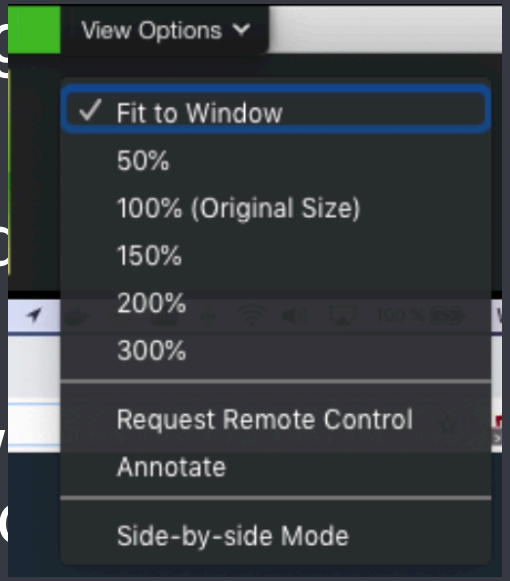
Der Elastic Stack für Logs und Metriken

Alexander Reelsen I Community Advocate
@spinscale
alex@elastic.co

Logistics

- Chat: Ensure you are writing messag
  everyone and not just the panelists
- Video: Ensure you select 'Fit to Wind
  to see the whole screen
- Chat: Write all your questions. We w
  them during the session or at the en
- Recording will made available!



elastic

Agenda

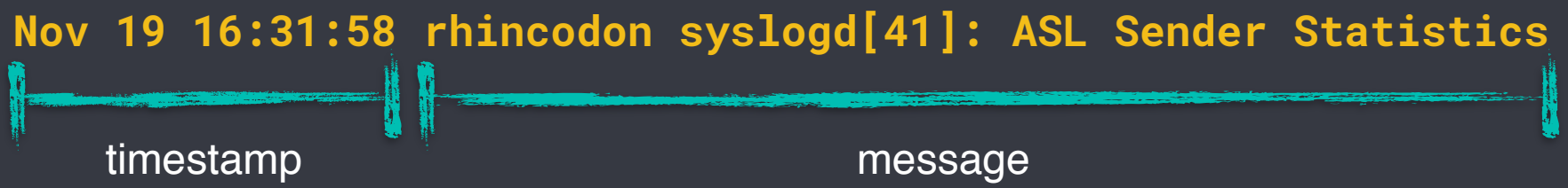
Agenda

- Logs & Metrics
- Elastic Stack Introduction
- Ingestion
- DEMO
- Q & A

elastic

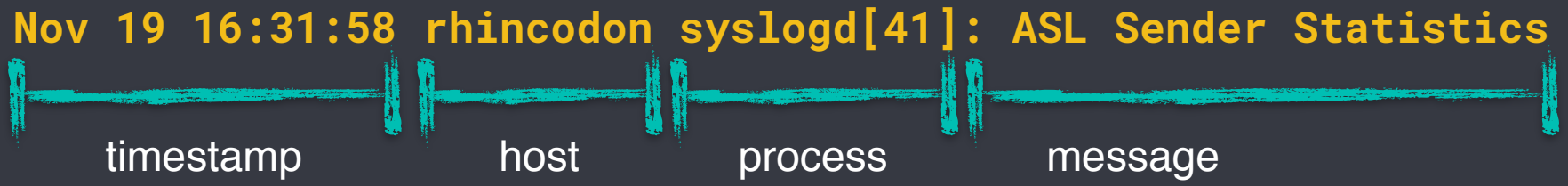
Logs & Metrics?

What is a log?

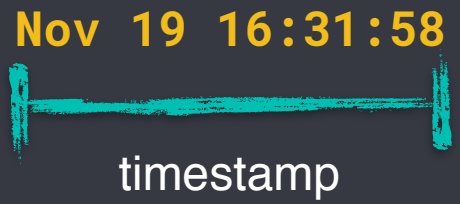


What is a log?

What is a structured log?



What is a log?



- Not unique!
- Granularity!
- Timezone!
- Year!
- Defaults required!

Date normalization

Nov 19 16:31:58

elastic

Date normalization

```
Nov 19 16:31:58

19/Jul/2015:08:13:42 +0000
```

Date normalization

```
Nov 19 16:31:58

19/Jul/2015:08:13:42 +0000

2015-01-01T12:10:30.123456789Z
```

Date normalization

```
Nov 19 16:31:58

19/Jul/2015:08:13:42 +0000

2015-01-01T12:10:30.123456789Z

2019-10-10
```

elastic

Date normalization

```
Nov 19 16:31:58

19/Jul/2015:08:13:42 +0000

2015-01-01T12:10:30.123456789Z

2019-10-10

1420070400
```

elastic

Date normalization

```
Nov 19 16:31:58

19/Jul/2015:08:13:42 +0000

2015-01-01T12:10:30.123456789Z

2019-10-10

1420070400

2019-11-19T17:05:38,752
```

Date normalization

```
Nov 19 16:31:58

19/Jul/2015:08:13:42 +0000

2015-01-01T12:10:30.123456789Z

2019-10-10

1420070400

2019-11-19T17:05:38,752

16:06:02.858
```

elastic

Date normalization

```
Nov 19 16:31:58

19/Jul/2015:08:13:42 +0000

2015-01-01T12:10:30.123456789Z

2019-10-10

1420070400

2019-11-19T17:05:38,752

16:06:02.858

2019-11-19T17:06:23.582+0100
```

elastic

Multi line events

```
[2019-07-25T00:10:02,240][WARN ][o.e.i.IndexService       ] [1563552203477145411] [migrate-bird-filebeat-7.0.0-alpha1-2019.07.2
5] failed to run task refresh - suppressing re-occurring exceptions unless the exception changes
org.elasticsearch.index.engine.RefreshFailedEngineException: Refresh failed
        at org.elasticsearch.index.engine.InternalEngine.refresh(InternalEngine.java:919) ~[elasticsearch-5.6.4.jar:5.6.4]
        at org.elasticsearch.index.shard.IndexShard.refresh(IndexShard.java:632) ~[elasticsearch-5.6.4.jar:5.6.4]
        at org.elasticsearch.index.IndexService.maybeRefreshEngine(IndexService.java:690) ~[elasticsearch-5.6.4.jar:5.6.4]
        at org.elasticsearch.index.IndexService.access$400(IndexService.java:92) ~[elasticsearch-5.6.4.jar:5.6.4]
        at org.elasticsearch.index.IndexService$AsyncRefreshTask.runInternal(IndexService.java:832) ~[elasticsearch-5.6.4.jar:5
.6.4]
        at org.elasticsearch.index.IndexService$BaseAsyncTask.run(IndexService.java:743) [elasticsearch-5.6.4.jar:5.6.4]
        at org.elasticsearch.common.util.concurrent.ThreadContext$ContextPreservingRunnable.run(ThreadContext.java:569) [elasti
csearch-5.6.4.jar:5.6.4]
        at java.util.concurrent.ThreadPoolExecutor.runWorker(Unknown Source) [?:1.8.0_181]
        at java.util.concurrent.ThreadPoolExecutor$Worker.run(Unknown Source) [?:1.8.0_181]
        at java.lang.Thread.run(Unknown Source) [?:1.8.0_181]
Caused by: org.apache.lucene.index.CorruptIndexException: compound sub-files must have a valid codec header and footer: file is too small (0 bytes)
(resource=BufferedChecksumIndexInput(MMapIndexInput(path="/data3/containers/1563552203477145411/es/data/nodes/0/indices/itne5EqpRE-vNw1wLMj2EA/1/index/
_8u.dim")))
        at org.apache.lucene.codecs.CodecUtil.verifyAndCopyIndexHeader(CodecUtil.java:282) ~[lucene-core-6.6.1.jar:6.6.1 unknown - elk - 2018-06-28
00:21:33]
        at org.apache.lucene.codecs.lucene50.Lucene50CompoundFormat.write(Lucene50CompoundFormat.java:96) ~[lucene-core-6.6.1.jar:6.6.1 unknown - elk -
2018-06-28 00:21:33]
        at org.apache.lucene.index.IndexWriter.createCompoundFile(IndexWriter.java:4945) ~[lucene-core-6.6.1.jar:6.6.1 unknown - elk - 2018-06-28
00:21:33]
        at org.apache.lucene.index.DocumentsWriterPerThread.sealFlushedSegment(DocumentsWriterPerThread.java:529) ~[lucene-core-6.6.1.jar:6.6.1 unknown
- elk - 2018-06-28 00:21:33]
        at org.apache.lucene.index.DocumentsWriterPerThread.flush(DocumentsWriterPerThread.java:481) ~[lucene-core-6.6.1.jar:6.6.1 unknown - elk -
2018-06-28 00:21:33]
        at org.apache.lucene.index.DocumentsWriter.doFlush(DocumentsWriter.java:539) ~[lucene-core-6.6.1.jar:6.6.1 unknown - elk - 2018-06-28 00:21:33]
        at org.apache.lucene.index.DocumentsWriter.flushAllThreads(DocumentsWriter.java:653) ~[lucene-core-6.6.1.jar:6.6.1 unknown - elk - 2018-06-28
00:21:33]
```

elastic

What is a metric?

