Elasticsearch

Logs

Philipp Krenn

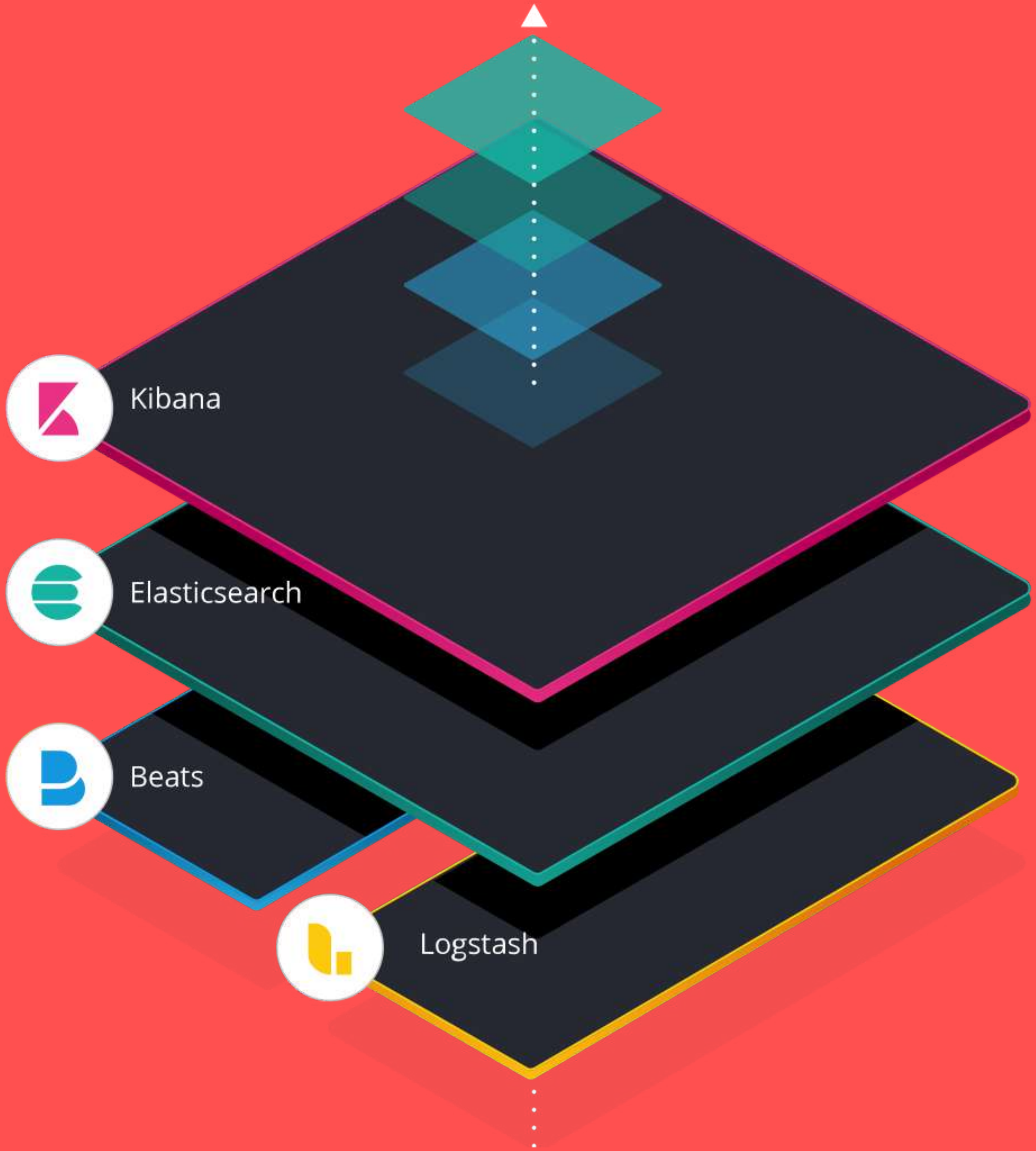
@xeraa

elastic

elastic

Search. Observe. Protect.

Developer 🥑



elastic

@xeraa

Elastic Observability

Elasticsearch

Server Logs

<cluster name>.log **and** *<cluster name>_server.json*

Log Structure

<name of logging hierarchy>=<level>

Log Level

https://logging.apache.org/log4j/2.0/manual/architecture.html#Log_Levels

`TRACE   DEBUG   INFO   WARN   ERROR`
`FATAL`

Log Hierarchy

https://logging.apache.org/log4j/2.0/manual/architecture.html#Logger_Hierarchy

logger.org.elasticsearch.transport →
elasticsearch/server/src/main/java/org/elasticsearch/transport/

Tip: *logger._root* **or** *logger.level*

Config: Command-Line

-E<name of logging hierarchy>=<level>

Temporary debugging on single node

Config: Command-Line

Demo: *./bin/elasticsearch* **vs** *./bin/elasticsearch -Elogger.level=WARN*

~~*./bin/elasticsearch -Elogger._root=WARN*~~

https://github.com/elastic/elasticsearch/issues/17320

Config: *elasticsearch.yml*

<name of logging hierarchy>: <level>

Temporary debugging of service or permanent change

Config: *elasticsearch.yml*

Demo: *./bin/elasticsearch* **with defaults vs** *logger.level: WARN*

~~*logger._root: WARN*~~

Config: Cluster Settings

```
PUT _cluster/settings
{
  "transient": {
    "<name of logging hierarchy>": "<level>"
} }
```

Most common and dynamic

Config: Cluster Settings

```
PUT _cluster/settings
{
  "transient": {
    "logger._root": "WARN"
} }
```

~~'logger.level': 'WARN'~~

PS: Reset to Default?

```
PUT _cluster/settings
{
  "transient": {
    "logger._root": null
} }
```

Config: *log4j2.properties*

```
logger.<unique_ID>.name = <name of logging hierarchy>
logger.<unique_ID>.level = <level>
```

Finer control (log to another file) but rare

Slow Logs

<cluster name>_index_indexing_slowlog.json
<cluster name>_index_indexing_slowlog.log
<cluster name>_index_search_slowlog.json
<cluster name>_index_search_slowlog.log

Example

```
PUT my_index/_settings
{
  "index.search.slowlog.threshold.query.warn": "500ms",
  "index.search.slowlog.threshold.query.info": "250ms",
  "index.search.slowlog.threshold.fetch.warn": "200ms",
  "index.search.slowlog.threshold.fetch.info": "100ms",
  "index.indexing.slowlog.threshold.index.warn": "1s",
  "index.indexing.slowlog.threshold.index.info": "500ms",
  "index.search.slowlog.level": "info"
}
```

Slow Log Features

Search (split into query and fetch) and index

By default disabled: *-1*

Slow Log Tricks

Log all queries with threshold *0*

Log all indices with *_all*

Demo

```
PUT my_index
PUT my_index/_settings
{
  "index.search.slowlog.threshold.query.warn": "0",
  "index.indexing.slowlog.threshold.index.warn": "0"
}
```

Demo

```
PUT my_index/_doc/1
{
  "name": "Philipp"
}

PUT my_index/_doc/2
{
  "name": "Alex"
}

less logs/elasticsearch_index_indexing_slowlog.log
```

Demo

```
GET my_index/_search
{
  "query": {
    "match": {
      "name": "philipp"
} } }

less logs/elasticsearch_index_search_slowlog.log
```

X-Opaque-Id **Header**

```
curl -XGET "http://localhost:9200/my_index/_search" \
           -H 'Content-Type: application/json' \
           -H 'X-Opaque-ID: my-id' \
           -d'{ "query": { "match": { "name": "philipp" } }}'

less logs/elasticsearch_index_search_slowlog.log
```

Deprecation Logs

<cluster name>_deprecation.json **and** *<cluster name>_deprecation.log*

Deprecation Logs

https://www.elastic.co/guide/en/elasticsearch/reference/master/breaking-changes-8.0.html

Default *logger.deprecation.level = warn*

Supports *X-Opaque-Id*

Demo

```
GET my_index/_search
{
  "query": {
    "match": {
      "name": {
        "query": "philipp",
        "cutoff_frequency": 0.1
} } } }

less logs/elasticsearch_deprecation.log
```

GC Logs

gc.log.0.current

GC Logs

https://openjdk.java.net/jeps/158

Enabled by default

Disable: *-Xlog:disable*

Demo

```
less logs/gc.log.0.current
```

Audit Logs

<cluster name>_audit.json

Audit Logs

Disabled by default

elasticsearch.yml

```
xpack.security.audit.enabled: true
```

Paid feature (Gold)

Audit Event Types

authentication_success

authentication_failed

anonymous_access_denied

...

Demo

```
vi elasticsearch.yml
```

↪️

```
xpack.security.audit.enabled: true
xpack.security.enabled: true
```

```
./bin/elasticsearch
```

```
./bin/elasticsearch-setup-passwords interactive
```

Demo

```
head -n1 logs/elasticsearch_audit.json | jq

{
  "type": "audit",
  "timestamp": "2020-07-29T20:11:08,529+0200",
  "node.id": "sDCzapQcSgCTgaOnebA07w",
  "event.type": "rest",
  "event.action": "anonymous_access_denied",
  "origin.type": "rest",
  "origin.address": "127.0.0.1:58611",
  "url.path": "/",
  "request.method": "HEAD",
  "request.id": "4s_UWL35TfiIOnGZvNeomA"
}
```

Elastic Logs

Filebeat Modules

```
filebeat.modules:
- module: elasticsearch

setup.kibana:
  host: "localhost:5601"

output.elasticsearch:
  hosts: ["localhost:9200"]
```

Customized Config

```
- module: elasticsearch
  server:
    var.paths:
      - ../elasticsearch*/logs/*_server.json
  slowlog:
    var.paths:
      - ../elasticsearch*/logs/*_index_search_slowlog.json
      - ../elasticsearch*/logs/*_index_indexing_slowlog.json
  gc:
    var.paths:
      - ../elasticsearch*/logs/gc.log.[0-9]*
      - ../elasticsearch*/logs/gc.log
  audit:
    var.paths:
      - ../elasticsearch*/logs/*_audit.json
```

Stack Monitoring

./filebeat -e

Enable Monitoring

Conclusion

Always More Logs

Server, Slow, Deprecation, GC, Audit

API & Centralized

elastic

@xeraa

Elastic Cloud?

elastic

@xeraa

Elasticsearch

Logs

Philipp Krenn **@xeraa**