Module

Kibana for Time Series Data

elastic

Topics

- Kibana Fundamentals
- Visualizations and Dashboards
- Time-Series Visualization Builder (TSVB)

Lesson 1

Kibana Fundamentals

elastic

Event Data

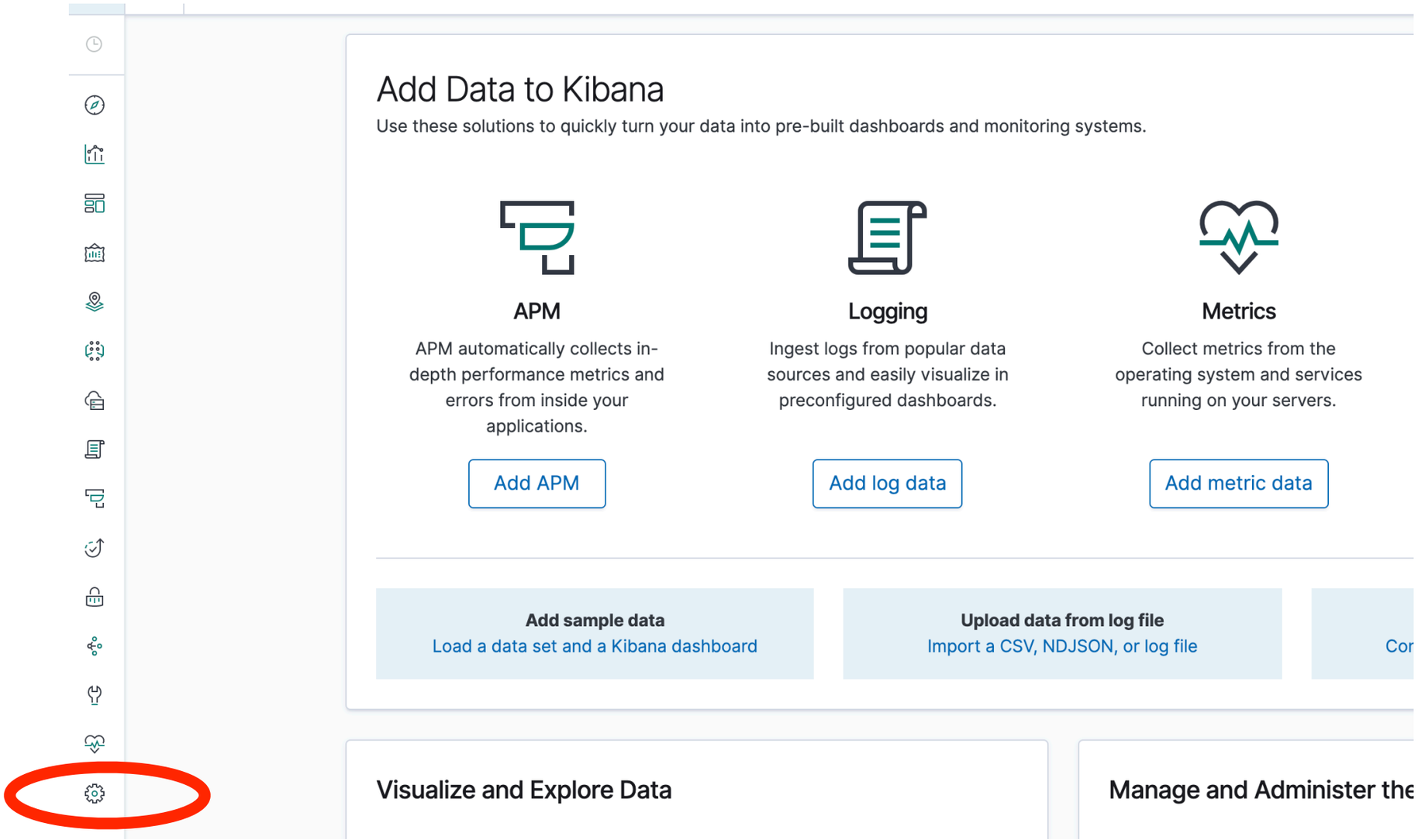
elastic

Configuring Index Patterns

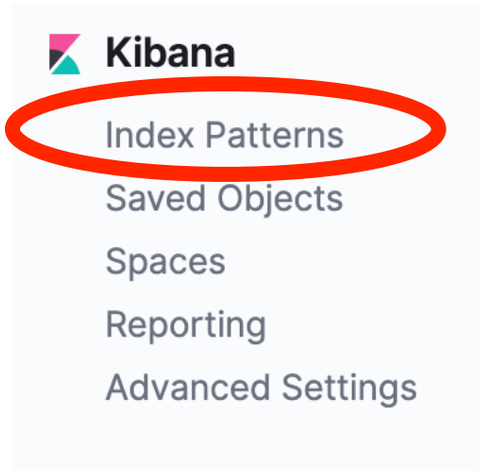
- Typically, Kibana data does contain "time-based" events, which contain a timestamp and some data
- Kibana requires ***index patterns*** in order to find this data as it lives in Elasticsearch
- Commonly, *time-series* indices will include some sort of timestamp in the index name
  - (e.g. "***apachelogs-2018.12.15***")
- Other times, the data may live in one *static* index
  - (e.g. "***products***")
- Kibana prefers a timestamp field, so that it can render visualizations over time (for example date histograms)
  - (e.g. "***@timestamp***")

First look at Kibana

- Click on Management in the left nav to begin



- Then click on the "Index Patterns" link:

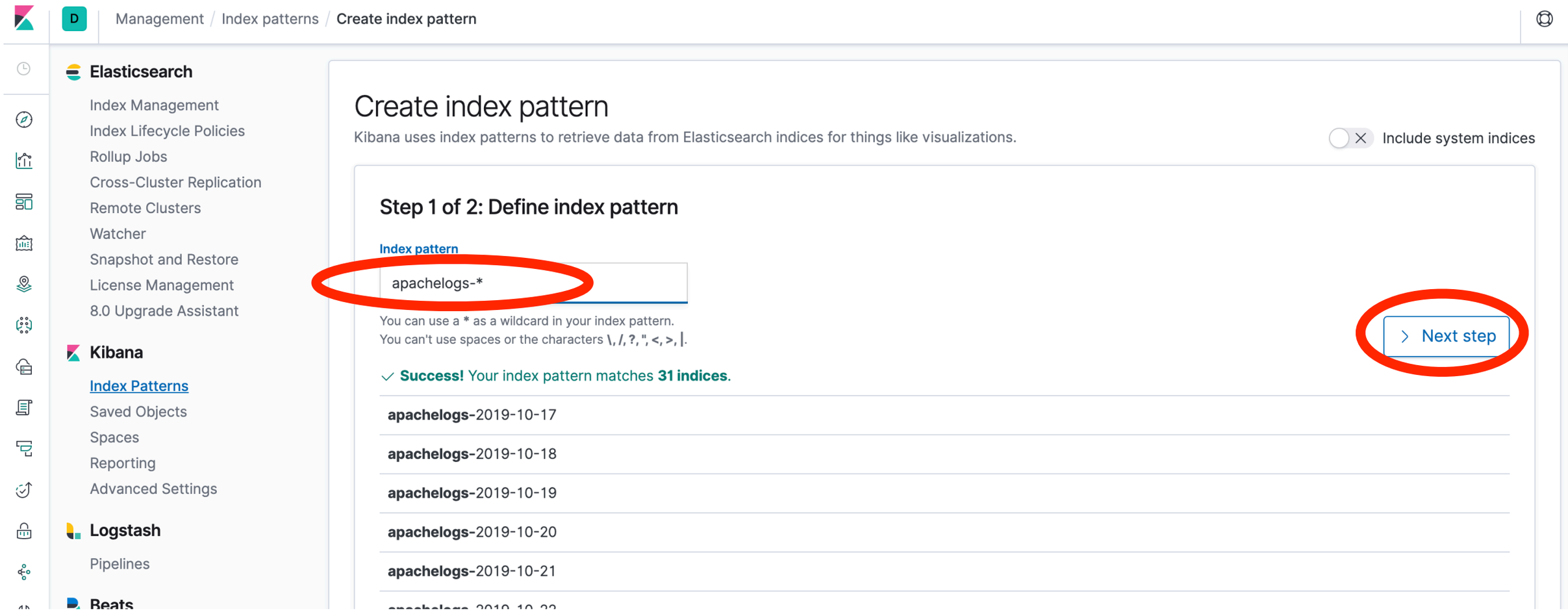


Index Patterns

elastic

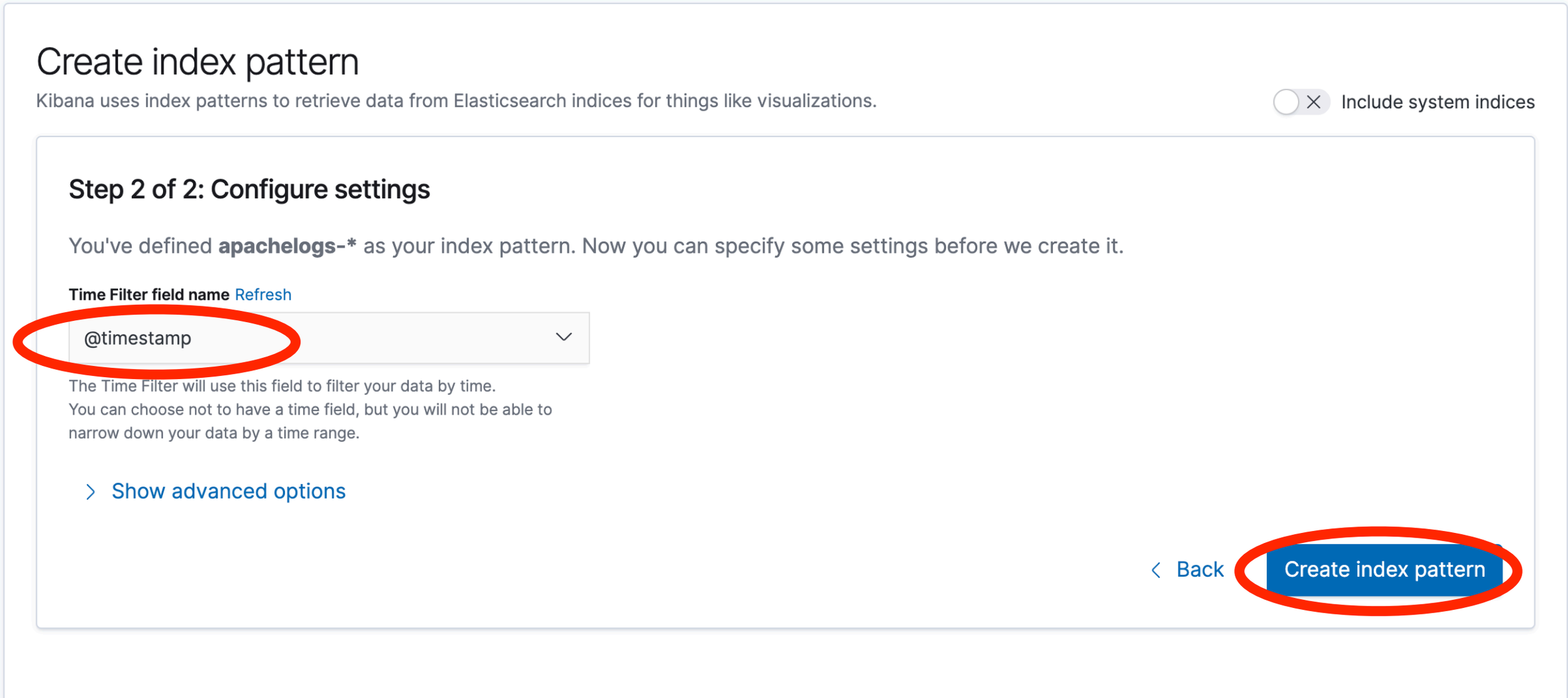
Configuring an index pattern

- Type "**apachelogs-***" in the Index pattern box then click on the "Next step" button



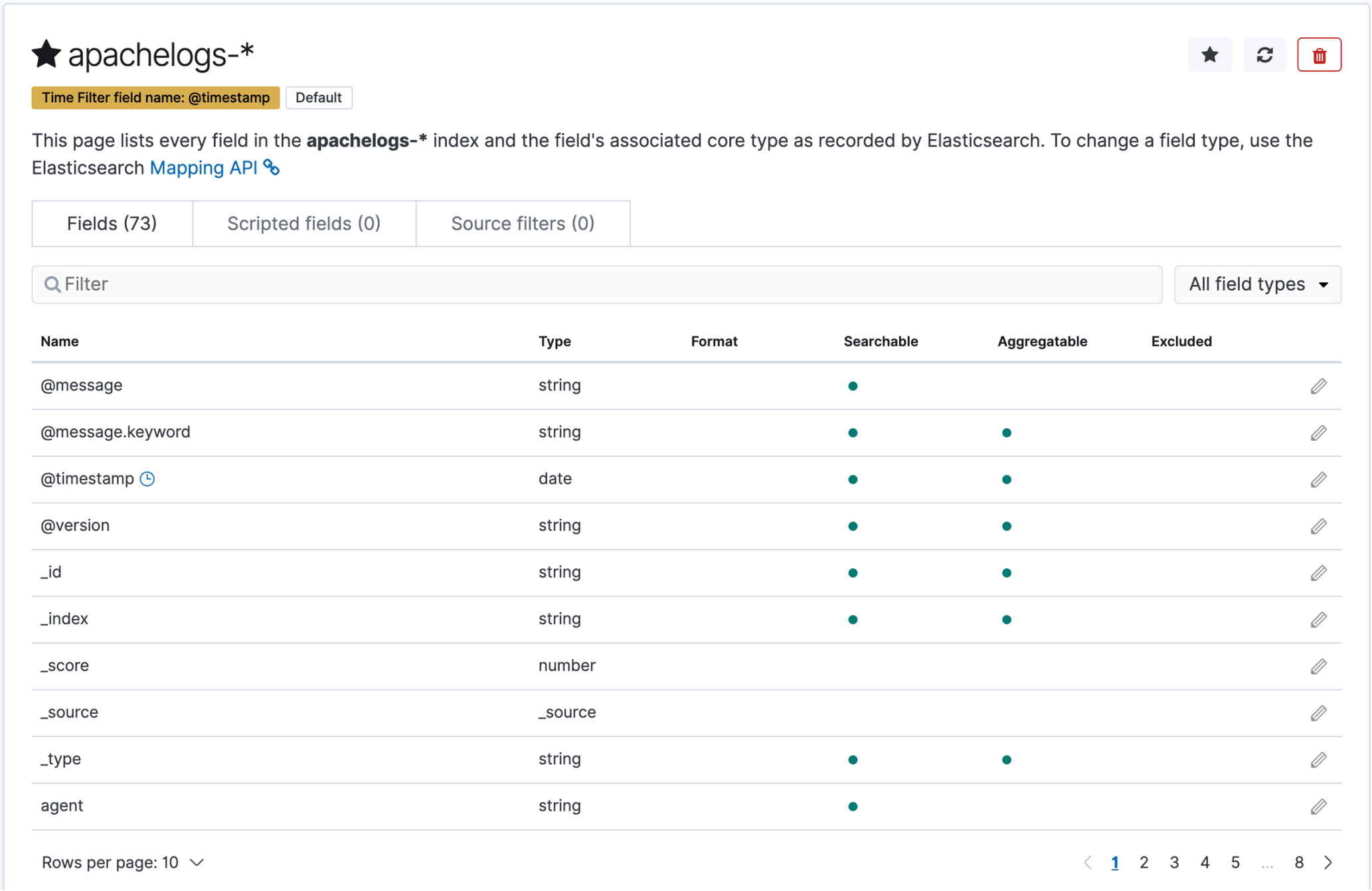
Picking the time filter field

- Select the field which Kibana will use to render time-based visualizations: **@timestamp** works well for us here. Then click the Create Index pattern button.



Index Pattern successfully created

- After successful creation, you will be able to view the various fields which the documents in this pattern contain