- measurement at a point in time

Logs vs. Metrics

- log: event based
- metric: constant measurement

Log centralization

- Access rights
- Short lived containers
- Search across services
- Correlation
- Retention
- Alerting
- Cost of storage/density

Data normalization

- Timestamps
- Field name convention (lowercase, tense)
- Same field names across services
- Elastic Common Schema

`https://www.elastic.co/guide/en/ecs/current/ecs-reference.html`

Elastic Stack

elastic

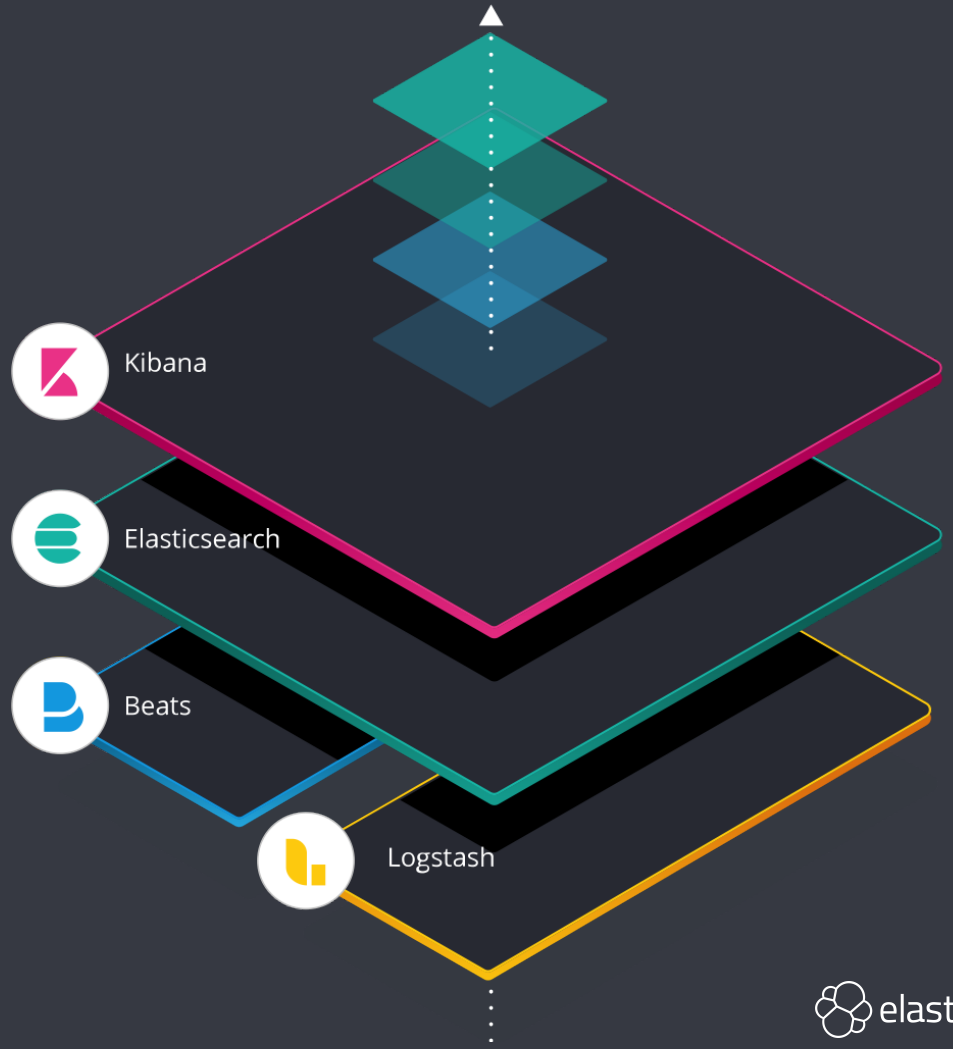
Elastic Stack

Visualize

Store

Ingest

Ingest



elastic

Solutions

APM

Search

Logs

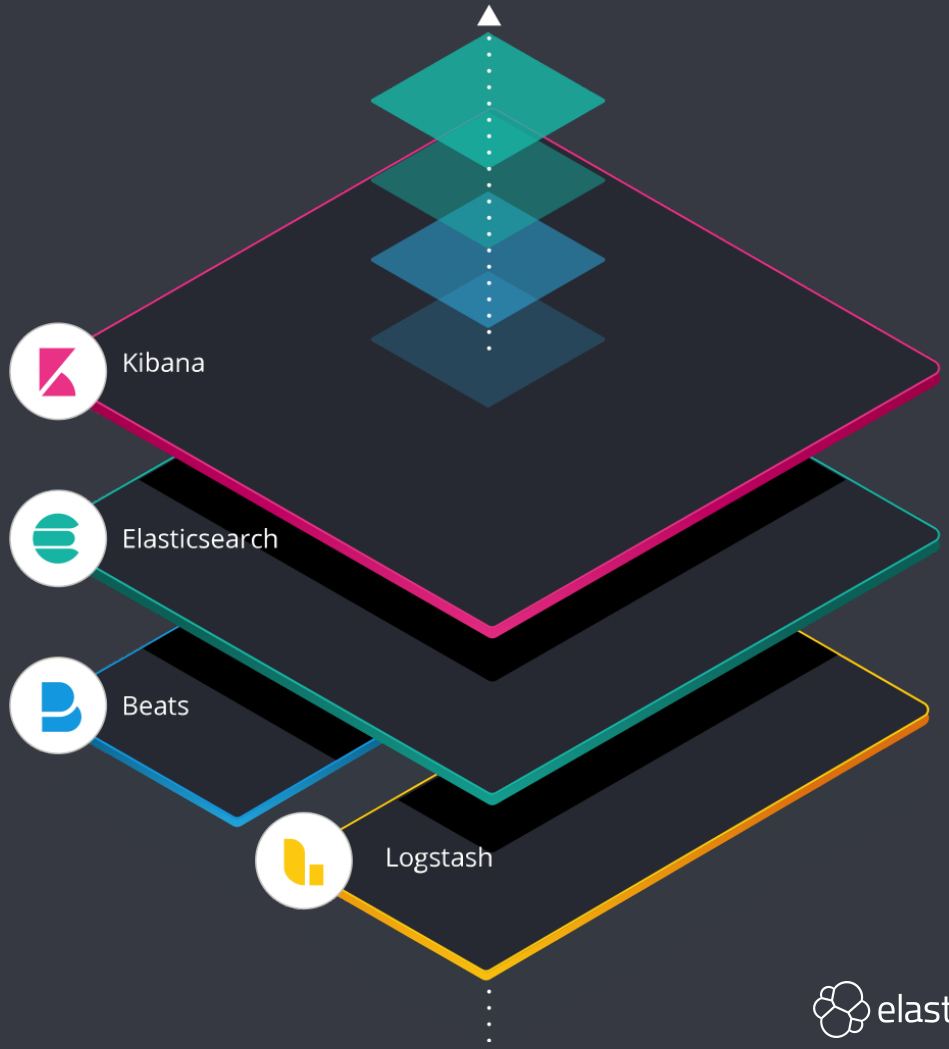
Uptime

Metrics

Analytics

SIEM

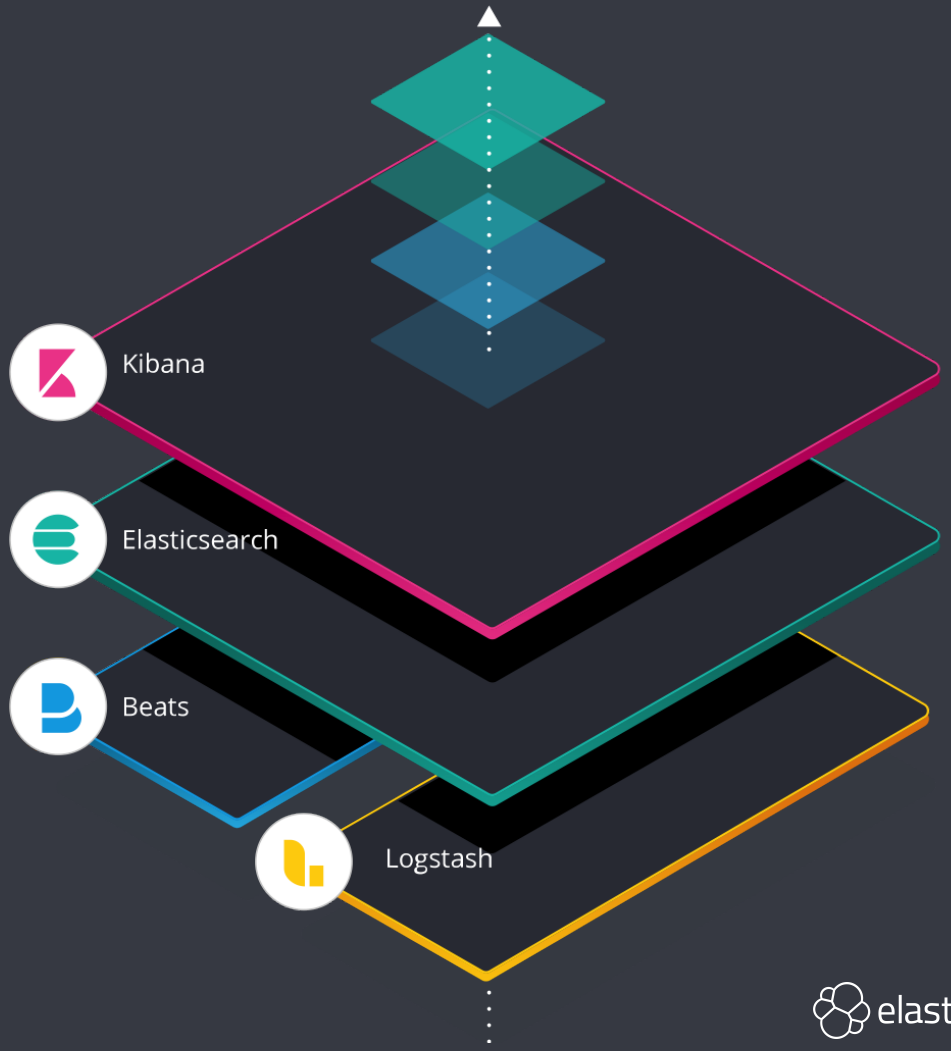
Maps



elastic

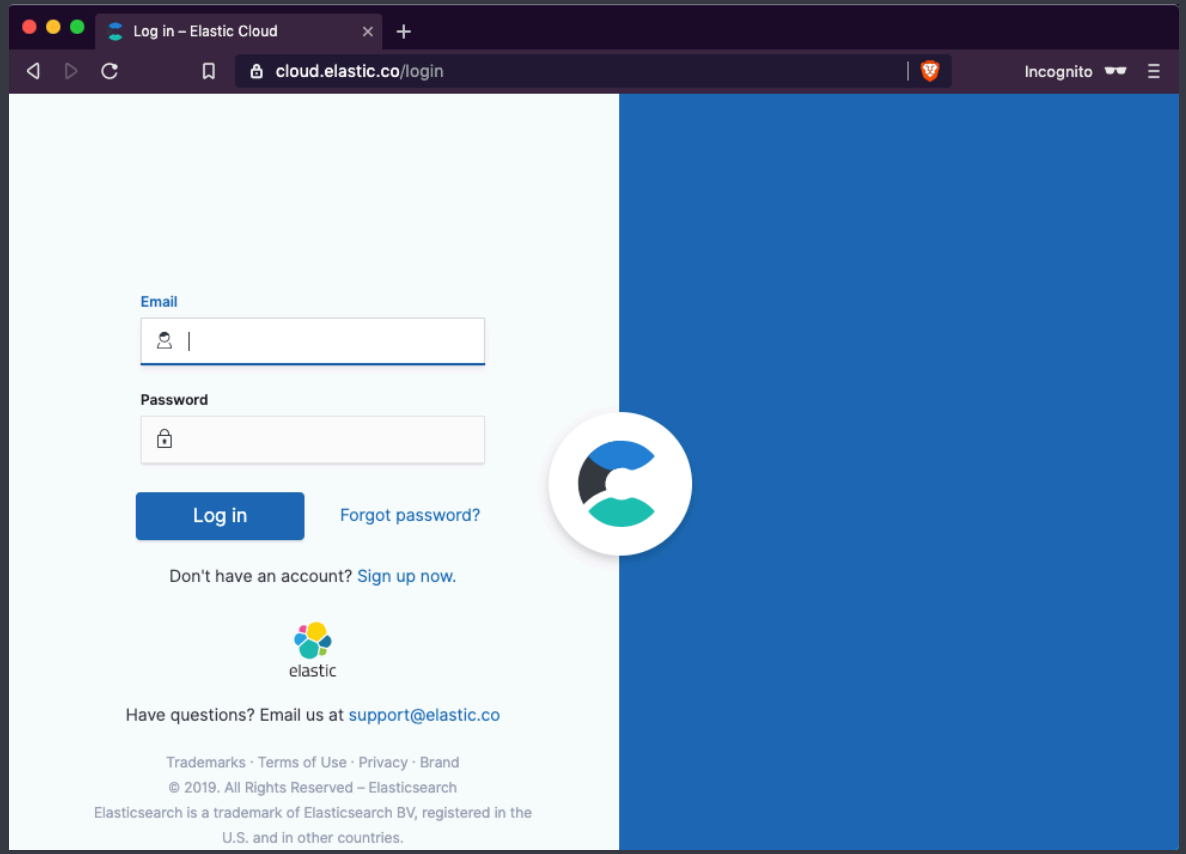
Deployment

- Elastic Cloud
- Elastic Cloud Enterprise
- Elastic Cloud on K8s
