Exercises

Download and start elasticsearch

- Download elasticsearch from http://elastic.co
- Unpack
- Start elasticsearch using bin/elasticsearch.bat
- See that it started by accessing http://localhost:9200

Download and start Kibana

- Download Kibana from http://elastic.co
- Unpack
- Start Kibana using bin/kibana.bat
- Access the console on http://localhost:5601

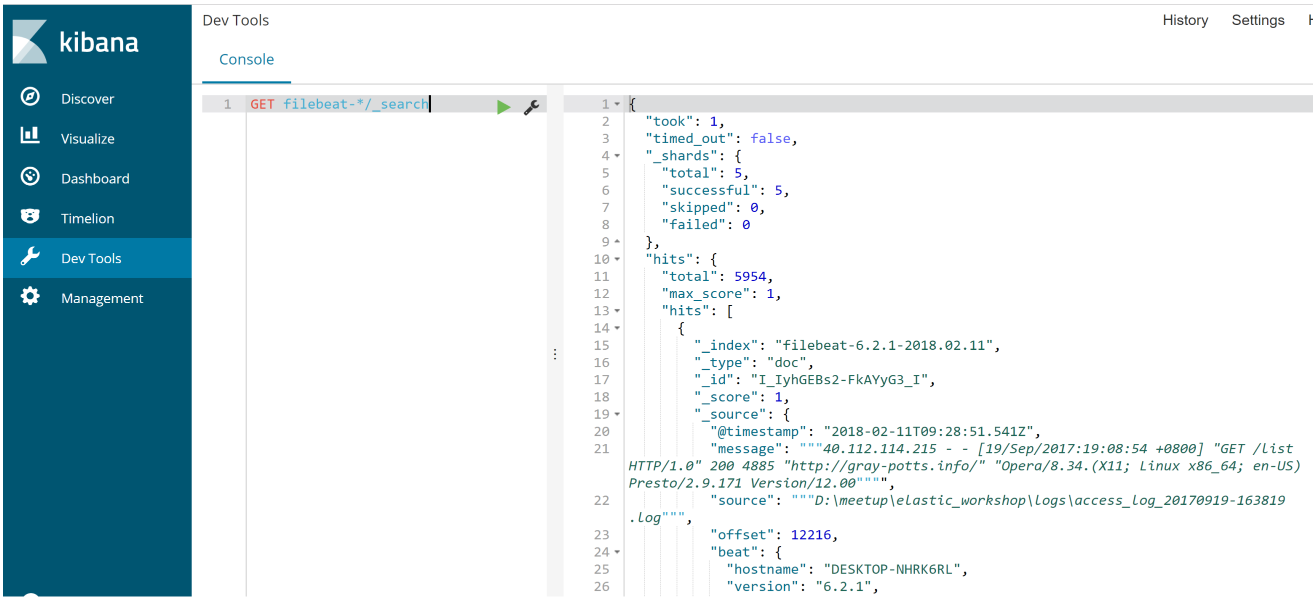
Configure Filebeat to read access log

- Download filebeat for your OS from http://elastic.co
- Unpack
- Configure in `filebeat.yml`
    - prospector path pointing to your file
    - if necessary configure elasticsearch output
- Run filebeat

```
filebeat.exe -c filebeat.yml
```

- Make sure the log events are in elasticsearch. In DevTools submit the request:

```
GET /filebeat-*/_search
```



