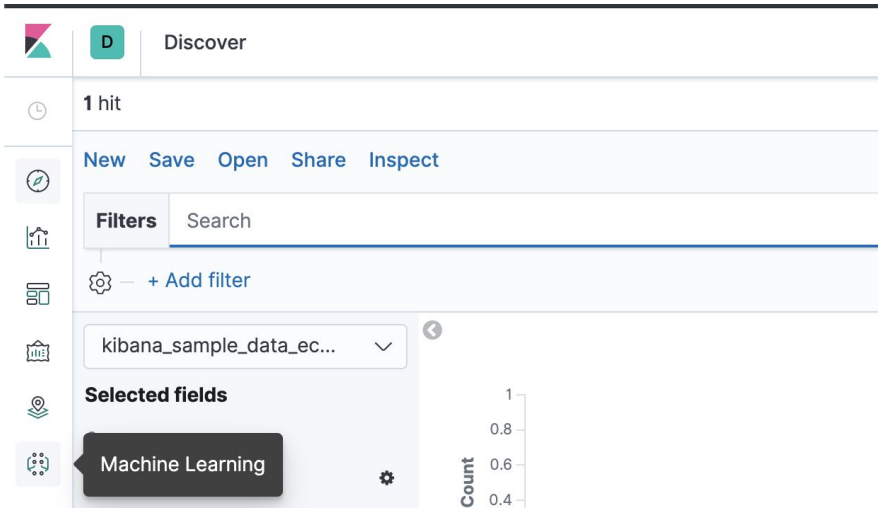
Elastic SIEM Workshop

Lab 3 - Detect Anomalies using ML

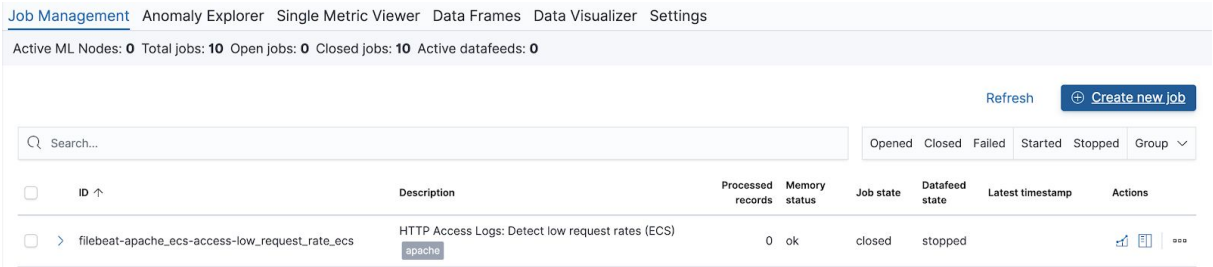
HTTP Access Logs: Detect unusual status code rates

In this lab we are going to create an Elastic ML job to detect unusual status code rates in NGIX logs, leveraging the the 'Sample Web Logs Dataset'.

