



# Statuscake vs Kibana alerting

---

Diana Todea - SRE - Platform Observability  
@ Elastic  
SREDay Presenter - September 2023, London, UK



1

What is Elastic

---

2

SRE @ Observability

---

3

Statuscake alerts

---

4

In house alerting

---

5

Synthetic monitoring

---

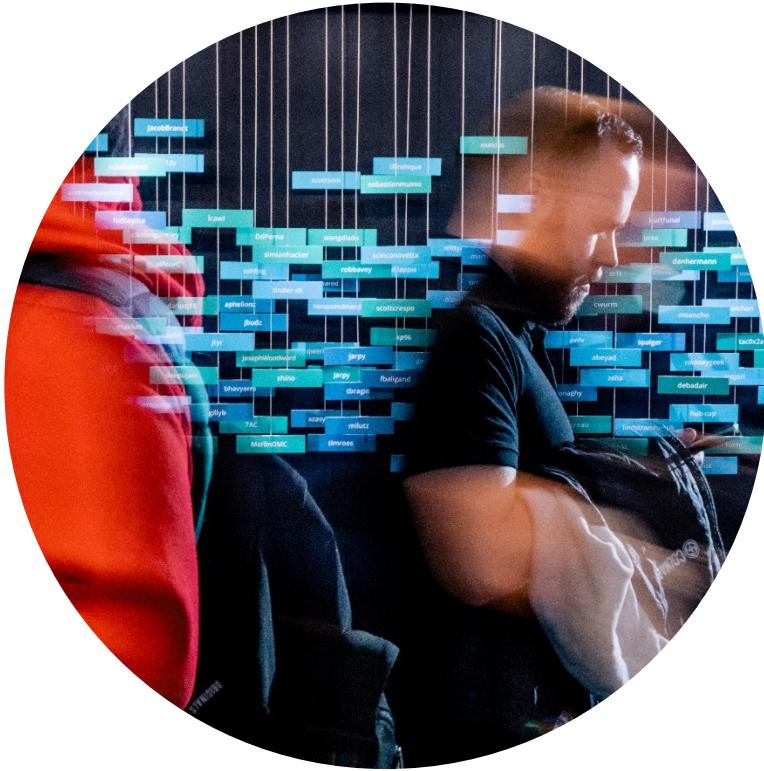
6

SRE on call experience

---

7

Going forward



# Search Source Code ElasticON Tour



A photograph of two police officers in uniform, looking towards the camera with expressions of surprise or concern. One officer is in the foreground, and another is partially visible behind him.

# Neighbourhood Watch

SRE



# Search. Observe. Protect.



APM



LOGS



METRICS

Microservices  
Cloud-native  
OpenTelemetry  
Serverless

Application  
Cloud  
Container  
Database  
Infrastructure  
Web

Container  
Database  
Host  
Network  
Storage



SYNTHETIC

Uptime  
User experience  
User journey  
Web performance



PROFILING

Application  
Cloud-native  
eBPF  
Infrastructure  
Services  
Whole system

# Past: Statuscake

What is Statuscake?  
An uptime monitoring platform

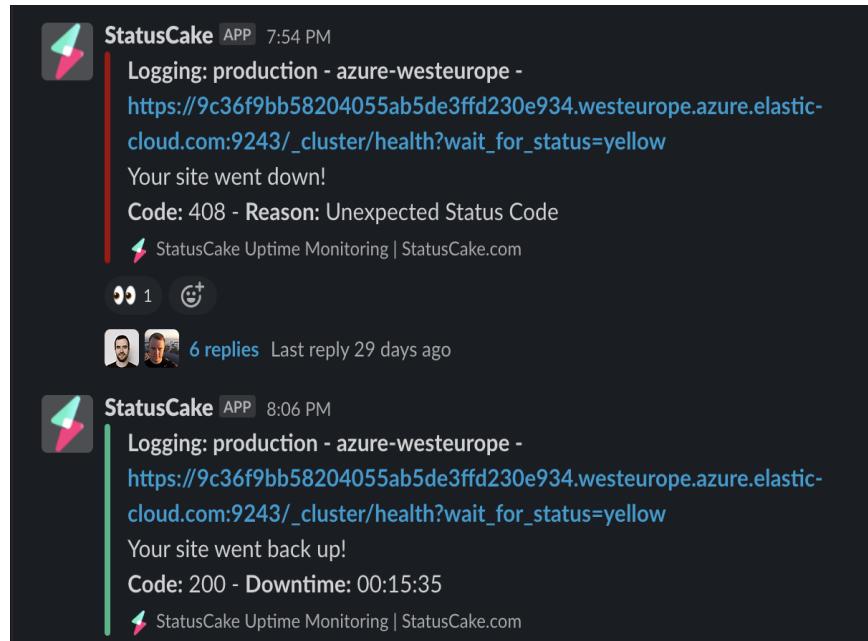
Pros:

fast alerting response (almost live)

Cons:

external tool>slower management

Can we use in-house alerting?



# Proposal: Kibana alerting

## Pros:

in-house tool that has integration with synthetic monitoring

## Cons:

slightly slower alerting response



O11y Alertbot APP 11:02 AM

[Production]Observability deployment check | Monitor | Runbook | Alert Details

production: logging - gcp-us-central1 from Europe - United Kingdom

The deployment status is unhealthy

Reason: production: logging - gcp-us-central1 from Europe - United Kingdom failed 2 times in the last 5 mins. Alert when > 2.

AlertID: Observability deployment check | production: logging - gcp-us-central1

✓ [Production] Alert recovered for production: logging - gcp-us-central1 from North America - US East.

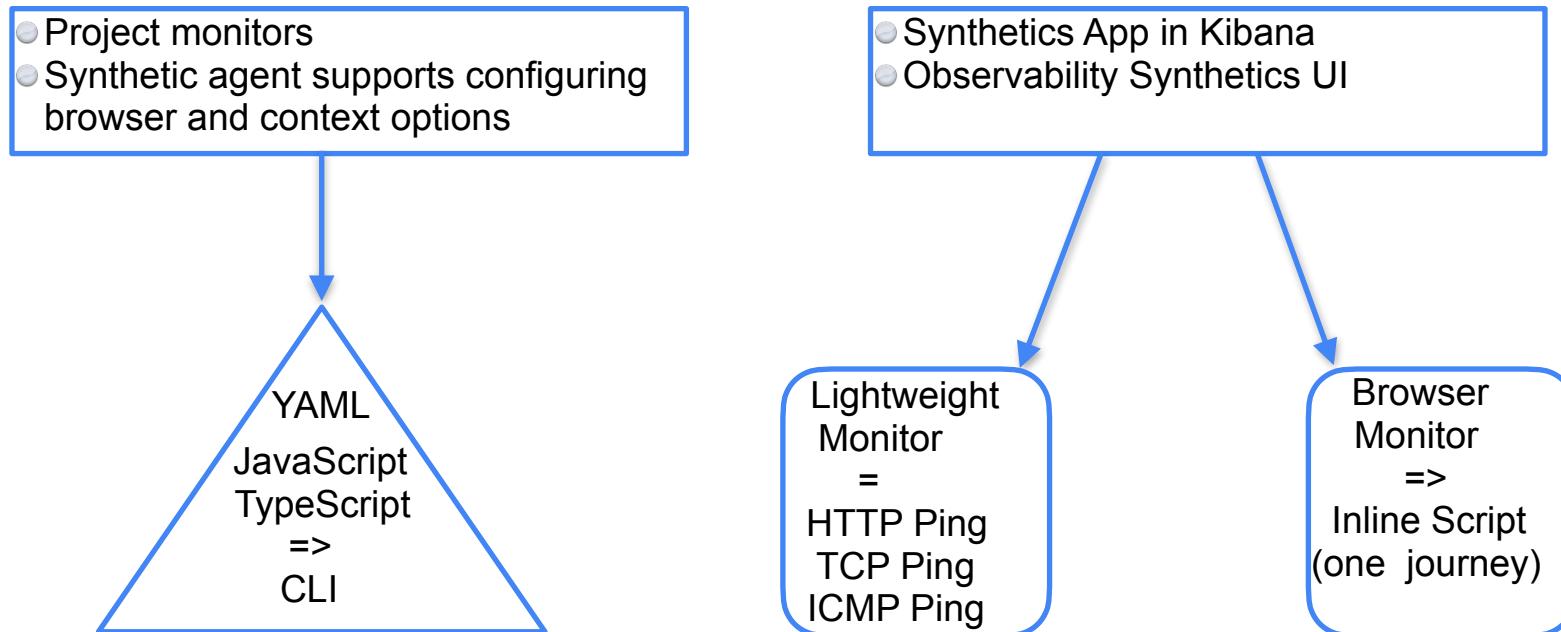
AlertID: Observability deployment check | production: logging - gcp-us-central1

