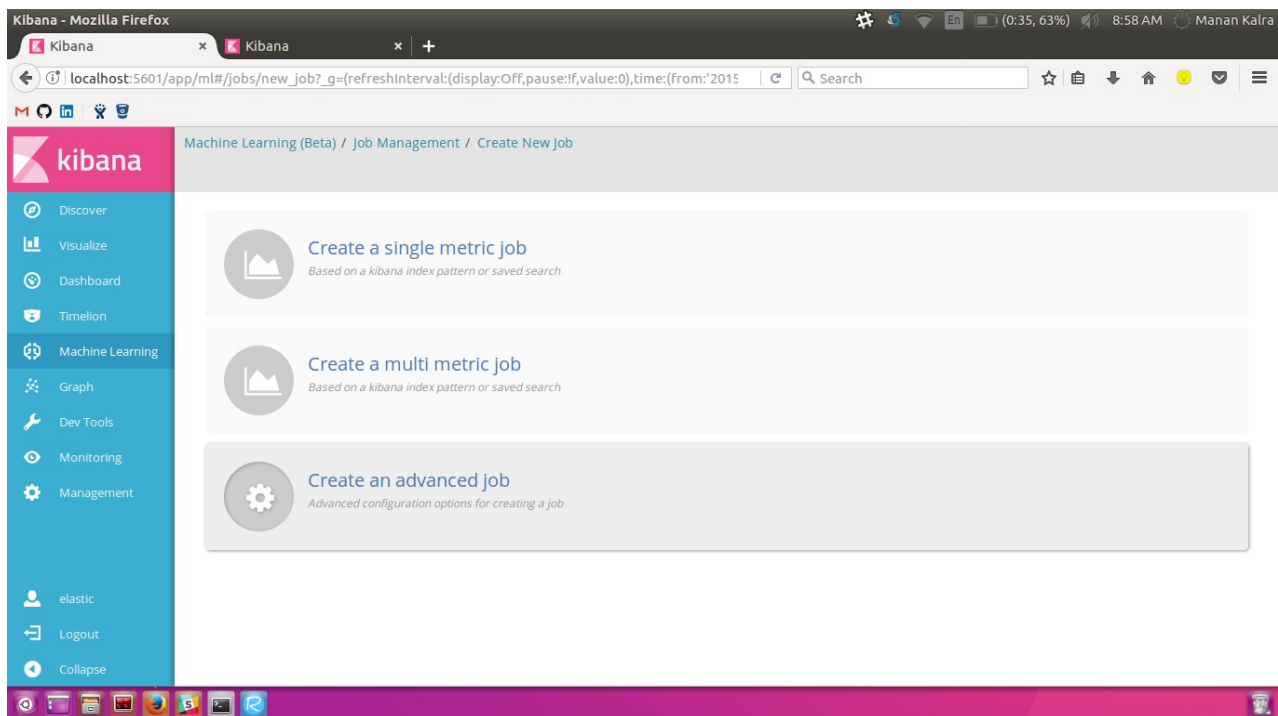


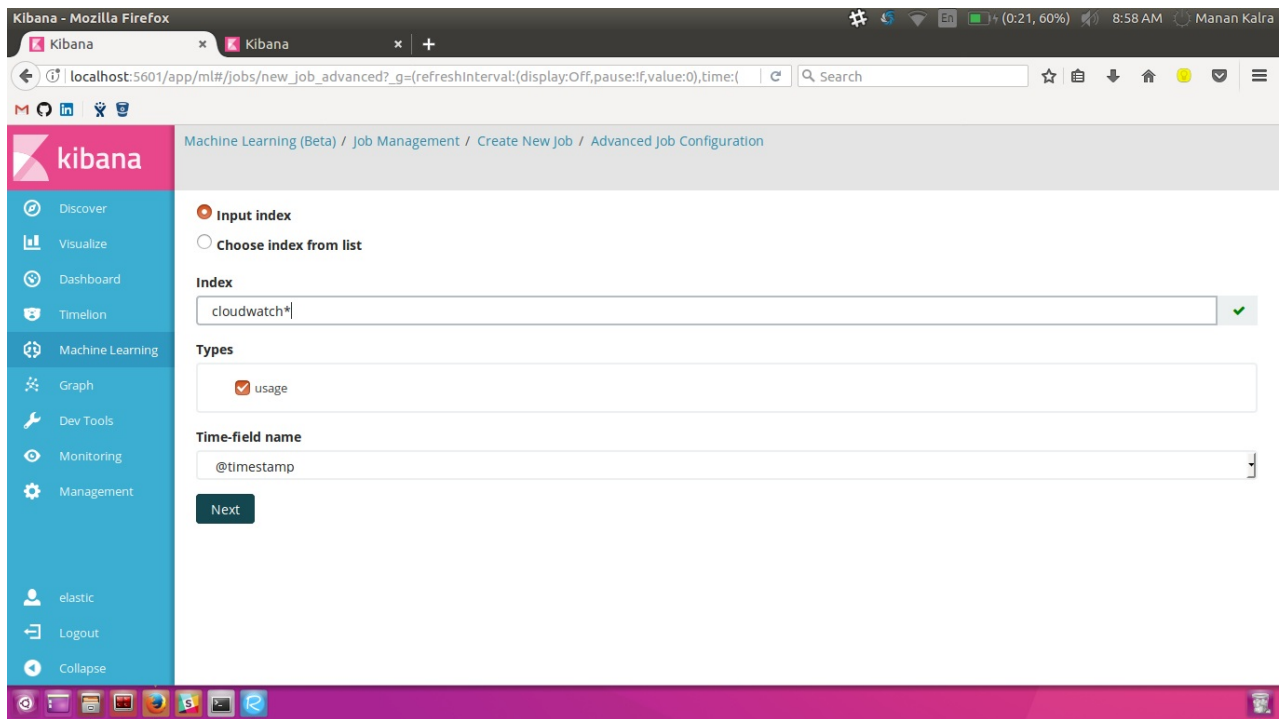


X-Pack: Machine Learning

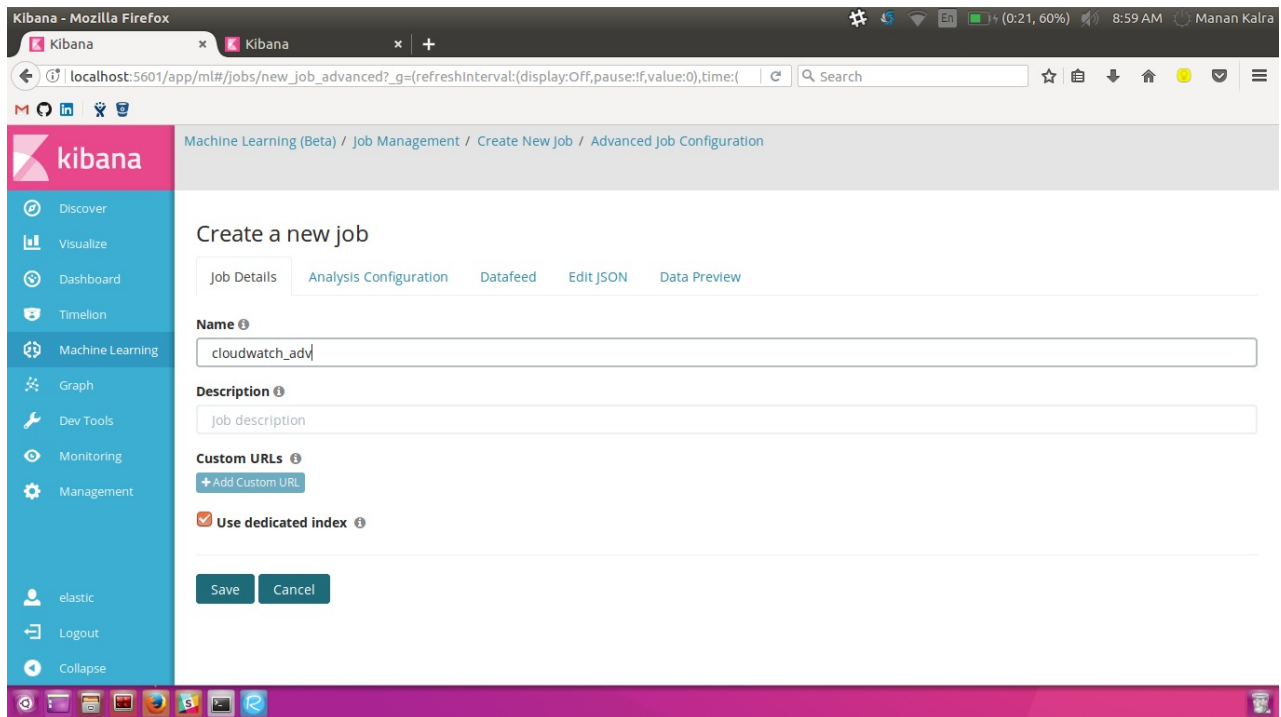
Advanced Job Cloudwatch

- 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 Management 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.

