# Splunk Workshop: Log Analysis

In this workshop we will focus on Splunk Enterprise. Splunk Enterprise is a platform to collect, analyze and visualize machine generated data. This data includes log files, application metrics, network data and industrial data to name a few.

In this workshop we will utilize Docker to run Splunk. Once Splunk it running we will upload synthetic logs to the platform and analyze the logs with Splunk commands.

## Server Log

The "**`log_data.csv`**" is a synthetic log that contains data on server events. The log is saved as a comma separated values (csv) format. There are four fields in the log: **`timestamp`** (date/time the event occurred), **`host`** (server or device for the event), **`event_type`** (login, logout, error) and **`event_description`** (description of the event). We will upload this log into Splunk and analyze the data.

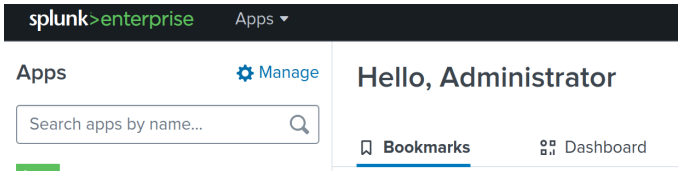
1. **PULLING THE DOCKER IMAGE AND RUNNING SPLUNK**

- To pull and run the Splunk image in a container use the command "**`docker run -d -p 8000:8000 -p 8088:8088 -p 9997:9997 -e SPLUNK_START_ARGS="--accept-license" -e SPLUNK_PASSWORD="password" --name splunk splunk/splunk:latest`**" in your terminal. Docker pulls down the Splunk image, it will take a few minutes.
- Run "**`docker ps -a`**". You should see a Splunk container running. Under the "**`status`**" header, once the status displays as "**`Up (healthy)`** " you can access Splunk.

2. **ACCESSING SPLUNK**

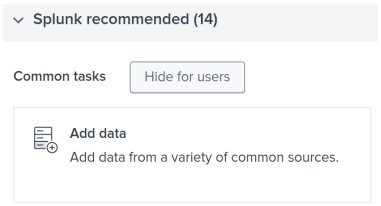
- Bring up a web browser and in the search bar run "**`http://localhost:8000/`**".
- The Username is "**`Admin`**" and the password is "**`password`**".


- Once logged in you will be brought to the Splunk Enterprise homepage.



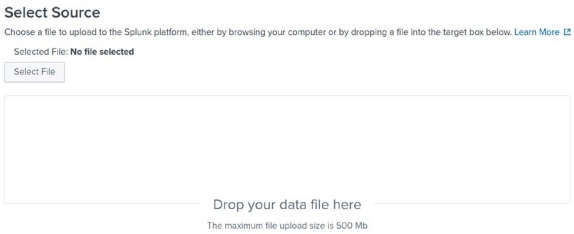

3. **ADDING DATA TO SPLUNK**

- On the homepage select "**`Add Data`**".




- On the next page select "**`Upload files from my computer`**".


- Select "**`Choose File`**" and upload the "**`log_data.csv`**" file or drag and drop the file into the page.




- On the "**`Set Source Type`**" page, ensue that the "**`Source type`**" is set as a CSV. Select next.
- On the "**`Input Settings`**" in the "**`Host field value`**" type "**`on_prem_servers`**". The "**`Host field value`**" denotes the machine where the uploaded log came from.
- Still on the "**`Input Settings`**" page select "**`Create a new index`**". Type "**`servers`**" for the Index Name. Use the default setting for the rest of the fields and select "**`Save`**". Select "**`Review`**".
- Select "**`Submit`**" on the "**`Review`**" page.

## 4. Check How the Data is Indexed

- In the top right corner select the search bar "**`Find`**".
- Search for "**`Indexes and Volumes: Instance`**".
- Under the "**`Index`**" column check that "**`servers`**" is listed.

