

syslog شادحأ لاسرإل ةباجتسالا ةرادإ نيوكت SPLUNK ىلإ

تايوتحمل

[ةمدقملا](#)

[ةيساسالاب لطلتلا](#)

[تاب لطلتلا](#)

[ةمدختسمل تانوكمل](#)

[صصخملا ددحمل دزنملا وأ 514 UDP ربع SNA ىلع syslog نيوكت](#)

[1.SNA رادصلا SNA ماظن ربع ةباجتسالا ةرادا](#)

[عانيم UDP ربع syslogs SNA ملتسي، نأ Splunk لكشي، 2.](#)

[ددحم صصخم دزنم وأ 6514 TCP ربع SNA ىلع syslog نيوكت](#)

[TCP دزنم ربع SNA قيقدت تالجتس يقلت Splunk نيوكت، 1.](#)

[2.SPLUNK ل ةداهش عاشنا،](#)

[3.SNA ىلع قيقدتلا لجتس ةهجو نيوكت.](#)

[اهخالصاو عاطحألا فاشكتسا](#)

ةمدقملا

شادحألا لاسرإل "ةنمآلا تاليلحتلا ةباجتسالا ةرادا" ةزيم نيوكت ةيفيك دنتسمل اذه فصوي
Splunk لثم ةيجراخ ةهج ىلإ syslog ربع.

ةيساسالاب لطلتلا

تاب لطلتلا

ةيلالتلا عيضاوملاب ةفرعم لكي دل نوكت نأ Cisco ي صوت:

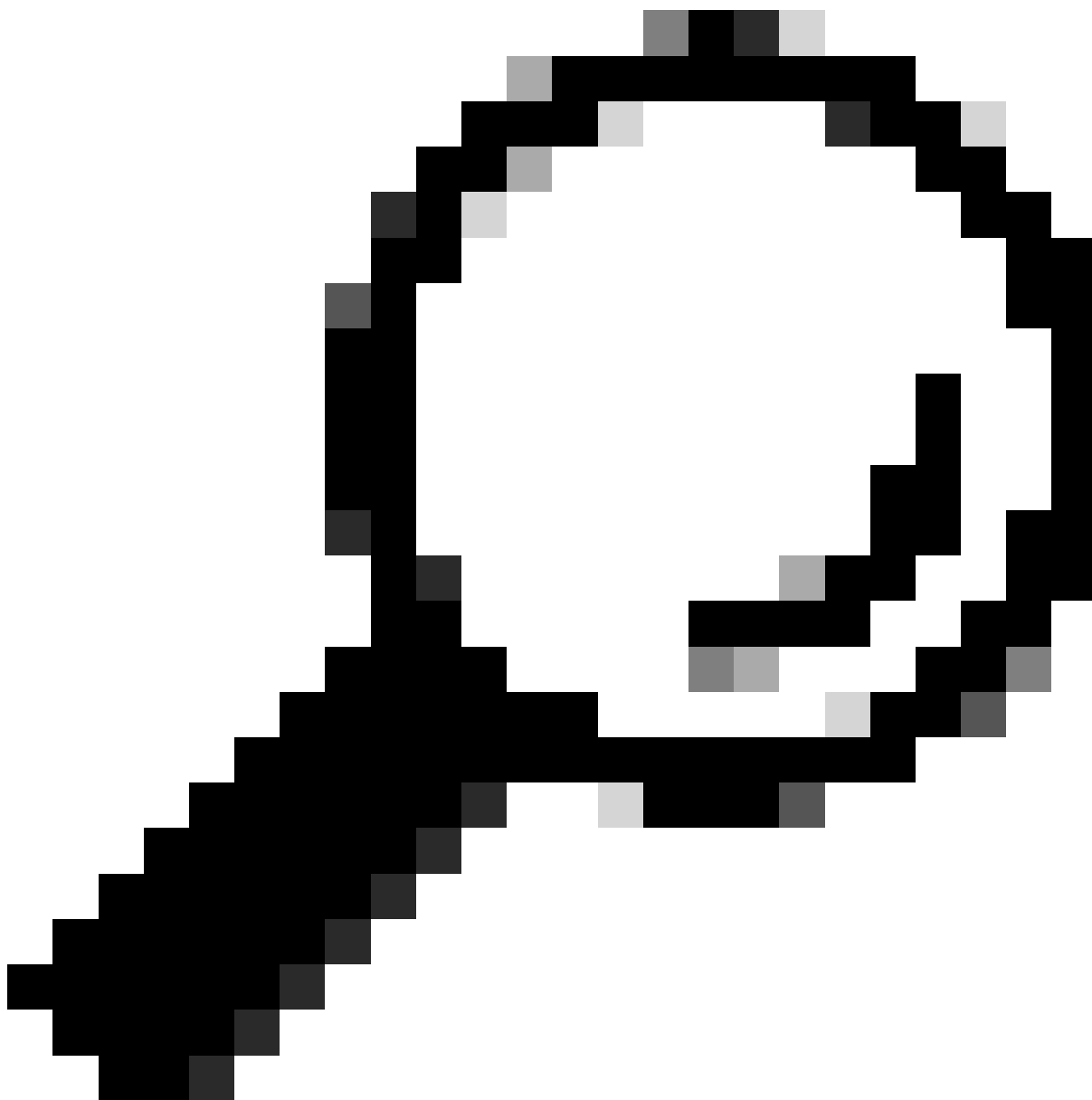
- ةنمآلا ةكبشل تاليلحتلا ةباجتسالا ةرادا.
- Splunk Syslog

ةمدختسمل تانوكمل

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألا نم دنتسمل اذه يف ةدراول تامولعمل عاشنإ مت
تناك اذا. (يضايرتفا) حوسمم نيوكتب دنتسمل اذه يف ةمدختسمل ةزهجألا عيمج تأدب
رمأ يأل لمحتمل ريثأتلل كمهف نم دكأتف، ليغشتلا ديقتك ككبش.

- لقألا ىلع دحاو Manager زاهج ىلع يوتحت يتللا (SNA) ةنمآلا ةكبشل تاليلحت رشن
دحاو قفدت عجم زاهجو.
- اذف نم 443 ربع هيلإ لوصولو Splunk مداختي بثت مت.

