**Download Items:**

**Elastic Search:**

1. Open Below URL.

<https://www.elastic.co/downloads/elasticsearch>

1. Download Elastic Search TAR File.
2. Untar file elasticsearch-5.3.0.tar.gz file.
3. Copy the extracted folder in 10.99.18.152 machine.
4. Run the elastic search shell file under bin folder(./bin/elasticsearch.sh)

**Kibana:**

1. Open Below URL.

<https://www.elastic.co/downloads/kibana>

1. Download Kibana TAR File.
2. Untar file kibana-5.3.0-linux-x86\_64.tar.gz file.
3. Copy the extracted folder in 10.99.18.152 machine.
4. Open the Kibana.yml under config folder and make the changes as per below file(Hostname and Port)



1. Run the kibana shell file under bin folder(./bin/kibana.sh)

**Logstash:**

1. Open Below URL.

<https://www.elastic.co/downloads/logstash>

1. Download Logstash TAR file.
2. Untar file logstash-5.3.0-linux-x86\_64.tar.gz file.
3. Copy the extracted folder in 10.99.18.152 machine.
4. Open the config folder and paste below file under config folder.



1. Run the logstash shell file under bin folder(./bin/logstash -f logstash.conf)

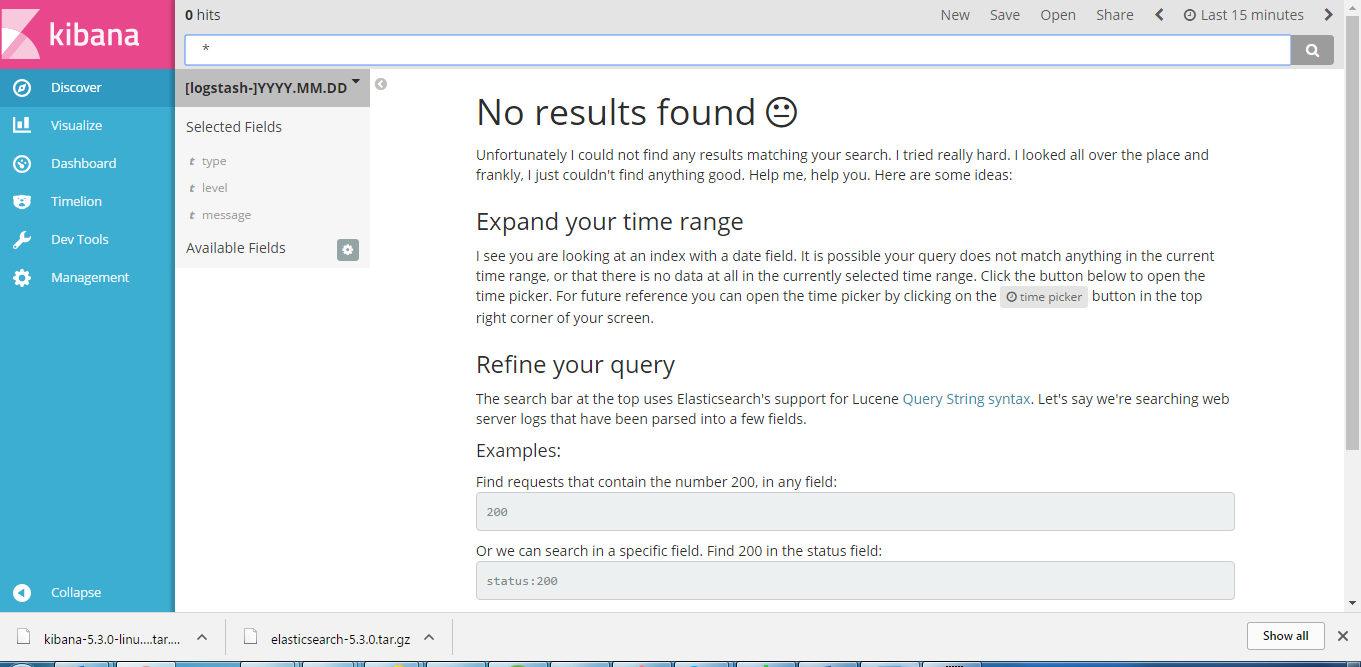
**How to SetUp Kibana**

Kibana is used for GUI representation of the logs that are indexed and stored by elastic search after fetching it through file location by logstash.

Open below URL.

