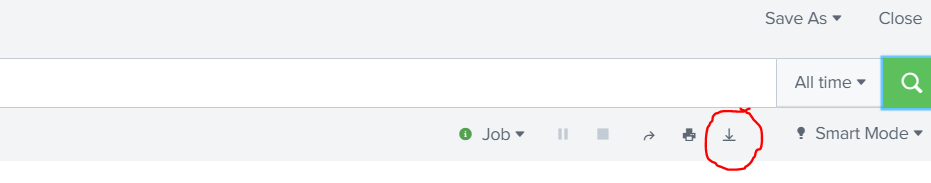
**1) Splunk Enterprise UI / Splunk Cloud:**

If you want to use splunk enterprise’s web ui then follow these steps / for splunk cloud follow from step 6:

1. <https://www.splunk.com/en_us/download/splunk-enterprise.html> Download splunk enterprise and install it .
2. Splunk-enterprise has limit of reading 10,000 bits by default and rest are truncated so to change it in the installation directory for windows it’s *C:\Program Files\Splunk*
3. Then go to **Splunk > etc > system > local > props.conf**
4. Set **TRUNCATE=0**  and save it .
5. In Splunk Web, go to **Settings > Server controls** and then click on **Restart Splunk.**
6. ***\*\* If using Splunk cloud then follow from here .***
7. **NOTE THAT SPLUNK TAKES IN *JSON FILE ONLY* SO USE “tojson.py” (**present in static folder**) TO CONVERT AVRO FILE TO A JSON FILE THAT CAN BE USED IN SPLUNK.**
8. Click on **Add Data.**
9. In bottom left click on **Upload.**
10. Click on select file and upload the .json file obtained in 7th step then click on **Next .**
11. Set source type to json.
12. Ignore timestamp warning Click on **Next.**
13. Set some **Host Field Value** and remember it \*\* , leave index to default then click on **review**.
14. Click on **submit** and then click on **start searching.**
15. host="from step 13"| stats values as \* by name search this in in new search



1. Click on Dowload / Export button and download the file as .csv and it’s done .

**2) Using script with Splunk Enterprise HEC(HTTP Event Collector):**

If you want to use *“avro\_to\_csv.py”* then you have to enable http event collector in splunk

1. Open splunk web ui click on settings and then data input
2. Scroll to http event collector and click on add new
3. Assign some Name
4. Click on next and then set source type to json
5. App context will be searching & reporting(search)
6. Select main in the index then click on review
7. Then click on submit.
8. Copy the token value and click on start searching.
9. Again go to settings > data inputs > http event collector and click on http event collector and make sure that HEC that you create is enable if not then enable it.
10. HEC will also work with splunk cloud
11. Edit the avro\_to\_csv.py and set your token value in the main() function.
12. Now execute the avro\_to\_csv.py file and it will convert .avsc file to raw data csv file and it’s done