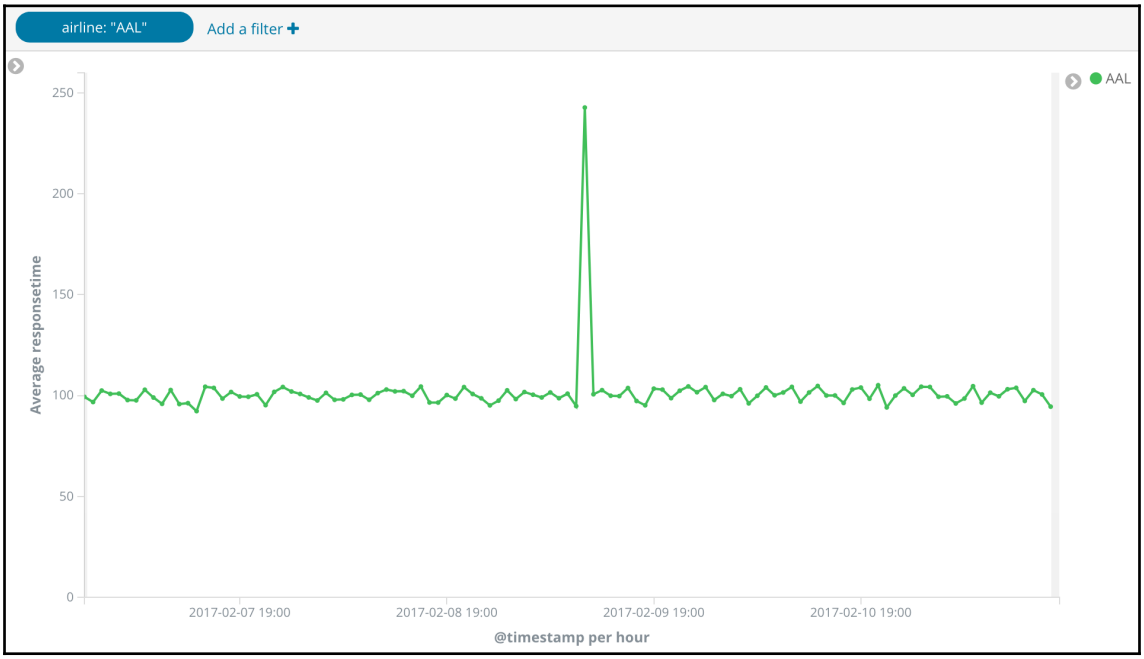
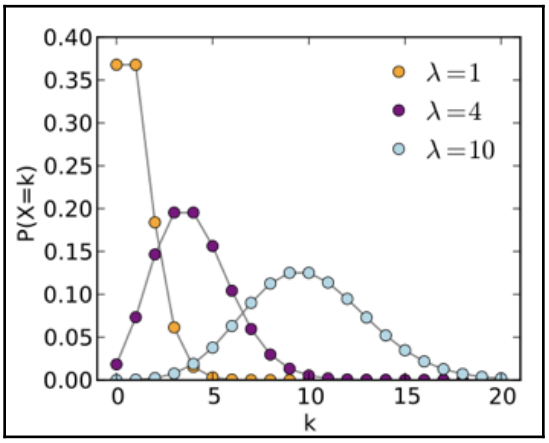
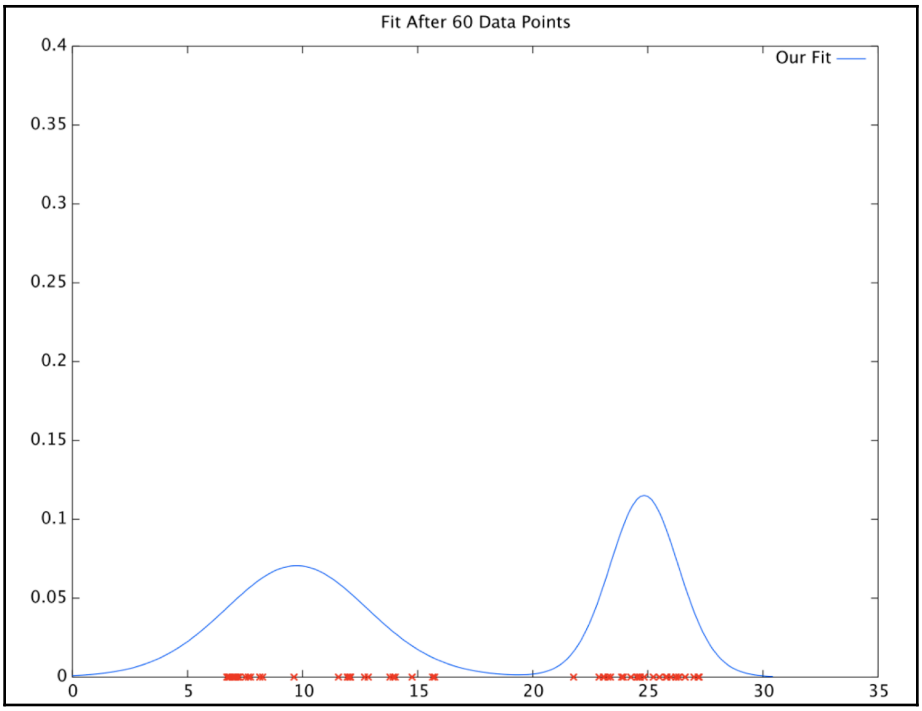
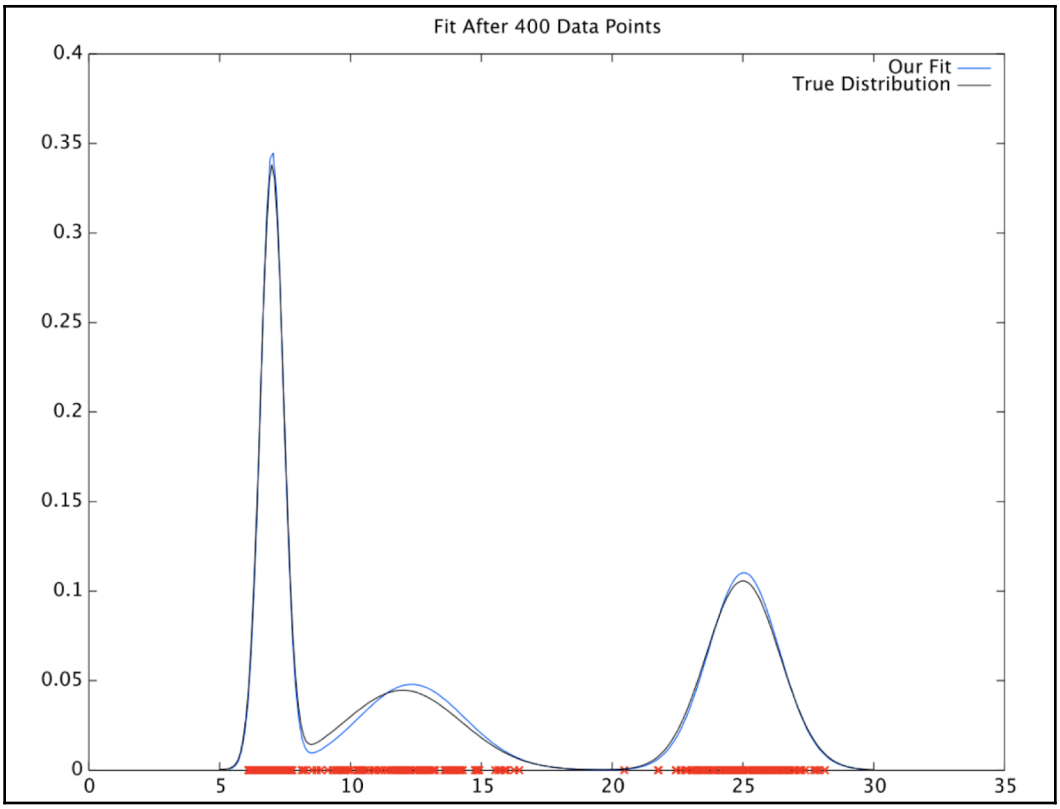
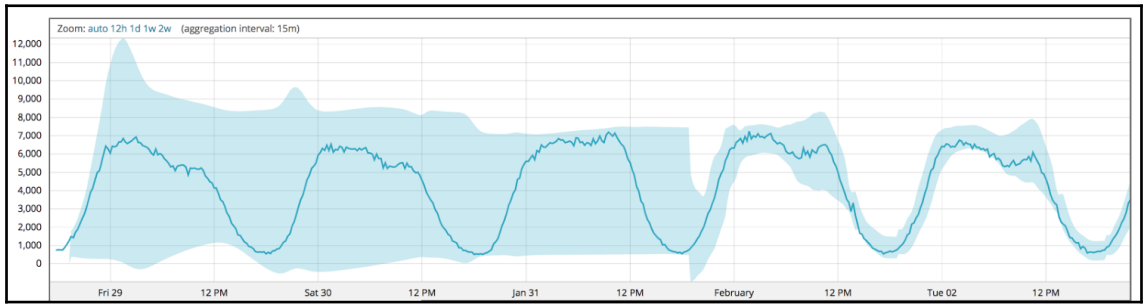
Chapter 1: Machine Learning for IT



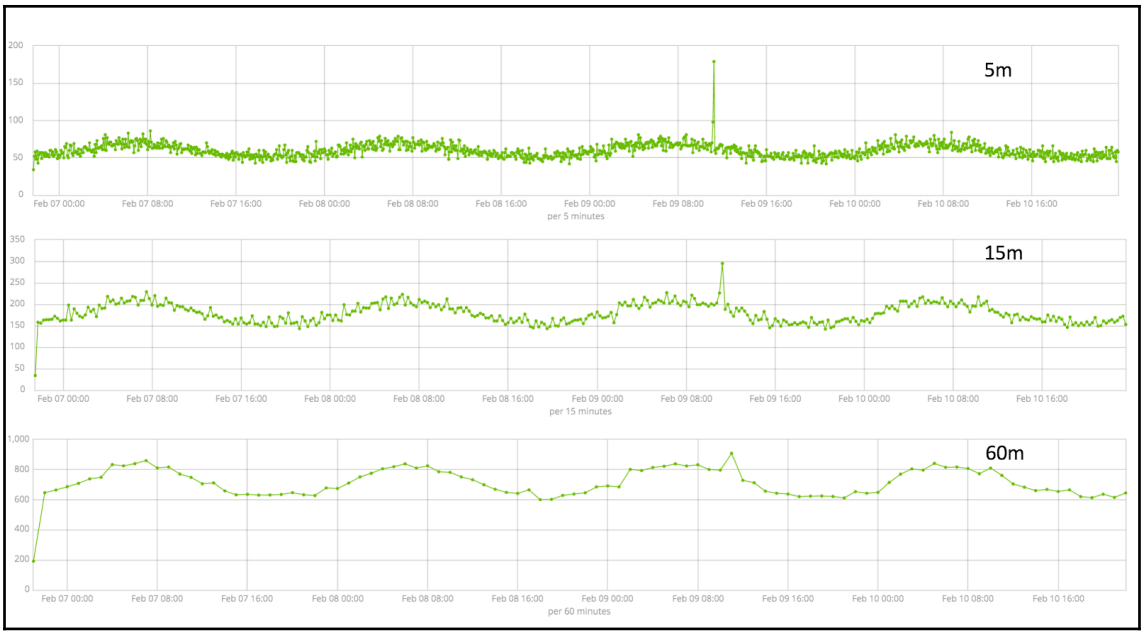

0.40
0.35
0.30
0.25
0.20
0.15
0.10
0.05
0.00
P(X=k)
0
5
10
15
20
k
λ=1
λ=4
λ=10

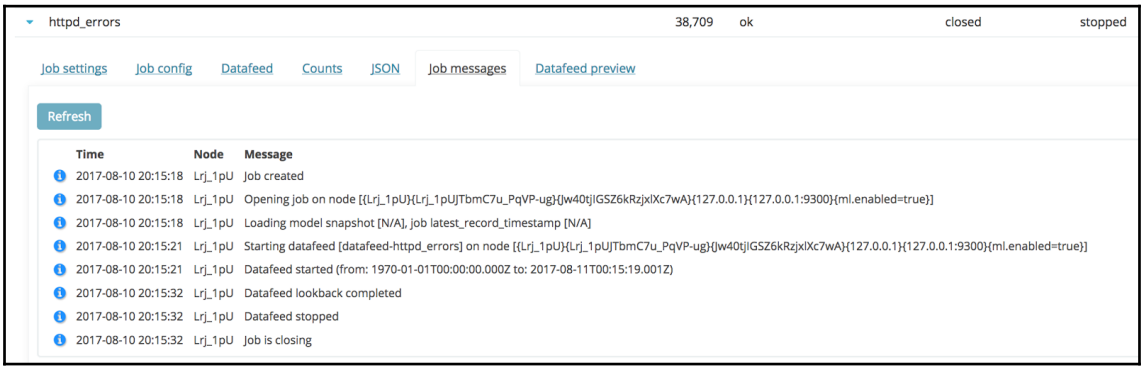

Fit After 60 Data Points
Our Fit
0.4
0.35
0.3
0.25
0.2
0.15
0.1
0.05
0
0
5
10
15
20
25
30
35

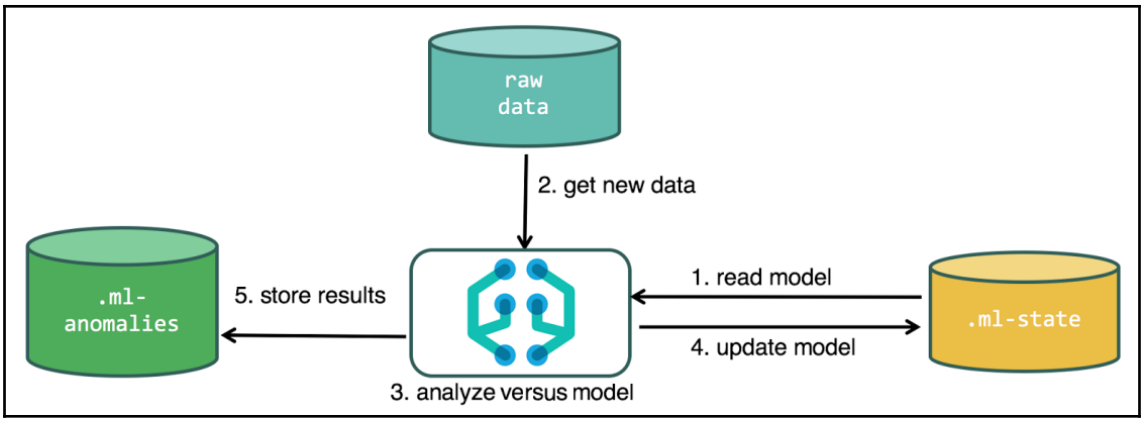

Fit After 400 Data Points
Our Fit
True Distribution
0.4
0.35
0.3
0.25
0.2
0.15
0.1
0.05
0
0
5
10
15
20
25
30
35


Zoom: auto 12h 1d 1w 2w (aggregation interval: 15m)
12,000
11,000
10,000
9,000
8,000
7,000
6,000
5,000
4,000
3,000
2,000
1,000
0
Fri 29
12 PM
Sat 30
12 PM
Jan 31
12 PM
February
12 PM
Tue 02
12 PM

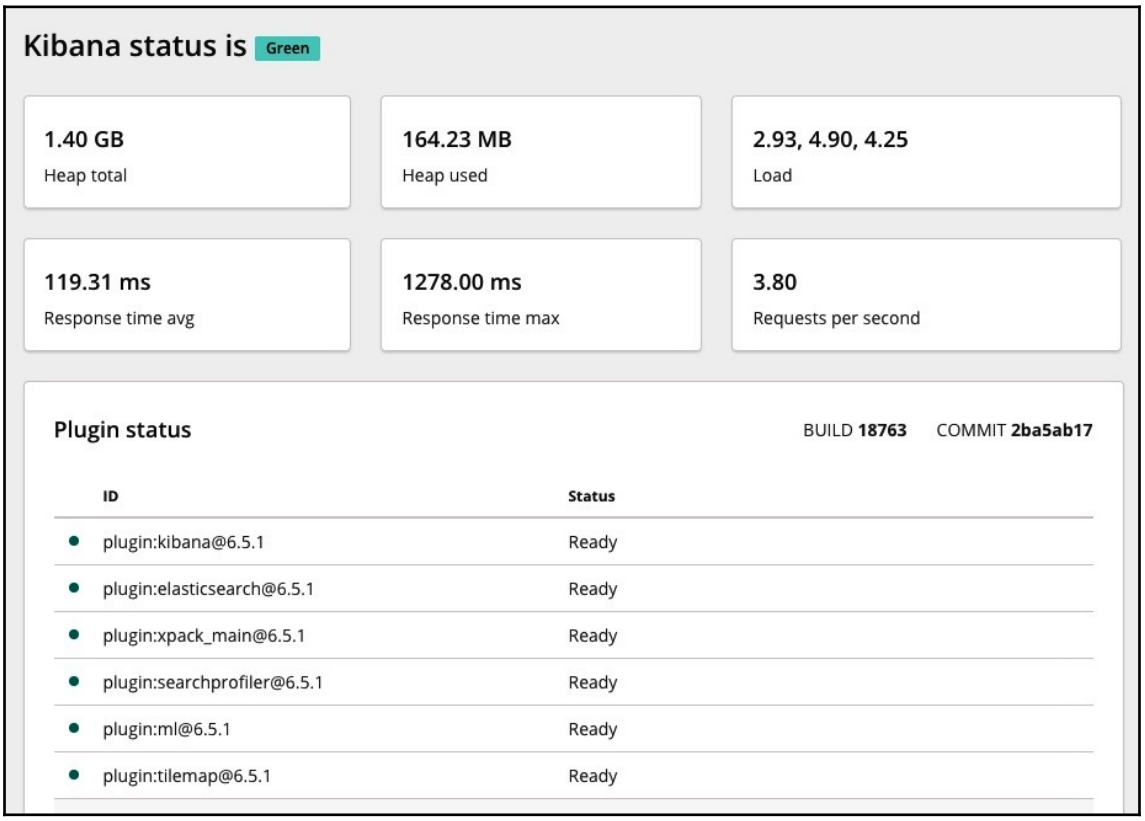

```
top - 11:56:59 up 26 min,  1 user,  load average: 0.06, 0.18, 0.48
Tasks:  91 total,   1 running,  90 sleeping,   0 stopped,   0 zombie
Cpu0  :  0.0%us,  0.0%sy,  0.0%ni,100.0%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu1  :  0.3%us,  0.0%sy,  0.0%ni, 99.7%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu2  :  0.7%us,  0.0%sy,  0.0%ni, 99.3%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu3  :  0.3%us,  0.0%sy,  0.0%ni, 99.7%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:  15405348k total, 10182940k used,  5222408k free,    59148k buffers
Swap:        0k total,        0k used,        0k free,   813512k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 1835 ec2-user  20   0 15.1g 8.8g 214m S  1.0 59.9   6:39.09 /usr/lib/jvm/java/bin/java -Xms8g -Xmx8g -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOcc
 1863 ec2-user  20   0 1276m 145m  20m S  1.0  1.0   0:25.73 /opt/elastic/ml/kibana/bin/../node/bin/node --no-warnings /opt/elastic/ml/kibana/bin/
 1958 ec2-user  20   0  138m 8224 7536 S  0.0  0.1   0:06.72 /opt/elastic/ml/elasticsearch/plugins/x-pack/platform/linux-x86_64/bin/controller
 2016 ec2-user  20   0  115m 3936 2840 S  0.0  0.0   0:00.06 sshd: ec2-user@pts/0
 2017 ec2-user  20   0  112m 3356 2876 S  0.0  0.0   0:00.01 -bash
 2060 ec2-user  20   0 15308 2132 1820 R  0.0  0.0   0:01.68 top
 2349 ec2-user  20   0 90388  26m  16m S  0.0  0.2   0:00.08 ./autodetect --jobid=weblogs --licenseValidation=846052866894315 --bucketspan=900 --l
```

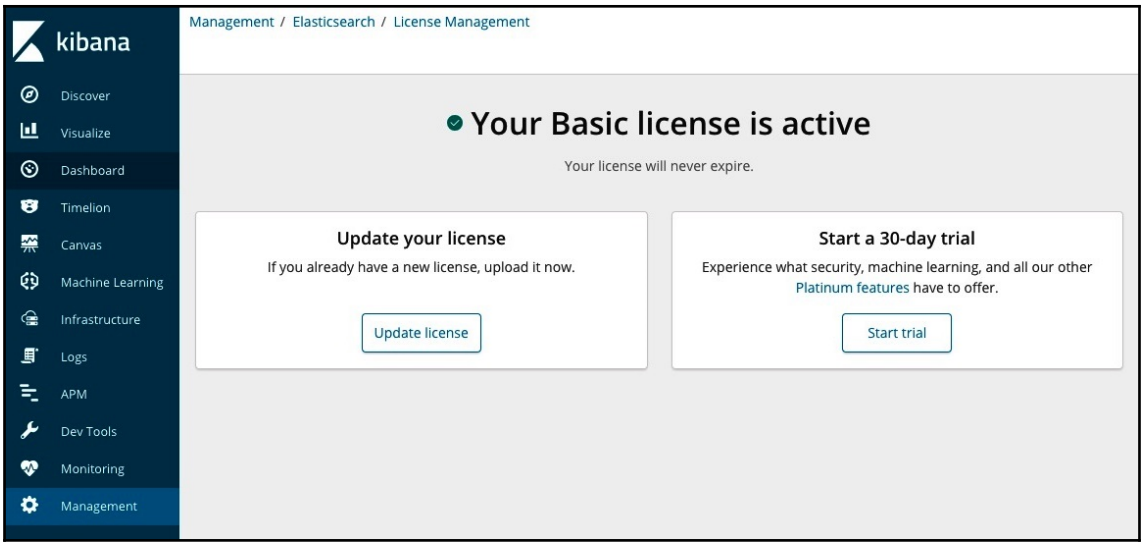

5m
15m
60m
per 5 minutes
per 15 minutes
per 60 minutes

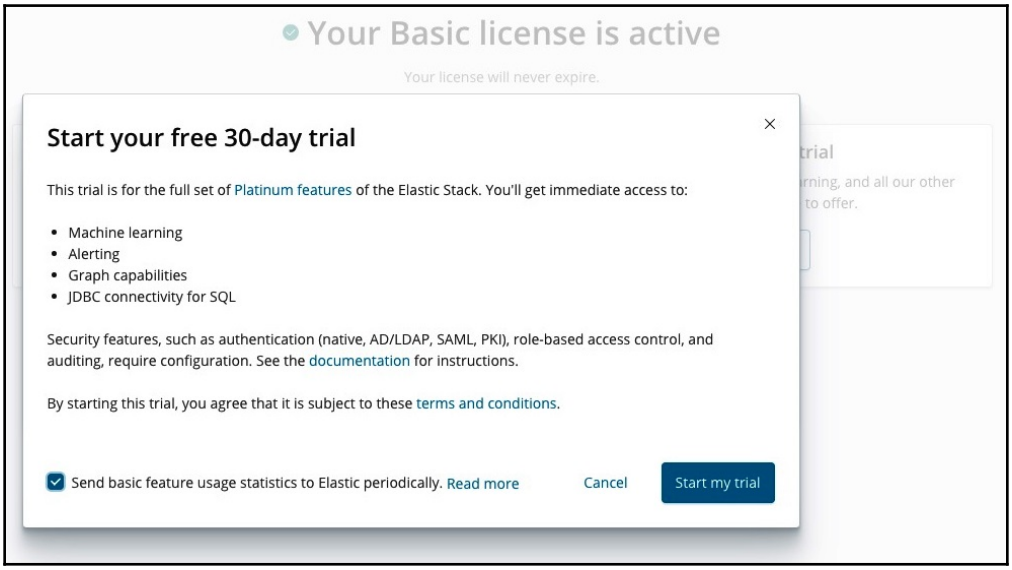

httpd_errors
38,709
ok
closed
stopped
Job settings
Job config
Datafeed
Counts
JSON
Job messages
Datafeed preview
Refresh
Time
Node
Message
2017-08-10 20:15:18 Lrj_1pU Job created
2017-08-10 20:15:18 Lrj_1pU Opening job on node [{Lrj_1pU}{Lrj_1pUJTbmC7u_PqVP-ug}{jw40tjIGSZ6kRzjxlXc7wA}{127.0.0.1}{127.0.0.1:9300}{ml.enabled=true}]
2017-08-10 20:15:18 Lrj_1pU Loading model snapshot [N/A], job latest_record_timestamp [N/A]
2017-08-10 20:15:21 Lrj_1pU Starting datafeed [datafeed-httpd_errors] on node [{Lrj_1pU}{Lrj_1pUJTbmC7u_PqVP-ug}{jw40tjIGSZ6kRzjxlXc7wA}{127.0.0.1}{127.0.0.1:9300}{ml.enabled=true}]
2017-08-10 20:15:21 Lrj_1pU Datafeed started (from: 1970-01-01T00:00:00.000Z to: 2017-08-11T00:15:19.001Z)
2017-08-10 20:15:32 Lrj_1pU Datafeed lookback completed
2017-08-10 20:15:32 Lrj_1pU Datafeed stopped
2017-08-10 20:15:32 Lrj_1pU Job is closing

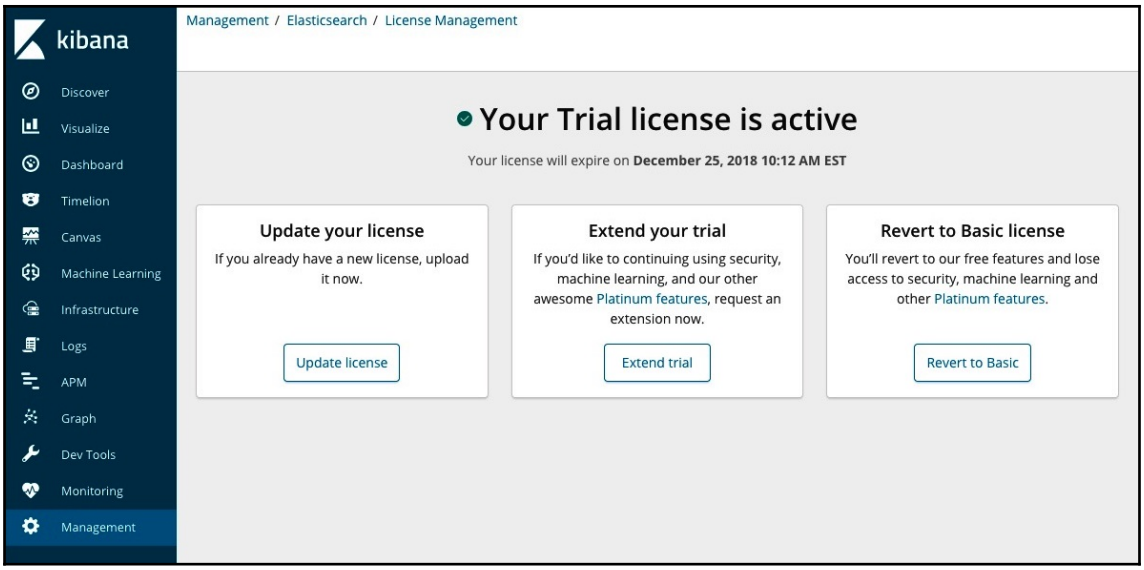

raw
data
2. get new data
.ml-
anomalies
5. store results
1. read model
.ml-state
4. update model
3. analyze versus model

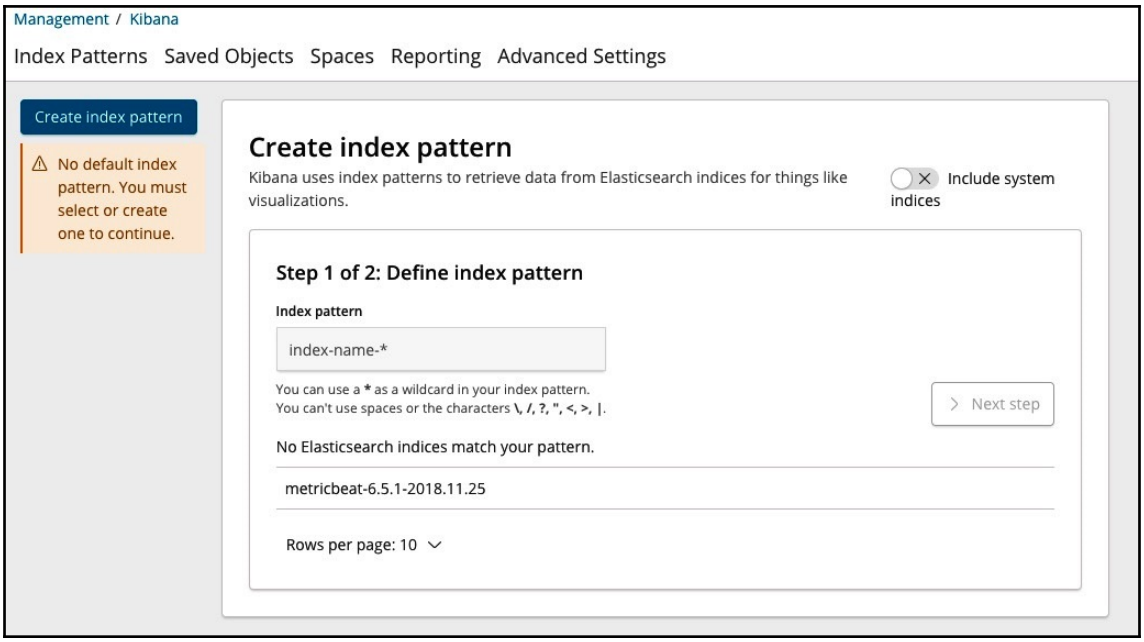
Chapter 2: Installing the Elastic Stack with Machine Learning

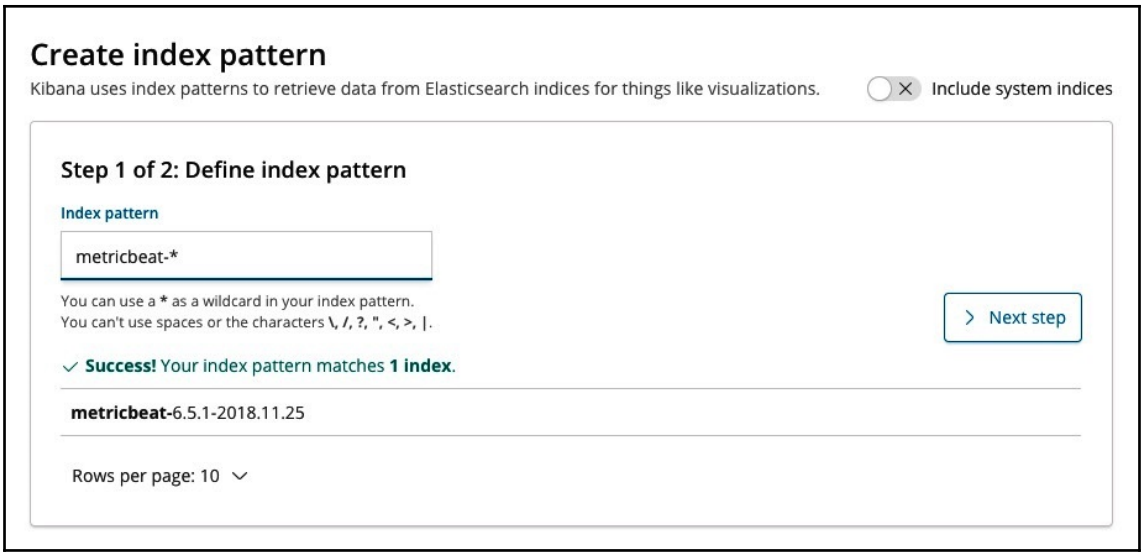


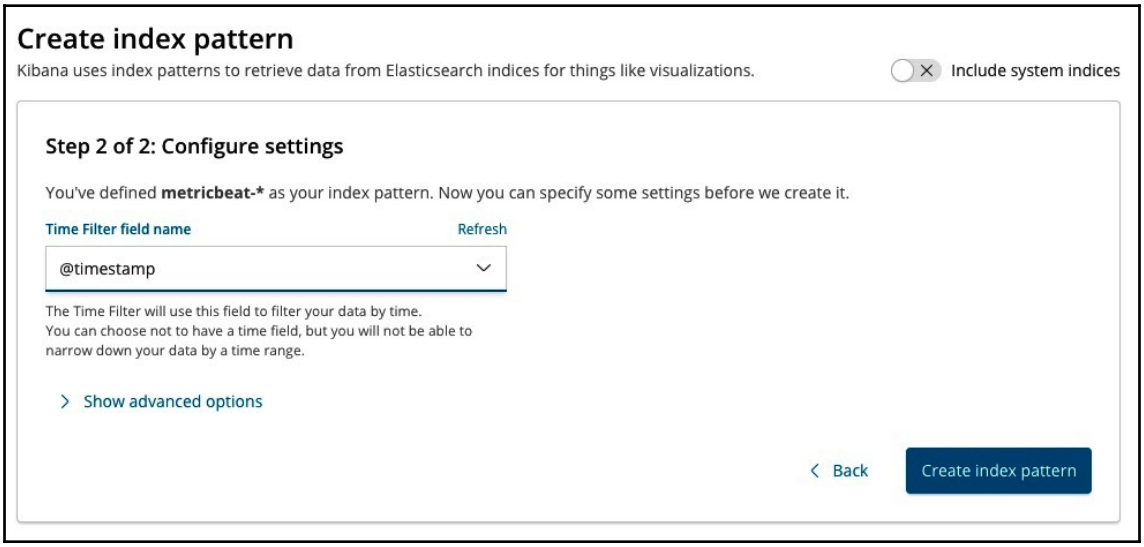

kibana
Discover
Visualize
Dashboard
Timelion
Canvas
Machine Learning
Infrastructure
Logs
APM
Dev Tools
Monitoring
Management
Management / Elasticsearch / License Management
Your Basic license is active
Your license will never expire.
Update your license
If you already have a new license, upload it now.
Update license
Start a 30-day trial
Experience what security, machine learning, and all our other Platinum features have to offer.
Start trial

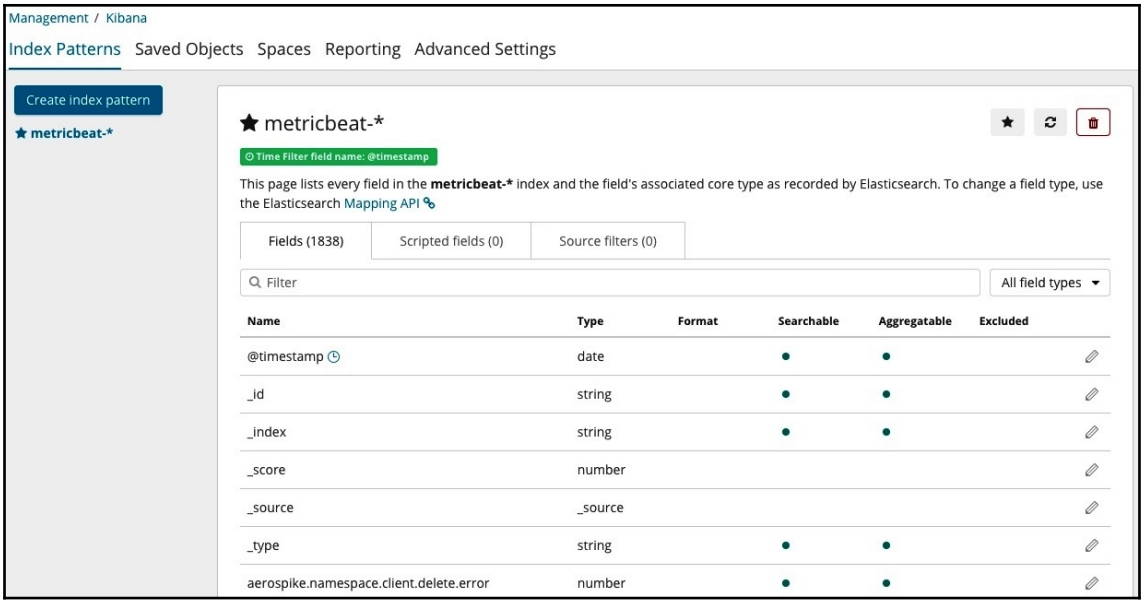

Your Basic license is active
Your license will never expire.
Start your free 30-day trial
This trial is for the full set of Platinum features of the Elastic Stack. You'll get immediate access to:
Machine learning
Alerting
Graph capabilities
JDBC connectivity for SQL
Security features, such as authentication (native, AD/LDAP, SAML, PKI), role-based access control, and auditing, require configuration. See the documentation for instructions.
By starting this trial, you agree that it is subject to these terms and conditions.
Send basic feature usage statistics to Elastic periodically. Read more
Cancel
Start my trial

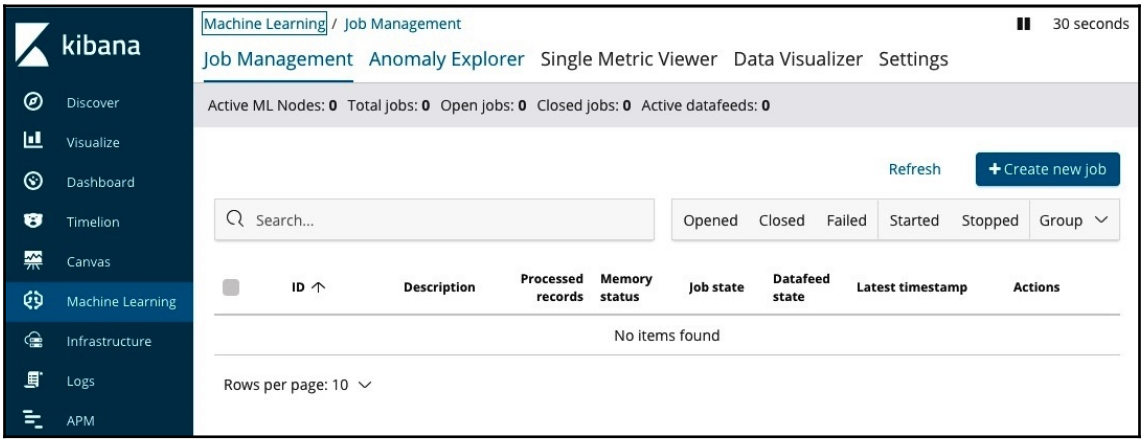

kibana
Discover
Visualize
Dashboard
Timelion
Canvas
Machine Learning
Infrastructure
Logs
APM
Graph
Dev Tools
Monitoring
Management
Management / Elasticsearch / License Management
Your Trial license is active
Your license will expire on December 25, 2018 10:12 AM EST
Update your license
If you already have a new license, upload it now.
Update license
Extend your trial
If you'd like to continuing using security, machine learning, and our other awesome Platinum features, request an extension now.
Extend trial
Revert to Basic license
You'll revert to our free features and lose access to security, machine learning and other Platinum features.
Revert to Basic

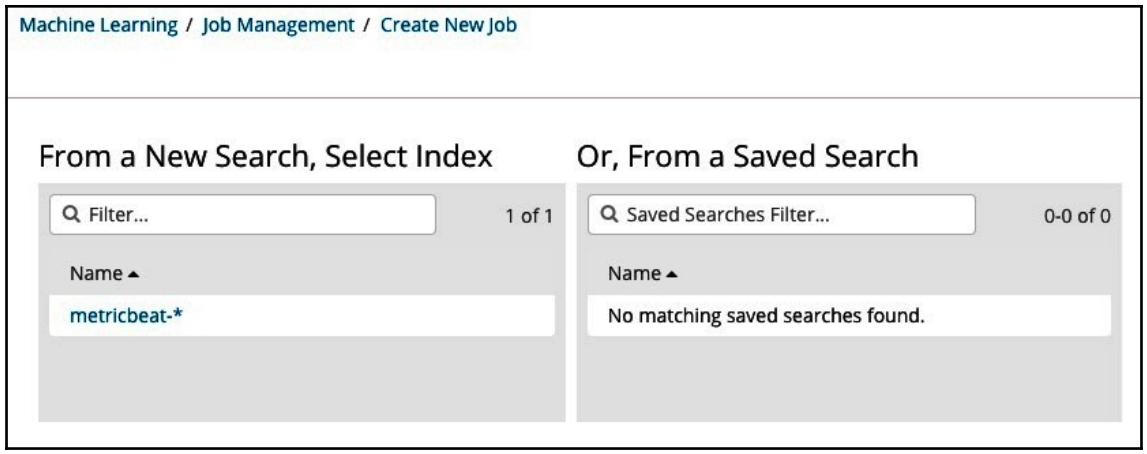

Management / Kibana
Index Patterns
Saved Objects
Spaces
Reporting
Advanced Settings
Create index pattern
No default index pattern. You must select or create one to continue.
Create index pattern
Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.
Include system indices
Step 1 of 2: Define index pattern
Index pattern
index-name-*
You can use a * as a wildcard in your index pattern.
You can't use spaces or the characters \, /, ?, ", <, >, |.
Next step
No Elasticsearch indices match your pattern.
metricbeat-6.5.1-2018.11.25
Rows per page: 10

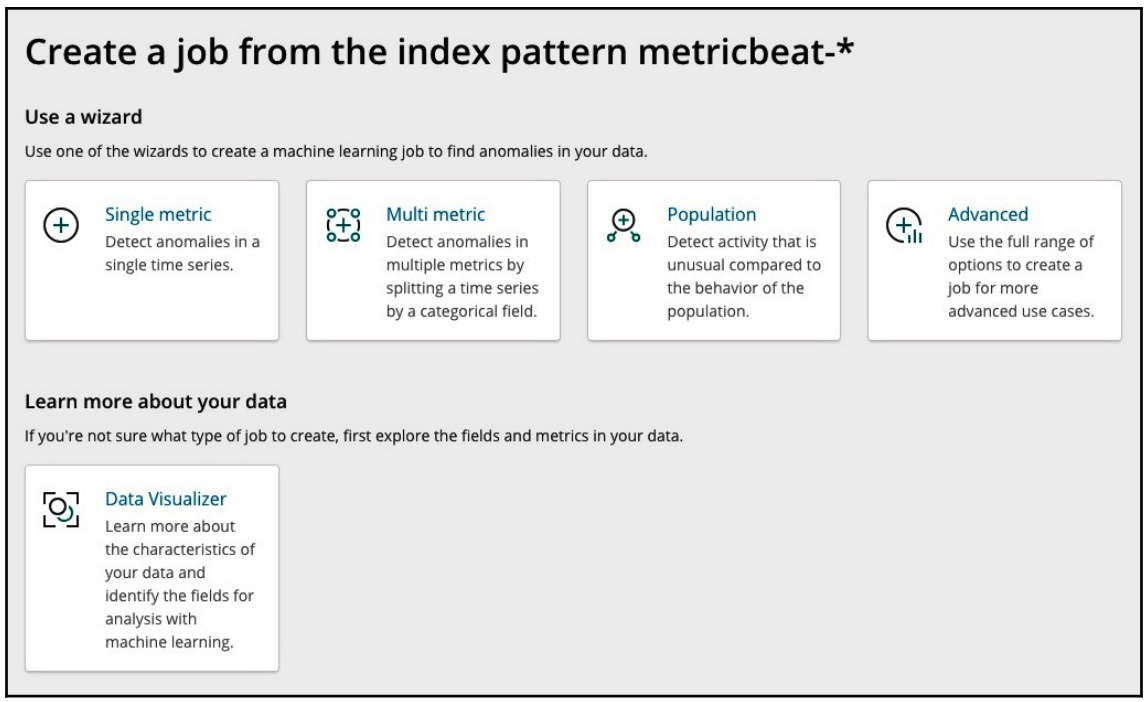

Create index pattern
Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.
Include system indices
Step 1 of 2: Define index pattern
Index pattern
metricbeat-*
You can use a * as a wildcard in your index pattern.
You can't use spaces or the characters \, /, ?, ", <, >, |.
Next step
Success! Your index pattern matches 1 index.
metricbeat-6.5.1-2018.11.25
Rows per page: 10

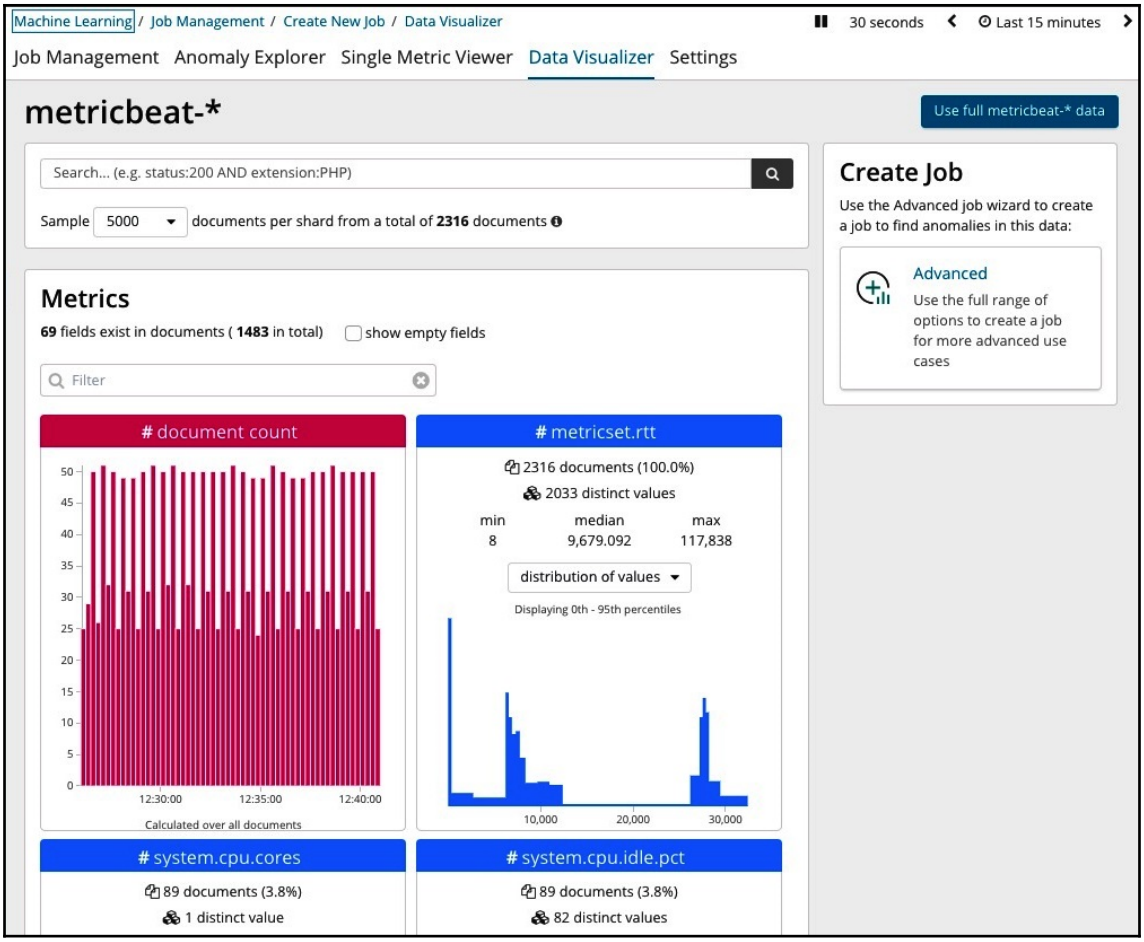

Create index pattern
Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.
Include system indices
Step 2 of 2: Configure settings
You've defined metricbeat-* as your index pattern. Now you can specify some settings before we create it.
Time Filter field name
Refresh
@timestamp
The Time Filter will use this field to filter your data by time.
You can choose not to have a time field, but you will not be able to narrow down your data by a time range.
Show advanced options
Back
Create index pattern

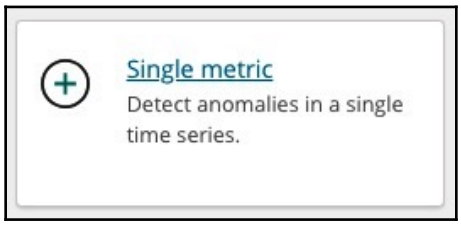

Management / Kibana
Index Patterns
Saved Objects
Spaces
Reporting
Advanced Settings
Create index pattern
metricbeat-*
metricbeat-*
Time Filter field name: @timestamp
This page lists every field in the metricbeat-* index and the field's associated core type as recorded by Elasticsearch. To change a field type, use the Elasticsearch Mapping API
Fields (1838)
Scripted fields (0)
Source filters (0)
Filter
All field types
Name
Type
Format
Searchable
Aggregatable
Excluded
@timestamp
date
_id
string
_index
string
_score
number
_source
_source
_type
string
aerospike.namespace.client.delete.error
number


kibana
Discover
Visualize
Dashboard
Timelion
Canvas
Machine Learning
Infrastructure
Logs
APM
Machine Learning / Job Management
30 seconds
Job Management
Anomaly Explorer
Single Metric Viewer
Data Visualizer
Settings
Active ML Nodes: 0 Total jobs: 0 Open jobs: 0 Closed jobs: 0 Active datafeeds: 0
Refresh
+ Create new job
Search...
Opened
Closed
Failed
Started
Stopped
Group
ID
Description
Processed records
Memory status
Job state
Datafeed state
Latest timestamp
Actions
No items found
Rows per page: 10

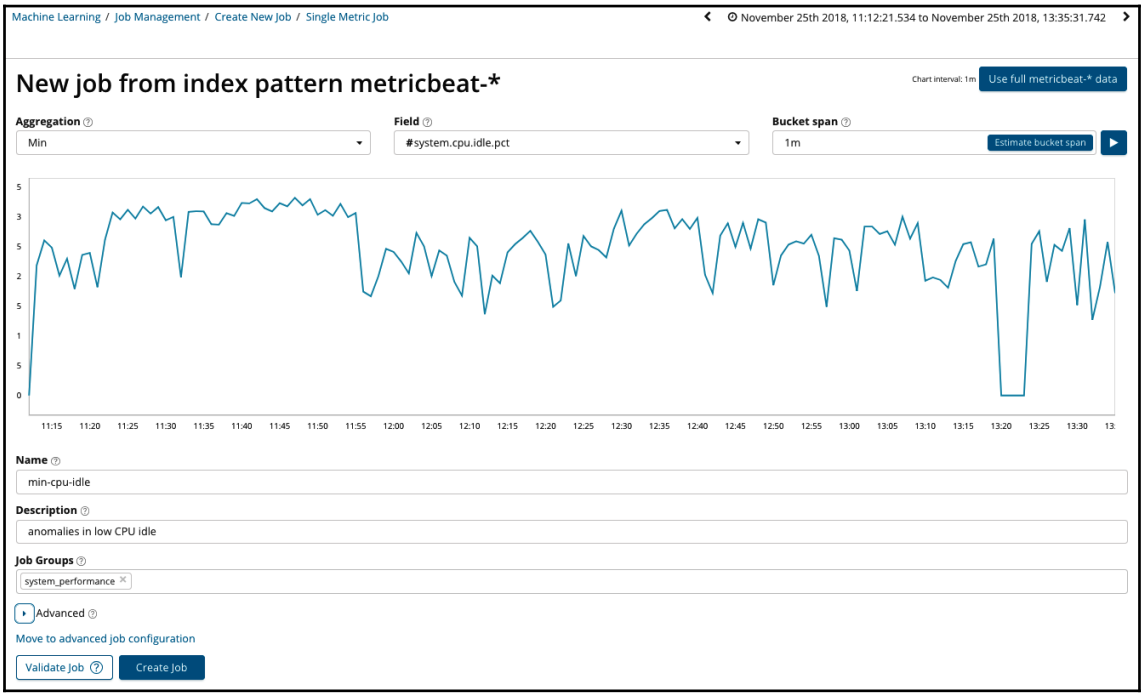

Machine Learning / Job Management / Create New Job
From a New Search, Select Index
Filter...
1 of 1
Name
metricbeat-*
Or, From a Saved Search
Saved Searches Filter...
0-0 of 0
Name
No matching saved searches found.

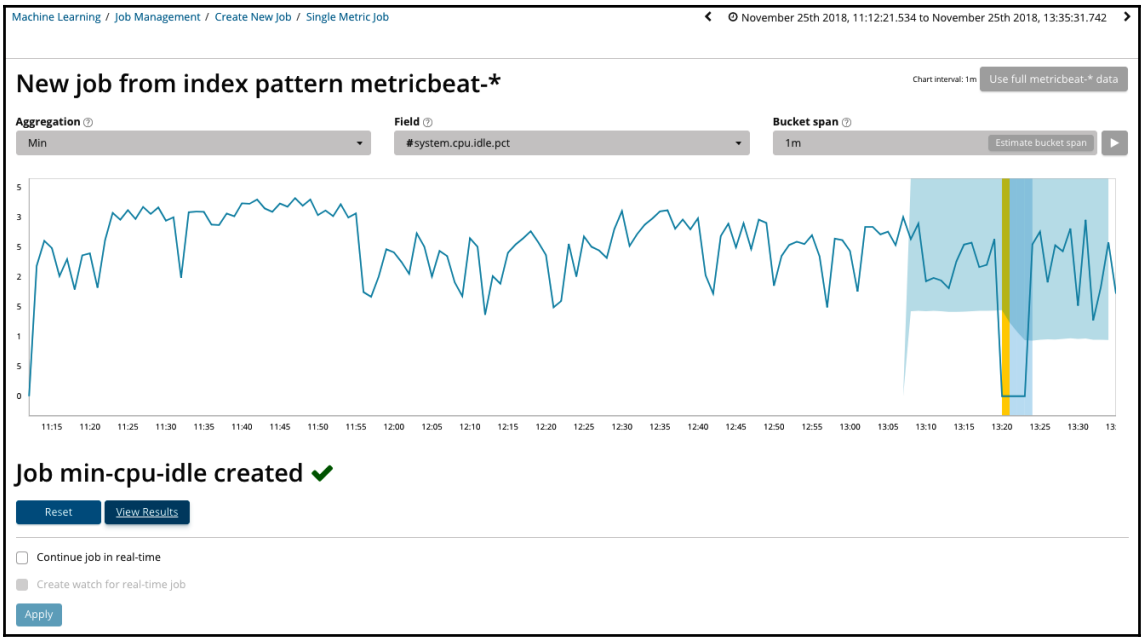

Create a job from the index pattern metricbeat-*
Use a wizard
Use one of the wizards to create a machine learning job to find anomalies in your data.
Single metric
Detect anomalies in a single time series.
Multi metric
Detect anomalies in multiple metrics by splitting a time series by a categorical field.
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.

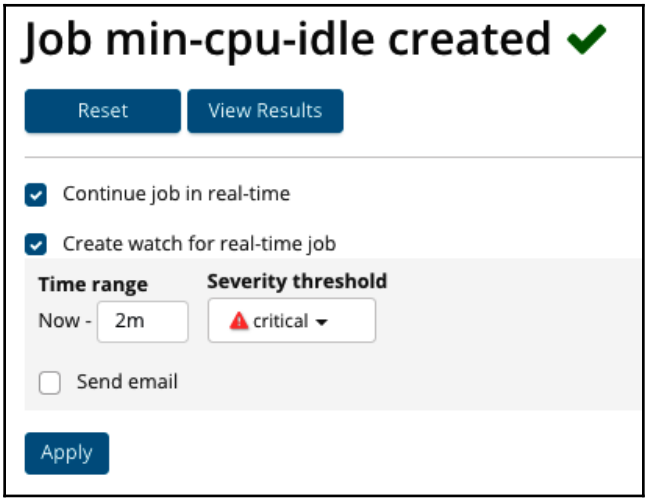

Machine Learning / Job Management / Create New Job / Data Visualizer
30 seconds
Last 15 minutes
Job Management
Anomaly Explorer
Single Metric Viewer
Data Visualizer
Settings
metricbeat-*
Use full metricbeat-* data
Search... (e.g. status:200 AND extension:PHP)
Sample 5000 documents per shard from a total of 2316 documents
Create Job
Use the Advanced job wizard to create a job to find anomalies in this data:
Advanced
Use the full range of options to create a job for more advanced use cases
Metrics
69 fields exist in documents (1483 in total)
show empty fields
Filter
document count
50
45
40
35
30
25
20
15
10
5
0
12:30:00
12:35:00
12:40:00
Calculated over all documents
metricset.rtt
2316 documents (100.0%)
2033 distinct values
min
8
median
9,679.092
max
117,838
distribution of values
Displaying 0th - 95th percentiles
10,000
20,000
30,000
system.cpu.cores
89 documents (3.8%)
1 distinct value
system.cpu.idle.pct
89 documents (3.8%)
82 distinct values

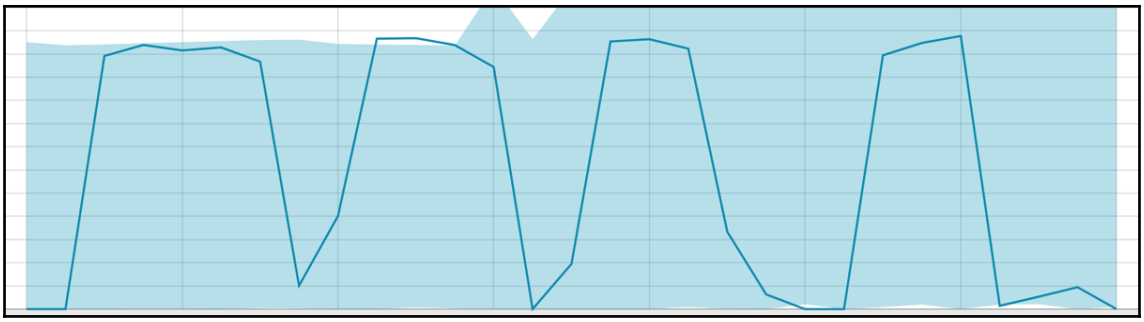

Single metric
Detect anomalies in a single time series.

