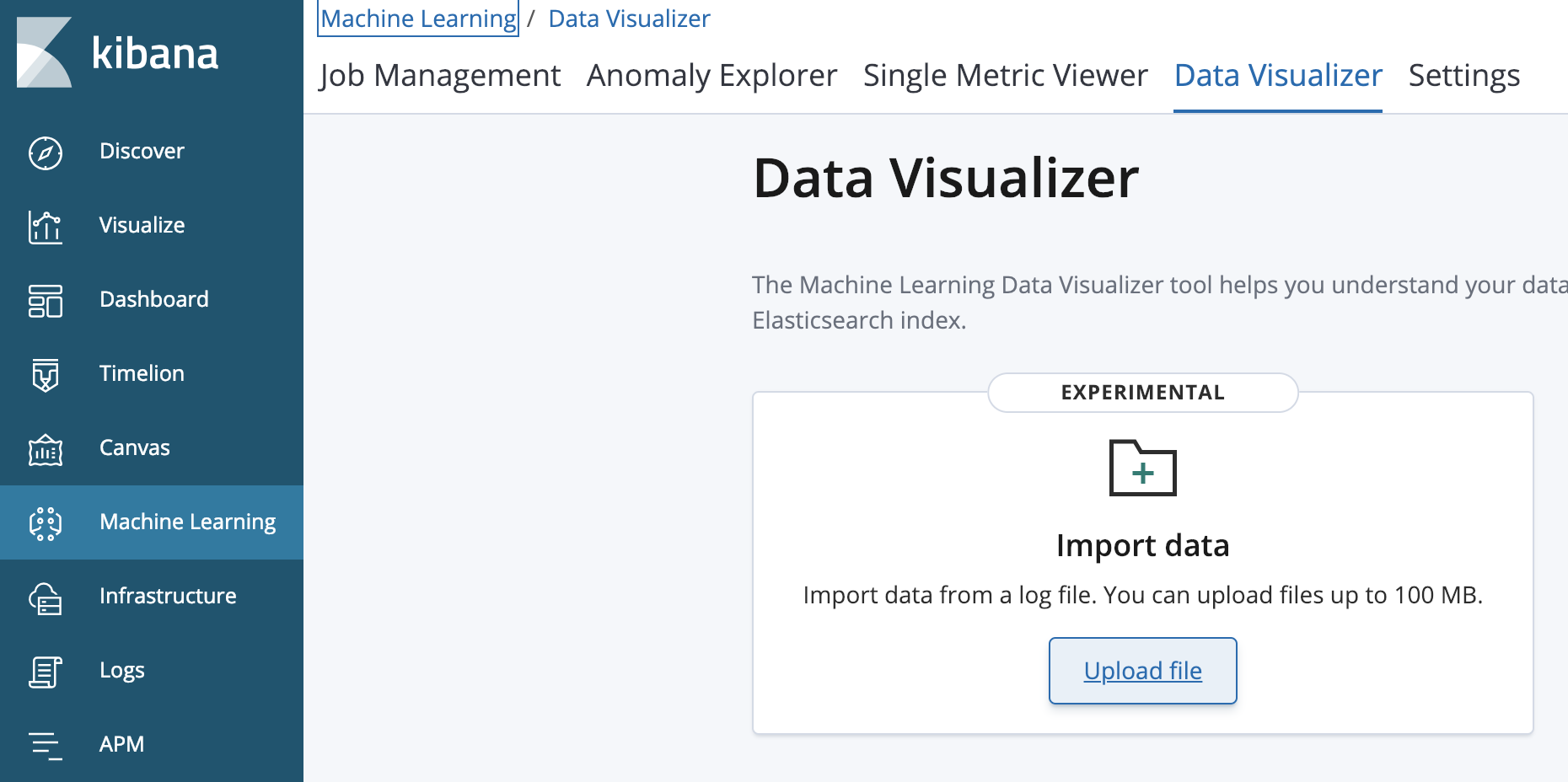
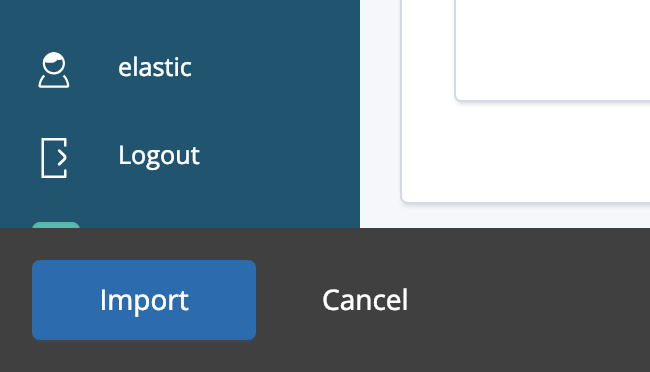
# Lab 4