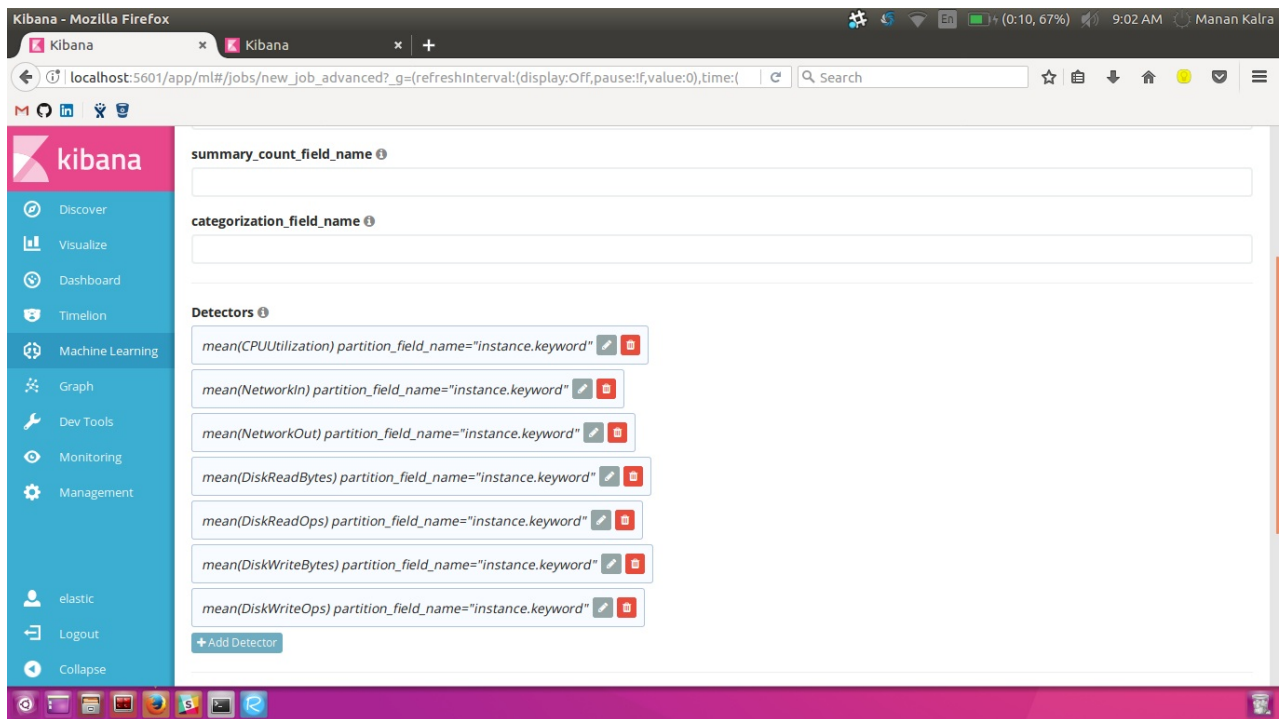
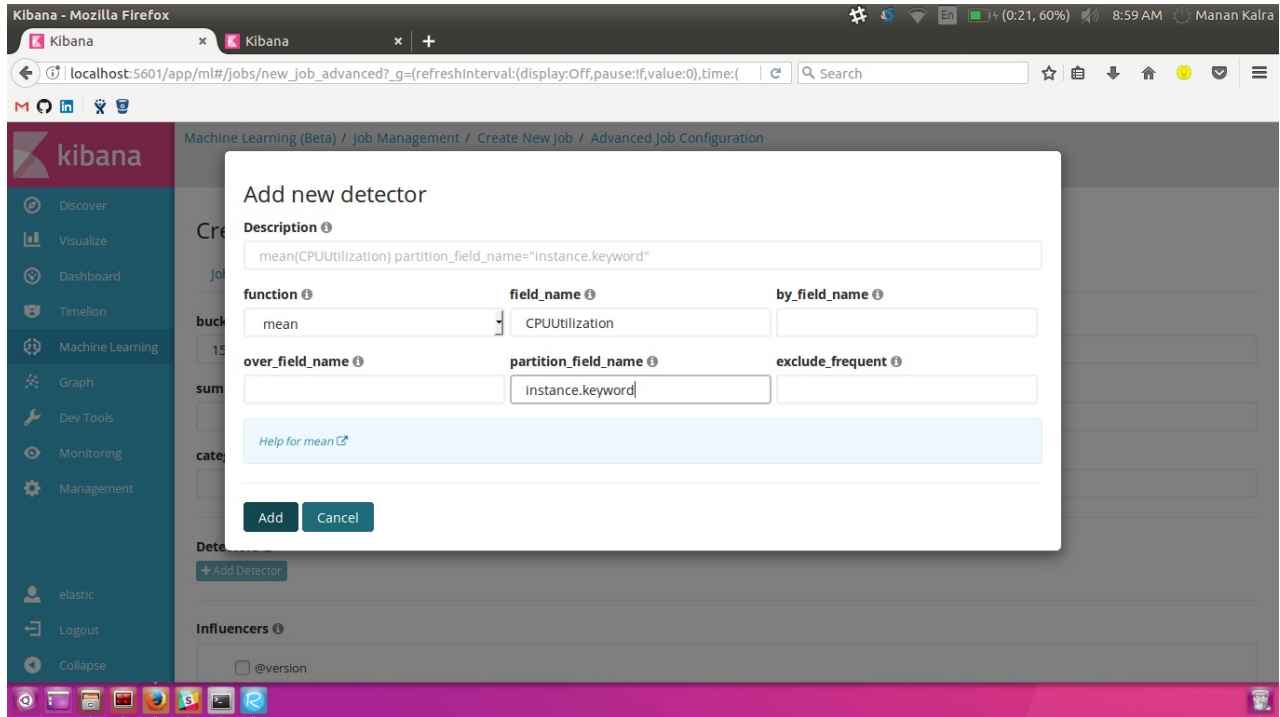


