

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

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurez syslog sur SNA sur UDP 514 ou sur un port personnalisé](#)

[1.Gestion des réponses SNA](#)

[2.Configuration du Splunk pour recevoir les Syslogs SNA sur le port UDP](#)

[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](#)

[2.Generate Certificat pour le Splunk](#)

[3.Configurez la destination du journal d'audit sur SNA](#)

[Dépannage](#)

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 :

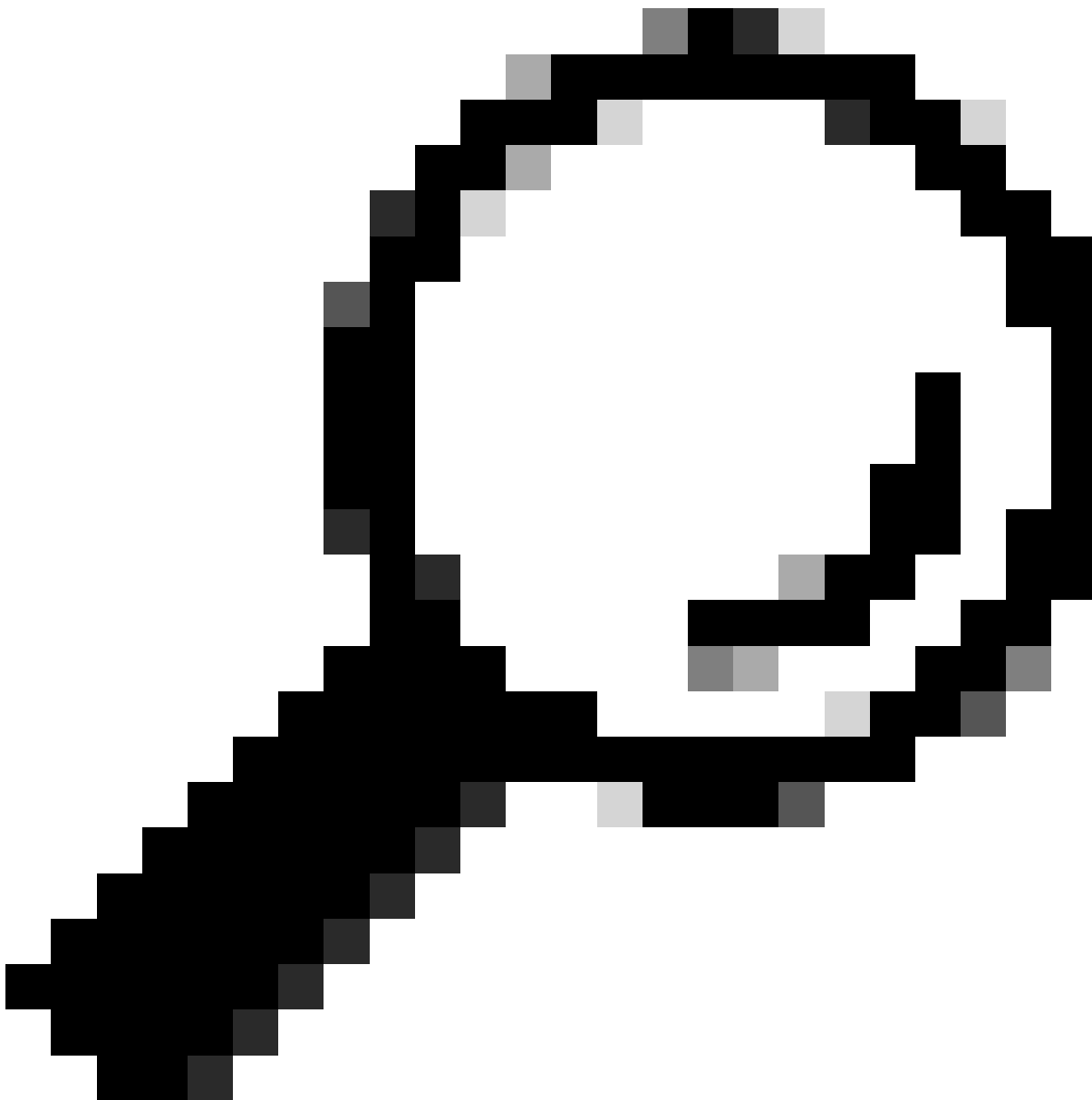
- Gestion des réponses Secure Network Analytics.
- Splunk Syslog

