Awesome Monitoring Infrastructure Using the Elastic Stack

Mark Walkom @warkolm
Karen Carcamo @karencfv
www.elastic.co

LCA
LINUX.CONF.AU
21-25 January
2019
Christchurch, NZ

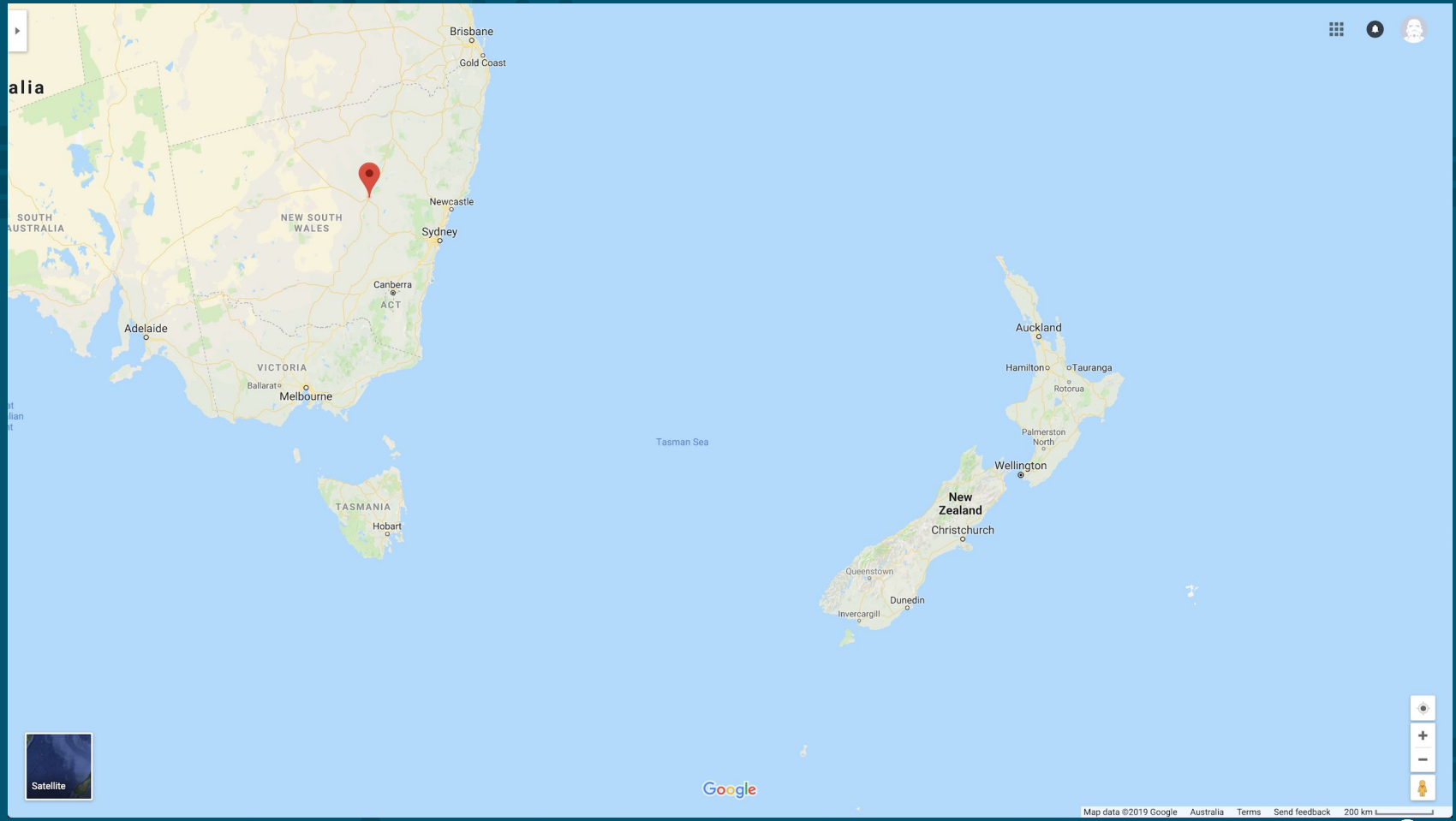
Please install Docker :)

