجابة الخاص بالتحليلات الآمنة (SA) لتكوين القواعد والإجراءات ووجهات syslog.

يجب تكوين هذه الخيارات للإرسال/إعادة توجيه تنبيهات Secure Analytics إلى وجهات أخرى.

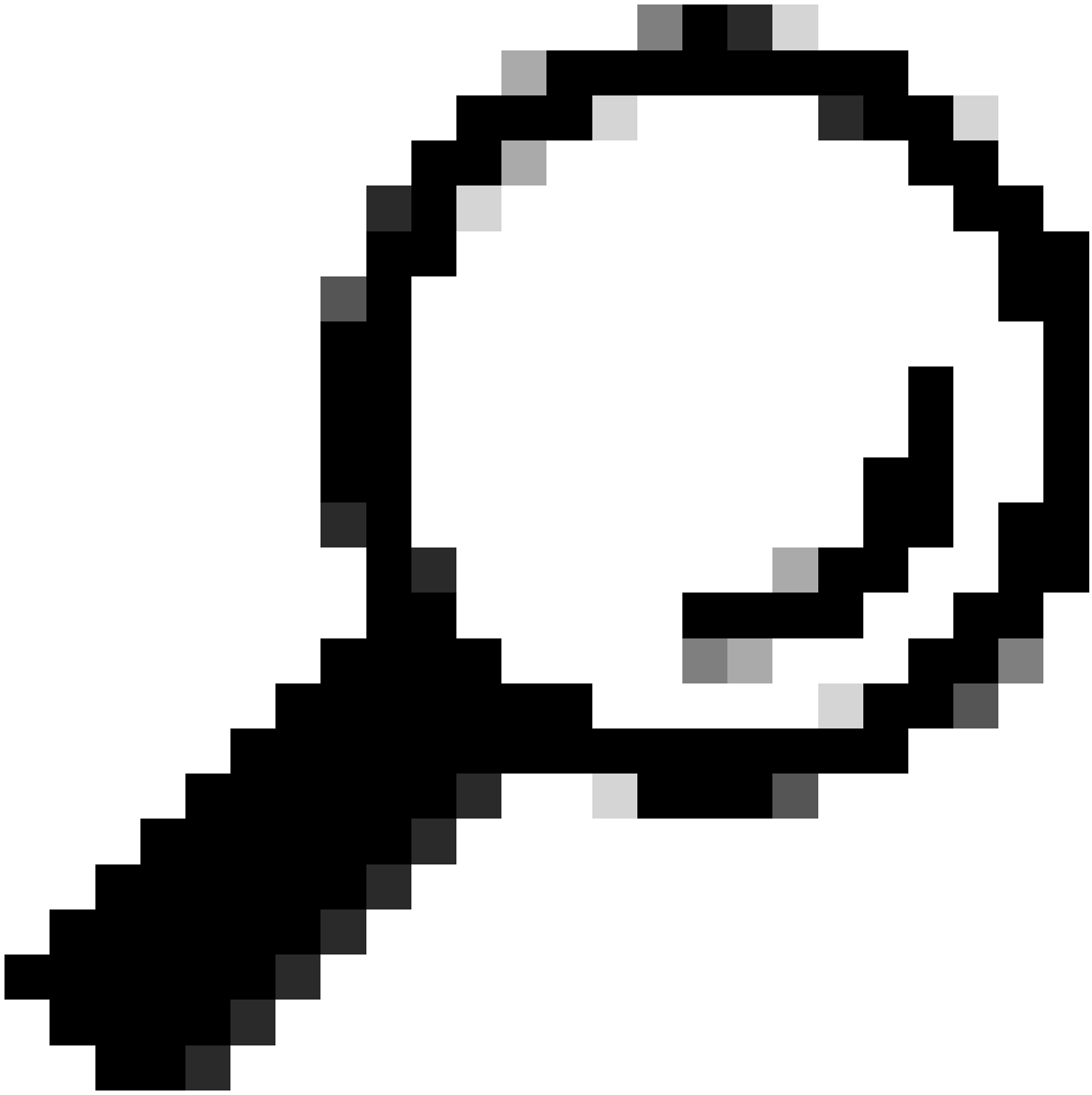
الخطوة 1: قم بتسجيل الدخول إلى جهاز إدارة SA وانتقل إلى التكوين > إدارة إستجابة الكشف.



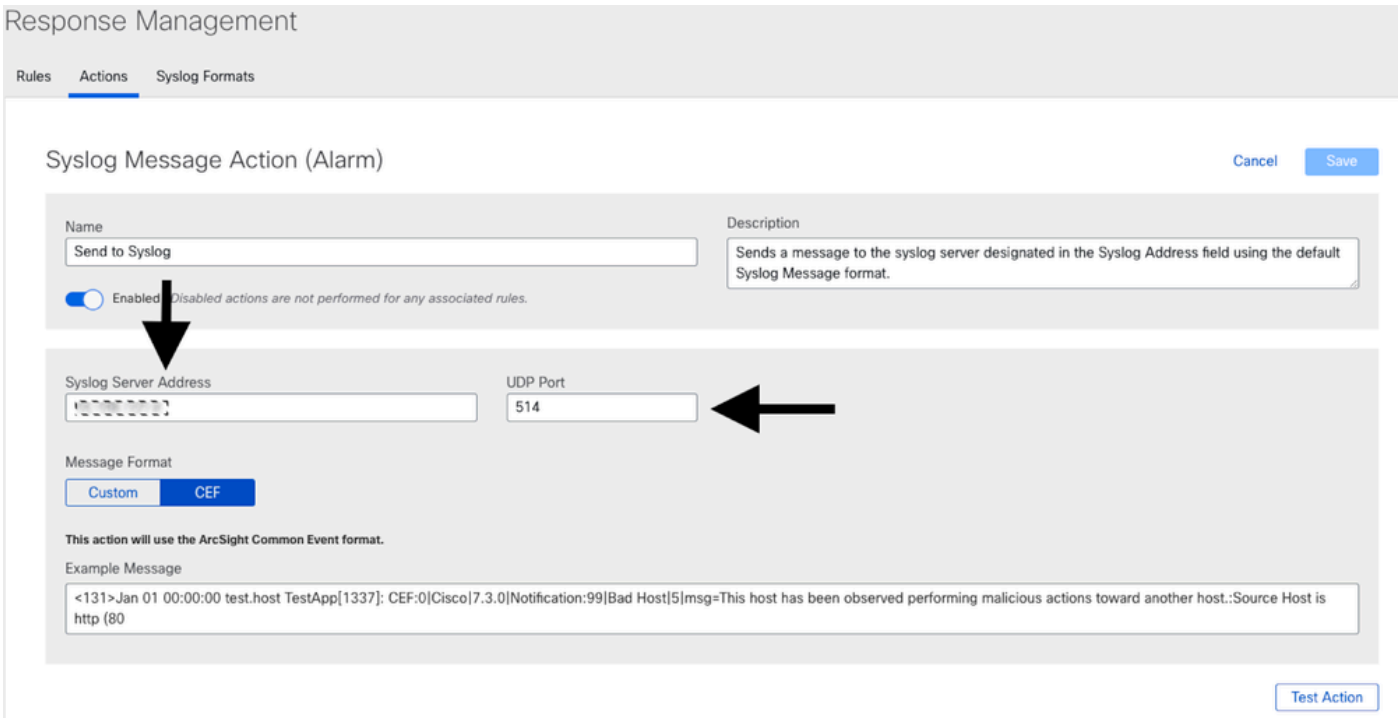
الخطوة 2: في الصفحة الجديدة، انتقل إلى علامة التبويب إجراءات، حدد مكان عنصر السطر إرسال إلى syslog الافتراضي وانقر فوق علامة الحذف (...) في عمود الإجراء، ثم تحرير.



الخطوة 3: دخلت الغاية عنوان في ال syslog نادل عنوان مجال، واولجهة ب يستلم ميناء في ال UDP ميناء مجال. في تنسيق الرسالة حدد CEF.
الخطوة 4: عند الإكمال، انقر زر حفظ الأزرق في الزاوية العليا اليمنى.



