SPLUNK IMPLEMETATION (STUDENT DATA) CERTIFICATION PROJECT

Neeraj Agarwal

MINDTREE LTD

Problem Statement

Objective: Implement a Splunk project for the Student details. Under this project, you will have to work with the log files of Student data. Following parts should be covered

1. Log Files Creation
2. Data Inputs
3. Fields Extraction
4. Lookups
5. Alerts
6. Report
7. Dashboard

The following are the fields that are to be added in the log files:

1. Date
2. Time
3. Student_ID
4. Student _First_Name
5. Student _Last_Name
6. Student _Father_Name
7. Class

Abstract

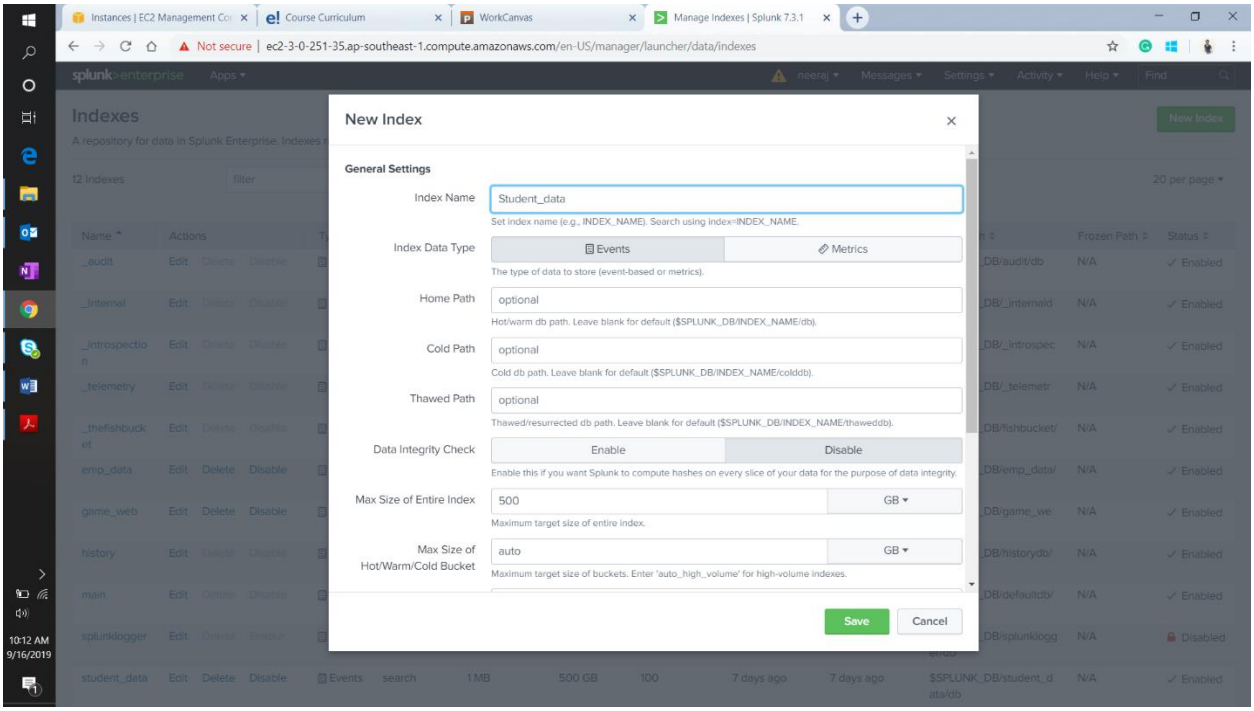
This Document includes step by step procedure for monitoring set up of Student data. This includes

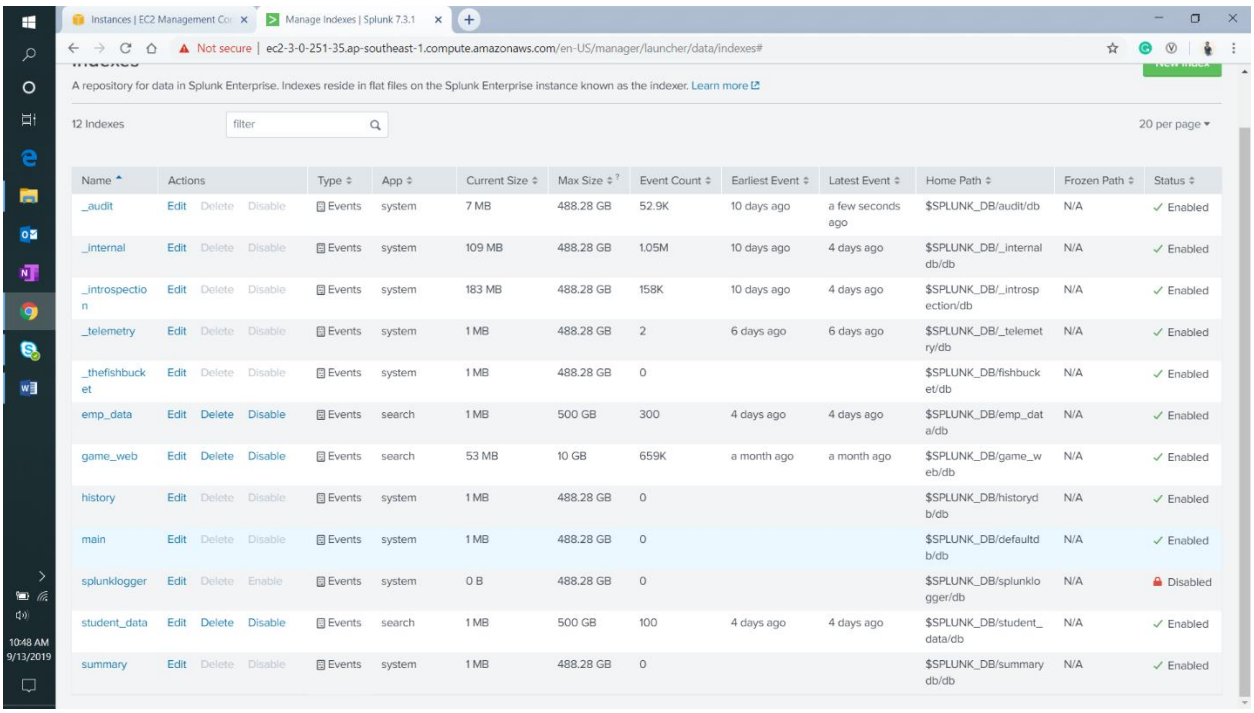
- **Creating an index**
- **Adding data sets**
- **Adding lookup tables**
- **Creating reports and alerts**
- **Creating dashboards**

Contents

Creating an index

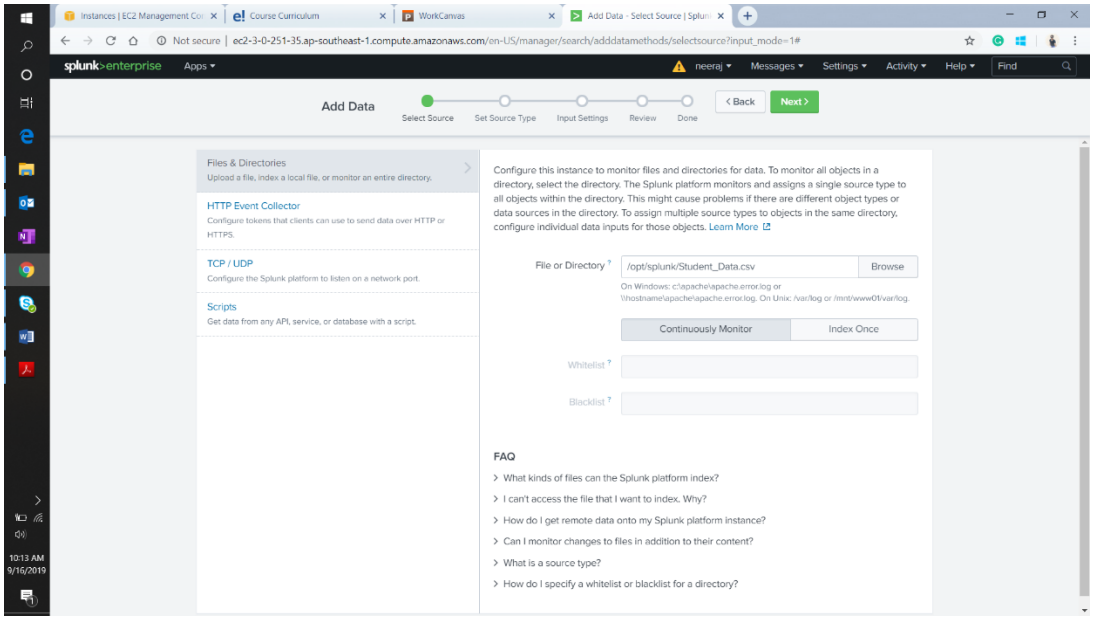
First I have created an index specifically for monitoring the Student data.

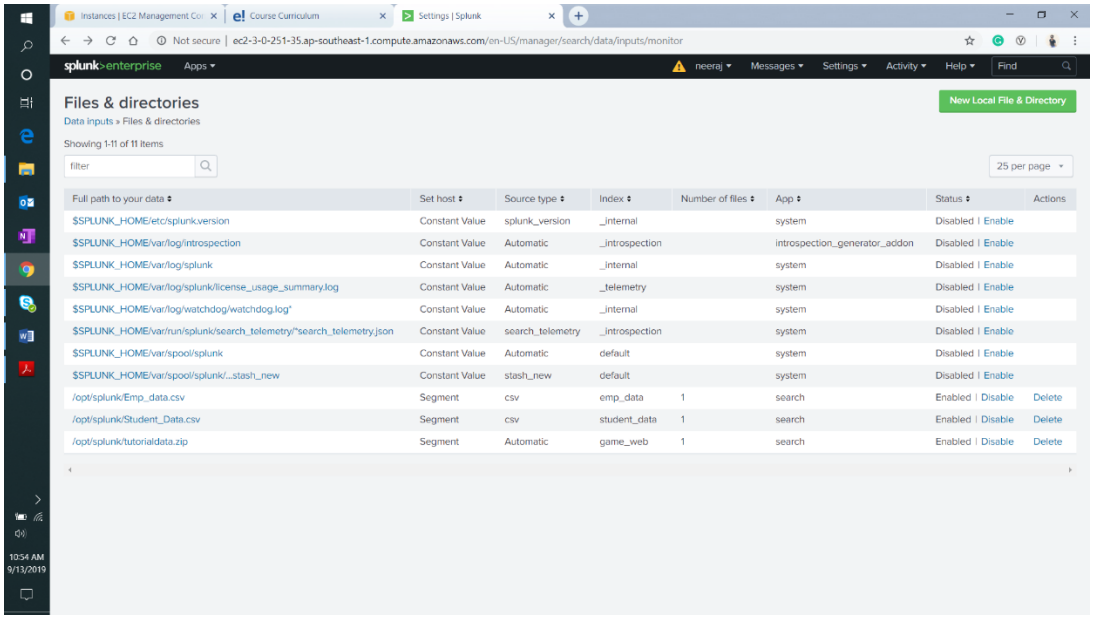




Adding data inputs

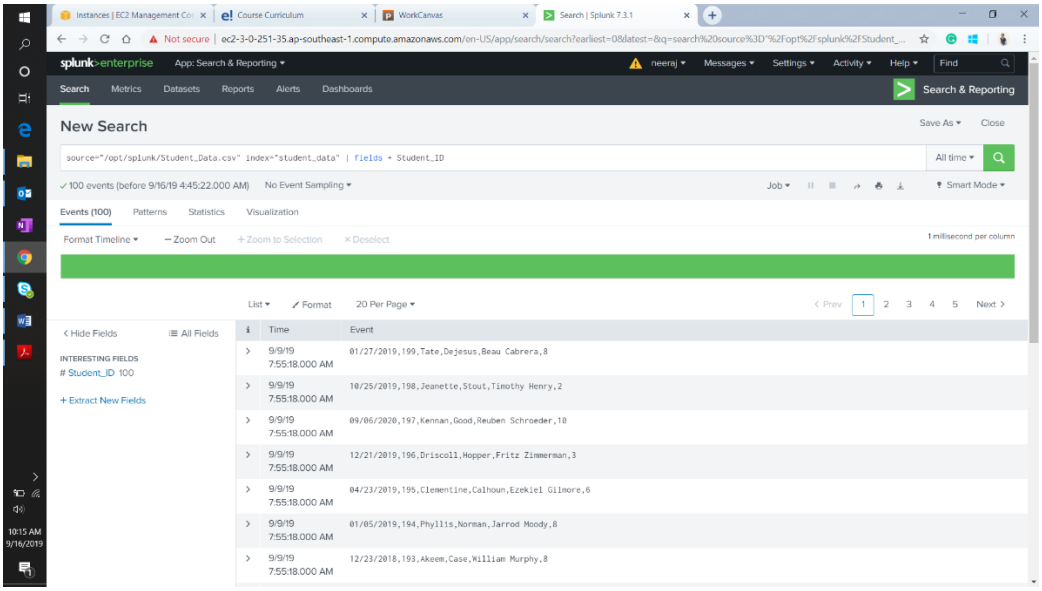
I have created a static csv file which contains details of 100 Students to add as a data set. I will add this file to monitor under the index created previously.



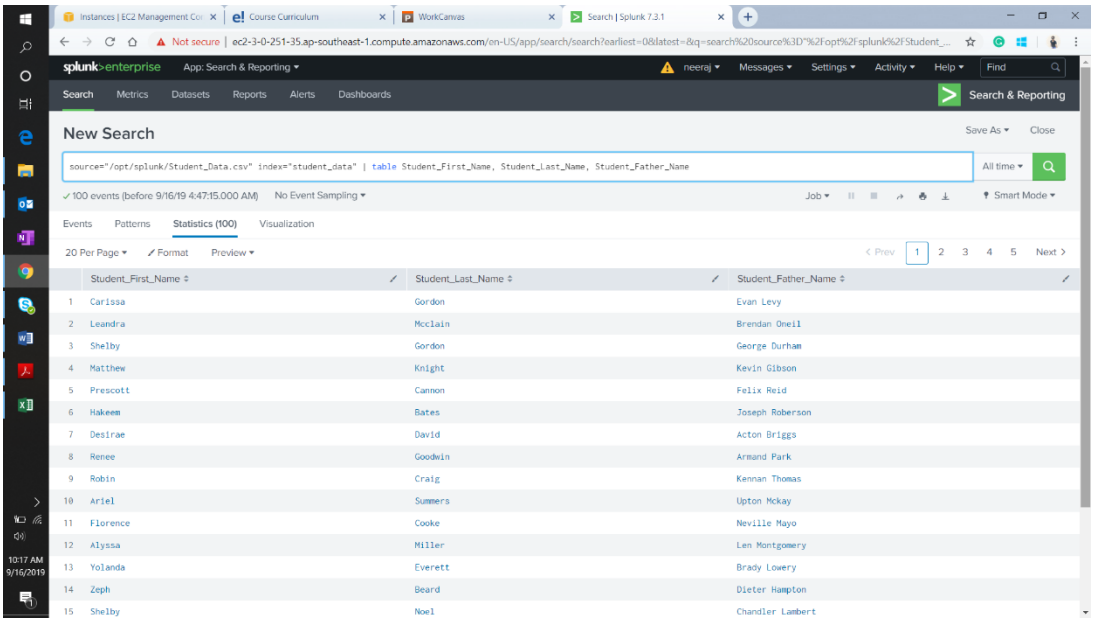


Basic searches (Fields Extraction)

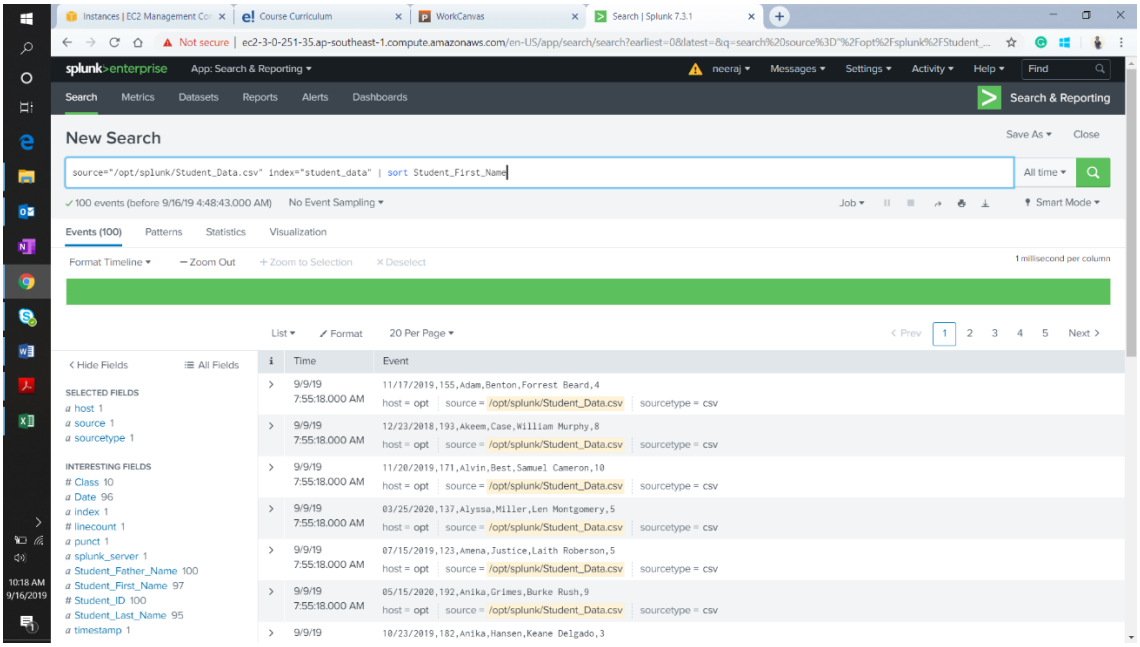
In this section, I have attached a few screenshots of the searches using various fields and commands.



