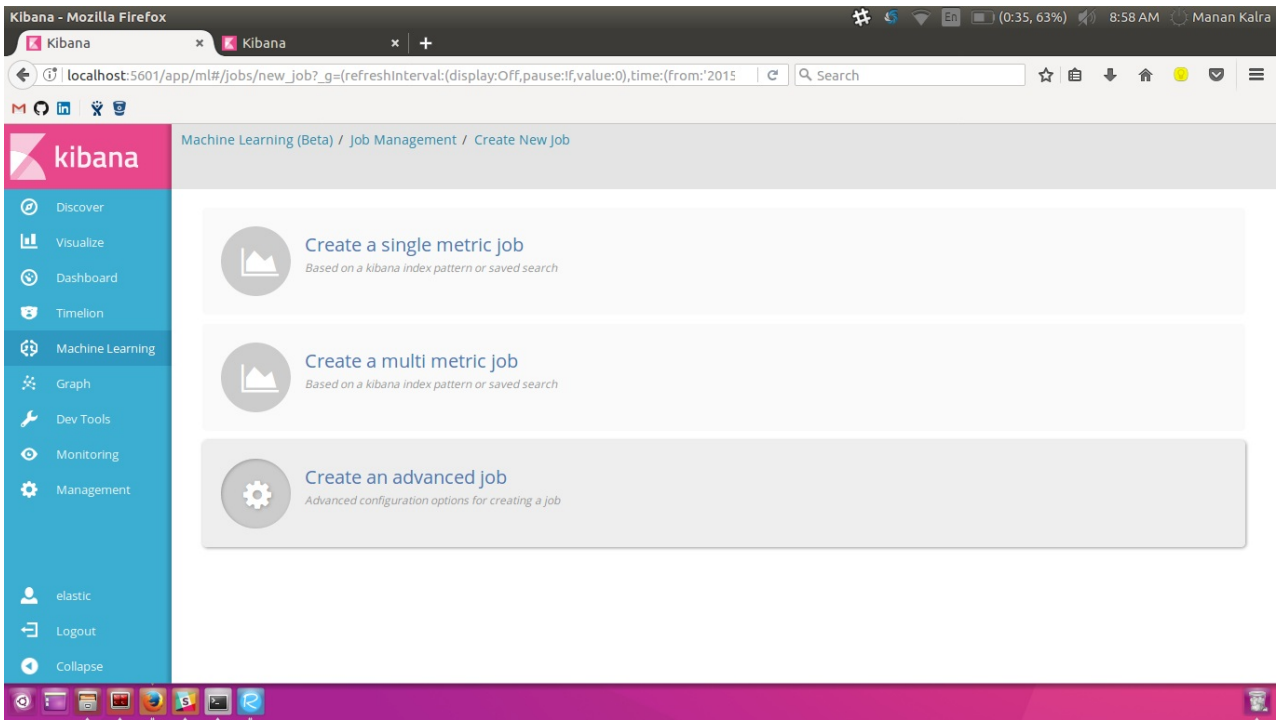
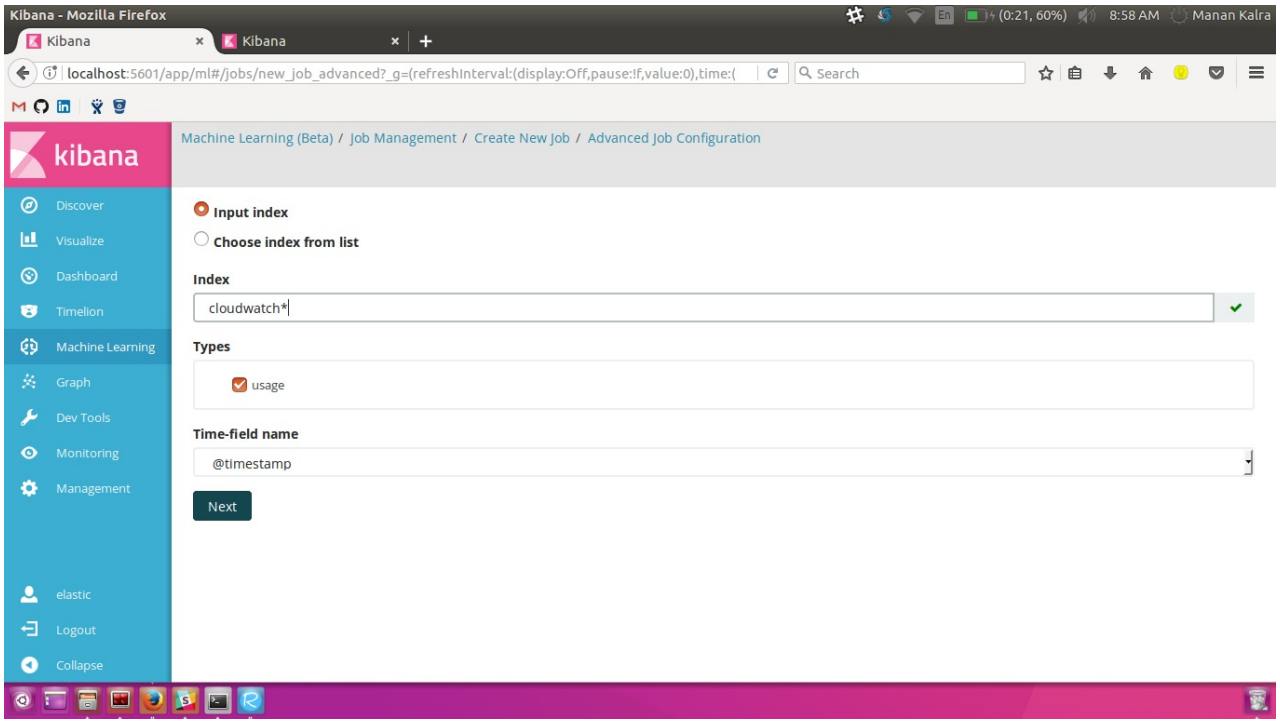
X-Pack: Machine Learning