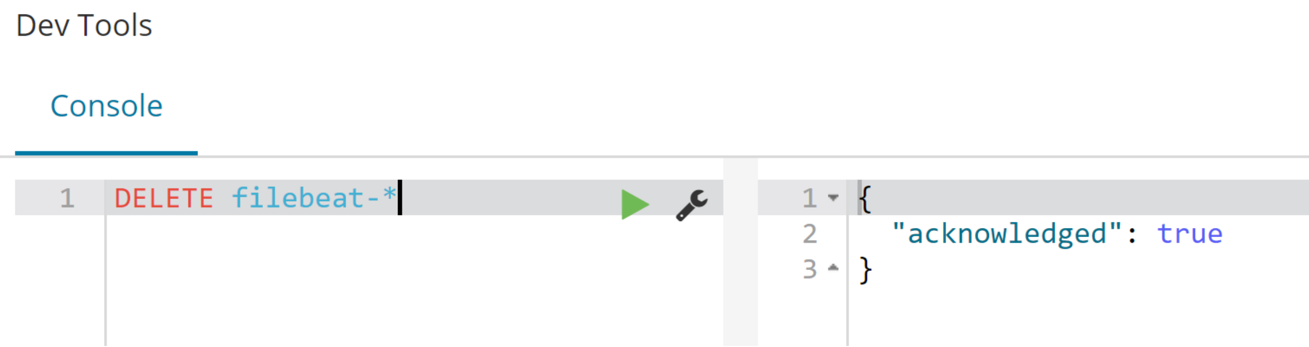
```
GET filebeat-*/_search
```

```
{
  "took": 1,
  "timed_out": false,
  "_shards": {
    "total": 5,
    "successful": 5,
    "skipped": 0,
    "failed": 0
  },
  "hits": {
    "total": 5954,
    "max_score": 1,
    "hits": [
      {
        "_index": "filebeat-6.2.1-2018.02.11",
        "_type": "doc",
        "_id": "I_IyhGEBs2-FkAYyG3_I",
        "_score": 1,
        "_source": {
          "@timestamp": "2018-02-11T09:28:51.541Z",
          "message": """40.112.114.215 - - [19/Sep/2017:19:08:54 +0800] "GET /list HTTP/1.0" 200 4885 "http://gray-potts.info/" "Opera/8.34.(X11; Linux x86_64; en-US) Presto/2.9.171 Version/12.00"""",
          "source": """D:\meetup\elastic_workshop\logs\access_log_20170919-163819.log""",
          "offset": 12216,
          "beat": {
            "hostname": "DESKTOP-NHRK6RL",
            "version": "6.2.1",
```

- See the structure of the events

Configure Logstash

- Stop the filebeat process
- Delete the registry file in the beats data dir (data/registry for .tar.gz and .zip, /var/lib/filebeat/registry for DEB and RPM packages)
- Delete the filebeat-* index in elasticsearch (in DevTools: DELETE filebeat-*)



```
DELETE filebeat-*
```

```
{
  "acknowledged": true
}
```

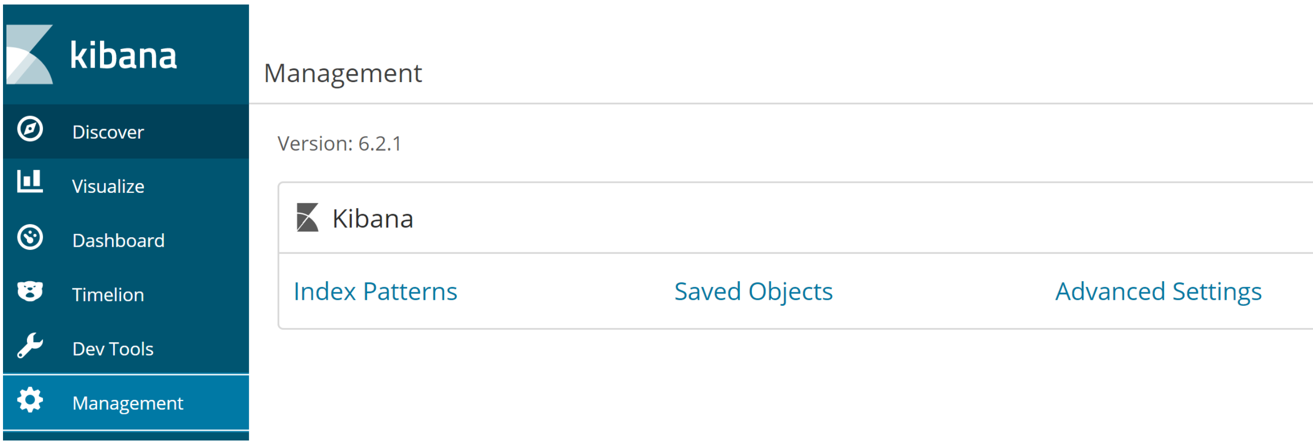
- Create a logstash configuration that pipes the logs to elasticsearch
    - Filters: One grok filter for COMBINEDAPACHELOG
- Configure filebeat output to send events to Logstash
- Start logstash

```
logstash.bat -f logstash.conf
```

- Start filebeat
- Check the structure of the documents in Kibana

Kibana

- Create an index pattern for filebeat-*

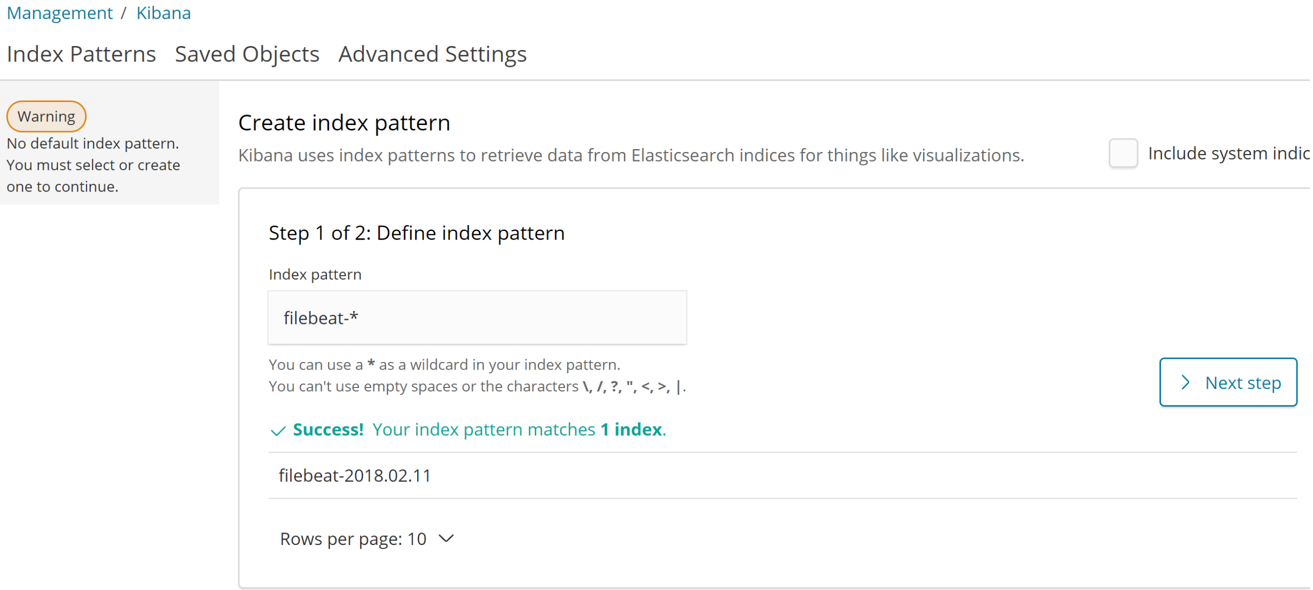


Management

Version: 6.2.1

Kibana

Index Patterns   Saved Objects   Advanced Settings



Management / Kibana

Index Patterns   Saved Objects   Advanced Settings

Warning
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 indic

Step 1 of 2: Define index pattern

Index pattern

filebeat-*

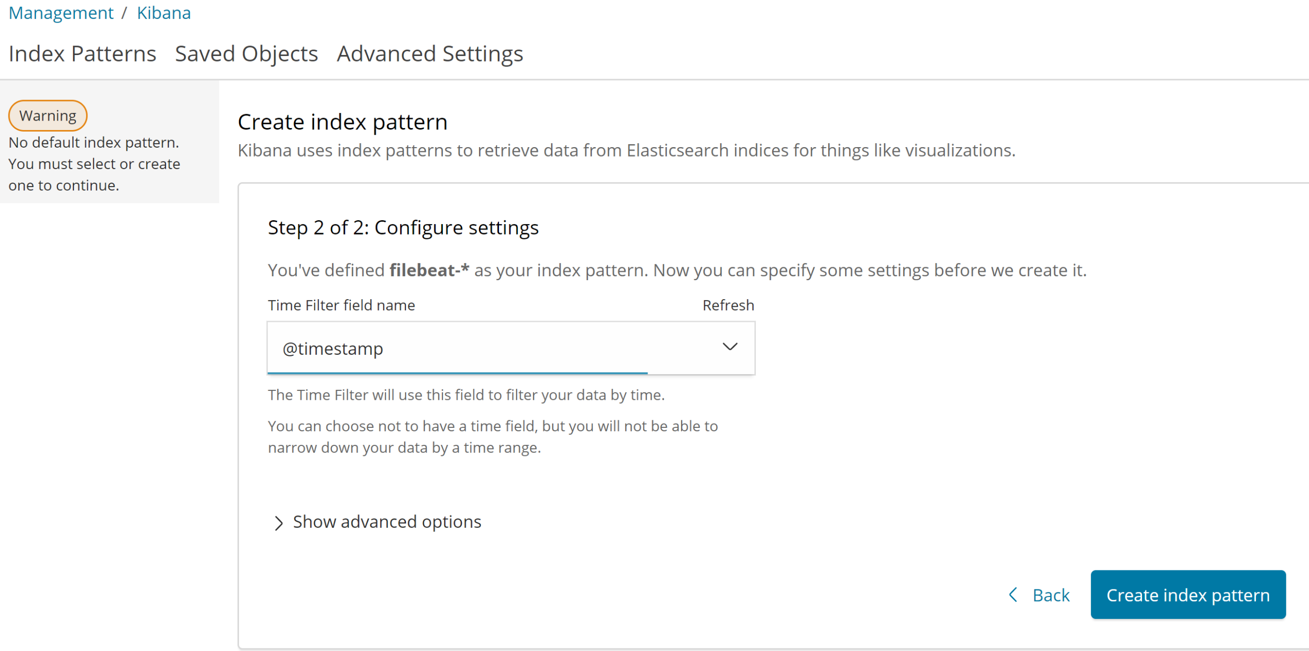
You can use a * as a wildcard in your index pattern.
You can't use empty spaces or the characters \, /, ?, ", <, >, |.

> Next step

✓ **Success!** Your index pattern matches **1 index**.

filebeat-2018.02.11

Rows per page: 10



Management / Kibana

Index Patterns   Saved Objects   Advanced Settings

Warning
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.

Step 2 of 2: Configure settings

You've defined **filebeat-*** as your index pattern. Now you can specify some settings before we create it.