✓ [Production] Alert recovered for production: logging - gcp-us-central1 from Europe - United Kingdom.

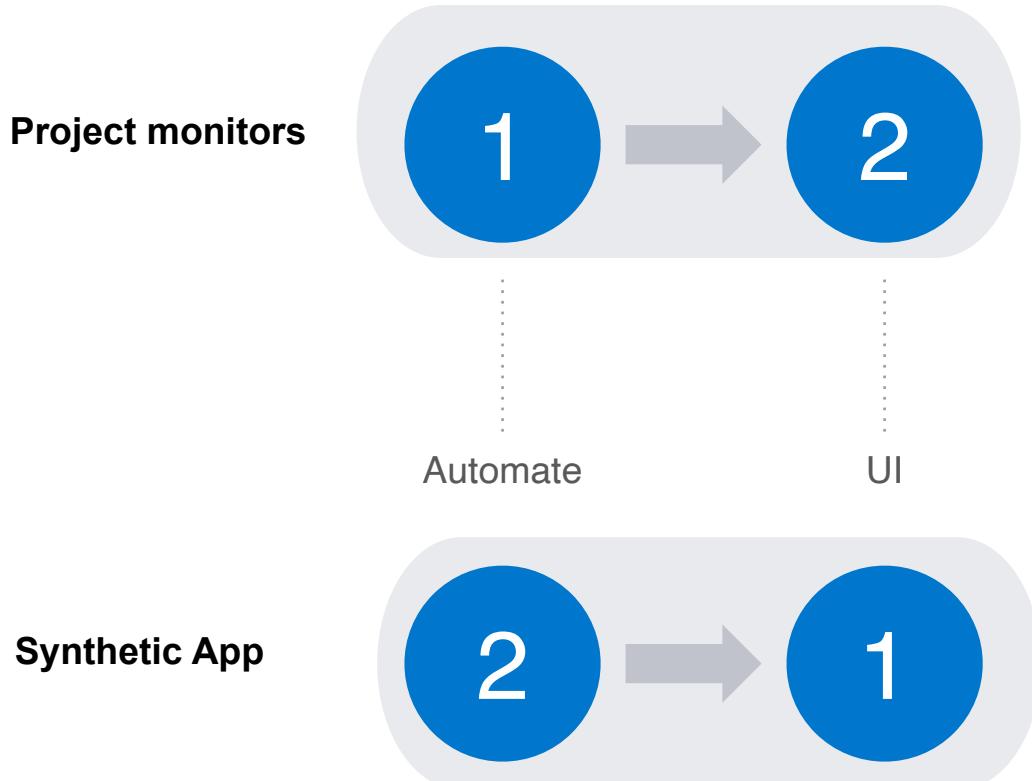
AlertID: Observability deployment check | production: logging - gcp-us-central1

# Synthetic monitoring

<https://www.elastic.co/guide/en/observability/current/monitor-upptime-synthetics.html>



# Workflow



github.com/elastic/synthetics-monitors

New Hire Info-Sec Tools Observability Github Staging Docs IBM conversations Misc K8s On-call HR Synthetics Jira Career talk Tax Spain ecctl VKB Welcome to Micro...

elastic / synthetics-monitors

Code Issues Pull requests Projects Wiki Security Insights Settings

synthetics-monitors · Private

Watch 14 Fork 8 Star 0

main 1 branch 0 tags

Go to file Add file Code

rhass Add Linux support to Makefile and clean target. (#24) af34c12 5 days ago 104 commits