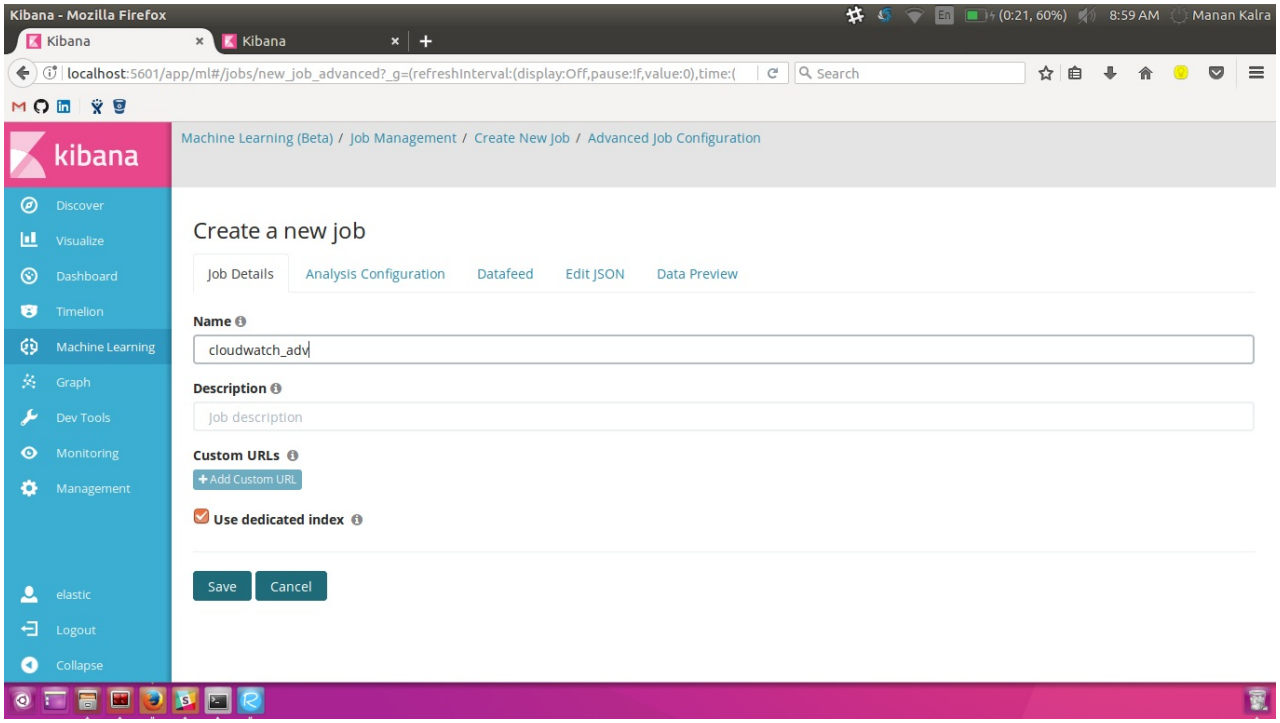
Advanved Job
Cloudwatch

- Start the Elasticsearch cluster. Start Kibana.
