

Splunkにsyslogイベントを送信するための応答管理の設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[SNA over UDP 514またはカスタム定義ポートでsyslogを設定する](#)

[1.SNA応答管理](#)

[2. UDPポートでSNA Syslogを受信するためのSplunkの設定](#)

[SNA over TCPポート6514またはカスタム定義ポートでsyslogを設定する](#)

[1. TCPポート経由でSNA監査ログを受信するためのSplunkの設定](#)

[2. Splunkの証明書の生成](#)

[3. SNAでの監査ログの宛先の設定](#)

[トラブルシューティング](#)

はじめに

このドキュメントでは、syslogを介してSplunkなどのサードパーティにイベントを送信するようにSecure Analytics応答管理機能を設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

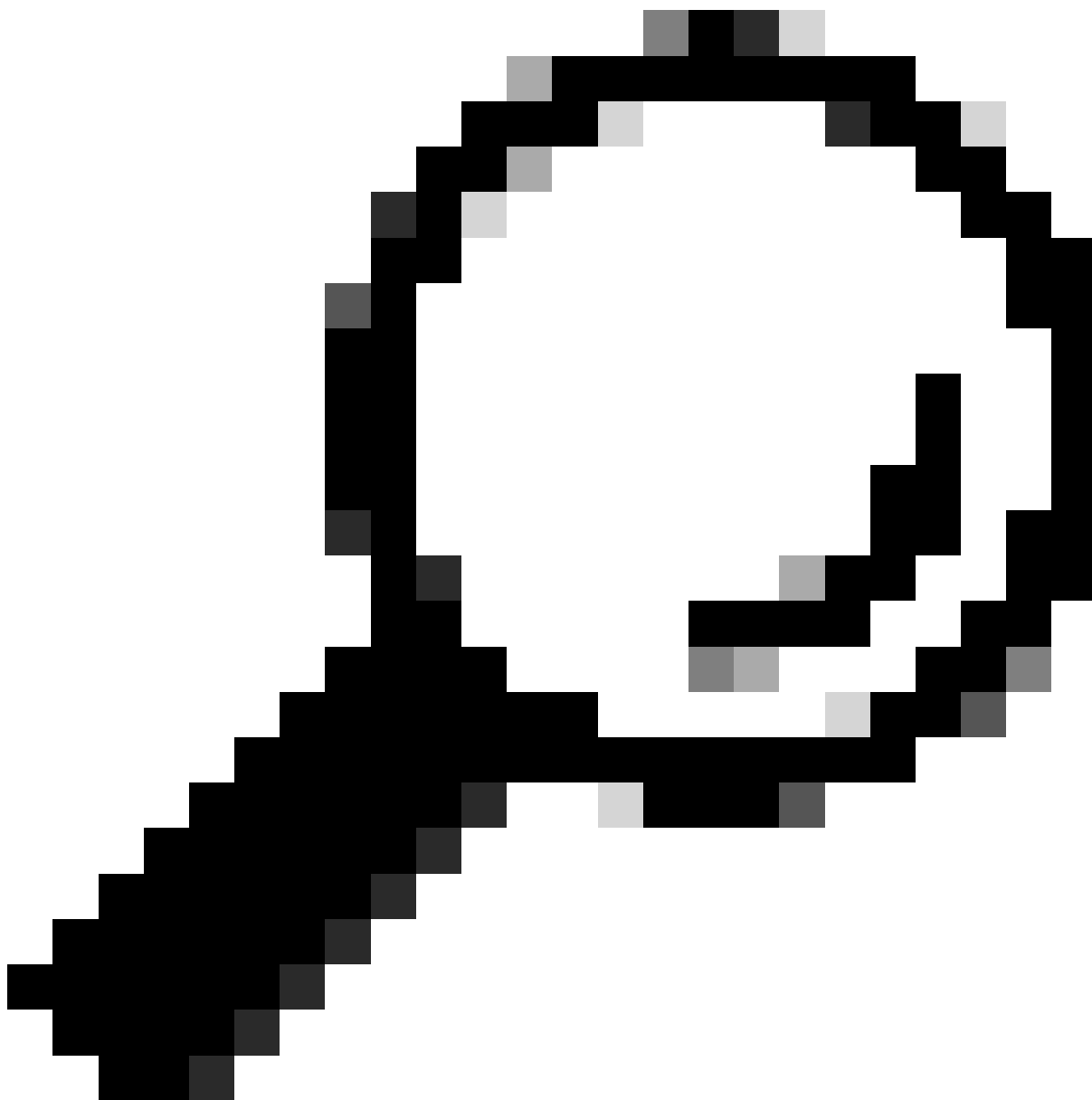
- Secure Network Analytics Response Managementの略。
- Splunkのsyslog

使用するコンポーネント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

- 1つ以上のManagerアプライアンスと1つのFlow Collectorアプライアンスを含むSecure Network Analytics(SNA)展開。
- Splunkサーバがインストールされ、443ポート経由でアクセス可能になりました。