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



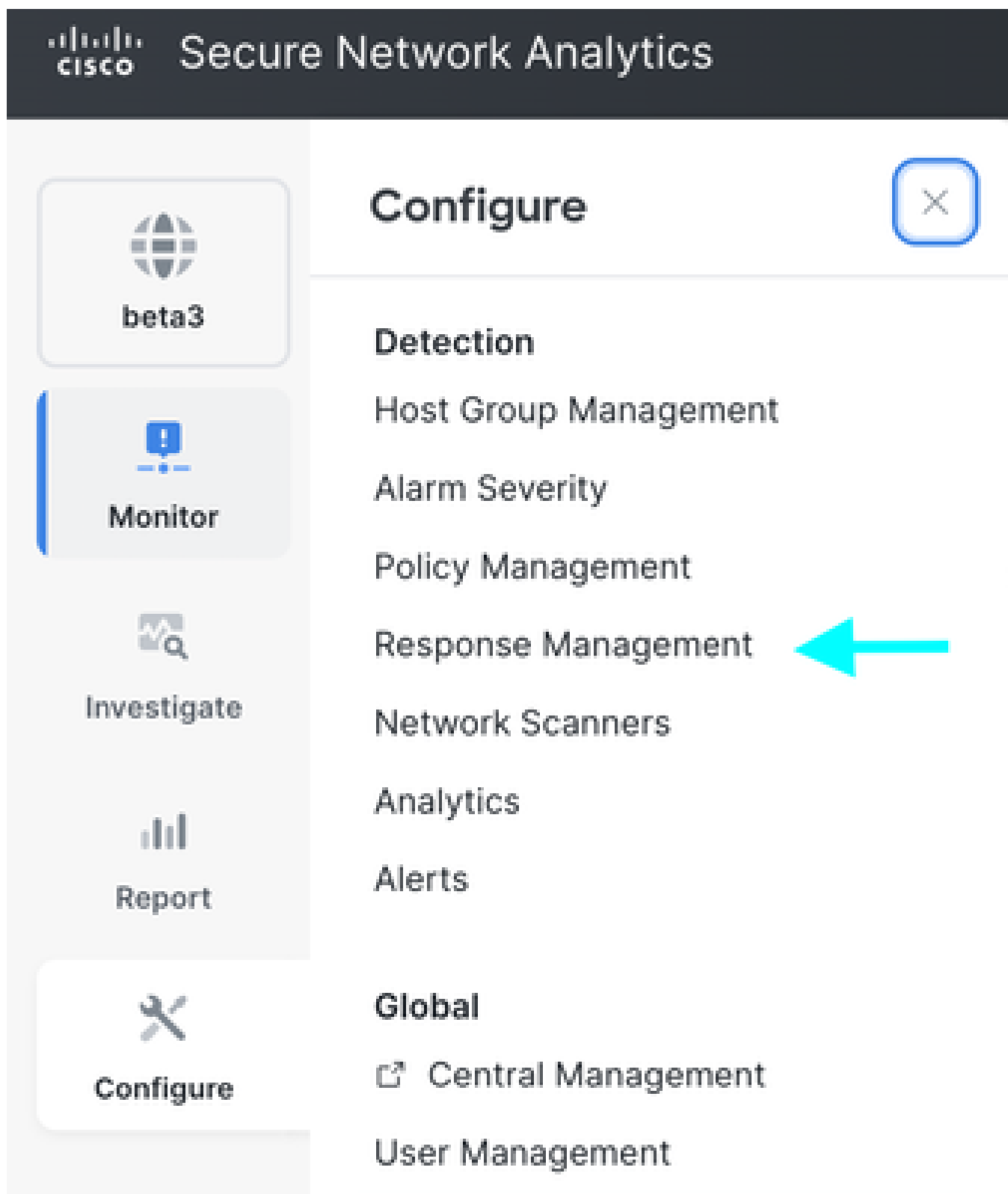
Conseil : assurez-vous que les protocoles UDP/514, TCP/6514 ou tout port personnalisé que vous choisirez pour Syslog sont autorisés sur les pare-feu ou les périphériques intermédiaires entre SNA et Splunk.

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'apppliance SA Manager et accédez à Configurer > Détection Réponse Gestion.



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.

