



Uptime Introduction

Alexander Reelsen
Community Advocate
alex@elastic.co | spinscale



Agenda

What is the Elastic Stack?

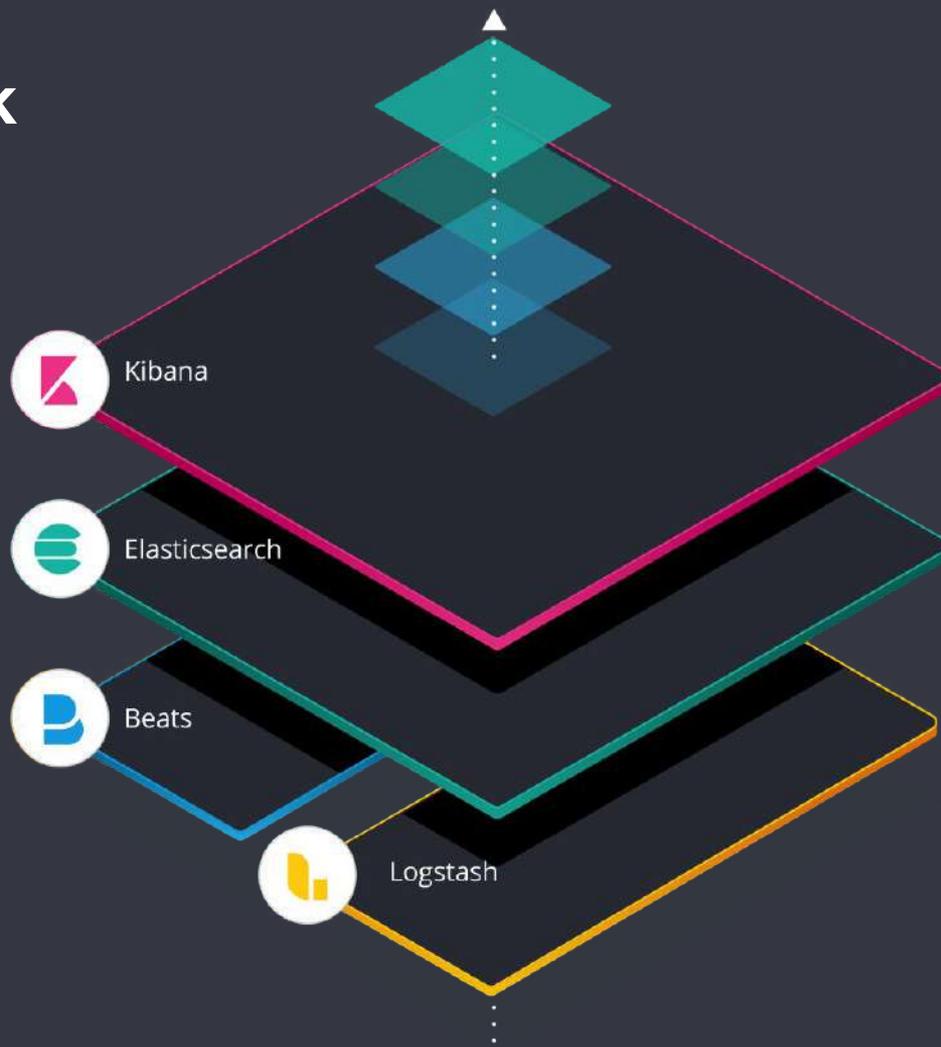
Installing

Heartbeat Deep Dive

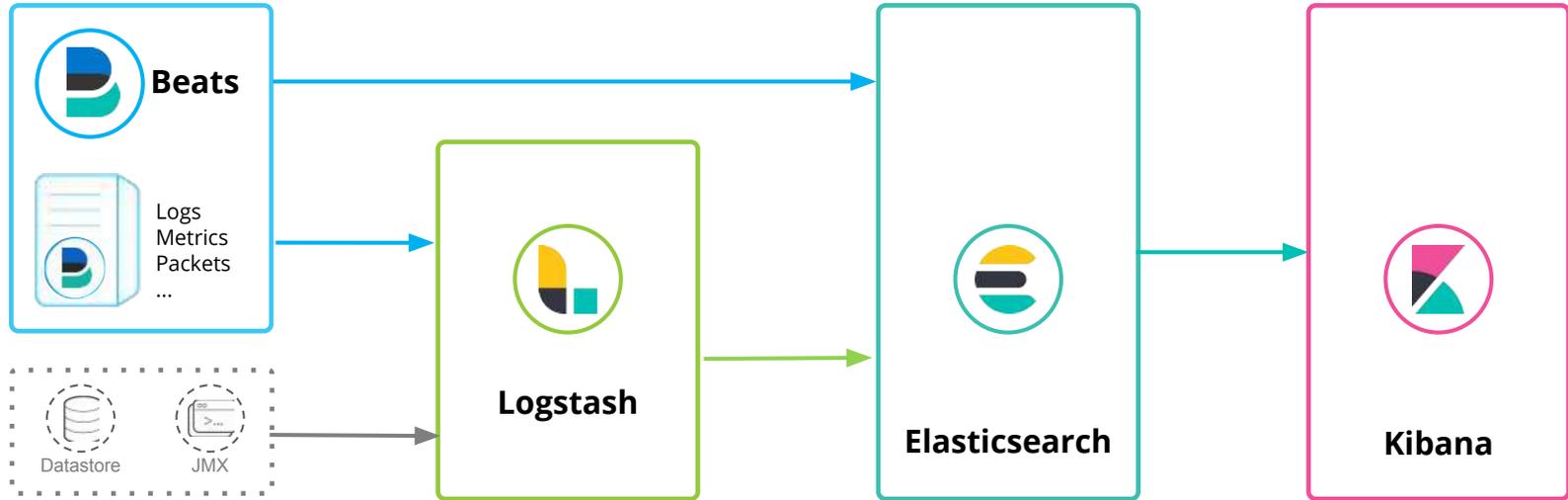
Uptime in the Kibana UI

Next steps

Elastic Stack



Elastic Stack - Data flows



Observability with the Elastic Stack

- Logs
- Metrics
- APM
- Infrastructure
- **Uptime**

Default

Customize

03/26/2019 7:12:22 PM

Stream live

```

2019-03-26 07:12:54.149 [kafka.log][INFO] Retrying leaderEpoch request for partition __consumer_offsets-33 as the leader reported an error: NOT_LEADER_FOR_PARTITION
2019-03-26 07:12:54.149 [kafka.log][INFO] Retrying leaderEpoch request for partition __consumer_offsets-15 as the leader reported an error: NOT_LEADER_FOR_PARTITION
2019-03-26 07:12:54.149 [kafka.log][INFO] Retrying leaderEpoch request for partition logs-0 as the leader reported an error: NOT_LEADER_FOR_PARTITION
2019-03-26 10:57:32.403 [kafka.log][INFO] Opening socket connection to server kafka-zookeeper/10.47.244.48:2181. Will not attempt to authenticate using SASL (unknown error)
2019-03-26 10:57:32.456 [kafka.log][INFO] Opening socket connection to server kafka-zookeeper/10.47.244.48:2181. Will not attempt to authenticate using SASL (unknown error)
2019-03-26 11:57:30.553 [kafka.log][INFO] Opening socket connection to server kafka-zookeeper/10.47.244.48:2181. Will not attempt to authenticate using SASL (unknown error)
2019-03-26 13:57:32.752 [kafka.log][INFO] Opening socket connection to server kafka-zookeeper/10.47.244.48:2181. Will not attempt to authenticate using SASL (unknown error)
2019-03-26 19:12:22.369 [kafka.log][INFO] Error sending fetch request (sessionId=839052068, epoch=517118) to node 2: java.nio.channels.ClosedSelectorException.
2019-03-26 19:12:22.785 [kafka.log][INFO] Retrying leaderEpoch request for partition __consumer_offsets-47 as the leader reported an error: NOT_LEADER_FOR_PARTITION
2019-03-26 19:12:22.786 [kafka.log][INFO] Retrying leaderEpoch request for partition __consumer_offsets-11 as the leader reported an error: NOT_LEADER_FOR_PARTITION
2019-03-26 19:12:22.786 [kafka.log][INFO] Retrying leaderEpoch request for partition __consumer_offsets-41 as the leader reported an error: NOT_LEADER_FOR_PARTITION
2019-03-26 19:12:22.786 [kafka.log][INFO] Retrying leaderEpoch request for partition __consumer_offsets-5 as the leader reported an error: NOT_LEADER_FOR_PARTITION
2019-03-26 19:12:22.786 [kafka.log][INFO] Retrying leaderEpoch request for partition __consumer_offsets-35 as the leader reported an error: NOT_LEADER_FOR_PARTITION
2019-03-26 19:12:22.786 [kafka.log][INFO] Retrying leaderEpoch request for partition __consumer_offsets-17 as the leader reported an error: NOT_LEADER_FOR_PARTITION
2019-03-26 19:12:25.493 [kafka.log][INFO] Error sending fetch request (sessionId=1303574239, epoch=127483) to node 0: java.nio.channels.ClosedSelectorException.

```

09 AM

12 PM

03 PM

06 PM

09 PM

Wed 27

03 AM

06 AM

View: Kubernetes ▾

Search for infrastructure data... (e.g. host.name:host-1)

10/28/2019 5:20:18 PM

▶ Auto-refresh

Metric: CPU usage ▾

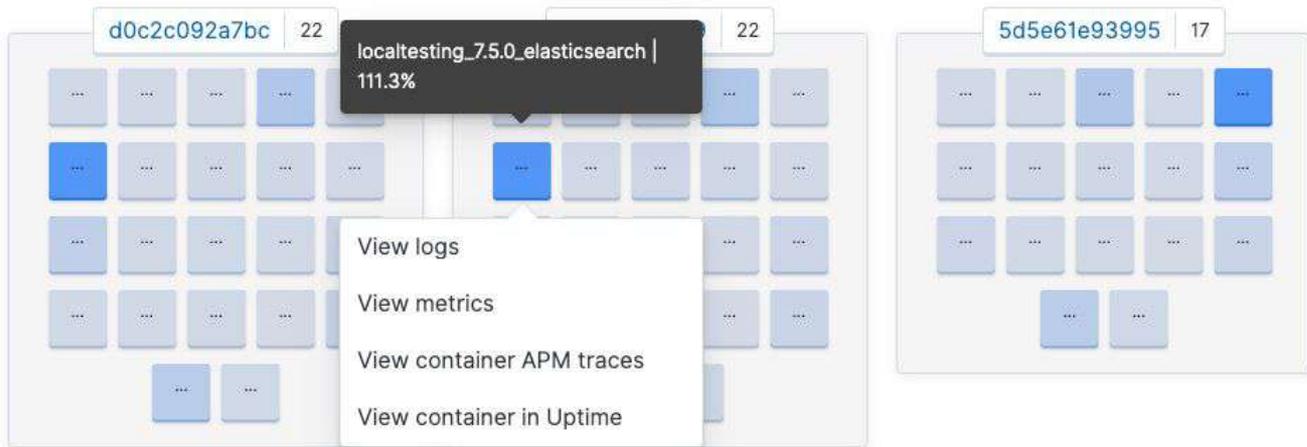
Group By: All ▾

Save Load

Map view

Table view

Showing the last 1 minute of data at the selected time



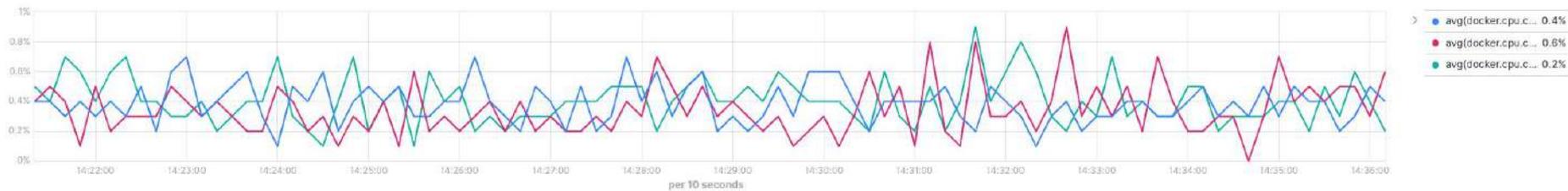
Save Share Inspect Refresh

Last 15 minutes

Show dates

Refresh

Time Series Metric Top N Gauge Markdown Table



Auto apply

The changes will be automatically applied.

Data Panel options Annotations

avg(docker.cpu.core.0.pct)

Metrics Options

Aggregation

Average

Field

docker.cpu.core.0.pct

Group by

Everything

avg(docker.cpu.core.1.pct)

Metrics Options

Aggregation

Average

Field

docker.cpu.core.1.pct

Group by



Trace sample

Actions ▾

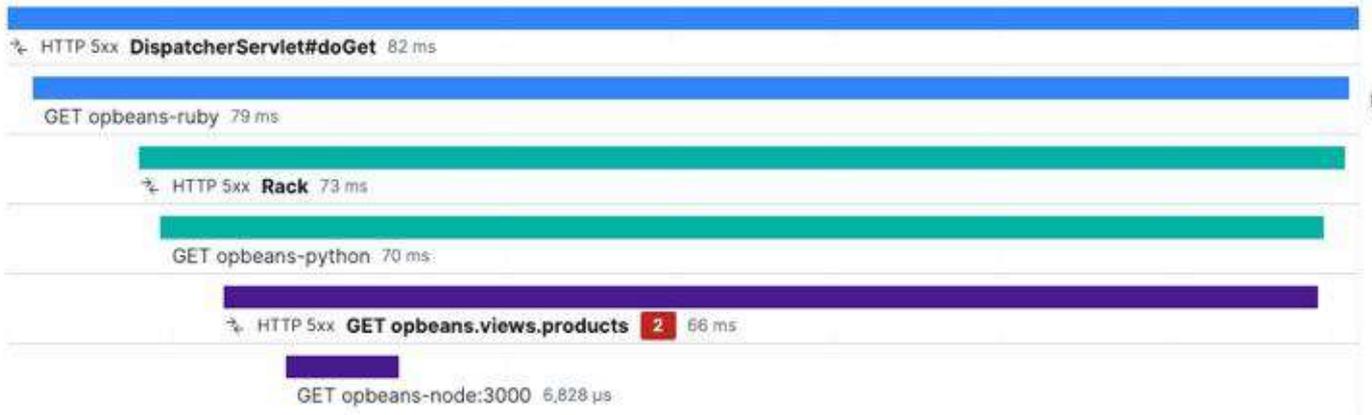
[View full trace](#)

16 minutes ago | 82 ms (89.9% of trace) | GET http://opbeans-java:3000/api/products | 500 Internal Server Error | 2 Errors | Other

Timeline Metadata

Services ● opbeans-java ● opbeans-ruby ● opbeans-python

0 ms 10 ms 20 ms 30 ms 40 ms 50 ms 60 ms 70 ms 82 ms



Uptime in 1 minute

- Metrics, Logs, APM == Internal application state
- User perception and SLAs == External application state
- Host reachability
- Service reachability
- Service response
- Response times outside of your data center?
- TCP connection durations, load balancing, TLS handshake duration

Overview

⌵ Last 15 minutes Show dates Refresh

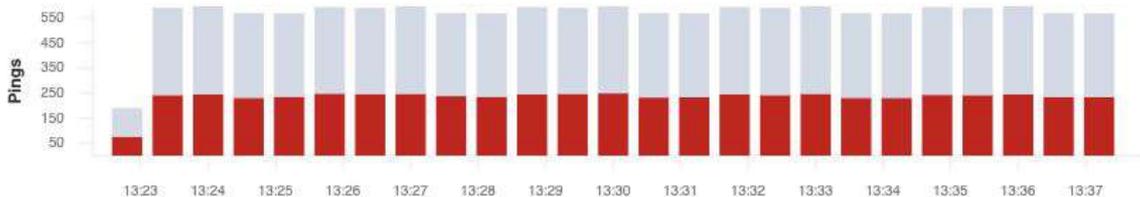
🔍 Search monitor IDs, names, and protocol types...

Up Down Location 3 Port 7 Scheme 3

12/33 monitors are down



Pings over time



Monitor status

Status	Name	URL	Downtime history	Integrations
● Down a few seconds ago	UseCases	https://www.elastic.co/use-cases/ <small>🔗</small>		⋮ ⌵
● Up a few seconds ago	Unnamed - auto-http-0X14D5C52E77FA69FF	https://www.elastic.co/ <small>🔗</small>		⋮ ⌵
● Up a few seconds ago	Just Elastic	https://www.elastic.co/ <small>🔗</small>		⋮ ⌵
● Down a few seconds ago	NodeJS	http://opbeans-node:3000/api/customers <small>🔗</small>		⋮ ⌵
● Down a few seconds ago	NodeJS	http://opbeans-node:3000/api/customers <small>🔗</small>		⋮ ⌵

Service Monitor

Last 15 minutes

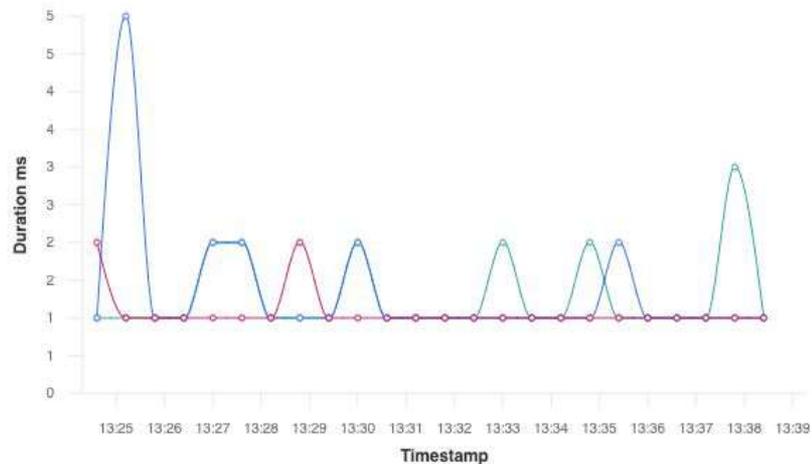
Show dates

Refresh

auto-tcp-0X59D12A2A76D484B4

Up tcp://8.8.8.8:53 1ms a few seconds ago

Monitor duration



Pings over time



History

Status: All Location: All

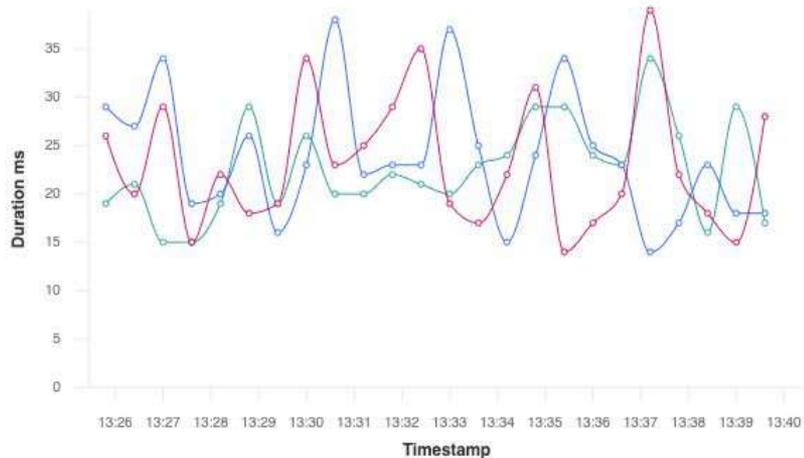
RubyAPI

🕒 Last 15 minutes
Show dates
🔄 Refresh

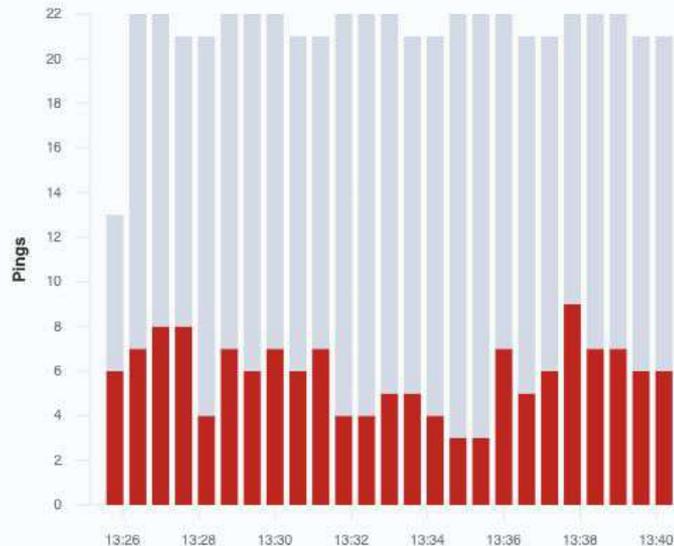
auto-http-0X690192E6E8794587-3e4ce6d2d3838a27

● Down <http://opbeans-ruby:3000/api/customers/2> 79ms a few seconds ago

Monitor duration



Pings over time



● nyc-dc1-rack1 17
● uk-dc2-rack3 18
● ca-dc2-rack1 28

History

Status: All
 Location: All

Monitor status

Status	Name	URL	Downtime history	Integrations
● Down a few seconds ago	UseCases	https://www.elastic.co/use-cases/ 🔗		⋮ ▾
● Up a few seconds ago	Unnamed - auto-http-0X14D5C52E77FA69FF	https://www.elastic.co/ 🔗		⋮ ▾
● Up a few seconds ago	Just Elastic	https://www.elastic.co/ 🔗		⋮ ▾
● Down a few seconds ago	NodeJS	http://opbeans-node:3000/api/customers 🔗		⋮ ▾
● Down a few seconds ago	NodeJS	http://opbeans-node:3000/api/stats 🔗		⋮ ▾
● Down a few seconds ago	NodeJS	http://opbeans-node:3000/api/orders 🔗		⋮ ▾
● Down a few seconds ago	SecurityContents	https://www.elastic.co/products/siem 🔗		⋮ ▾
● Down a few seconds ago	Unnamed - auto-http-0X42CA05022552551B	http://172.21.0.10:3000 🔗		⋮ ▾
● Down a few seconds ago	Twitter Explained	https://twitter.com/ 🔗		⋮ ▾
● Up a few seconds ago	RubyAPI	http://opbeans-ruby:3000/api/customers/2 🔗		⋮ ▾



Heartbeat

- **Lightweight data shipper**
- Configure hosts, TCP/HTTP endpoints
- Periodically poll endpoints
- Index results into Elasticsearch



Heartbeat

- Spool results into file in case of availability issues
- Resolve all IPs of a DNS name and check
- YAML based configuration can be checked into VCS
- Keystore to handle secrets/passwords

Installation Elasticsearch + Kibana

- Elastic Cloud
- ECE
- ECK
- Self-Hosted (docker, rpm, deb, tar.gz)

Installation heartbeat

- Self-Hosted (docker, rpm, deb, tar.gz)
- Multiple instances
 - Cross data center
 - Cross continents
 - Where your customers are



DEMO



Installation & Start

```
# https://www.elastic.co/downloads/beats/heartbeat
wget https://artifacts.elastic.co/downloads/beats/heartbeat/heartbeat-7.5.2-darwin-x86\_64.tar.gz
# wget https://artifacts.elastic.co/downloads/beats/heartbeat/heartbeat-7.5.2-linux-x86\_64.tar.gz
# wget https://artifacts.elastic.co/downloads/beats/heartbeat/heartbeat-7.5.2-windows-x86\_64.zip

tar zxvf heartbeat-7.5.2-darwin-x86_64.tar.gz
cd heartbeat-7.5.2-darwin-x86_64
```

Overview

🕒 Last 15 minutes

Show dates

🔄 Refresh

🔍 Search monitor IDs, names, and protocol types...

Up

Down

Location 0

Port 2

Scheme 3

3/12 monitors are down



Pings over time



Monitor status

Status	Name	URL	Downtime history	Integrations
● Up a few seconds ago	Unnamed - auto-http-0X28C25EF2EC007B6A	https://httpbin.org/status/404	🔗	🔌 ⌵
● Up a few seconds ago	Unnamed - auto-http-0X55DCE8E620C0449	https://httpbin.org/response-headers?freeform=my_value	🔗	🔌 ⌵
● Down a few seconds ago	Unnamed - auto-http-0X7031309F3B29FB86	https://httpbin.org/status/404	🔗	🔌 ⌵
● Up a few seconds ago	Unnamed - auto-http-0XB15E1367EE7612D	https://httpbin.org	🔗	🔌 ⌵
● Up a few seconds ago	my-other-httpbin-check	https://httpbin.org	🔗	🔌 ⌵
● Up a few seconds ago	Unnamed - auto-http-0XD09000EC08D0D93F	https://httpbin.org/basic-auth/my_user/my_password	🔗	🔌 ⌵
● Up a few seconds ago	Unnamed - auto-http-0XD8F53E6A037CC990	https://httpbin.org	🔗	🔌 ⌵

- 🕒
- 🔍
- 🏠
- 📊
- 📅
- 🌐
- 🔌
- 📧
- 👤
- ⚙️
- 🔒
- 🔧
- 🔗
- 🔌
- ⚙️

google-dns-tcp-check

🕒 Last 15 minutes

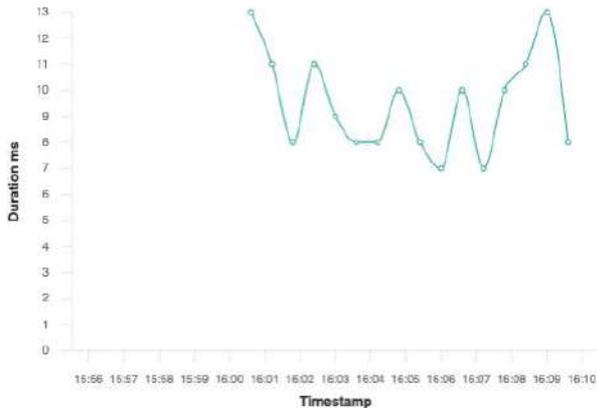
Show dates

🔄 Refresh

auto-tcp-OXFABD1BA9242B12B0

● Up tcp://8.8.8.8:53 8ms a few seconds ago

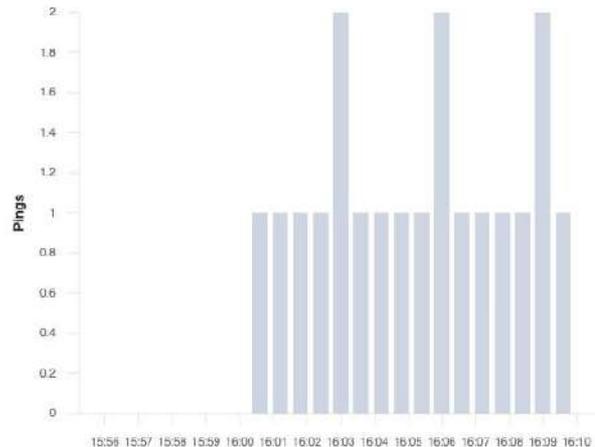
Monitor duration



● spinscale-at-home

8

Pings over time



History

Status

All ▾

Location

All ▾

Status	Location	IP	Duration	Error type
--------	----------	----	----------	------------

● Up	spinscale-at-home	8.8.8.8	8 ms	▾
Checked a few seconds ago				



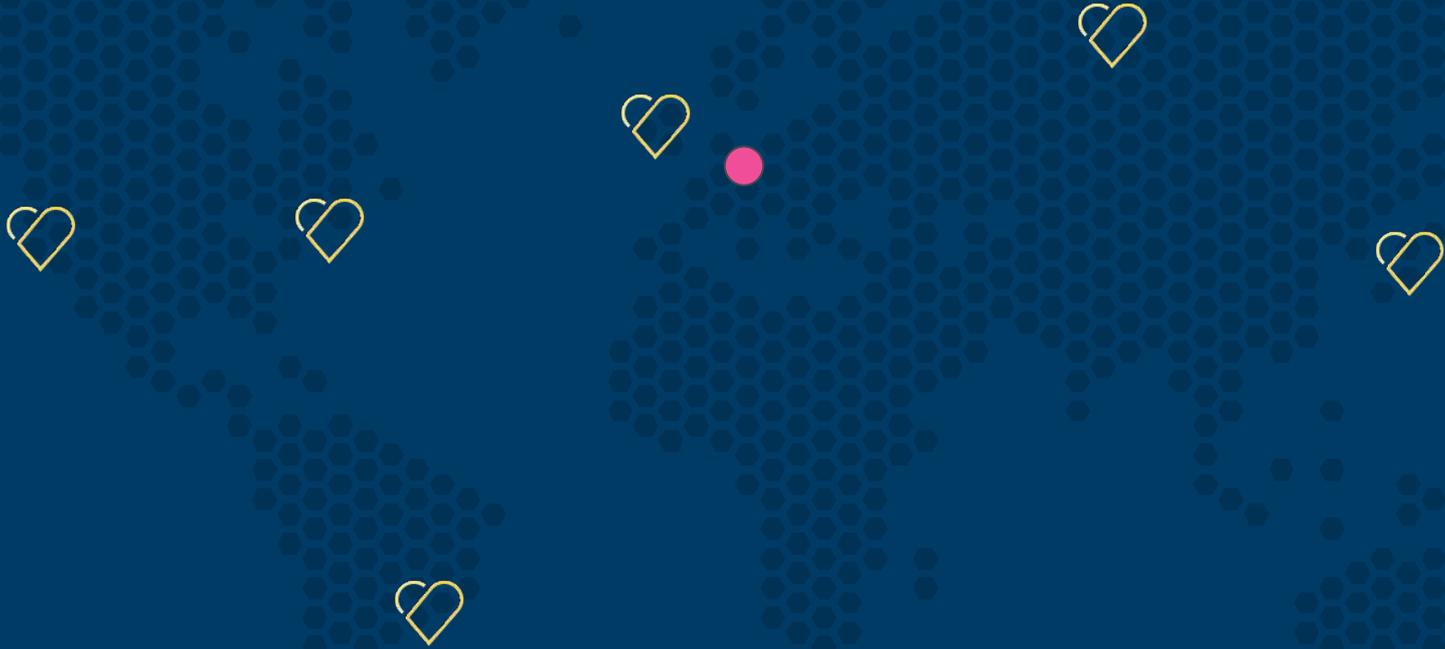
Summary



Summary

- External state knowledge is important
- Understand up/down states
- Understand response times
- Visualize changes over time

Location Location Location!



Next steps

- Autodiscovery
- Configure custom CAs
- Configure scheduler limit and timezone
- Add processors like `add_locale`, `add_observer_metadata`
- Security privileges

In development

- Kibana Alerting Integration
- ML Integration
- CCS support
- Central management

Elastic Cloud

elastic Products Learn Company Pricing Contact Try Free Login

SAAS Elastic Cloud STANDALONE Elastic on-prem ORCHESTRATION Elastic on-prem

Elastic Cloud pricing

Pricing for our suite of SaaS offerings, which make it easy to deploy, operate, and scale Elastic products in the cloud.

 Elasticsearch Service <p>Easily spin up a deployment on AWS, GCP or Azure with Kibana and features you can't get anywhere else.</p>	AS LOW AS \$16/month	See pricing	Start free trial
 App Search Service <p>Build a fast, relevant, search experience for your custom application in just a few minutes.</p>	AS LOW AS \$49/month	See pricing	Start free trial
 Site Search Service <p>Everything you need to deliver a powerful search experience for your website — without the learning curve.</p>	AS LOW AS \$79/month	See pricing	Start free trial

[SAAS](#)
[Elastic Cloud](#)
[STANDALONE](#)
[Elastic on-prem](#)
[ORCHESTRATION](#)
[Elastic on-prem](#)

Elastic Stack subscriptions

The Elastic Stack — Elasticsearch, Kibana, Beats, and Logstash — powers a variety of use cases. And we have flexible plans to help you get the most out of your on-prem subscriptions.

FREE					
Open Source Apache 2.0: Now and always.	Basic The forever-free plan.	Gold More features. Dedicated support.	Platinum Advanced functionality. Around the clock support.	Enterprise Stack orchestration and endpoint protection by default.	
Feature highlights include: <ul style="list-style-type: none"> ✓ Clustering & high availability ✓ Powerful search and analysis ✓ Data visualization and dashboarding ✓ And more 	Everything in Open Source plus: <ul style="list-style-type: none"> ✓ Core security features ✓ Solutions such as APM, SIEM, Maps, and more ✓ Canvas ✓ And more 	Everything in Basic plus: <ul style="list-style-type: none"> ✓ Alerting ✓ Reporting ✓ Ingest management ✓ Business hours support ✓ And more 	Everything in Gold plus: <ul style="list-style-type: none"> ✓ Advanced security features ✓ Machine learning ✓ Cross-cluster replication ✓ 24/7/365 support ✓ And more 	Everything in Platinum plus: <ul style="list-style-type: none"> ✓ Endpoint prevention ✓ Endpoint detection and response mapped to MITRE ATT&CK ✓ Endpoint event collection ✓ Access to ECE & ECK orchestration features 	
Free download		Contact us	Contact us	Contact us	Contact us

Elastic Support Subscriptions



Getting help



Discuss forum

<https://discuss.elastic.co>

elastic

all categories all tags Categories Latest New (117) Unread (917) Top + New Topic

Category Topics Latest

Announcements 385
Release announcements, end of life notifications and other bits about Elastic products that we think will be useful to everyone.
Community Ecosystem

Beats 51 / week
Any questions regarding Beats, forwarders and shippers for various types of data.
Filebeat 1 unread Packetbeat 1 new Metricbeat 3 new
Winlogbeat 2 new Heartbeat 1 new Auditbeat
Functionbeat Journalbeat Beats Developers
Community Beats 1 new Topbeat Central Management

Elasticsearch 178 / week
Any questions related to Elasticsearch, including specific features, language clients and plugins.
Rally 1 unread

Logstash 95 / week
Everything related to your favorite centralized logging platform, including plugins and recipes.

Kibana 113 / week
All things about visualizing data in Elasticsearch & Logstash, including how to use Kibana and extending the platform.

APM 12 / week
Everything related to APM – whether it is the APM Server, the Kibana dashboards, or the agents.

Logs 55
Everything related to the Logs app – setup with Filebeat, Filebeat modules, and using the Kibana Logs app.

Metrics 1 / week
Everything related to metrics - Metricbeat integrations and modules, Kibana dashboards and the Metrics app.

Notes on Using These Forums 2
Meta Elastic Apr 2017

Couldn't push logs to elasticsearch using filebeat 1
Filebeat 3m

<BarSeries> configuration 0
Kibana 6m

Dec 15th, 2019: [EN] Elasticsearch Snapshot Lifecycle Management (SLM) with Minio.io S3 0
advent-staging 7m

Invalid IP network, skipping {network=>\"10.13.7.0/10.13.7.24\"} 0
Logstash 10m

FScrawler stuck at 2.6gb index size 2
Elasticsearch 11m

Elastic APM Java agent - sanitize_fields_names on application/json* data 1
APM java 21m

Metricbeat Failed to connect EOF 5
Metricbeat 22m

Mix free and paid licenses 0
Elasticsearch license 23m

Filebeat CPU utilization metrics are not normalized by default 2
Beats stack-monitoring 23m

How do I aggregate these documents 6
Logstash 26m

Metricbeat error 1
Metricbeat 28m



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

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

Official Elastic Training

<https://training.elastic.co>



Thanks for listening!

Q & A

Alexander Reelsen
Community Advocate
alex@elastic.co | spinscale

