



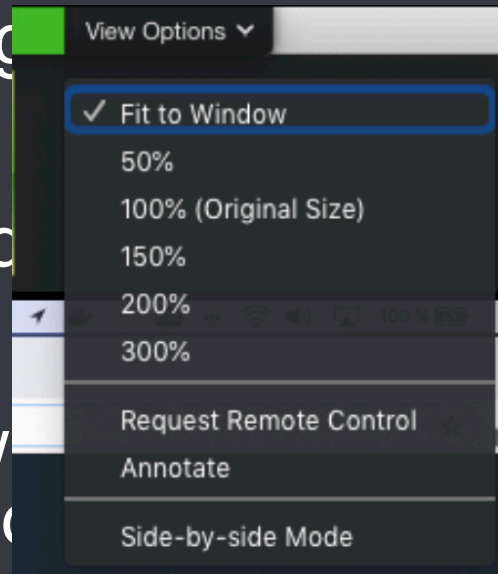
Der Elastic Stack für Logs und Metriken

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



Logistics

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



Agenda

Agenda

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

Logs & Metrics?

What is a log?

Nov 19 16:31:58 rhincodon syslogd[41]: ASL Sender Statistics

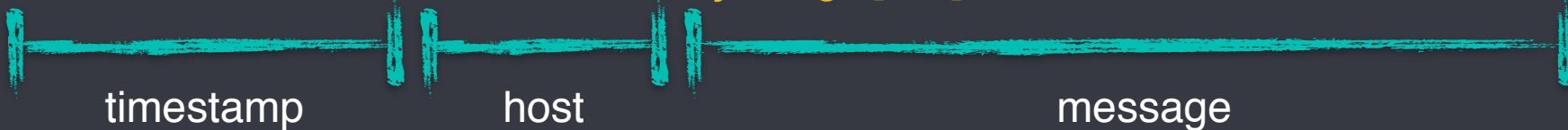


timestamp

message

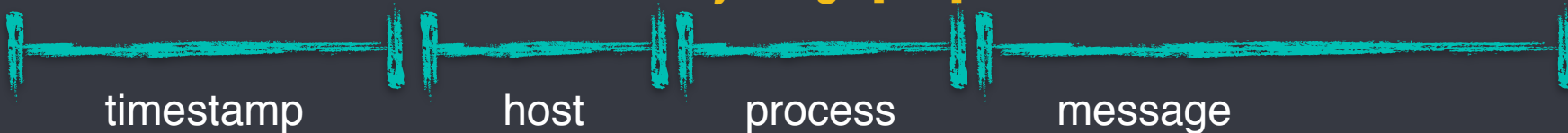
What is a log?

Nov 19 16:31:58 rhincodon syslogd[41]: ASL Sender Statistics



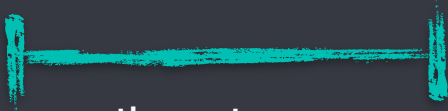
What is a structured log?

Nov 19 16:31:58 rhincodon syslogd[41]: ASL Sender Statistics



What is a log?

Nov 19 16:31:58



timestamp

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

Date normalization

Nov 19 16:31:58

Date normalization

Nov 19 16:31:58

19/Ju1/2015:08:13:42 +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

Date normalization

Nov 19 16:31:58

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

2015-01-01T12:10:30.123456789Z

2019-10-10

1420070400

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

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

Multi line events

```
[2019-07-25T00:10:02,240][WARN ][o.e.i.IndexService      ] [1563552203477145411] [migrate-bird-filebeat-7.0.0-alpha1-2019.07.25] 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) [elasticsearch-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.dïm"))))
  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]
```