Response Management

Rules Actions Syslog Formats

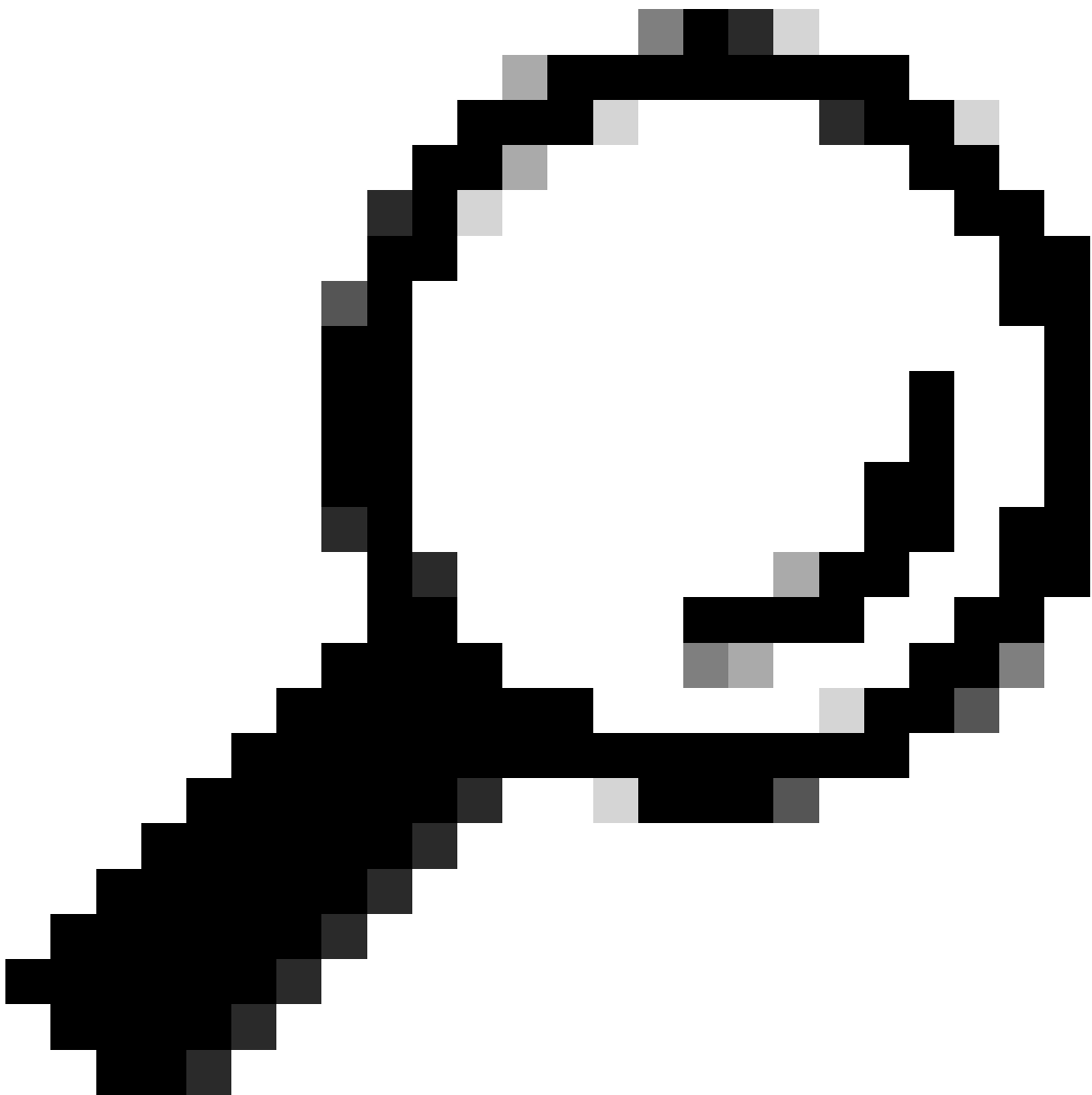
Actions [Add New Action](#)

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	☐	...
Send email	Email (Alert)	Sends an email to the recipients designated in the To field on the Email (Alert) Action page.	2	☐	...
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	☒	...
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	☐	...

Edit Duplicate Delete

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

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

192.168.1.1

UDP Port

514

Message Format

Custom

CEF

This action will use the ArcSight Common Event format.