.github/workflows Replace github actions to a generic one 9 months ago

production/production\_overview\_m... Add aws-eu-north-1 to Synthetics monitors (#25) 2 weeks ago

qa Cluster api journey (#26) last week

scripts Add loadbalance SLA checks (#7) last month

staging/staging\_overview\_monitors Add loadbalance SLA checks (#7) last month

tools Add aws-eu-north-1 to Synthetics monitors (#25) 2 weeks ago

.gitignore Add loadbalance SLA checks (#7) last month

Makefile Add Linux support to Makefile and clean target. (#24) 5 days ago

README.md Add loadbalance SLA checks (#7) last month

README.md

## Synthetics Internal monitors

GITHUB ACTIONS ARE DISABLED IN THIS REPO

Type ⌘ to search

About Repository for synthetics monitors used in Elastic

Readme Security policy Activity 0 stars 14 watching 8 forks

Releases No releases published Create a new release

Packages No packages published Publish your first package

Contributors 12

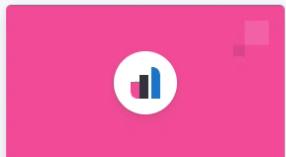


## Welcome home



### Enterprise Search

Create search experiences with a refined set of APIs and tools.



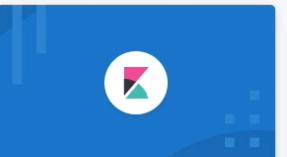
### Observability

Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs.



### Security

Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.



### Analytics

Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications.

## Get started by adding integrations

To start working with your data, use one of our many ingest options. Collect data from an app or service, or upload a file. If you're not ready to use your own data, play with a sample data set.

[Setup guides](#)[+ Add integrations](#)[Try sample data](#)[Upload a file](#)

## Management

[Dev Tools](#) [Stack Management](#)[Manage permissions](#)[Monitor the stack](#)[Back up and restore](#)[Manage index lifecycles](#)

 elastic

Find apps, content, and more.

Updated 20s ago 1m Alerts and rules Settings Explore data Inspect

D Observability Synthetics Overview

## Monitors

Overview Management

⚠ Alerts are not being sent  
You have monitors with alerting enabled, but there is no default connector configured to send those alerts.  
[Configure now](#)

Search by name, URL, host, tag, project or location

Up Down Disabled Type 2 Location 10 Tags 4 Frequency 3 Project 2

**Current status**  
1610 Up 10 Down 0 Disabled

**Last 6 hours**  
14 Errors 

**Last 12 hours**  
14 Alerts 

Showing 1,620 Monitors Sort by Status Group by None

Test Metadata Access	Duration
Asia/Pacific - Japan	16 s
Asia/Pacific - Singapore	16 s
Asia/Pacific - Australia East	16 s
Asia/Pacific - India	16 s
Europe - United Kingdom	16 s
Europe - Germany	16 s
North America - Canada East	16 s
South America - Brazil	16 s

# PagerDuty integration

## Errored Actions

Message		
rule executed: xpack.uptime.alerts.monitorStatus:6bc9bdd0-6fc4-11ed-bdfe-fd5199a89568: 'Observability deployment check'		
<span style="background-color: #f08080; border-radius: 5px; padding: 2px 5px;">2</span> errored actions		
Timestamp ↓	Type	Message
Apr 25, 2023 @ 09:49:42.474	actions	action execution failure: .pagerduty:fed2b030-ddd0-11ed-933a-8f1e1945f2fc: pd-production-alert - error validating action params: [dedupKey]: value has length [268] but it must have a maximum length of [255].
Apr 25, 2023 @ 09:49:42.455	actions	action execution failure: .pagerduty:fed2b030-ddd0-11ed-933a-8f1e1945f2fc: pd-production-alert - error validating action params: [dedupKey]: value has length [268] but it must have a maximum length of [255].

<https://github.com/elastic/cloud/issues/114170>

**Observability deployment check alert doesn't fire in PD #114170**

Closed ElasticViking opened this issue 2 days ago · 3 comments

ElasticViking commented 2 days ago · edited

Observability deployment check alert in production doesn't fire in PD anymore  
The alert fires in #cloud-alerts-critical.  
Slack: <https://elastic.slack.com/archives/CGM2U8Q84/p1682258596075599>  
Linked to: #114115  
Initial troubleshooting:  
Alert is not firing since April 20th, 7:23 AM.