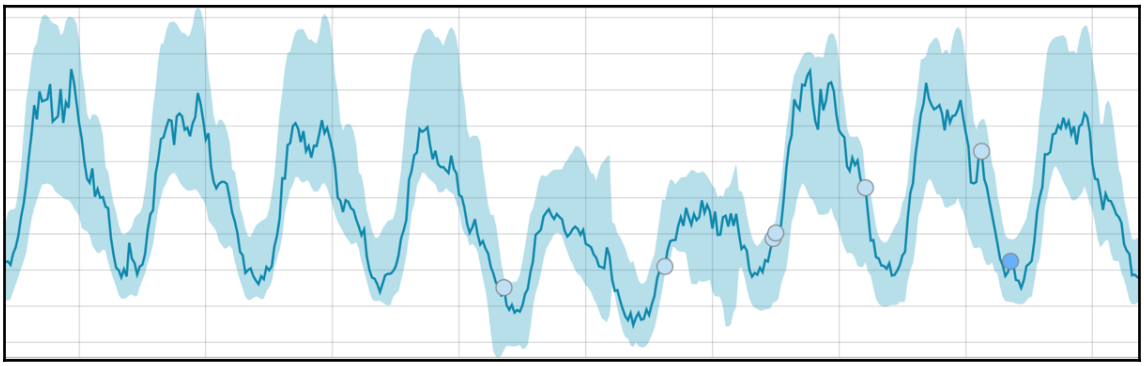

Machine Learning / Job Management / Create New Job / Single Metric Job
Last 15 minutes
New job from index pattern metricbeat-*
Use full metricbeat-* data
Aggregation
Select an aggregation
Field
Select a field
Bucket span
15m
Estimate bucket span

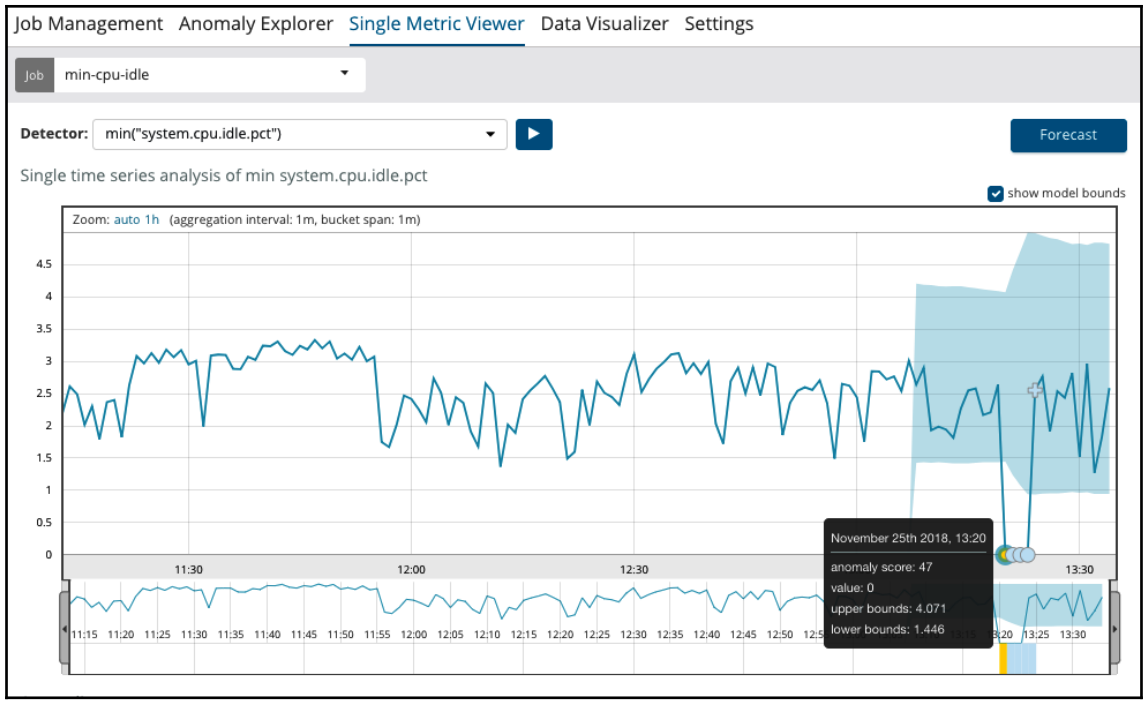

Machine Learning / Job Management / Create New Job / Single Metric Job
November 25th 2018, 11:12:21.534 to November 25th 2018, 13:35:31.742
New job from index pattern metricbeat-*
Chart interval: 1m
Use full metricbeat-* data
Aggregation
Min
Field
#system.cpu.idle.pct
Bucket span
1m
Estimate bucket span
Name
min-cpu-idle
Description
anomalies in low CPU idle
Job Groups
system_performance
Advanced
Move to advanced job configuration
Validate Job
Create Job

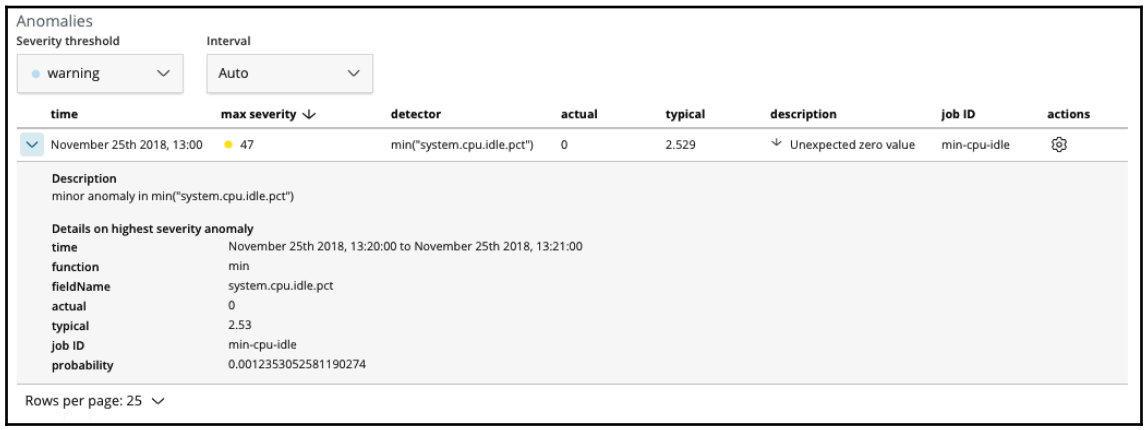

Machine Learning / Job Management / Create New Job / Single Metric Job
November 25th 2018, 11:12:21.534 to November 25th 2018, 13:35:31.742
New job from index pattern metricbeat-*
Chart interval: 1m
Use full metricbeat-* data
Aggregation
Min
Field
#system.cpu.idle.pct
Bucket span
1m
Estimate bucket span
11:15 11:20 11:25 11:30 11:35 11:40 11:45 11:50 11:55 12:00 12:05 12:10 12:15 12:20 12:25 12:30 12:35 12:40 12:45 12:50 12:55 13:00 13:05 13:10 13:15 13:20 13:25 13:30
Job min-cpu-idle created
Reset
View Results
Continue job in real-time
Create watch for real-time job
Apply

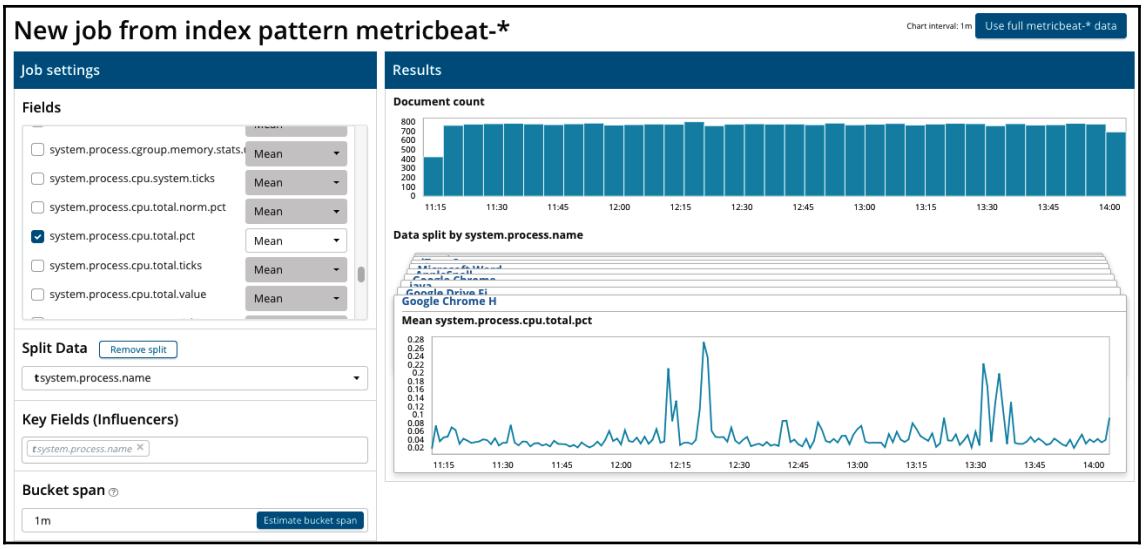

Job min-cpu-idle created
Reset
View Results
Continue job in real-time
Create watch for real-time job
Time range
Now -
2m
Severity threshold
critical
Send email
Apply

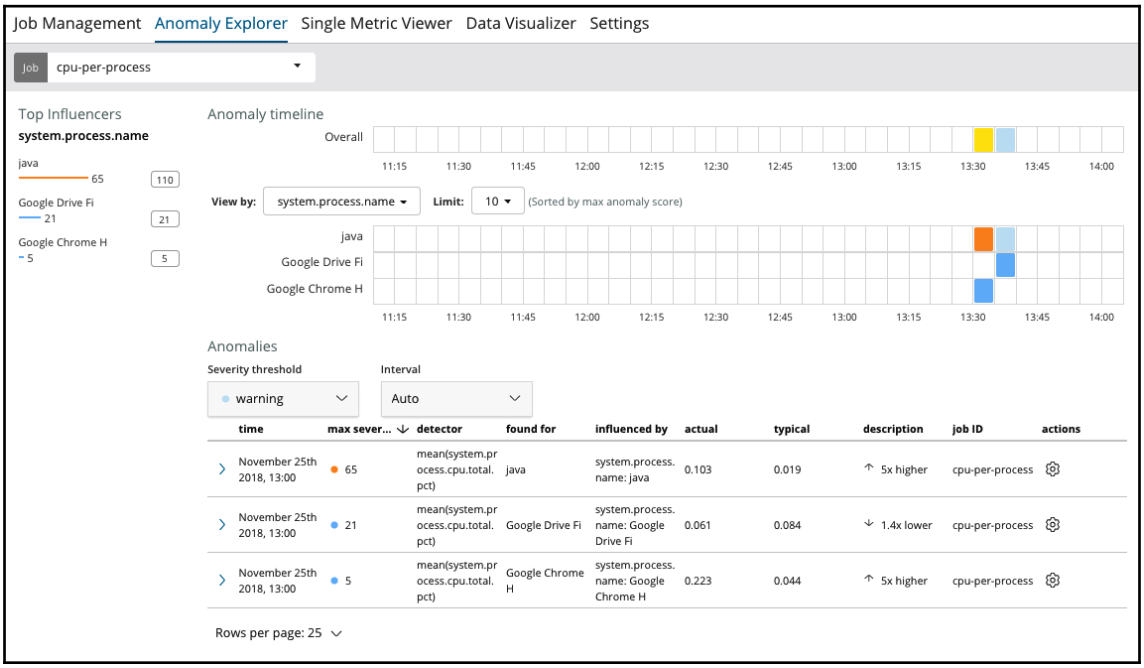


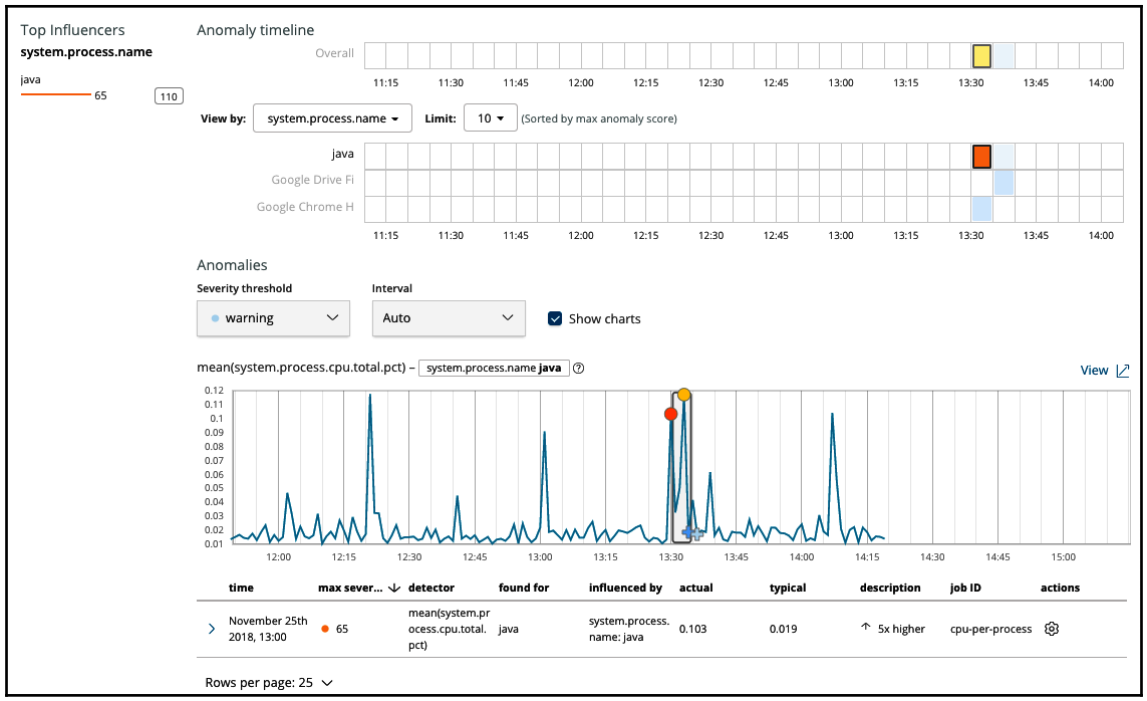


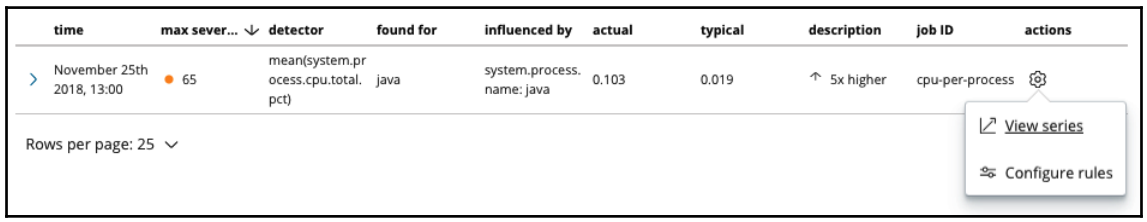

Job Management
Anomaly Explorer
Single Metric Viewer
Data Visualizer
Settings
Job
min-cpu-idle
Detector:
min("system.cpu.idle.pct")
Forecast
Single time series analysis of min system.cpu.idle.pct
show model bounds
Zoom: auto 1h (aggregation interval: 1m, bucket span: 1m)
4.5
4
3.5
3
2.5
2
1.5
1
0.5
0
11:30
12:00
12:30
13:30
November 25th 2018, 13:20
anomaly score: 47
value: 0
upper bounds: 4.071
lower bounds: 1.446

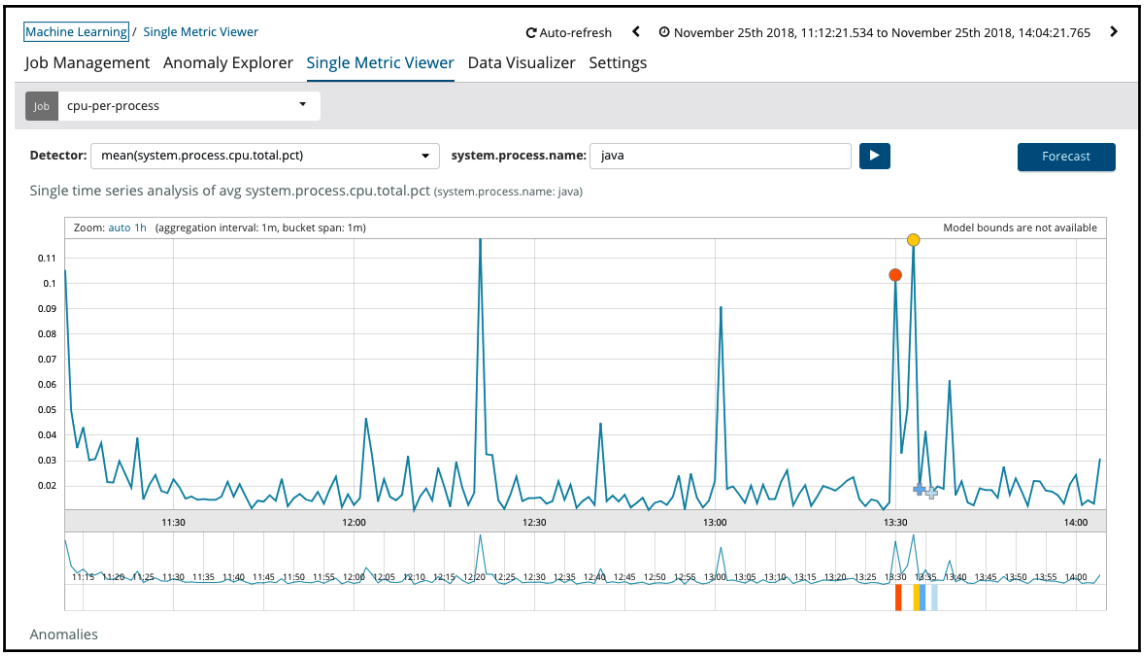

Anomalies
Severity threshold
warning
Interval
Auto
time
max severity
detector
actual
typical
description
job ID
actions
November 25th 2018, 13:00
47
min("system.cpu.idle.pct")
0
2.529
Unexpected zero value
min-cpu-idle
Description
minor anomaly in min("system.cpu.idle.pct")
Details on highest severity anomaly
time
November 25th 2018, 13:20:00 to November 25th 2018, 13:21:00
function
min
fieldName
system.cpu.idle.pct
actual
0
typical
2.53
job ID
min-cpu-idle
probability
0.0012353052581190274
Rows per page: 25

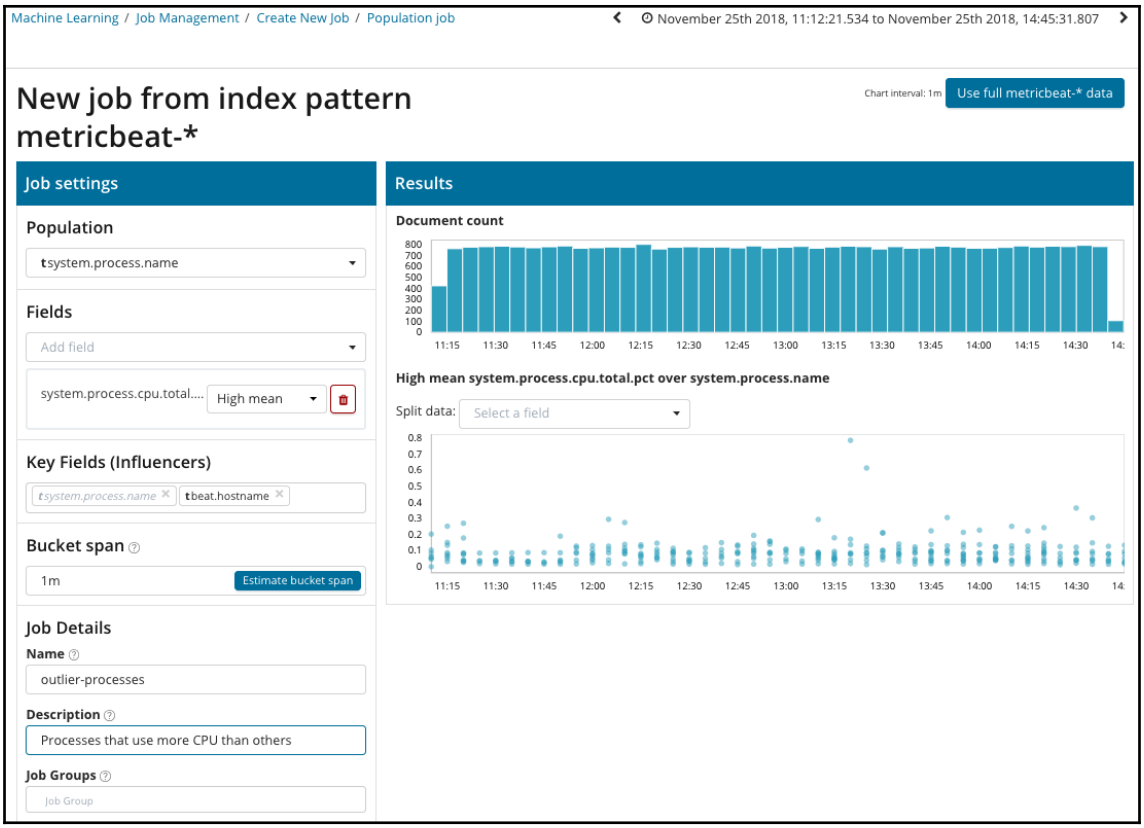

New job from index pattern metricbeat-*
Chart interval: 1m
Use full metricbeat-* data
Job settings
Fields
system.process.cgroup.memory.stats.
system.process.cpu.system.ticks
system.process.cpu.total.norm.pct
system.process.cpu.total.pct
system.process.cpu.total.ticks
system.process.cpu.total.value
Mean
Split Data
Remove split
tsystem.process.name
Key Fields (Influencers)
tsystem.process.name
Bucket span
1m
Estimate bucket span
Results
Document count
Data split by system.process.name
Google Chrome H
Mean system.process.cpu.total.pct

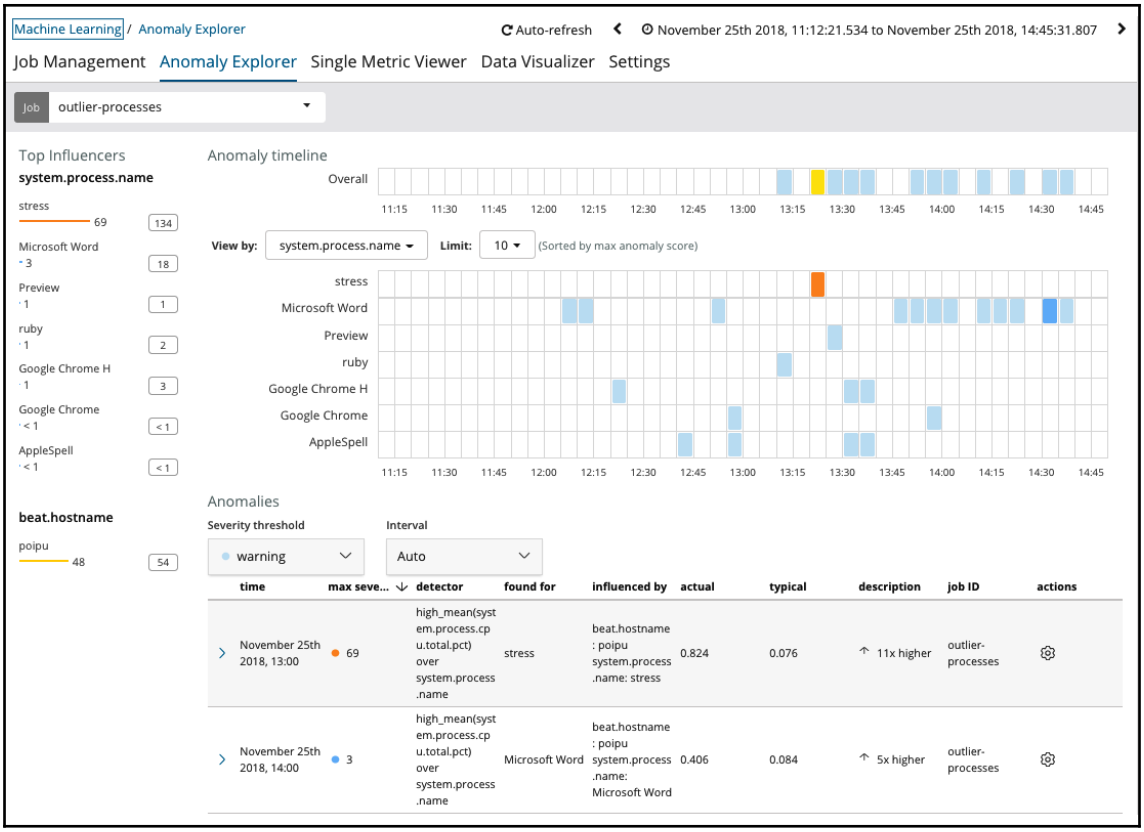

Job Management
Anomaly Explorer
Single Metric Viewer
Data Visualizer
Settings
Job
cpu-per-process
Top Influencers
system.process.name
java
65
110
Google Drive Fi
21
21
Google Chrome H
5
5
Anomaly timeline
Overall
View by:
system.process.name
Limit:
10
(Sorted by max anomaly score)
java
Google Drive Fi
Google Chrome H
Anomalies
Severity threshold
warning
Interval
Auto
time
max sever...
detector
found for
influenced by
actual
typical
description
job ID
actions
November 25th 2018, 13:00
65
mean(system.process.cpu.total.pct)
java
system.process.name: java
0.103
0.019
5x higher
cpu-per-process
November 25th 2018, 13:00
21
mean(system.process.cpu.total.pct)
Google Drive Fi
system.process.name: Google Drive Fi
0.061
0.084
1.4x lower
cpu-per-process
November 25th 2018, 13:00
5
mean(system.process.cpu.total.pct)
Google Chrome H
system.process.name: Google Chrome H
0.223
0.044
5x higher
cpu-per-process
Rows per page: 25


Top Influencers
system.process.name
java
65
110
Anomaly timeline
Overall
11:15 11:30 11:45 12:00 12:15 12:30 12:45 13:00 13:15 13:30 13:45 14:00
View by: system.process.name
Limit: 10
(Sorted by max anomaly score)
java
Google Drive Fi
Google Chrome H
Anomalies
Severity threshold
warning
Interval
Auto
Show charts
mean(system.process.cpu.total.pct) – system.process.name java
View
0.12 0.11 0.1 0.09 0.08 0.07 0.06 0.05 0.04 0.03 0.02 0.01
12:00 12:15 12:30 12:45 13:00 13:15 13:30 13:45 14:00 14:15 14:30 14:45 15:00
time
max sever...
detector
found for
influenced by
actual
typical
description
job ID
actions
November 25th 2018, 13:00
65
mean(system.process.cpu.total.pct)
java
system.process.name: java
0.103
0.019
5x higher
cpu-per-process
Rows per page: 25


time
max sever...
detector
found for
influenced by
actual
typical
description
job ID
actions
November 25th 2018, 13:00
65
mean(system.process.cpu.total.pct)
java
system.process.name: java
0.103
0.019
5x higher
cpu-per-process
View series
Configure rules
Rows per page: 25

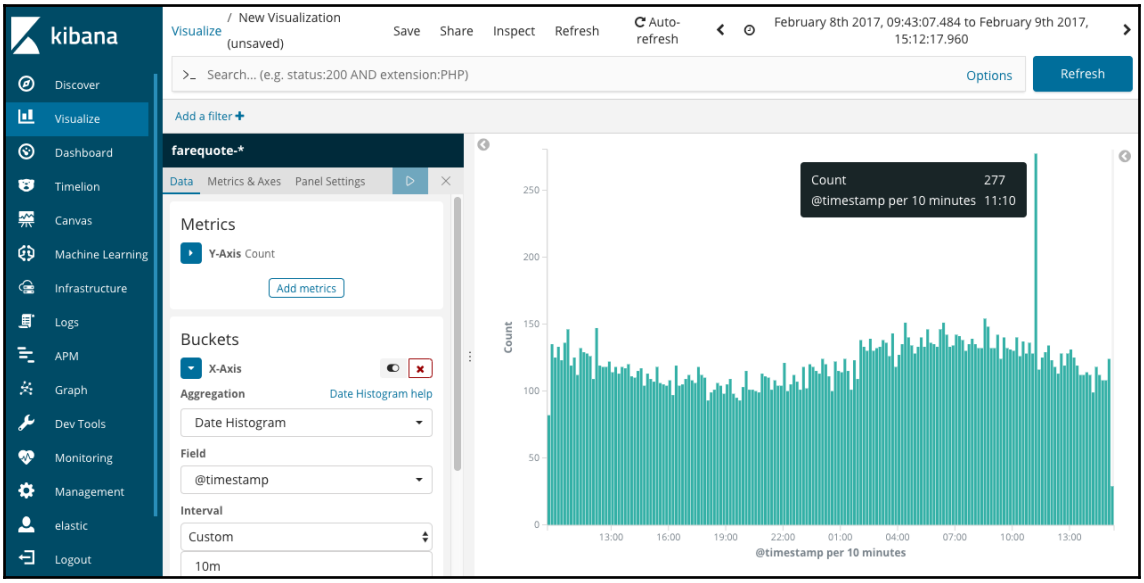

Machine Learning / Single Metric Viewer
Auto-refresh
November 25th 2018, 11:12:21.534 to November 25th 2018, 14:04:21.765
Job Management
Anomaly Explorer
Single Metric Viewer
Data Visualizer
Settings
Job
cpu-per-process
Detector:
mean(system.process.cpu.total.pct)
system.process.name:
java
Forecast
Single time series analysis of avg system.process.cpu.total.pct (system.process.name: java)
Zoom: auto 1h (aggregation interval: 1m, bucket span: 1m)
Model bounds are not available
0.11
0.1
0.09
0.08
0.07
0.06
0.05
0.04
0.03
0.02
11:30
12:00
12:30
13:00
13:30
14:00
Anomalies

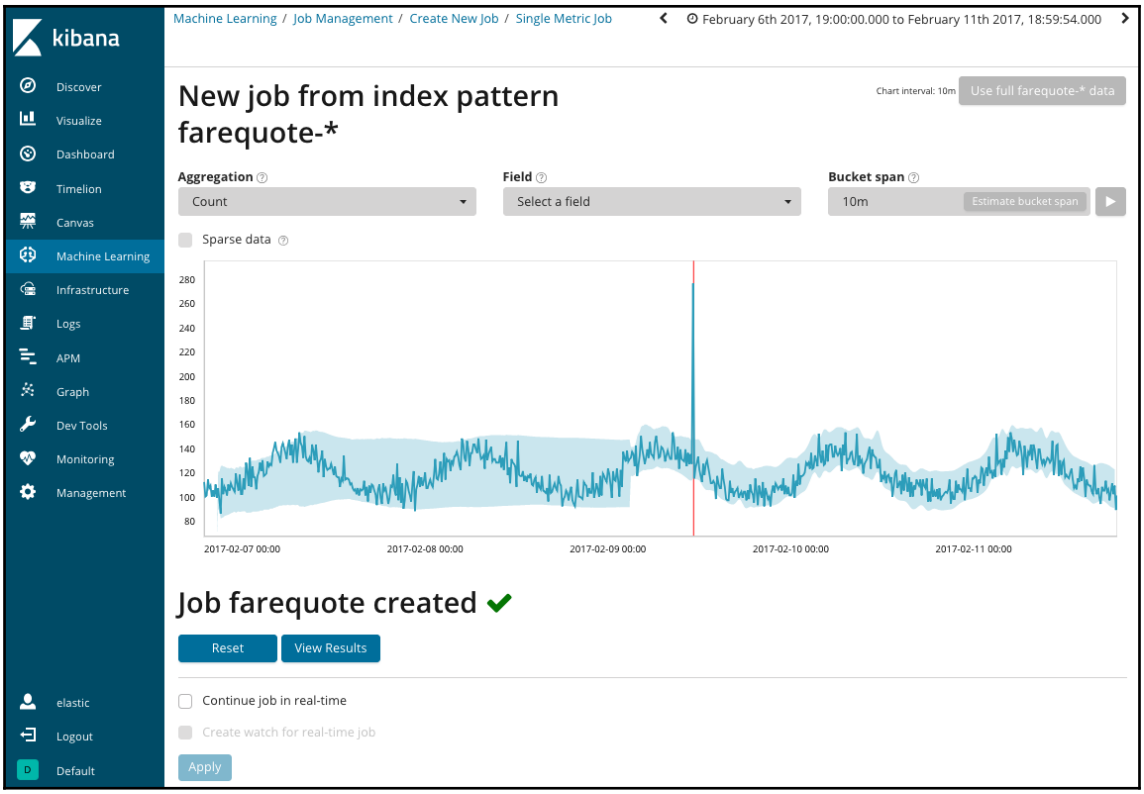

Machine Learning / Job Management / Create New Job / Population job
November 25th 2018, 11:12:21.534 to November 25th 2018, 14:45:31.807
New job from index pattern metricbeat-*
Chart interval: 1m
Use full metricbeat-* data
Job settings
Population
tsystem.process.name
Fields
Add field
system.process.cpu.total....
High mean
Key Fields (Influencers)
tsystem.process.name
tbeat.hostname
Bucket span
1m
Estimate bucket span
Job Details
Name
outlier-processes
Description
Processes that use more CPU than others
Job Groups
Job Group
Results
Document count
800
700
600
500
400
300
200
100
0
11:15
11:30
11:45
12:00
12:15
12:30
12:45
13:00
13:15
13:30
13:45
14:00
14:15
14:30
High mean system.process.cpu.total.pct over system.process.name
Split data:
Select a field
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0

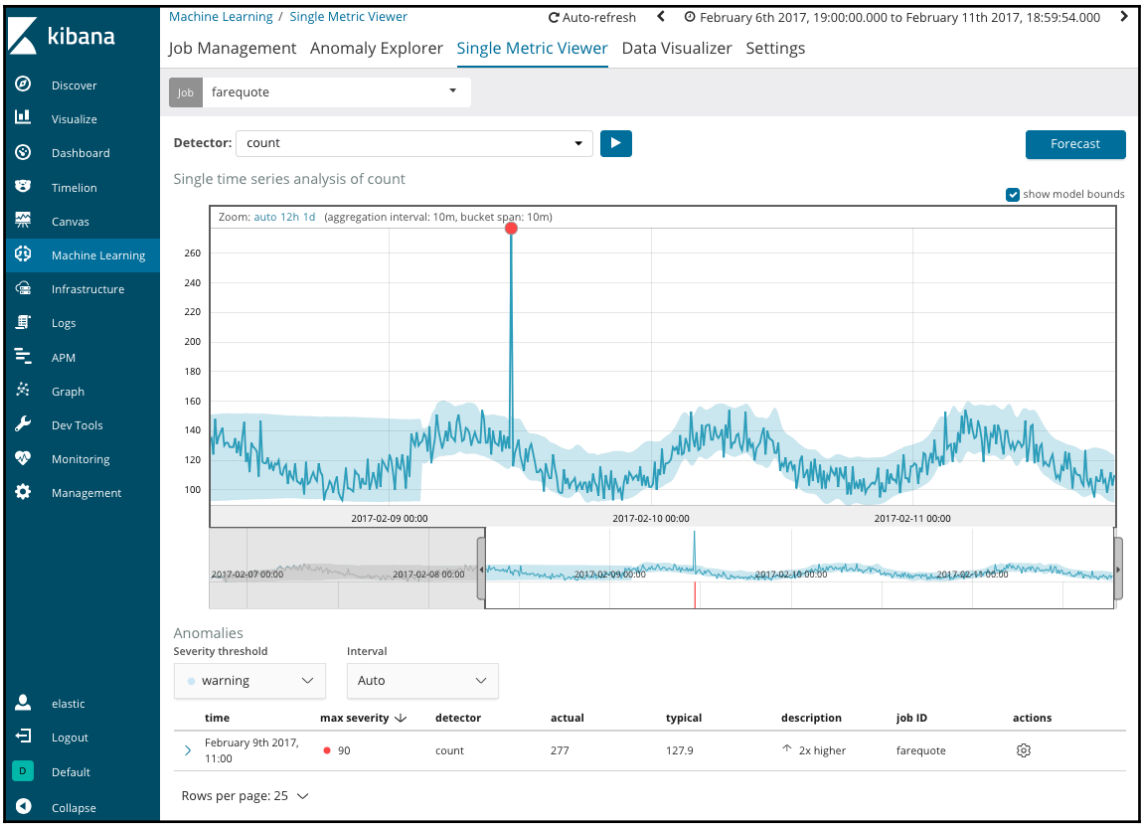

Machine Learning / Anomaly Explorer
Auto-refresh
November 25th 2018, 11:12:21.534 to November 25th 2018, 14:45:31.807
Job Management
Anomaly Explorer
Single Metric Viewer
Data Visualizer
Settings
Job
outlier-processes
Top Influencers
system.process.name
stress
69
134
Microsoft Word
3
18
Preview
1
1
ruby
1
2
Google Chrome H
1
3
Google Chrome
< 1
< 1
AppleSpell
< 1
< 1
beat.hostname
poipu
48
54
Anomaly timeline
Overall
11:15
11:30
11:45
12:00
12:15
12:30
12:45
13:00
13:15
13:30
13:45
14:00
14:15
14:30
14:45
View by:
system.process.name
Limit:
10
(Sorted by max anomaly score)
stress
Microsoft Word
Preview
ruby
Google Chrome H
Google Chrome
AppleSpell
Anomalies
Severity threshold
warning
Interval
Auto
time
max seve...
detector
found for
influenced by
actual
typical
description
job ID
actions
November 25th 2018, 13:00
69
high_mean(system.process.cpu.total.pct) over system.process.name
stress
beat.hostname: poipu system.process.name: stress
0.824
0.076
11x higher
outlier-processes
November 25th 2018, 14:00
3
high_mean(system.process.cpu.total.pct) over system.process.name
Microsoft Word
beat.hostname: poipu system.process.name: Microsoft Word
0.406
0.084
5x higher
outlier-processes

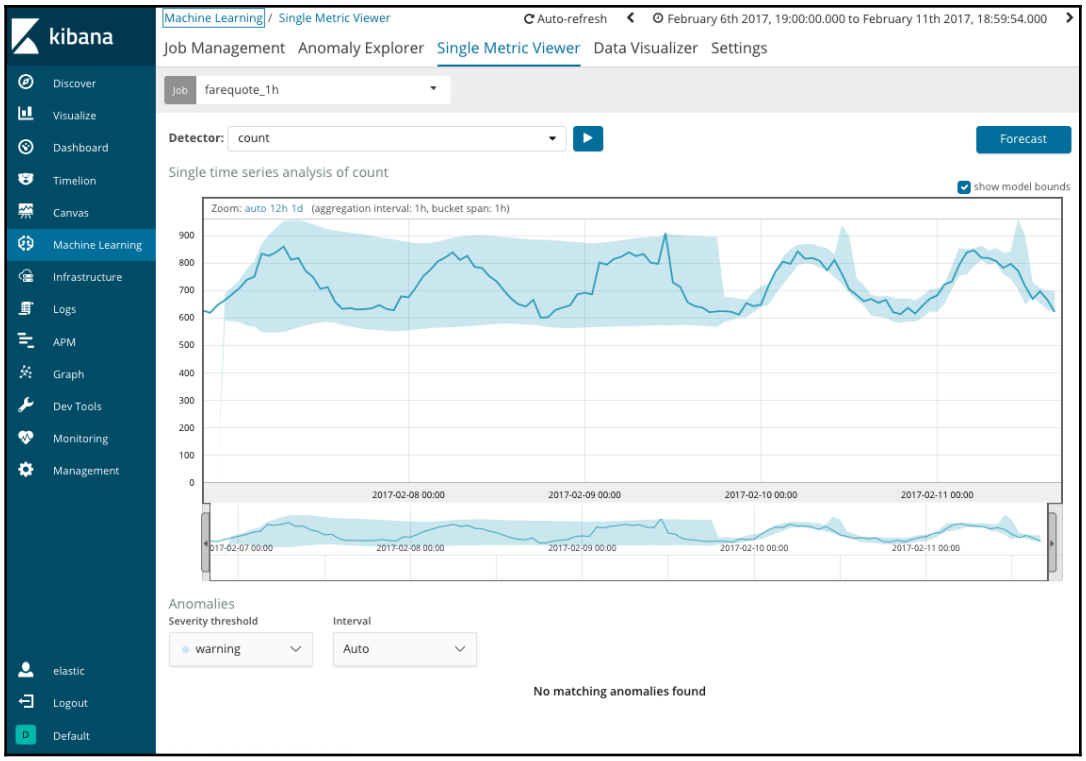

Top Influencers
system.process.name
stress
69
134
beat.hostname
poipu
48
50
Anomaly timeline
Overall
11:15 11:30 11:45 12:00 12:15 12:30 12:45 13:00 13:15 13:30 13:45 14:00 14:15 14:30 14:45
View by: system.process.name
Limit: 10
(Sorted by max anomaly score)
stress
Microsoft Word
Preview
ruby
Google Chrome H
Google Chrome
AppleSpell
11:15 11:30 11:45 12:00 12:15 12:30 12:45 13:00 13:15 13:30 13:45 14:00 14:15 14:30 14:45
Anomalies
Severity threshold
warning
Interval
Auto
Show charts
high_mean(system.process.cpu.total.pct) over system.process.name
View
system.process.name stress
0.9 0.8 0.7 0.6 0.5 0.4 0.3 0.2 0.1 0
11:50 12:05 12:20 12:35 12:50 13:05 13:20 13:35 13:50 14:05 14:20 14:35 14:50
time
max seve...
detector
found for
influenced by
actual
typical
description
job ID
actions
November 25th 2018, 13:00
69
high_mean(system.process.cpu.total.pct) over system.process.name
stress
beat.hostname: poipu system.process.name: stress
0.824
0.076
11x higher
outlier-processes

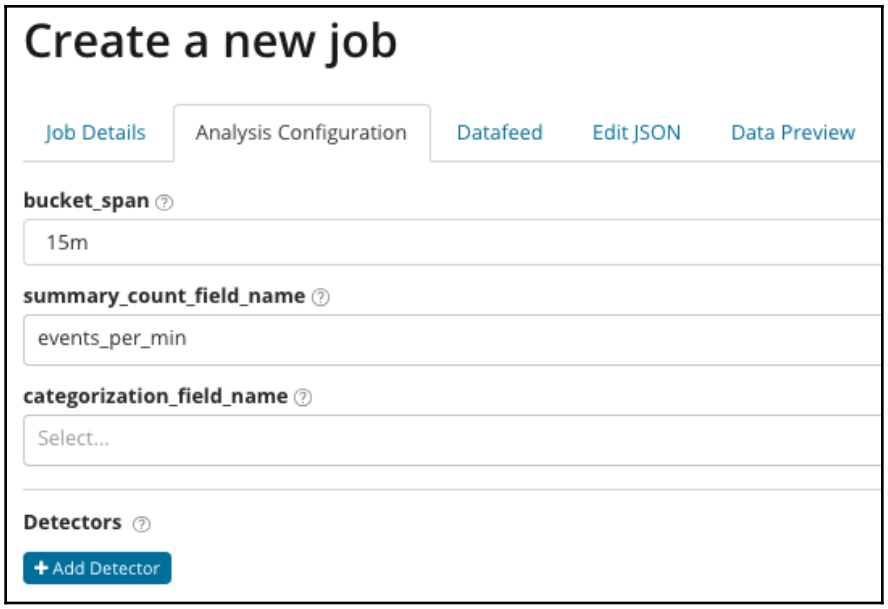
Chapter 3: Event Change Detection

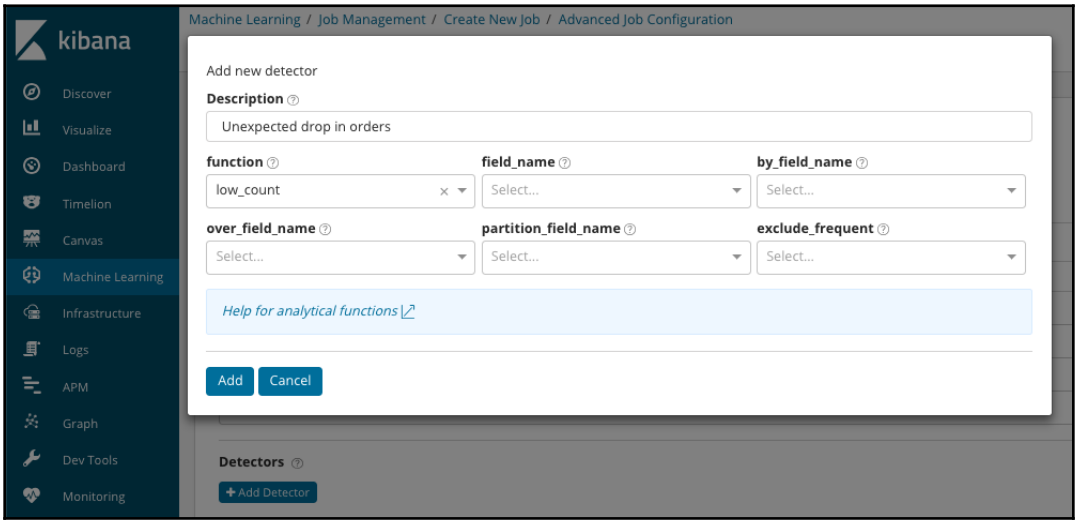


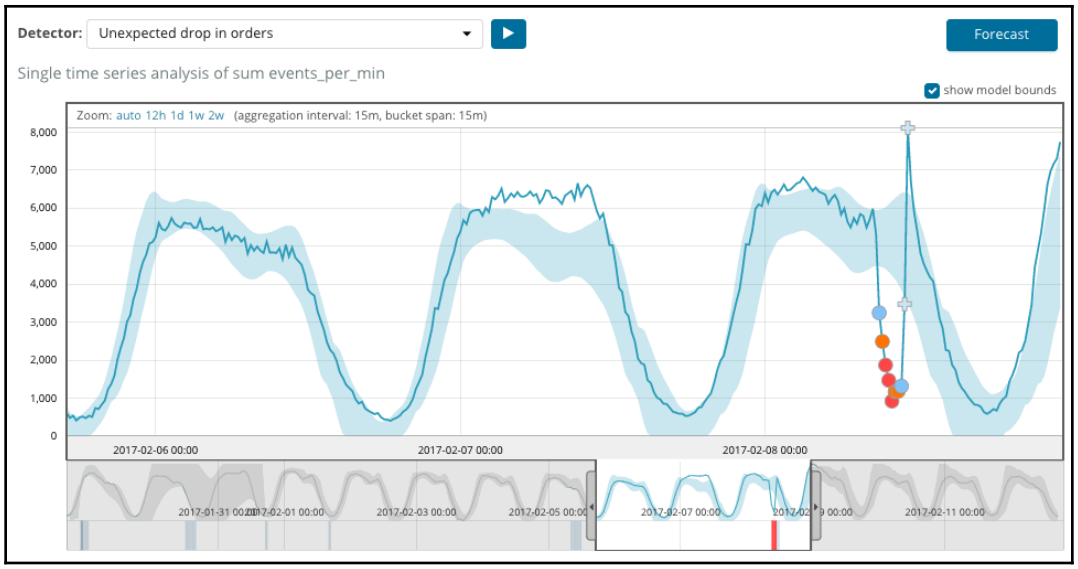

kibana
Discover
Visualize
Dashboard
Timelion
Canvas
Machine Learning
Infrastructure
Logs
APM
Graph
Dev Tools
Monitoring
Management
elastic
Logout
Default
Machine Learning / Job Management / Create New Job / Single Metric Job
February 6th 2017, 19:00:00.000 to February 11th 2017, 18:59:54.000
New job from index pattern farequote-*
Chart interval: 10m
Use full farequote-* data
Aggregation
Count
Field
Select a field
Bucket span
10m
Estimate bucket span
Sparse data
280
260
240
220
200
180
160
140
120
100
80
2017-02-07 00:00
2017-02-08 00:00
2017-02-09 00:00
2017-02-10 00:00
2017-02-11 00:00
Job farequote created
Reset
View Results
Continue job in real-time
Create watch for real-time job
Apply

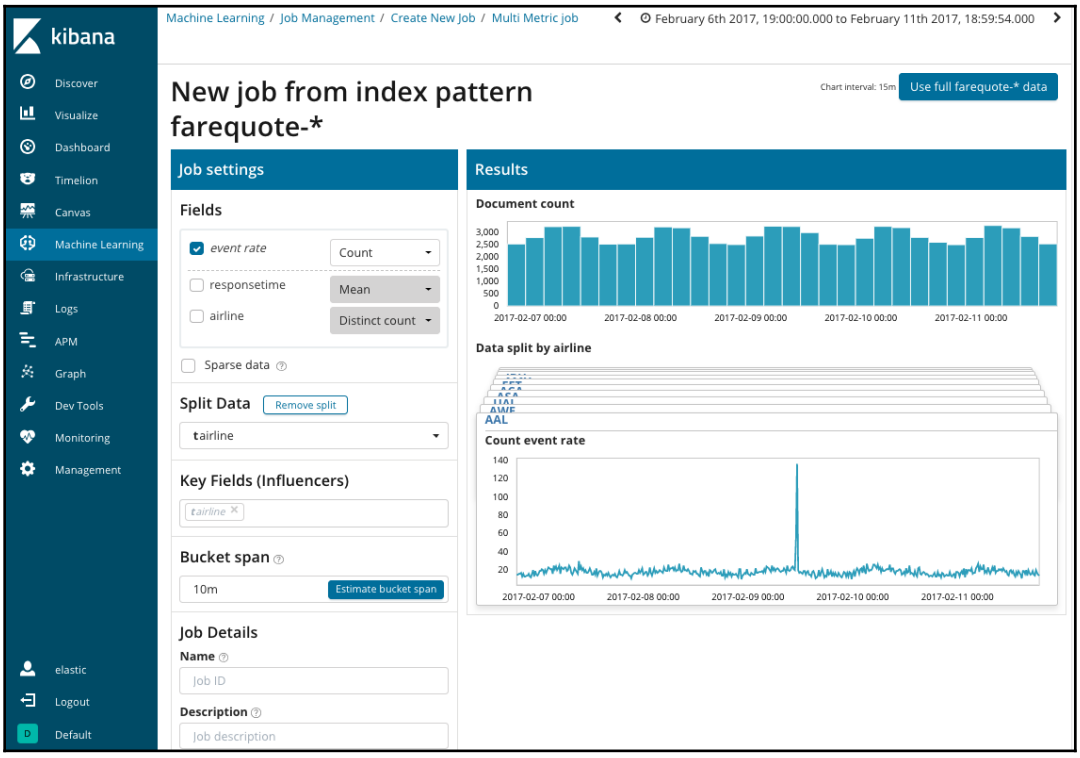

kibana
Discover
Visualize
Dashboard
Timelion
Canvas
Machine Learning
Infrastructure
Logs
APM
Graph
Dev Tools
Monitoring
Management
elastic
Logout
Default
Collapse
Machine Learning / Single Metric Viewer
Auto-refresh
February 6th 2017, 19:00:00.000 to February 11th 2017, 18:59:54.000
Job Management
Anomaly Explorer
Single Metric Viewer
Data Visualizer
Settings
Job
farequote
Detector:
count
Forecast
Single time series analysis of count
show model bounds
Zoom: auto 12h 1d (aggregation interval: 10m, bucket span: 10m)
260
240
220
200
180
160
140
120
100
2017-02-09 00:00
2017-02-10 00:00
2017-02-11 00:00
2017-02-07 00:00
2017-02-08 00:00
Anomalies
Severity threshold
warning
Interval
Auto
time
max severity
detector
actual
typical
description
job ID
actions
February 9th 2017, 11:00
90
count
277
127.9
2x higher
farequote
Rows per page: 25

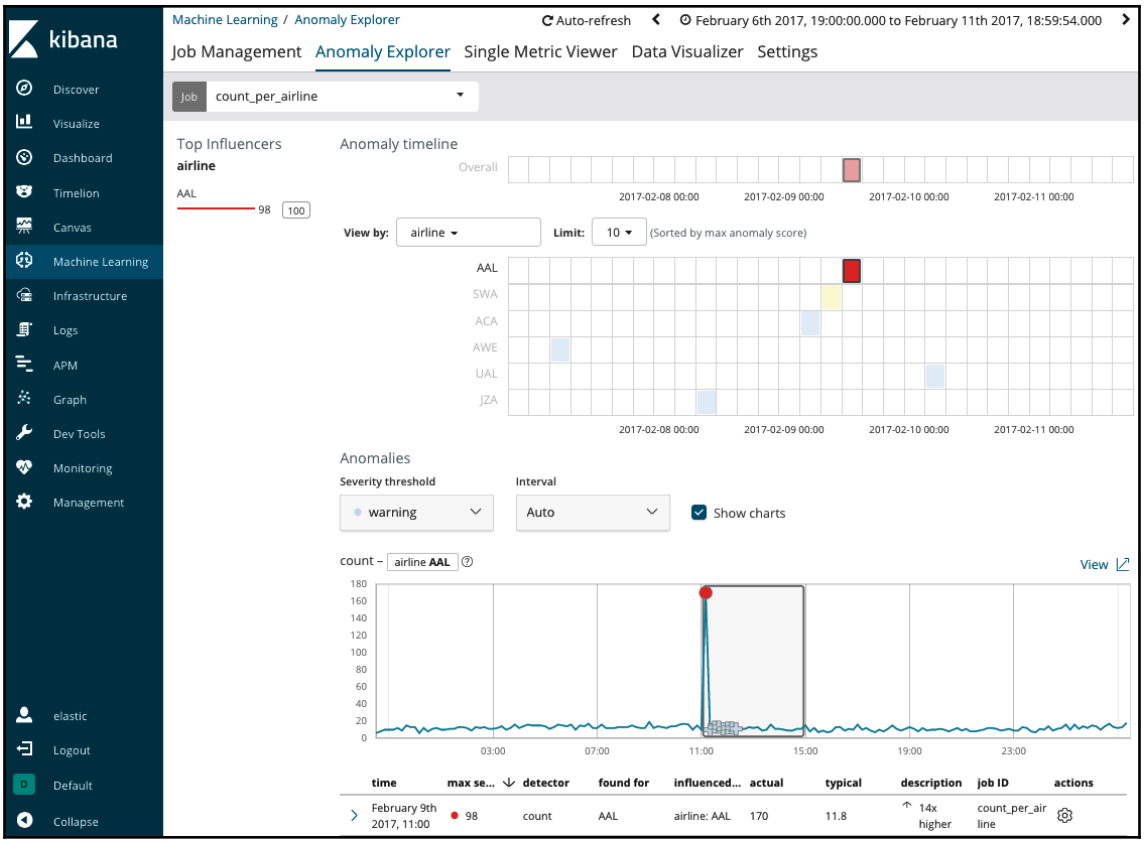

kibana
Machine Learning / Single Metric Viewer
Auto-refresh
February 6th 2017, 19:00:00.000 to February 11th 2017, 18:59:54.000
Job Management
Anomaly Explorer
Single Metric Viewer
Data Visualizer
Settings
Discover
Visualize
Dashboard
Timelion
Canvas
Machine Learning
Infrastructure
Logs
APM
Graph
Dev Tools
Monitoring
Management
elastic
Logout
Default
Job
farequote_1h
Detector:
count
Forecast
Single time series analysis of count
show model bounds
Zoom: auto 12h 1d (aggregation interval: 1h, bucket span: 1h)
900
800
700
600
500
400
300
200
100
0
2017-02-08 00:00
2017-02-09 00:00
2017-02-10 00:00
2017-02-11 00:00
2017-02-07 00:00
2017-02-08 00:00
2017-02-09 00:00
2017-02-10 00:00
2017-02-11 00:00
Anomalies
Severity threshold
warning
Interval
Auto
No matching anomalies found

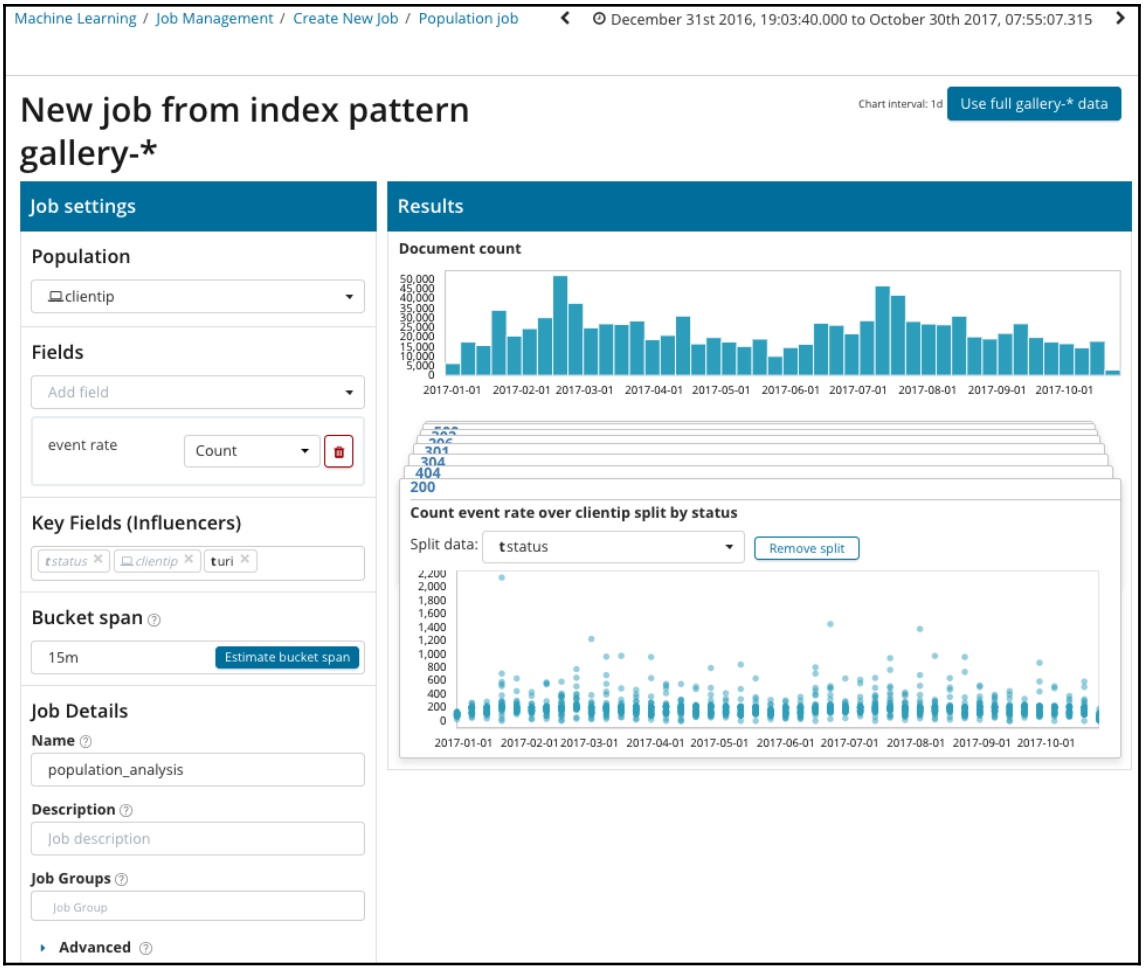

Create a new job
Job Details
Analysis Configuration
Datafeed
Edit JSON
Data Preview
bucket_span
15m
summary_count_field_name
events_per_min
categorization_field_name
Select...
Detectors
+ Add Detector

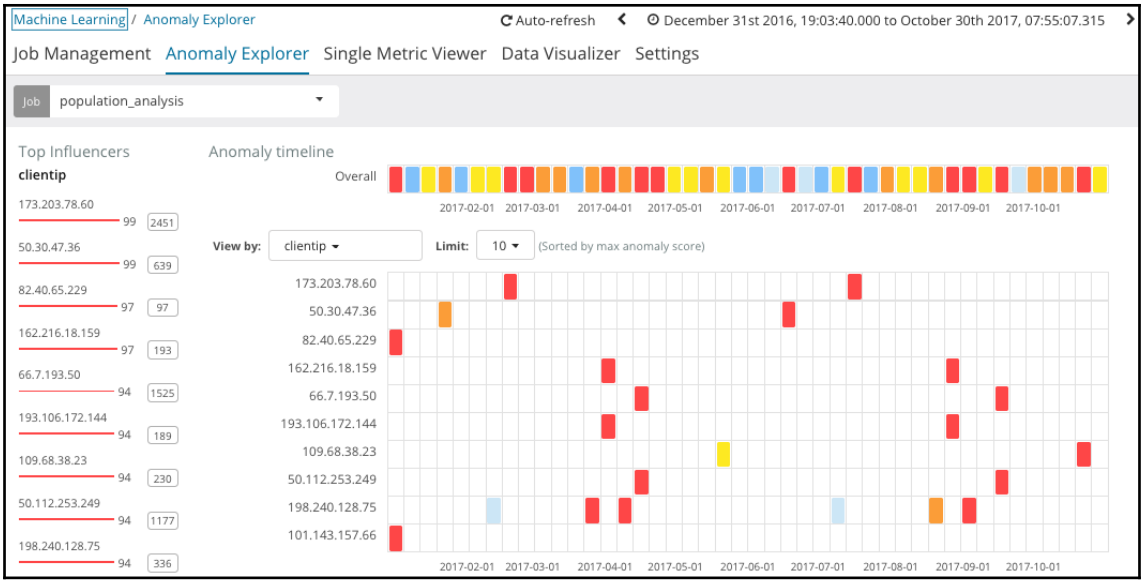

kibana
Discover
Visualize
Dashboard
Timelion
Canvas
Machine Learning
Infrastructure
Logs
APM
Graph
Dev Tools
Monitoring
Machine Learning / Job Management / Create New Job / Advanced Job Configuration
Add new detector
Description
Unexpected drop in orders
function
low_count
field_name
Select...
by_field_name
Select...
over_field_name
Select...
partition_field_name
Select...
exclude_frequent
Select...
Help for analytical functions
Add
Cancel
Detectors
+ Add Detector

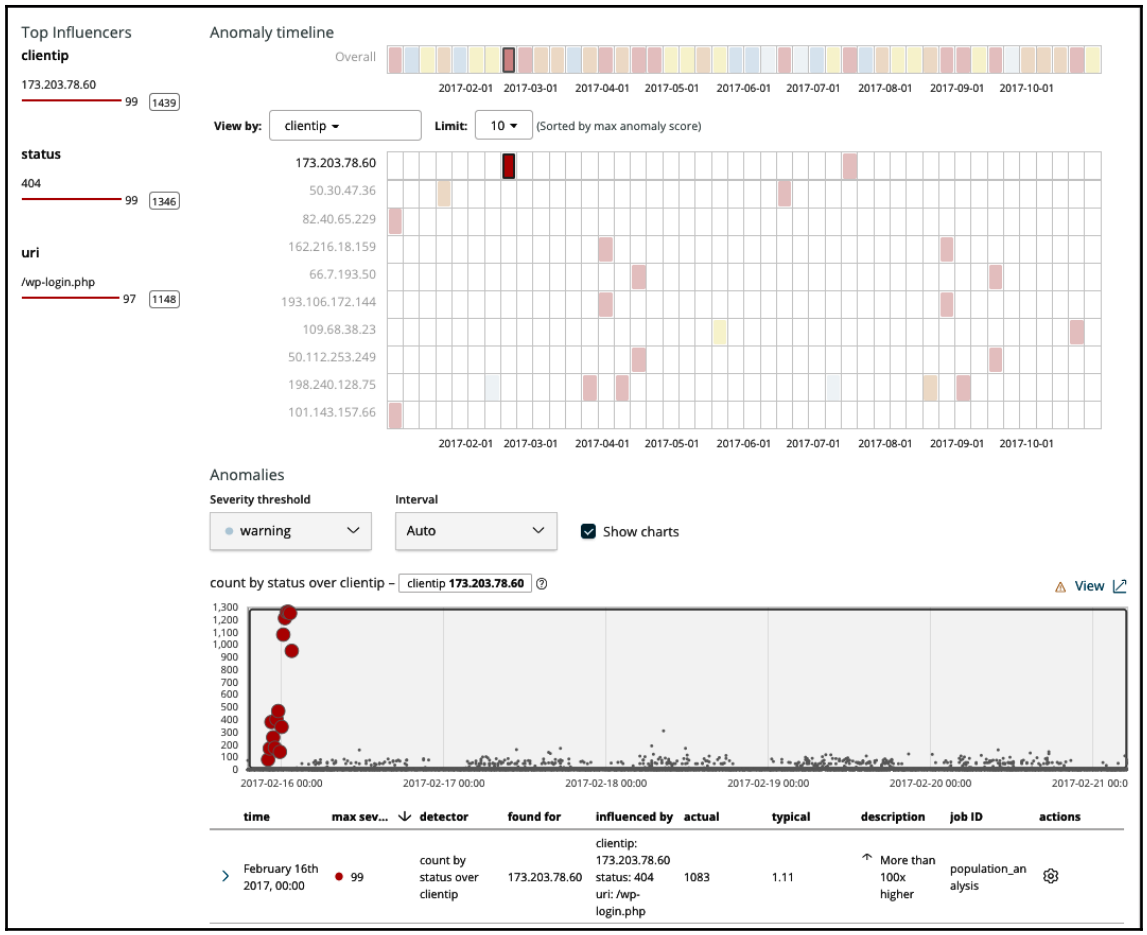

Detector: Unexpected drop in orders
Forecast
Single time series analysis of sum events_per_min
show model bounds
Zoom: auto 12h 1d 1w 2w (aggregation interval: 15m, bucket span: 15m)
8,000
7,000
6,000
5,000
4,000
3,000
2,000
1,000
0
2017-02-06 00:00
2017-02-07 00:00
2017-02-08 00:00
2017-01-31 00:00
2017-02-01 00:00
2017-02-03 00:00
2017-02-05 00:00
2017-02-07 00:00
2017-02-11 00:00