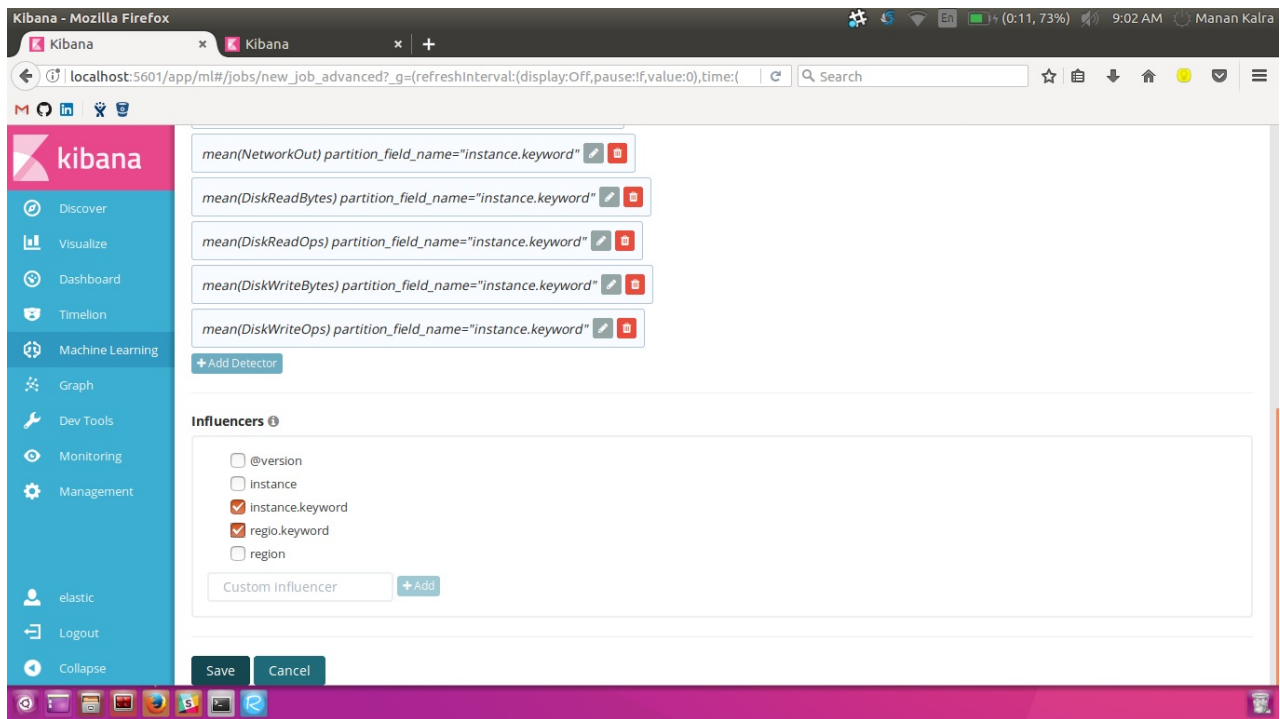


- Now you need to edit *Job Details* and *Analysis Configuration*. Using a dedicated index is a better choice while creating an advanced job.

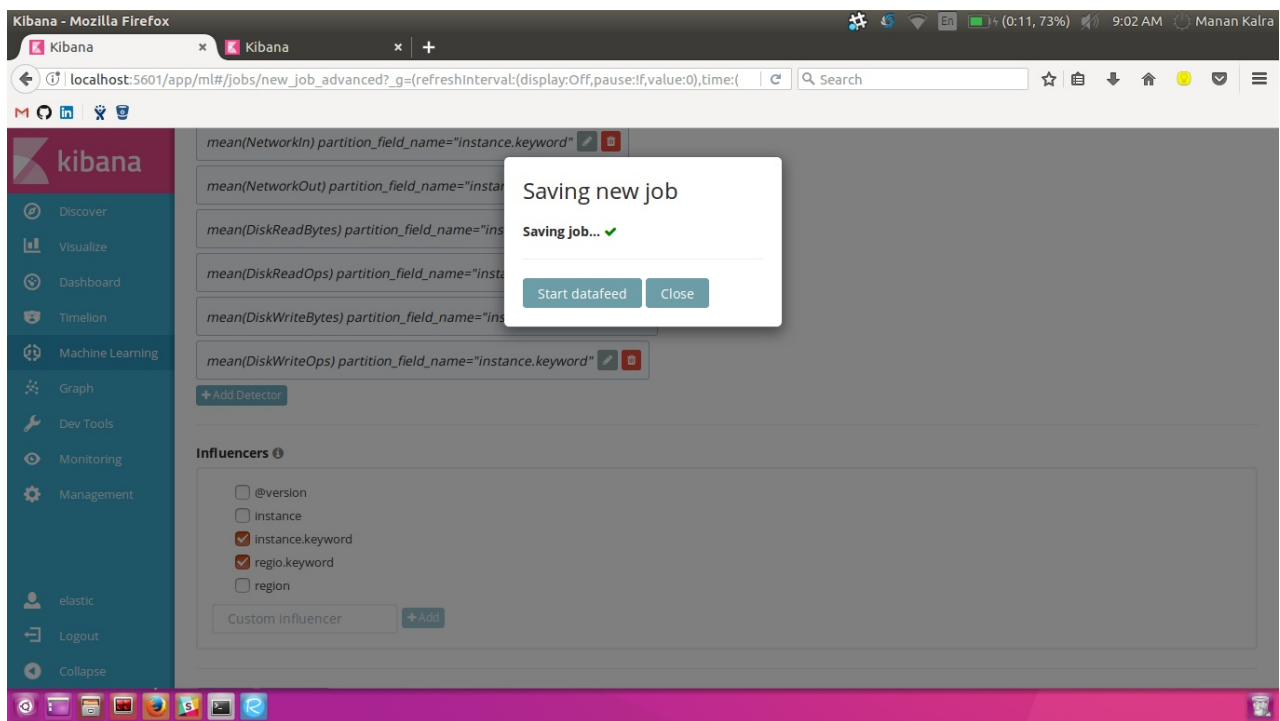


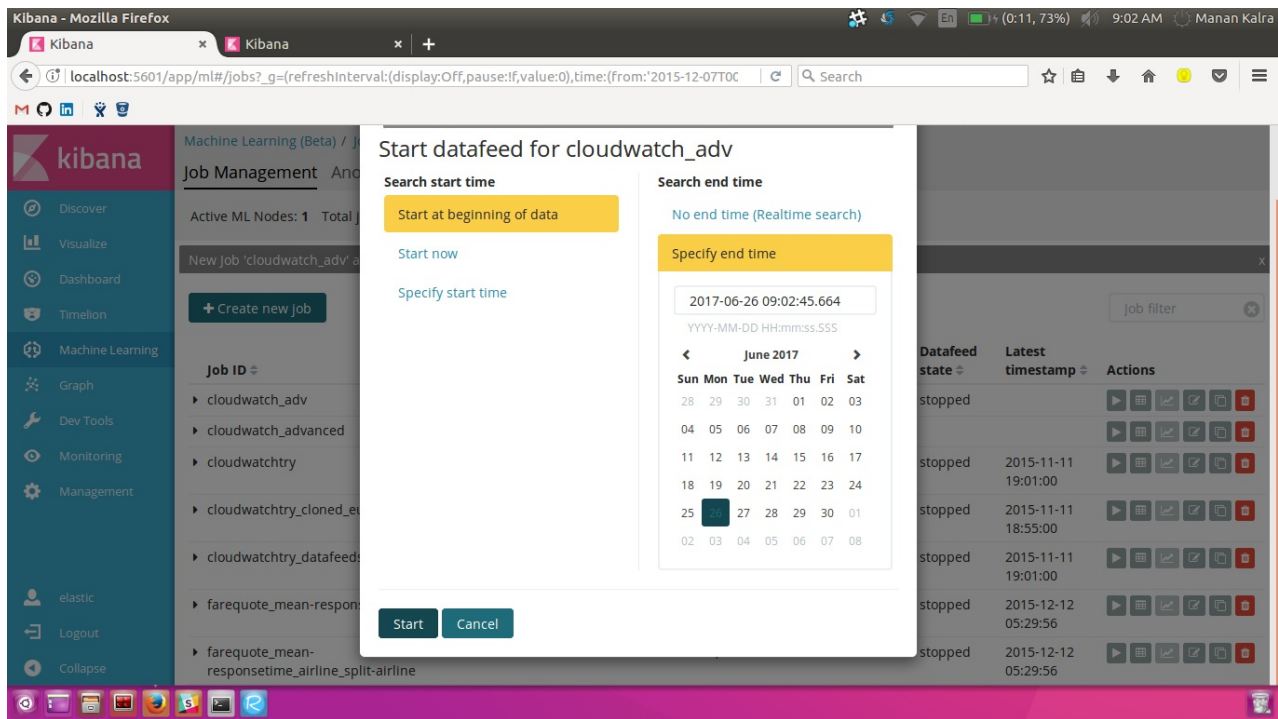
- In the *Analysis Configuration* section, you can set multiple detectors and influencers.