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 Stack

Visualize



Kibana

Store



Elasticsearch

Ingest



Beats

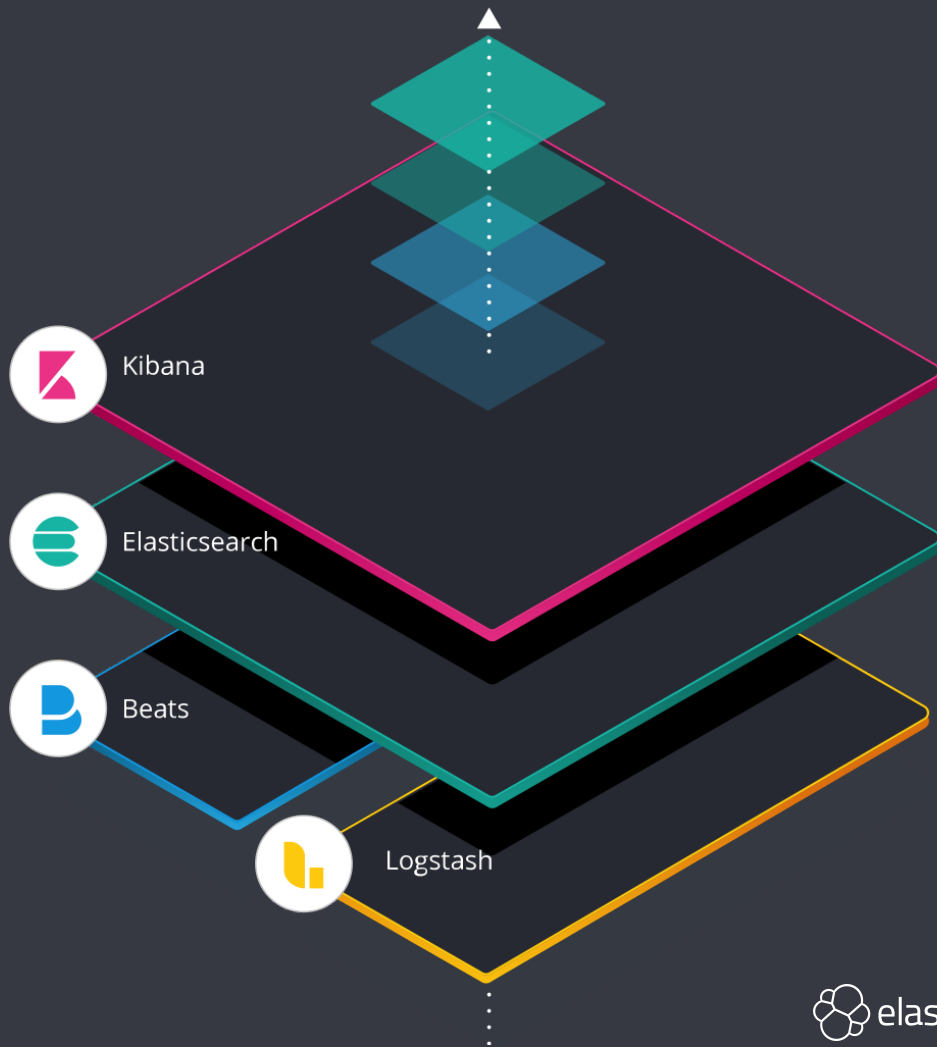
Ingest



Logstash

Solutions

APM
Search
Logs
Uptime
Metrics
Analytics
Maps
SIEM

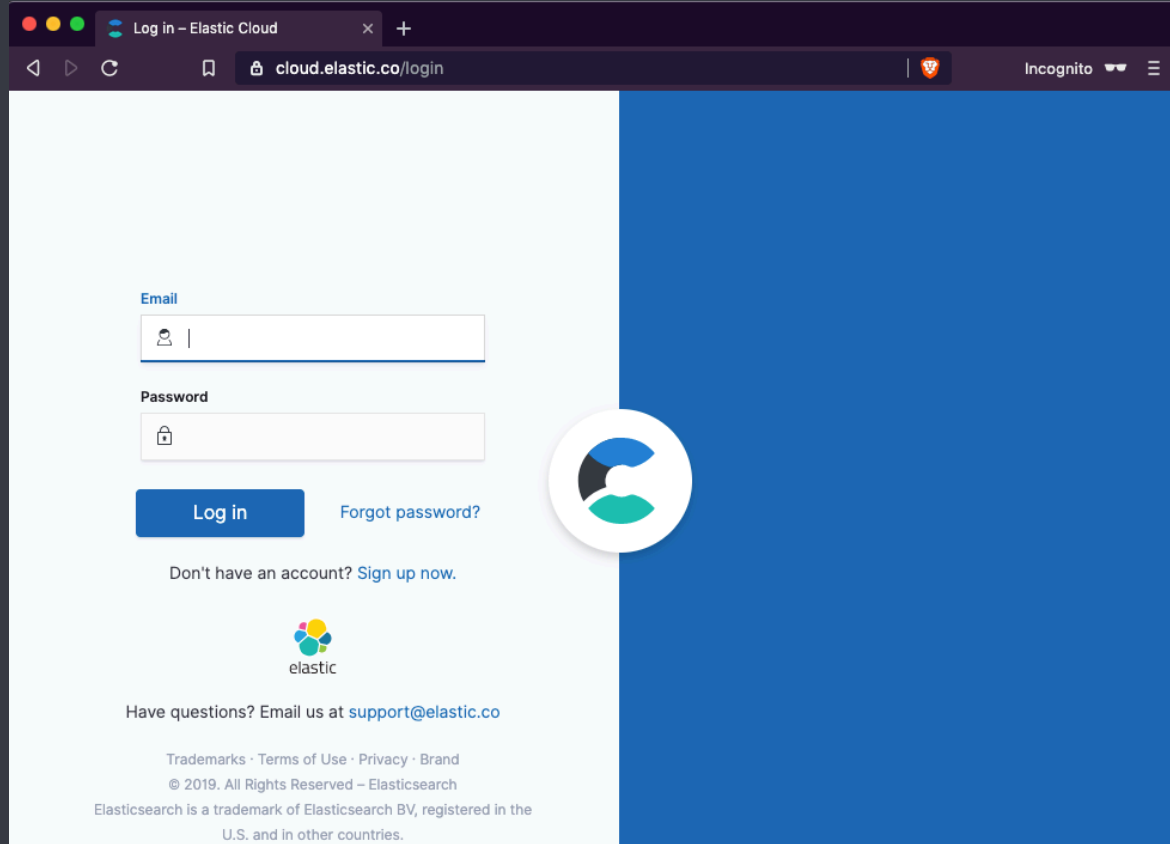


Deployment

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



Elastic Cloud



The image shows a browser window with the URL `cloud.elastic.co/login`. The page is titled "Log in - Elastic Cloud" and is displayed in an Incognito window. The login form includes an "Email" field with a person icon, a "Password" field with a lock icon, a blue "Log in" button, and a "Forgot password?" link. Below the form, there is a link to "Sign up now" for users without an account. The Elastic logo is centered below the form, followed by contact information: "Have questions? Email us at support@elastic.co". At the bottom, there are links for "Trademarks", "Terms of Use", "Privacy", and "Brand", along with copyright information: "© 2019. All Rights Reserved - Elasticsearch" and a trademark notice for Elasticsearch in the U.S. and other countries.

Log in - Elastic Cloud

cloud.elastic.co/login

Incognito

Email

Person icon |


Password

Lock icon

Log in

Forgot password?

Don't have an account? [Sign up now.](#)


elastic

Have questions? Email us at support@elastic.co

Trademarks · Terms of Use · Privacy · Brand

© 2019. All Rights Reserved - Elasticsearch

Elasticsearch is a trademark of Elasticsearch BV, registered in the U.S. and in other countries.