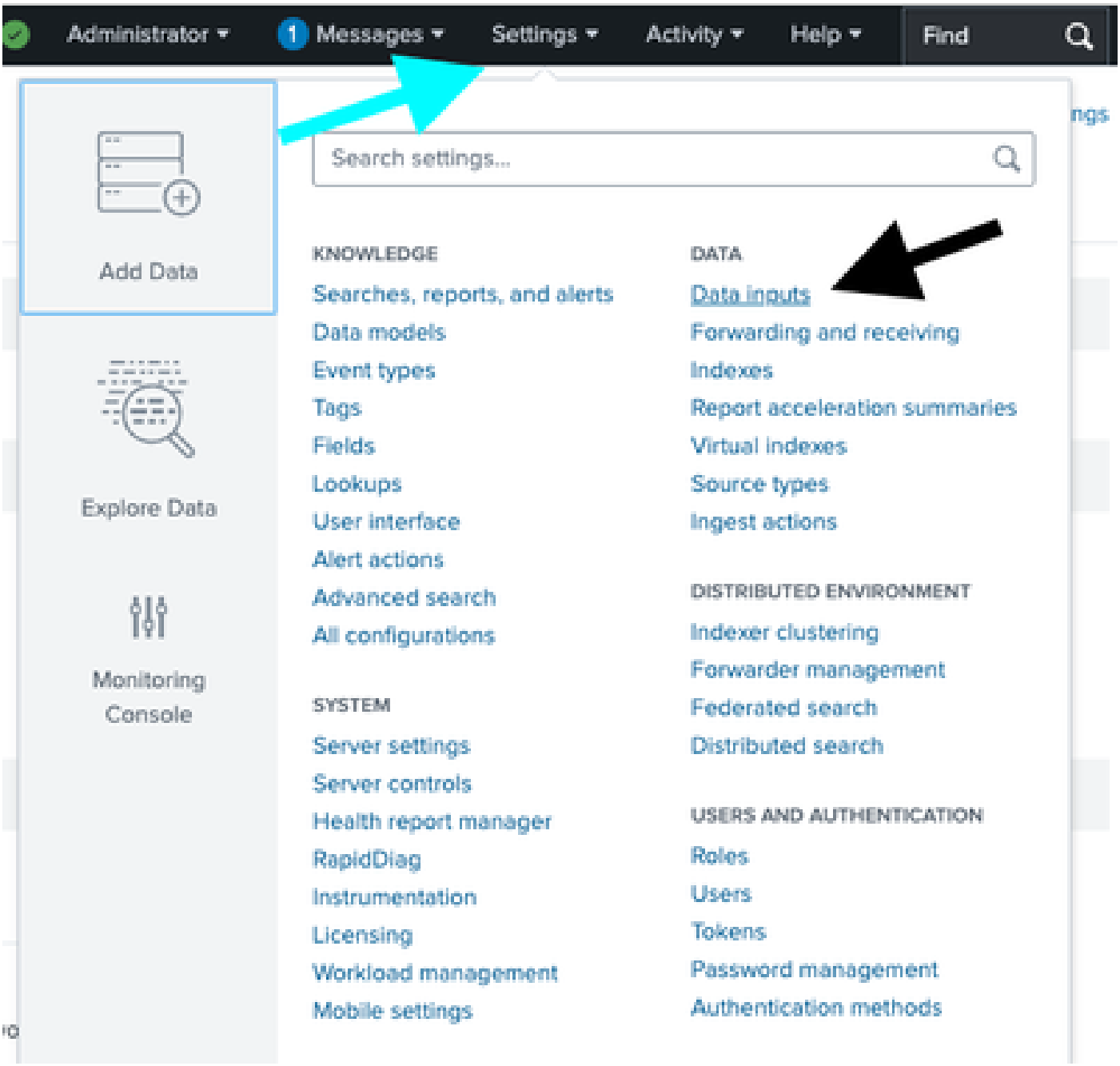
تلميح: التقصير UDP ميناء ل syslog 514



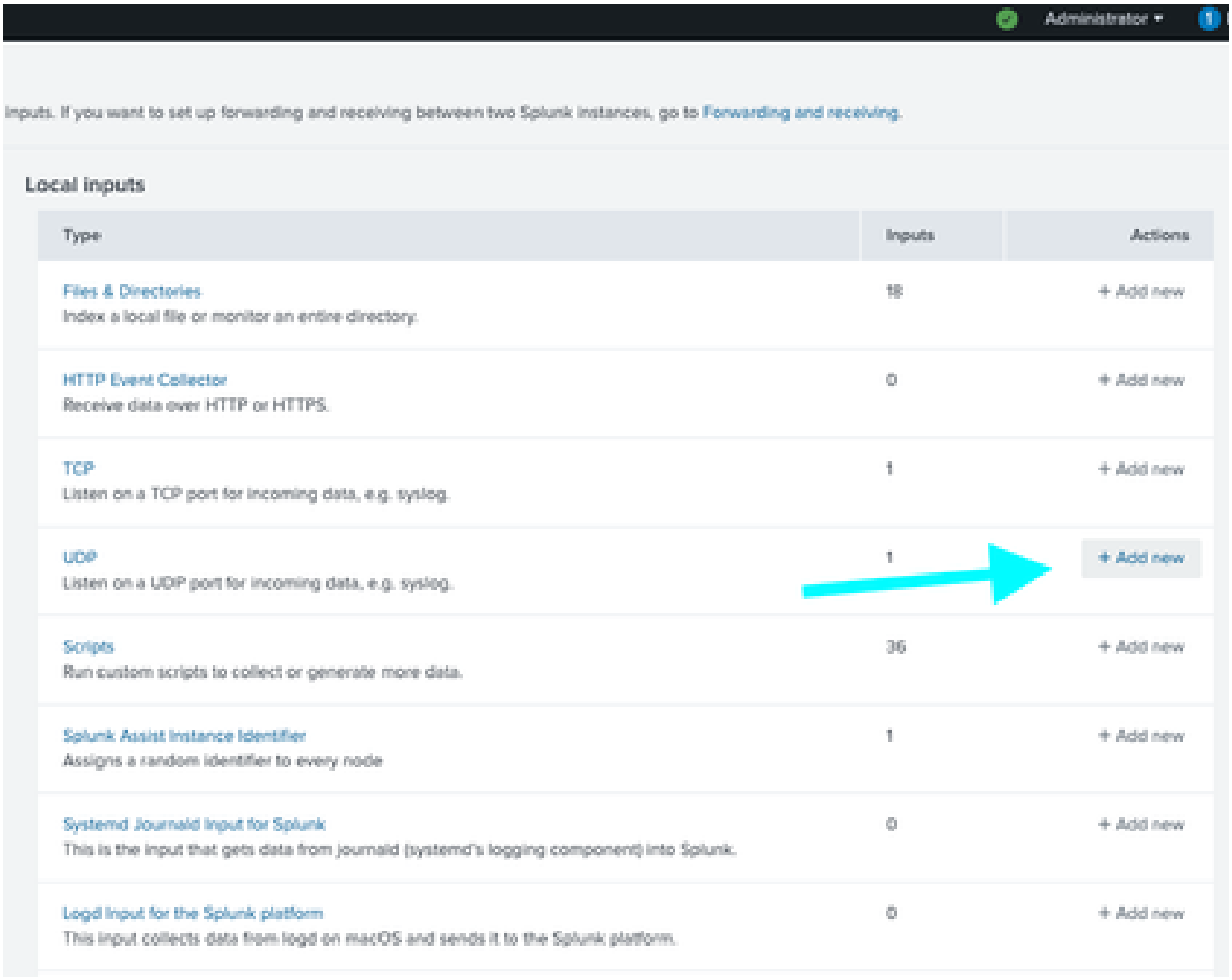
2.يشكل Splunk أن يستلم SNA syslogs عبر UDP ميناء

بعد تطبيق التغييرات الخاصة بك على واجهة مستخدم ويب لإدارة تحليلات الشبكة الآمنة، يجب تكوين إدخال البيانات في Splunk.

الخطوة 1: قم بتسجيل الدخول إلى Splunk وانتقل إلى الإعدادات > إضافة بيانات > إدخالات بيانات البيانات.

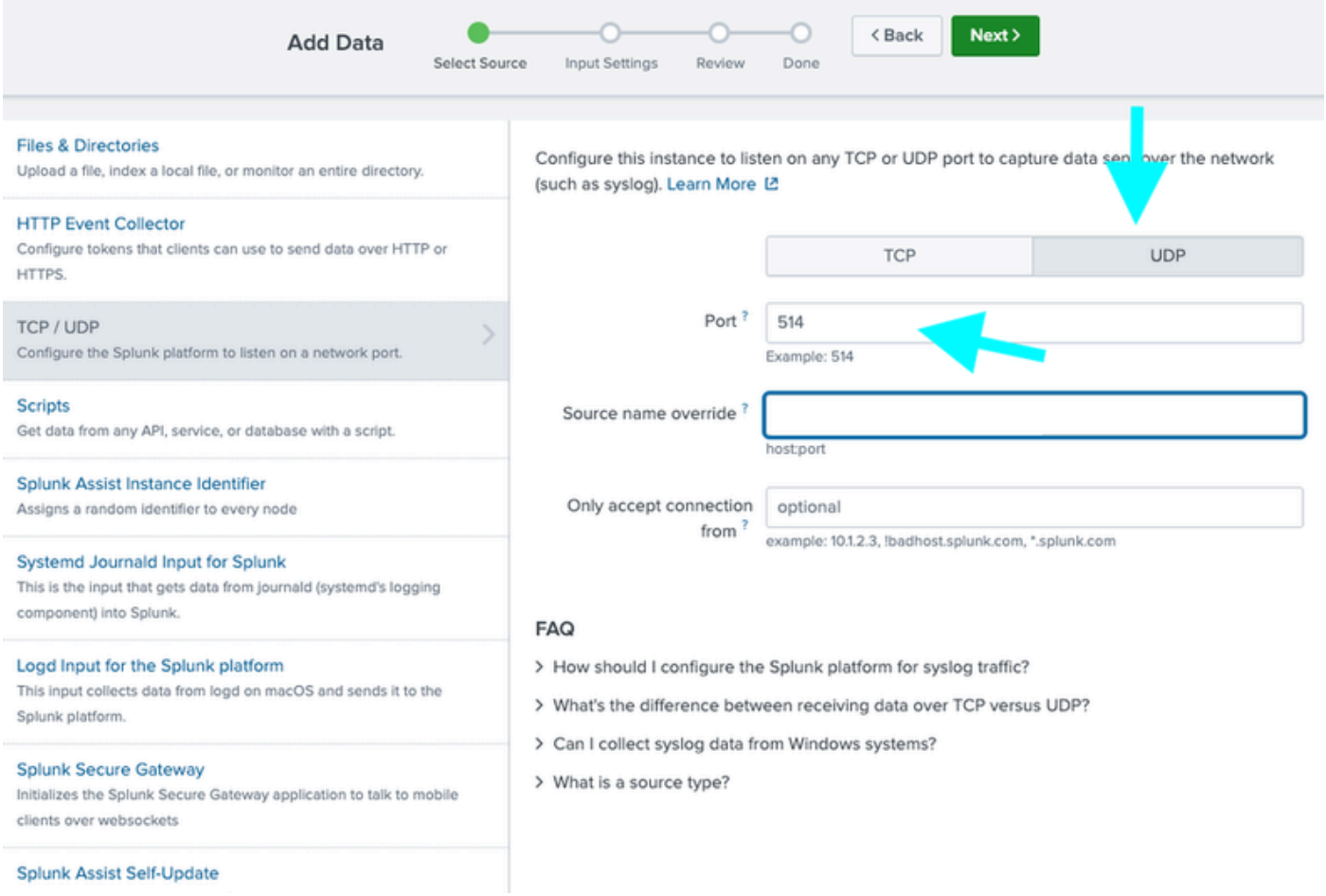


الخطوة 2: حدد موقع سطر UDP وحدد +إضافة جديد.



الخطوة 3: في الصفحة الجديدة حدد UDP، دخلت ال يستلم ميناء مثل 514 في الميناء مجال.
الخطوة 4: في حقل تجاوز اسم المصدر، أدخل desired name of source.

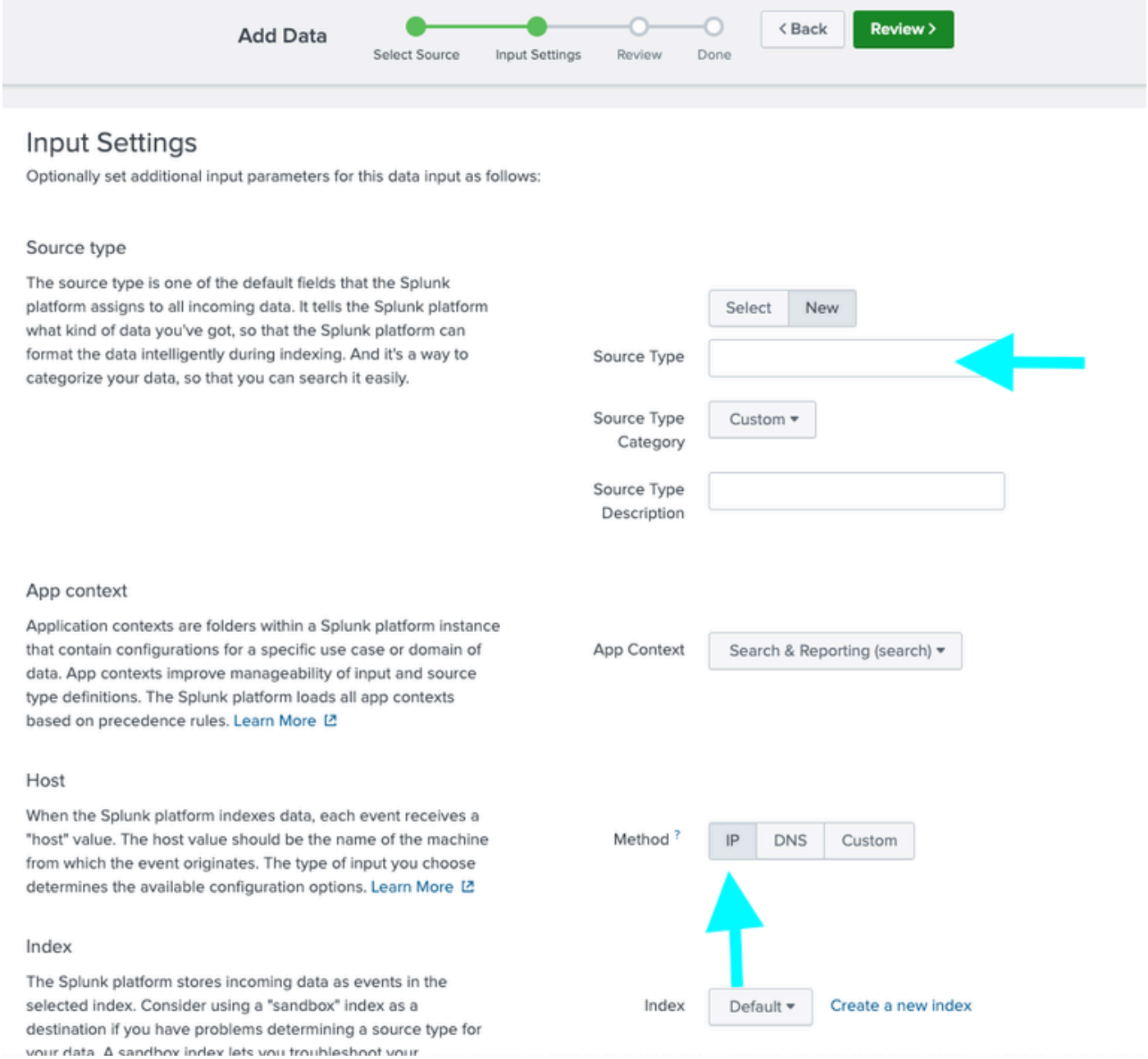
الخطوة 5: عند الانتهاء، انقر فوق الزر التالي للأخضر >الموجود أعلى النافذة.



الخطوة 6: في الصفحة التالية، قم بالتبديل إلى خيار جديد حدد مكان حقل نوع المصدر وأدخل desired source .