SNA over UDP 514またはカスタム定義ポートでsyslogを設定する



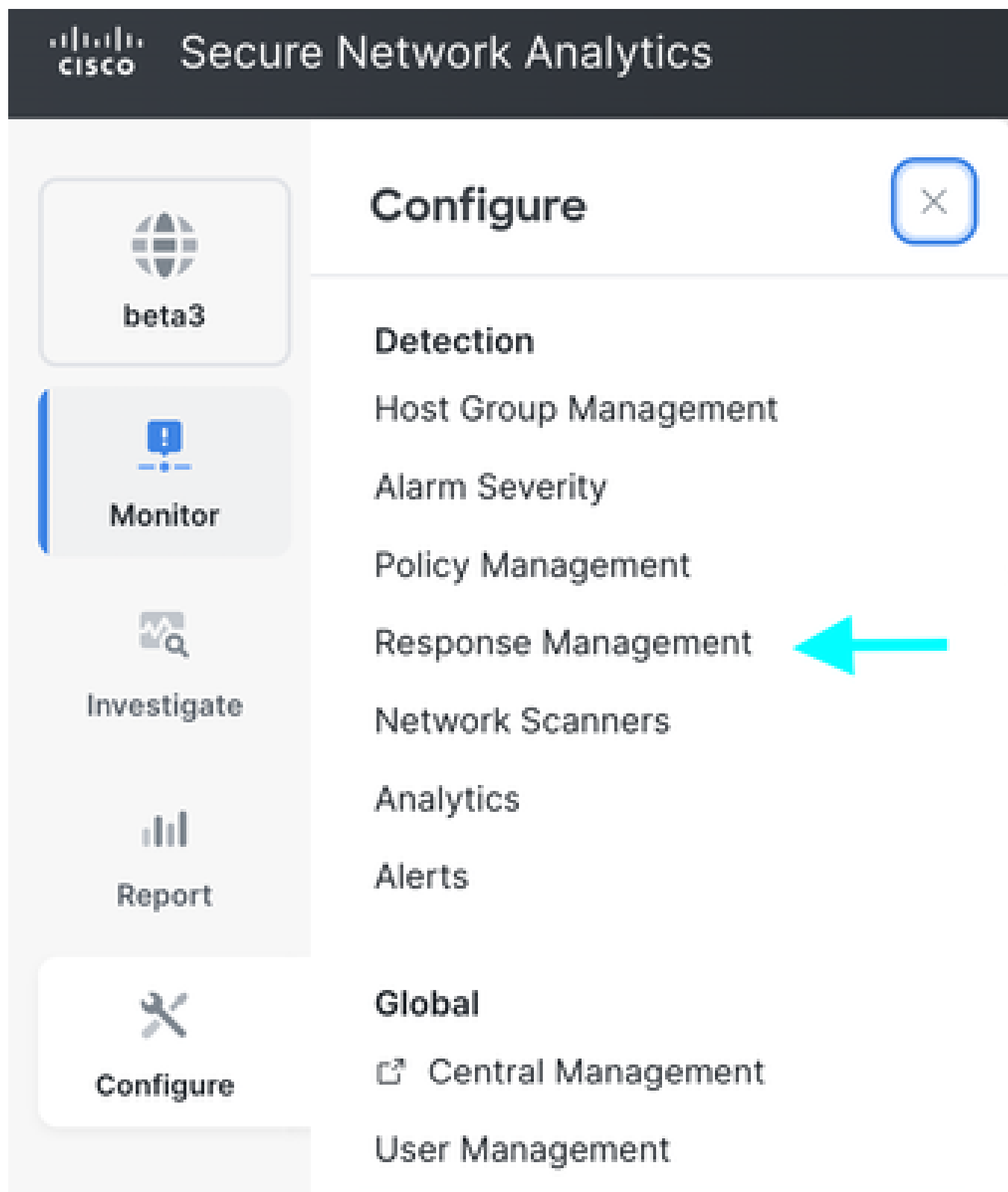
ヒント:SNAとSplunk間のすべてのファイアウォールまたは中間デバイスで、UDP/514、TCP/6514、またはsyslog用に選択したカスタムポートが許可されていることを確認してください。

1.SNA応答管理

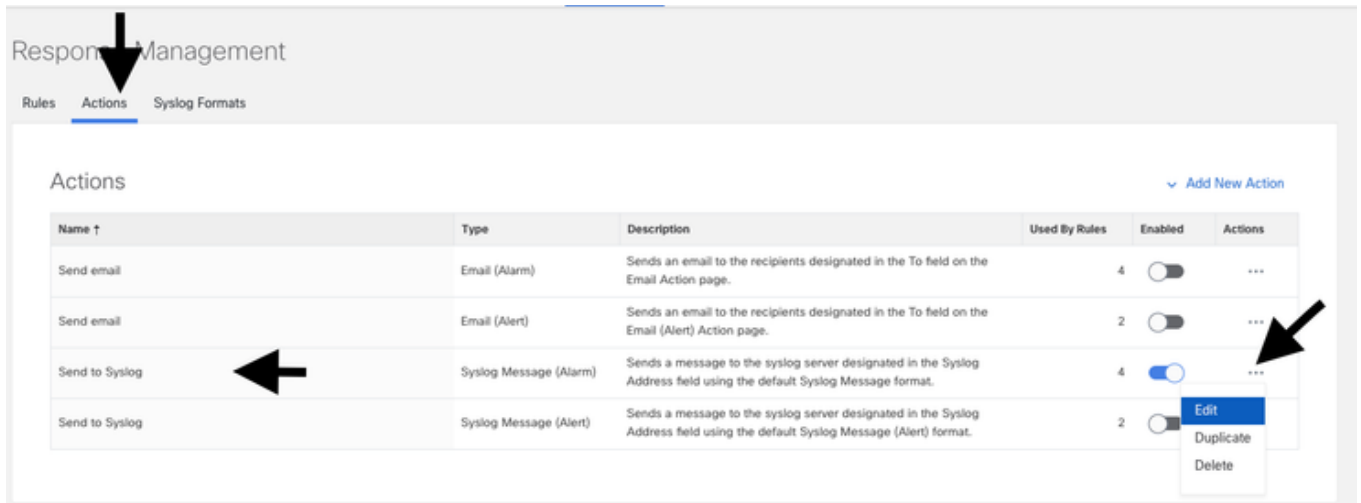
Secure Analytics(SA)の応答管理コンポーネントを使用して、ルール、アクション、およびsyslogの宛先を設定できます。