Elastic Cloud

The screenshot shows the 'Create deployment' page in the Elastic Cloud console. On the left is a navigation sidebar with links for 'Deployments', 'Custom plugins', 'Account', and 'Help'. The main content area is titled 'Create deployment' and includes a sub-header 'Spin up your deployment to start configuring your Elastic Stack, either with templates or customized data. Learn more'. The process is divided into three numbered steps: 1. Name your deployment (with a text input field), 2. Select a cloud platform (with buttons for Amazon Web Services, Google Cloud Platform, and BETA Azure), and 3. Select a region (with buttons for various global regions like US East, EU, and Asia Pacific).

Deployments
[Create deployment](#)

Custom plugins

Account

Help

Create deployment

Spin up your deployment to start configuring your Elastic Stack, either with templates or customized data. [Learn more](#)

- 1 Name your deployment**

Give your deployment a name
- 2 Select a cloud platform**

Pick your cloud and let us handle the rest. No additional accounts required.

aws
Amazon Web Services

Google Cloud Platform

BETA
Azure
- 3 Select a region**

US East (N. Virginia)

US West (N. California)

US West (Oregon)

EU (Ireland)

Asia Pacific (Singapore)

Asia Pacific (Tokyo)

South America East

Asia Pacific (Sydney)

EU (Frankfurt)

EU (London)

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](#)