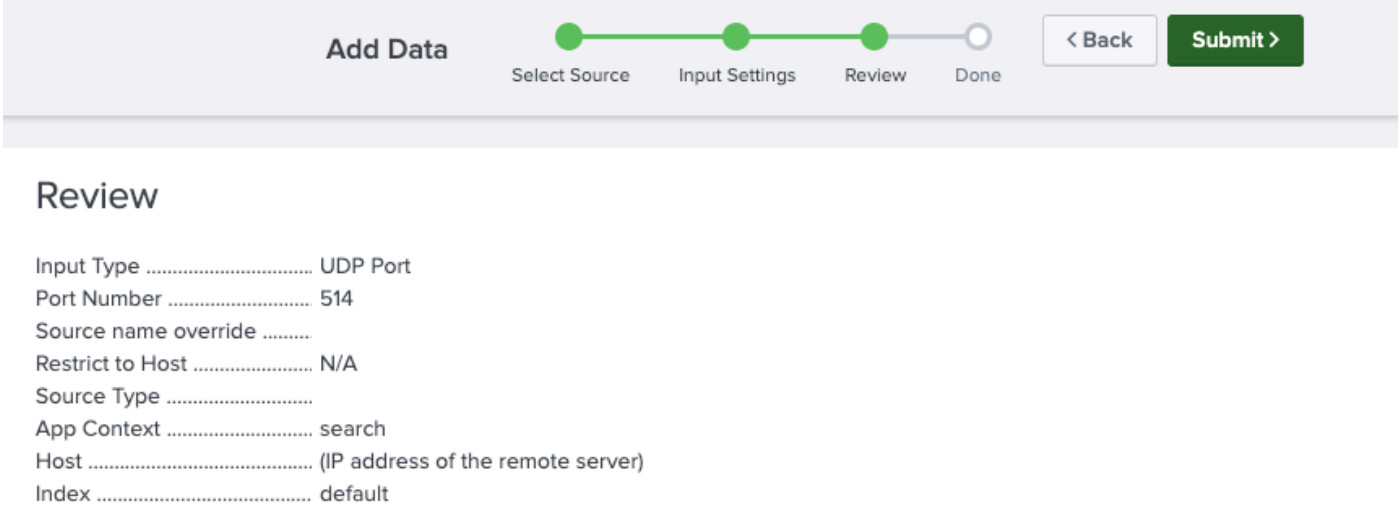
الخطوة 7: حدد IP للأسلوب.

الخطوة 8: انقر فوق زر مراجعة > الأخضر الموجود أعلى الشاشة.

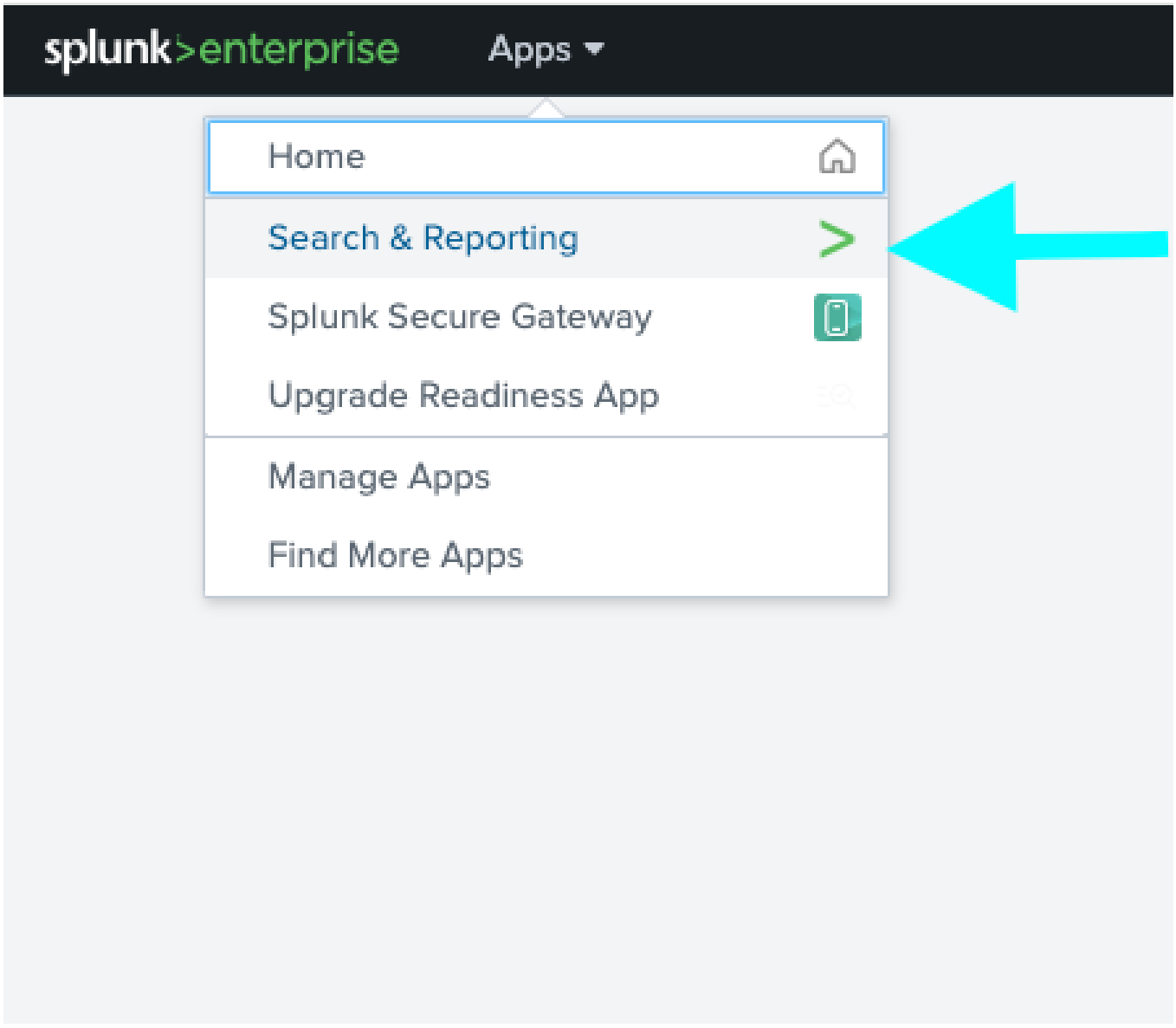


الخطوة 9: في الإطار التالي، راجع إعداداتك وحرر إذا لزم الأمر.

الخطوة 10: انقر فوق زر إرسال >الأخضر" الموجود أعلى الإطار بمجرد التحقق من صحته.

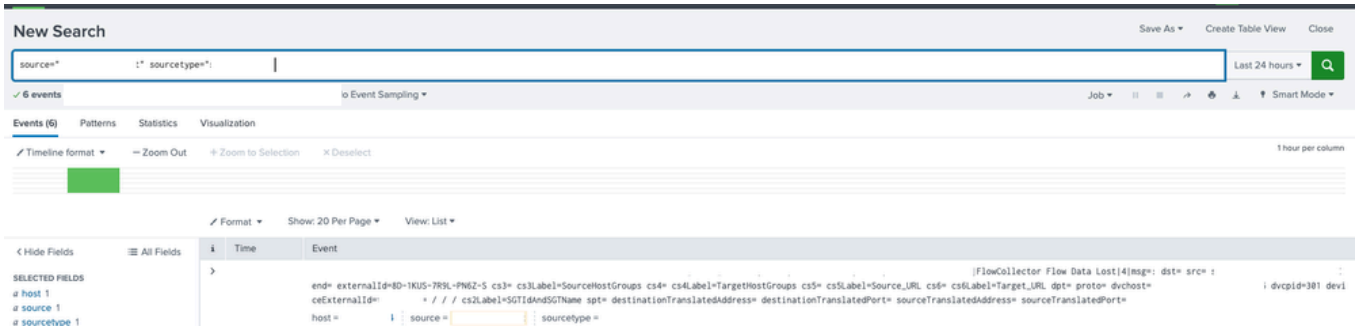


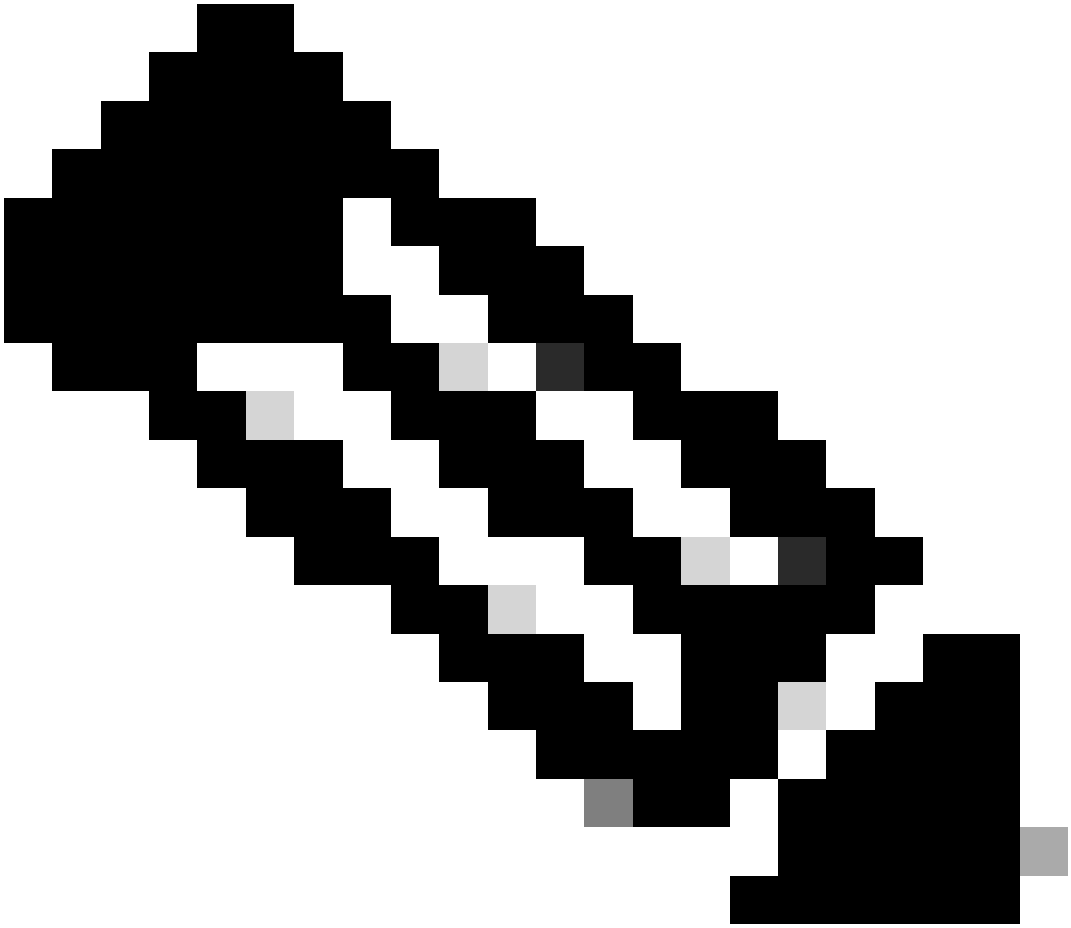
الخطوة 11: انتقل إلى تطبيقات > بحث وإعداد تقارير في واجهة مستخدم الويب.



