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
- Test that it can connect to elasticsearch by issuing the request GET /

Configure beat 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 Kibana console issue:

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

- See the structure of the events

Configure Logstash

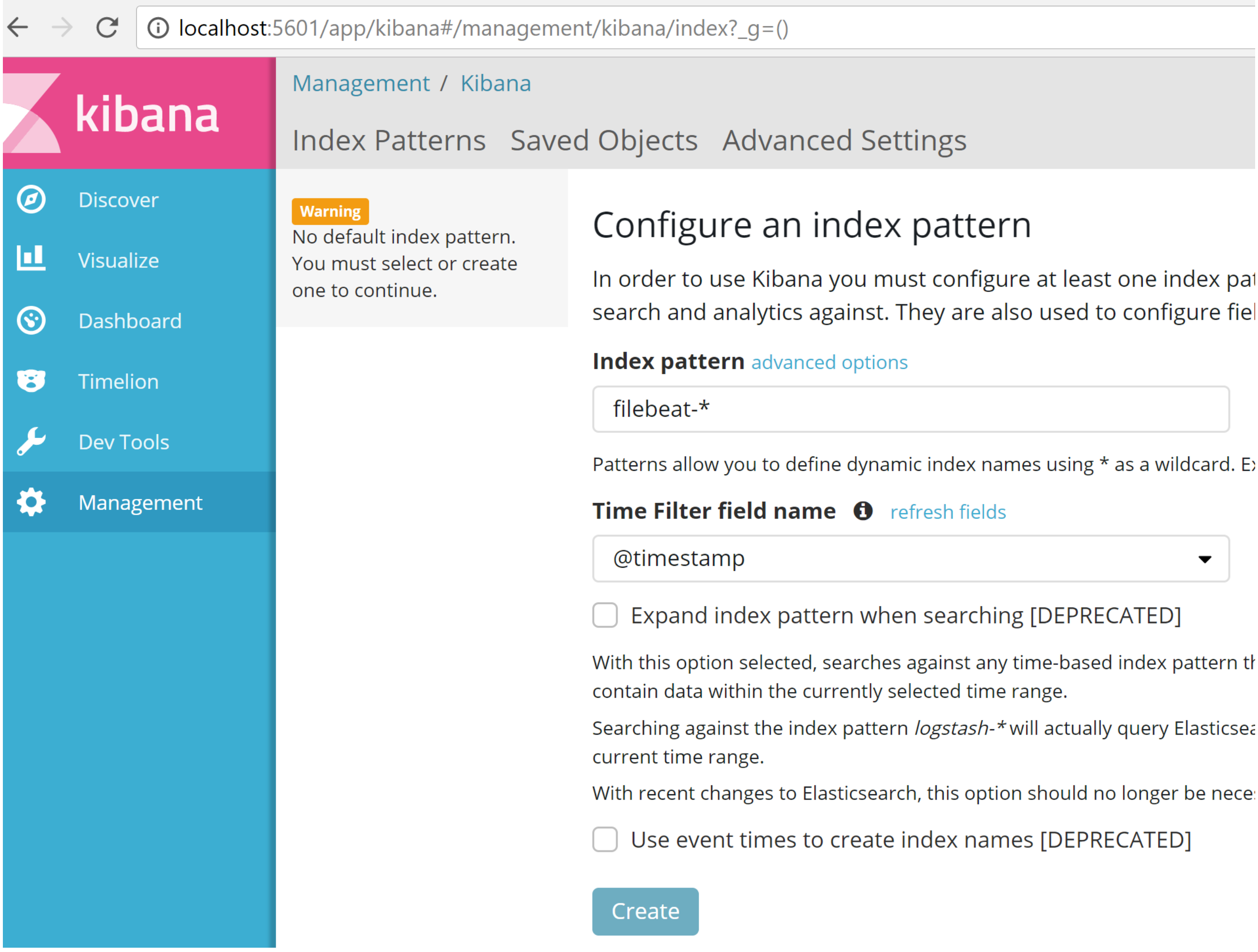
- Stop the filebeat process
- Delete the registry file in the beats data dir (data/registry for .tar.gz, /var/lib/filebeat/registry for DEB and RPM packages, c:\ProgramData\filebeat\registry for the Windows zip file)
- Delete the filebeat-* index in elasticsearch (in Kibana console: DELETE filebeat-*)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



Warning
No default index pattern. You must select or create one to continue.

Configure an index pattern

In order to use Kibana you must configure at least one index pat
search and analytics against. They are also used to configure fiel

Index pattern advanced options

filebeat-*

Patterns allow you to define dynamic index names using * as a wildcard. E›

Time Filter field name refresh fields

@timestamp

□ Expand index pattern when searching [DEPRECATED]

With this option selected, searches against any time-based index pattern th
contain data within the currently selected time range.