Time Filter field name   Refresh

@timestamp

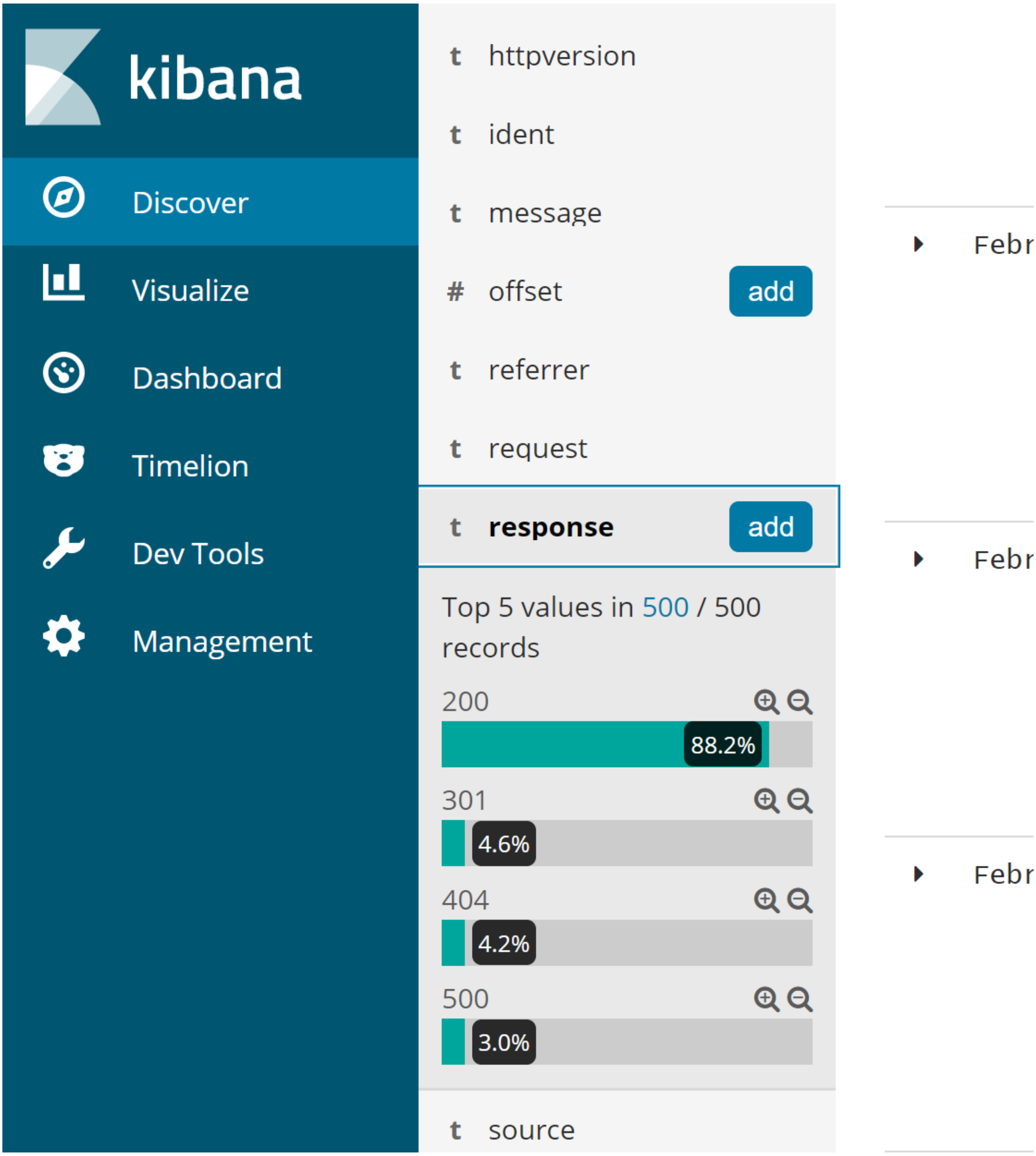
The Time Filter will use this field to filter your data by time.

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

- Using Discover, filter the documents to display only the 404 responses.