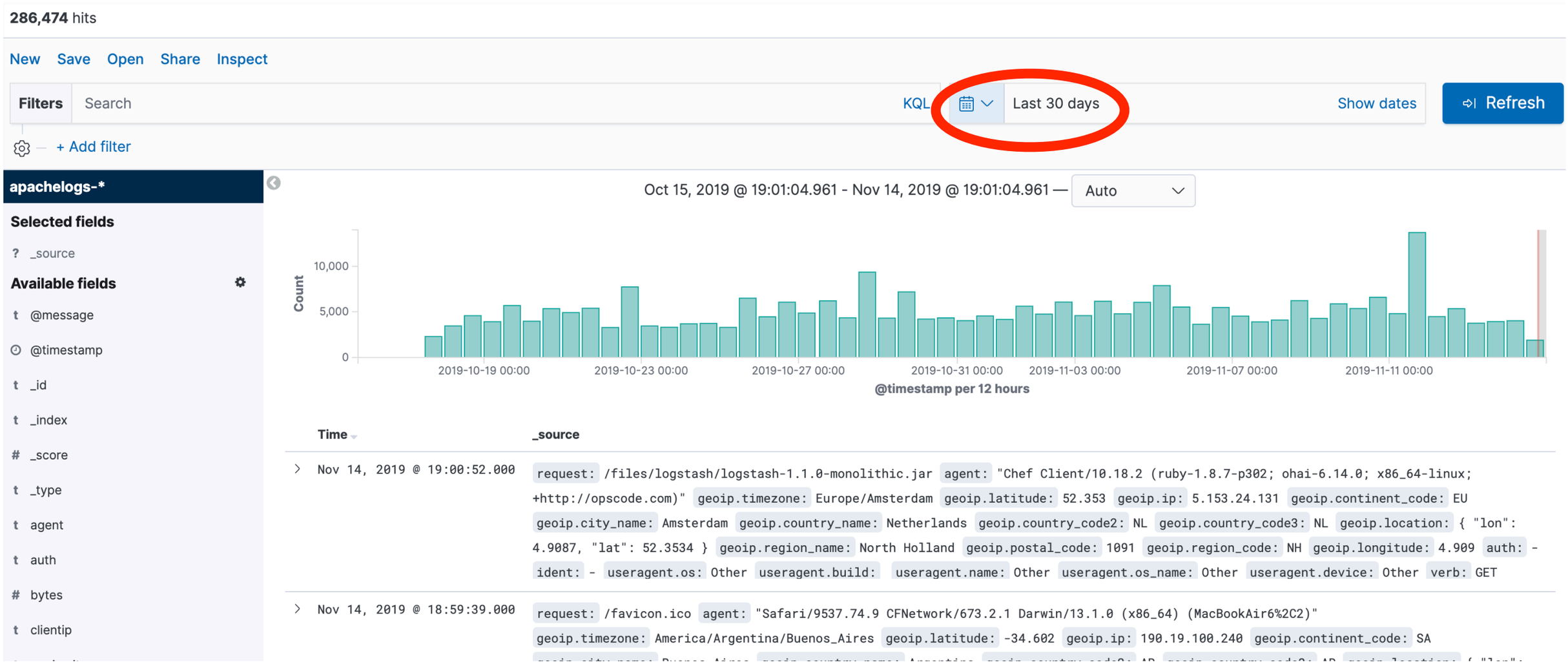


Discover

elastic

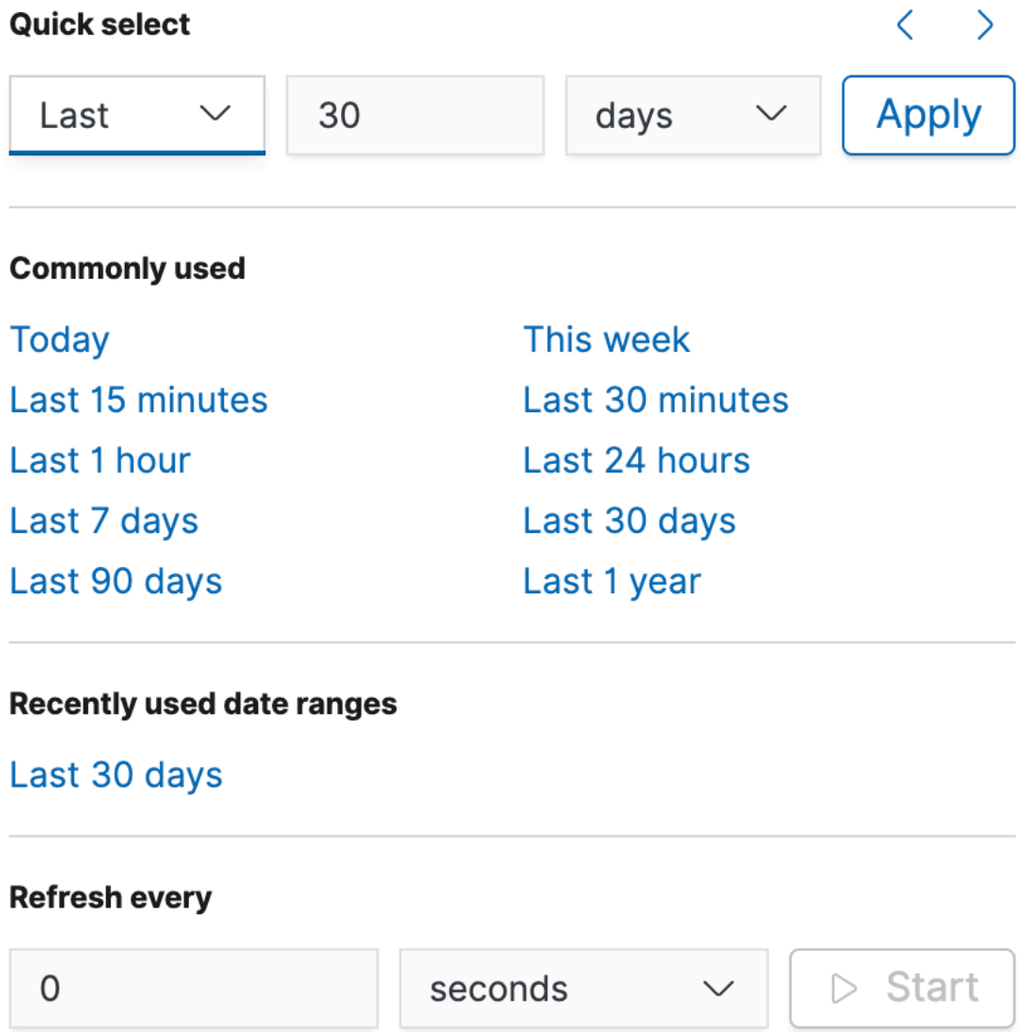
Discover Main Page

- Clicking on the Discover tab on the left nav brings you here
- Click to ensure the time picker reflects "Last 30 days" for your lab's dataset



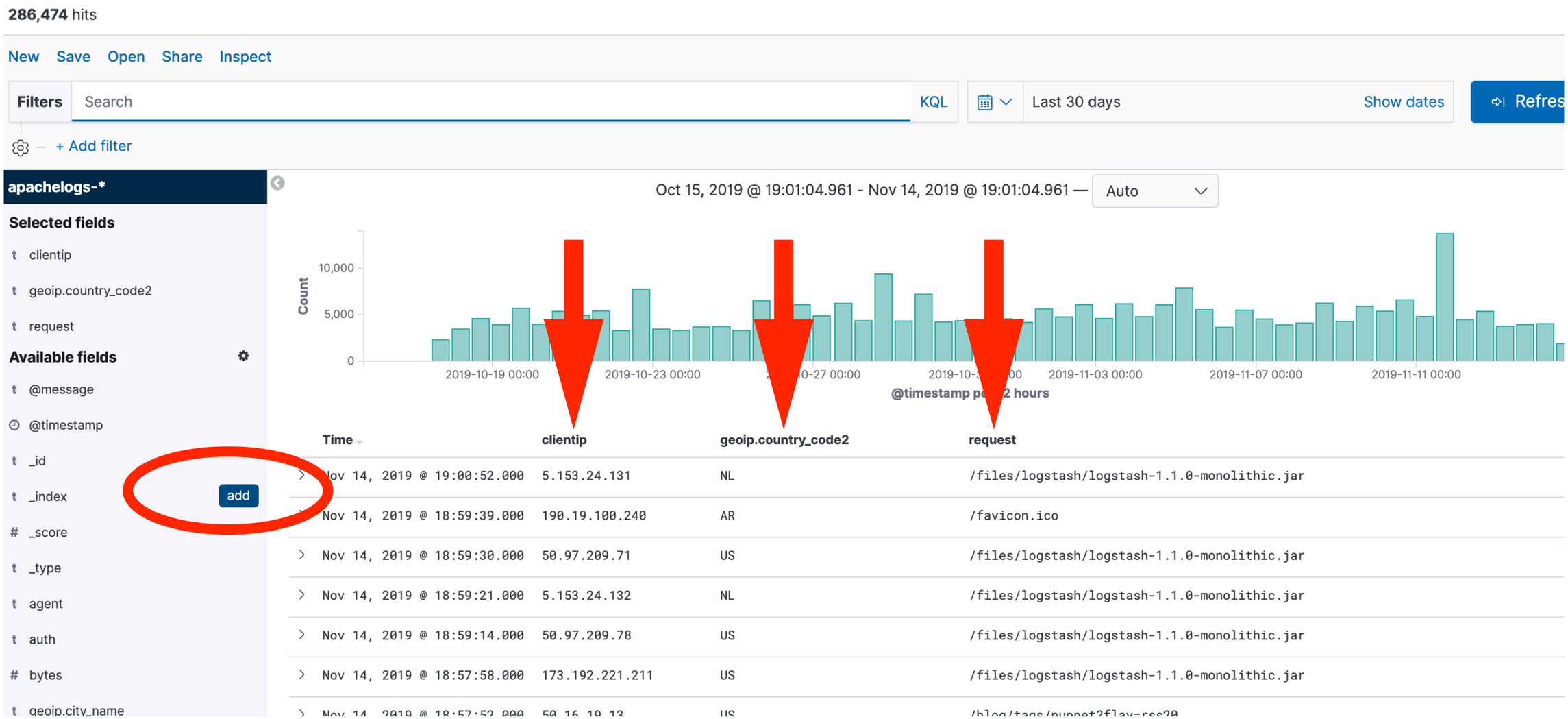
Time Picker

- Quick: convenient shortcuts
- Relative: "last 7 days", "a week ago until a day ago" etc
- Absolute: fine-grained selection using calendar
- Recent: your history



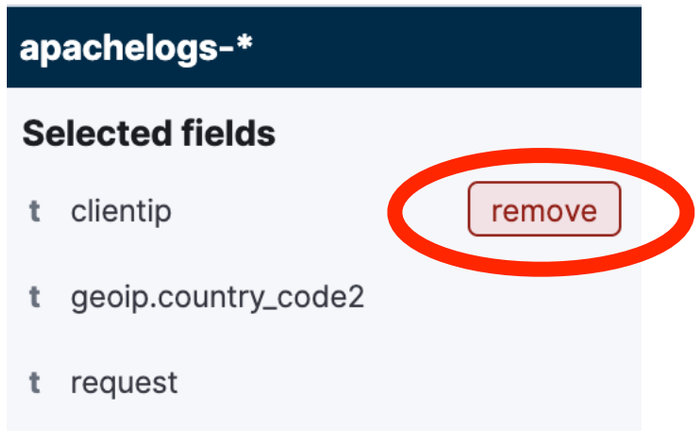
Customized Columnar View

- Add columns to view from the left nav:

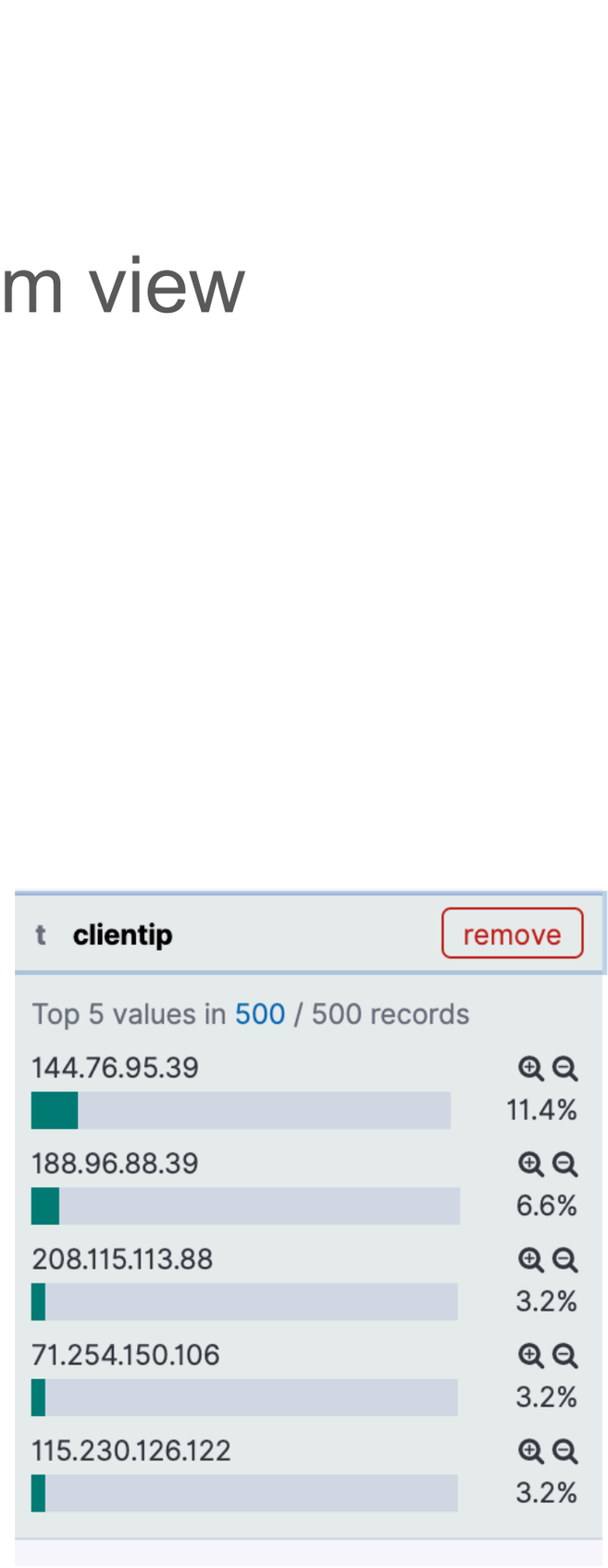


Field-level controls

- Click "remove" to delete column from custom view



- Click fieldname to review sampled stats:



Document view

- Table View (shown here) or original JSON
- Can create a filter easily here!
- Link to view document or documents "surrounding" this one

	Time	clientip	geoip.country_code2	request
>	Nov 14, 2019 @ 19:00:52.000	5.153.24.131	NL	/files/logstash/logstash-1.1.0-monolithic.jar
v	Nov 14, 2019 @ 18:59:39.000	190.19.100.240	AR	/favicon.ico

Expanded document

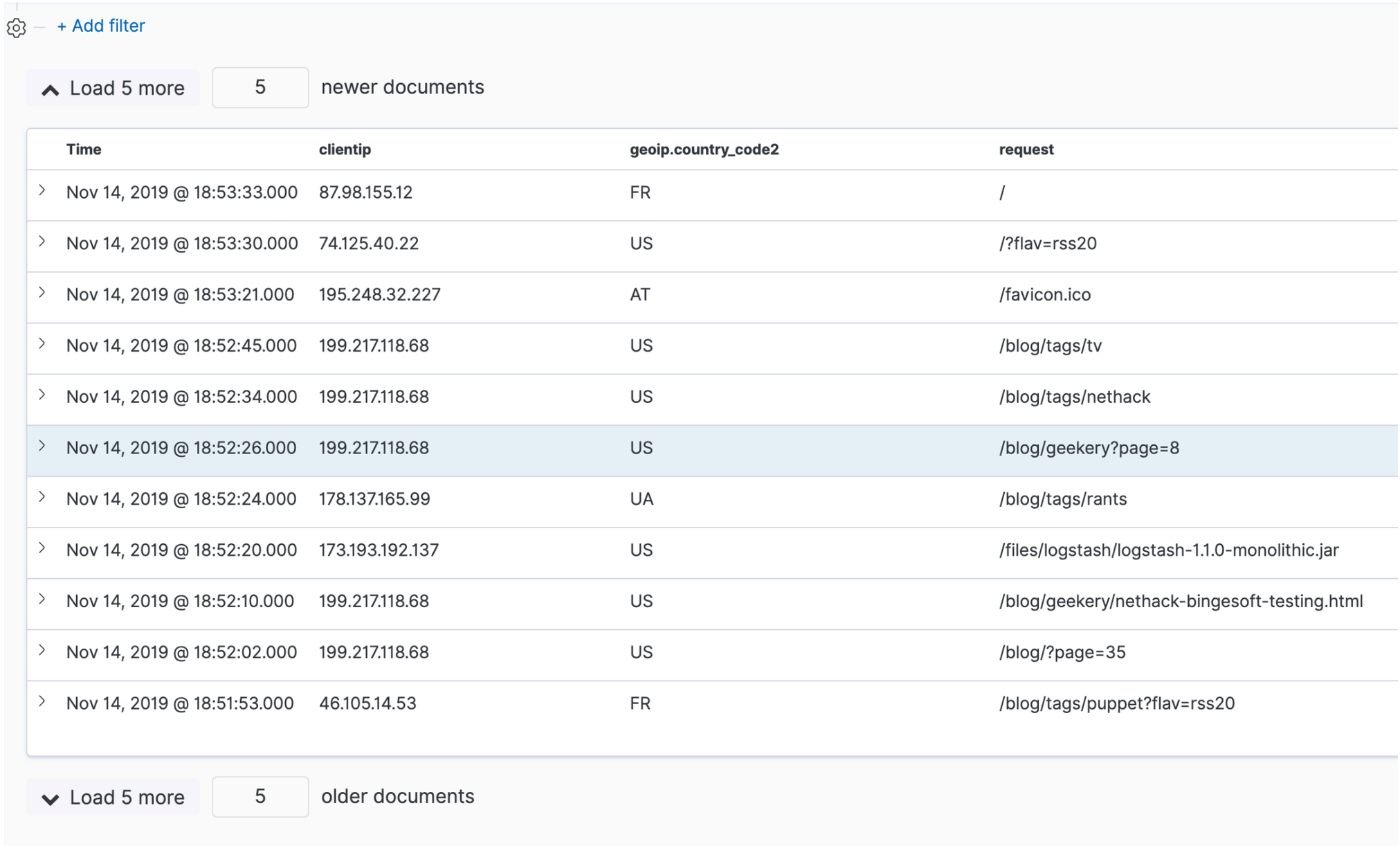
View surrounding documents | View single document

Table | JSON

t	@message	190.19.100.240 GET /favicon.ico
clock	@timestamp	Nov 14, 2019 @ 18:59:39.000
t	_id	y540am4B0HbrE43Q5tBM
t	_index	apachelogs-2019-11-14
#	_score	-
t	_type	_doc
t	agent	"Safari/9537.74.9 CFNetwork/673.2.1 Darwin/13.1.0 (x86_64) (MacBookAir6%2C2)"
t	auth	-
#	bytes	3,638
t	clientip	190.19.100.240
t	geoip.city_name	Buenos Aires
t	geoip.continent_code	SA
t	geoip.country_code2	AR

Surrounding Document view

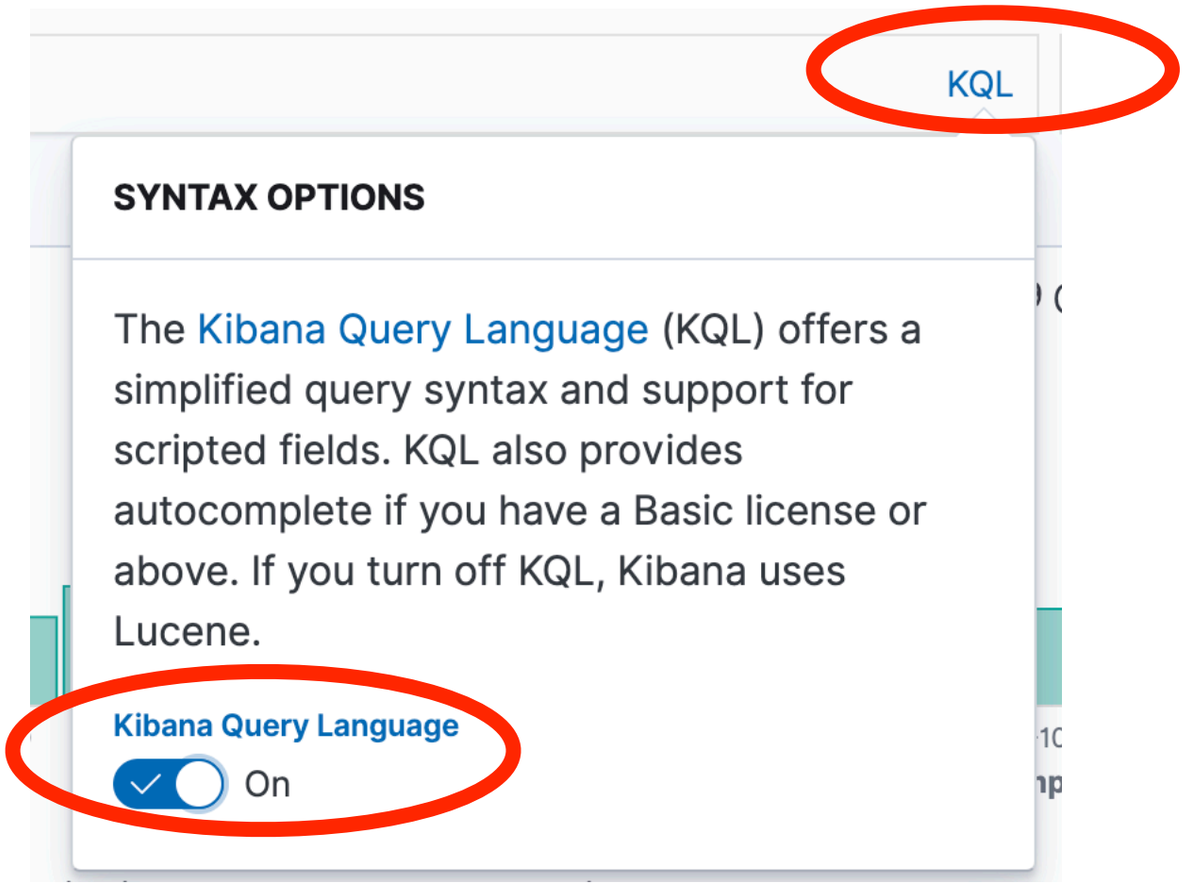
- Five before/after by default, but you can load more
- Before/after determined by sorting on timestamp field