الخطوة 12: في صفحة البحث، أستخدم عامل التصفيةsource="As_configured"

للبحث عن السجلات التي تم تلقيها."sourcetype="As_configured



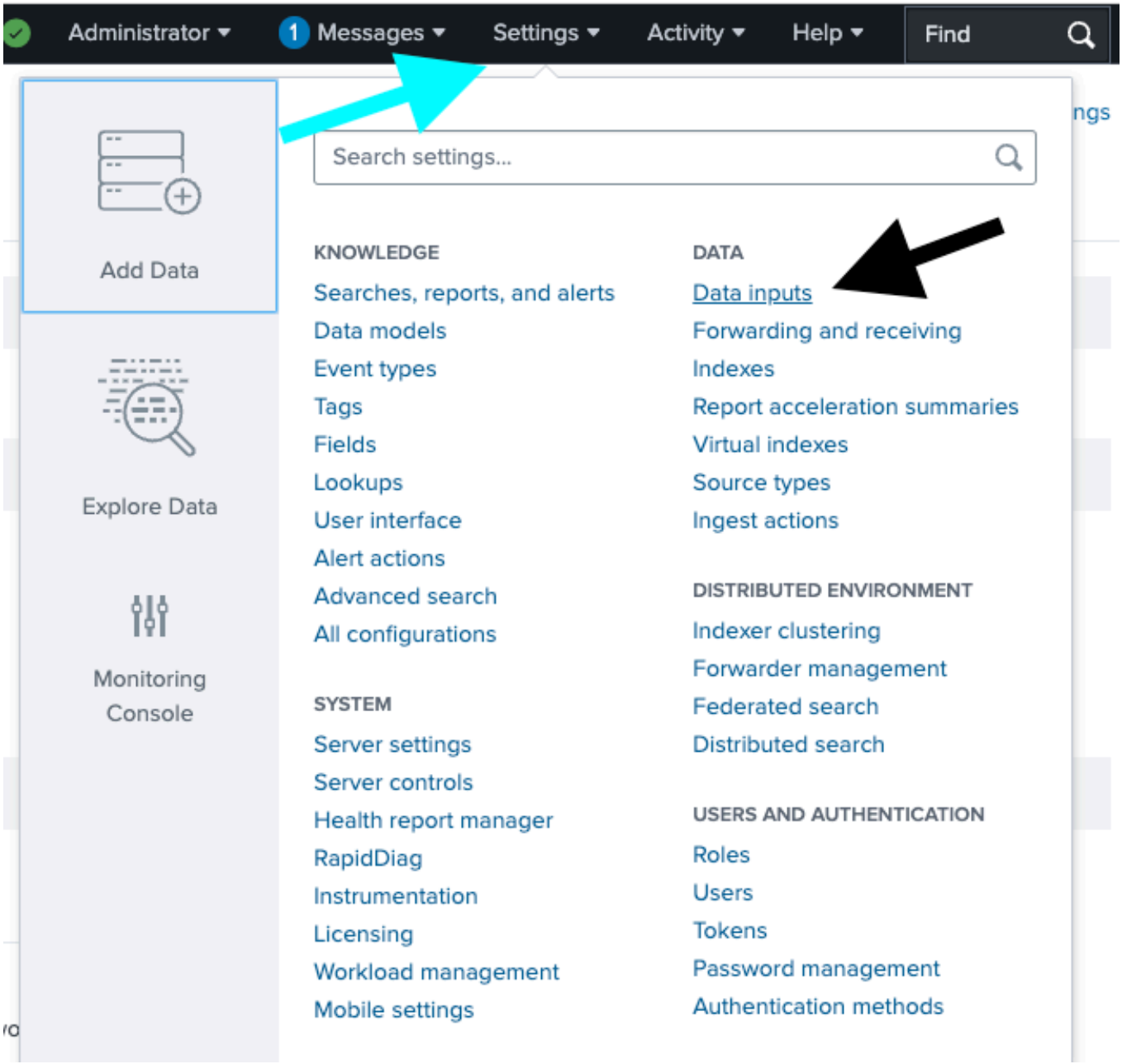


ملاحظة: للحصول على المصدر، راجع الخطوة 4
للحصول على source_type راجع الخطوة 6

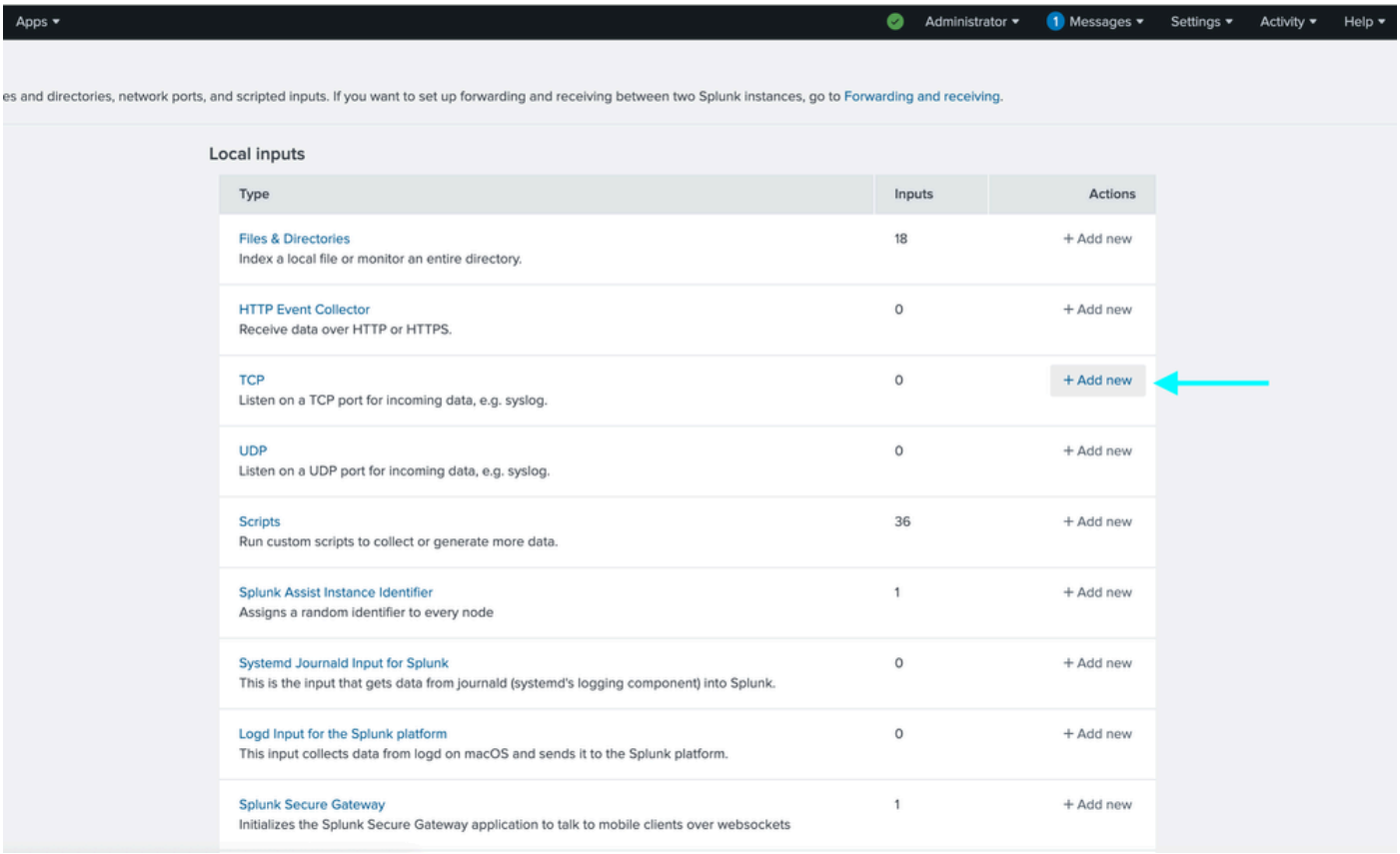
تكوين syslog على SNA عبر TCP منفذ 6514 أو منفذ مخصص محدد

1.تكوين Splunk لتلقي سجلات تدقيق SNA عبر منفذ TCP

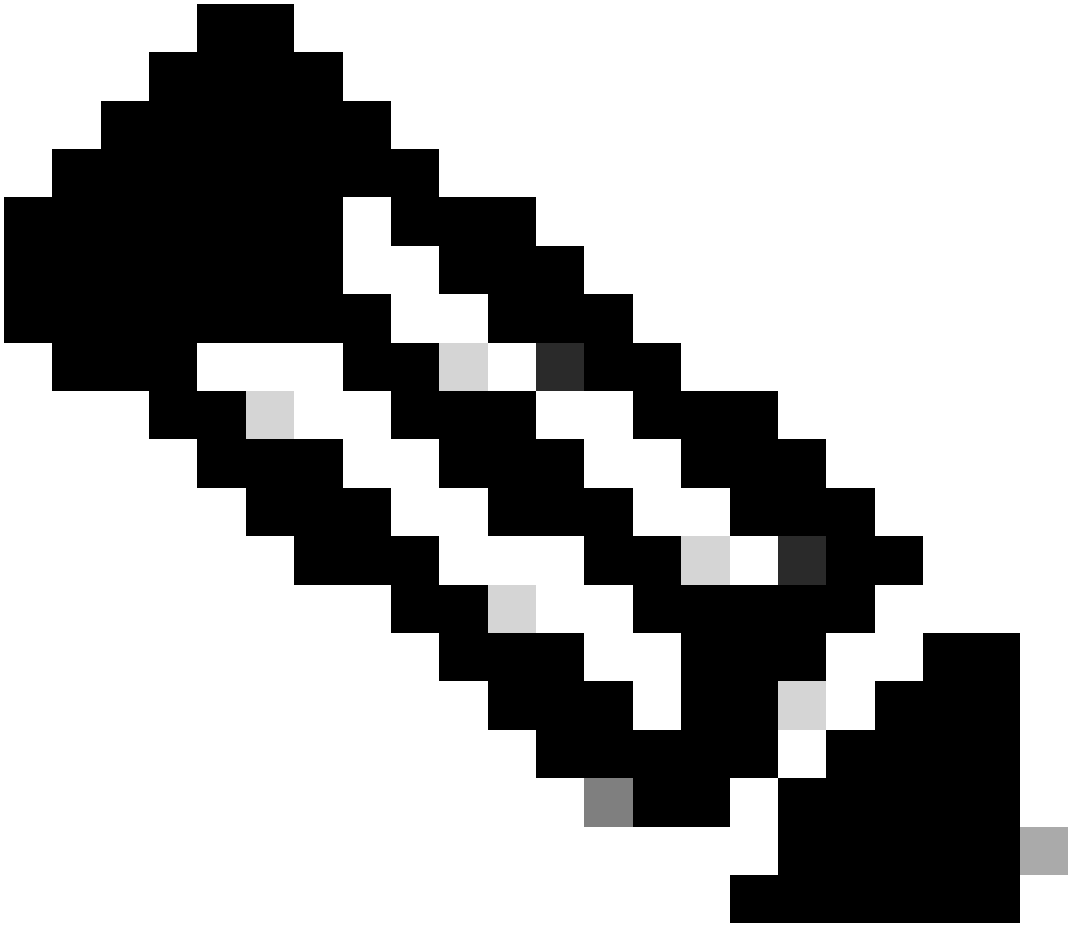
الخطوة 1: في واجهة مستخدم Splunk، انتقل إلى الإعدادات > إضافة بيانات > مدخلات بيانات البيانات.



الخطوة 2: حدد موقع سطر TCP وحدد + إضافة جديد.

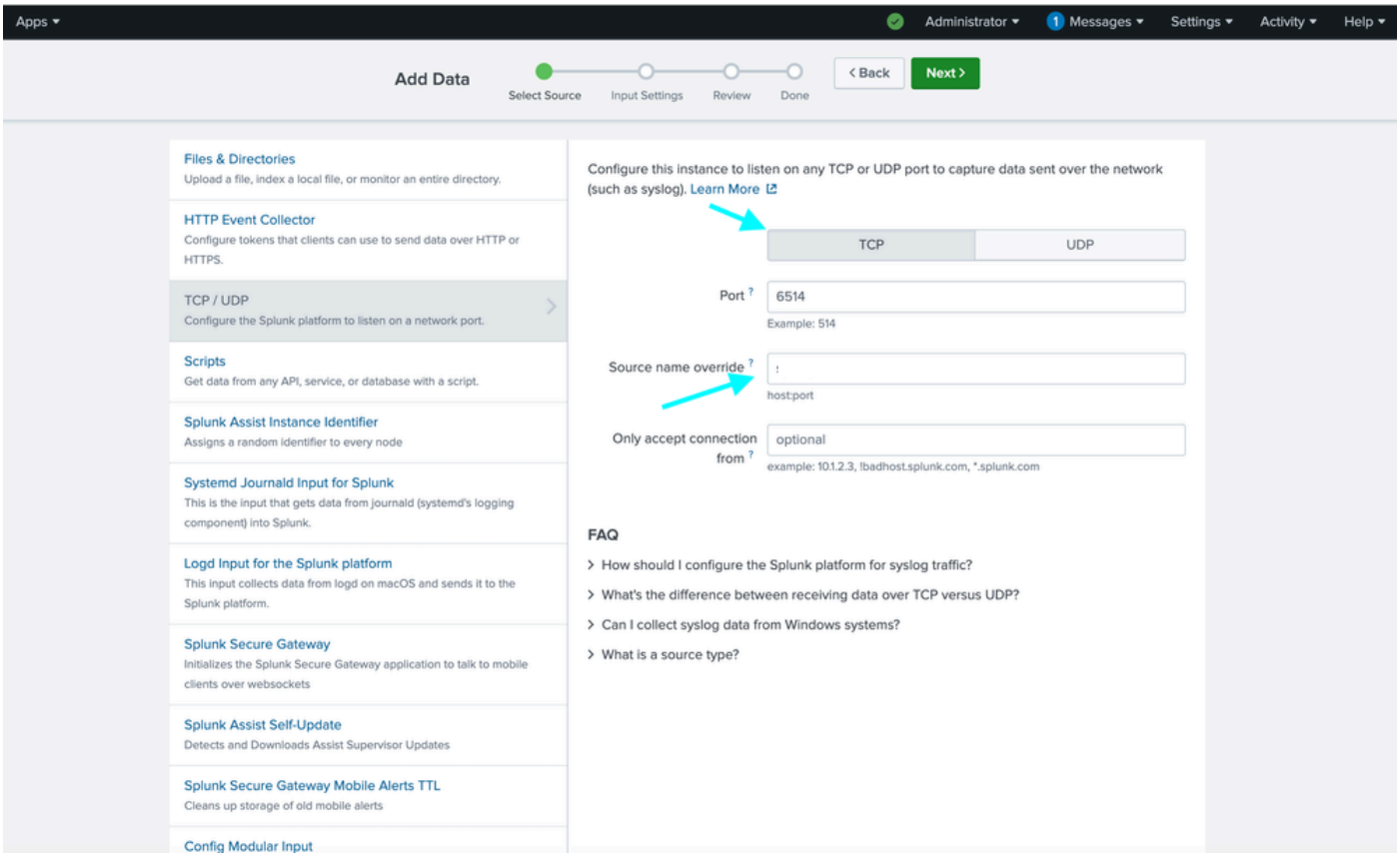


الخطوة 3: في النافذة الجديدة حدد TCP، أدخل منفذ الاستقبال المطلوب، في مثال صورة ميناء 6514، وأدخل "الاسم المرغوب" في حقل تجاوز اسم المصدر.