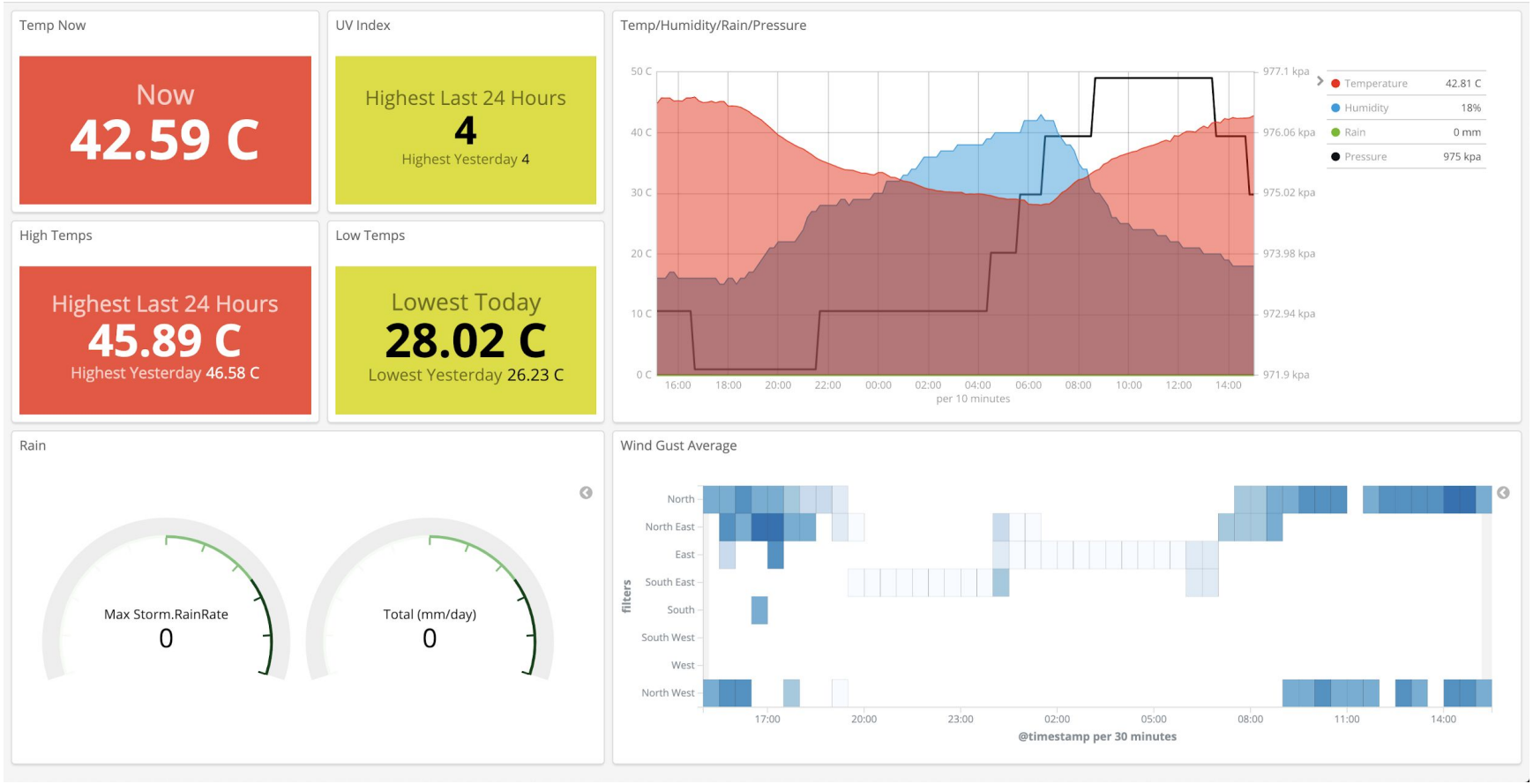
```
docker pull
docker.elastic.co/elasticsearch/elasticsearch:6.5.4
docker.elastic.co/elasticsearch/elasticsearch:6.5.4-oss

docker pull docker.elastic.co/kibana/kibana:6.5.4
docker pull docker.elastic.co/kibana/kibana:6.5.4-oss
```

Commands at https://go.es.io/2MjxC9M
Slides at https://go.es.io/2FN9ufo

Us!

elastic


Brisbane
Gold Coast
alia
SOUTH AUSTRALIA
NEW SOUTH WALES
Newcastle
Sydney
Canberra
ACT
Adelaide
VICTORIA
Ballarat
Melbourne
TASMANIA
Hobart
Tasman Sea
Auckland
Hamilton
Tauranga
Rotorua
Palmerston North
Wellington
New Zealand
Christchurch
Queenstown
Dunedin
Invercargill
Satellite
Google
Map data ©2019 Google
Australia
Terms
Send feedback
200 km



