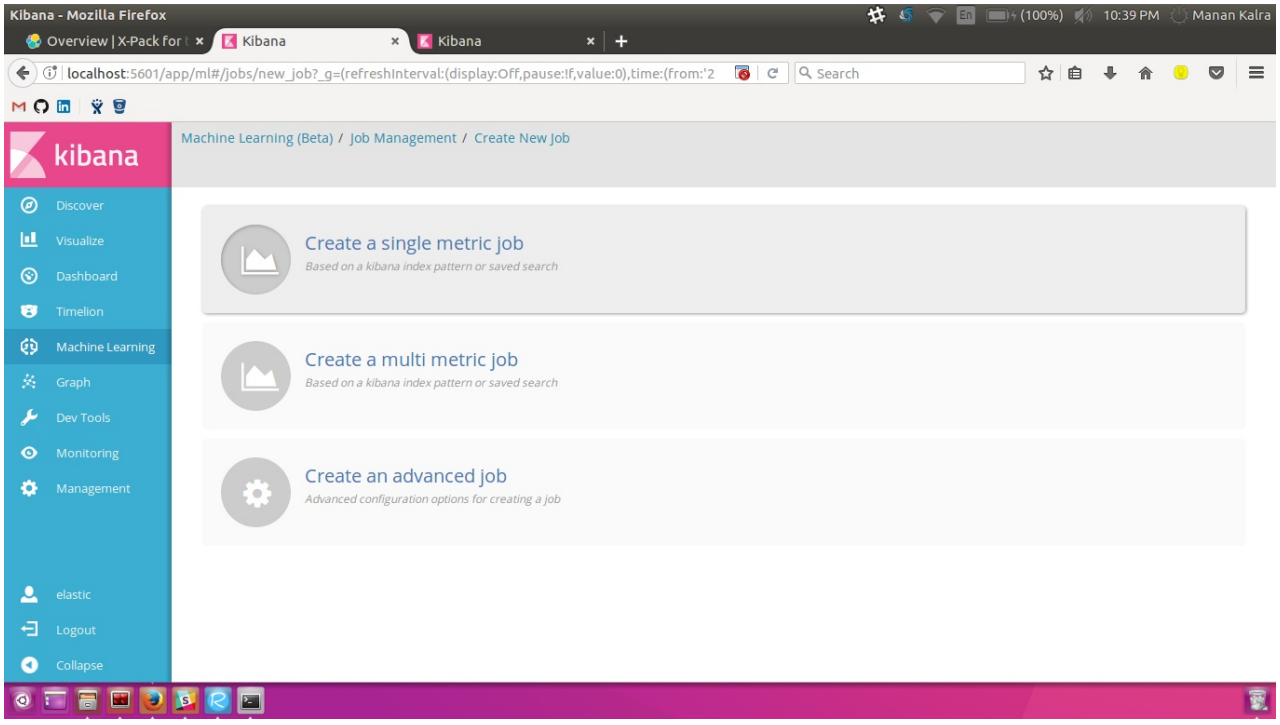
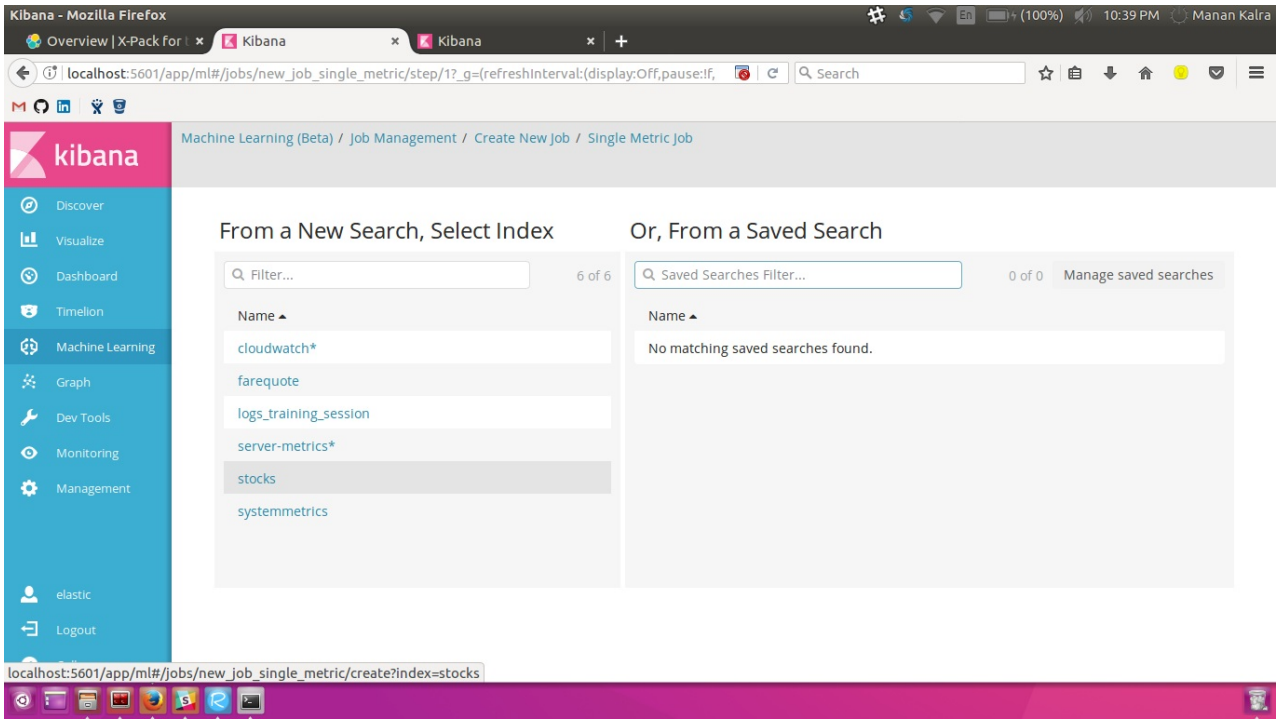
X-Pack: Machine Learning