ددحم لآ ذفنم لآ وأ 514 UDP رب ع SNA ىل ع syslog ني وكت ص صخم لآ



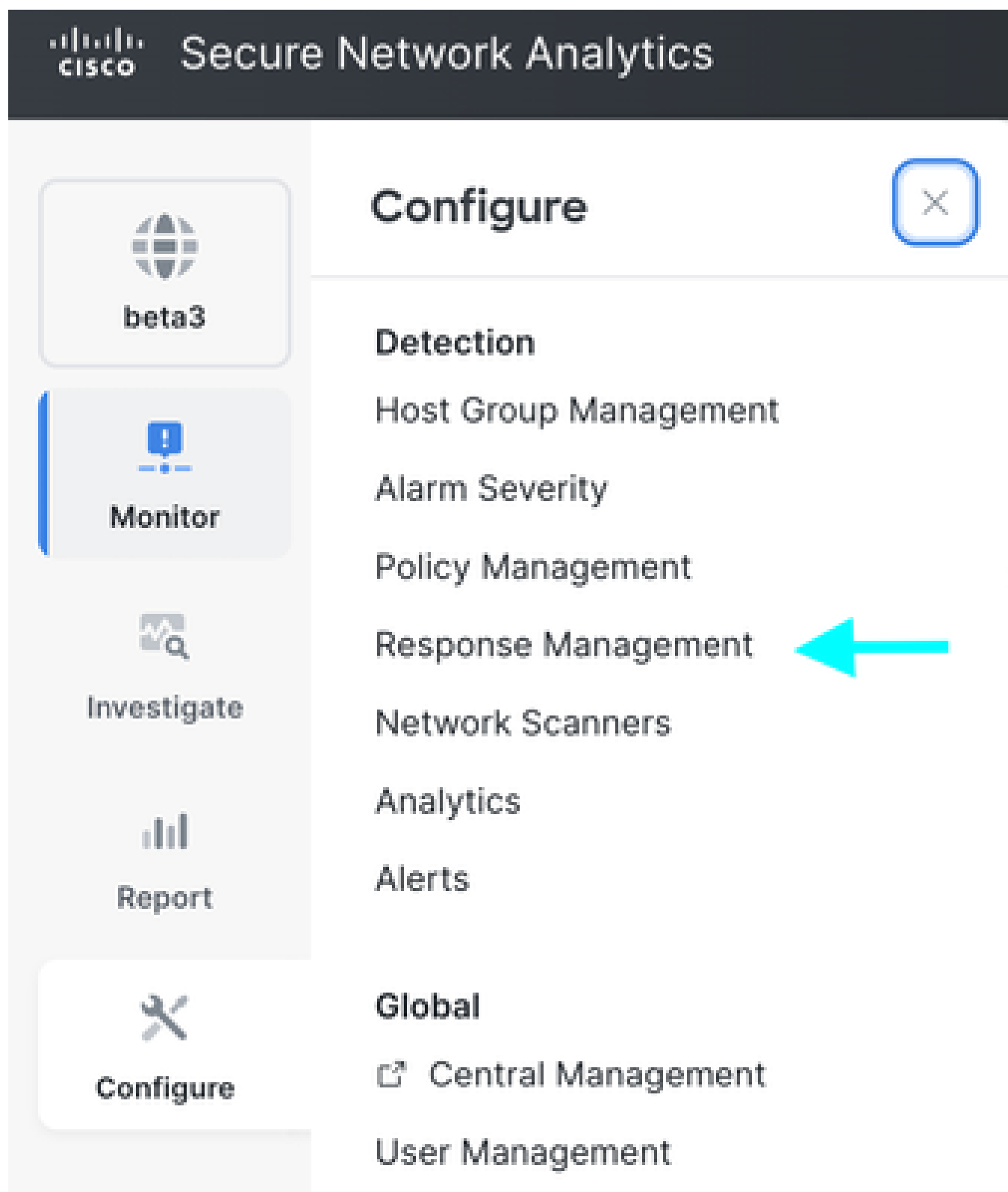
ه ب حوم سم syslog ل هراتخت ص صخم ذفنم يآ وأ TCP/6514، UDP/514 نأ نم دكأت: حيم لت
SNA و Splunk. ني ب ةطيسو ةزهجأ وأ ةيامح ناردي يآ ىل ع

1. SNA رادصل لآ SNA ماظن رب ع ةباجت سالا ةرادإ

دعاوق لآ ني وكت ل (SA) ةنم لآ تاليلحت لآب ص لآ ةباجت سالا ةرادإ نوكم مادختسا نكم ي
syslog. تاهجوو تاءارجل او

ىرخأ تاهجوو لآ Secure Analytics تاهي بن ت هيجوت ةداع لآ لاس رال تارايل لآ هذو ني وكت ب جي

ةباجتسا ةرادا > نيوكتل الى لقتناو SA ةرادا زاهج الى لوخدلا ليچستب مق 1: ةوطخل
فشكلا.



رطسلا رصنع ناكم ددح، تاءارجا بيوبتل ةمالع الى لقتنا، ةديدل ءحفصل يف 2: ةوطخل
ريحت مٲ، ءارجلا دومع يف (...) فذل ءمالع قوف رقناو يضارتفالا syslog الى لاسرا.