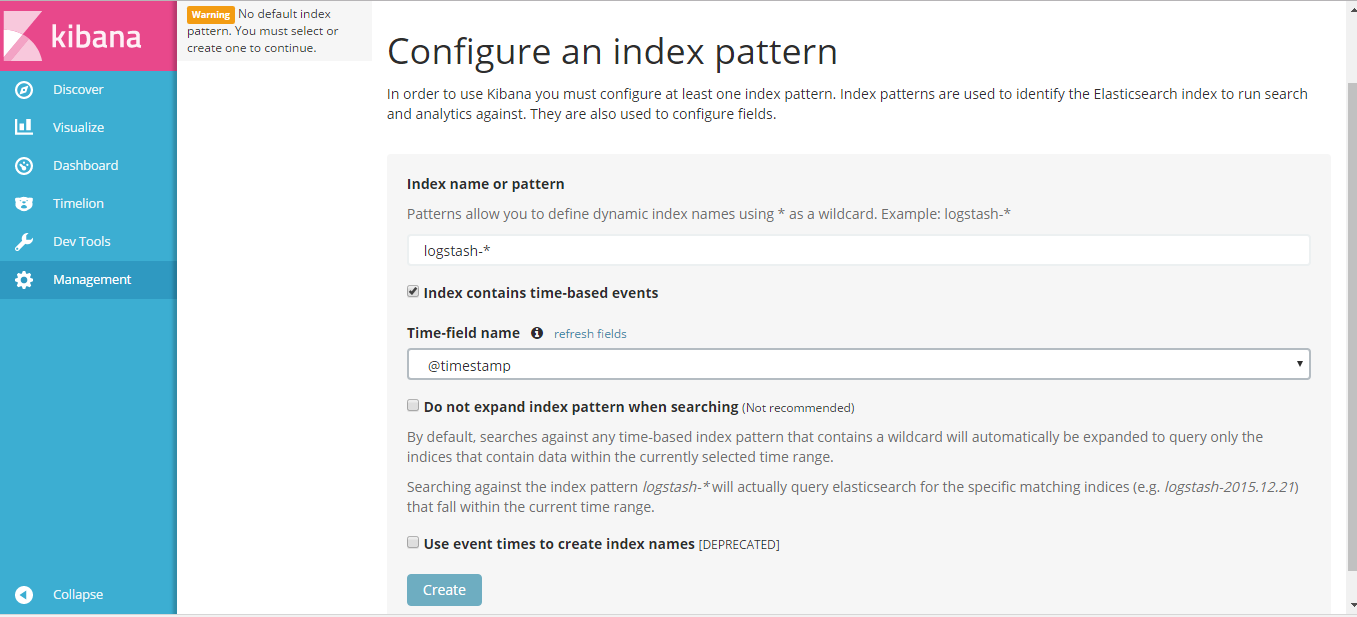
<http://10.99.18.152:50630>

URL will open below page if Kibana Stared properly.