Ingestion

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

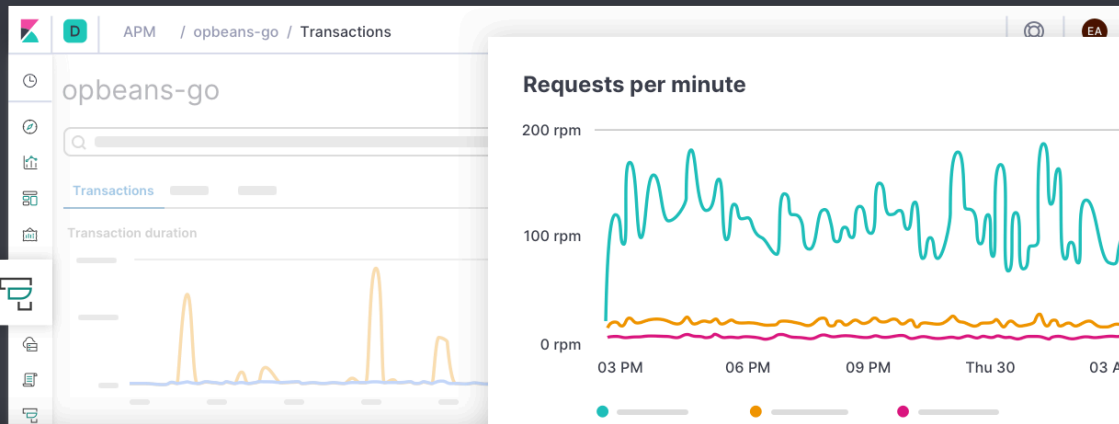


DEMO

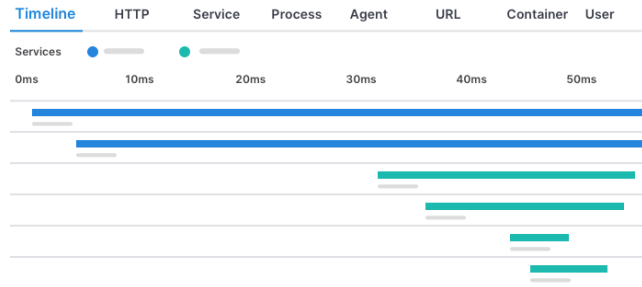


Next steps

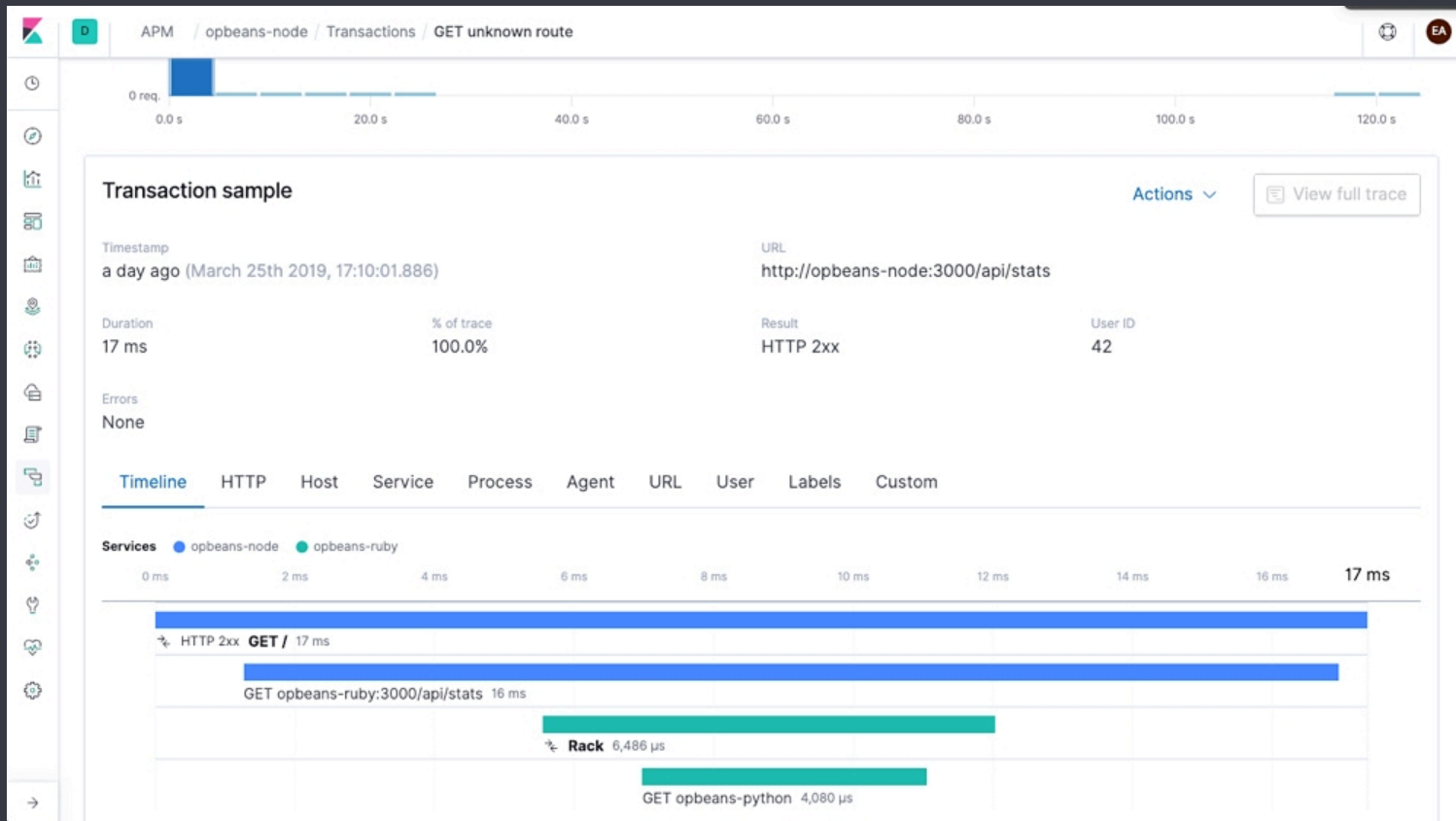
APM & Distributed Tracing



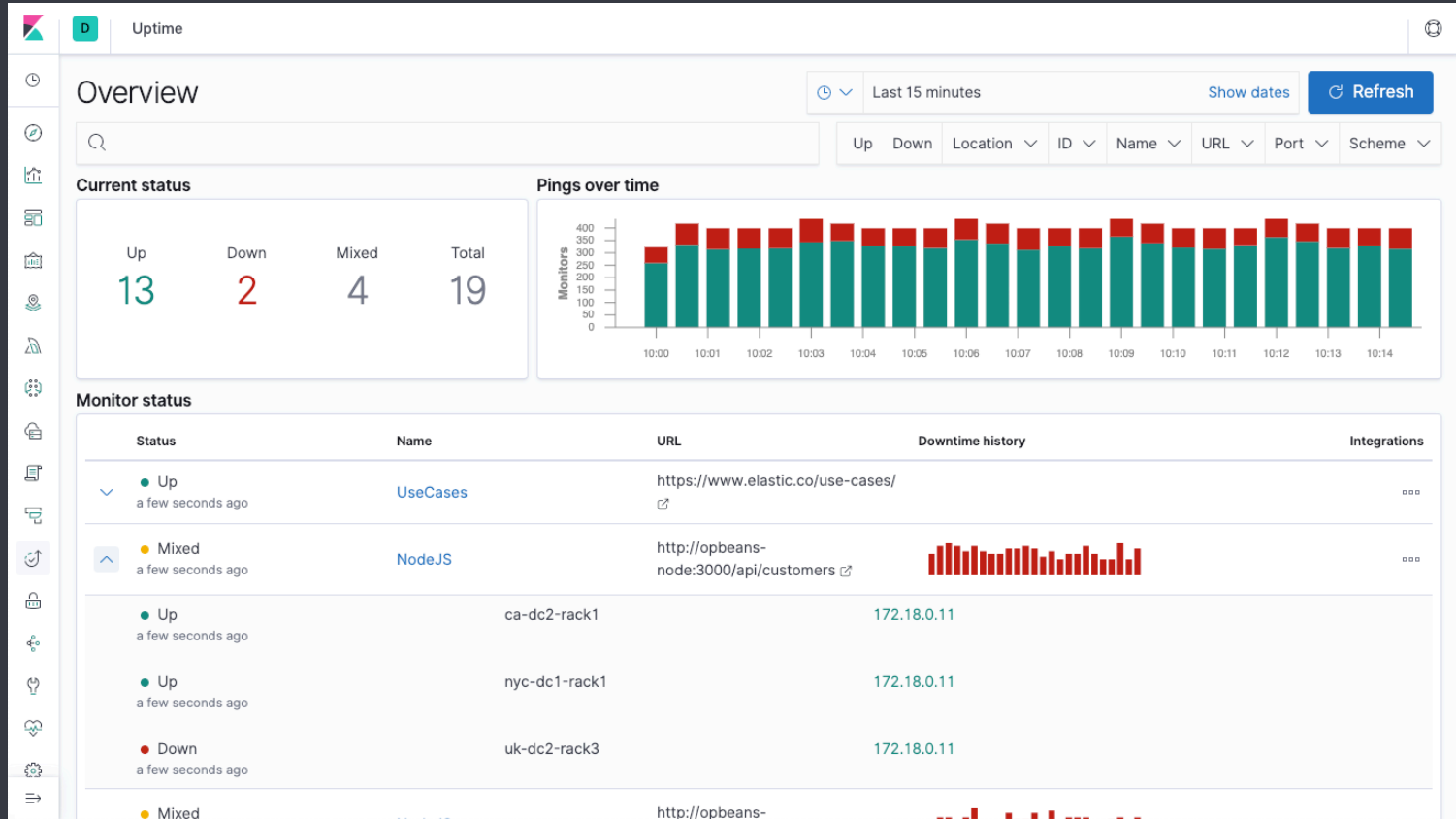
Transaction sample



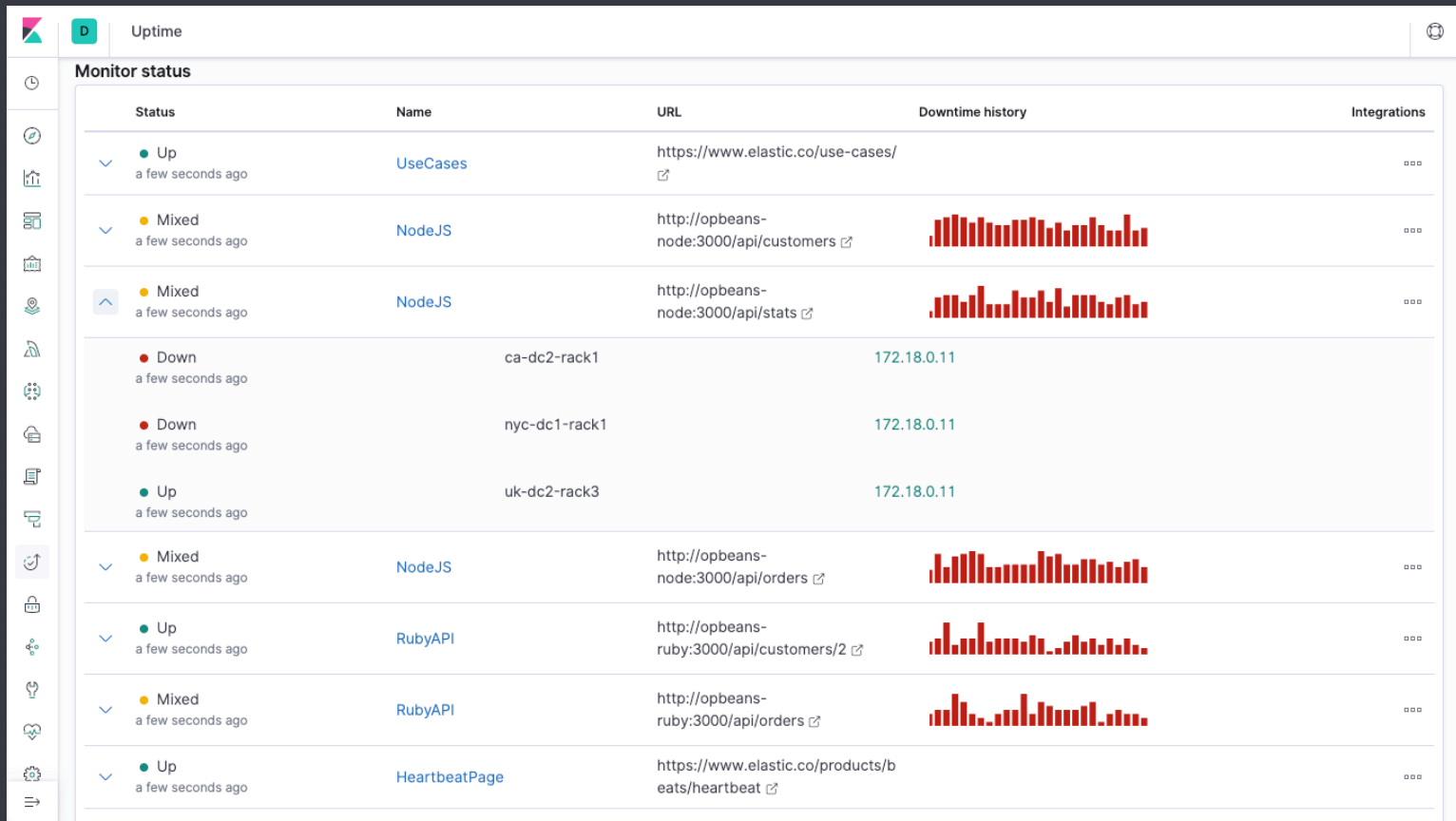
APM & Distributed Tracing



Uptime



Uptime



Elastic Approach to Observability

Dev & Ops Teams



Log Data

Metrics Data

APM Data

Uptime Data

Web Logs
App Logs
Database Logs
Container Logs

Container Metrics
Host Metrics
Database Metrics
Network Metrics
Storage Metrics

Real User Monitoring
Txn Perf Monitoring
Distributed Tracing

Uptime
Response Time

Elastic Common Schema



SIEM

The screenshot displays the Elastic SIEM interface for the 'Hosts' section. The top navigation bar includes 'Overview', 'Hosts', 'Network', and 'Timelines'. The 'Hosts' overview contains three summary cards: a total of 904 hosts, 10,633 successful events and 33 failed events, and 1,165 source hosts with 985 destination hosts. A search bar and a 'Refresh' button are visible at the top right.

A query builder window is open, showing an 'Untitled Timeline' with a search query: `host.name: "siem-es"`. Below this, an 'AND' filter is applied with the query: `event.action:"config_change" and event.dataset:"file"`. The 'Fields' section lists: `@timestamp`, `event.severity`, `event.category`, `event.action`, and `host.name`.

The search results snippet shows an event from 'Jun 3, 2019 @ 19:40:15.160' with the type 'audit-rule' and action 'executed' on host 'siem-es'. The session details are: `Session # unset @ siem-es in / executed >. ip route is table local type local scope host dev eth0 proto 66 with result success`.

