LAB 5 – Elastic Machine Learning

Estimated Time for This Lab: 45 Min

Introduction

Elastic machine learning features automate the analysis of time-series data by creating accurate baselines of normal behavior in the data and identifying anomalous patterns in that data. You can submit your data for analysis in batches or continuously in real-time datafeeds.

Using proprietary machine learning algorithms, the following circumstances are detected, scored, and linked with statistically significant influencers in the data:

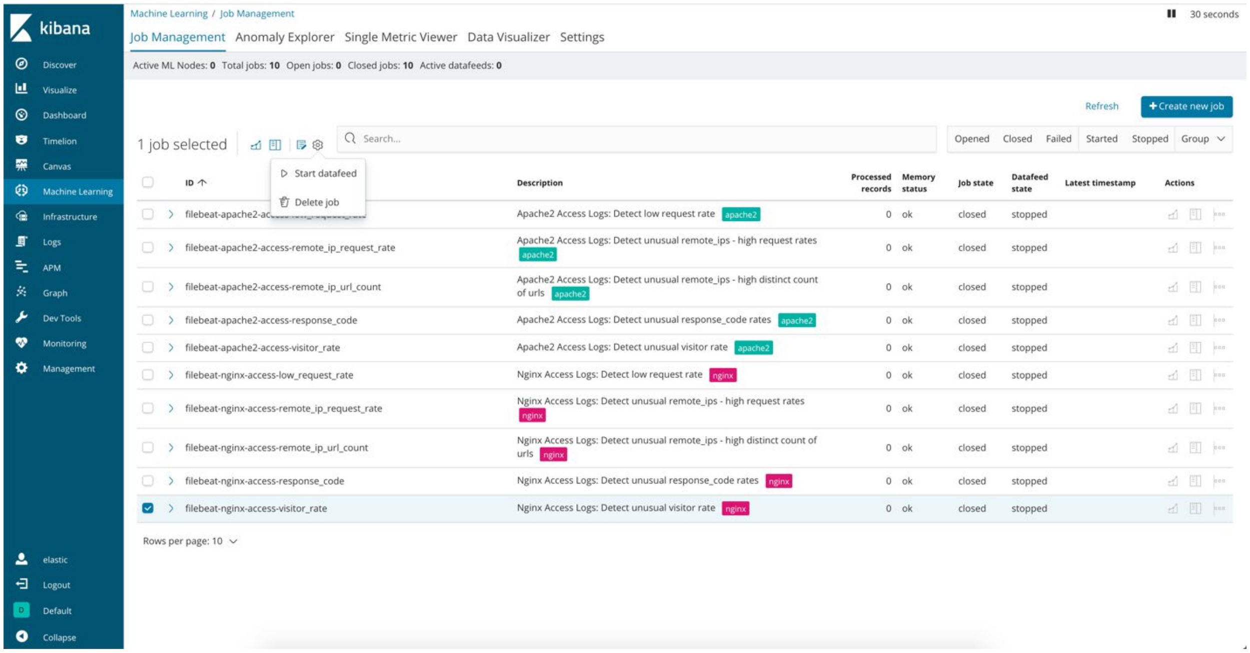
- Anomalies related to temporal deviations in values, counts, or frequencies
- Statistical rarity
- Unusual behaviors for a member of a population
- Automated periodicity detection and quick adaptation to changing data ensure that you don’t need to specify algorithms, models, or other data science-related configurations in order to get the benefits of machine learning.

You can view the machine learning results in Kibana where, for example, charts illustrate the actual data values, the bounds for the expected values, and the anomalies that occur outside these bounds.

Machine Learning is a very powerful addition to your toolkit when working with log data. In this lab we will use Elastic Machine Learning to review the EGINX logs we loaded in Lab 1.

Let’s get started!

1. In Kibana click on “Machine Learning” item in the menu. In the list of jobs select “filebeat-nginx-access-visitor_rate” and click on “Start datafeed”.



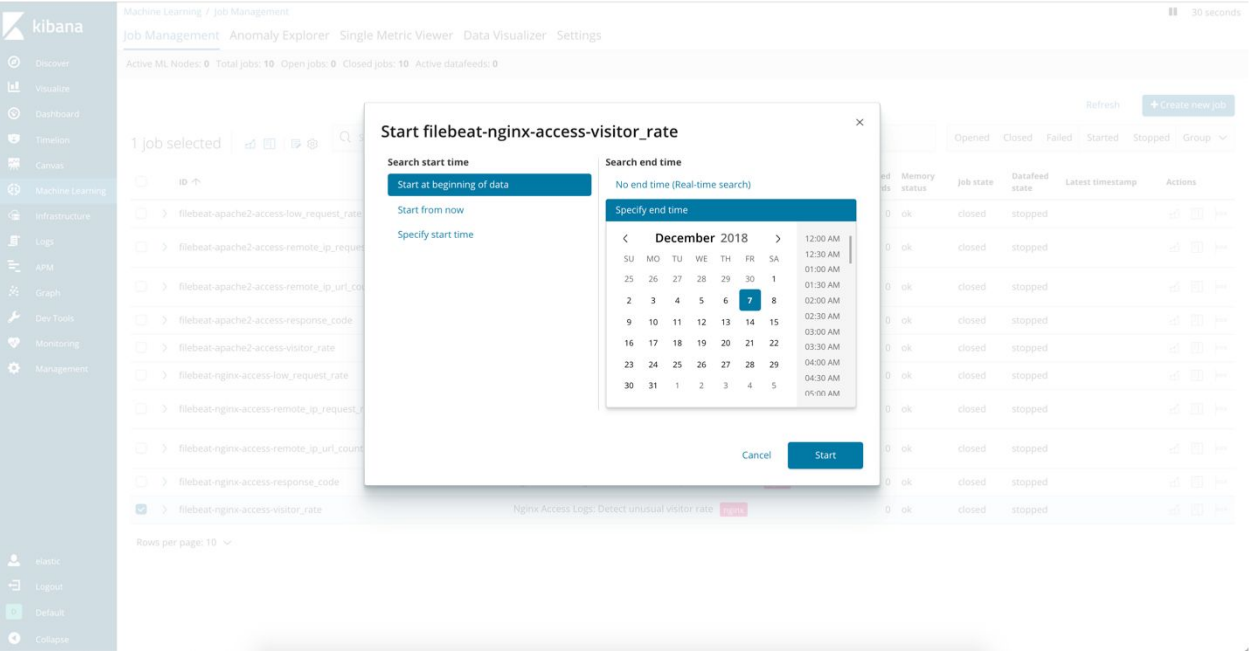
Active ML Nodes: **0** Total jobs: **10** Open jobs: **0** Closed jobs: **10** Active datafeeds: **0**

1 job selected

	ID ↑	Description	Processed records	Memory status	Job state	Datafeed state	Latest timestamp	Actions
□	filebeat-apache2-ac	Apache2 Access Logs: Detect low request rate apache2	0	ok	closed	stopped		
□	filebeat-apache2-access-remote_ip_request_rate	Apache2 Access Logs: Detect unusual remote_ips - high request rates apache2	0	ok	closed	stopped		
□	filebeat-apache2-access-remote_ip_url_count	Apache2 Access Logs: Detect unusual remote_ips - high distinct count of urls apache2	0	ok	closed	stopped		
□	filebeat-apache2-access-response_code	Apache2 Access Logs: Detect unusual response_code rates apache2	0	ok	closed	stopped		
□	filebeat-apache2-access-visitor_rate	Apache2 Access Logs: Detect unusual visitor rate apache2	0	ok	closed	stopped		
□	filebeat-nginx-access-low_request_rate	Nginx Access Logs: Detect low request rate nginx	0	ok	closed	stopped		
□	filebeat-nginx-access-remote_ip_request_rate	Nginx Access Logs: Detect unusual remote_ips - high request rates nginx	0	ok	closed	stopped		
□	filebeat-nginx-access-remote_ip_url_count	Nginx Access Logs: Detect unusual remote_ips - high distinct count of urls nginx	0	ok	closed	stopped		
□	filebeat-nginx-access-response_code	Nginx Access Logs: Detect unusual response_code rates nginx	0	ok	closed	stopped		
☑	filebeat-nginx-access-visitor_rate	Nginx Access Logs: Detect unusual visitor rate nginx	0	ok	closed	stopped		

Rows per page: 10

2. Select time period “Start at beginning of data” and click on “Start”.



Start filebeat-nginx-access-visitor_rate

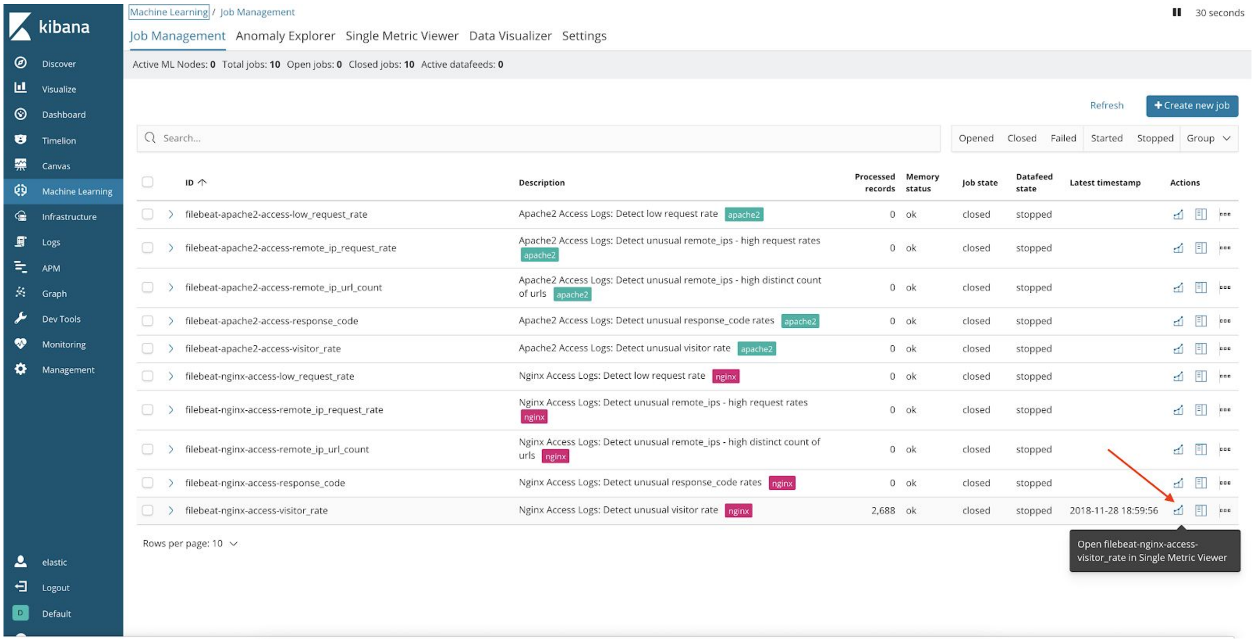
Search start time

- Start at beginning of data
- Start from now
- Specify start time

Search end time

- No end time (Real-time search)
- Specify end time

3. Wait until the Datafeed state changes to “stopped” and click on the results icon to view the output of the job in Single Metrics viewer



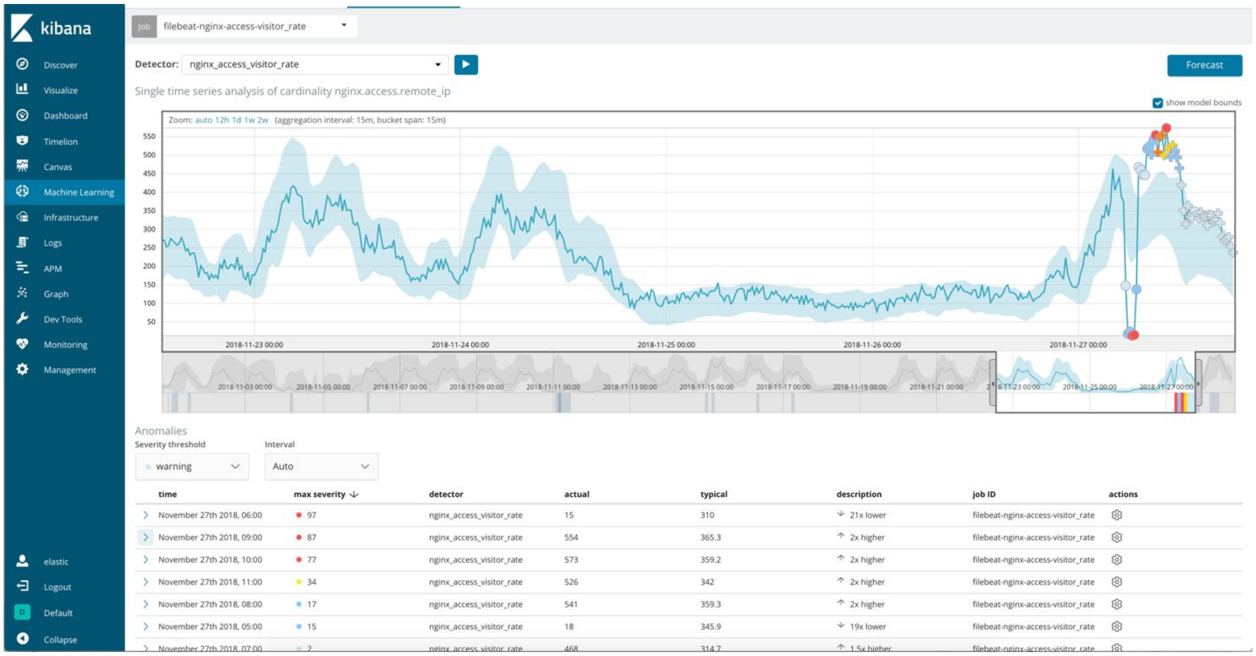
Active ML Nodes: **0** Total jobs: **10** Open jobs: **0** Closed jobs: **10** Active datafeeds: **0**

ID ↑	Description	Processed records	Memory status	Job state	Datafeed state	Latest timestamp	Actions
filebeat-apache2-access-low_request_rate	Apache2 Access Logs: Detect low request rate apache2	0	ok	closed	stopped		
filebeat-apache2-access-remote_ip_request_rate	Apache2 Access Logs: Detect unusual remote_ips - high request rates apache2	0	ok	closed	stopped		
filebeat-apache2-access-remote_ip_url_count	Apache2 Access Logs: Detect unusual remote_ips - high distinct count of urls apache2	0	ok	closed	stopped		
filebeat-apache2-access-response_code	Apache2 Access Logs: Detect unusual response_code rates apache2	0	ok	closed	stopped		
filebeat-apache2-access-visitor_rate	Apache2 Access Logs: Detect unusual visitor rate apache2	0	ok	closed	stopped		
filebeat-nginx-access-low_request_rate	Nginx Access Logs: Detect low request rate nginx	0	ok	closed	stopped		
filebeat-nginx-access-remote_ip_request_rate	Nginx Access Logs: Detect unusual remote_ips - high request rates nginx	0	ok	closed	stopped		
filebeat-nginx-access-remote_ip_url_count	Nginx Access Logs: Detect unusual remote_ips - high distinct count of urls nginx	0	ok	closed	stopped		
filebeat-nginx-access-response_code	Nginx Access Logs: Detect unusual response_code rates nginx	0	ok	closed	stopped		
filebeat-nginx-access-visitor_rate	Nginx Access Logs: Detect unusual visitor rate nginx	2,688	ok	closed	stopped	2018-11-28 18:59:56	

Rows per page: 10

Open filebeat-nginx-access-visitor_rate in Single Metric Viewer

4. Slide the window to see how the model (shaded blue area) was built and how it got narrower (i.e. more precise) over time. The anomaly that you will see towards the end is the sudden drop in visitor rate and then the spike.



Job: filebeat-nginx-access-visitor_rate

Detector: nginx_access_visitor_rate

Single time series analysis of cardinality nginx.access.remote_ip

Zoom: auto 12h 1d 1w 2w (aggregation interval: 15m, bucket span: 15m)

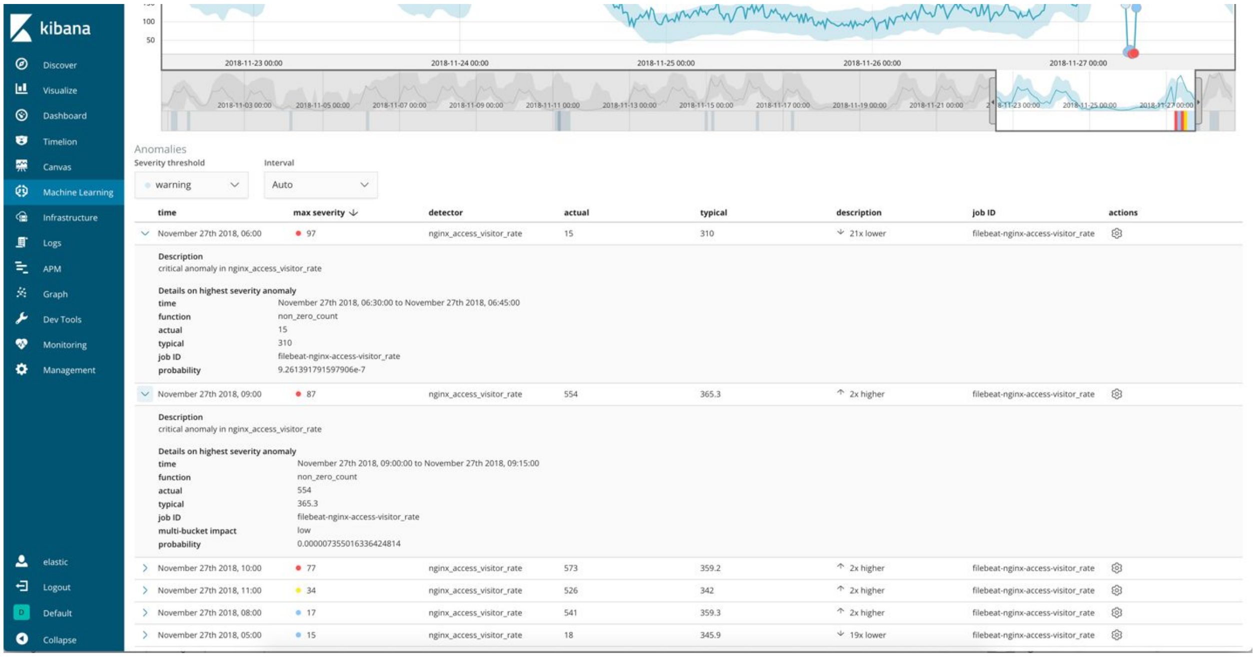
Anomalies

Severity threshold: warning

Interval: Auto

time	max severity ↓	detector	actual	typical	description	job ID	actions
November 27th 2018, 06:00	● 97	nginx_access_visitor_rate	15	310	↓ 21x lower	filebeat-nginx-access-visitor_rate	⚙
November 27th 2018, 09:00	● 87	nginx_access_visitor_rate	554	365.3	↑ 2x higher	filebeat-nginx-access-visitor_rate	⚙
November 27th 2018, 10:00	● 77	nginx_access_visitor_rate	573	359.2	↑ 2x higher	filebeat-nginx-access-visitor_rate	⚙
November 27th 2018, 11:00	● 34	nginx_access_visitor_rate	526	342	↑ 2x higher	filebeat-nginx-access-visitor_rate	⚙
November 27th 2018, 08:00	● 17	nginx_access_visitor_rate	541	359.3	↑ 2x higher	filebeat-nginx-access-visitor_rate	⚙
November 27th 2018, 05:00	● 15	nginx_access_visitor_rate	18	345.9	↓ 19x lower	filebeat-nginx-access-visitor_rate	⚙
November 27th 2018, 07:00	● 2	nginx_access_visitor_rate	468	314.7	↑ 1.5x higher	filebeat-nginx-access-visitor_rate	⚙

5. Expand top two anomalies by clicking on them. Note how both anomalies are severe, despite the drop is 21x lower, and the spike is 2x higher. The reason for that is because what contributes to anomaly is not how much higher/lower the actual value is against the expected value, but the probability of its occurrence. The probability value is provided once you click on Anomalies to expand the results.



Anomalies

Severity threshold: warning

Interval: Auto

time	max severity	detector	actual	typical	description	job ID	actions
November 27th 2018, 06:00	● 97	nginx_access_visitor_rate	15	310	↓ 21x lower	filebeat-nginx-access-visitor_rate	⚙

Description
critical anomaly in nginx_access_visitor_rate

Details on highest severity anomaly

time	November 27th 2018, 06:30:00 to November 27th 2018, 06:45:00
function	non_zero_count
actual	15
typical	310
job ID	filebeat-nginx-access-visitor_rate
probability	9.261391791597906e-7

November 27th 2018, 09:00	● 87	nginx_access_visitor_rate	554	365.3	↑ 2x higher	filebeat-nginx-access-visitor_rate	⚙

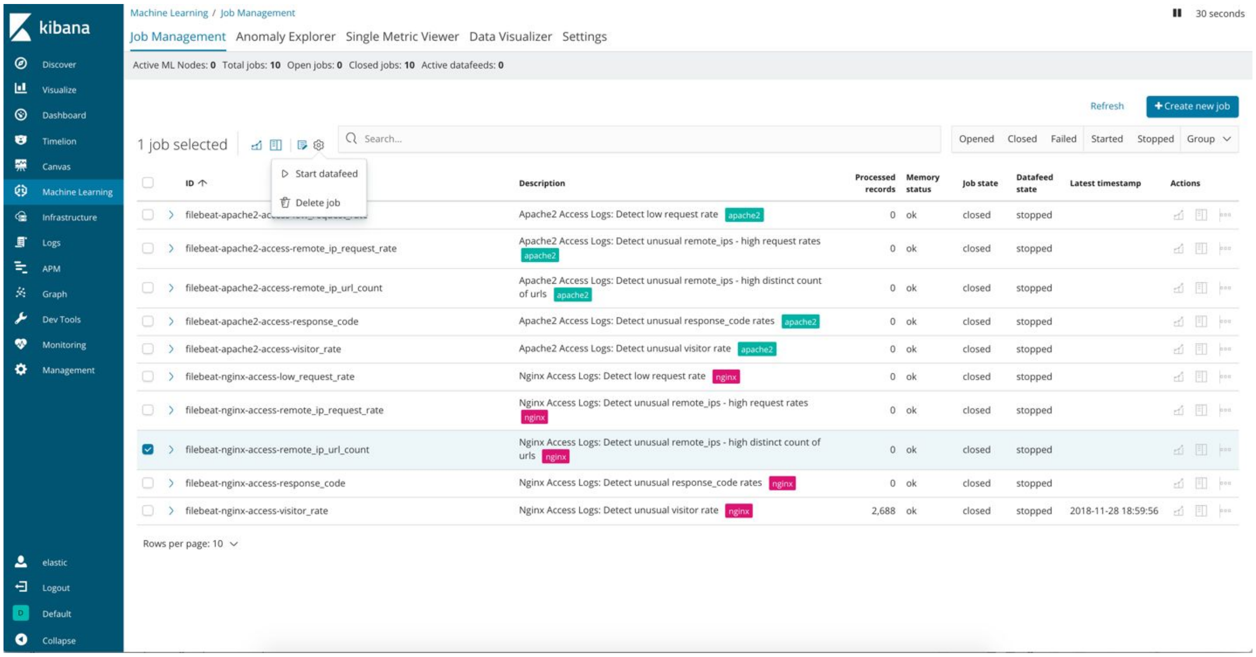
Description
critical anomaly in nginx_access_visitor_rate

Details on highest severity anomaly

time	November 27th 2018, 09:00:00 to November 27th 2018, 09:15:00
function	non_zero_count
actual	554
typical	365.3
job ID	filebeat-nginx-access-visitor_rate
multi-bucket impact	low
probability	0.000007355016336424814

November 27th 2018, 10:00	● 77	nginx_access_visitor_rate	573	359.2	↑ 2x higher	filebeat-nginx-access-visitor_rate	⚙
November 27th 2018, 11:00	● 34	nginx_access_visitor_rate	526	342	↑ 2x higher	filebeat-nginx-access-visitor_rate	⚙
November 27th 2018, 08:00	● 17	nginx_access_visitor_rate	541	359.3	↑ 2x higher	filebeat-nginx-access-visitor_rate	⚙
November 27th 2018, 05:00	● 15	nginx_access_visitor_rate	18	345.9	↓ 19x lower	filebeat-nginx-access-visitor_rate	⚙

6. Click on “Machine Learning” menu in Kibana again. Select “filebeat-nginx-access-remote_ip_url_count” job and start datafeed. Start from the beginning of data and click on Start.

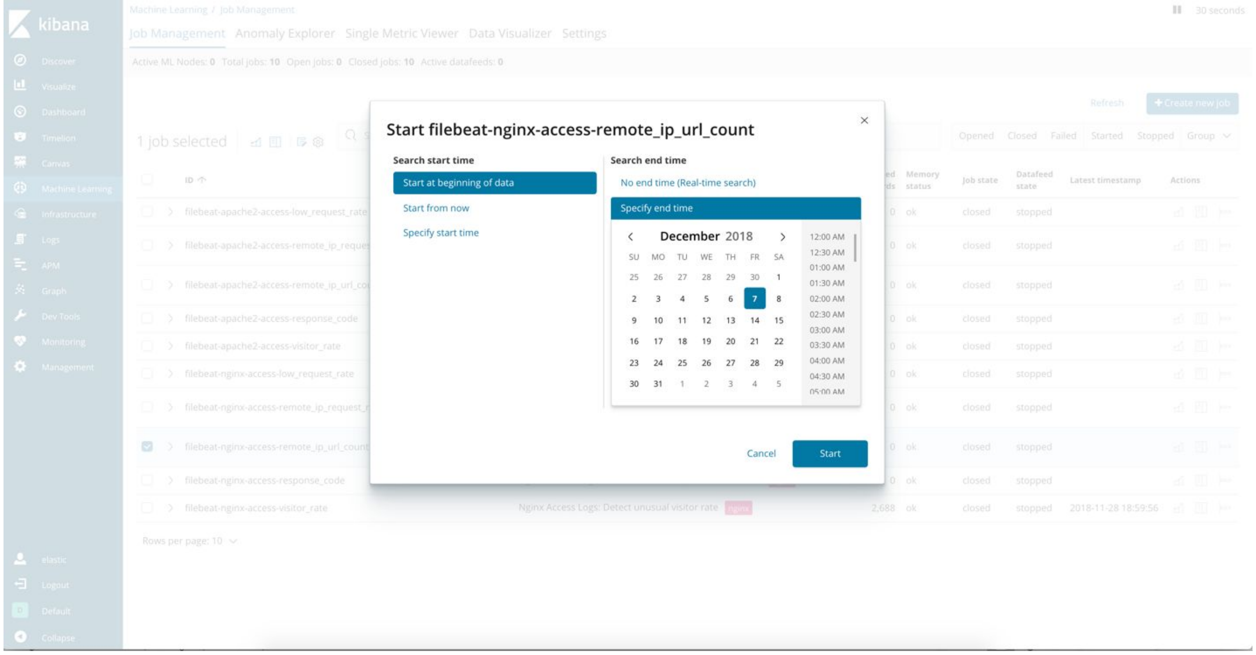


Active ML Nodes: 0 Total jobs: 10 Open jobs: 0 Closed jobs: 10 Active datafeeds: 0

1 job selected

	ID	Description	Processed records	Memory status	Job state	Datafeed state	Latest timestamp
□	filebeat-apache2-ac	Apache2 Access Logs: Detect low request rate apache2	0	ok	closed	stopped	
□	filebeat-apache2-access-remote_ip_request_rate	Apache2 Access Logs: Detect unusual remote_ips - high request rates apache2	0	ok	closed	stopped	
□	filebeat-apache2-access-remote_ip_url_count	Apache2 Access Logs: Detect unusual remote_ips - high distinct count of urls apache2	0	ok	closed	stopped	
□	filebeat-apache2-access-response_code	Apache2 Access Logs: Detect unusual response_code rates apache2	0	ok	closed	stopped	
□	filebeat-apache2-access-visitor_rate	Apache2 Access Logs: Detect unusual visitor rate apache2	0	ok	closed	stopped	
□	filebeat-nginx-access-low_request_rate	Nginx Access Logs: Detect low request rate nginx	0	ok	closed	stopped	
□	filebeat-nginx-access-remote_ip_request_rate	Nginx Access Logs: Detect unusual remote_ips - high request rates nginx	0	ok	closed	stopped	
☑	filebeat-nginx-access-remote_ip_url_count	Nginx Access Logs: Detect unusual remote_ips - high distinct count of urls nginx	0	ok	closed	stopped	
□	filebeat-nginx-access-response_code	Nginx Access Logs: Detect unusual response_code rates nginx	0	ok	closed	stopped	
□	filebeat-nginx-access-visitor_rate	Nginx Access Logs: Detect unusual visitor rate nginx	2,688	ok	closed	stopped	2018-11-28 18:59:56

Rows per page: 10



Start filebeat-nginx-access-remote_ip_url_count

Search start time

- Start at beginning of data
- Start from now
- Specify start time

Search end time

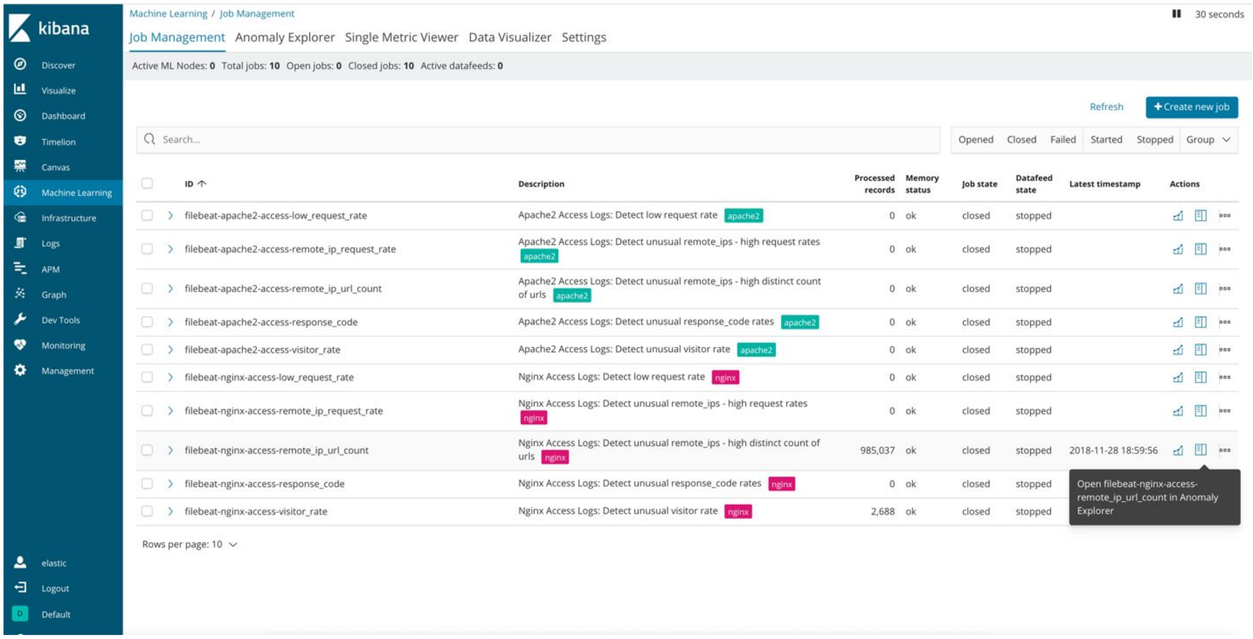
- No end time (Real-time search)
- Specify end time

December 2018

SU	MO	TU	WE	TH	FR	SA
25	26	27	28	29	30	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

12:00 AM
12:30 AM
01:00 AM
01:30 AM
02:00 AM
02:30 AM
03:00 AM
03:30 AM
04:00 AM
04:30 AM
05:00 AM

7. Wait until the datafeed state changes to “stopped” and click on the results icon to view the output of the job in Anomaly Explorer.

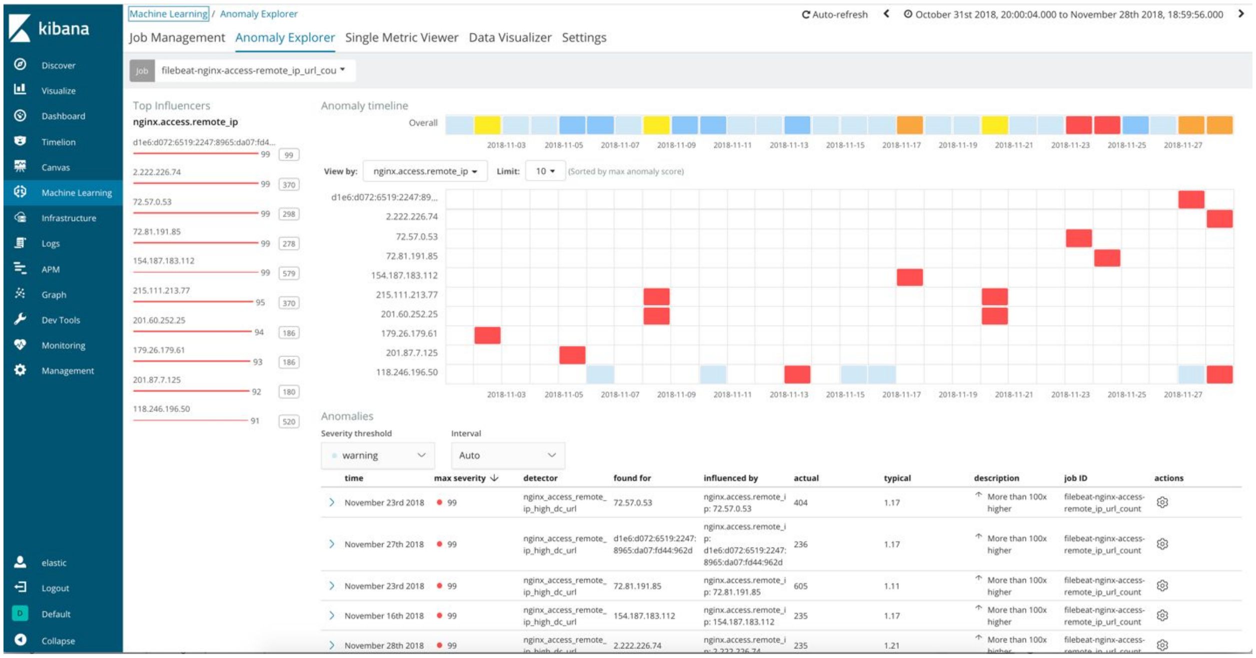


Active ML Nodes: **0** Total jobs: **10** Open jobs: **0** Closed jobs: **10** Active datafeeds: **0**

ID	Description	Processed records	Memory status	Job state	Datafeed state	Latest timestamp	Actions
filebeat-apache2-access-low_request_rate	Apache2 Access Logs: Detect low request rate apache2	0	ok	closed	stopped		
filebeat-apache2-access-remote_ip_request_rate	Apache2 Access Logs: Detect unusual remote_ips - high request rates apache2	0	ok	closed	stopped		
filebeat-apache2-access-remote_ip_url_count	Apache2 Access Logs: Detect unusual remote_ips - high distinct count of urls apache2	0	ok	closed	stopped		
filebeat-apache2-access-response_code	Apache2 Access Logs: Detect unusual response_code rates apache2	0	ok	closed	stopped		
filebeat-apache2-access-visitor_rate	Apache2 Access Logs: Detect unusual visitor rate apache2	0	ok	closed	stopped		
filebeat-nginx-access-low_request_rate	Nginx Access Logs: Detect low request rate nginx	0	ok	closed	stopped		
filebeat-nginx-access-remote_ip_request_rate	Nginx Access Logs: Detect unusual remote_ips - high request rates nginx	0	ok	closed	stopped		
filebeat-nginx-access-remote_ip_url_count	Nginx Access Logs: Detect unusual remote_ips - high distinct count of urls nginx	985,037	ok	closed	stopped	2018-11-28 18:59:56	
filebeat-nginx-access-response_code	Nginx Access Logs: Detect unusual response_code rates nginx	0	ok	closed	stopped		
filebeat-nginx-access-visitor_rate	Nginx Access Logs: Detect unusual visitor rate nginx	2,688	ok	closed	stopped		

Open filebeat-nginx-access-remote_ip_url_count in Anomaly Explorer

8. You will see the anomaly explorer where the results are broken down by particular ips. The influencers that you see are statistically significant elements in our data set contributing to the anomaly. You have an option to select a particular field in your data as contributors when you're creating a Machine Learning job. On top of the Anomaly Timeline you see Overall result for the job, and inside the matrix you see the result of the job for a particular IP. Note that results are not the same. Hover over the overall results to see the score across the whole population and over particular IPs contributing to that same score. When the score for IP "154.187.183.112" is 99 overall anomaly score is only 55.

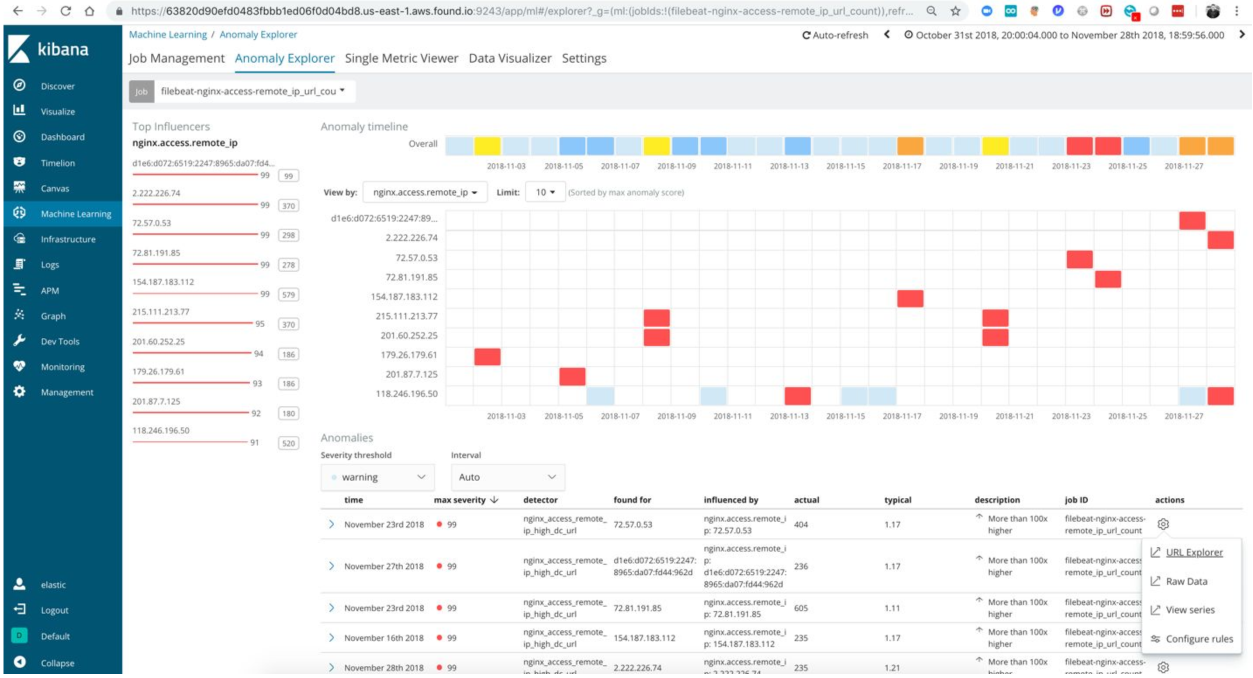


Top Influencers
nginx.access.remote_ip

d1e6:d072:6519:2247:8965:da07:fd4...	99	99
2.222.226.74	99	370
72.57.0.53	99	298
72.81.191.85	99	278
154.187.183.112	99	579
215.111.213.77	95	370
201.60.252.25	94	186
179.26.179.61	93	186
201.87.7.125	92	180
118.246.196.50	91	520

time	max severity ↓	detector	found for	influenced by	actual	typical	description	job ID	actions
November 23rd 2018	● 99	nginx_access_remote_ip_high_dc_url	72.57.0.53	nginx.access.remote_ip: 72.57.0.53	404	1.17	↑ More than 100x higher	filebeat-nginx-access-remote_ip_url_count	⚙
November 27th 2018	● 99	nginx_access_remote_ip_high_dc_url	d1e6:d072:6519:2247:8965:da07:fd44:962d	nginx.access.remote_ip: d1e6:d072:6519:2247:8965:da07:fd44:962d	236	1.17	↑ More than 100x higher	filebeat-nginx-access-remote_ip_url_count	⚙
November 23rd 2018	● 99	nginx_access_remote_ip_high_dc_url	72.81.191.85	nginx.access.remote_ip: 72.81.191.85	605	1.11	↑ More than 100x higher	filebeat-nginx-access-remote_ip_url_count	⚙
November 16th 2018	● 99	nginx_access_remote_ip_high_dc_url	154.187.183.112	nginx.access.remote_ip: 154.187.183.112	235	1.17	↑ More than 100x higher	filebeat-nginx-access-remote_ip_url_count	⚙
November 28th 2018	● 99	nginx_access_remote_ip_high_dc_url	2.222.226.74	nginx.access.remote_ip: 2.222.226.74	235	1.21	↑ More than 100x higher	filebeat-nginx-access-remote_ip_url_count	⚙

9. We have the ability to link the anomaly results of ML job with particular views when we setup the job. When opening the views the metadata from the job can be passed to it. Click on “actions” next to top anomaly and click on “URL Explorer”.

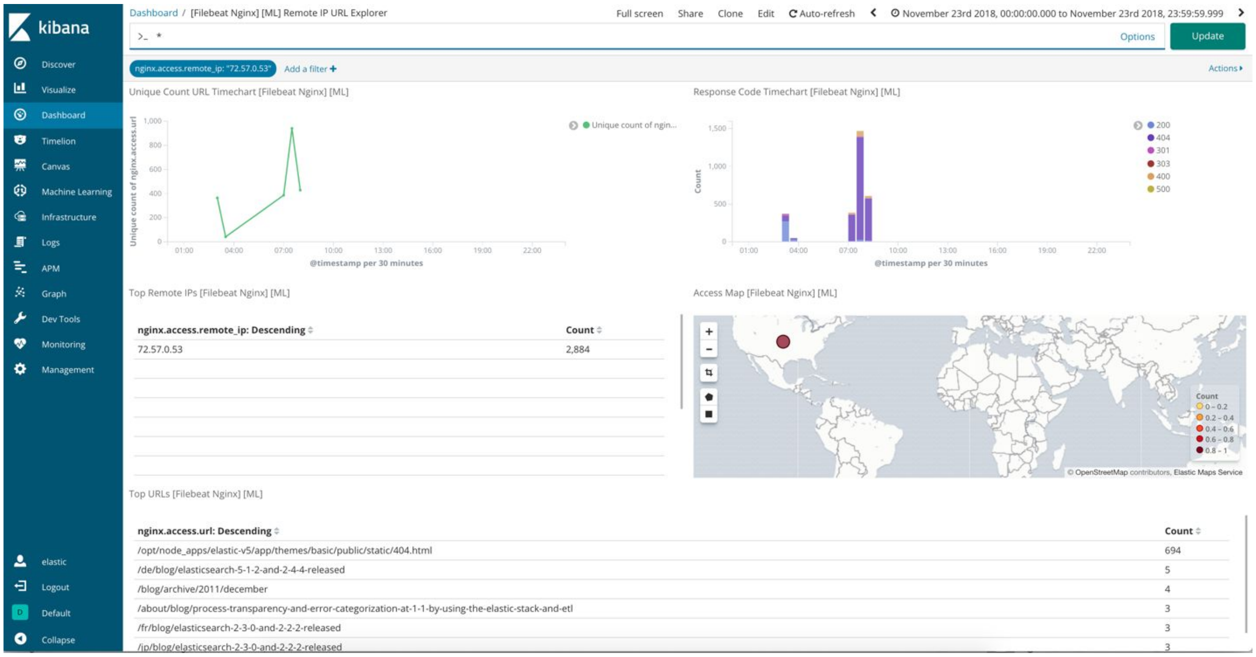


Top Influencers
nginx.access.remote_ip

d1e6:d072:6519:2247:8965:da07:fd4...	99	99
2.222.226.74	99	370
72.57.0.53	99	298
72.81.191.85	99	278
154.187.183.112	99	579
215.111.213.77	95	370
201.60.252.25	94	186
179.26.179.61	93	186
201.87.7.125	92	180
118.246.196.50	91	520

time	max severity ↓	detector	found for	influenced by	actual	typical	description	job ID	actions
November 23rd 2018	● 99	nginx_access_remote_ip_high_dc_url	72.57.0.53	nginx.access.remote_ip: 72.57.0.53	404	1.17	↑ More than 100x higher	filebeat-nginx-access-remote_ip_url_count	⚙
November 27th 2018	● 99	nginx_access_remote_ip_high_dc_url	d1e6:d072:6519:2247:8965:da07:fd44:962d	nginx.access.remote_ip: d1e6:d072:6519:2247:8965:da07:fd44:962d	236	1.17	↑ More than 100x higher	filebeat-nginx-access-remote_ip_url_count	
November 23rd 2018	● 99	nginx_access_remote_ip_high_dc_url	72.81.191.85	nginx.access.remote_ip: 72.81.191.85	605	1.11	↑ More than 100x higher	filebeat-nginx-access-remote_ip_url_count	
November 16th 2018	● 99	nginx_access_remote_ip_high_dc_url	154.187.183.112	nginx.access.remote_ip: 154.187.183.112	235	1.17	↑ More than 100x higher	filebeat-nginx-access-remote_ip_url_count	
November 28th 2018	● 99	nginx_access_remote_ip_high_dc_url	2.222.226.74	nginx.access.remote_ip: 2.222.226.74	235	1.21	↑ More than 100x higher	filebeat-nginx-access-remote_ip_url_count	⚙

Review the Remote IP URL Explorer dashboard, note how its view was customized based on the IP for the anomaly (i.e. on the metadata from the ML job on the previous screen)



Dashboard / [Filebeat Nginx] [ML] Remote IP URL Explorer

November 23rd 2018, 00:00:00.000 to November 23rd 2018, 23:59:59.999

>_ *

nginx.access.remote_ip: "72.57.0.53"

Unique Count URL Timechart [Filebeat Nginx] [ML]

Response Code Timechart [Filebeat Nginx] [ML]

Top Remote IPs [Filebeat Nginx] [ML]

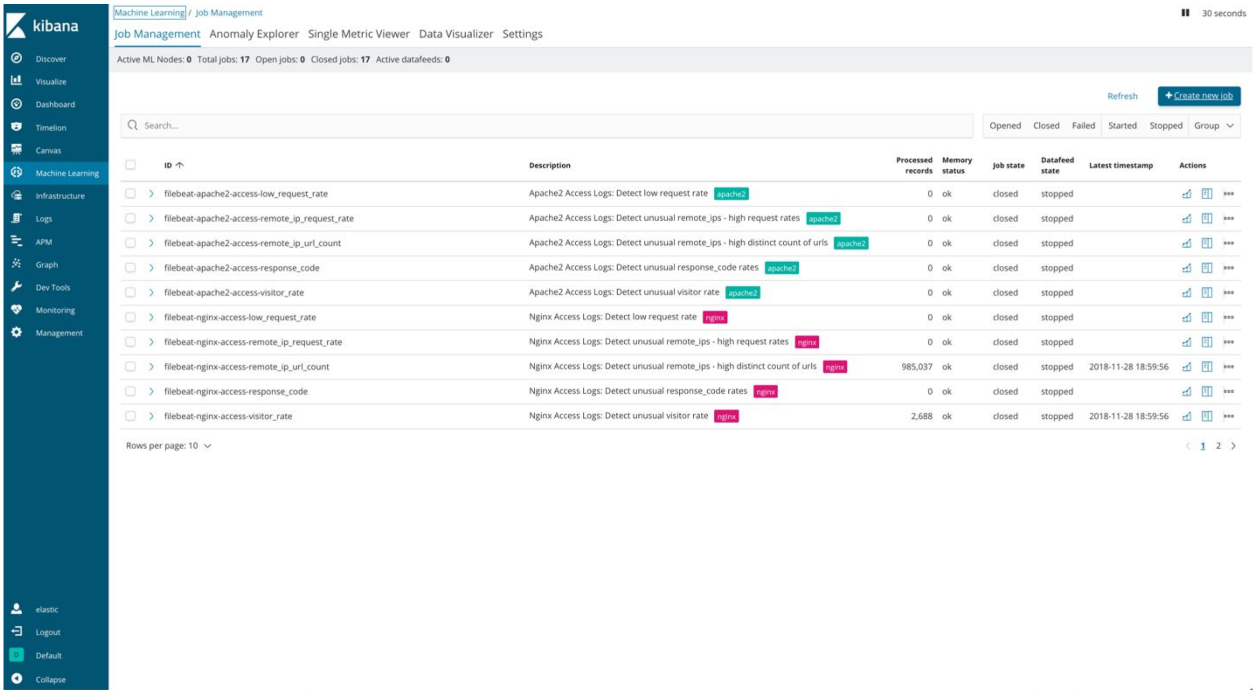
nginx.access.remote_ip: Descending	Count
72.57.0.53	2,884

Access Map [Filebeat Nginx] [ML]

Top URLs [Filebeat Nginx] [ML]

nginx.access.url: Descending	Count
/opt/node_apps/elastic-v5/app/themes/basic/public/static/404.html	694
/de/blog/elasticsearch-5-1-2-and-2-4-4-released	5
/blog/archive/2011/december	4
/about/blog/process-transparency-and-error-categorization-at-1-1-by-using-the-elastic-stack-and-etl	3
/fr/blog/elasticsearch-2-3-0-and-2-2-2-released	3
/jp/blog/elasticsearch-2-3-0-and-2-2-2-released	3

10. (This and next steps are optional) Create your own Single Metrics Machine Learning job. Click on Machine Learning in Kibana menu. Click on Create Job.



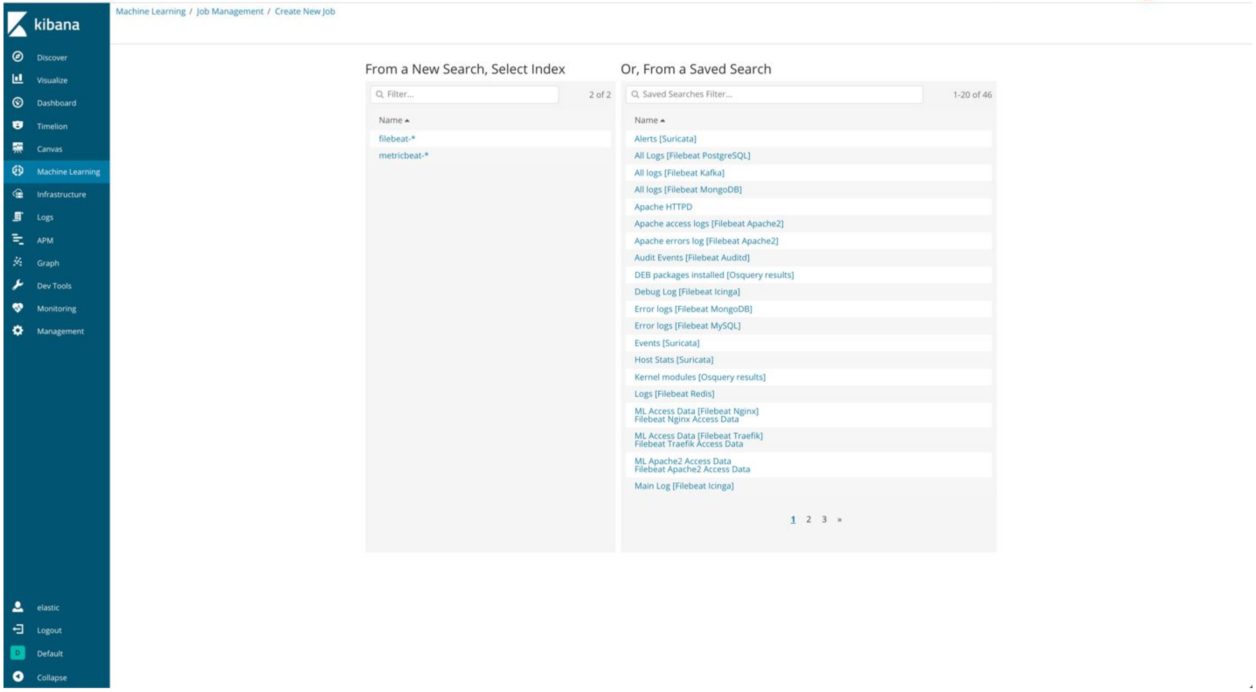
Machine Learning / Job Management

Job Management Anomaly Explorer Single Metric Viewer Data Visualizer Settings

Active ML Nodes: **0** Total jobs: **17** Open jobs: **0** Closed jobs: **17** Active datafeeds: **0**

ID ↑	Description	Processed records	Memory status	Job state	Datafeed state	Latest timestamp
filebeat-apache2-access-low_request_rate	Apache2 Access Logs: Detect low request rate apache2	0	ok	closed	stopped	
filebeat-apache2-access-remote_ip_request_rate	Apache2 Access Logs: Detect unusual remote_ips - high request rates apache2	0	ok	closed	stopped	
filebeat-apache2-access-remote_ip_url_count	Apache2 Access Logs: Detect unusual remote_ips - high distinct count of urls apache2	0	ok	closed	stopped	
filebeat-apache2-access-response_code	Apache2 Access Logs: Detect unusual response_code rates apache2	0	ok	closed	stopped	
filebeat-apache2-access-visitor_rate	Apache2 Access Logs: Detect unusual visitor rate apache2	0	ok	closed	stopped	
filebeat-nginx-access-low_request_rate	Nginx Access Logs: Detect low request rate nginx	0	ok	closed	stopped	
filebeat-nginx-access-remote_ip_request_rate	Nginx Access Logs: Detect unusual remote_ips - high request rates nginx	0	ok	closed	stopped	
filebeat-nginx-access-remote_ip_url_count	Nginx Access Logs: Detect unusual remote_ips - high distinct count of urls nginx	985,037	ok	closed	stopped	2018-11-28 18:59:56
filebeat-nginx-access-response_code	Nginx Access Logs: Detect unusual response_code rates nginx	0	ok	closed	stopped	
filebeat-nginx-access-visitor_rate	Nginx Access Logs: Detect unusual visitor rate nginx	2,688	ok	closed	stopped	2018-11-28 18:59:56

Select “filebeat*” index pattern and click on creating Single metric job.



Machine Learning / Job Management / Create New Job

From a New Search, Select Index

Filter... 2 of 2

Name ▲

- filebeat-*
- metricbeat-*

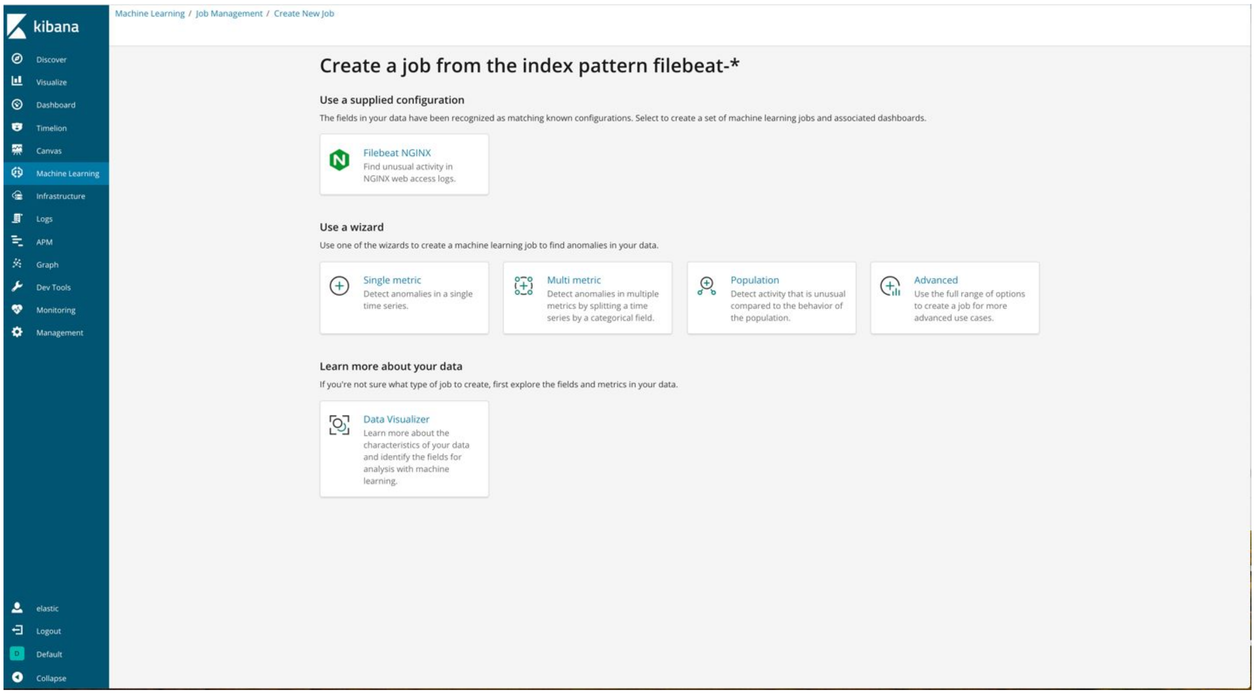
Or, From a Saved Search

Saved Searches Filter... 1-20 of 46

Name ▲

- Alerts [Suricata]
- All Logs [Filebeat PostgreSQL]
- All logs [Filebeat Kafka]
- All logs [Filebeat MongoDB]
- Apache HTTPD
- Apache access logs [Filebeat Apache2]
- Apache errors log [Filebeat Apache2]
- Audit Events [Filebeat Auditd]
- DEB packages installed [Osquery results]
- Debug Log [Filebeat Icinga]
- Error logs [Filebeat MongoDB]
- Error logs [Filebeat MySQL]
- Events [Suricata]
- Host Stats [Suricata]
- Kernel modules [Osquery results]
- Logs [Filebeat Redis]
- ML Access Data [Filebeat Nginx]
Filebeat Nginx Access Data
- ML Access Data [Filebeat Traefik]
Filebeat Traefik Access Data
- ML Apache2 Access Data
Filebeat Apache2 Access Data
- Main Log [Filebeat Icinga]

1 2 3 »



Machine Learning / Job Management / Create New Job

Create a job from the index pattern filebeat-*

Use a supplied configuration

The fields in your data have been recognized as matching known configurations. Select to create a set of machine learning jobs and associated dashboards.

Filebeat NGINX
Find unusual activity in NGINX web access logs.

Use a wizard

Use one of the wizards to create a machine learning job to find anomalies in your data.

Single metric
Detect anomalies in a single time series.

Multi metric
Detect anomalies in multiple metrics by splitting a time series by a categorical field.

Population
Detect activity that is unusual compared to the behavior of the population.

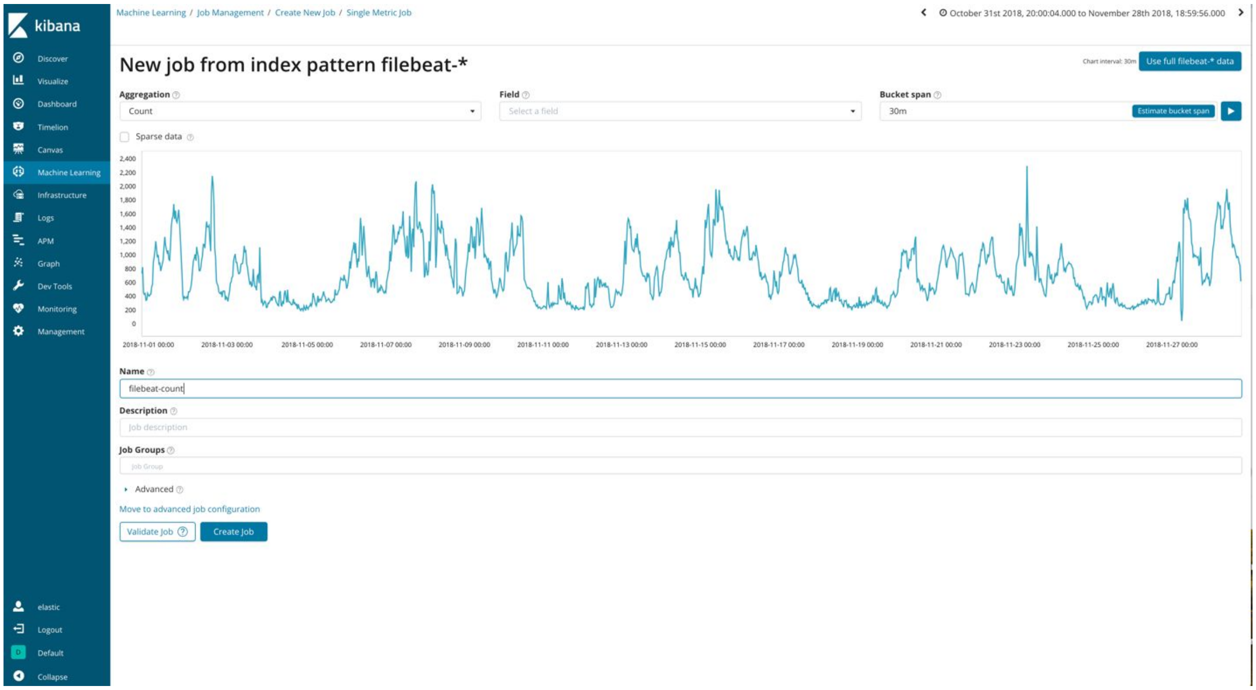
Advanced
Use the full range of options to create a job for more advanced use cases.

Learn more about your data

If you're not sure what type of job to create, first explore the fields and metrics in your data.

Data Visualizer
Learn more about the characteristics of your data and identify the fields for analysis with machine learning.

As function select “count”, leave field blank, set bucket span to 30m and click on “Use full filebeat-* data”. Give your job a name and click on “Create Job”.



New job from index pattern filebeat-*

Aggregation: Count

Field: Select a field

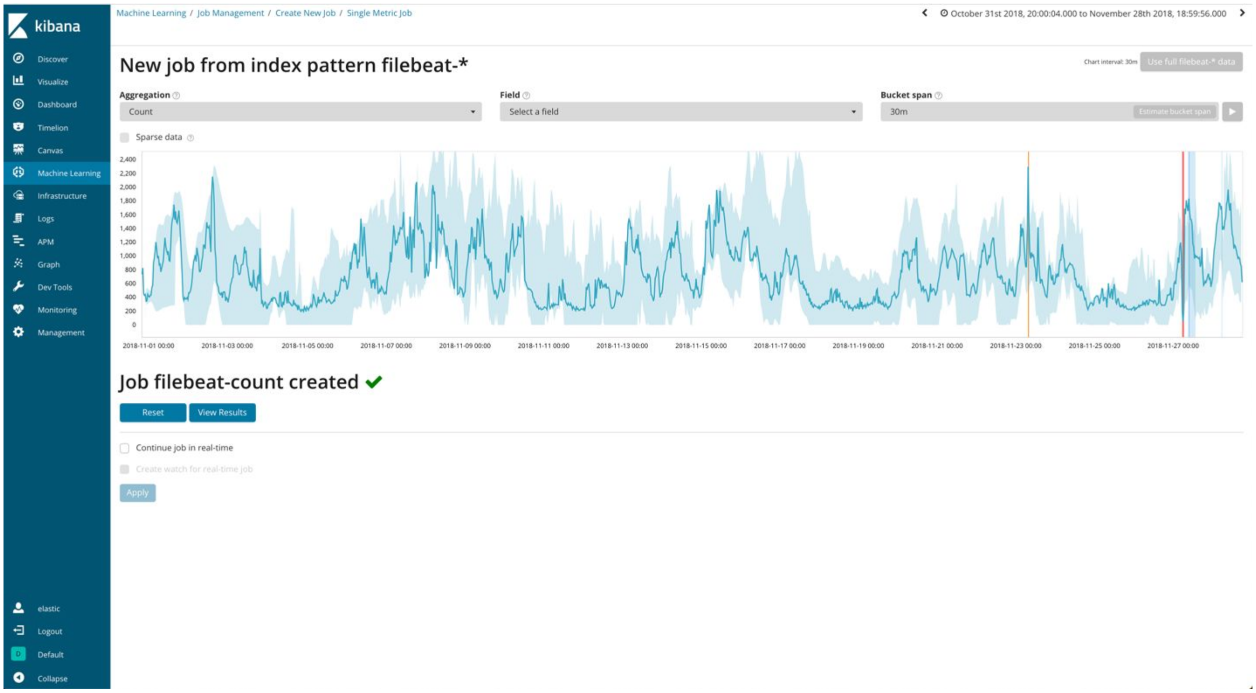
Bucket span: 30m

Name: filebeat-count

Description: Job description

Job Groups: Job Group

After the job completes click on “View Results”.



New job from index pattern filebeat-*

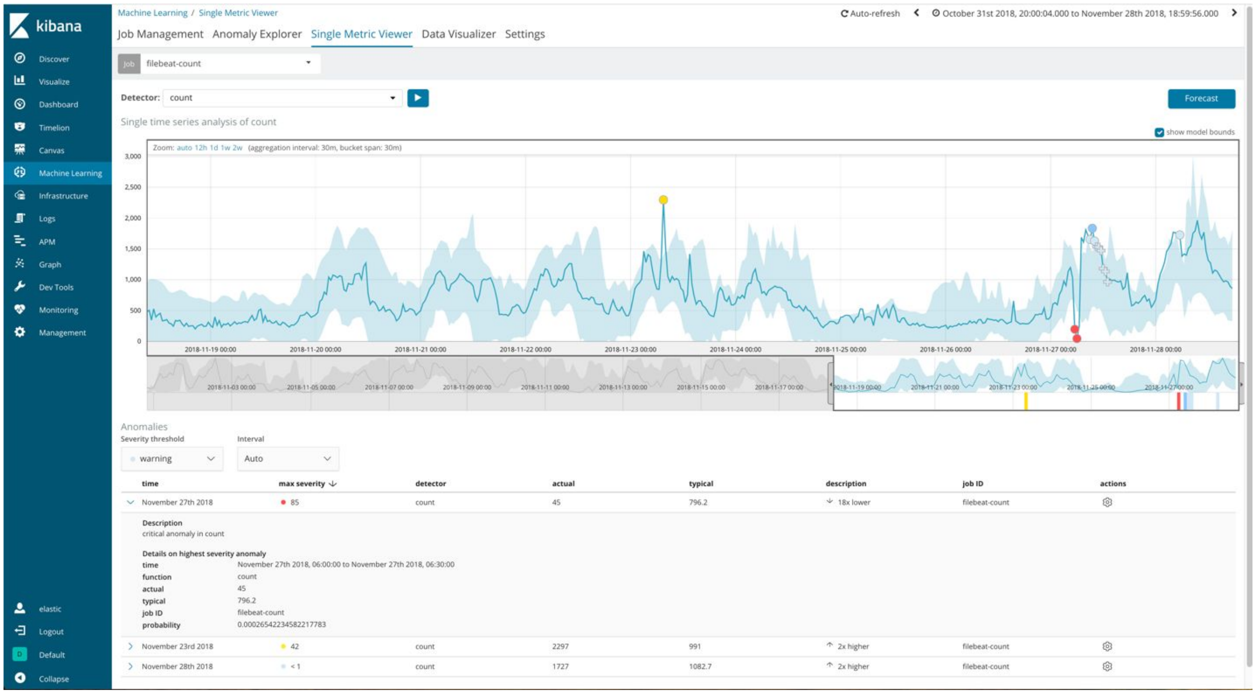
Aggregation: Count

Field: Select a field

Bucket span: 30m

Job filebeat-count created ✓

On the results screen slide the window in the Single Metrics viewer and click on the anomalies. What does this anomaly represent? Remember that we've picked the function count of all events over 30min buckets.



October 31st 2018, 20:00:04.000 to November 28th 2018, 18:59:56.000

Job: filebeat-count

Detector: count

Single time series analysis of count

(aggregation interval: 30m, bucket span: 30m)

Anomalies

Severity threshold: warning

Interval: Auto

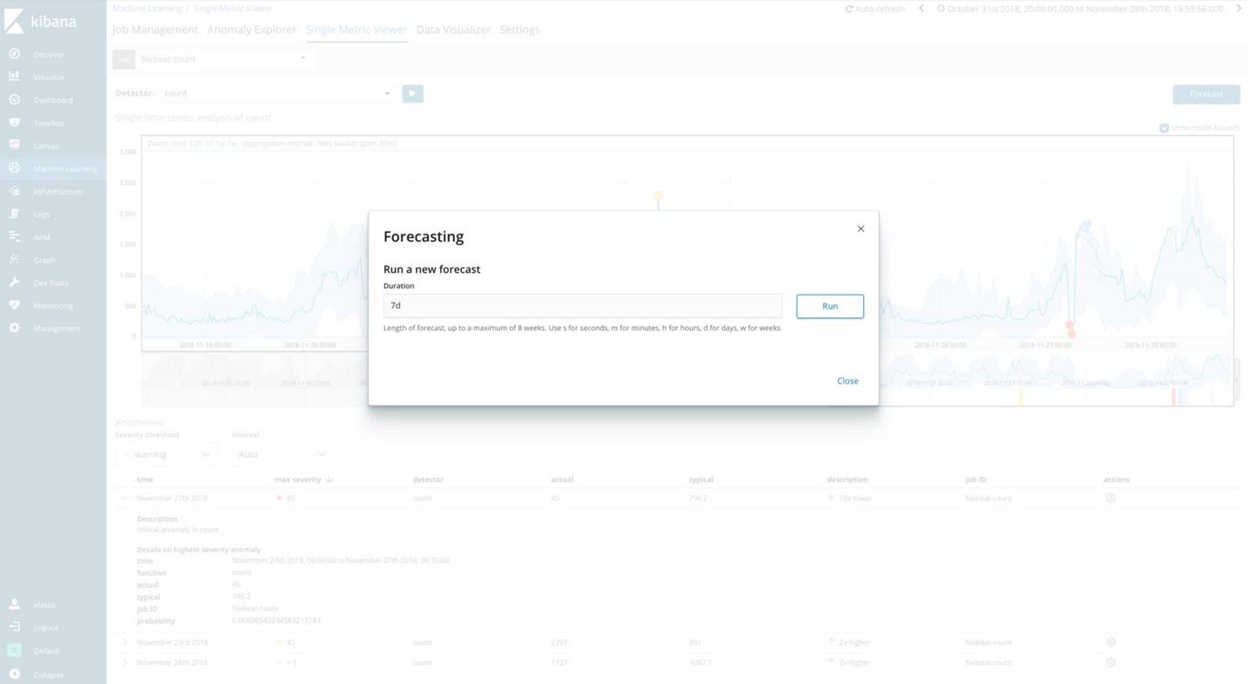
time	max severity	detector	actual	typical	description	job ID	actions
November 27th 2018	● 85	count	45	796.2	↓ 18x lower	filebeat-count	⚙
November 23rd 2018	● 42	count	2297	991	↑ 2x higher	filebeat-count	⚙
November 28th 2018	● < 1	count	1727	1082.7	↑ 2x higher	filebeat-count	⚙

Description
critical anomaly in count

Details on highest severity anomaly

time	November 27th 2018, 06:00:00 to November 27th 2018, 06:30:00
function	count
actual	45
typical	796.2
job ID	filebeat-count
probability	0.00026542234582217783

Click on Forecast button and give it a length of 7d and click on Run.



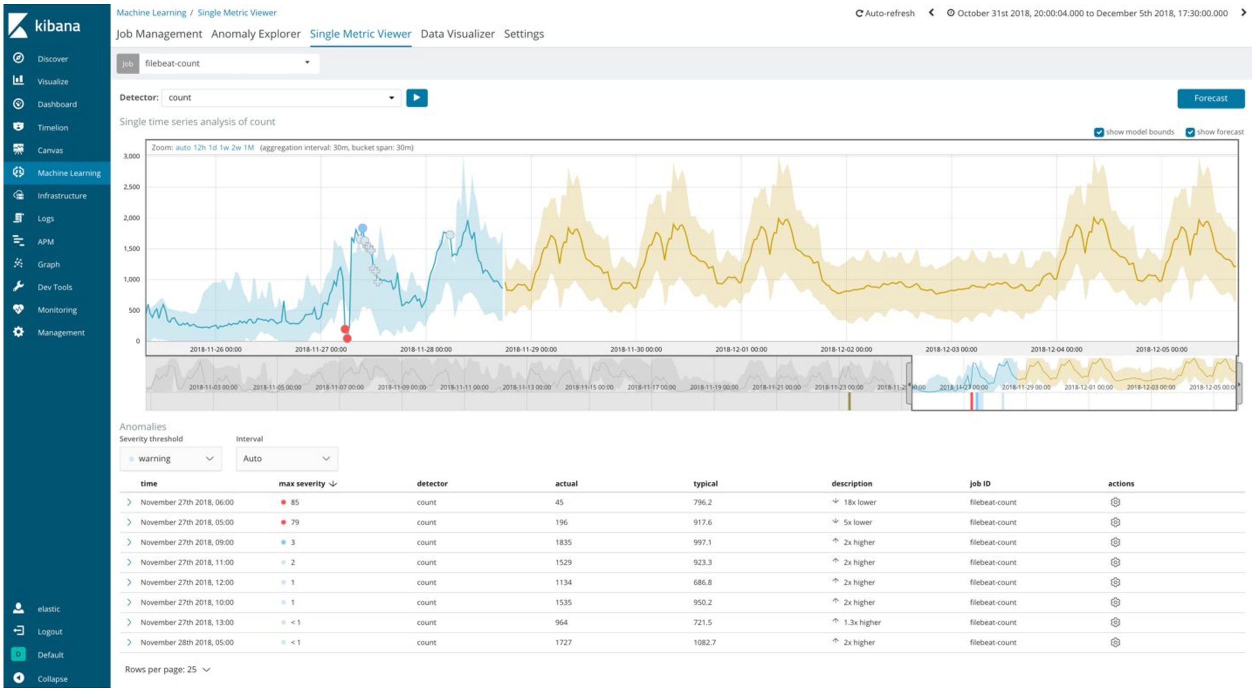
Forecasting

Run a new forecast

Duration: 7d

Length of forecast, up to a maximum of 8 weeks. Use s for seconds, m for minutes, h for hours, d for days, w for weeks.

View the forecasting result. The forecast part of the metrics and the model is in brown.



October 31st 2018, 20:00:04.000 to December 5th 2018, 17:30:00.000

Job: filebeat-count

Detector: count

Single time series analysis of count

(aggregation interval: 30m, bucket span: 30m)

Anomalies

Severity threshold: warning

Interval: Auto

time	max severity	detector	actual	typical	description	job ID	actions
November 27th 2018, 06:00	● 85	count	45	796.2	↓ 18x lower	filebeat-count	
November 27th 2018, 05:00	● 79	count	196	917.6	↓ 5x lower	filebeat-count	
November 27th 2018, 09:00	● 3	count	1835	997.1	↑ 2x higher	filebeat-count	
November 27th 2018, 11:00	● 2	count	1529	923.3	↑ 2x higher	filebeat-count	
November 27th 2018, 12:00	● 1	count	1134	686.8	↑ 2x higher	filebeat-count	
November 27th 2018, 10:00	● 1	count	1535	950.2	↑ 2x higher	filebeat-count	
November 27th 2018, 13:00	● < 1	count	964	721.5	↑ 1.3x higher	filebeat-count	
November 28th 2018, 05:00	● < 1	count	1727	1082.7	↑ 2x higher	filebeat-count	