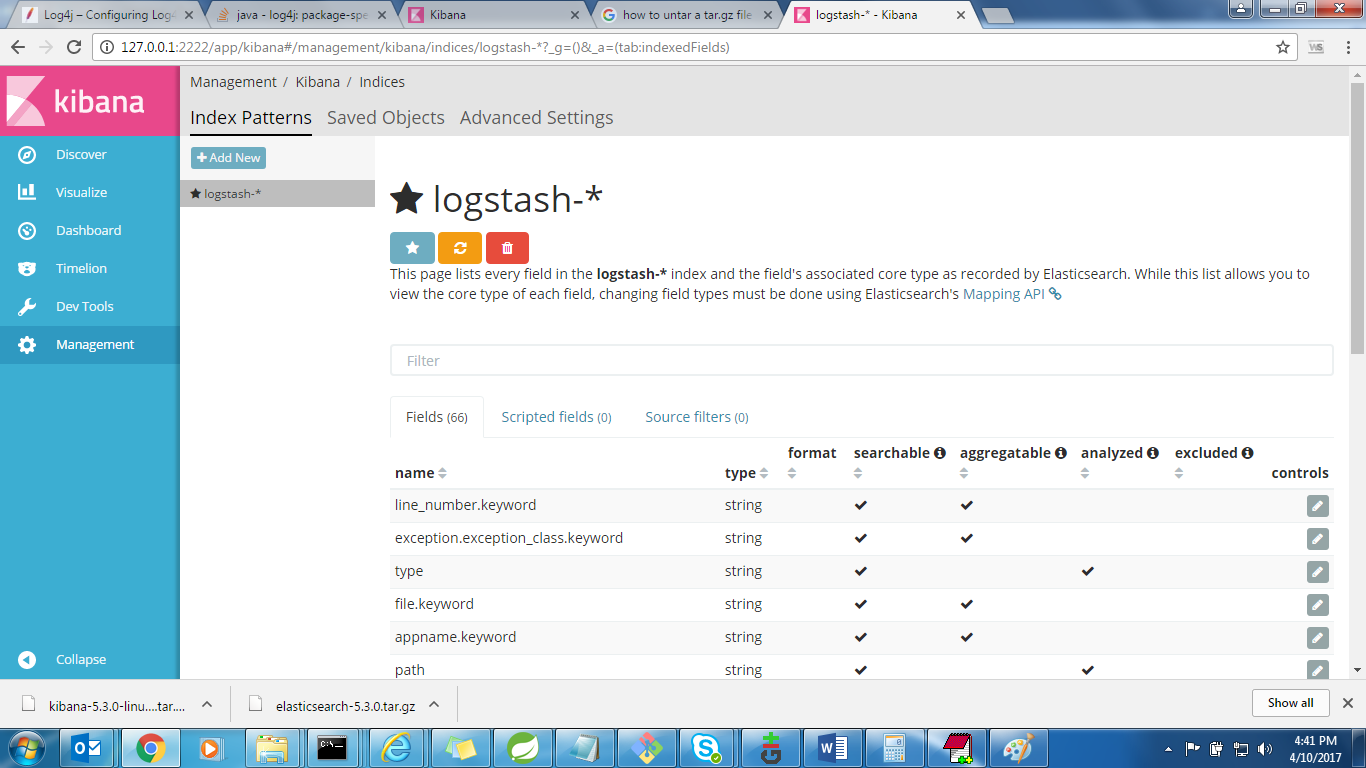


**Management and Discover Tab:**

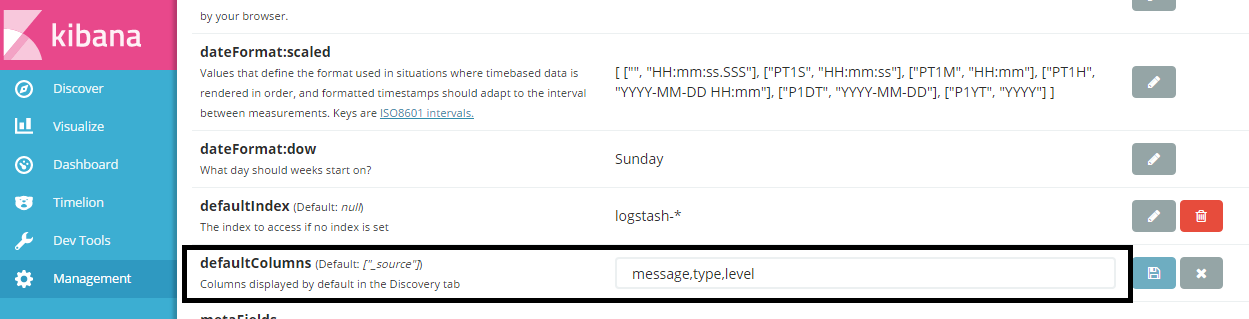
1. Go to Management Tab and click on Index Pattern( Management🡪 Index Pattern)
2. In the Index Name, Enter logstash-\*
3. Select ‘Index contains time based events’ checkbox from screen,
4. Select @timestamp from drop down menu item.
5. Click on Create button as shown in below screen.



