

Guide for ingesting data.

Draft event in json format:

```
[{"publish_time": 1691770693.545, "data": {"insertId": "abcd02efghijkl", "jsonPayload": {"eventId": "12345-2lad", "client": {"ip": "127.0.0.6", "port": 52847}, "component": "OAuth", "eventName": "ACCESS-OUTCOME", "http": {"request": {"headers": [{"accept": ["application/json"], "host": ["authz-api.euw2.test01"], "user-agent": ["Java/11.0.15"], "x-forwarded-for": ["10.10.10.2"], "x-forwarded-proto": ["https"], "x-request-id": ["Test01-cyber01"]}], "method": "GET", "path": "http://authz-api.euw2.cyber/root/abc_uri", "secure": false}}, "level": "INFO", "realm": "/", "response": {"elapsedTime": 2, "elapsedTimeUnit": "MILLISECONDS", "status": "SUCCESSFUL", "statusCode": "200"}, "source": "CyberEscape", "timestamp": "2023-08-11T16:18:10.630z", "topic": "access", "transactionId": "12345-2lad-1234"}, "labels": {"compute.googleapis.com/resource_name": "test01-CyberEscape01", "k8s-pod/app": "cyber", "k8s-pod/app_kubernetes_io/managed-by": "CyberEscape", "k8s-pod/app-kubernetes_io/name": "cyber", "k8s-pod/pod-template-hash": "2c975669ab", "k8s-pod/tier": "middle"}, "logName": "projects/cyber01/logs/stdout", "receiveTimeStamp": "2023-08-11T16:18:13.230378875z", "resource": {"labels": {"cluster_name": "test01-CyberEscape01-euwe2", "container_name": "opencyber", "location": "europe-west2", "pod_name": "cyber-1234cd", "project_id": "test01-CyberEscape01"}, "type": "k8s_container", "severity": "INFO", "timestamp": "2023-08-11T16:18:10.630351429z"}, "attributes": {"logging.googleapis.com/label": {"logging.googleapis.com/label": "2023-08-11T16:18:10.630351429z"}}, "tags": [{"key": "category", "value": "access"}, {"key": "type", "value": "OAuth"}, {"key": "realm", "value": "/"}]}]
```

Settings > add data

The screenshot shows the Splunk Enterprise interface. At the top, there's a navigation bar with 'splunk>enterprise' and various dropdown menus like 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a search bar. Below the navigation is a main dashboard area titled 'Hello, Administrator'. It features several cards: 'Add data' (highlighted with a yellow box), 'Search your data', 'Add team members', 'Manage permissions', 'Product tours', and 'Learn more with Splunk Doc'. To the right of the dashboard is a sidebar titled 'Monitoring Console' which includes sections for 'KNOWLEDGE', 'DATA', 'DISTRIBUTED ENVIRONMENT', 'SYSTEM', and 'USERS AND AUTHENTICATION'. At the bottom right of the dashboard, there's a note about 'Actionable guidance on the Splunk Lantern Customer Success Center'.

Click on 'upload files from my computer'

Follow guides for onboarding popular data sources

Cloud computing

Get your cloud computing data in to the Splunk platform.

10 data sources



Networking

Get your networking data in to the Splunk platform.

2 data sources



Operating System

Get your operating system data in to the Splunk platform.

1 data source



Security

Get your security data in to the Splunk platform.

3 data sources

4 data sources in total

Or get data in with the following methods



Upload

files from my computer
Local log files
Local structured files (e.g. CSV)
[Tutorial for adding data](#)



Monitor

files and ports on this Splunk platform instance
Files - HTTP - WMI - TCP/UDP - Scripts
Modular inputs for external data sources



Forward

data from a Splunk forwarder
Files - TCP/UDP - Scripts

Select file > Next

Add Data

Selected File: **alert1.json**

Next >

Select Source

Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. [Learn More](#)