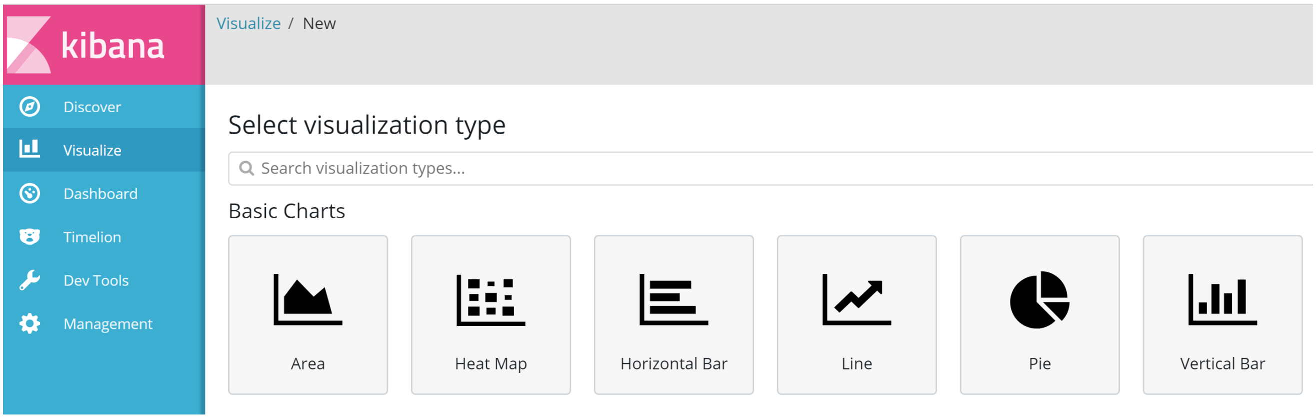
Searching against the index pattern *logstash-** will actually query Elasticsea
current time range.

With recent changes to Elasticsearch, this option should no longer be nece

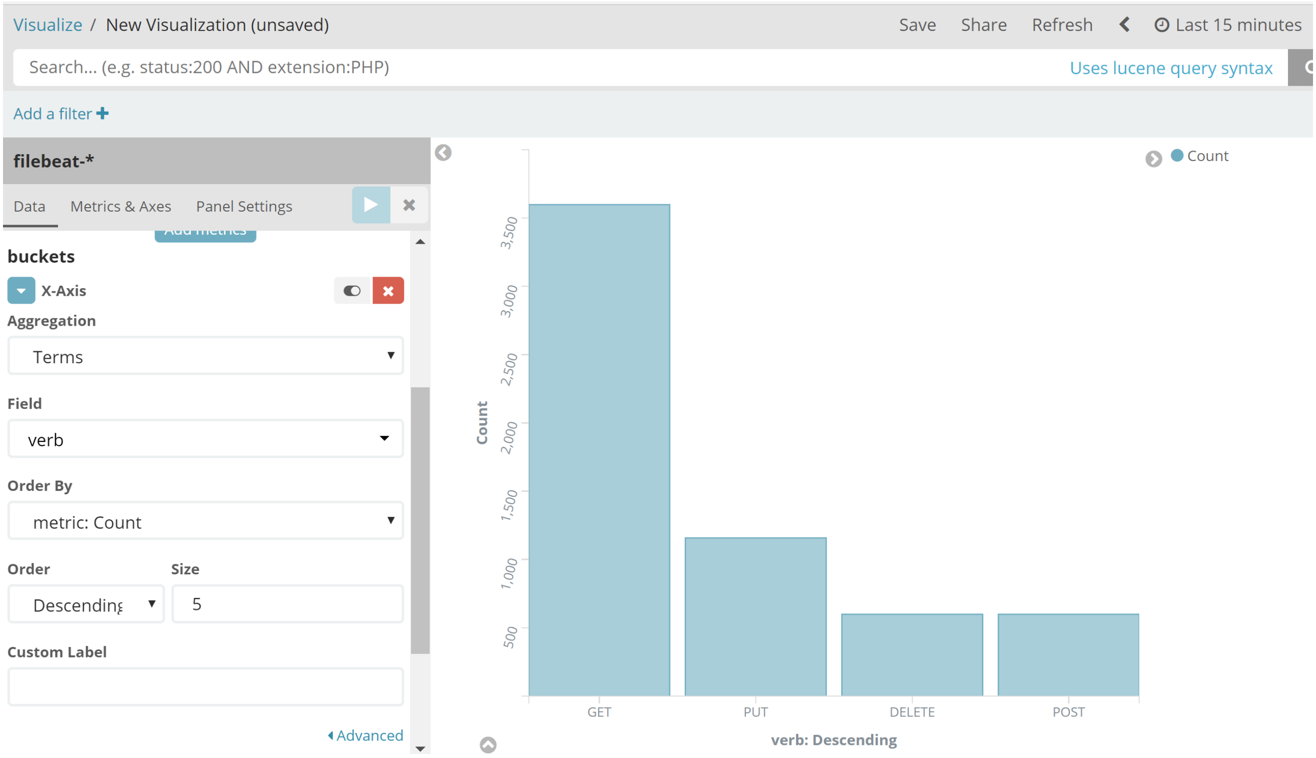
□ Use event times to create index names [DEPRECATED]

Create

- Check the distribution of events across time (you might have to adjust the date picker in the top right)
- Search for all resources that have a status of 404 (in the query bar: status:404)
- Create a new visualization
- Select bar chart



- Display the count of documents per Verb



buckets

X-Axis

Aggregation: Terms

Field: verb

Order By: metric: Count

Order: Descending

Size: 5

Custom Label: