



SPLUNK IMPLEMENTATION (EMPLOYEE DATA) CERTIFICATION PROJECT



Neeraj Agarwal
MINDTREE LTD

Problem Statement

Objective: Implement a Splunk project for the Employee details. Under this project, you will have to work with the log files of employee 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. Emp_ID
4. Emp_First_Name
5. Emp_Last_Name
6. Emp_Job_Title
7. Emp_Salary

Abstract

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

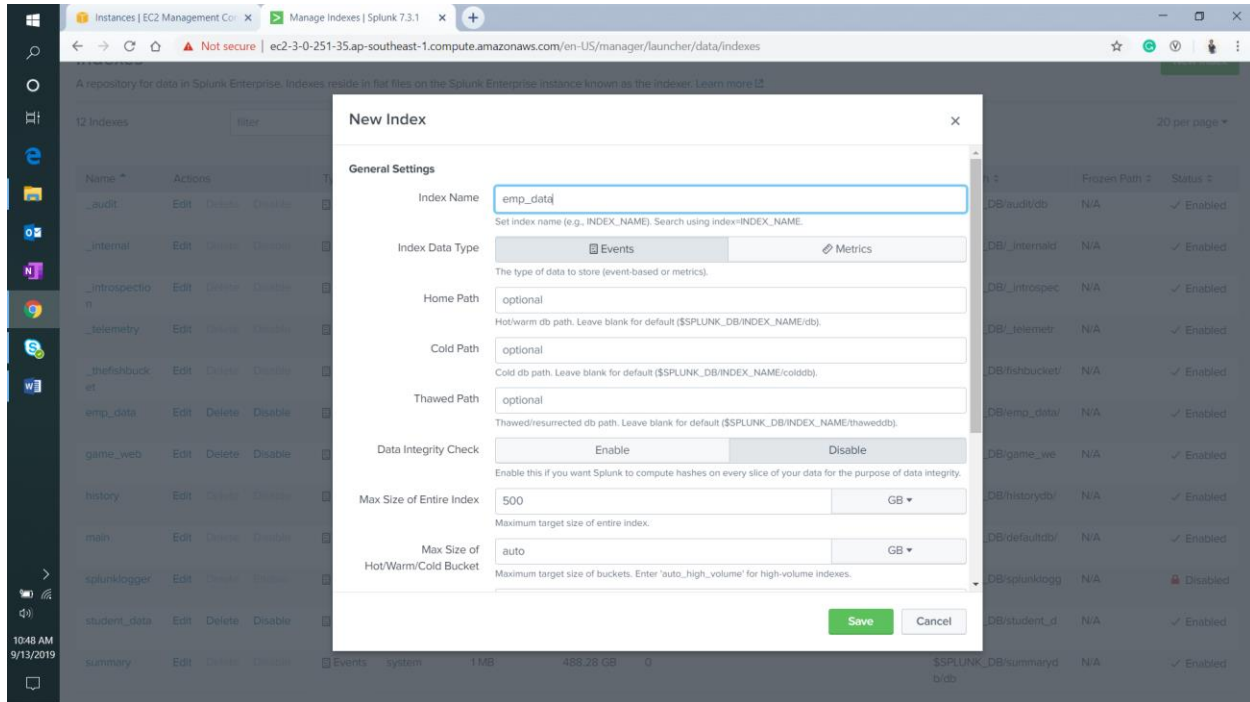
- **Creating an index**
- **Adding data sets**
- **Adding lookup tables**
- **Creating reports and alerts**
- **Creating dashboards**

Contents

| | |
|---|-----------|
| Creating an index..... | 4 |
| Adding data inputs..... | 5 |
| Basic searches (Fields Extraction) | 6 |
| Lookups | 11 |
| Adding an alert..... | 14 |
| Creating Reports..... | 16 |
| Creating A Dashboard..... | 20 |
| Conclusion | 21 |

Creating an index

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

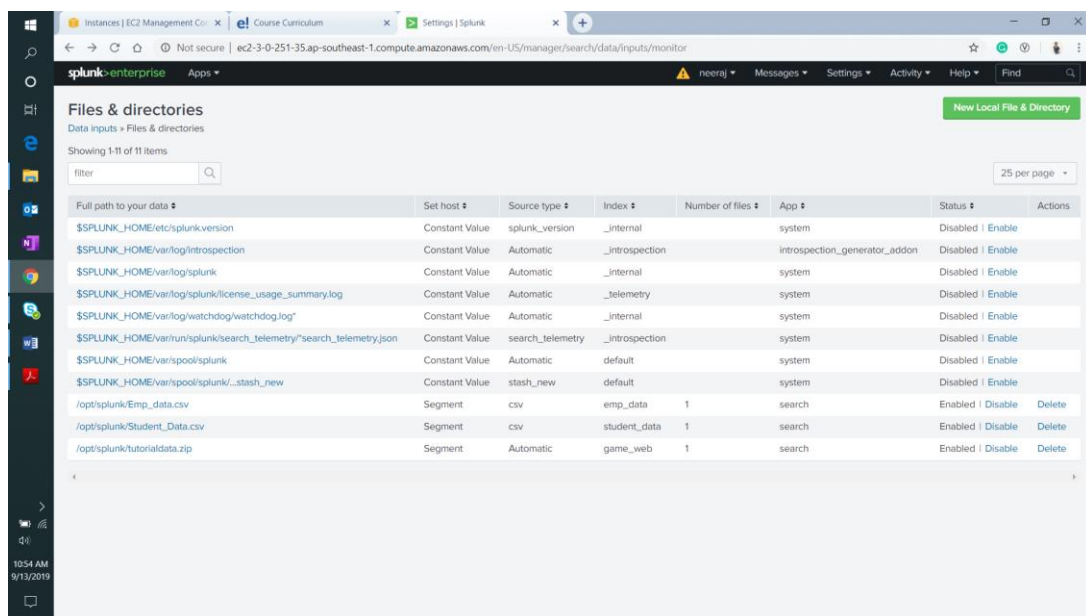
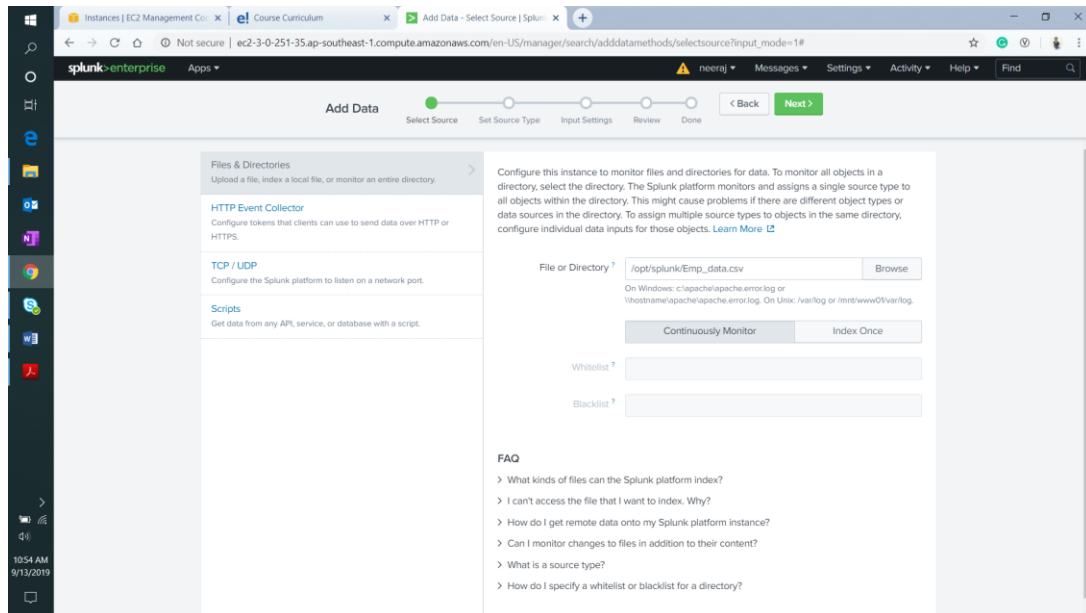


The screenshot shows the 'Manage Indexes' page in Splunk. The table lists 12 indexes. The 'emp_data' index is highlighted.

| Name | Actions | Type | App | Current Size | Max Size | Event Count | Earliest Event | Latest Event | Home Path | Frozen Path | Status |
|----------------|---------------------|--------|--------|--------------|-----------|-------------|----------------|-------------------|-------------------------------|-------------|------------|
| _audit | Edit Delete Disable | Events | system | 7 MB | 488.28 GB | 52.9K | 10 days ago | a few seconds ago | \$SPLUNK_DB/audit/db | N/A | ✓ Enabled |
| _internal | Edit Delete Disable | Events | system | 109 MB | 488.28 GB | 1.05M | 10 days ago | 4 days ago | \$SPLUNK_DB/_internal/db/db | N/A | ✓ Enabled |
| _introspection | Edit Delete Disable | Events | system | 183 MB | 488.28 GB | 158K | 10 days ago | 4 days ago | \$SPLUNK_DB/_introspection/db | N/A | ✓ Enabled |
| _telemetry | Edit Delete Disable | Events | system | 1 MB | 488.28 GB | 2 | 6 days ago | 6 days ago | \$SPLUNK_DB/_telemetry/db | N/A | ✓ Enabled |
| _thefishbucket | Edit Delete Disable | Events | system | 1 MB | 488.28 GB | 0 | | | \$SPLUNK_DB/fishbucket/db | N/A | ✓ Enabled |
| emp_data | Edit Delete Disable | Events | search | 1 MB | 500 GB | 300 | 4 days ago | 4 days ago | \$SPLUNK_DB/emp_data/db | N/A | ✓ Enabled |
| game_web | Edit Delete Disable | Events | search | 53 MB | 10 GB | 659K | a month ago | a month ago | \$SPLUNK_DB/game_web/db | N/A | ✓ Enabled |
| history | Edit Delete Disable | Events | system | 1 MB | 488.28 GB | 0 | | | \$SPLUNK_DB/history/db | N/A | ✓ Enabled |
| main | Edit Delete Disable | Events | system | 1 MB | 488.28 GB | 0 | | | \$SPLUNK_DB/defaultdb/db | N/A | ✓ Enabled |
| splunklogger | Edit Delete Enable | Events | system | 0 B | 488.28 GB | 0 | | | \$SPLUNK_DB/splunklogger/db | N/A | ✗ Disabled |
| student_data | Edit Delete Disable | Events | search | 1 MB | 500 GB | 100 | 4 days ago | 4 days ago | \$SPLUNK_DB/student_data/db | N/A | ✓ Enabled |
| summary | Edit Delete Disable | Events | system | 1 MB | 488.28 GB | 0 | | | \$SPLUNK_DB/summarydb/db | N/A | ✓ Enabled |

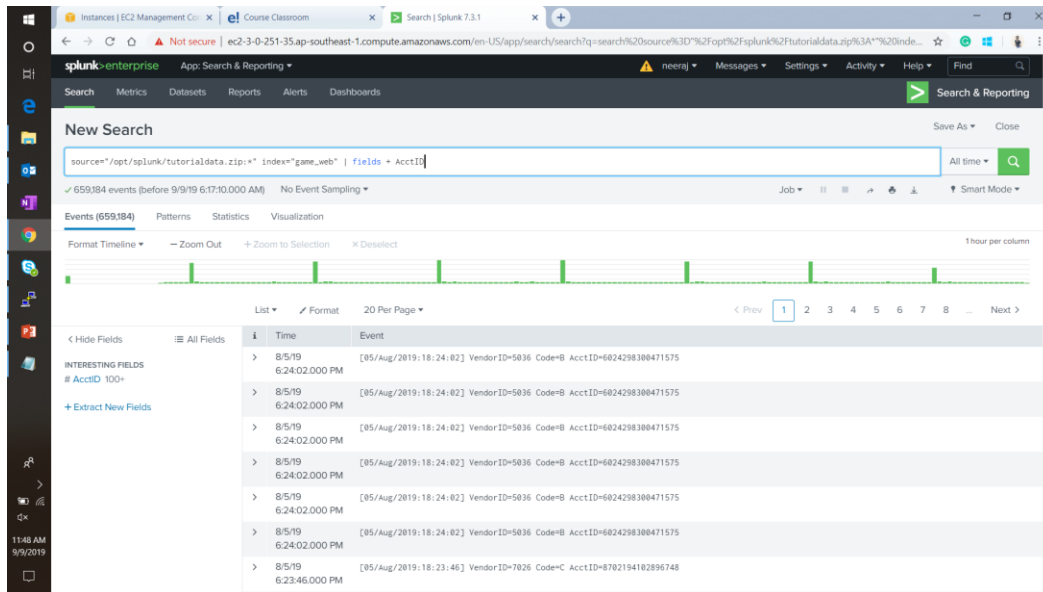
Adding data inputs

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

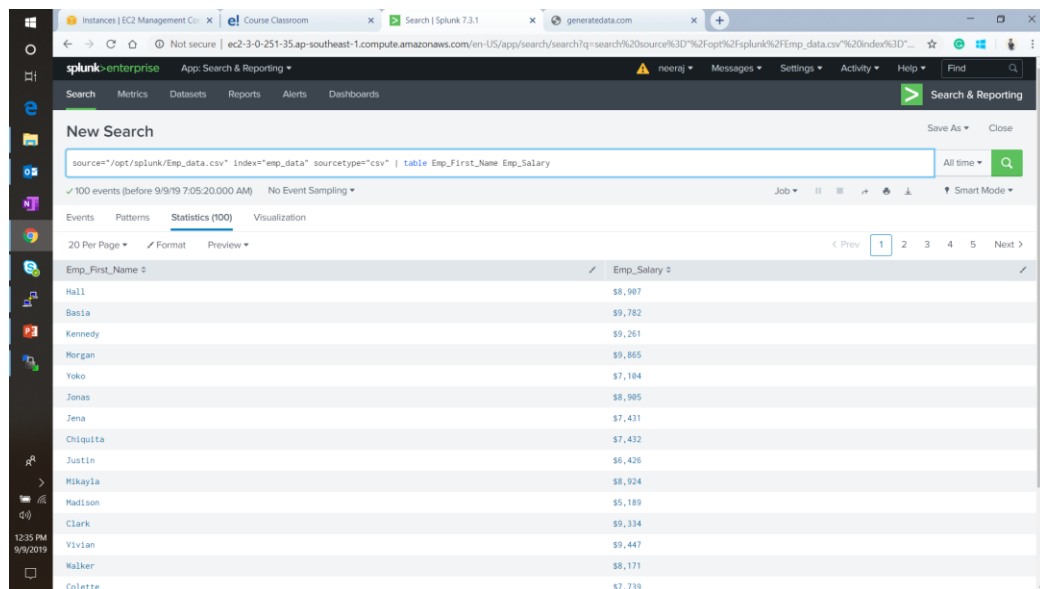


Basic searches (Fields Extraction)

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



Field Extraction



Example of “Table” command

The screenshot shows the Splunk Enterprise interface with a search results page. The search bar contains the query: `source="/opt/splunk/Emp_data.csv" index="emp_data" sourcetype="csv" | sort 5 Emp_Salary desc`. The results are displayed in a table with columns for Time and Event. The 'Event' column shows the salary for each employee, sorted in descending order.

| Time | Event |
|-----------------------|--|
| 9/9/19 6:57:28.000 AM | 06/27/28,184,Vance,Gay,Legal Department,"\$9,987" |
| 9/9/19 6:57:28.000 AM | 03/28/19,145,Morgan,Saunders,Quality Assurance,"\$9,865" |
| 9/9/19 6:57:28.000 AM | 03/11/19,147,Basia,Irwin,Customer Relations,"\$9,782" |
| 9/9/19 6:57:28.000 AM | 01/07/19,188,Amy,Wess,Asset Management,"\$9,781" |
| 9/9/19 6:57:28.000 AM | 09/26/19,126,Bryar,Haynes,Human Resources,"\$9,697" |