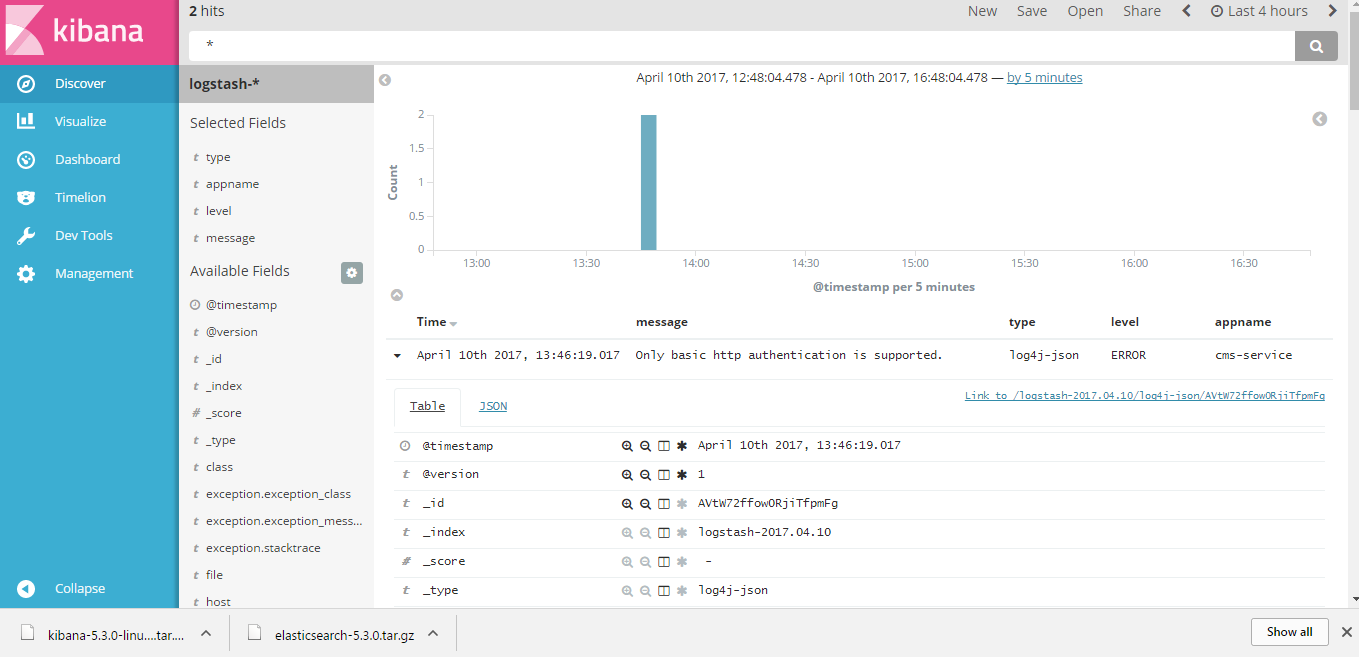
After creation of index Pattern, below screen would appear.



1. Now click on Advanced Settings.
2. Click on Default Columns text box and select the columns you want to show on the discover tab (Time, message, level, appname, host)

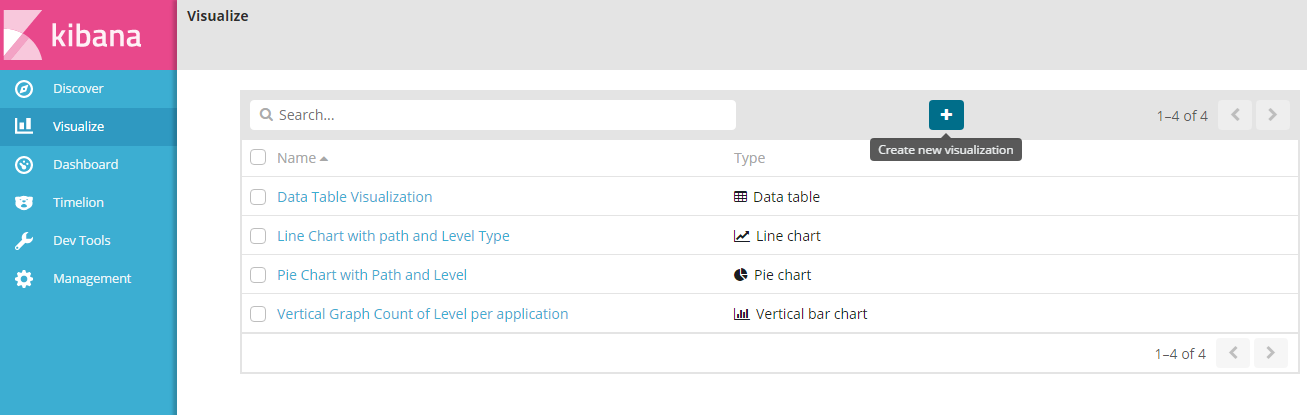


1. Now Click on Discover Tab and click on search button in discover tab
2. If Micro services would be running, there logs would be shown as per below screenshot.