- Self hosted



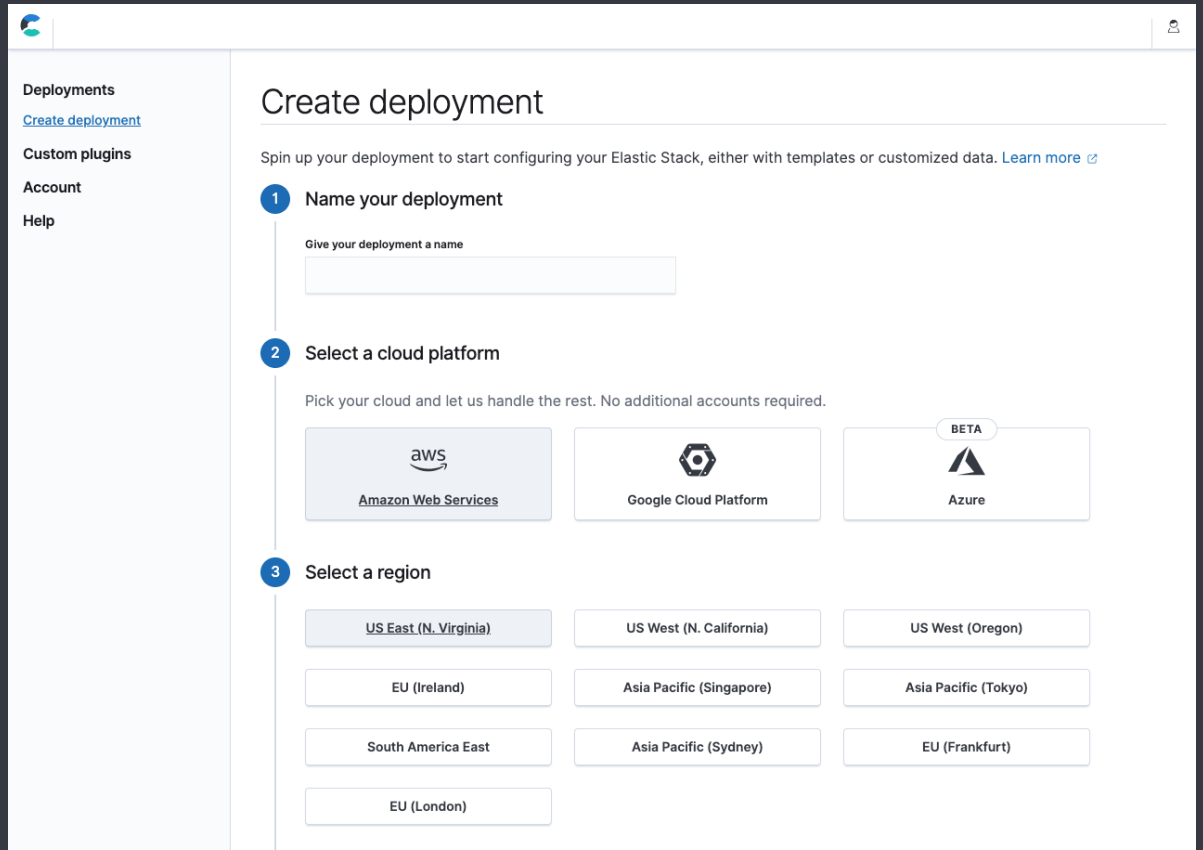
elastic

Elastic Cloud



elastic

Elastic Cloud



elastic

4 Set up your deployment

Elastic Stack version

7.4.2 Edit

Select a deployment to restore from its latest snapshot

Monitoring

Enable monitoring by shipping metrics to a deployment

5 Optimize your deployment

I/O Optimized

Recommended

Use for search and general all-purpose workloads. Includes a balance of compute, memory, and storage.

Default specs

Compute Optimized

Run CPU-intensive workloads or run smaller workloads cost-effectively when you need less memory and storage.

Default specs

Memory Optimized

Perform memory-intensive operations efficiently, including workloads with frequent aggregations.

Default specs

Hot-Warm Architecture

Use for time-series analytics and logging workloads that benefit from automatic index curation.