Response Management

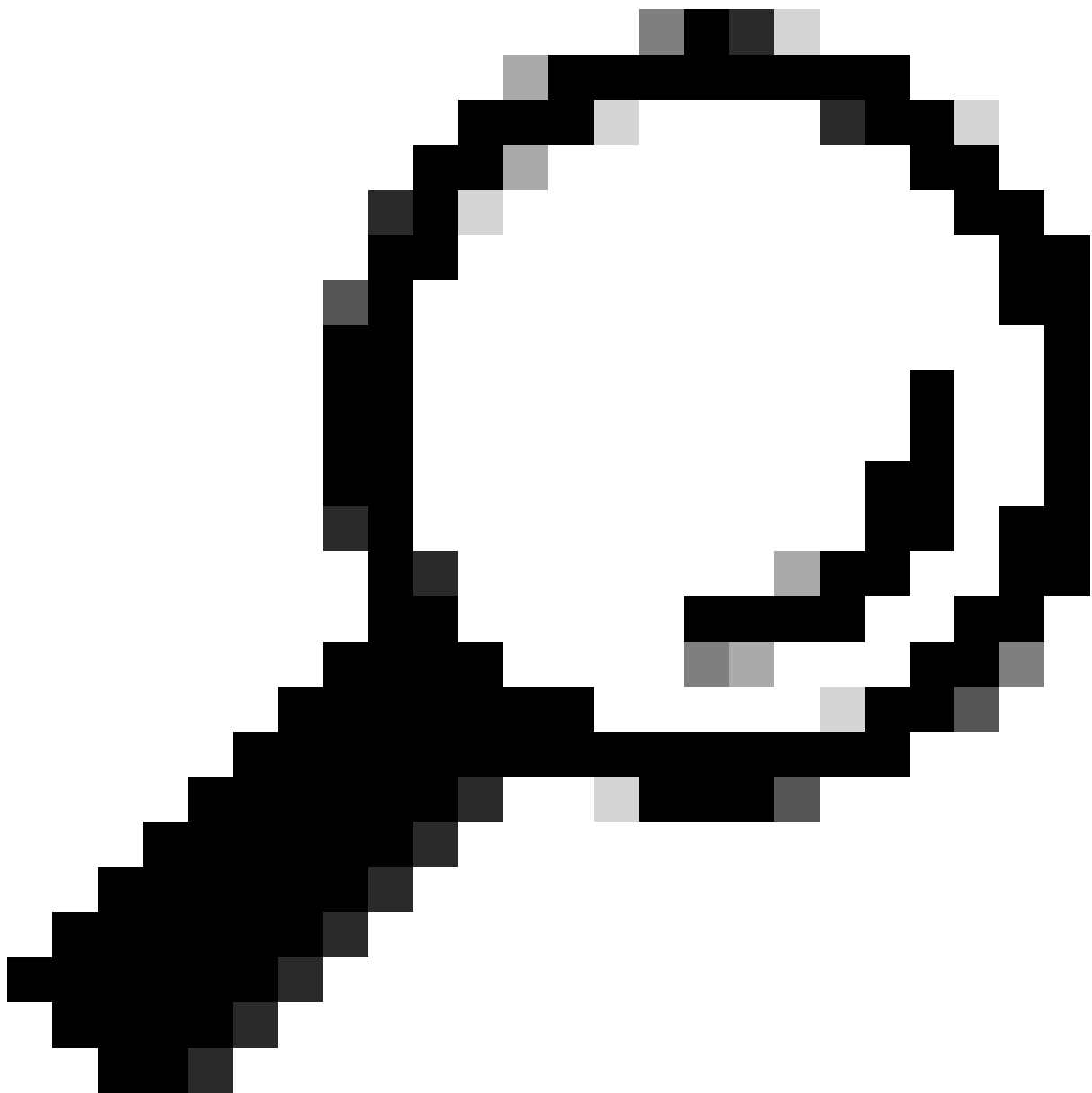
Rules Actions Syslog Formats

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	☒	... Edit Duplicate Delete
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	☐	

لا يفءانيم ملتسي بةهچولوا، لاجم ناوع لدان syslog ل يف ناوع ةيغال تلخد: 3 ةوطخل
CEF دح ةلاسرل قيسنت يف. لاجم ءانيم UDP
ينمي لاي لعل ةيوازلا يف قرزالا ظفح رز رقنا، لامكإل دنع: 4 ةوطخل



514 syslog لءانېم UDP رېصقتلا :خېملت

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

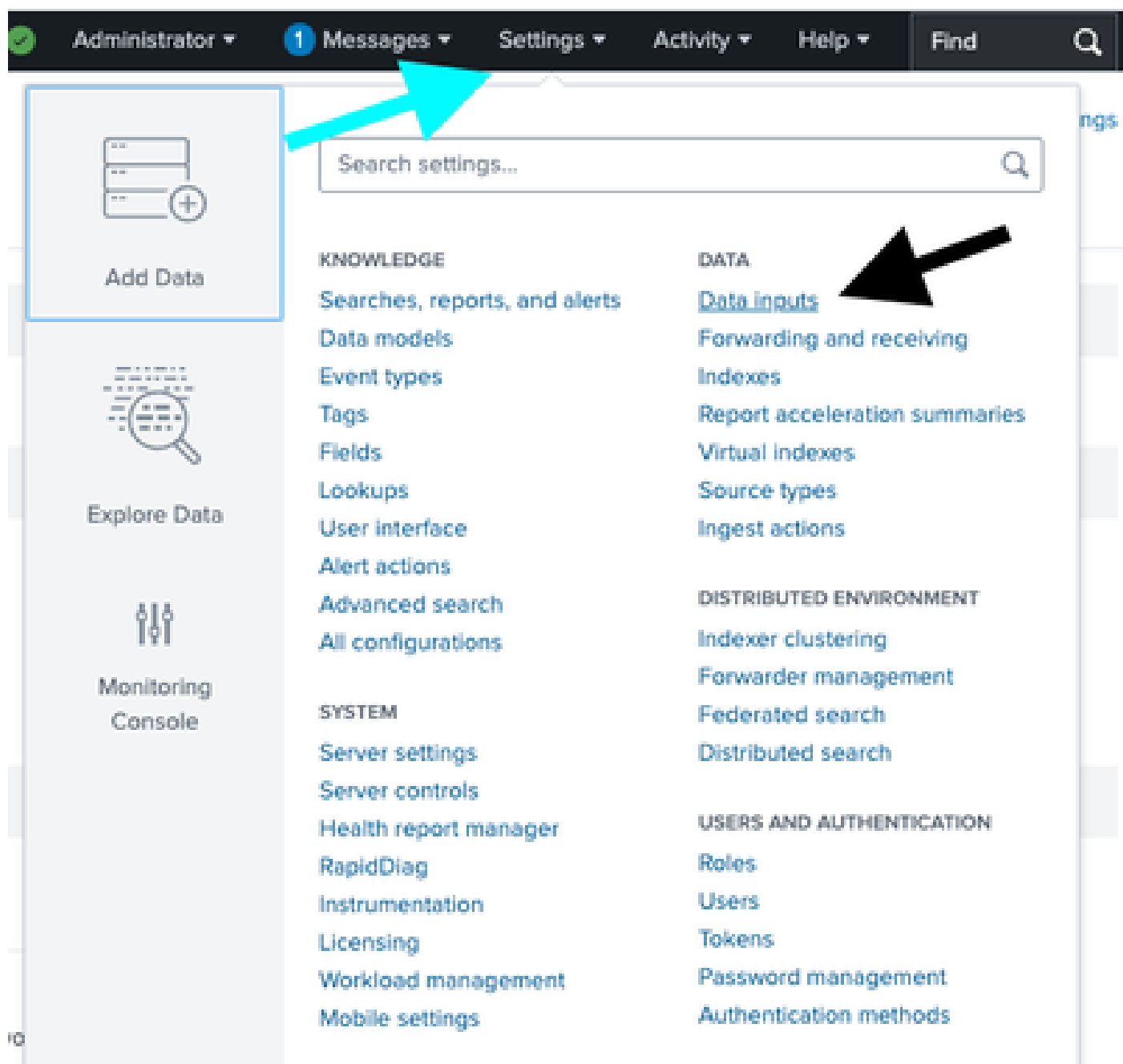
<131>Jan 01 00:00:00 test.host TestApp[1337]: CEF:0|Cisco|7.3.0|Notification:99|Bad Host|5|msg=This host has been observed performing malicious actions toward another host.:Source Host is http (80