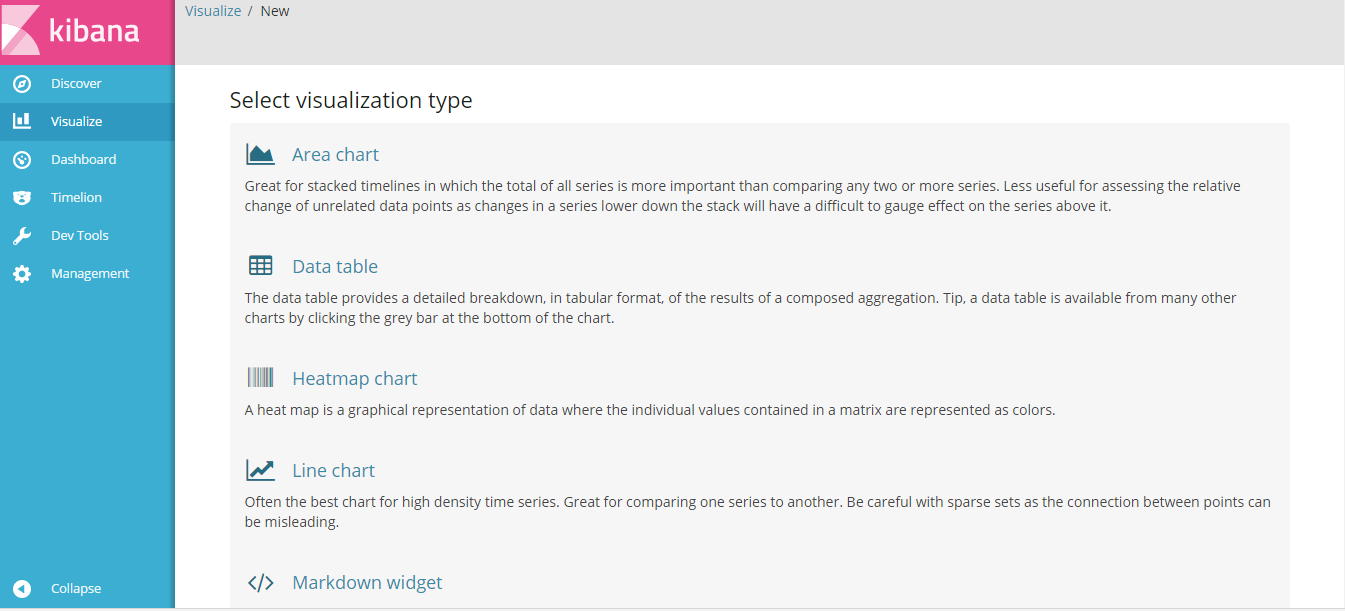


**Visualization and Dashboard Tab:**

We can show the visualization through the saved searches or the search that is running.