Secure Analyticsアラームを他の宛先に送信/転送するには、これらのオプションを設定する必要があります。

ステップ1: SA Managerアプライアンスにログインし、Configure > Detection Response Managementの順に移動します。

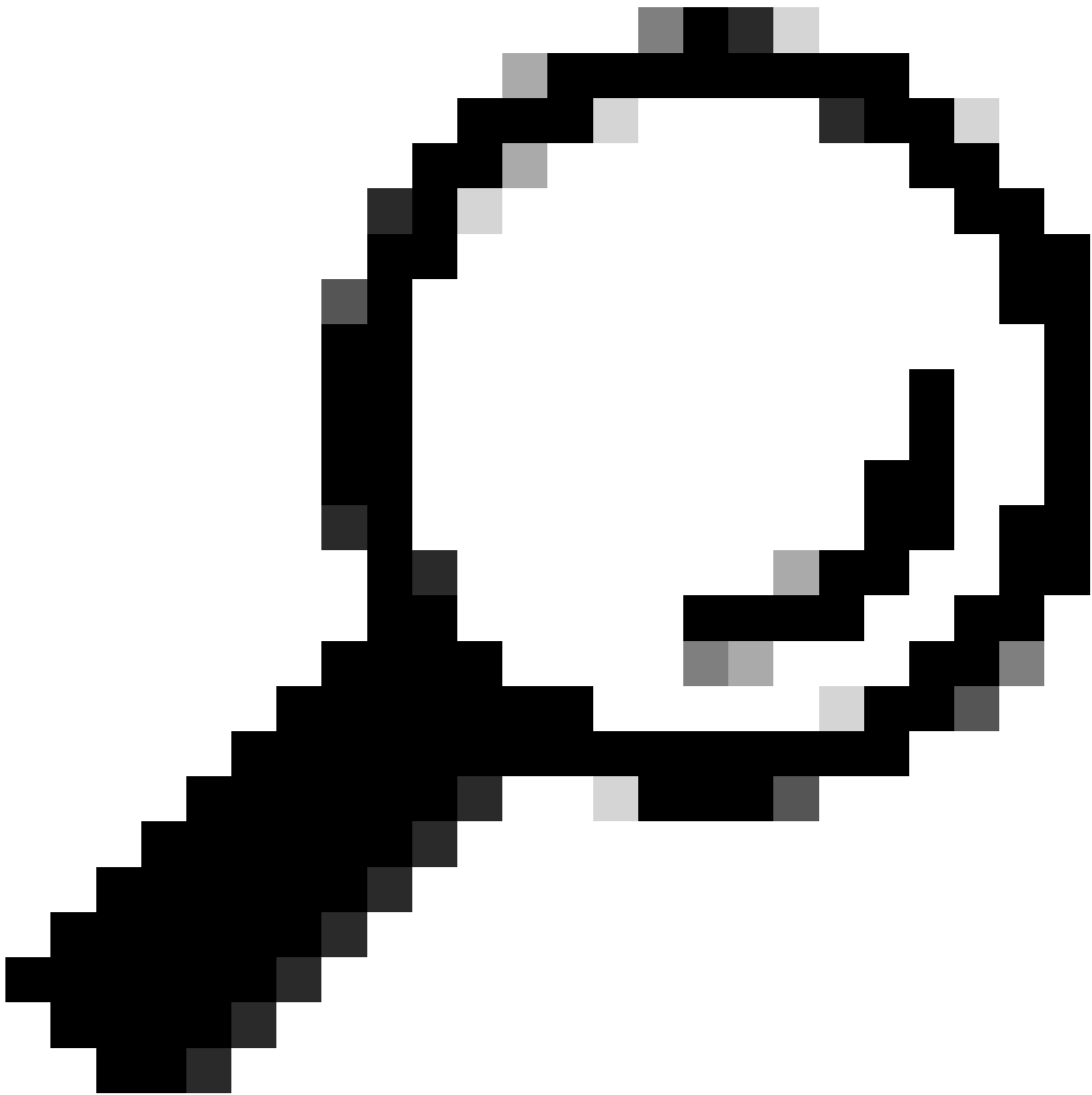


ステップ2: 新しいページでActionsタブに移動し、デフォルトのSend to Syslog行項目を見つけて、Action列の省略記号(...)をクリックし、Editをクリックします。



ステップ3: Syslog Server Addressフィールドに目的の宛先アドレスを入力し、UDP Portフィールドに目的の宛先受信ポートを入力します。Message FormatでCEFを選択します。