Test Action

ءانيم UDP ربع SNA syslogs ملتسي نأ Splunk لكشي.2

ةكبشلا تاليلحت ةرادإل بيو مدختسم ةهجاو ىلع كب ةصاخلا تاريغيغتلا قيبطت دعب
Splunk في تانايبلا لاخدا نيوكت بجي ،ةنمآلا

تالاخدا > تانايب ةفاضإ > تادادعإلا ىلإ لقتناو Splunk ىلإ لوخدلا ليچستب مق :1 ةوطخلا
تانايبلا تانايب



ديج ةفاض|+ ددجو UDP رطس ع قوم ددج: 2 ةوطخلا

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

لإضافة UDP كمدخل جديد، انقر على + Add new في عمود UDP. لاحظ أن العدد 1 في عمود Inputs يشير إلى أن هناك مدخل واحد من نوع UDP موجود بالفعل. إذا كنت ترغب في إضافة مدخل جديد، فسيكون العدد 2.

الخطوة 5: إعداد المدخل UDP. في صفحة إعداد المدخل، أدخل اسم المصدر (desired name of source) في حقل Name، وحدد نوع المدخل كـ UDP في قائمة Input type.

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?

ردصملا عون لقح ناكم ددح ديدج رايج ىلإ ليدبتلاب مق ،ةيلاتلا ةحفصلا يف 6 ةوطخلا desired source . لخدأو

بولسألل IP ددح 7 ةوطخلا .

ةشاشلا ىلعأ دوجوملا رضخألا > ةعجارم رزقوف رقنا 8 ةوطخلا .

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.

SelectNew

Source Type

Source Type Category

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 ?

IPDNSCustom

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

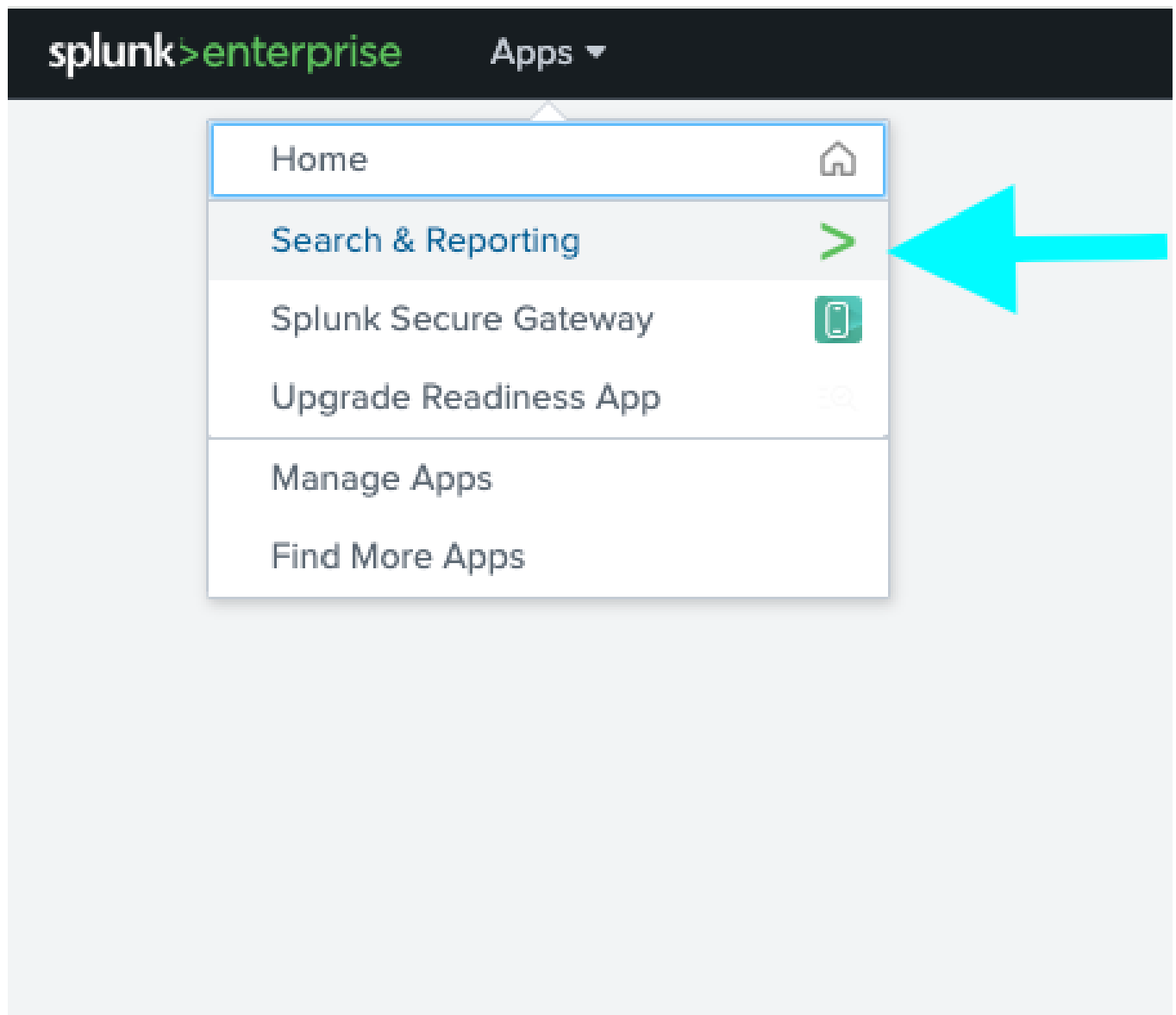
- رمأل مزل اذا ررحوكتادادعإعجار،يلالاتل راطإلال في 9 ةوطخل

