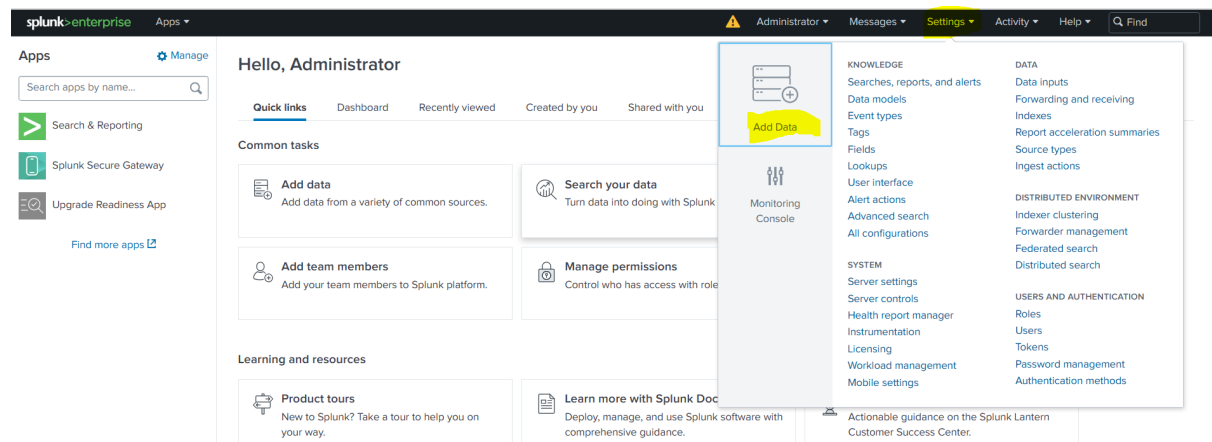


# Guide for ingesting data.

## Draft event in json format:

```
{
  "publish_time": 1691770693.545, "data":
  {
    "insertId": "abcd8z4efghhijk", "jsonPayload":
    {
      "_eventId": "12345-2lad", "client":
      {
        "ip": "127.0.0.6", "port": 52047
      },
      "component": "OAuth", "eventName": "ACCESS-OUTCOME", "http":
      {
        "request":
        {
          "headers":
          {
            "accept": ["application/json"], "host": ["auth-api.eu2.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://auth-api.eu2/cyber/root/abc_uri", "secure": false
        },
        "level": "INFO", "realm": "/", "response": |
        {
          "elapsedTime": 2, "elapsedTimeUnits": "MILLISECONDS", "status": "SUCCESSFUL", "statusCode": "200"
        },
        "source": "CyberEscape", "timestamp": "2023-08-11T16:18:10.6302", "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": "2c975b69ab", "k8s-pod/tier": "middle"
      },
      "logName": "projects/cyber01/logs/stdout", "receiveTimestamp": "2023-08-11T16:18:10.2303788752", "resource":
      {
        "labels":
        {
          "cluster_name": "test01-CyberEscape01-euw2", "container_name": "opencyber", "location": "europe-west2", "pod_name": "cyber-1234cd", "project_id": "test01-CyberEscape01"
        },
        "type": "k8s_container"
      },
      "severity": "INFO", "timestamp": "2023-08-11T16:18:10.6303514292"
    },
    "attributes":
    {
      "logging.googleapis.com/timestamp": "2023-08-11T16:18:10.6303514292"
    }
  }
}
```

## Settings > add data



## 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

Select Source Set Source Type Input Settings Review Done

< Back 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](#)

Selected File: alert1.json

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

	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**

### Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If you want to proceed, use the options below to define proper event breaks and your data, create a new one by clicking "Save As".

Source: alert1.json

Source type: \_json

Save As

Timestamp

Determine how timestamps for the incoming data are defined.

Extraction Auto Curr... Adv... Con...

### Save Source Type

Name

Description

Category

App

Cancel Save

**Click Next**

Add Data

Select Source

Set Source Type

Input Settings

Review

Done

< Back

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

As

Table

Format

20 Per Page

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

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

Add Data

Select Source

Set Source Type

Input Settings

Review

Done

< Back

Review >

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



### General Settings

Index Name

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

Hot/warm db path. Leave blank for default (\$SPLUNK\_DB/INDEX\_NAME/db).

Cold Path

Cold db path. Leave blank for default (\$SPLUNK\_DB/INDEX\_NAME/colddb).

Thawed Path

Thawed/resurrected db path. Leave blank for default (\$SPLUNK\_DB/INDEX\_NAME/thaweddb).

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

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

[< Back](#)
[Review >](#)

**Add Data**

Select Source
Set Source Type
Input Settings
Review
Done

[< Back](#)
[Submit >](#)

### Review

Input Type ..... Uploaded File  
 File Name ..... alert1.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

index="gcp" sourcetype="kubernetes" All time

✓ 1 event (before 8/11/23 6:25:42.000 PM) No Event Sampling

Job Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 millisecond per column

List Format 20 Per Page

< Hide Fields All Fields

**SELECTED FIELDS**

host 1

source 1

sourcetype 1

**INTERESTING FIELDS**

attributes.logging.googleapis.com/timestamp 1

data.insertId 1

data.jsonPayload.eventId 1

data.jsonPayload.client.ip 1

data.jsonPayload.client.port 1

data.jsonPayload.component 1

data.jsonPayload.eventName 1

data.jsonPayload.http.request.headers 1

Time	Event
8/11/23 4:18:13.545 PM	<pre>{   "attributes": {     "logging.googleapis.com/timestamp": "2023-08-11T16:18:13.545Z"   },   "data": {     "insertId": "abcd8z4efgh4hijk",     "jsonPayload": {       "severity": "INFO",       "timestamp": "2023-08-11T16:18:10.630351429Z"     },     "labels": {       "logName": "projects/cyber01/logs/stdout",       "receiveTimestamp": "2023-08-11T16:18:13.230378875Z",       "resource": {         "type": "kubernetes_container",         "cluster": "gcp-cluster",         "namespace": "default",         "pod": "pod-1",         "container": "container-1"       }     }   } }</pre>

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/ti  
mestamp 1  
a data.insertId 1  
a data.jsonPayload.\_eventId 1

sourcetype

1 Value, 100% of events Selected Yes No

Reports  
Top values Top values by time Rare values  
Events with this field

Values	Count	%
kubernetes	1	100%

port: 5284/

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.

New Search

Save As Create Table View Close

index="windows" sourcetype="webserver"

All time

2,420 events (before 8/11/23 6:08:38.000 PM)

No Event Sampling

Job

Events (2,420)PatternsStatisticsVisualization

Format Timeline Zoom Out Zoom to Selection Deselect

1 day per column

List Format 20 Per Page

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

Hide Fields

All Fields

SELECTED FIELDS

host 1

source 1

sourcetype 1

INTERESTING FIELDS

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

i	Time	Event
>	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" 404 290 "-" 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 /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/xmlsrv/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

Save As Create Table View Close

index="honeypot" sourcetype="honeypot"

All time

46,972 events (before 8/11/23 6:10:21.000 PM)

No Event Sampling

Job

Events (46,972)PatternsStatisticsVisualization

Format Timeline Zoom Out Zoom to Selection Deselect

1 millisecond per column

List Format 20 Per Page

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

Hide Fields

All Fields

SELECTED FIELDS

host 1

source 1

sourcetype 1

INTERESTING FIELDS

attackerIP 100+

attackerPort 100+

channel 4

connection\_protocol 12

connection\_transport 2

connection\_type 2

destination\_ip 3

destination\_port 100+

id field 100+

127.0.0.1:8000/en-US

i	Time	Event
>	8/6/23 2:48:14.000 PM	{ [-] _id: { [+] channel: dionaea.connections ident: a13907c8-c1c1-11e4-9ee4-9a8b6e7c3e9e normalized: true payload: {"connection_type": "reject", "local_host": "162.244.38.100", "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
>	8/6/23 2:48:14.000 PM	{ [-] _id: { [+]