Example Message

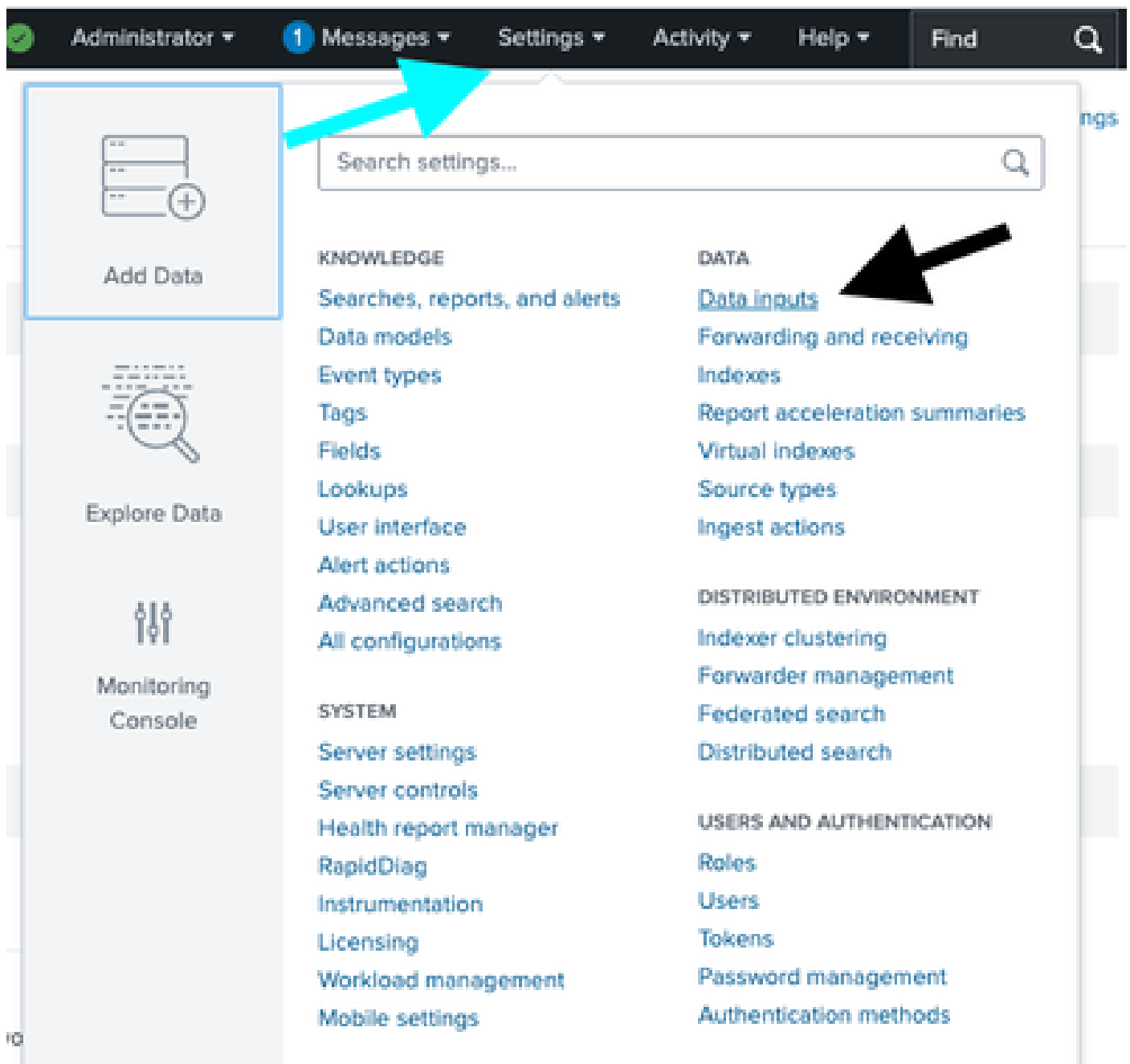
<131>Jan 01 00:00:00 test.host TestApp[1337]: CEF:0|Cisco|7.3.0|Notification:99|Bad Host|5|msg=This host has been observed performing malicious actions toward another host.:Source Host is http (80

Test Action

2. 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.

Administrator

1

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

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.

Add Data

< 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 Journal 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 ?

514

Example: 514

Source name override ?

host:port

Only accept connection from ?

optional

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?

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.

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](#)

