

Elasticsearch - A hands-on introduction

Alexander Reelsen

Community Advocate

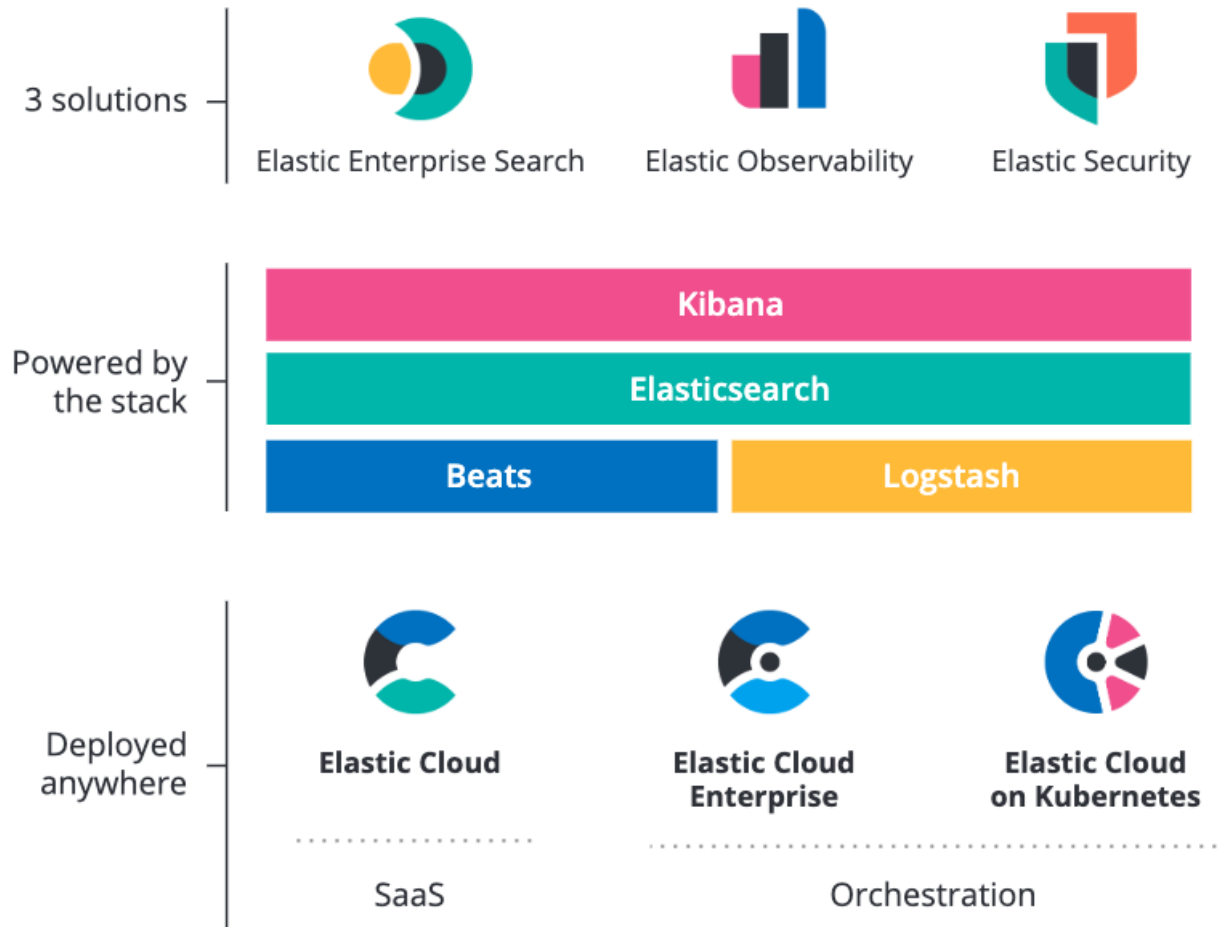
alex@elastic.co | [@spinscale](https://twitter.com/spinscale)



Agenda

- What is the Elastic Stack
- Elasticsearch introduction
- Elasticsearch practical demo
- Integrating Elasticsearch into your application

Product Overview



Solutions

on top of the Elastic Stack

3 solutions powered by 1 stack



Elastic Enterprise Search



Elastic Observability



Elastic Security



Elastic Stack

Elastic Stack

building & lego blocks



Deployment options



Elastic Cloud

SaaS



**Elastic Cloud
Enterprise**



**Elastic Cloud on
Kubernetes**

Orchestration

Licensing

		FREE		PAID		
SELF-MANAGED	OPEN SOURCE	BASIC	GOLD	PLATINUM	ENTERPRISE	
	Open Source Features	Free Proprietary Features	Paid Proprietary Features + Elastic Support			
PAID						
SaaS	ELASTIC CLOUD					

Elastic Stack

building & lego blocks



Elasticsearch in 10 seconds

- Search Engine (FTS, Analytics, Geo), near real-time
- Distributed, scalable, highly available, resilient
- Interface: HTTP & JSON
- Heart of the Elastic Stack (Kibana, Logstash, Beats)