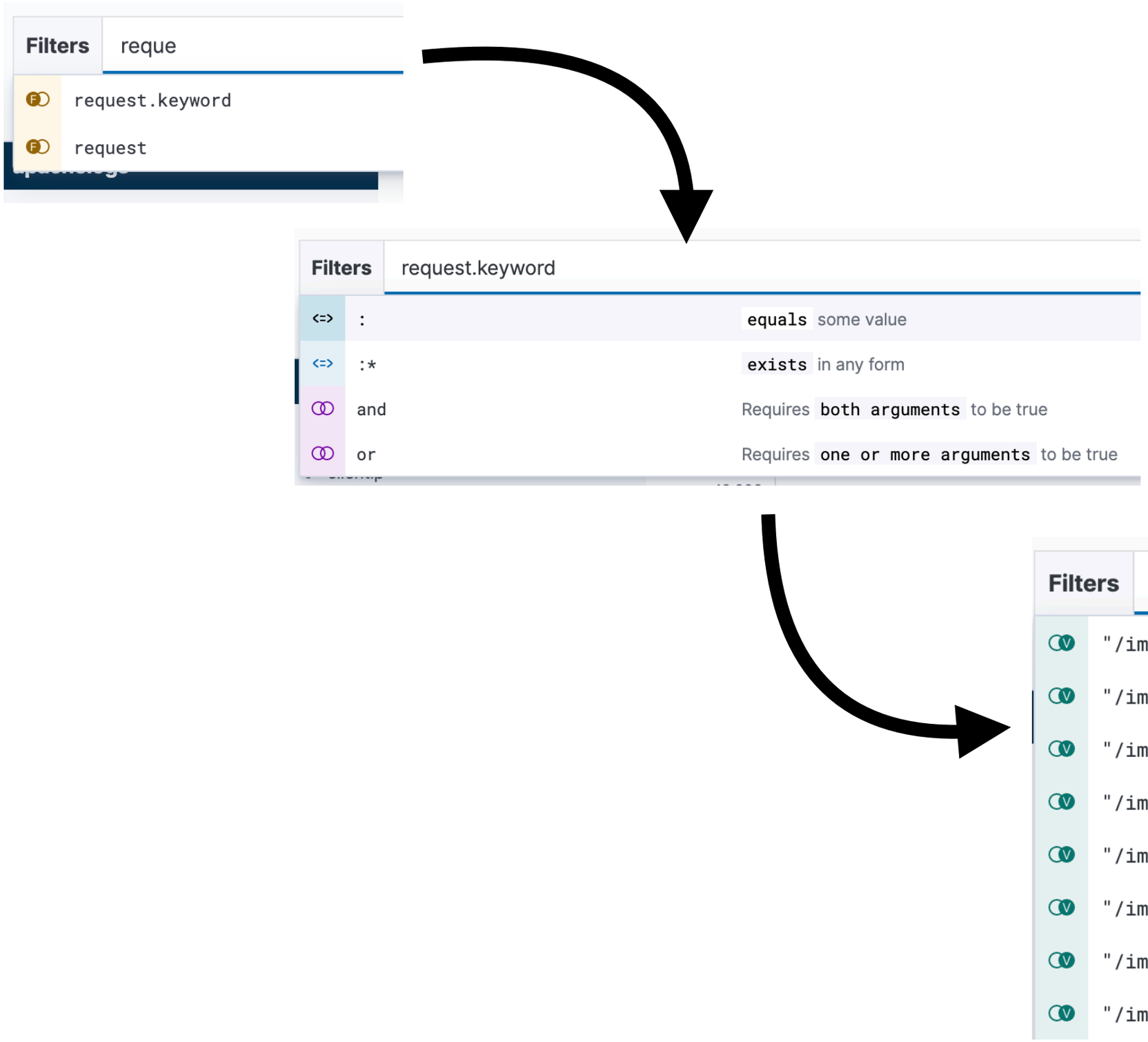
Text Search

Text search

- The default search is Kibana Query Language (KQL)
- Click the “KQL" link and turn off KQL to enable Lucene Query Syntax

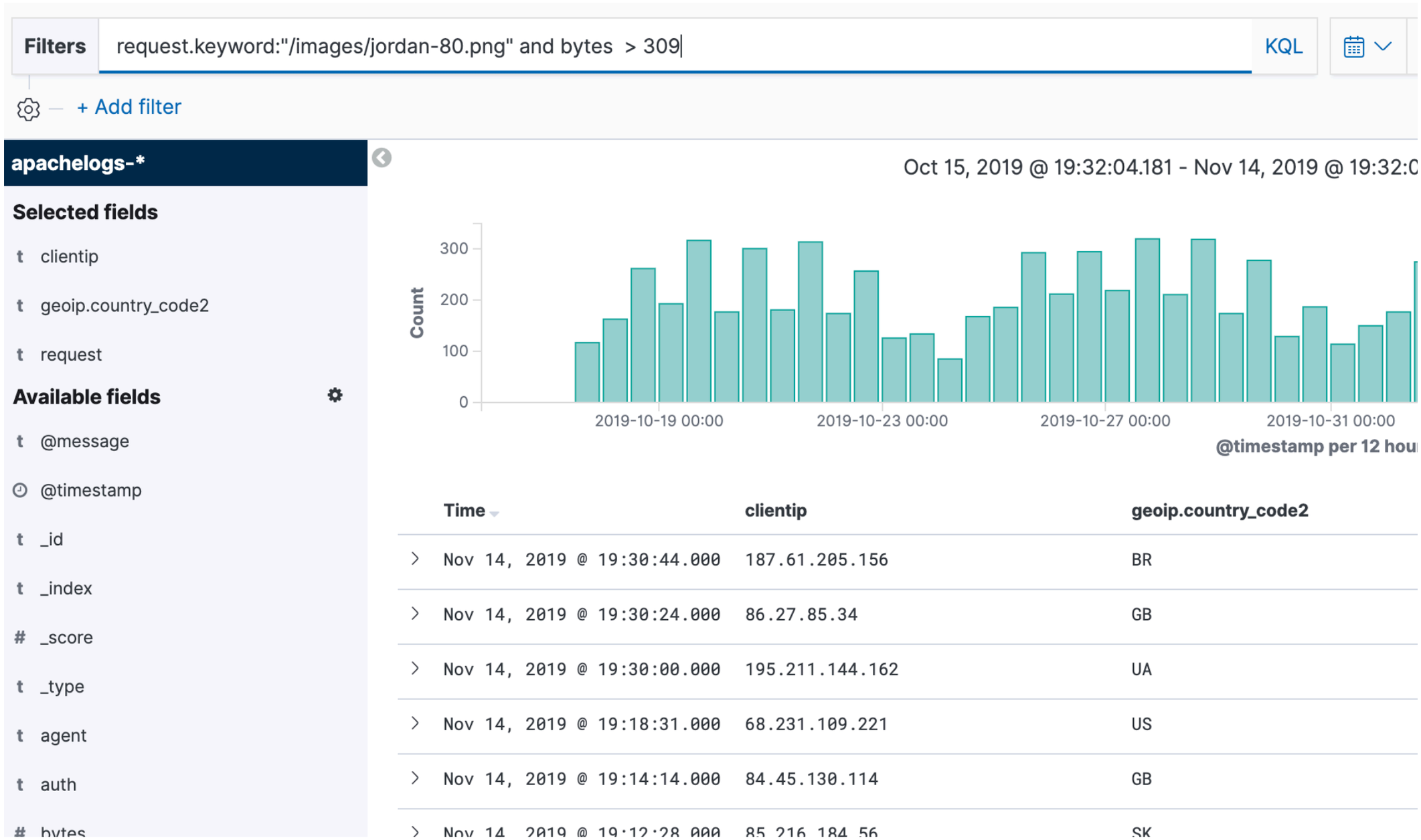


Auto-complete in Kibana query language



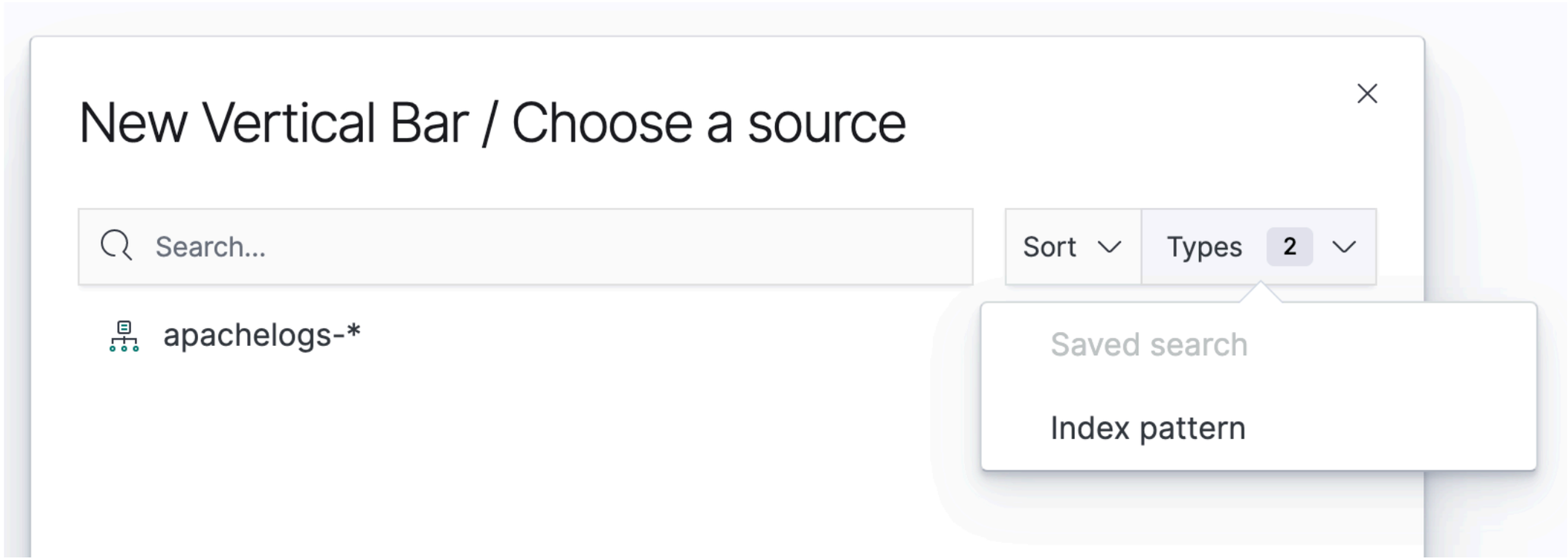
Compound Boolean Queries

- Use operators such as **and, or, not** in Kibana queries



Saved searches

- Any search can be saved
- Any time you find an interesting search, go ahead and save it for later use (just like creating filters)
- Saved searches can be attached to visualizations in the Create Visualization screen



Manipulating Filters

elastic

Using and Manipulating Filters

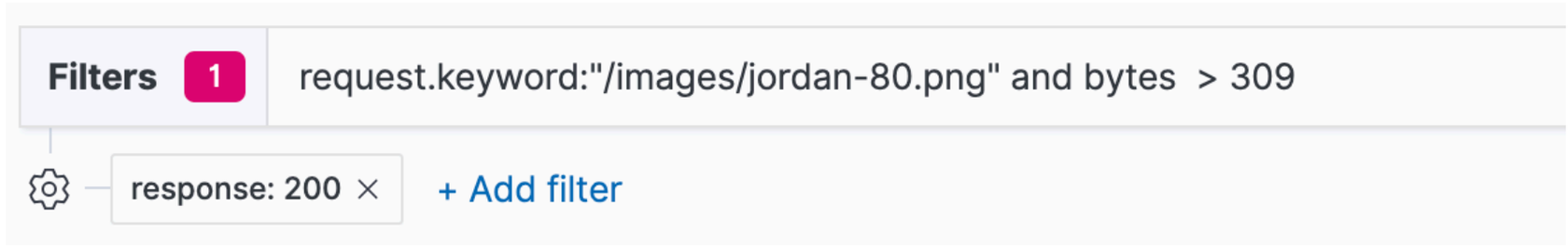
- Filters are are important tool in your discovery process
- They can help you include or exclude documents in searches as well as visualizations
- Look for the "magnifying glass" icons, or click on any element of a visualization representing a value
- It's easy to toggle a filter on and off for comparison
- "Pin" filters and they will follow you throughout Kibana
- Filters can be associated with a visualization, also

Creating a filter by clicking on a value

- Anywhere Kibana shows you a particular value, you can create a filter by clicking on it. Two common examples:

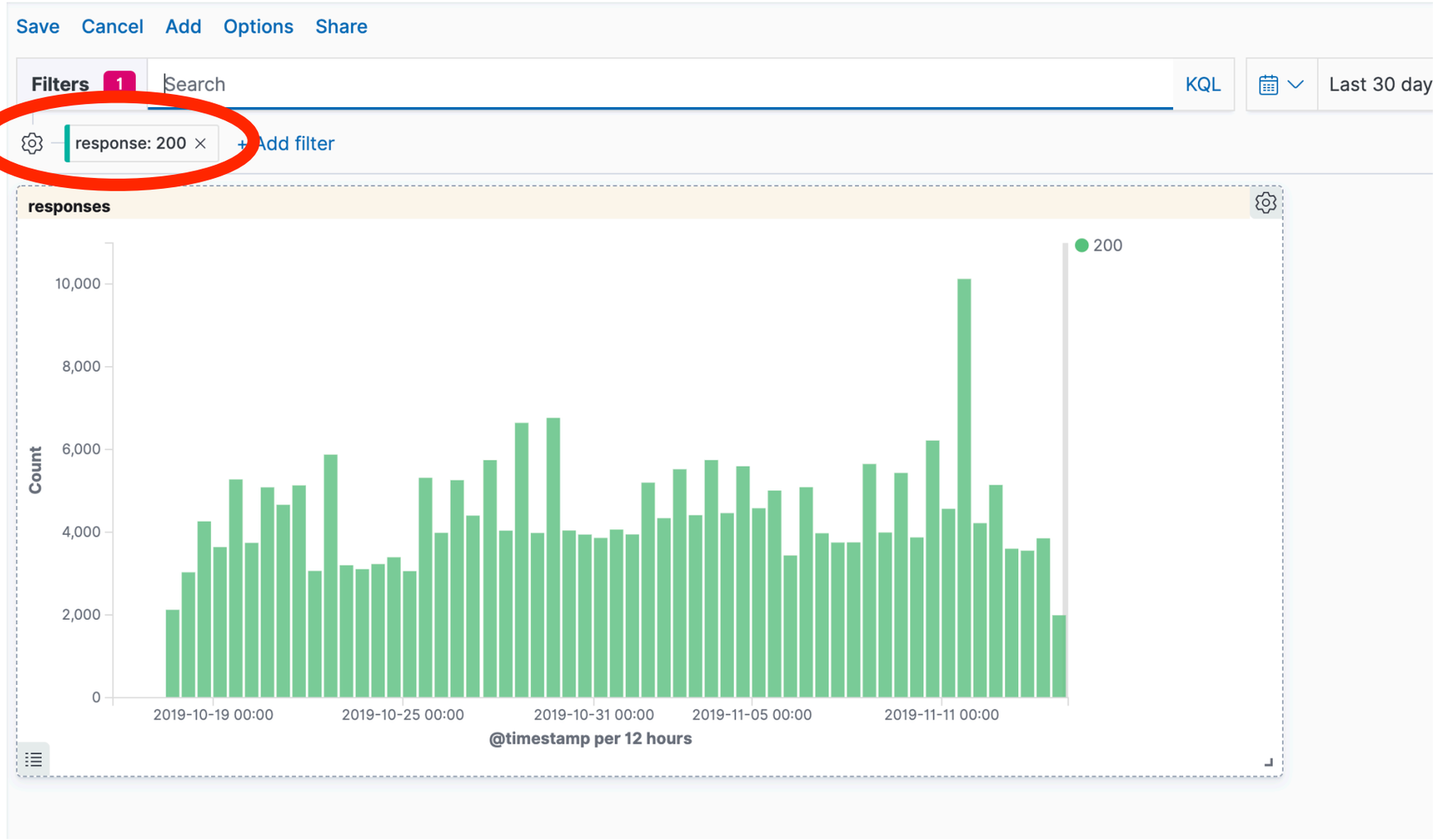
Applying Filters

- Kibana will prompt you to apply the filters
- In the example, we can apply a filter such as **response:404**



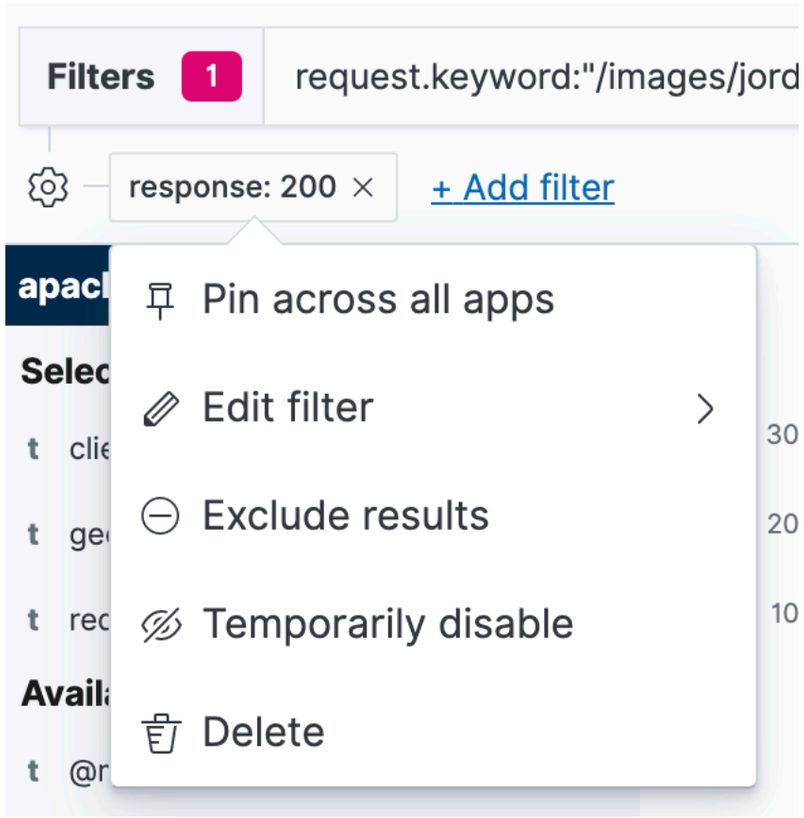
Effect of Filters

- You can pin a filter to be used across different applications
- Example: when browsing back to a dashboard, a pinned filter will apply, and you will only see matching documents visualized



Filter Actions (descriptions on next slide)

- You can manipulate each filter in several ways

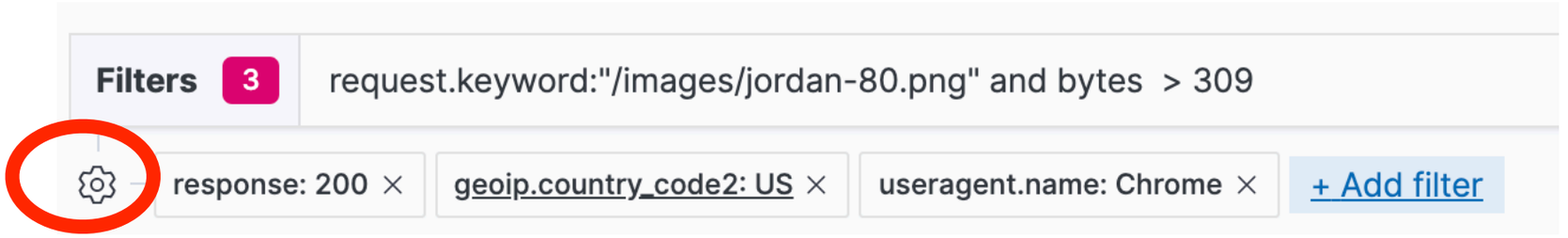


Filter Actions

- Toggle: Turn the effect of the filter on / off. Useful to see the influence of a filter on a visualization when toggled rapidly.
- Pin: When a filter is pinned, it will follow you around the various areas of Kibana. Whenever you spot an "interesting" data point, you should consider creating and pinning a filter, for later inspection.
- Invert: Change the filter's effect from "matches this value" to "does not match this value"
- Delete: Remove a filter