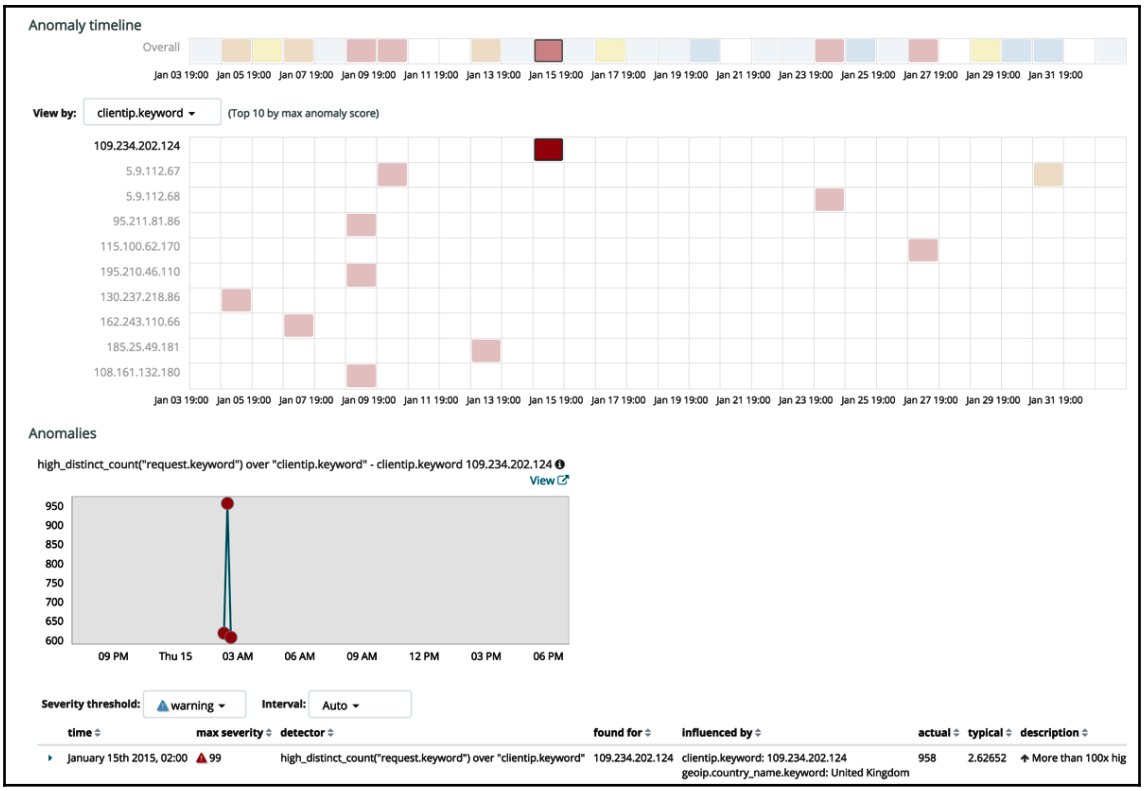

kibana
Discover
Visualize
Dashboard
Timelion
Canvas
Machine Learning
Infrastructure
Logs
APM
Graph
Dev Tools
Monitoring
Management
elastic
Logout
Default
Machine Learning / Job Management / Create New Job / Multi Metric job
February 6th 2017, 19:00:00.000 to February 11th 2017, 18:59:54.000
New job from index pattern farequote-*
Chart interval: 15m
Use full farequote-* data
Job settings
Fields
event rate
Count
responsetime
Mean
airline
Distinct count
Sparse data
Split Data
Remove split
tairline
Key Fields (Influencers)
tairline
Bucket span
10m
Estimate bucket span
Job Details
Name
Job ID
Description
Job description
Results
Document count
3,000
2,500
2,000
1,500
1,000
500
0
2017-02-07 00:00
2017-02-08 00:00
2017-02-09 00:00
2017-02-10 00:00
2017-02-11 00:00
Data split by airline
AAL
Count event rate
140
120
100
80
60
40
20
2017-02-07 00:00
2017-02-08 00:00
2017-02-09 00:00
2017-02-10 00:00
2017-02-11 00:00

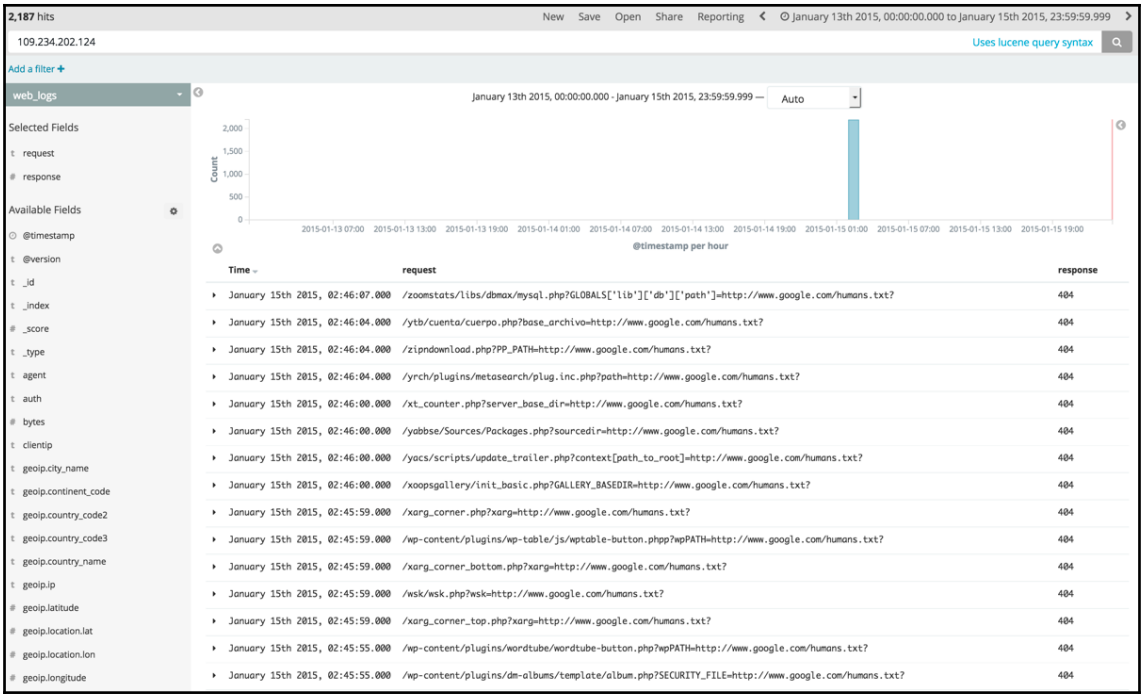

kibana
Discover
Visualize
Dashboard
Timelion
Canvas
Machine Learning
Infrastructure
Logs
APM
Graph
Dev Tools
Monitoring
Management
elastic
Logout
Default
Collapse
Machine Learning / Anomaly Explorer
Auto-refresh
February 6th 2017, 19:00:00.000 to February 11th 2017, 18:59:54.000
Job Management
Anomaly Explorer
Single Metric Viewer
Data Visualizer
Settings
Job
count_per_airline
Top Influencers
airline
AAL
98
100
Anomaly timeline
Overall
2017-02-08 00:00
2017-02-09 00:00
2017-02-10 00:00
2017-02-11 00:00
View by:
airline
Limit:
10
(Sorted by max anomaly score)
AAL
SWA
ACA
AWE
UAL
JZA
Anomalies
Severity threshold
warning
Interval
Auto
Show charts
count – airline AAL
View
180
160
140
120
100
80
60
40
20
0
03:00
07:00
11:00
15:00
19:00
23:00
time
max se...
detector
found for
influenced...
actual
typical
description
job ID
actions
February 9th 2017, 11:00
98
count
AAL
airline: AAL
170
11.8
14x higher
count_per_airline

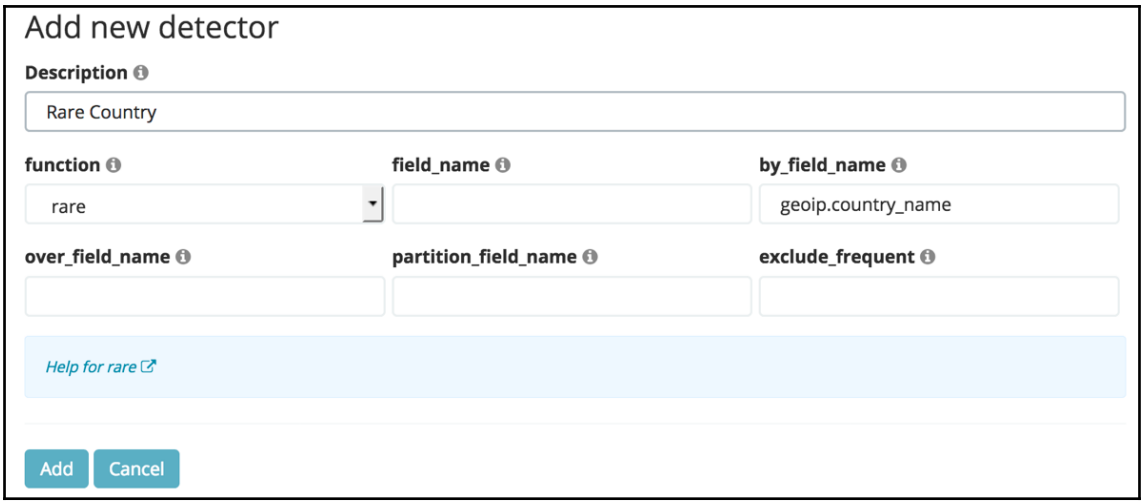

Machine Learning / Job Management / Create New Job / Population job
December 31st 2016, 19:03:40.000 to October 30th 2017, 07:55:07.315
New job from index pattern gallery-*
Chart interval: 1d
Use full gallery-* data
Job settings
Population
clientip
Fields
Add field
event rate
Count
Key Fields (Influencers)
tstatus
clientip
turi
Bucket span
15m
Estimate bucket span
Job Details
Name
population_analysis
Description
Job description
Job Groups
Job Group
Advanced
Results
Document count
50,000
45,000
40,000
35,000
30,000
25,000
20,000
15,000
10,000
5,000
0
2017-01-01 2017-02-01 2017-03-01 2017-04-01 2017-05-01 2017-06-01 2017-07-01 2017-08-01 2017-09-01 2017-10-01
301
304
404
200
Count event rate over clientip split by status
Split data:
tstatus
Remove split
2,200
2,000
1,800
1,600
1,400
1,200
1,000
800
600
400
200
0
2017-01-01 2017-02-01 2017-03-01 2017-04-01 2017-05-01 2017-06-01 2017-07-01 2017-08-01 2017-09-01 2017-10-01

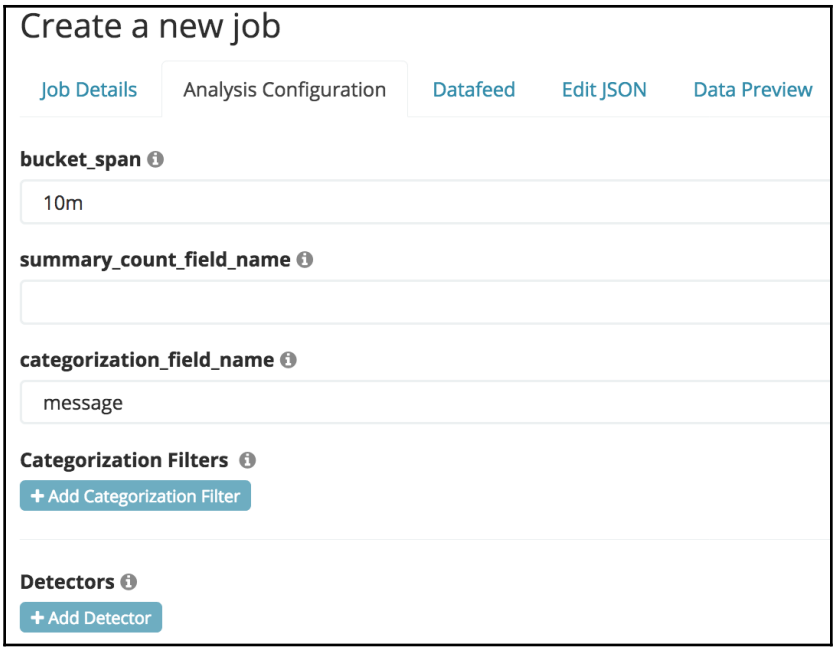

Machine Learning / Anomaly Explorer
Auto-refresh
December 31st 2016, 19:03:40.000 to October 30th 2017, 07:55:07.315
Job Management
Anomaly Explorer
Single Metric Viewer
Data Visualizer
Settings
Job
population_analysis
Top Influencers
clientip
173.203.78.60
99
2451
50.30.47.36
99
639
82.40.65.229
97
97
162.216.18.159
97
193
66.7.193.50
94
1525
193.106.172.144
94
189
109.68.38.23
94
230
50.112.253.249
94
1177
198.240.128.75
94
336
Anomaly timeline
Overall
2017-02-01
2017-03-01
2017-04-01
2017-05-01
2017-06-01
2017-07-01
2017-08-01
2017-09-01
2017-10-01
View by:
clientip
Limit:
10
(Sorted by max anomaly score)
173.203.78.60
50.30.47.36
82.40.65.229
162.216.18.159
66.7.193.50
193.106.172.144
109.68.38.23
50.112.253.249
198.240.128.75
101.143.157.66

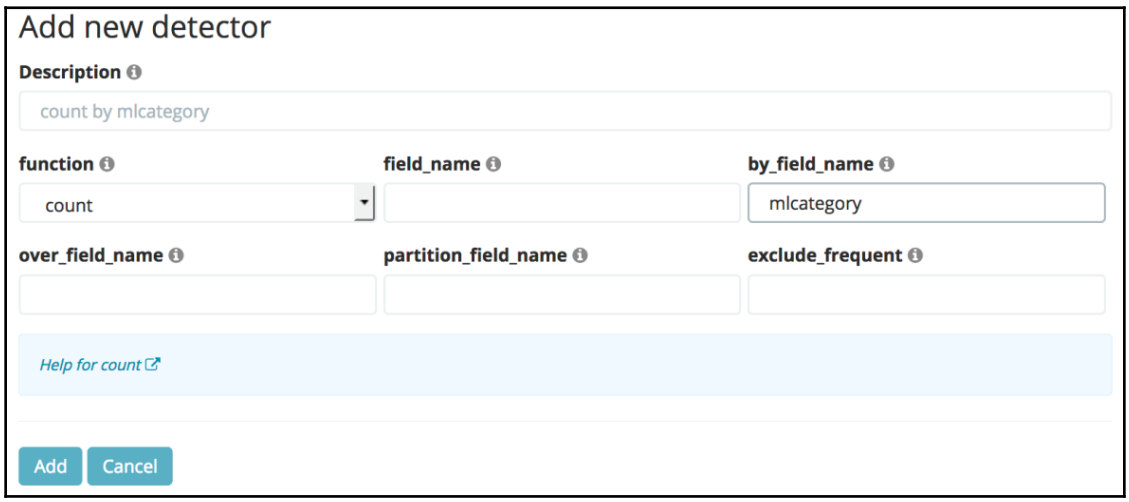

Top Influencers
clientip
173.203.78.60
99
1439
status
404
99
1346
uri
/wp-login.php
97
1148
Anomaly timeline
Overall
2017-02-01
2017-03-01
2017-04-01
2017-05-01
2017-06-01
2017-07-01
2017-08-01
2017-09-01
2017-10-01
View by:
clientip
Limit:
10
(Sorted by max anomaly score)
173.203.78.60
50.30.47.36
82.40.65.229
162.216.18.159
66.7.193.50
193.106.172.144
109.68.38.23
50.112.253.249
198.240.128.75
101.143.157.66
Anomalies
Severity threshold
warning
Interval
Auto
Show charts
count by status over clientip – clientip 173.203.78.60
View
1,300
1,200
1,100
1,000
900
800
700
600
500
400
300
200
100
0
2017-02-16 00:00
2017-02-17 00:00
2017-02-18 00:00
2017-02-19 00:00
2017-02-20 00:00
2017-02-21 00:0
time
max sev...
detector
found for
influenced by
actual
typical
description
job ID
actions
February 16th 2017, 00:00
99
count by status over clientip
173.203.78.60
clientip: 173.203.78.60 status: 404 uri: /wp-login.php
1083
1.11
More than 100x higher
population_analysis

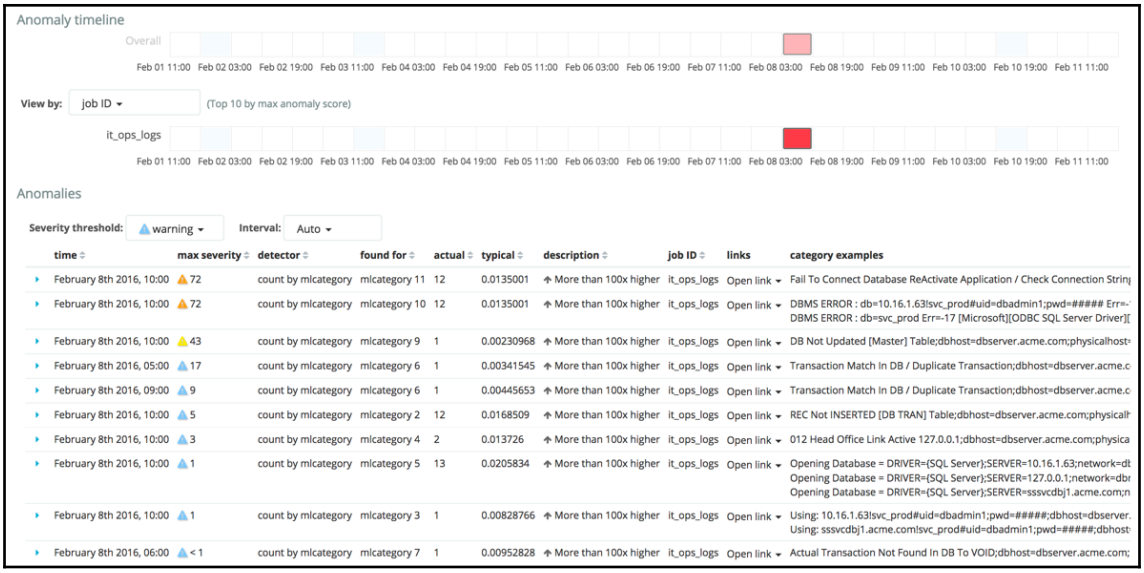

Anomaly timeline
Overall
Jan 03 19:00 Jan 05 19:00 Jan 07 19:00 Jan 09 19:00 Jan 11 19:00 Jan 13 19:00 Jan 15 19:00 Jan 17 19:00 Jan 19 19:00 Jan 21 19:00 Jan 23 19:00 Jan 25 19:00 Jan 27 19:00 Jan 29 19:00 Jan 31 19:00
View by: clientip.keyword (Top 10 by max anomaly score)
109.234.202.124
5.9.112.67
5.9.112.68
95.211.81.86
115.100.62.170
195.210.46.110
130.237.218.86
162.243.110.66
185.25.49.181
108.161.132.180
Jan 03 19:00 Jan 05 19:00 Jan 07 19:00 Jan 09 19:00 Jan 11 19:00 Jan 13 19:00 Jan 15 19:00 Jan 17 19:00 Jan 19 19:00 Jan 21 19:00 Jan 23 19:00 Jan 25 19:00 Jan 27 19:00 Jan 29 19:00 Jan 31 19:00
Anomalies
high_distinct_count("request.keyword") over "clientip.keyword" - clientip.keyword 109.234.202.124
View
950
900
850
800
750
700
650
600
09 PM Thu 15 03 AM 06 AM 09 AM 12 PM 03 PM 06 PM
Severity threshold: warning Interval: Auto
time max severity detector found for influenced by actual typical description
January 15th 2015, 02:00 99 high_distinct_count("request.keyword") over "clientip.keyword" 109.234.202.124 clientip.keyword: 109.234.202.124 geoip.country_name.keyword: United Kingdom 958 2.62652 More than 100x hig


2,187 hits
New Save Open Share Reporting
January 13th 2015, 00:00:00.000 to January 15th 2015, 23:59:59.999
109.234.202.124
Uses lucene query syntax
Add a filter +
web_logs
Selected Fields
request
response
Available Fields
@timestamp
@version
_id
_index
_score
_type
agent
auth
bytes
clientip
geoip.city_name
geoip.continent_code
geoip.country_code2
geoip.country_code3
geoip.country_name
geoip.ip
geoip.latitude
geoip.location.lat
geoip.location.lon
geoip.longitude
January 13th 2015, 00:00:00.000 - January 15th 2015, 23:59:59.999 —
Auto
Count
@timestamp per hour
Time
request
response
January 15th 2015, 02:46:07.000 /zoomstats/libs/dbmax/mysql.php?GLOBALS['lib']['db']['path']=http://www.google.com/humans.txt? 404
January 15th 2015, 02:46:04.000 /ytb/cuenta/cuerpo.php?base_archivo=http://www.google.com/humans.txt? 404
January 15th 2015, 02:46:04.000 /zipndownload.php?PP_PATH=http://www.google.com/humans.txt? 404
January 15th 2015, 02:46:04.000 /yrch/plugins/metasearch/plug.inc.php?path=http://www.google.com/humans.txt? 404
January 15th 2015, 02:46:00.000 /xt_counter.php?server_base_dir=http://www.google.com/humans.txt? 404
January 15th 2015, 02:46:00.000 /yabbse/Sources/Packages.php?sourcedir=http://www.google.com/humans.txt? 404
January 15th 2015, 02:46:00.000 /yacs/scripts/update_trailer.php?context[path_to_root]=http://www.google.com/humans.txt? 404
January 15th 2015, 02:46:00.000 /xoopsgallery/init_basic.php?GALLERY_BASEDIR=http://www.google.com/humans.txt? 404
January 15th 2015, 02:45:59.000 /xarg_corner.php?xarg=http://www.google.com/humans.txt? 404
January 15th 2015, 02:45:59.000 /wp-content/plugins/wp-table/js/wptable-button.phpp?wpPATH=http://www.google.com/humans.txt? 404
January 15th 2015, 02:45:59.000 /xarg_corner_bottom.php?xarg=http://www.google.com/humans.txt? 404
January 15th 2015, 02:45:59.000 /wsk/wsk.php?wsk=http://www.google.com/humans.txt? 404
January 15th 2015, 02:45:59.000 /xarg_corner_top.php?xarg=http://www.google.com/humans.txt? 404
January 15th 2015, 02:45:55.000 /wp-content/plugins/wordtube/wordtube-button.php?wpPATH=http://www.google.com/humans.txt? 404
January 15th 2015, 02:45:55.000 /wp-content/plugins/dm-albums/template/album.php?SECURITY_FILE=http://www.google.com/humans.txt? 404

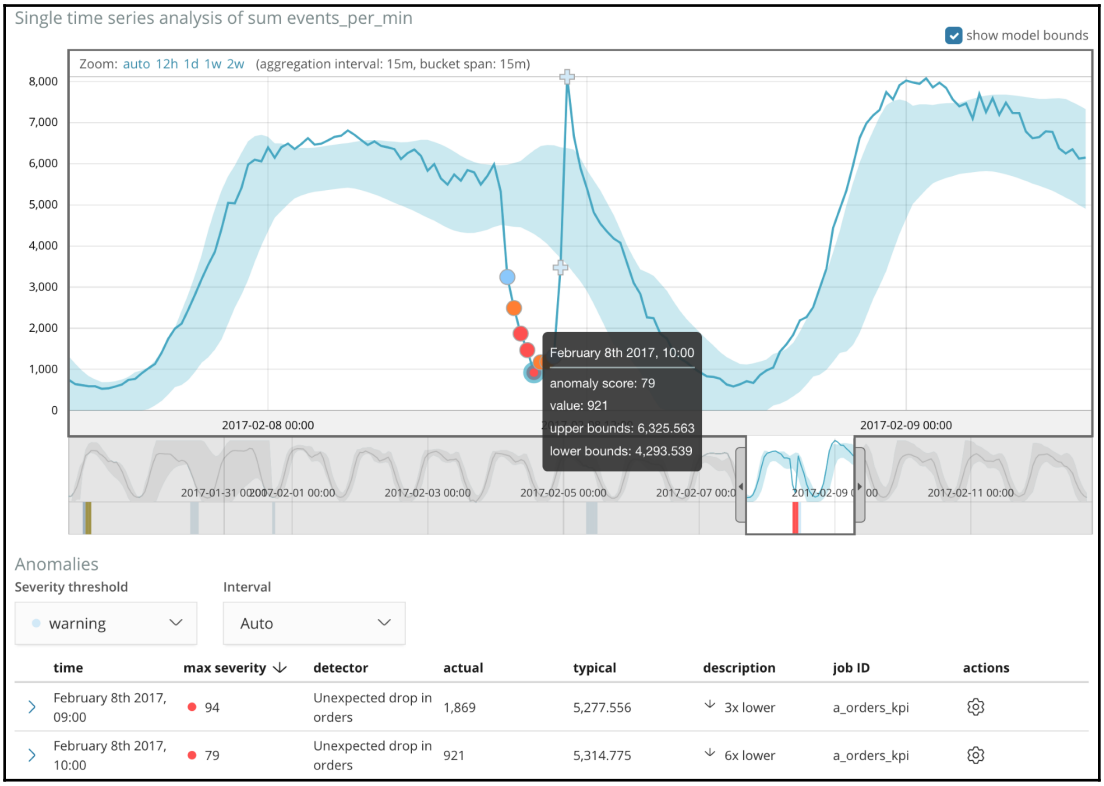

Add new detector
Description
Rare Country
function
rare
field_name
by_field_name
geoip.country_name
over_field_name
partition_field_name
exclude_frequent
Help for rare
Add
Cancel

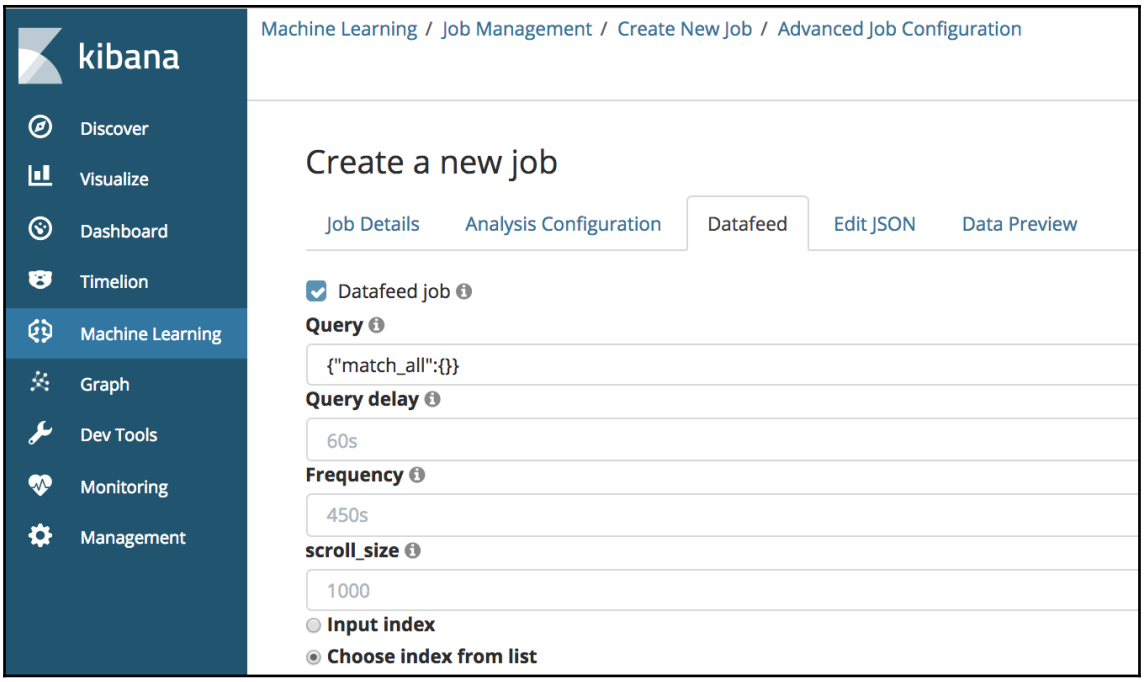

Create a new job
Job Details
Analysis Configuration
Datafeed
Edit JSON
Data Preview
bucket_span
10m
summary_count_field_name
categorization_field_name
message
Categorization Filters
+ Add Categorization Filter
Detectors
+ Add Detector

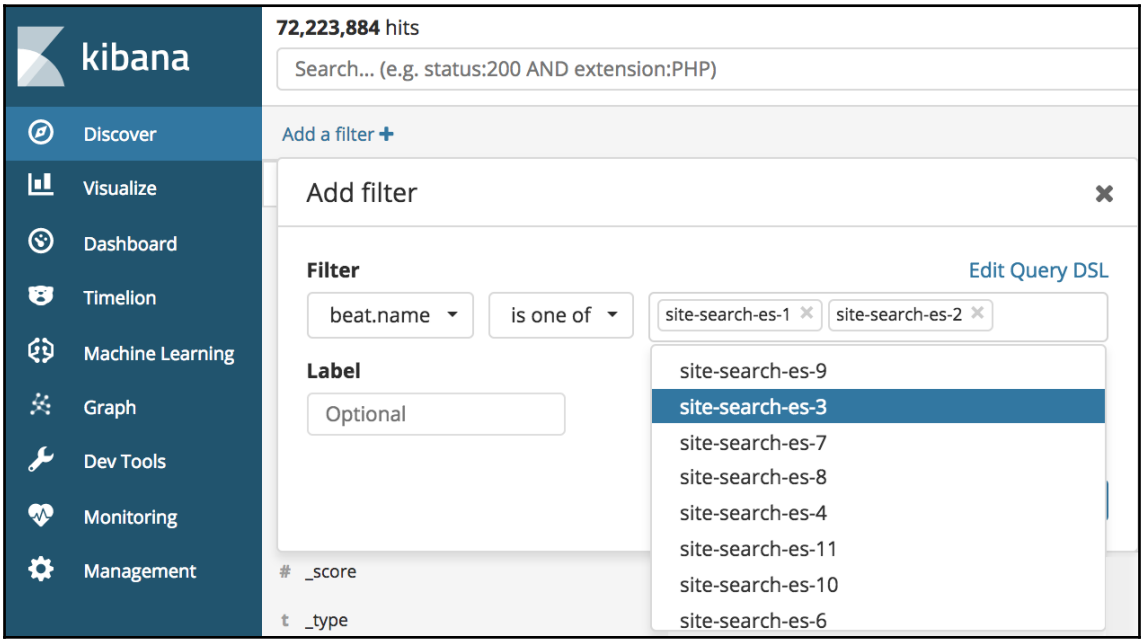

Add new detector
Description
count by mlcategory
function
count
field_name
by_field_name
mlcategory
over_field_name
partition_field_name
exclude_frequent
Help for count
Add
Cancel

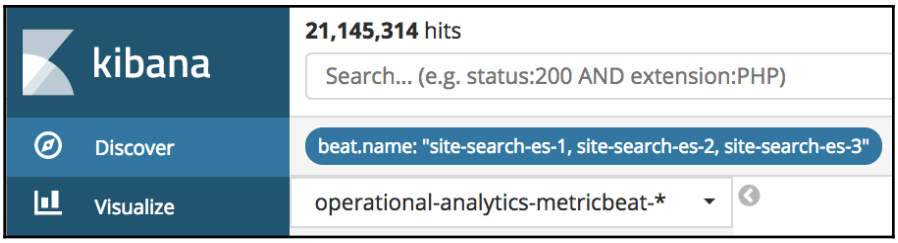

Anomaly timeline
Overall
Feb 01 11:00 Feb 02 03:00 Feb 02 19:00 Feb 03 11:00 Feb 04 03:00 Feb 04 19:00 Feb 05 11:00 Feb 06 03:00 Feb 06 19:00 Feb 07 11:00 Feb 08 03:00 Feb 08 19:00 Feb 09 11:00 Feb 10 03:00 Feb 10 19:00 Feb 11 11:00
View by: job ID (Top 10 by max anomaly score)
it_ops_logs
Feb 01 11:00 Feb 02 03:00 Feb 02 19:00 Feb 03 11:00 Feb 04 03:00 Feb 04 19:00 Feb 05 11:00 Feb 06 03:00 Feb 06 19:00 Feb 07 11:00 Feb 08 03:00 Feb 08 19:00 Feb 09 11:00 Feb 10 03:00 Feb 10 19:00 Feb 11 11:00
Anomalies
Severity threshold: warning Interval: Auto
time max severity detector found for actual typical description job ID links category examples
February 8th 2016, 10:00 72 count by mlcategory mlcategory 11 12 0.0135001 More than 100x higher it_ops_logs Open link Fail To Connect Database ReActivate Application / Check Connection Strin
February 8th 2016, 10:00 72 count by mlcategory mlcategory 10 12 0.0135001 More than 100x higher it_ops_logs Open link DBMS ERROR : db=10.16.1.63!svc_prod#uid=dbadmin1;pwd=##### Err=-
DBMS ERROR : db=svc_prod Err=-17 [Microsoft][ODBC SQL Server Driver][
February 8th 2016, 10:00 43 count by mlcategory mlcategory 9 1 0.00230968 More than 100x higher it_ops_logs Open link DB Not Updated [Master] Table;dbhost=dbserver.acme.com;physicalhost=
February 8th 2016, 05:00 17 count by mlcategory mlcategory 6 1 0.00341545 More than 100x higher it_ops_logs Open link Transaction Match In DB / Duplicate Transaction;dbhost=dbserver.acme.c
February 8th 2016, 09:00 9 count by mlcategory mlcategory 6 1 0.00445653 More than 100x higher it_ops_logs Open link Transaction Match In DB / Duplicate Transaction;dbhost=dbserver.acme.c
February 8th 2016, 10:00 5 count by mlcategory mlcategory 2 12 0.0168509 More than 100x higher it_ops_logs Open link REC Not INSERTED [DB TRAN] Table;dbhost=dbserver.acme.com;physicalH
February 8th 2016, 10:00 3 count by mlcategory mlcategory 4 2 0.013726 More than 100x higher it_ops_logs Open link 012 Head Office Link Active 127.0.0.1;dbhost=dbserver.acme.com;physica
February 8th 2016, 10:00 1 count by mlcategory mlcategory 5 13 0.0205834 More than 100x higher it_ops_logs Open link Opening Database = DRIVER={SQL Server};SERVER=10.16.1.63;network=dt
Opening Database = DRIVER={SQL Server};SERVER=127.0.0.1;network=dbr
Opening Database = DRIVER={SQL Server};SERVER=ssvcdbj1.acme.com;n
February 8th 2016, 10:00 1 count by mlcategory mlcategory 3 1 0.00828766 More than 100x higher it_ops_logs Open link Using: 10.16.1.63!svc_prod#uid=dbadmin1;pwd=#####;dbhost=dbserver.
Using: sssvcdbj1.acme.com!svc_prod#uid=dbadmin1;pwd=#####;dbhost
February 8th 2016, 06:00 < 1 count by mlcategory mlcategory 7 1 0.00952828 More than 100x higher it_ops_logs Open link Actual Transaction Not Found In DB To VOID;dbhost=dbserver.acme.com;

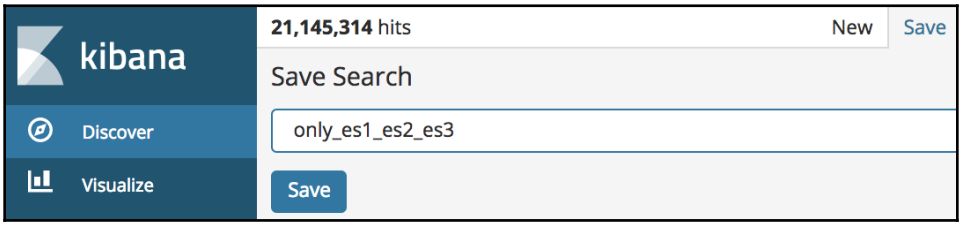
Chapter 4: IT Operational Analytics and Root Cause Analysis

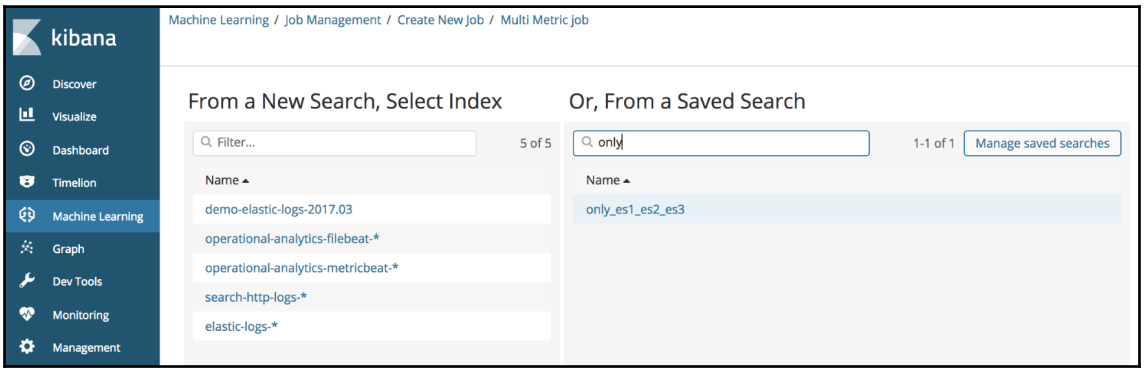


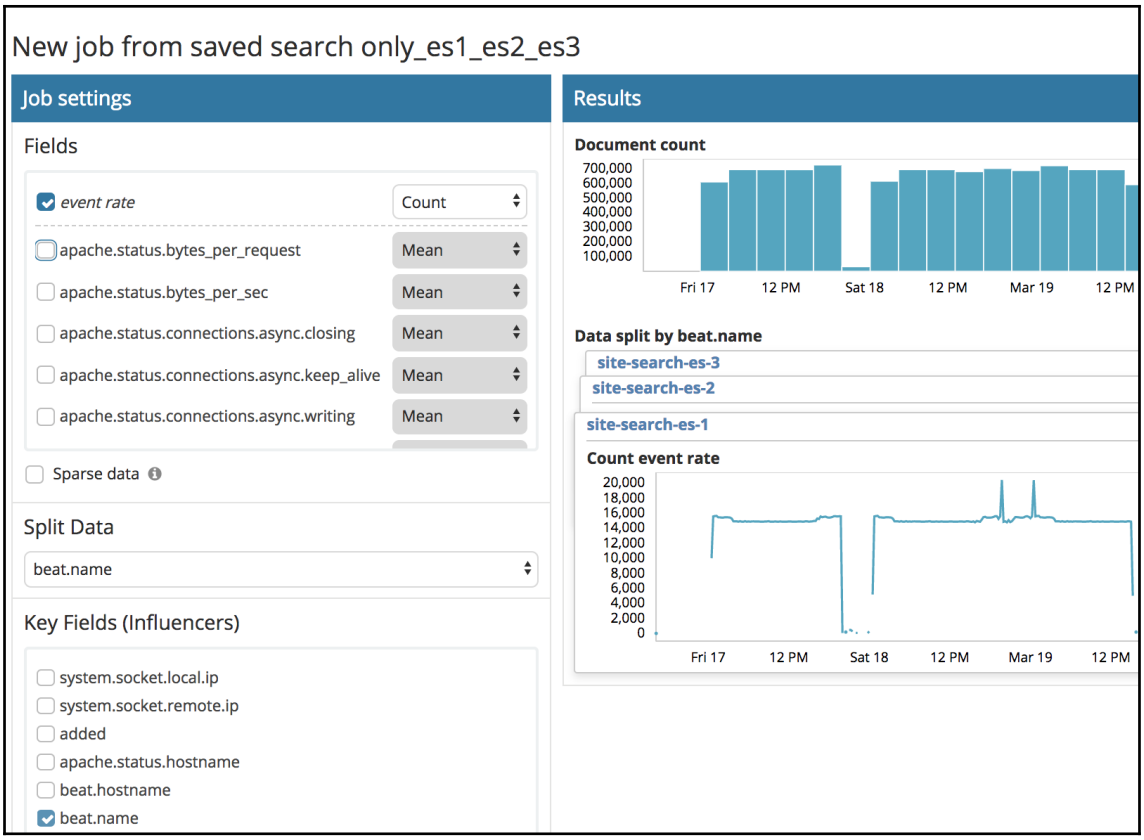

kibana
Discover
Visualize
Dashboard
Timelion
Machine Learning
Graph
Dev Tools
Monitoring
Management
Machine Learning / Job Management / Create New Job / Advanced Job Configuration
Create a new job
Job Details
Analysis Configuration
Datafeed
Edit JSON
Data Preview
Datafeed job
Query
{"match_all":{}}
Query delay
60s
Frequency
450s
scroll_size
1000
Input index
Choose index from list

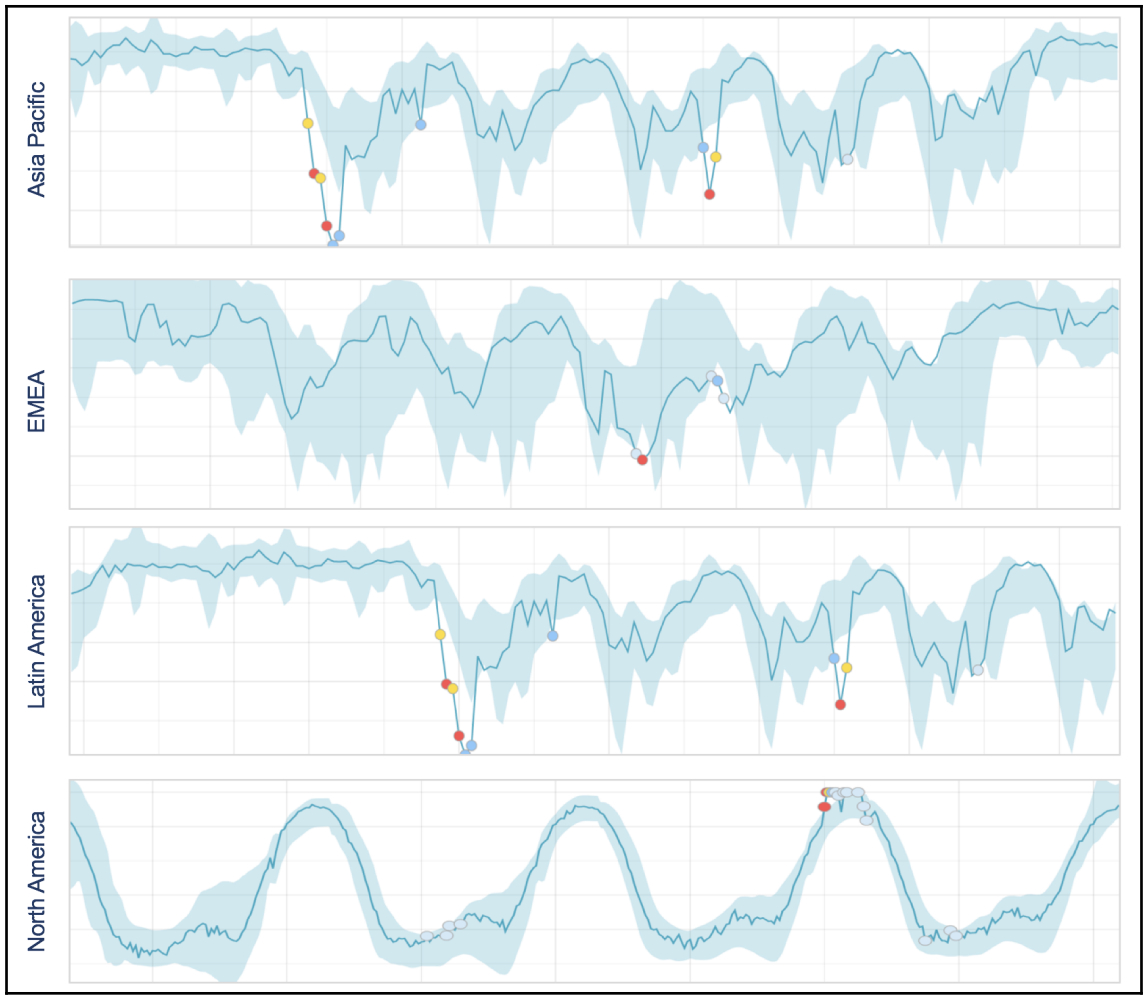

kibana
Discover
Visualize
Dashboard
Timelion
Machine Learning
Graph
Dev Tools
Monitoring
Management
72,223,884 hits
Search... (e.g. status:200 AND extension:PHP)
Add a filter +
Add filter
Filter
Edit Query DSL
beat.name
is one of
site-search-es-1
site-search-es-2
Label
Optional
site-search-es-9
site-search-es-3
site-search-es-7
site-search-es-8
site-search-es-4
site-search-es-11
site-search-es-10
site-search-es-6
_score
t _type

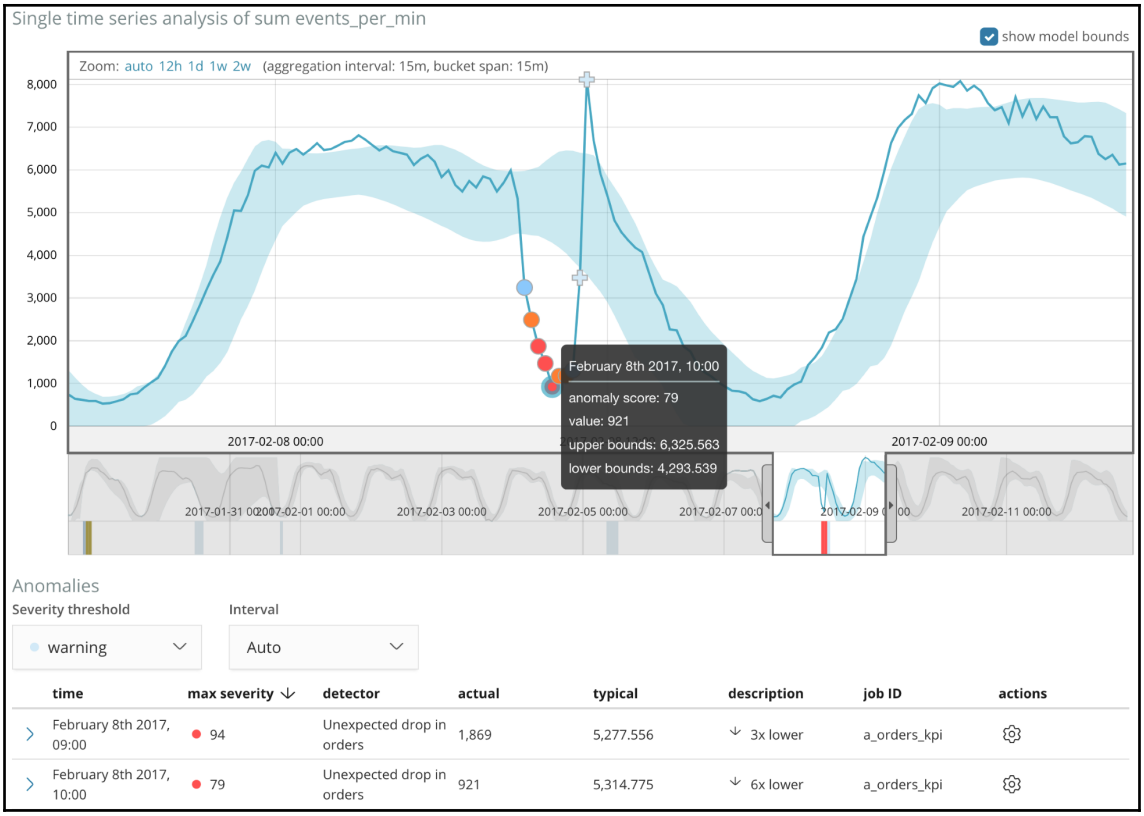

kibana
21,145,314 hits
Search... (e.g. status:200 AND extension:PHP)
Discover
beat.name: "site-search-es-1, site-search-es-2, site-search-es-3"
Visualize
operational-analytics-metricbeat-*

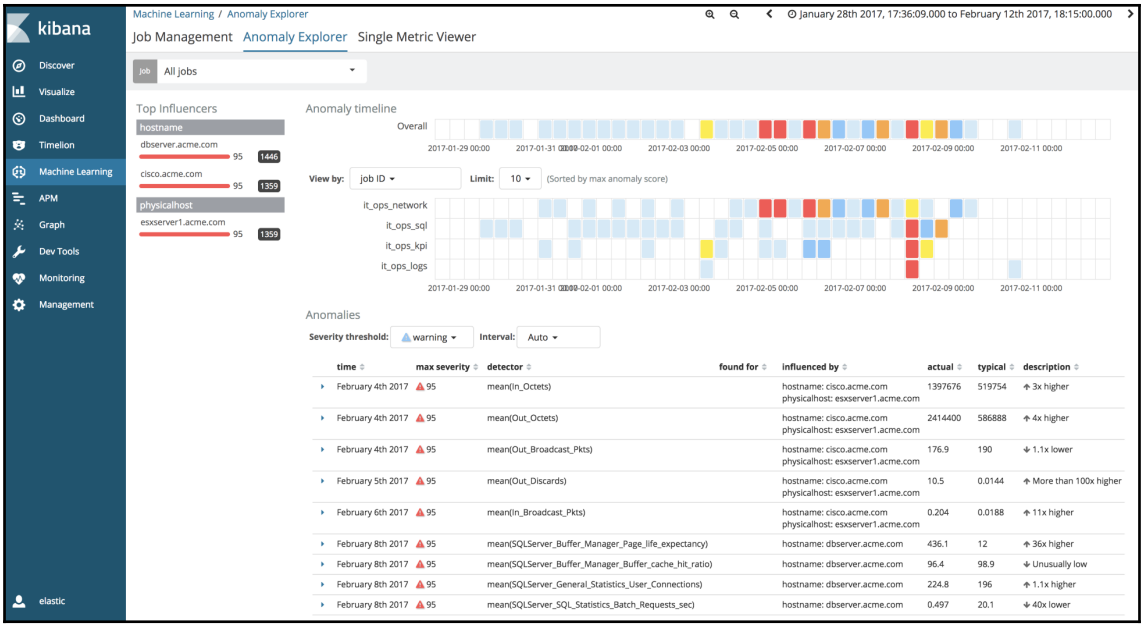

kibana
21,145,314 hits
New
Save
Save Search
Discover
only_es1_es2_es3
Visualize
Save


kibana
Machine Learning / Job Management / Create New Job / Multi Metric job
Discover
Visualize
Dashboard
Timelion
Machine Learning
Graph
Dev Tools
Monitoring
Management
From a New Search, Select Index
Filter...
5 of 5
Name
demo-elastic-logs-2017.03
operational-analytics-filebeat-*
operational-analytics-metricbeat-*
search-http-logs-*
elastic-logs-*
Or, From a Saved Search
only
1-1 of 1
Manage saved searches
Name
only_es1_es2_es3

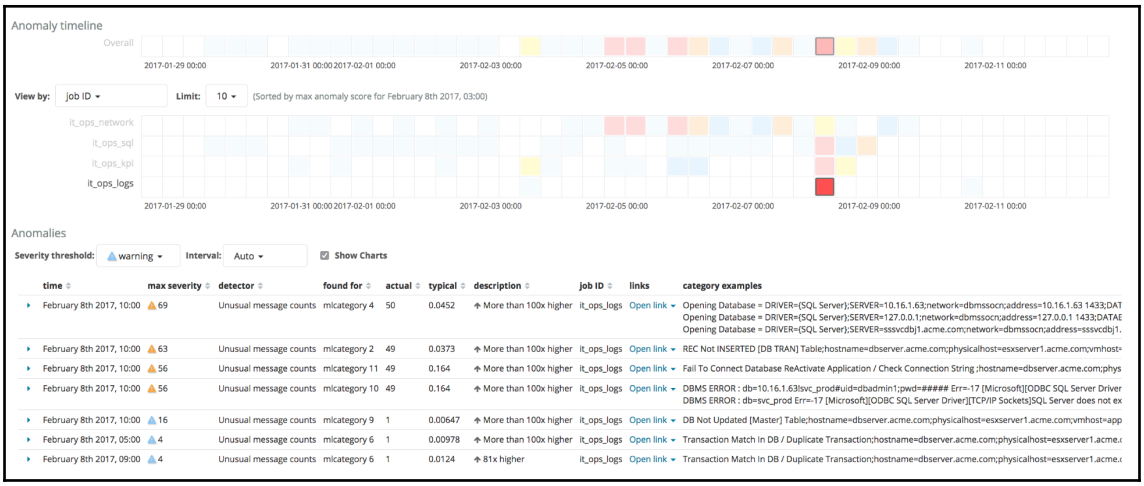

New job from saved search only_es1_es2_es3
Job settings
Fields
event rate
Count
apache.status.bytes_per_request
Mean
apache.status.bytes_per_sec
Mean
apache.status.connections.async.closing
Mean
apache.status.connections.async.keep_alive
Mean
apache.status.connections.async.writing
Mean
Sparse data
Split Data
beat.name
Key Fields (Influencers)
system.socket.local.ip
system.socket.remote.ip
added
apache.status.hostname
beat.hostname
beat.name
Results
Document count
700,000
600,000
500,000
400,000
300,000
200,000
100,000
Fri 17
12 PM
Sat 18
12 PM
Mar 19
12 PM
Data split by beat.name
site-search-es-3
site-search-es-2
site-search-es-1
Count event rate
20,000
18,000
16,000
14,000
12,000
10,000
8,000
6,000
4,000
2,000
0
Fri 17
12 PM
Sat 18
12 PM
Mar 19
12 PM


Asia Pacific
EMEA
Latin America
North America

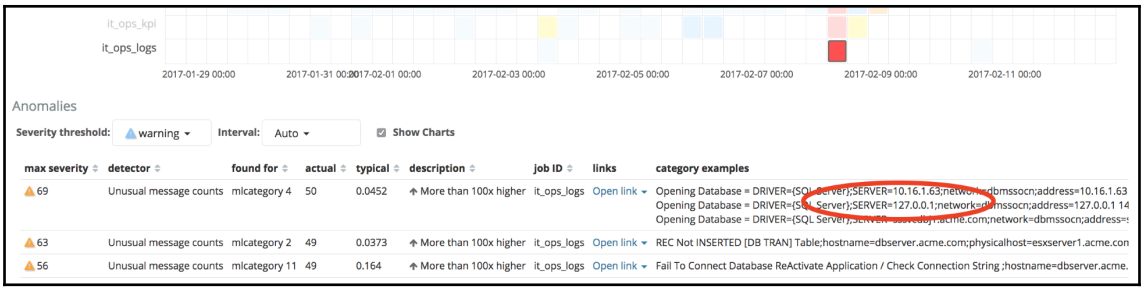

Single time series analysis of sum events_per_min
show model bounds
Zoom: auto 12h 1d 1w 2w (aggregation interval: 15m, bucket span: 15m)
8,000
7,000
6,000
5,000
4,000
3,000
2,000
1,000
0
2017-02-08 00:00
2017-02-09 00:00
February 8th 2017, 10:00
anomaly score: 79
value: 921
upper bounds: 6,325.563
lower bounds: 4,293.539
2017-01-31 00:00
2017-02-01 00:00
2017-02-03 00:00
2017-02-05 00:00
2017-02-07 00:00
2017-02-11 00:00
Anomalies
Severity threshold
warning
Interval
Auto
time
max severity
detector
actual
typical
description
job ID
actions
February 8th 2017, 09:00
94
Unexpected drop in orders
1,869
5,277.556
3x lower
a_orders_kpi
February 8th 2017, 10:00
79
Unexpected drop in orders
921
5,314.775
6x lower
a_orders_kpi

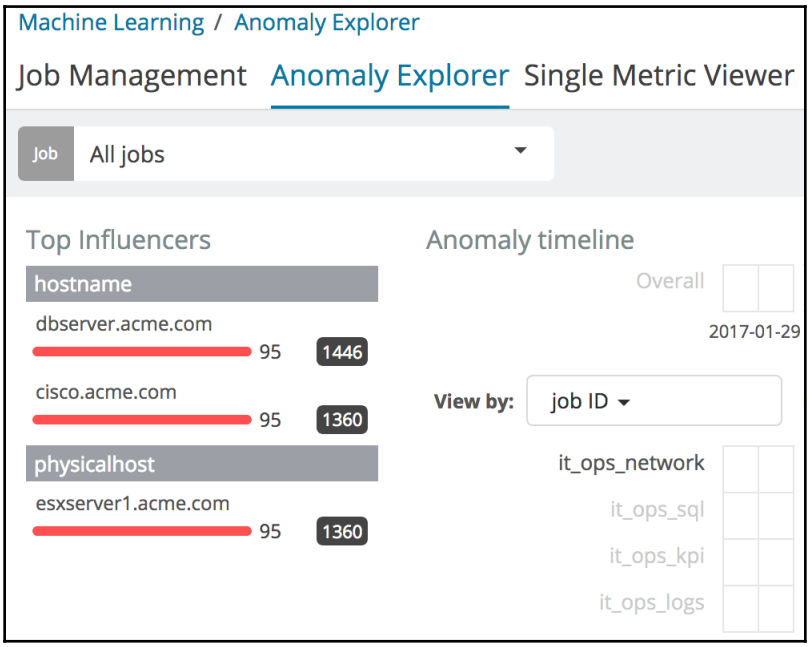

kibana
Discover
Visualize
Dashboard
Timelion
Machine Learning
APM
Graph
Dev Tools
Monitoring
Management
elastic
Machine Learning / Anomaly Explorer
January 28th 2017, 17:36:09.000 to February 12th 2017, 18:15:00.000
Job Management
Anomaly Explorer
Single Metric Viewer
Job
All jobs
Top Influencers
hostname
dbserver.acme.com
95
1446
cisco.acme.com
95
1359
physicalhost
esxserver1.acme.com
95
1359
Anomaly timeline
Overall
2017-01-29 00:00
2017-01-31 00:00
2017-02-01 00:00
2017-02-03 00:00
2017-02-05 00:00
2017-02-07 00:00
2017-02-09 00:00
2017-02-11 00:00
View by:
job ID
Limit:
10
(Sorted by max anomaly score)
it_ops_network
it_ops_sql
it_ops_kpi
it_ops_logs
Anomalies
Severity threshold:
warning
Interval:
Auto
time
max severity
detector
found for
influenced by
actual
typical
description
February 4th 2017
95
mean(In_Octets)
hostname: cisco.acme.com
physicalhost: esxserver1.acme.com
1397676
519754
3x higher
February 4th 2017
95
mean(Out_Octets)
hostname: cisco.acme.com
physicalhost: esxserver1.acme.com
2414400
586888
4x higher
February 4th 2017
95
mean(Out_Broadcast_Pkts)
hostname: cisco.acme.com
physicalhost: esxserver1.acme.com
176.9
190
1.1x lower
February 5th 2017
95
mean(Out_Discards)
hostname: cisco.acme.com
physicalhost: esxserver1.acme.com
10.5
0.0144
More than 100x higher
February 6th 2017
95
mean(In_Broadcast_Pkts)
hostname: cisco.acme.com
physicalhost: esxserver1.acme.com
0.204
0.0188
11x higher
February 8th 2017
95
mean(SQLServer_Buffer_Manager_Page_life_expectancy)
hostname: dbserver.acme.com
436.1
12
36x higher
February 8th 2017
95
mean(SQLServer_Buffer_Manager_Buffer_cache_hit_ratio)
hostname: dbserver.acme.com
96.4
98.9
Unusually low
February 8th 2017
95
mean(SQLServer_General_Statistics_User_Connections)
hostname: dbserver.acme.com
224.8
196
1.1x higher
February 8th 2017
95
mean(SQLServer_SQL_Statistics_Batch_Requests_sec)
hostname: dbserver.acme.com
0.497
20.1
40x lower


Machine Learning / Anomaly Explorer
January 28th 2017, 17:36:09.000 to February 12th 2017, 18:15:00.000
Job Management
Anomaly Explorer
Single Metric Viewer
All jobs
All jobs selected
Top Influencers
hostname
dbserver.acme.com
95
1446
cisco.acme.com
95
1360
physicalhost
esxserver1.acme.com
95
1360
Anomaly timeline
View by:
job ID
Limit:
10
(Sorted by max anomaly score for February 8th 2017, 03:00)
Anomalies
Severity threshold:
warning
Interval:
Auto
Show Charts
mean(SQLServer_SQL_Statistics_Batch_Requests_sec)
mean(SQLServer_General_Statistics_User_Connections)
mean(SQLServer_Buffer_Manager_Page_life_expectancy)
mean(SQLServer_Buffer_Manager_Buffer_cache_hit_ratio)
View
time
max severity
detector
influenced by
actual
typical
description
job ID
links
February 8th 2017, 03:00
95
mean(SQLServer_SQL_Statistics_Batch_Requests_sec)
hostname: dbserver.acme.com
0.497
20.1
40x lower
it_ops_sql
Open link
February 8th 2017, 03:00
95
mean(SQLServer_Buffer_Manager_Page_life_expectancy)
hostname: dbserver.acme.com
436.1
12
36x higher
it_ops_sql
Open link

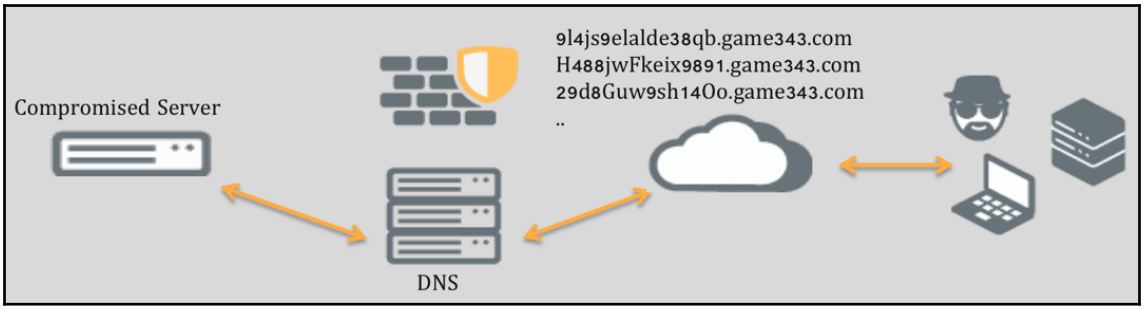

Anomaly timeline
Overall
2017-01-29 00:00
2017-01-31 00:00
2017-02-01 00:00
2017-02-03 00:00
2017-02-05 00:00
2017-02-07 00:00
2017-02-09 00:00
2017-02-11 00:00
View by: job ID
Limit: 10
(Sorted by max anomaly score for February 8th 2017, 03:00)
it_ops_network
it_ops_sql
it_ops_kpi
it_ops_logs
Anomalies
Severity threshold: warning
Interval: Auto
Show Charts
time
max severity
detector
found for
actual
typical
description
job ID
links
category examples
February 8th 2017, 10:00 69 Unusual message counts mlcategory 4 50 0.0452 More than 100x higher it_ops_logs Open link Opening Database = DRIVER={SQL Server};SERVER=10.16.1.63;network=dbmssocn;address=10.16.1.63 1433;DAT
Opening Database = DRIVER={SQL Server};SERVER=127.0.0.1;network=dbmssocn;address=127.0.0.1 1433;DATAE
Opening Database = DRIVER={SQL Server};SERVER=ssvcdbj1.acme.com;network=dbmssocn;address=ssvcdbj1.
February 8th 2017, 10:00 63 Unusual message counts mlcategory 2 49 0.0373 More than 100x higher it_ops_logs Open link REC Not INSERTED [DB TRAN] Table;hostname=dbserver.acme.com;physicalhost=esxserver1.acme.com;vmhost=
February 8th 2017, 10:00 56 Unusual message counts mlcategory 11 49 0.164 More than 100x higher it_ops_logs Open link Fail To Connect Database ReActivate Application / Check Connection String ;hostname=dbserver.acme.com;phys
February 8th 2017, 10:00 56 Unusual message counts mlcategory 10 49 0.164 More than 100x higher it_ops_logs Open link DBMS ERROR : db=10.16.1.63|svc_prod#uid=dbadmin1;pwd=##### Err=-17 [Microsoft][ODBC SQL Server Driver
DBMS ERROR : db=svc_prod Err=-17 [Microsoft][ODBC SQL Server Driver][TCP/IP Sockets]SQL Server does not ex
February 8th 2017, 10:00 16 Unusual message counts mlcategory 9 1 0.00647 More than 100x higher it_ops_logs Open link DB Not Updated [Master] Table;hostname=dbserver.acme.com;physicalhost=esxserver1.acme.com;vmhost=app
February 8th 2017, 05:00 4 Unusual message counts mlcategory 6 1 0.00978 More than 100x higher it_ops_logs Open link Transaction Match In DB / Duplicate Transaction;hostname=dbserver.acme.com;physicalhost=esxserver1.acme.
February 8th 2017, 09:00 4 Unusual message counts mlcategory 6 1 0.0124 81x higher it_ops_logs Open link Transaction Match In DB / Duplicate Transaction;hostname=dbserver.acme.com;physicalhost=esxserver1.acme.