- Create an index via Logstash:
  - Redirect to the directory where Logstash is installed.
  - Copy the provided CSV and configuration file to this location.
  - Make changes in the configuration files, if required.
  - Execute `cat cloudwatch.csv | ./bin/logstash/cloudwatch.conf`.
- Verify your created indices by redirecting to: `localhost:9200/_cat/indices?v`.
- You will see multiple indices named *cloudwatch-YYYY.MM.DD*.
- Create an index pattern in the Managemet tab of the Kibana console to view the loaded data. If you want to load all the indices at once, while creating the index pattern, use a wild-card such as *cloudwatch**.
- Click on the *Machine Learning* tab and then on *Create a new job*. We'll select an *Advanced Job* here as we need to analyze data from multiple indices. Choose the *cloudwatch** as the input index.

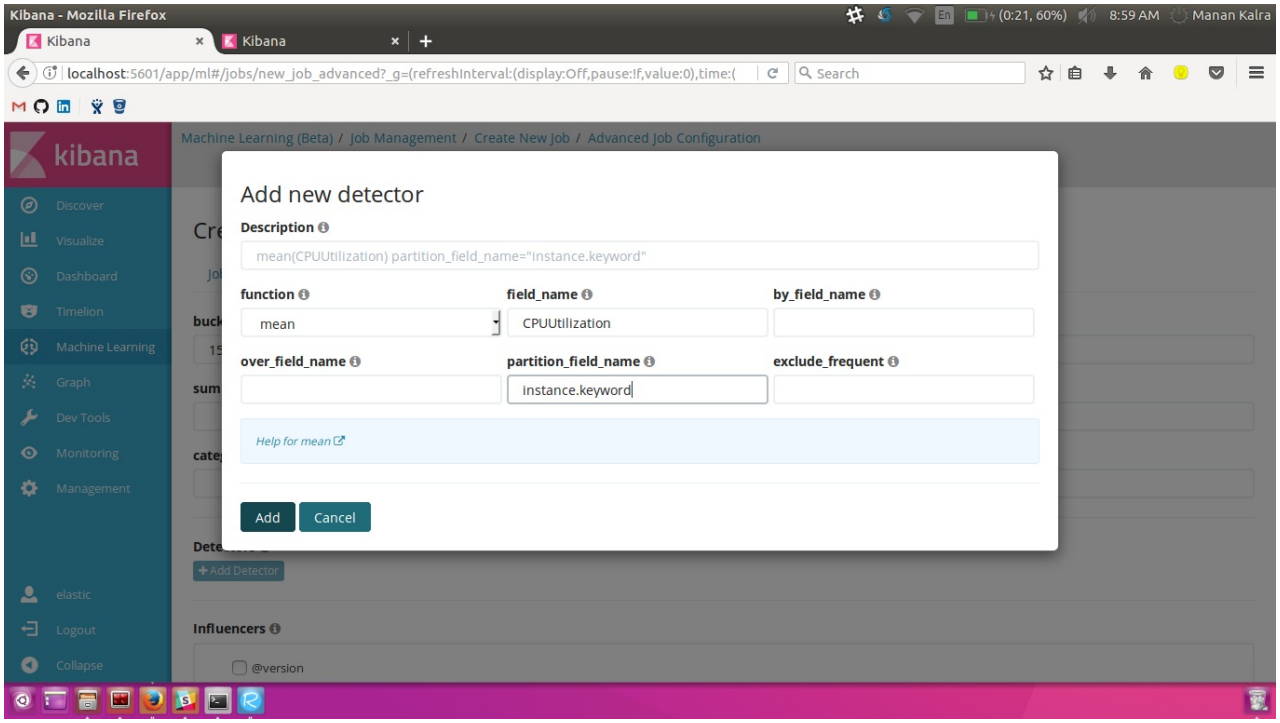


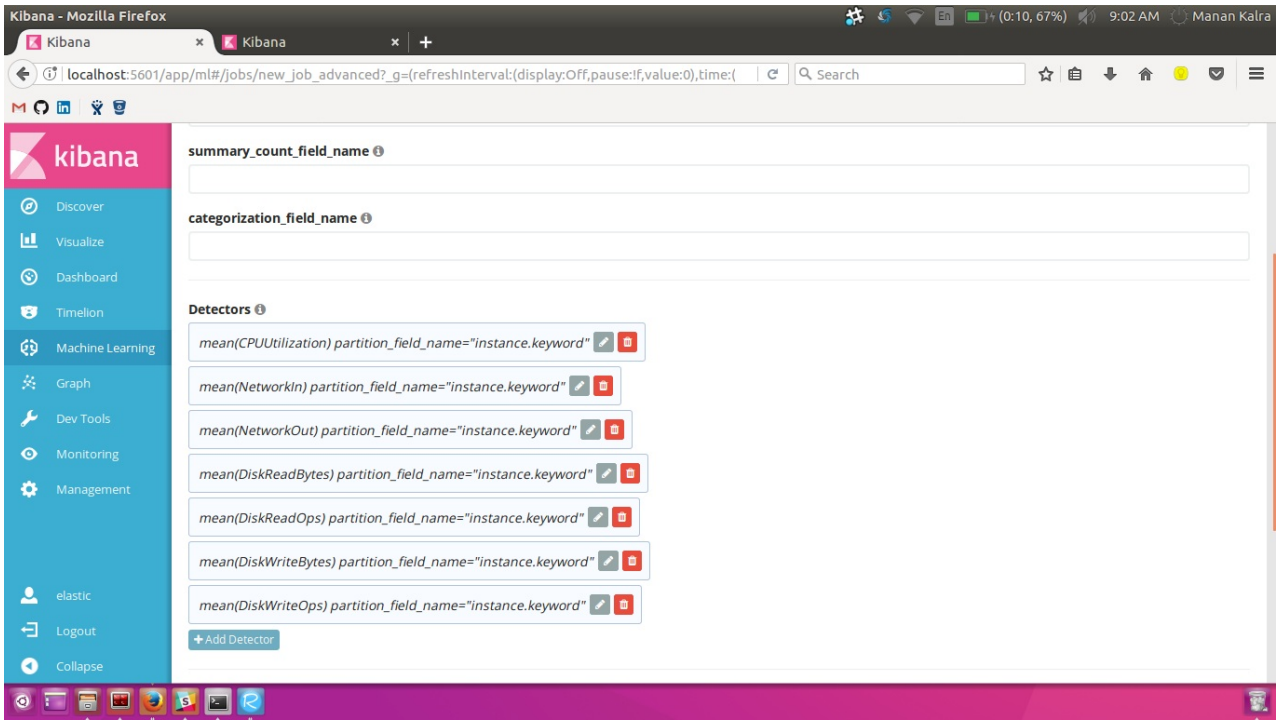


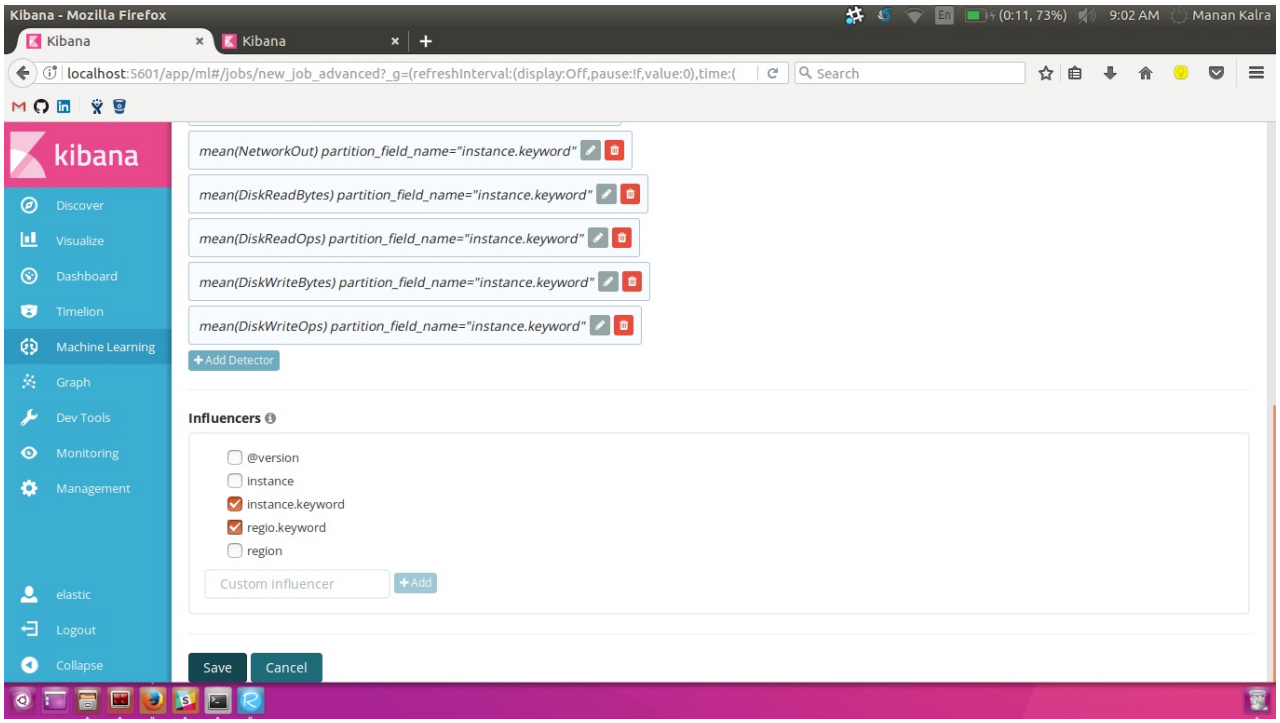
- Now you need to edit *Job Details* and *Analysis Configuration*. Using a dedicated index is a better choice while creating an advanced job.



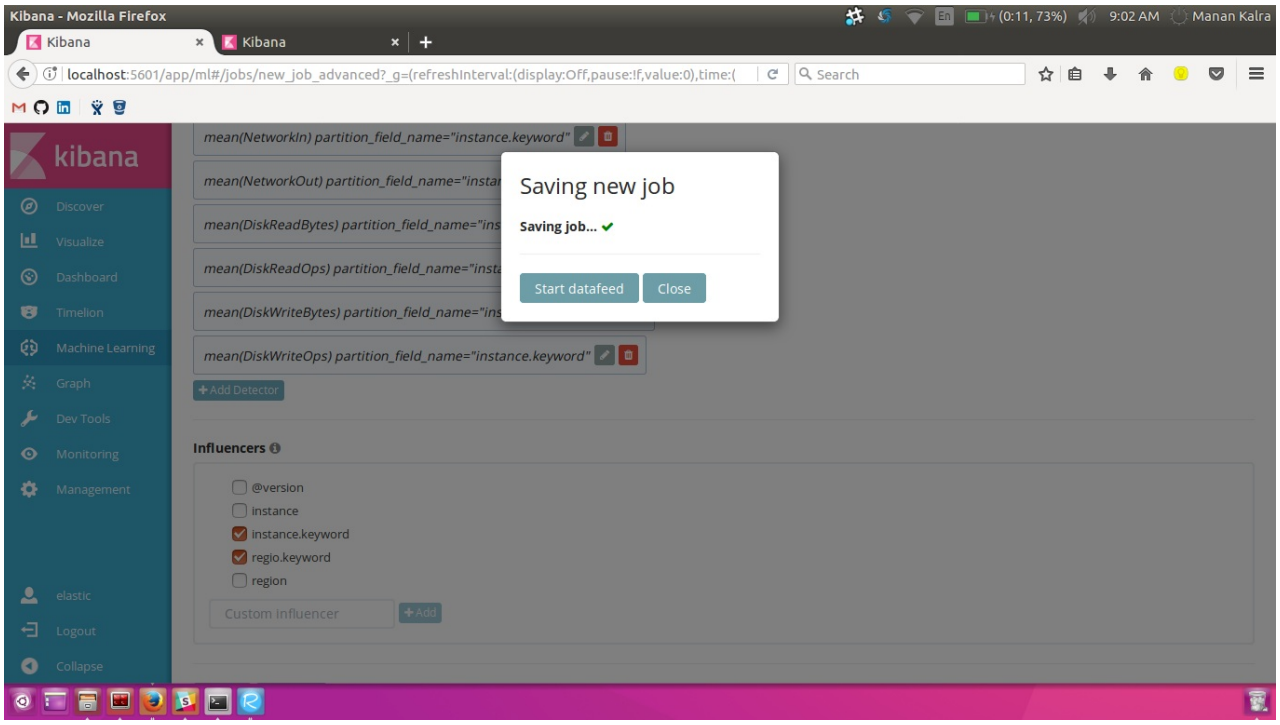
- In the *Analysis Configuration* section, you can set multiple detectors and influencers.