ملاحظة: TCP 6514 تقصير ميناء ل syslog عبر TLS

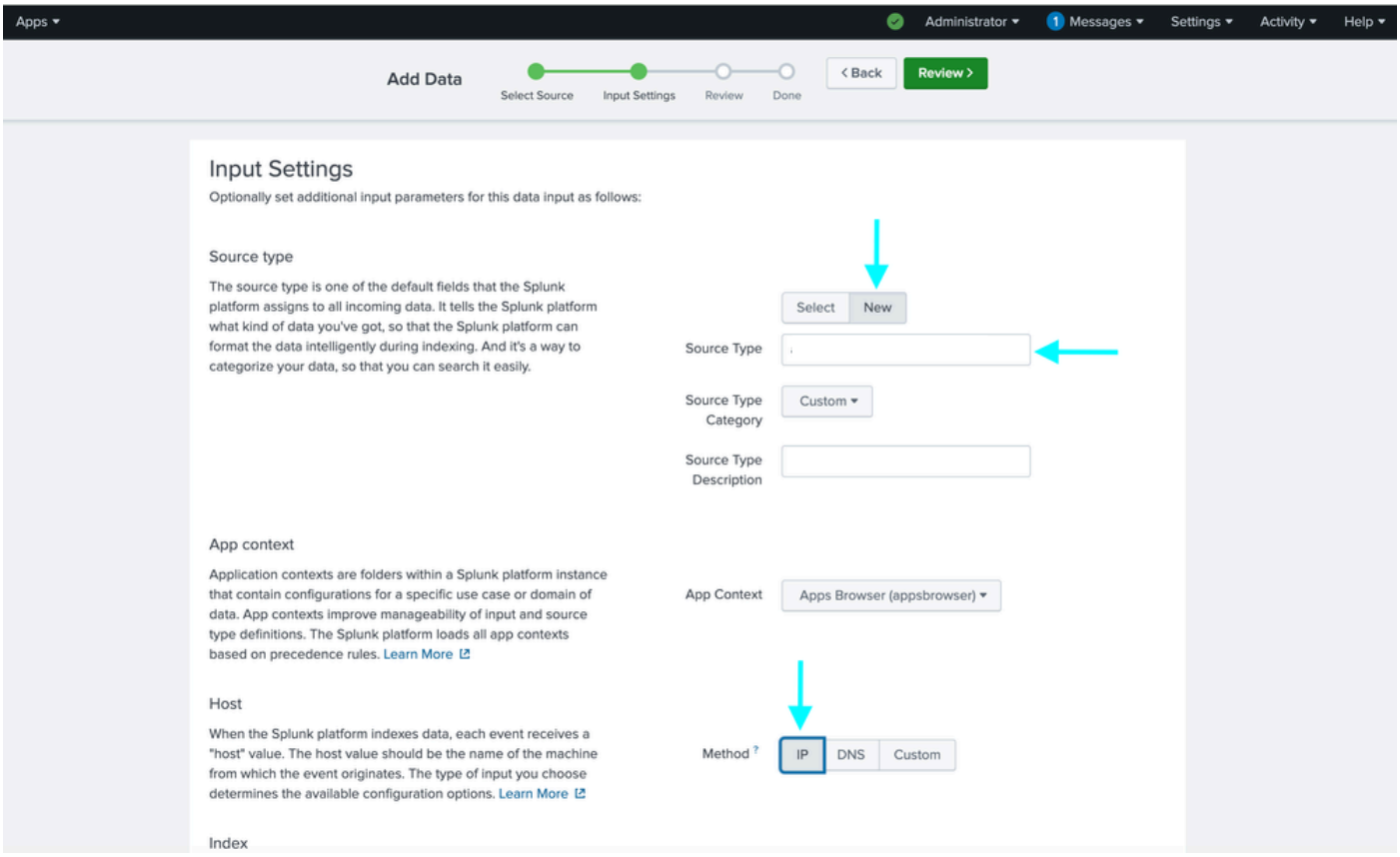
الخطوة 4: عند الانتهاء، انقر فوق الزر التالي للأخضر >الموجود أعلى النافذة.



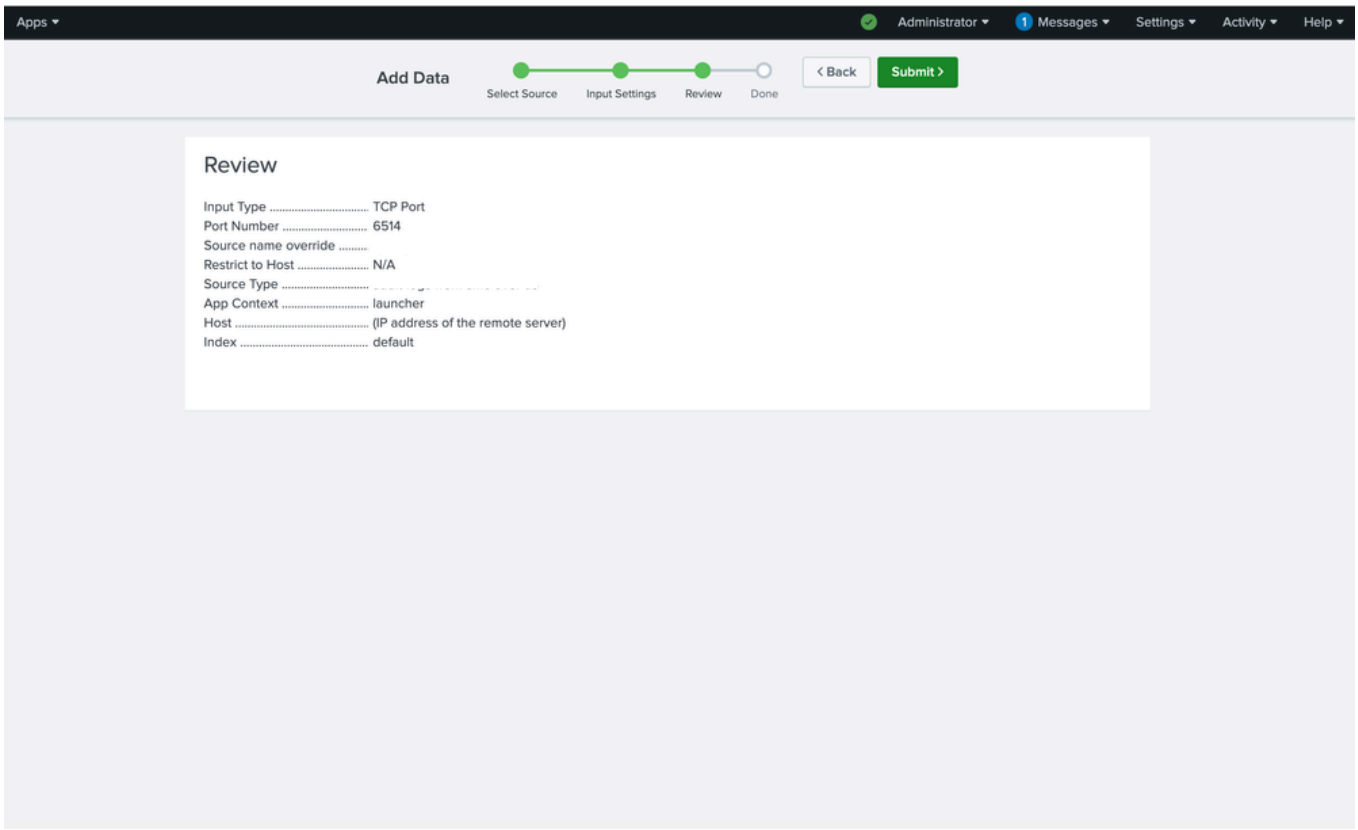
الخطوة 5: في النافذة الجديدة حدد جديد في قسم نوع المصدر، أدخل الاسم المرغوب في حقل نوع المصدر.

الخطوة 6: حدد IP للأسلوب في قسم المضيف.

الخطوة 7: عند الإكمال، حدد زر مراجعة > الخضراء الموجود أعلى النافذة.



الخطوة 8: في الإطار التالي، راجع إعداداتك وحرر إذا لزم الأمر. ما إن تم التحقق من الصحة، انقر فوق زر إرسال >الأخضر" الموجود أعلى الإطار.



2.إنشاء شهادة ل SPLUNK

الخطوة 1: باستخدام جهاز تم تثبيت OpenSSL عليه، قم بتشغيل الأمرsudo openssl req -x509 -newkey rsa:4096 -keyout server_key.pem -out server_cert.pem -sha256 -days 3650 -subj /CN=10.106.127.4، مع إستبدال المثال IP الخاص بجهاز Splunk. الخاص ب 10.106.127.4 ب IP سيطلب منك مرتين إدخال عبارة مرور معرفة من قبل المستخدم. في المثال، يتم تشغيل الأوامر من سطر الأوامر الخاص بجهاز 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:
```

عند اكتمال الأمر، يتم إنشاء ملفين. ملف server_cert.pem و 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:
```

الخطوة 2: التبديل إلى المستخدم الجذري.

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

الخطوة 3: انسخ الشهادة التي تم إنشاؤها حديثا إلى /opt/splunk/etc/auth/ .

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

الخطوة 4: إلحاق ملف spunkweb.cet بمفتاح خاص.

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

الخطوة 5: تغيير ملكية شهادة تقسيم.

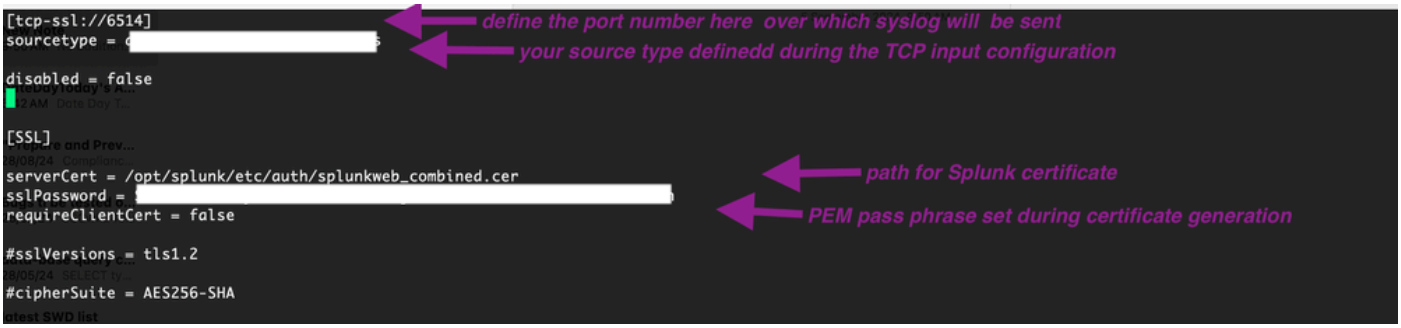
```
user@examplehost:~# chown 10777:10777/opt/splunk/etc/auth/splunkweb.cer
```

الخطوة 6: تغيير الإذن لشهادة التقسيم.

