

# Awesome Monitoring Infrastructure Using the Elastic Stack

Mark Walkom @awarkolm  
Karen Carcamo @karencfv  
[www.elastic.co](http://www.elastic.co)



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

The Linux of Things | #LCA2019 | @linuxconfau

# Please install Docker :)

```
docker pull
```

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

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

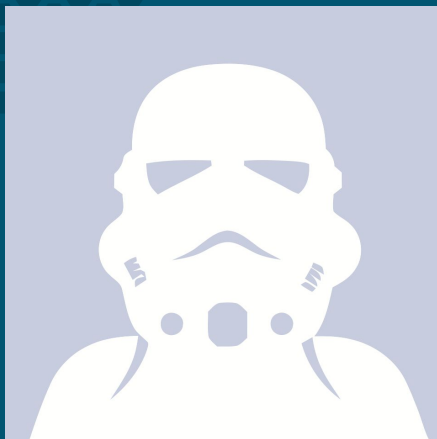
```
docker pull docker.elastic.co/kibana/kibana:6.5.4
```

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

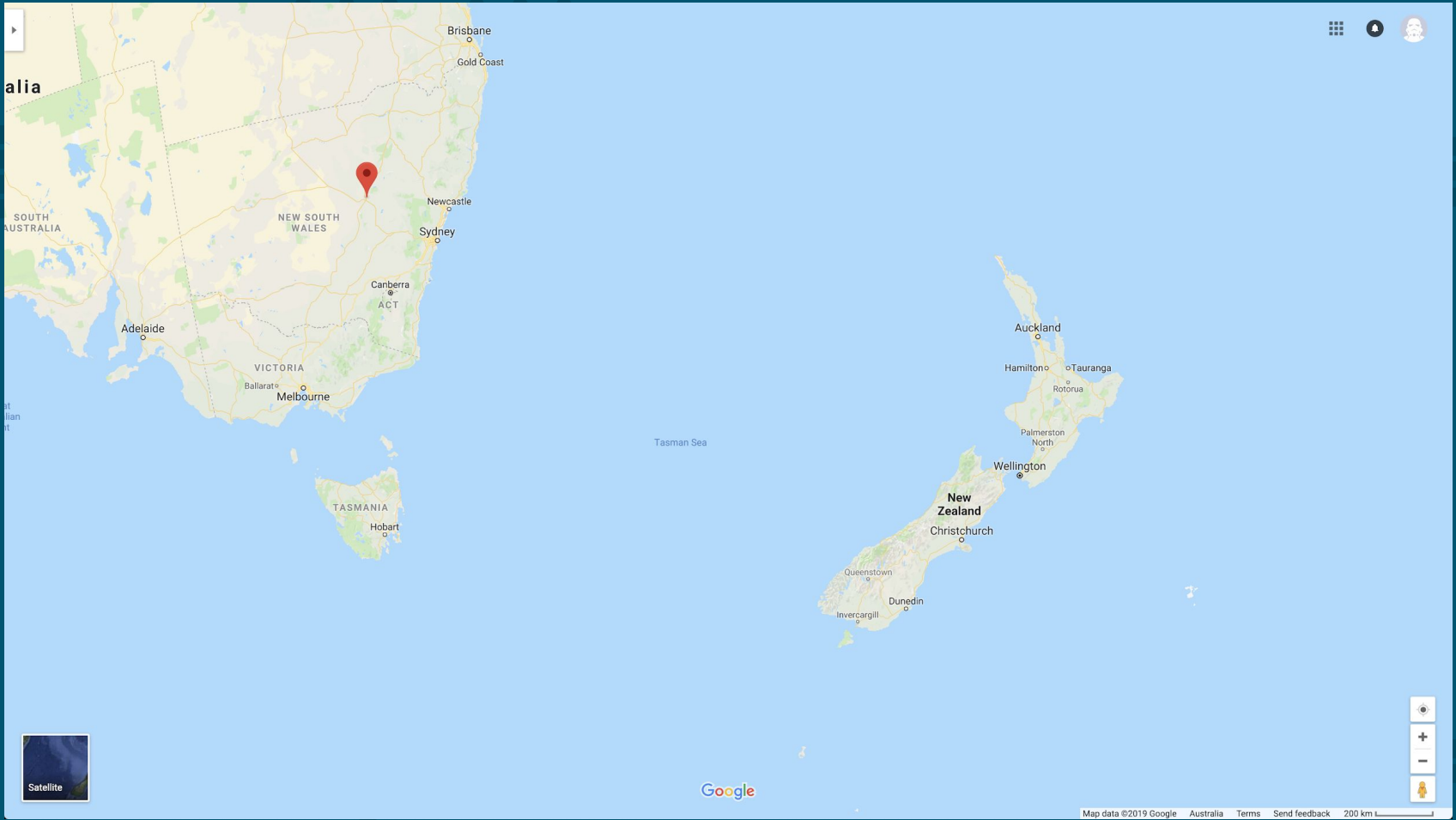
Commands at <https://go.es.io/2MjxC9M>

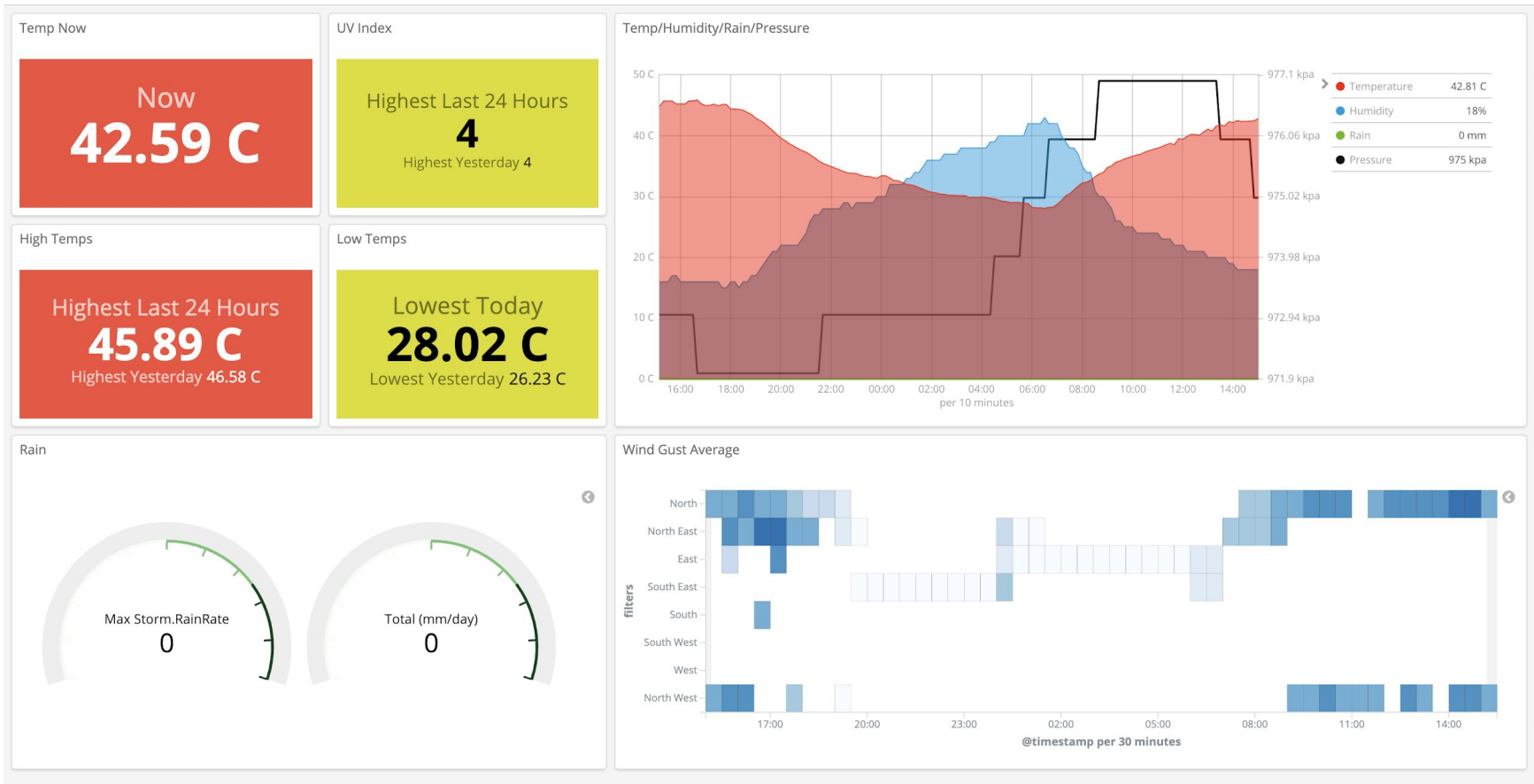
Slides at <https://go.es.io/2FN9ufo>





Us!