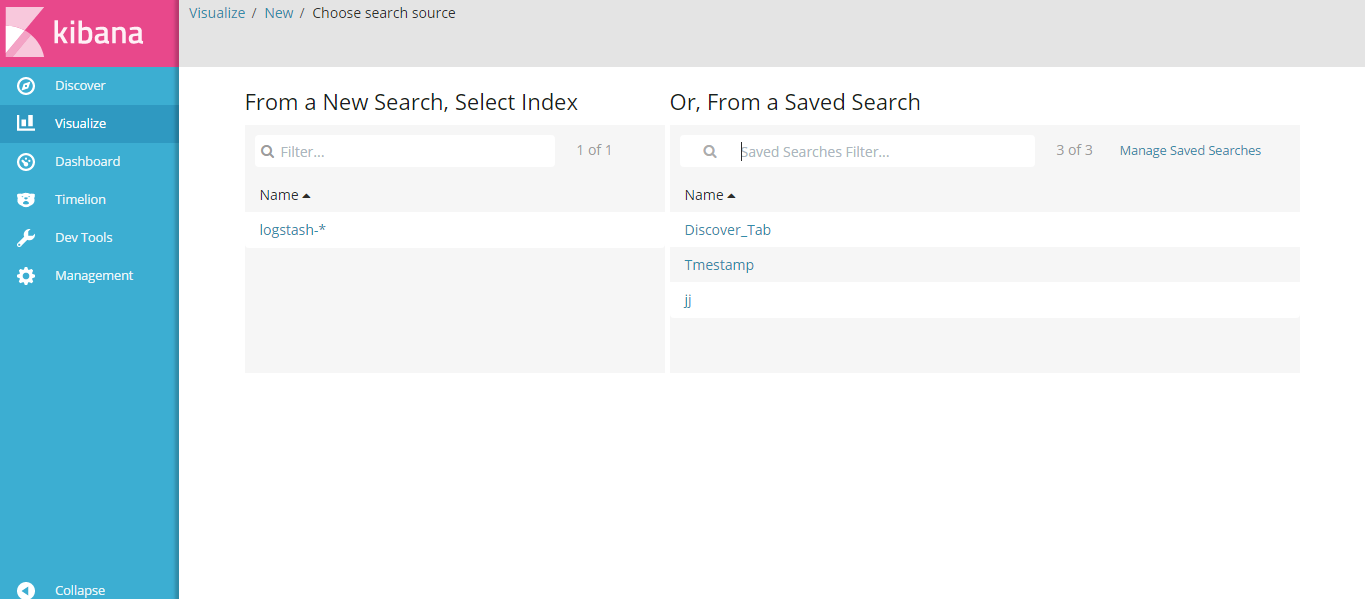


Click on ‘Create New visualization’

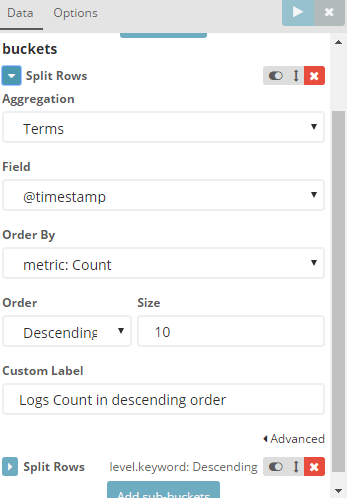


**Data Table:**

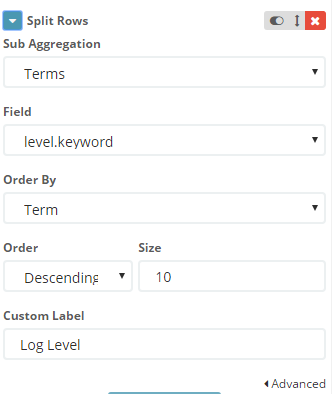
1. Click on Data Table.
2. Select from a New Search and Select logstash-\*



1. Expand ‘Split Rows’ and enter the value as per screenshot.



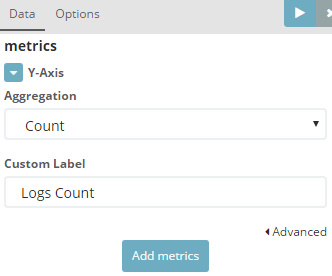
1. Next Click on ‘Add Sub Buckets and add values as per below screenshot.



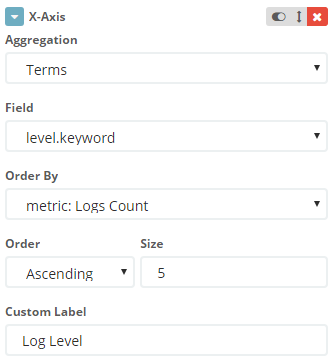
1. Click on Apply Changes
2. Now Save the search with particular name through save button in top bar menu.

**Line Chart**

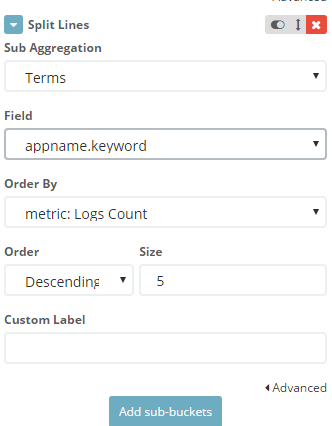
1. Click on Line Chart.
2. Select from a New Search and Select logstash-\*
3. In Y-axis parameters, change the values as per below screenshot.



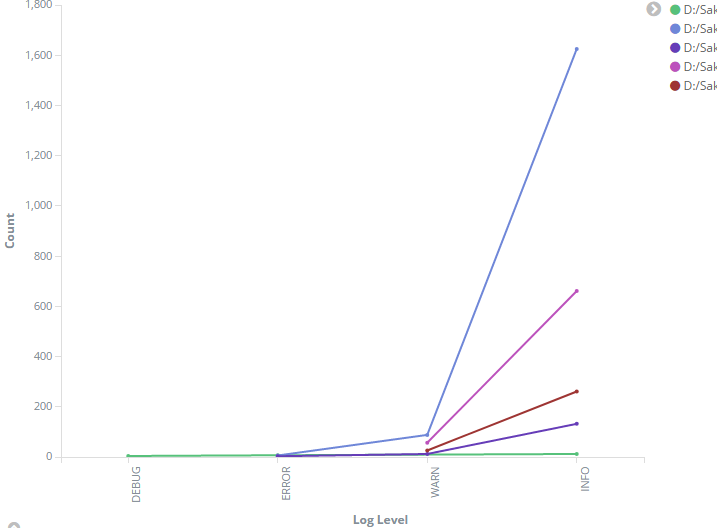
1. In X- axis parameter, add the values as per below screenshot.