هتحص نم ققحتلال درجمب راطإلال ىلعأ دوجومل "رضخأل" لاسرل رزقوف رقنا 10 ةوطخل

Review

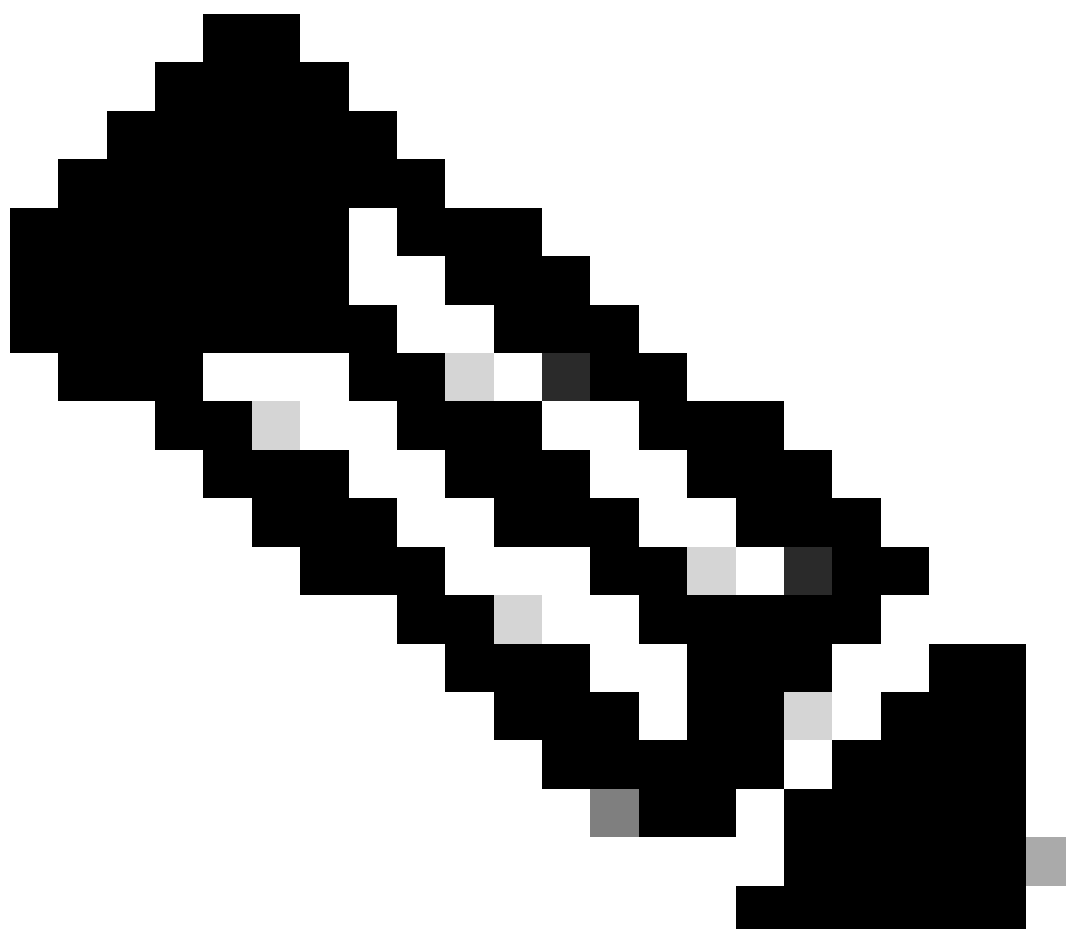
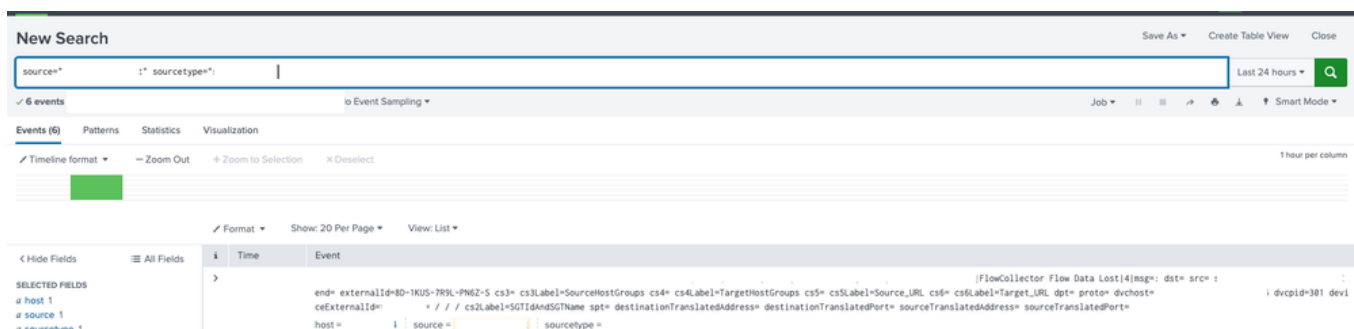
Input Type UDP Port
 Port Number 514
 Source name override
 Restrict to Host N/A
 Source Type
 App Context search
 Host (IP address of the remote server)
 Index default