ElasticViking added Team:Observability, sre-on-call-improvements labels 2 days ago

ElasticViking self-assigned this 2 days ago

ElasticViking added the Team:Observability.alert-response label 2 days ago

ElasticViking commented 2 days ago · edited

Alert was firing correctly up to 20th of April 7:23 AM. The synthetic monitors trigger correctly the alarm via Kibana, the timing coincides with the alerts from slack.  
Tested the PD connector via Kibana: <https://elastic.pagerduty.com/incidents/Q379012GJ3RXAA>. Result ok.  
Looks like a dedup key error:

Observability deployment check	Errorred Actions													
Last updated by elastic on Apr 25, 2023 · Created by elastic on Nov 20, 2022 · 0 files	<p>Action: <a href="#">Archive</a></p> <p>Message</p> <p>Rule executed: <code>spark-update.alarms.monitor.status.doc{body@0-8t-1fe8-baf6-fd19fb9a9568}::Observability deployment check</code></p> <p>Errored actions</p> <table border="1"><thead><tr><th>Search log message</th><th>Last 24 hours</th></tr></thead><tbody><tr><td><input type="text"/></td><td><input type="button"/></td></tr><tr><td>Timestamp</td><td>Type</td><td>Message</td></tr><tr><td>Apr 25, 2023 @ 09:49:42.414</td><td>actions</td><td>action execution failure: pagerduty/hel2020-09-09-11ep-933a-ef7e1945f7c [208] but it must have a maximum length of 1255.</td></tr><tr><td></td><td></td><td>action execution failure: pagerdry/hel2020-09-09-11ep-933a-ef7e1945f7c [208] but it must have a maximum length of 1255.</td></tr></tbody></table>	Search log message	Last 24 hours	<input type="text"/>	<input type="button"/>	Timestamp	Type	Message	Apr 25, 2023 @ 09:49:42.414	actions	action execution failure: pagerduty/hel2020-09-09-11ep-933a-ef7e1945f7c [208] but it must have a maximum length of 1255.			action execution failure: pagerdry/hel2020-09-09-11ep-933a-ef7e1945f7c [208] but it must have a maximum length of 1255.
Search log message	Last 24 hours													
<input type="text"/>	<input type="button"/>													
Timestamp	Type	Message												
Apr 25, 2023 @ 09:49:42.414	actions	action execution failure: pagerduty/hel2020-09-09-11ep-933a-ef7e1945f7c [208] but it must have a maximum length of 1255.												
		action execution failure: pagerdry/hel2020-09-09-11ep-933a-ef7e1945f7c [208] but it must have a maximum length of 1255.												

# Grouped in PagerDuty but not resolved

ALERTS > ALERT DETAILS

Observability deployment check Kibana: The deployment status is unhealthy. production: logging - gcp-us-central1 from Europe - United Kingdom failed 2 times in the last 5 mins. Alert when > 2. ALERT

Belongs to Incident: [#369733] Observability deployment check Kibana: The deployment status is u... (Resolved)

Severity Critical  
Alert Times Open from Apr 26, 2023 at 11:11 AM to Apr 26, 2023 at 11:17 AM (for 6 minutes)  
Alert Key production-logging-gcp-us-central1-prod\_overview\_monitors-default

Current Status Resolved  
Service Name External Monitoring for Cloud  
Integration APIv2  
Source Kibana Action fed2b030-ddd0-11ed-933a-8f1e1945f2fc

**Details**

SUMMARY  
Observability deployment check Kibana: The deployment status is unhealthy. production: logging - gcp-us-central1 from North America - US East failed 2 times in the last 5 mins. Alert when > 2.  
[View Message](#)