Single Metric Job

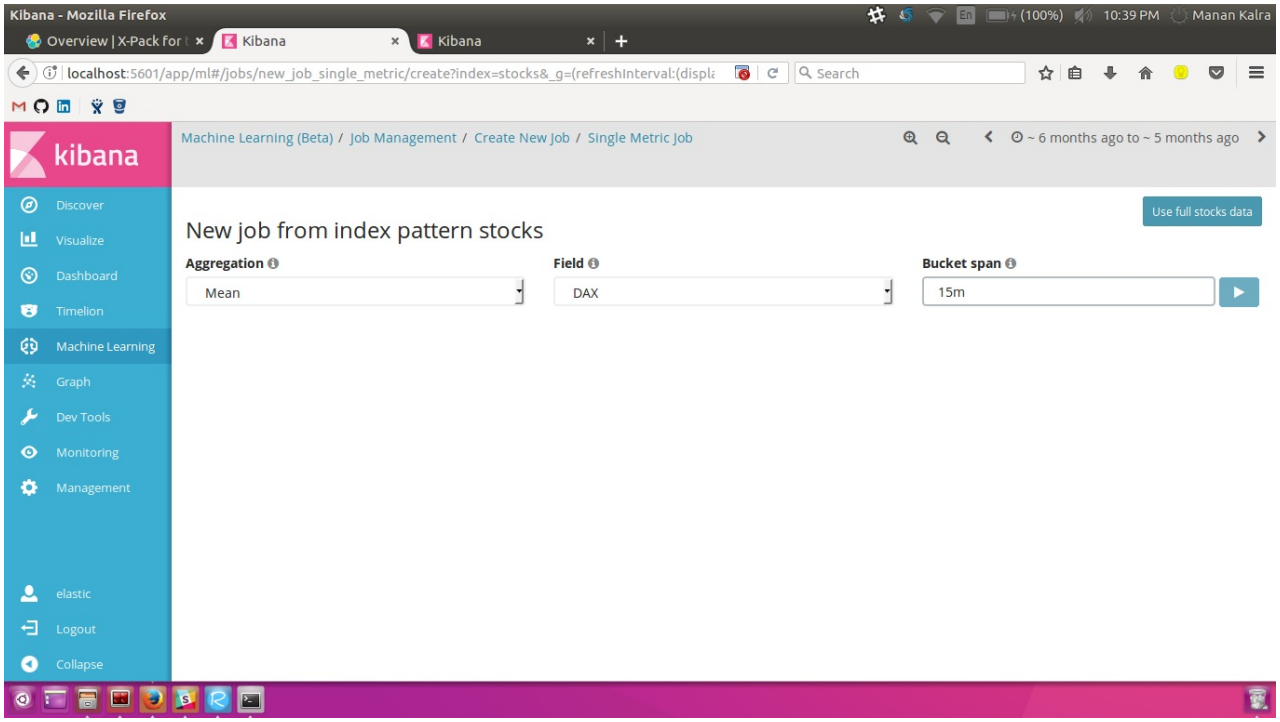
Stocks

- 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 stocks.csv | ./bin/logstash/stocks.conf`.
- Create an index pattern in the Managemet tab of the Kibana console to view the loaded data.
- Click on the *Machine Learning* tab and then on *Create a new job*.
- Select *Single Metric Job* and choose the *stocks* index.