ステップ4: 完了したら、右上隅にある青色の保存ボタンをクリックします。



ヒント: syslogのデフォルトのUDPポートは514です

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

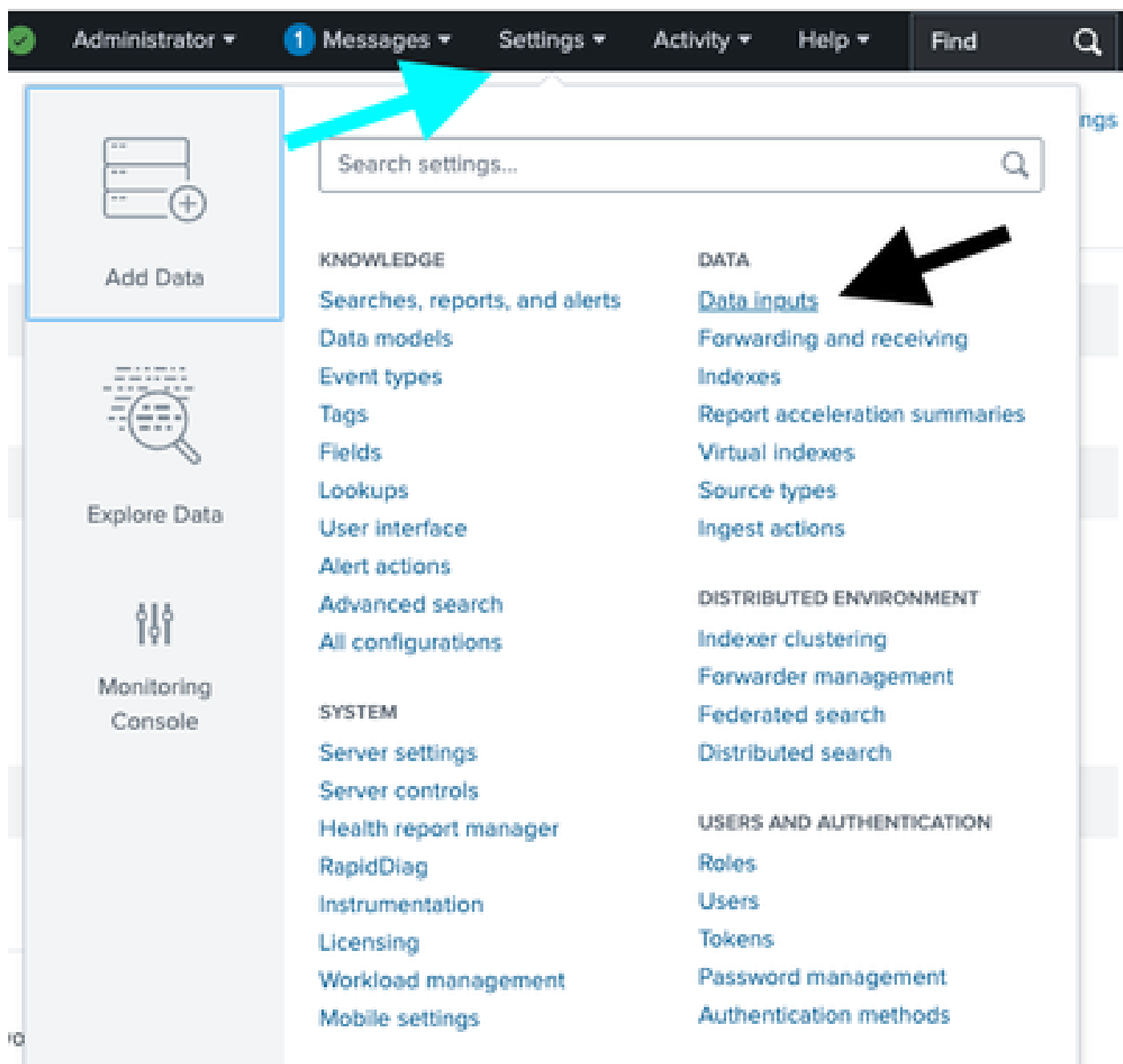
<131>Jan 01 00:00:00 test.host TestApp[1337]: CEF:0|Cisco|7.3.0|Notification:99|Bad Host|5|msg=This host has been observed performing malicious actions toward another host.:Source Host is http (80

Test Action

2. UDPポートでSNA Syslogを受信するためのSplunkの設定

Secure Network Analytics Manager Web UIで変更を適用した後は、Splunkでデータ入力を設定する必要があります。

ステップ1: Splunkにログインし、設定>データの追加>データ入力に移動します。



ステップ2:UDP行を探し、+Add newを選択します。

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

- ステップ3：新しいページでUDPを選択し、Portフィールドに514などの受信ポートを入力します。
- ステップ4:Source name overrideフィールドに、desired name of source.
- ステップ5：完了したら、ウィンドウ上部の緑色のNext >ボタンをクリックします。

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 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?

ステップ6：次のページでNewオプションに切り替え、Source Typeフィールドを見つけて入力します desired source .

ステップ7:方式としてIPを選択します。

ステップ8：画面の上部にある緑色のReview > ボタンをクリックします。

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](#)