## Load the “it\_ops\*” data

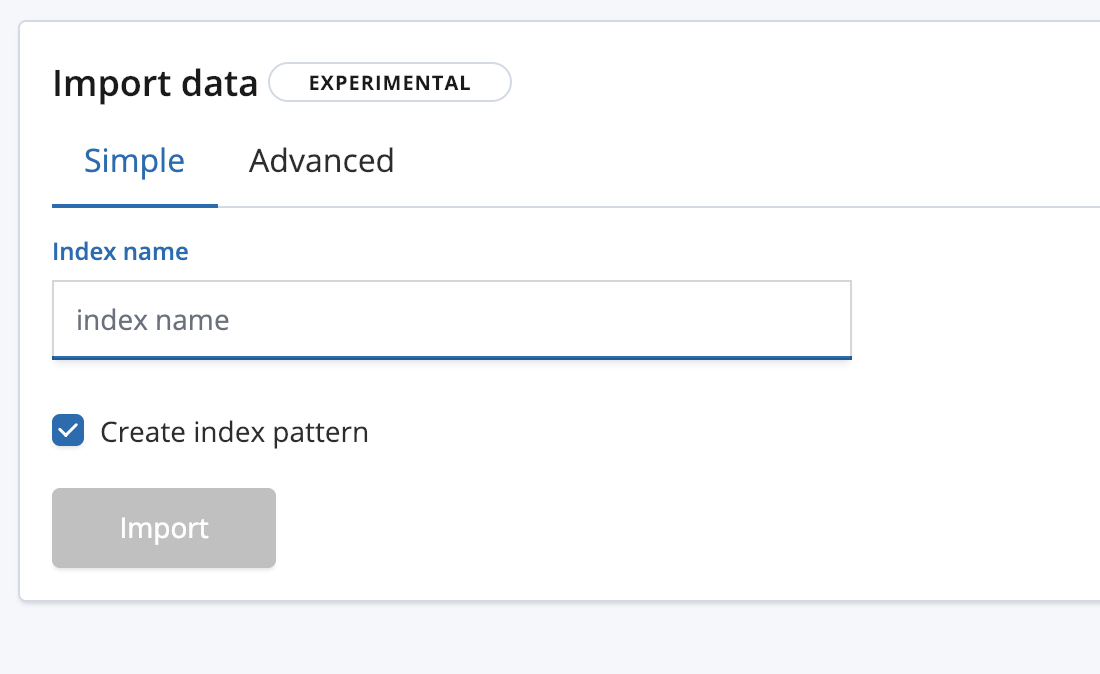
1. From Machine Learning tab, select Data visualiser -> Import Data and load the “it\_ops\_app\_logs.json” file