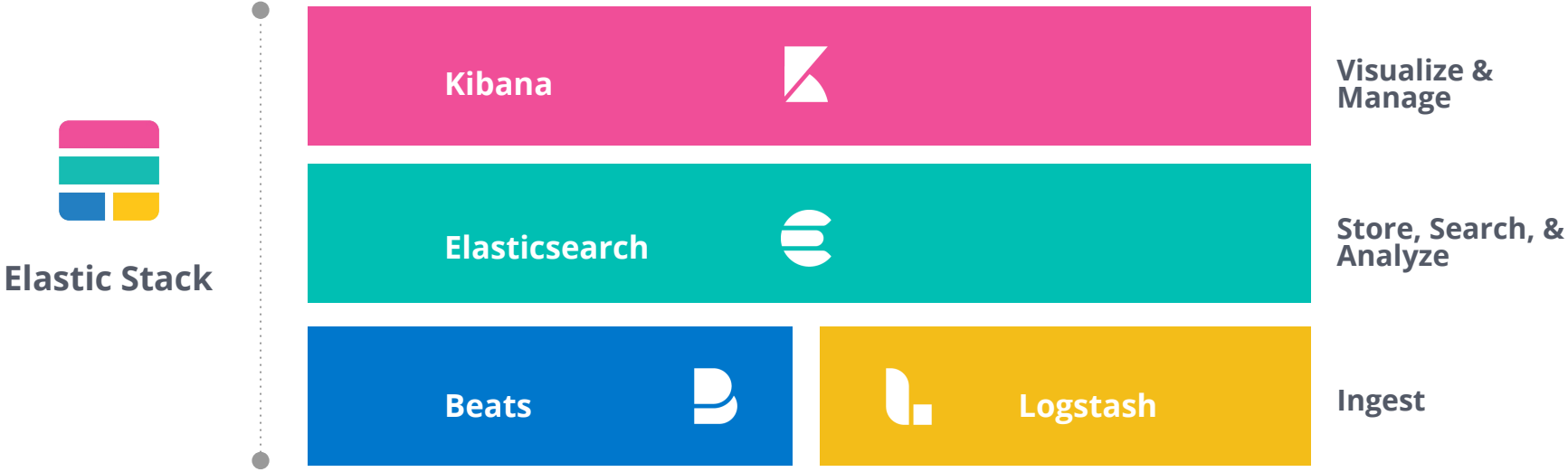
https://github.com/markwalkom/bloomsky-on-elastic

elastic

Elastic **Stack**

Elasticsearch, Kibana, Beats, and Logstash

Elastic **Stack**

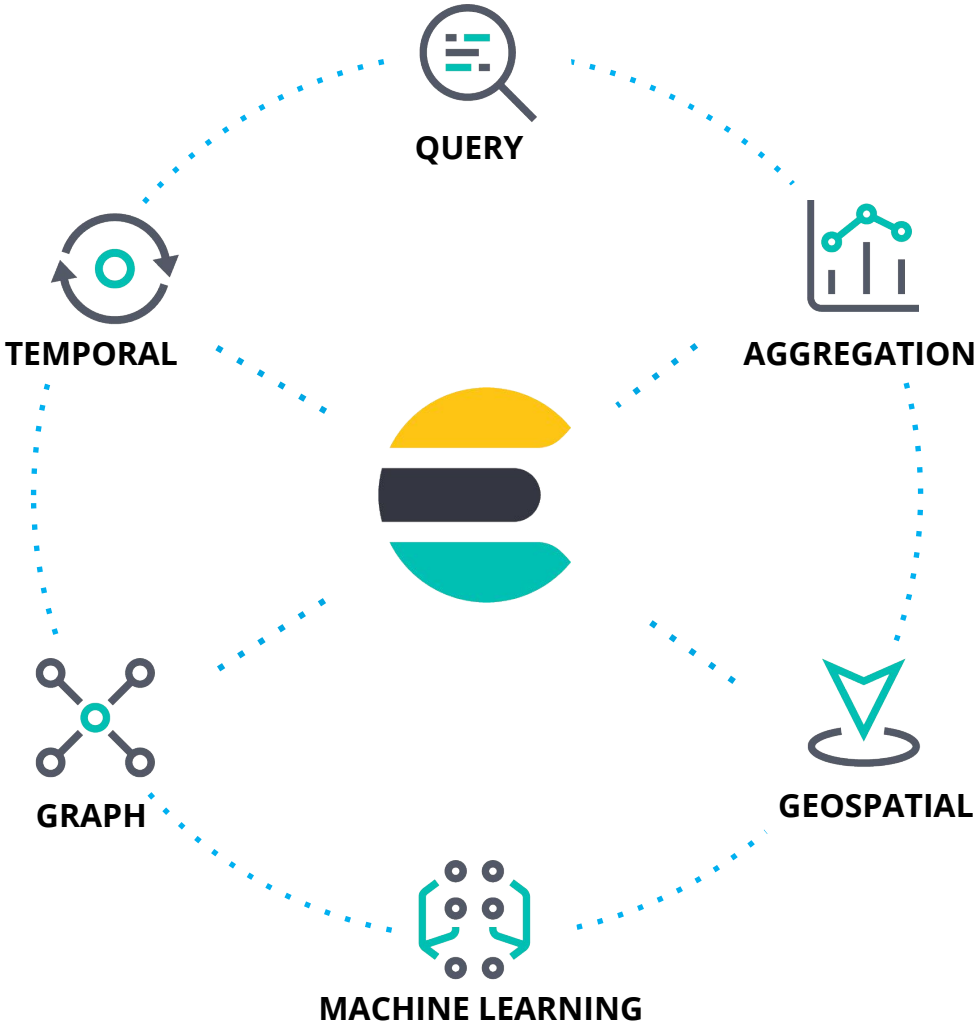


Elasticsearch

Heart of the Elastic Stack

- Scalable
- Real-time
- Highly available
- Developer-friendly
- Versatile storage
- Query & aggregations