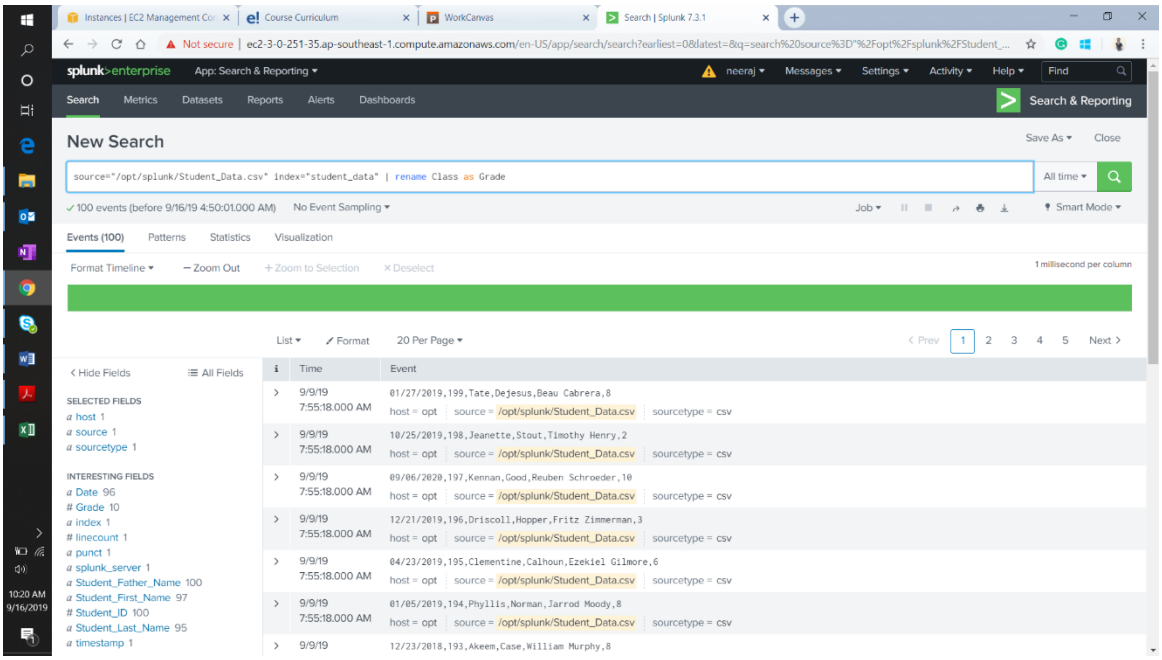
Field Extraction



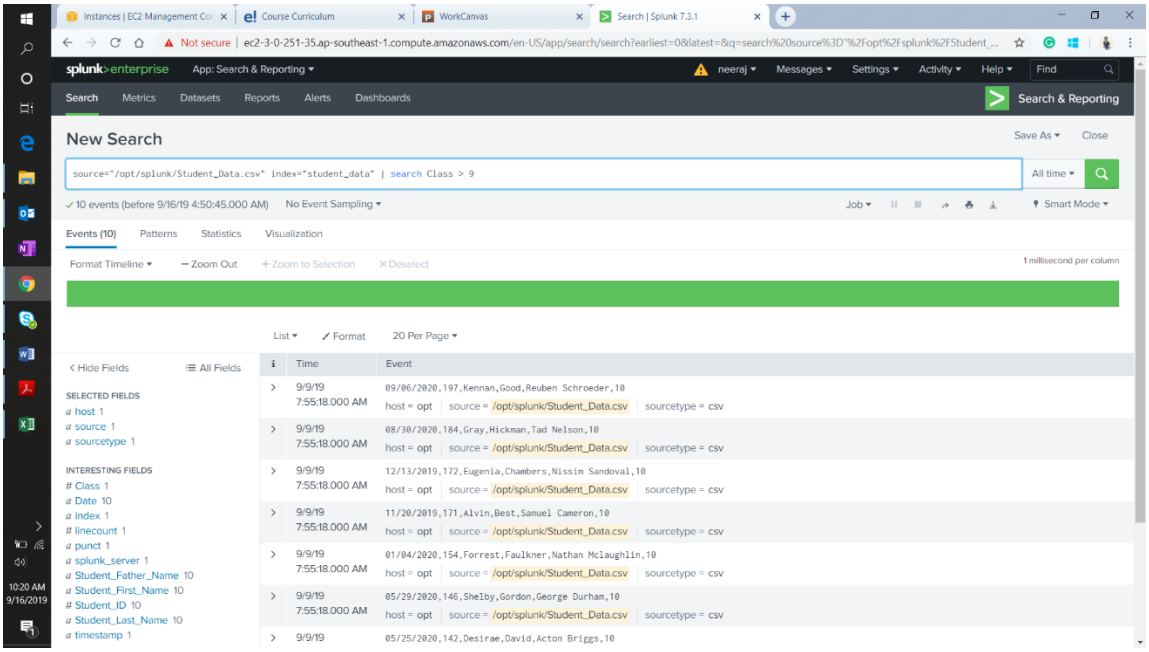
Example of "Table" command



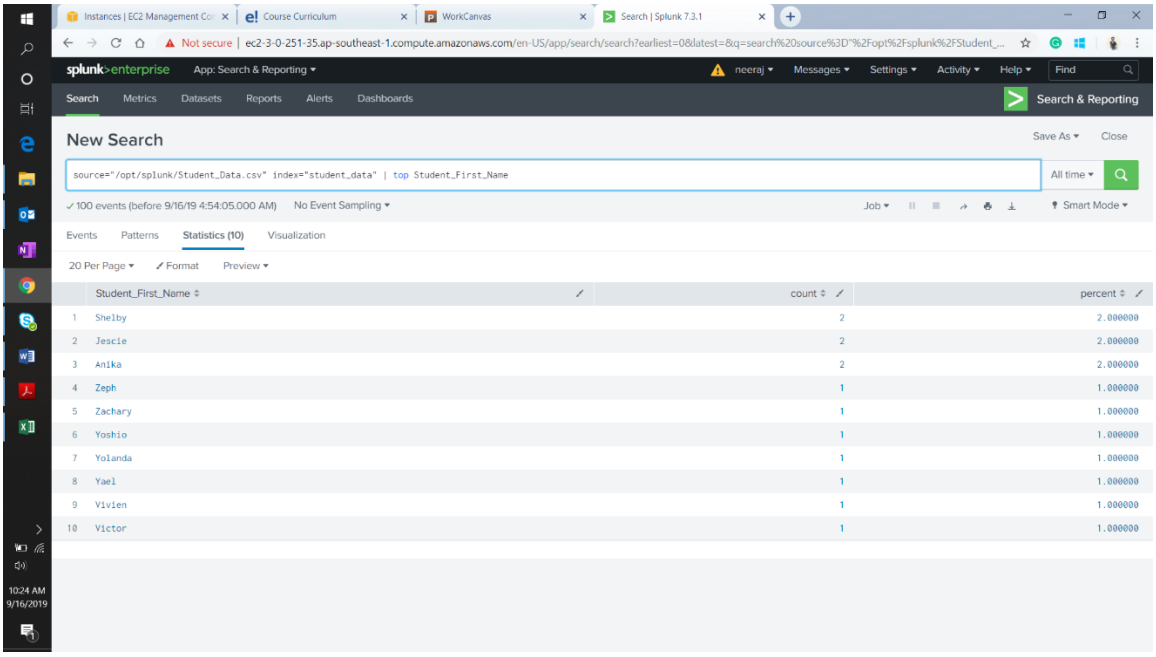
Example of "Sort" command



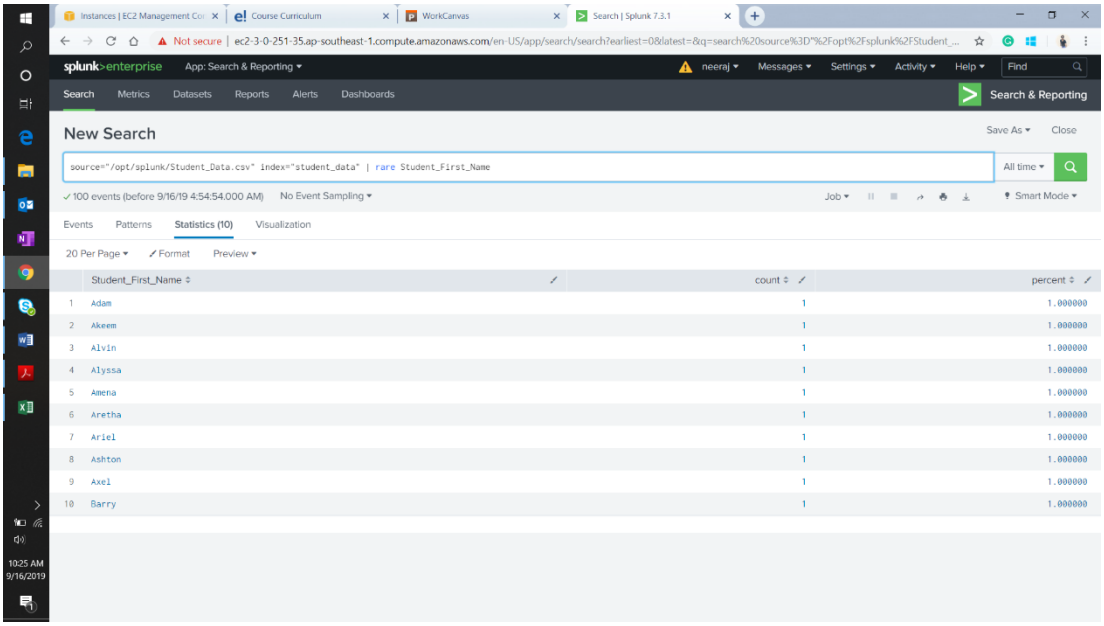
Example of "Rename" command



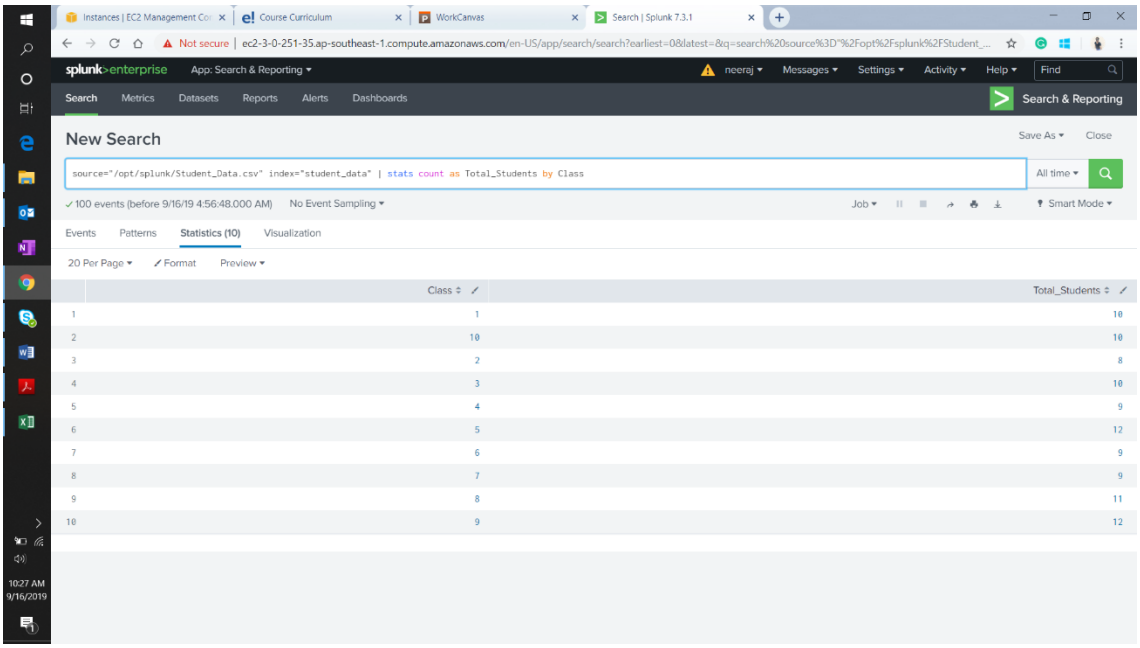
Example of "search" command



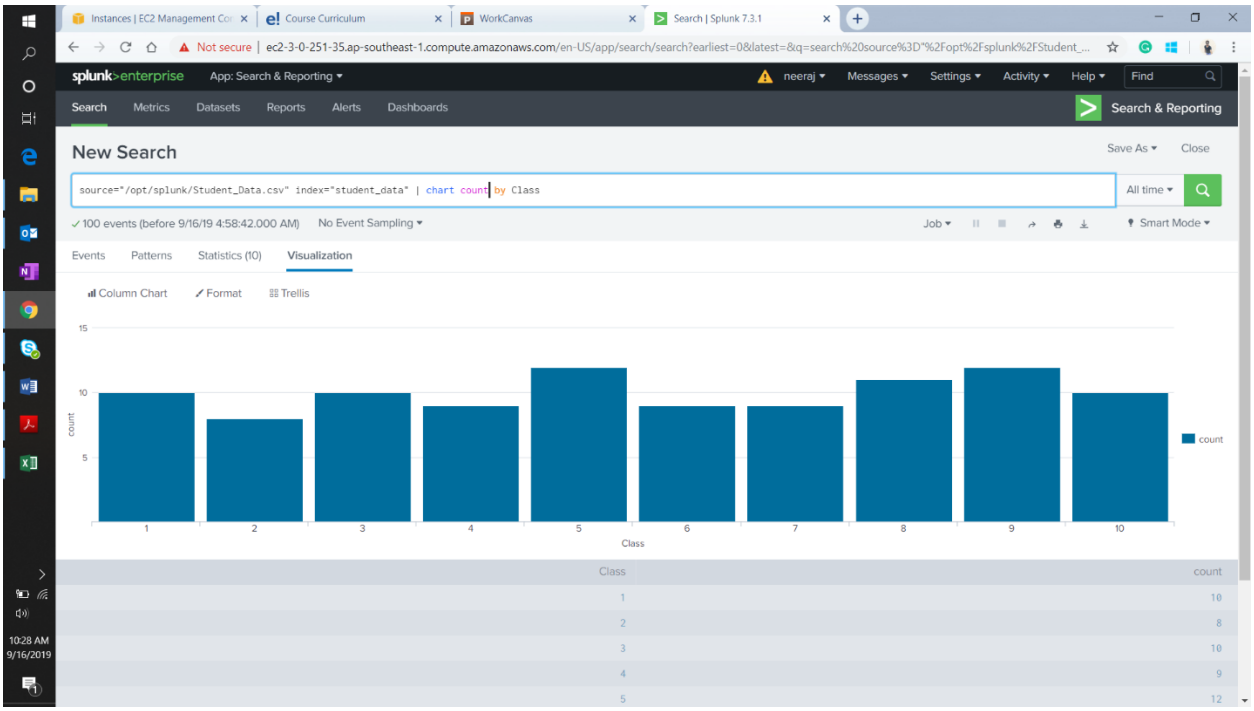
Example of "Top" command



Example of "Rare" command



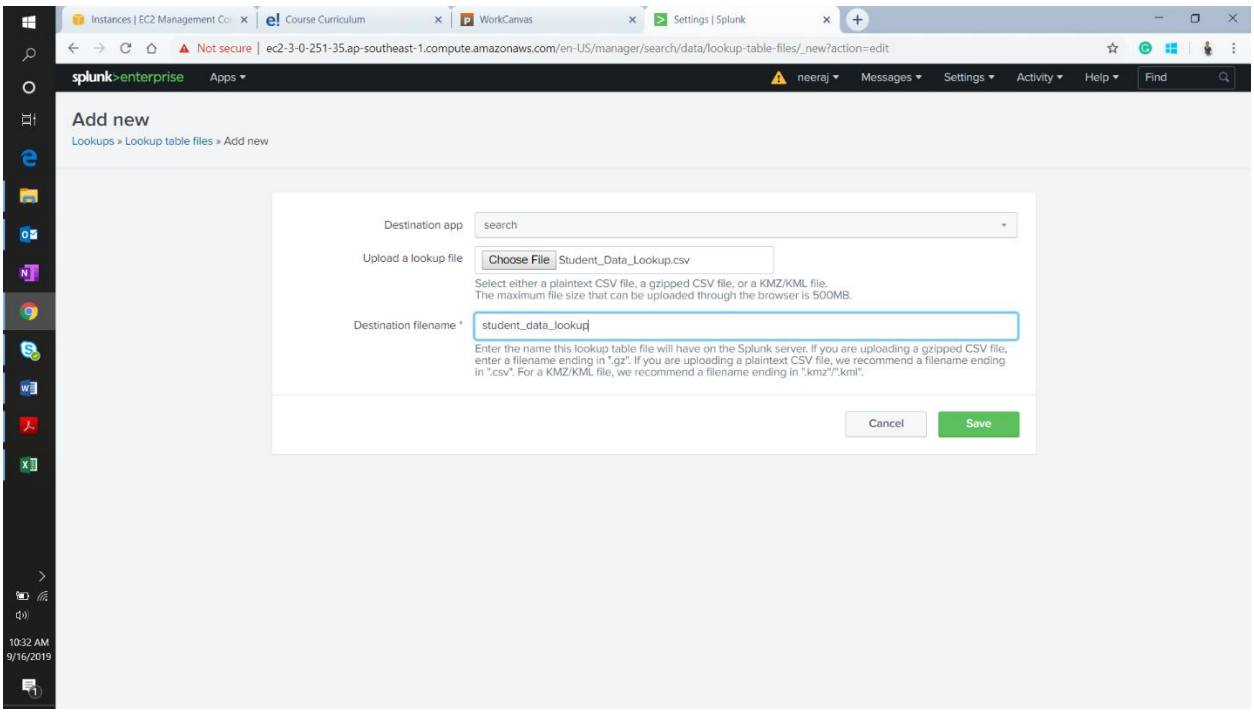
Example of "Stats" command



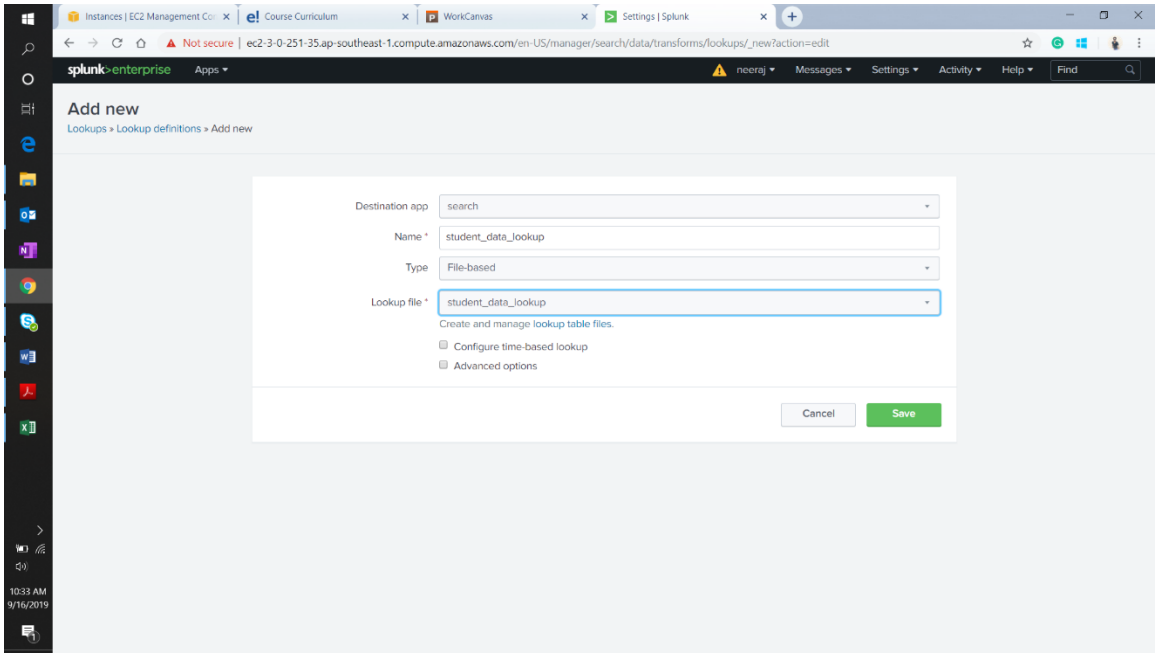
Example of "Chart" command

Lookups

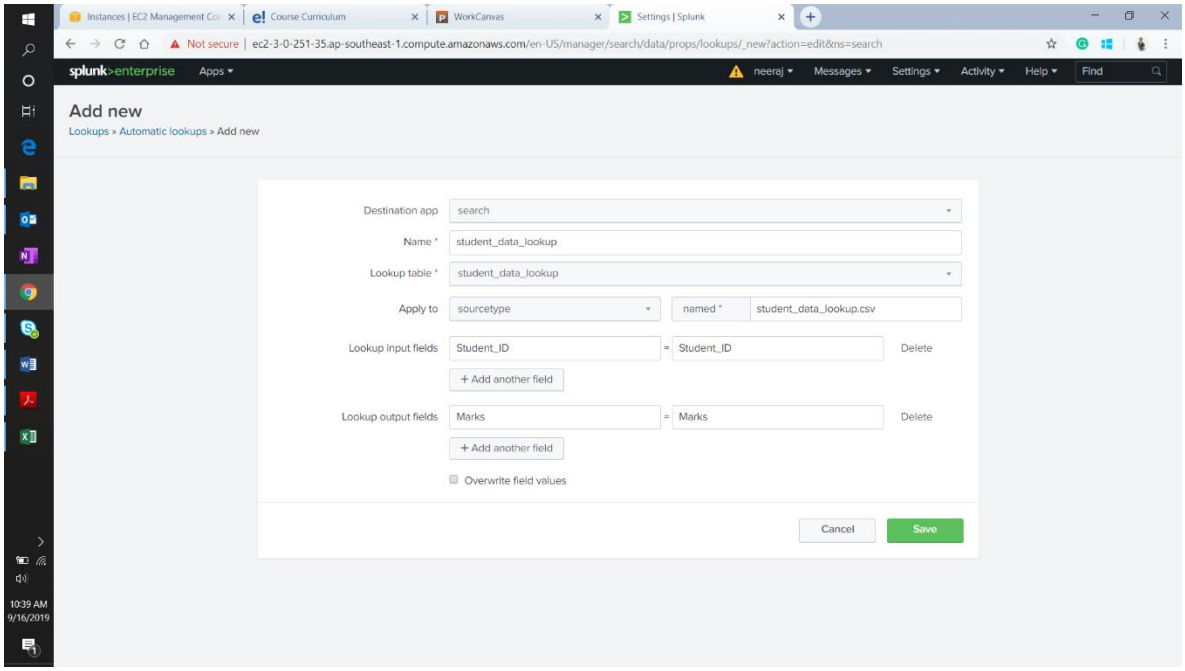
In this section, I will add a lookup table to map the Student's job title to the company they are associated with. I have created a csv file with above-mentioned data.



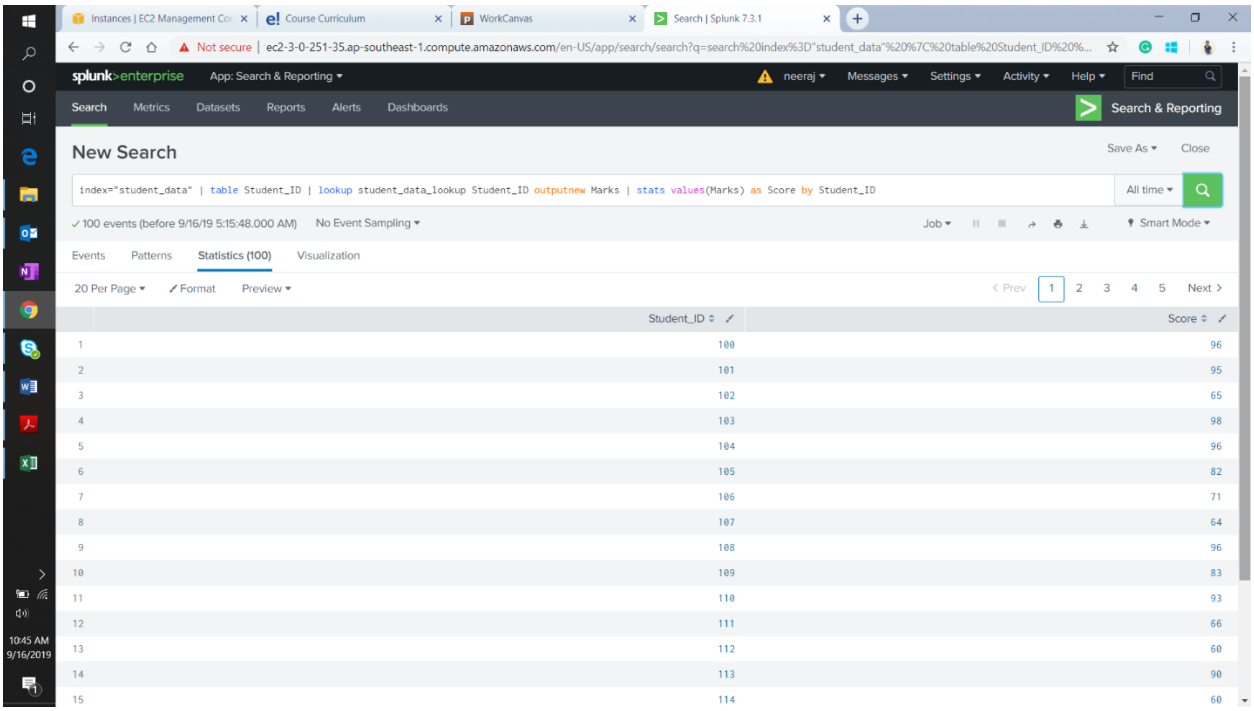
Adding the lookup file



Adding a new lookup definition



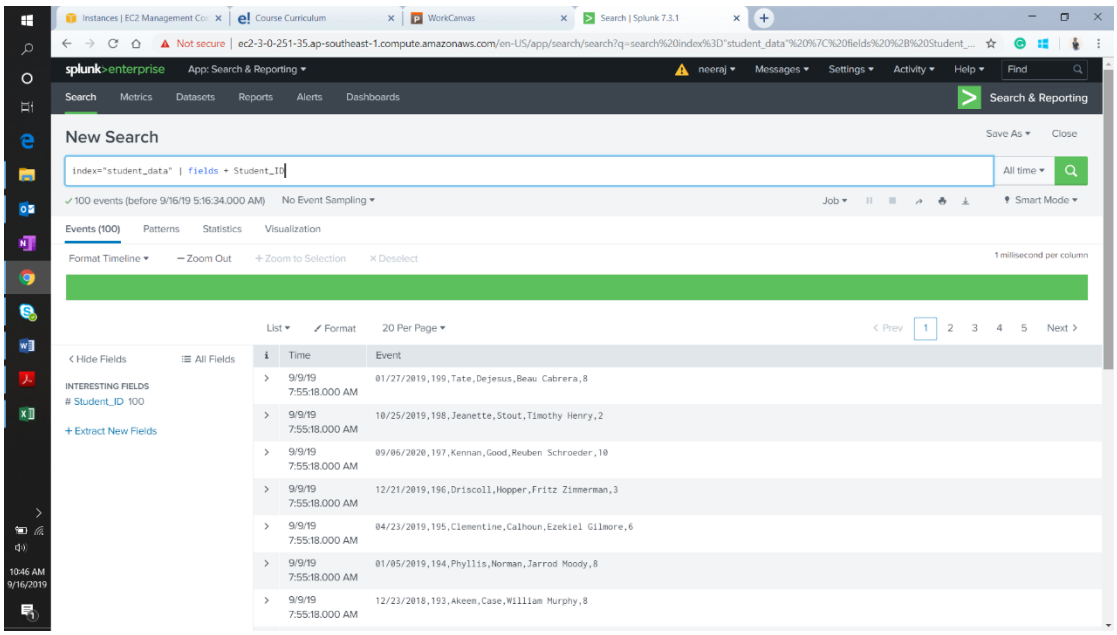
Adding automatic lookup



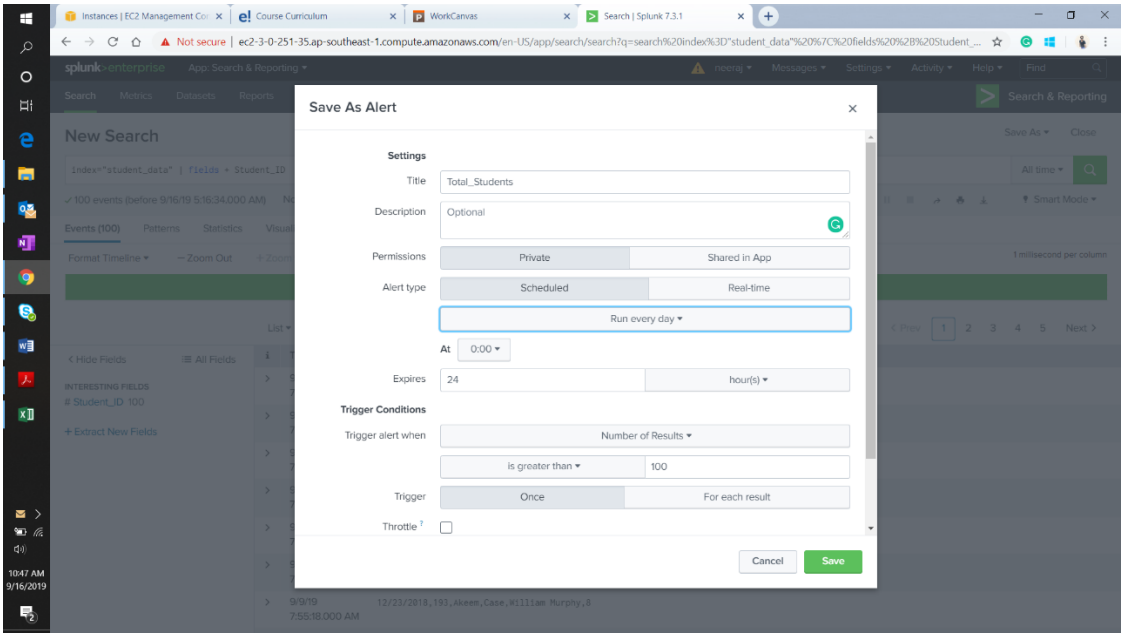
Example of a search which utilizes lookup

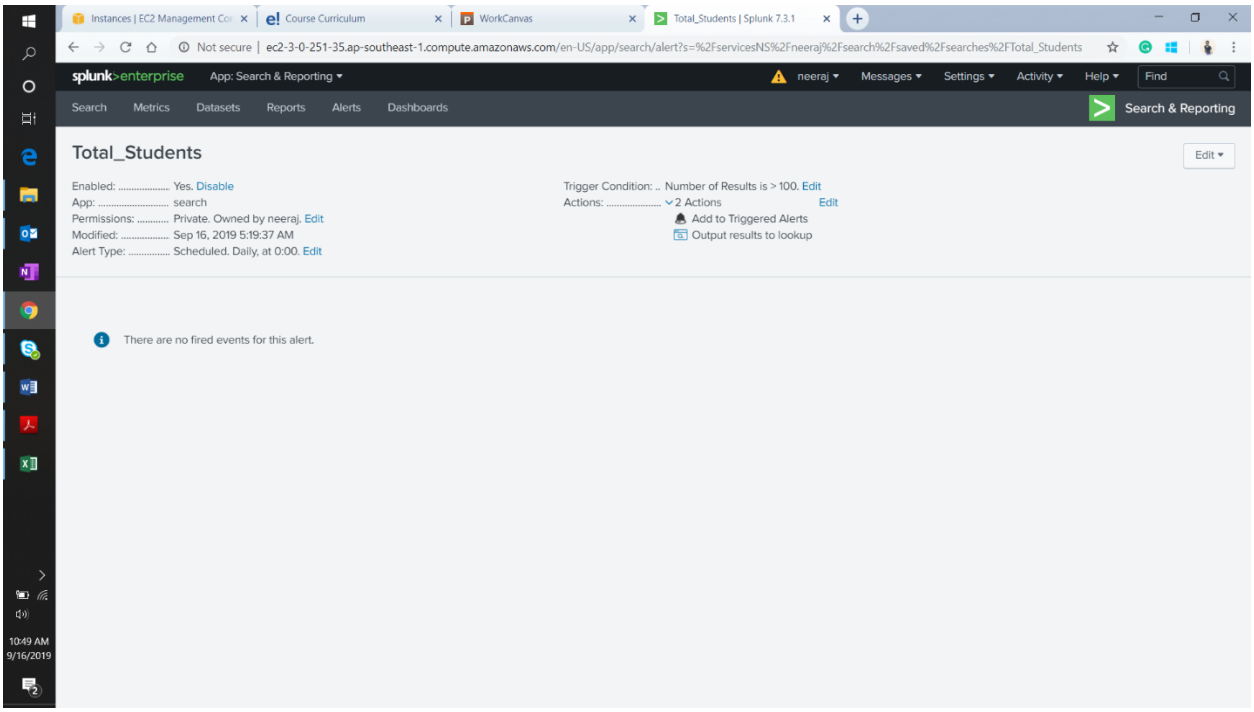
Adding an alert

Here I am configuring an alert where if the search returns showing more than 100 Students in the organization data. This search runs every day at midnight and raises an alert, as well as outputs, result in lookup.



The search string to be configured as alert





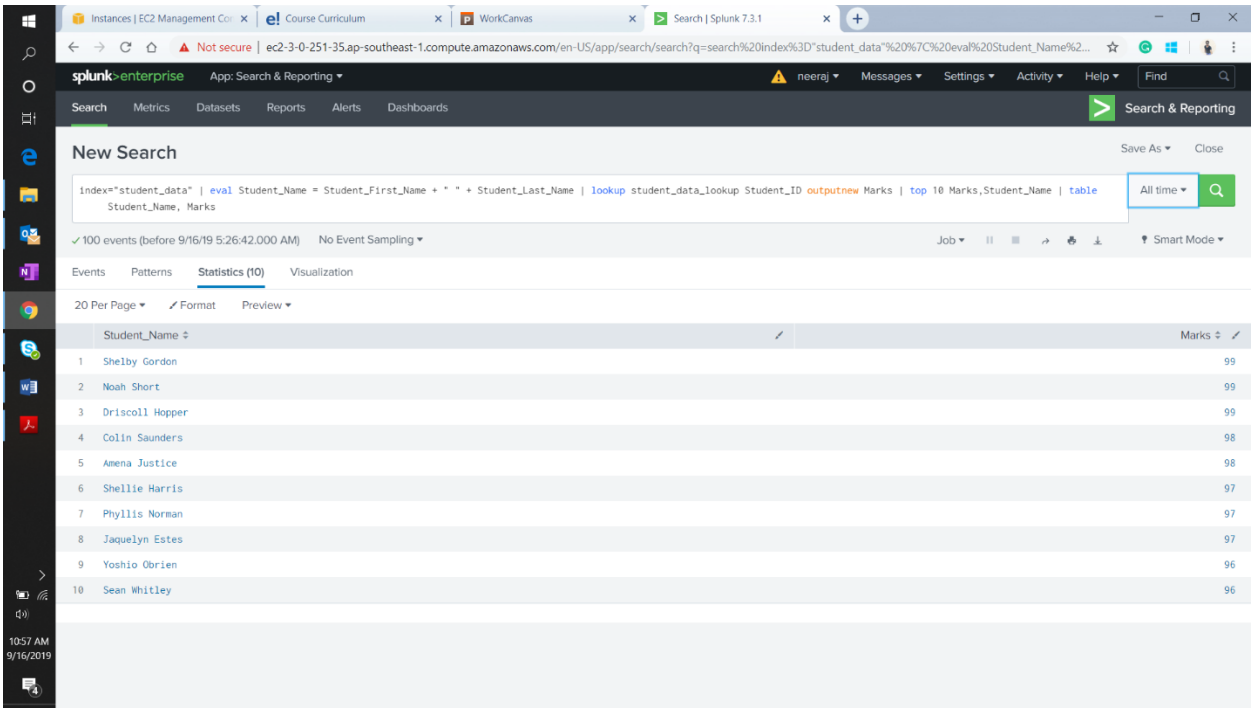
The alert configured

Creating Reports

For this project, I have created four reports which will be used to create a dashboard in the next section. Below is the list of the reports

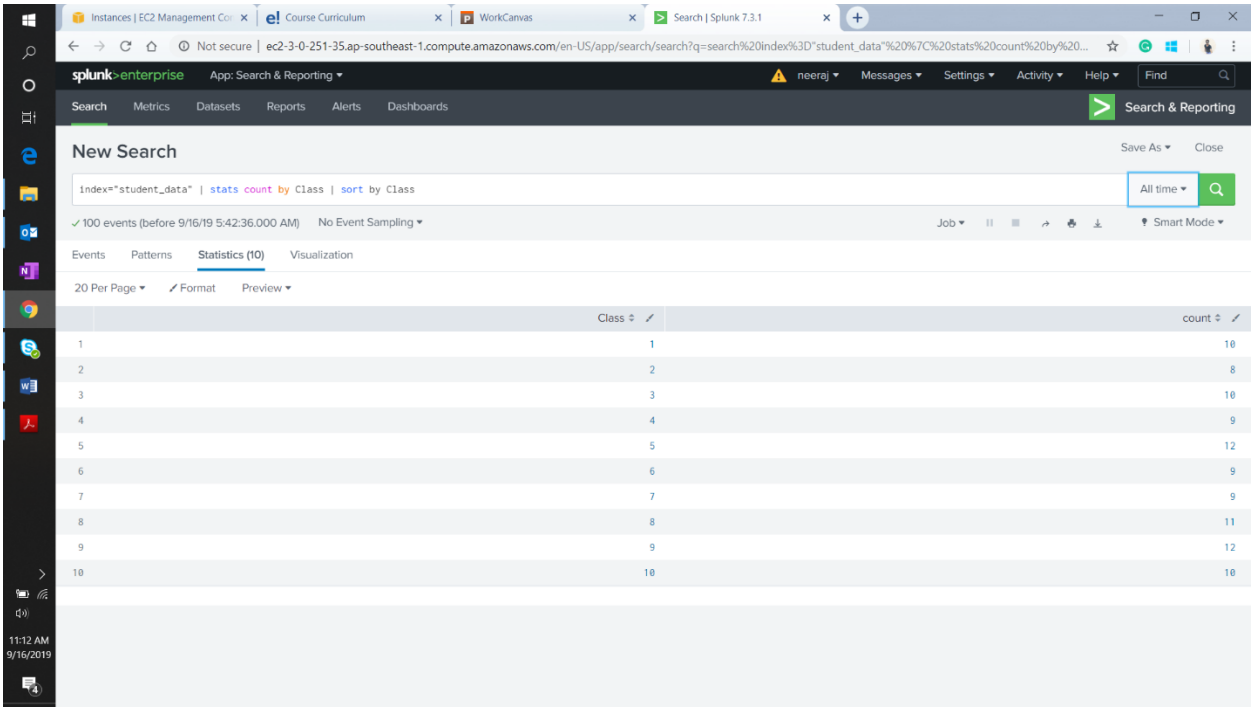
1. Top 10 scoring Students
   Search string :

```
index="student_data" | eval Student_Name = Student_First_Name + " " + Student_Last_Name | lookup student_data_lookup Student_ID outputnew Marks | top 10 Marks,Student_Name | table  Student_Name, Marks
```