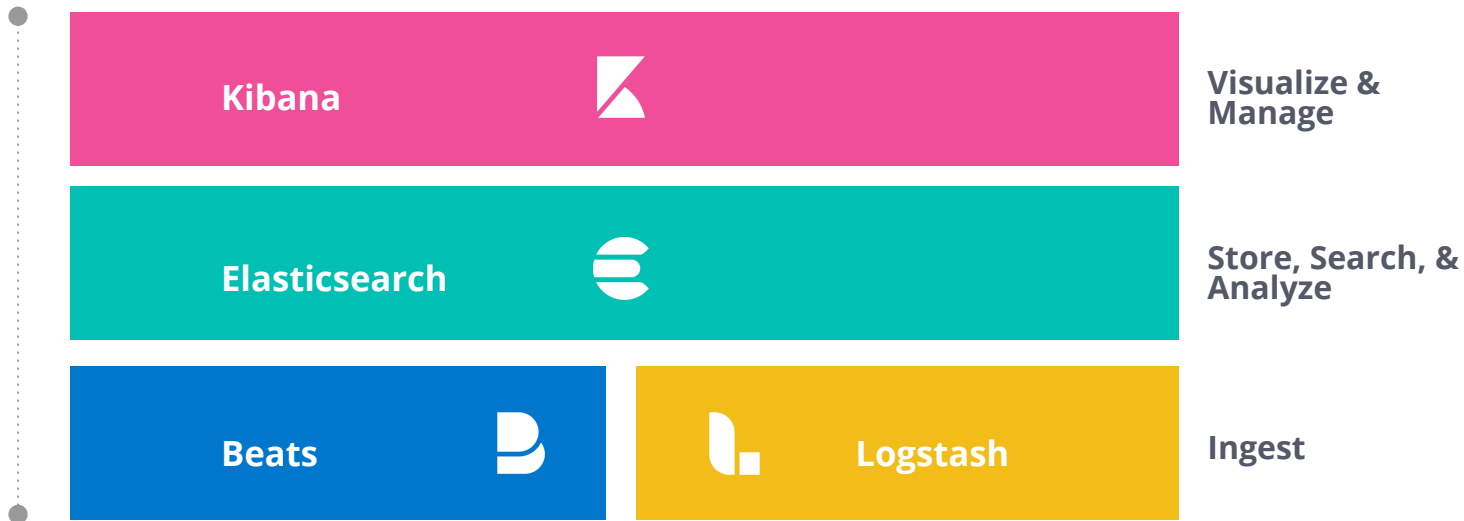


<https://github.com/markwalkom/bloomsy-on-elastic>

# Elastic Stack

Elasticsearch, Kibana, Beats, and Logstash

# Elastic Stack



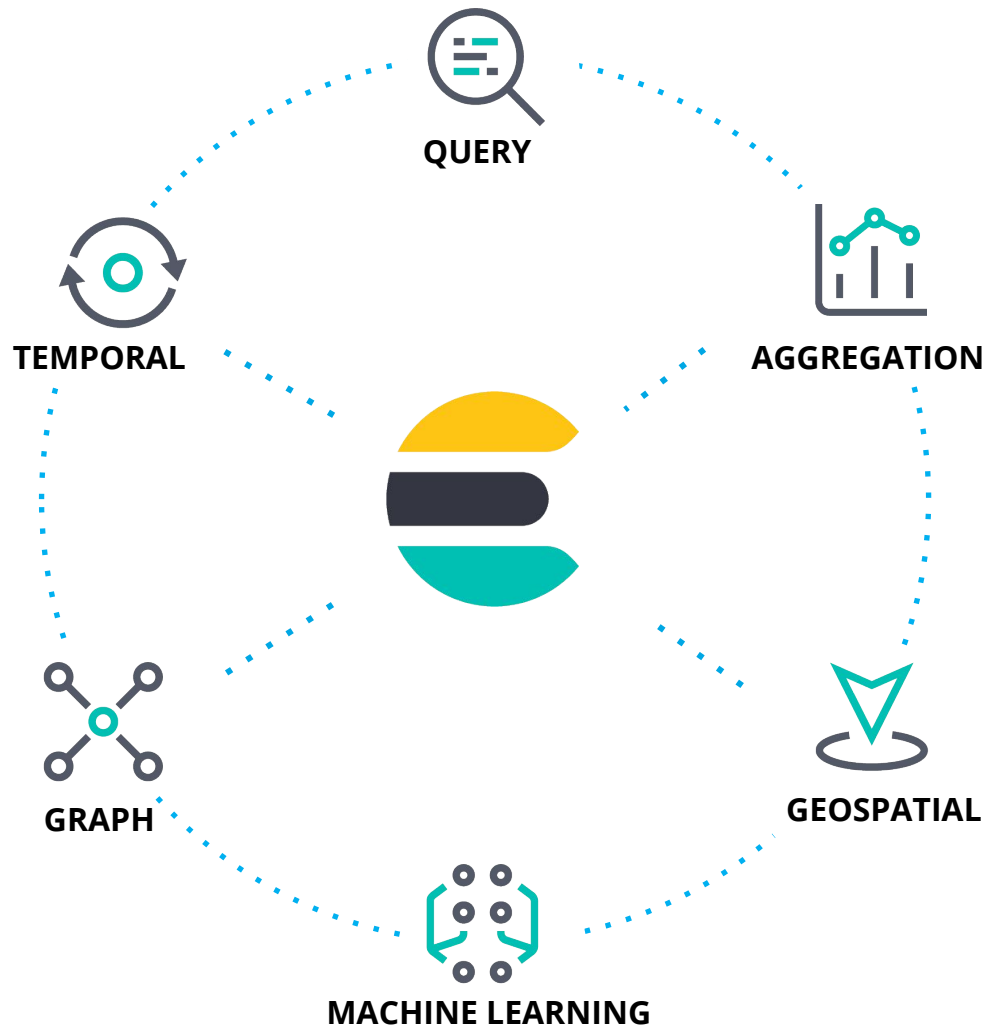


# Elasticsearch

Heart of the Elastic Stack

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





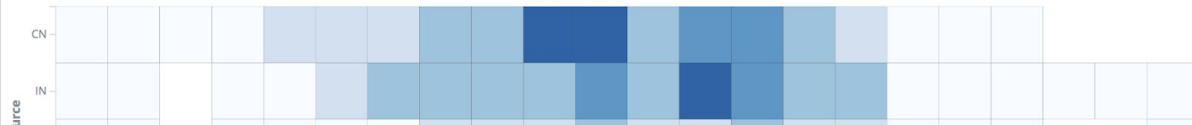
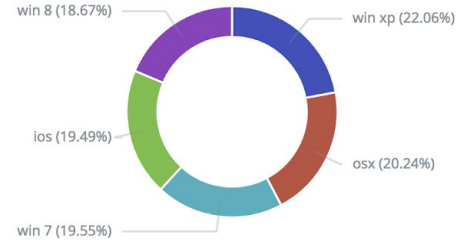
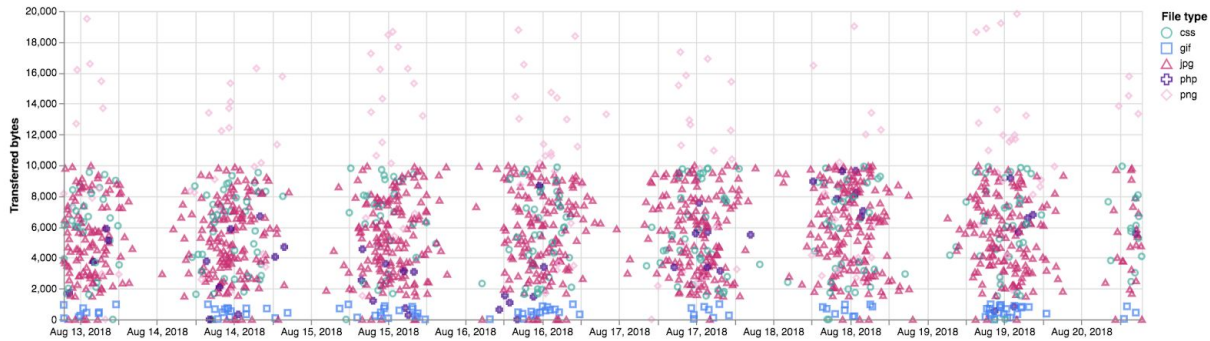
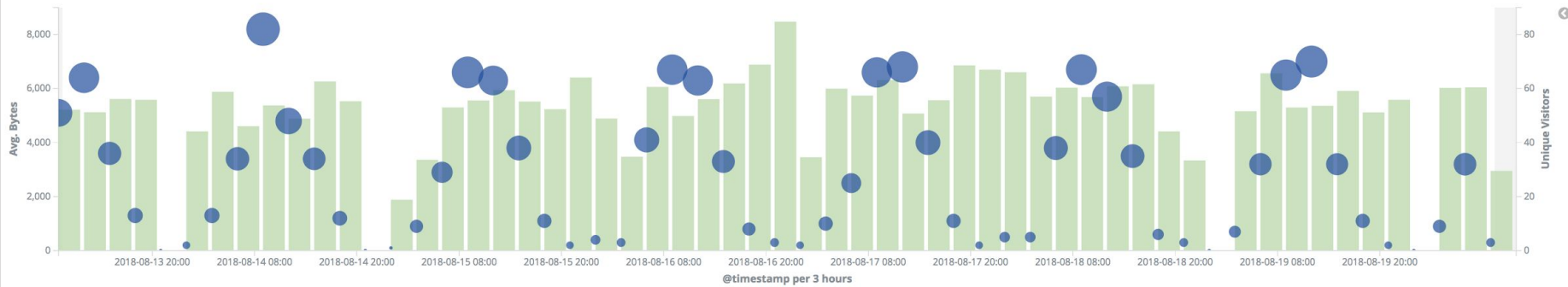


# Kibana

Window into the Elastic Stack

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

# All the visualizations you expect, and then some more



# OOTB dashboards for 50+ (and growing) data sources

Dashboard / [Metricbeat System] Host overview Full screen Share Clone Edit Reporting Last 15 minutes

beat.hostname:"orion.company.co" Uses lucene query syntax

Add a filter +

System Navigation [Metricbeat System]

System Overview | Host Overview | Containers overview

CPU Usage Gauge [Metricbeat System] Memory Usage Gauge [Metricbeat System] Load Gauge [Metricbeat System] Inbound Traffic [Metricbeat System] Outbound Traffic [Metricbeat System] Packetloss [Metricbeat System]

CPU Usage **17.39%**

Memory Usage **79.2%**

5m Load **2.4**

Inbound Traffic **5.3KB/s**  
Total Transferred 5.9MB

Outbound Traffic **776.2B/s**  
Total Transferred 2.8MB

In Packetloss **0**  
Out Packetloss 2

Swap usage [Metricbeat System] Memory usage vs total Number of processes [Metricbeat System] Disk used [Metricbeat System] Disk Usage [Metricbeat System]

Swap usage **91.9%**

Memory usage **12.7GB**  
Total Memory 16.0GB

Processes **25**

Disk used **39.44%**

/Volumes/MobileBackups	100%
/	34.2%
/Volumes/Clone	25.9%
/Volumes/TimeMachine	25.4%
/net	0%
/home	0%

CPU Usage [Metricbeat System]

user	67.5%
system	71.6%
nice	0%
irq	0%
softirq	0%

System Load [Metricbeat System]

1m	2.36
5m	2.4
15m	2.51



## Beats

Lightweight data shippers

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



**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**



# Logstash

Data processing pipeline

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

# Modules

Data to dashboards in 5 minutes

Turnkey for many formats

Automated data parsing

Out of the box dashboards

Preconfigured ML jobs

The screenshot displays the 'Add Data to Kibana' interface. At the top, there is a navigation bar with 'Home' and a list of tabs: 'All', 'Logging', 'Metrics', 'Security analytics', and 'Sample data'. The 'All' tab is selected. Below the tabs, a grid of 16 data source modules is shown, each with an icon, a title, and a brief description:

- Aerospike metrics**: Fetch internal metrics from the Aerospike server.
- Apache logs**: Collect and parse access and error logs created by the Apache HTTP server.
- Apache metrics**: Fetch internal metrics from the Apache 2 HTTP server.
- APM**: Collect in-depth performance metrics and errors from inside your applications.
- Ceph metrics**: Fetch internal metrics from the Ceph server.
- Couchbase metrics**: Fetch internal metrics from Couchbase.
- Docker metrics**: Fetch metrics about your Docker containers.
- Dropwizard metrics**: Fetch internal metrics from Dropwizard Java application.
- Elasticsearch logs**: Collect and parse logs created by Elasticsearch.
- Elasticsearch metrics**: Fetch internal metrics from Elasticsearch.
- Etd metrics**: Fetch internal metrics from the Etd server.
- Golang metrics**: Fetch internal metrics from a Golang app.
- HAProxy metrics**: Fetch internal metrics from the HAProxy server.
- IIS logs**: Collect and parse access and error logs created by the IIS HTTP server.
- Kafka logs**: Collect and parse logs created by Kafka.
- Kafka metrics**: Fetch internal metrics from the Kafka server.
- Kibana metrics**: Fetch internal metrics from Kibana.
- Kubernetes metrics**: Fetch metrics from your Kubernetes cluster.
- Logstash logs**: Collect and parse debug and slow logs created by Logstash.
- Logstash metrics**: Fetch internal metrics from Logstash.



The background is a solid blue color. It is decorated with various small, scattered geometric shapes in white, yellow, and green. These shapes include circles, squares, diamonds, and plus signs, distributed across the entire page.

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](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](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
```

## 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**  
Surface and analyze relevant data.



**Infrastructure**  
Explore 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 your saved searches.



**Security Settings**  
Protect your data and easily manage who has access to it.



# 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>



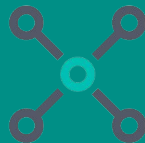
Let's kick it  
up a notch



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!



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

The Linux of Things | #LCA2019 | @linuxconfau