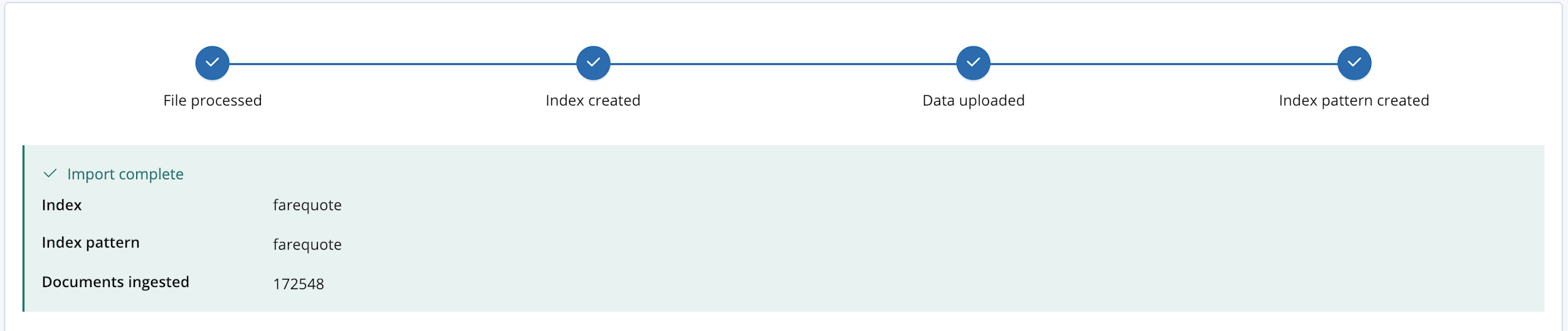
2. Cllick Import



3. Enter the index name “it\_ops\_app\_logs”



4. Wait for the Upload to finish.



5. Repeat the above steps to create the following indices:

* It\_ops\_sql from it\_ops\_sql.json
* It\_ops\_network from it\_ops\_network.json
* It\_ops\_kpi from it\_ops\_kpi.json