1. In Split Lines, add the values as per below screenshot.



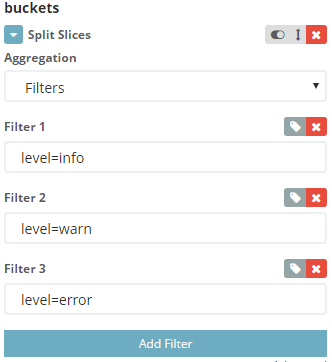
1. Click on Apply Changes, somewhere near to below image would be created.
2. Now Save the search with particular name through save button in top bar menu.



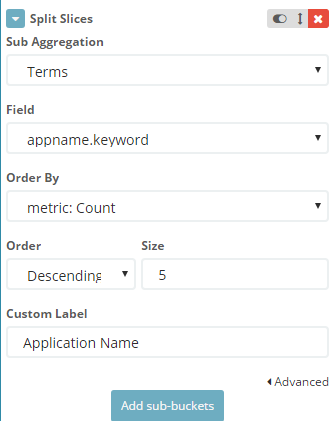
1. Save the Line chart through save button in top bar.

**Pie Chart:**

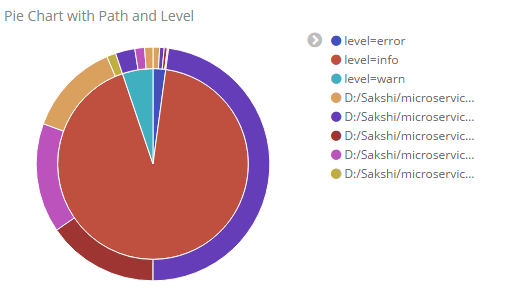
1. Click on Pie Chart.
2. Select from a New Search and Select logstash-\*
3. In Split Slices, change the values as per below screenshot.



1. Click on ‘Add Sub –buckets’ and enter below values.



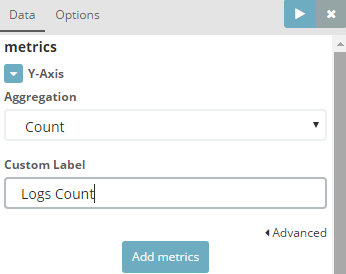
1. Somewhere below pie chart would be seen there, this would be as per your logs.



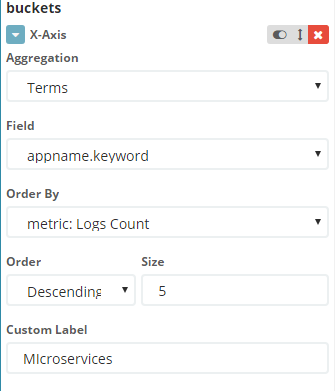
1. Now Save the search with particular name through save button in top bar menu.

**Vertical Graph:**

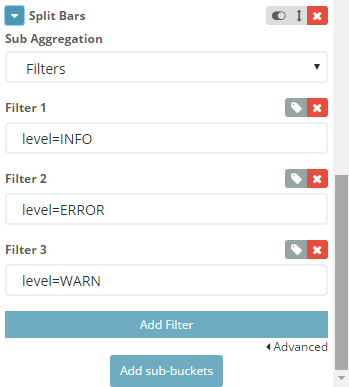
1. Click on Vertical Graph.
2. Select from a New Search and Select logstash-\*
3. In Y-Axis, change the values as per below screenshot.



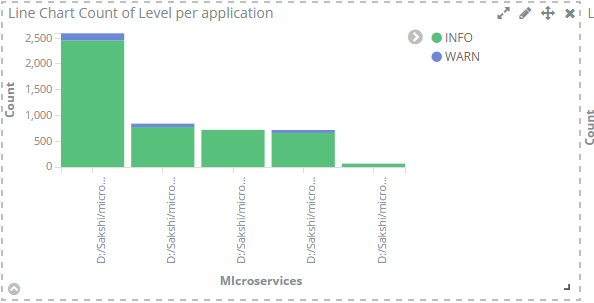
1. In X-Axis, change the values as per below screenshot.