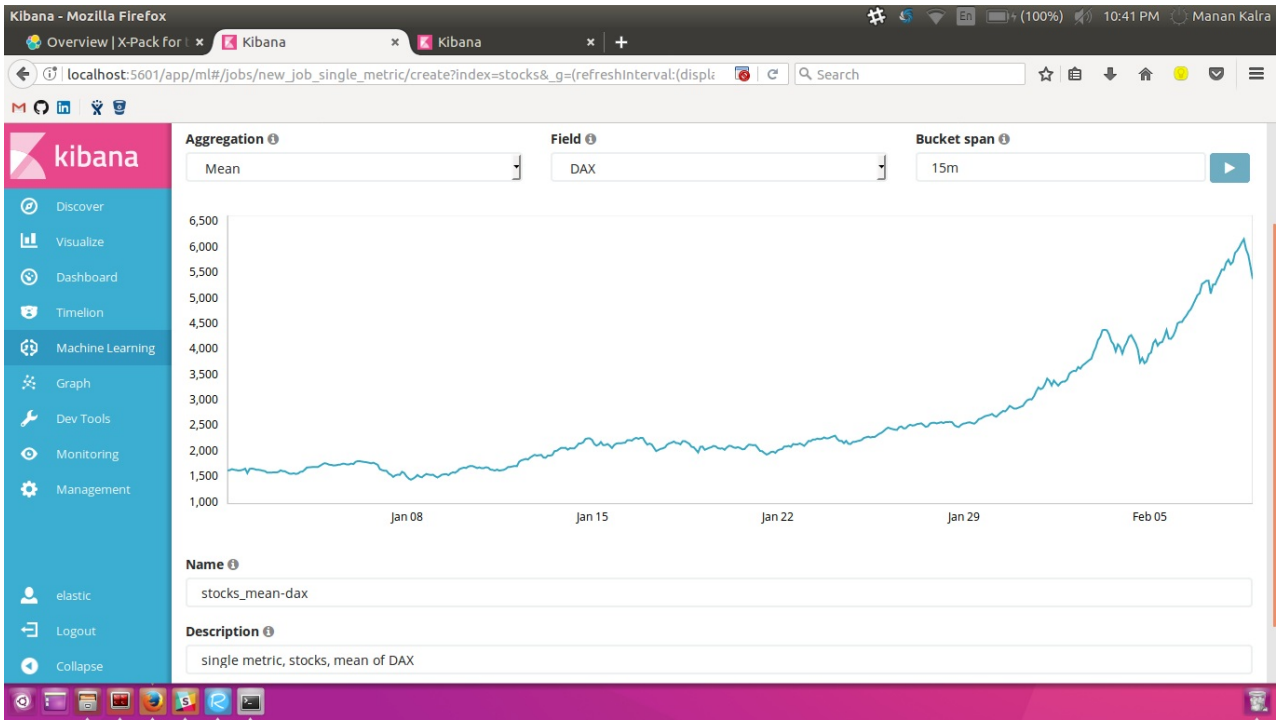




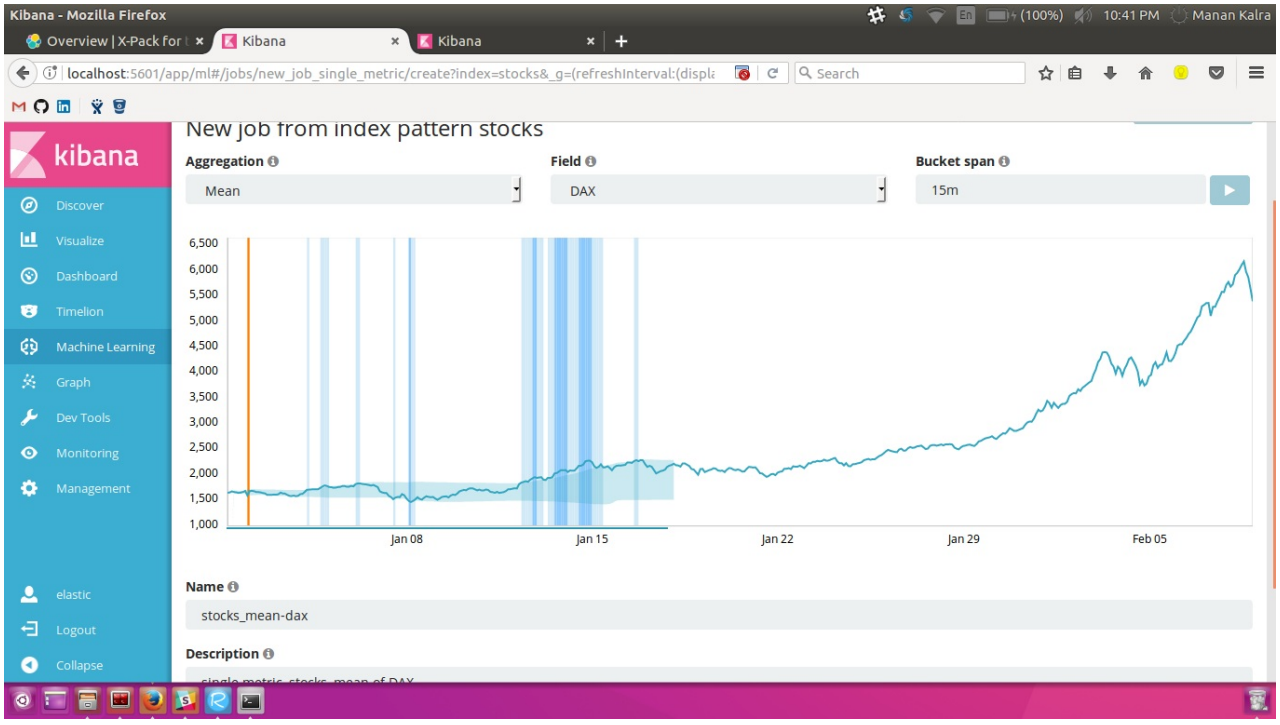
- Click on *Use full stocks data* as the data we are using is static.
- Select an Aggregation, for example: *Mean*.
- Select the field on which the aggregation or analysis function needs to be applied, for example: *DAX*.
- Use an appropiate bucket span, for example: 15m.