Installation & Start

```
# https://www.elastic.co/downloads/elasticsearch
wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-7.7.0-darwin-x86_64.tar.gz
# wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-7.7.0-linux-x86_64.tar.gz
# wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-7.7.0-windows-x86_64.zip

tar xzf elasticsearch-7.7.0-darwin-x86_64.tar.gz
cd elasticsearch-7.7.0

./bin/elasticsearch
```

```
wget https://artifacts.elastic.co/downloads/kibana/kibana-7.7.0-darwin-x86_64.tar.gz
# wget https://artifacts.elastic.co/downloads/kibana/kibana-7.7.0-linux-x86_64.tar.gz
# wget https://artifacts.elastic.co/downloads/kibana/kibana-7.7.0-windows-x86_64.zip

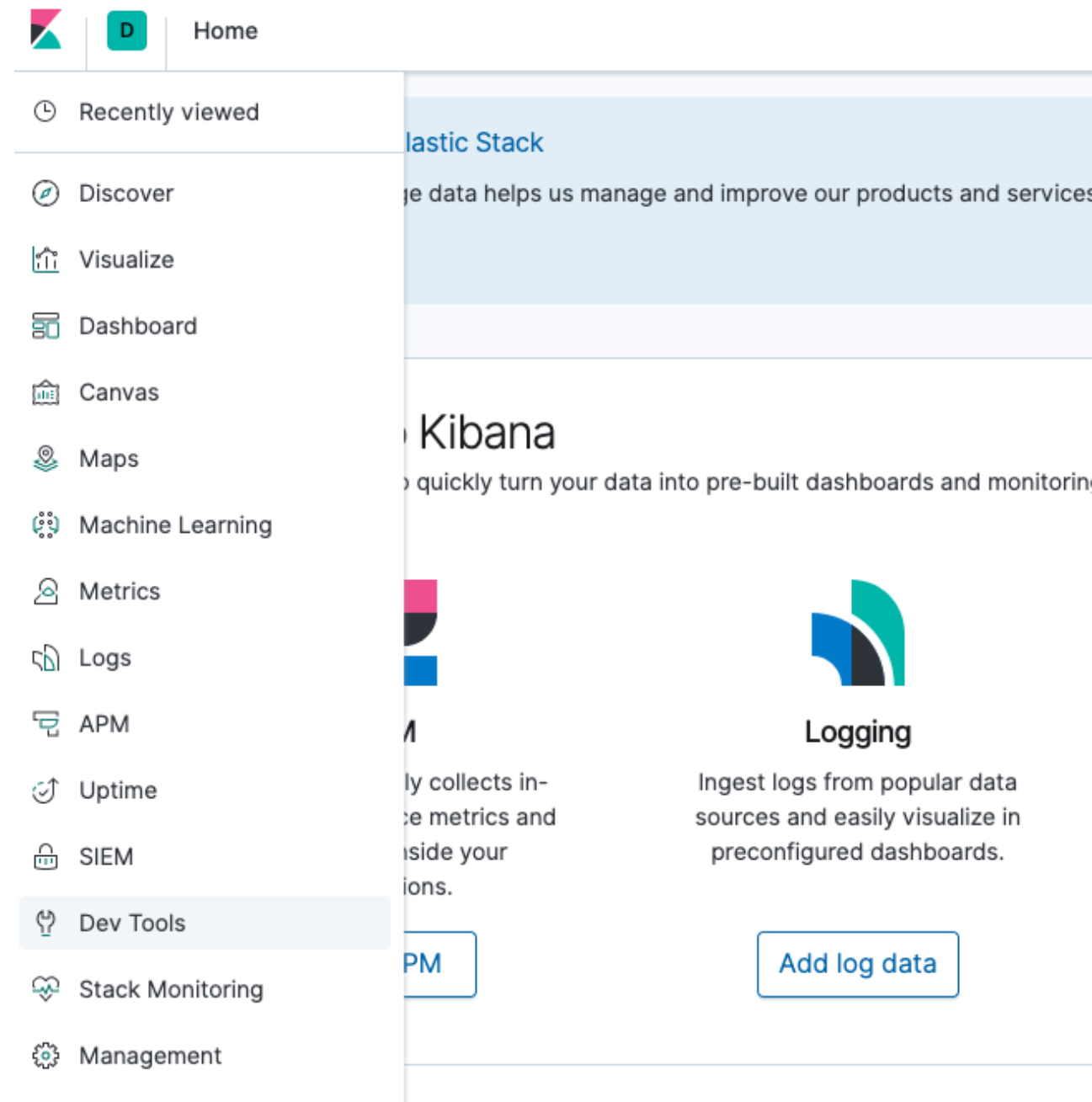
tar xzf kibana-7.7.0-darwin-x86_64.tar.gz
cd kibana-7.7.0
./bin/kibana
```

Point your browser to <http://localhost:5601/>

Click Dev-Tools

Samples in Kibana

Samples in Github





Dev Tools



Console

Search Profiler

Grok Debugger



History

Settings

Help



1 GET /

2

3 GET _cat/indices



1 # GET /

2 {

3 "name" : "rhincodon",

4 "cluster_name" : "elasticsearch",

5 "cluster_uuid" : "fQGQJn_oQgu5ou0Z9WNDHg",

6 "version" : {

7 "number" : "7.5.0",

8 "build_flavor" : "default",

9 "build_type" : "tar",

10 "build_hash" : "e9ccaed468e2fac2275a3761849cbee64b39519f",

11 "build_date" : "2019-11-26T01:06:52.518245Z",

12 "build_snapshot" : false,

13 "lucene_version" : "8.3.0",

14 "minimum_wire_compatibility_version" : "6.8.0",

15 "minimum_index_compatibility_version" : "6.0.0-beta1"

16 },

17 "tagline" : "You Know, for Search"

18 }

19

20

21 # GET _cat/indices

22 green open .kibana_task_manager_1 nVdc4g8NRi0mshOWPq63zQ 1 0 2 6 42

.9kb 42.9kb

23 green open .apm-agent-configuration uyFzuj-nS76soUaGN3MYSQ 1 0 0 0

230b 230b

24 green open .kibana_1 JRM24T5aScmZ5fhYxzRCpg 1 0 4 0 16

.3kb 16.3kb

25



elastic

Demo

Indexing, Mapping & Enrichment

- Index API
- Bulk API
- Put Mapping API
- Datatypes
- Enrichment

Document search & Aggregations

- Query DSL
- Search API
- Aggregations

Administration tasks

- Snapshot and restore
- Reindexing
- ILM
- Monitoring
- Frozen Indices
- Securing a cluster

Elasticsearch Clients

- Not just glorified HTTP clients
- Retry after failure
- Sniffing
- Bulk helpers
- Java, JavaScript, Ruby, Go, .NET, PHP, Perl, Python, Rust

Elasticsearch is distributed!

