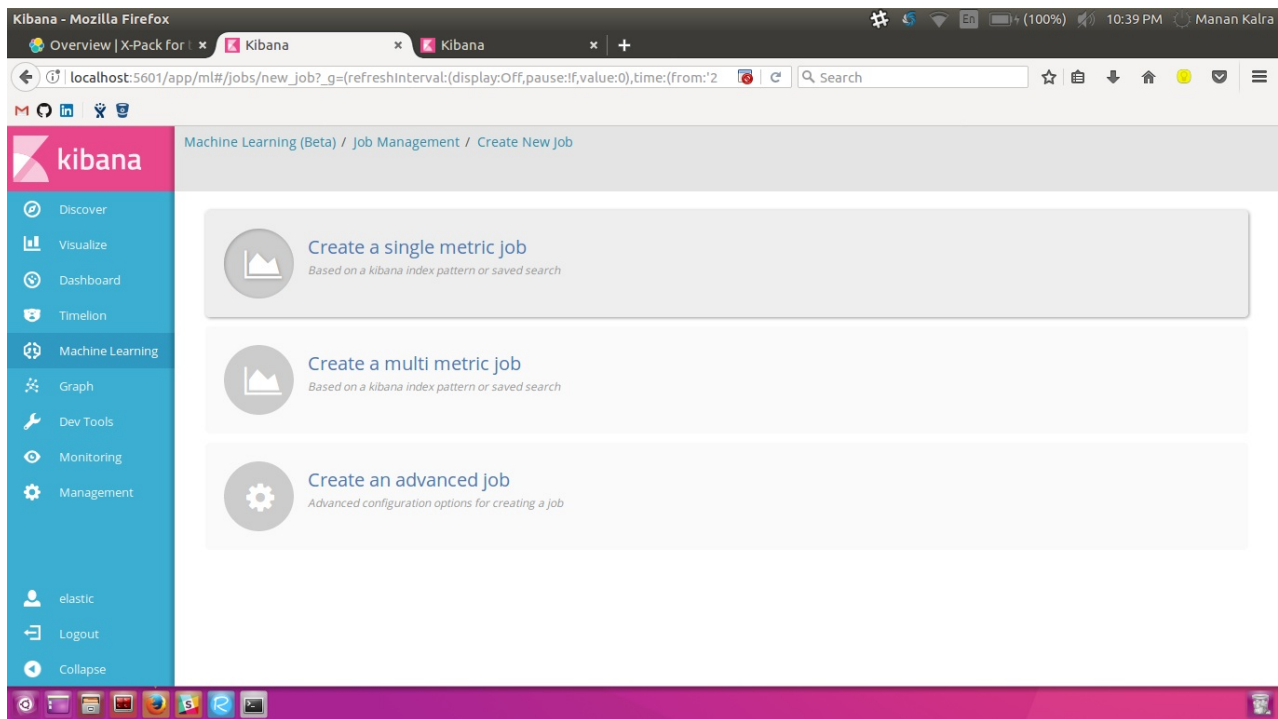


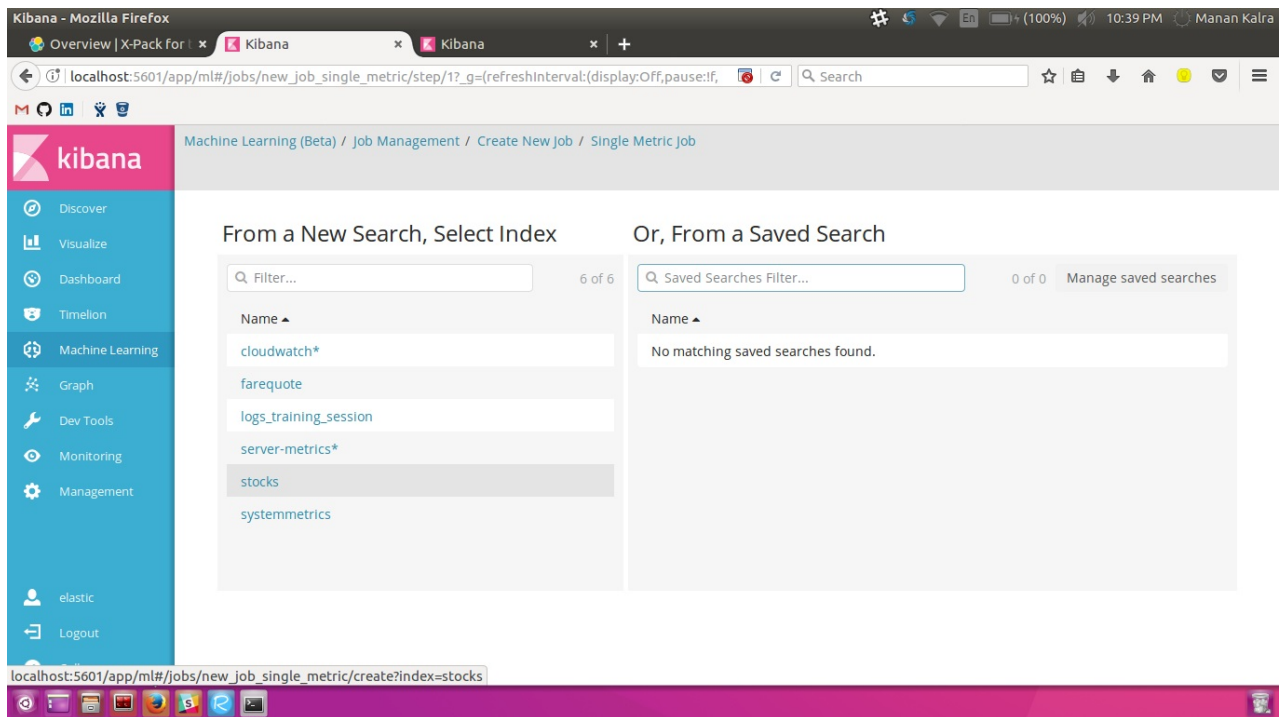


X-Pack: Machine Learning

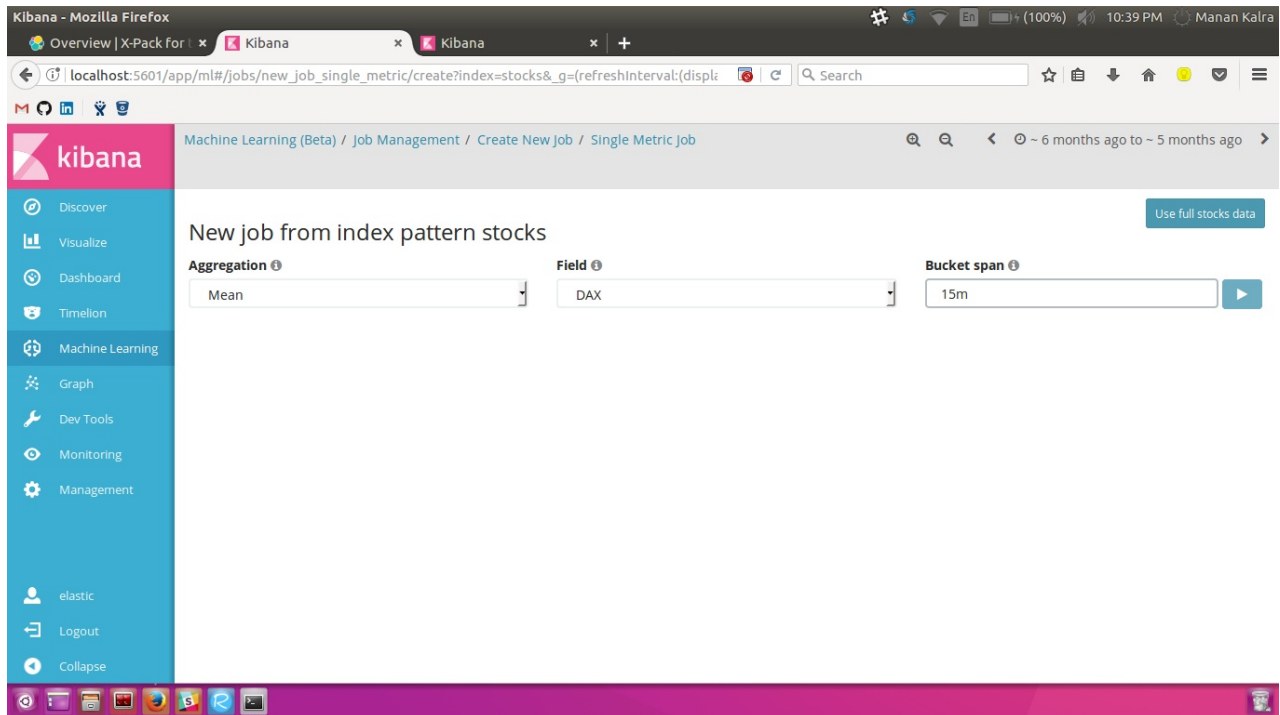
Single Metric Job Stocks

- 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 Management 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 appropriate bucket span, for example: 15m.



- [illegible]

- Kibana - Mozilla Firefox

Overview | X-Pack for | x Kibana x Kibana x +

localhost:5601/app/ml#/jobs/new_job_single_metric/create?index=stocks&_g=(refreshInterval:displ... Search

kibana

New job from index pattern stocks

Aggregation **Field** **Bucket span**

Mean DAX 15m

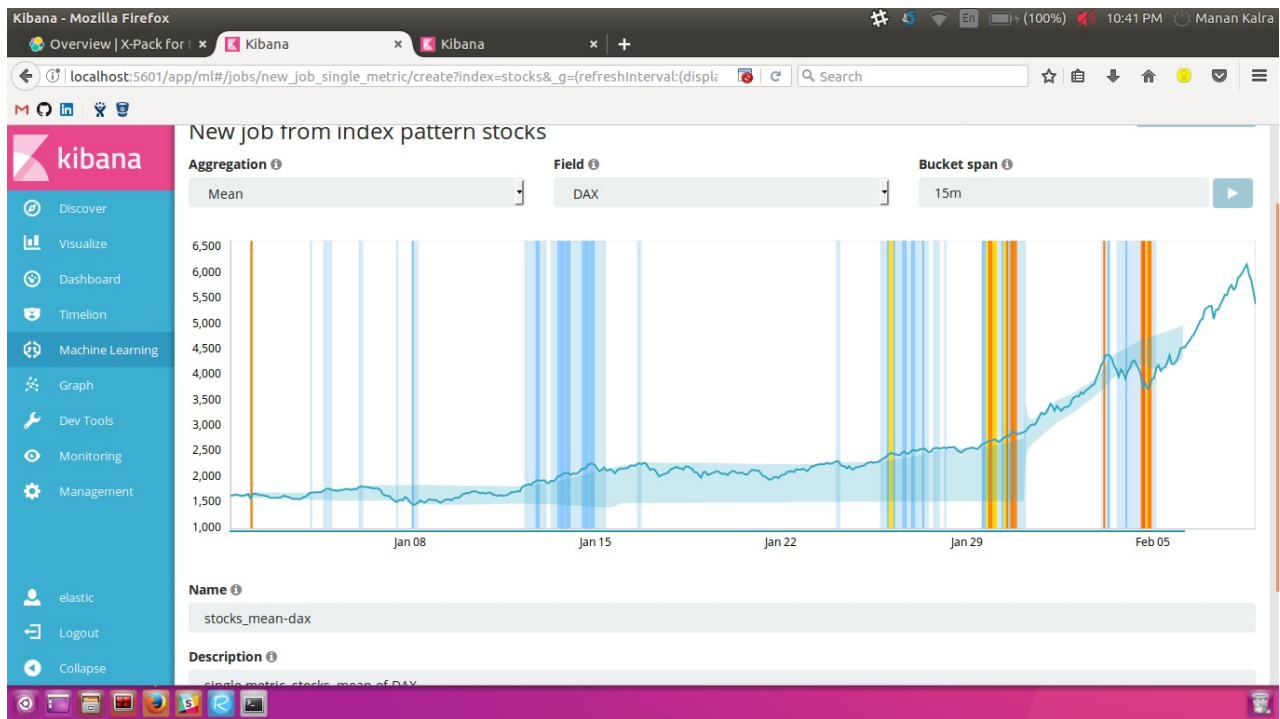
Jan 08 Jan 15 Jan 22 Jan 29 Feb 05

Name

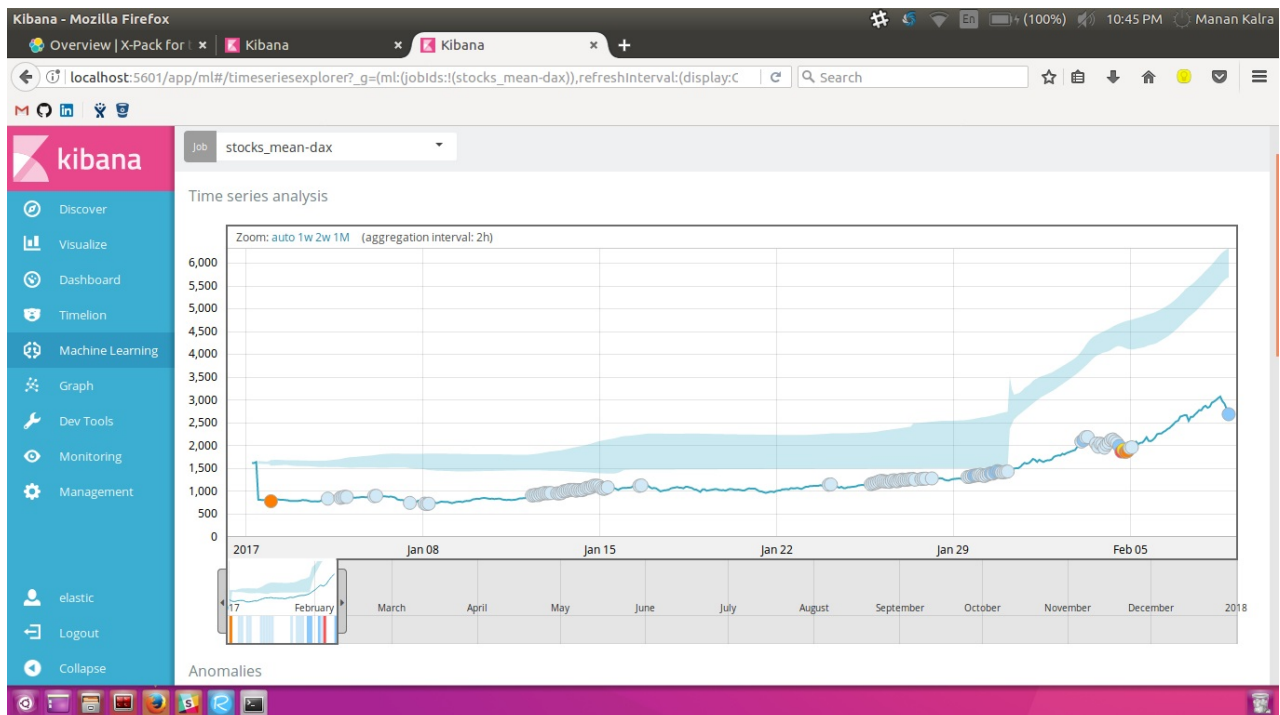
stocks_mean-dax

Description

single metric stocks mean of DAX



- 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.

Kibana - Mozilla Firefox

Overview | X-Pack for | Kibana

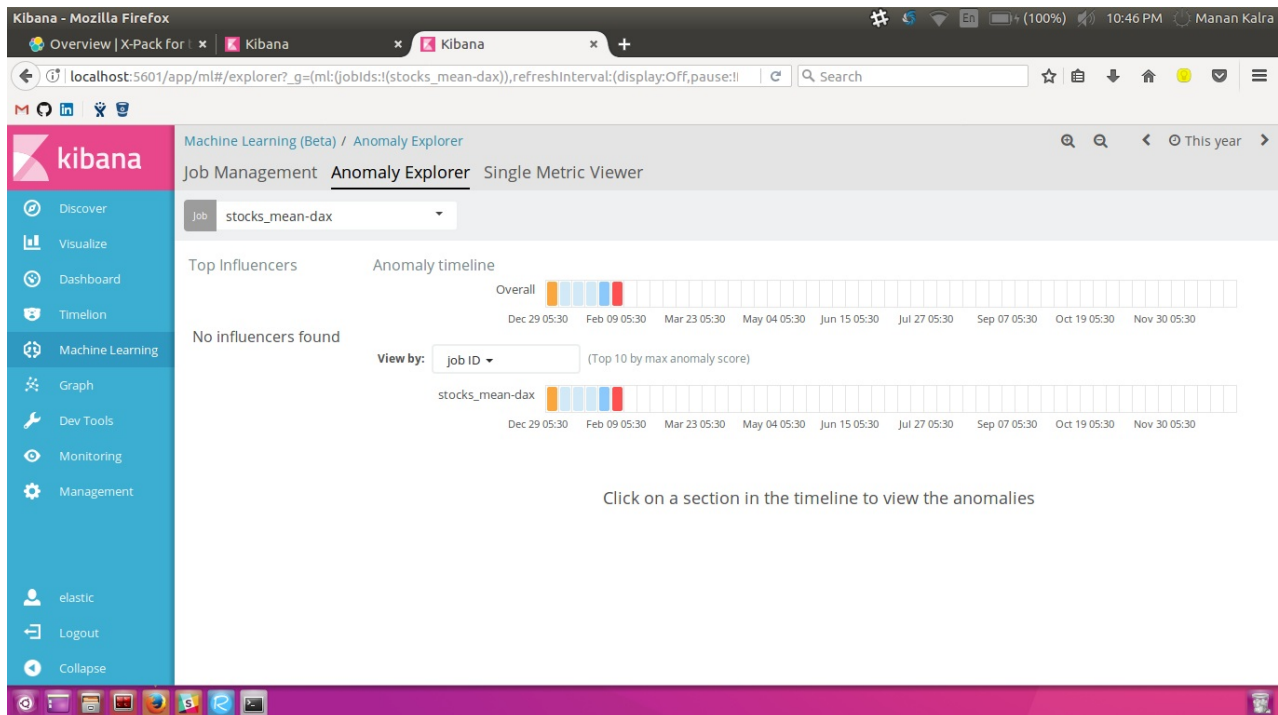
localhost:5601/app/ml#/timeseriesexplorer?_g=(ml:(jobs:(stocks_mean-dax)),refreshInterval:(display:C

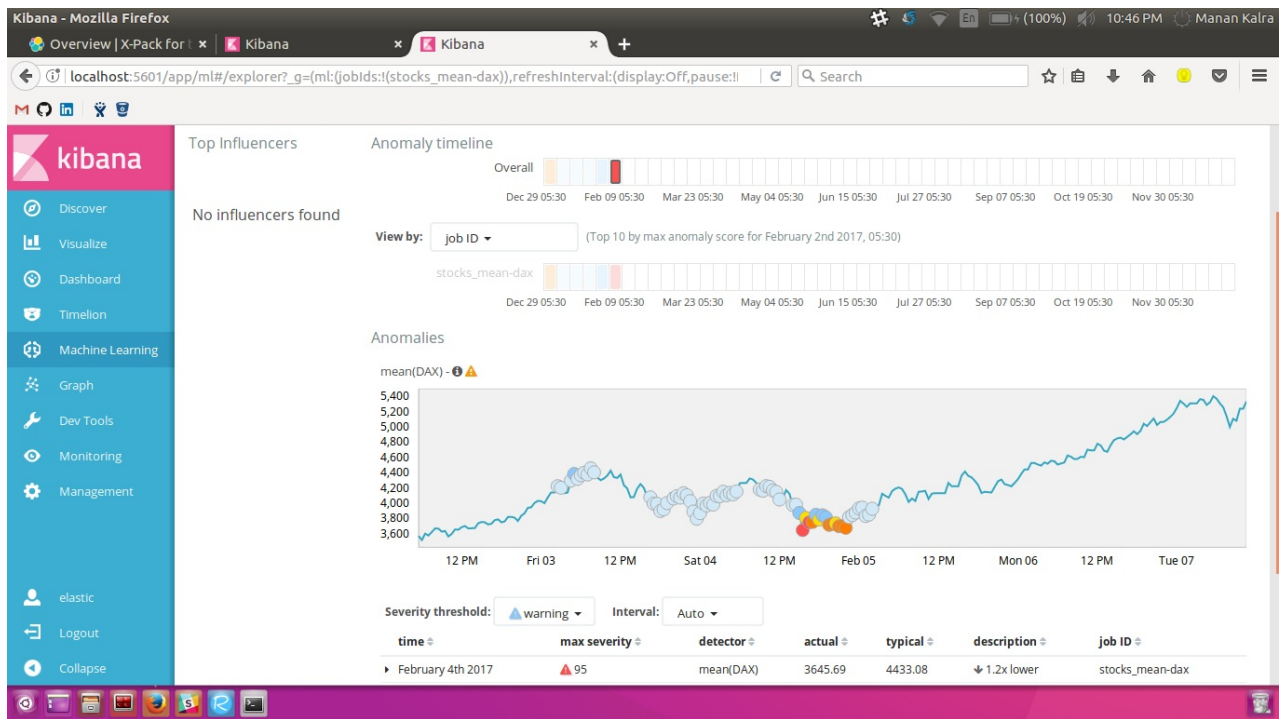
Search

Severity threshold: warning Interval: Show all

time	severity	detector	actual	typical	description	job ID
February 4th 2017, 15:30:00	95	mean(DAX)	3645.69	4433.08	1.2x lower	stocks_mean-dax
February 4th 2017, 16:30:00	77	mean(DAX)	3748.88	4434.28	1.2x lower	stocks_mean-dax
February 4th 2017, 17:00:00	73	mean(DAX)	3753.66	4434.64	1.2x lower	stocks_mean-dax
February 4th 2017, 19:30:00	70	mean(DAX)	3715.38	4435.17	1.2x lower	stocks_mean-dax
February 4th 2017, 21:00:00	62	mean(DAX)	3697.48	4433.26	1.2x lower	stocks_mean-dax
February 4th 2017, 22:00:00	61	mean(DAX)	3676.65	4431.16	1.2x lower	stocks_mean-dax
February 4th 2017, 20:00:00	55	mean(DAX)	3728.37	4434.69	1.2x lower	stocks_mean-dax
February 4th 2017, 21:30:00	51	mean(DAX)	3701.94	4432.3	1.2x lower	stocks_mean-dax
January 1st 2017, 23:30:00	50	mean(DAX)	1501.82	1625.1	1.1x lower	stocks_mean-dax
February 4th 2017, 16:00:00	40	mean(DAX)	3806.66	4433.74	1.2x lower	stocks_mean-dax
February 4th 2017, 20:30:00	37	mean(DAX)	3734.79	4434.07	1.2x lower	stocks_mean-dax
February 4th 2017, 18:00:00	30	mean(DAX)	3784.8	4435.22	1.2x lower	stocks_mean-dax
February 8th 2017, 22:00:00	20	mean(DAX)	5285.78	6002.31	1.1x lower	stocks_mean-dax
January 30th 2017, 18:00:00	12	mean(DAX)	2900.76	2076.48	1.4x higher	stocks_mean-dax
February 4th 2017, 19:00:00	10	mean(DAX)	3813.88	4435.5	1.2x lower	stocks_mean-dax
February 4th 2017, 15:00:00	9	mean(DAX)	3871.39	4431.51	1.1x lower	stocks_mean-dax
January 30th 2017, 19:00:00	7	mean(DAX)	2894.43	2077.48	1.4x higher	stocks_mean-dax
February 4th 2017, 17:30:00	7	mean(DAX)	3847.73	4435.11	1.2x lower	stocks_mean-dax
January 30th 2017, 18:30:00	6	mean(DAX)	2880.89	2076.08	1.4x higher	stocks_mean-dax

- 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