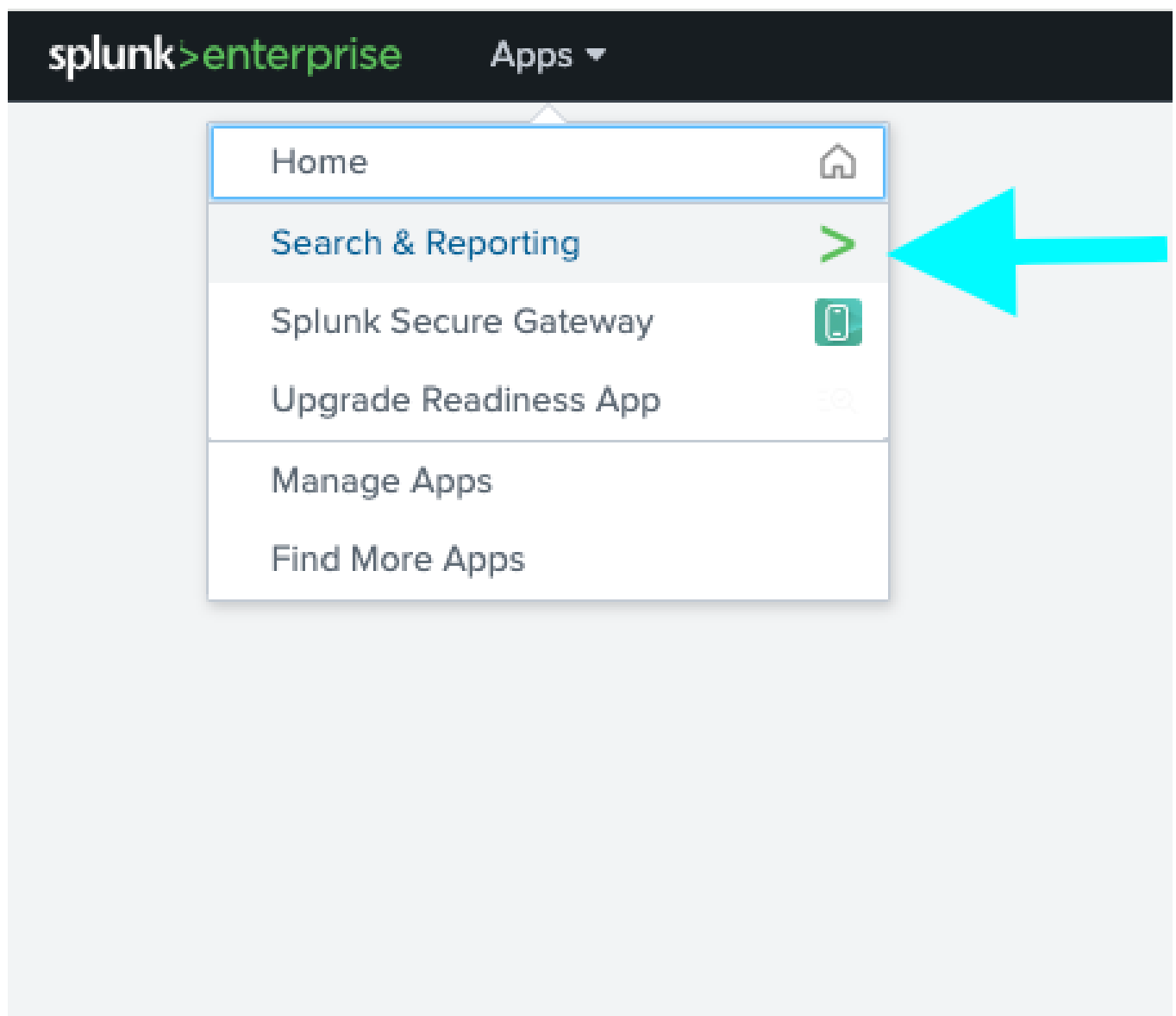
ステップ9：次のウィンドウで、設定を確認し、必要に応じて編集します。

ステップ10：検証されたら、ウィンドウの上部にある緑色のSubmit >ボタンをクリックします。

Review

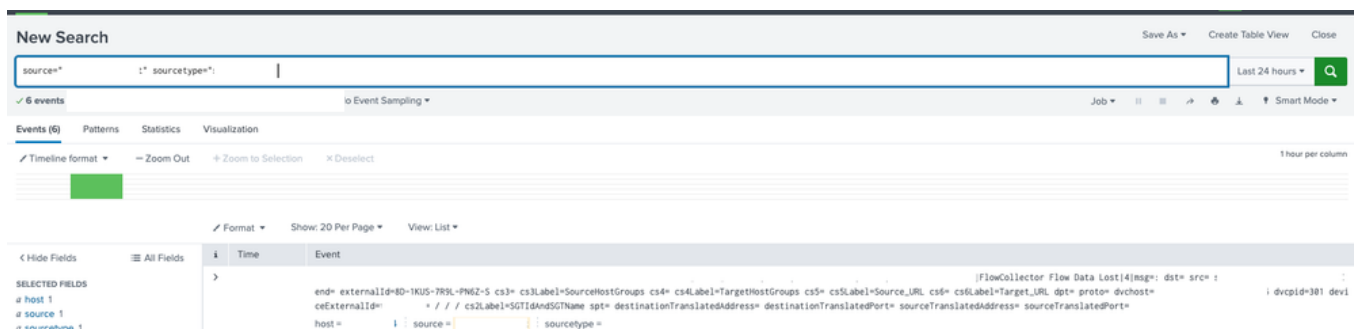
Input Type UDP Port
Port Number 514
Source name override
Restrict to Host N/A
Source Type
App Context search
Host (IP address of the remote server)
Index default