Machine Learning



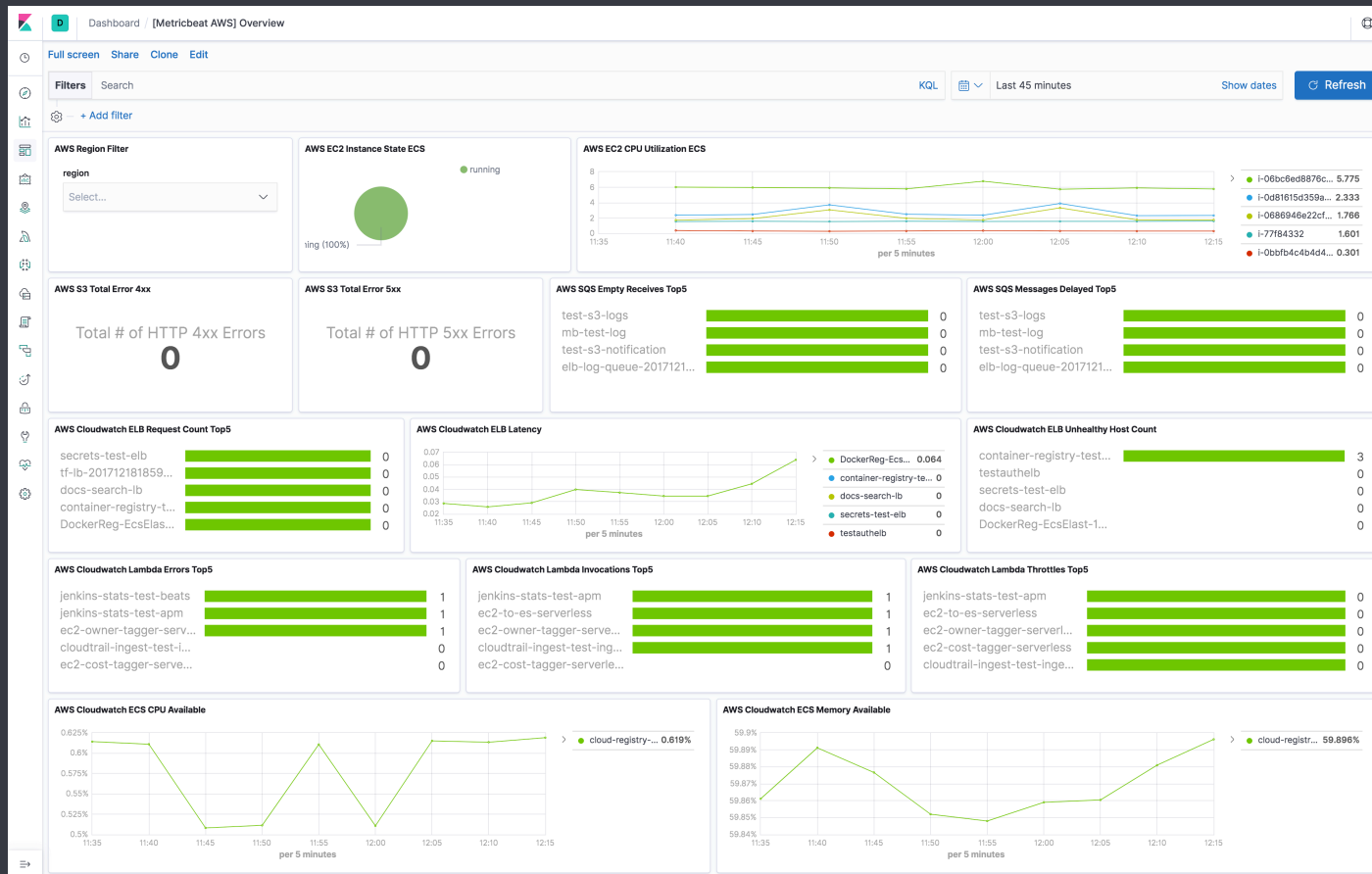
Machine Learning

The screenshot displays the Elastic Machine Learning interface for a job named 'nginx(5 jobs)'. The interface is divided into several sections:

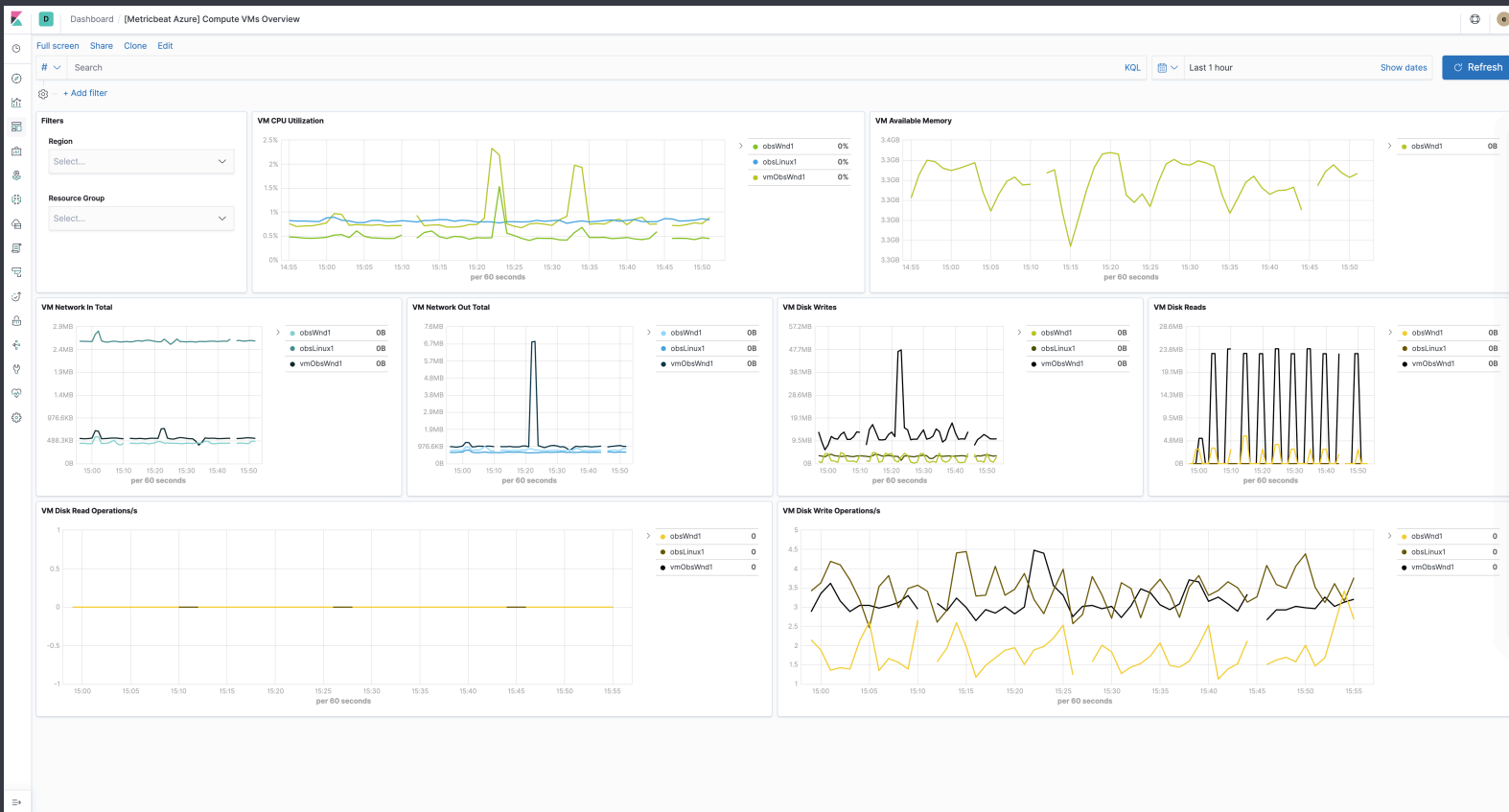
- Job Management:** Shows the job name 'nginx(5 jobs)', a 'demo' tag, and an 'Edit job selection' link.
- Filter:** A search bar with the text 'Filter by influencer fields... (source.address : 72.570.53)'. Below it, a 'Top Influencers' list for 'source.address' shows IP addresses and their corresponding counts (e.g., 72.570.53 with 993).
- Anomaly Timeline:** A horizontal bar chart showing the overall anomaly timeline from 2017-02-05 to 2017-03-05. Below it, a 'View by' dropdown is set to 'job ID' with a 'Limit' of 10. A heatmap shows anomalies for various jobs, with 'demo' and 'demo-source_ip_url_co...' showing significant activity.
- Anomalies Table:** A table listing detected anomalies with columns for time, severity, detector, found for, influenced by, actual, typical, description, job ID, and actions.

time	severity ↓	detector	found for	influenced by	actual	typical	description	job ID	actions
> February 1st 2017	● 99	Nginx access source IP high count	19.199.239.172	source.address: 19.199.239.172	5338	2.43	↑ More than 100x higher	demo-source_ip_request_rate_ecs	

Cloud: AWS



Cloud: Azure



Kibana Lens

metricbeat-7.2.0-2019.11.14-000001

Search field names

Filter by type 0

Records

Individual fields

@timestamp

agent.ephemeral_id

agent.hostname

agent.id

agent.type

agent.version

ecs.version

event.dataset

event.duration

event.module

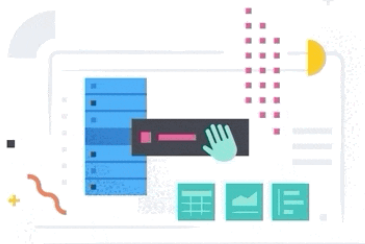
host.architecture

host.hostname

host.id

host_name

Drop some fields here to start



Lens is a new tool for creating visualizations **BETA**

[Make requests and give feedback](#)

Stacked bar chart

metricbeat-7.2.0-2019.11.14-000001

X-axis

+ Drop a field here

Y-axis

+ Drop a field here

Break down by

+ Drop a field here

+ Drop a field here

Further information

Category Topics

Announcements 384

Release announcements, end of life notifications and other bits about Elastic products that we think will be useful to everyone.

Community Ecosystem

Beats 61 / week

Any questions regarding Beats, forwarders and shippers for various types of data.

- Filebeat 1 unread 9 new
- Packetbeat 1 new
- Metricbeat 2 new
- Winlogbeat
- Heartbeat 1 new
- Auditbeat 1 new
- Functionbeat
- Journalbeat
- Beats Developers
- Community Beats
- Topbeat
- Central Management

Elasticsearch 189 / week

Any questions related to Elasticsearch, including specific features, language clients and plugins.

Rally 1 unread 3 new

Logstash 118 / week

Everything related to your favorite centralized logging platform, including plugins and recipes.

Kibana 104 / week

All things about visualizing data in Elasticsearch & Logstash, including how to use Kibana and extending the platform.

APM 18 / week

Everything related to APM - whether it is the APM Server, the Kibana dashboards, or the agents.

Endpoint Security 4 / week

As simple as antivirus, but way more powerful. Prevent, detect, hunt for, and respond to malware and adversaries.

Metrics 38

Everything related to metrics - Metricbeat, integrations and modules, Kibana dashboards and the Metrics app.

Latest

[Notes on Using These Forums](#) 2
Apr 2017
Meta Elastic

[Why is Elasticsearch SQL excruciatingly slow?](#) 5
3m
Elasticsearch

[How to index documents which contain pascal-case strings and do some stemming associations?](#) 0
6m
Elasticsearch

[Canvas - ! symbol](#) 0
6m
Kibana

[Java.lang.illegalstateexception](#) 0
7m
Kibana

[Number of transactions per minute reported by APM is significantly different than Request Count in monitoring. Possible reasons for the discrepancy?](#) 1
14m
APM ruby

[New user can't login kibana](#) 4
15m
Elastic Cloud on Kubernetes (ECK)

[\[METRICBEAT\] Infrastructure kubernetes inventory empty](#) 1
16m
Beats

[Openid based user access changes is not reflecting immediately in elasticsearch](#) 1
16m
Elasticsearch stack-security

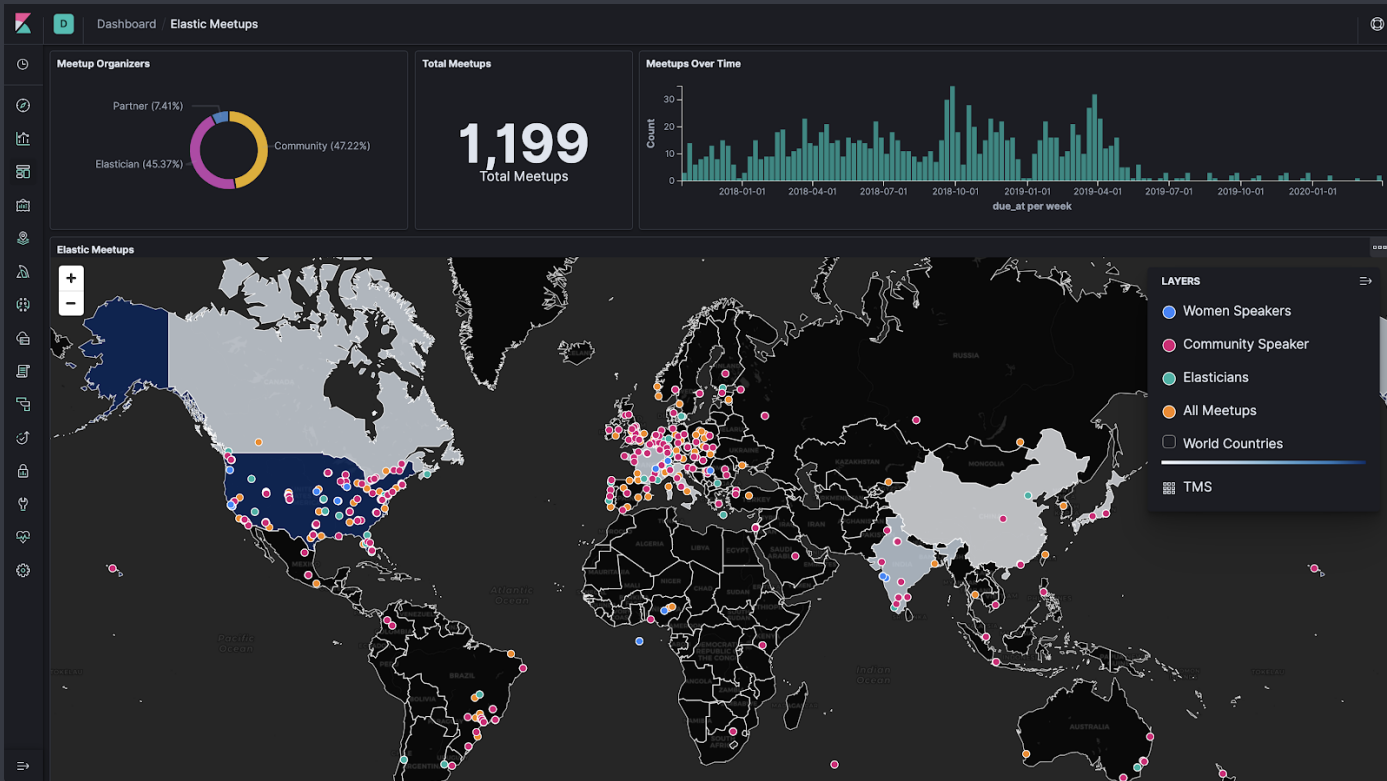
[Python Agent how to track various counters/values evolution over time?](#) 4
18m
APM python

[Creating ILM in a automated way](#) 0
18m
Elasticsearch index-lifecycle-management

<https://discuss.elastic.co>

Join a local meetup!

<https://community.elastic.co>



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 Location [Search](#)[Reset Filters](#)[Elasticsearch Engineer I](#)[BERLIN, Germany](#)

Dec 9, 2019 -

Dec 10, 2019

[Register Now](#)

50% off second seat

[Elasticsearch Engineer II](#)[BERLIN, Germany](#)

Dec 11, 2019 -

Dec 12, 2019

[Register Now](#)

50% off second seat

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 Location

Elasticsearch Engineer I

DUSSELDORF, GermanyJan 13, 2020 -
Jan 14, 2020

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

Elasticsearch Engineer II

DUSSELDORF, GermanyJan 15, 2020 -
Jan 16, 2020

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

Official Elastic Training



Elasticsearch Engineer I

FRANKFURT, Germany

Feb 12, 2020 -

[Register Now](#)

Feb 13, 2020

Early bird expires 18 Dec

50% off second seat

Elasticsearch Engineer II

FRANKFURT, Germany

Feb 12, 2020 -

[Register Now](#)

Feb 13, 2020

Early bird expires 18 Dec

50% off second seat

Kibana Data and Ops Analyst

FRANKFURT, Germany

Feb 12, 2020 -

[Register Now](#)

Feb 14, 2020

Early bird expires 18 Dec

50% off second seat

Frankfurt

11 FEBRUARY 2020

[REGISTER](#)

[SEE AGENDA](#)



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



Q & A