**Alert Log**

Time	Activity
on Apr 26, 2023 at 11:17 AM	Resolved by Faisal Zulfiqar through the website.
on Apr 26, 2023 at 11:12 AM	Triggered and updated Summary. <a href="#">SHOW DETAILS</a>
on Apr 26, 2023 at 11:11 AM	Triggered and automatically linked. <input checked="" type="checkbox"/> HIDE DETAILS Automatically added to Incident [#369733] Observability deployment check Kibana: The deployment status is unhealthy. production: logging - gcp-us-central1 from North America - US East failed 2 times in the last 5 mins. Alert when > 2. <input checked="" type="checkbox"/> Triggered through the API. Description: Observability deployment check Kibana: The deployment status is unhealthy. production: logging - gcp-us-central1 from North America - US East failed 2 times in the last 5 mins. Alert when > 2. <a href="#">(View Message)</a>

Manually resolved by the on-call SRE

"dedupKey": "{{rule.id}}:  
{{alert.id}}"

"dedupKey":  
"{{state.monitorId}}"

# "dedupKey": "{{rule.id}}:{{alert.id}}" = Resolved through API

ALERTS > ALERT DETAILS

ZK Learners Check Region: azure-eastus Region: azure-eastus Region: azure-eastus Region: azure-eastus has failed (ALERT)

Belongs to Incident: [\[#400614\] ZK Learners Check Region: azure-eastus Region: azure-eastus Region...](#) (Resolved)

Severity Critical

Alert Times Open from Aug 18, 2023 at 5:17 PM to Aug 18, 2023 at 5:37 PM (for 20 minutes)

Alert Key 2fc8caf0-2af0-1lee-b047-71cb251ee80e:query matched

Current Status Resolved

Service Name External Monitoring for Cloud

Integration APIN2

Source Kibana Action 92e890b0-b89b-11ed-8f92-1b8618dced20

## Details

### SUMMARY

ZK Learners Check Region: azure-eastus Region: azure-eastus Region: azure-eastus Region: azure-eastus has failed

[View Message](#)

## Alert Log

Time	Activity	<span>SHOW ALL DETAILS</span>
on Aug 18, 2023 at 5:37 PM	<span>Resolved through the API.</span> <a href="#">(View Message)</a>	
on Aug 18, 2023 at 5:17 PM	<span>Triggered</span> and automatically linked. <a href="#">(Show Details)</a>	



# Solution

ALERTS > ALERT DETAILS

Observability deployment check Kibana: The deployment status is unhealthy. Monitor "production: logging - azure-eastus2" from Europe - United Kingdom failed 3 times in the last 5 mins. Alert when > 3. Checked at September 11, 2023 1:33 PM. [ALERT](#)

Belongs to Incident: [\[#411283\] Observability deployment check Kibana: The deployment status is u...](#) (Resolved)

Severity Critical

Alert Times Open from 3:34 PM to 3:38 PM (for 4 minutes)

Alert Key 6bc9bdd0-6fc4-11ed-bdfe-fd5199a89568:9c9cd26b-e9ce-47e6-b12d-51b92ab7098e

Current Status Resolved

Service Name External Monitoring for Cloud

Integration APIv2

Source Kibana Action fed2b030-ddd0-11ed-933a-8f1e1945f2fc

## Details

### SUMMARY

Observability deployment check Kibana: The deployment status is unhealthy. Monitor "production: logging - azure-eastus2" from Europe - United Kingdom failed 3 times in the last 5 mins. Alert when > 3. Checked at September 11, 2023 1:33 PM.

[View Message](#)

## Alert Log

Time	Activity	<a href="#">SHOW ALL DETAILS</a>
at 3:38 PM	<a href="#">Resolved through the API.</a> <a href="#">(View Message)</a>	
at 3:34 PM	Triggered and automatically linked. <a href="#">SHOW DETAILS</a>	

```
"dedupKey": "{{rule.id}}:  
{{alert.id}}"
```

```
"dedupKey": "{{rule.id}}:  
{{alert.uuid}}"
```

alert.id=The ID of the alert that scheduled the action.

alert.uuid=A universally unique identifier for the alert. While the alert is active, the UUID value remains unchanged each time the rule runs.



# Going forward

- In-house alert management 
- Cross team collaboration for feature requests
- Better SRE on-call experience

# Improvements

- Faster alert response for Kibana
- Grouping the alerts in  cloud-alerts-critical



# Q&A

---