ステップ11: Web UIで、Apps > Search & Reportingの順に移動します。



ステップ12：検索ページで、フィルタ`source="As_configured" sourcetype="As_configured"`を使用して、受信した

ログを検索します。

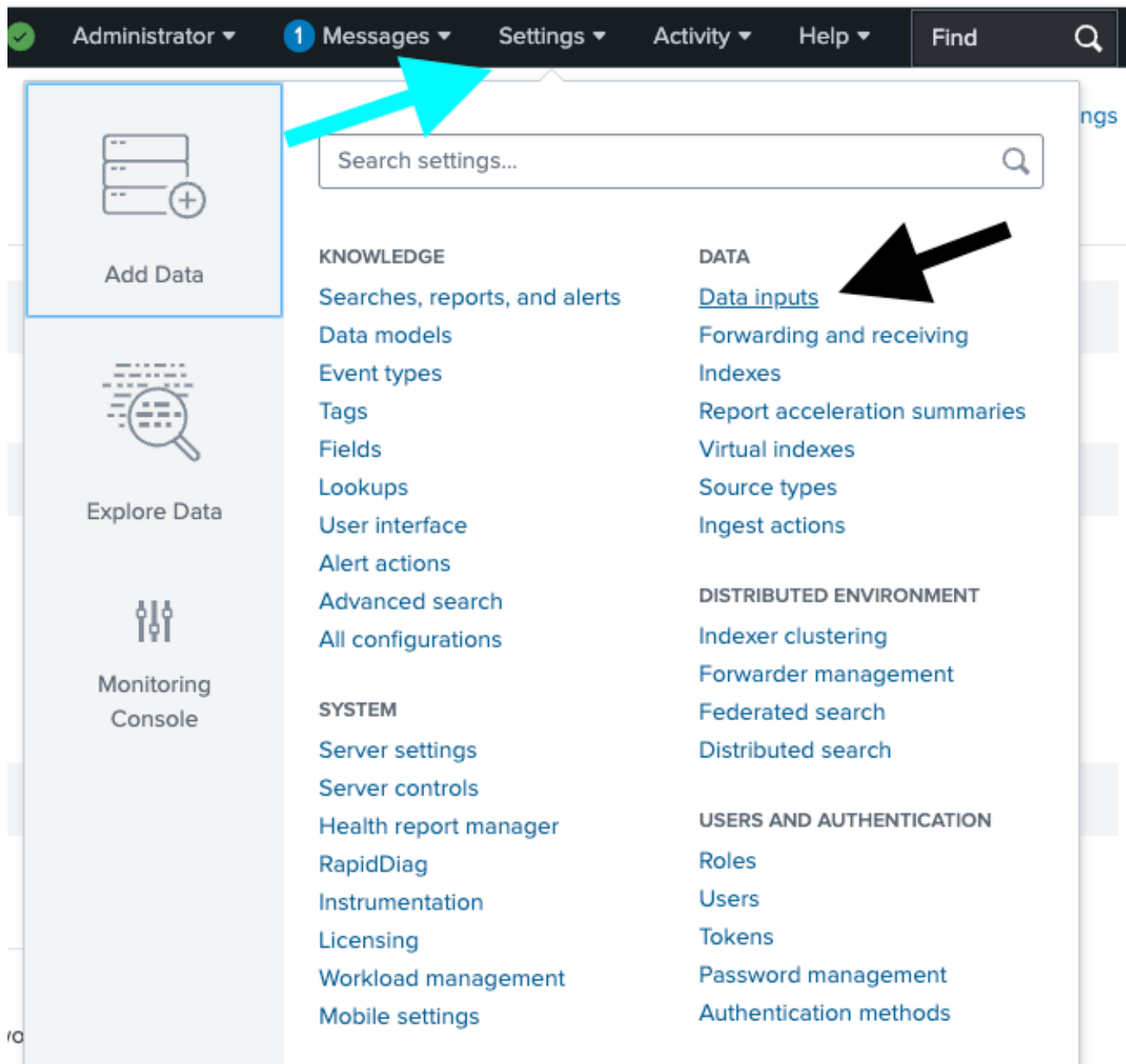


注：出典についてはステップ4を参照
source_typeについては、ステップ6を参照してください

SNA over TCPポート6514またはカスタム定義ポートでsyslogを設定する

1. TCPポート経由でSNA監査ログを受信するためのSplunkの設定

ステップ1: Splunk UIで、設定>データの追加>データ入力に移動します。



ステップ2: TCP回線を見つけて、+ Add newを選択します。

Apps

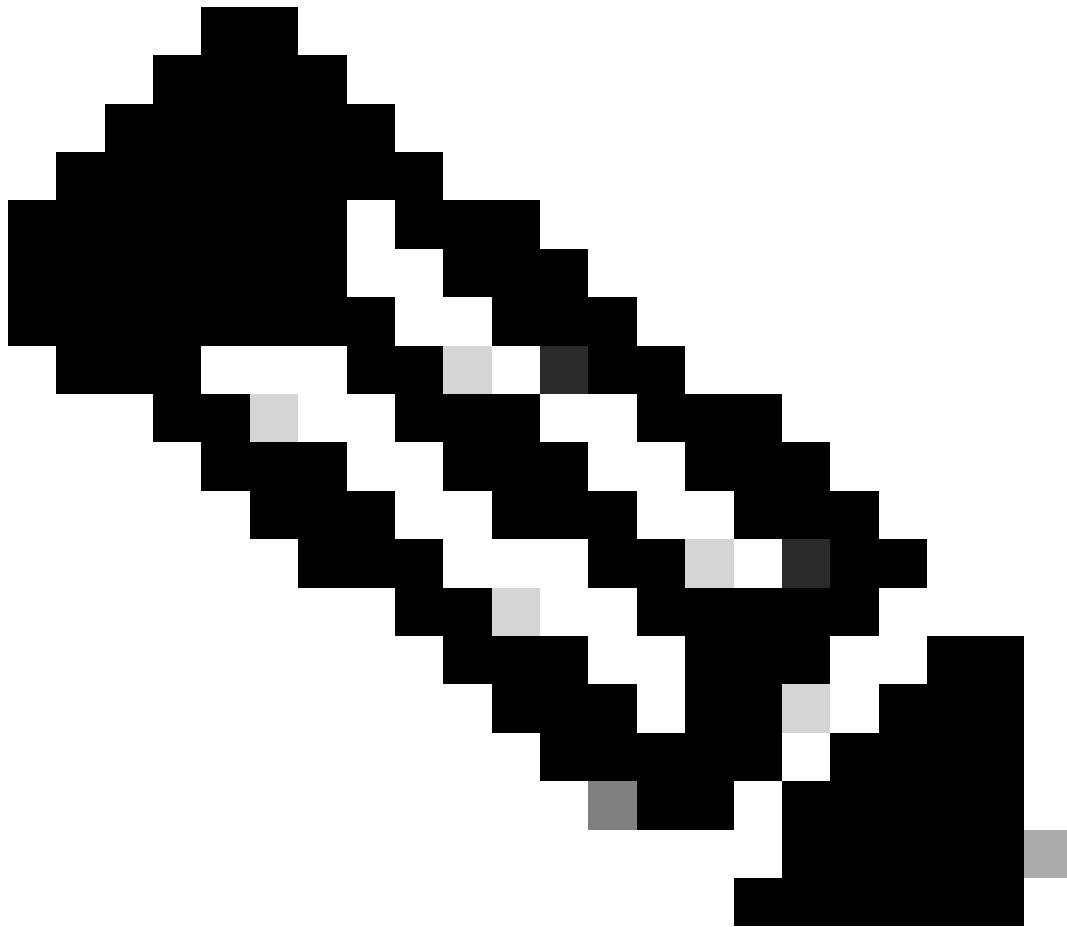
Administrator1 MessagesSettingsActivityHelp