elastic


QUERY
AGGREGATION
GEOSPATIAL
MACHINE LEARNING
GRAPH
TEMPORAL

elastic

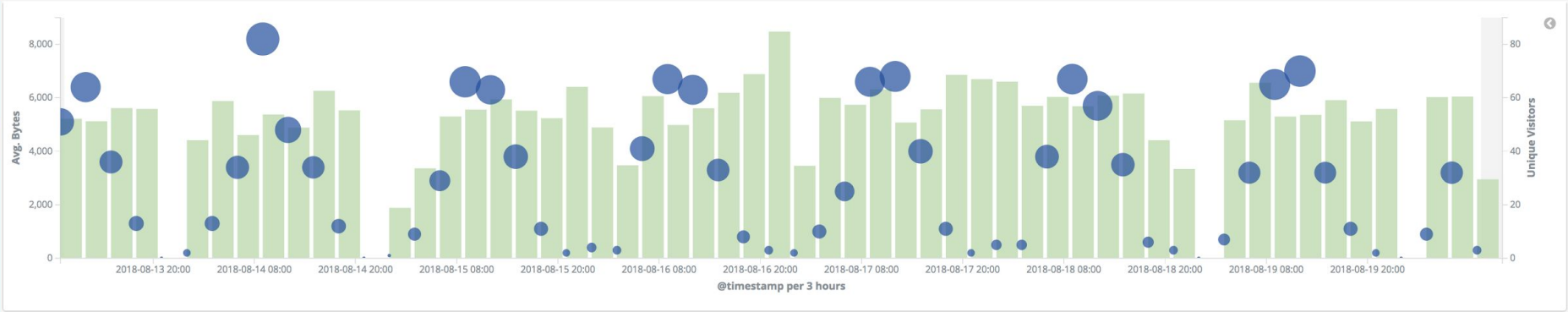
Kibana

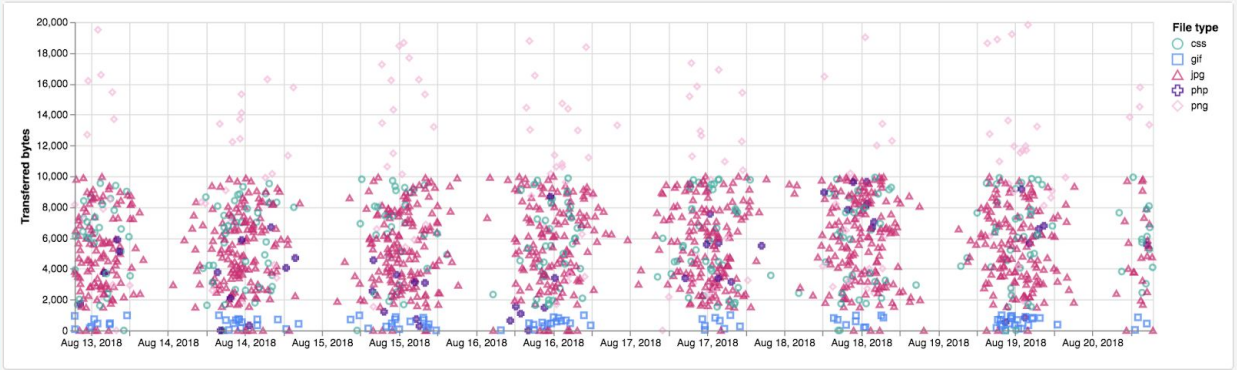
Window into the Elastic Stack

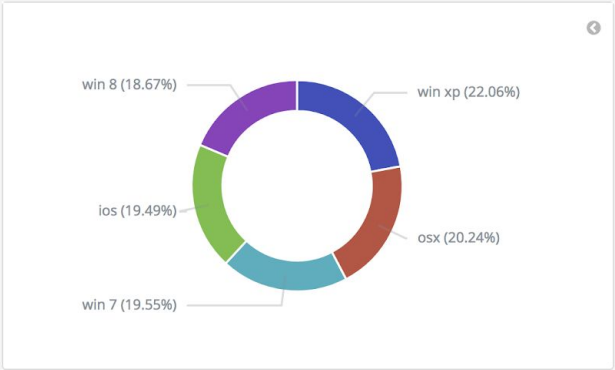
- Visualize and explore
- Manage and monitor
- Share and report
- Developer tools
- Time-series analysis
- Geospatial exploration

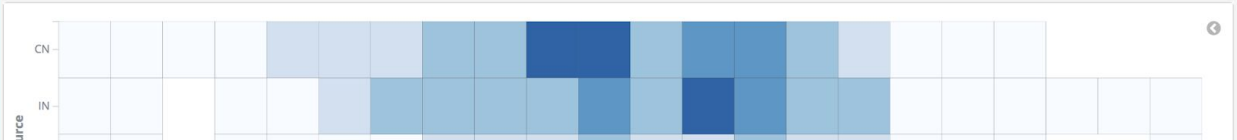
elastic

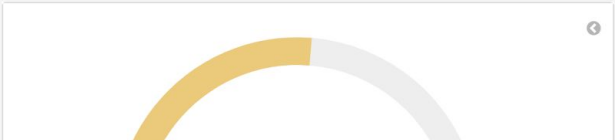
All the visualizations you expect, and then some more



