Uptime Introduction

Alexander Reelsen
Community Advocate
alex@elastic.co | spinscale

Agenda

What is the Elastic Stack?
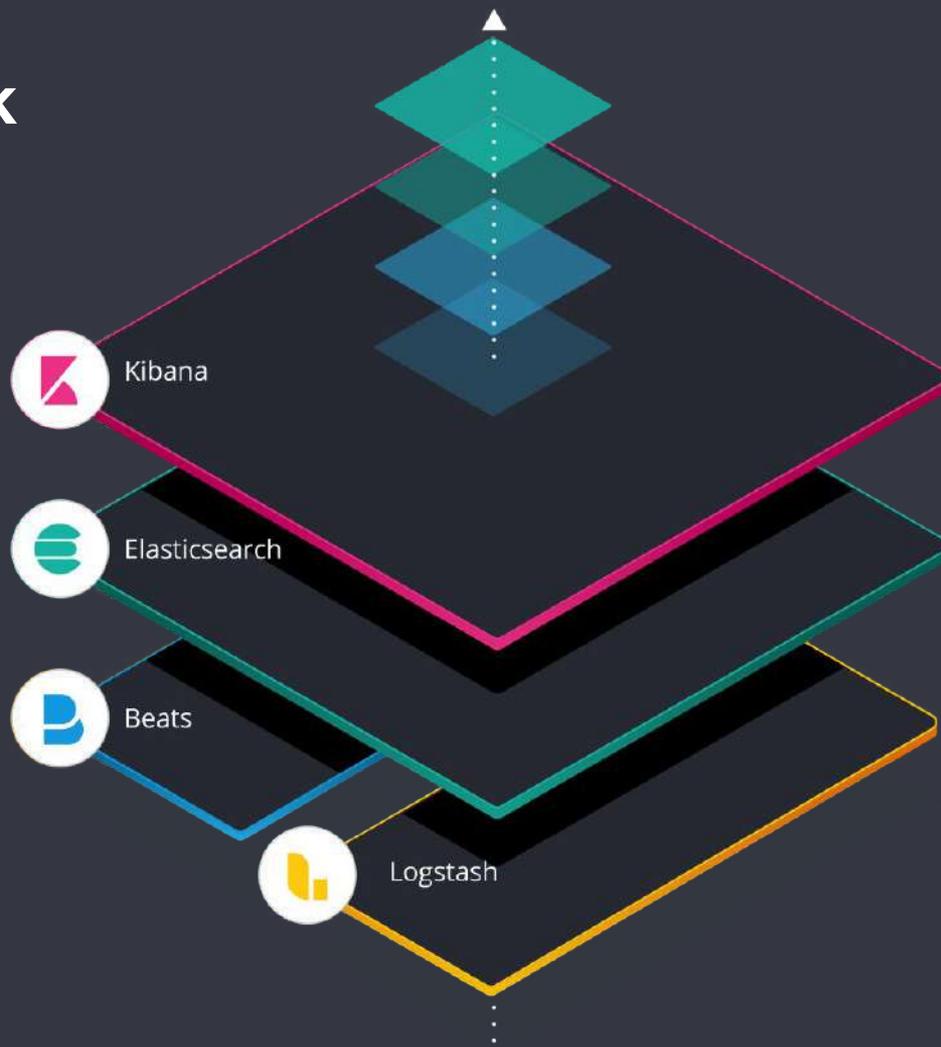
Installing

Heartbeat Deep Dive
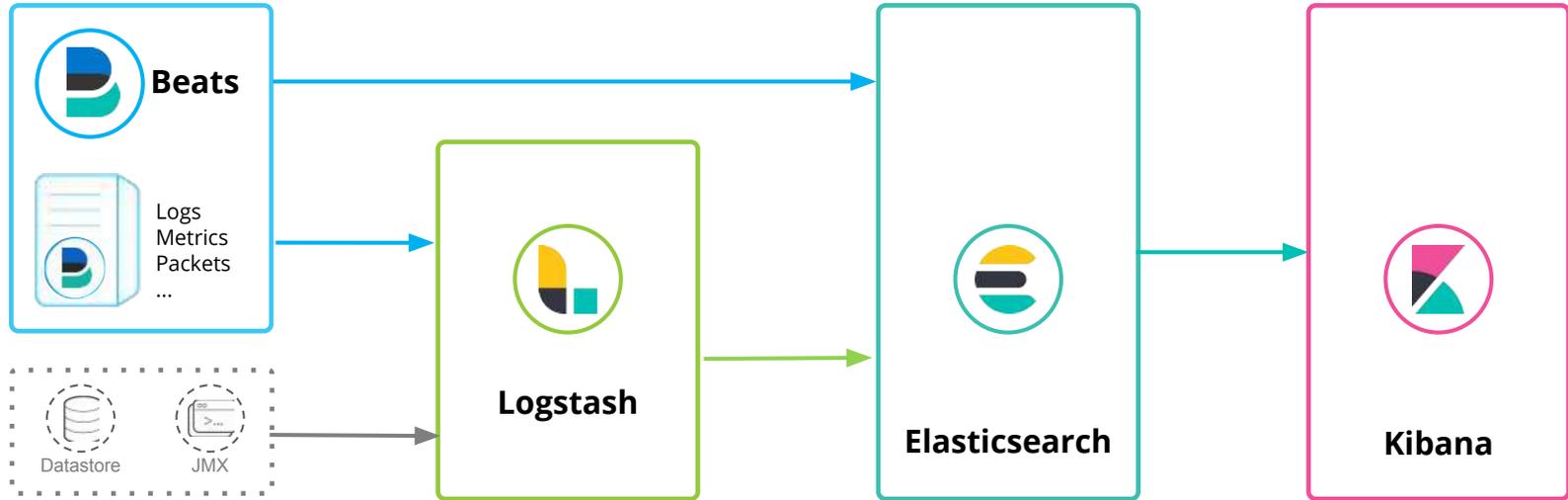
Uptime in the Kibana UI

Next steps

elastic

Elastic Stack

Kibana

Elasticsearch

Beats

Logstash

5

elastic

Elastic Stack - Data flows

Observability with the Elastic Stack

- Logs

- Metrics

- APM

- Infrastructure

- **Uptime**