Select File

Drop your data file here

The maximum file upload size is 500 Mb

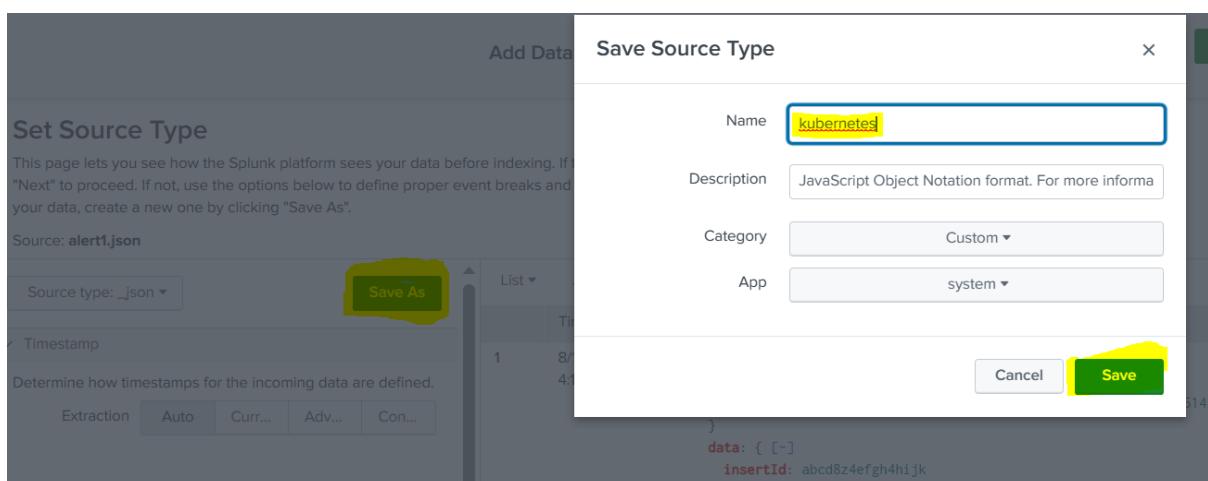
File Successfully Uploaded

Check if the data is parsed properly

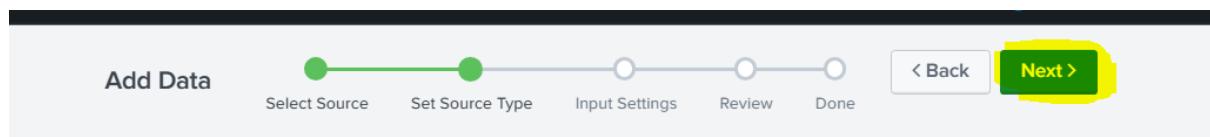
List Format 20 Per Page

	Time	Event
1	8/11/23 4:18:13.545 PM	<pre>{ attributes: { [-] }, logging. googleapis.com/timestamp: 2023-08-11T16:18:10.630351429Z } data: { [-] } insertId: abcd8z4efgh4hijk jsonPayload: { [-] } eventId: 12345-21ad client: { [-] } ip: 127.0.0.6 port: 52847 } component: OAuth eventName: ACCESS-OUTCOME http: { [-] } request: { [-] } headers: { [+] } } method: GET path: http://authz-api.ew2/cyber/root/abc_uri secure: false }</pre>

Set source type > save as > name:kubernetes > save



Click Next



r data before indexing. If the events look correct and have the right timestamps, click proper event breaks and timestamps. If you cannot find an appropriate source type for

Table ▾				
	_time	attributes.logging.googleapis.com/timestamp	data.insertId	data.jsonPayload._ever
1	8/11/23 4:18:13.545 PM	2023-08-11T16:18:10.630351429Z	abcd8z4efgh4hijk	12345-21ad
1...				

If the index doesn't exist then create a new index

The screenshot shows the 'Input Settings' step of the 'Add Data' wizard. The progress bar shows 'Select Source' and 'Set Source Type' are completed (green dots), while 'Input Settings' is in progress (light blue circle). A yellow box highlights the 'Review >' button.