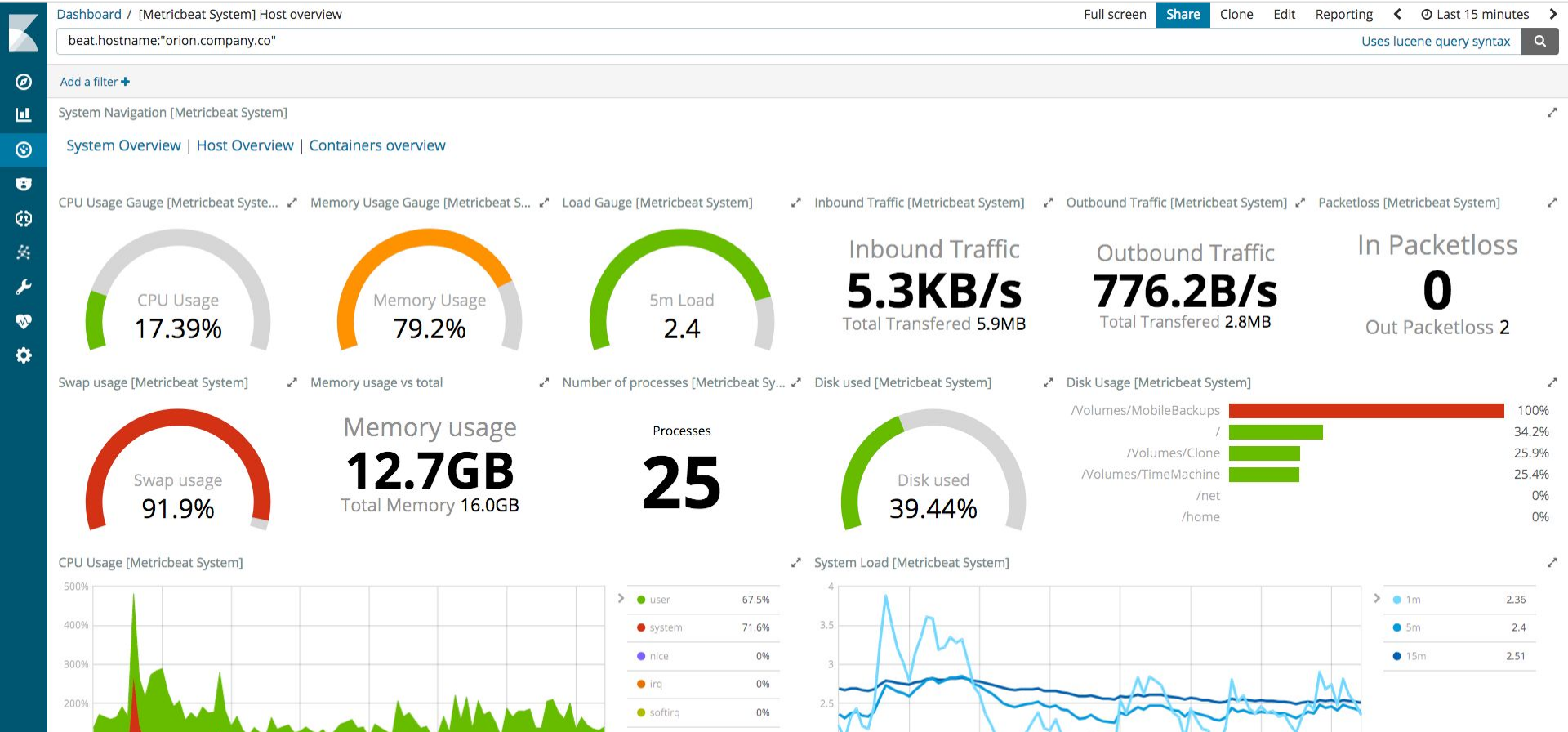








OOTB dashboards for 50+ (and growing) data sources



Beats

Lightweight data shippers

- Ship from any source
- Transform at the edge
- Docker and k8s ready
- Cloud metadata enrichment
- 70+ community Beats
- 50+ modules

elastic

FILEBEAT
Log Files

METRICBEAT
Metrics

PACKETBEAT
Network Data

FUNCTIONBEAT
Serverless Monitoring

WINLOGBEAT
Window Events

HEARTBEAT
Uptime Monitoring

AUDITBEAT
Audit Data

Plus a growing set of community Beats

elastic

Logstash

Data processing pipeline

- Flexible ETL engine
- Parse & transform data
- Many inputs & outputs
- Horizontally scalable
- 200+ plugins