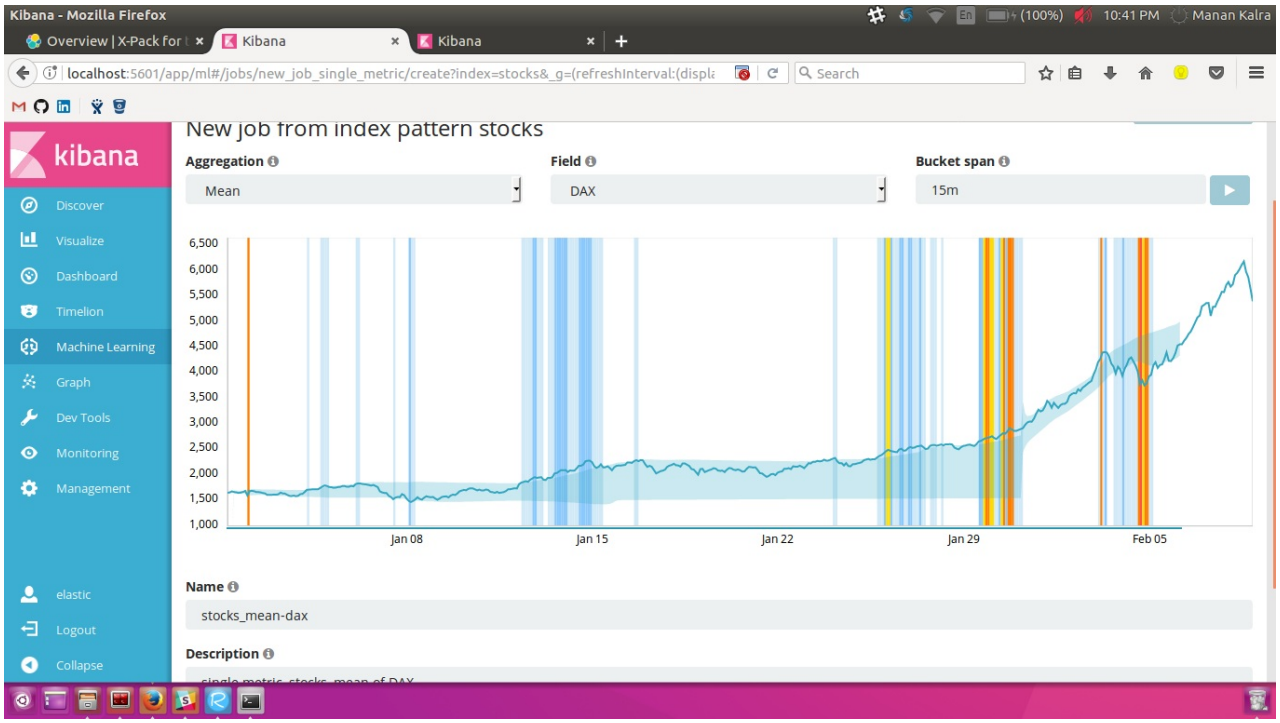


- Give your job a name. You can create a dedicated index for this job under the *Advanced* drop-down, if required.