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

ステップ3：新しいウィンドウでTCPを選択し、目的の受信ポートを入力します(例のイメージポート6514)。次に、Source name overrideフィールドに「desired name」と入力します。



注:TCP 6514は、TLS上のsyslogのデフォルトポートです

ステップ4 : 完了したら、ウィンドウ上部の緑色のNext >ボタンをクリックします。

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?

ステップ5：新しいウィンドウで、Source typeセクションのNewを選択し、Source Typeフィールドに希望する名前を入力します。

ステップ6:Hostセクションで、MethodにIPを選択します。

ステップ7：完了したら、ウィンドウの上部にある緑色のReview >ボタンを選択します。

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

Add Data

Select Source Input Settings Review Done

< 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.

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

ステップ8：次のウィンドウで、設定を確認し、必要に応じて編集します。検証が終わったら、ウィンドウの上部にある緑色のSubmit >ボタンをクリックします。

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

Add Data

Select Source Input Settings Review Done

< 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. Splunkの証明書の生成

ステップ1:opensslがインストールされたマシンを使用して、`sudo openssl req -x509 -newkey rsa:4096 -keyout server_key.pem -out server_cert.pem -sha256 -days 3650 -subj /CN=10.106.127.4`コマンドを実行し、10.106.127.4の例のIPをSplunkデバイスのIPに置き換えます。ユーザー定義のパスフレーズを入力するように求めるプロンプトが2回表示されます。この例では、Splunkマシンのコマンドラインからコマンドが実行されています。

[illegible]

コマンドが完了すると、2つのファイルが生成されます。server_cert.pemファイルとserver_key.pemファイル

```
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:
```

手順2: rootユーザーに切り替えます。

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

ステップ3: 新しく生成された証明書を /opt/splunk/etc/auth/ にコピーします。

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

ステップ4: spunkweb.cerファイルに秘密キーを追加します。

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

ステップ5:Splunk証明書の所有権を変更します。

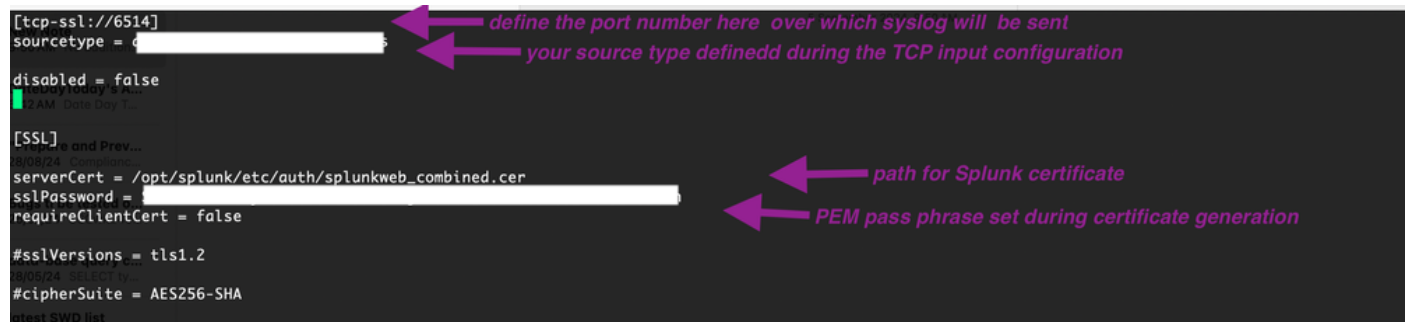
```
user@examplehost:~# chown 10777:10777/opt/splunk/etc/auth/splunkweb.cer
```