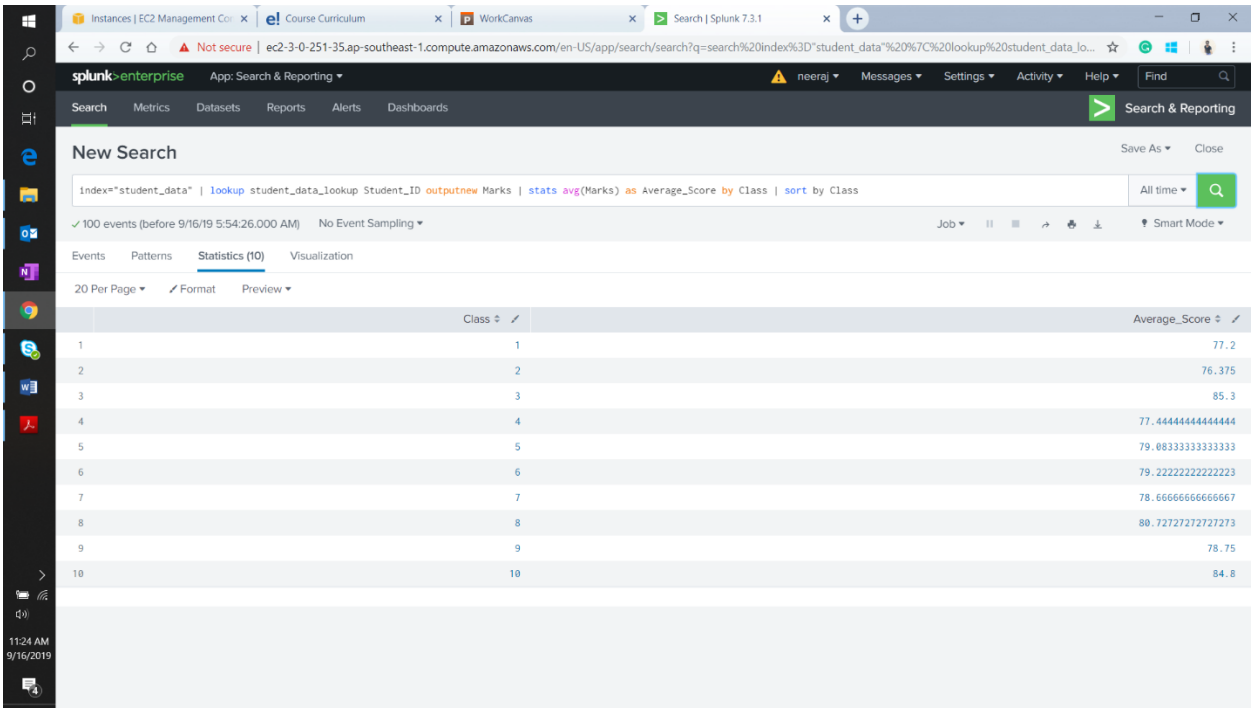
2. Total Students in each Class
   Search string :

```
index="student_data" | stats count by Class | sort by Class
```



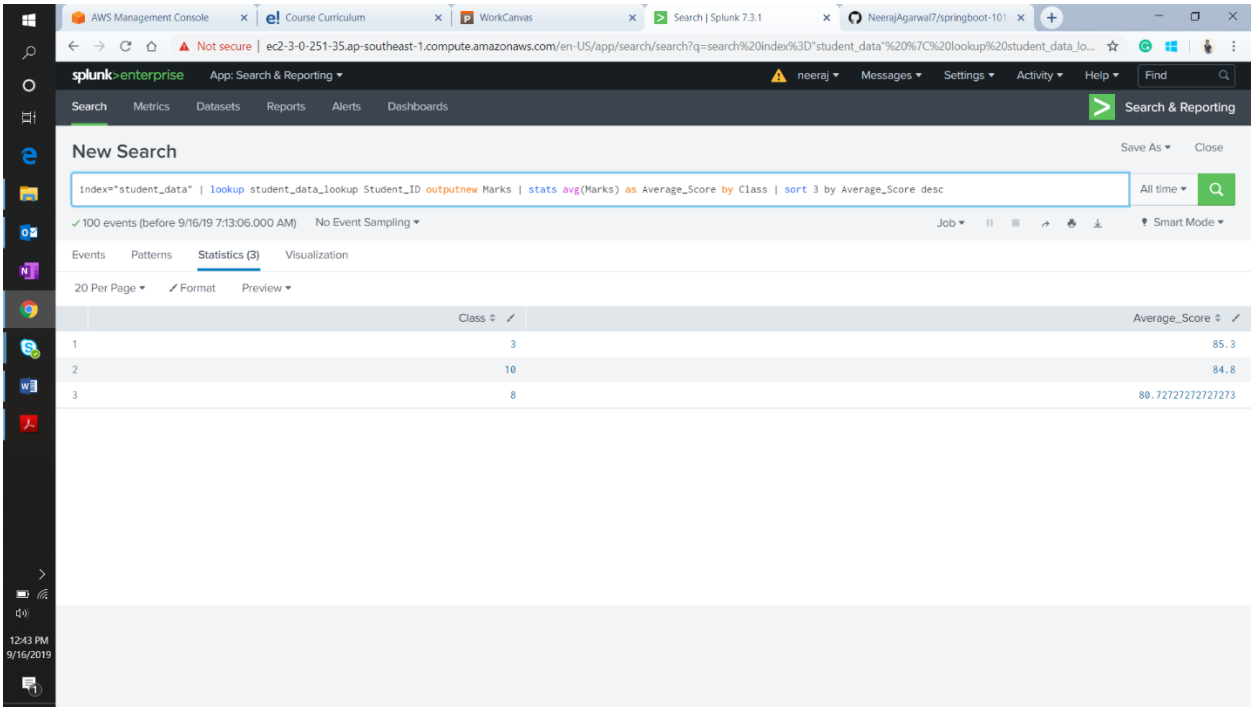
3. Average Marks in each Class
   Search string :

```
index="student_data" | lookup student_data_lookup Student_ID outputnew Marks | stats avg(Marks) as Average_Score by Class | sort by Class
```



4. Top 3 performing class
   Search String :

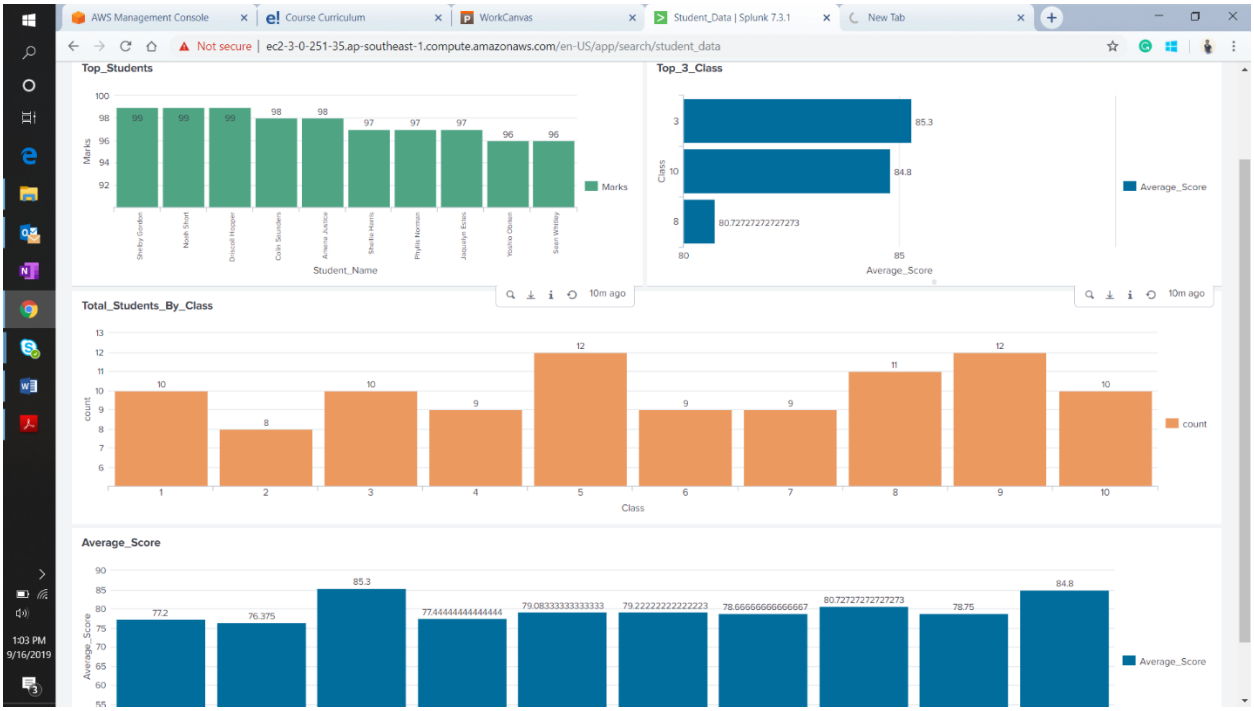
```
index="student_data" | lookup student_data_lookup Student_ID outputnew Marks | stats avg(Marks) as Average_Score by Class | sort 3 by Average_Score desc
```



Creating A Dashboard

Using the reports mentioned in the previous section I will create a simple dashboard consisting of bar charts to visualize the results of these searches instead of just a tabular form. I do this by creating a blank dashboard and selecting **add panel → new from reports**.

This is what we get after adding all 4 reports.



We can export it as pdf and share with other users as well.

Conclusion

This concludes the technical documentation for the solution to the project statement given.

As required I have,

- Created a data file with all the required data
- Created an index and added data to it
- Performed various searches
- Added lookup table
- Configured alert
- Created reports
- Created Dashboard

All the required files including the original data file will be present along with this document of reference.