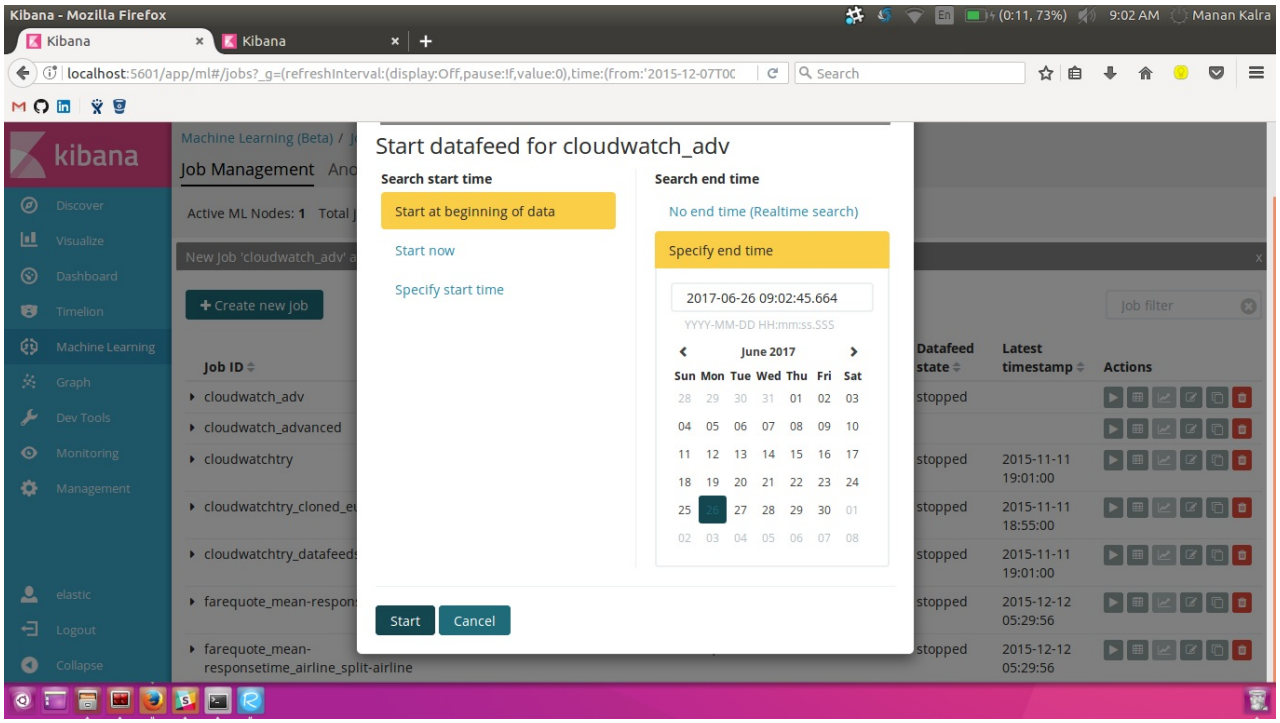




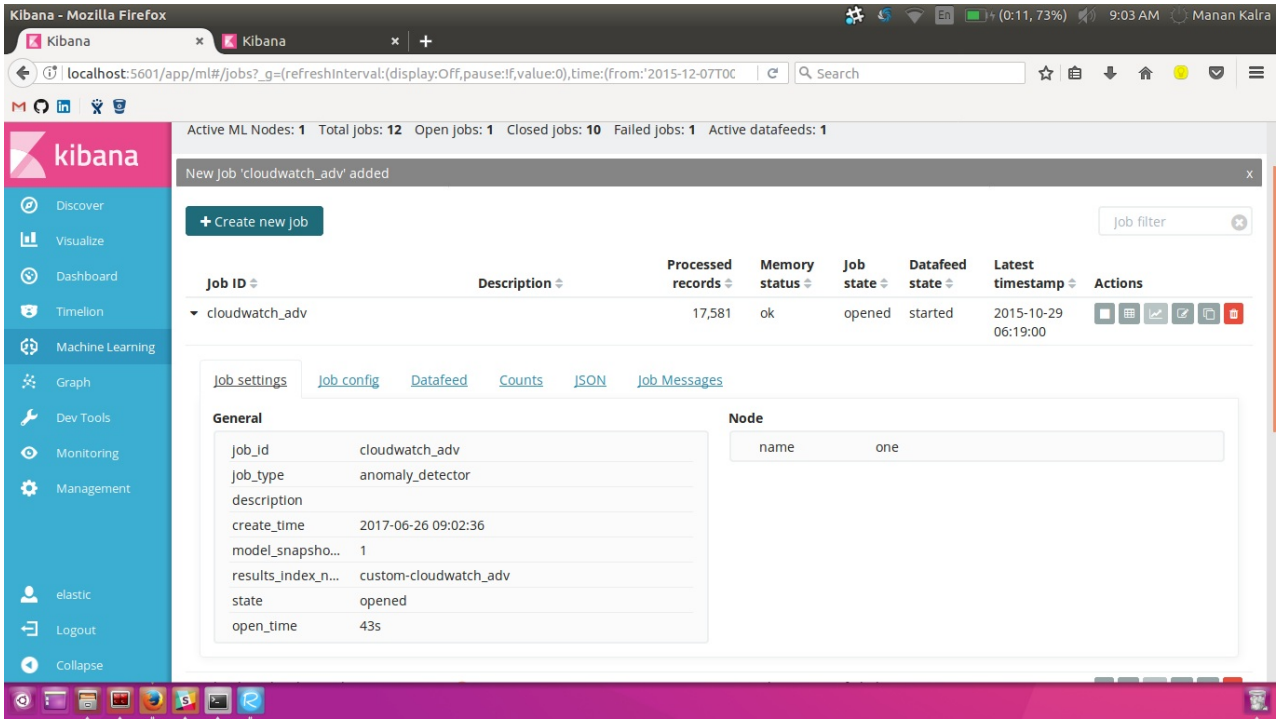