- Scaling reads, scaling writes, ensuring high availability
- Run as single node or hundreds of nodes together
- Users should never care if they query/index against a small or big cluster
- Add a new node, Elasticsearch will balance data & queries automatically
- Specialized roles (master, data, ingest, ml, voting only)
- Orchestration becomes more important as use-case clusters might be easier to maintain & upgrade than the one big cluster

More, more, more...

- More Queries, aggregations & data types
- Text analysis (phonetic search, search as you type)
- ILM, rollup, transform, frozen indices
- Security
- Alerting
- SQL
- Machine Learning
- Stack Monitoring
- Major version upgrades & deprecations
- Solutions (Observability, Enterprise Search, Security)

Summary

- Understanding search is hard
- Use the reference documentation
- Ask your users about expectations, do not guess!

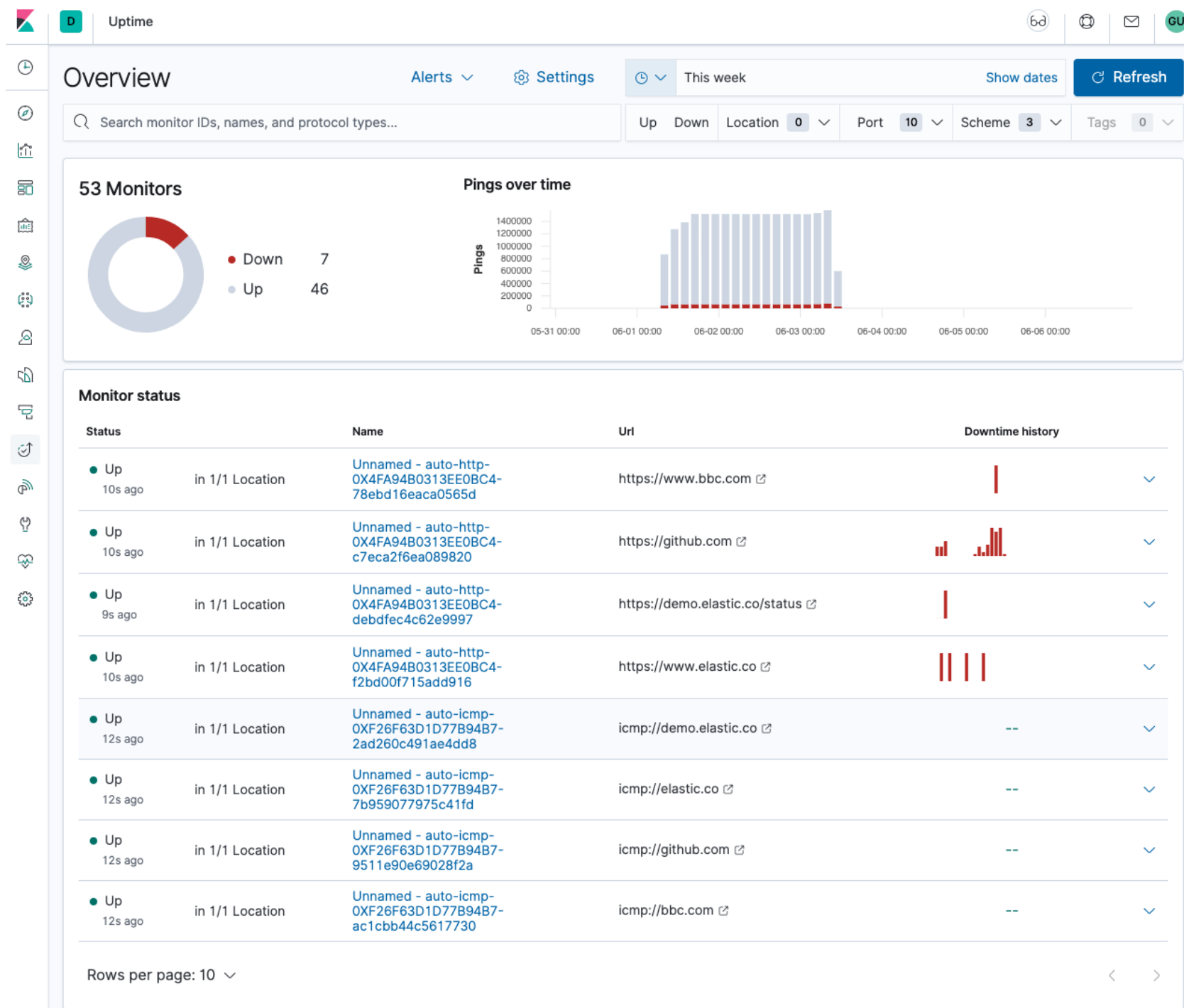
Next steps

Check out <https://demo.elastic.co>

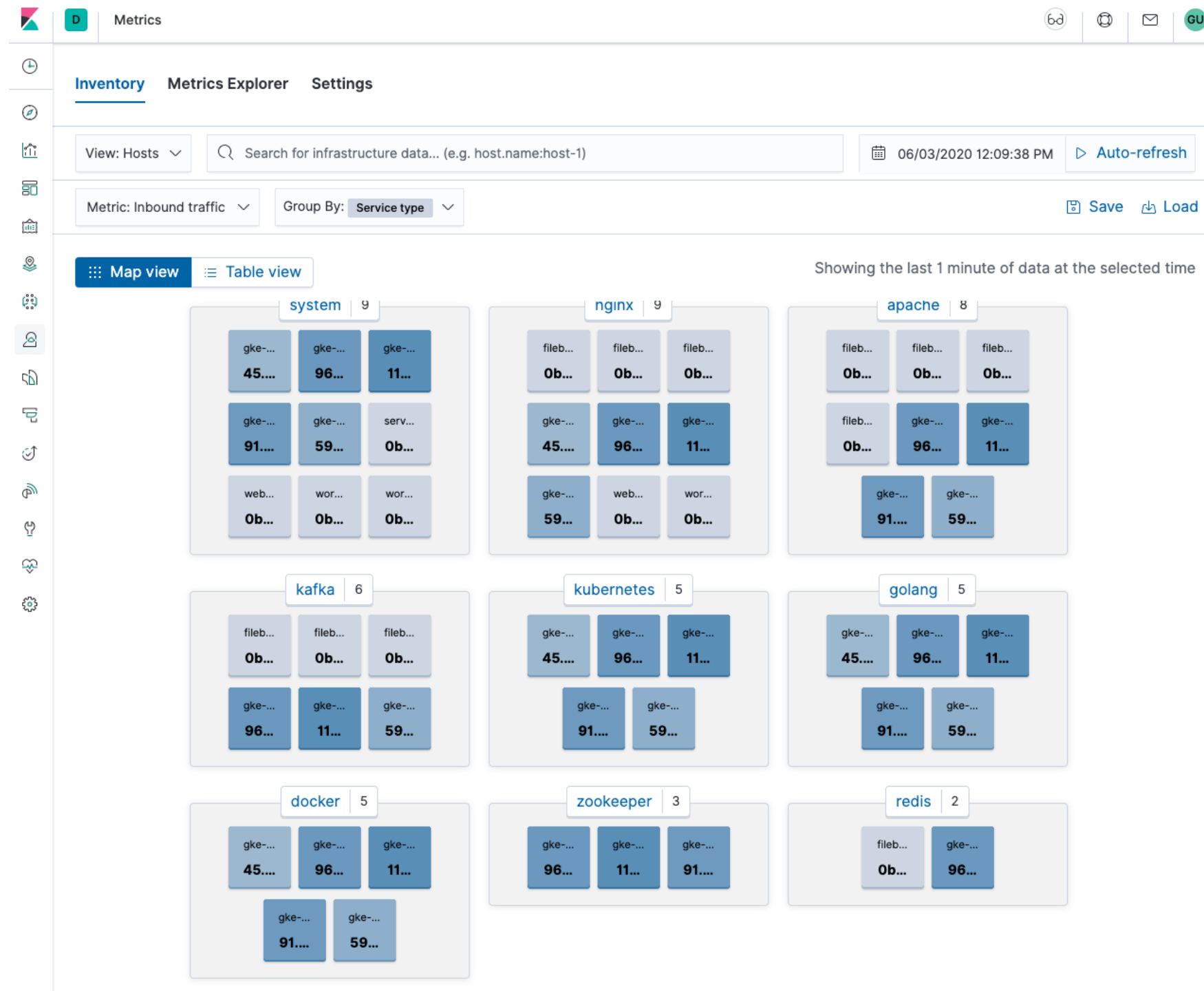