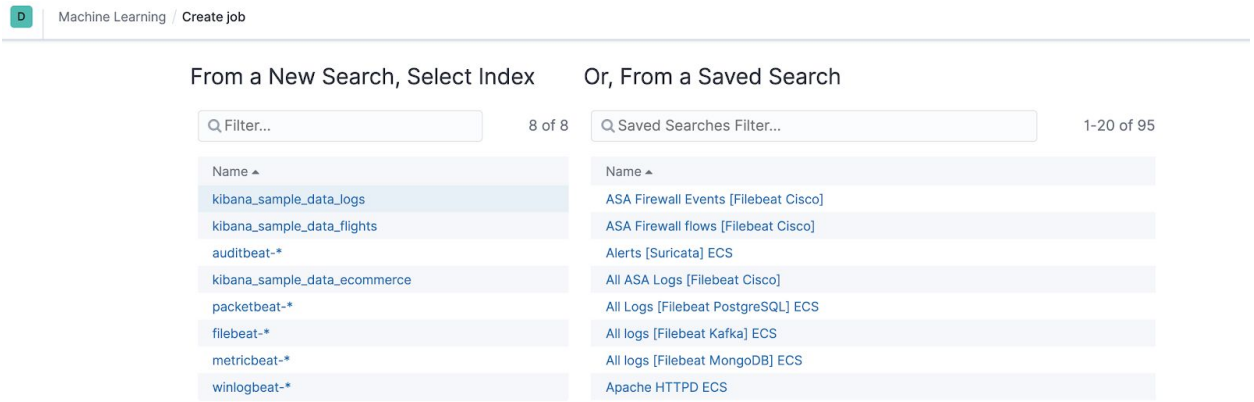
1. Open the Machine Learning App



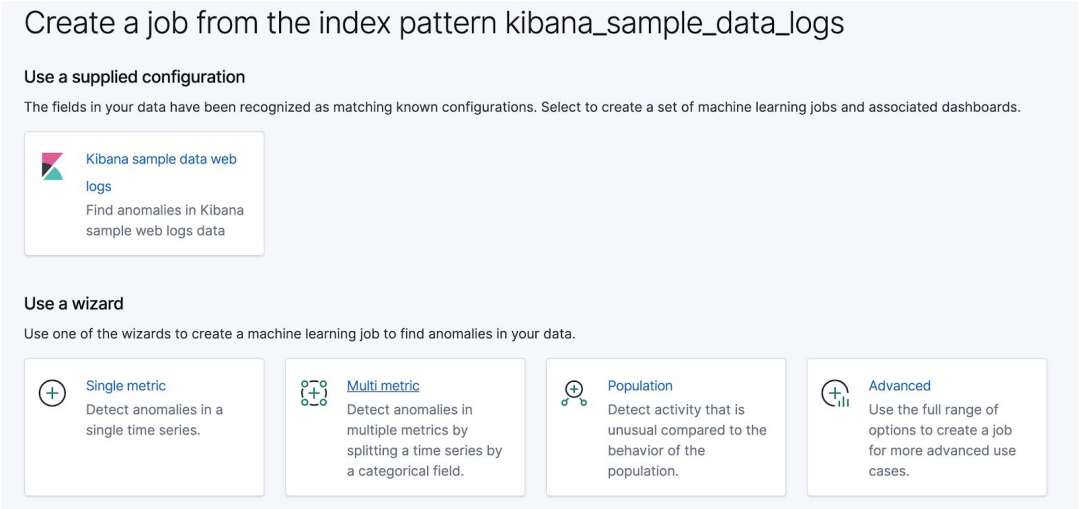
2. Click on the "Create New Job" button.



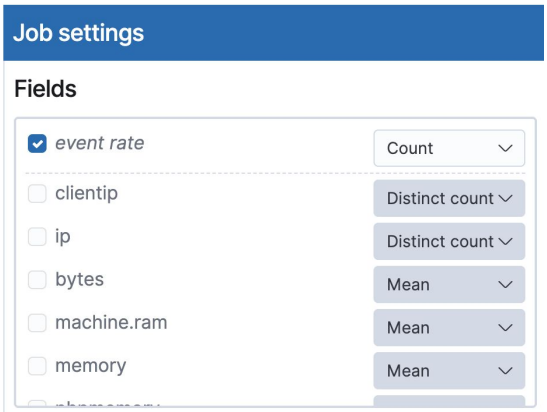
3. Select “kibana_sample_data_logs” as the dataset that the ML job you are creating will use to build the model.



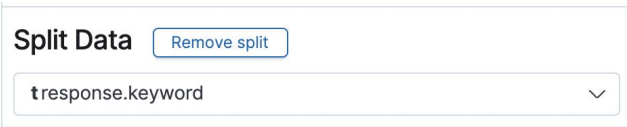
4. Select the “Multi Metric” wizard



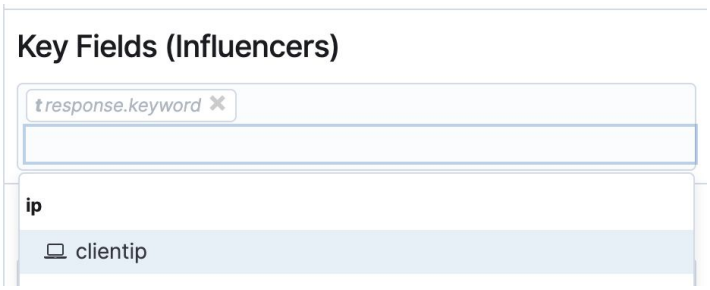
5. Select “Count” as the aggregation for “event rate”



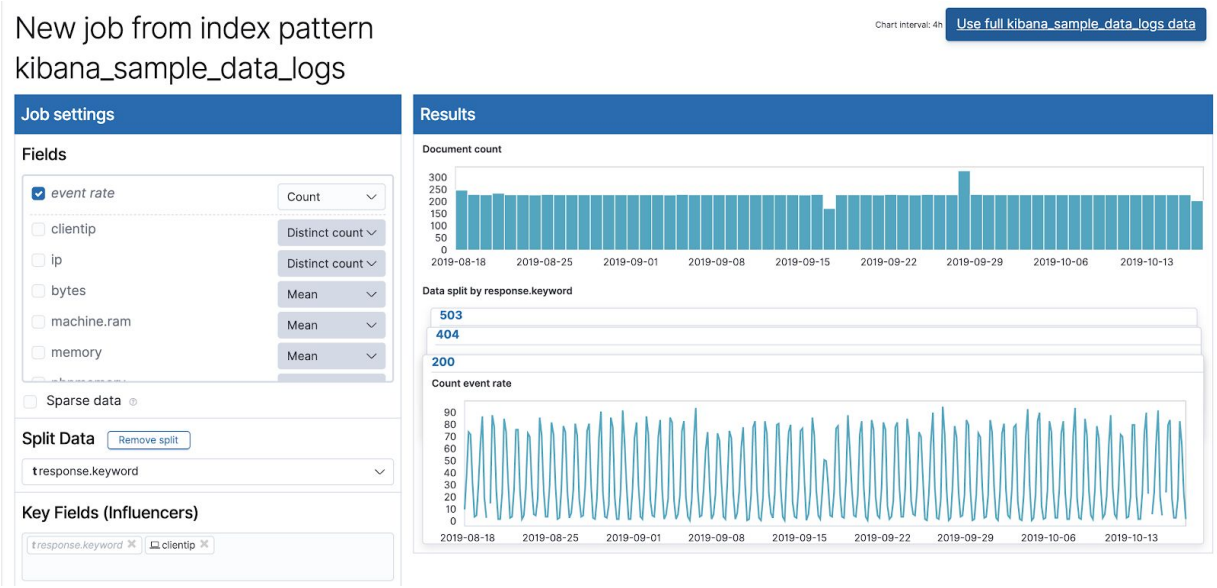
5. Split Data as “response.keyword”