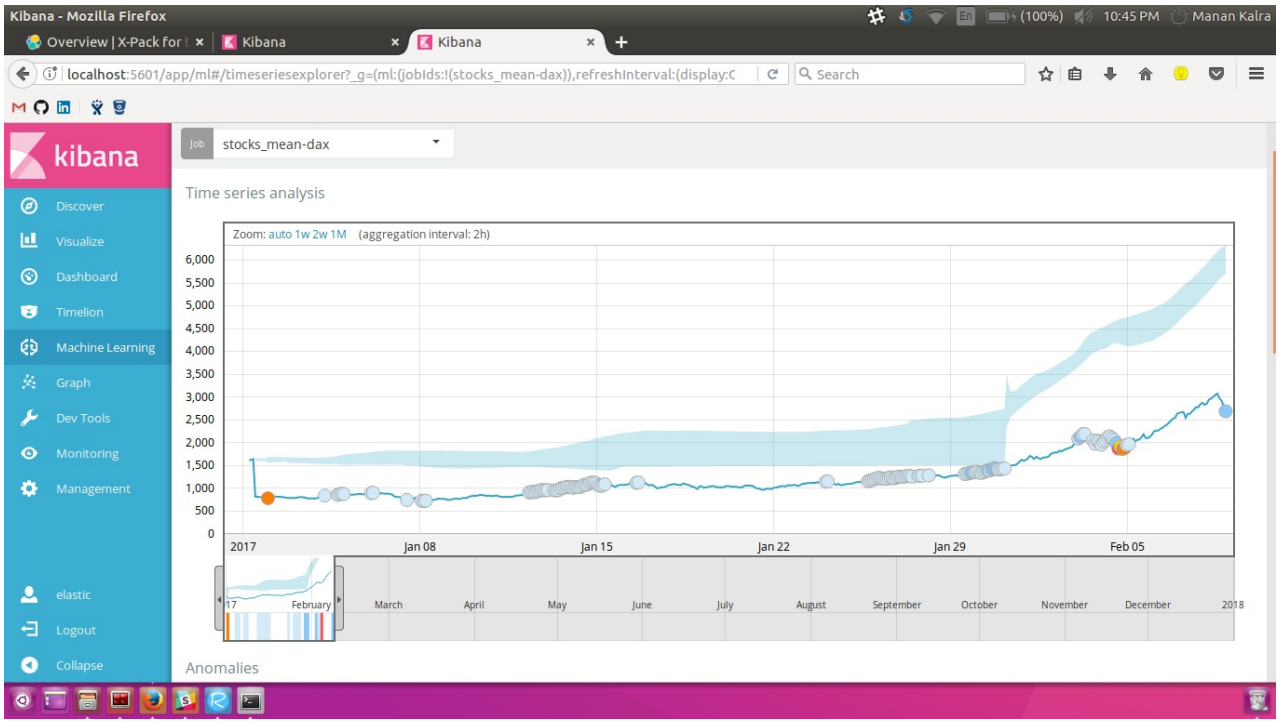


- Click on *Create Job*.