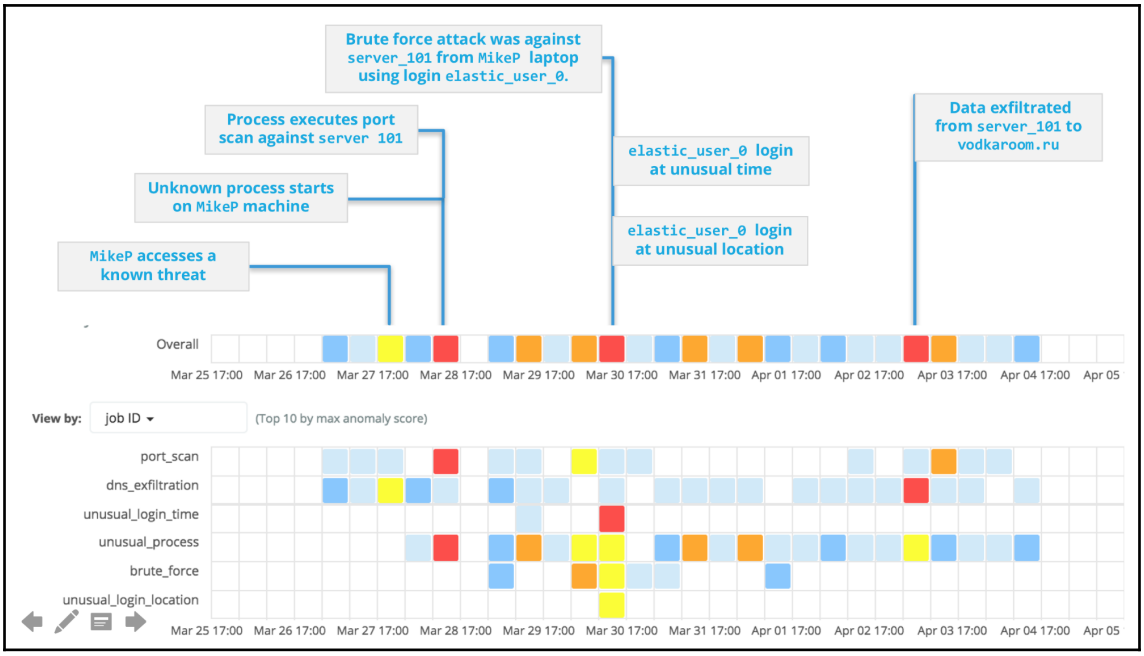

Anomaly timeline
Overall
2017-01-29 00:00
2017-01-31 00:00
2017-02-01 00:00
2017-02-03 00:00
2017-02-05 00:00
2017-02-07 00:00
2017-02-09 00:00
2017-02-11 00:00
View by: job ID
Limit: 10
(Sorted by max anomaly score for February 8th 2017, 03:00)
it_ops_network
it_ops_sql
it_ops_kpi
it_ops_logs
February 8th 2017, 03:00
job ID: it_ops_network
Max anomaly score: 30
Anomalies
Severity threshold: warning
Interval: Auto
Show Charts
mean(Out_Discards)
View
mean(In_Octets)
mean(Out_Octets)
mean(Out_Broadcast_Pkts)
2017-02-07 12:00
2017-02-08 00:00
2017-02-08 12:00
2017-02-09 00:00

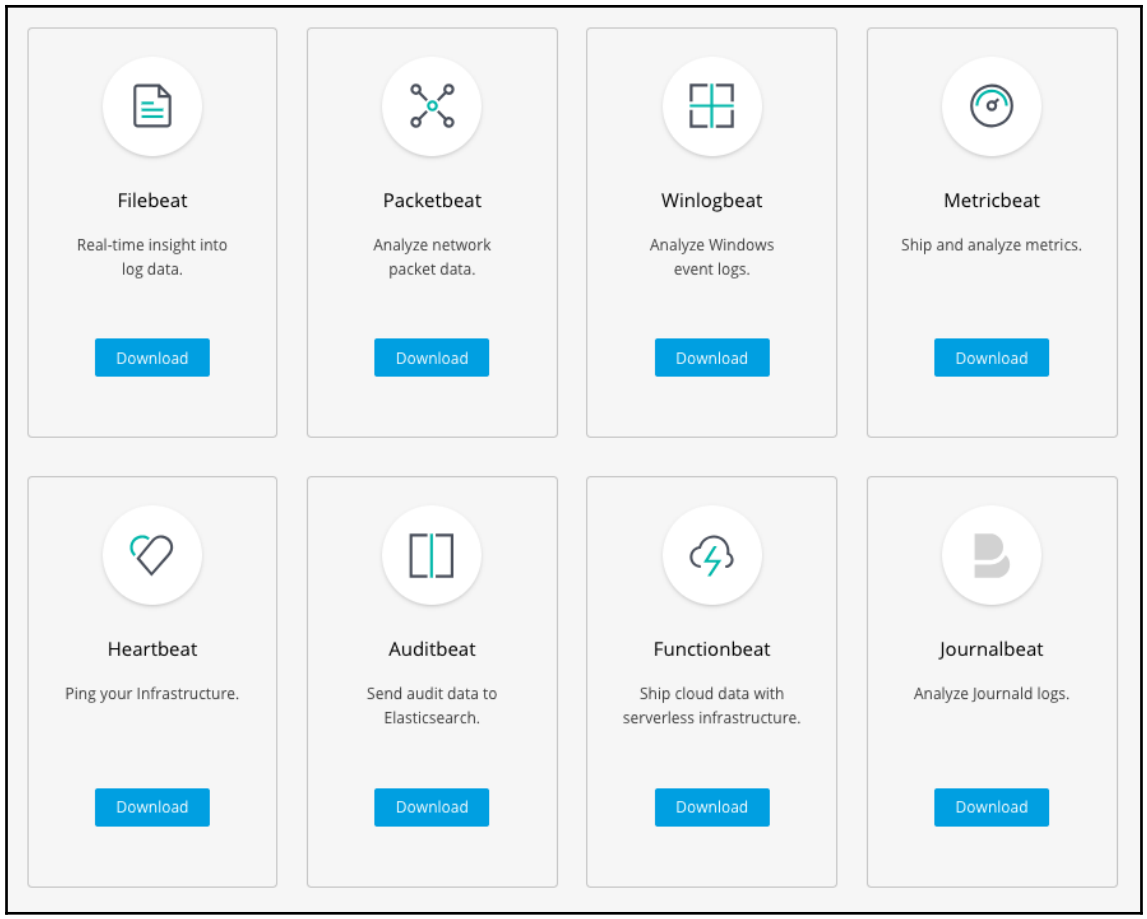

it_ops_kpi
it_ops_logs
2017-01-29 00:00
2017-01-31 00:00
2017-02-01 00:00
2017-02-03 00:00
2017-02-05 00:00
2017-02-07 00:00
2017-02-09 00:00
2017-02-11 00:00
Anomalies
Severity threshold: warning
Interval: Auto
Show Charts
max severity
detector
found for
actual
typical
description
job ID
links
category examples
69
Unusual message counts
mlcategory 4
50
0.0452
More than 100x higher
it_ops_logs
Open link
Opening Database = DRIVER={SQL Server};SERVER=10.16.1.63;network=dbmssocn;address=10.16.1.63
Opening Database = DRIVER={SQL Server};SERVER=127.0.0.1;network=dbmssocn;address=127.0.0.1 14
Opening Database = DRIVER={SQL Server};SERVER=dbserver.acme.com;network=dbmssocn;address=
63
Unusual message counts
mlcategory 2
49
0.0373
More than 100x higher
it_ops_logs
Open link
REC Not INSERTED [DB TRAN] Table;hostname=dbserver.acme.com;physicalhost=esxserver1.acme.con
56
Unusual message counts
mlcategory 11
49
0.164
More than 100x higher
it_ops_logs
Open link
Fail To Connect Database ReActivate Application / Check Connection String ;hostname=dbserver.acme.


Machine Learning / Anomaly Explorer
Job Management
Anomaly Explorer
Single Metric Viewer
Job
All jobs
Top Influencers
hostname
dbserver.acme.com
95
1446
cisco.acme.com
95
1360
physicalhost
esxserver1.acme.com
95
1360
Anomaly timeline
Overall
2017-01-29
View by:
job ID
it_ops_network
it_ops_sql
it_ops_kpi
it_ops_logs

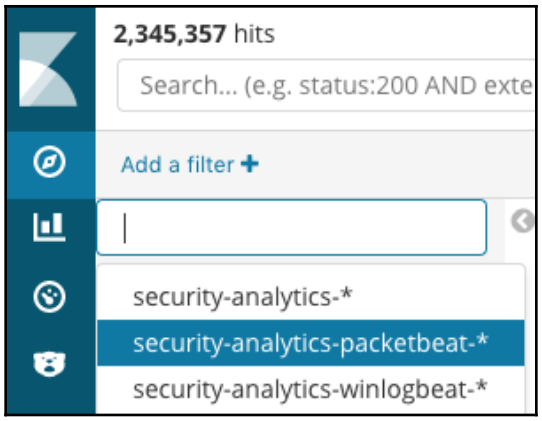
Chapter 5: Security Analytics with Elastic Machine Learning

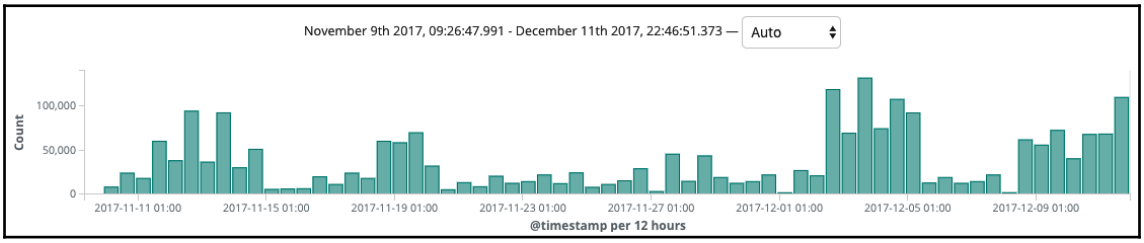


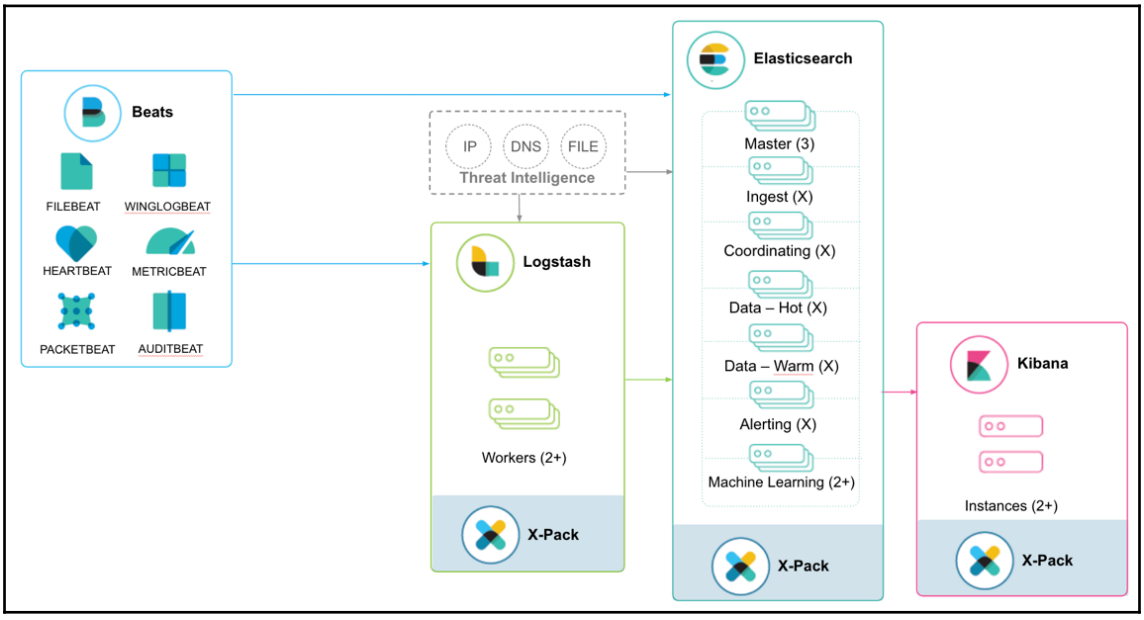


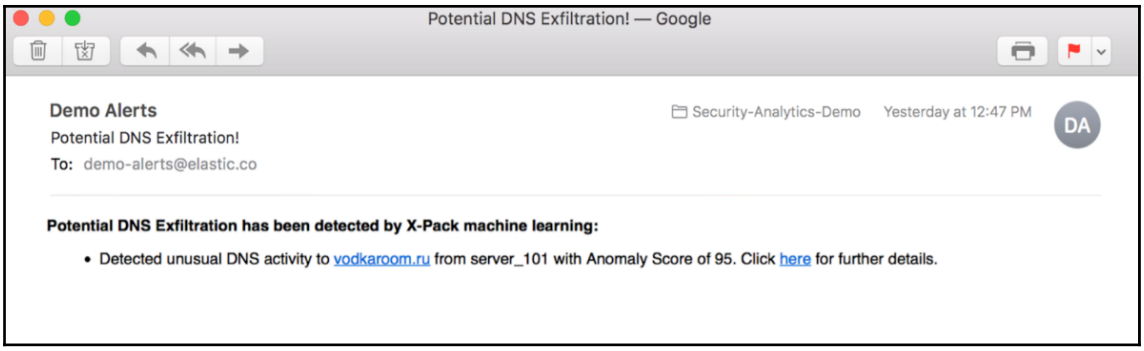

Filebeat
Real-time insight into log data.
Download
Packetbeat
Analyze network packet data.
Download
Winlogbeat
Analyze Windows event logs.
Download
Metricbeat
Ship and analyze metrics.
Download
Heartbeat
Ping your Infrastructure.
Download
Auditbeat
Send audit data to Elasticsearch.
Download
Functionbeat
Ship cloud data with serverless infrastructure.
Download
Journalbeat
Analyze Journald logs.
Download

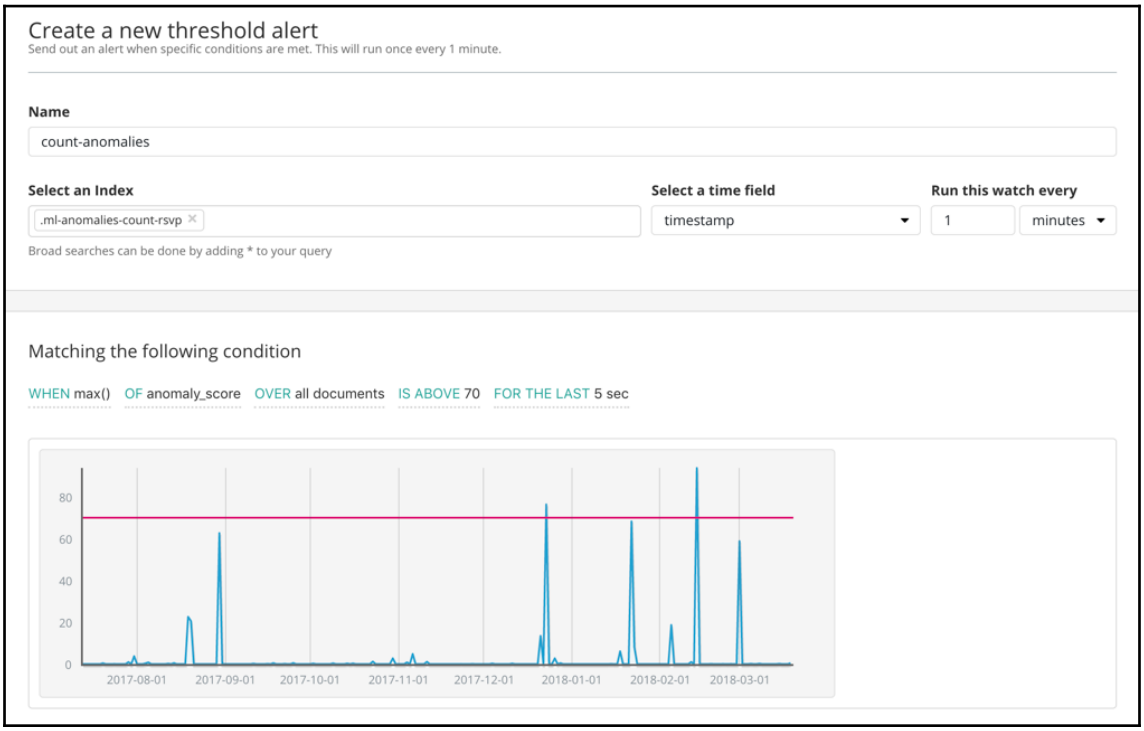
- *AMQP fields*
- *Beat fields*
- *Cassandra fields*
- *Cloud provider metadata fields*
- *Common fields*
- *DNS fields*
- *Docker fields*
- *Flow Event fields*
- *HTTP fields*
- *ICMP fields*
- *Kubernetes fields*
- *Memcache fields*
- *MongoDb fields*
- *MySQL fields*
- *NFS fields*
- *PostgreSQL fields*
- *Raw fields*
- *Redis fields*
- *Thrift-RPC fields*
- *TLS fields*
- *Transaction Event fields*
- *Measurements (Transactions) fields*

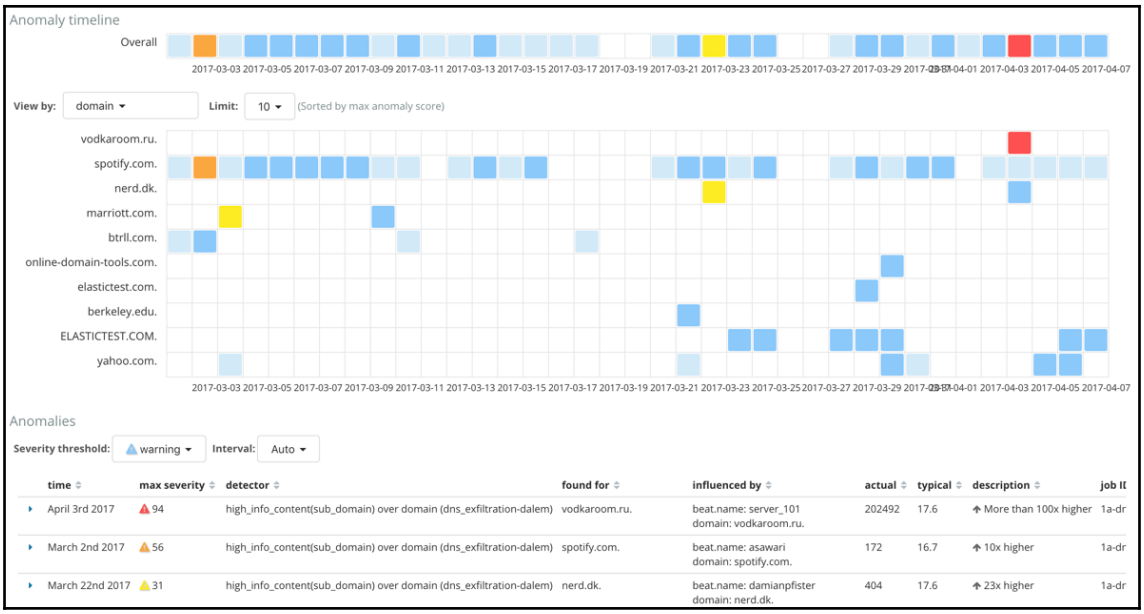

2,345,357 hits
Search... (e.g. status:200 AND exte
Add a filter +
security-analytics-*
security-analytics-packetbeat-*
security-analytics-winlogbeat-*

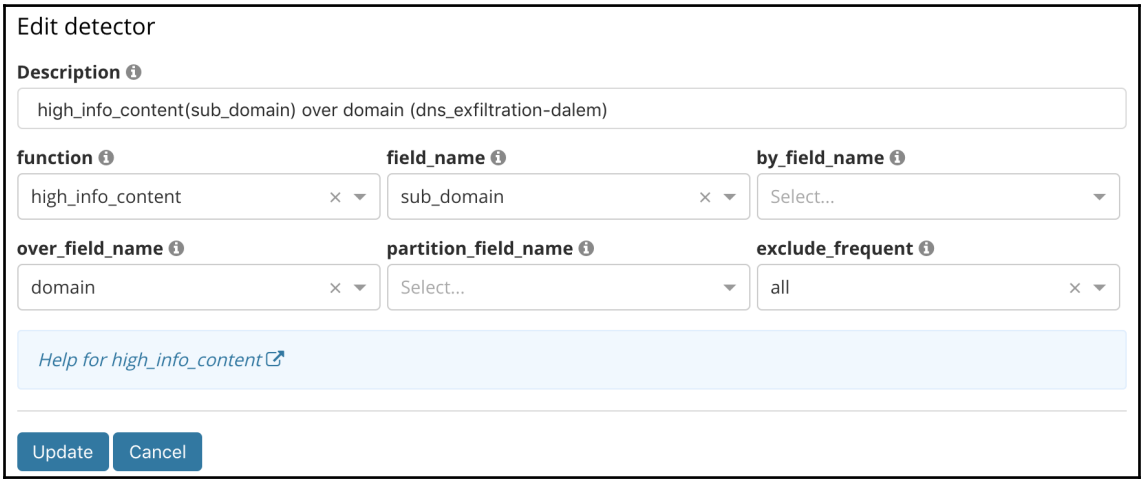

November 9th 2017, 09:26:47.991 - December 11th 2017, 22:46:51.373 —
Auto
Count
100,000
50,000
0
2017-11-11 01:00
2017-11-15 01:00
2017-11-19 01:00
2017-11-23 01:00
2017-11-27 01:00
2017-12-01 01:00
2017-12-05 01:00
2017-12-09 01:00
@timestamp per 12 hours

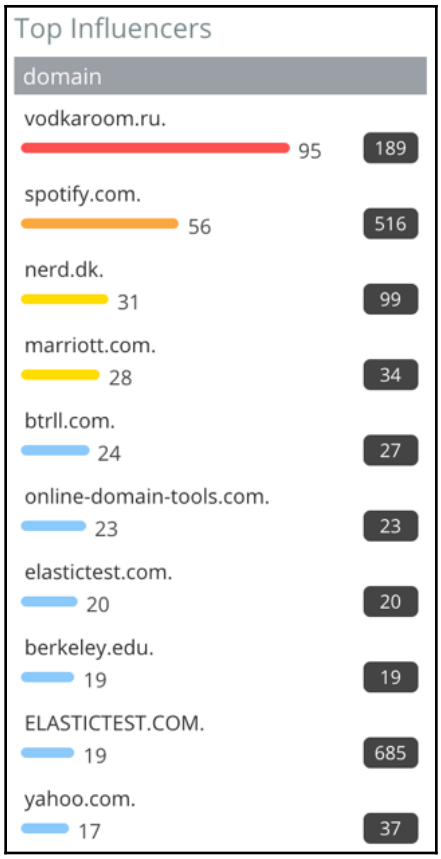

Beats
FILEBEAT
WINGLOGBEAT
HEARTBEAT
METRICBEAT
PACKETBEAT
AUDITBEAT
IP
DNS
FILE
Threat Intelligence
Logstash
Workers (2+)
X-Pack
Elasticsearch
Master (3)
Ingest (X)
Coordinating (X)
Data – Hot (X)
Data – Warm (X)
Alerting (X)
Machine Learning (2+)
X-Pack
Kibana
Instances (2+)
X-Pack

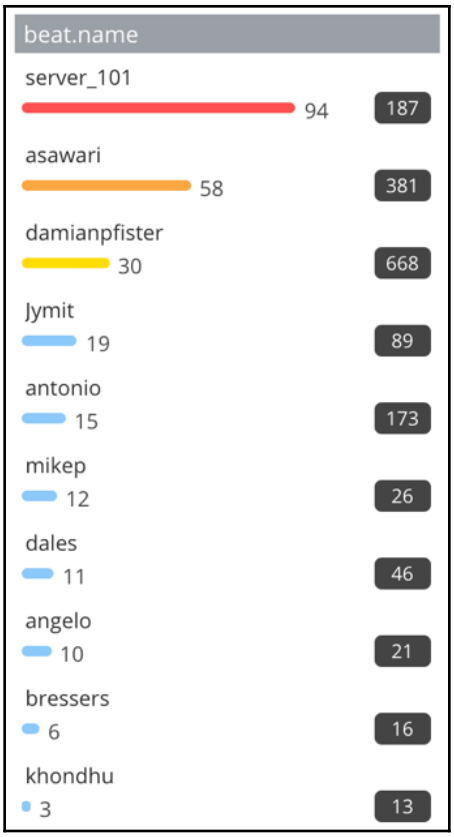

Potential DNS Exfiltration! — Google
Demo Alerts
Potential DNS Exfiltration!
To: demo-alerts@elastic.co
Security-Analytics-Demo
Yesterday at 12:47 PM
DA
Potential DNS Exfiltration has been detected by X-Pack machine learning:
Detected unusual DNS activity to vodkaroom.ru from server_101 with Anomaly Score of 95. Click here for further details.


Create a new threshold alert
Send out an alert when specific conditions are met. This will run once every 1 minute.
Name
count-anomalies
Select an Index
.ml-anomalies-count-rsvp
Broad searches can be done by adding * to your query
Select a time field
timestamp
Run this watch every
1
minutes
Matching the following condition
WHEN max() OF anomaly_score OVER all documents IS ABOVE 70 FOR THE LAST 5 sec
80
60
40
20
0
2017-08-01
2017-09-01
2017-10-01
2017-11-01
2017-12-01
2018-01-01
2018-02-01
2018-03-01


Anomaly timeline
Overall
2017-03-03 2017-03-05 2017-03-07 2017-03-09 2017-03-11 2017-03-13 2017-03-15 2017-03-17 2017-03-19 2017-03-21 2017-03-23 2017-03-25 2017-03-27 2017-03-29 2017-04-01 2017-04-03 2017-04-05 2017-04-07
View by: domain
Limit: 10
(Sorted by max anomaly score)
vodkaroom.ru.
spotify.com.
nerd.dk.
marriott.com.
btrll.com.
online-domain-tools.com.
elastictest.com.
berkeley.edu.
ELASTICTEST.COM.
yahoo.com.
2017-03-03 2017-03-05 2017-03-07 2017-03-09 2017-03-11 2017-03-13 2017-03-15 2017-03-17 2017-03-19 2017-03-21 2017-03-23 2017-03-25 2017-03-27 2017-03-29 2017-04-01 2017-04-03 2017-04-05 2017-04-07
Anomalies
Severity threshold: warning
Interval: Auto
time
max severity
detector
found for
influenced by
actual
typical
description
job ID
April 3rd 2017
94
high_info_content(sub_domain) over domain (dns_exfiltration-dalem)
vodkaroom.ru.
beat.name: server_101
domain: vodkaroom.ru.
202492
17.6
More than 100x higher
1a-dr
March 2nd 2017
56
high_info_content(sub_domain) over domain (dns_exfiltration-dalem)
spotify.com.
beat.name: asawari
domain: spotify.com.
172
16.7
10x higher
1a-dr
March 22nd 2017
31
high_info_content(sub_domain) over domain (dns_exfiltration-dalem)
nerd.dk.
beat.name: damianpfister
domain: nerd.dk.
404
17.6
23x higher
1a-dr


Edit detector
Description
high_info_content(sub_domain) over domain (dns_exfiltration-dalem)
function
high_info_content
field_name
sub_domain
by_field_name
Select...
over_field_name
domain
partition_field_name
Select...
exclude_frequent
all
Help for high_info_content
Update
Cancel


Top Influencers
domain
vodkaroom.ru.
95
189
spotify.com.
56
516
nerd.dk.
31
99
marriott.com.
28
34
btrll.com.
24
27
online-domain-tools.com.
23
23
elastictest.com.
20
20
berkeley.edu.
19
19
ELASTICTEST.COM.
19
685
yahoo.com.
17
37



time	max severity	detector	found for	influenced by	actual	typical	description
April 3rd 2017, 14:00	94	high_info_content(sub_domain) over domain (dns_exfiltration-dalem)	vodkaroom.ru.	beat.name: server_101 domain: vodkaroom.ru.	202492	17.6	More than 100x higher

Description:
critical anomaly in high_info_content(sub_domain) over domain (dns_exfiltration-dalem) found for domain vodkaroom.ru.

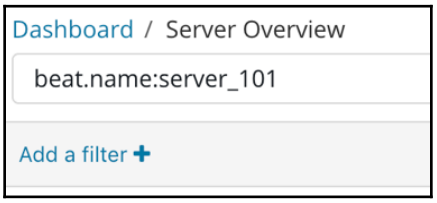
Details on highest severity anomaly:

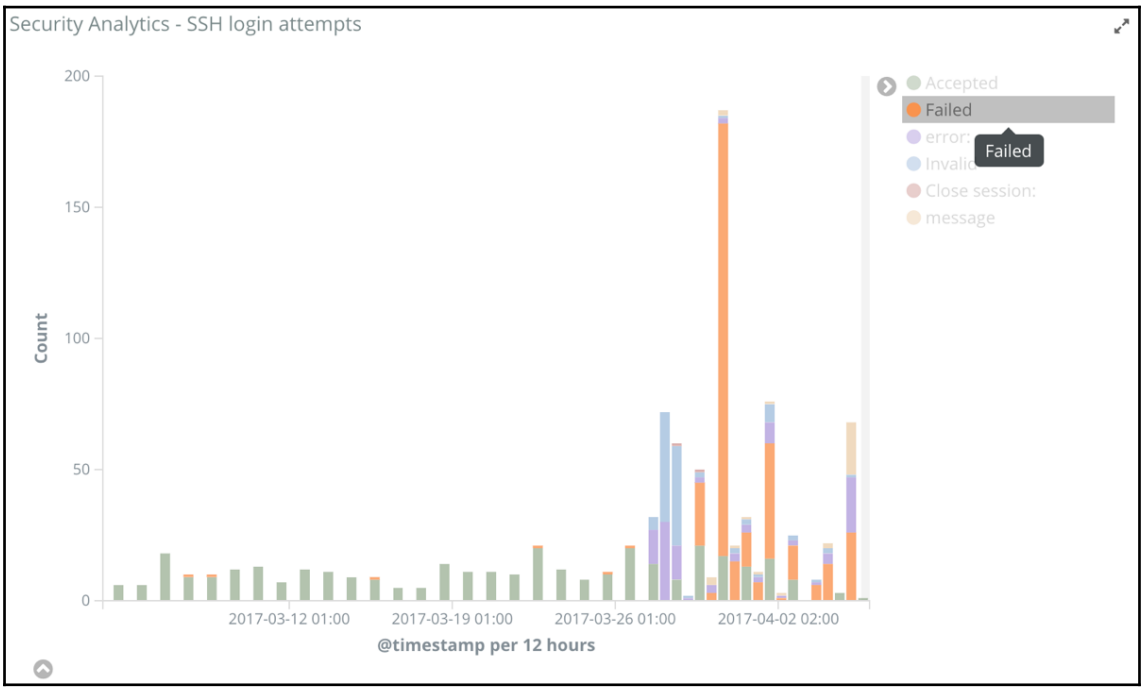
domain:	vodkaroom.ru.
time:	April 3rd 2017, 14:40:00 to April 3rd 2017, 14:45:00
function:	high_info_content
fieldName:	sub_domain
actual:	202492
typical:	17.6
job ID:	1a-dns_exfiltration
probability:	4.216341836121852e-165

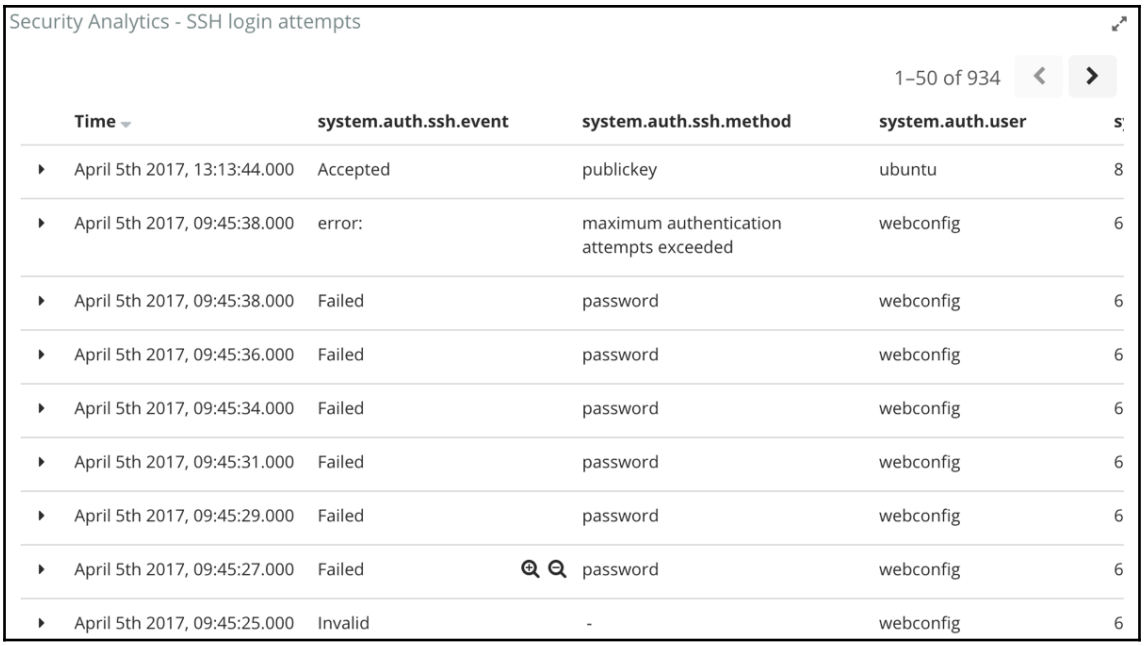
Influenced by:

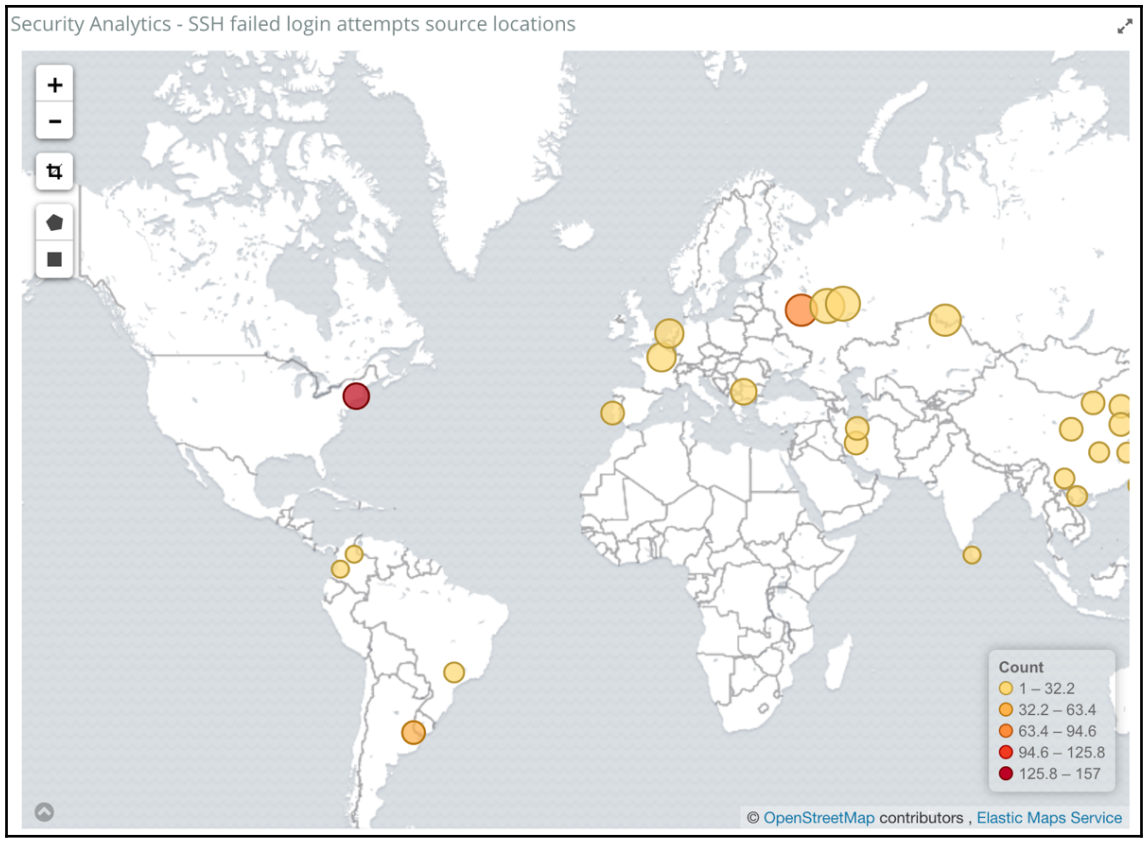
beat.name	server_101
domain	vodkaroom.ru.

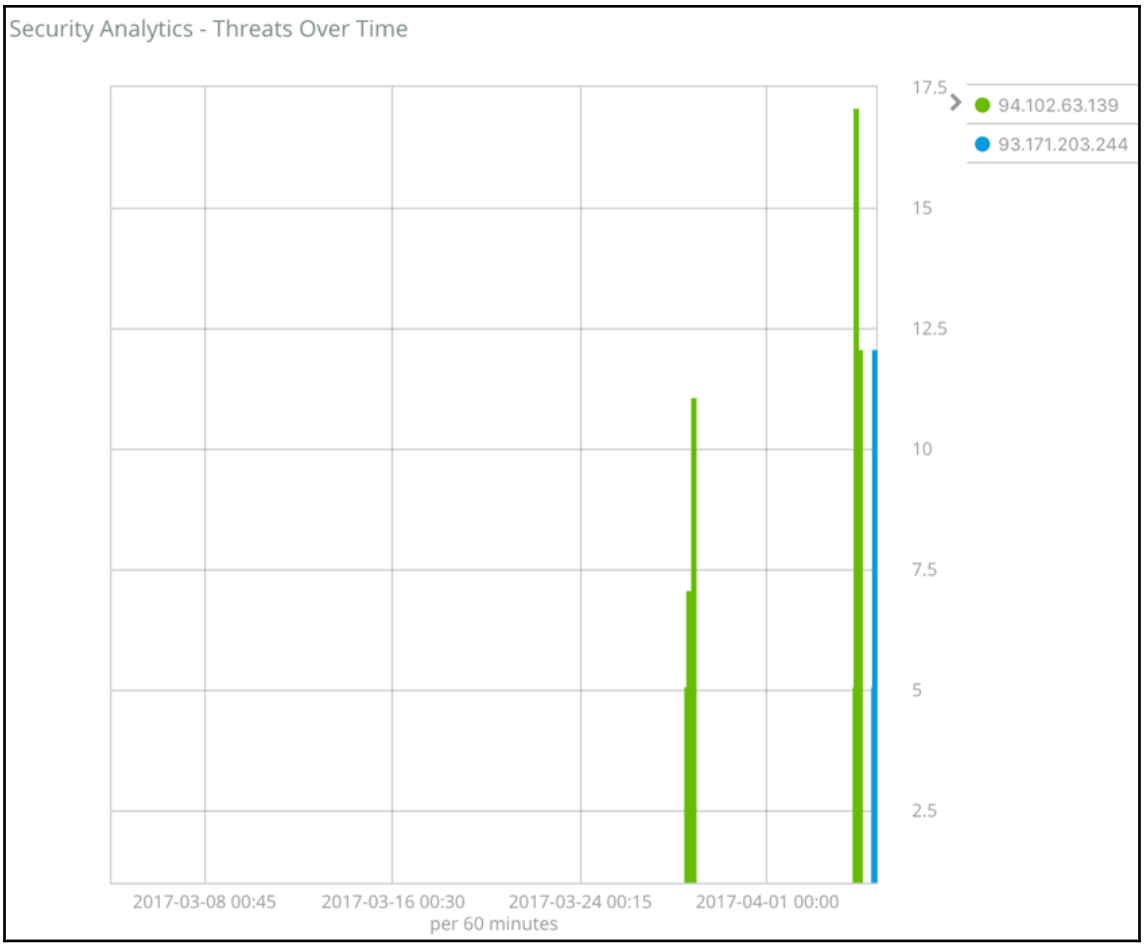

description
job ID
links
More than 100x higher
1a-dns_exfiltration
Open link
Explore Server

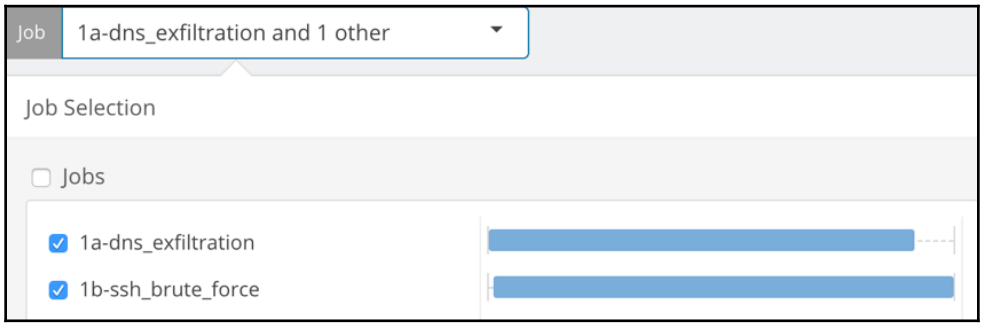

Dashboard / Server Overview
beat.name:server_101
Add a filter +

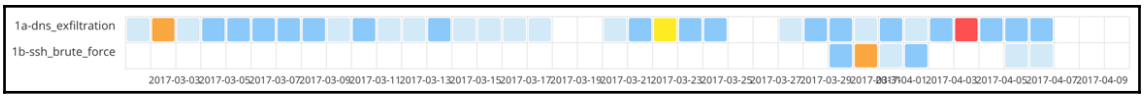

Security Analytics - SSH login attempts
200
150
100
50
0
Count
2017-03-12 01:00
2017-03-19 01:00
2017-03-26 01:00
2017-04-02 02:00
@timestamp per 12 hours
Accepted
Failed
error:
Failed
Close session:
message


Security Analytics - SSH login attempts
1–50 of 934
Time
system.auth.ssh.event
system.auth.ssh.method
system.auth.user
April 5th 2017, 13:13:44.000 Accepted publickey ubuntu 8
April 5th 2017, 09:45:38.000 error: maximum authentication attempts exceeded webconfig 6
April 5th 2017, 09:45:38.000 Failed password webconfig 6
April 5th 2017, 09:45:36.000 Failed password webconfig 6
April 5th 2017, 09:45:34.000 Failed password webconfig 6
April 5th 2017, 09:45:31.000 Failed password webconfig 6
April 5th 2017, 09:45:29.000 Failed password webconfig 6
April 5th 2017, 09:45:27.000 Failed password webconfig 6
April 5th 2017, 09:45:25.000 Invalid - webconfig 6


Security Analytics - SSH failed login attempts source locations
Count
1 – 32.2
32.2 – 63.4
63.4 – 94.6
94.6 – 125.8
125.8 – 157
© OpenStreetMap contributors , Elastic Maps Service


Security Analytics - Threats Over Time
17.5
15
12.5
10
7.5
5
2.5
94.102.63.139
93.171.203.244
2017-03-08 00:45
2017-03-16 00:30
2017-03-24 00:15
2017-04-01 00:00
per 60 minutes


Job
1a-dns_exfiltration and 1 other
Job Selection
Jobs
1a-dns_exfiltration
1b-ssh_brute_force



Top Influencers

system.auth.ssh.ip

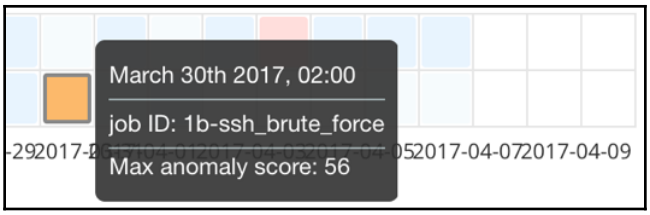
24.151.103.17	57	95
181.25.206.27	21	21
85.245.107.41	11	11
181.26.186.35	5	5
181.25.201.155	< 1	< 1
34.204.227.175	< 1	< 1
122.189.198.238	< 1	< 1
60.187.118.40	< 1	< 1
42.184.142.151	< 1	< 1
82.64.2.59	< 1	< 1

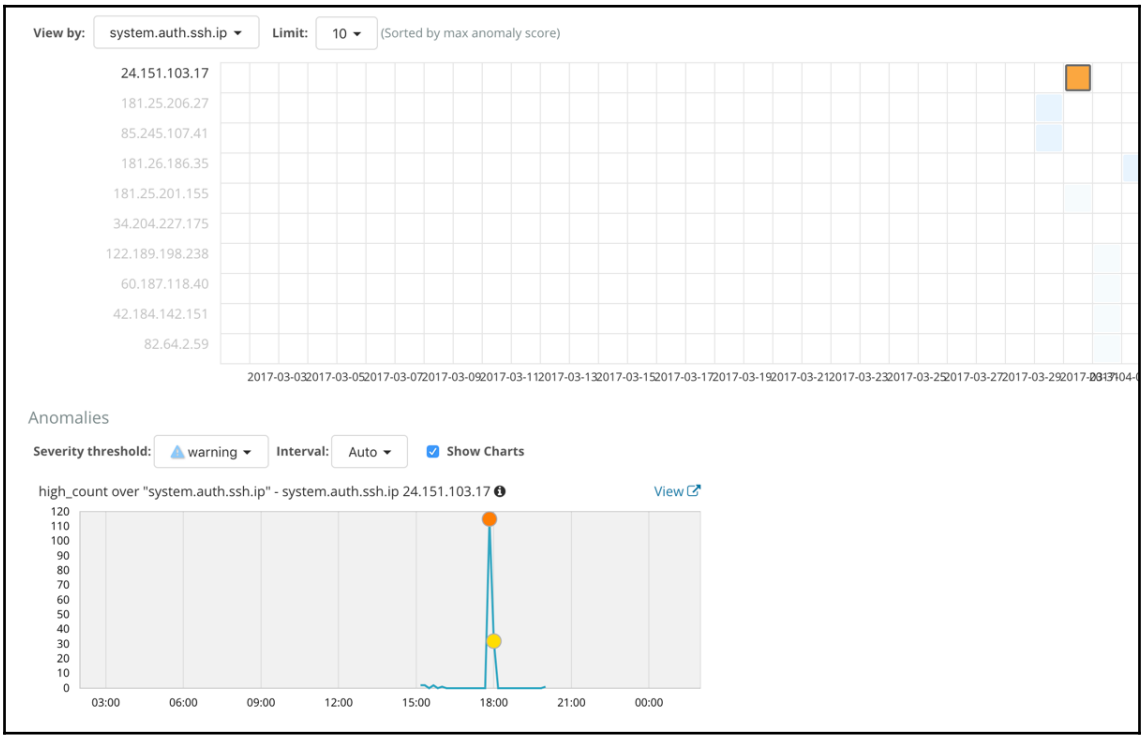
beat.name

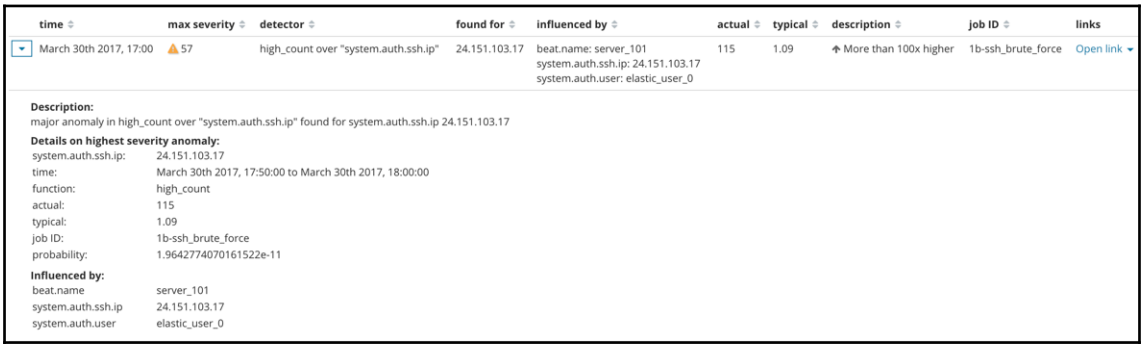
server_101	55	126

system.auth.user

elastic_user_0	55	90







time	max severity	detector	found for	influenced by	actual	typical	description	job ID	links
March 30th 2017, 17:00	57	high_count over "system.auth.ssh.ip"	24.151.103.17	beat.name: server_101 system.auth.ssh.ip: 24.151.103.17 system.auth.user: elastic_user_0	115	1.09	More than 100x higher	1b-ssh_brute_force	Open link

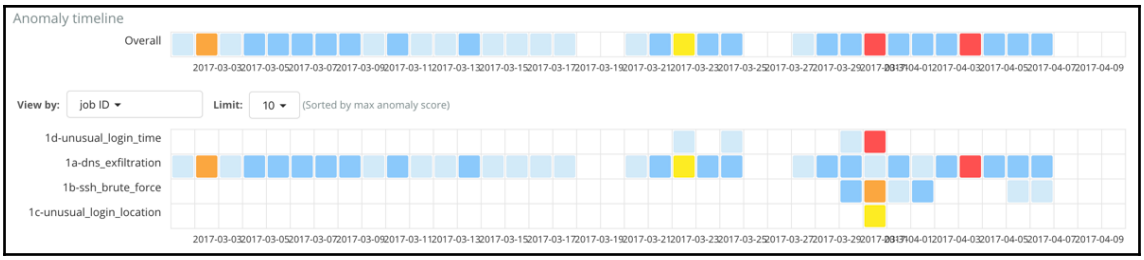
Description:
major anomaly in high_count over "system.auth.ssh.ip" found for system.auth.ssh.ip 24.151.103.17

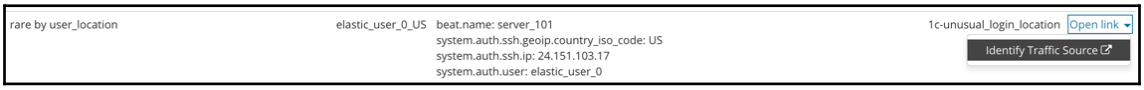
Details on highest severity anomaly:

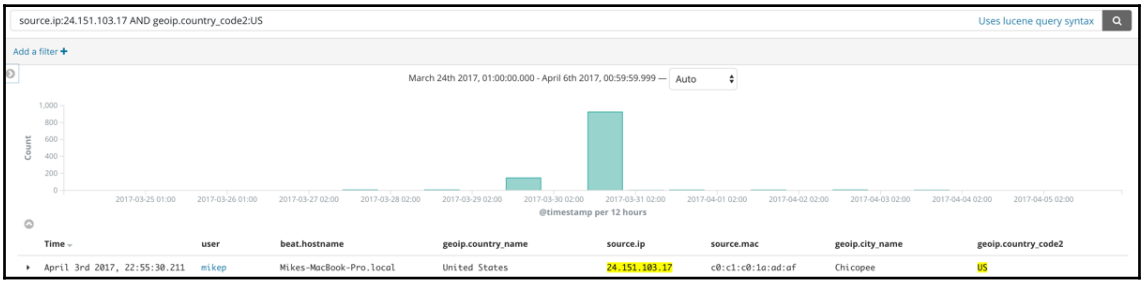
system.auth.ssh.ip:	24.151.103.17
time:	March 30th 2017, 17:50:00 to March 30th 2017, 18:00:00
function:	high_count
actual:	115
typical:	1.09
job ID:	1b-ssh_brute_force
probability:	1.9642774070161522e-11

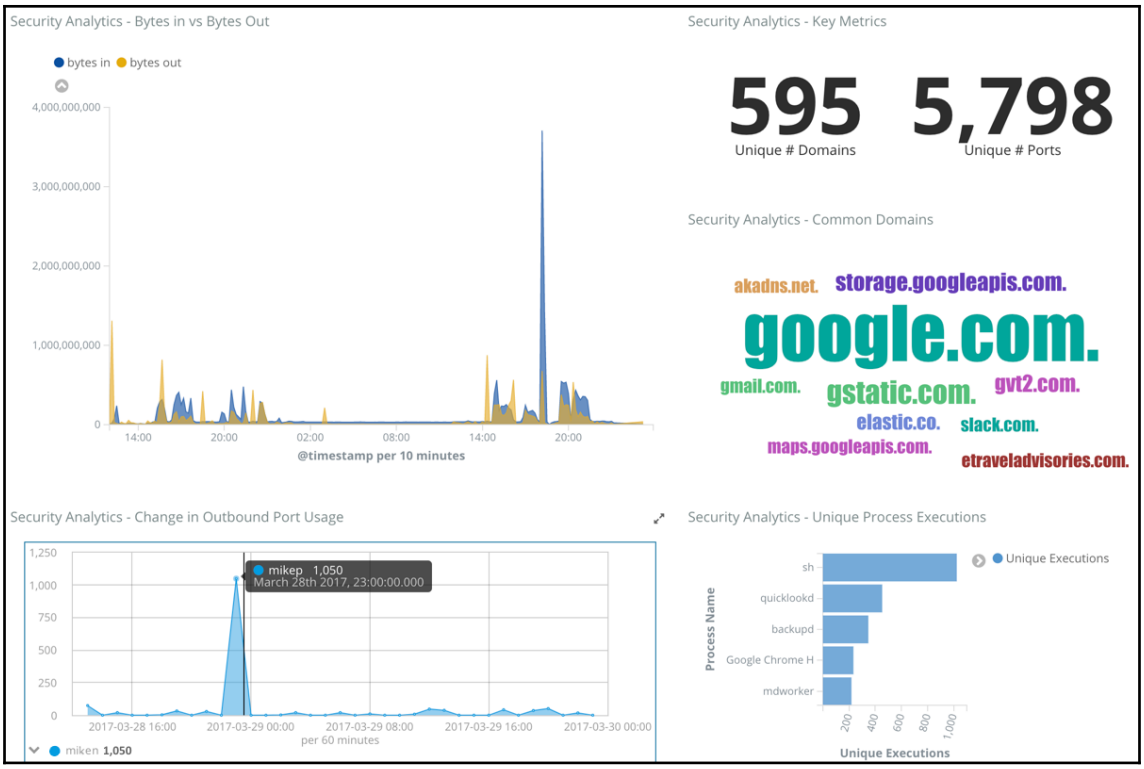
Influenced by:

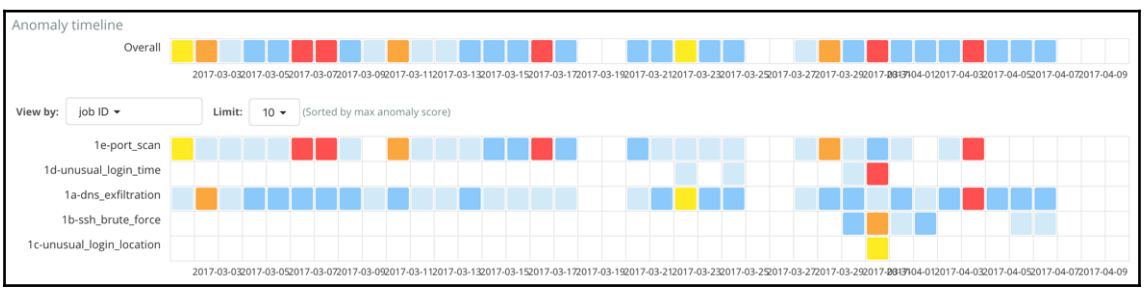
beat.name	server_101
system.auth.ssh.ip	24.151.103.17
system.auth.user	elastic_user_0


Anomaly timeline
Overall
2017-03-03 2017-03-05 2017-03-07 2017-03-09 2017-03-11 2017-03-13 2017-03-15 2017-03-17 2017-03-19 2017-03-21 2017-03-23 2017-03-25 2017-03-27 2017-03-29 2017-03-31 2017-04-01 2017-04-03 2017-04-05 2017-04-07 2017-04-09
View by: job ID
Limit: 10
(Sorted by max anomaly score)
1d-unusual_login_time
1a-dns_exfiltration
1b-ssh_brute_force
1c-unusual_login_location


rare by user_location
elastic_user_0_US
beat.name: server_101
system.auth.ssh.geoip.country_iso_code: US
system.auth.ssh.ip: 24.151.103.17
system.auth.user: elastic_user_0
1c-unusual_login_location
Open link
Identify Traffic Source


source.ip:24.151.103.17 AND geoip.country_code2:US
Uses lucene query syntax
Add a filter
March 24th 2017, 01:00:00.000 - April 6th 2017, 00:59:59.999 —
Auto
Count
@timestamp per 12 hours
Time
user
beat.hostname
geoip.country_name
source.ip
source.mac
geoip.city_name
geoip.country_code2
April 3rd 2017, 22:55:30.211
mikep
Mikes-MacBook-Pro.local
United States
24.151.103.17
c0:c1:c0:1a:ad:af
Chicopee
US


Security Analytics - Bytes in vs Bytes Out
bytes in
bytes out
4,000,000,000
3,000,000,000
2,000,000,000
1,000,000,000
0
14:00
20:00
02:00
08:00
14:00
20:00
@timestamp per 10 minutes
Security Analytics - Key Metrics
595
Unique # Domains
5,798
Unique # Ports
Security Analytics - Common Domains
akadns.net.
storage.googleapis.com.
google.com.
gmail.com.
gstatic.com.
gvt2.com.
elastic.co.
slack.com.
maps.googleapis.com.
etraveladvisories.com.
Security Analytics - Change in Outbound Port Usage
1,250
1,000
750
500
250
0
mikep 1,050
March 28th 2017, 23:00:00.000
2017-03-28 16:00
2017-03-29 00:00
2017-03-29 08:00
2017-03-29 16:00
2017-03-30 00:00
per 60 minutes
miken 1,050
Security Analytics - Unique Process Executions
Unique Executions
Process Name
sh
quicklookd
backupd
Google Chrome H
mdworker
200
400
600
800
1,000
Unique Executions


Anomaly timeline
Overall
2017-03-03
2017-03-05
2017-03-07
2017-03-09
2017-03-11
2017-03-13
2017-03-15
2017-03-17
2017-03-19
2017-03-21
2017-03-23
2017-03-25
2017-03-27
2017-03-29
2017-04-01
2017-04-03
2017-04-05
2017-04-07
2017-04-09
View by:
job ID
Limit:
10
(Sorted by max anomaly score)
1e-port_scan
1d-unusual_login_time
1a-dns_exfiltration
1b-ssh_brute_force
1c-unusual_login_location

time	max severity	detector	found for	influenced by	actual	typical	description	job ID	links
March 28th 2017, 23:00	85	high_distinct_count("dest.port") partitionfield="beat.name"	mikep	beat.name: mikep dest.ip: 34.253.76.153	654	39.7	16x higher	1e-port_scan	Open link