## Problem

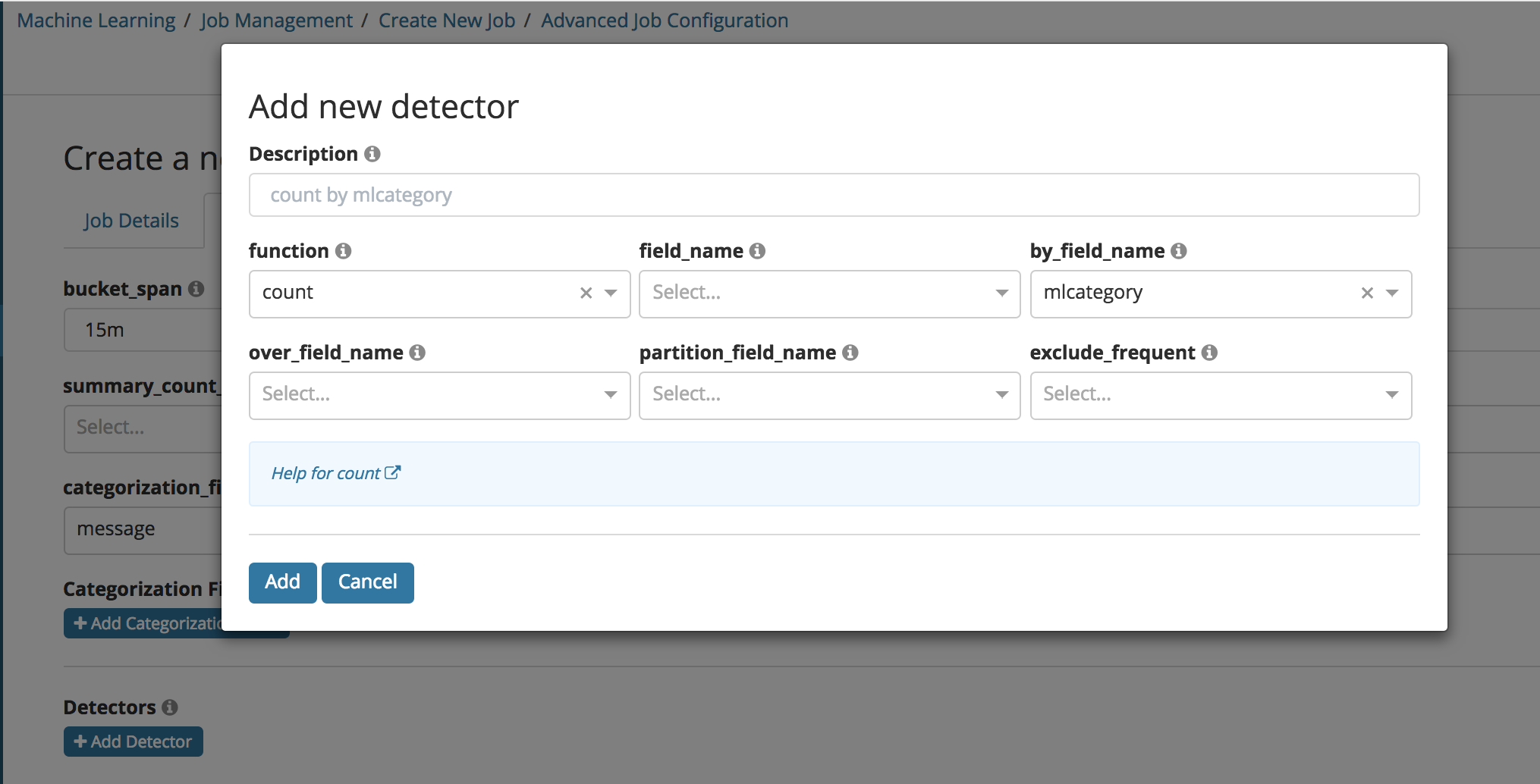
* Transaction processing app records # transactions per minute in an index called “it\_ops\_kpi”. Find the anomaly in it.
* Also, SQL Database and Network performance metrics were gathered for the application environment (it\_ops\_network and it\_ops\_sql). Use multi-metric jobs to see what might be going on in there.
* Lastly, there’s an index (it\_ops\_app\_logs) that has the application’s log lines in them. See if there’s anything anomalous in there as well.  
  View all jobs correlated together in the Anomaly Explorer