ب.ي.ول المدخستسم ةهجاو ي ف ريراقت دادعإو ثحب > تاقبيبطت ىلإ لقتنا : 11 ةوطخلا



12 ةوطخلا source="As_configured" في صفتلا لماع مدختسأ ،ثحبلا ةحفص ي ف

source="As_configured" اه ي قل ت م ت ي ل ل ا ل ا ل ج س ل ل ا ن ع ش ح ب ل ل

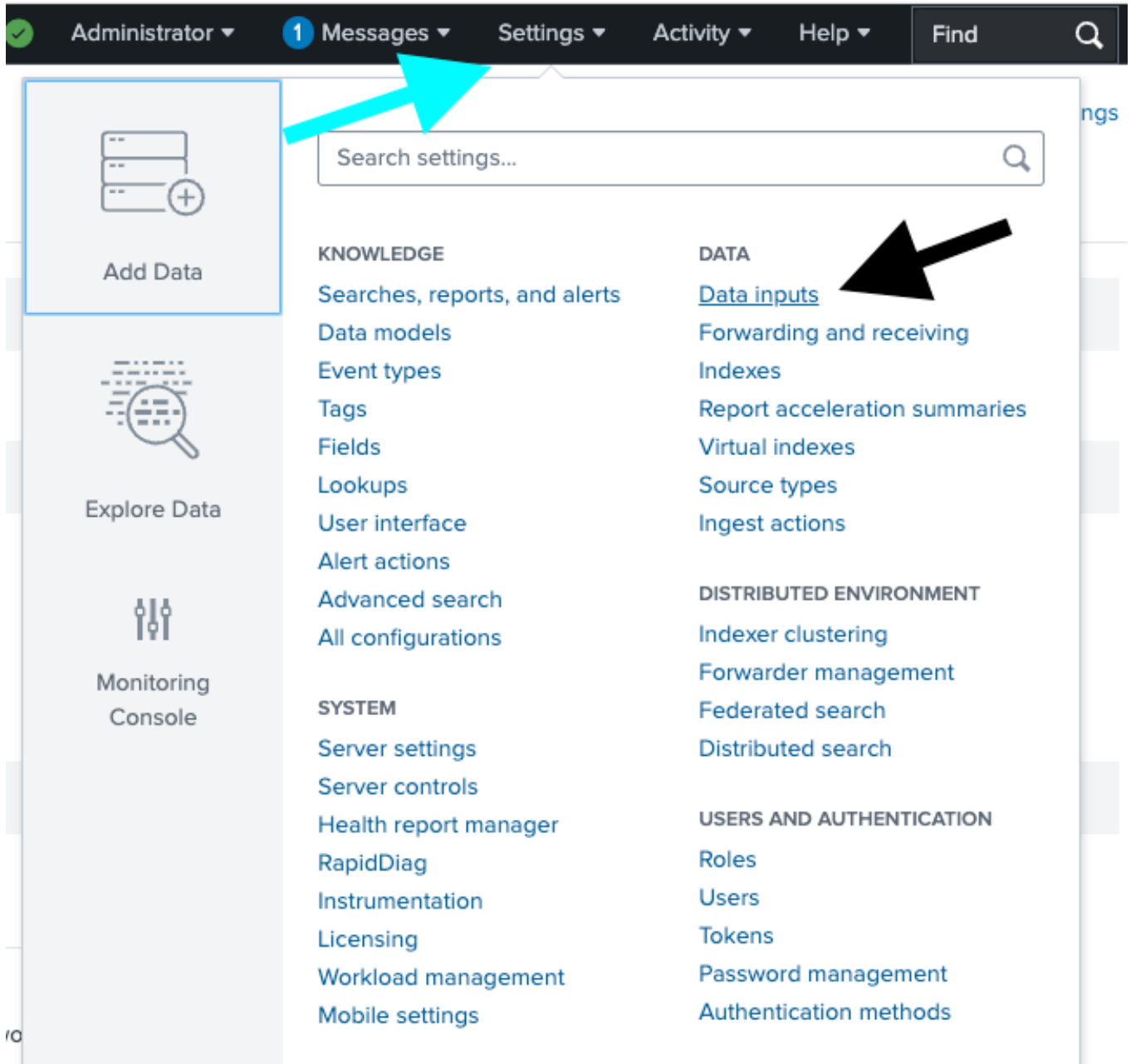


4 ة و ط خ ل ا ع ج ا ر ، ر د ص م ل ا ي ل ع ل و ص ح ل ل : ة ط ح ا ل م
6 ة و ط خ ل ا ع ج ا ر source_type ي ل ع ل و ص ح ل ل

ص ص خ م ذ ف ن م و ا 6514 ذ ف ن م TCP ر ب ع SNA ي ل ع syslog ن ي و ك ت
د د ح م

TCP ذفنم ربع SNA قيقدت تالچس يقلتل Splunk نيوكت.1

تانايب تالخدم > تانايب ةفاضإ > تادادعإلإ لقتنا Splunk، مدختسم ةهجاو يف 1: ةوطخل تانايبلا.