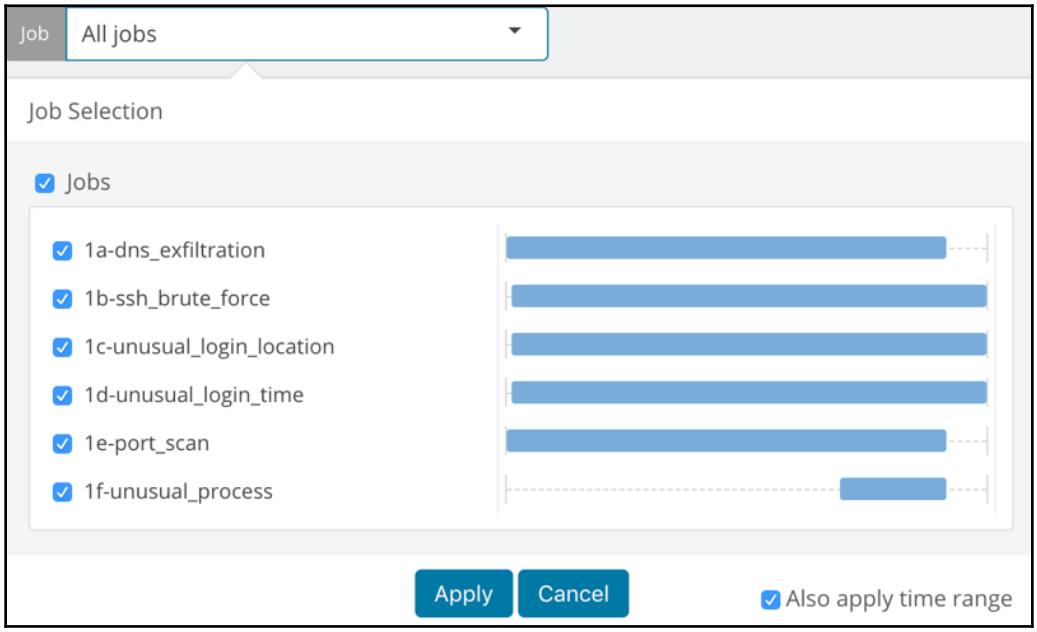
Description:
critical anomaly in high_distinct_count("dest.port") partitionfield="beat.name" found for beat.name mikep

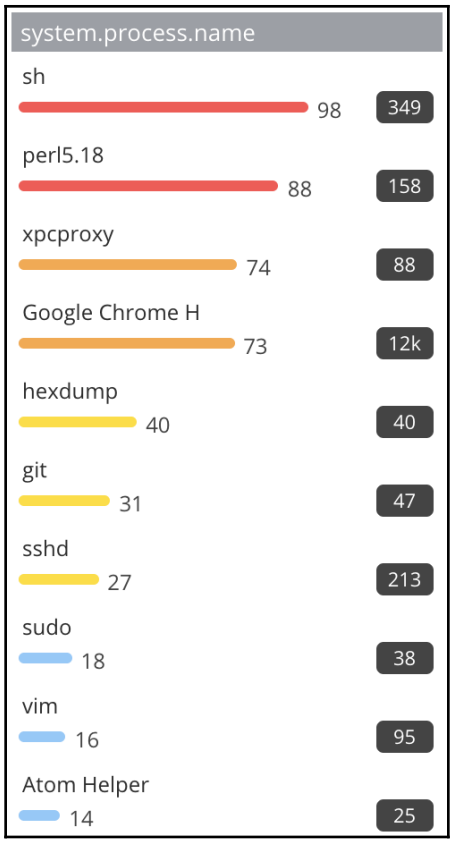
Details on highest severity anomaly:

beat.name:	mikep
time:	March 28th 2017, 23:20:00 to March 28th 2017, 23:30:00
function:	high_distinct_count
fieldName:	dest.port
actual:	654
typical:	39.7
job ID:	1e-port_scan
probability:	2.762639714887249e-7

Influenced by:

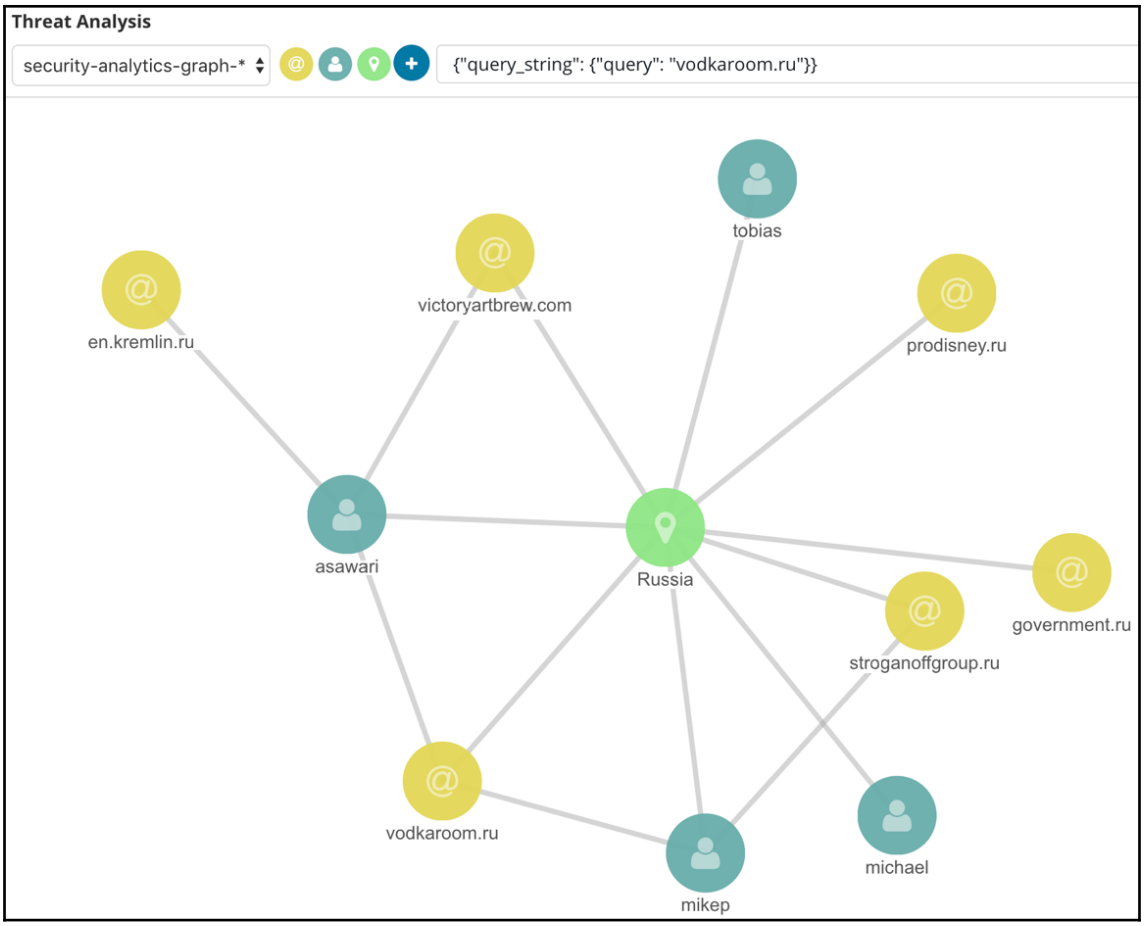
beat.name	mikep
dest.ip	34.253.76.153

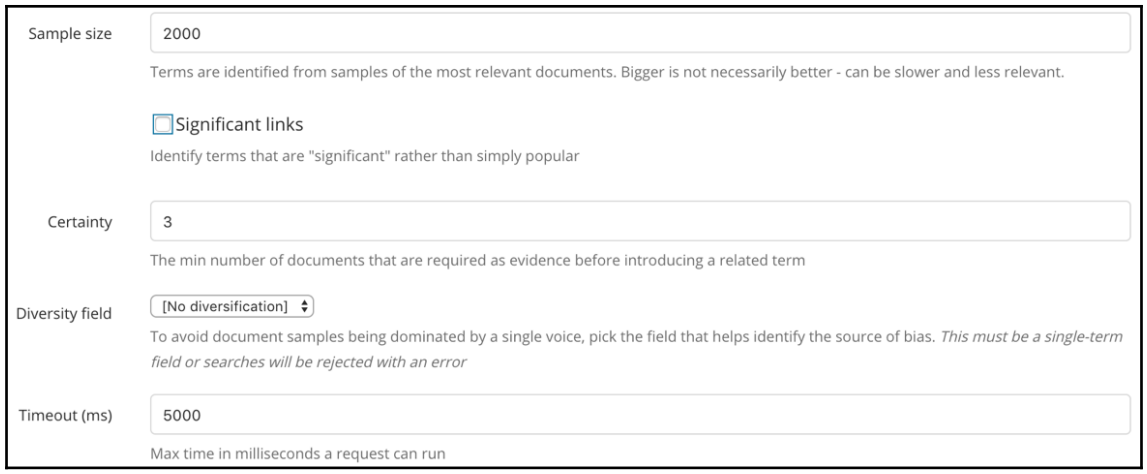


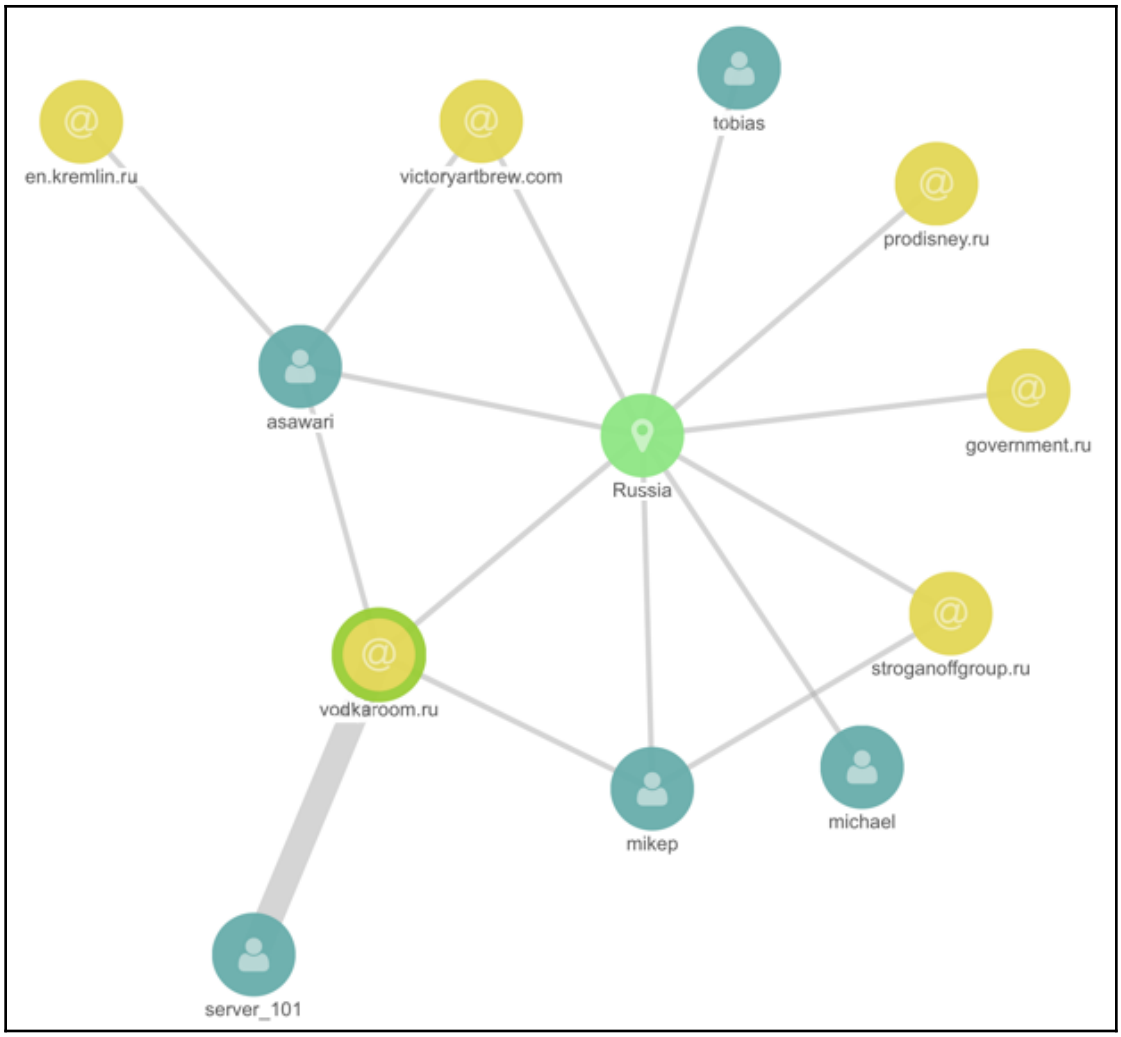

system.process.name
sh
98
349
perl5.18
88
158
xpcproxy
74
88
Google Chrome H
73
12k
hexdump
40
40
git
31
47
sshd
27
213
sudo
18
38
vim
16
95
Atom Helper
14
25

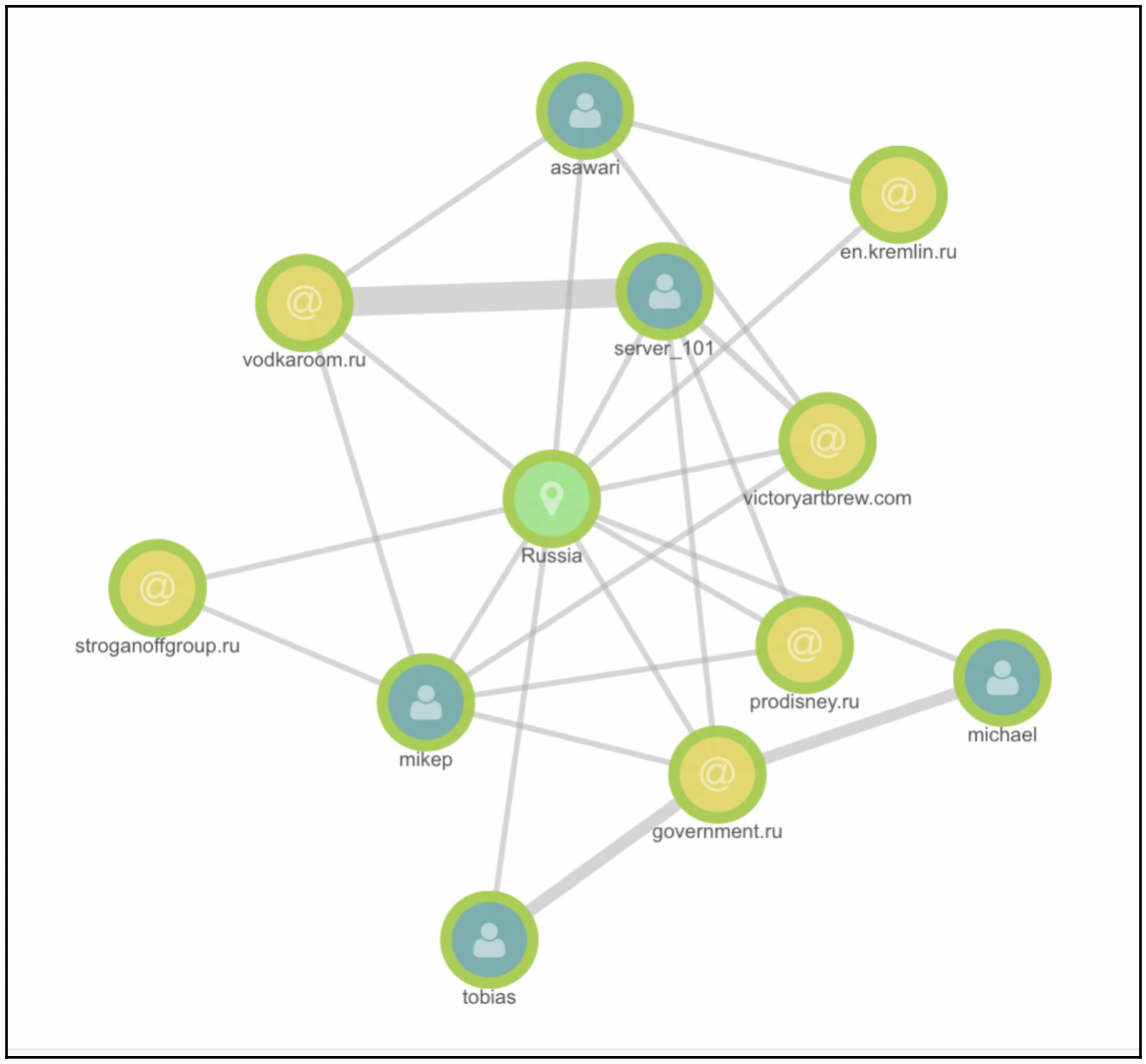
Security Analytics - Domains by Unique Subdomain Count

Domains	IP	Graph Analysis	# of Subdomains
vodkaroom.ru.	5.101.152.77	Graph Analysis - vodkaroom.ru	5,445
ubuntu.com.	54.195.20.85	Graph Analysis - ubuntu.com	1
ubuntu.com.	54.216.255.40	Graph Analysis - ubuntu.com	1
ubuntu.com.	54.217.129.123	Graph Analysis - ubuntu.com	1

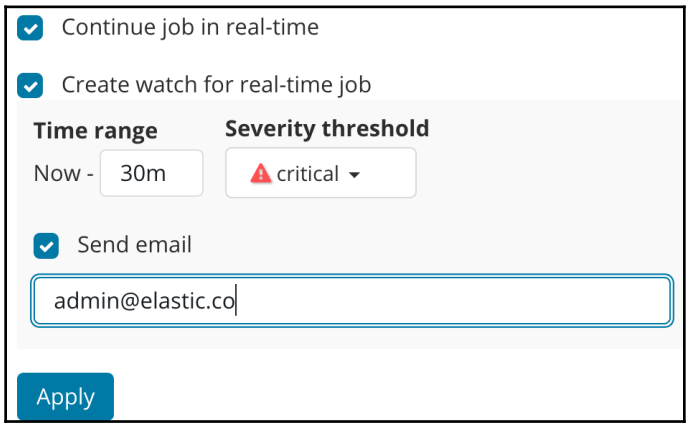

Threat Analysis
security-analytics-graph-*
{"query_string": {"query": "vodkaroom.ru"}}
tobias
victoryartbrew.com
en.kremlin.ru
prodisney.ru
asawari
Russia
government.ru
stroganoffgroup.ru
vodkaroom.ru
michael
mikep


Sample size
2000
Terms are identified from samples of the most relevant documents. Bigger is not necessarily better - can be slower and less relevant.
Significant links
Identify terms that are "significant" rather than simply popular
Certainty
3
The min number of documents that are required as evidence before introducing a related term
Diversity field
[No diversification]
To avoid document samples being dominated by a single voice, pick the field that helps identify the source of bias. This must be a single-term field or searches will be rejected with an error
Timeout (ms)
5000
Max time in milliseconds a request can run


en.kremlin.ru
victoryartbrew.com
tobias
prodisney.ru
asawari
government.ru
Russia
stroganoffgroup.ru
vodkaroom.ru
mikep
michael
server_101


asawari
en.kremlin.ru
vodkaroom.ru
server_101
victoryartbrew.com
Russia
stroganoffgroup.ru
prodisney.ru
michael
mikep
government.ru
tobias

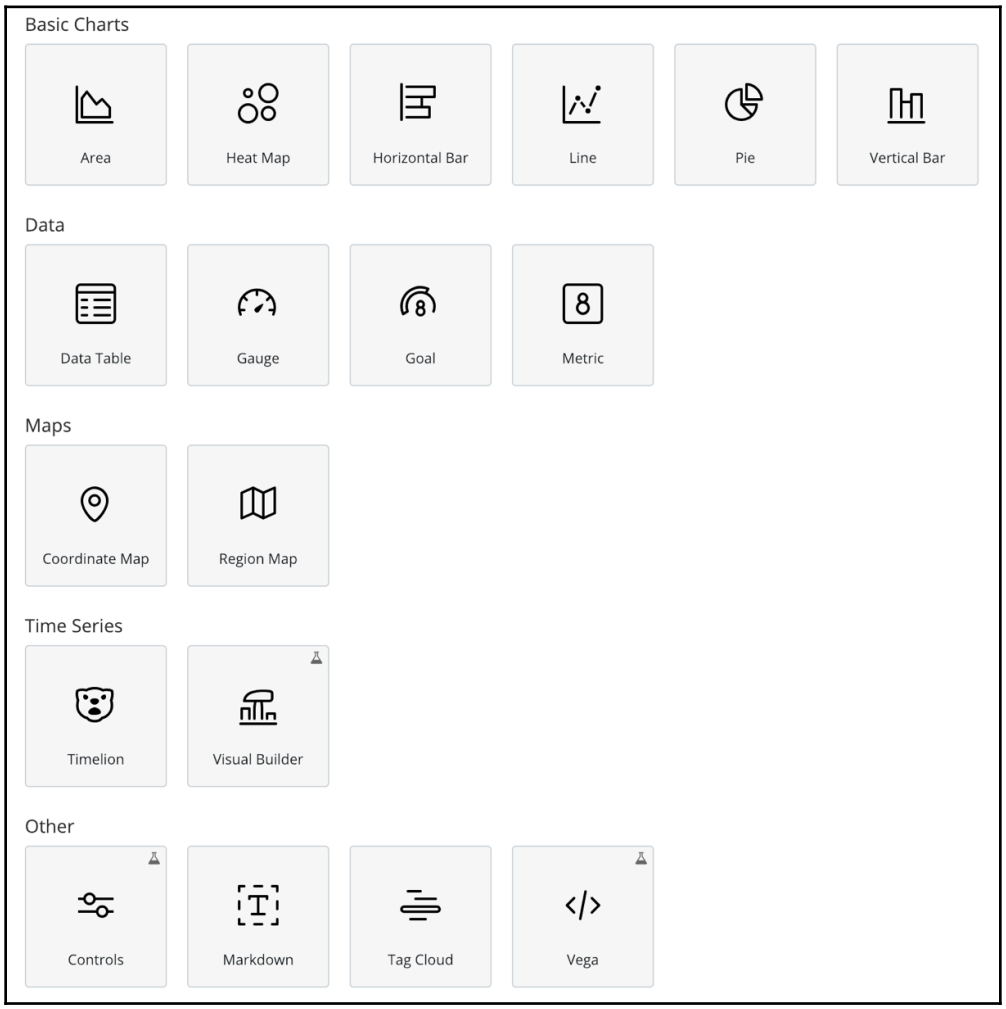
Chapter 6: Alerting on ML Analysis



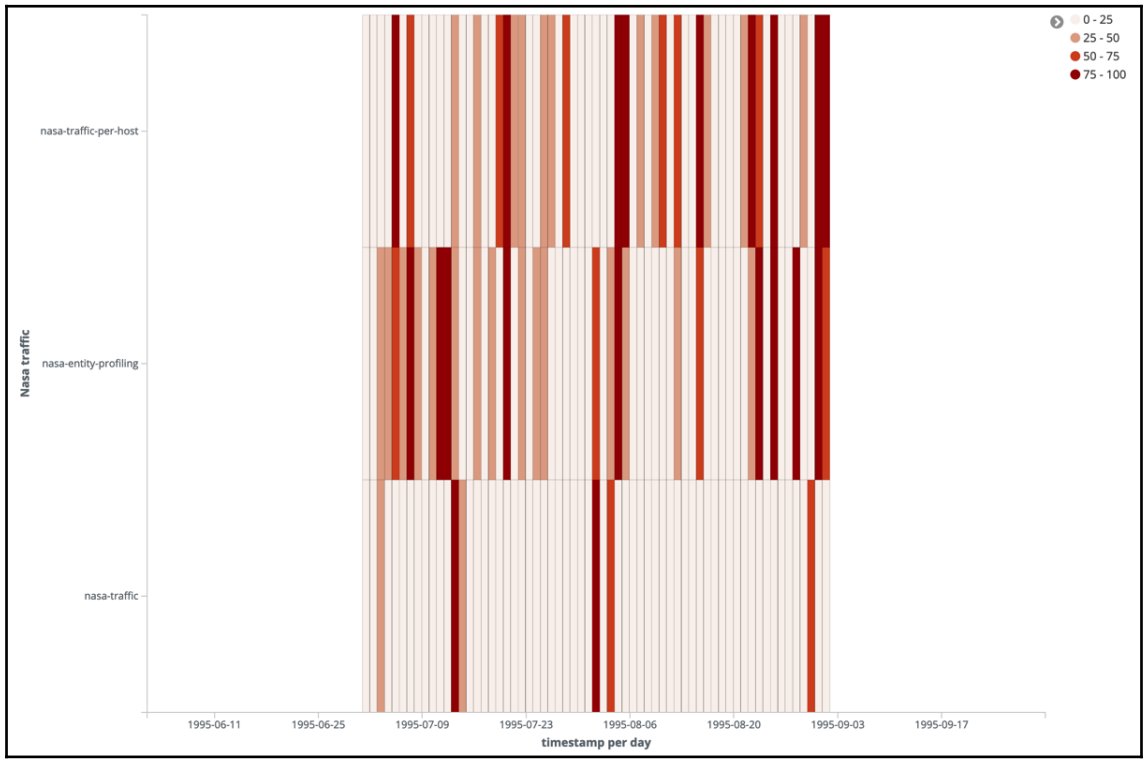

```
"aggs": {
  "bucket_results": {},
  "influencer_results": {},
  "record_results": {}
}
```

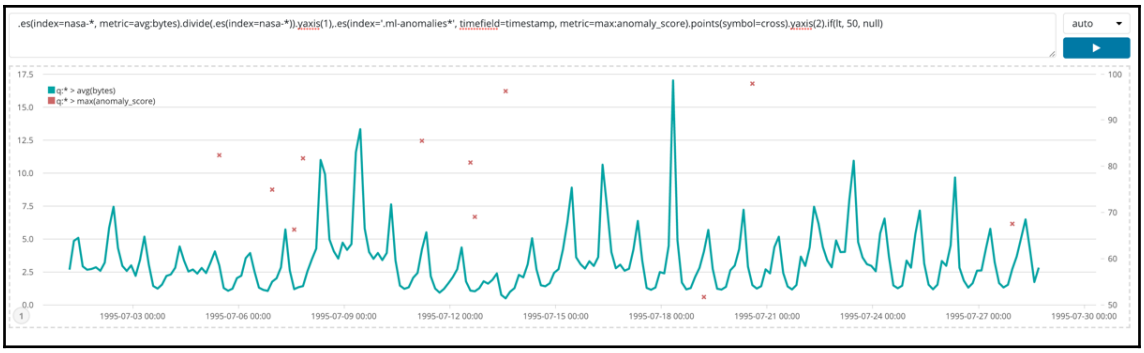
```
"input": {
  "chain": {
    "inputs": [
      {
        "job1": {}
      },
      {
        "job2": {}
      },
      {
        "job3": {}
      }
    ]
  }
},
```

Chapter 7: Using Elastic ML Data in Kibana Dashboards

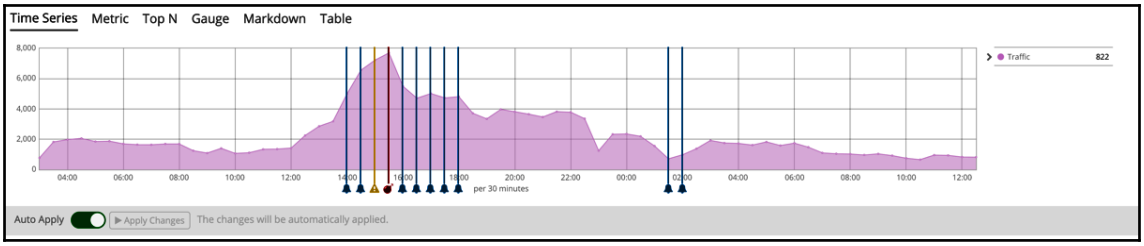


URI	Hits
/shuttle/missions/sts-69/mission-sts-69.html	24,589
/shuttle/missions/missions.html	47,298
/shuttle/countdown/liftoff.html	29,860
/shuttle/countdown/	64,737
/ksc.html	83,874
/images/WORLD-logosmall.gif	125,928
/images/USA-logosmall.gif	127,076
/images/NASA-logosmall.gif	208,728
/images/MOSAIC-logosmall.gif	127,912
/images/launchmedium.gif	40,684




.es(index=nasa-*, metric=avg:bytes).divide(.es(index=nasa-*)).yaxis(1),.es(index='.ml-anomalies*', timefield=timestamp, metric=max:anomaly_score).points(symbol=cross).yaxis(2).if(lt, 50, null)
auto
q:* > avg(bytes)
q:* > max(anomaly_score)
1995-07-03 00:00
1995-07-06 00:00
1995-07-09 00:00
1995-07-12 00:00
1995-07-15 00:00
1995-07-18 00:00
1995-07-21 00:00
1995-07-24 00:00
1995-07-27 00:00
1995-07-30 00:00


Time Series
Metric
Top N
Gauge
Markdown
Table

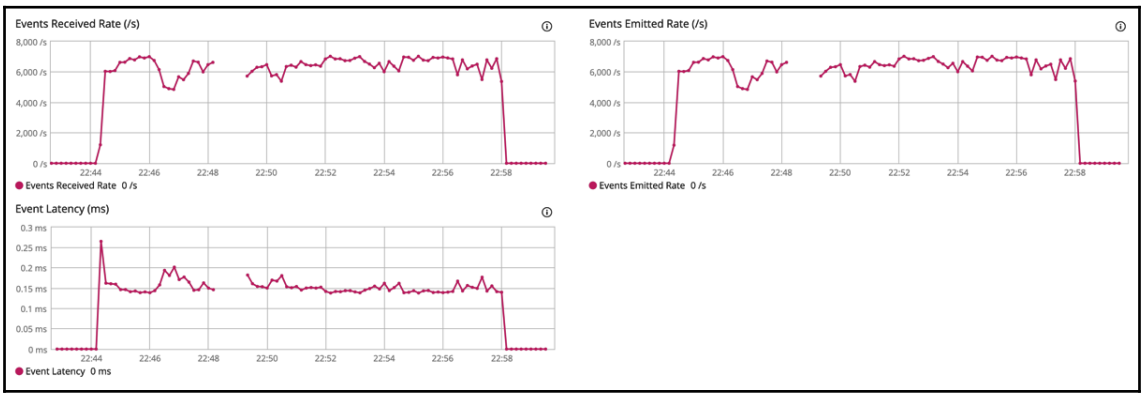

Time Series
Metric
Top N
Gauge
Markdown
Table
Traffic
822
per 30 minutes
Auto Apply
Apply Changes
The changes will be automatically applied.

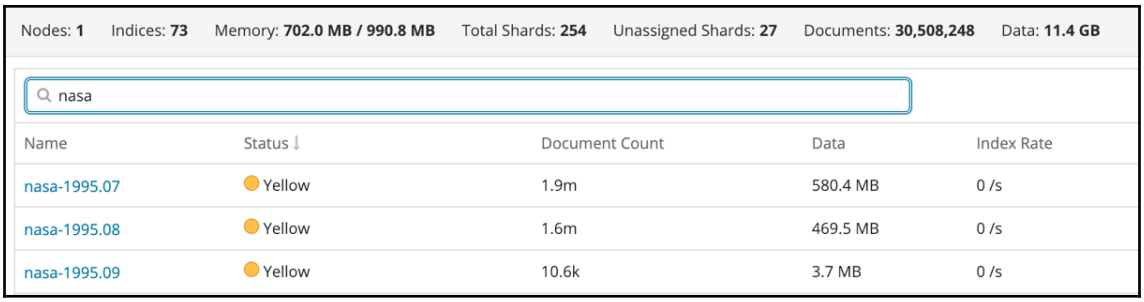
Description

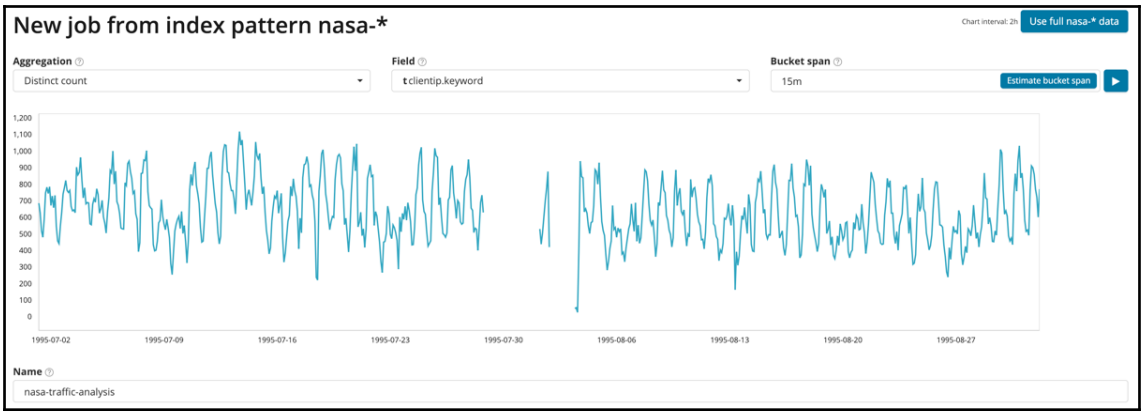
NASA 90s HTTP Logs pipeline

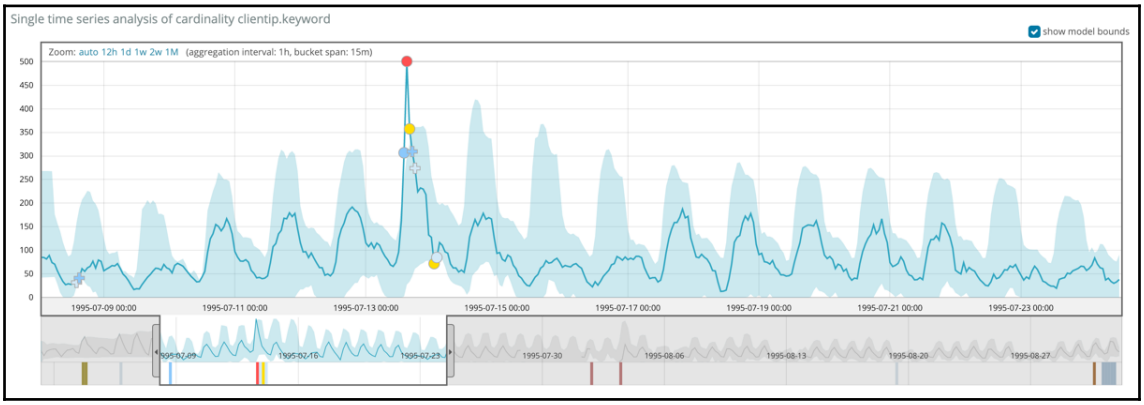
Pipeline

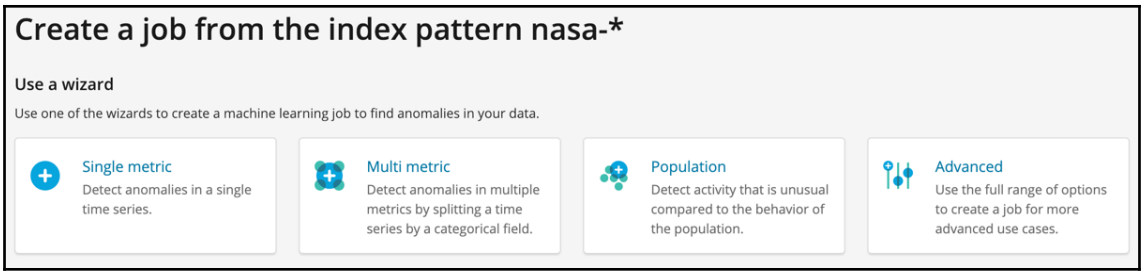
```
input {
  file {
    id => "nasa_file"
    path => "/Users/baha/Downloads/data/*.log"
    start_position => "beginning"
    sincedb_path => "/dev/null"
  }
}

filter {
  grok {
    id => "nasa_grok_filter"
    match => { "message" => "%{COMMONAPACHELOG}" }
  }
  date {
    match => ["timestamp", "dd/MMM/yyyy:HH:mm:ss Z"]
    target => "@timestamp"
    remove_field => [ "timestamp" ]
  }
}

output {
  elasticsearch {
    id => "nasa_elasticsearch_output"
    hosts => "localhost:9200"
    user => "elastic"
    password => "*********"
    index => "nasa-%{+YYYY.MM}"
    template => "/Users/baha/Downloads/data/template.conf"
    template_name => "nasa"
    template_overwrite => "false"
  }
}
```

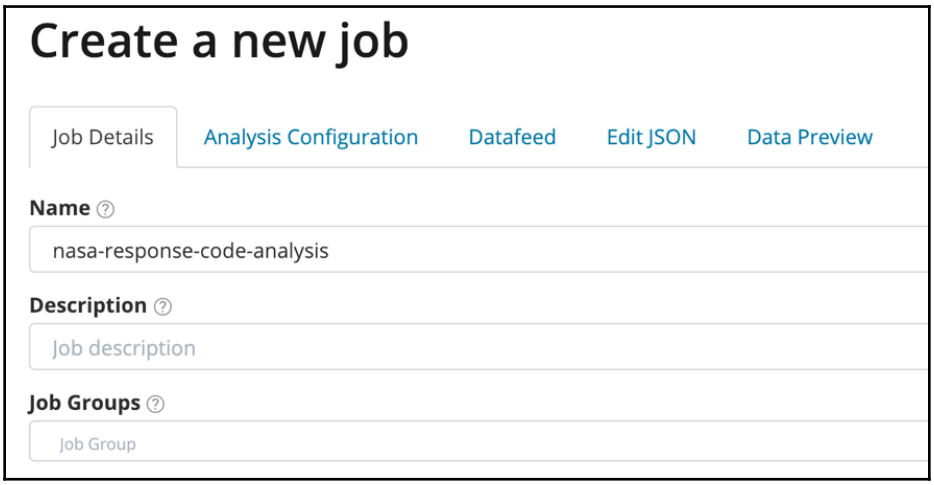


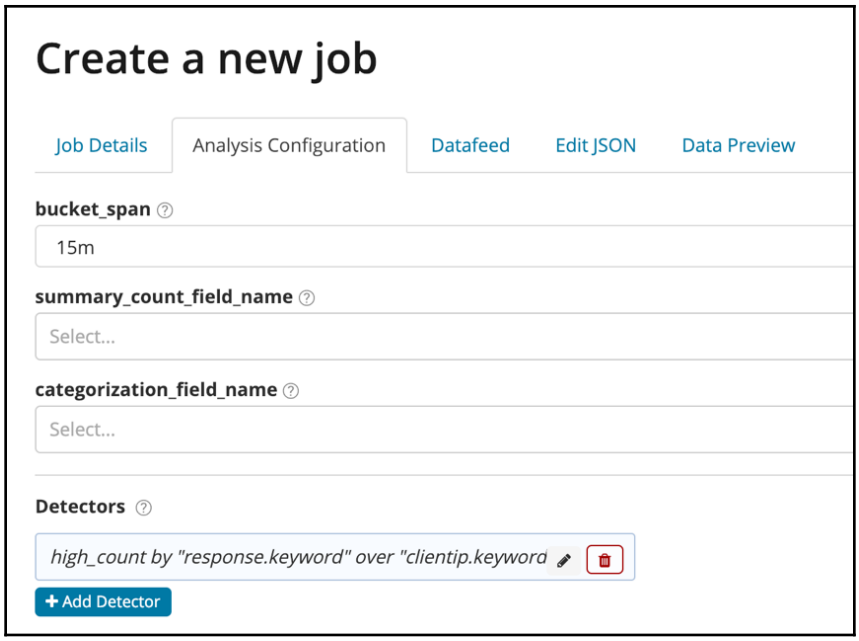

Nodes: 1 Indices: 73 Memory: 702.0 MB / 990.8 MB Total Shards: 254 Unassigned Shards: 27 Documents: 30,508,248 Data: 11.4 GB
nasa
Name Status Document Count Data Index Rate
nasa-1995.07 Yellow 1.9m 580.4 MB 0 /s
nasa-1995.08 Yellow 1.6m 469.5 MB 0 /s
nasa-1995.09 Yellow 10.6k 3.7 MB 0 /s

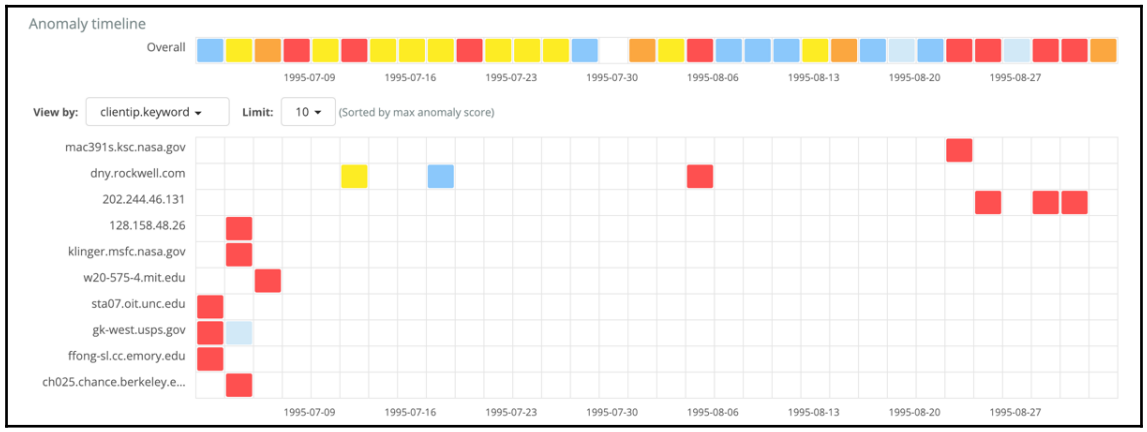

New job from index pattern nasa-*
Chart interval: 2h
Use full nasa-* data
Aggregation
Distinct count
Field
t clientip.keyword
Bucket span
15m
Estimate bucket span
1,200
1,100
1,000
900
800
700
600
500
400
300
200
100
0
1995-07-02
1995-07-09
1995-07-16
1995-07-23
1995-07-30
1995-08-06
1995-08-13
1995-08-20
1995-08-27
Name
nasa-traffic-analysis


Single time series analysis of cardinality clientip.keyword
show model bounds
Zoom: auto 12h 1d 1w 2w 1M (aggregation interval: 1h, bucket span: 15m)
500
450
400
350
300
250
200
150
100
50
0
1995-07-09 00:00
1995-07-11 00:00
1995-07-13 00:00
1995-07-15 00:00
1995-07-17 00:00
1995-07-19 00:00
1995-07-21 00:00
1995-07-23 00:00
1995-07-09
1995-07-16
1995-07-23
1995-07-30
1995-08-06
1995-08-13
1995-08-20
1995-08-27

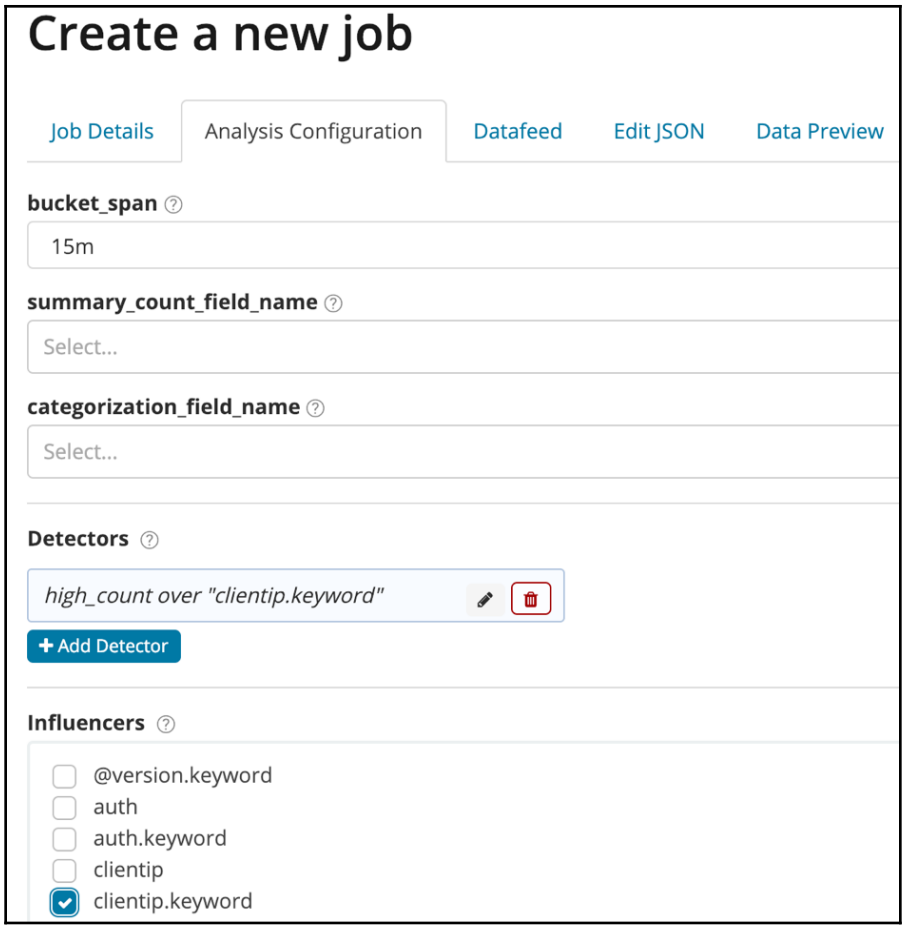

Create a job from the index pattern nasa-*
Use a wizard
Use one of the wizards to create a machine learning job to find anomalies in your data.
Single metric
Detect anomalies in a single time series.
Multi metric
Detect anomalies in multiple metrics by splitting a time series by a categorical field.
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.

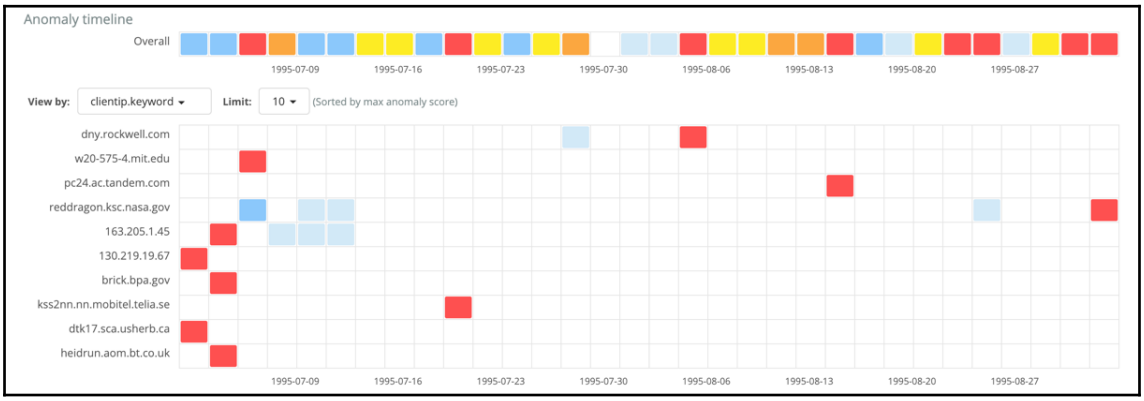

Create a new job
Job Details
Analysis Configuration
Datafeed
Edit JSON
Data Preview
Name
nasa-response-code-analysis
Description
Job description
Job Groups
Job Group


Create a new job
Job Details
Analysis Configuration
Datafeed
Edit JSON
Data Preview
bucket_span
15m
summary_count_field_name
Select...
categorization_field_name
Select...
Detectors
high_count by "response.keyword" over "clientip.keyword
+ Add Detector

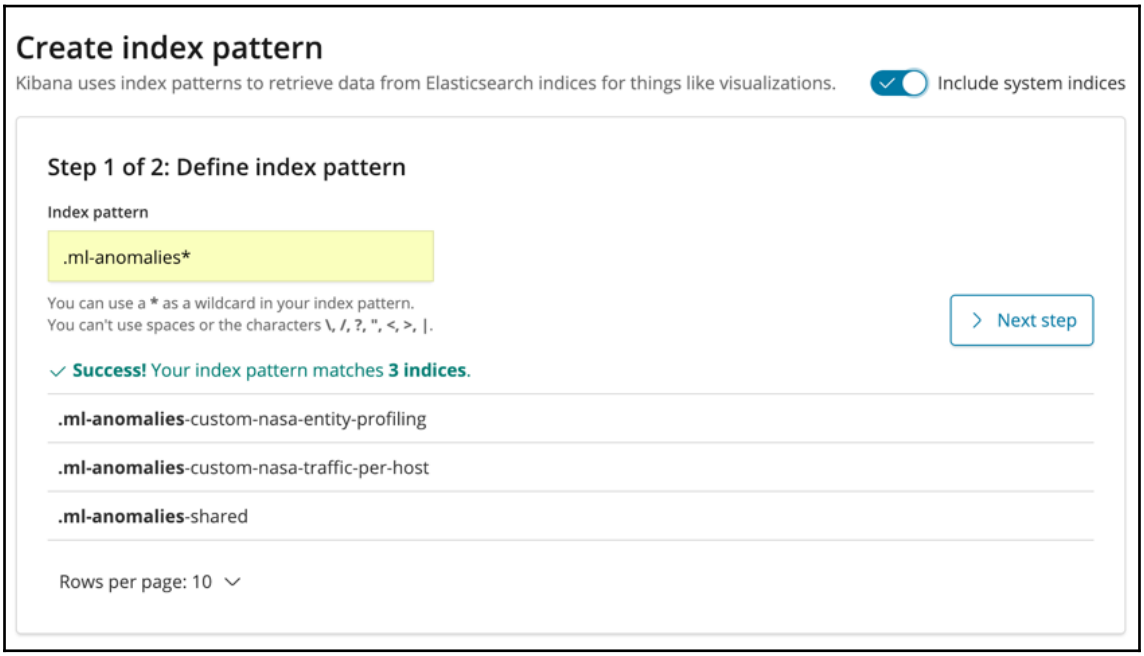

Anomaly timeline
Overall
1995-07-09
1995-07-16
1995-07-23
1995-07-30
1995-08-06
1995-08-13
1995-08-20
1995-08-27
View by:
clientip.keyword
Limit:
10
(Sorted by max anomaly score)
mac391s.ksc.nasa.gov
dny.rockwell.com
202.244.46.131
128.158.48.26
klinger.msfc.nasa.gov
w20-575-4.mit.edu
sta07.oit.unc.edu
gk-west.usps.gov
ffong-sl.cc.emory.edu
ch025.chance.berkeley.e...

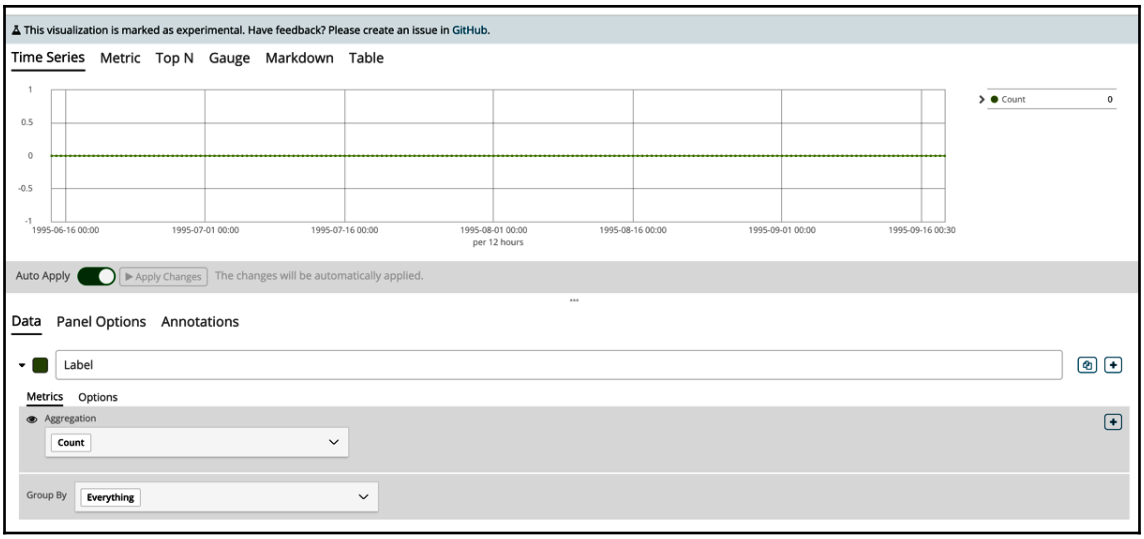

Anomalies
Severity threshold
warning
Interval
Auto
Show charts
high_count by "response.keyword" over "clientip.keyword"
clientip.keyword w20-575-4.mit.edu
130
120
110
100
90
80
70
60
50
40
30
20
10
0
1995-07-05 02:00
time
max severity
detector
found for
influenced by
actual
typical
description
July 5th 1995, 13:00
98
high_count by "response.keyword" over "clientip.keyword"
w20-575-4.mit.edu
clientip.keyword: w20-575-4.mit.edu
Description
critical anomaly in high_count by "response.keyword" over "clientip.keyword" found for clientip.keyword w20-575-4.mit.edu
Details on highest severity anomaly
clientip.keyword
w20-575-4.mit.edu
time
July 5th 1995, 13:00:00 to July 5th 1995, 13:15:00
function
high_count
job ID
nasa-entity-profiling
probability
1.4375301598989583e-11
response.keyword values
200 (actual 119, typical 4.65, probability 2.2909176231980907e-9)
404 (actual 10, typical 1.35, probability 0.00016246674219092243)
Influencers
clientip.keyword
w20-575-4.mit.edu

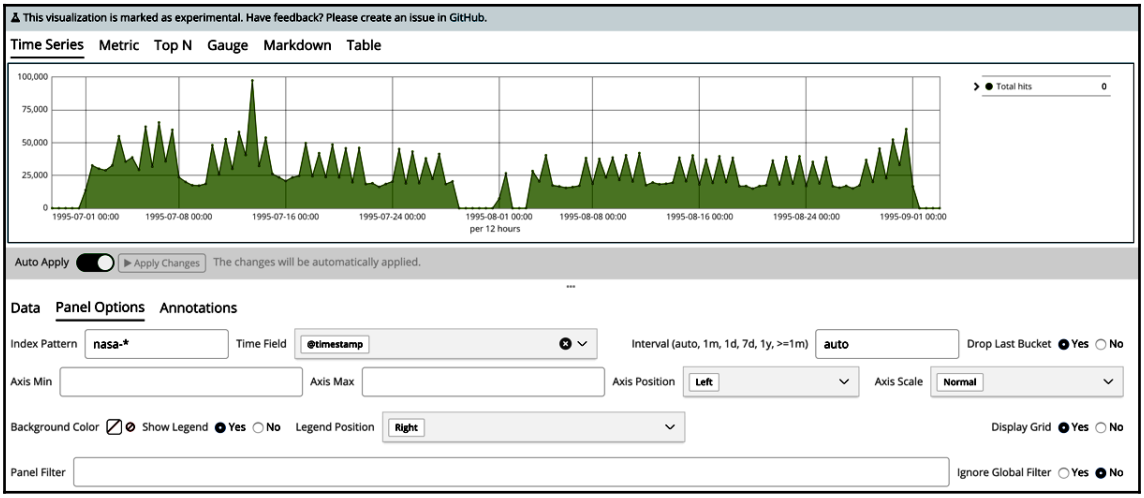

Create a new job
Job Details
Analysis Configuration
Datafeed
Edit JSON
Data Preview
bucket_span
15m
summary_count_field_name
Select...
categorization_field_name
Select...
Detectors
high_count over "clientip.keyword"
+ Add Detector
Influencers
@version.keyword
auth
auth.keyword
clientip
clientip.keyword

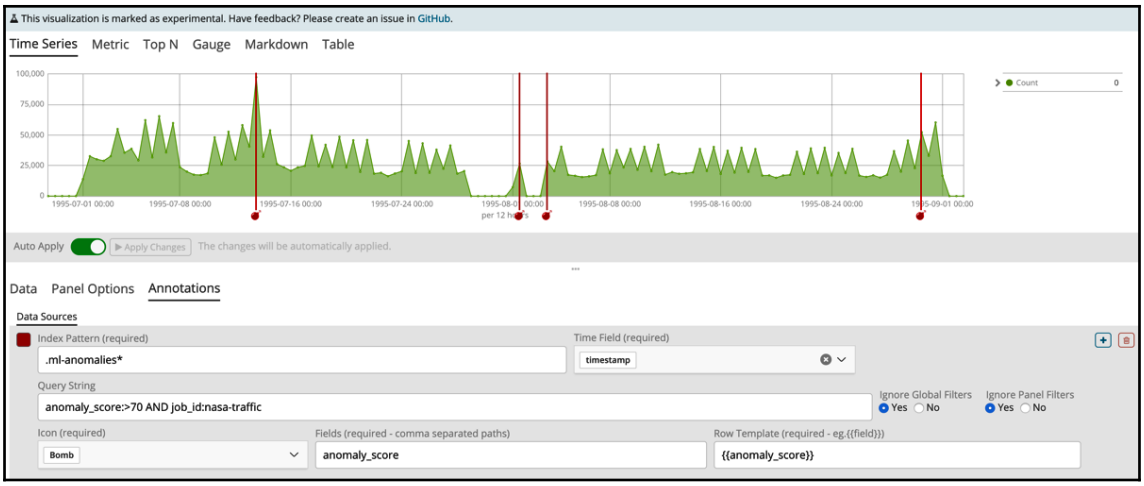

Anomaly timeline
Overall
1995-07-09
1995-07-16
1995-07-23
1995-07-30
1995-08-06
1995-08-13
1995-08-20
1995-08-27
View by:
clientip.keyword
Limit:
10
(Sorted by max anomaly score)
dny.rockwell.com
w20-575-4.mit.edu
pc24.ac.tandem.com
reddragon.ksc.nasa.gov
163.205.1.45
130.219.19.67
brick.bpa.gov
kss2nn.nn.mobitel.telia.se
dtk17.sca.usherb.ca
heidrun.aom.bt.co.uk


high_count over "clientip.keyword"
View
clientip.keyword pc24.ac.tandem.com
200
180
160
140
120
100
80
60
40
20
0
1995-08-14 02:00
1995-08-16 02:00
time
max severity
detector
found for
influenced by
actual
typical
description
job ID
actions
August 15th 1995, 22:00
99
high_count over "clientip.keyword"
pc24.ac.tandem.com
clientip.keyword: pc24.ac.tandem.com
192
6.17
31x higher
nasa-traffic-per-host
Description
critical anomaly in high_count over "clientip.keyword" found for clientip.keyword pc24.ac.tandem.com
Details on highest severity anomaly
clientip.keyword pc24.ac.tandem.com
time August 15th 1995, 22:00:00 to August 15th 1995, 22:15:00
function high_count
actual 192
typical 6.17
job ID nasa-traffic-per-host
probability 7.021671077292123e-13
Influencers
clientip.keyword pc24.ac.tandem.com

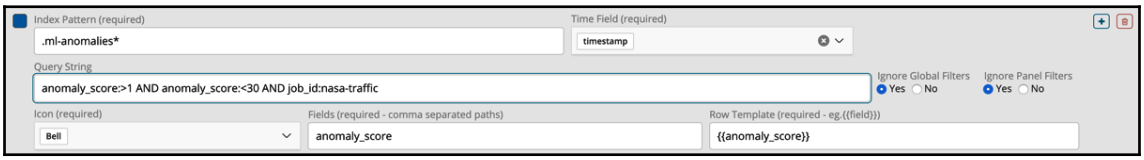

Create index pattern
Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.
Include system indices
Step 1 of 2: Define index pattern
Index pattern
.ml-anomalies*
You can use a * as a wildcard in your index pattern.
You can't use spaces or the characters \, /, ?, ", <, >, |.
Next step
Success! Your index pattern matches 3 indices.
.ml-anomalies-custom-nasa-entity-profiling
.ml-anomalies-custom-nasa-traffic-per-host
.ml-anomalies-shared
Rows per page: 10

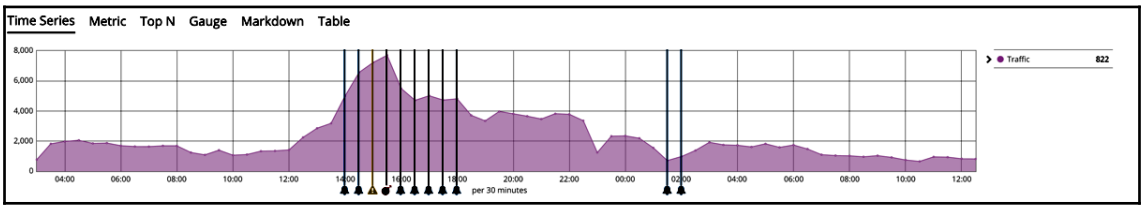

This visualization is marked as experimental. Have feedback? Please create an issue in GitHub.
Time Series
Metric
Top N
Gauge
Markdown
Table
1
0.5
0
-0.5
-1
1995-06-16 00:00
1995-07-01 00:00
1995-07-16 00:00
1995-08-01 00:00
per 12 hours
1995-08-16 00:00
1995-09-01 00:00
1995-09-16 00:30
Count
0
Auto Apply
Apply Changes
The changes will be automatically applied.
Data
Panel Options
Annotations
Label
Metrics
Options
Aggregation
Count
Group By
Everything