Input Settings

Optionally set additional input parameters for this data input as follows:

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 ↗](#)

Constant value
 Regular expression on path
 Segment in path

Host field value: EC2AMAZ-NVS61EL

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 configuration without impacting production indexes. You can always change this setting later. [Learn More ↗](#)

Index: Default ▾ [Create a new index](#)

Name: gcp > save

New Index

X

General Settings

Index Name **gcp**

Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Index Data Type

Events

Metrics

The type of data to store (event-based or metrics).

Home Path **optional**

Hot/warm db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/db).

Cold Path **optional**

Cold db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/colddb).

Thawed Path **optional**

Thawed/resurrected db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/thawedb).

Data Integrity Check

Enable

Disable

Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.

Max Size of Entire Index

500

GB ▾

Maximum target size of entire index.

Save

Cancel

Click Review

Check all the fields and click Submit

Add Data

Select Source Set Source Type Input Settings Review Done

Review

Input Type Uploaded File
 File Name alert.json
 Source Type kubernetes
 Host EC2AMAZ-NVS61EL
 Index gcp

splunk>enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Apps Manage

Search apps by name...

Search & Reporting

Splunk Secure Gateway

Upgrade Readiness App

Find more apps

Hello, Administrator

Quick links Dashboard Recently viewed Created by you Shared with you

Common tasks

- Add data Add data from a variety of common sources.
- Search your data Turn data into doing with Splunk search.
- Visualize your data Create dashboards that work for your data.

Go in the ‘Search & Reporting’ and type:

index="gcp" sourcetype="kubernetes"

Time: all time

New Search

Save As ▾ Create Table View Close

All time ▾

Events (1) Patterns Statistics Visualization

Format Timeline ▾ – Zoom Out + Zoom to Selection × Deselect

1 millisecond per column

List ▾ Format 20 Per Page ▾			
< Hide Fields	≡ All Fields	i Time	Event
SELECTED FIELDS		> 2023-08-11T16:18:10.630351429Z	{ [-] attributes: ([*]) data: { [-] insertId: abcd8z4efghijkl jsonPayload: { [*] } labels: { [*] } logName: projects/cyber01/logs/stdout receiveTimestamp: 2023-08-11T16:18:13.230378875Z resource: { [*] } severity: INFO timestamp: 2023-08-11T16:18:10.630351429Z }
INTERESTING FIELDS			
@attributes.logging.googleapis.com/tl @host @source @sourcetype			
@data.insertId @data.jsonPayload._eventId @data.jsonPayload.client.ip # @data.jsonPayload.client.port @data.jsonPayload.component @data.jsonPayload.eventName @data.jsonPayload.http.request.header			

The fields are indexed on the left panel

index="gcp" sourcetype="kubernetes"

✓ 1 event (before 8/11/23 6:00:06.000 PM) No Event Sampling ▾

Events (1) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect

List ▾ ✓ Format 20 Per Page ▾

✗ Hide Fields All Fields

SELECTED FIELDS

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

INTERESTING FIELDS

- a attributes.logging.googleapis.com/timestamp 1
- a data.insertId 1
- a data.jsonPayload._eventId 1

sourcetype

1 Value, 100% of events Selected Yes No 35

Reports

Top values Top values by time Rare values

Events with this field

Values Count %

Values	Count	%
kubernetes	1	100%

port: 52847

splunk>enterprise Apps ▾

Administrator Messages Settings Activity Help Find

Apps Manage

Search apps by name...

Search & Reporting

Splunk Secure Gateway

Upgrade Readiness App

Find more apps

Hello, Administrator

Quick links Dashboard Recently viewed Created by you Shared with you

Common tasks

Add data Search your data Visualize your data

New Search

index="windows" sourcetype="webserver"

✓ 2,420 events (before 8/11/23 6:08:38.000 PM) No Event Sampling •

Events (2,420) Patterns Statistics Visualization

Format Timeline ▾ – Zoom Out + Zoom to Selection × Deselect

All time ▾ 1 day Smart Mode ▾

List ▾ ✓ Format 20 Per Page ▾

< Prev 1 2 3 4 5 6 7 8 ... Next >

Selected Fields	All Fields	i Time	Event
a host 1 a source 1 a sourcetype 1		> 12/31/22 8:44:35.000 PM	55.45.20.74 - - [31/Dec/2022:21:44:35 +0100] "POST /drupal/xmlrpc.php HTTP/1.1" 404 298 "-" "Mozilla/5.0(Linux;Android9;AMN-LX9) AppleWebKit/537.36(KHTML, likeGecko) Chrome/85.0.4183.81MobileSafari/537.36" "-" host = EC2AMAZ-NVS61EL source = splunk_dataset_cyberescape.log sourcetype = webserver
INTERESTING FIELDS a access_request 140+ # date_hour 20 # date_mday 5 # date_minute 60 # date_month 1 # date_second 60 # date_wday 4 # date_year 1 # date_zone 1		> 12/31/22 8:44:35.000 PM	55.45.20.74 - - [31/Dec/2022:21:44:35 +0100] "POST /blogs/xmlsrv/xmlrpc.php HTTP/1.1" 404 296 "-" "Mozilla/5.0(Linux;Android9;AMN-LX9) AppleWebKit/537.36(KHTML, likeGecko) Chrome/85.0.4183.81MobileSafari/537.36" "-" host = EC2AMAZ-NVS61EL source = splunk_dataset_cyberescape.log sourcetype = webserver
		> 12/31/22 8:44:35.000 PM	55.45.20.74 - - [31/Dec/2022:21:44:35 +0100] "POST /blog/xmlrpc.php HTTP/1.1" 404 295 "-" "Mozilla/5.0(Linux;Android9;AMN-LX9) AppleWebKit/537.36(KHTML, likeGecko) Chrome/85.0.4183.81MobileSafari/537.36" "-" host = EC2AMAZ-NVS61EL source = splunk_dataset_cyberescape.log sourcetype = webserver
		> 12/31/22 8:44:35.000 PM	55.45.20.74 - - [31/Dec/2022:21:44:35 +0100] "POST /blog/xmlrpc.php HTTP/1.1" 404 288 "-" "Mozilla/5.0(Linux;Android9;AMN-LX9) AppleWebKit/537.36(KHTML, likeGecko) Chrome/85.0.4183.81MobileSafari/537.36" "-" host = EC2AMAZ-NVS61EL source = splunk_dataset_cyberescape.log sourcetype = webserver

New Search

index="honeypot" sourcetype="honeypot"

✓ 46,972 events (before 8/11/23 6:10:21.000 PM) No Event Sampling •

Events (46,972) Patterns Statistics Visualization

Format Timeline ▾ – Zoom Out + Zoom to Selection × Deselect

All time ▾ 1 millisecond per column

List ▾ ✓ Format 20 Per Page ▾

< Prev 1 2 3 4 5 6 7 8 ... Next >

Selected Fields	All Fields	i Time	Event
a host 1 a source 1 a sourcetype 1		> 8/6/23 2:48:14.000 PM	{ [-] _id: { [+] } channel: dionaea connections ident: a13987c8-c1c1-11e4-9ee4-0a0b6e7c3e9e normalized: true payload: {"connection_type": "reject", "local_host": "162.244.30.100", "connection_protocol": "pcap", "remote_port": 57794, "local_port": 1080, "remote_hostname": "", "connection_transport": "tcp", "remote_host": "107.150.45.234"} timestamp: { [-] } } Show as raw text host = EC2AMAZ-NVS61EL source = honeypot.txt sourcetype = honeypot
INTERESTING FIELDS a attackerIP 100+ # attackerPort 100+ a channel 4 a connection_protocol 12 a connection_transport 2 a connection_type 2 a destination_ip 3 # destination_port 100+ a file_size 100+ 127.0.0.1:8000/en-US		> 8/6/23 2:48:14.000 PM	{ [-] _id: { [+]