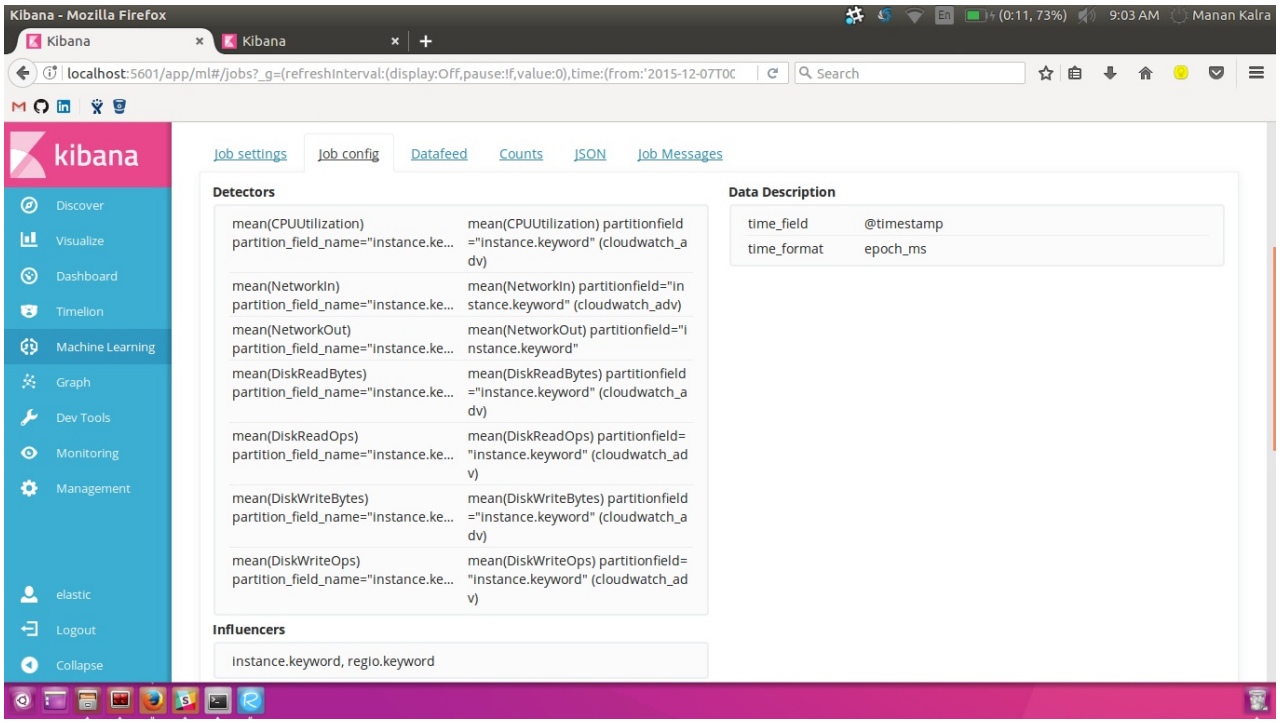
- Save the job and start datafeed from the beginning of data.



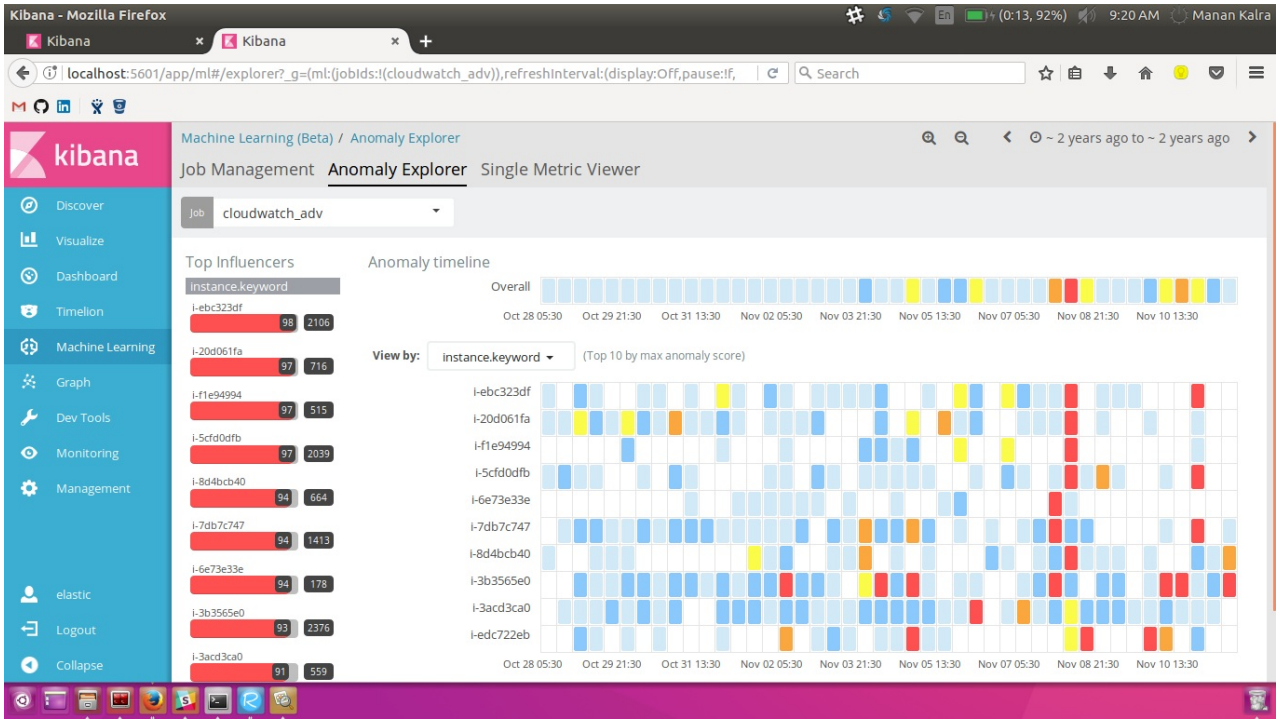


- Now all the records will be processed. Job configuration and datafeed details can also be viewed under the Job Management tab.





- After the job state is closed and datafeed is stopped, click on the Anomaly Explorer icon to view results. ou can view the timeline by different influencers too.



- Drilling down to a particular timeline index is also possible.