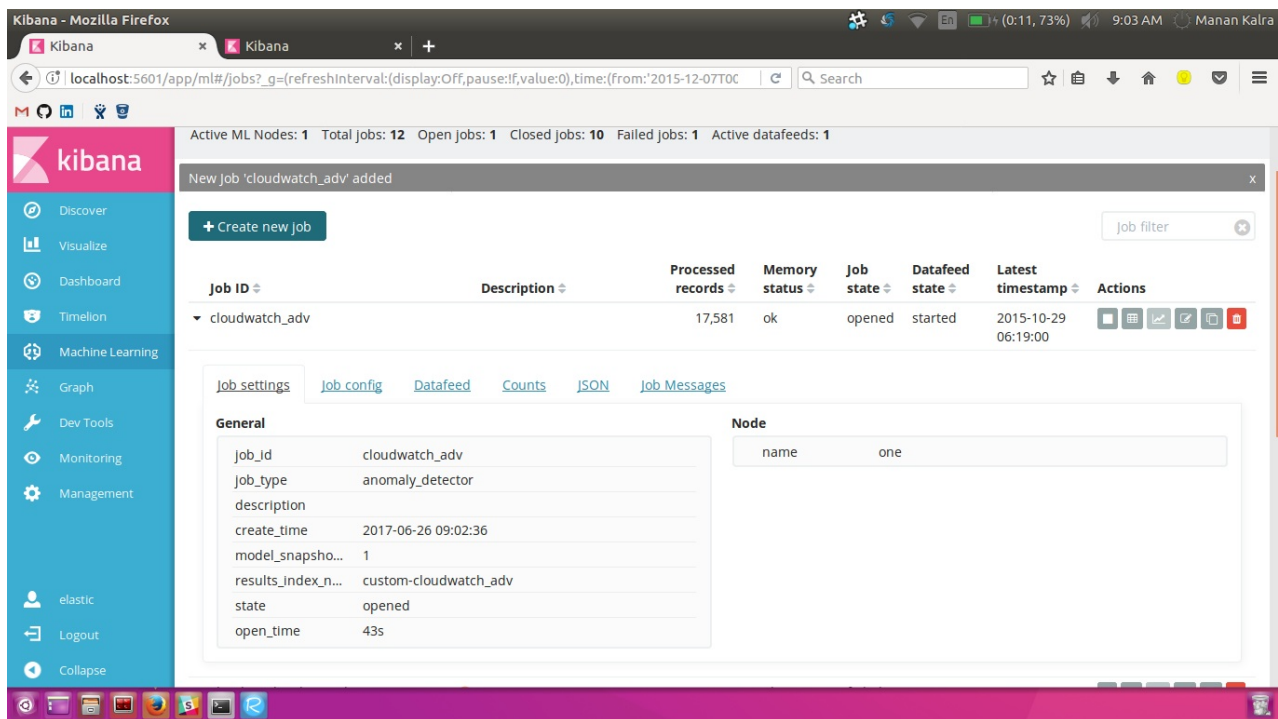


- Save the job and start datafeed from the beginning of data.