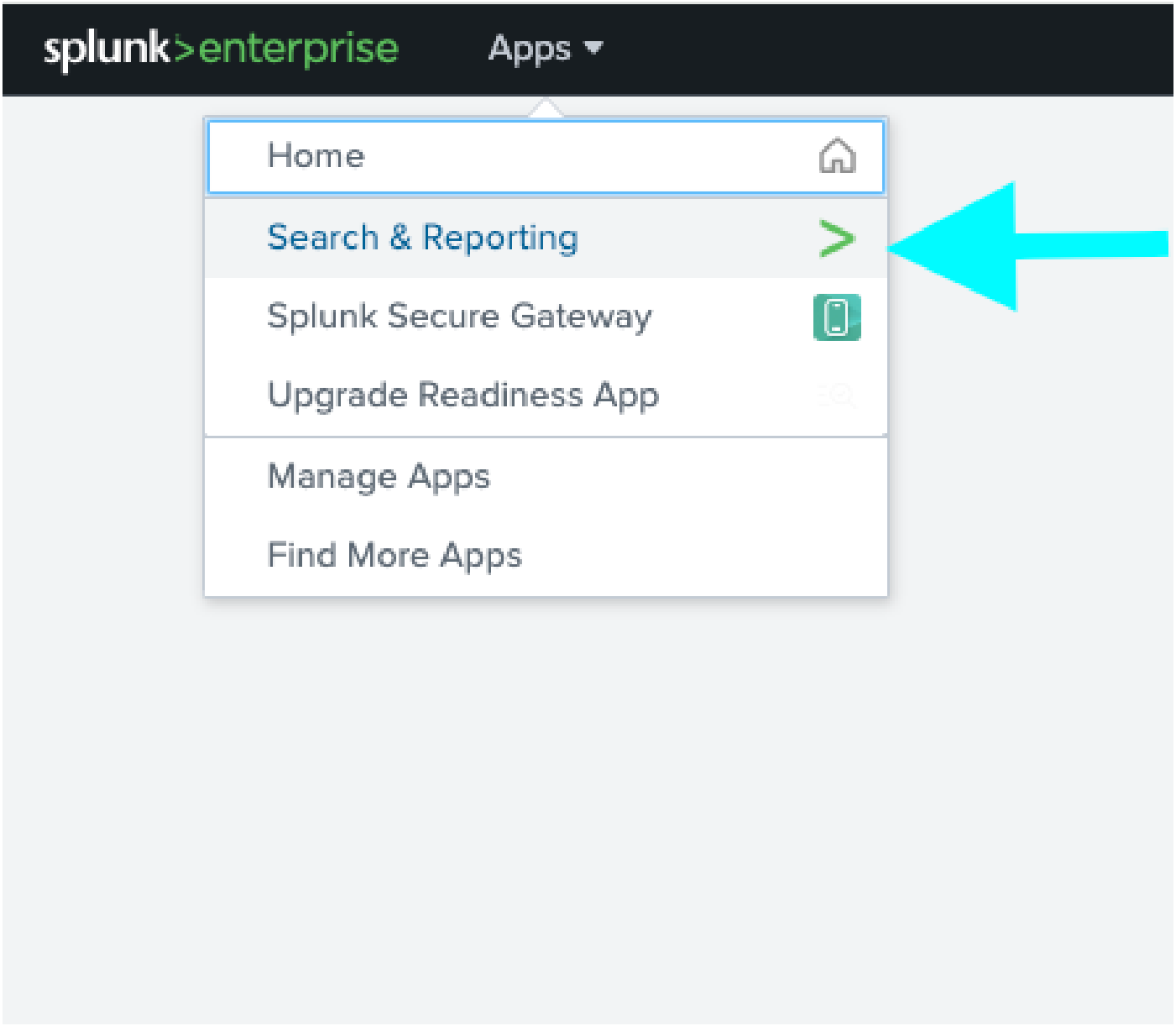
```
user@examplehost:~# chmod 600/opt/splunk/etc/auth/splunkweb.cer
```

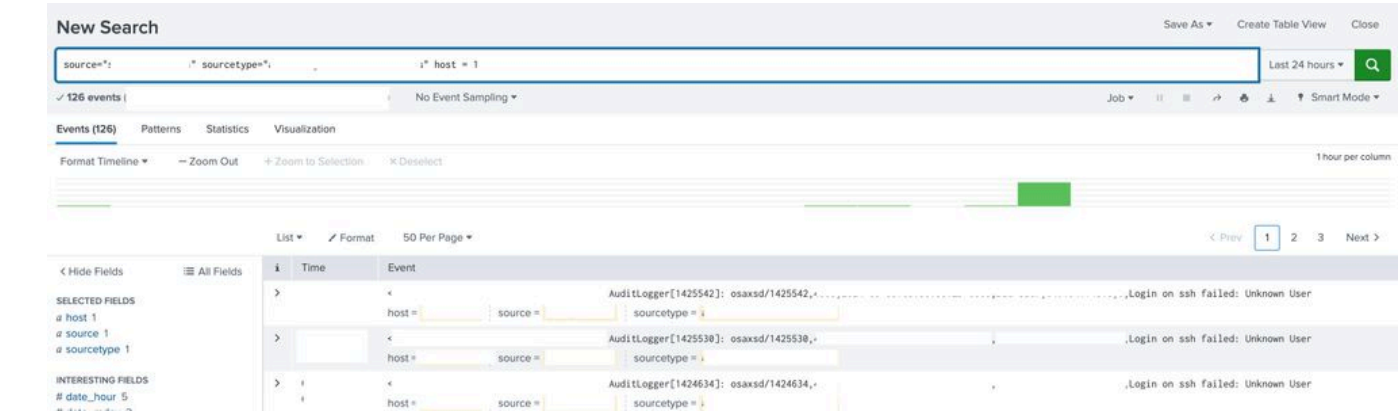
الخطوة 7: قم بإنشاء ملف input.conf جديد.

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



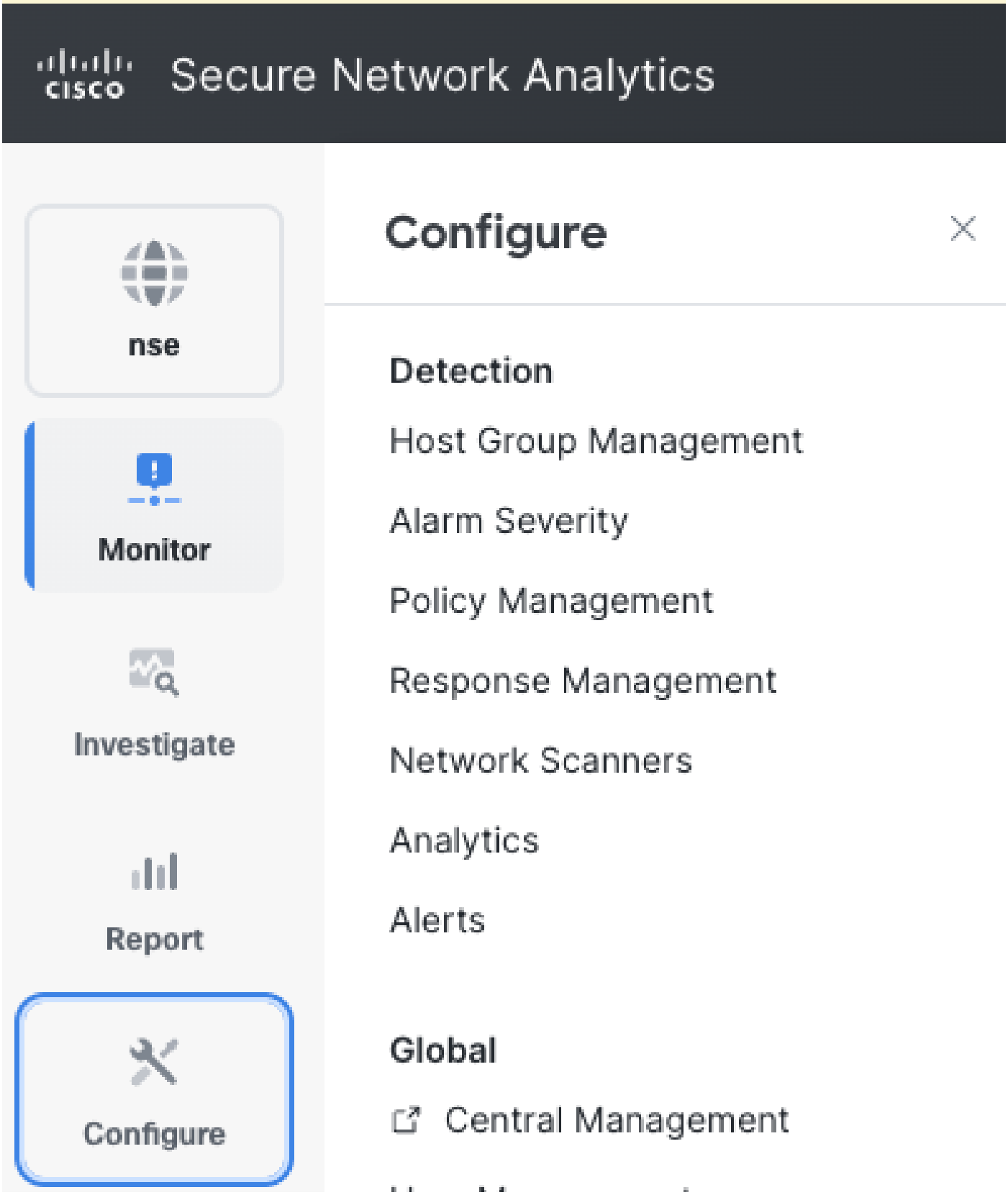
الخطوة 8: دقق ال syslogs يستعمل بحث.