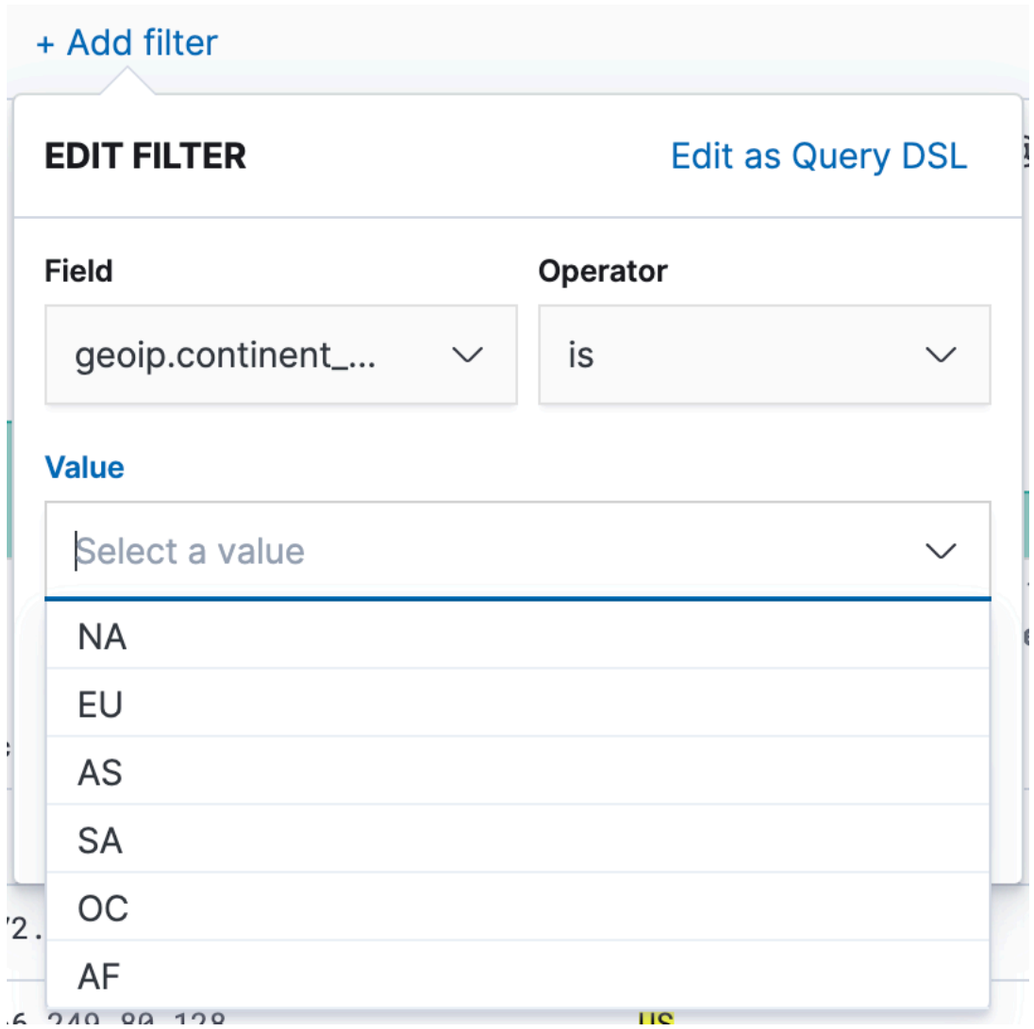
Actions on multiple filters

- You can add as many filters as you like
- Pin them! They will follow you in Kibana
- The "Gear" icon on the left will allow you to perform a particular action on all of the filters simultaneously



Adding a filter manually

- You can specify exactly the criteria which the filter matches



Lesson 1

Review - Kibana Fundamentals

elastic

Summary

- Kibana requires the use of Index Patterns for time-series datasets
- Sometimes the index pattern is created for you, but other times you must configure it yourself
- Kibana has a multitude of visualization types which give you a rich set of tools to build custom panels
- Dashboards are constructed by adding existing visualizations and re-arranging as necessary
- Filters are a useful tool in exploring your data
- Pinning filters is an easy strategy to help you visualize data.
- Filters can be toggled on and off to perform comparisons

Quiz

1. **True or False:** Kibana will automatically discover your data and pre-configure index patterns 100% for you.
2. **True or False:** Kibana Discover allows you to inspect individual documents
3. Which strategy allows you to make a filter "permanent", so it will follow you around as you browse Kibana?
4. **True or False:** Kibana Discover allows you to view only documents matching a particular query and/or filter
5. Which tool allows you to zoom in on the last 7 days?
6. What are the two query languages available in Kibana?
7. **True or False:** searches can be saved and attached to visualizations

Kibana for Time Series Data

Lesson 1

Lab - Kibana Fundamentals

elastic

Kibana for Time Series Data

Lesson 2

Visualizations and Dashboards

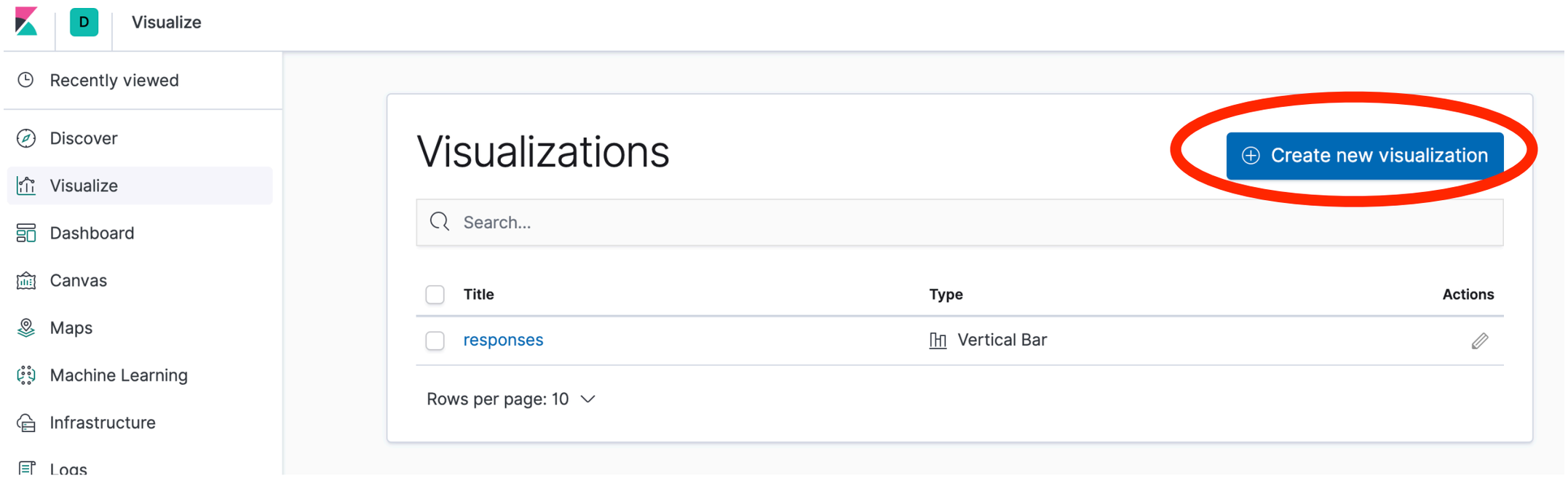
elastic

Visualizations

elastic

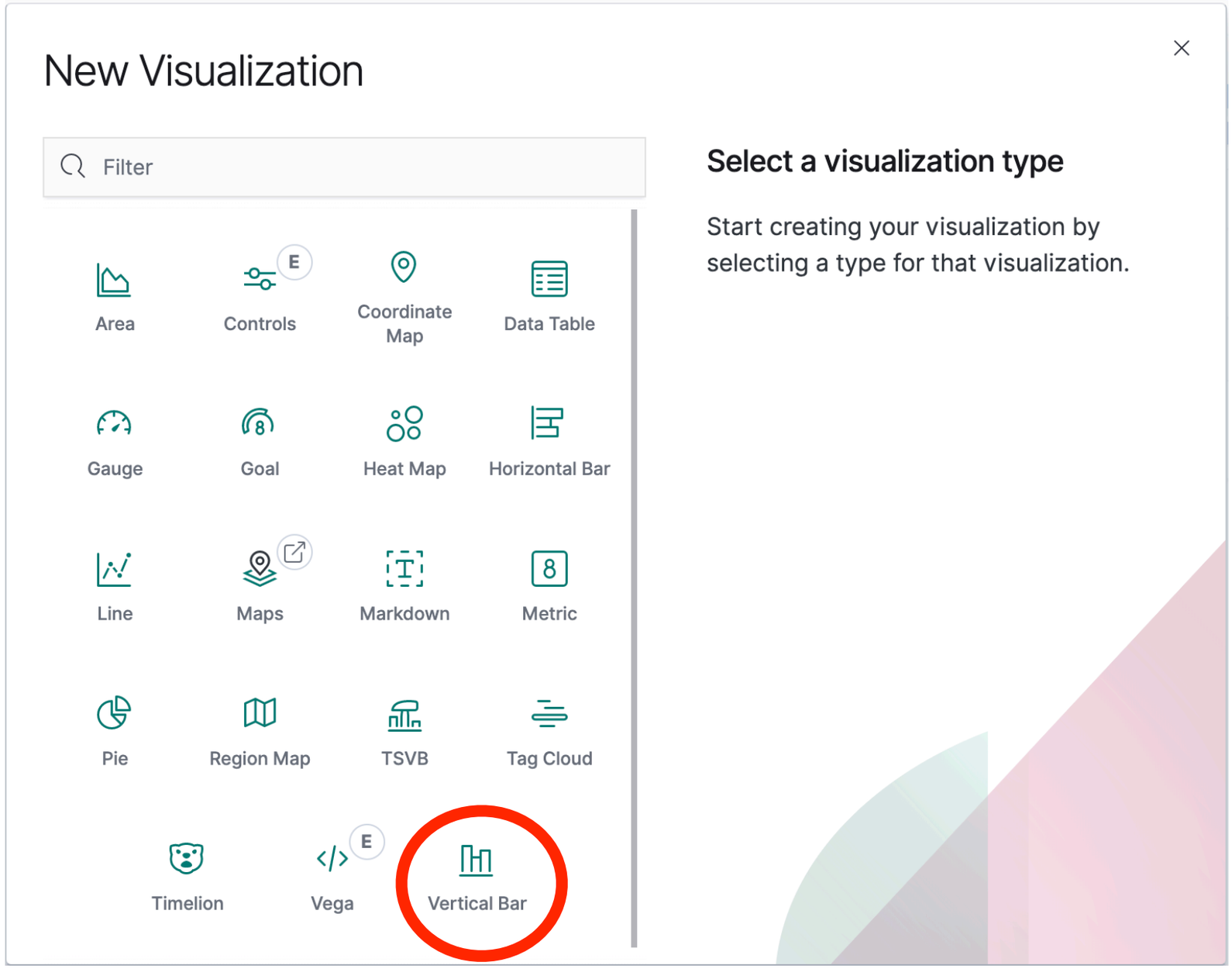
Creating Visualizations

- After clicking on the “Visualize" tab in the left nav, you will see the interface for creating visualizations
- Click on the “Create new visualization” button to begin configuring the visualization



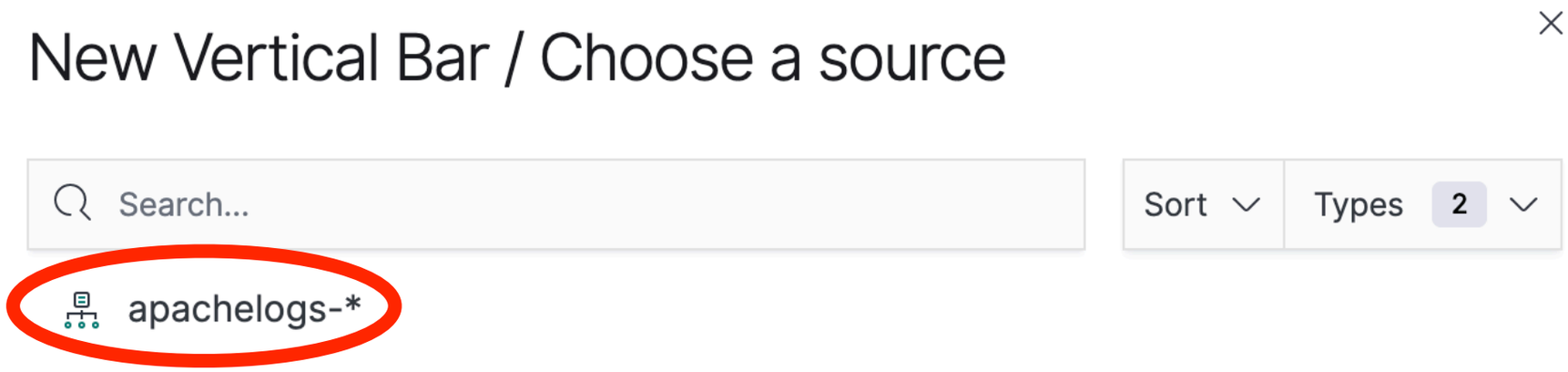
Visualization types

- As you can see, there are many types to choose from



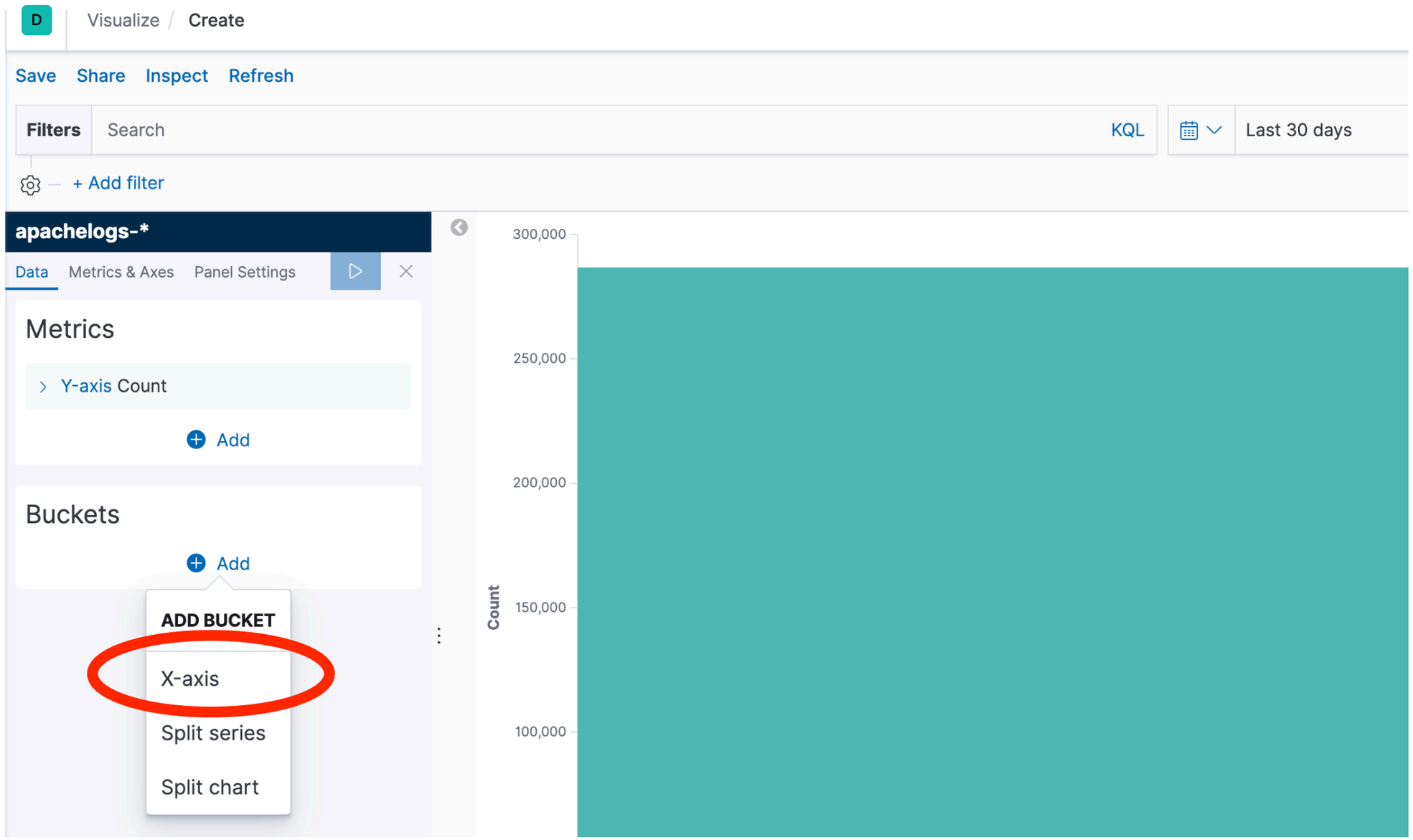
Select the index pattern

- We only have one index pattern, so let's use it



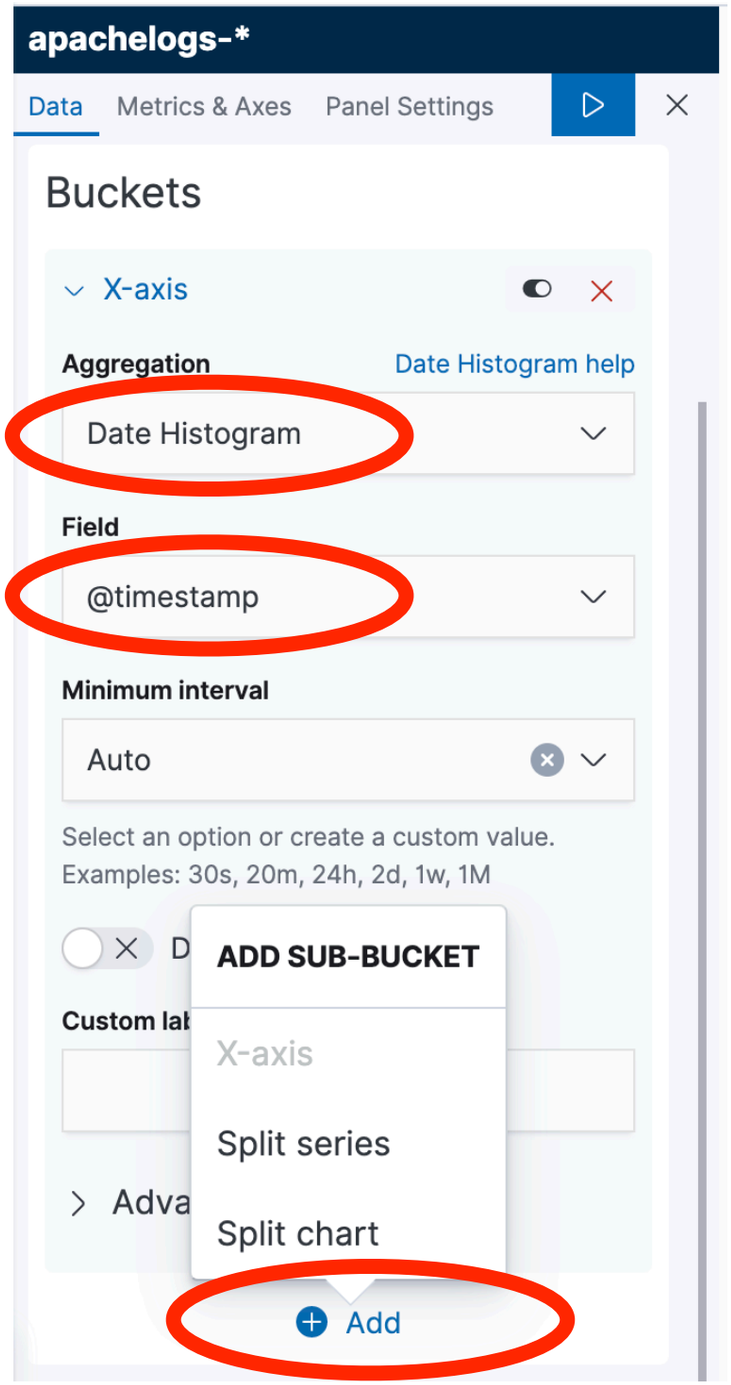
Configure the vertical bar chart

- We will use a ***date histogram*** to build this chart
- Click on "X-axis" to continue