Default specs

Cross Cluster Search

Use to search data across one or more associated deployments

Default specs

Elastic Cloud supports many more options to cater to your specific use case such as hot-warm architecture optimized for logging, compute-focused setup optimized for analytics etc. Learn more

Deployment pricing

Hourly rate $0.3789

Create deployment | Customize deployment

elastic

Ingestion

elastic

Ingestion

- Read data
- Ship data
- Modify data
- Acknowledging
- Fail safety

Logstash is an open source, server-side data processing pipeline that ingests data from a multitude of sources simultaneously, transforms it, and then sends it to your favorite "stash."

https://www.elastic.co/products/logstash

Beats is the platform for single-purpose data shippers. They send data from hundreds or thousands of machines and systems to Logstash or Elasticsearch.

https://www.elastic.co/products/beats

Ingestion - Beats

- Filebeat
- Metricbeat
- Packetbeat
- Winlogbeat
- Auditbeat
- Heartbeat
- Functionbeat

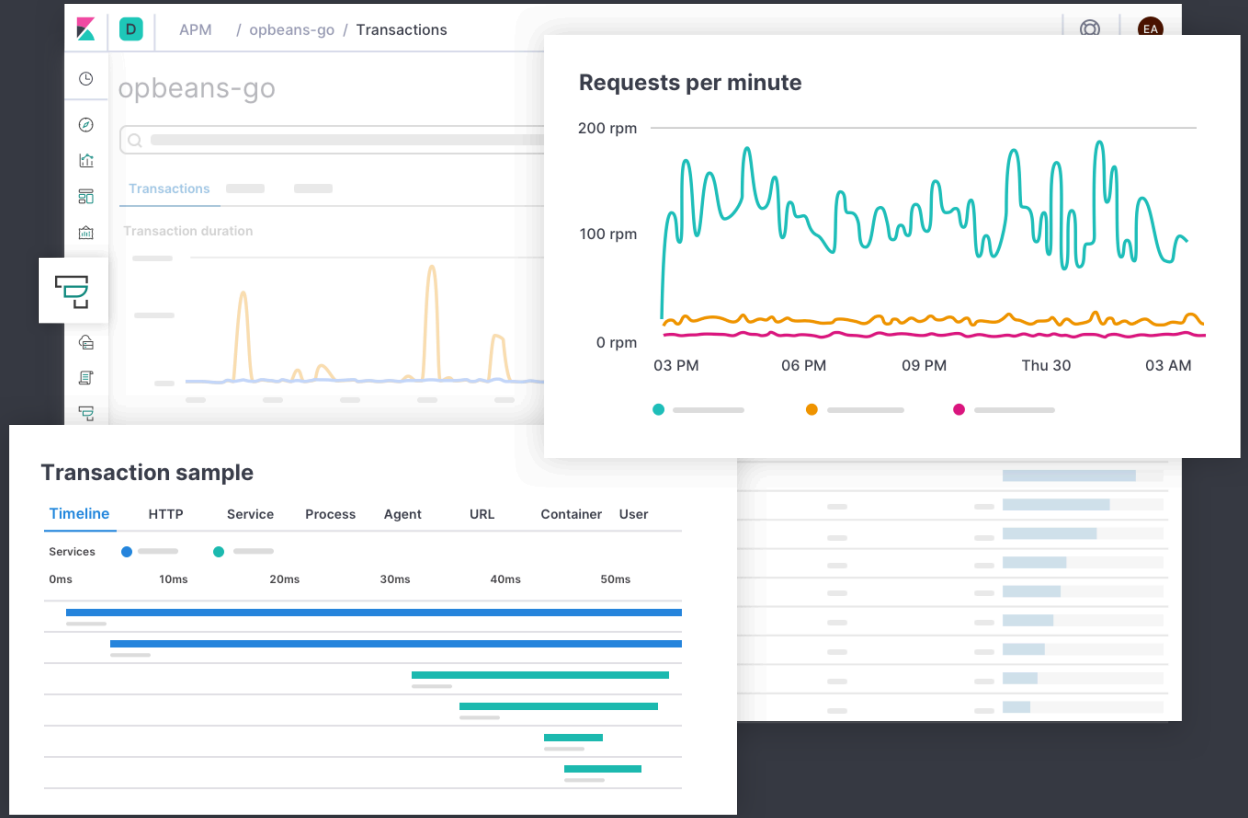
Today's setup

- Elasticsearch/Kibana on Elastic Cloud
- nginx running locally
- Filebeat: Ingest HTTP logs
- Metricbeat: Ingest metrics