elastic

Modules

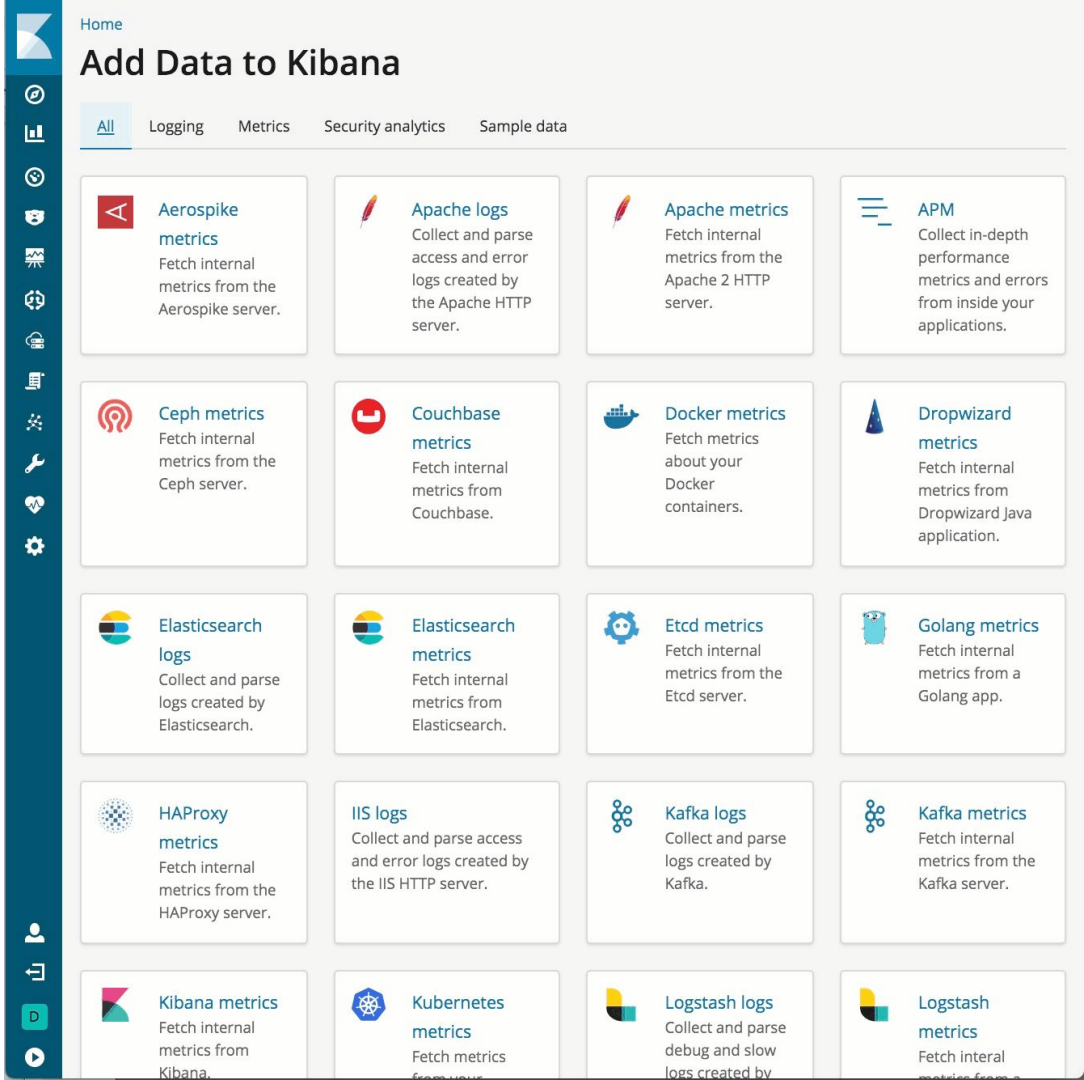
Data to dashboards in 5 minutes

Turnkey for many formats

Automated data parsing

Out of the box dashboards

Preconfigured ML jobs



Let’s get started

Let’s Install Elasticsearch

```
docker pull
docker.elastic.co/elasticsearch/elasticsearch:6.5.4
```

Or

```
docker pull
docker.elastic.co/elasticsearch/elasticsearch-oss:6.5.4
```

- https://www.elastic.co/guide/en/elasticsearch/reference/6.5/docker.html
- https://www.docker.elastic.co/
- https://hub.docker.com/_/elasticsearch

Let’s Run Elasticsearch

```
docker run -p 9200:9200 -p 9300:9300 -e
"discovery.type=single-node"
docker.elastic.co/elasticsearch/elasticsearch:6.5.4
```

Or

```
docker run -d -p 9200:9200 -p 9300:9300 -e
"discovery.type=single-node"
docker.elastic.co/elasticsearch/elasticsearch:6.5.4
```

- https://www.elastic.co/guide/en/elasticsearch/reference/6.5/docker.html

Let’s docker-compose Elasticsearch

```
version: '2.2'
services:
  elasticsearch:
    image:
docker.elastic.co/elasticsearch/elasticsearch:6.5.4
    volumes:
      - esdata:/usr/share/elasticsearch/data
    ports:
      - 9200:9200

volumes:
  esdata:
    driver: local
```

Let’s (just) Elasticsearch

```
curl 0:9200/_cat/
curl 0:9200/_cat/health
curl 0:9200/_cat/indices?v
```

- https://www.elastic.co/guide/en/elasticsearch/reference/6.5/cat.html

Kibana Install

```
docker pull docker.elastic.co/kibana/kibana:6.5.4
```

Or

```
docker pull docker.elastic.co/kibana/kibana-oss:6.5.4
```

- https://www.elastic.co/guide/en/kibana/6.5/docker.html
- https://www.docker.elastic.co/
- https://hub.docker.com/_/kibana