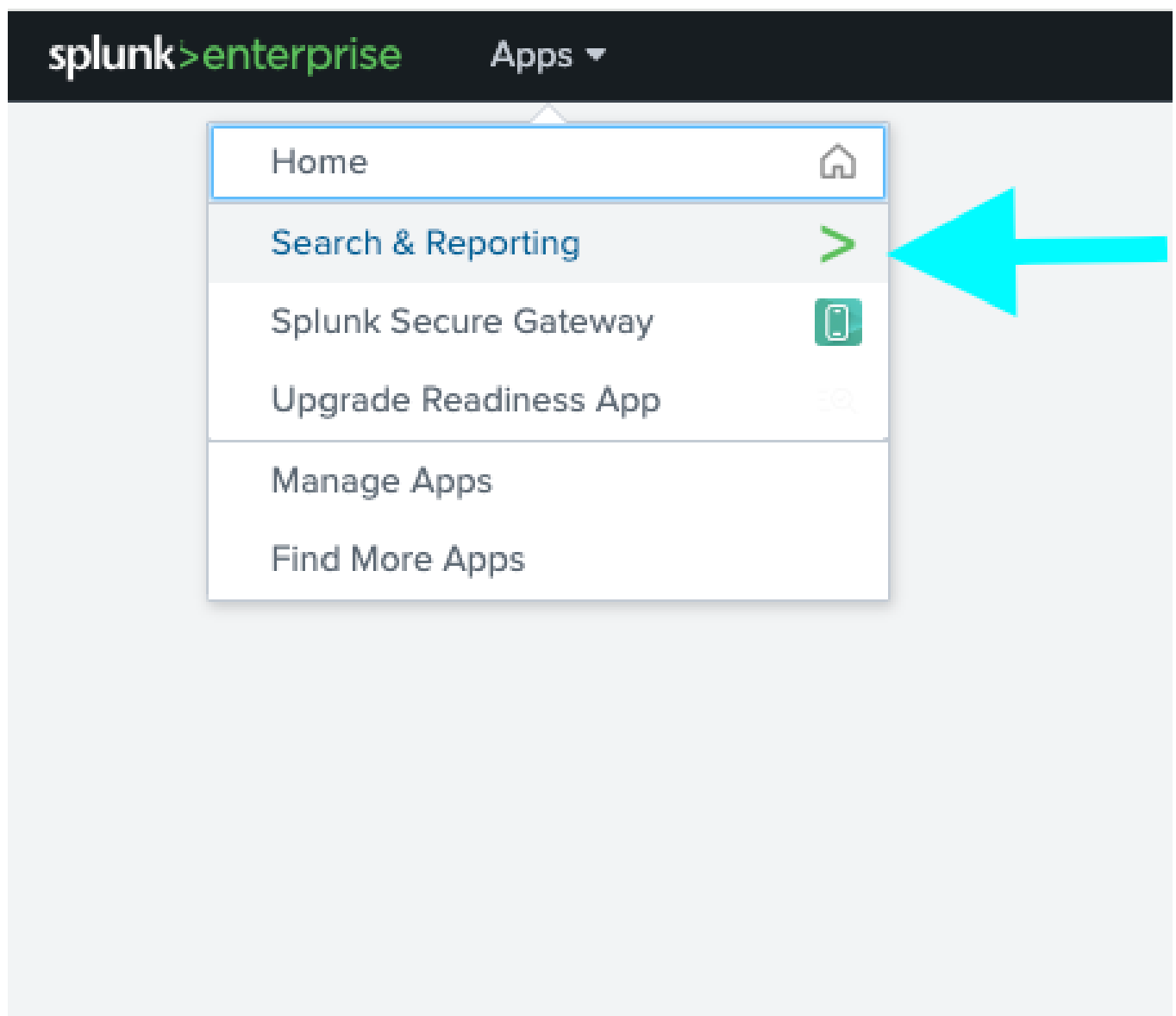
Étape 9 : Dans la fenêtre suivante, vérifiez vos paramètres et modifiez-les si nécessaire.

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

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

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.

New Search

source* :* sourcetype* |

6 events

Events (6) Patterns Statistics Visualization

Timeline format Zoom Out Zoom to Selection Deselect

Format Show: 20 Per Page View: List

Time	Event
	end= externalId=80-1KUS-7R9L-PN6Z-5 cs3= cs3Label=SourceHostGroups cs4= cs4Label=TargetHostGroups cs5= cs5Label=Source_URL cs6= cs6Label=Target_URL dpt= proto= dvchost= ceExternalId= * / / cs2Label=SGTIdAndSGTName spt= destinationTranslatedAddress= destinationTranslatedPort= sourceTranslatedAddress= sourceTranslatedPort=
	host = source = sourcetype =

SELECTED FIELDS

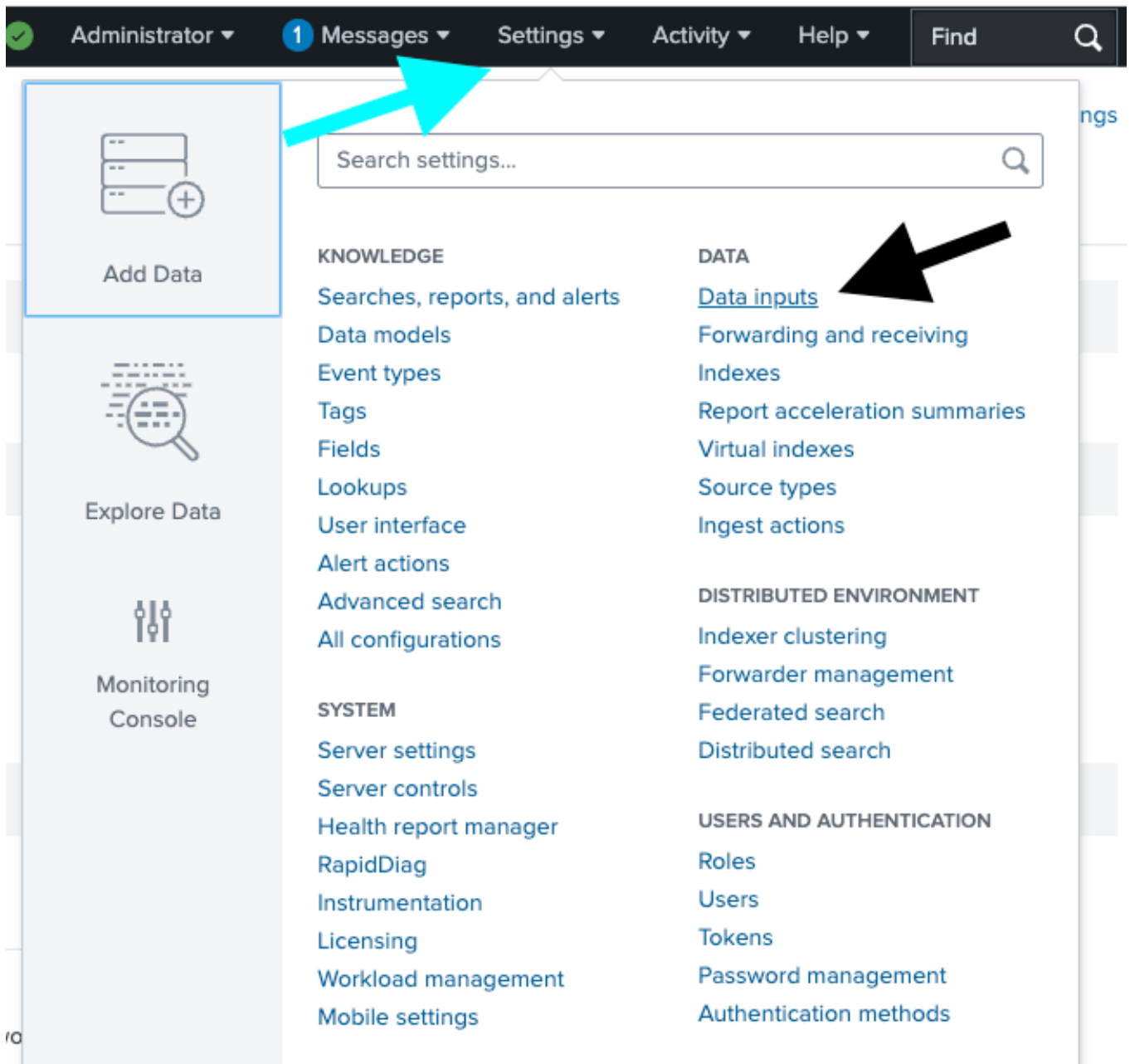
- host 1
- source 1
- sourcetype 1

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.

Apps

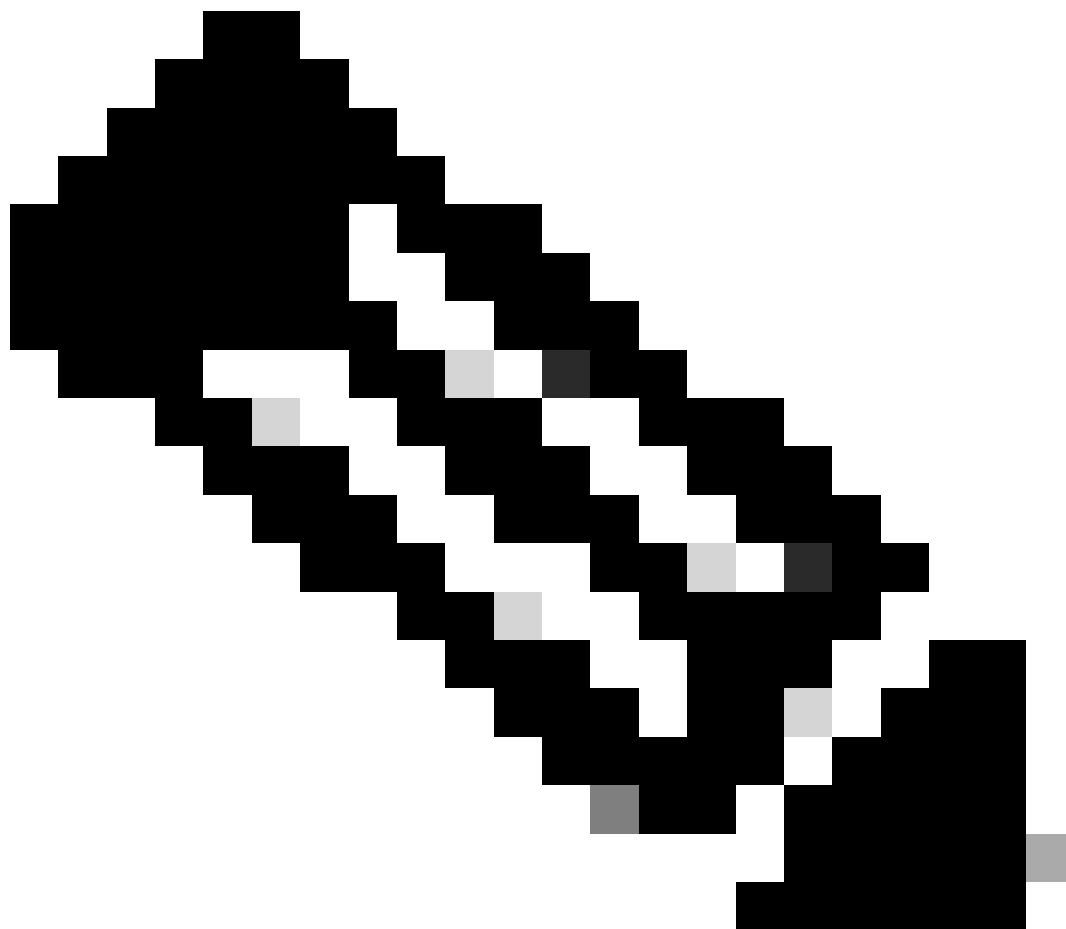
Administrator1 MessagesSettingsActivityHelp

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
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.	0	+ Add new
UDP Listen on a UDP port for incoming data, e.g. syslog.	0	+ 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 Journal 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

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.