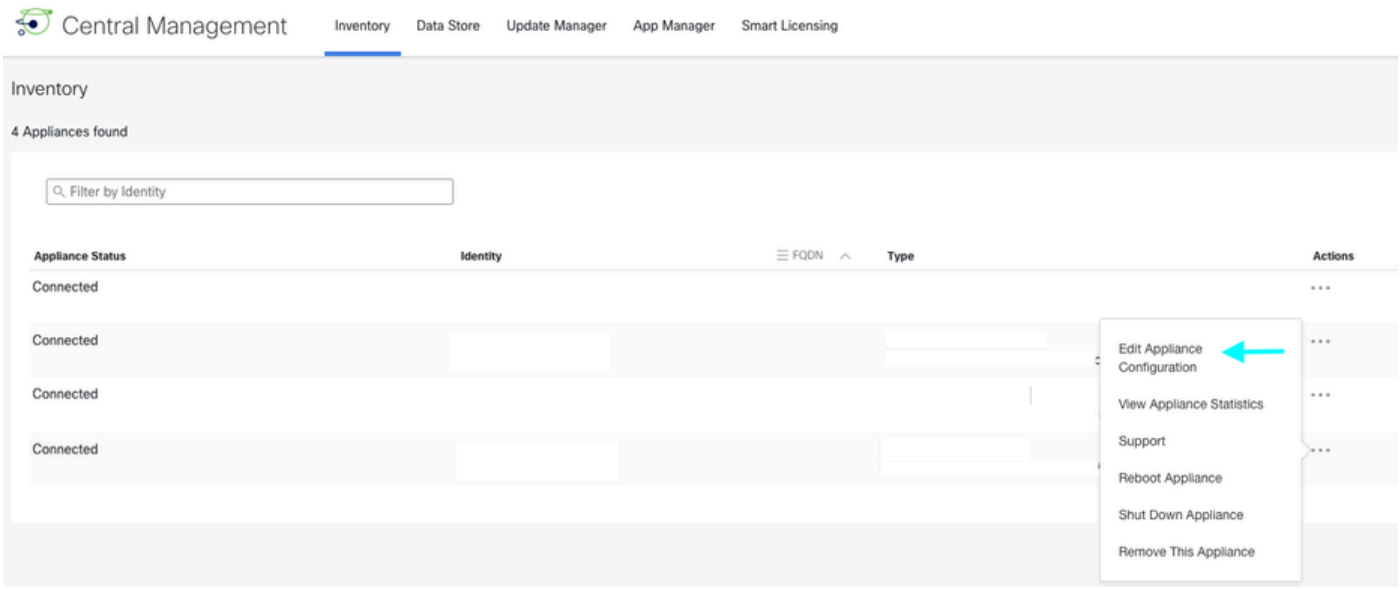


3.تكوين وجهة سجل التدقيق على SNA

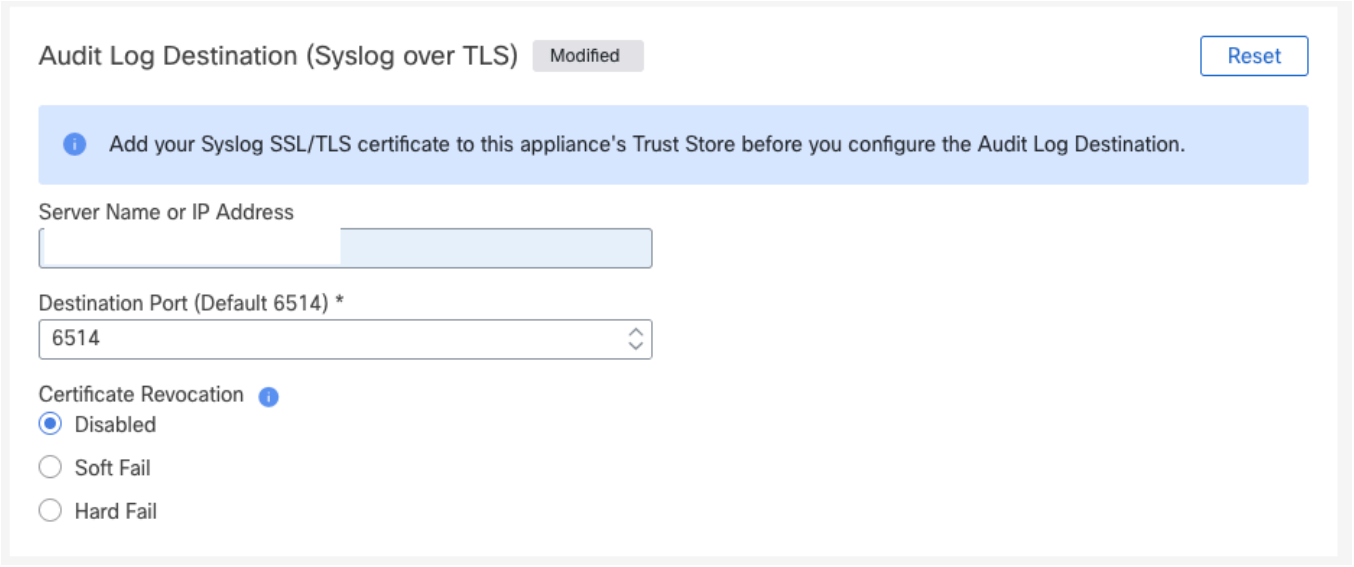
الخطوة 1: سجل الدخول إلى SMC UI انتقل إلى تكوين > الإدارة المركزية.



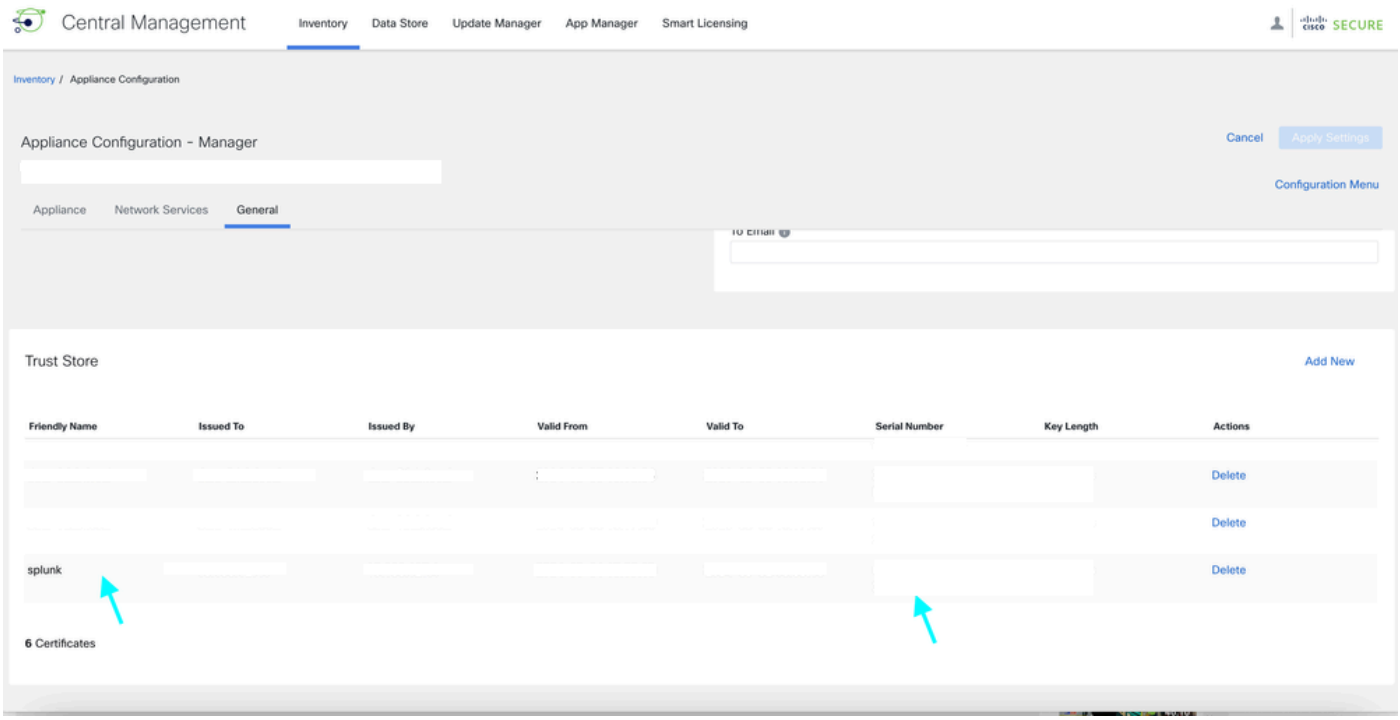
الخطوة 2: انقر على رمز الشكل البيضاوي لجهاز SNA المطلوب حدد تحرير تكوين الجهاز.



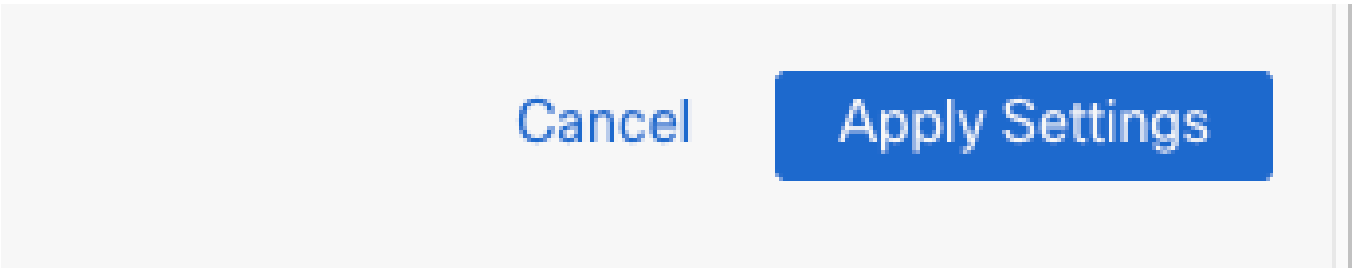
الخطوة 3: انتقل إلى علامة التبويب خدمات الشبكة وأدخل تفاصيل وجهة سجل التدقيق (Syslog عبر TLS).



الخطوة 4: انتقل إلى علامة التبويب "عام"، ثم قم بالتمرير إلى أسفل انقر فوق إضافة جديد لتحميل شهادة Splunk التي تم إنشاؤها مسبقا باسم server_cert.pem.

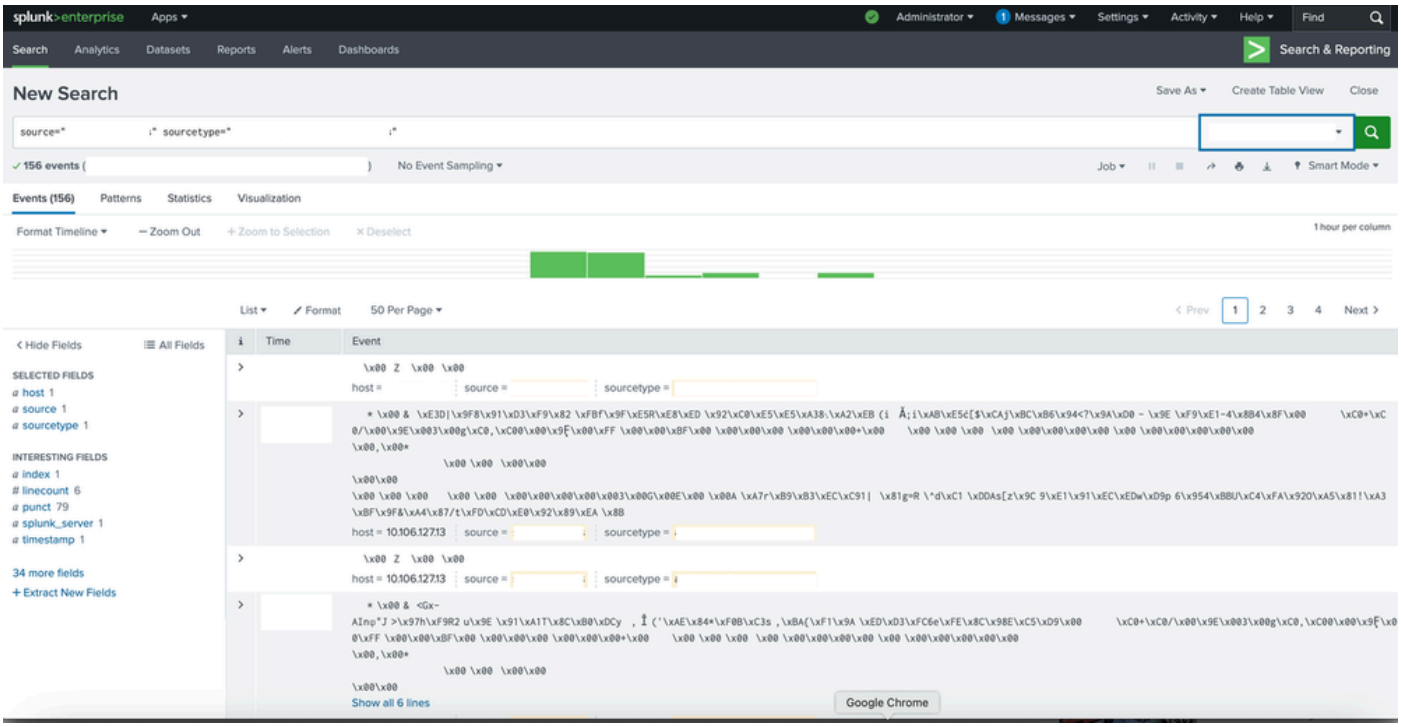


الخطوة 5: طقطقة يطبق عملية إعداد.