Example of “Sort” command

The screenshot shows the Splunk Enterprise interface with a search results page. The search bar contains the query: `source="/opt/splunk/Emp_data.csv" index="emp_data" sourcetype="csv" | Rename Emp_Salary as Salary`. The results are displayed in a table with columns for Time and Event. The 'Event' column shows the salary for each employee, with the field name 'Emp_Salary' renamed to 'Salary'.

| Time | Event |
|-----------------------|---|
| 9/9/19 6:57:28.000 AM | 08/19/28,199,Jerome,Foley,Sales and Marketing,"\$6,981" |
| 9/9/19 6:57:28.000 AM | 09/01/28,198,George,Colon,Asset Management,"\$9,342" |
| 9/9/19 6:57:28.000 AM | 04/08/19,197,Jerome,Buck,Public Relations,"\$5,686" |
| 9/9/19 6:57:28.000 AM | 08/11/28,196,Garrett,Johns,Research and Development,"\$5,895" |
| 9/9/19 6:57:28.000 AM | 06/28/28,195,Xenos,David,Customer Service,"\$5,583" |
| 9/9/19 6:57:28.000 AM | 05/18/28,194,Melissa,Jimenez,Accounting,"\$5,346" |
| 9/9/19 6:57:28.000 AM | 10/28/18,193,Orlando,Hopkins,Customer Relations,"\$5,766" |

Example of “Rename” command

New Search

source=opt/splunk/Emp_data.csv index=emp_data sourcetype=csv | search Emp_ID > 100

✓ 9 events (before 9/9/19 7:08:23.000 AM) No Event Sampling

| Time | Event |
|-----------------------|---|
| 9/9/19 6:57:28.000 AM | 08/19/20,199,Jerome,Foley,Sales and Marketing,"\$6,981" |
| 9/9/19 6:57:28.000 AM | 09/01/20,198,George,Colon,Asset Management,"\$9,342" |
| 9/9/19 6:57:28.000 AM | 04/08/19,197,Jerome,Buck,Public Relations,"\$5,686" |
| 9/9/19 6:57:28.000 AM | 08/11/20,196,Garrett,Johns,Research and Development,"\$5,895" |
| 9/9/19 6:57:28.000 AM | 06/20/20,195,Xenos,David,Customer Service,"\$5,583" |
| 9/9/19 6:57:28.000 AM | 05/18/20,194,Melissa,Jimenez,Accounting,"\$5,346" |
| 9/9/19 | 10/20/18,193,Orlando,Hopkins,Customer Relations,"\$5,766" |

Example of “search” command

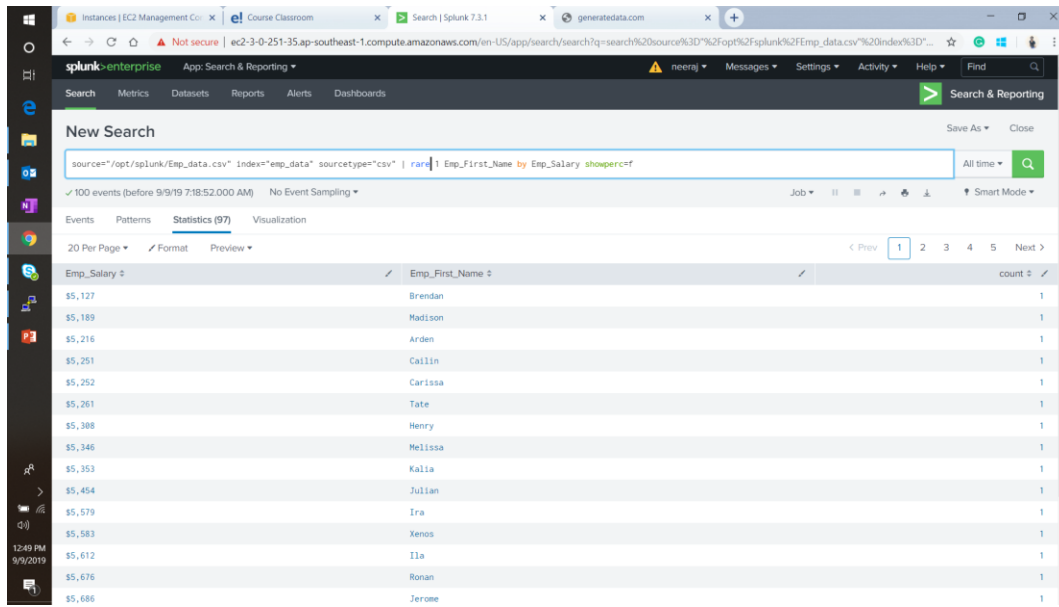
New Search

source=opt/splunk/Emp_data.csv index=emp_data sourcetype=csv | top 1 Emp_First_Name by Emp_Salary showperc=f

✓ 100 events (before 9/9/19 7:17:36.000 AM) No Event Sampling

| Emp_Salary | Emp_First_Name | count |
|------------|----------------|-------|
| \$5,127 | Brendan | 1 |
| \$5,189 | Madison | 1 |
| \$5,216 | Arden | 1 |
| \$5,251 | Callin | 1 |
| \$5,252 | Carlissa | 1 |
| \$5,261 | Tate | 1 |
| \$5,308 | Henry | 1 |
| \$5,346 | Melissa | 1 |
| \$5,353 | Kalia | 1 |
| \$5,454 | Julian | 1 |
| \$5,579 | Ira | 1 |
| \$5,583 | Xenos | 1 |
| \$5,612 | Ila | 1 |
| \$5,676 | Ronan | 1 |
| \$5,686 | Jerome | 1 |

Example of “Top” command



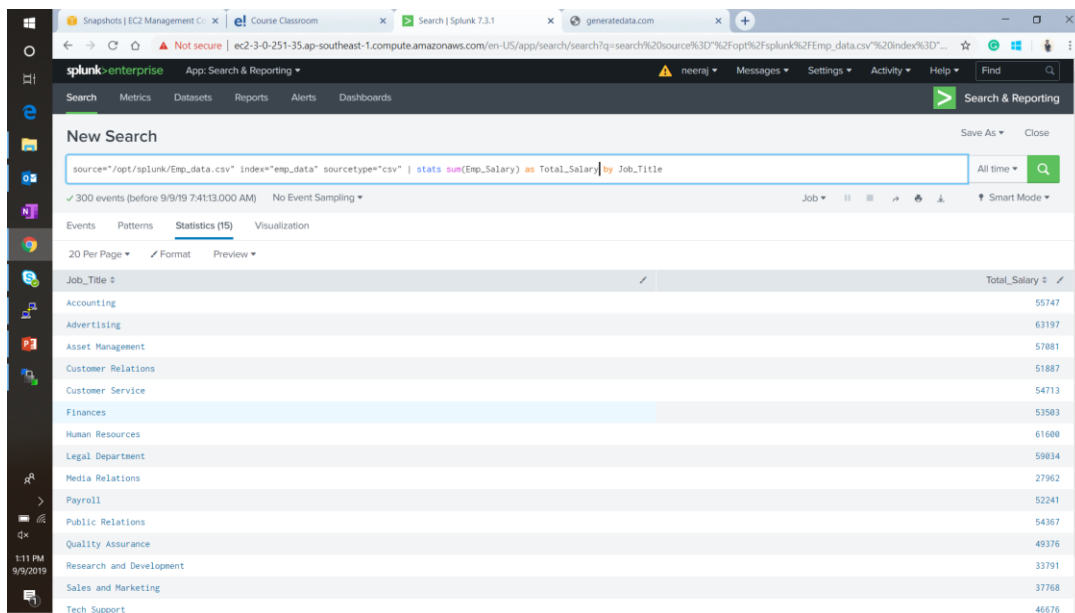
New Search

source="/opt/splunk/Emp_data.csv" index="emp_data" sourcetype="csv" | rare | Emp_First_Name by Emp_Salary showperc=f

100 events (before 9/9/19 7:18:52.000 AM) No Event Sampling

| Emp_Salary | Emp_First_Name | count |
|------------|----------------|-------|
| \$5,127 | Brendan | 1 |
| \$5,189 | Madison | 1 |
| \$5,216 | Arden | 1 |
| \$5,251 | Callin | 1 |
| \$5,252 | Carissa | 1 |
| \$5,261 | Tate | 1 |
| \$5,388 | Henry | 1 |
| \$5,346 | Melissa | 1 |
| \$5,353 | Kalia | 1 |
| \$5,454 | Julian | 1 |
| \$5,579 | Ira | 1 |
| \$5,583 | Xenos | 1 |
| \$5,612 | Ila | 1 |
| \$5,676 | Ronan | 1 |
| \$5,686 | Jerome | 1 |

Example of “Rare” command



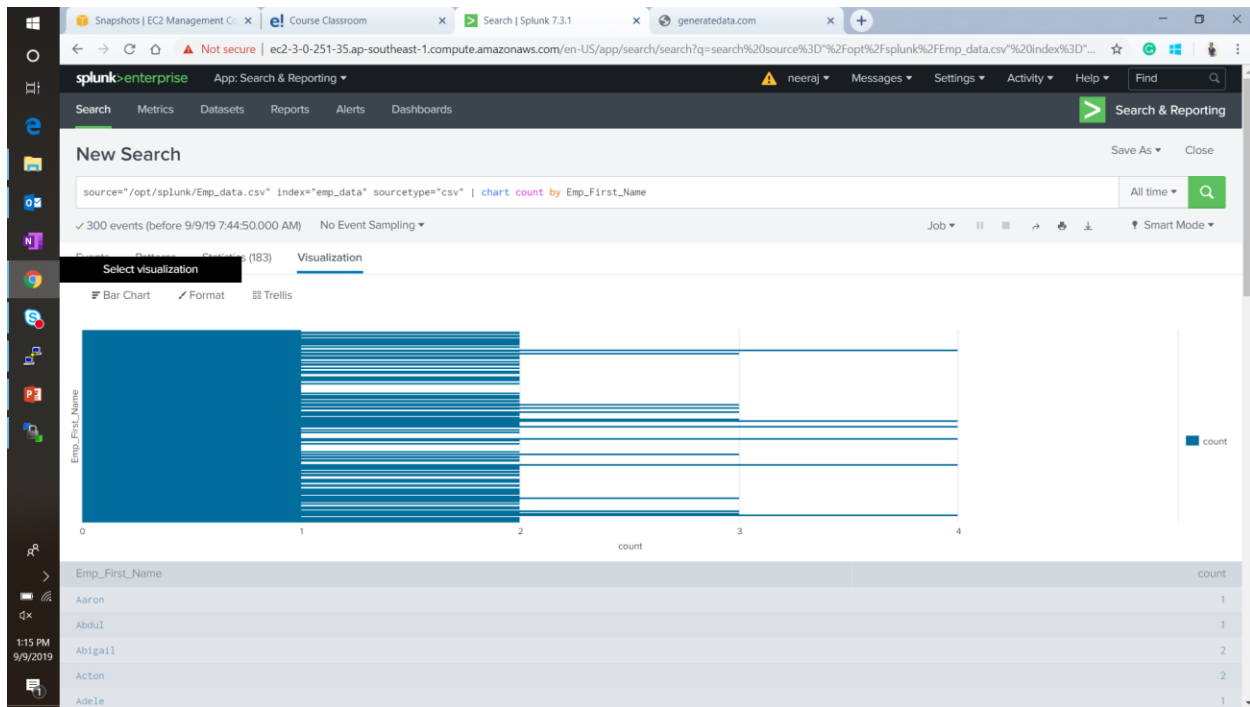
New Search

source="/opt/splunk/Emp_data.csv" index="emp_data" sourcetype="csv" | stats sum(Emp_Salary) as Total_Salary by Job_Title

300 events (before 9/9/19 7:41:13.000 AM) No Event Sampling

| Job_Title | Total_Salary |
|--------------------------|--------------|
| Accounting | 55747 |
| Advertising | 63197 |
| Asset Management | 57881 |
| Customer Relations | 51887 |
| Customer Service | 54713 |
| Finances | 53583 |
| Human Resources | 61688 |
| Legal Department | 59834 |
| Media Relations | 27962 |
| Payroll | 52241 |
| Public Relations | 54367 |
| Quality Assurance | 49376 |
| Research and Development | 33791 |
| Sales and Marketing | 37768 |
| Tech Support | 46676 |

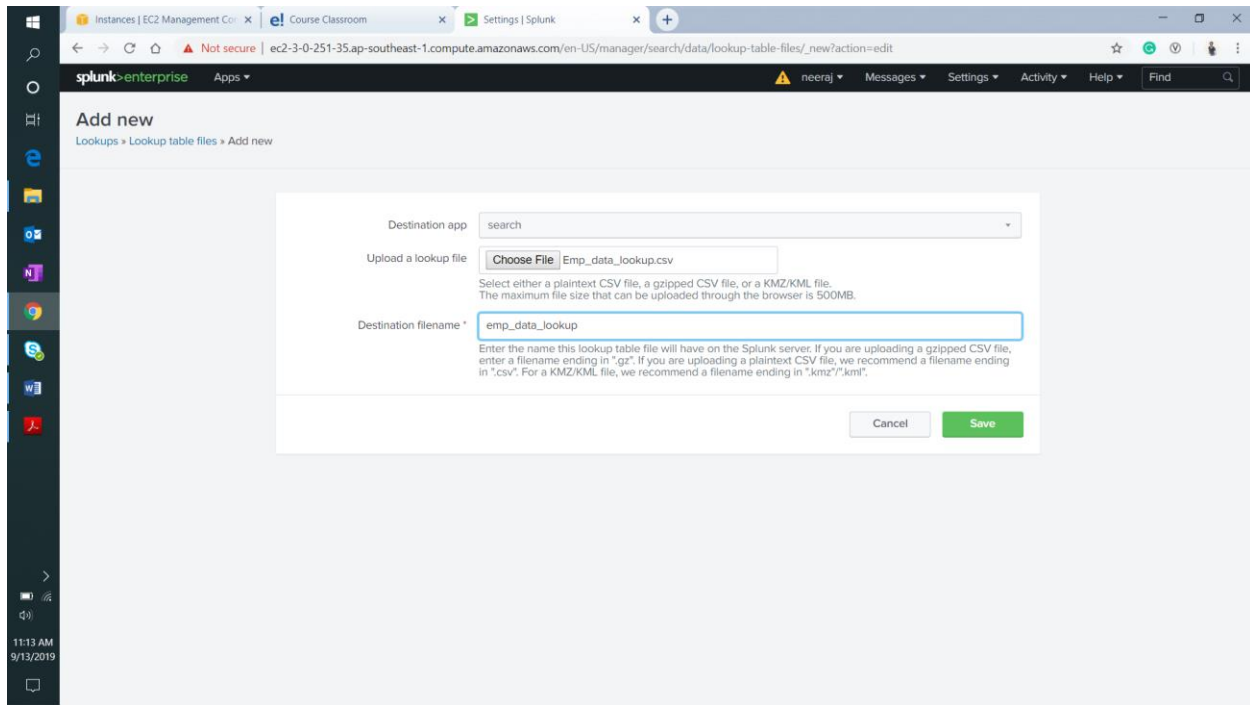
Example of “Stats” command



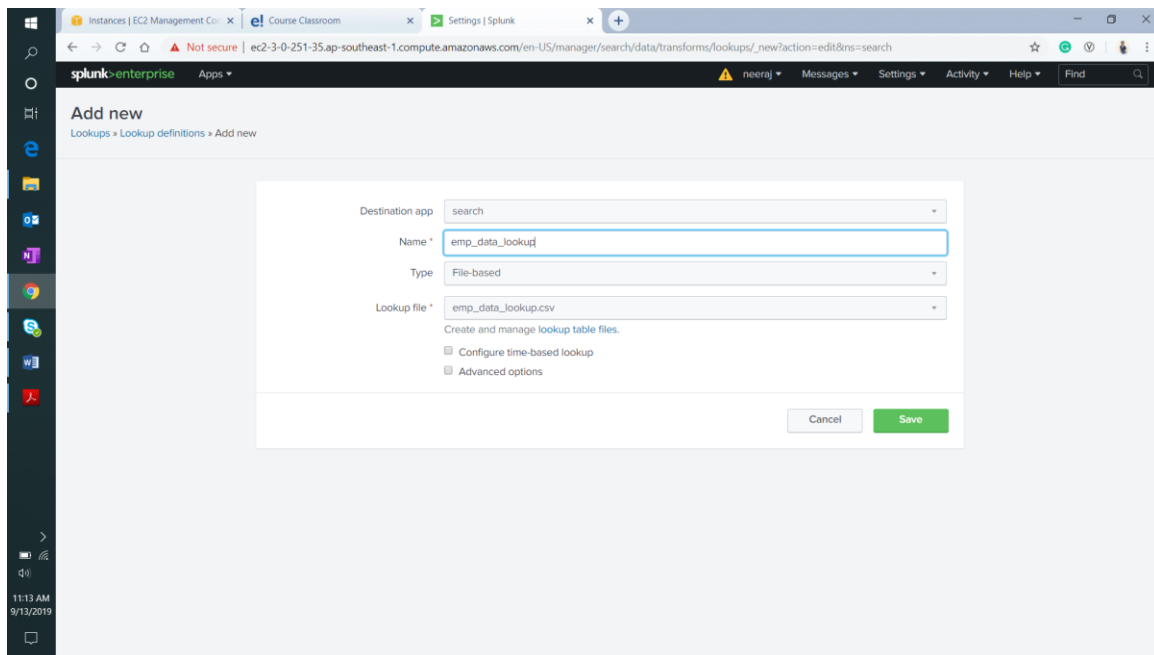
Example of “Chart” command

Lookups

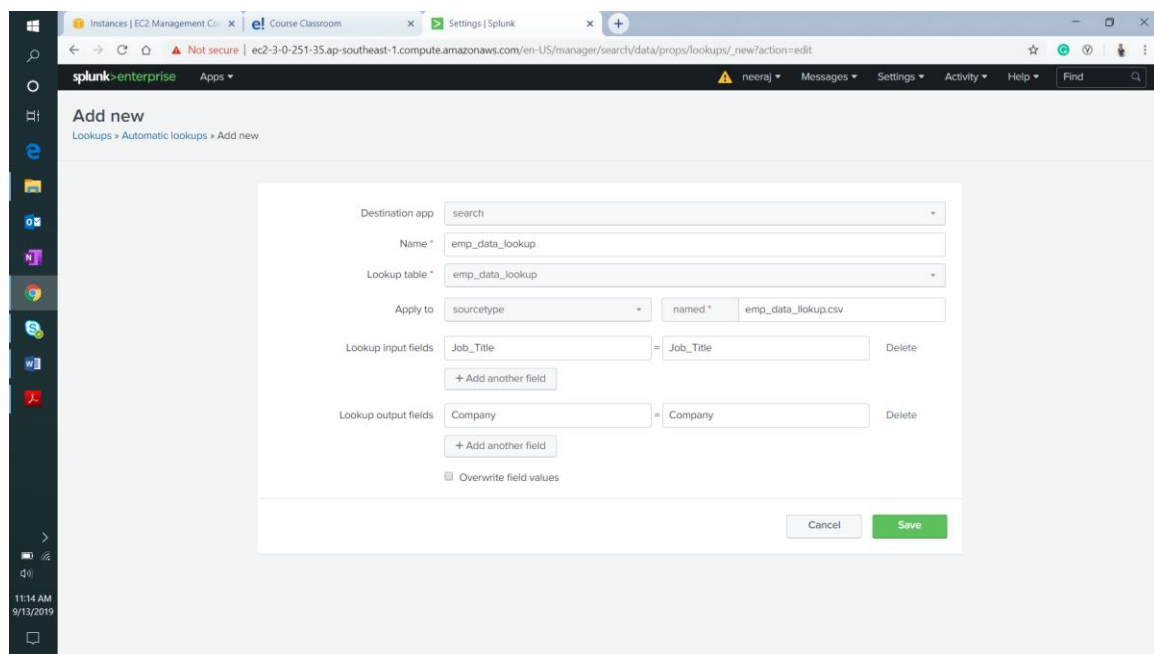
In this section, I will add a lookup table to map the employee's job title to the company they are associated with. I have created a csv file with above-mentioned data.



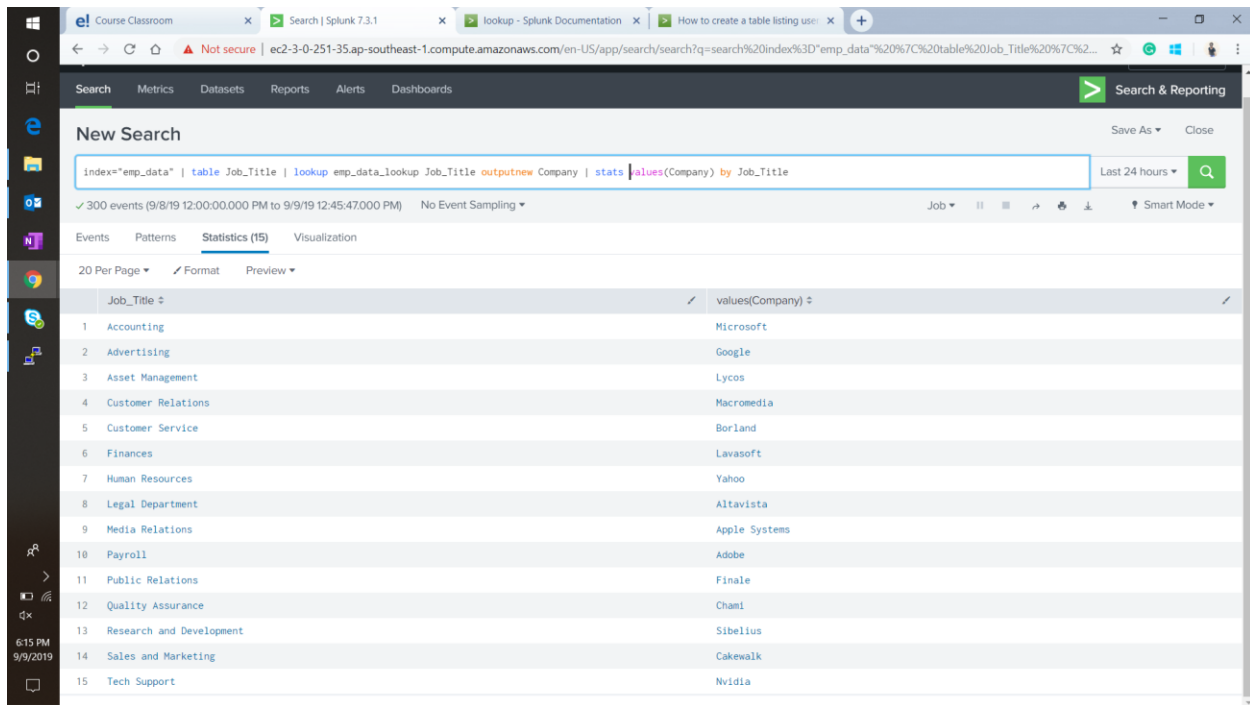
Adding the lookup file



Adding a new lookup definition



Adding automatic lookup



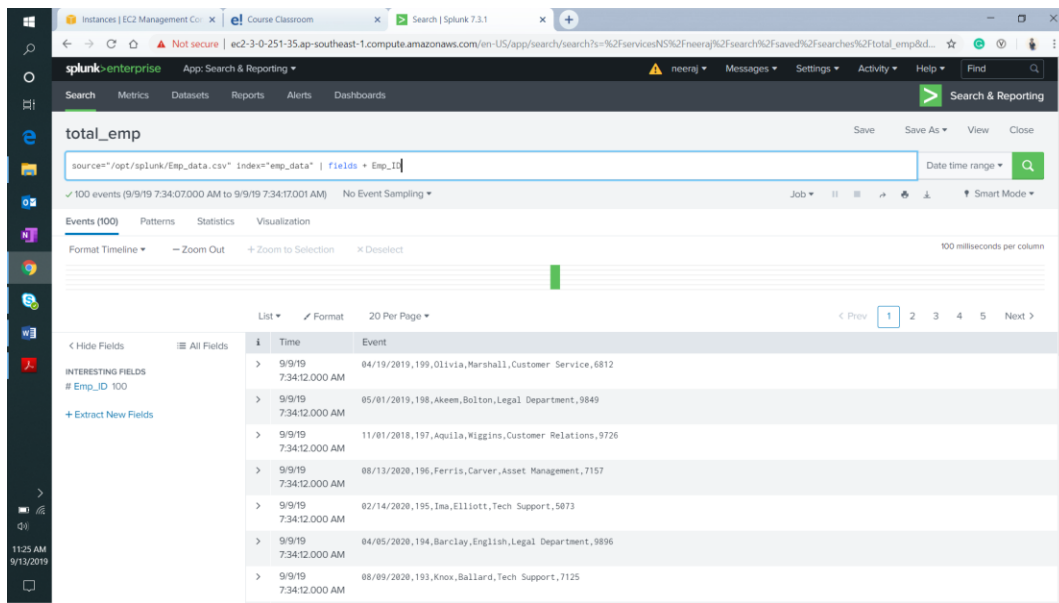
The screenshot shows the Splunk Search interface. The search bar contains the query: `index="emp_data" | table Job_Title | lookup emp_data_lookup Job_Title outputnew Company | stats values(Company) by Job_Title`. The search results are displayed in a table with two columns: `Job_Title` and `values(Company)`. The table lists 15 job titles and their corresponding companies. The interface includes a sidebar with navigation options (Search, Metrics, Datasets, Reports, Alerts, Dashboards) and a top navigation bar with a search bar and a 'Search & Reporting' button. The search results are shown in 'Statistics (15)' mode, with a '20 Per Page' dropdown and a 'Format' button. The search results are displayed in a table with two columns: `Job_Title` and `values(Company)`. The table lists 15 job titles and their corresponding companies.

| Job_Title | values(Company) |
|-----------------------------|-----------------|
| 1 Accounting | Microsoft |
| 2 Advertising | Google |
| 3 Asset Management | Lycos |
| 4 Customer Relations | Macromedia |
| 5 Customer Service | Borland |
| 6 Finances | Lavasoft |
| 7 Human Resources | Yahoo |
| 8 Legal Department | Altavista |
| 9 Media Relations | Apple Systems |
| 10 Payroll | Adobe |
| 11 Public Relations | Finale |
| 12 Quality Assurance | Chani |
| 13 Research and Development | Sibelius |
| 14 Sales and Marketing | Cakewalk |
| 15 Tech Support | Nvidia |

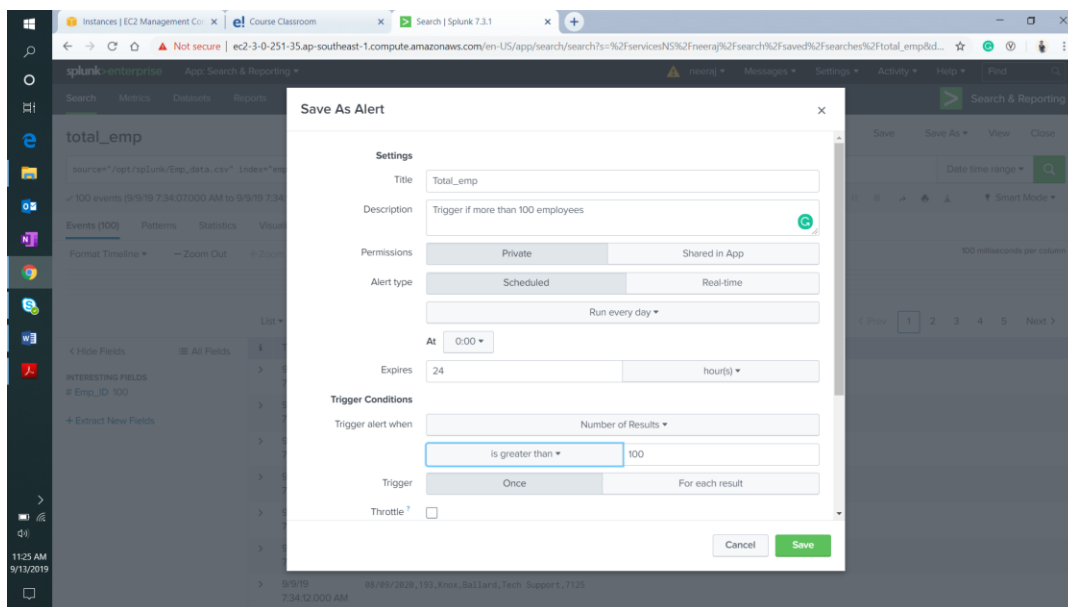
Example of a search which utilizes lookup

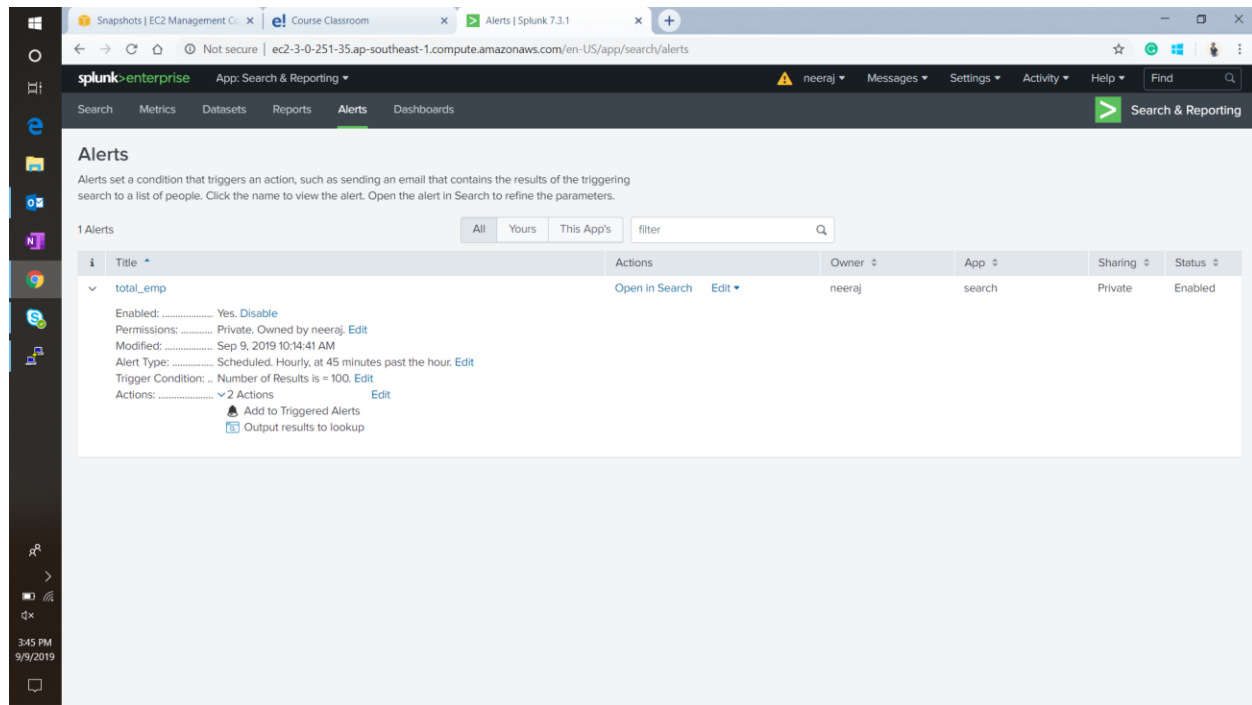
Adding an alert

Here I am configuring an alert where if the search returns showing more than 100 employees 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

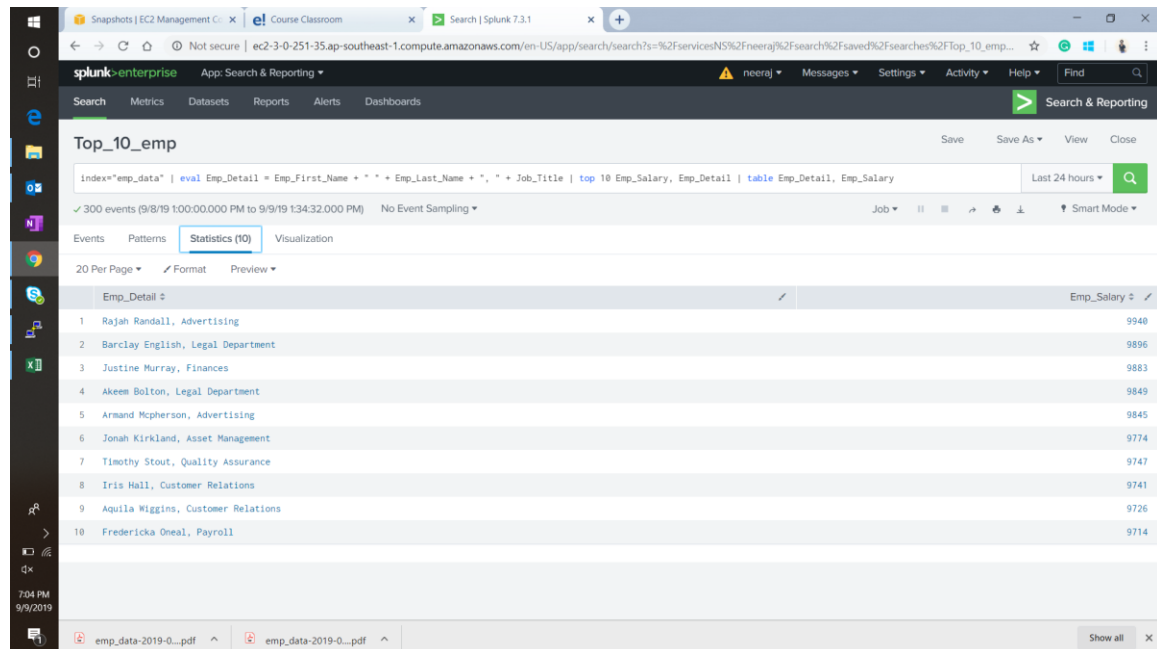
Creating Reports

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 earning employees

Search string :

```
index="emp_data" | eval Emp_Detail = Emp_First_Name + " " +  
Emp_Last_Name + ", " + Job_Title | top 10 Emp_Salary,  
Emp_Detail | table Emp_Detail, Emp_Salary
```



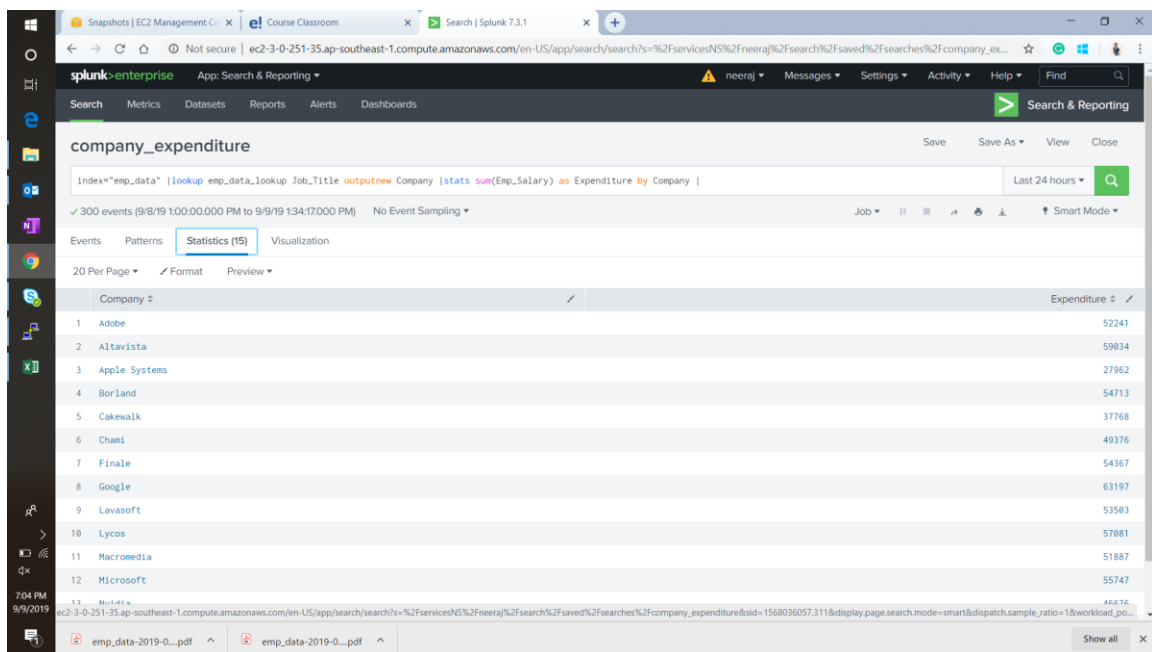
The screenshot displays the Splunk Search & Reporting interface. The search string is: `index="emp_data" | eval Emp_Detail = Emp_First_Name + " " + Emp_Last_Name + ", " + Job_Title | top 10 Emp_Salary, Emp_Detail | table Emp_Detail, Emp_Salary`. The results are sorted by salary in descending order.

| Emp_Detail | Emp_Salary |
|--------------------------------------|------------|
| 1 Rajah Randall, Advertising | 9940 |
| 2 Barclay English, Legal Department | 9896 |
| 3 Justine Murray, Finances | 9883 |
| 4 Akeem Bolton, Legal Department | 9849 |
| 5 Armand Mcpherson, Advertising | 9845 |
| 6 Jonah Kirkland, Asset Management | 9774 |
| 7 Timothy Stout, Quality Assurance | 9747 |
| 8 Iris Hall, Customer Relations | 9741 |
| 9 Aquila Wiggins, Customer Relations | 9726 |
| 10 Fredericka Oneal, Payroll | 9714 |

2. Expenditure of each company in employee salaries

Search string :

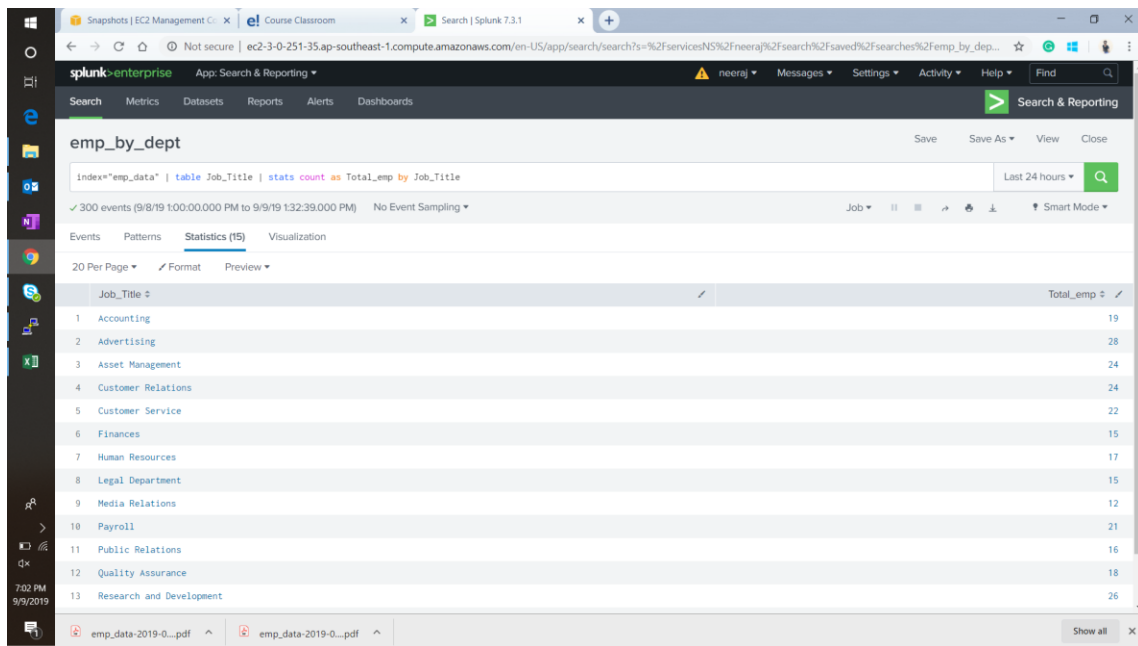
```
index="emp_data" |lookup emp_data_lookup Job_Title  
outputnew Company |stats sum(Emp_Salary) as Expenditure by  
Company
```