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



Kibana - Mozilla Firefox

Kibana

localhost:5601/app/ml#/jobs?_g=(refreshInterval:(display:Off,pause:If,value:0),time:(from:'2015-12-07T00

Search

Discover
Visualize
Dashboard
Timelion
Machine Learning
Graph
Dev Tools
Monitoring
Management

elastic
Logout
Collapse

Job settings Job config Datafeed Counts JSON Job Messages

Detectors

mean(CPUUtilization) partition_field_name="Instance.ke...	mean(CPUUtilization) partitionfield="Instance.keyword" (cloudwatch_adv)
mean(NetworkIn) partition_field_name="Instance.ke...	mean(NetworkIn) partitionfield="Instance.keyword" (cloudwatch_adv)
mean(NetworkOut) partition_field_name="Instance.ke...	mean(NetworkOut) partitionfield="Instance.keyword" (cloudwatch_adv)
mean(DiskReadBytes) partition_field_name="Instance.ke...	mean(DiskReadBytes) partitionfield="Instance.keyword" (cloudwatch_adv)
mean(DiskReadOps) partition_field_name="Instance.ke...	mean(DiskReadOps) partitionfield="Instance.keyword" (cloudwatch_adv)
mean(DiskWriteBytes) partition_field_name="Instance.ke...	mean(DiskWriteBytes) partitionfield="Instance.keyword" (cloudwatch_adv)
mean(DiskWriteOps) partition_field_name="Instance.ke...	mean(DiskWriteOps) partitionfield="Instance.keyword" (cloudwatch_adv)

Influencers

Instance.keyword, regio.keyword

Data Description

time_field	@timestamp
time_format	epoch_ms

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

Kibana - Mozilla Firefox

Kibana

localhost:5601/app/ml/#/explorer?_g=(ml:(jobs:(cloudwatch_adv)),refreshInterval:(display:Off,pause:If,

Search

Discover
Visualize
Dashboard
Timelion
Machine Learning
Graph
Dev Tools
Monitoring
Management

elastic
Logout
Collapse

Machine Learning (Beta) / Anomaly Explorer

Job Management Anomaly Explorer Single Metric Viewer

Job: cloudwatch_adv

Top Influencers

Instance Keyword	Score	Count
i-ebc323df	98	2106
i-20d061fa	97	716
i-f1e94994	97	515
i-5cfd0dfb	97	2039
i-8d4bcb40	94	664
i-7db7c747	94	1413
i-6e73e33e	94	178
i-3b3565e0	93	2376
i-3acd3ca0	91	559

Anomaly timeline

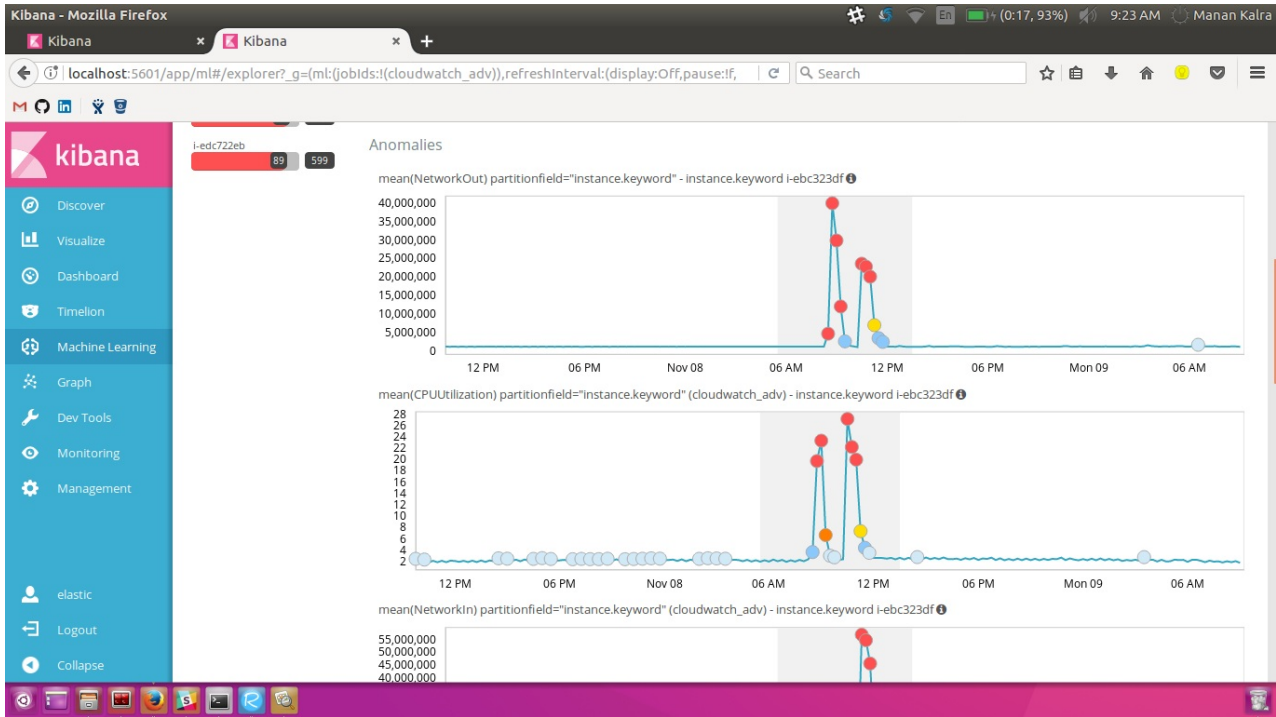
Overall

View by: Instance.keyword (Top 10 by max anomaly score)