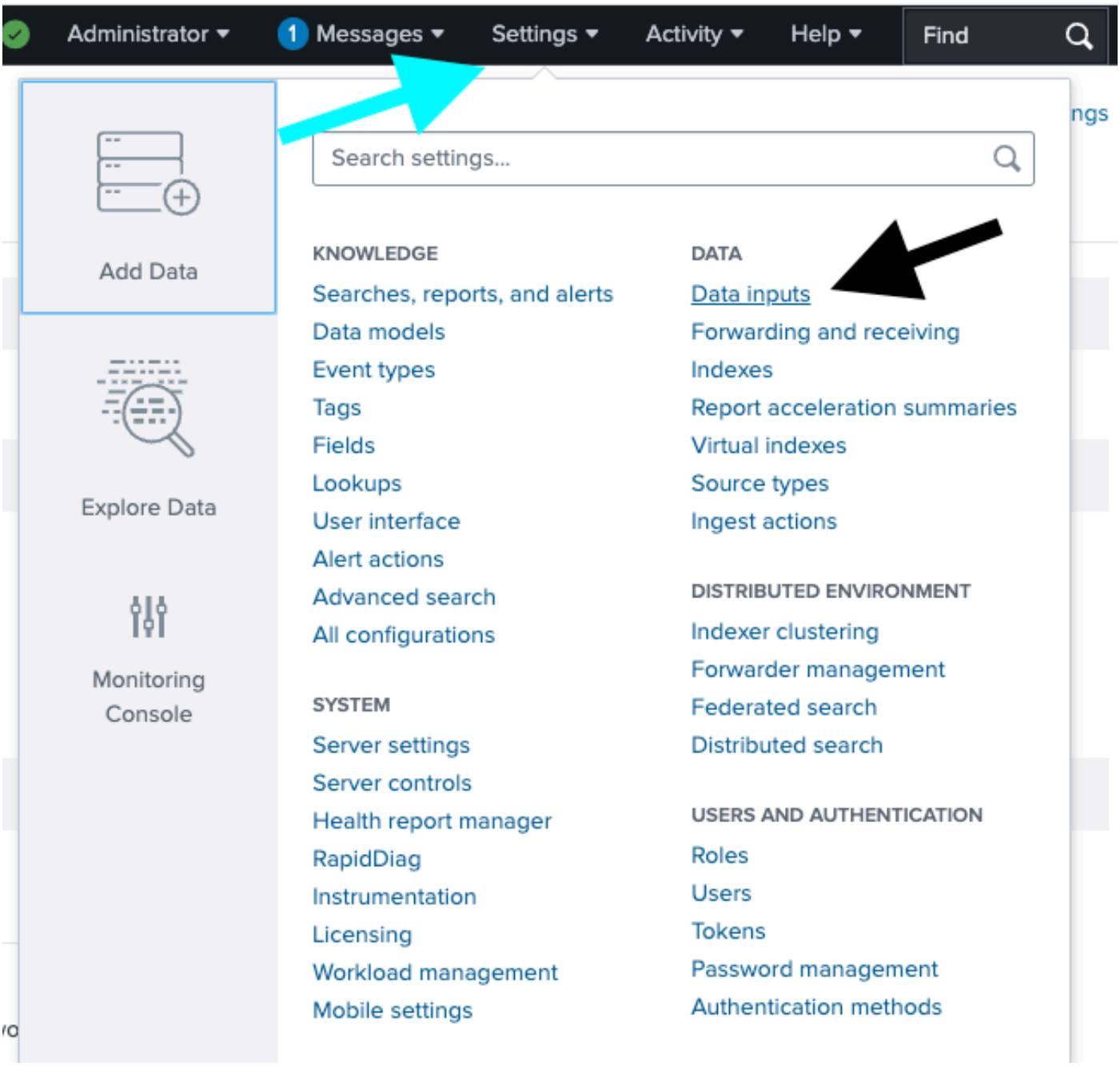
استكشاف الأخطاء وإصلاحها

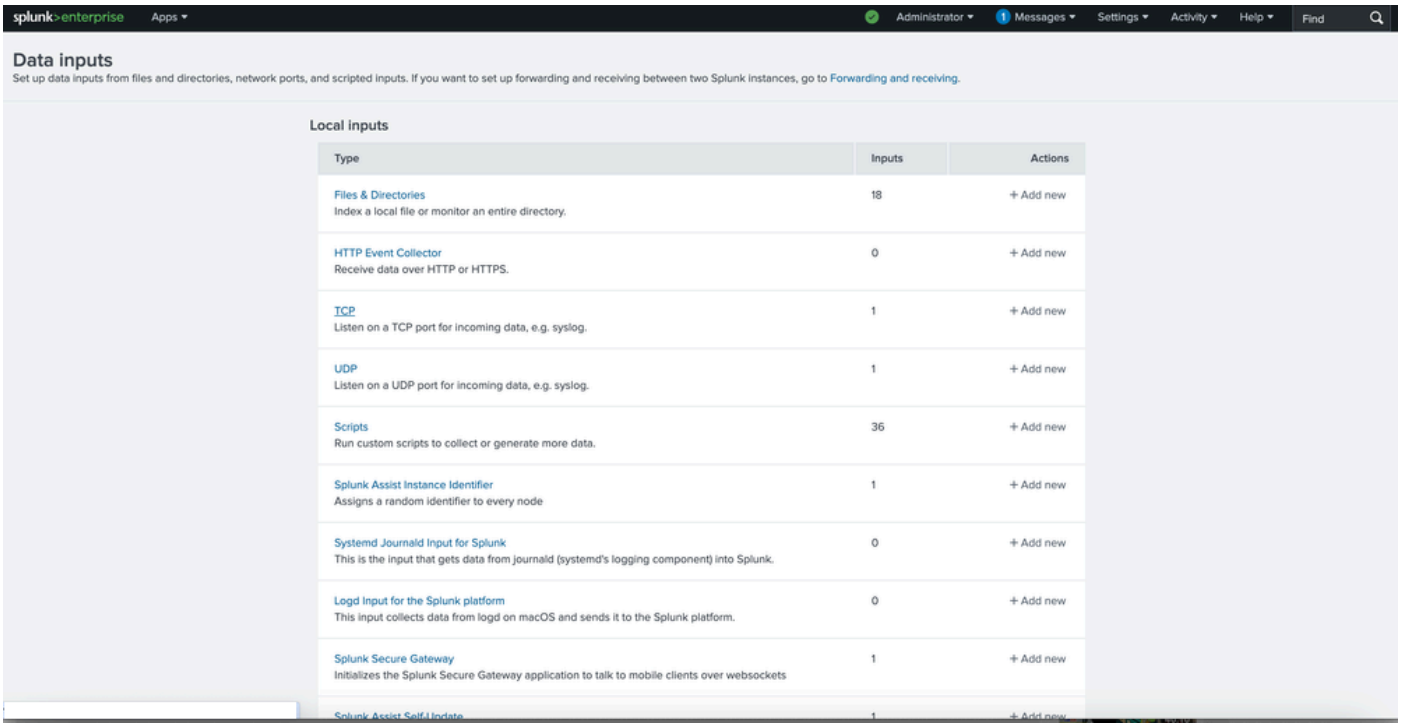
يمكن أن يكون هناك غموض كامل يظهر على البحث.

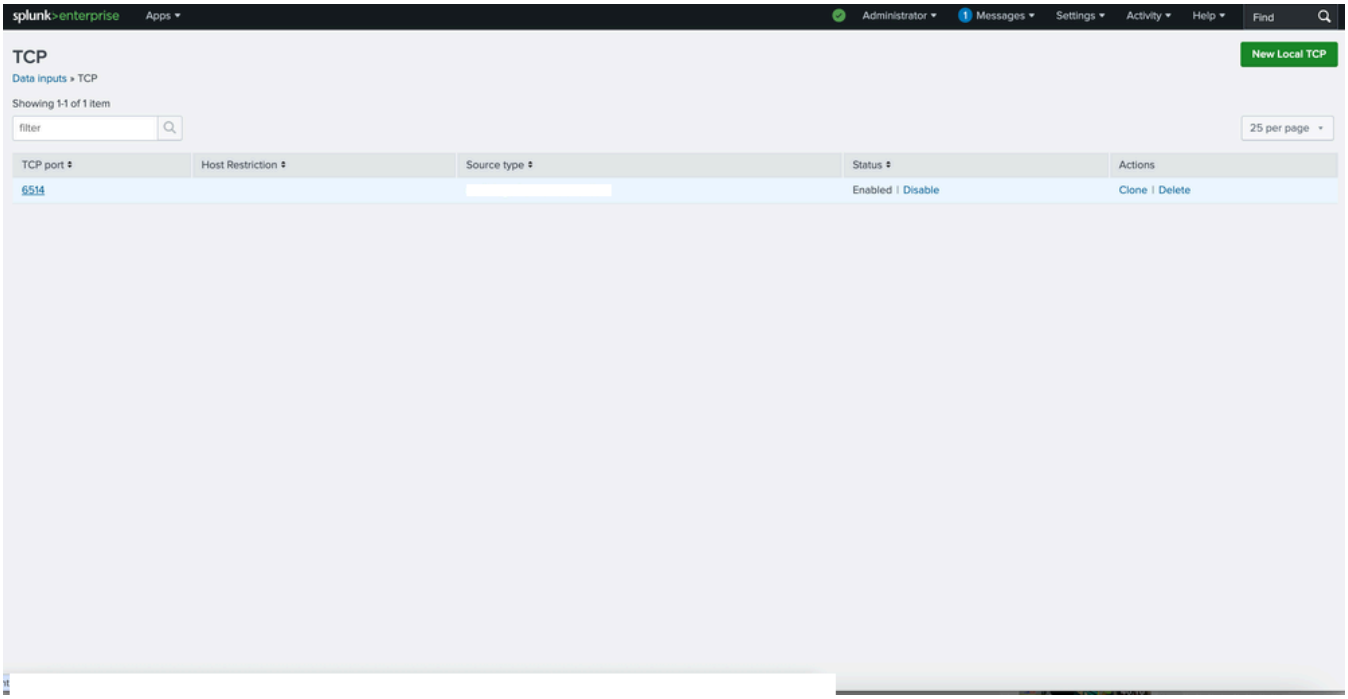


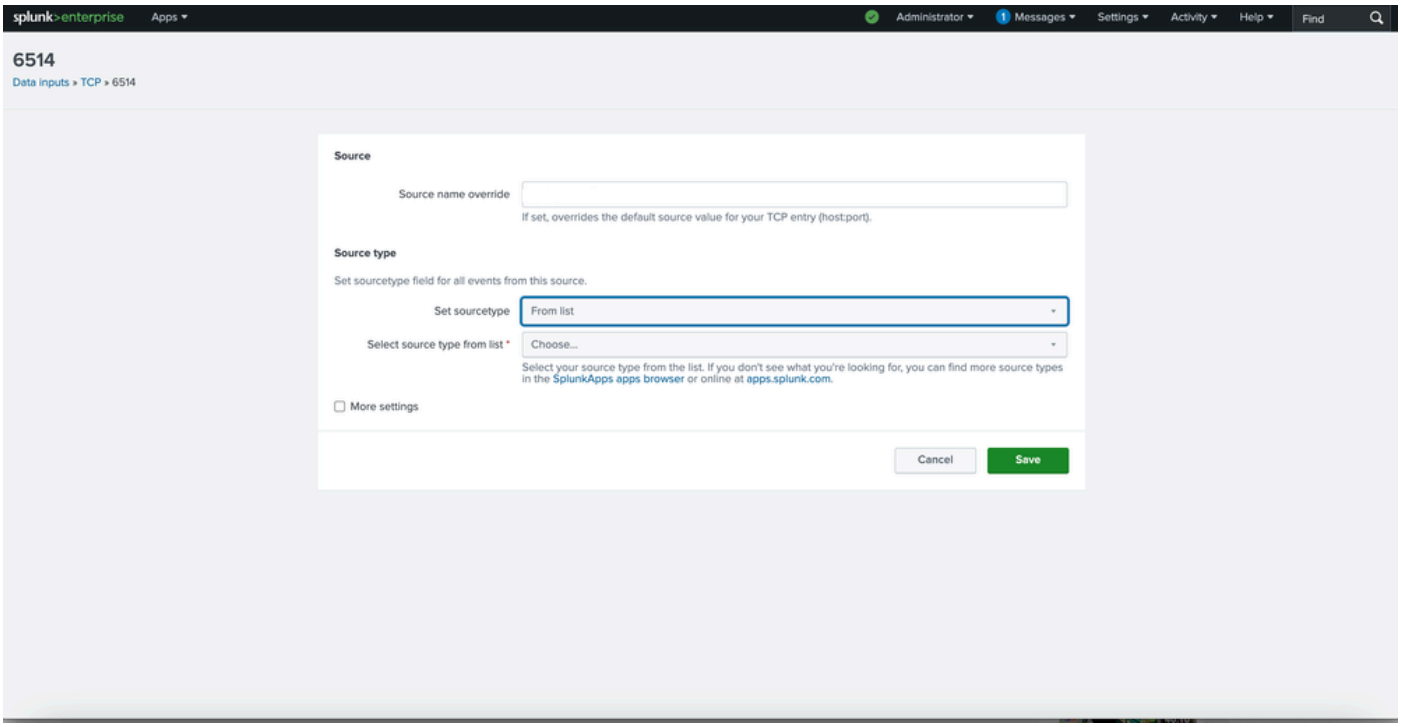
الحل:

قم بتعيين الإدخال إلى نوع المصدر الصحيح.


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

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).