ステップ6: Splunk証明書の権限を変更します。

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

ステップ7: 新しいinput.confファイルを作成します。

```
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

ステップ8: searchを使用してsyslogを確認します。

Home



Search & Reporting



Splunk Secure Gateway

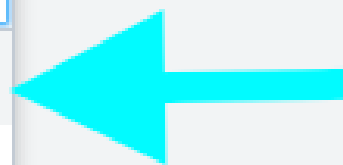


Upgrade Readiness App



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. SNAでの監査ログの宛先の設定

ステップ1: SMC UIにログインし、Configure > Central Managementの順に選択します。



nse



Monitor



Investigate



Report



Configure

Configure



Detection

Host Group Management

Alarm Severity

Policy Management

Response Management

Network Scanners

Analytics

Alerts

Global

 Central Management

... ..

ステップ2：目的のSNAアプライアンスの省略記号アイコンをクリックして、Edit Appliance Configurationを選択します。

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				...

ステップ3:Network Servicesタブに移動し、Audit Log Destination(Syslog over TLS)の詳細を入力します。

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) *

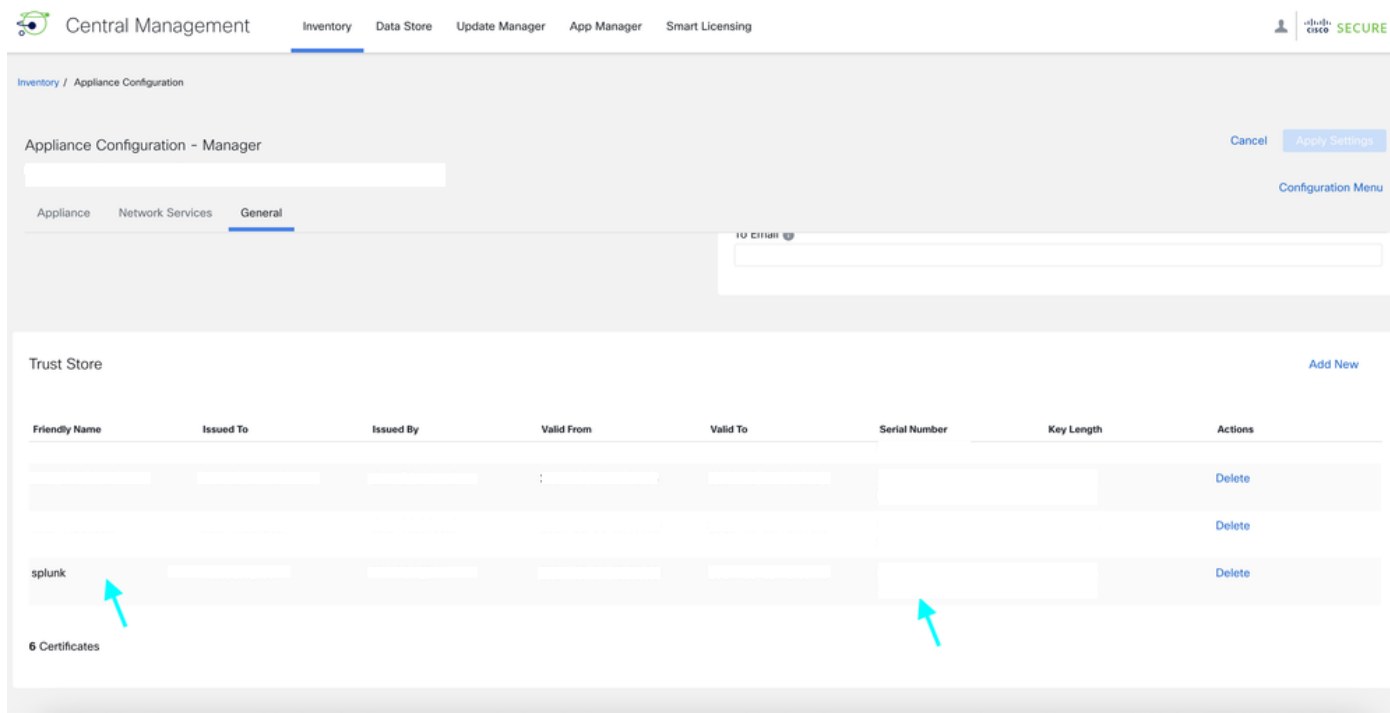
Certificate Revocation

☒ Disabled

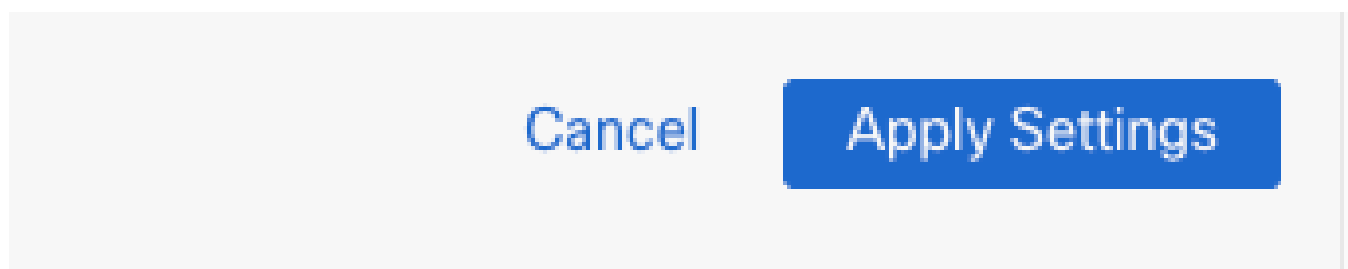
☐ Soft Fail

☐ Hard Fail

ステップ4:Generalタブに移動し、一番下までスクロールします。Add newをクリックし、前に作成したserver_cert.pemという名前のSplunk証明書をアップロードします。



ステップ5:Apply settingsをクリックします。



トラブルシューティング

検索で完全な意味不明の文字列が表示される可能性があります。



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

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。