Kibana Run

```
docker run docker.elastic.co/kibana/kibana:6.5.4 -p
5601:5601 -e "elasticsearch.url=localhost:9200"
```

- (wait for it)
- Open http://localhost:5601/

Let’s docker-compose Kibana

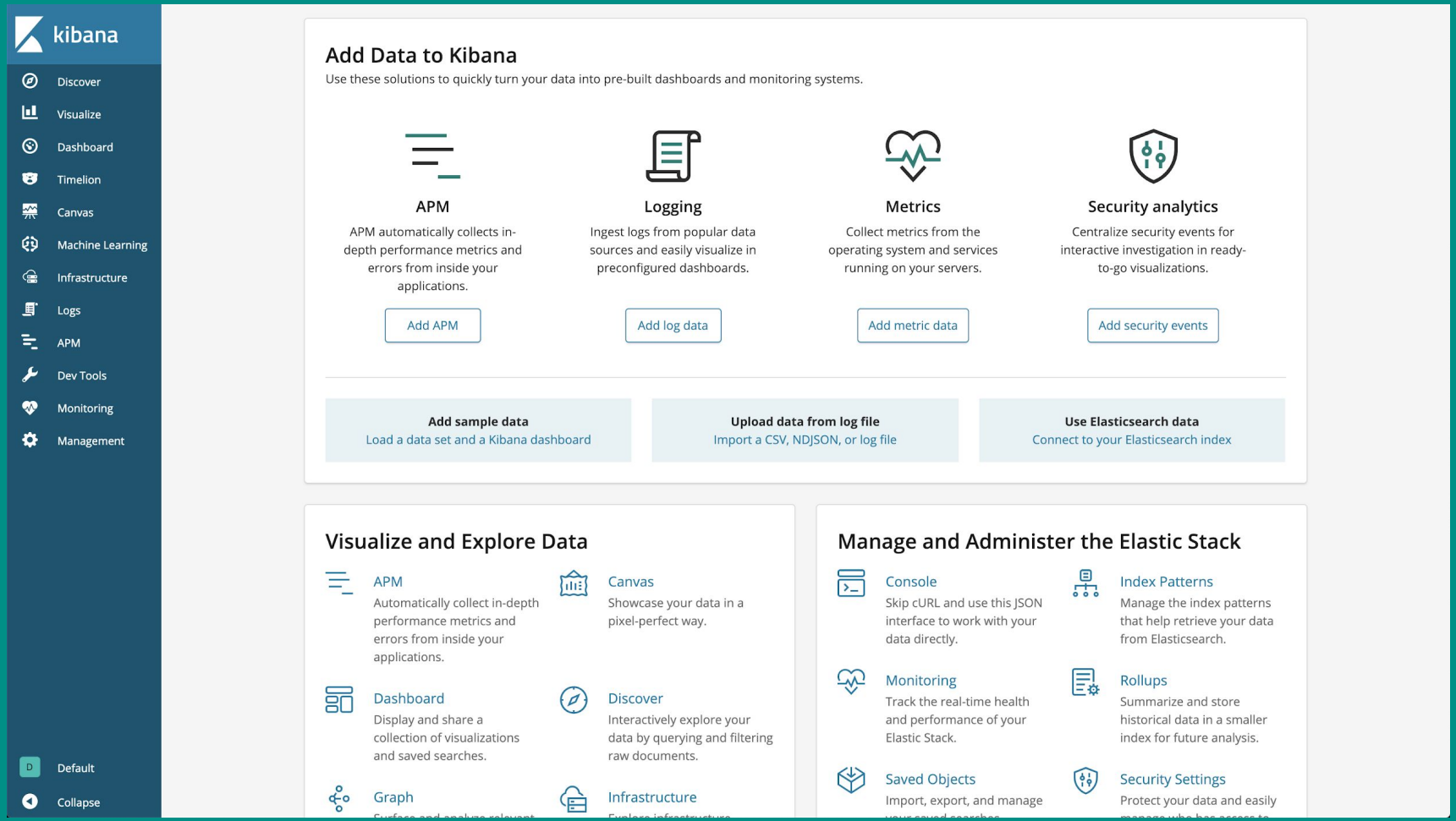
```
kibana:
    image: docker.elastic.co/kibana/kibana:6.5.4
    links:
      - elasticsearch
    ports:
      - 5601:5601
```