DEMO

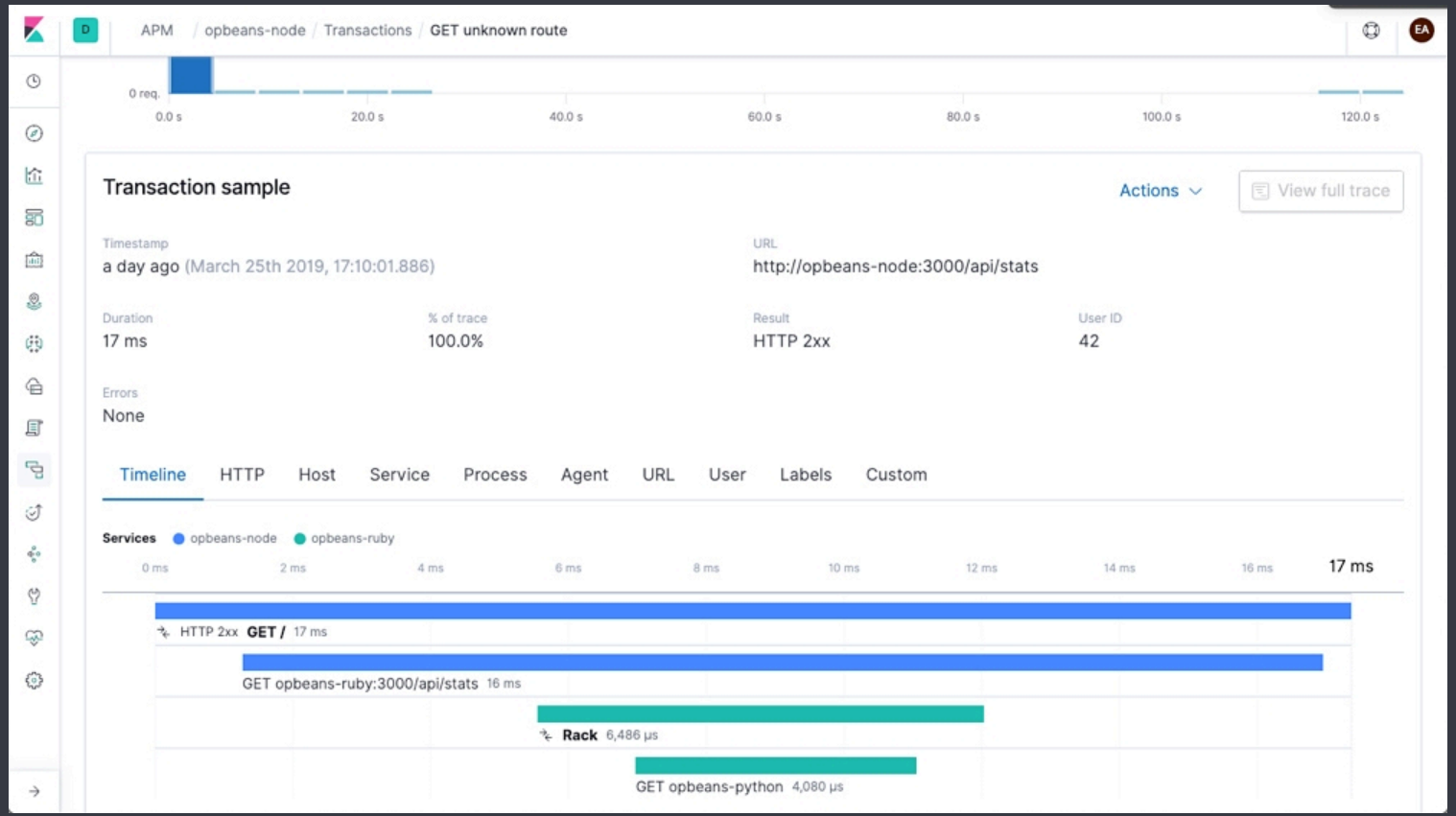
Next steps

APM & Distributed Tracing



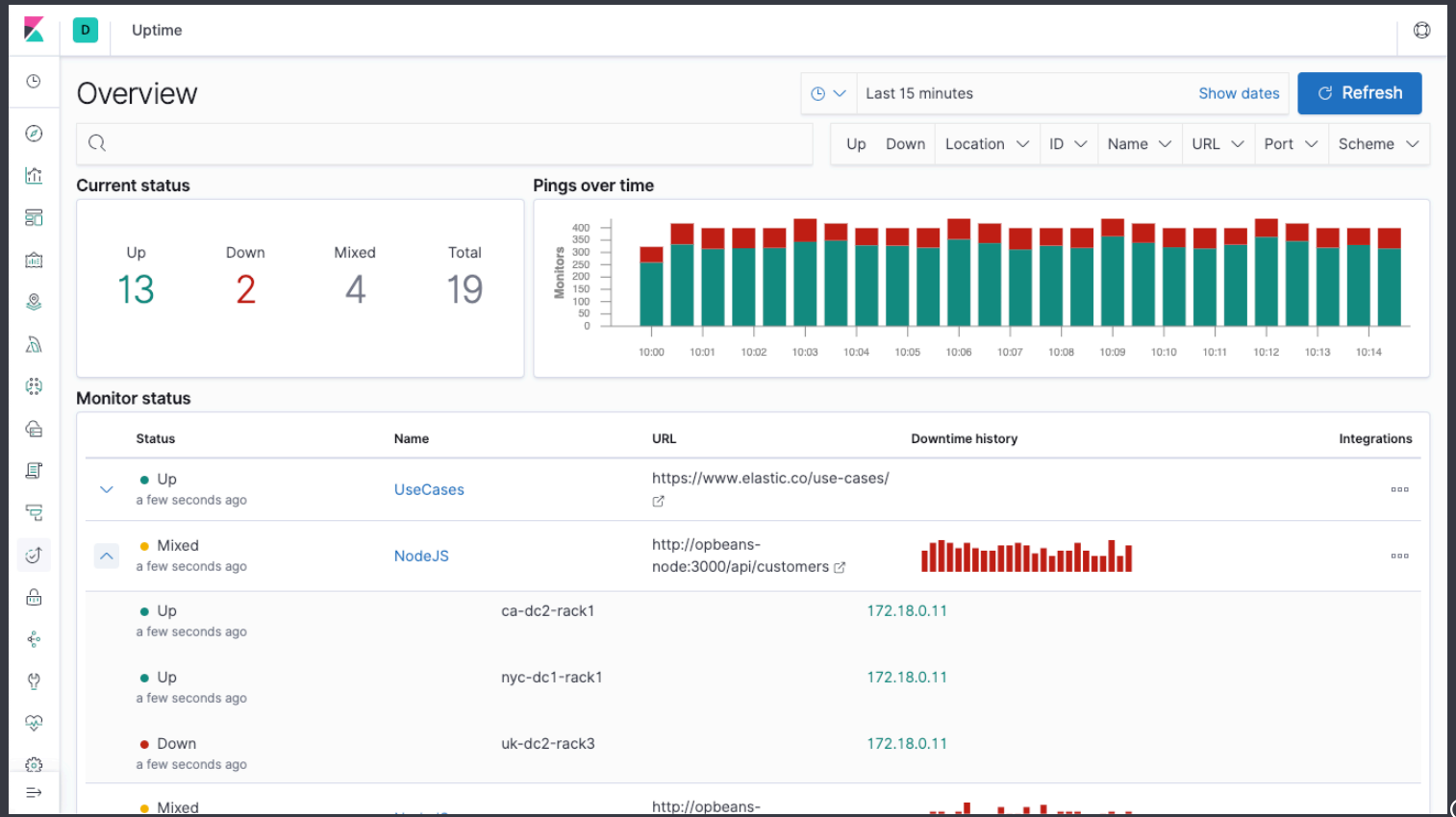
elastic

APM & Distributed Tracing



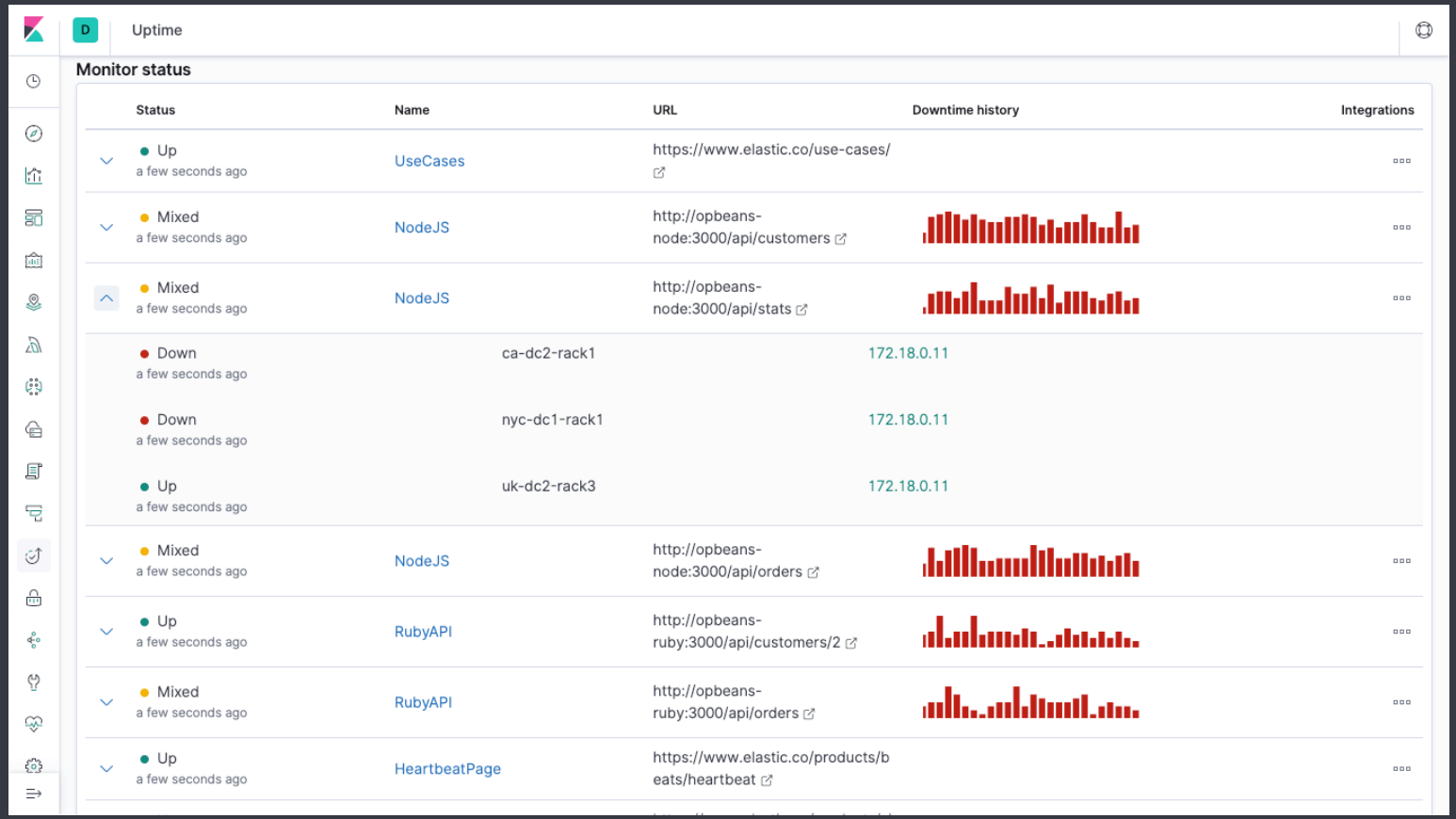
elastic

Uptime



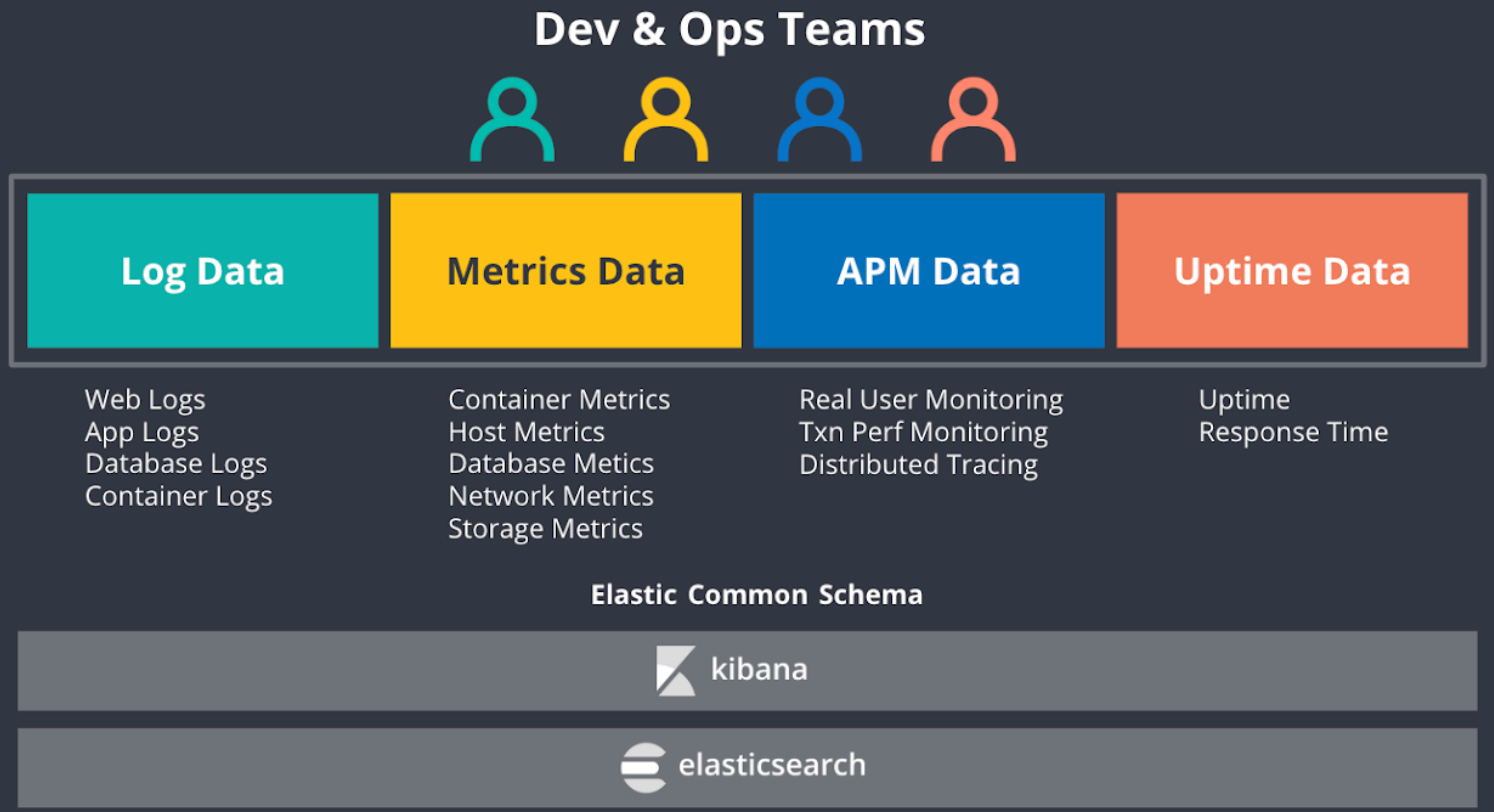
elastic

Uptime

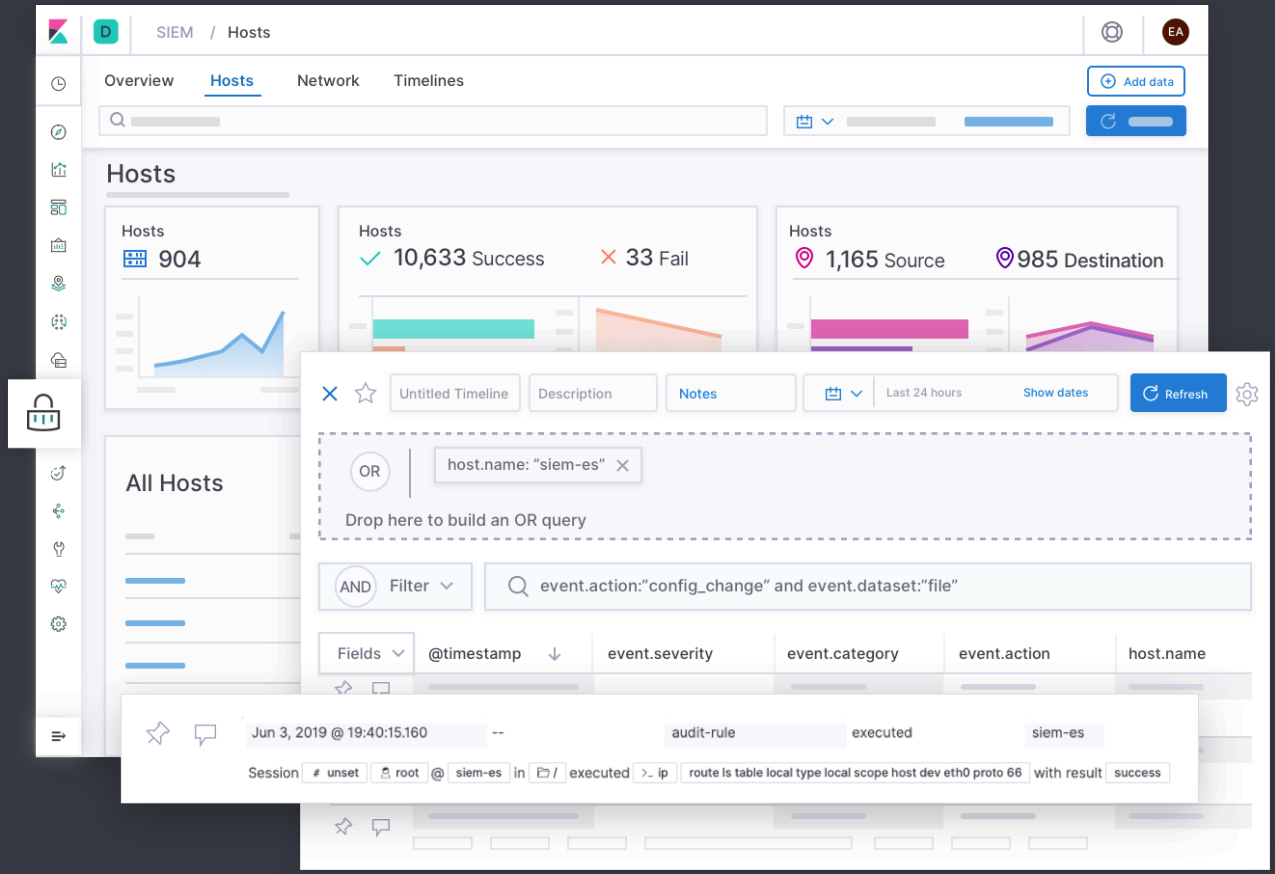


elastic

Elastic Approach to Observability



SIEM

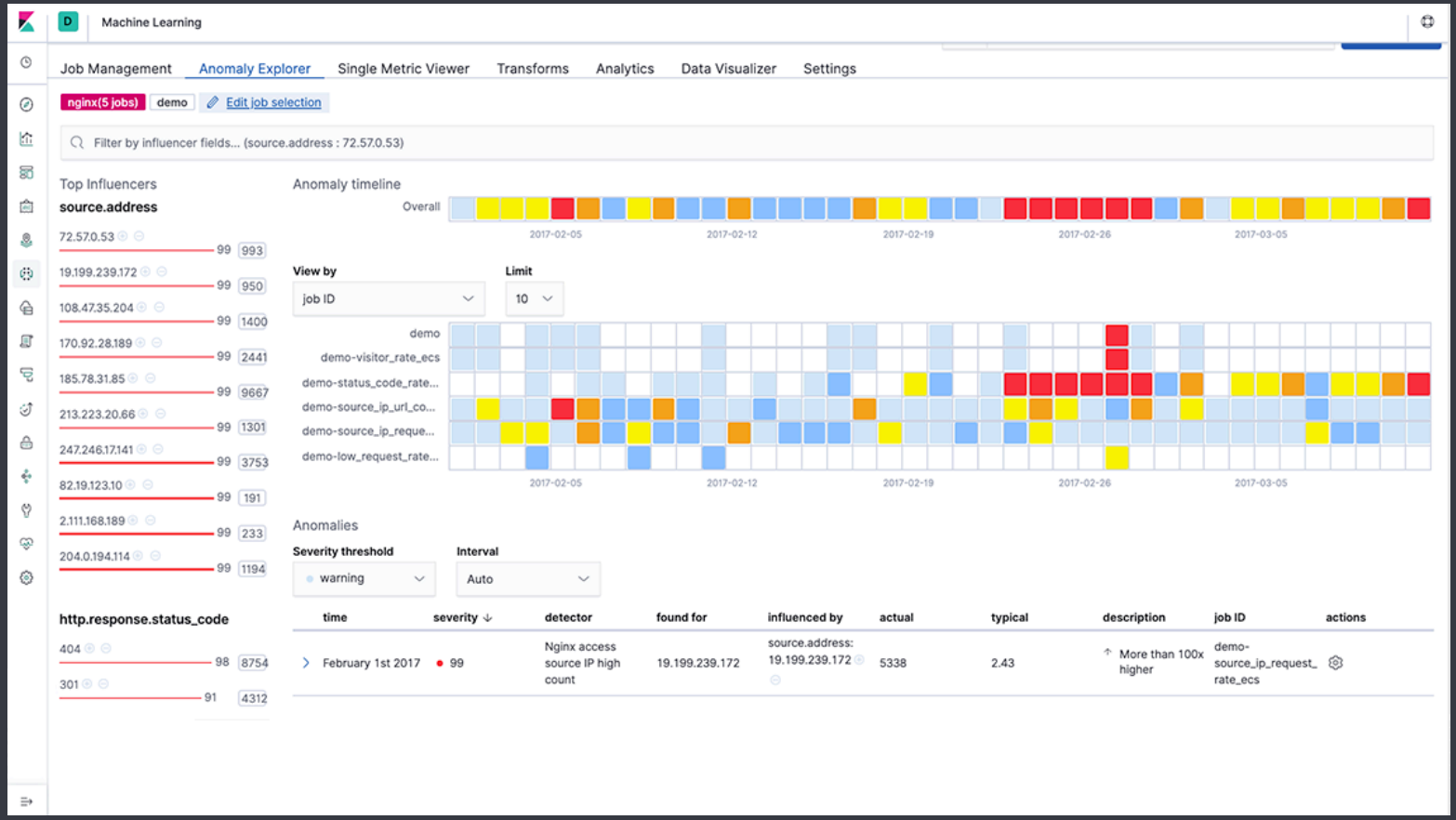


elastic

Machine Learning

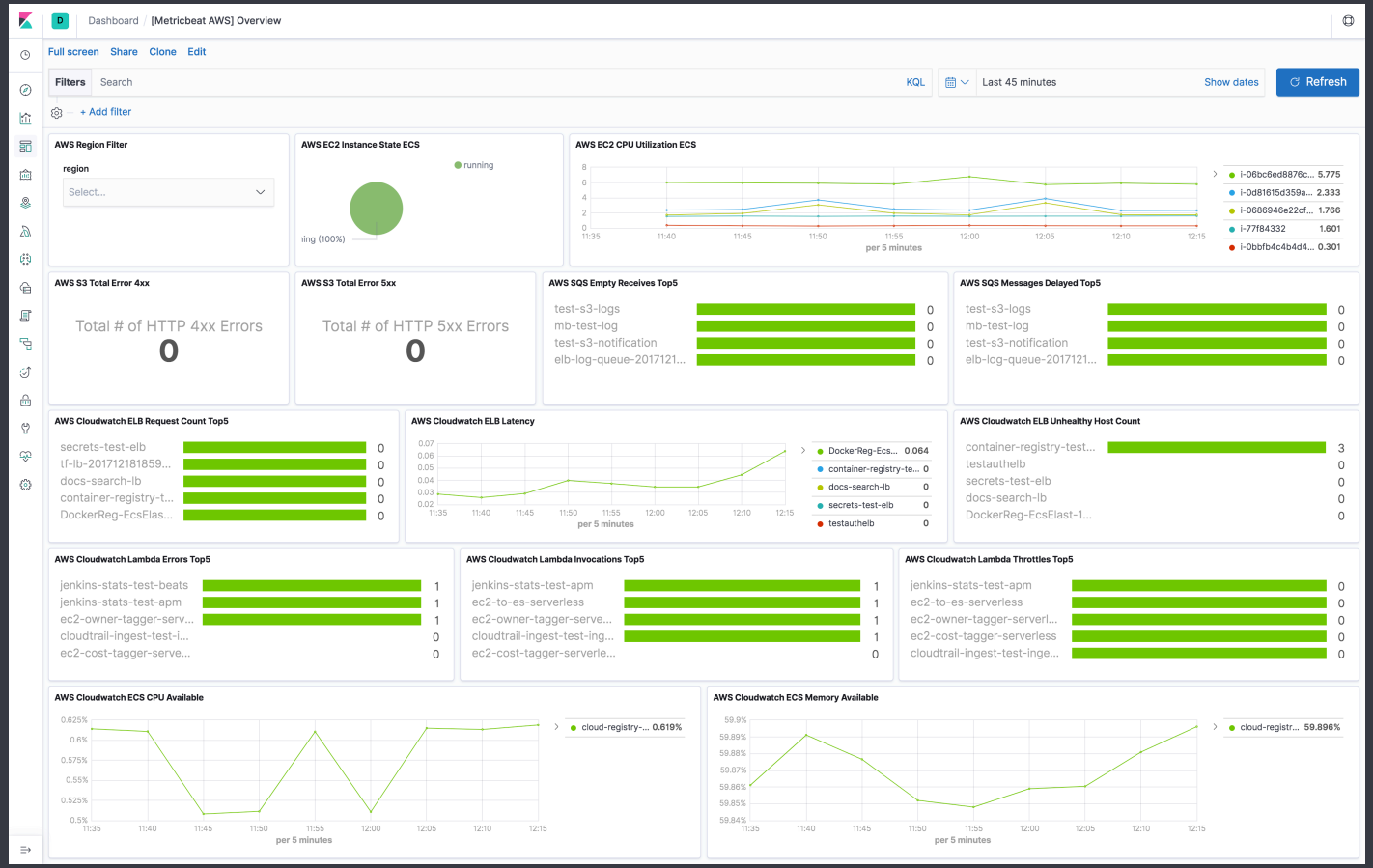
elastic

Machine Learning



elastic

Cloud: AWS

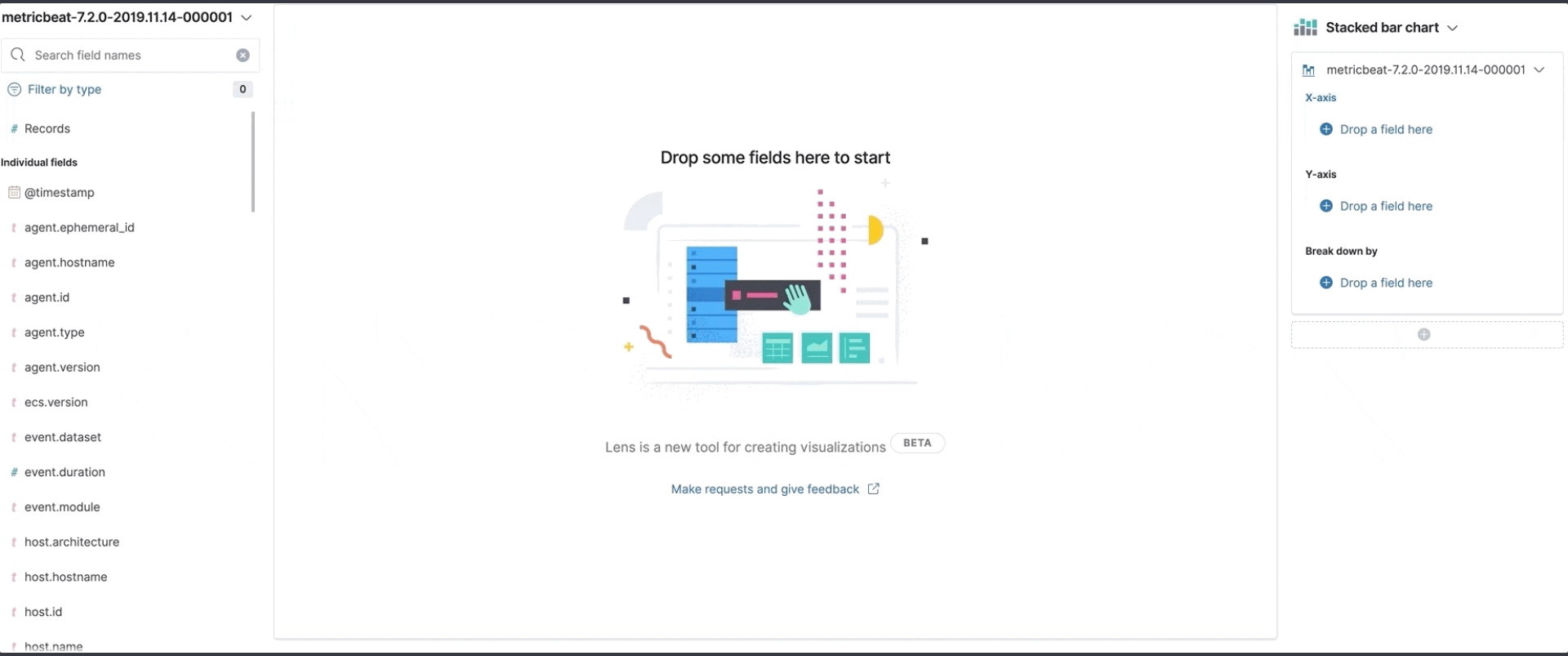


elastic

Cloud: Azure

elastic