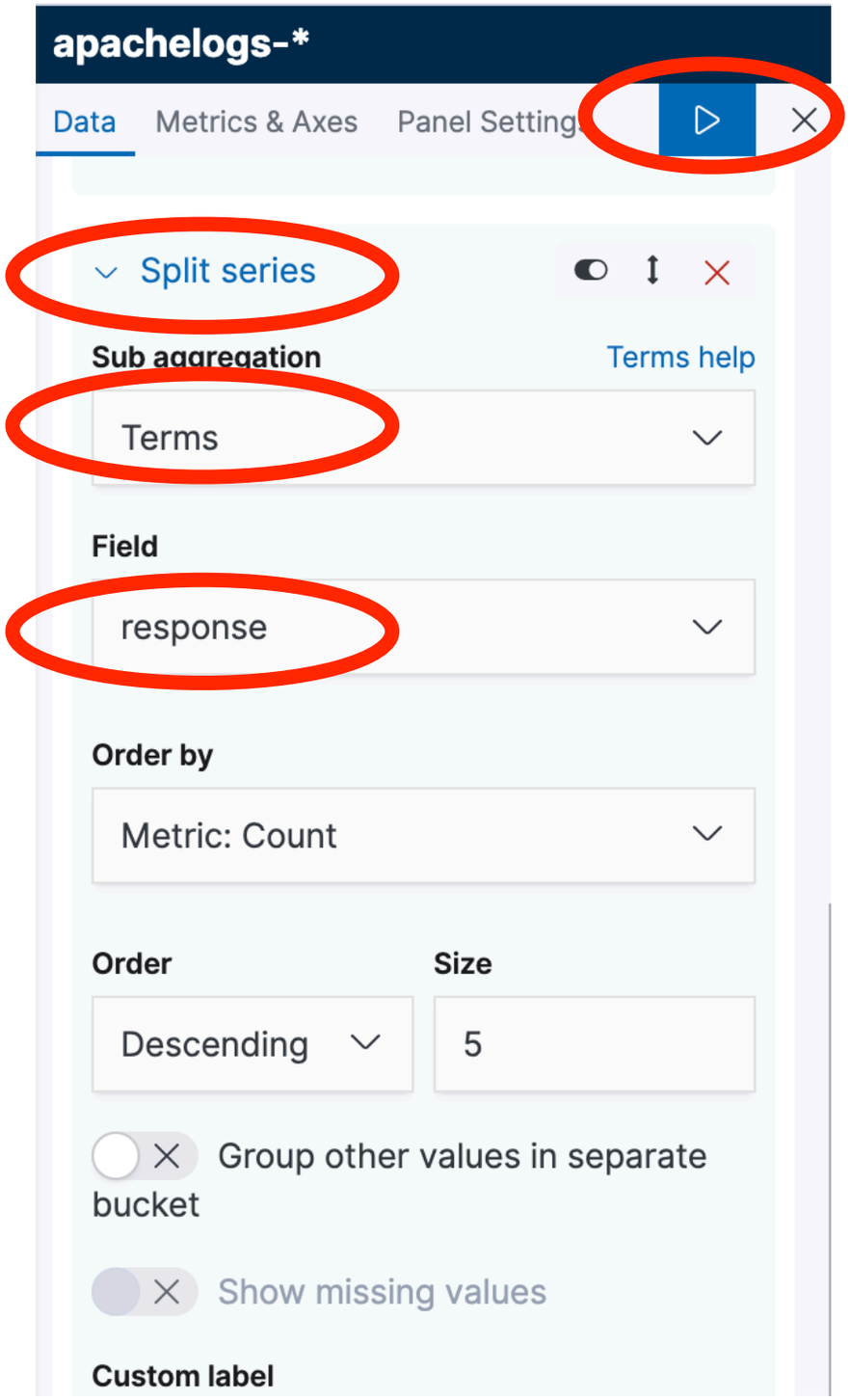
Configure buckets

- Use the Date Histogram and select the ***@timestamp*** field
- Then click "Add sub-bucket"



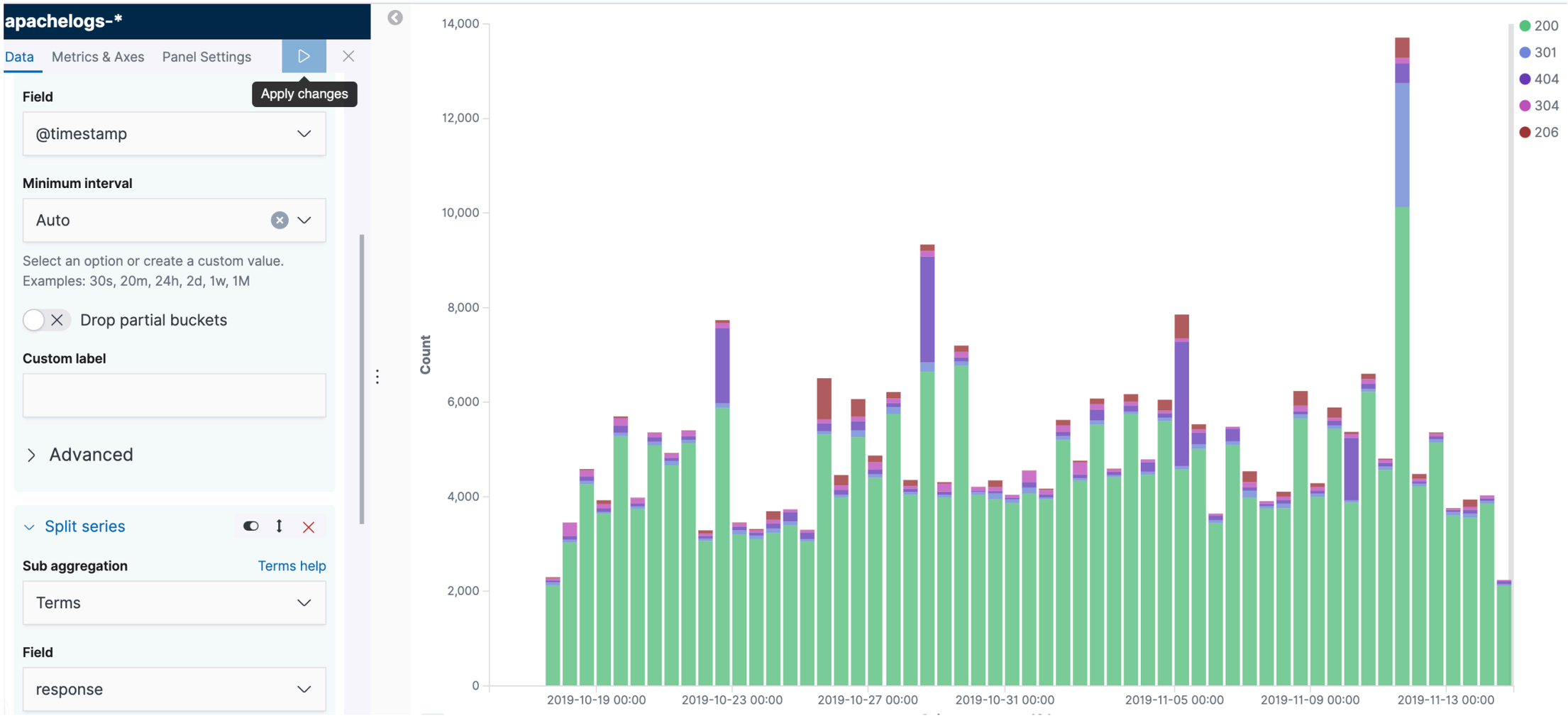
Configure buckets

- Use "Split Series"
- Sub-Aggregation: ***Terms***
- Field: ***response***
- Click blue "play" arrow at top right



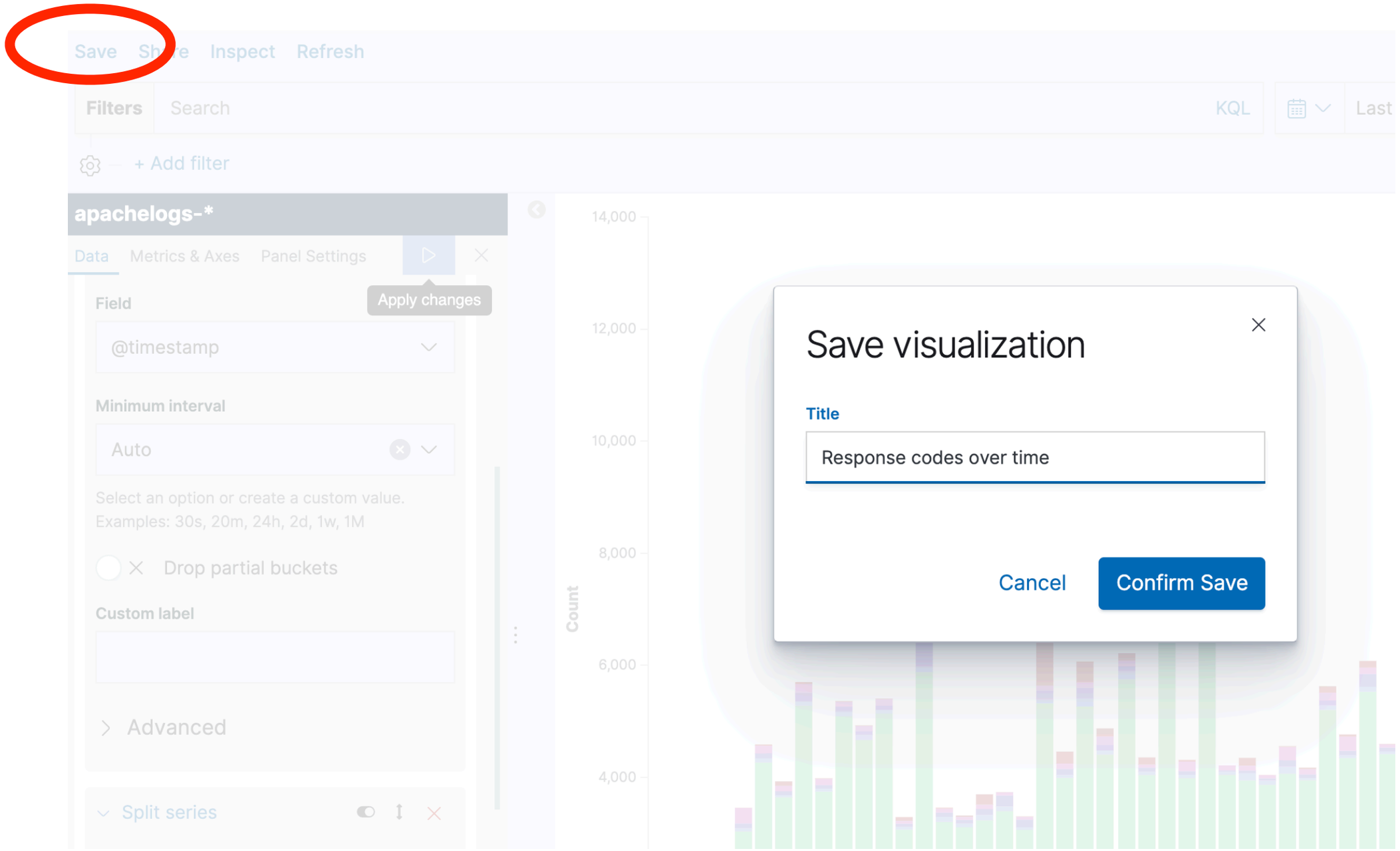
Multi-bucket visualization

- Now you can see the result: each color-coded bar shows the ratio of response codes per time bucket



Saving visualizations

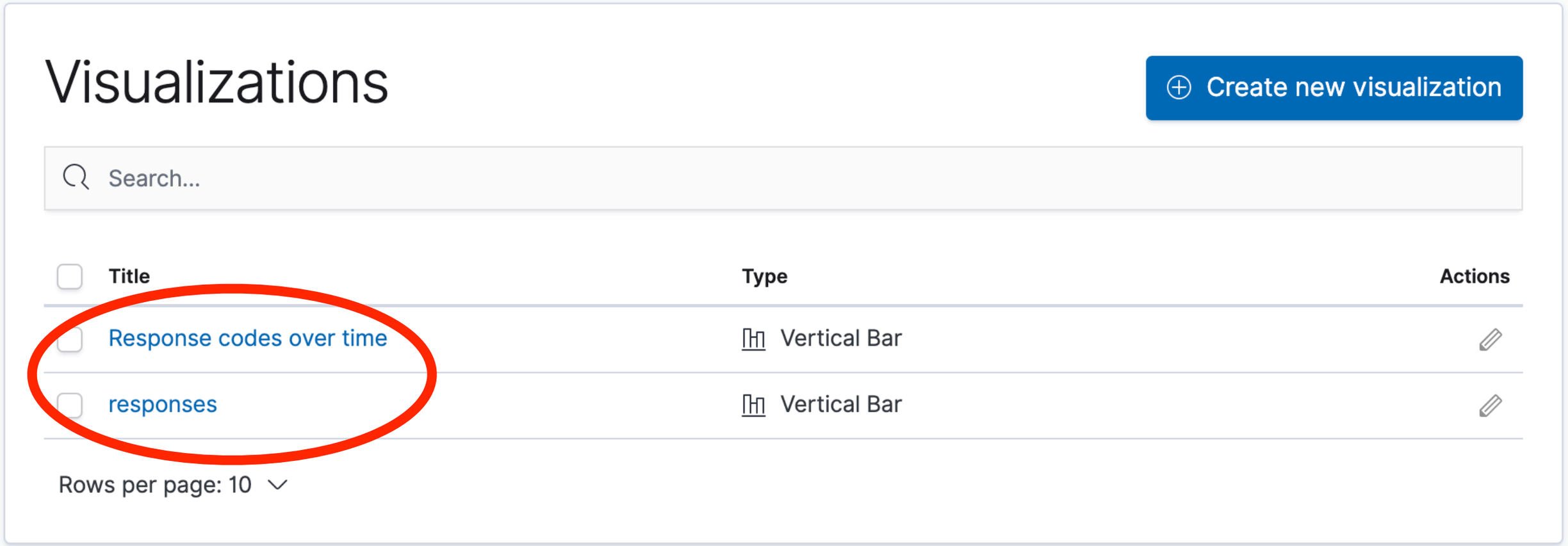
- Don't forget to save any visualizations you create; you can add them to dashboards later



elastic

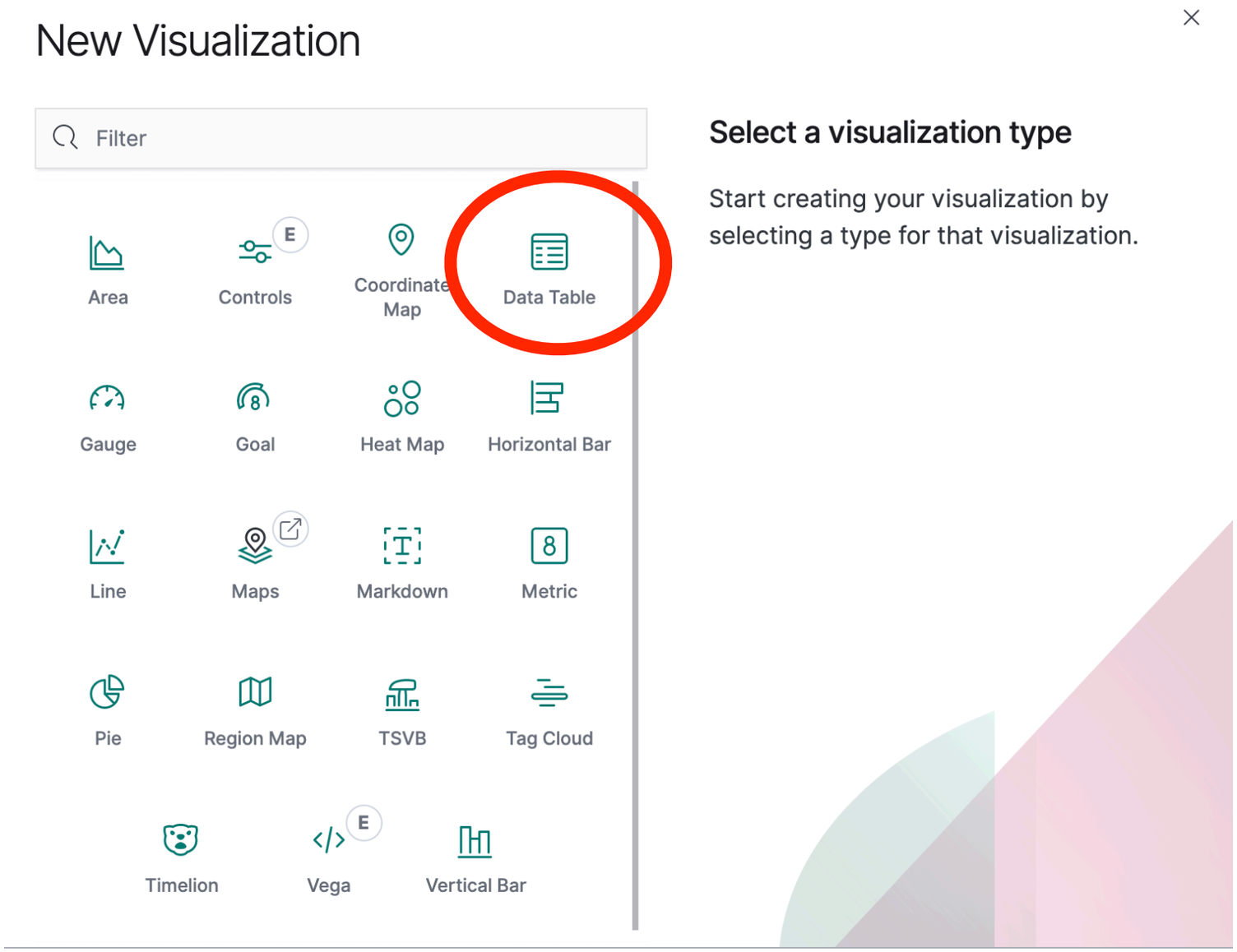
Saving visualizations

- You can be able to view saved visualizations in the next screen. As you build more, they will appear. Later, we will see how to add them to dashboards.