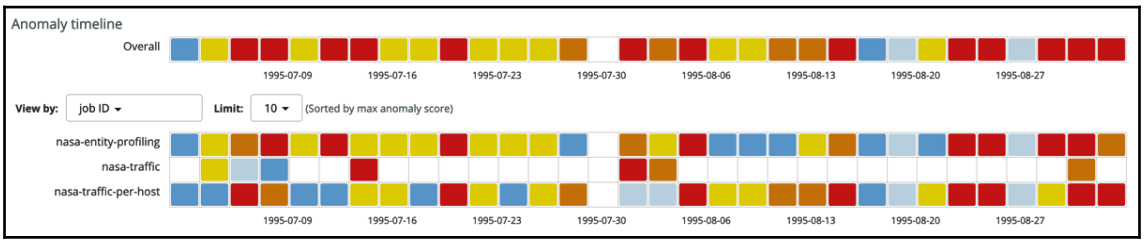

This visualization is marked as experimental. Have feedback? Please create an issue in GitHub.
Time Series
Metric
Top N
Gauge
Markdown
Table
100,000
75,000
50,000
25,000
0
1995-07-01 00:00
1995-07-08 00:00
1995-07-16 00:00
1995-07-24 00:00
1995-08-01 00:00
per 12 hours
1995-08-08 00:00
1995-08-16 00:00
1995-08-24 00:00
1995-09-01 00:00
Total hits
0
Auto Apply
Apply Changes
The changes will be automatically applied.
Data
Panel Options
Annotations
Index Pattern
nasa-*
Time Field
@timestamp
Interval (auto, 1m, 1d, 7d, 1y, >=1m)
auto
Drop Last Bucket
Yes
No
Axis Min
Axis Max
Axis Position
Left
Axis Scale
Normal
Background Color
Show Legend
Yes
No
Legend Position
Right
Display Grid
Yes
No
Panel Filter
Ignore Global Filter
Yes
No

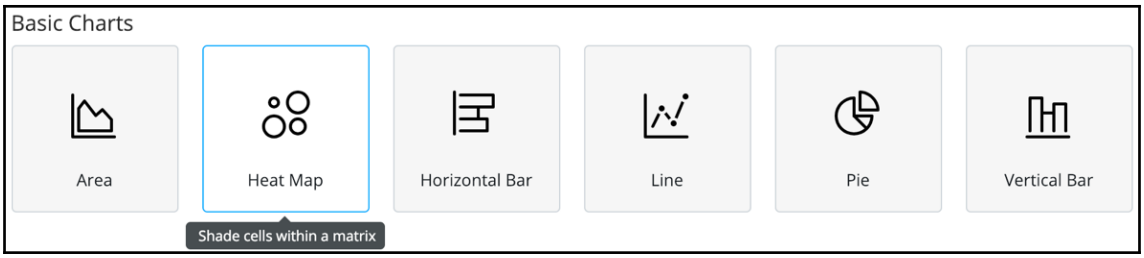

This visualization is marked as experimental. Have feedback? Please create an issue in GitHub.
Time Series
Metric
Top N
Gauge
Markdown
Table
Count
0
Auto Apply
Apply Changes
The changes will be automatically applied.
Data
Panel Options
Annotations
Data Sources
Index Pattern (required)
.ml-anomalies*
Time Field (required)
timestamp
Query String
anomaly_score:>70 AND job_id:nasa-traffic
Ignore Global Filters
Ignore Panel Filters
Yes
No
Icon (required)
Bomb
Fields (required - comma separated paths)
anomaly_score
Row Template (required - eg.{{field}})
{{anomaly_score}}

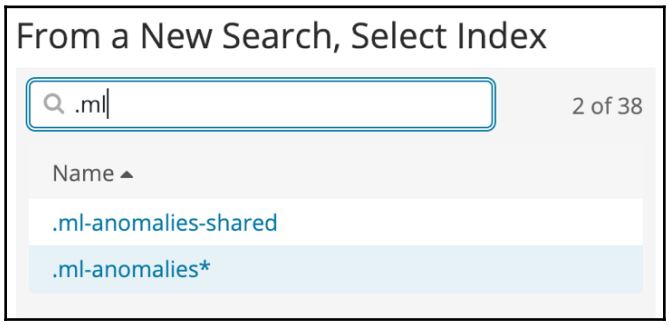

Index Pattern (required)
.ml-anomalies*
Time Field (required)
timestamp
Query String
anomaly_score:>30 AND anomaly_score:<70 AND job_id:nasa-traffic
Ignore Global Filters
Ignore Panel Filters
Yes
No
Icon (required)
Exclamation Triangle
Fields (required - comma separated paths)
anomaly_score
Row Template (required - eg.{{field}})
{{anomaly_score}}

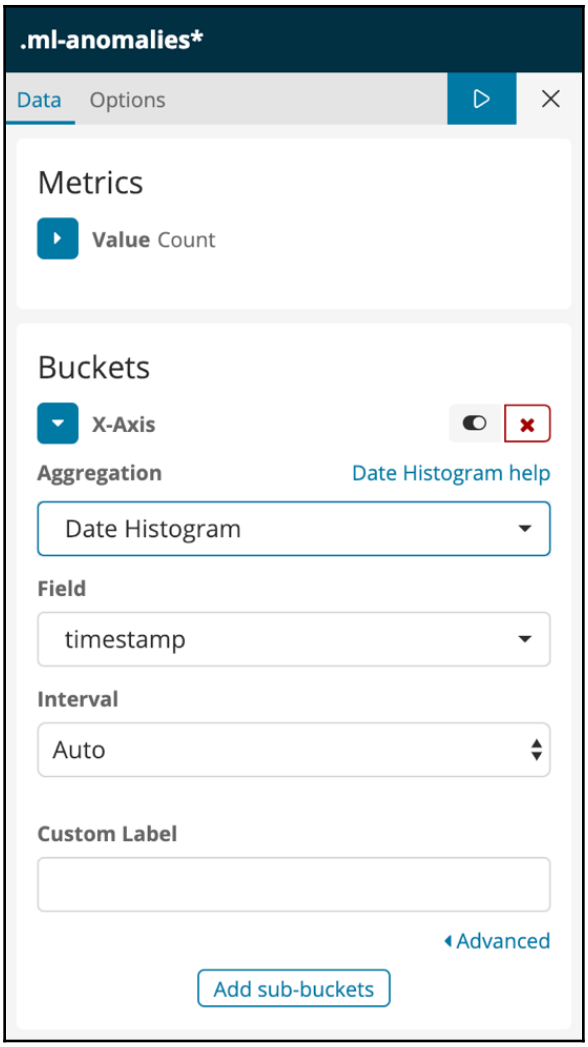

Index Pattern (required)
.ml-anomalies*
Time Field (required)
timestamp
Query String
anomaly_score:>1 AND anomaly_score:<30 AND job_id:nasa-traffic
Ignore Global Filters
Ignore Panel Filters
Yes
No
Icon (required)
Bell
Fields (required - comma separated paths)
anomaly_score
Row Template (required - eg.{{field}})
{{anomaly_score}}

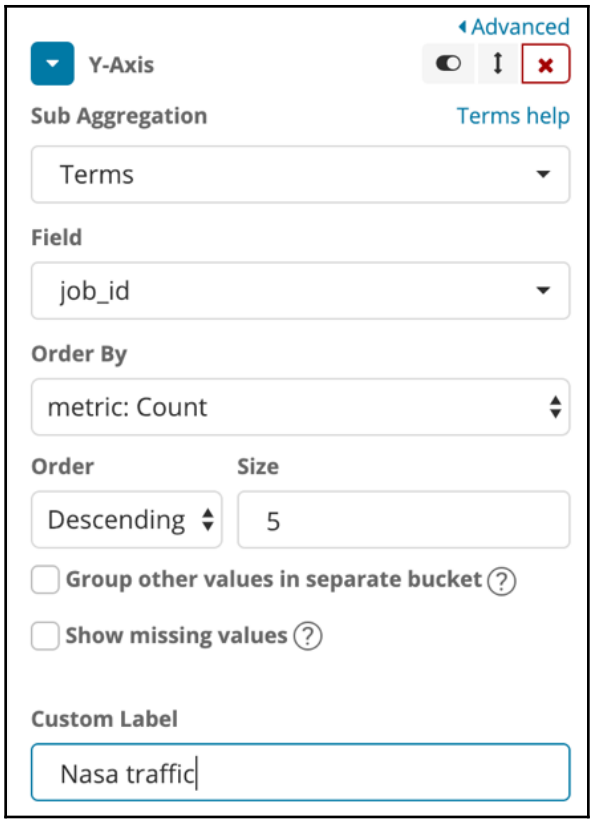

Time Series
Metric
Top N
Gauge
Markdown
Table
Traffic
822
per 30 minutes

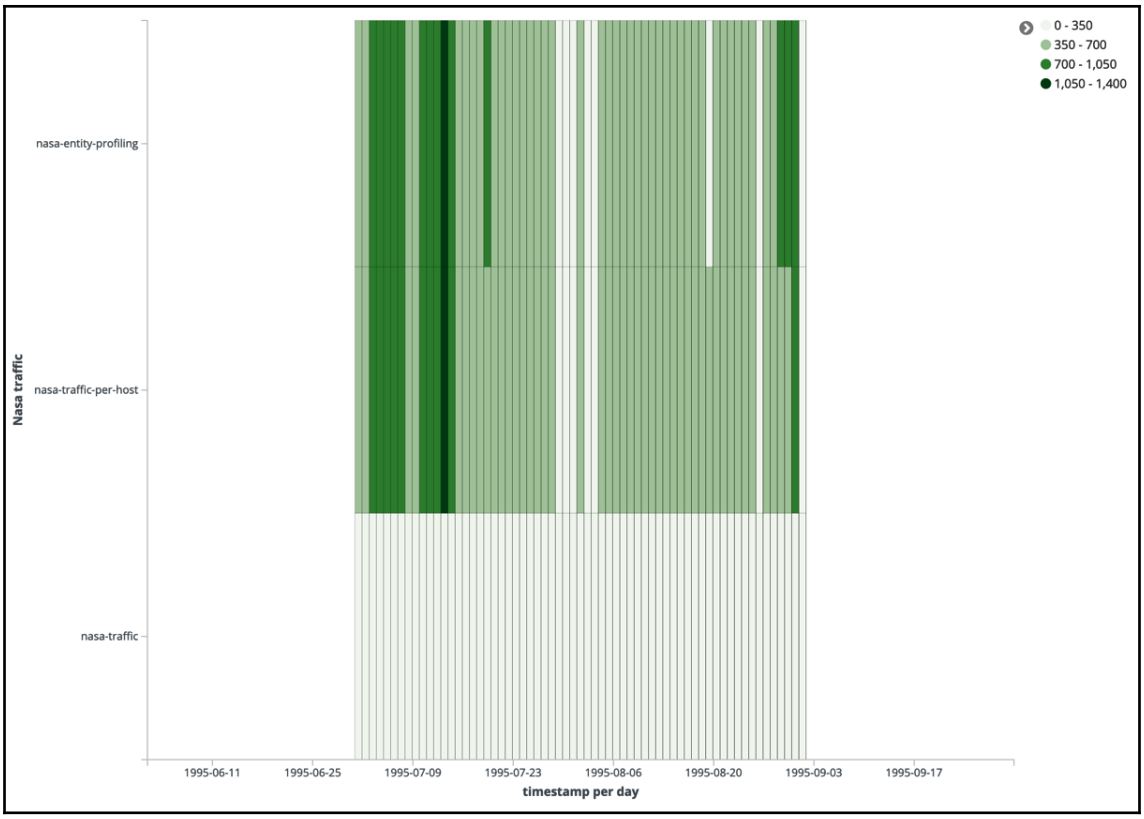

Anomaly timeline
Overall
1995-07-09
1995-07-16
1995-07-23
1995-07-30
1995-08-06
1995-08-13
1995-08-20
1995-08-27
View by:
job ID
Limit:
10
(Sorted by max anomaly score)
nasa-entity-profiling
nasa-traffic
nasa-traffic-per-host

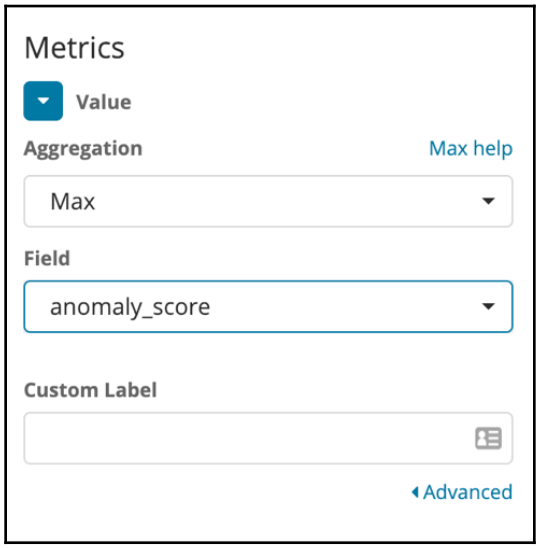

Basic Charts
Area
Heat Map
Horizontal Bar
Line
Pie
Vertical Bar
Shade cells within a matrix

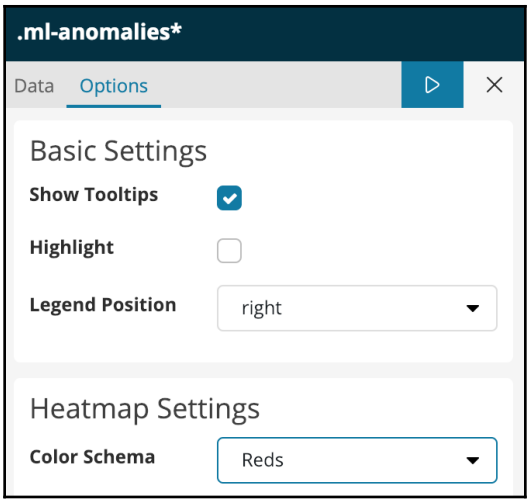

From a New Search, Select Index
.ml
2 of 38
Name
.ml-anomalies-shared
.ml-anomalies*

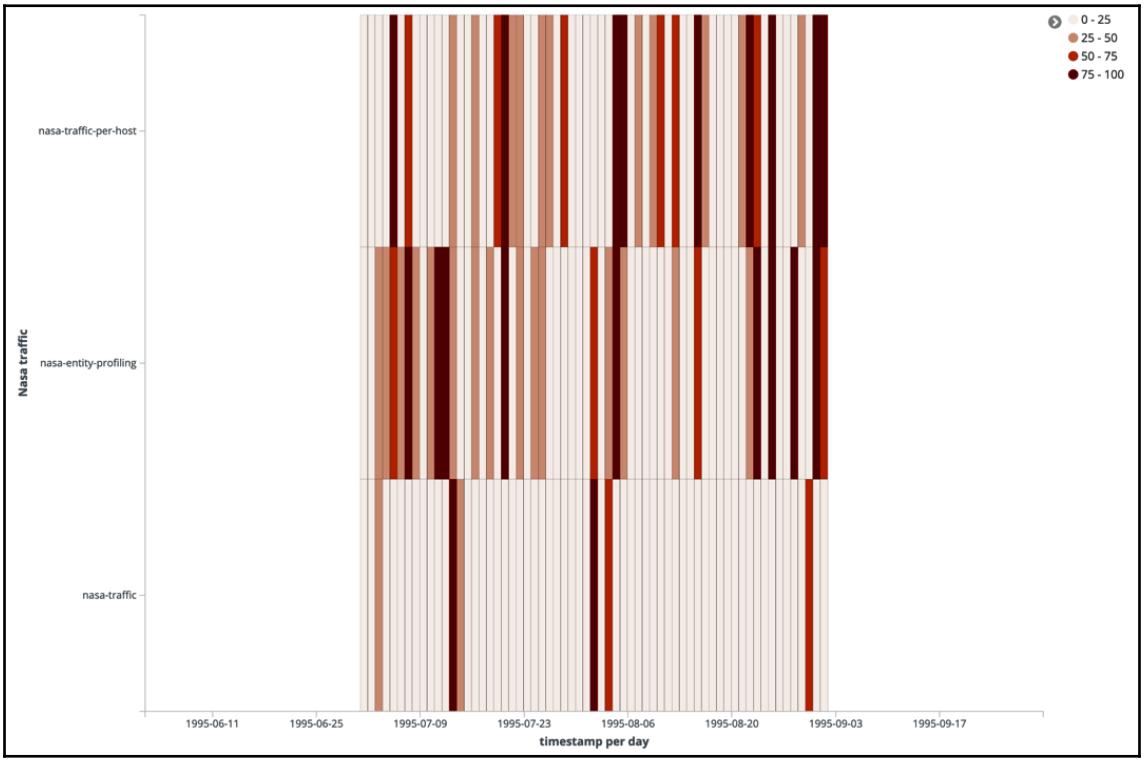

.ml-anomalies*
Data
Options
Metrics
Value Count
Buckets
X-Axis
Aggregation
Date Histogram help
Date Histogram
Field
timestamp
Interval
Auto
Custom Label
Advanced
Add sub-buckets

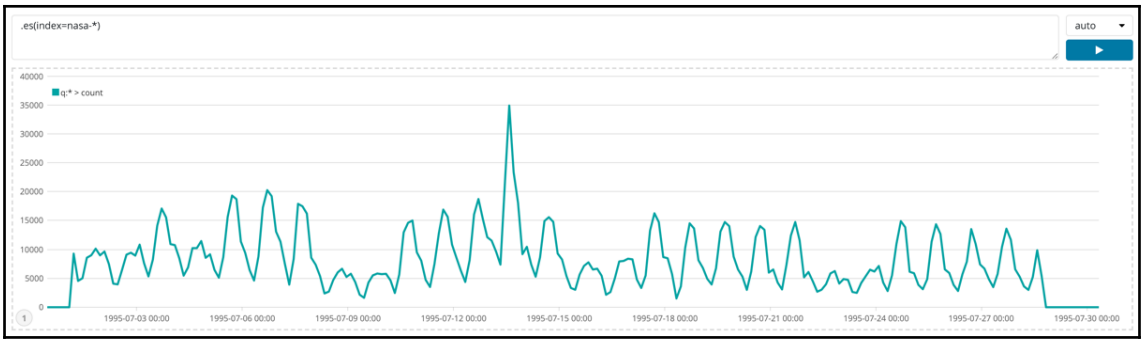

Advanced
Y-Axis
Sub Aggregation
Terms help
Terms
Field
job_id
Order By
metric: Count
Order
Size
Descending
5
Group other values in separate bucket
Show missing values
Custom Label
Nasa traffic

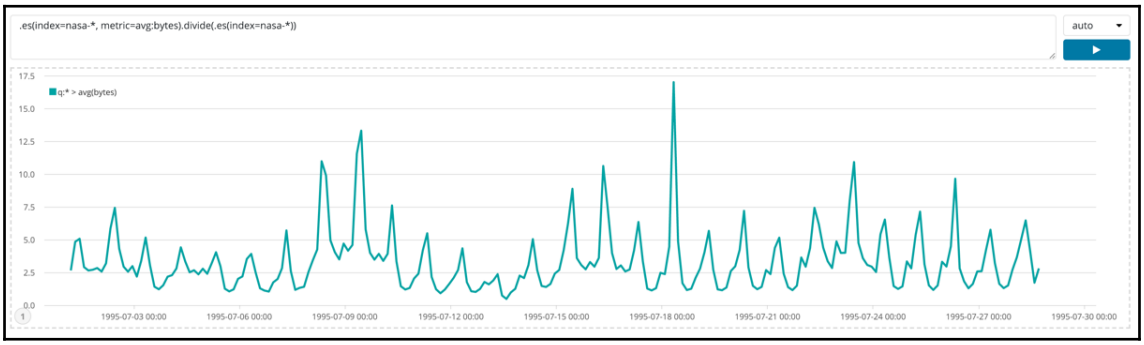

0 - 350
350 - 700
700 - 1,050
1,050 - 1,400
nasa-entity-profiling
nasa-traffic-per-host
nasa-traffic
Nasa traffic
1995-06-11
1995-06-25
1995-07-09
1995-07-23
1995-08-06
1995-08-20
1995-09-03
1995-09-17
timestamp per day

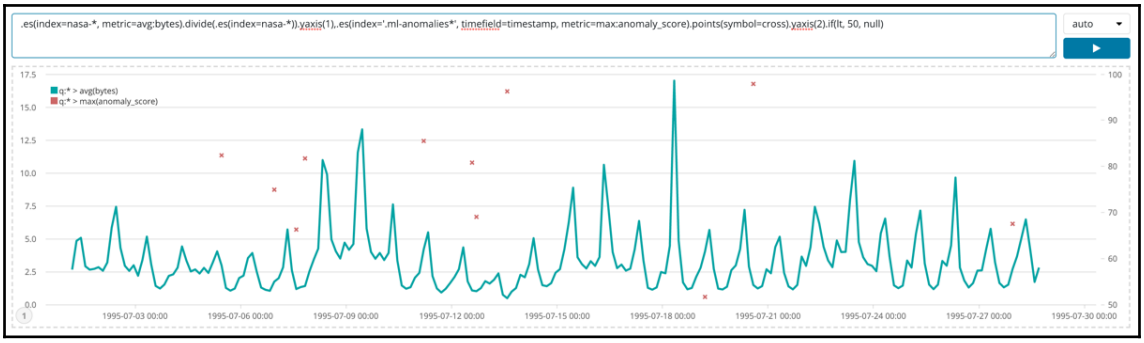

Metrics
Value
Aggregation
Max help
Max
Field
anomaly_score
Custom Label
Advanced

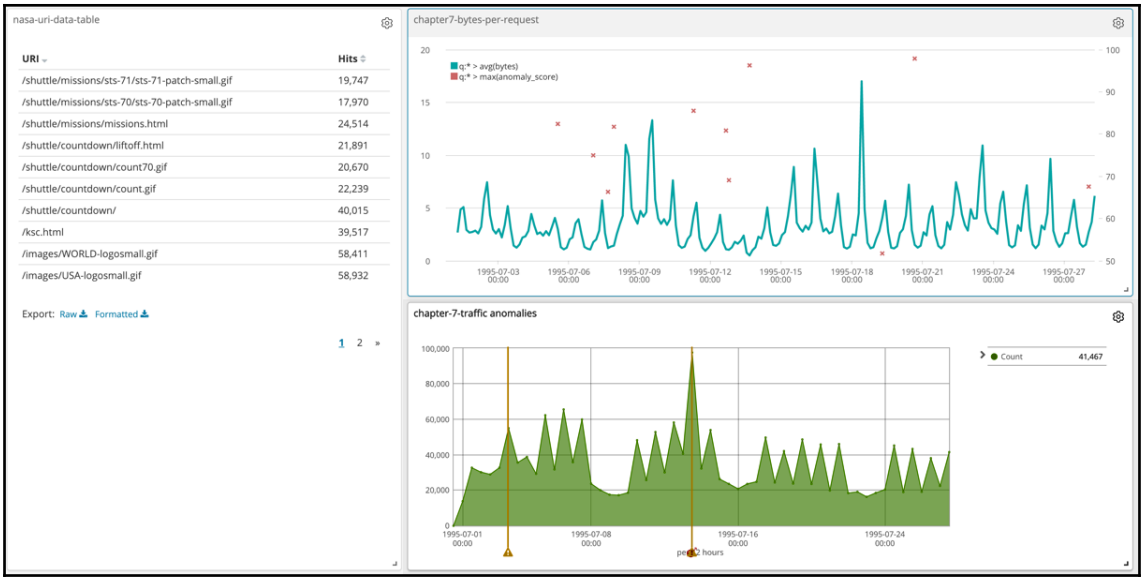

.ml-anomalies*
Data
Options
Basic Settings
Show Tooltips
Highlight
Legend Position
right
Heatmap Settings
Color Schema
Reds

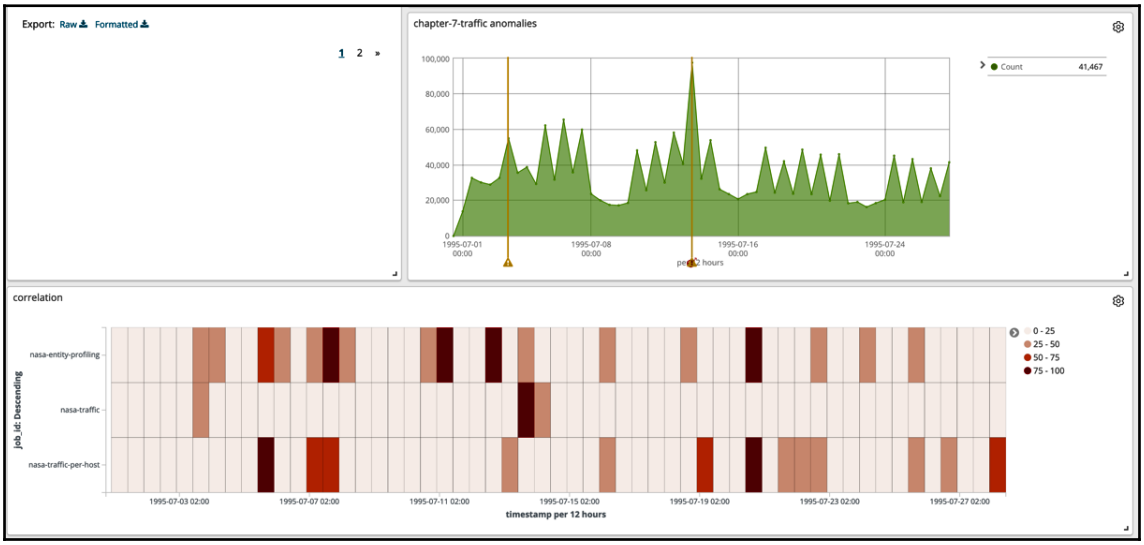

0 - 25
25 - 50
50 - 75
75 - 100
nasa-traffic-per-host
nasa-entity-profiling
nasa-traffic
Nasa traffic
1995-06-11
1995-06-25
1995-07-09
1995-07-23
1995-08-06
1995-08-20
1995-09-03
1995-09-17
timestamp per day


.es(index=nasa-*)
auto
q:* > count
40000
35000
30000
25000
20000
15000
10000
5000
0
1995-07-03 00:00
1995-07-06 00:00
1995-07-09 00:00
1995-07-12 00:00
1995-07-15 00:00
1995-07-18 00:00
1995-07-21 00:00
1995-07-24 00:00
1995-07-27 00:00
1995-07-30 00:00

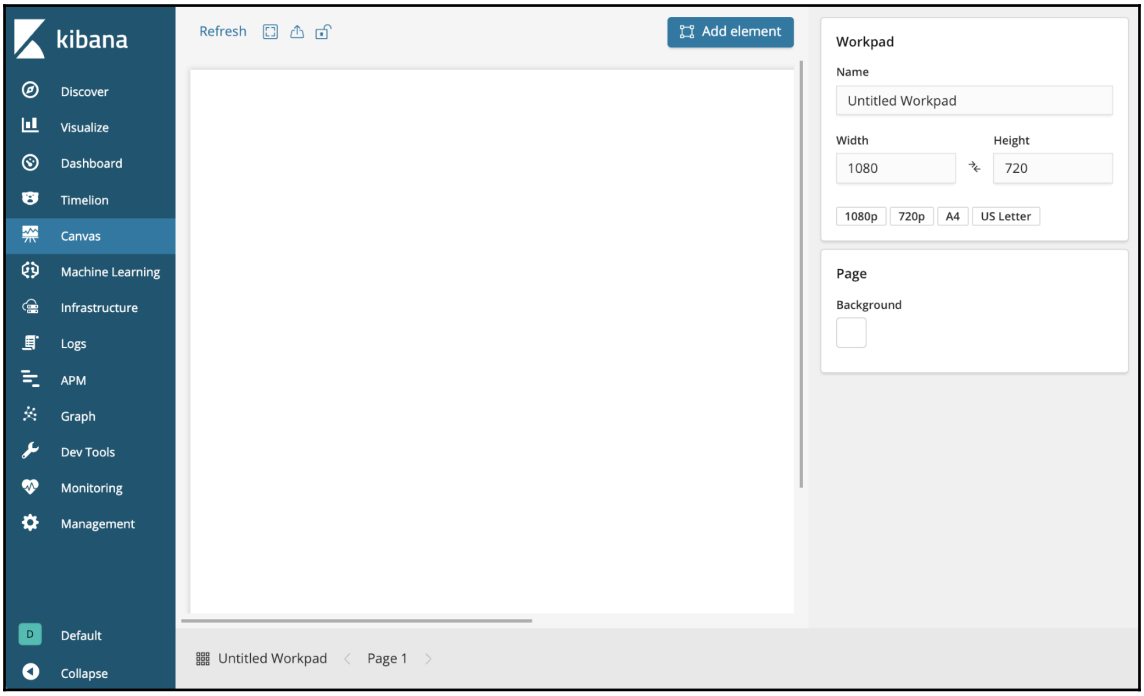

.es(index=nasa-*, metric=avg:bytes).divide(.es(index=nasa-*))
auto
q:* > avg(bytes)
17.5
15.0
12.5
10.0
7.5
5.0
2.5
0.0
1995-07-03 00:00
1995-07-06 00:00
1995-07-09 00:00
1995-07-12 00:00
1995-07-15 00:00
1995-07-18 00:00
1995-07-21 00:00
1995-07-24 00:00
1995-07-27 00:00
1995-07-30 00:00

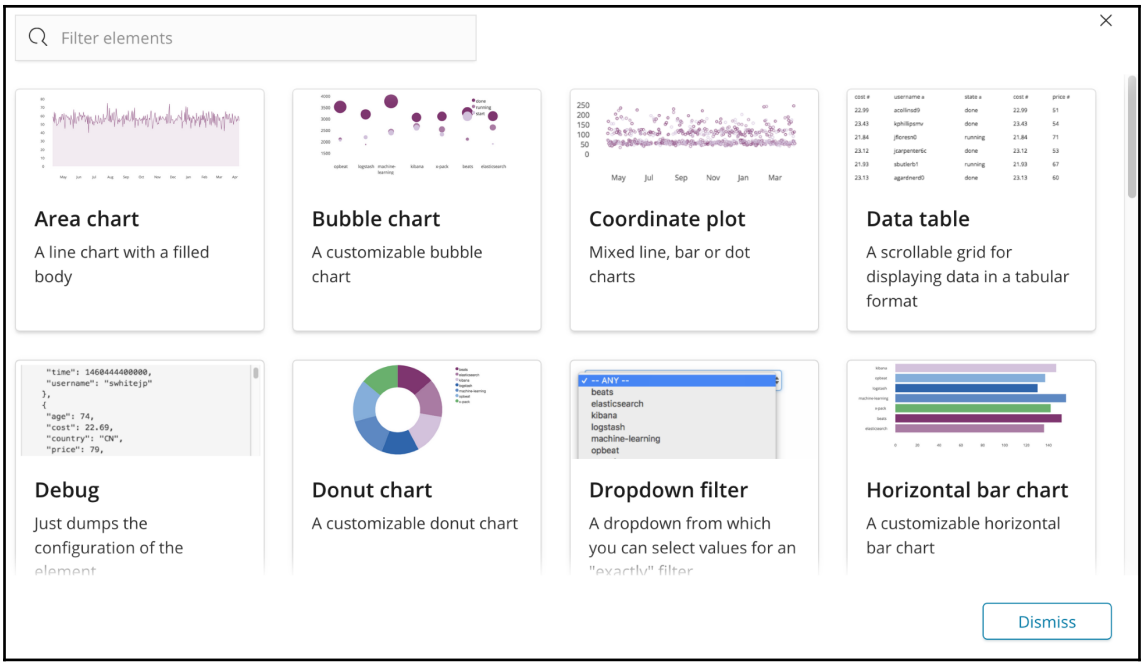

.es(index=nasa-*, metric=avg:bytes).divide(.es(index=nasa-*)).yaxis(1),.es(index='.ml-anomalies*', timefield=timestamp, metric=max:anomaly_score).points(symbol=cross).yaxis(2).if(lt, 50, null)
auto
q:* > avg(bytes)
q:* > max(anomaly_score)
17.5
15.0
12.5
10.0
7.5
5.0
2.5
0.0
100
90
80
70
60
50
1995-07-03 00:00
1995-07-06 00:00
1995-07-09 00:00
1995-07-12 00:00
1995-07-15 00:00
1995-07-18 00:00
1995-07-21 00:00
1995-07-24 00:00
1995-07-27 00:00
1995-07-30 00:00

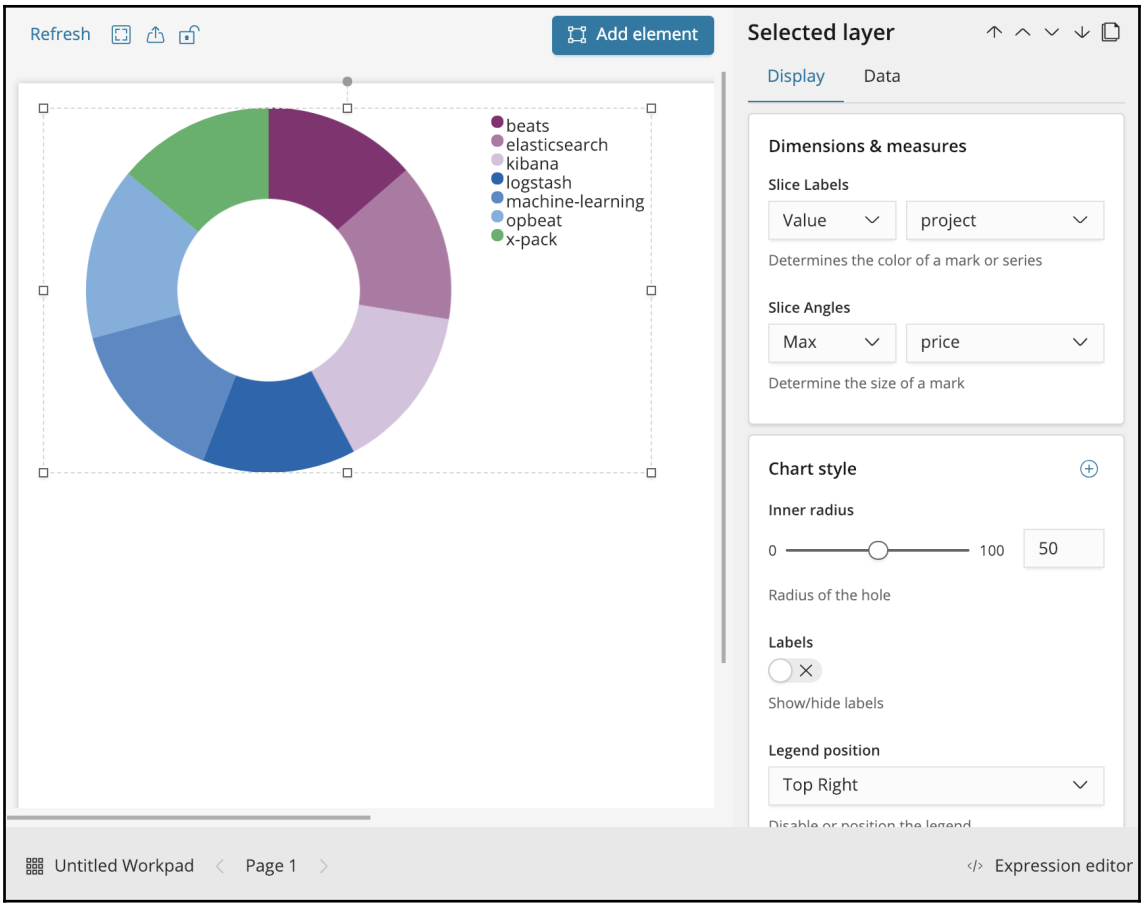

nasa-uri-data-table
URI
Hits
/shuttle/missions/sts-71/sts-71-patch-small.gif 19,747
/shuttle/missions/sts-70/sts-70-patch-small.gif 17,970
/shuttle/missions/missions.html 24,514
/shuttle/countdown/liftoff.html 21,891
/shuttle/countdown/count70.gif 20,670
/shuttle/countdown/count.gif 22,239
/shuttle/countdown/ 40,015
/ksc.html 39,517
/images/WORLD-logosmall.gif 58,411
/images/USA-logosmall.gif 58,932
Export: Raw Formatted
1 2 »
chapter7-bytes-per-request
q:* > avg(bytes)
q:* > max(anomaly_score)
chapter-7-traffic anomalies
Count 41,467
per 12 hours

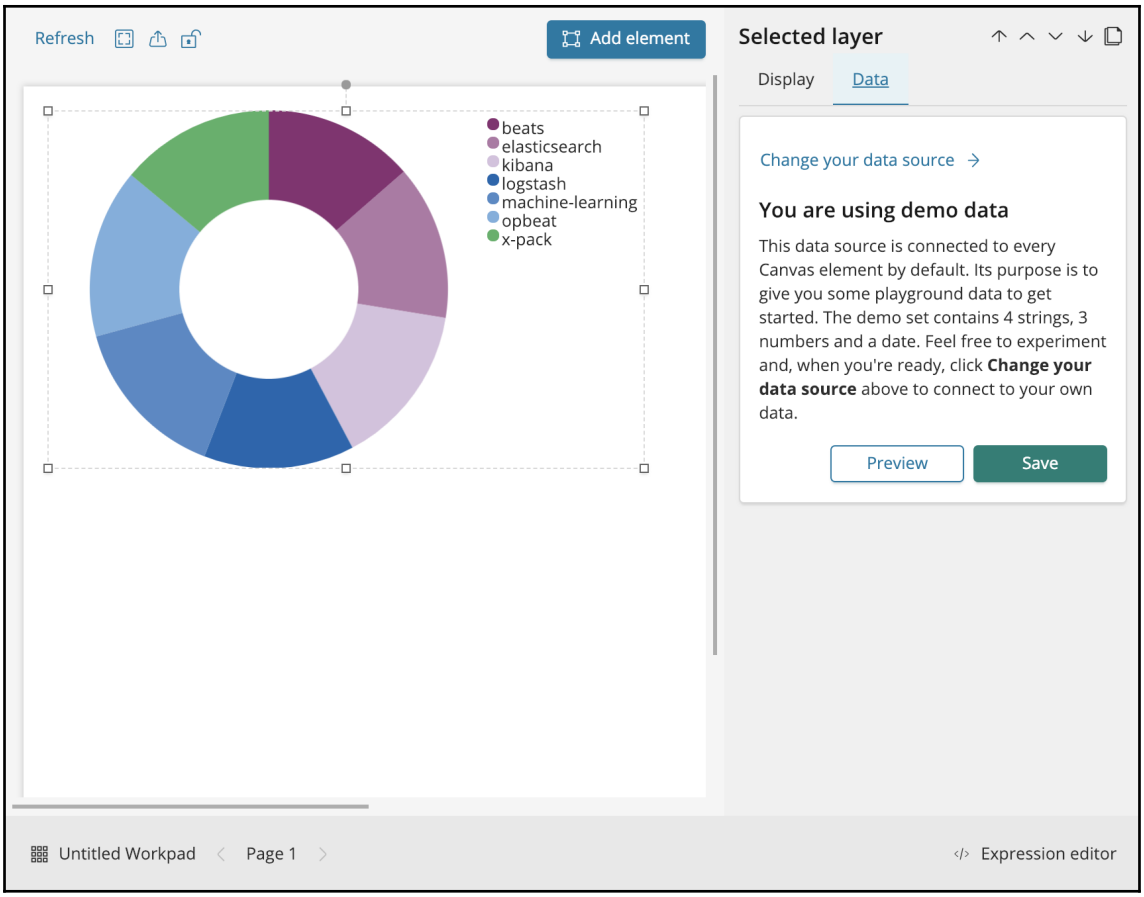

Export: Raw Formatted
1 2 »
chapter-7-traffic anomalies
Count 41,467
per 12 hours
correlation
nasa-entity-profiling
nasa-traffic
nasa-traffic-per-host
job_id: Descending
0 - 25
25 - 50
50 - 75
75 - 100
timestamp per 12 hours

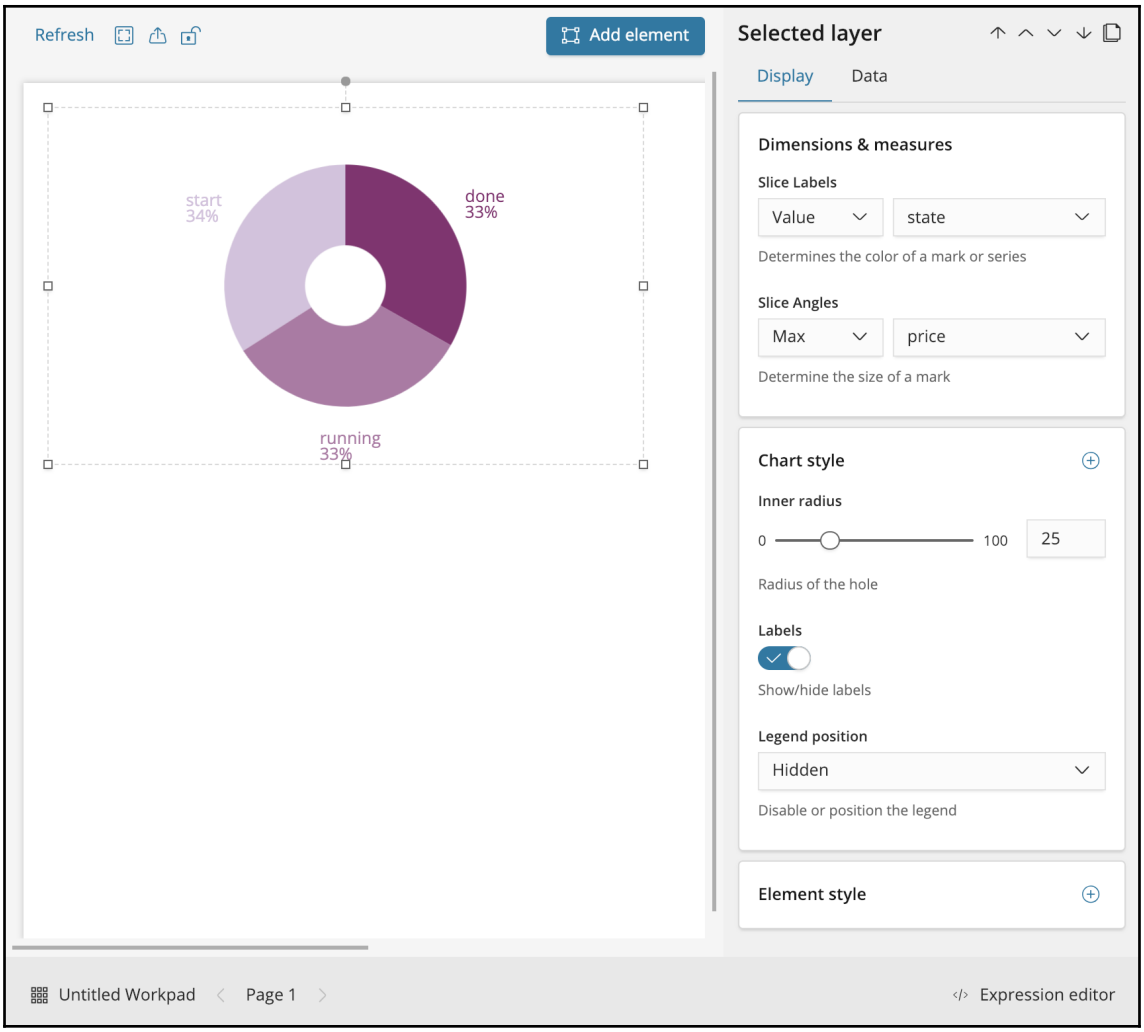
Chapter 8: Using Elastic ML with Kibana Canvas

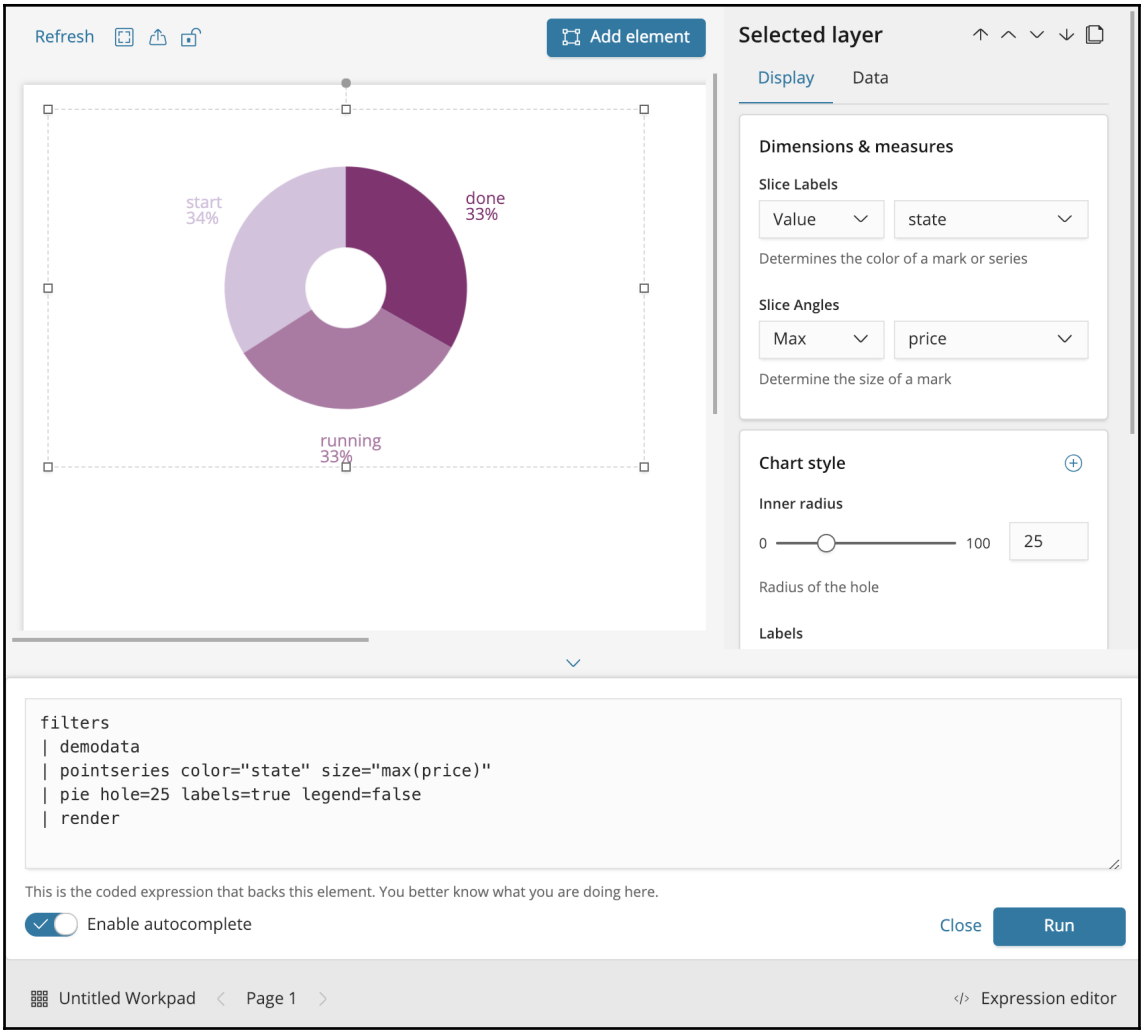


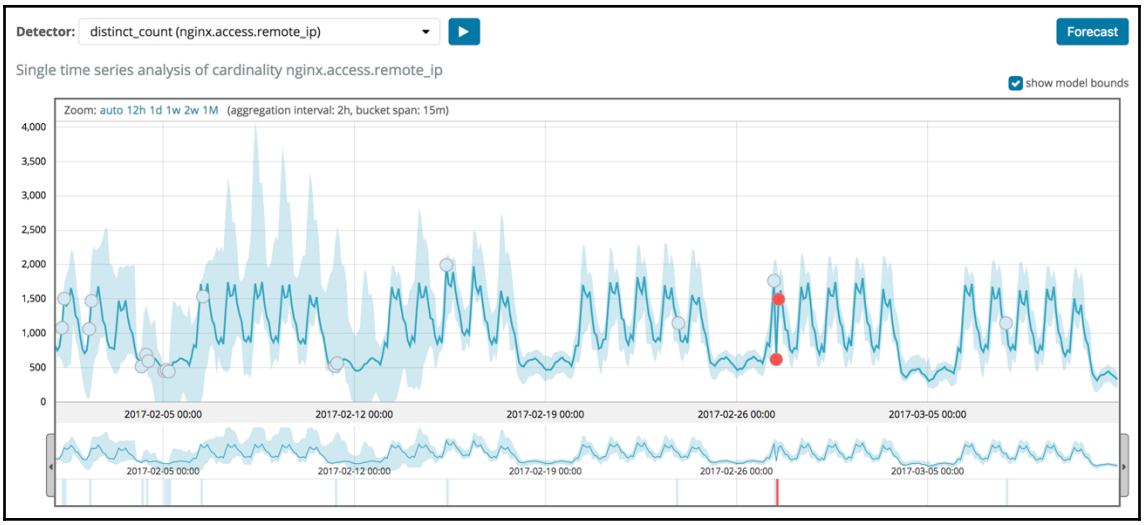

Filter elements
Area chart
A line chart with a filled body
Bubble chart
A customizable bubble chart
Coordinate plot
Mixed line, bar or dot charts
Data table
A scrollable grid for displaying data in a tabular format
Debug
Just dumps the configuration of the element
Donut chart
A customizable donut chart
Dropdown filter
A dropdown from which you can select values for an "exactly" filter
Horizontal bar chart
A customizable horizontal bar chart
-- ANY --
beats
elasticsearch
kibana
logstash
machine-learning
opbeat
Dismiss

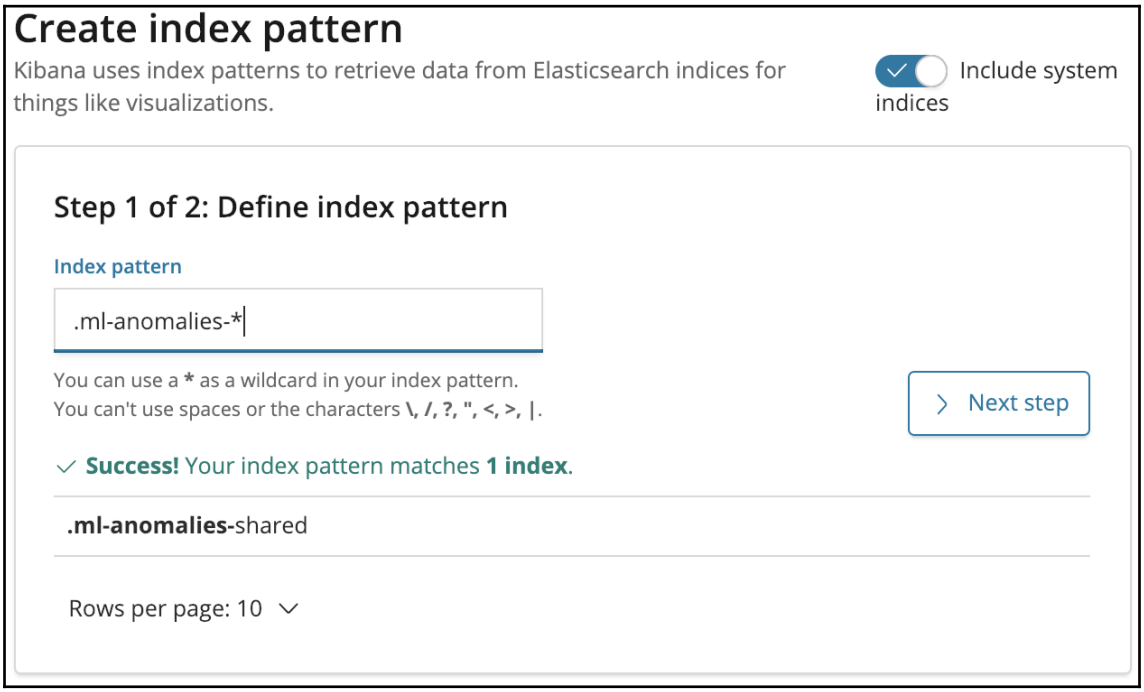

Refresh
Add element
beats
elasticsearch
kibana
logstash
machine-learning
opbeat
x-pack
Selected layer
Display
Data
Dimensions & measures
Slice Labels
Value
project
Determines the color of a mark or series
Slice Angles
Max
price
Determine the size of a mark
Chart style
Inner radius
0
100
50
Radius of the hole
Labels
Show/hide labels
Legend position
Top Right
Untitled Workpad
Page 1
Expression editor

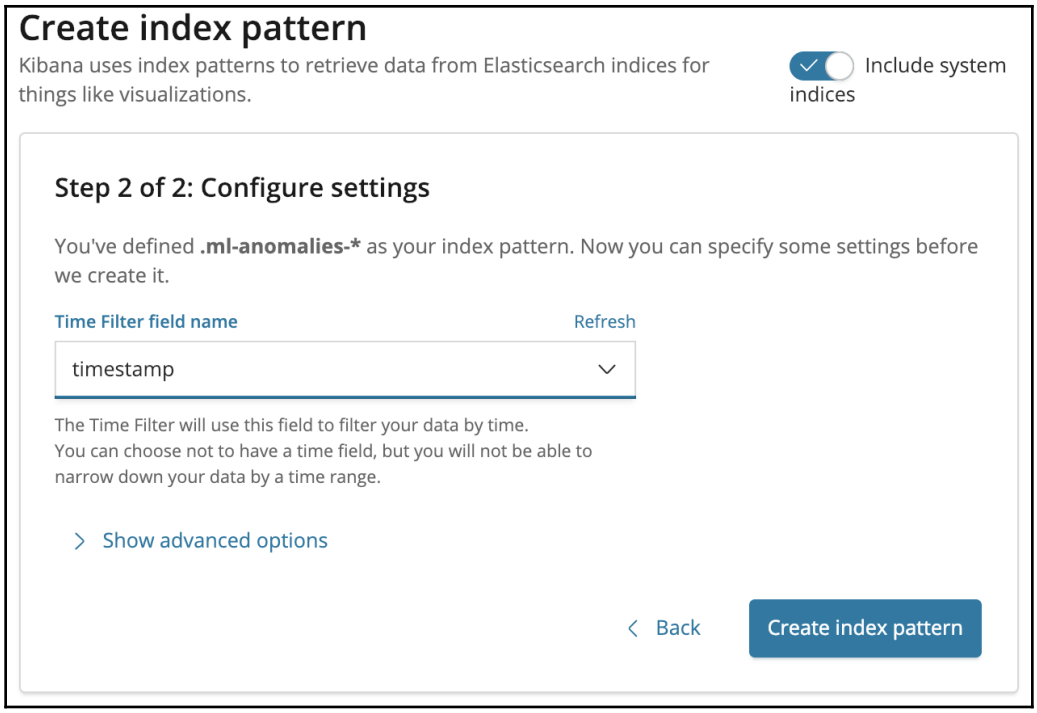

Refresh
Add element
Selected layer
Display
Data
beats
elasticsearch
kibana
logstash
machine-learning
opbeat
x-pack
Change your data source
You are using demo data
This data source is connected to every Canvas element by default. Its purpose is to give you some playground data to get started. The demo set contains 4 strings, 3 numbers and a date. Feel free to experiment and, when you're ready, click Change your data source above to connect to your own data.
Preview
Save
Untitled Workpad
Page 1
Expression editor


Refresh
Add element
start
34%
done
33%
running
33%
Selected layer
Display
Data
Dimensions & measures
Slice Labels
Value
state
Determines the color of a mark or series
Slice Angles
Max
price
Determine the size of a mark
Chart style
Inner radius
0
100
25
Radius of the hole
Labels
Show/hide labels
Legend position
Hidden
Disable or position the legend
Element style
Untitled Workpad
Page 1
Expression editor


Refresh
Add element
start
34%
done
33%
running
33%
Selected layer
Display
Data
Dimensions & measures
Slice Labels
Value
state
Determines the color of a mark or series
Slice Angles
Max
price
Determine the size of a mark
Chart style
Inner radius
0
100
25
Radius of the hole
Labels
filters
| demodata
| pointseries color="state" size="max(price)"
| pie hole=25 labels=true legend=false
| render
This is the coded expression that backs this element. You better know what you are doing here.
Enable autocomplete
Close
Run
Untitled Workpad
Page 1
Expression editor

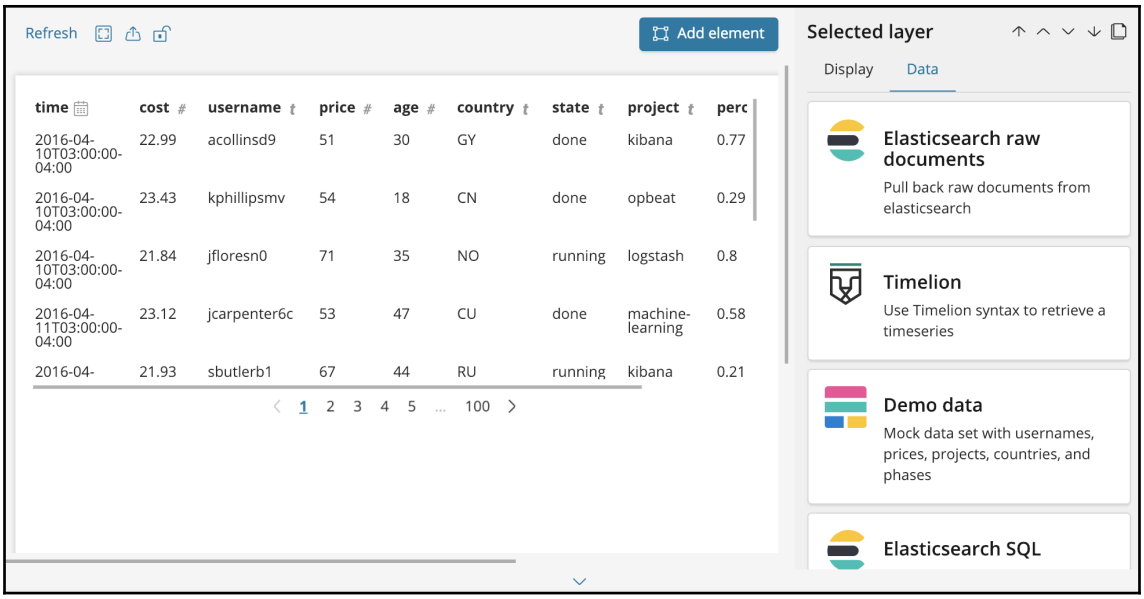

Detector: distinct_count (nginx.access.remote_ip)
Forecast
Single time series analysis of cardinality nginx.access.remote_ip
show model bounds
Zoom: auto 12h 1d 1w 2w 1M (aggregation interval: 2h, bucket span: 15m)
4,000
3,500
3,000
2,500
2,000
1,500
1,000
500
0
2017-02-05 00:00
2017-02-12 00:00
2017-02-19 00:00
2017-02-26 00:00
2017-03-05 00:00

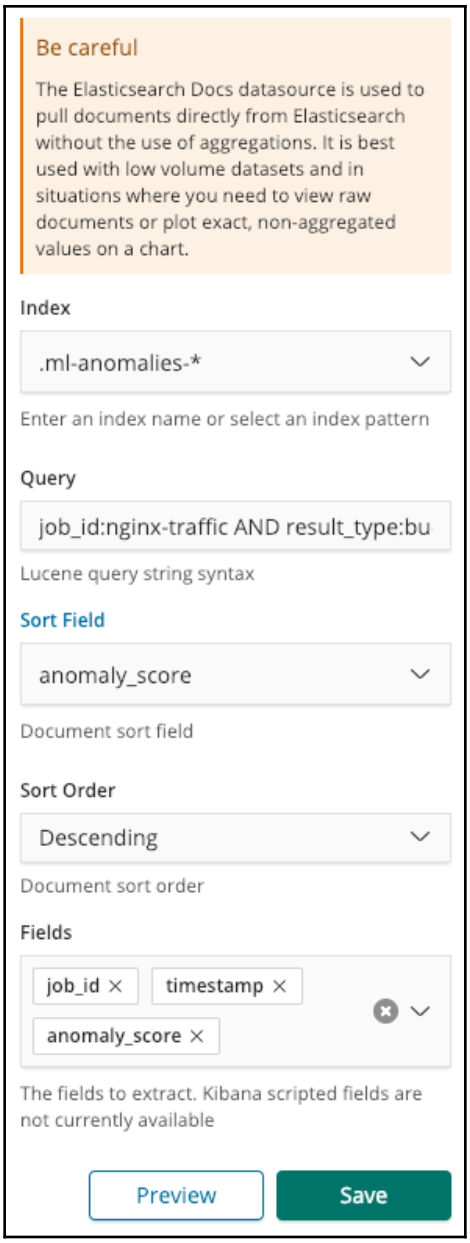

Create index pattern
Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.
Include system indices
Step 1 of 2: Define index pattern
Index pattern
.ml-anomalies-*
You can use a * as a wildcard in your index pattern.
You can't use spaces or the characters \, /, ?, ", <, >, |.
Next step
Success! Your index pattern matches 1 index.
.ml-anomalies-shared
Rows per page: 10