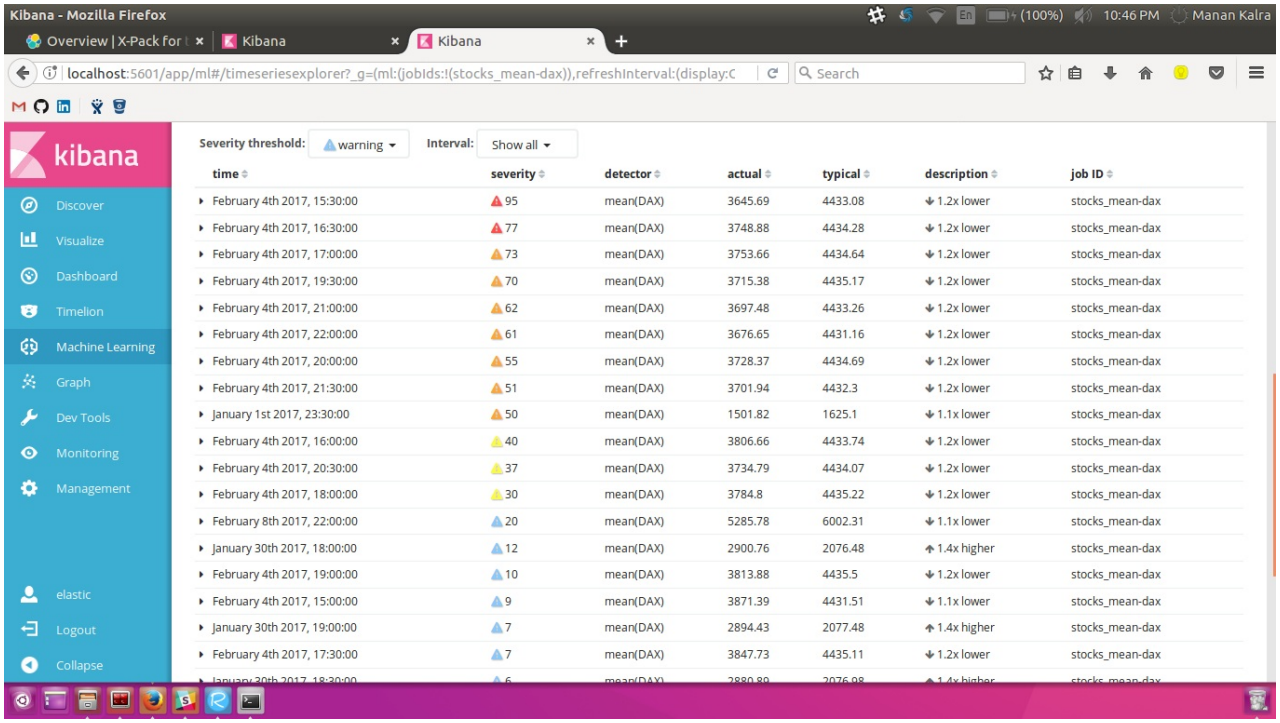




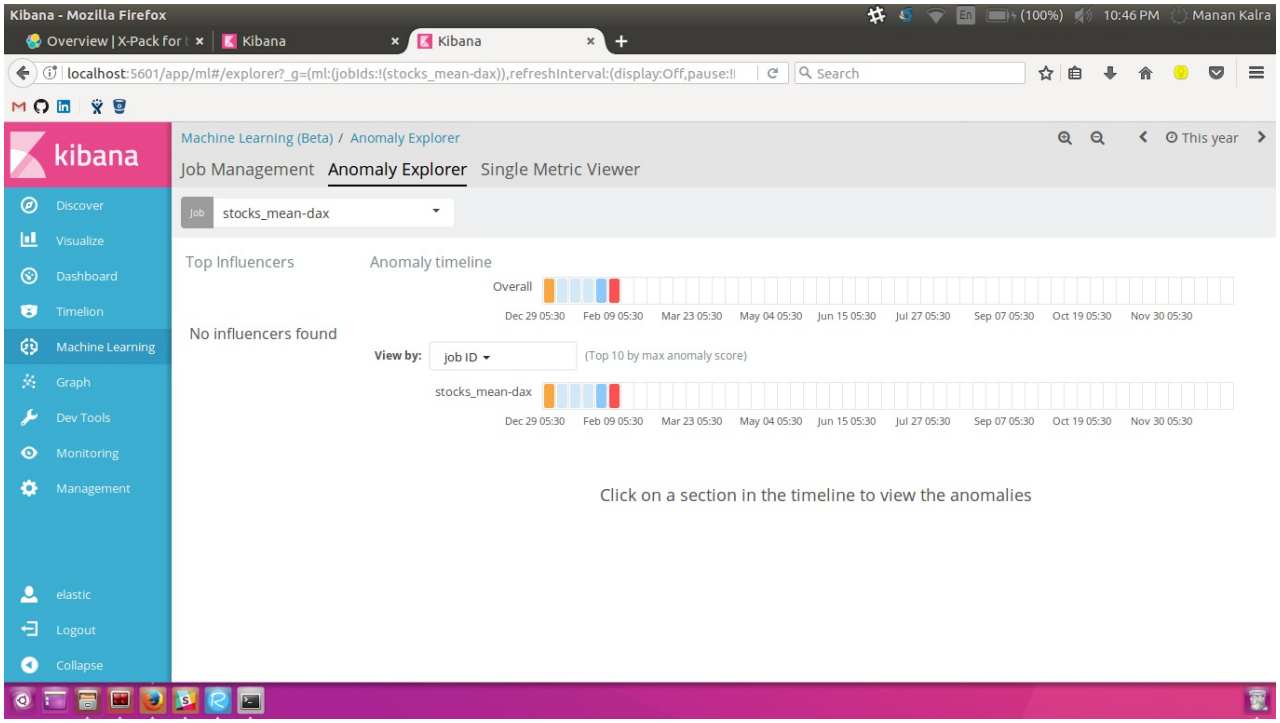
- To view the results of the analytical task, click on *View Results*.
- Allow pop-ups. A Single Metric Viewer will appear.