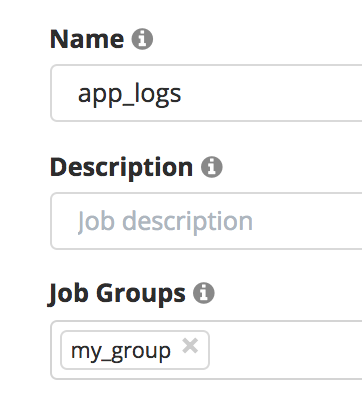
# Solution

## Create and Advanced job for “it\_ops\_app\_logs” index

For index:it\_ops\_app\_logs

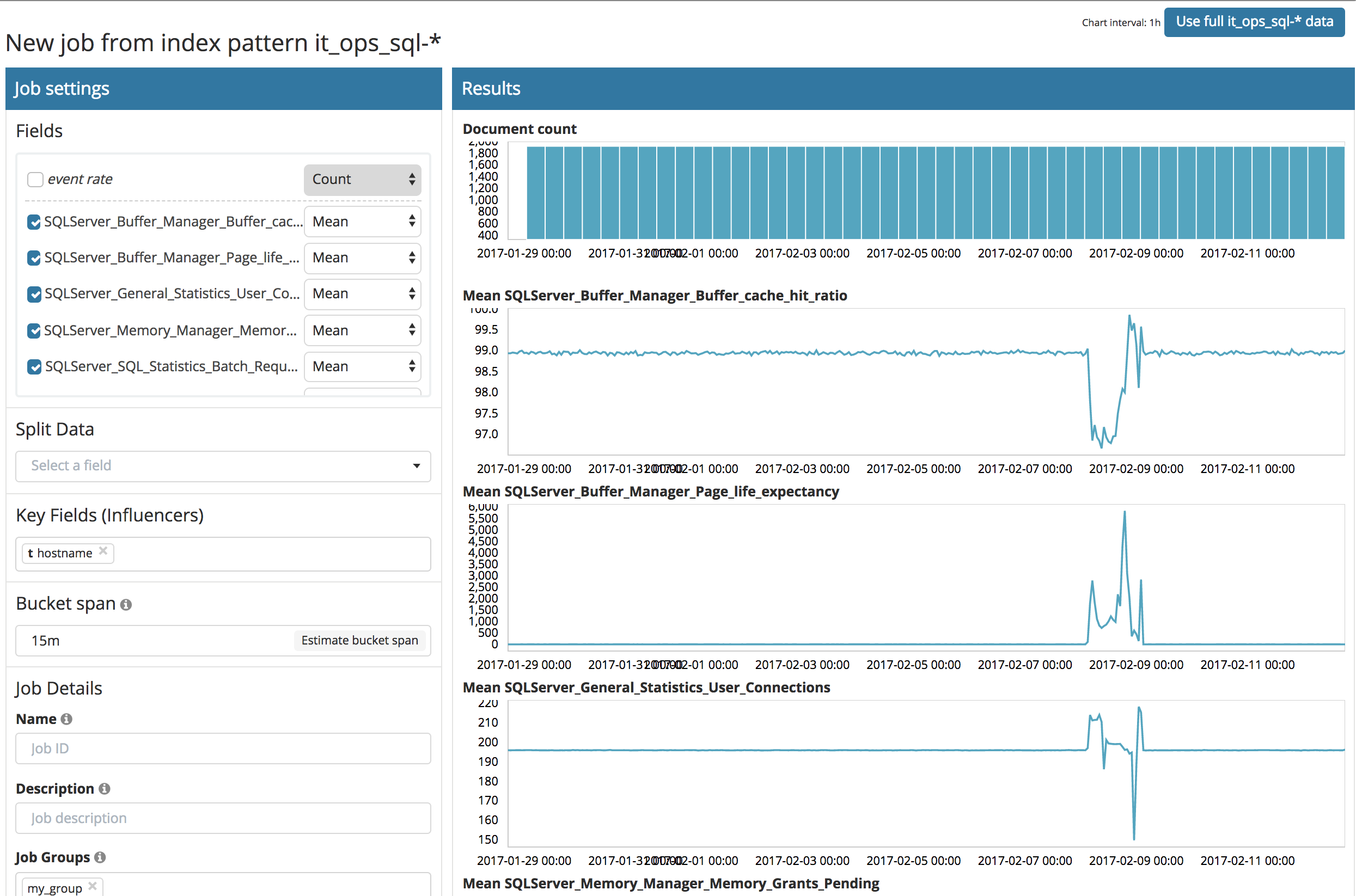
* create an advanced job
* put job in a group
* make sure you choose   
  “message” for  
  categorization\_field\_name
* detector is:  
  count with by\_field\_name of  
  “mlcategory”