t httpversion

t ident

t message

offset

t referrer

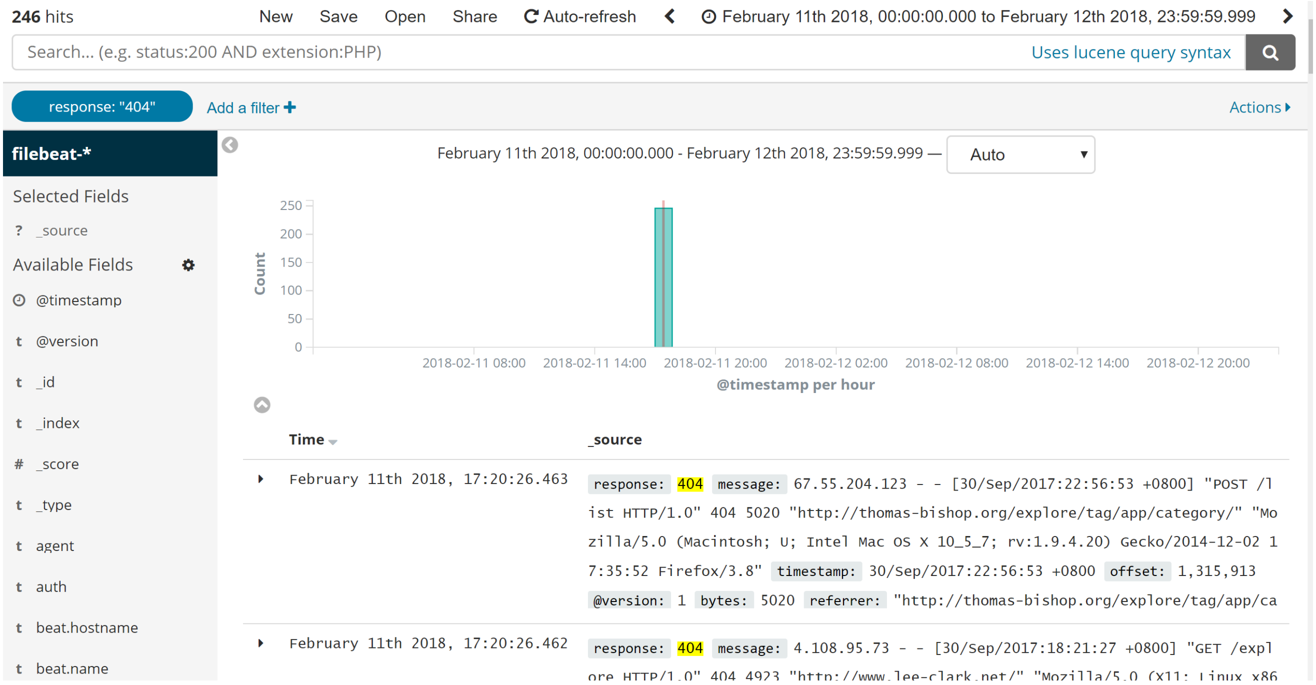
t request

t **response**

Top 5 values in 500 / 500 records

200	88.2%
301	4.6%
404	4.2%
500	3.0%

t source

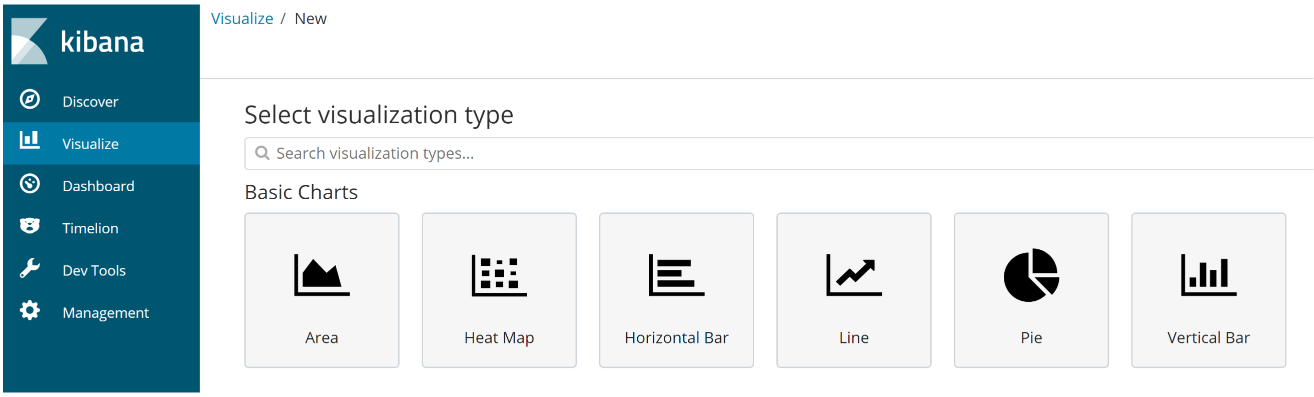


response: "404"