Apps
Administrator
1 Messages
Settings
Activity
Help

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
Detects and Downloads Assist Supervisor Updates

Splunk Secure Gateway Mobile Alerts TTL
Cleans up storage of old mobile alerts

Config Modular Input

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 ? 6514
Example: 514

Source name override ? :
host:port

Only accept connection from ? optional
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?

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.

Apps ▾ Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾

Add Data ● ● ○ ○ < Back Review >

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.

Source Type 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 Apps Browser (appsbrowser) ▾

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

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.

Apps ▾ Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾

Add Data ● ● ● ○ < Back Submit >

Review

Input Type TCP Port

Port Number 6514

Source name override

Restrict to Host N/A

Source Type

App Context launcher

Host (IP address of the remote server)

Index default

2.Generate Certificat pour le Splunk

Étape 1 : À l'aide d'une machine sur laquelle openssl est installé, exécutez la 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.

[illegible]

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.

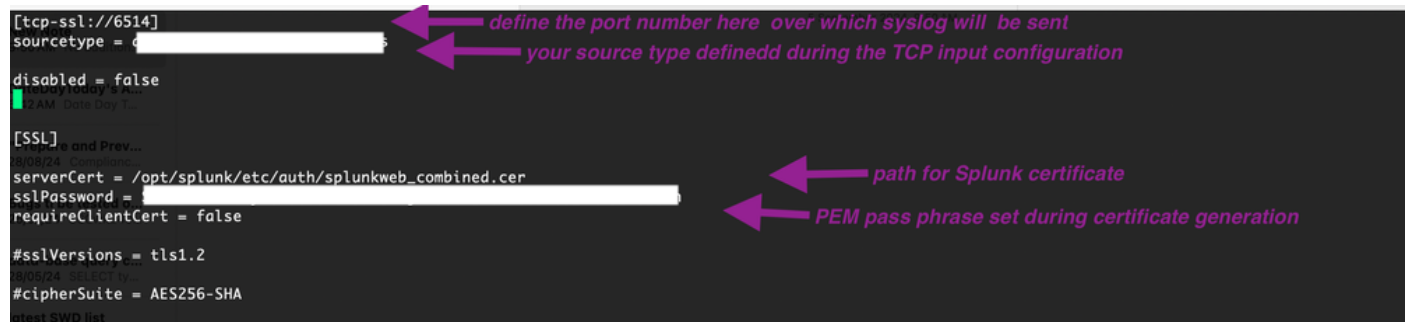
```
user@examplehost:~# chown 10777:10777/opt/splunk/etc/auth/splunkweb.cer
```

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
```



```
[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

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

Home



Search & Reporting



Splunk Secure Gateway

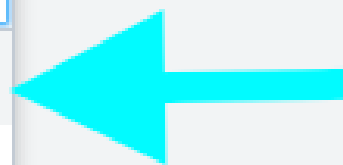


Upgrade Readiness App



Manage Apps

Find More Apps



New Search

Save As ▾ Create Table View Close

source="*" "sourcetype=" " host = 1

Last 24 hours



✓ 126 events

No Event Sampling ▾

Job ▾ || || → ⬇ ⬆ Smart Mode ▾

Events (126) Patterns Statistics Visualization

Format Timeline ▾ Zoom Out Zoom to Selection Deselect

1 hour per column

List ▾ Format 50 Per Page ▾

< Prev 1 2 3 Next >

< Hide Fields

All Fields

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

date_hour 5

Time	Event
>	< AuditLogger[1425542]: osaxsd/1425542,.....Login on ssh failed: Unknown User
	host = source = sourcetype =
>	< AuditLogger[1425538]: osaxsd/1425538,.....Login on ssh failed: Unknown User
	host = source = sourcetype =
>	< AuditLogger[1424634]: osaxsd/1424634,.....Login on ssh failed: Unknown User
	host = source = sourcetype =

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

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



nse



Monitor



Investigate



Report



Configure

Configure



Detection

Host Group Management

Alarm Severity

Policy Management

Response Management

Network Scanners

Analytics

Alerts

Global

 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.