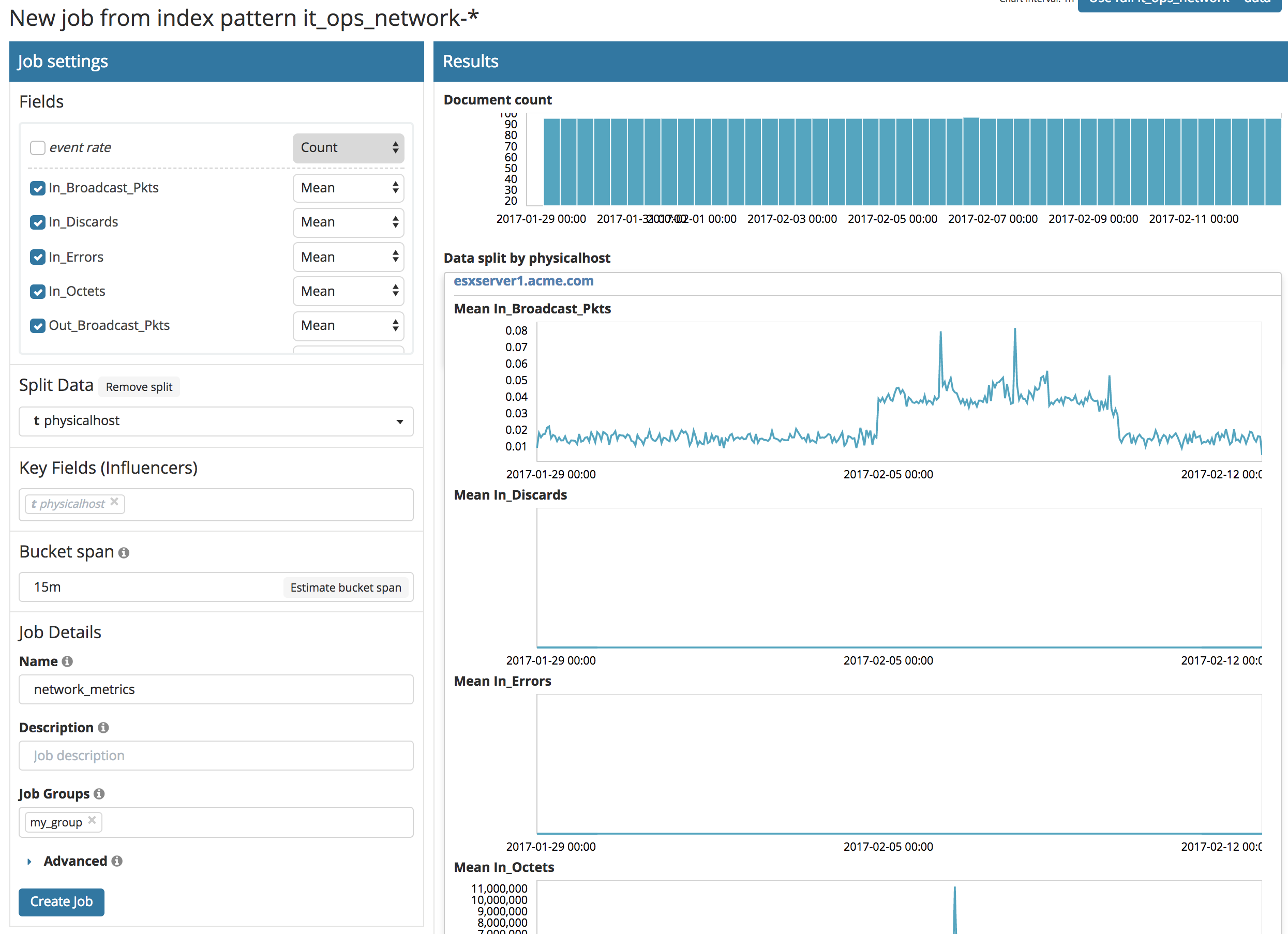


## Create Multi-Metric jobs for the following indices “it\_ops\_sql” and “It\_ops\_network”

For index:it\_ops\_sql\* create multi-metric job. Set “mean” for all SQL metrics. Also put job in same Job Group as the app logs job.