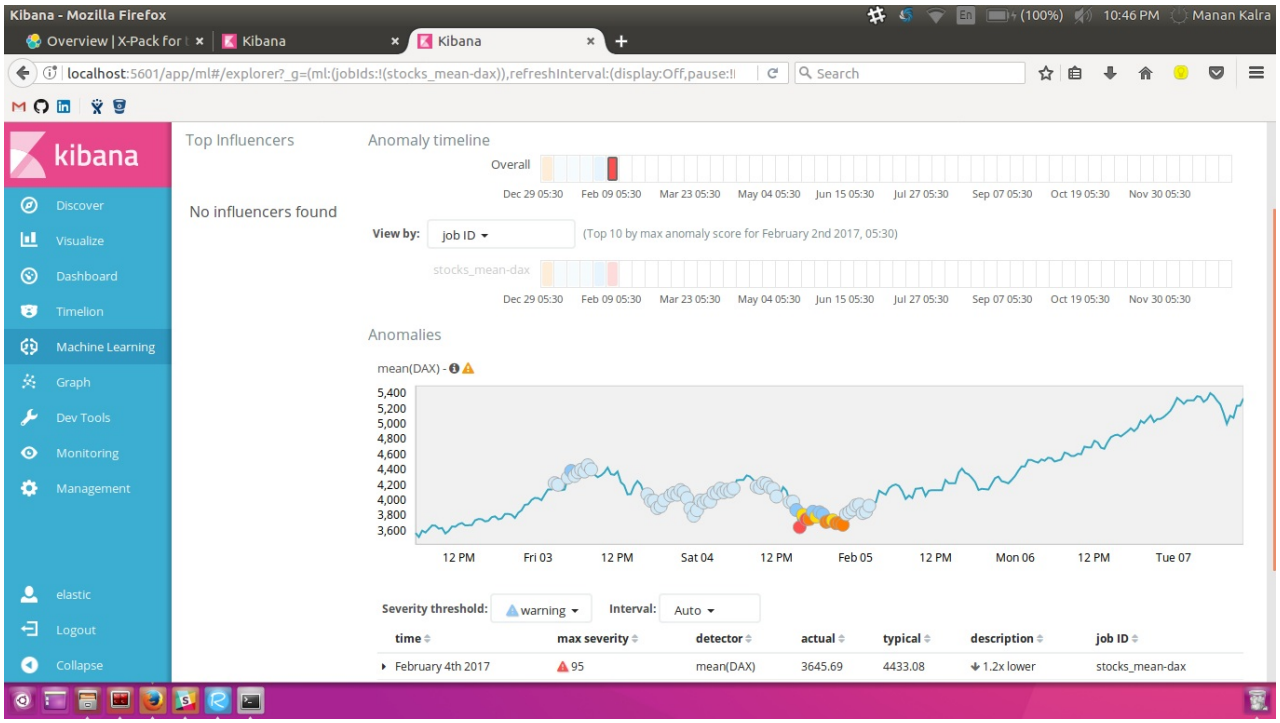


- Scroll down to see a list of the detected anomalies.