6. Add “client ip” as a *Key Field (influencers)*

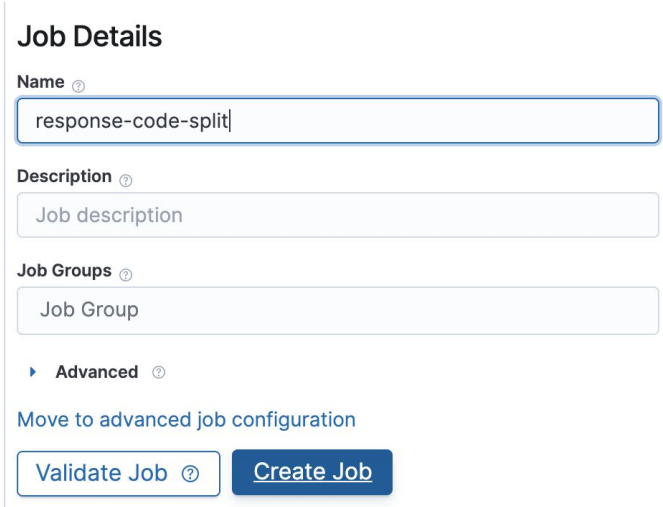


7. Click on “Use full kibana_sample_data_logs_data” button on the top right.

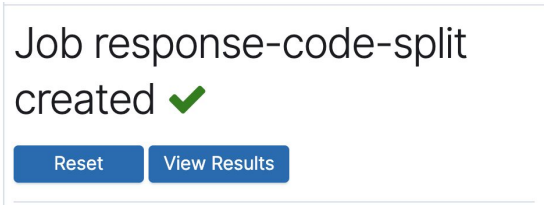


8. Use 60m as the “Bucket Span”

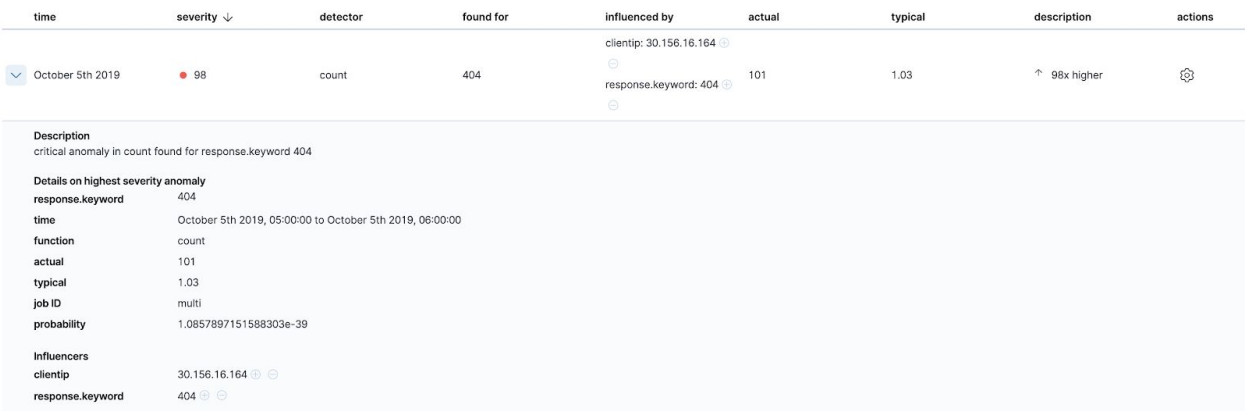
9. Name your ML job (e.g., “response-code-split) and click on the “Create Job” button.



10. Once the job is created, click on “View Results” to open the “Anomaly Explorer” view.



11. From the “Anomaly Explorer” look at the anomaly with highest severity, related to a client ip with a high rate of 404 requests. What’s the client ip in question?



time	severity	detector	found for	influenced by	actual	typical	description	actions
October 5th 2019	98	count	404	clientip: 30.156.16.164 response.keyword: 404	101	1.03	98x higher	

Description
critical anomaly in count found for response.keyword 404

Details on highest severity anomaly

response.keyword	404
time	October 5th 2019, 05:00:00 to October 5th 2019, 06:00:00
function	count
actual	101
typical	1.03
job ID	multi
probability	1.0857897151588303e-39

Influencers

clientip	30.156.16.164
response.keyword	404