ديج ةفاضإ + ددحو TCP رطس عقوم ددح: 2: ةوطخل

Apps

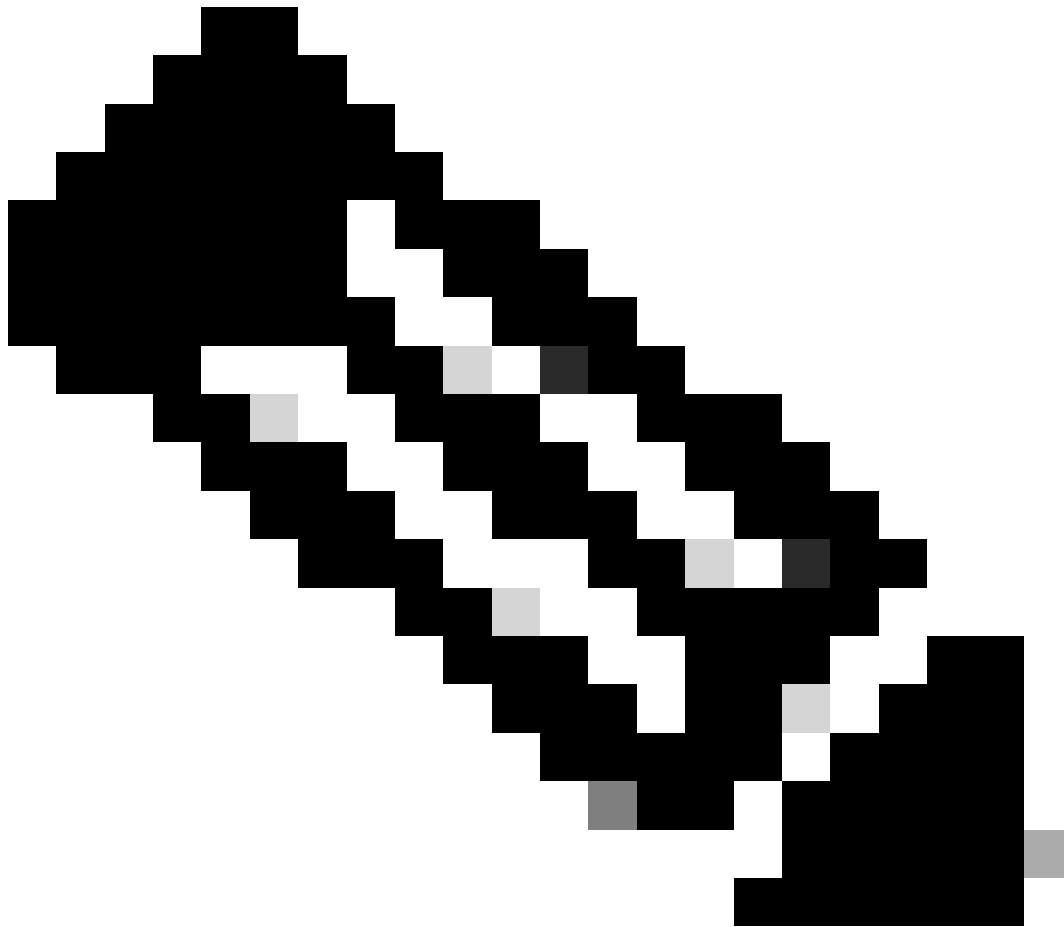
Administrator1 MessagesSettingsActivityHelp

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

ةروس لاثم ي ف ،بولطمال لابقتسالال ذفنم لخدأ ،TCP دح ةديجال ةذفانلالي ف :3 ةوطخلال
ردصمالمسا زواجت لقح ي ف "بوغرمالمسالال" لخدأو ،6514 ءانيم



TLS رېب ع syslog ل ءانيم ري صقت TCP 6514 :ةطحالم

.ةذفانلا ىل عأ دوجوملا > رضألل يلاتلا زللا قوف رقنا ،ءاهت نالا دن ع :4 ةوطخلا

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 Journal Input for Splunk
This is the input that gets data from journal (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?

لحق في بوجرمال مسالا لخدأ ، ردصملا عون مسق في ديدج دح ةديدجال ةذفانلا في : 5 ةوطخل ردصملا عون

فيضمل مسق في بولسألل IP دح : 6 ةوطخل

ةذفانلا ىلعأ دوجوملا عارضخل > ةعجارم رز دح ، لامكإل دنع : 7 ةوطخل

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.

Source Type: (Select New)

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

رقنا، ءحصلال نم ققحتال مت نإ ام .رمأل مزل اذا ررحوكتادادعإ عجار ،يلالال رابطال ي ف :8 ةوطخال رابطال لىلعأ ءوومال "رضألأ" لاسرل رز قوف

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

SPLUNK ل ةءاهش عاشنإ.2

-x509 sudo openssl req -x509 -keyout server_key.pem -out server_cert.pem -sha256 -days 3650 -subj /CN=10.106.127.4 newkey rsa:4096 -keyout server_key.pem -out server_cert.pem -sha256 -days 3650 -subj /CN=10.106.127.4

IP لاثم ال لادبتسا عم ،هيعل OpenSSL تيبتت مت زاه مادختساب :1 ةوطخال

ةفرعم رورم ةرابع لاخدا نيترم كنم بلطي س. Splunk زاهب صاخال IP ب 10.106.127.4 ب صاخال

Splunk زاهب صاخال رماوال رطس نم رماوال ليغشت متي ،ةلثم ال ي ف. مدختسم ال لبق نم

```
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:
```

server_key.pem و server_cert.pem افلم. نى فلم عاشن امتى، رمالا لامتك دنع

```
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:
```

۲. ورودی‌ها را به خروجی‌ها اختصاص دهید.

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

3: عوطخلا /opt/splunk/etc/auth/ ىل اشي دح اهؤاشن مت يتل ءداهشل خسن:

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

صا خات فمب spunkweb.cet فلم قاحل: 4 ةوطخل

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

میسقت ۋداهش ۋیكل مریغت : 5 ۋوطخلا

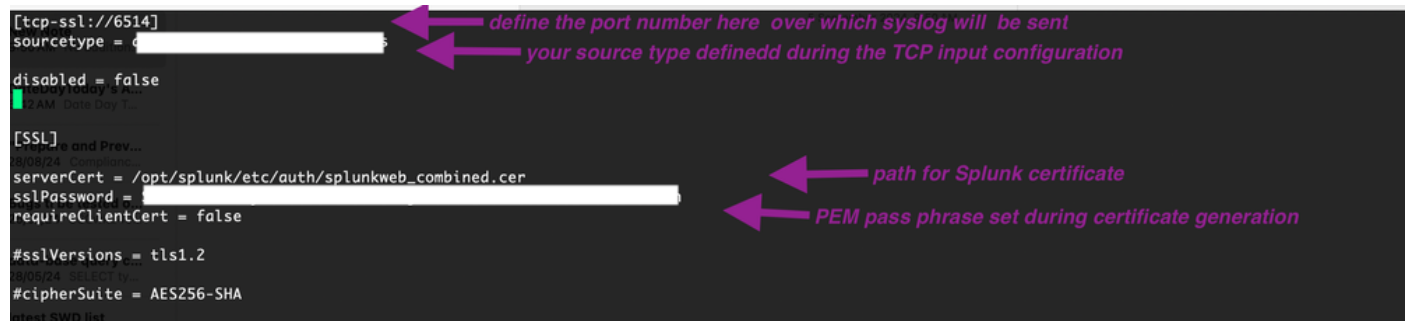
```
user@examplehost:~# chown 10777:10777/opt/splunk/etc/auth/splunkweb.cer
```

ميسقتال اءءاهشل نءال ريغت 6: ءوطءال

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

ءيءء input.conf فللم ءاشناب مق 7: ءوطءال

```
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

ءءب للمءءسسي syslogs ال ءققء 8: ءوطءال

Home



Search & Reporting



Splunk Secure Gateway

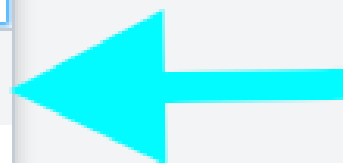


Upgrade Readiness App



Manage Apps

Find More Apps



New Search

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

126 events | No Event Sampling

Events (126) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

1 hour per column

List Format 50 Per Page

< Hide Fields All Fields

SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- # date_hour 5

Time	Event
>	<
host = source = sourcetype =	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

SNA ىل ع قيقدتلا لىس ةهجو نيوكت.3

ةيزكرمل ةرادلا > نيوكت ىلا لقنتنا SMC UI ىلا لوخذلا لىس :1 ةوطخلا



nse



Monitor



Investigate



Report



Configure

Configure



Detection

Host Group Management

Alarm Severity

Policy Management

Response Management

Network Scanners

Analytics

Alerts

Global

 Central Management

زاهج النيوكت ريرحت ددح بولطم ال SNA زاهج ل يواضي بل لكشال زمر لىل عرقنا 2: ةوطخل

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				...

قيقدت ال لجس ةهجو لي صافات لخدأو ةكبش ال امدخ بيوبت ال ةمالع ىلإ لقتنا : 3 ةوطخل (Syslog ربع 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

ةفاضل قوف رقنا لفسأ ىلإ ريرمتلاب مق م، "ماع" بيوبت ال ةمالع ىلإ لقتنا : 4 ةوطخل server_cert.pem مساب اقبس م اهؤاشنإ مت يت ال Splunk ةداهش ليحتل ديدج

Central Management

Inventory
Data Store
Update Manager
App Manager
Smart Licensing

Inventory / Appliance Configuration

Appliance Configuration - Manager

Cancel
Apply Settings

Configuration Menu

Appliance
Network Services
General

TO EMAIL

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

دادعإ ةي لمع قبطي ةق طقط : 5 ةوطخل

Cancel

Apply Settings

اهحال صإو ءاطخأل افاشكتسا

ثحبلا ىلع رهظي لماك ضومغ كانه نوكي نأ نكمي

splunk>enterpriseApps

AdministratorMessagesSettingsActivityHelpFind

SearchAnalyticsDatasetsReportsAlertsDashboards

Search & Reporting

New Search

Save AsCreate Table ViewClose

source*" sourcetype*" i"

156 events () No Event Sampling

Job

Smart Mode

Events (156)PatternsStatisticsVisualization

Format TimelineZoom OutZoom to SelectionDeselect

1 hour per column

ListFormat50 Per Page

< Hide FieldsAll Fields

SELECTED FIELDS
host 1
source 1
sourcetype 1

INTERESTING FIELDS
index 1
linecount 6
punct 79
splunk_server 1
timestamp 1

34 more fields
+ Extract New Fields

i	Time	Event
>		<pre>\x00 Z \x00 \x00 host = source = sourcetype =</pre>
>		<pre>* \x00 & \xE3D \x9F8\x91\xD3\xF9\x82 \xF8F\x9F\xE5R\xE8\xED \x92\xC0\xE5\xE5\xA38:\xA2\xEB (i 0/\x00\x9E\x00J\x00g\xC0,\xC00\x00\x9F\x00\xFF \x00\x00\xBF\x00 \x00\x00\x00 \x00\x00\x00+\x00 \x00,\x00* \x00 \x00 \x00\x00 \x00 \x00 \x00 \x00 \x00\x00\x00\x00\x00\x00G\x00E\x00 \x00A \xA7\xB9\xB3\xEC\xC91 \x81g=R \^d\xC1 \xD0As[z\x9C 9\xE1\x91\xEC\xEDw\xD9p 6\x954\x88U\xC4\xFA\x920\xA5\x81!\xA3 \x00\x9F&\xA4\x87/t\xFD\xCD\xE0\x92\x89\xEA \x88 host = 10106.12713 source = sourcetype =</pre>
>		<pre>\x00 Z \x00 \x00 host = 10106.12713 source = sourcetype =</pre>
>		<pre>* \x00 & <Gk- AInp"J >\x97h\xF9R2 u\x9E \x91\xATT\x8C\xB0\xDCY , I (' \xAE\x84+\xF0B\xC3s , \xBA(\xF1\x9A \xED\xD3\xFC6\xFE\x8C\x98E\xC5\xD9\x00 0\xFF \x00\x00\xBF\x00 \x00\x00\x00 \x00\x00\x00+\x00 \x00 \x00 \x00 \x00\x00\x00\x00 \x00 \x00\x00\x00\x00\x00 \x00,\x00* \x00 \x00 \x00\x00 \x00 \x00</pre>

Show all 6 lines

Google Chrome

الحل:

حی حاصل ردصملا عون یلإ لاخ دال نیی عتب مق



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

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م ج ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م ج ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م ج ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م ج ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م ج ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا