

File upload log analysis

I downloaded a free .zip compressed file from an online platform. We can upload it and use it at our source of information

Add Data

Select Source

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](#)

 Preview is not supported for this archive file, but it can still be indexed.

Selected File: **tutorialdata.zip**

Select File





Drop your data file here

The maximum file upload size is 500 Mb

FAQ

- > What kinds of files can the Splunk platform index?
- > What is a source?

Make sure everything is correctly configured & investigate.

List  Format 		20 Per Page 		< Prev 1 2 3 4 5 6 7 8 ...	
Hide Fields 	All Fields	#	Time	Event	
SELECTED FIELDS host 1 source 8 sourcetype 3		>	08/09/2022 18:24:02.000	[08/Sep/2022:18:24:02] VendorID=5036 Code=B AcctID=6024298300471575 host = ip-172-31-6-161.us-east-2.compute.internal source = tutorialdata.zip/vendor_sales/vendor_sales.log sourcetype = vendor_sales	
		>	08/09/2022 18:23:46.000	[08/Sep/2022:18:23:46] VendorID=7026 Code=C AcctID=8702194102896748 host = ip-172-31-6-161.us-east-2.compute.internal source = tutorialdata.zip/vendor_sales/vendor_sales.log sourcetype = vendor_sales	
RESTING FIELDS ctcid 100+ res 100+ entip 100+ ode 14 ite_hour 24 ite_mday 8 ite_minute 60 ite_month 1 ite_second 60 ite_wday 7 ite_year 1 ite_zone 1 e 14 ent 1 ent 1		>	08/09/2022 18:23:31.000	[08/Sep/2022:18:23:31] VendorID=1043 Code=B AcctID=2063718909897951 host = ip-172-31-6-161.us-east-2.compute.internal source = tutorialdata.zip/vendor_sales/vendor_sales.log sourcetype = vendor_sales	
		>	08/09/2022 18:22:59.000	[08/Sep/2022:18:22:59] VendorID=1243 Code=F AcctID=8768831614147676 host = ip-172-31-6-161.us-east-2.compute.internal source = tutorialdata.zip/vendor_sales/vendor_sales.log sourcetype = vendor_sales	
		>	08/09/2022 18:22:48.000	[08/Sep/2022:18:22:48] VendorID=1239 Code=K AcctID=5822351159954740 host = ip-172-31-6-161.us-east-2.compute.internal source = tutorialdata.zip/vendor_sales/vendor_sales.log sourcetype = vendor_sales	
		>	08/09/2022 18:22:32.000	[08/Sep/2022:18:22:32] VendorID=7033 Code=E AcctID=439644811207834 host = ip-172-31-6-161.us-east-2.compute.internal source = tutorialdata.zip/vendor_sales/vendor_sales.log sourcetype = vendor_sales	
		>	08/09/2022 18:22:16.000	91.205.189.15 - - [08/Sep/2022:18:22:16] "GET /oldlink?itemID=EST-14&Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.4 Safari/536.5" 159 host = ip-172-31-6-161.us-east-2.compute.internal source = tutorialdata.zip/www2/access.log sourcetype = access_combined_wcookie	

HAPPY SPLUNKIN'

5 minute window

Presets

REAL-TIME

30 second window

1 minute window

5 minute window

30 minute window

1 hour window

All time (real-time)

RELATIVE

Today

Week to date

Business week to date

Month to date

Year to date

Yesterday

Previous week

Previous business week

Previous month

Previous year

OTHER

Last 15 minutes

Last 60 minutes

Last 4 hours

Last 24 hours

Last 7 days

Last 30 days

All time

> Relative

> Real-time

splunk>enterprise

Apps

Administrator

2 Messages

Settings

Activity

Help

Find

Search

Analytics

Datasets

Reports

Alerts

Dashboards

Search & Report

Create Table View

Cancel

source="tutorialdata.zip:*" host="ip-172-31-6-161.us-east-2.compute.internal"

Select existing fields

Filter existing fields

a Code

date_hour

date_mday

date_minute

date_month

date_second

date_wday

date_year

date_zone

a file

✓ a host

a ident

a index

itemid

items

a JSESSIONID

linecount

Done

✓ Previewing 50 events (01/09/2022 00:15:01.000 to 09/10/2025 11:38:21.000) Sample: Latest

*	@ _time	a host	a source	a sourcetype	> _raw
1	2022-09-08T18:24:02.000Z	ip-172-31-6-161.us-east-2.compute.internal	tutorialdata.zip:./vendor_sales/vendor_sales.log	vendor_sales	[08/Sep/2022:18:24:02] VendorID=5036 C
2	2022-09-08T18:23:46.000Z	ip-172-31-6-161.us-east-2.compute.internal	tutorialdata.zip:./vendor_sales/vendor_sales.log	vendor_sales	[08/Sep/2022:18:23:46] VendorID=7026 C
3	2022-09-08T18:23:31.000Z	ip-172-31-6-161.us-east-2.compute.internal	tutorialdata.zip:./vendor_sales/vendor_sales.log	vendor_sales	[08/Sep/2022:18:23:31] VendorID=1043 C
4	2022-09-08T18:22:59.000Z	ip-172-31-6-161.us-east-2.compute.internal	tutorialdata.zip:./vendor_sales/vendor_sales.log	vendor_sales	[08/Sep/2022:18:22:59] VendorID=1243 C
5	2022-09-08T18:22:48.000Z	ip-172-31-6-161.us-east-2.compute.internal	tutorialdata.zip:./vendor_sales/vendor_sales.log	vendor_sales	[08/Sep/2022:18:22:48] VendorID=1239 C
6	2022-09-08T18:22:32.000Z	ip-172-31-6-161.us-east-2.compute.internal	tutorialdata.zip:./vendor_sales/vendor_sales.log	vendor_sales	[08/Sep/2022:18:22:32] VendorID=7033 C
7	2022-09-08T18:22:16.000Z	ip-172-31-6-161.us-east-2.compute.internal	tutorialdata.zip:./www2/access.log	access_combined_wcookie	91.205.189.15 - - [08/Sep/2022:18:22:14&JSESSIONID=5D65L7FF7ADFF53113 HTTP ItemID=EST-14" Mozilla/5.0 (Windows NT Chrome/19.0.1084.46 Safari/536.5" 159
8	2022-09-08T18:22:15.000Z	ip-172-31-6-161.us-east-	tutorialdata.zip:./www2/acces	access_combined_wcookie	91.205.189.15 - - [08/Sep/2022:18:22:1