Check out Observability

- Uptime
- Metrics
- Logs
- APM

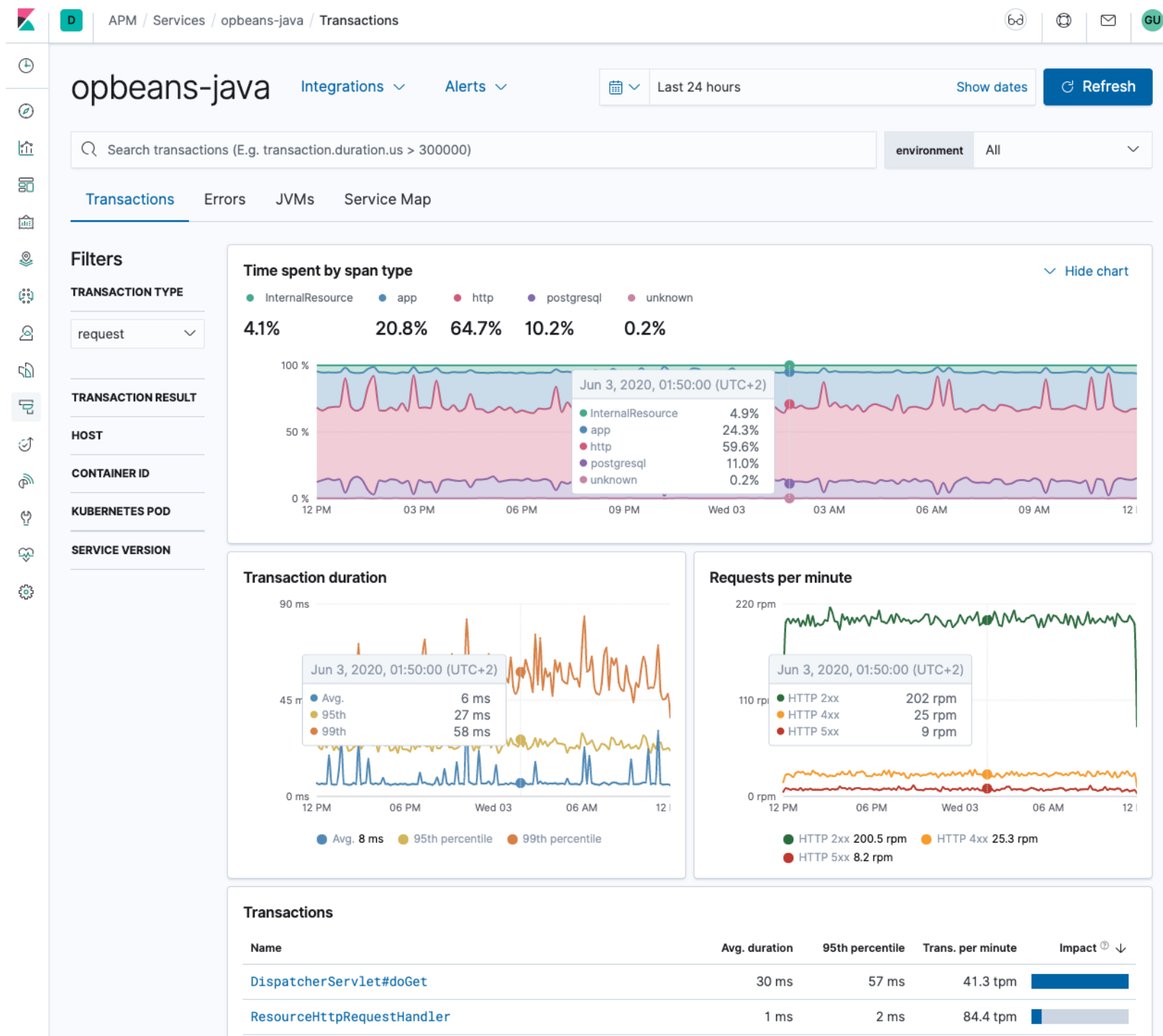
Uptime



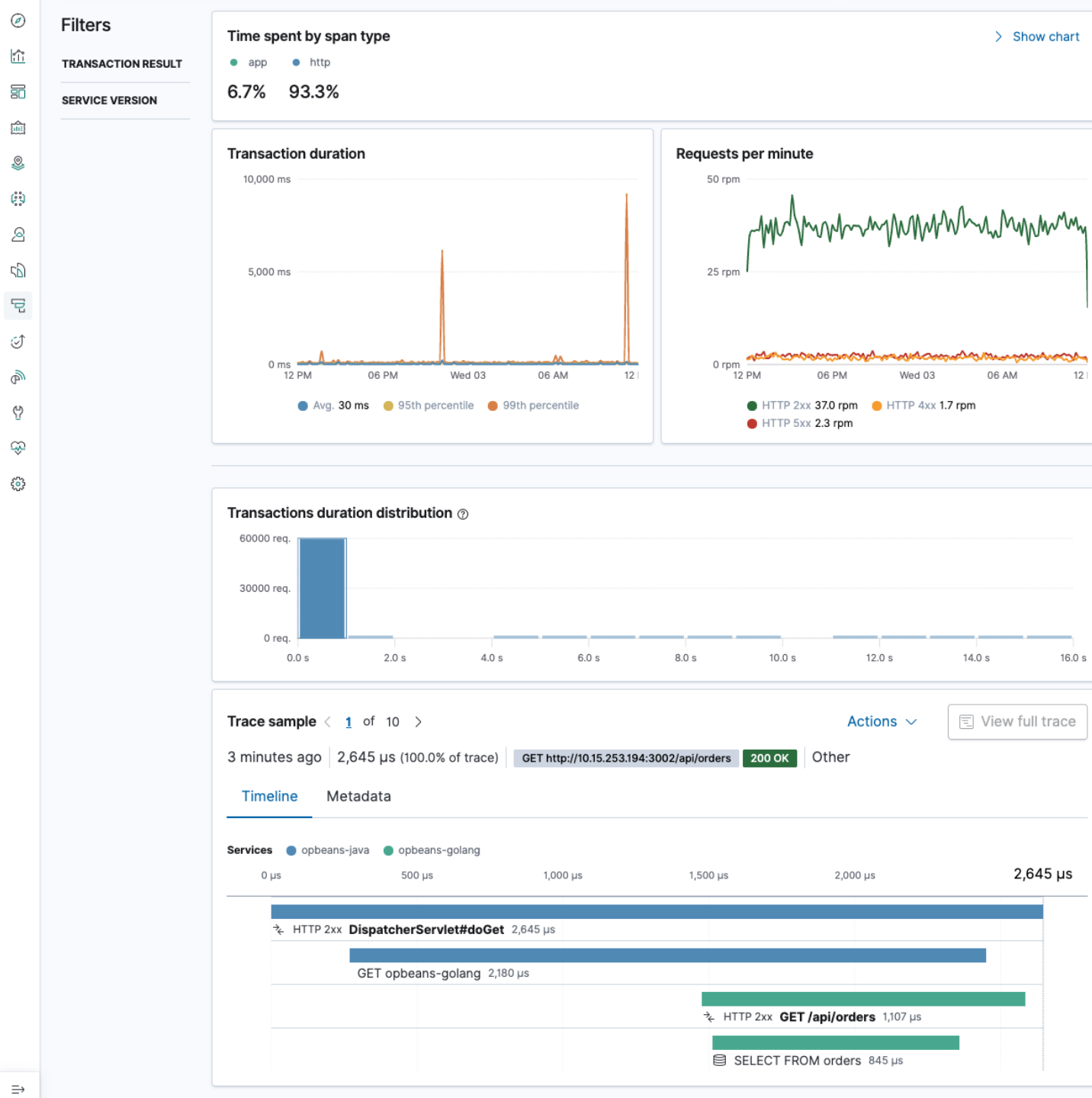
Metrics



APM



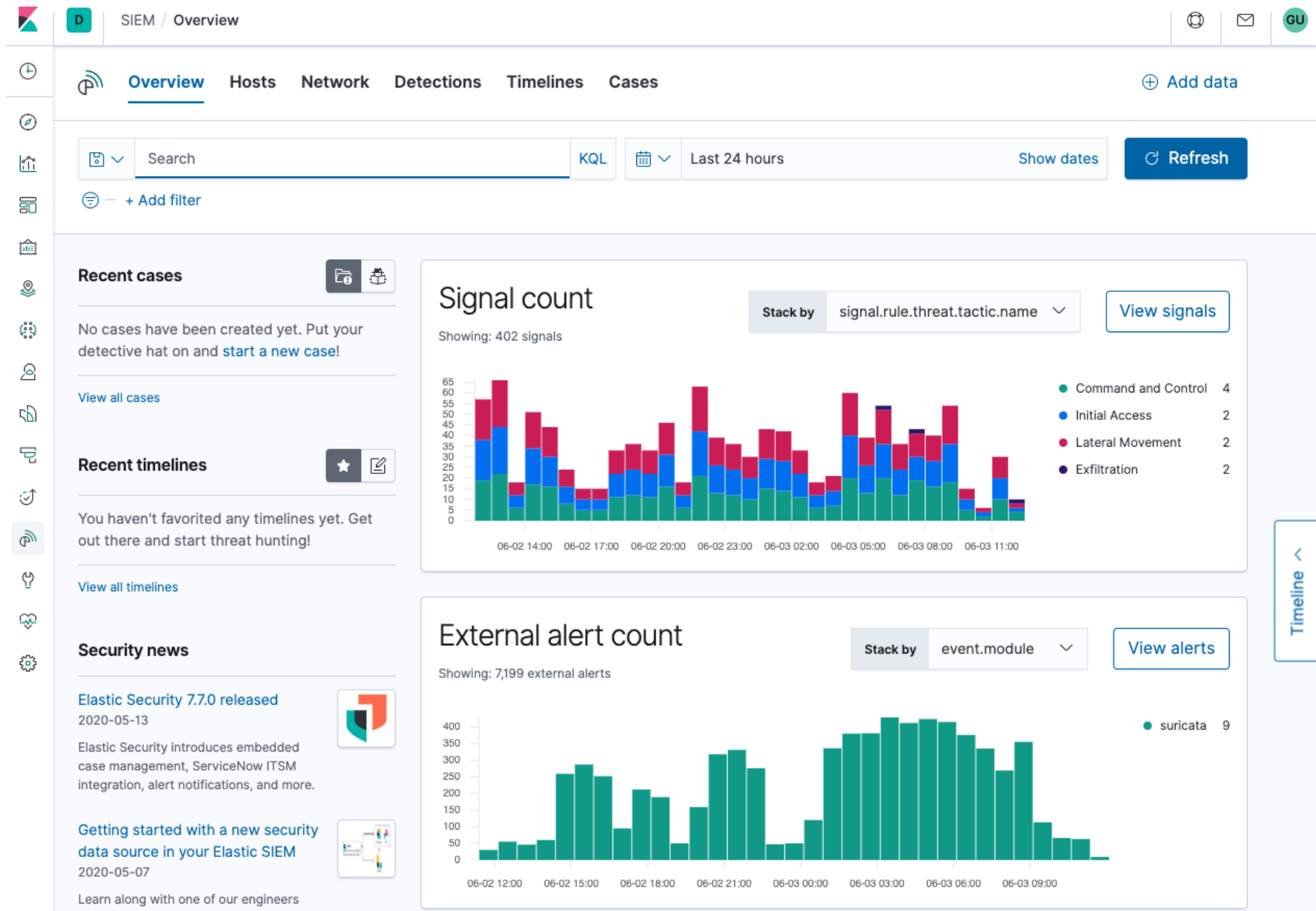
APM



Check out Security

- SIEM
- Endpoint Security

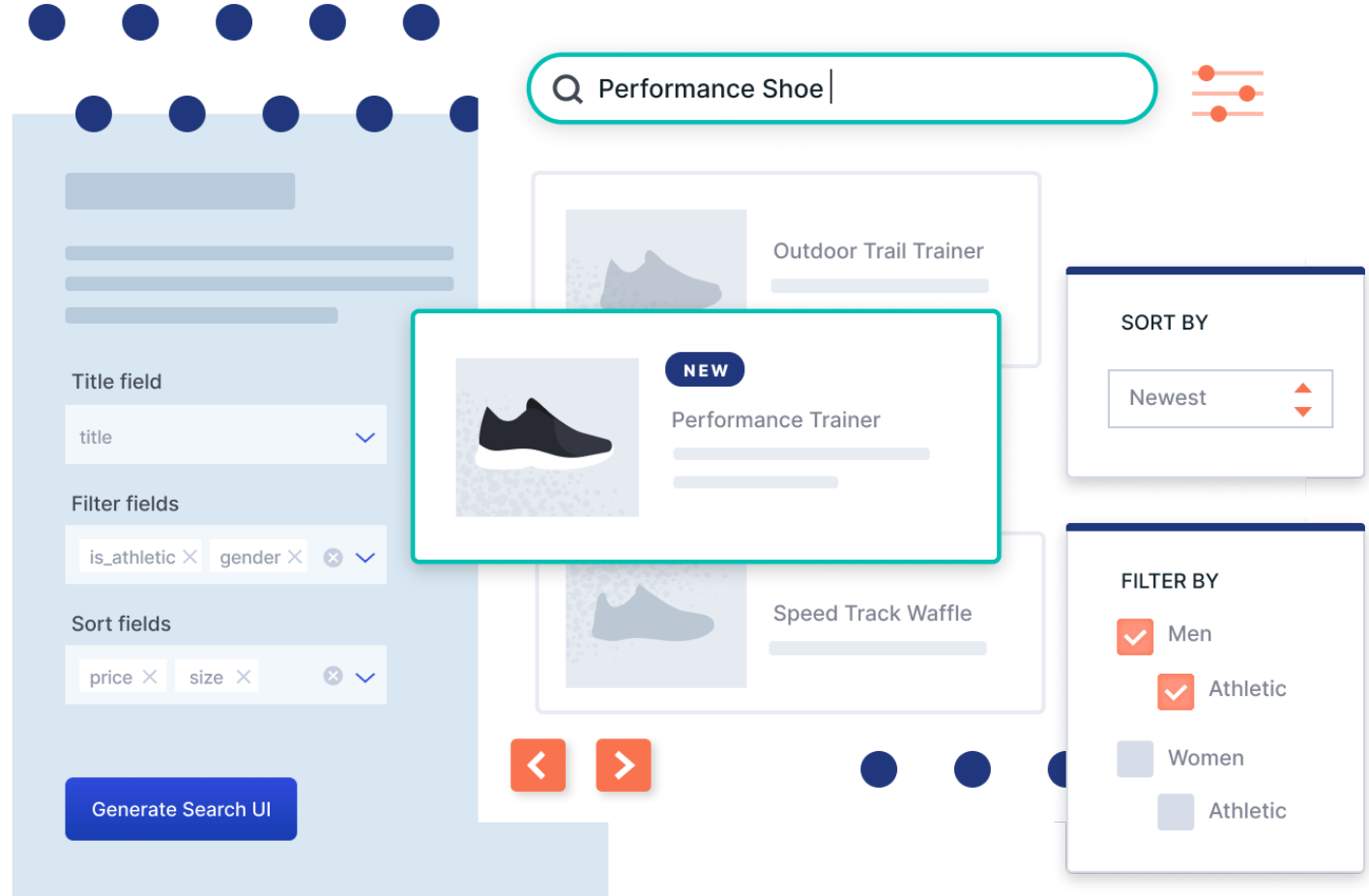
SIEM




Check out Enterprise Search

- Workplace Search
- App Search

App Search



Workplace Search

 workplace search

Past Week ▾

Relevance ▾

My Account ▾

Clear All

All Sources

Dropbox

15

SharePoint

4

Legal Document ...

4

OneDrive

1

GitHub

—

Google Drive

—

Marketing Conta...

—

Customer Record...

—

Showing results for acme inc contract updated last week.

Acme Inc - FY2020 Contractual Agreement

... contractually binding, unless stated explicitly. All trademarks, service marks and logos included on the Site ("Marks") are the property of Elasticsearch or third parties, and you may not use such Marks without the express, prior written consent of Elasticsearch or the applicable third party...

<https://vault.acme.co/file/155290094192>

VAULT

Last updated by Peggie Labadie 3/17/20 at 1:16pm

Acme Inc - Account 17635

DROPBOX

/acme-17635

DRAFT - Acme Inc Contract - Red Line For Approval.pdf

... contractually binding, unless stated explicitly. All trademarks, service marks and logos included on the Site ("Marks") are the property of Elasticsearch or third parties, and you may not use such Marks without the express, prior written consent of Elasticsearch or the applicable third party...

<https://acme.dropbox.com/file/152602380610>

Last updated by Emilio Murphy 3/15/20 at 10:05am

Acme Inc - Renewal Notes.pdf

... owner Emilio Murphy. A clear explanation on the nature of the contract was provided during the legal conversation, and the agreement has been sent for final approval to the applicable third party...

<https://acme.dropbox.com/file/54155412424>

Legal Document Vault

Acme Inc - FY2020 Contract...

<https://vault.acme.co/file/155290094192>

Excerpt

... contractually binding, unless stated explicitly. All trademarks, service marks and logos included on the Site ("Marks") are the property of Elasticsearch or third parties, and you may not use such Marks without the express, prior written consent of Elasticsearch or the applicable third party...

Created at

3/17/20 at 12:40am

Created by

Peggie Labadie

View in Legal Document Vault

Connectors



Google Drive

G Suite docs, stored files, and more



SharePoint

Sites, stored files, and more



OneDrive

Stored files, metadata, and more



ServiceNow

Users, incidents, articles, and more



Salesforce

Contacts, opportunities, leads, and more



GitHub

Issues, pull requests, repos, and more



Confluence

Spaces, pages, blog posts, and more



Jira

Epics, projects, issues, and more



Dropbox

Stored files, metadata, and more



Zendesk

Ticket content, status, priority, and more



Getting more help



Discuss Forum

<https://discuss.elastic.co>



elastic

all categories ▾all tags ▾

CategoriesLatestNew (117)Unread (917)Top

+ New Topic

CategoryTopicsLatest

Announcements

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

Community Ecosystem

3855 unread

Beats

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

Filebeat

1 unread7 new

Winlogbeat

2 new

Functionbeat

1 new

Community Beats

1 new

Packetbeat

1 new

Heartbeat

1 new

Journalbeat

1 new

Beats Developers

1 new

Topbeat

1 new

Metricbeat

3 new

Auditbeat

1 new

Central Management

1 new

61 / week1 unread15 new

Elasticsearch

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

Rally

178 / week831 unread36 new

Logstash

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

95 / week29 unread24 new

Kibana

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

113 / week42 unread19 new

APM

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

12 / week5 new

Logs

Everything related to the Logs app – setup with Filebeat, Filebeat modules, and using the Kibana Logs app.