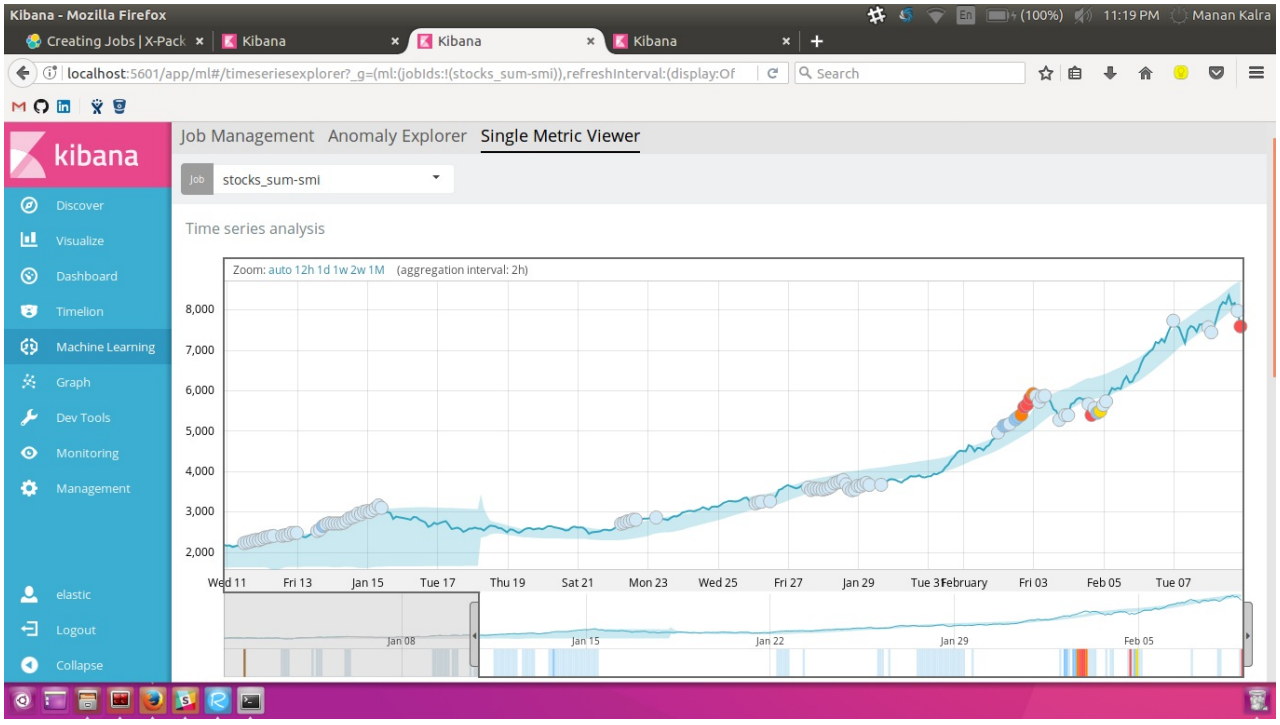


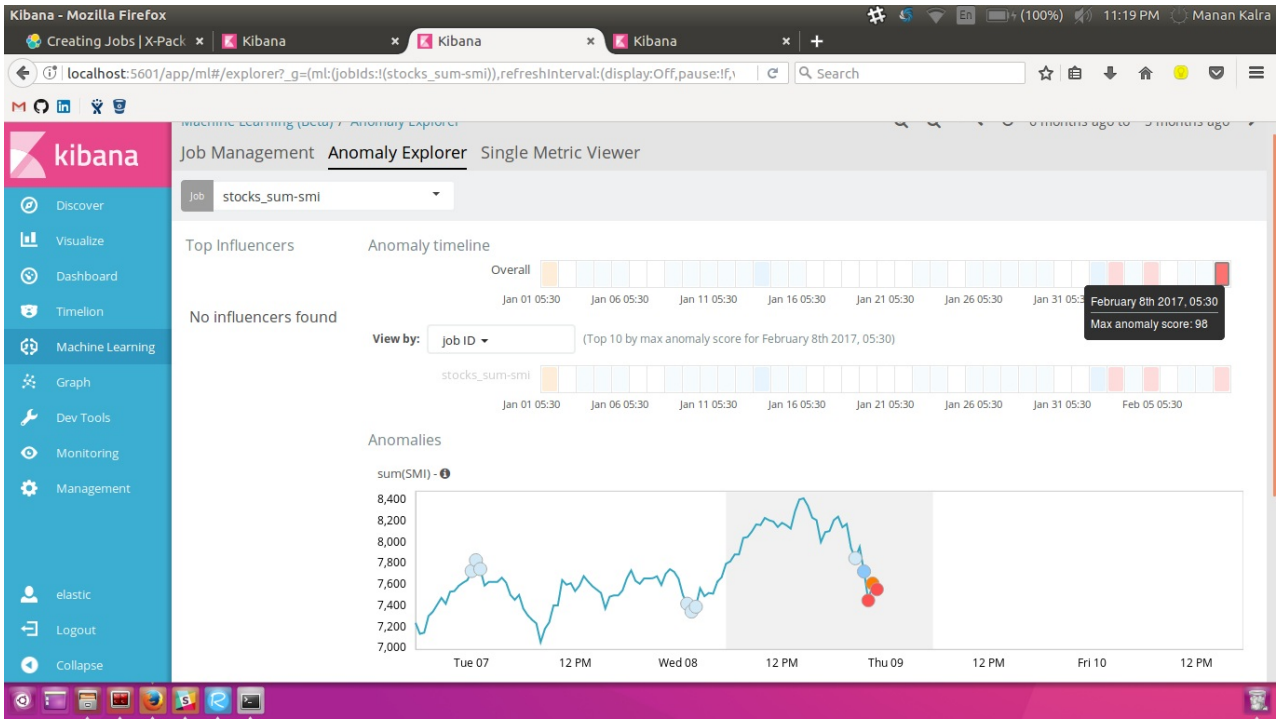
- In the Anomaly Explorer, the anomaly timeline can be viewed. Also, you can drill down to a particular span.





- Similarly, you can play around with different combinations of aggregations and fields. Create whatever fits best for your use-case.
- Another example: Sum of SMI in the stocks data




Kibana - Mozilla Firefox
Creating Jobs | X-Pack
Kibana
Kibana
Kibana
localhost:5601/app/ml#/explorer?_g=(ml:(jobIds:!(stocks_sum-smi)),refreshInterval:(display:Off,pause:!f,
Search
kibana
Discover
Visualize
Dashboard
Timelion
Machine Learning
Graph
Dev Tools
Monitoring
Management
elastic
Logout
Collapse
Job Management
Anomaly Explorer
Single Metric Viewer
Job
stocks_sum-smi
Top Influencers
No influencers found
Anomaly timeline
Overall
Jan 01 05:30
Jan 06 05:30
Jan 11 05:30
Jan 16 05:30
Jan 21 05:30
Jan 26 05:30
Jan 31 05:30
February 8th 2017, 05:30
Max anomaly score: 98
View by:
job ID
(Top 10 by max anomaly score for February 8th 2017, 05:30)
stocks_sum-smi
Feb 05 05:30
Anomalies
sum(SMI)
8,400
8,200
8,000
7,800
7,600
7,400
7,200
7,000
Tue 07
12 PM
Wed 08
12 PM
Thu 09
12 PM
Fri 10
12 PM