Oct 28 05:30 Oct 29 21:30 Oct 31 13:30 Nov 02 05:30 Nov 03 21:30 Nov 05 13:30 Nov 07 05:30 Nov 08 21:30 Nov 10 13:30

i-ebc323df
i-20d061fa
i-f1e94994
i-5cfd0dfb
i-6e73e33e
i-7db7c747
i-8d4bcb40
i-3b3565e0
i-3acd3ca0
i-edc722eb

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



Kibana - Mozilla Firefox

Kibana

localhost:5601/app/ml/#/explorer?_g=(ml:(jobs:(cloudwatch_adv)),refreshInterval:(display:Off,pause:if,))

Search

kibana

Discover

Visualize

Dashboard

Timeline

Machine Learning

Graph

Dev Tools

Monitoring

Management

elastic

Logout

Collapse

Severity threshold: warning Interval: Auto

time	max severity	detector	found for	influenced by
November 8th 2015, 09:00	97	mean(NetworkOut) partitionfield="instance.keyword"	i-ebc323df	instance.keyword: i-ebc323d
November 8th 2015, 08:00	97	mean(NetworkOut) partitionfield="instance.keyword"	i-ebc323df	instance.keyword: i-ebc323d
November 8th 2015, 09:00	95	mean(CPUUtilization) partitionfield="instance.keyword" (cloudwatch_adv)	i-ebc323df	instance.keyword: i-ebc323d
November 8th 2015, 08:00	94	mean(CPUUtilization) partitionfield="instance.keyword" (cloudwatch_adv)	i-ebc323df	instance.keyword: i-ebc323d
November 8th 2015, 10:00	94	mean(CPUUtilization) partitionfield="instance.keyword" (cloudwatch_adv)	i-ebc323df	instance.keyword: i-ebc323d
November 8th 2015, 11:00	94	mean(CPUUtilization) partitionfield="instance.keyword" (cloudwatch_adv)	i-ebc323df	instance.keyword: i-ebc323d
November 8th 2015, 10:00	88	mean(NetworkOut) partitionfield="instance.keyword"	i-ebc323df	instance.keyword: i-ebc323d
November 8th 2015, 11:00	83	mean(NetworkOut) partitionfield="instance.keyword"	i-ebc323df	instance.keyword: i-ebc323d
November 8th 2015, 10:00	77	mean(NetworkIn) partitionfield="instance.keyword" (cloudwatch_adv)	i-ebc323df	instance.keyword: i-ebc323d
November 8th 2015, 11:00	76	mean(NetworkIn) partitionfield="instance.keyword" (cloudwatch_adv)	i-ebc323df	instance.keyword: i-ebc323d
November 8th 2015, 09:00	68	mean(NetworkIn) partitionfield="instance.keyword" (cloudwatch_adv)	i-ebc323df	instance.keyword: i-ebc323d
November 8th 2015, 08:00	50	mean(NetworkIn) partitionfield="instance.keyword" (cloudwatch_adv)	i-ebc323df	instance.keyword: i-ebc323d
November 8th 2015, 09:00	2	mean(DiskWriteBytes) partitionfield="instance.keyword" (cloudwatch_adv)	i-ebc323df	instance.keyword: i-ebc323d
November 8th 2015, 08:00	1	mean(DiskWriteBytes) partitionfield="instance.keyword" (cloudwatch_adv)	i-ebc323df	instance.keyword: i-ebc323d
November 8th 2015, 09:00	1	mean(DiskWriteOps) partitionfield="instance.keyword" (cloudwatch_adv)	i-ebc323df	instance.keyword: i-ebc323d
November 8th 2015, 08:00	< 1	mean(DiskWriteOps) partitionfield="instance.keyword" (cloudwatch_adv)	i-ebc323df	instance.keyword: i-ebc323d
November 8th 2015, 12:00	< 1	mean(DiskWriteOps) partitionfield="instance.keyword" (cloudwatch_adv)	i-ebc323df	instance.keyword: i-ebc323d
November 8th 2015, 12:00	< 1	mean(DiskWriteBytes) partitionfield="instance.keyword" (cloudwatch_adv)	i-ebc323df	instance.keyword: i-ebc323d