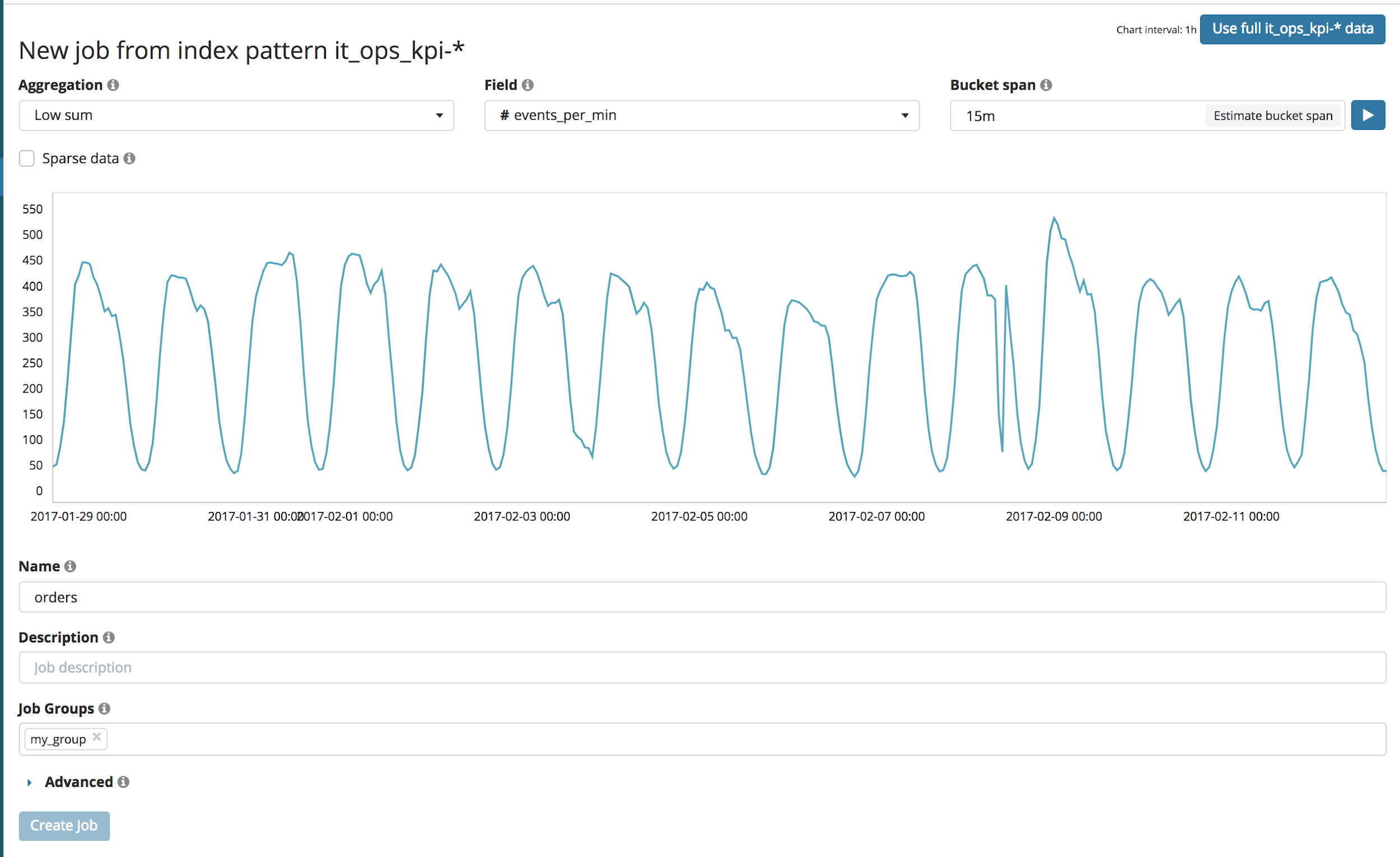


For index:it\_ops\_network create multi-metric job. Set “mean” for all metrics. Also put job in same Job Group as the app logs job.



## Create a “low\_sum” Single-Metric job for the following index “it\_ops\_kpi”

For index:it\_ops\_kpi create single-metric job “low\_sum” for field “events\_per\_min”. Also put job in same Job Group as the app logs job



## View all jobs overlaid in the Explorer View

View all jobs in Group, see correlated anomalies