Inventory

4 Appliances found

Filter by Identity

Appliance Status	Identity	FQDN	Type	Actions
Connected				...
Connected				- Edit Appliance Configuration - View Appliance Statistics - Support - Reboot Appliance - Shut Down Appliance - Remove This Appliance
Connected				...
Connected				...

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

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) *

6514

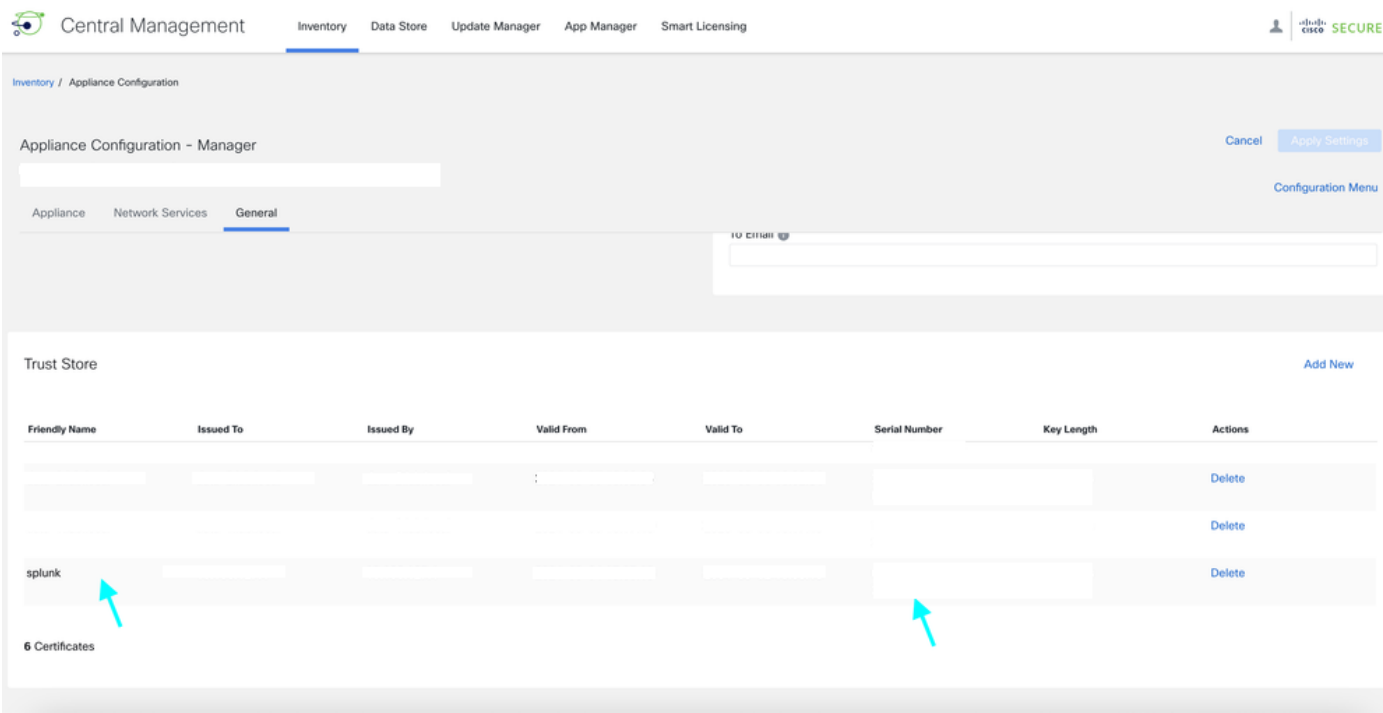
Certificate Revocation

☒ Disabled

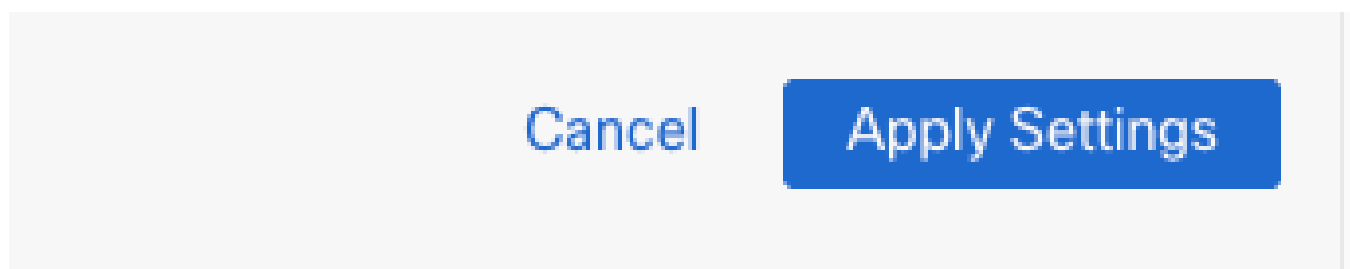
☐ Soft Fail

☐ Hard Fail

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.



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
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

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

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

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.