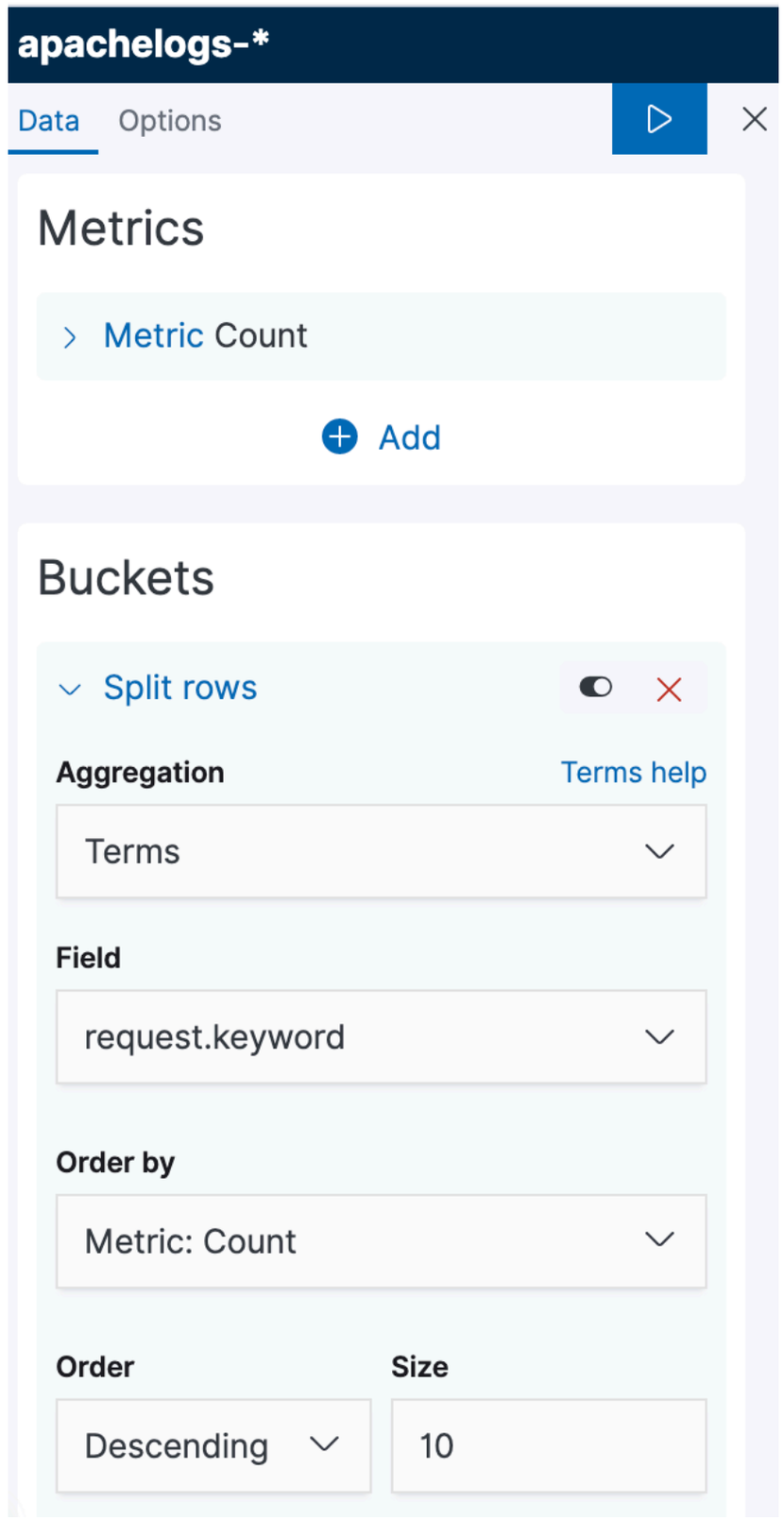
Data Tables

- Browse to the Visualization page again
- Click on the data table icon to build a "Top" terms viz



Configure data table

- Use the Count metric
- Choose to Split Rows
- Terms Aggregation
- Field: request.keyword
- Size: 10
- Click the "play" button



Top Requests

- You can now see the top request URLs
- Don't forget to save it!

request.keyword: Descending	Count
/favicon.ico	17,942
/files/logstash/logstash-1.1.0-monolithic.jar	13,290
/style2.css	12,338
/reset.css	12,237
/images/jordan-80.png	11,941
/images/web/2009/banner.png	11,676
/blog/tags/puppet?flav=rss20	10,829
/	5,912
/presentations/fpm-scale12x.pdf	4,933
/?flav=rss20	4,856

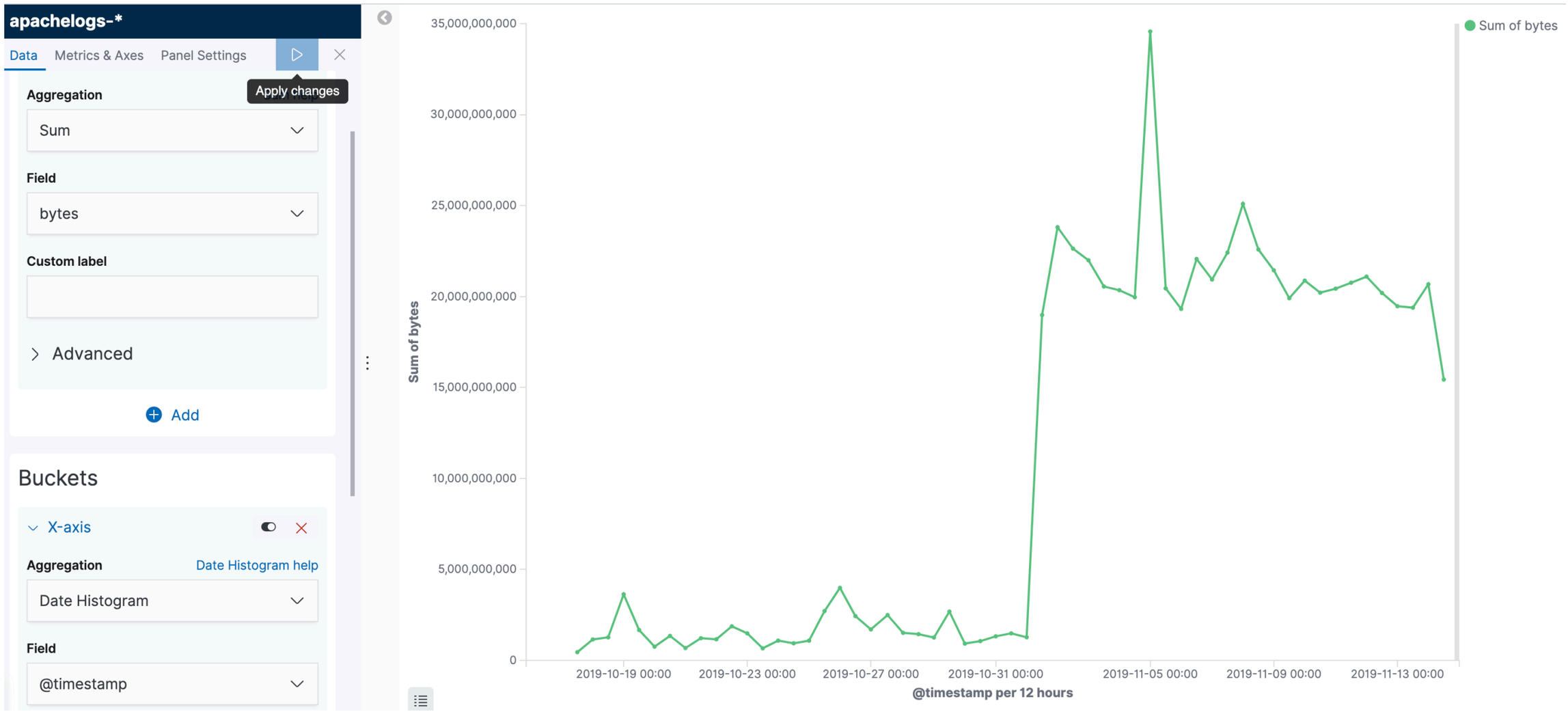
Export: Raw Formatted

Line Graph

- Let's see how the line graph visualization works
- Create a new visualization
- Select "Line Graph"
- This time, Use "Sum" Metric on the "Bytes" field
- Split the buckets on the X-Axis
- Use the Date Histogram
- Select the "@timestamp" field
- Click the Play button to render the visualization

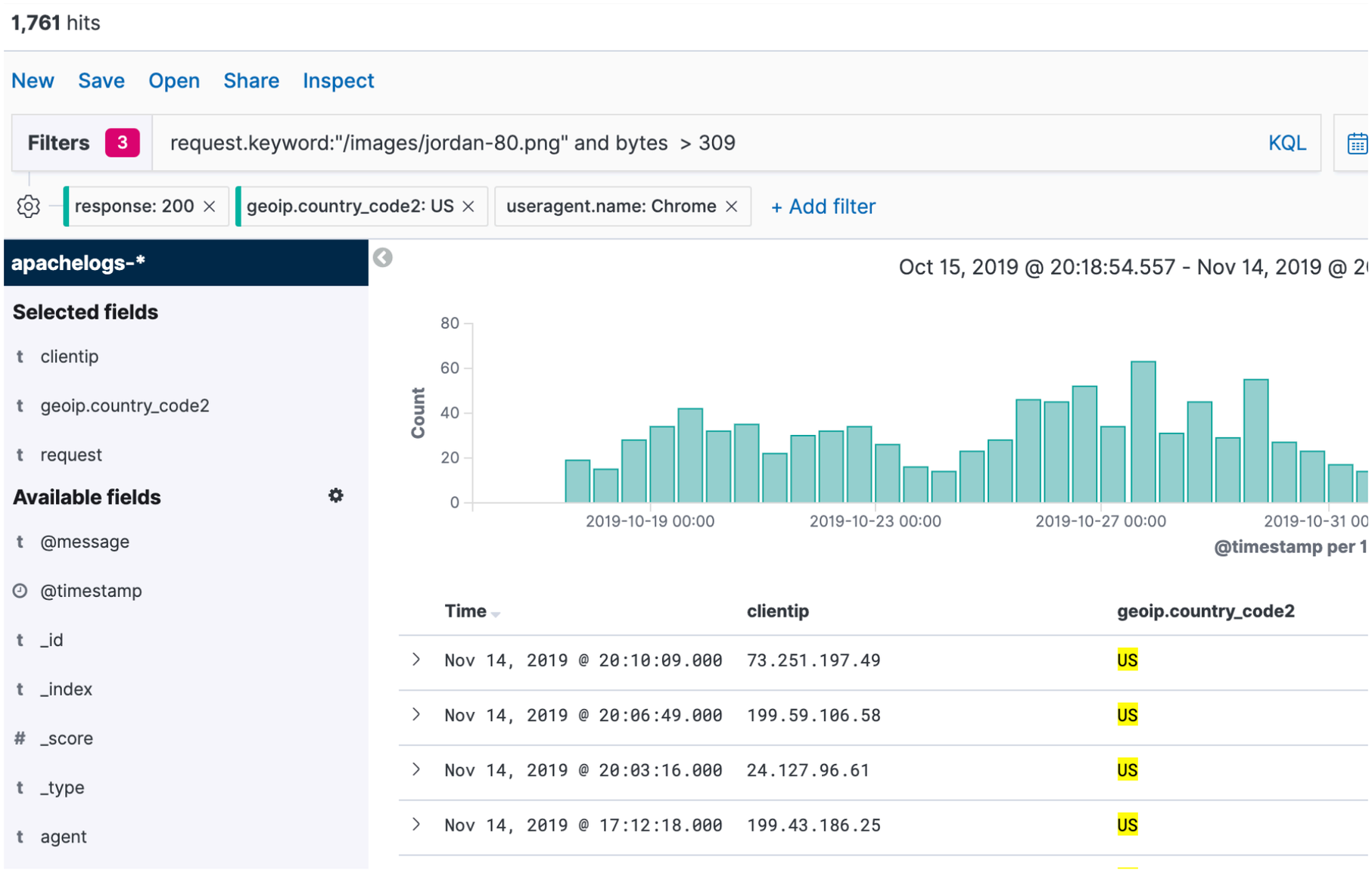
Completed Line Graph

- Should look something like this. Don't forget to save it!



Putting it all together

- Create a visualization based on a search and/or filter
- Combine with pinned filters for maximum power!



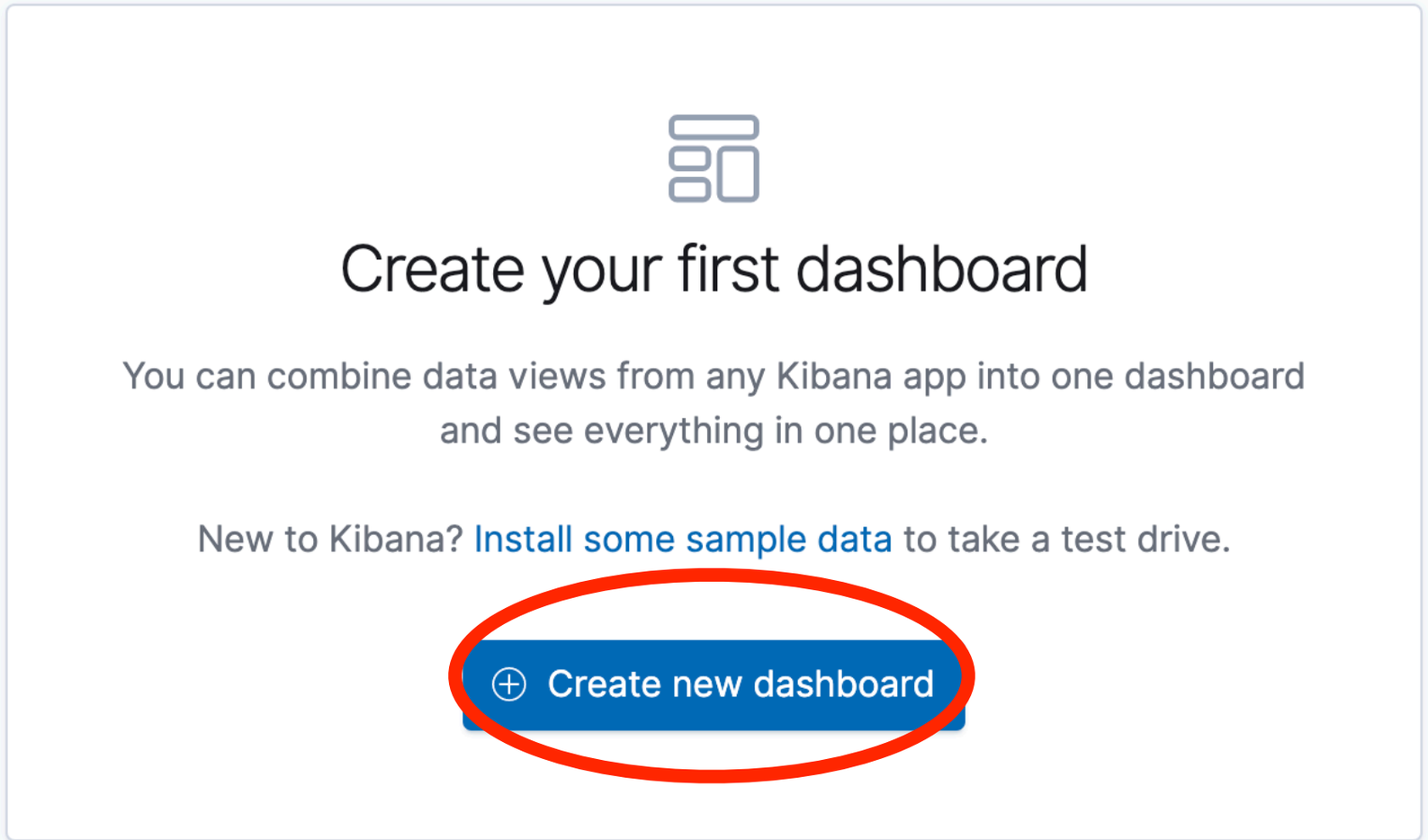
elastic

Dashboards

elastic

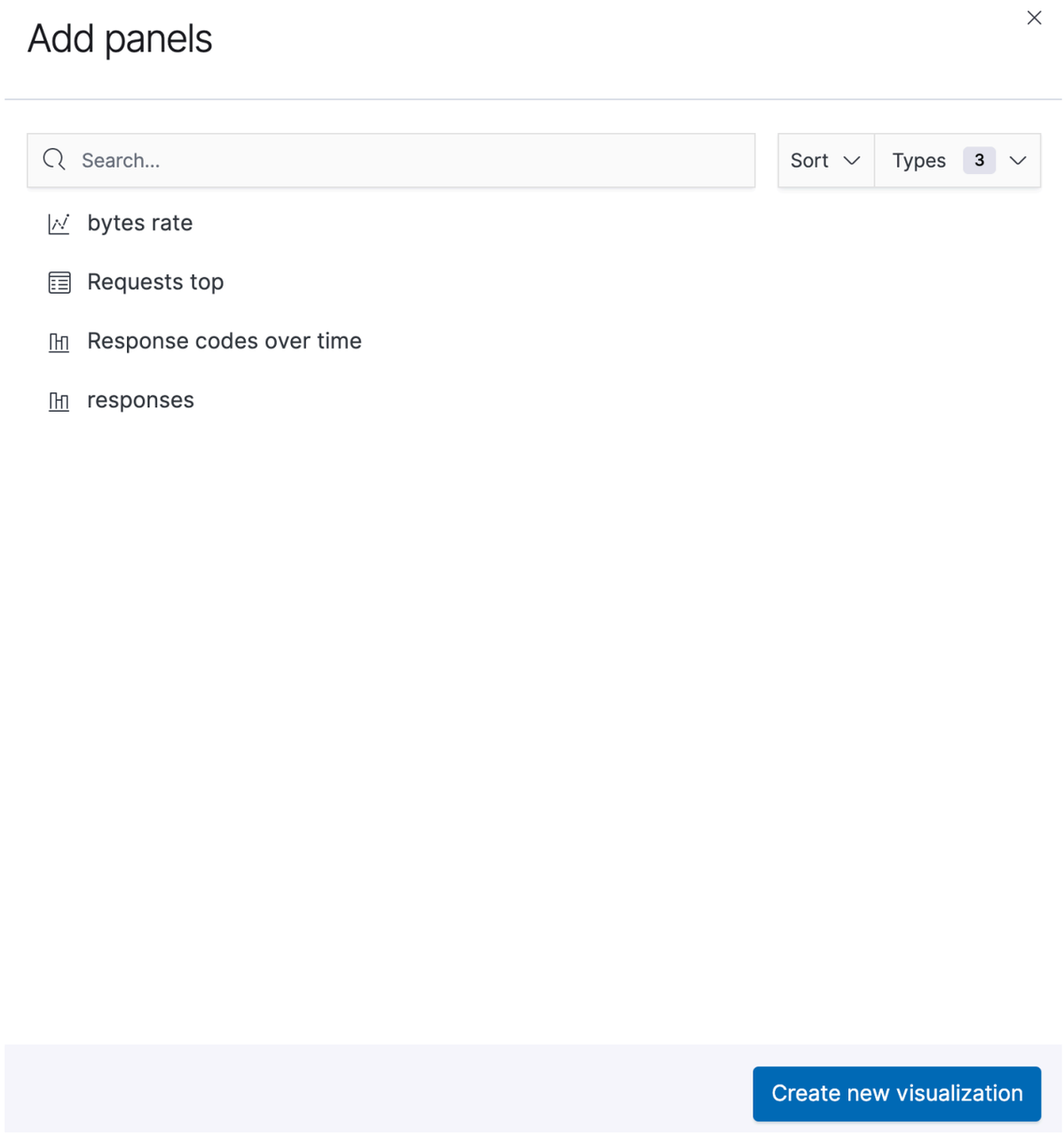
Creating Dashboards

- Select the dashboard icon in the left nav:
- Click on the "Create new dashboard" button