- Use the complete Docker compose file in the gist

docker-compose up

- Just run that command
- Alternatively;

```
docker-compose up -d
```


kibana
Discover
Visualize
Dashboard
Timelion
Canvas
Machine Learning
Infrastructure
Logs
APM
Dev Tools
Monitoring
Management
Default
Collapse
Add Data to Kibana
Use these solutions to quickly turn your data into pre-built dashboards and monitoring systems.
APM
APM automatically collects in-depth performance metrics and errors from inside your applications.
Add APM
Logging
Ingest logs from popular data sources and easily visualize in preconfigured dashboards.
Add log data
Metrics
Collect metrics from the operating system and services running on your servers.
Add metric data
Security analytics
Centralize security events for interactive investigation in ready-to-go visualizations.
Add security events
Add sample data
Load a data set and a Kibana dashboard
Upload data from log file
Import a CSV, NDJSON, or log file
Use Elasticsearch data
Connect to your Elasticsearch index
Visualize and Explore Data
APM
Automatically collect in-depth performance metrics and errors from inside your applications.
Canvas
Showcase your data in a pixel-perfect way.
Dashboard
Display and share a collection of visualizations and saved searches.
Discover
Interactively explore your data by querying and filtering raw documents.
Graph
Infrastructure
Manage and Administer the Elastic Stack
Console
Skip cURL and use this JSON interface to work with your data directly.
Index Patterns
Manage the index patterns that help retrieve your data from Elasticsearch.
Monitoring
Track the real-time health and performance of your Elastic Stack.
Rollups
Summarize and store historical data in a smaller index for future analysis.
Saved Objects
Import, export, and manage
Security Settings
Protect your data and easily

elastic

Metricbeat

https://www.elastic.co/guide/en/beats/metricbeat/current/index.html

Metricbeat Install and Run

- Download the binary
- Extract

```
./metricbeat
```

- STOP!

```
./metricbeat setup --help
```

```
./metricbeat modules --help
```

Metricbeat Install and Run

```
./metricbeat modules list

./metricbeat setup --template -E
output.logstash.enabled=false -E
'output.elasticsearch.hosts=["localhost:9200"]'

./metricbeat setup --dashboards


./metricbeat
```

- Enable the system module
- See also https://go.es.io/2T44qWN

Filebeat

https://www.elastic.co/guide/en/beats/filebeat/current/index.html

Filebeat Install and Run

- Download the binary
- Extract

```
./filebeat
```

- Remember

```
./filebeat setup --help
```

```
./filebeat modules --help
```

Filebeat Install and Run

```
./filebeat modules list

./filebeat setup --template -E
output.logstash.enabled=false -E
'output.elasticsearch.hosts=["localhost:9200"]'

./filebeat setup --dashboards


./filebeat
```

- Enable the system module
- See also https://go.es.io/2T44qWN

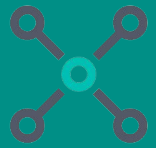
Let’s kick it up a notch

elastic

Metricbeat - Enable the docker module

Filebeat - Enable the docker input

Let’s analyse Elasticsearch traffic!



Packetbeat

https://www.elastic.co/guide/en/beats/packetbeat/current/index.html

Packetbeat Install and Run

- Download the binary
- Extract

```
./packetbeat
```

- Remember

```
./packetbeat setup --help
```

```
./packetbeat modules --help
```

Metricbeat Install and Run

```
./packetbeat modules list

./packetbeat setup --template -E
output.logstash.enabled=false -E
'output.elasticsearch.hosts=["localhost:9200"]'

./packetbeat setup --dashboards


./packetbeat
```

- See also https://go.es.io/2T44qWN

Heartbeat

https://www.elastic.co/guide/en/beats/heartbeat/current/index.html

Heartbeat Install and Run

- Download the binary
- Extract

```
./heartbeat
```

- Remember

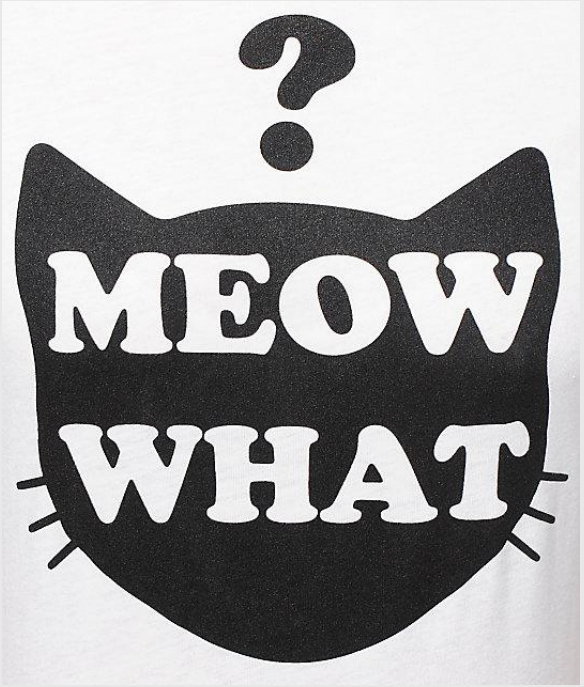
```
./heartbeat setup --help
```

```
./heartbeat modules --help
```

Heartbeat Install and Run

```
./heartbeat modules list

./heartbeat setup --template -E
output.logstash.enabled=false -E
'output.elasticsearch.hosts=["localhost:9200"]'

./heartbeat setup --dashboards


./heartbeat
```

- See also https://go.es.io/2T44qWN



Community beats
Logstash!
Elasticsearch Ingest
[Heart|Winlog|DIY]beat
APM
Dashboards

Whakawhetai Koe!