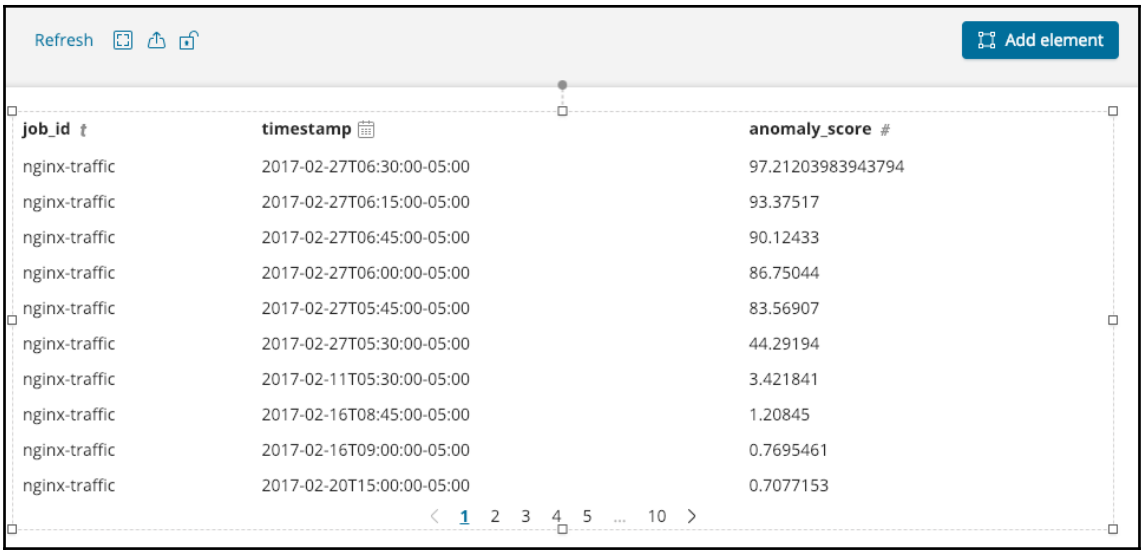


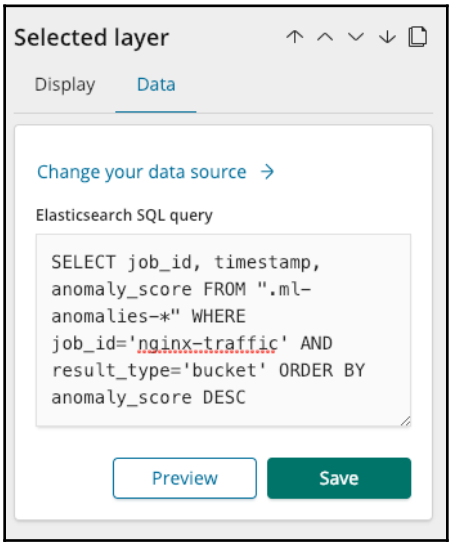
time	cost #	username a	price #	age #	country a	state a	project a
2016-04-10T09:00:00+02:00	22.99	acollinsd9	51	30	GY	done	kibana
2016-04-10T09:00:00+02:00	23.43	kphillipsmv	54	18	CN	done	opbeat
2016-04-10T09:00:00+02:00	21.84	jfloresn0	71	35	NO	running	logstash
2016-04-11T09:00:00+02:00	23.12	jcarpenter6c	53	47	CU	done	machine-learning
2016-04-11T09:00:00+02:00	21.93	sbutlerb1	67	44	RU	running	kibana
2016-04-11T09:00:00+02:00	23.13	agardnerd0	60	49	ID	done	logstash
2016-04-11T09:00:00+02:00	22.73	preyesej	53	33	CN	done	machine-learning
2016-04-12T09:00:00+02:00	22.75	swhitejp	53	32	CN	done	opbeat
2016-04-13T09:00:00+02:00	22.69	rjackson2q	79	74	CN	done	opbeat
2016-04-13T09:00:00+02:00	23.63	sgraya7	64	70	ID	start	logstash

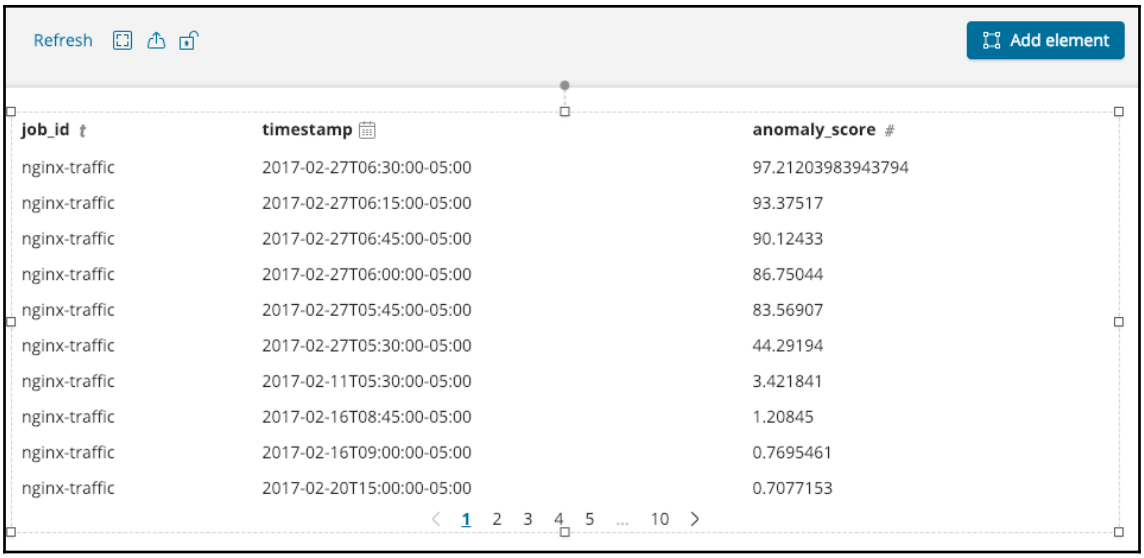
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 ›

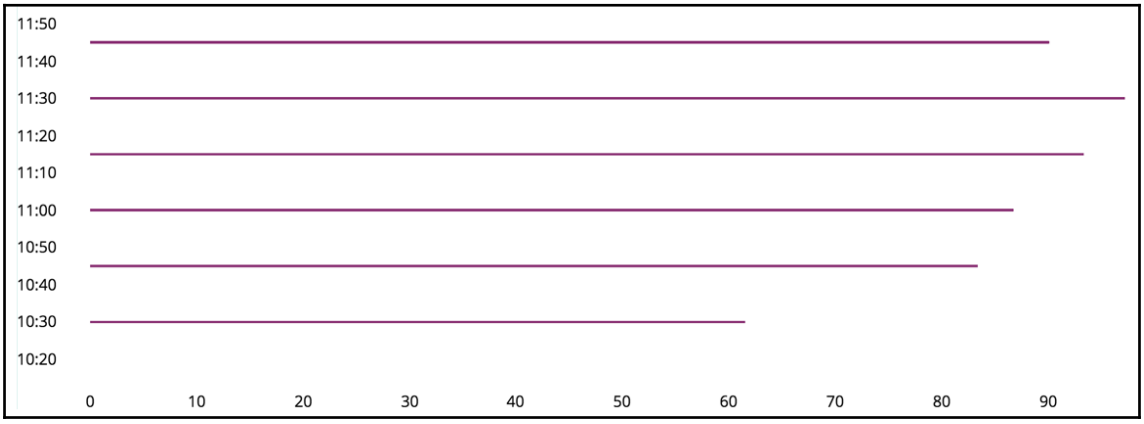

Refresh
Add element
Selected layer
Display
Data
time
cost
username
price
age
country
state
project
perc
2016-04-10T03:00:00-04:00
22.99
acollinsd9
51
30
GY
done
kibana
0.77
2016-04-10T03:00:00-04:00
23.43
kphillipsmv
54
18
CN
done
opbeat
0.29
2016-04-10T03:00:00-04:00
21.84
jfloresn0
71
35
NO
running
logstash
0.8
2016-04-11T03:00:00-04:00
23.12
jcarpenter6c
53
47
CU
done
machine-learning
0.58
2016-04-
21.93
sbutlerb1
67
44
RU
running
kibana
0.21
1 2 3 4 5 ... 100
Elasticsearch raw documents
Pull back raw documents from elasticsearch
Timelion
Use Timelion syntax to retrieve a timeseries
Demo data
Mock data set with usernames, prices, projects, countries, and phases
Elasticsearch SQL

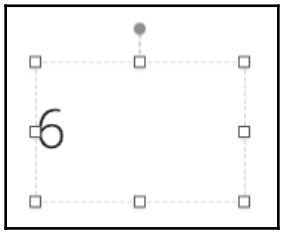

Be careful
The Elasticsearch Docs datasource is used to pull documents directly from Elasticsearch without the use of aggregations. It is best used with low volume datasets and in situations where you need to view raw documents or plot exact, non-aggregated values on a chart.
Index
.ml-anomalies-*
Enter an index name or select an index pattern
Query
job_id:nginx-traffic AND result_type:bu
Lucene query string syntax
Sort Field
anomaly_score
Document sort field
Sort Order
Descending
Document sort order
Fields
job_id ×
timestamp ×
anomaly_score ×
The fields to extract. Kibana scripted fields are not currently available
Preview
Save

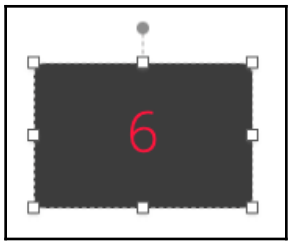

Refresh
Add element
job_id
timestamp
anomaly_score
nginx-traffic 2017-02-27T06:30:00-05:00 97.21203983943794
nginx-traffic 2017-02-27T06:15:00-05:00 93.37517
nginx-traffic 2017-02-27T06:45:00-05:00 90.12433
nginx-traffic 2017-02-27T06:00:00-05:00 86.75044
nginx-traffic 2017-02-27T05:45:00-05:00 83.56907
nginx-traffic 2017-02-27T05:30:00-05:00 44.29194
nginx-traffic 2017-02-11T05:30:00-05:00 3.421841
nginx-traffic 2017-02-16T08:45:00-05:00 1.20845
nginx-traffic 2017-02-16T09:00:00-05:00 0.7695461
nginx-traffic 2017-02-20T15:00:00-05:00 0.7077153
1 2 3 4 5 ... 10

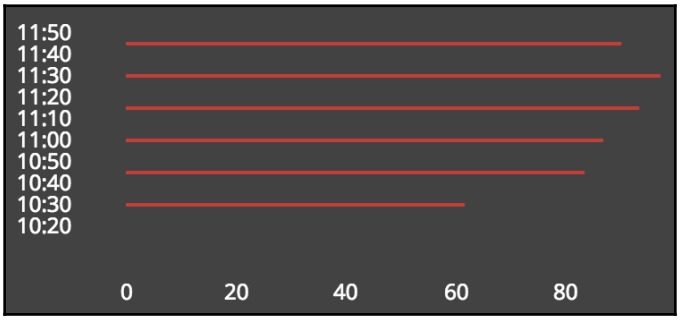

Selected layer
Display
Data
Change your data source
Elasticsearch SQL query
SELECT job_id, timestamp, anomaly_score FROM ".ml-anomalies-*" WHERE job_id='nginx-traffic' AND result_type='bucket' ORDER BY anomaly_score DESC
Preview
Save

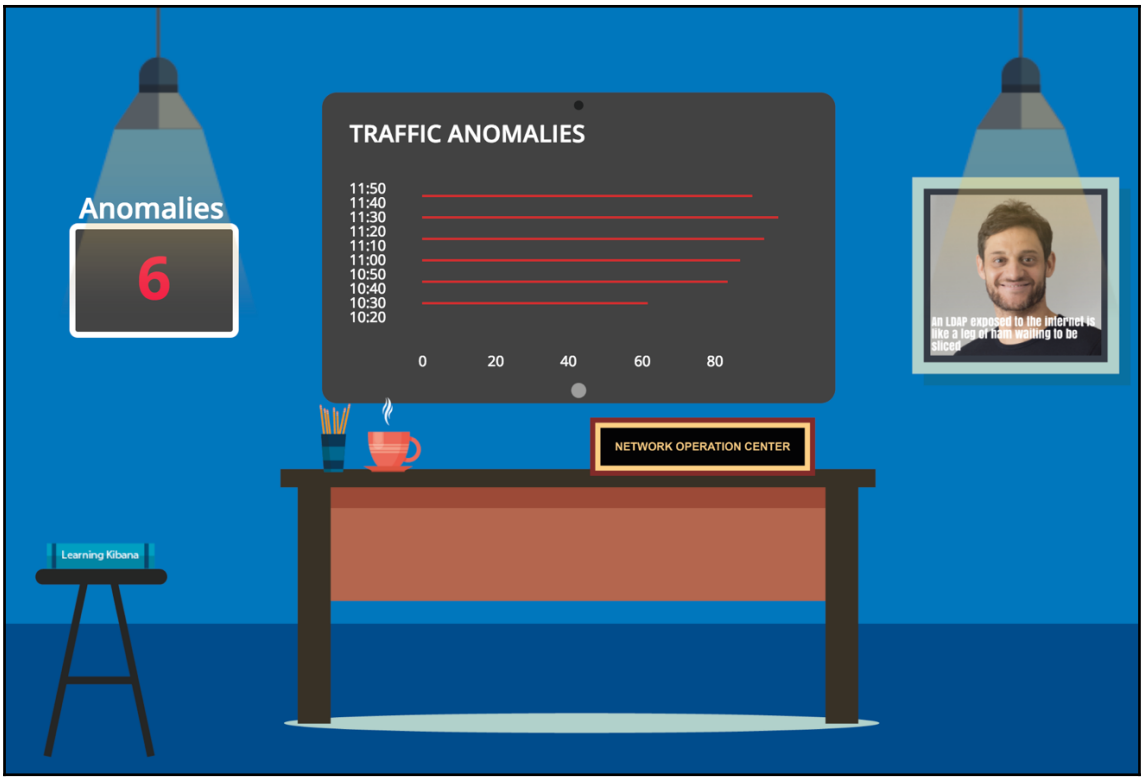

Refresh
Add element
job_id
timestamp
anomaly_score
nginx-traffic 2017-02-27T06:30:00-05:00 97.21203983943794
nginx-traffic 2017-02-27T06:15:00-05:00 93.37517
nginx-traffic 2017-02-27T06:45:00-05:00 90.12433
nginx-traffic 2017-02-27T06:00:00-05:00 86.75044
nginx-traffic 2017-02-27T05:45:00-05:00 83.56907
nginx-traffic 2017-02-27T05:30:00-05:00 44.29194
nginx-traffic 2017-02-11T05:30:00-05:00 3.421841
nginx-traffic 2017-02-16T08:45:00-05:00 1.20845
nginx-traffic 2017-02-16T09:00:00-05:00 0.7695461
nginx-traffic 2017-02-20T15:00:00-05:00 0.7077153
1 2 3 4 5 ... 10


11:50
11:40
11:30
11:20
11:10
11:00
10:50
10:40
10:30
10:20
0 10 20 30 40 50 60 70 80 90

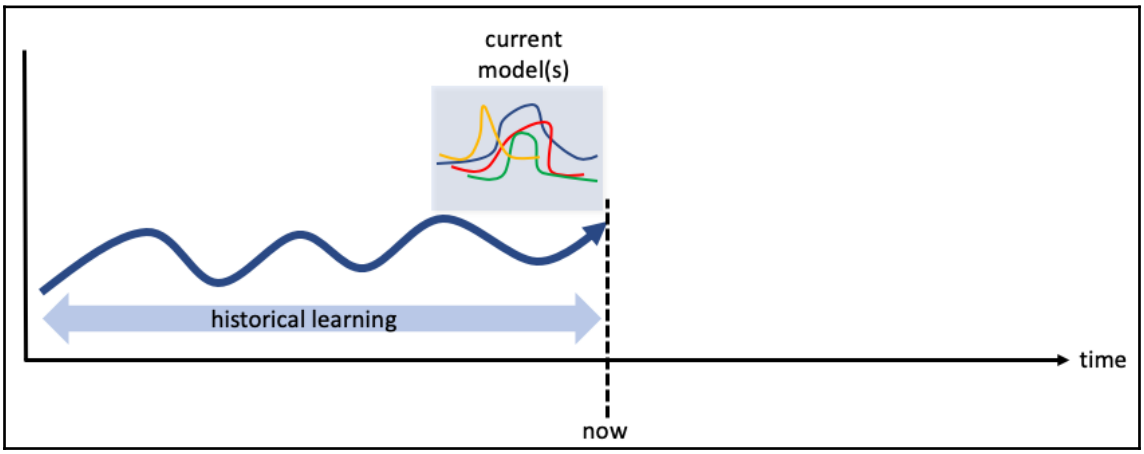

6

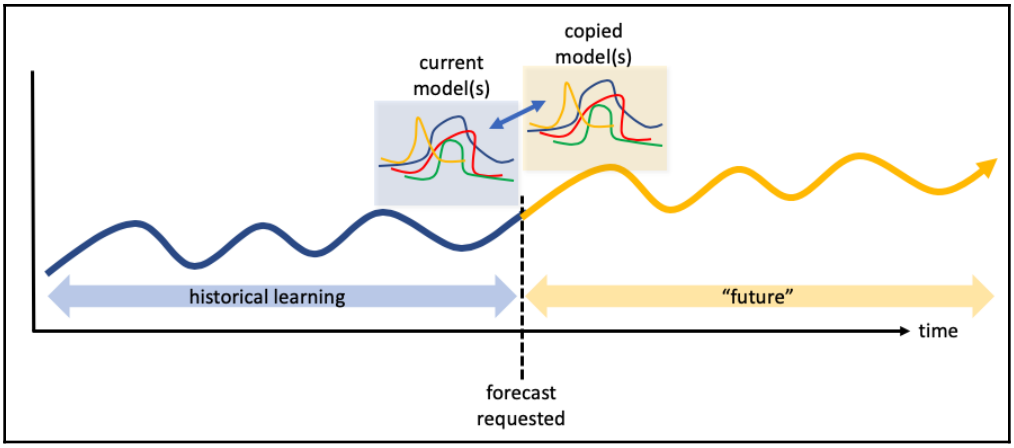

6

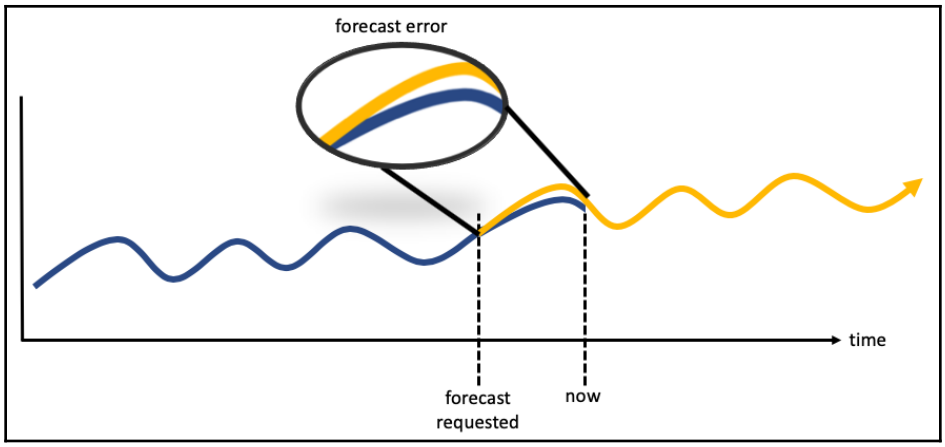

11:50
11:40
11:30
11:20
11:10
11:00
10:50
10:40
10:30
10:20
0
20
40
60
80

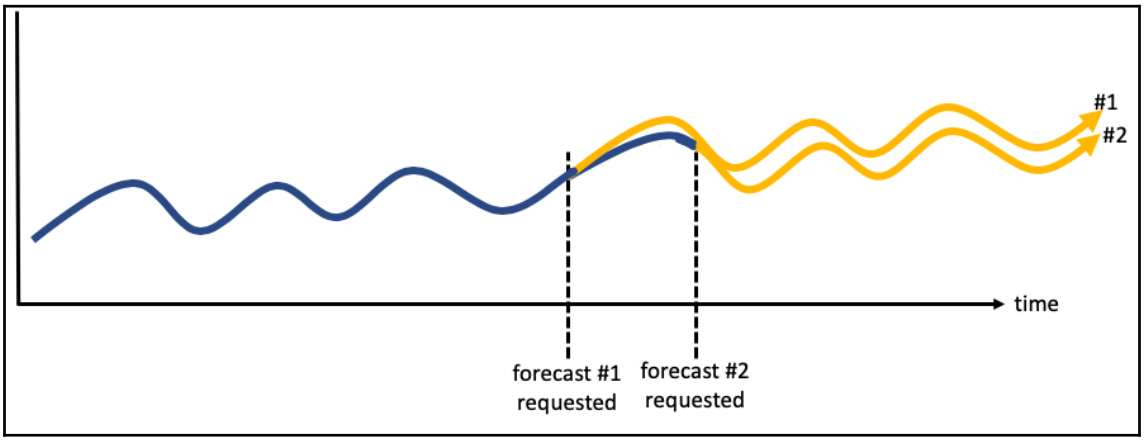

Anomalies
6
TRAFFIC ANOMALIES
11:50
11:40
11:30
11:20
11:10
11:00
10:50
10:40
10:30
10:20
0
20
40
60
80
NETWORK OPERATION CENTER
Learning Kibana

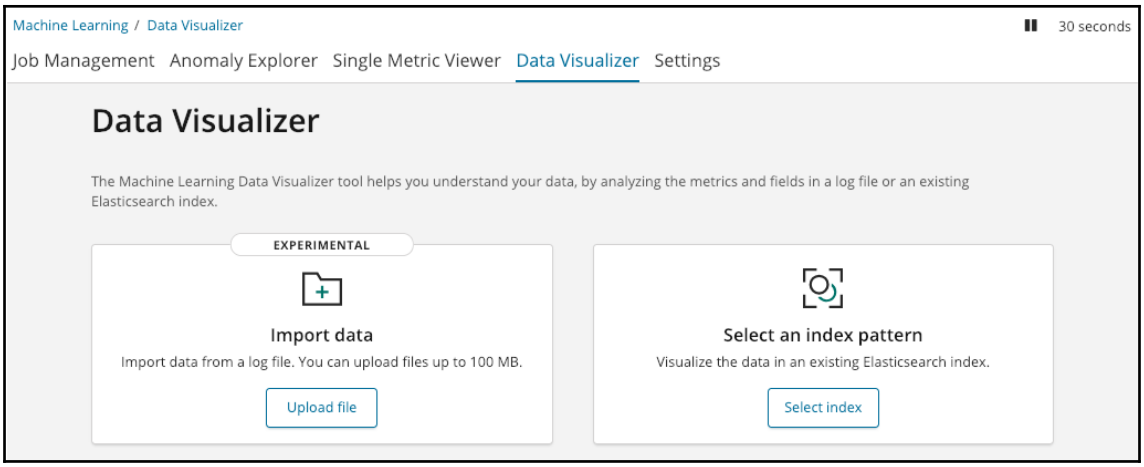
Chapter 9:Forecasting

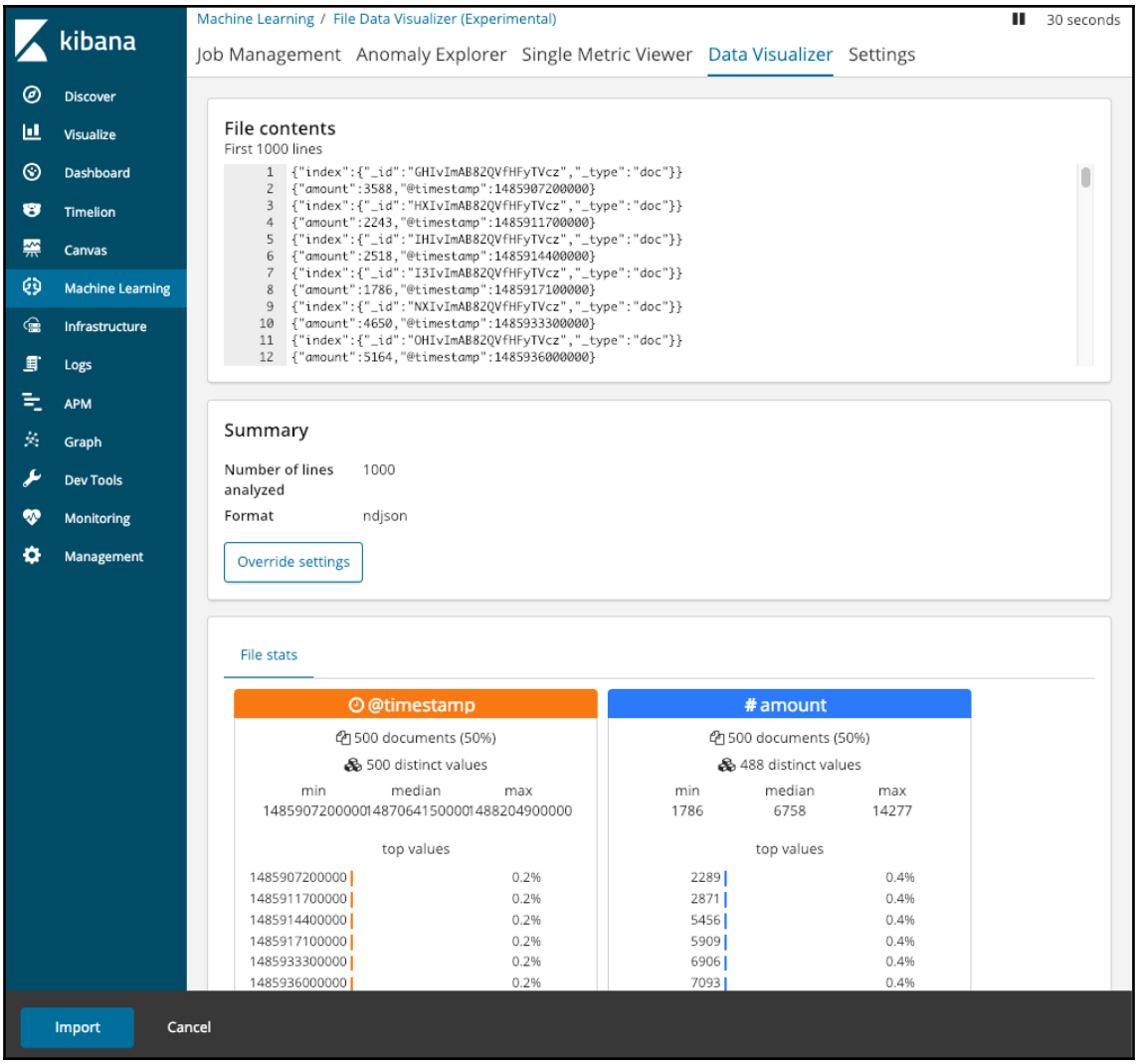


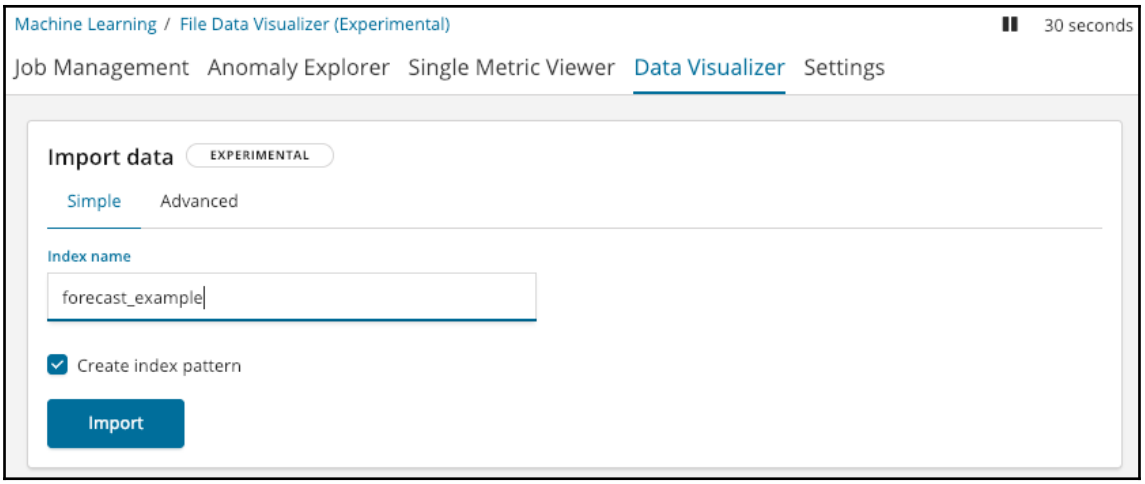


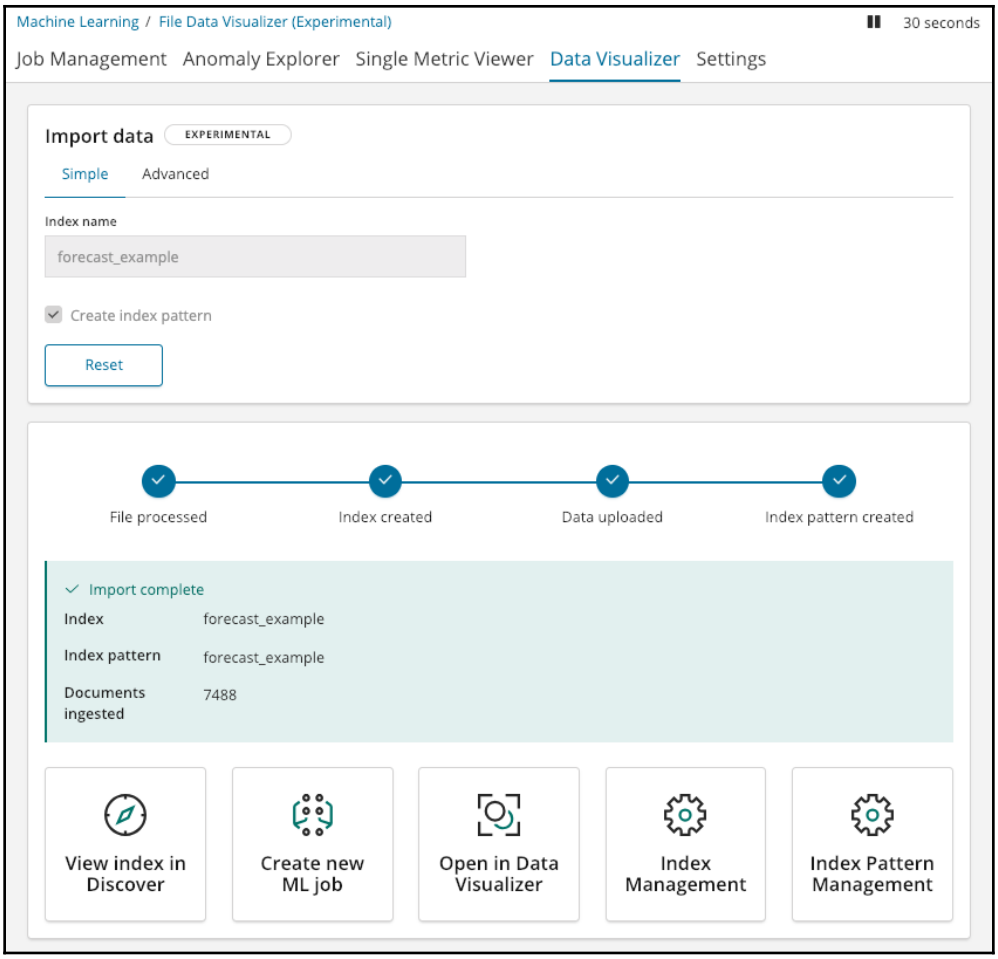

forecast error
time
forecast
requested
now

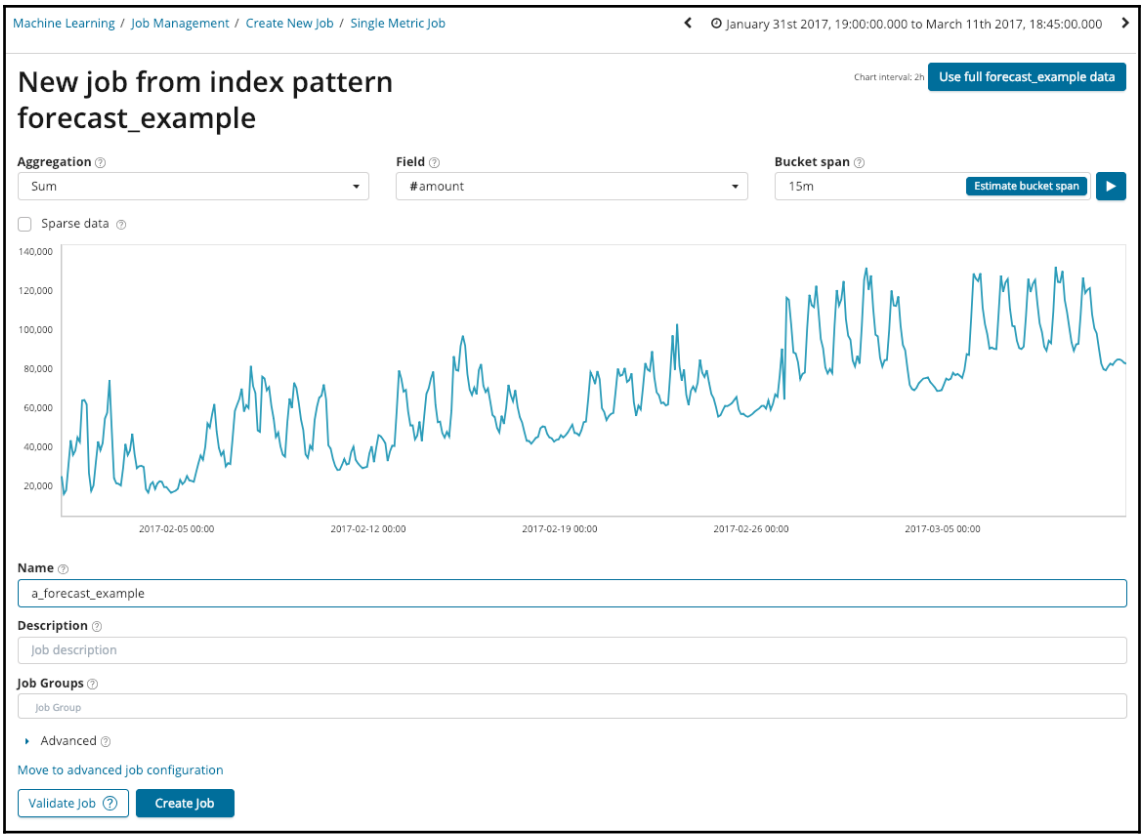

#1
#2
time
forecast #1
requested
forecast #2
requested

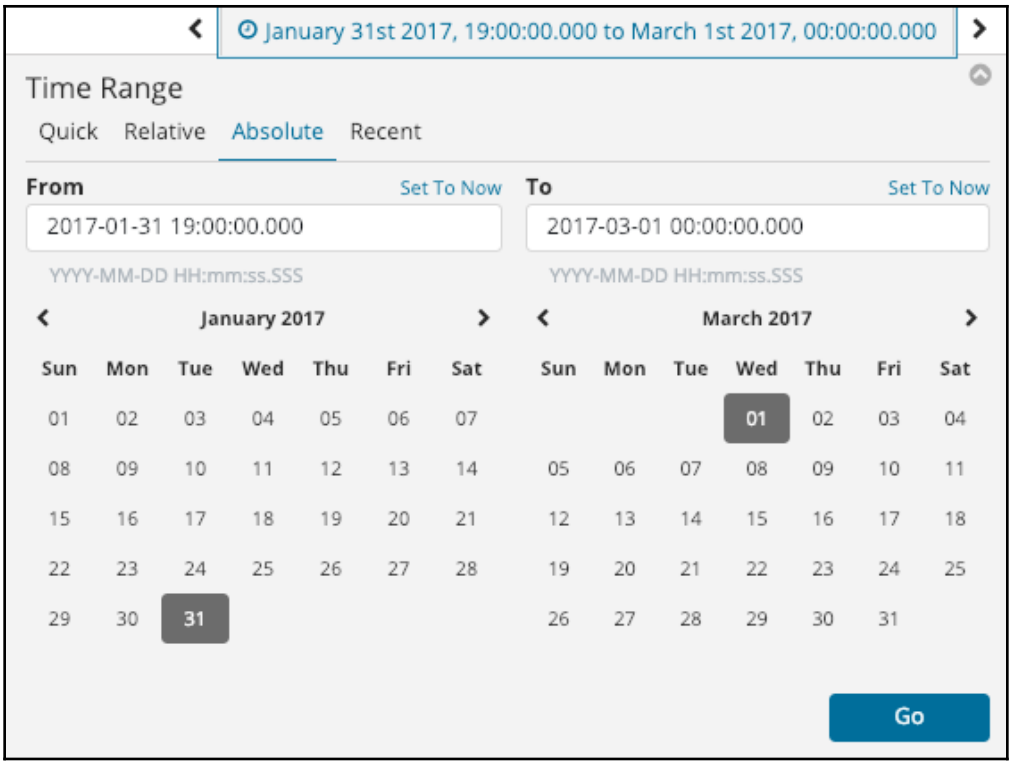

Machine Learning / Data Visualizer
30 seconds
Job Management
Anomaly Explorer
Single Metric Viewer
Data Visualizer
Settings
Data Visualizer
The Machine Learning Data Visualizer tool helps you understand your data, by analyzing the metrics and fields in a log file or an existing Elasticsearch index.
EXPERIMENTAL
Import data
Import data from a log file. You can upload files up to 100 MB.
Upload file
Select an index pattern
Visualize the data in an existing Elasticsearch index.
Select index

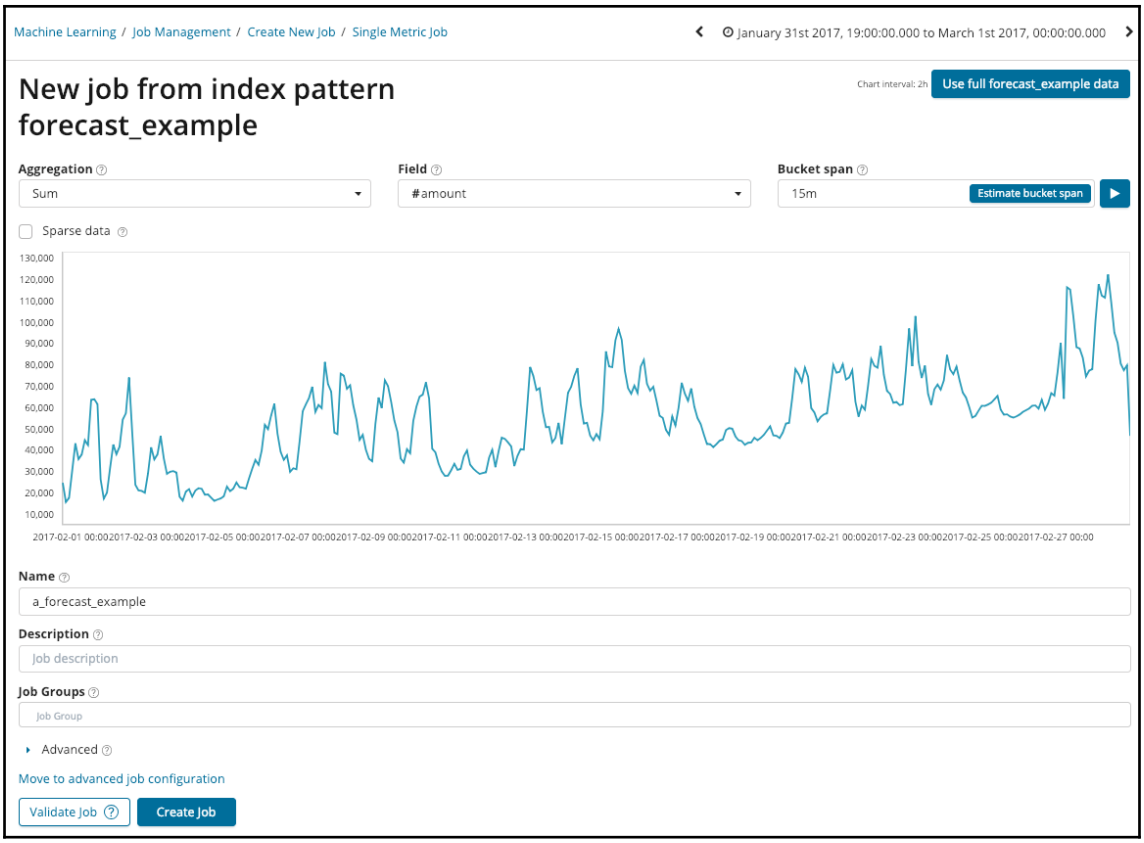

kibana
Discover
Visualize
Dashboard
Timelion
Canvas
Machine Learning
Infrastructure
Logs
APM
Graph
Dev Tools
Monitoring
Management
Machine Learning / File Data Visualizer (Experimental)
30 seconds
Job Management
Anomaly Explorer
Single Metric Viewer
Data Visualizer
Settings
File contents
First 1000 lines
1 {"index":{"_id":"GHIvImAB82QVfHFyTVcz","_type":"doc"}}
2 {"amount":3588,"@timestamp":1485907200000}
3 {"index":{"_id":"HXIvImAB82QVfHFyTVcz","_type":"doc"}}
4 {"amount":2243,"@timestamp":1485911700000}
5 {"index":{"_id":"IHIvImAB82QVfHFyTVcz","_type":"doc"}}
6 {"amount":2518,"@timestamp":1485914400000}
7 {"index":{"_id":"I3IvImAB82QVfHFyTVcz","_type":"doc"}}
8 {"amount":1786,"@timestamp":1485917100000}
9 {"index":{"_id":"NXIvImAB82QVfHFyTVcz","_type":"doc"}}
10 {"amount":4650,"@timestamp":1485933300000}
11 {"index":{"_id":"OHIvImAB82QVfHFyTVcz","_type":"doc"}}
12 {"amount":5164,"@timestamp":1485936000000}
Summary
Number of lines analyzed 1000
Format ndjson
Override settings
File stats
@timestamp
500 documents (50%)
500 distinct values
min median max
1485907200000 1487064150000 1488204900000
top values
1485907200000 0.2%
1485911700000 0.2%
1485914400000 0.2%
1485917100000 0.2%
1485933300000 0.2%
1485936000000 0.2%
amount
500 documents (50%)
488 distinct values
min median max
1786 6758 14277
top values
2289 0.4%
2871 0.4%
5456 0.4%
5909 0.4%
6906 0.4%
7093 0.4%
Import
Cancel

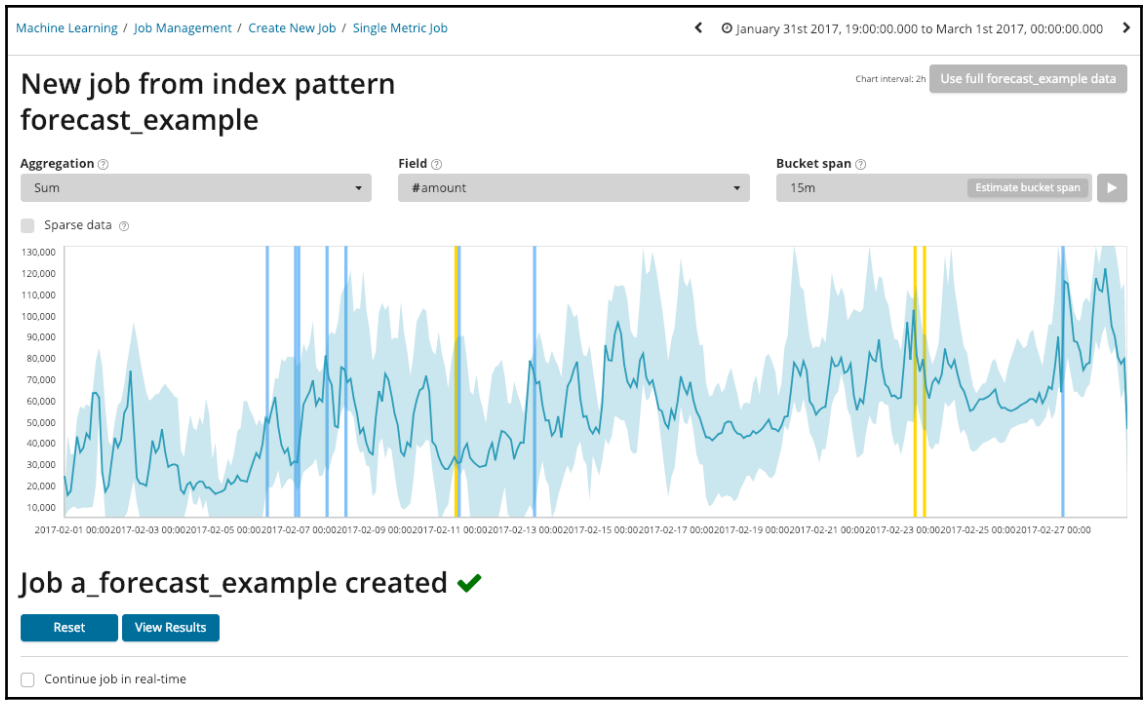

Machine Learning / File Data Visualizer (Experimental)
30 seconds
Job Management
Anomaly Explorer
Single Metric Viewer
Data Visualizer
Settings
Import data
EXPERIMENTAL
Simple
Advanced
Index name
forecast_example
Create index pattern
Import

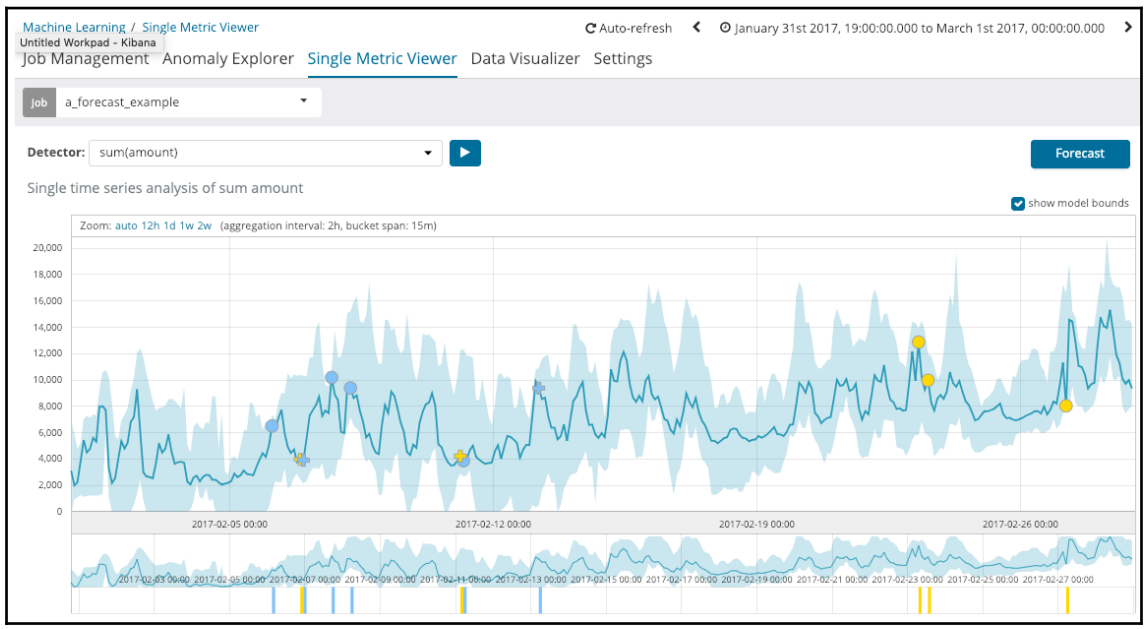

Machine Learning / File Data Visualizer (Experimental)
30 seconds
Job Management
Anomaly Explorer
Single Metric Viewer
Data Visualizer
Settings
Import data
EXPERIMENTAL
Simple
Advanced
Index name
forecast_example
Create index pattern
Reset
File processed
Index created
Data uploaded
Index pattern created
Import complete
Index
forecast_example
Index pattern
forecast_example
Documents ingested
7488
View index in Discover
Create new ML job
Open in Data Visualizer
Index Management
Index Pattern Management


Machine Learning / Job Management / Create New Job / Single Metric Job
January 31st 2017, 19:00:00.000 to March 11th 2017, 18:45:00.000
New job from index pattern forecast_example
Chart interval: 2h
Use full forecast_example data
Aggregation
Sum
Field
#amount
Bucket span
15m
Estimate bucket span
Sparse data
140,000
120,000
100,000
80,000
60,000
40,000
20,000
2017-02-05 00:00
2017-02-12 00:00
2017-02-19 00:00
2017-02-26 00:00
2017-03-05 00:00
Name
a_forecast_example
Description
Job description
Job Groups
Job Group
Advanced
Move to advanced job configuration
Validate Job
Create Job

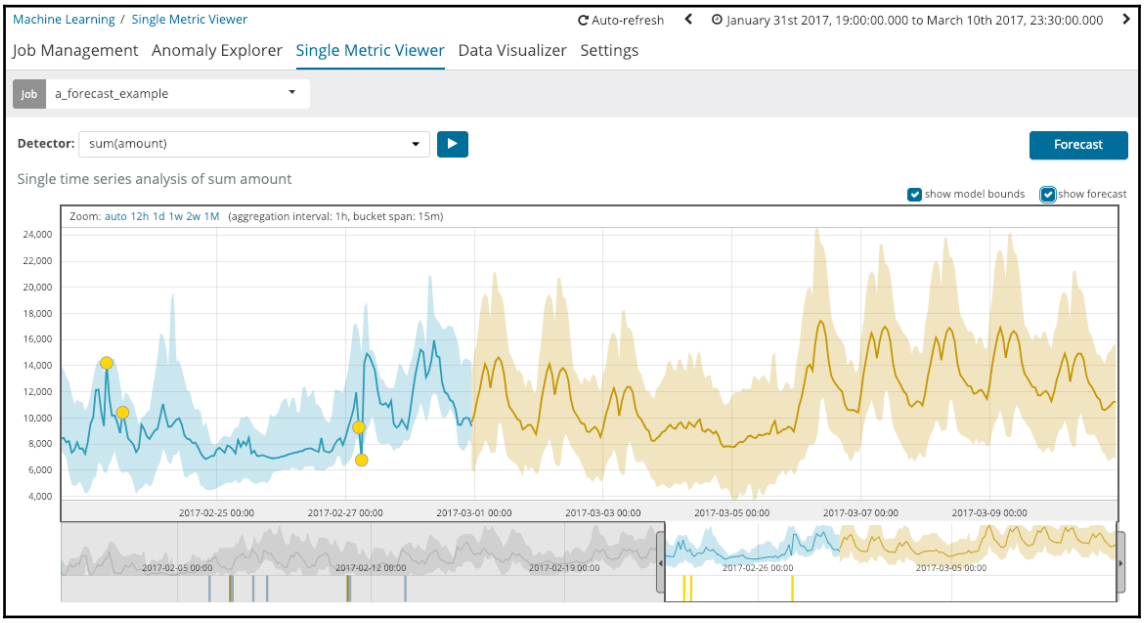

January 31st 2017, 19:00:00.000 to March 1st 2017, 00:00:00.000
Time Range
Quick
Relative
Absolute
Recent
From
Set To Now
2017-01-31 19:00:00.000
YYYY-MM-DD HH:mm:ss.SSS
January 2017
Sun Mon Tue Wed Thu Fri Sat
01 02 03 04 05 06 07
08 09 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
29 30 31
To
Set To Now
2017-03-01 00:00:00.000
YYYY-MM-DD HH:mm:ss.SSS
March 2017
Sun Mon Tue Wed Thu Fri Sat
01 02 03 04
05 06 07 08 09 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28 29 30 31
Go

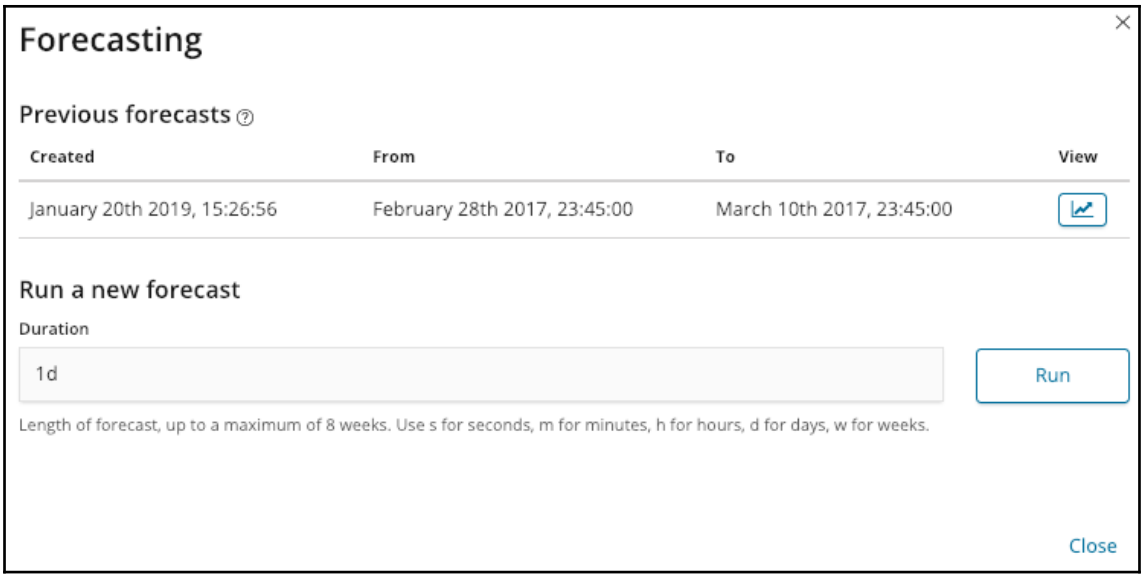

Machine Learning / Job Management / Create New Job / Single Metric Job
January 31st 2017, 19:00:00.000 to March 1st 2017, 00:00:00.000
New job from index pattern forecast_example
Chart interval: 2h
Use full forecast_example data
Aggregation
Sum
Field
#amount
Bucket span
15m
Estimate bucket span
Sparse data
130,000
120,000
110,000
100,000
90,000
80,000
70,000
60,000
50,000
40,000
30,000
20,000
10,000
2017-02-01 00:002017-02-03 00:002017-02-05 00:002017-02-07 00:002017-02-09 00:002017-02-11 00:002017-02-13 00:002017-02-15 00:002017-02-17 00:002017-02-19 00:002017-02-21 00:002017-02-23 00:002017-02-25 00:002017-02-27 00:00
Name
a_forecast_example
Description
Job description
Job Groups
Job Group
Advanced
Move to advanced job configuration
Validate Job
Create Job

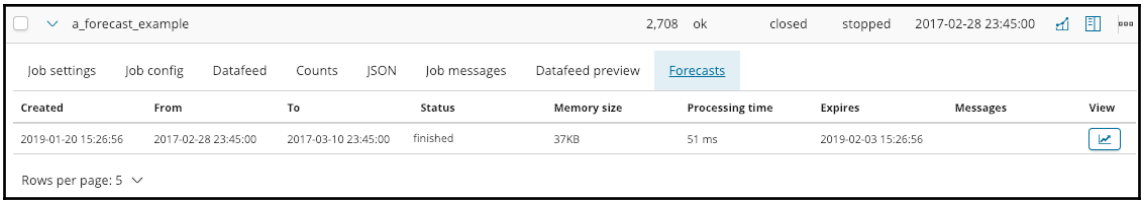

Machine Learning / Job Management / Create New Job / Single Metric Job
January 31st 2017, 19:00:00.000 to March 1st 2017, 00:00:00.000
New job from index pattern forecast_example
Chart interval: 2h
Use full forecast_example data
Aggregation
Sum
Field
#amount
Bucket span
15m
Estimate bucket span
Sparse data
130,000
120,000
110,000
100,000
90,000
80,000
70,000
60,000
50,000
40,000
30,000
20,000
10,000
2017-02-01 00:00 2017-02-03 00:00 2017-02-05 00:00 2017-02-07 00:00 2017-02-09 00:00 2017-02-11 00:00 2017-02-13 00:00 2017-02-15 00:00 2017-02-17 00:00 2017-02-19 00:00 2017-02-21 00:00 2017-02-23 00:00 2017-02-25 00:00 2017-02-27 00:00
Job a_forecast_example created
Reset
View Results
Continue job in real-time

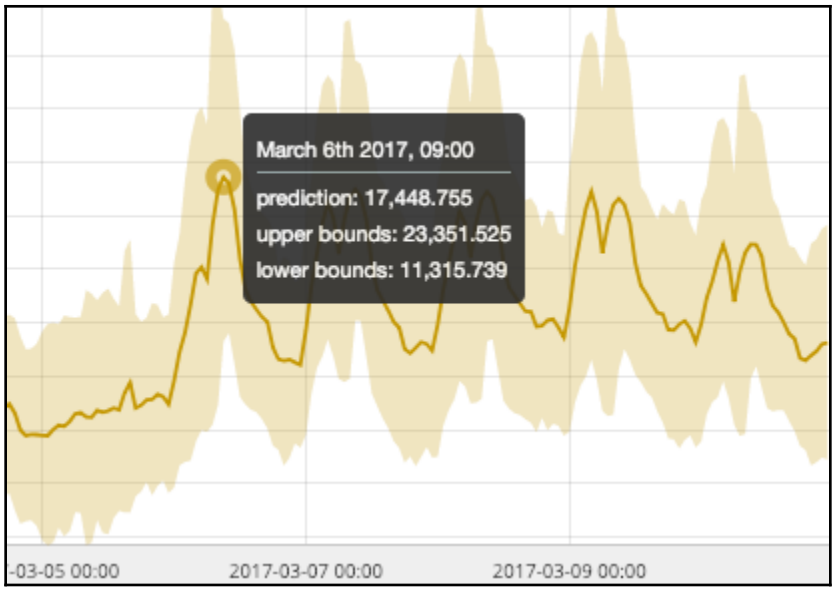

Machine Learning / Single Metric Viewer
Auto-refresh
January 31st 2017, 19:00:00.000 to March 1st 2017, 00:00:00.000
Untitled Workpad - Kibana
Job Management
Anomaly Explorer
Single Metric Viewer
Data Visualizer
Settings
Job
a_forecast_example
Detector:
sum(amount)
Forecast
Single time series analysis of sum amount
show model bounds
Zoom: auto 12h 1d 1w 2w (aggregation interval: 2h, bucket span: 15m)
20,000
18,000
16,000
14,000
12,000
10,000
8,000
6,000
4,000
2,000
0
2017-02-05 00:00
2017-02-12 00:00
2017-02-19 00:00
2017-02-26 00:00

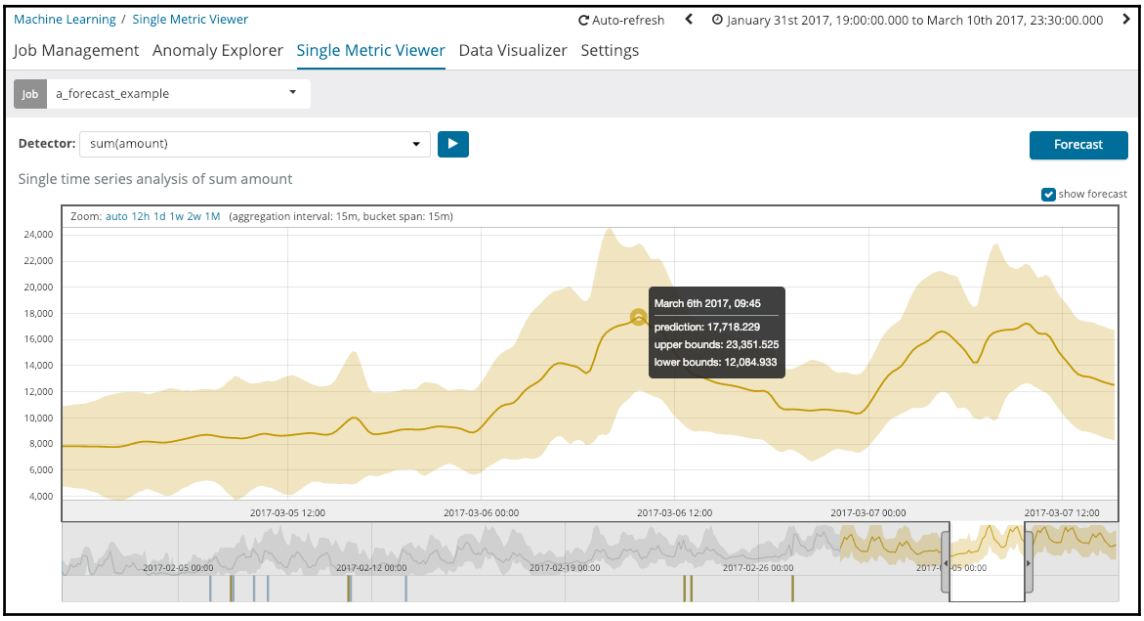

Forecasting
Run a new forecast
Duration
10d
Run
Length of forecast, up to a maximum of 8 weeks. Use s for seconds, m for minutes, h for hours, d for days, w for weeks.
Close

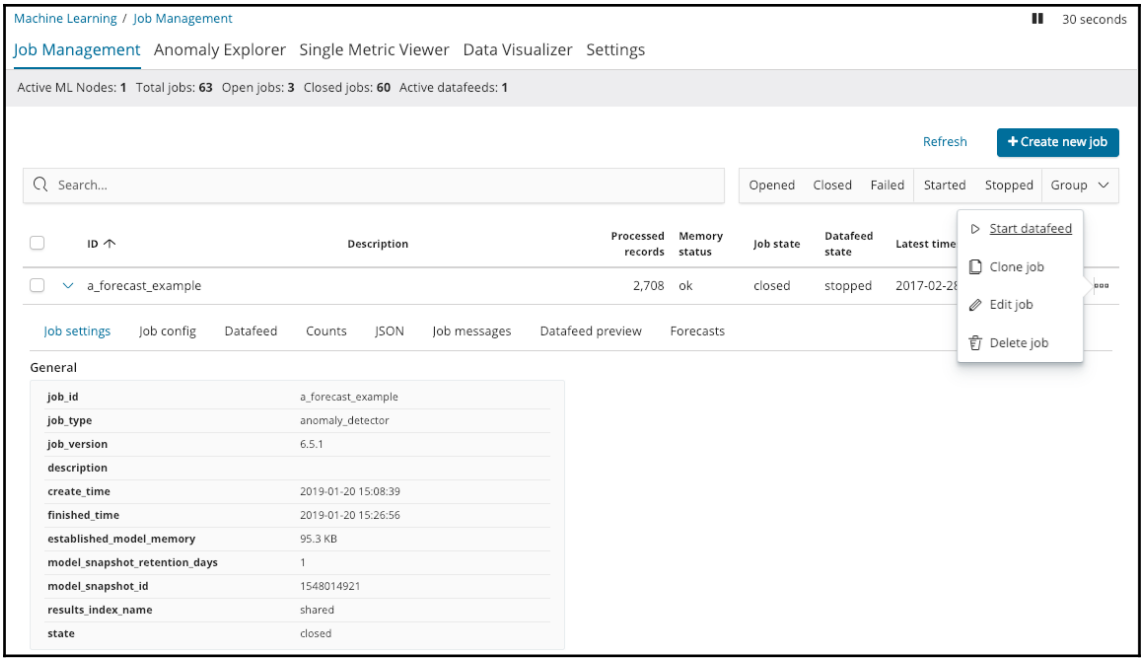

Machine Learning / Single Metric Viewer
Auto-refresh
January 31st 2017, 19:00:00.000 to March 10th 2017, 23:30:00.000
Job Management
Anomaly Explorer
Single Metric Viewer
Data Visualizer
Settings
Job
a_forecast_example
Detector:
sum(amount)
Forecast
Single time series analysis of sum amount
show model bounds
show forecast
Zoom: auto 12h 1d 1w 2w 1M (aggregation interval: 1h, bucket span: 15m)
24,000
22,000
20,000
18,000
16,000
14,000
12,000
10,000
8,000
6,000
4,000
2017-02-25 00:00
2017-02-27 00:00
2017-03-01 00:00
2017-03-03 00:00
2017-03-05 00:00
2017-03-07 00:00
2017-03-09 00:00
2017-02-05 00:00
2017-02-12 00:00
2017-02-19 00:00
2017-02-26 00:00
2017-03-05 00:00

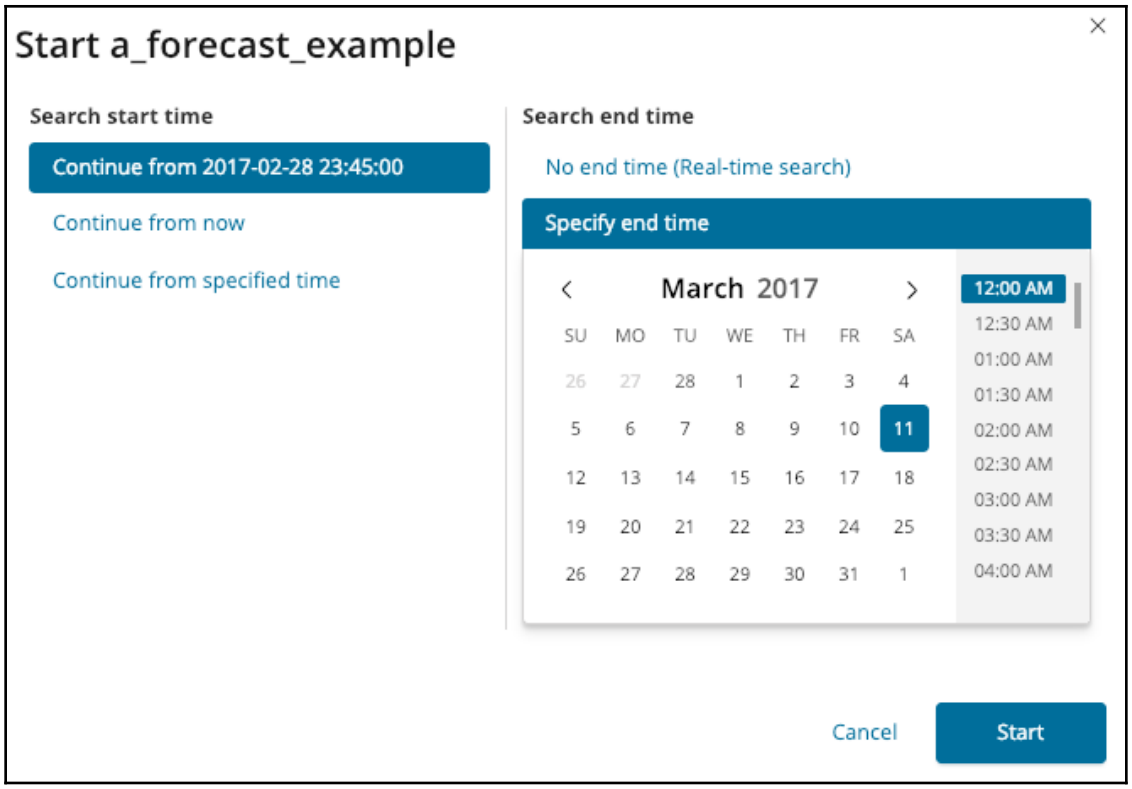

Forecasting
Previous forecasts
Created
From
To
View
January 20th 2019, 15:26:56
February 28th 2017, 23:45:00
March 10th 2017, 23:45:00
Run a new forecast
Duration
1d
Run
Length of forecast, up to a maximum of 8 weeks. Use s for seconds, m for minutes, h for hours, d for days, w for weeks.
Close

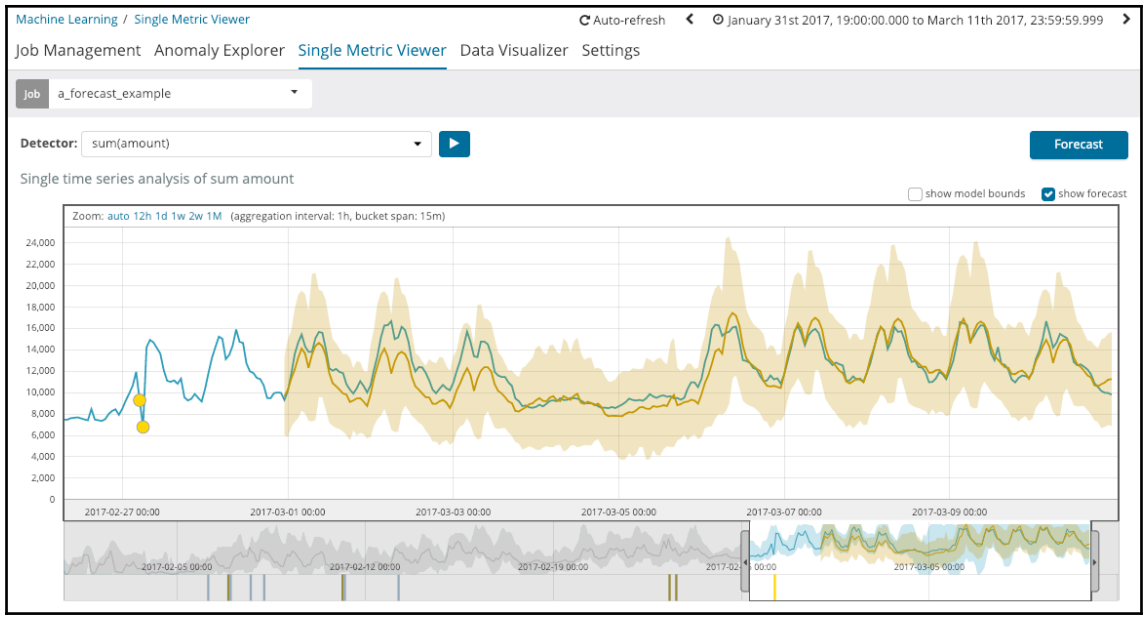

a_forecast_example
2,708
ok
closed
stopped
2017-02-28 23:45:00
Job settings
Job config
Datafeed
Counts
JSON
Job messages
Datafeed preview
Forecasts
Created
From
To
Status
Memory size
Processing time
Expires
Messages
View
2019-01-20 15:26:56
2017-02-28 23:45:00
2017-03-10 23:45:00
finished
37KB
51 ms
2019-02-03 15:26:56
Rows per page: 5

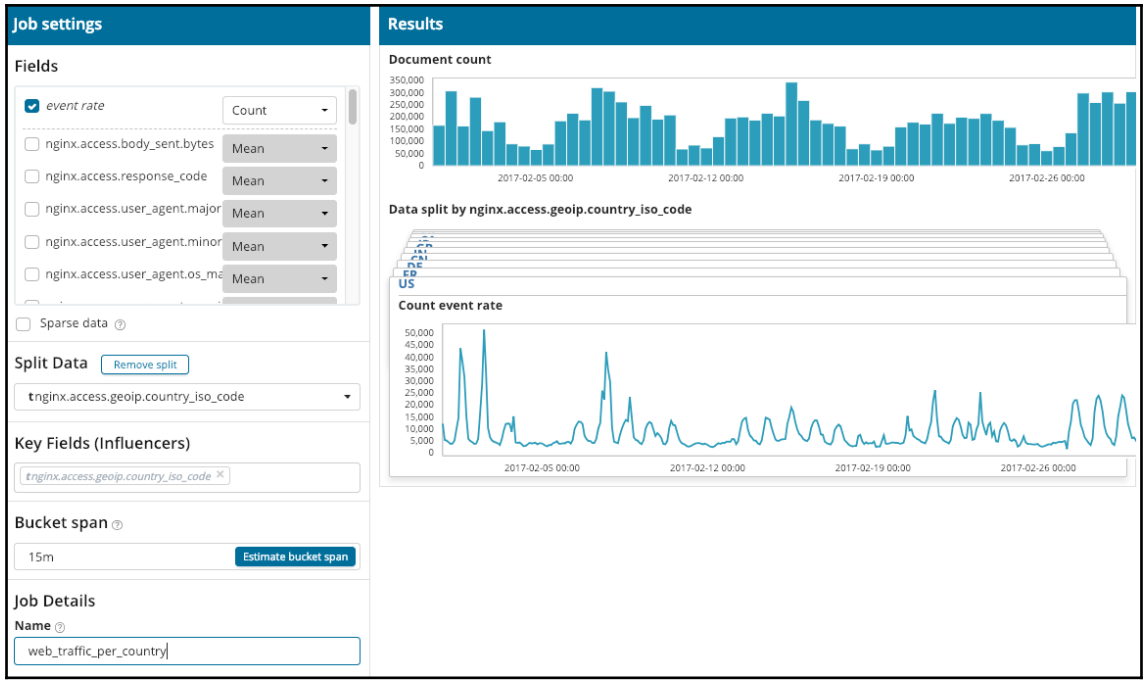

March 6th 2017, 09:00
prediction: 17,448.755
upper bounds: 23,351.525
lower bounds: 11,315.739
-03-05 00:00
2017-03-07 00:00
2017-03-09 00:00

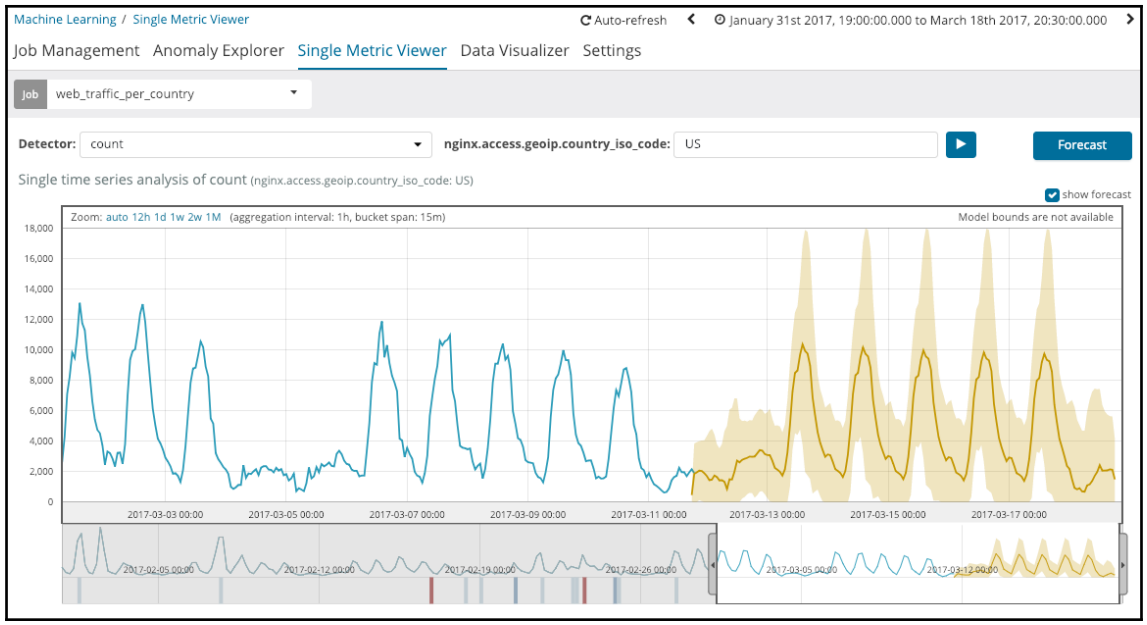

Machine Learning / Single Metric Viewer
Auto-refresh
January 31st 2017, 19:00:00.000 to March 10th 2017, 23:30:00.000
Job Management
Anomaly Explorer
Single Metric Viewer
Data Visualizer
Settings
Job
a_forecast_example
Detector:
sum(amount)
Forecast
Single time series analysis of sum amount
show forecast
Zoom: auto 12h 1d 1w 2w 1M (aggregation interval: 15m, bucket span: 15m)
24,000
22,000
20,000
18,000
16,000
14,000
12,000
10,000
8,000
6,000
4,000
March 6th 2017, 09:45
prediction: 17,718.229
upper bounds: 23,351.525
lower bounds: 12,084.933
2017-03-05 12:00
2017-03-06 00:00
2017-03-06 12:00
2017-03-07 00:00
2017-03-07 12:00
2017-02-05 00:00
2017-02-12 00:00
2017-02-19 00:00
2017-02-26 00:00

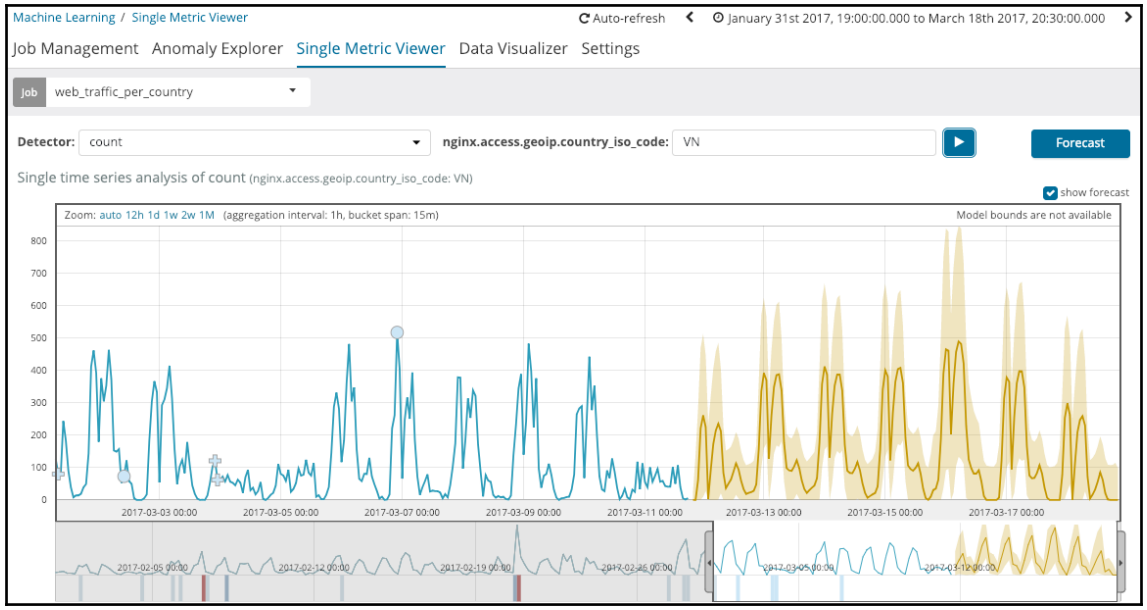

Machine Learning / Job Management
30 seconds
Job Management
Anomaly Explorer
Single Metric Viewer
Data Visualizer
Settings
Active ML Nodes: 1 Total jobs: 63 Open jobs: 3 Closed jobs: 60 Active datafeeds: 1
Refresh
+ Create new job
Search...
Opened
Closed
Failed
Started
Stopped
Group
ID
Description
Processed records
Memory status
Job state
Datafeed state
Latest time
a_forecast_example
2,708
ok
closed
stopped
Start datafeed
Clone job
Edit job
Delete job
Job settings
Job config
Datafeed
Counts
JSON
Job messages
Datafeed preview
Forecasts
General
job_id
a_forecast_example
job_type
anomaly_detector
job_version
6.5.1
description
create_time
2019-01-20 15:08:39
finished_time
2019-01-20 15:26:56
established_model_memory
95.3 KB
model_snapshot_retention_days
1
model_snapshot_id
1548014921
results_index_name
shared
state
closed


Start a_forecast_example
Search start time
Continue from 2017-02-28 23:45:00
Continue from now
Continue from specified time
Search end time
No end time (Real-time search)
Specify end time
March 2017
SU MO TU WE TH FR SA
26 27 28 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
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
Cancel
Start

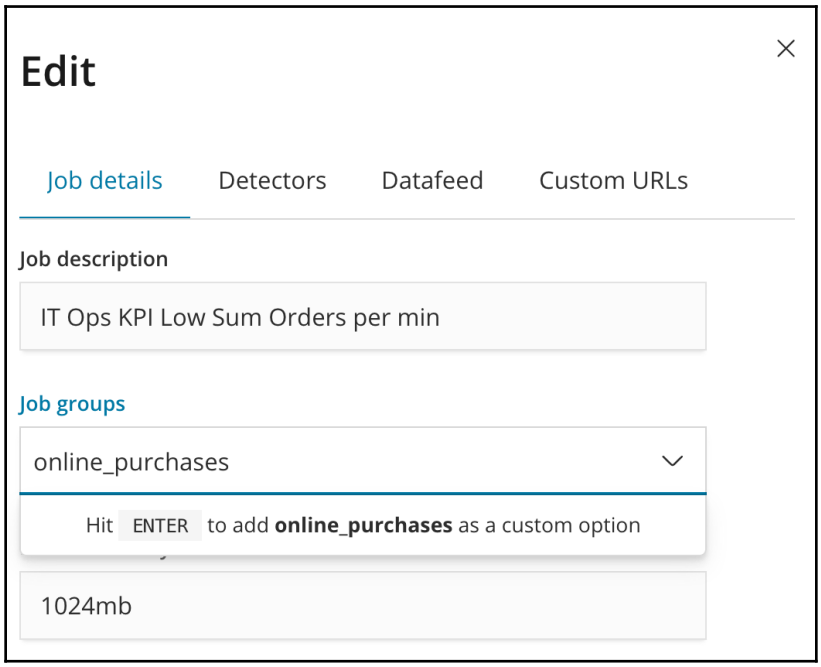

Machine Learning / Single Metric Viewer
Auto-refresh
January 31st 2017, 19:00:00.000 to March 11th 2017, 23:59:59.999
Job Management
Anomaly Explorer
Single Metric Viewer
Data Visualizer
Settings
Job
a_forecast_example
Detector:
sum(amount)
Forecast
Single time series analysis of sum amount
show model bounds
show forecast
Zoom: auto 12h 1d 1w 2w 1M (aggregation interval: 1h, bucket span: 15m)
24,000
22,000
20,000
18,000
16,000
14,000
12,000
10,000
8,000
6,000
4,000
2,000
0
2017-02-27 00:00
2017-03-01 00:00
2017-03-03 00:00
2017-03-05 00:00
2017-03-07 00:00
2017-03-09 00:00
2017-02-05 00:00
2017-02-12 00:00
2017-02-19 00:00
2017-03-05 00:00

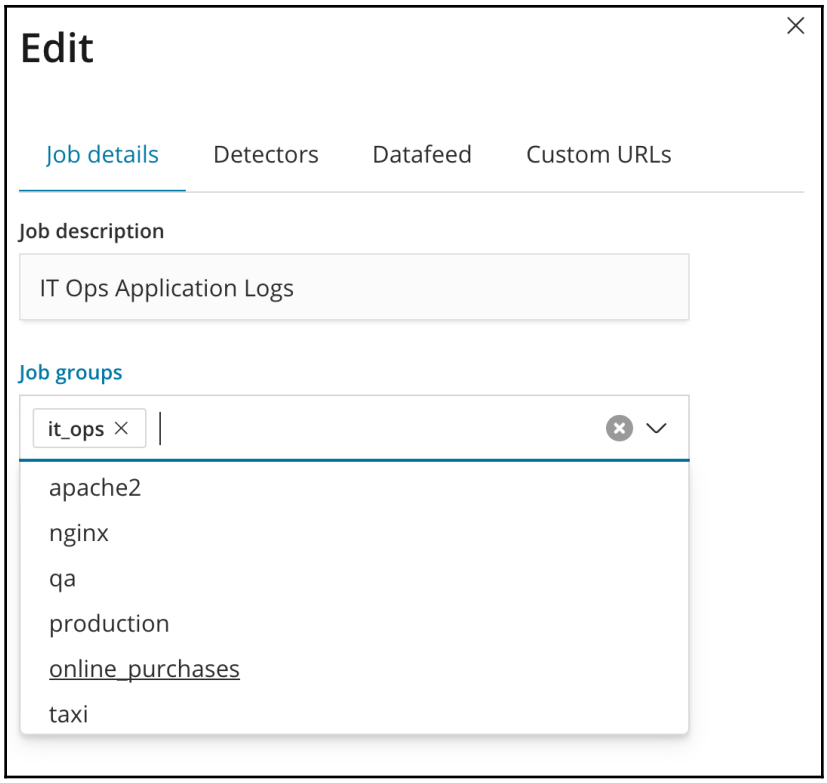

Job settings
Fields
event rate
Count
nginx.access.body_sent.bytes
Mean
nginx.access.response_code
Mean
nginx.access.user_agent.major
Mean
nginx.access.user_agent.minor
Mean
nginx.access.user_agent.os_ma
Mean
Sparse data
Split Data
Remove split
tnginx.access.geoip.country_iso_code
Key Fields (Influencers)
tnginx.access.geoip.country_iso_code
Bucket span
15m
Estimate bucket span
Job Details
Name
web_traffic_per_country
Results
Document count
350,000
300,000
250,000
200,000
150,000
100,000
50,000
0
2017-02-05 00:00
2017-02-12 00:00
2017-02-19 00:00
2017-02-26 00:00
Data split by nginx.access.geoip.country_iso_code
US
Count event rate
50,000
45,000
40,000
35,000
30,000
25,000
20,000
15,000
10,000
5,000
0
2017-02-05 00:00
2017-02-12 00:00
2017-02-19 00:00
2017-02-26 00:00

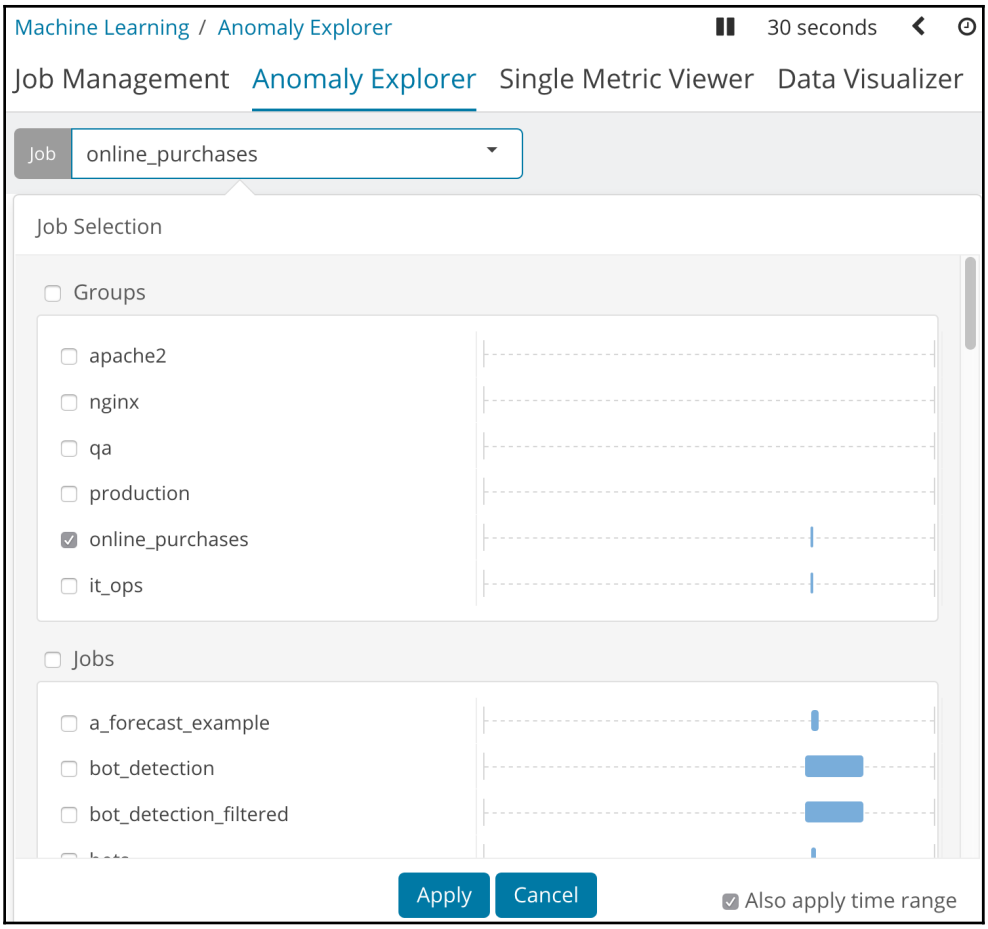

Machine Learning / Single Metric Viewer
Auto-refresh
January 31st 2017, 19:00:00.000 to March 18th 2017, 20:30:00.000
Job Management
Anomaly Explorer
Single Metric Viewer
Data Visualizer
Settings
Job
web_traffic_per_country
Detector:
count
nginx.access.geoip.country_iso_code:
US
Forecast
Single time series analysis of count (nginx.access.geoip.country_iso_code: US)
show forecast
Zoom: auto 12h 1d 1w 2w 1M (aggregation interval: 1h, bucket span: 15m)
Model bounds are not available
18,000
16,000
14,000
12,000
10,000
8,000
6,000
4,000
2,000
0
2017-03-03 00:00
2017-03-05 00:00
2017-03-07 00:00
2017-03-09 00:00
2017-03-11 00:00
2017-03-13 00:00
2017-03-15 00:00
2017-03-17 00:00
2017-02-05 00:00
2017-02-12 00:00
2017-02-19 00:00
2017-02-26 00:00
2017-03-05 00:00
2017-03-12 00:00

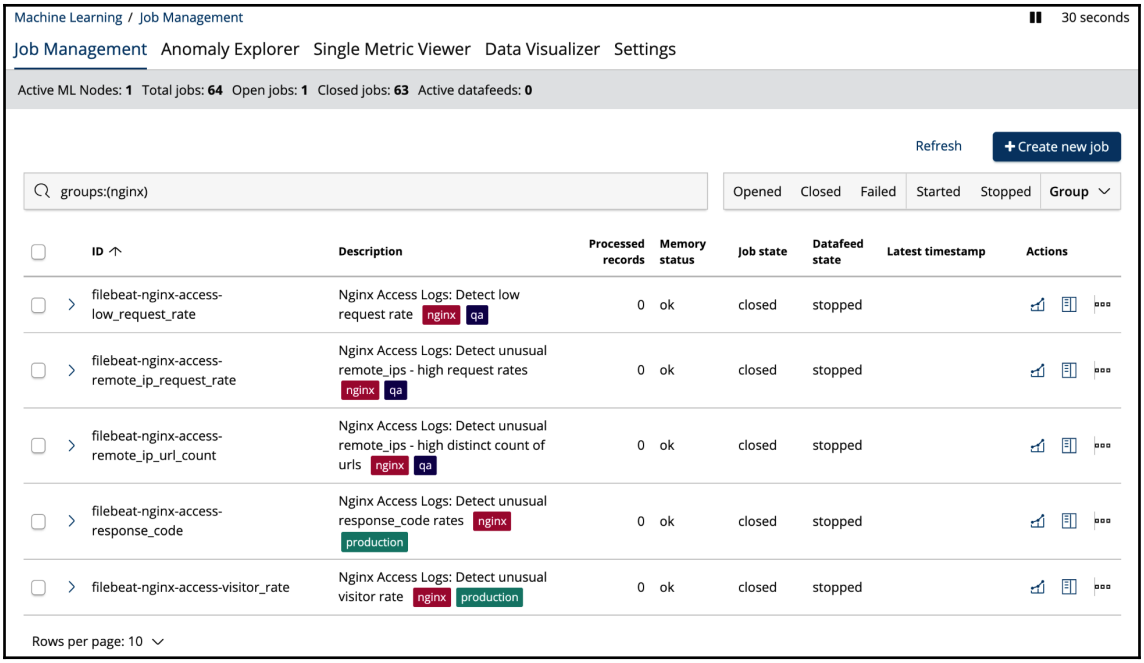

Machine Learning / Single Metric Viewer
Auto-refresh
January 31st 2017, 19:00:00.000 to March 18th 2017, 20:30:00.000
Job Management
Anomaly Explorer
Single Metric Viewer
Data Visualizer
Settings
Job
web_traffic_per_country
Detector:
count
nginx.access.geoip.country_iso_code:
VN
Forecast
Single time series analysis of count (nginx.access.geoip.country_iso_code: VN)
show forecast
Zoom: auto 12h 1d 1w 2w 1M (aggregation interval: 1h, bucket span: 15m)
Model bounds are not available
800
700
600
500
400
300
200
100
0
2017-03-03 00:00
2017-03-05 00:00
2017-03-07 00:00
2017-03-09 00:00
2017-03-11 00:00
2017-03-13 00:00
2017-03-15 00:00
2017-03-17 00:00
2017-02-05 00:00
2017-02-12 00:00
2017-02-19 00:00
2017-02-26 00:00
2017-03-05 00:00
2017-03-12 00:00

Chapter 10: ML Tips and Tricks



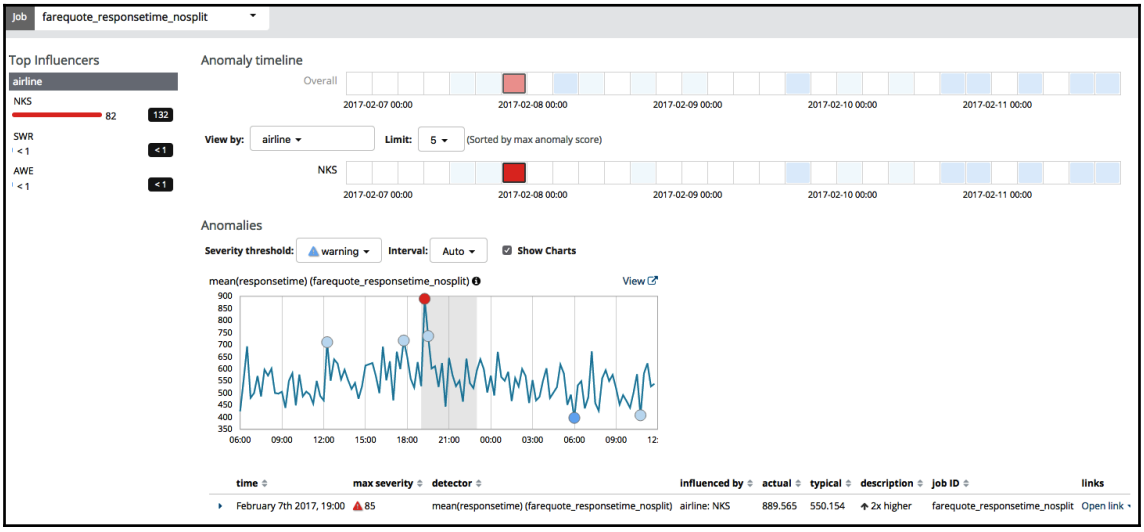

Edit
Job details
Detectors
Datafeed
Custom URLs
Job description
IT Ops Application Logs
Job groups
it_ops
apache2
nginx
qa
production
online_purchases
taxi

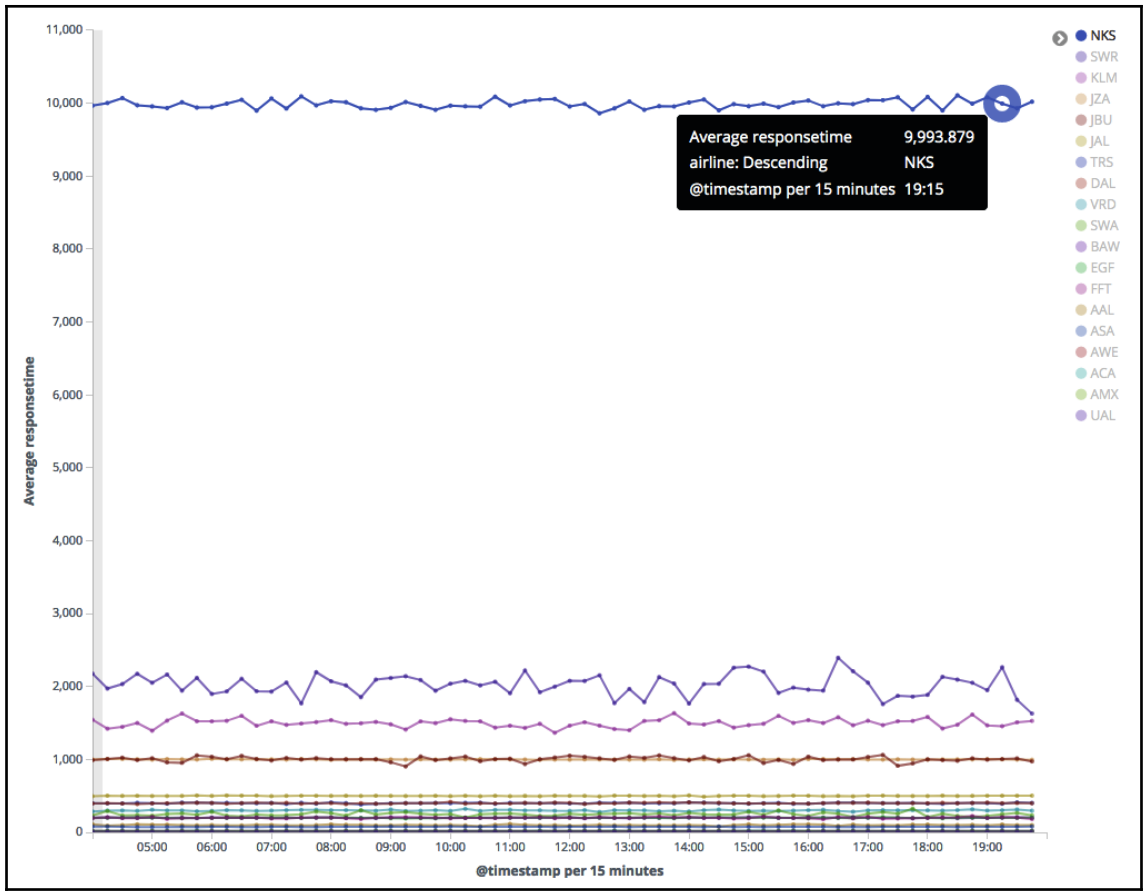

Machine Learning / Anomaly Explorer
30 seconds
Job Management
Anomaly Explorer
Single Metric Viewer
Data Visualizer
Job
online_purchases
Job Selection
Groups
apache2
nginx
qa
production
online_purchases
it_ops
Jobs
a_forecast_example
bot_detection
bot_detection_filtered
Apply
Cancel
Also apply time range

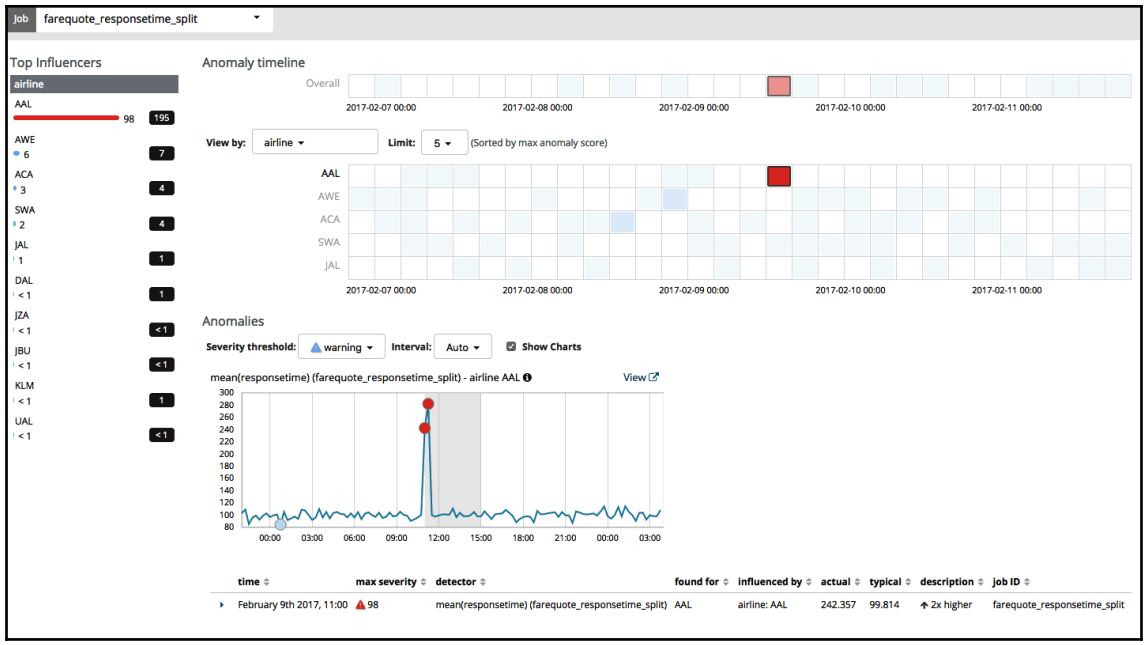

Machine Learning / Job Management
30 seconds
Job Management
Anomaly Explorer
Single Metric Viewer
Data Visualizer
Settings
Active ML Nodes: 1 Total jobs: 64 Open jobs: 1 Closed jobs: 63 Active datafeeds: 0
Refresh
+ Create new job
groups:(nginx)
Opened
Closed
Failed
Started
Stopped
Group
ID
Description
Processed records
Memory status
Job state
Datafeed state
Latest timestamp
Actions
filebeat-nginx-access-low_request_rate
Nginx Access Logs: Detect low request rate nginx qa
0 ok closed stopped
filebeat-nginx-access-remote_ip_request_rate
Nginx Access Logs: Detect unusual remote_ips - high request rates nginx qa
0 ok closed stopped
filebeat-nginx-access-remote_ip_url_count
Nginx Access Logs: Detect unusual remote_ips - high distinct count of urls nginx qa
0 ok closed stopped
filebeat-nginx-access-response_code
Nginx Access Logs: Detect unusual response_code rates nginx production
0 ok closed stopped
filebeat-nginx-access-visitor_rate
Nginx Access Logs: Detect unusual visitor rate nginx production
0 ok closed stopped
Rows per page: 10

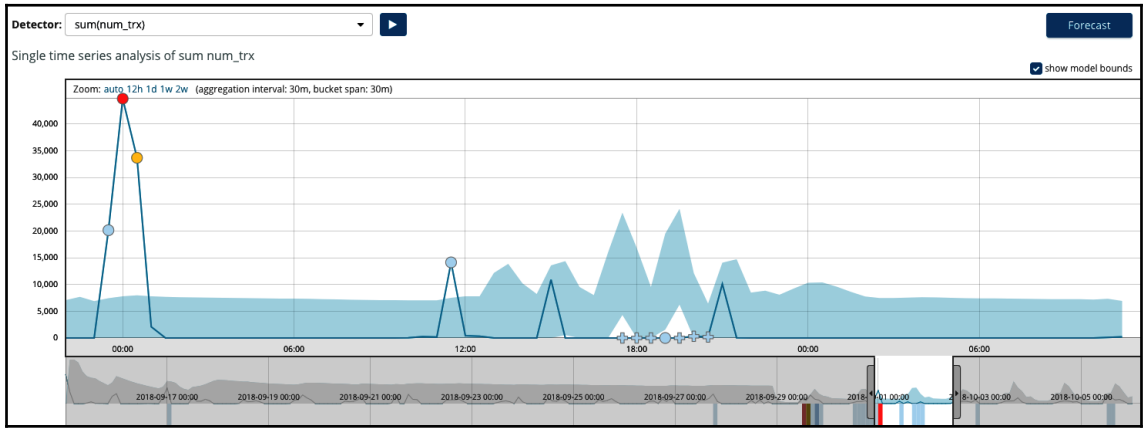

Job
farequote_count_nosplit
Top Influencers
airline
AAL 97
UAL < 1
AWE < 1
AMX < 1
Anomaly timeline
Overall
2017-02-07 00:00
2017-02-08 00:00
2017-02-09 00:00
2017-02-10 00:00
2017-02-11 00:00
View by: airline
Limit: 10
(Sorted by max anomaly score)
AAL
Anomalies
Severity threshold: warning
Interval: Auto
Show Charts
count (farequote_count_nosplit)
View
300
280
260
240
220
200
180
160
140
00:00
03:00
06:00
09:00
12:00
15:00
18:00
21:00
00:00
03:00
time
max severity
detector
influenced by
actual
typical
description
job ID
links
February 9th 2017, 11:00
90
count (farequote_count_nosplit)
airline: AAL
295
180.8
2x higher
farequote_count_nosplit
Open link

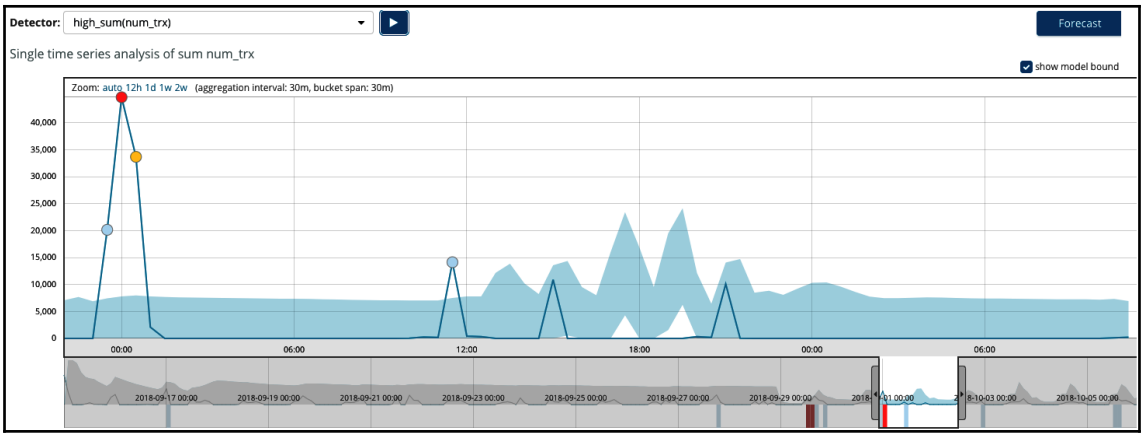

Job
farequote_count_split
Top Influencers
airline
AAL
98
188
ACA
5
5
UAL
1
1
SWA
1
3
KLM
< 1
< 1
NKS
< 1
< 1
EGF
< 1
< 1
JZA
< 1
< 1
AMX
< 1
< 1
VRD
< 1
< 1
Anomaly timeline
Overall
2017-02-07 00:00
2017-02-08 00:00
2017-02-09 00:00
2017-02-10 00:00
2017-02-11 00:00
View by:
airline
Limit:
5
(Sorted by max anomaly score)
AAL
ACA
UAL
SWA
KLM
Anomalies
Severity threshold:
warning
Interval:
Auto
Show Charts
count (farequote_count_split) - airline AAL
View
time
max severity
detector
found for
influenced by
actual
typical
description
job ID
links
February 9th 2017, 11:00
98
count (farequote_count_split)
AAL
airline: AAL
136
17.9
8x higher
farequote_count_split
Open link

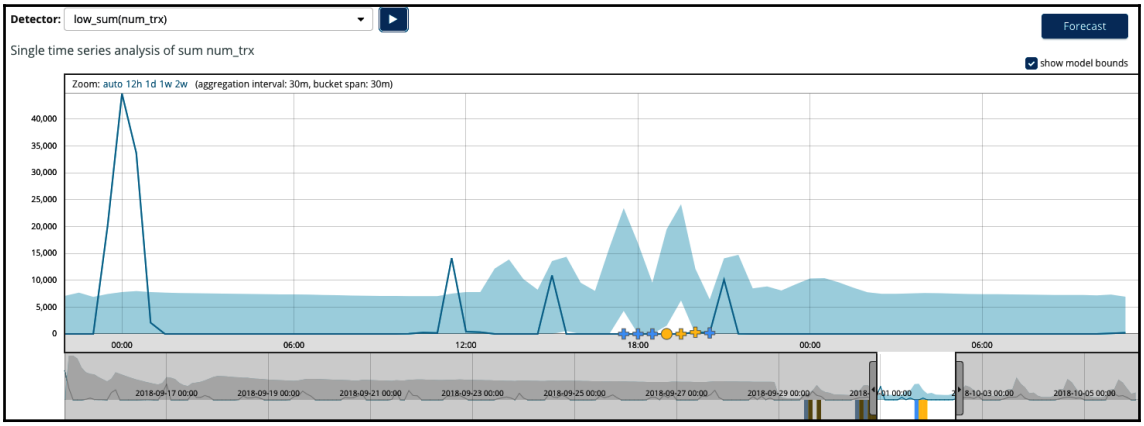

Job
farequote_responsetime_nosplit
Top Influencers
airline
NKS
82
132
SWR
< 1
< 1
AWE
< 1
< 1
Anomaly timeline
Overall
2017-02-07 00:00
2017-02-08 00:00
2017-02-09 00:00
2017-02-10 00:00
2017-02-11 00:00
View by:
airline
Limit:
5
(Sorted by max anomaly score)
NKS
Anomalies
Severity threshold:
warning
Interval:
Auto
Show Charts
mean(responsetime) (farequote_responsetime_nosplit)
View
time
max severity
detector
influenced by
actual
typical
description
job ID
links
February 7th 2017, 19:00
85
mean(responsetime) (farequote_responsetime_nosplit)
airline: NKS
889.565
550.154
2x higher
farequote_responsetime_nosplit
Open link

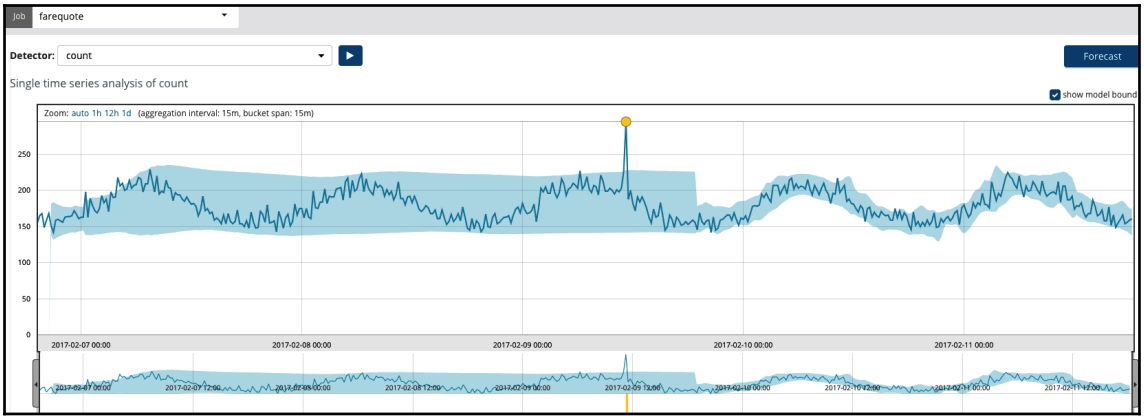

11,000
10,000
9,000
8,000
7,000
6,000
5,000
4,000
3,000
2,000
1,000
0
Average responsetime
05:00
06:00
07:00
08:00
09:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
17:00
18:00
19:00
@timestamp per 15 minutes
Average responsetime 9,993.879
airline: Descending NKS
@timestamp per 15 minutes 19:15
NKS
SWR
KLM
JZA
JBU
JAL
TRS
DAL
VRD
SWA
BAW
EGF
FFT
AAL
ASA
AWE
ACA
AMX
UAL

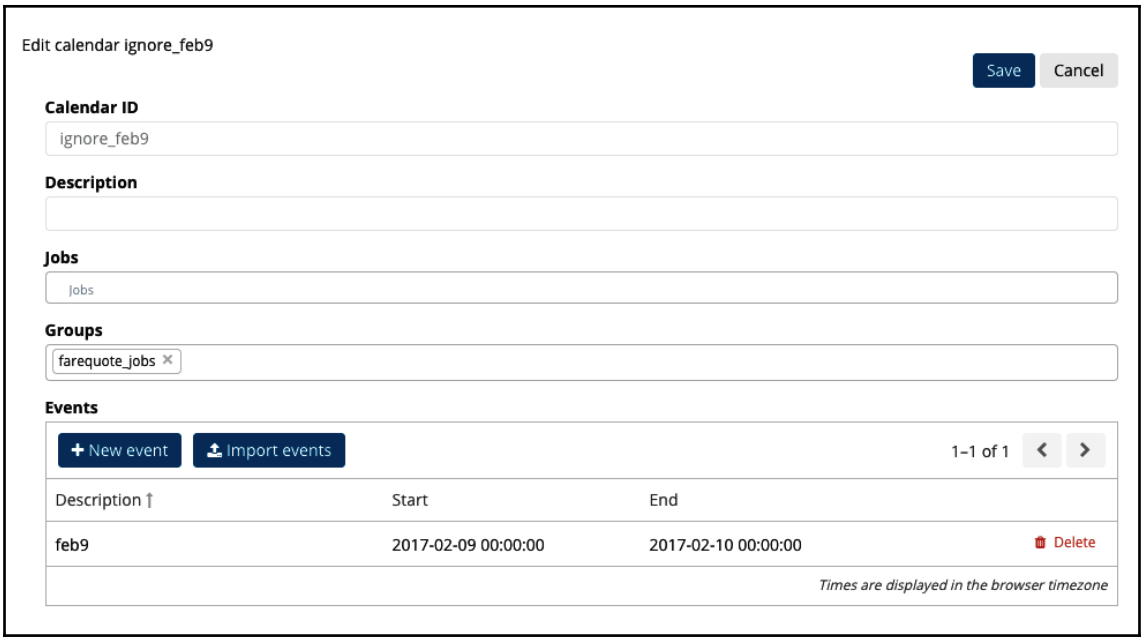

Job
farequote_responsetime_split
Top Influencers
airline
AAL
98
195
AWE
6
7
ACA
3
4
SWA
2
4
JAL
1
1
DAL
< 1
1
JZA
< 1
< 1
JBU
< 1
< 1
KLM
< 1
1
UAL
< 1
< 1
Anomaly timeline
Overall
2017-02-07 00:00
2017-02-08 00:00
2017-02-09 00:00
2017-02-10 00:00
2017-02-11 00:00
View by:
airline
Limit:
5
(Sorted by max anomaly score)
AAL
AWE
ACA
SWA
JAL
Anomalies
Severity threshold:
warning
Interval:
Auto
Show Charts
mean(responsetime) (farequote_responsetime_split) - airline AAL
View
time
max severity
detector
found for
influenced by
actual
typical
description
job ID
February 9th 2017, 11:00
98
mean(responsetime) (farequote_responsetime_split)
AAL
airline: AAL
242.357
99.814
2x higher
farequote_responsetime_split

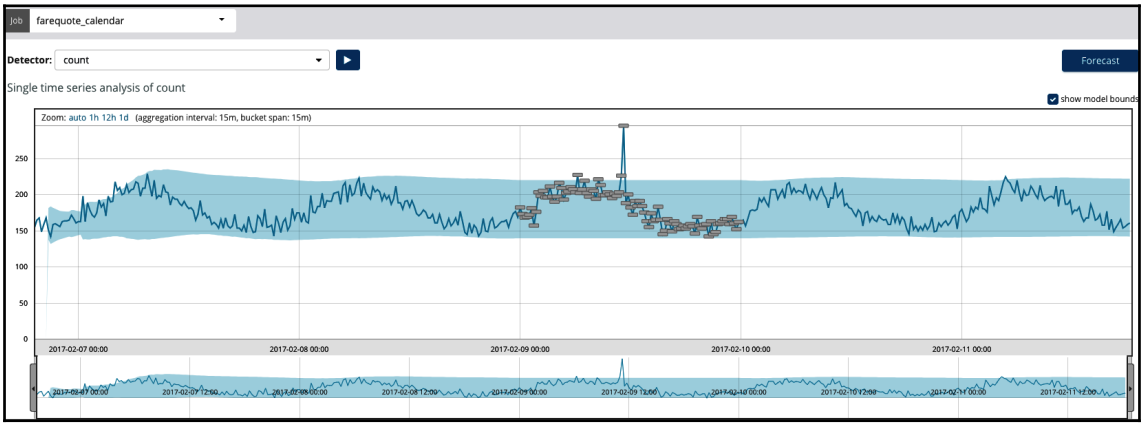

Detector:
sum(num_trx)
Forecast
Single time series analysis of sum num_trx
show model bounds
Zoom: auto 12h 1d 1w 2w
(aggregation interval: 30m, bucket span: 30m)
40,000
35,000
30,000
25,000
20,000
15,000
10,000
5,000
0
00:00
06:00
12:00
18:00
00:00
06:00

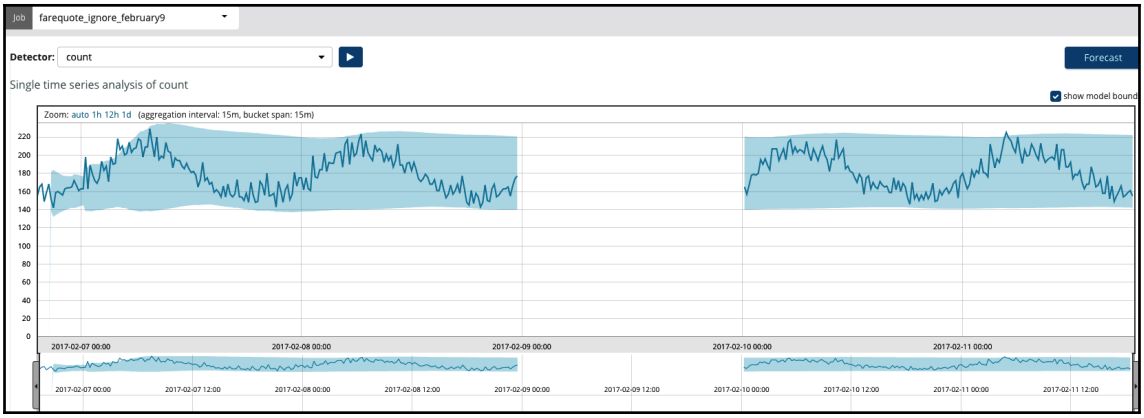

Detector: high_sum(num_trx)
Forecast
Single time series analysis of sum num_trx
show model bound
Zoom: auto 12h 1d 1w 2w (aggregation interval: 30m, bucket span: 30m)
40,000
35,000
30,000
25,000
20,000
15,000
10,000
5,000
0
00:00
06:00
12:00
18:00
00:00
06:00
2018-09-17 00:00
2018-09-19 00:00
2018-09-21 00:00
2018-09-23 00:00
2018-09-25 00:00
2018-09-27 00:00
2018-09-29 00:00
2018-10-03 00:00
2018-10-05 00:00

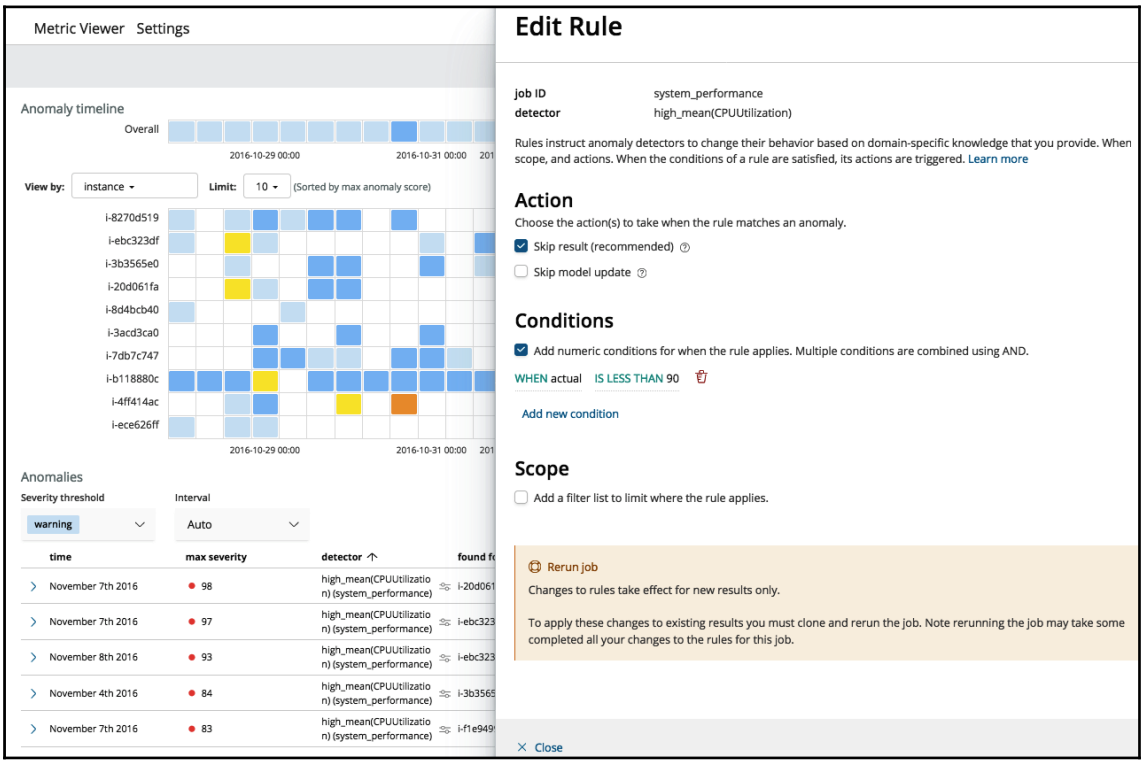

Detector: low_sum(num_trx)
Forecast
Single time series analysis of sum num_trx
show model bounds
Zoom: auto 12h 1d 1w 2w (aggregation interval: 30m, bucket span: 30m)
40,000
35,000
30,000
25,000
20,000
15,000
10,000
5,000
0
00:00
06:00
12:00
18:00
00:00
06:00
2018-09-17 00:00
2018-09-19 00:00
2018-09-21 00:00
2018-09-23 00:00
2018-09-25 00:00
2018-09-27 00:00
2018-09-29 00:00
2018-10-03 00:00
2018-10-05 00:00


Job farequote
Detector: count
Forecast
Single time series analysis of count
show model bound
Zoom: auto 1h 12h 1d (aggregation interval: 15m, bucket span: 15m)
250
200
150
100
50
0
2017-02-07 00:00
2017-02-08 00:00
2017-02-09 00:00
2017-02-10 00:00
2017-02-11 00:00


Edit calendar ignore_feb9
Save
Cancel
Calendar ID
ignore_feb9
Description
Jobs
Jobs
Groups
farequote_jobs
Events
New event
Import events
1–1 of 1
Description
Start
End
feb9
2017-02-09 00:00:00
2017-02-10 00:00:00
Delete
Times are displayed in the browser timezone


Job
farequote_calendar
Detector:
count
Forecast
Single time series analysis of count
show model bounds
Zoom: auto 1h 12h 1d (aggregation interval: 15m, bucket span: 15m)
250
200
150
100
50
0
2017-02-07 00:00
2017-02-08 00:00
2017-02-09 00:00
2017-02-10 00:00
2017-02-11 00:00


Job
farequote_ignore_february9
Detector:
count
Forecast
Single time series analysis of count
show model bound
Zoom: auto 1h 12h 1d (aggregation interval: 15m, bucket span: 15m)
220
200
180
160
140
120
100
80
60
40
20
0
2017-02-07 00:00
2017-02-08 00:00
2017-02-09 00:00
2017-02-10 00:00
2017-02-11 00:00
2017-02-07 12:00
2017-02-08 12:00
2017-02-09 12:00
2017-02-10 12:00
2017-02-11 12:00


Metric Viewer
Settings
Anomaly timeline
Overall
2016-10-29 00:00
2016-10-31 00:00
View by:
instance
Limit:
10
(Sorted by max anomaly score)
i-8270d519
i-ebc323df
i-3b3565e0
i-20d061fa
i-8d4bcb40
i-3acd3ca0
i-7db7c747
i-b118880c
i-4ff414ac
i-ece626ff
Anomalies
Severity threshold
warning
Interval
Auto
time
max severity
detector
November 7th 2016
98
high_mean(CPUUtilization) (system_performance)
November 7th 2016
97
high_mean(CPUUtilization) (system_performance)
November 8th 2016
93
high_mean(CPUUtilization) (system_performance)
November 4th 2016
84
high_mean(CPUUtilization) (system_performance)
November 7th 2016
83
high_mean(CPUUtilization) (system_performance)
Edit Rule
job ID
system_performance
detector
high_mean(CPUUtilization)
Rules instruct anomaly detectors to change their behavior based on domain-specific knowledge that you provide. When scope, and actions. When the conditions of a rule are satisfied, its actions are triggered. Learn more
Action
Choose the action(s) to take when the rule matches an anomaly.
Skip result (recommended)
Skip model update
Conditions
Add numeric conditions for when the rule applies. Multiple conditions are combined using AND.
WHEN actual IS LESS THAN 90
Add new condition
Scope
Add a filter list to limit where the rule applies.
Rerun job
Changes to rules take effect for new results only.
To apply these changes to existing results you must clone and rerun the job. Note rerunning the job may take some completed all your changes to the rules for this job.
Close