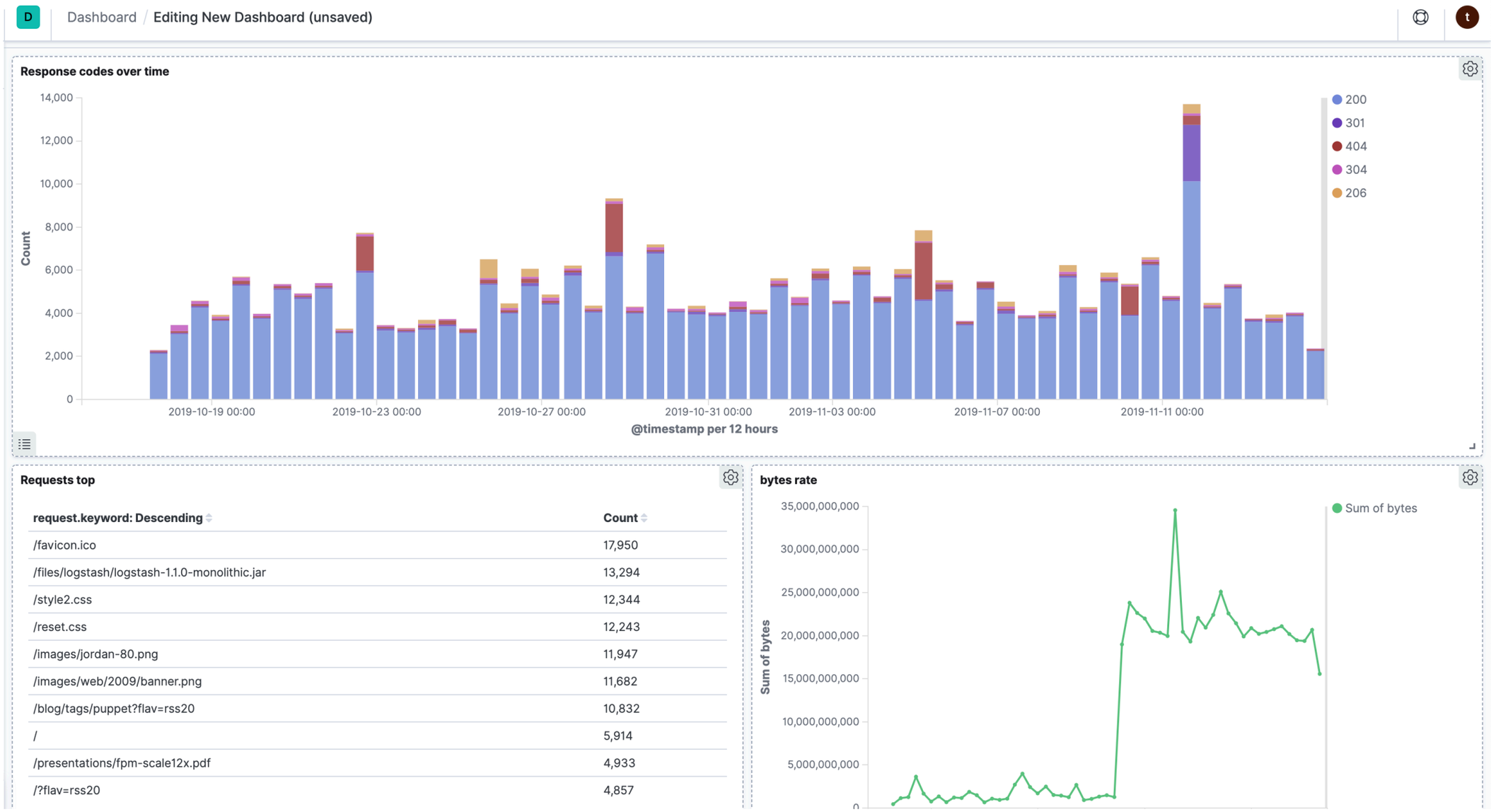
Add existing panels to a dashboard

- Simply click on the visualization name and it will be added!



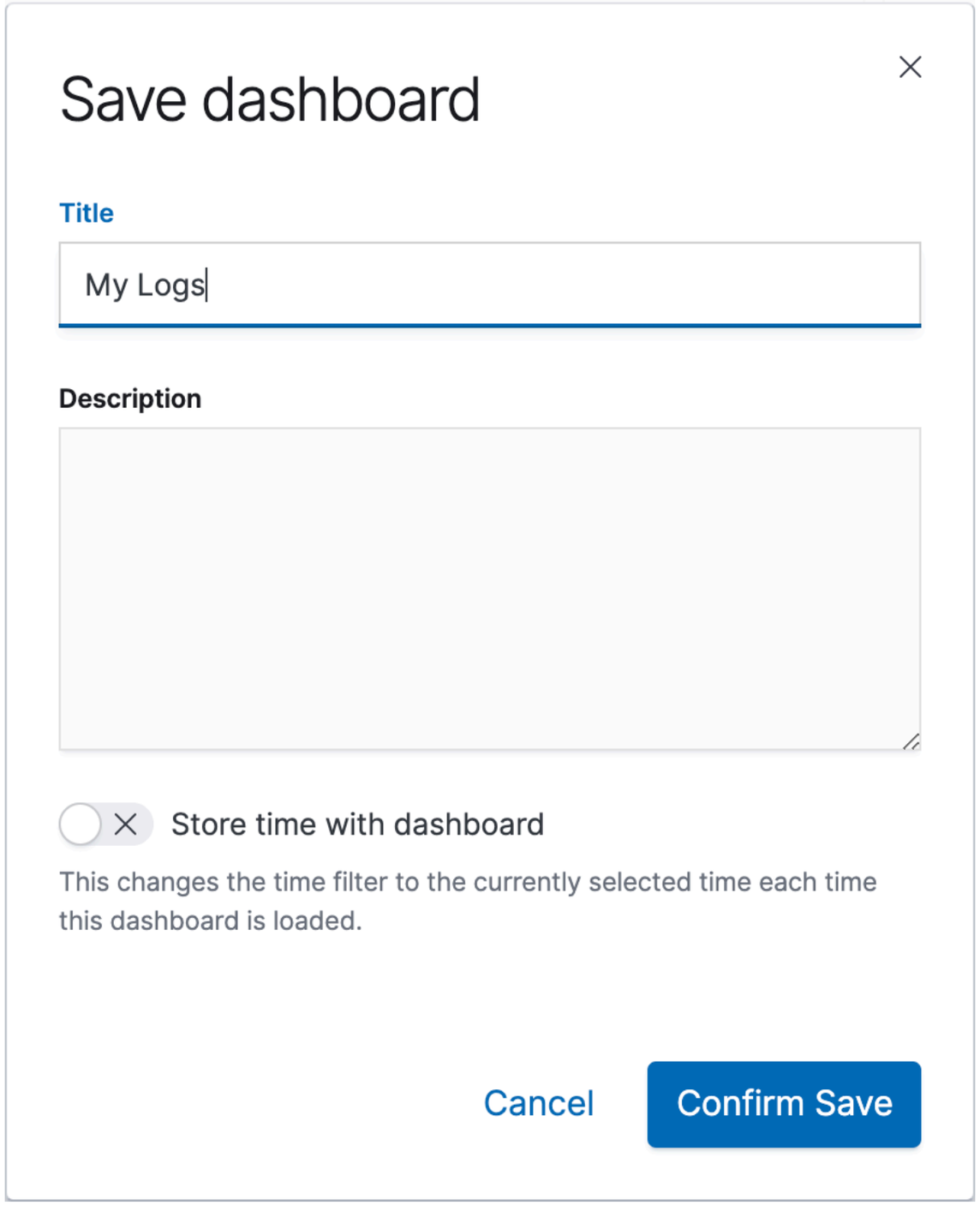
Arrange visualizations in the Dashboard

- Clicking on the title bar allows you to drag a visualization
- Clicking in the bottom right corner allows you to resize it



Save Dashboard

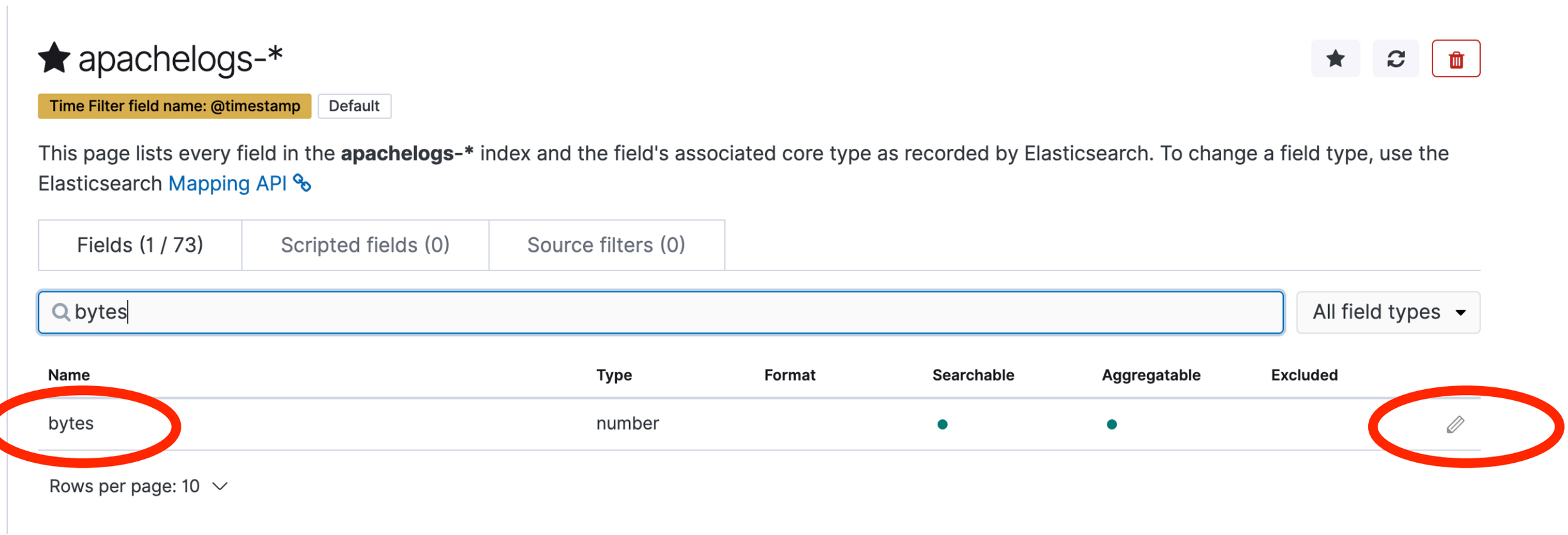
- As with all your Kibana creations, you can save dashboards



Field Formatters

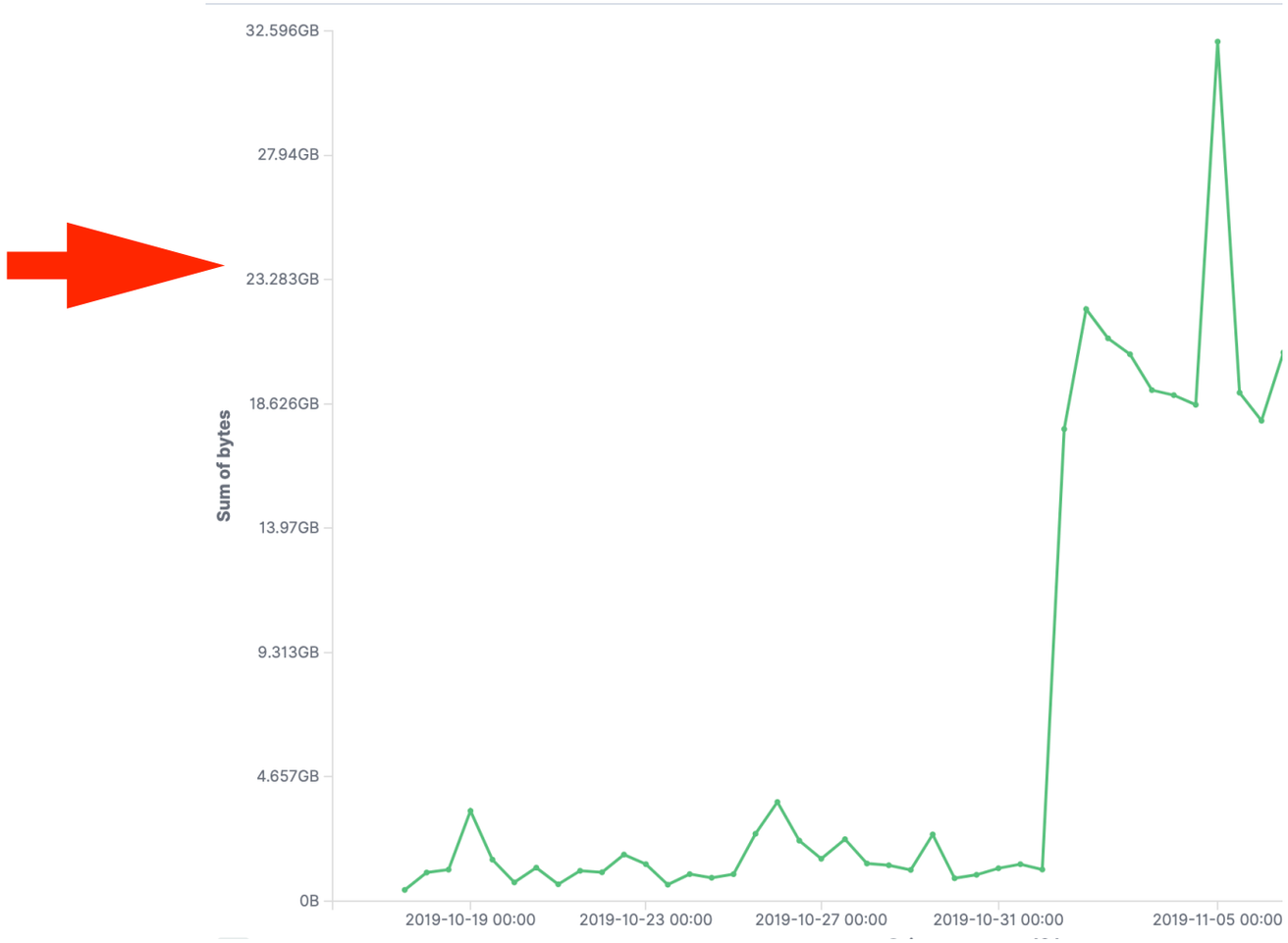
Field Formatters

- You might have noticed that the ***bytes*** values in the previous visualization looked awkward. Very large byte values are difficult for humans to read! Let's fix that.
- Browse to the Index Pattern, as shown below, and search or scroll to the ***bytes*** field in the mapping. Click Edit icon:



Field Formatters

- Select "Bytes" format
- Click "Save field"
- Browse back to visualization



Edit bytes

Type

number

Format (Default: `Number`)

Bytes

Formatting allows you to control the way that specific values are displayed. It can also cause values to be completely changed and prevent highlighting in Discover from working.

Numeral.js format pattern (Default: `0,0.[000]b`)

0,0.[000]b

Documentation

Samples

Input	Output
256	256B
1024	1KB
5150000	4.911MB
1990000000	1.853GB

Popularity

0

Save field Cancel

elastic

Lesson 2

Review - Visualizations and Dashboards

elastic

Summary

- Discover is Kibana's built-in search tool
- Use the Time Picker to select time ranges for viewing
- Customize Columnar views by adding fields
- View surrounding documents
- Lucene query syntax is the default text search
- Enabling Kibana query language allows auto-complete of field names, operators, and field values
- Searches can be saved, and visualizations can be created with searches attached

Quiz

1. **True or False:** You can create individual panels in the "Visualization" tab.
2. **True or False:** Dashboards are assembled by choosing pre-configured visualizations and simply adding them to the dashboard one-by-one.
3. **Which aggregation allows you to see "Top 10" things?**
4. **Which aggregation allows you to bucket by time period?**
5. **Which aggregation allows you calculate totals for a field?**

Lesson 2

Lab - Visualizations and Dashboards

elastic

Lesson 3

Time-Series Visualization Builder (TSVB)

elastic

Time-Series Visualization Builder

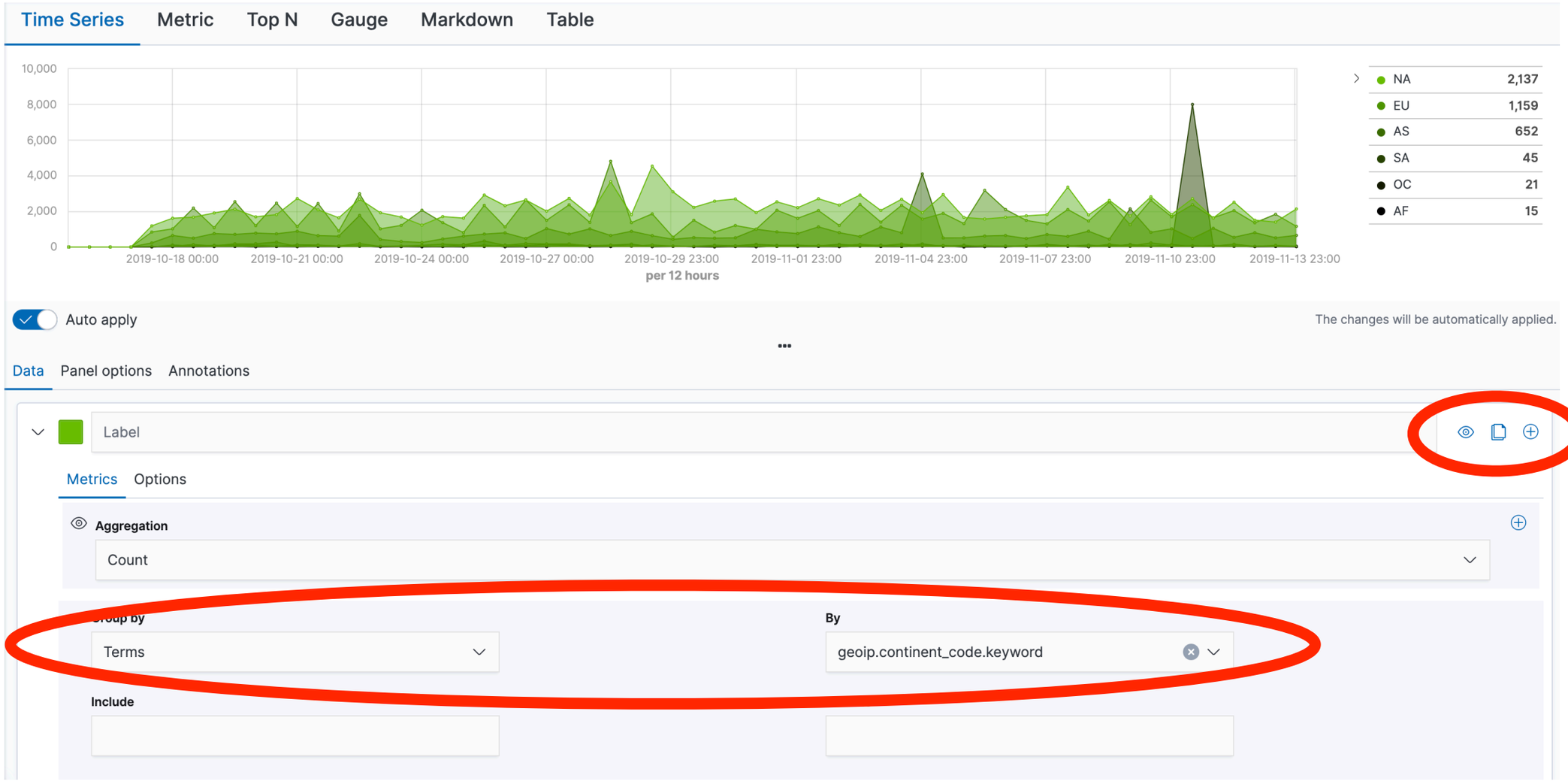
elastic

Time Series Visualization Builder

- TSVB was created especially for time series data; it's great for viewing log data
- Makes it possible to overlay multiple time series in one visualization!
- May be embedded into a Kibana dashboard just like standard visualizations
- Rich colors and customization
- Features visual annotations
- To begin, click this icon on the Create Visualization page:

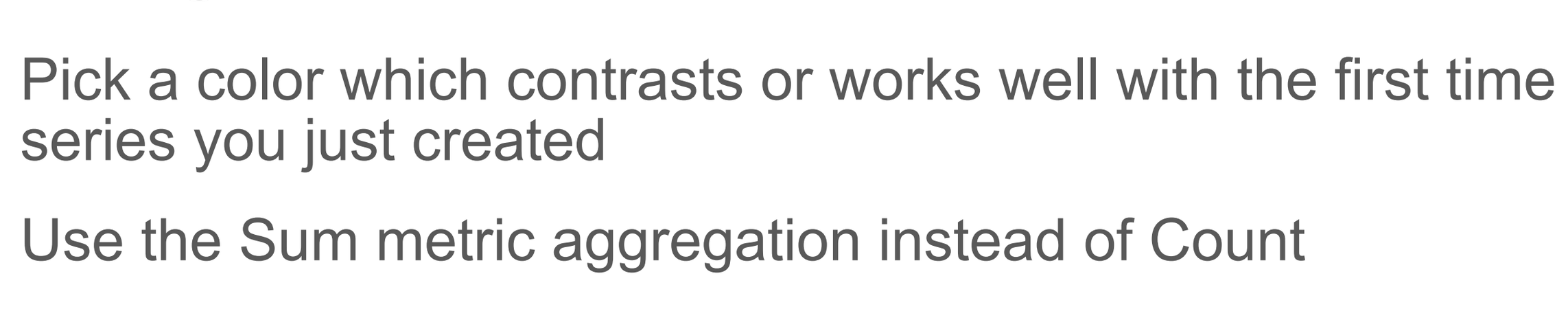
Creating a Time Series chart

- Start by selecting "Terms" to Group By. Use the geoip.continent_code.keyword field
- Then, click the plus sign on the right to add another chart



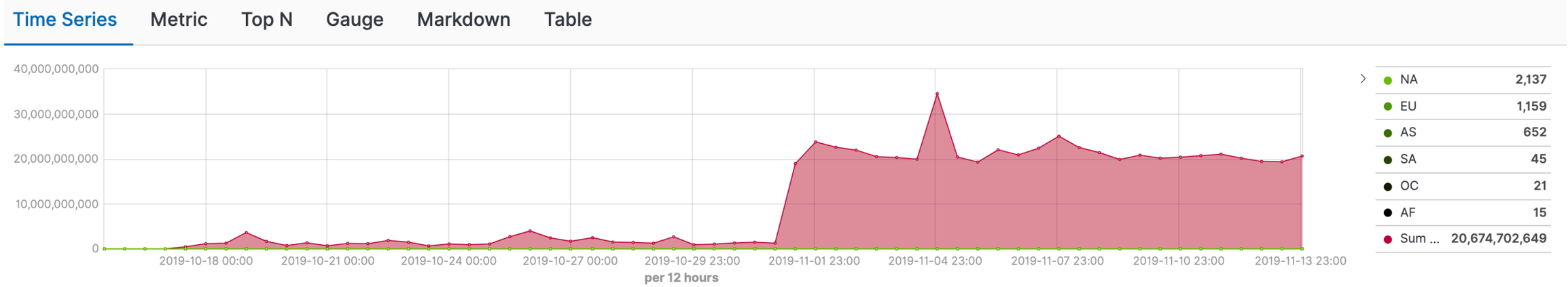
Adding the second time series

- Pick a color which contrasts or works well with the first time series you just created
- Use the Sum metric aggregation instead of Count
- Choose the ***bytes*** field
- Group by Everything
- Give it a meaningful label



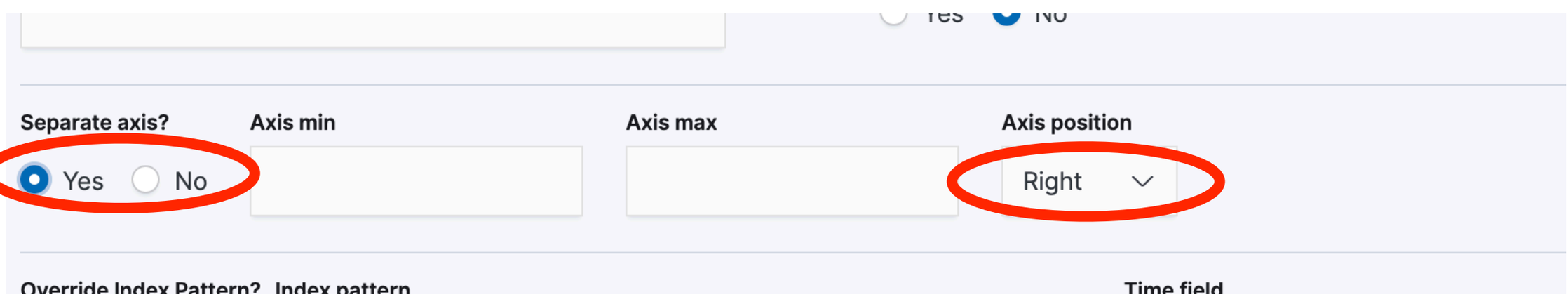
Incompatible y-axis?

- In this case, the values for the new (Sum of bytes) time series are on a completely different scale, so we can no longer view the original data



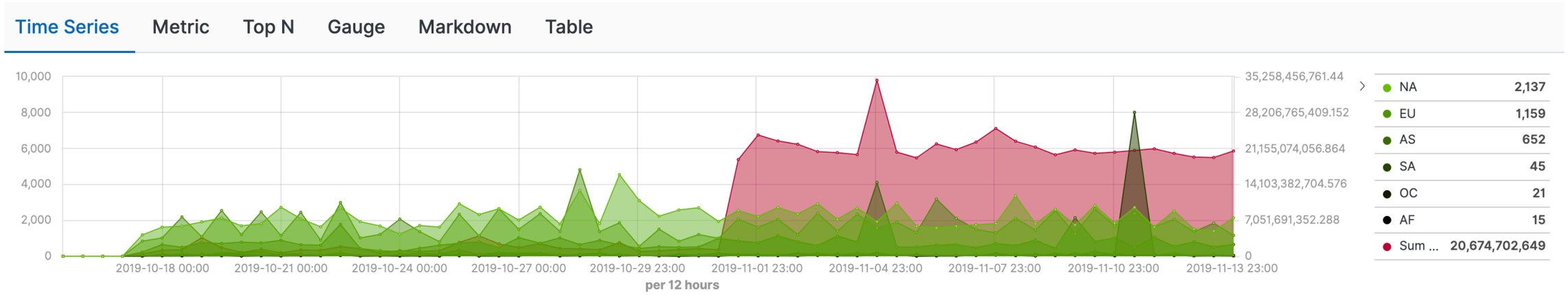
Separate Axis to the rescue!

- On the second (or any subsequent) time series, simply select the "Separate Axis" option, and a location (here we will display it to the right)



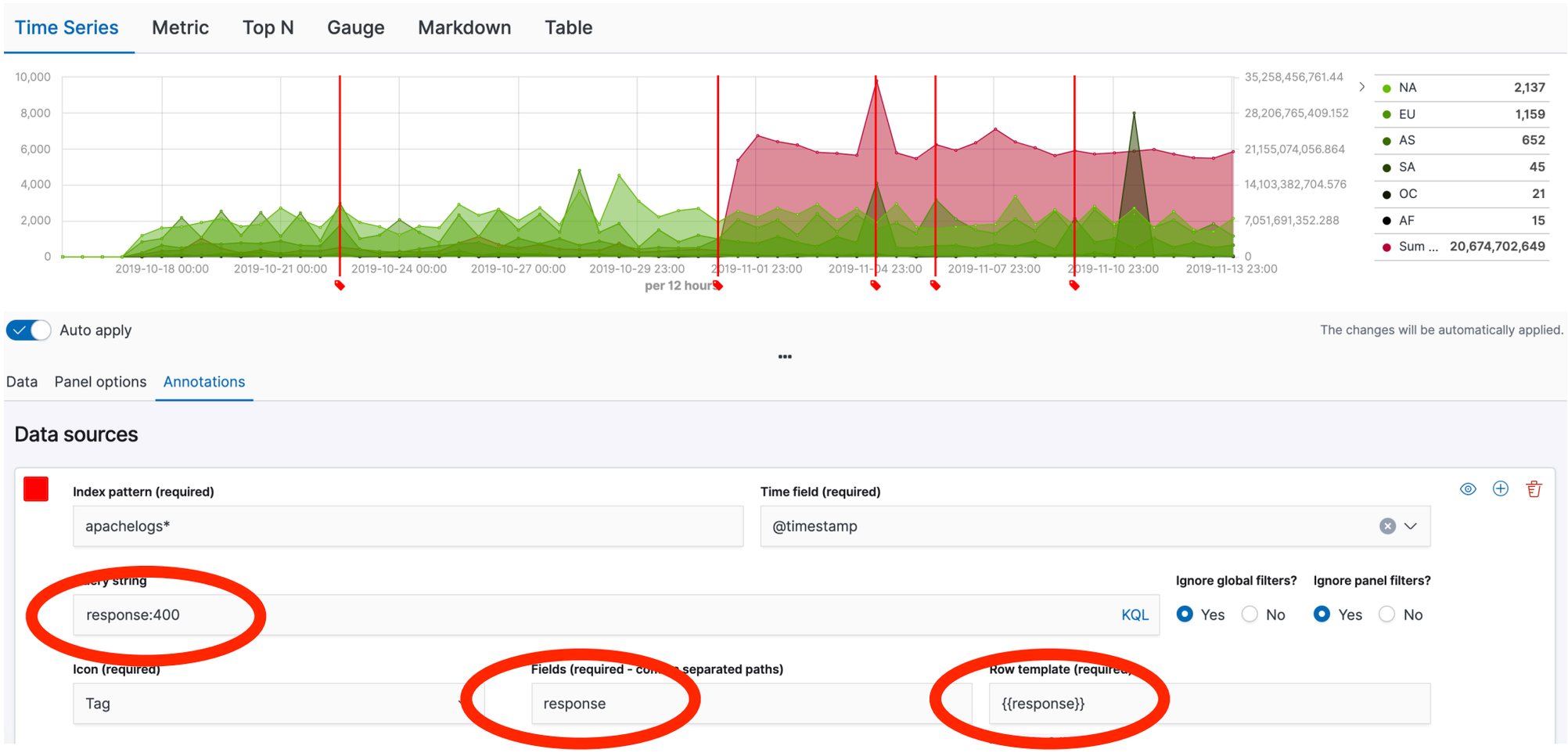
Separate Axis results

- Now we can see the first (green) time series, overlaid with the second (red) time series



Annotations in TSVB

- Annotations can be created by specifying a Query String which represents the events in Elasticsearch
- We will use "response:400"; don't forget to fill out the Fields and Row Template as shown below. Save your work!



Metrics

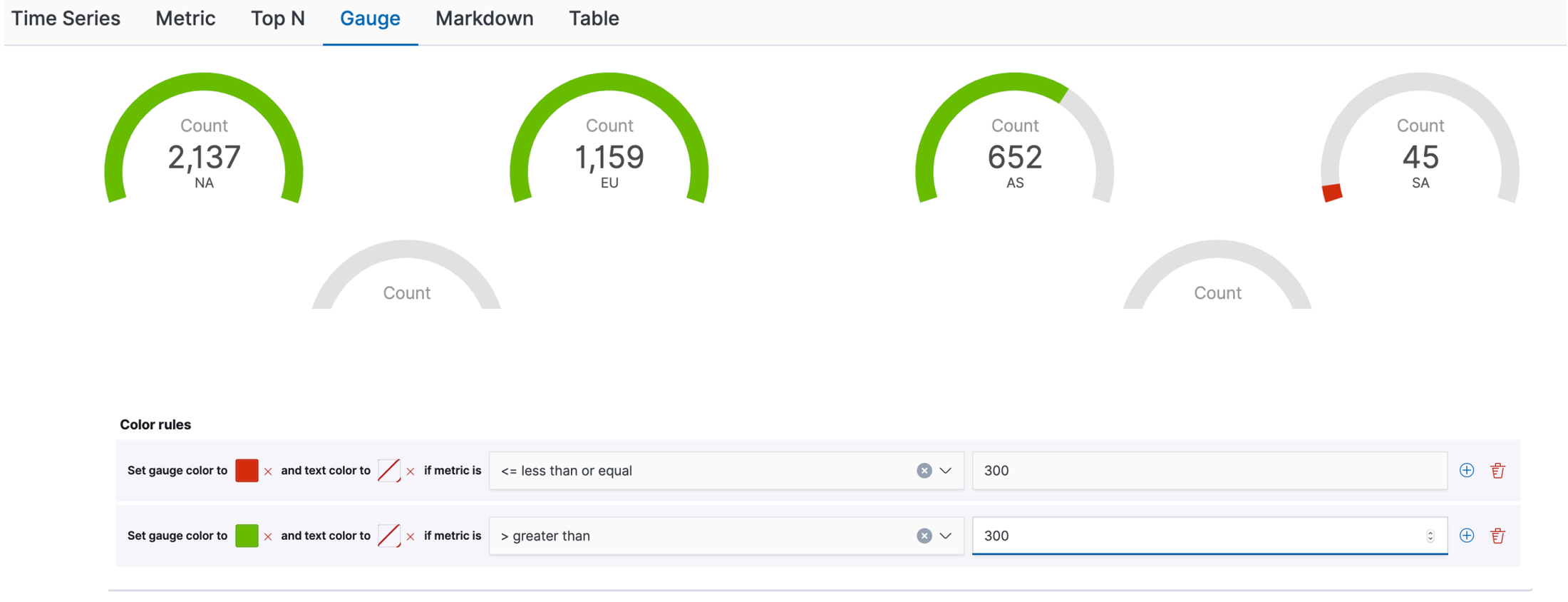
- Simple to create
- Reflects the value in the last time bucket. Therefore, if you do not have recent data, the value could be 0!

Count

356

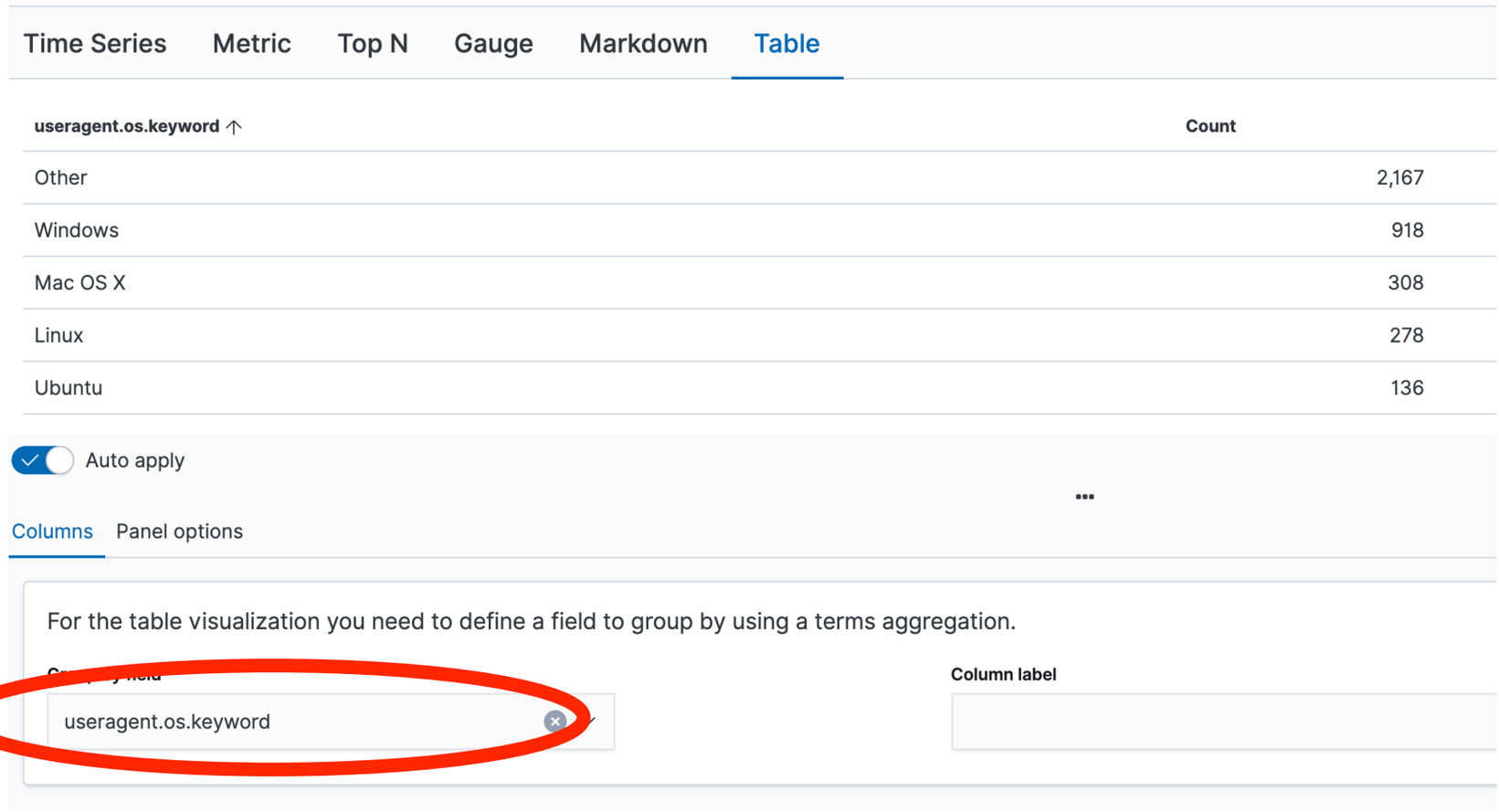
Gauges

- Gauges measure against a defined goal
- Set the "Gauge Max" value if desired
- Set gauge colors based on data values and conditionals



Tables

- Similar to Data Tables in Kibana
- Just pick the Group By field and number of Rows
- You may also specify different Metric aggs to display



Lesson 3

Review - Time-Series Visualization Builder

elastic

Summary

- Time-Series Visualization Builder (TSVB) was designed to work best with time series data
- Multiple time series can be overlaid in one visualization
- Options include Time Series, Metric, Gauge, Table

Quiz

1. **True or False:** Time Series Visual Builder is excellent for displaying log data
2. **True or False:** You should create one panel per time series, and display them one above another on the dashboard page
3. **True or False:** TSVB allows you to choose multiple color palettes in one visualization
4. What should you do if you overlay two visualizations with y-axis values on very different scales?

Lesson 3

Lab - Time-Series Visualization Builder

elastic

Quiz Answers

elastic

Kibana Fundamentals

1. False (usually). You must configure index patterns. (ML does have some advanced log detection algos)
2. True
3. Pinning filters
4. True
5. Time Picker
6. Lucene Query Syntax and Kibana Query Language
7. True

Visualizations and Dashboards

1. True
2. True
3. Terms bucket aggregation
4. Date Histogram bucket aggregation
5. Sum metric aggregation

Time-Series Visualization Builder (TSVB)

1. True
2. False, you can overlay them
3. True
4. Use "Separate Axis"