3. Total employees in each department

Search string :

```
index="emp_data" | table Job_Title | stats count as Total_emp  
by Job_Title
```



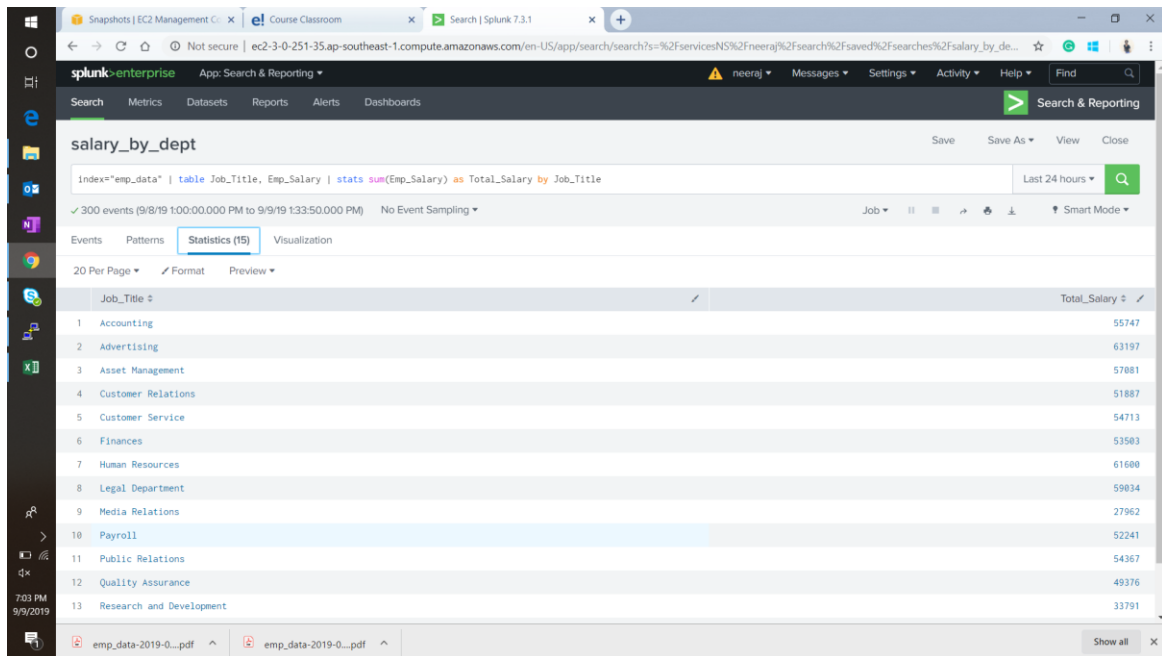
The screenshot shows the Splunk Search & Reporting interface. The search bar contains the query: `index="emp_data" | table Job_Title | stats count as Total_emp by Job_Title`. The results are displayed in a table with 13 rows, each representing a department and its corresponding employee count. The table has two columns: `Job_Title` and `Total_emp`. The data is as follows:

| Job_Title | Total_emp |
|-----------------------------|-----------|
| 1 Accounting | 19 |
| 2 Advertising | 28 |
| 3 Asset Management | 24 |
| 4 Customer Relations | 24 |
| 5 Customer Service | 22 |
| 6 Finances | 15 |
| 7 Human Resources | 17 |
| 8 Legal Department | 15 |
| 9 Media Relations | 12 |
| 10 Payroll | 21 |
| 11 Public Relations | 16 |
| 12 Quality Assurance | 18 |
| 13 Research and Development | 26 |

4. Total salary spent in each department

Search String :

```
index="emp_data" | table Job_Title, Emp_Salary | stats  
sum(Emp_Salary) as Total_Salary by Job_Title
```



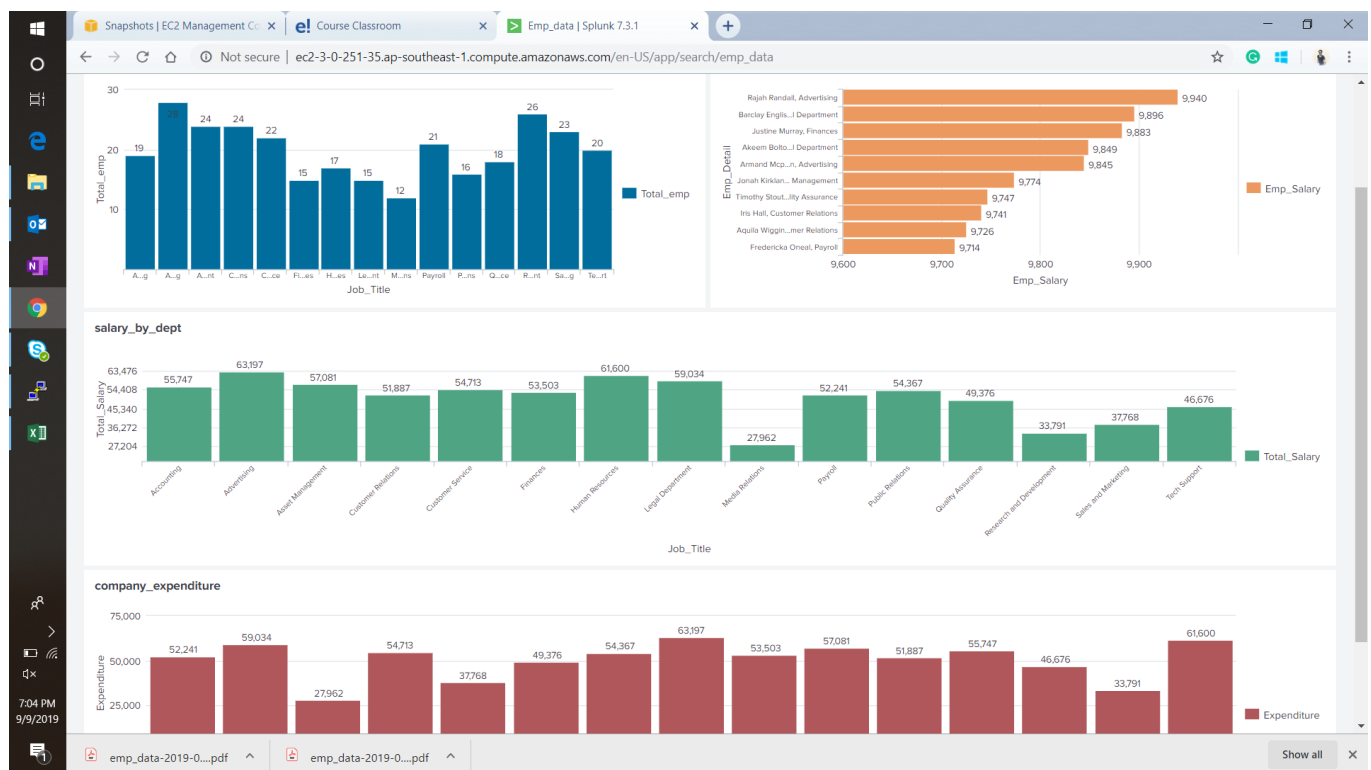
The screenshot shows the Splunk Search & Reporting interface. The search bar contains the query: `index="emp_data" | table Job_Title, Emp_Salary | stats sum(Emp_Salary) as Total_Salary by Job_Title`. The results are displayed in a table with two columns: Job_Title and Total_Salary. The table lists 13 departments and their corresponding total salaries.

| Job_Title | Total_Salary |
|-----------------------------|--------------|
| 1 Accounting | 55747 |
| 2 Advertising | 63197 |
| 3 Asset Management | 57881 |
| 4 Customer Relations | 51887 |
| 5 Customer Service | 54713 |
| 6 Finances | 53583 |
| 7 Human Resources | 61600 |
| 8 Legal Department | 59034 |
| 9 Media Relations | 27962 |
| 10 Payroll | 52241 |
| 11 Public Relations | 54367 |
| 12 Quality Assurance | 49376 |
| 13 Research and Development | 33791 |

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.