elastic

kubernetes.labels.app : "kafka" and error | 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-35 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.

09 AM

12 PM

03 PM

06 PM

09 PM

Wed 27

03 AM

06 AM

Inventory   Metrics Explorer   Settings

View: Kubernetes ∨ | Q Search for infrastructure data... (e.g. host.name:host-1) | 📅 10/28/2019 5:20:18 PM | ▷ Auto-refresh
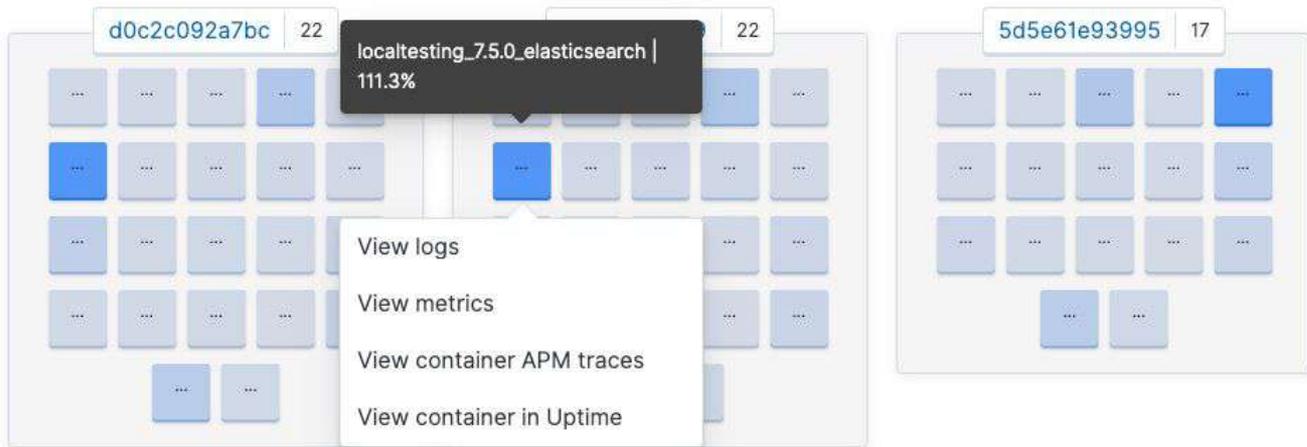
Metric: CPU usage ∨   Group By: All ∨

💾 Save   📤 Load

⠿ Map view   ≡ Table view
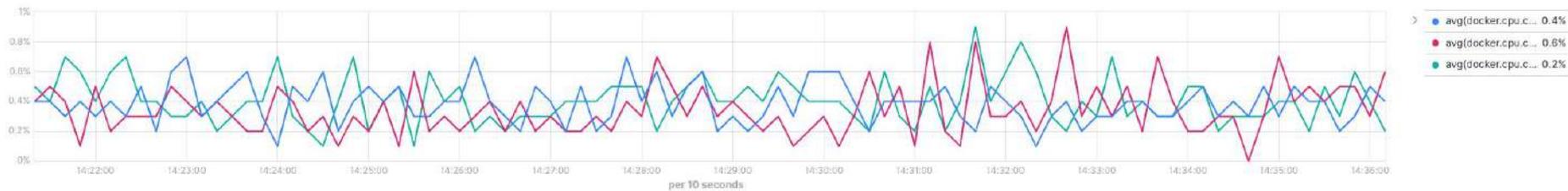
Showing the last 1 minute of data at the selected time

| d0c2c092a7bc | 22 |

localtesting_7.5.0_elasticsearch | 111.3%

| | 22 |

| 5d5e61e93995 | 17 |

View logs

View metrics

View container APM traces

View container in Uptime

0.3%

139.6%

Save   Share   Inspect   Refresh

Last 15 minutes   Show dates   Refresh

Time Series   Metric   Top N   Gauge   Markdown   Table

> ● avg(docker.cpu.c... **0.4%**
> ● avg(docker.cpu.c... **0.6%**
> ● avg(docker.cpu.c... **0.2%**

per 10 seconds

✓ Auto apply   The changes will be automatically applied.

Data   Panel options   Annotations

∨ ■ avg(docker.cpu.core.0.pct)   = 👁 📄 ⊕ 🗑

Metrics   Options

👁 **Aggregation**   **Field**   ⊕

Average   ∨   docker.cpu.core.0.pct   ⊗ ∨

Group by

Everything   ∨

∨ ■ avg(docker.cpu.core.1.pct)   = 👁 📄 ⊕ 🗑

Metrics   Options

👁 **Aggregation**   **Field**   ⊕

Average   ∨   docker.cpu.core.1.pct   ⊗ ∨

Group by

200 req.

0 req.

0 ms   50 ms   100 ms   150 ms   200 ms   250 ms   300 ms   350 ms   400 ms   450 ms   500 m

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**

⇆ HTTP 5xx **DispatcherServlet#doGet** 82 ms

GET opbeans-ruby 79 ms

⇆ HTTP 5xx **Rack** 73 ms

GET opbeans-python 70 ms

⇆ HTTP 5xx **GET opbeans.views.products** 2 66 ms

GET opbeans-node:3000 6,828 μs
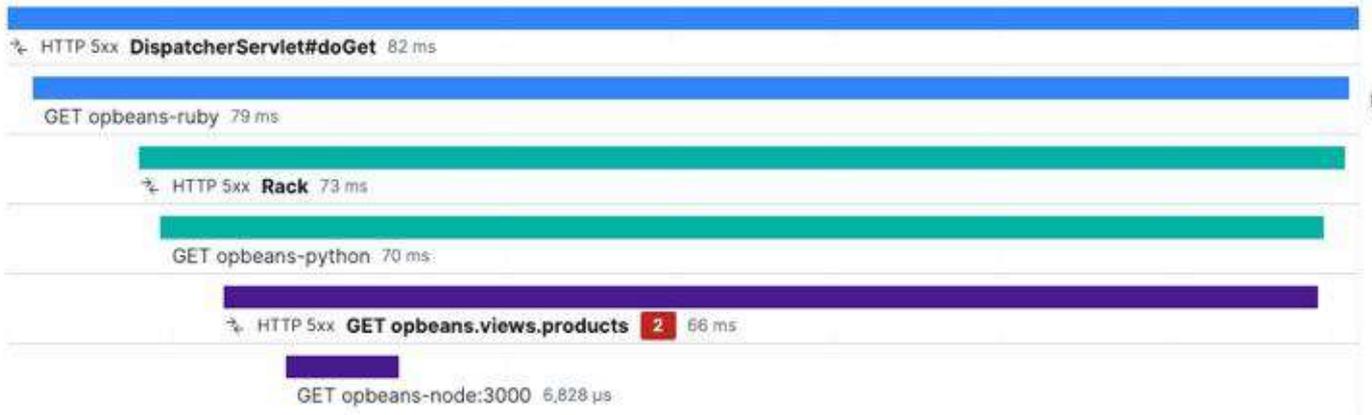
Uptime in 1 minute

- 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

elastic

Uptime

Overview

   ⟳ **Refresh**

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

| Up | Down | Location **3** ∨ | Port **7** ∨ | Scheme **3** ∨ |

12/33 monitors are down

- ● Down   12
- ● Up   21

Pings over time

Pings: 550 450 350 250 150 50

13:23 13:24 13:25 13:26 13:27 13:28 13:29 13:30 13:31 13:32 13:33 13:34 13:35 13:36 13:37

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 ⌐	▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮	⋯ ∨

Service Monitor

auto-tcp-0X59D12A2A76D484B4

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

Last 15 minutes   Show dates   ↻ Refresh

Monitor duration

Duration ms / Timestamp

● nyc-dc1-rack1	1	● uk-dc2-rack3	1
● ca-dc2-rack1	1		
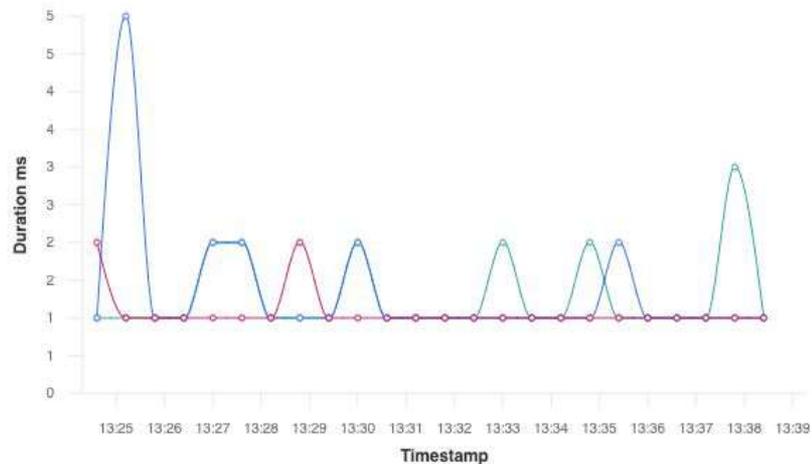
Pings over time

Pings

History

Status

All ⌄

Location

All ⌄

RubyAPI

auto-http-0X690192E6E8794587-3e4ce6d2d3838a27

Last 15 minutes   Show dates   ↻ **Refresh**

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

Monitor duration

Duration ms / Timestamp
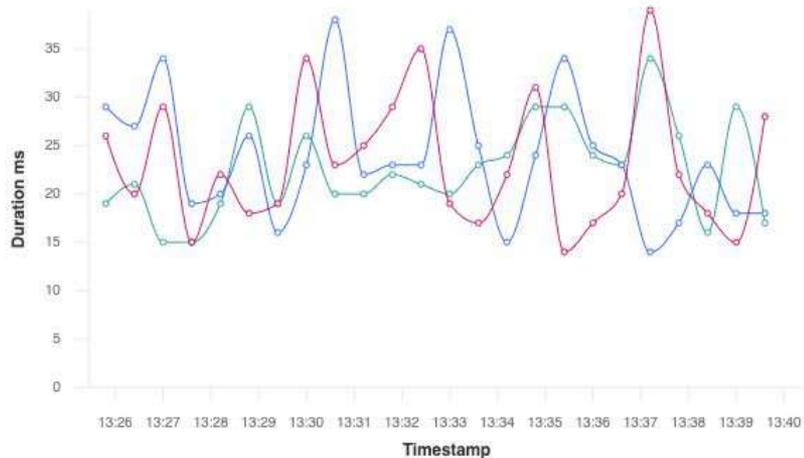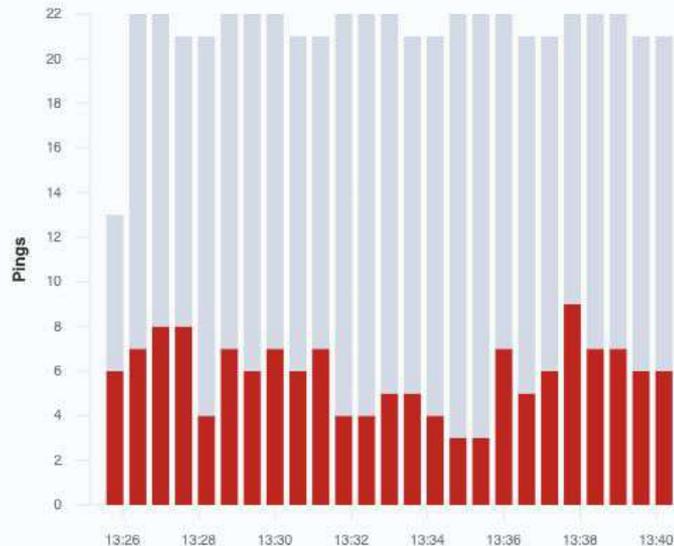
● nyc-dc1-rack1   17   ● uk-dc2-rack3   18
● ca-dc2-rack1   28

Pings over time

Pings

History

Status   **Location**

All ∨   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

elastic

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

elastic

Installation Elasticsearch + Kibana

- Elastic Cloud

- ECE

- ECK

- Self-Hosted (docker, rpm, deb, tar.gz)

elastic

Installation heartbeat

- Self-Hosted (docker, rpm, deb, tar.gz)

- Multiple instances

  – Cross data center

  – Cross continents

  – Where your customers are

elastic

elastic

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
```

elastic

Uptime

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

- Down   3
- Up   9

Pings over time

Pings: 22, 18, 14, 10, 6, 2

Time axis: 15:22 15:23 15:24 15:25 15:26 15:27 15:28 15:29 15:30 15:31 15:32 15:33 15:34 15:35 15:36

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-0X55DCE88E620C0449	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

Duration ms / Timestamp
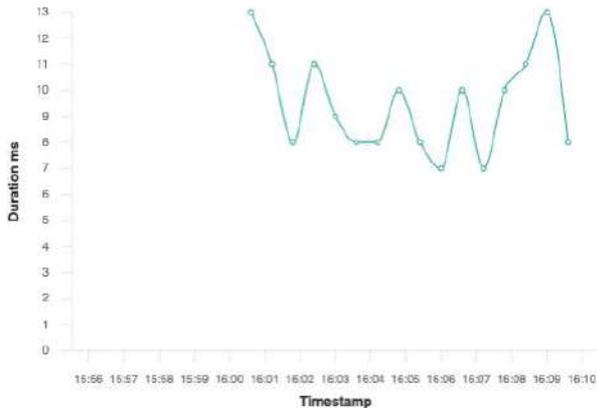
● spinscale-at-home   8

Pings over time

Pings
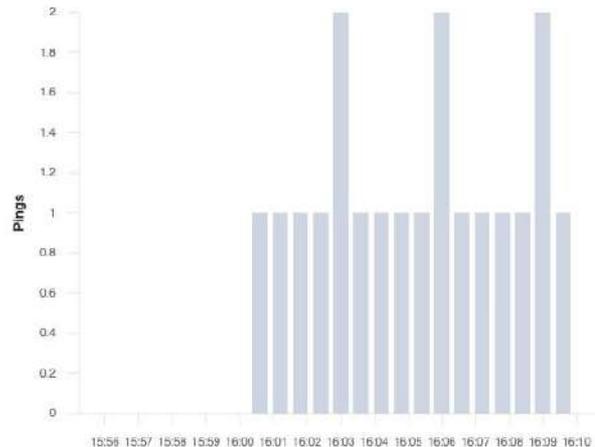
History

Status
All

Location
All

Status	Location	IP	Duration	Error type	
● Up Checked a few seconds ago	spinscale-at-home	8.8.8.8	8 ms		⌄

Summary

Summary

- External state knowledge is important

- Understand up/down states

- Understand response times

- Visualize changes over time

elastic

Location Location Location!
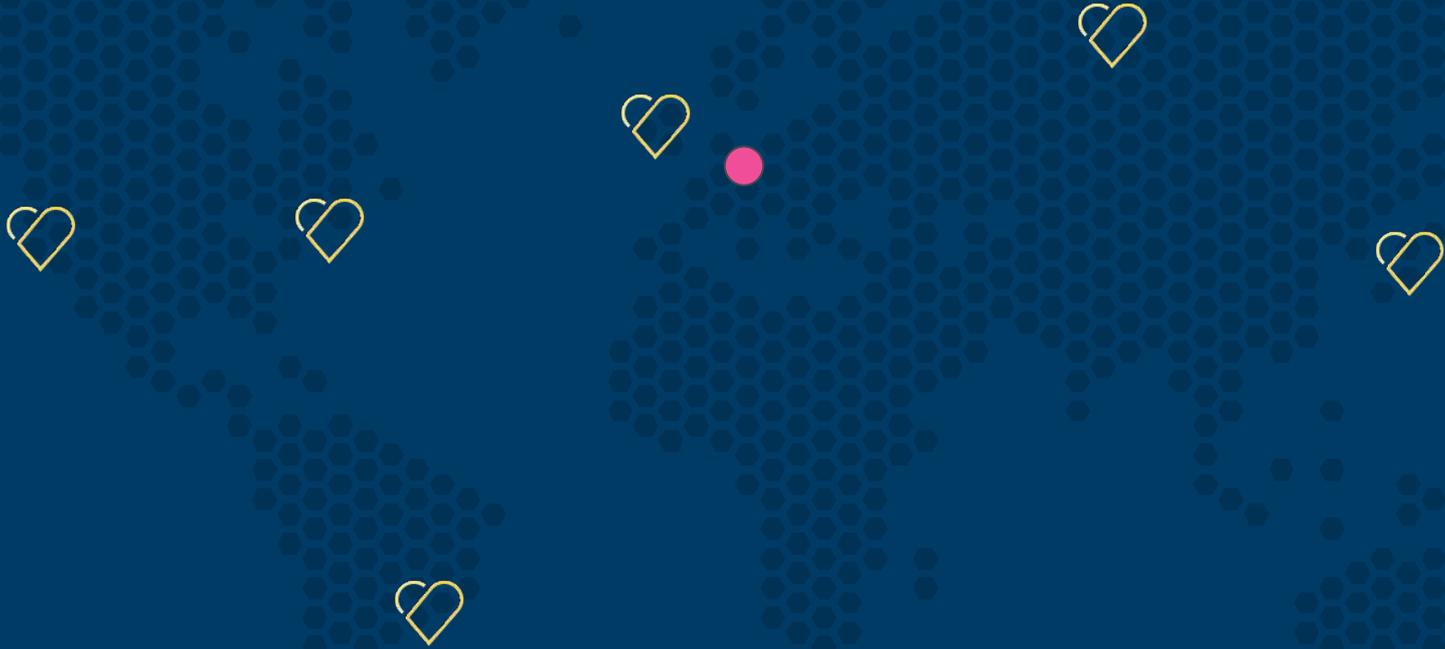
Next steps

- Autodiscovery

- Configure custom CAs

- Configure scheduler limit and timezone

- Add processors like `add_locale`, `add_observer_metadata`

- Security privileges

elastic

In development

- Kibana Alerting Integration

- ML Integration

- CCS support

- Central management

elastic

Elastic Cloud

Elastic Support Subscriptions

43

Getting help

Discuss forum

https://discuss.elastic.co

Community & Meetups

https://community.elastic.co

Official Elastic Training

https://training.elastic.co

Thanks for listening!

Q & A

Alexander Reelsen
Community Advocate
alex@elastic.co | spinscale