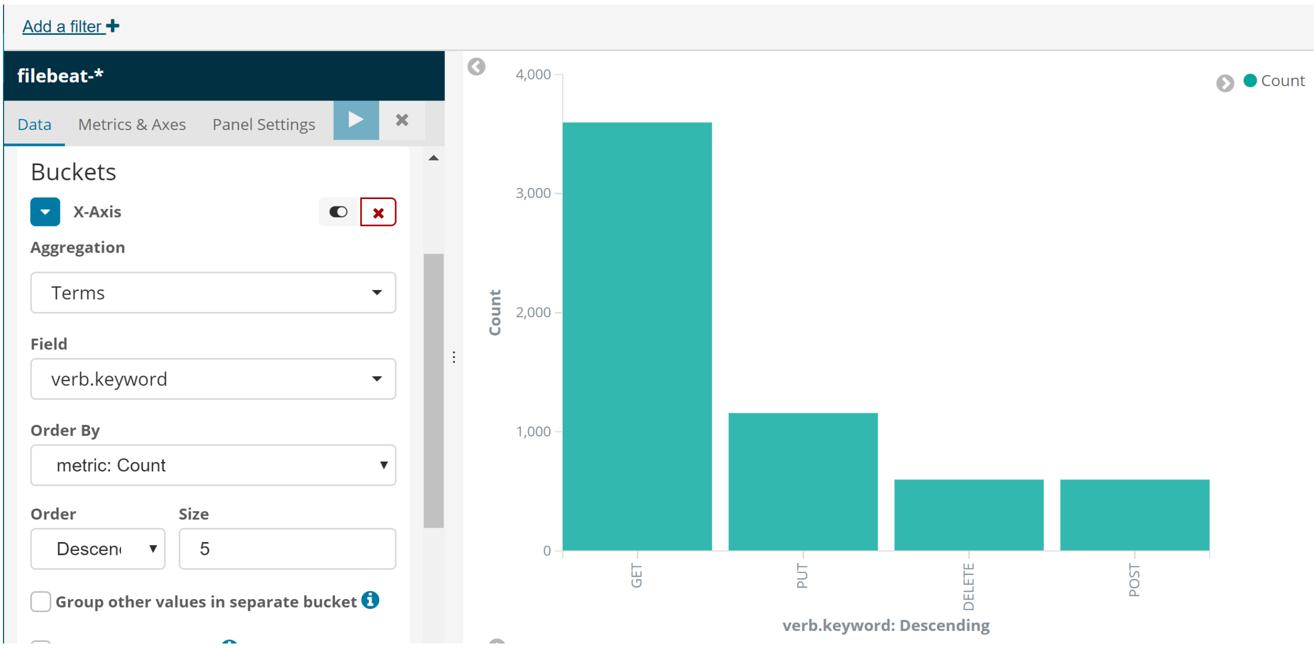
```
February 11th 2018, 17:20:26.463   response: 404 message: 67.55.204.123 - - [30/Sep/2017:22:56:53 +0800] "POST /l
                                   ist HTTP/1.0" 404 5020 "http://thomas-bishop.org/explore/tag/app/category/" "Mo
                                   zilla/5.0 (Macintosh; U; Intel Mac OS X 10_5_7; rv:1.9.4.20) Gecko/2014-12-02 1
                                   7:35:52 Firefox/3.8" timestamp: 30/Sep/2017:22:56:53 +0800 offset: 1,315,913
                                   @version: 1 bytes: 5020 referrer: "http://thomas-bishop.org/explore/tag/app/ca

February 11th 2018, 17:20:26.462   response: 404 message: 4.108.95.73 - - [30/Sep/2017:18:21:27 +0800] "GET /expl
                                   ore HTTP/1.0" 404 4923 "http://www.lee-clark.net/" "Mozilla/5.0 (X11; Linux x86
```

- Create a new visualization
- Select bar chart



- Display the count of documents per Verb



Aggregation: Terms

Field: verb.keyword

Order By: metric: Count

Order: Descen

Size: 5

□ Group other values in separate bucket