1. Click on Split Bars and add the values as per below screenshot.

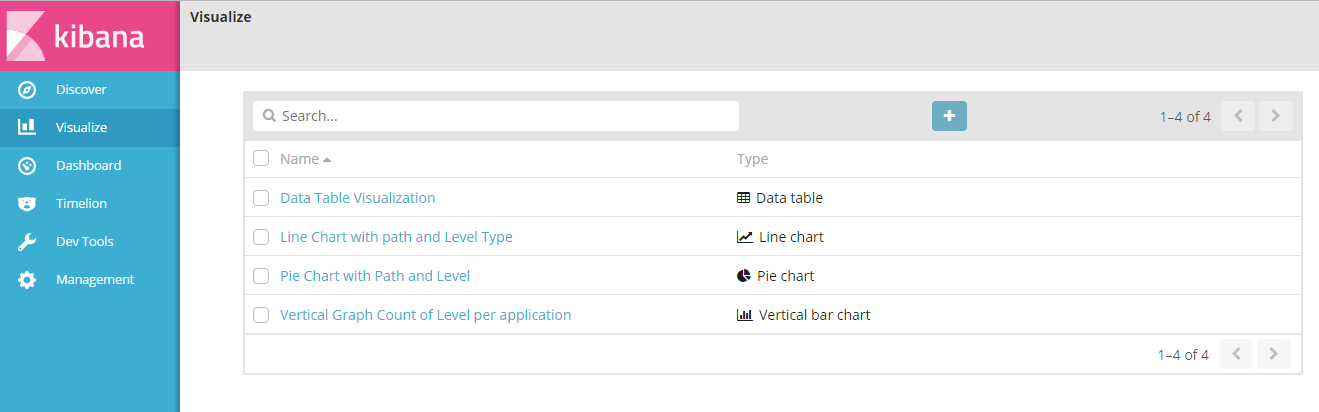


1. Somewhere below vertical graph would be seen there, this would be as per your logs.



1. Now Save the search with particular name through save button in top bar menu.

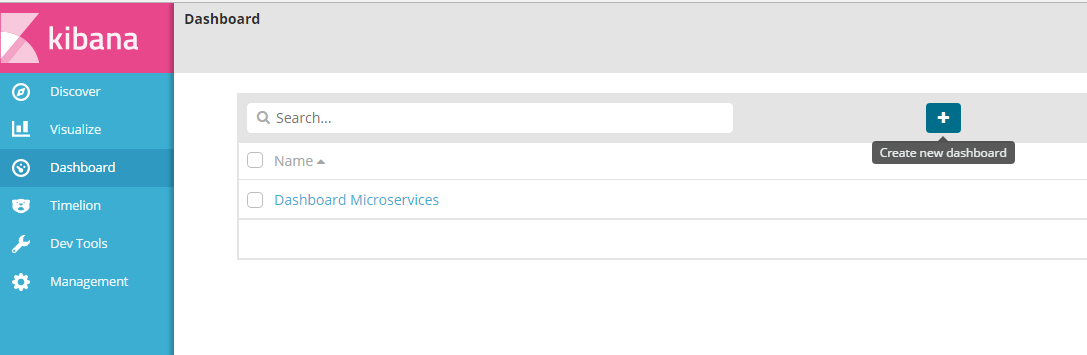
Now when you will click on Visualize tab, below screen would appear with you saved search name result.



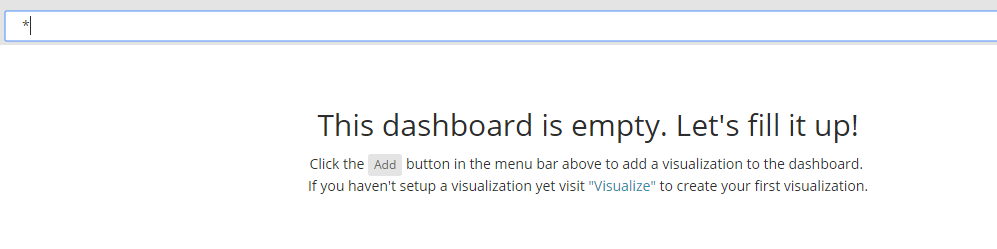
**DashBoard:**

Below is the sample dashboard created for multiple applications that can be customized more as per requirement.

1. Click on ‘Create Dashboard’ button.



1. Click on the ‘Add’ button on below screen



1. Add 4 saved visualize items and 1 discover tab.
2. Adjust them as per below screenshot on the dashboard.