55

Metrics

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

1 / week

⚙️ Notes on Using These Forums

Meta Elastic

2Apr 2017

Couldn't push logs to elasticsearch using filebeat

Filebeat

13m

<BarSeries> configuration

Kibana

06m

Dec 15th, 2019: [EN] Elasticsearch Snapshot Lifecycle Management (SLM) with Minio.io S3

advent-staging

07m

Invalid IP network, skipping {<network=>"10.13.7.0/10.13.7.24"

Logstash

010m

FScrawler stuck at 2.6gb index size

Elasticsearch

211m

Elastic APM Java agent - sanitize_fields_names on application/json* data

APMjava

121m

Metricbeat Failed to connect EOF

Metricbeat

522m

Mix free and paid licenses

Elasticsearchlicense

023m

Filebeat CPU utilization metrics are not normalized by default

Beatsstack-monitoring

223m

How do i aggregate these documets

Logstash

626m

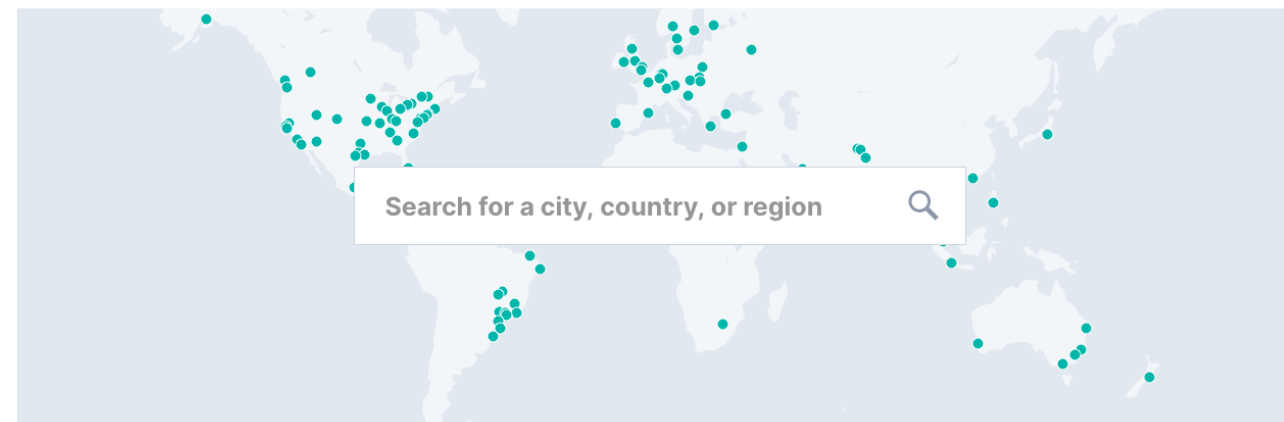
Metricbeat error

Metricbeat

128m

Community & Meetups

<https://community.elastic.co>



Explore by region

Asia Pacific and Japan **Europe, Middle East and Africa** North and South America Virtual

ELASTIC - BARCELONA Spain 🇪🇸	ELASTIC - COPENHAGEN Denmark 🇩🇰	ELASTIC - GÖTEBORG Sweden 🇸🇪	ELASTIC - SCOTLAND United Kingdom 🇬🇧
ELASTIC - STOCKHOLM Sweden 🇸🇪	ELASTIC - TEL AVIV Israel 🇮🇱	ELASTIC - TURKEY Turkey 🇹🇷	ELASTIC BONN USER GROUP Germany 🇩🇪
ELASTIC CAMBRIDGE & EAST ANGLIA USER GROUP United Kingdom 🇬🇧	ELASTIC DUBAI USER GROUP United Arab Emirates 🇦🇪	ELASTIC FR France 🇫🇷	ELASTIC GREECE Greece 🇬🇷
ELASTIC HELSINKI Finland 🇫🇮	ELASTIC KRAKOW USER GROUP Poland 🇵🇱	ELASTIC LONDON USER GROUP United Kingdom 🇬🇧	ELASTIC LUXEMBOURG USER GROUP Luxembourg 🇱🇺
ELASTIC MANCHESTER USER GROUP United Kingdom 🇬🇧	ELASTIC MOSCOW Russian Federation 🇷🇺	ELASTIC NIGERIA Nigeria 🇳🇮	ELASTIC OSLO USER GROUP Norway 🇳🇴
ELASTIC PORTUGAL Portugal 🇵🇹	ELASTIC RHEINRUHR Germany 🇩🇪	ELASTIC SLOVAK USER GROUP Slovakia 🇸🇰	ELASTIC USER GROUP - CZ Czech Republic 🇨🇪
ELASTIC USER GROUP - DUBLIN Ireland 🇮🇪	ELASTIC USER GROUP ABIDJAN Côte d'Ivoire 🇨🇮	ELASTIC WARSAW USER GROUP Poland 🇵🇱	ELASTIC ZAGREB Croatia 🇭🇷
ELASTICSEARCH - SOUTH AFRICA South Africa 🇿🇦	ELASTICSEARCH SWITZERLAND Switzerland 🇨🇭	ELASTICSEARCH USER GROUP PAKISTAN Pakistan 🇵🇰	SEARCH MEETUP MUNICH Germany 🇩🇪

Official Elastic Training

<https://training.elastic.co>



[contact](#)

Elastic Training

[Training Subscriptions](#) [Private Training](#) [Specializations](#) [Certification](#) [Catalog](#) | [Cart](#) [Login](#)

Official Elastic Training

Purchase two in-classroom training seats in select cities on the same order and get **50% off** the second seat.

Don't wait. Save 25% by purchasing your [Elastic Certified Engineer Exam](#) attempt by January 31, 2020!



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

Munich, Germany

Mar 2, 2020 -
Mar 3, 2020

[Register Now](#)

Early bird expires 6 Jan

50% off second seat

Elasticsearch Engineer II

Munich, Germany

Mar 4, 2020 -
Mar 5, 2020

[Register Now](#)

Early bird expires 6 Jan

50% off second seat

Thanks for listening

Q & A

Alexander Reelsen

Community Advocate

alex@elastic.co | [@spinscale](https://twitter.com/spinscale)