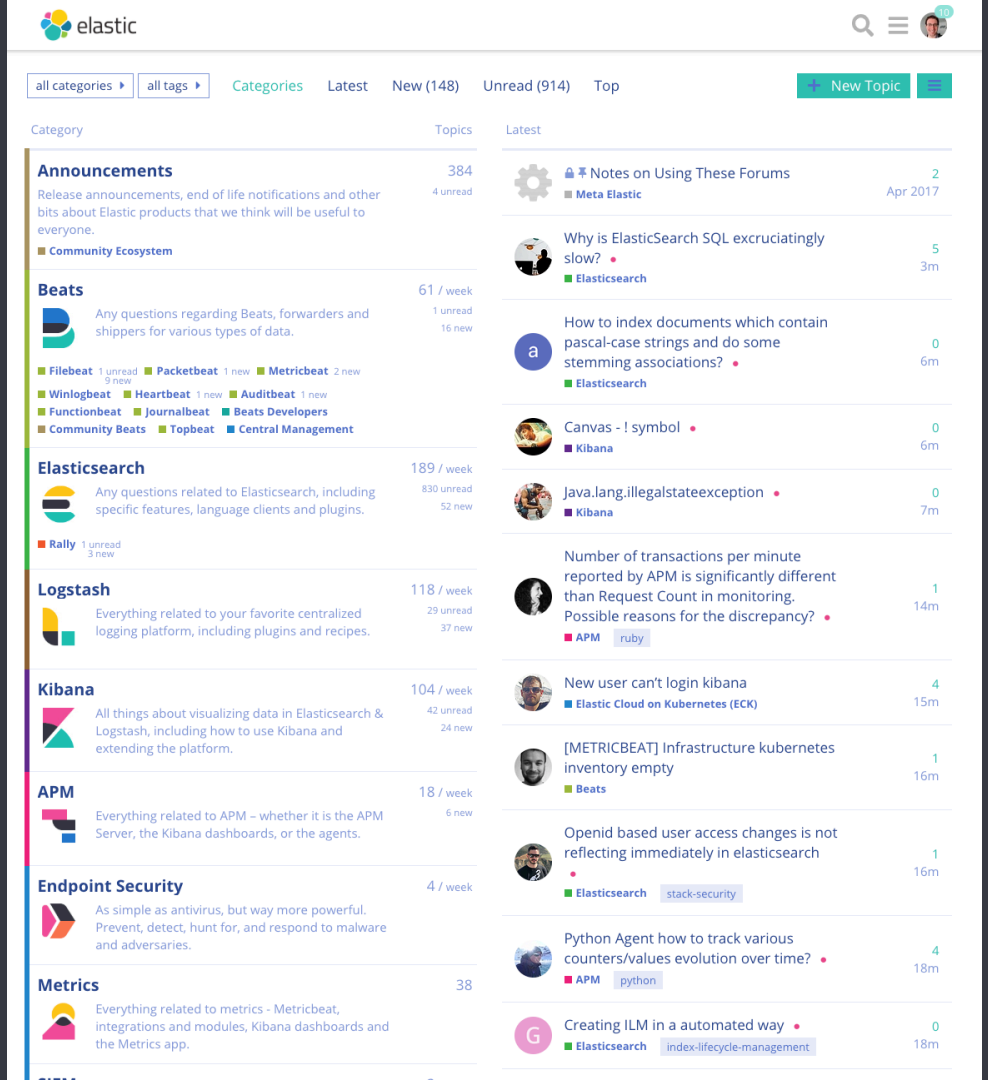
Kibana Lens



elastic

Further information

elastic

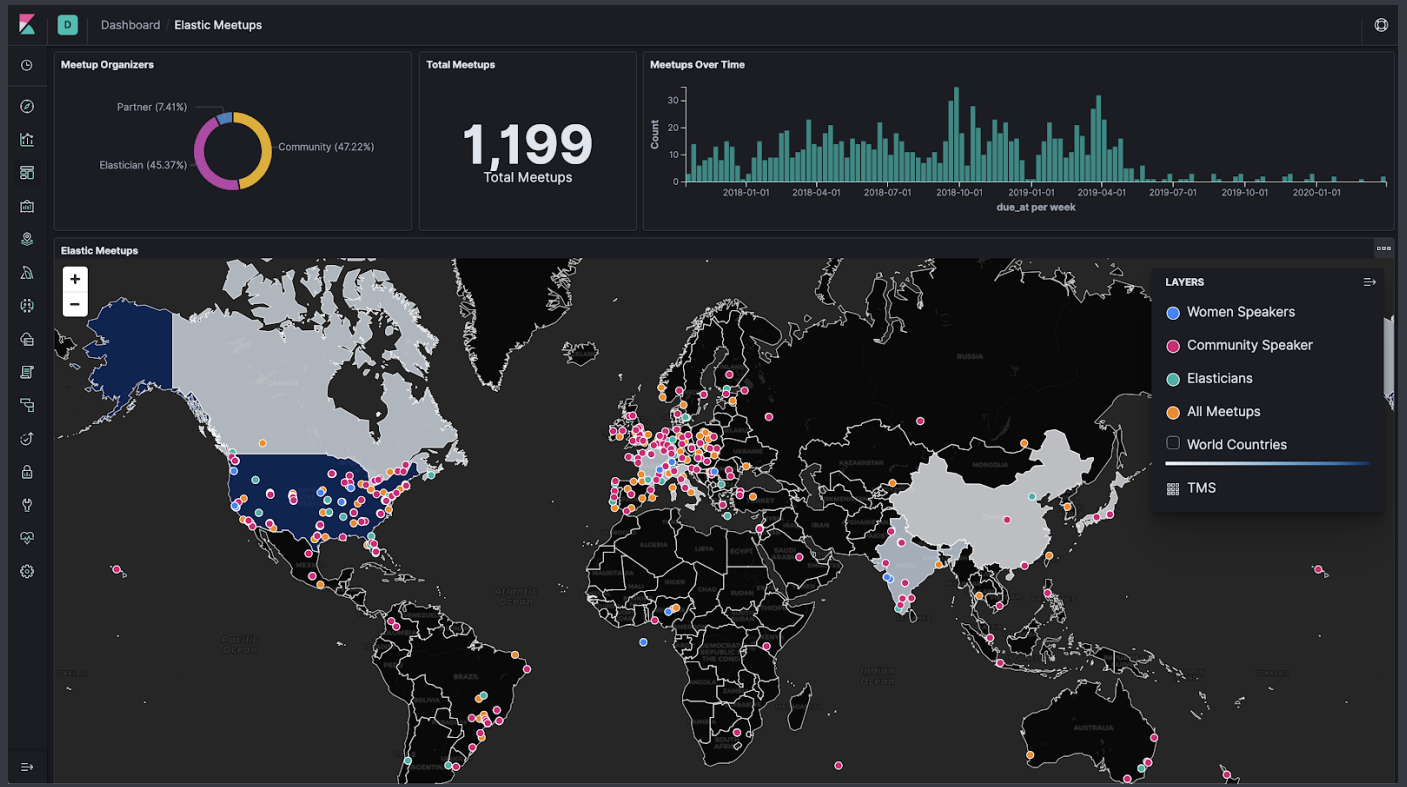


https://discuss.elastic.co

elastic

Join a local meetup!

https://community.elastic.co



elastic

elastic

contact

Elastic Training

Training Subscriptions | Private Training | Specializations | Certification | Catalog | Cart | Login

Official Elastic Training


Metrics


Elasticsearch Advanced Search


Logging


Data Science


Security Analytics


Elastic Stack Management

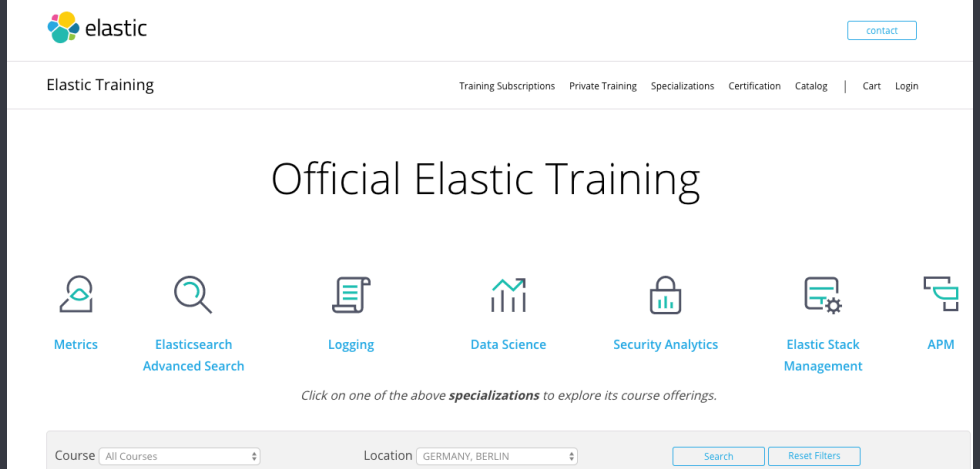

APM

*Click on one of the above **specializations** to explore its course offerings.*

Course All Courses | Location GERMANY, BERLIN | Search | Reset Filters

Elasticsearch Engineer I	BERLIN, Germany 50% off second seat	Dec 9, 2019 - Dec 10, 2019	Register Now
Elasticsearch Engineer II	BERLIN, Germany 50% off second seat	Dec 11, 2019 - Dec 12, 2019	Register Now

elastic



Elasticsearch Engineer I

DUSSELDORF, Germany

Unterrichtssprache ist Deutsch, Materialien auf Englisch. 50% Rabatt auf den zweiten Sitzplatz

Jan 13, 2020 - Jan 14, 2020

Register Now

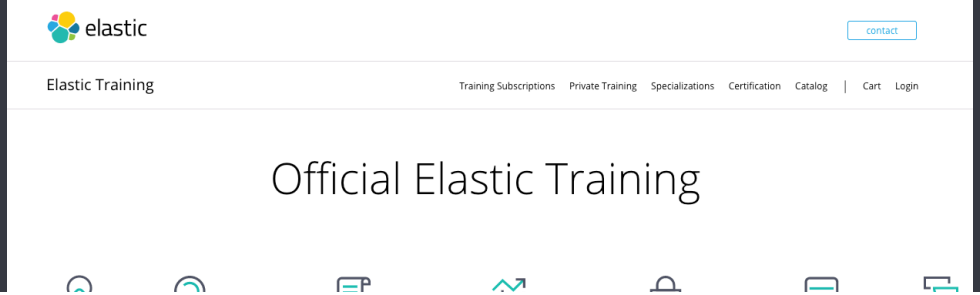
Elasticsearch Engineer II

DUSSELDORF, Germany

Unterrichtssprache ist Deutsch, Materialien auf Englisch. 50% Rabatt auf den zweiten Sitzplatz

Jan 15, 2020 - Jan 16, 2020

Register Now



Elasticsearch Engineer I	FRANKFURT, Germany Early bird expires 18 Dec 50% off second seat	Feb 12, 2020 - Feb 13, 2020	Register Now
Elasticsearch Engineer II	FRANKFURT, Germany Early bird expires 18 Dec 50% off second seat	Feb 12, 2020 - Feb 13, 2020	Register Now
Kibana Data and Ops Analyst	FRANKFURT, Germany Early bird expires 18 Dec 50% off second seat	Feb 12, 2020 - Feb 14, 2020	Register Now

elastic on TOUR

Learn More

Frankfurt

11 FEBRUARY 2020

REGISTER

SEE AGENDA

https://www.elastic.co/elasticon/tour/frankfurt

elastic

Q & A

elastic