## 5. Basic Splunk Searches

- Go back to the home page by selecting the "**`Splunk Enterprise`**" logo.
- Under "**`Apps`**" select "**`Search and Reporting`**".
- Next to the magnifying glass icon, select the "**`Last 24 hours`**" and change it to "**`All time`**" under "**`Other`**".
- Run the command "**`index=servers`**" in the search. This search retrieves all events that are stored in the "**`servers`**" index. It does not apply any additional filters or constraints, so it will return every event in the "**`servers`**" index.
- For the next search run "**`index= servers | stats count by event_type`**". This search will bucket all of the "**`events`**" by their corresponding "**`event types`**". Within our log we have 37 "**`errors`**", 72 "**`logins`**" and 38 "**`logouts`**". To look further into a specific event, select the event type and select "**`View Events`**".

## 6. Creating Graphs

- To visualize all of the events in the given log we can search for "**`index=servers earliest="07/25/2024:00:00:00" latest="07/30/2024:23:59:59" | timechart`**

**span=1d count**". To visualize the search select the "**Visualization**" tab. This will list out all the dates from July 25th to the 30th in single day intervals.

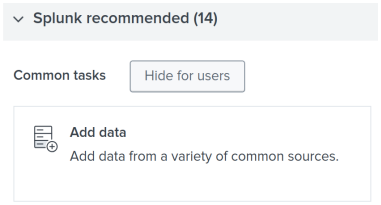
- We can breakout the bar charts by event type (login, logout, error) by searching the command "**index=servers earliest="07/25/2024:00:00:00" latest="07/30/2024:23:59:59" | timechart span=1d count by event_type**".
- Under the same search, change the chart type by selecting "**Column Chart**" and select the "**Line Chart**".
- To get the proportions of events by type we can run "**index=servers earliest="07/25/2024:00:00:00" latest="07/30/2024:23:59:59" | stats count by event_type | sort -count**". Change the chart type by selecting "**Line Chart**" and select the "**Pie Chart**".

## Amazon Web Services (AWS) Cloud Log

The "**aws_cloudtrail_log.json**" is a synthetic log that contains events for Amazon Web Services (AWS) actions and services. These services include Elastic Compute Cloud (EC2) instances, Simple Storage Service (S3) buckets, serverless Lambda Function computes amongst many others. The log is formatted as a JavaScript Object Notation (JSON) file. We will upload this log into Splunk and analyze the data.

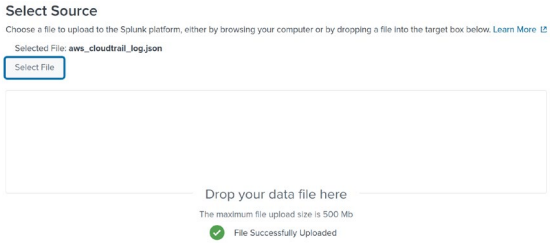
### 1. ADD AWS DATA TO SPLUNK

- On the homepage select "**Add Data**".



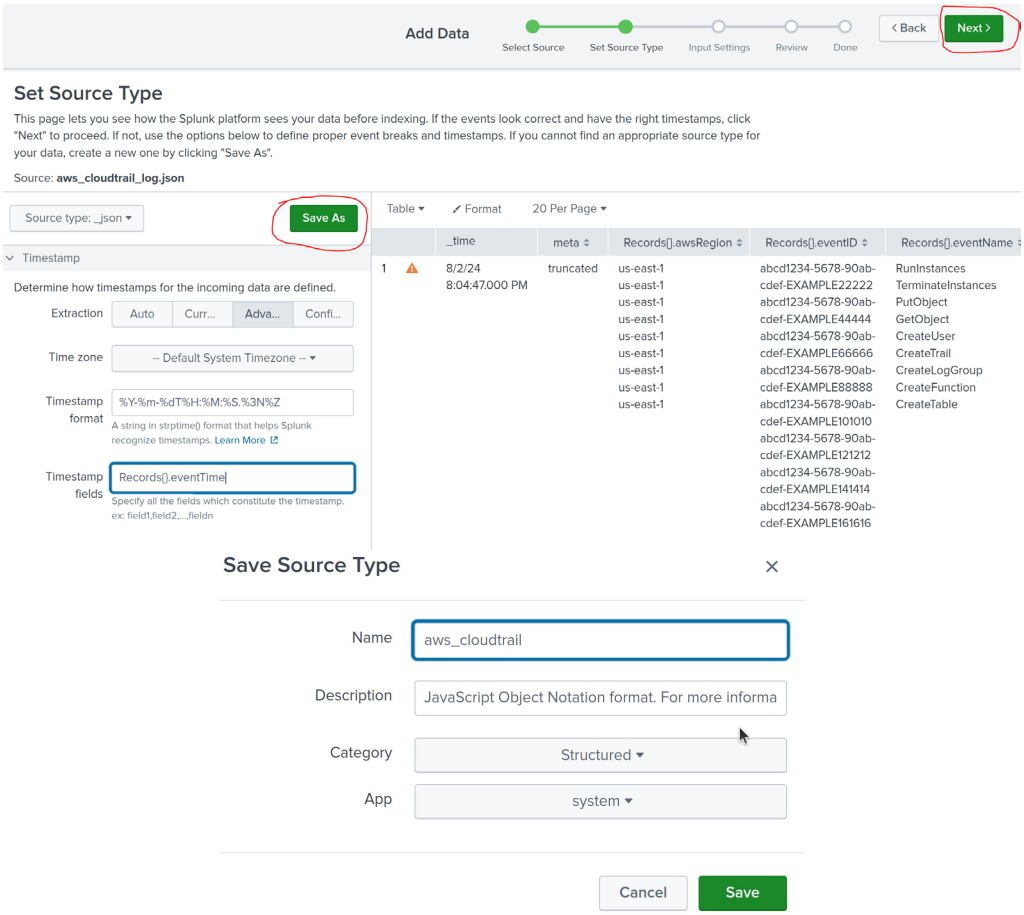

- On the next page select "**Upload files from my computer**".


- Select "**Choose File**" and upload the "**aws_cloudtrail_log.json**" file or drag and drop the file into the page.

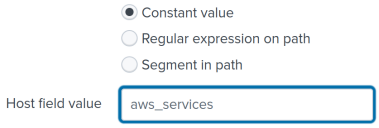



- On the "**Set Source Type**" page, ensue that the "**Source type**" is set as "**_json**". Select "**Timestamp**" and select "**Advanced**".
    - In the "**Timestamp format**" input "**%Y-%m-%dT%H:%M:%S.%3N%Z**"
    - In "**Timestamp field**" input "**Records{}.eventTime**"
        - Save the Source Type Name as "**aws_cloudtrail**"
    - Select "**Save As**", "**Save**" and select "**OK**" to overwrite.

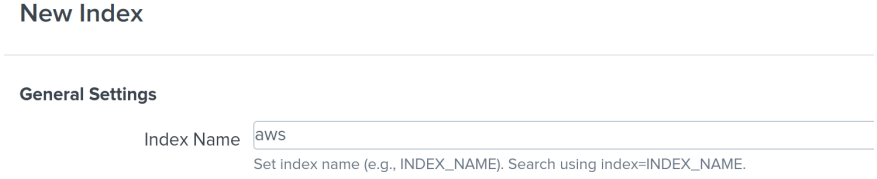
  Select next.




- On the "**`Input Settings`**" in the "**`Host field value`**" type "**`aws_services`**". The "**`Host field value`**" denotes the machine where the uploaded log came from.




- Still on the "**`Input Settings`**" page select "**`Create a new index`**". Type "**`aws`**" for the Index Name. Use the default setting for the rest of the fields and select "**`Save`**". Select "**`Review`**".




- Select "**`Submit`**" on the "**`Review`**" page.