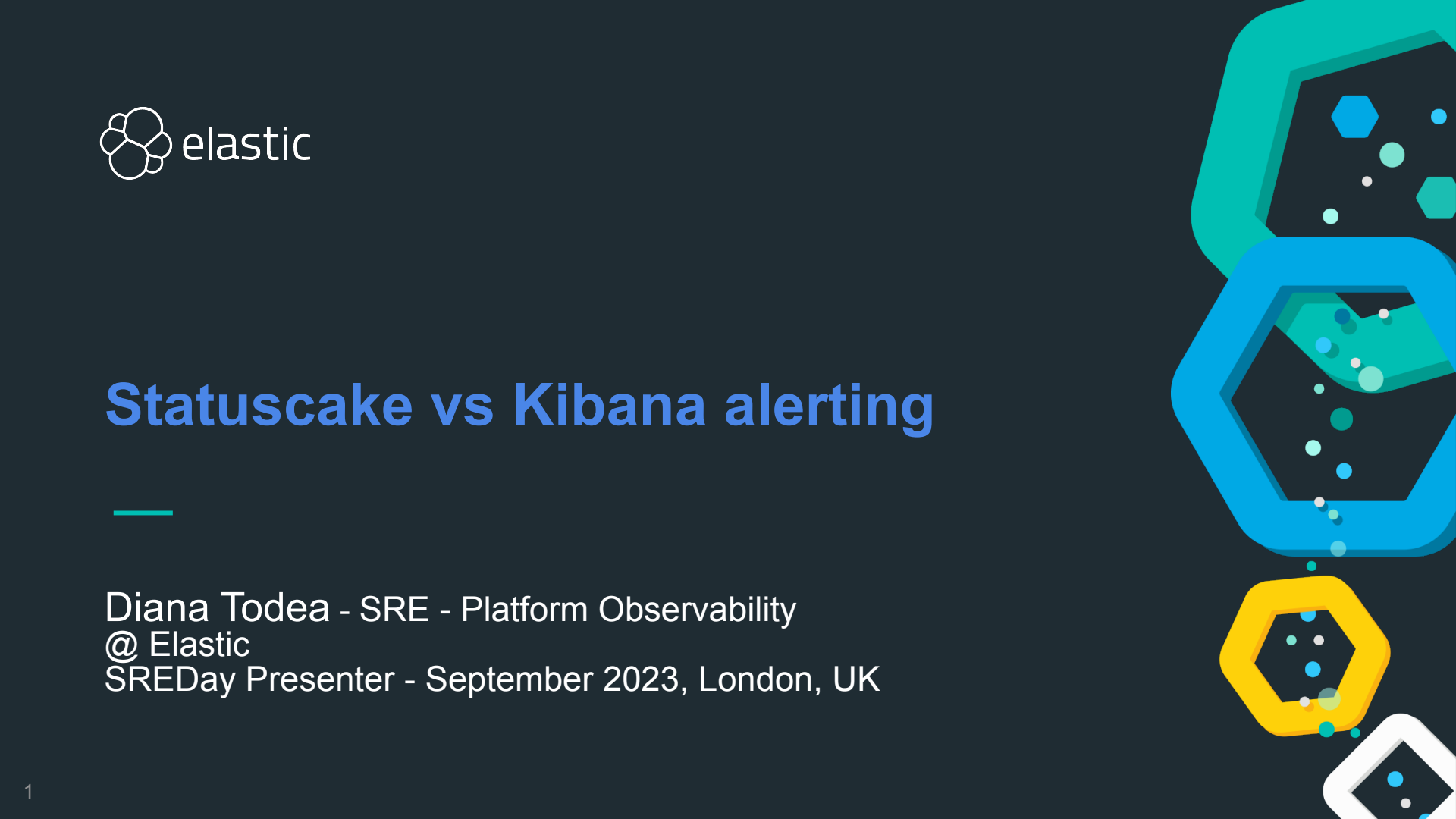


Statuscake vs Kibana alerting

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

elastic

Search
Source Code
ElasticON Tour


Neighbourhood
Watch
SRE
24/7

Search. Observe. Protect.

APM

Microservices
Cloud-native
OpenTelemetry
Serverless

LOGS

Application
Cloud
Container
Database
Infrastructure
Web

METRICS

Container
Database
Host
Network
Storage

SYNTHETIC

Uptime
User experience
User journey
Web performance

PROFILING

Application
Cloud-native
eBPF
Infrastructure
Services
Whole system

elastic

Past: Statuscake

What is Statuscake?
An uptime monitoring platform

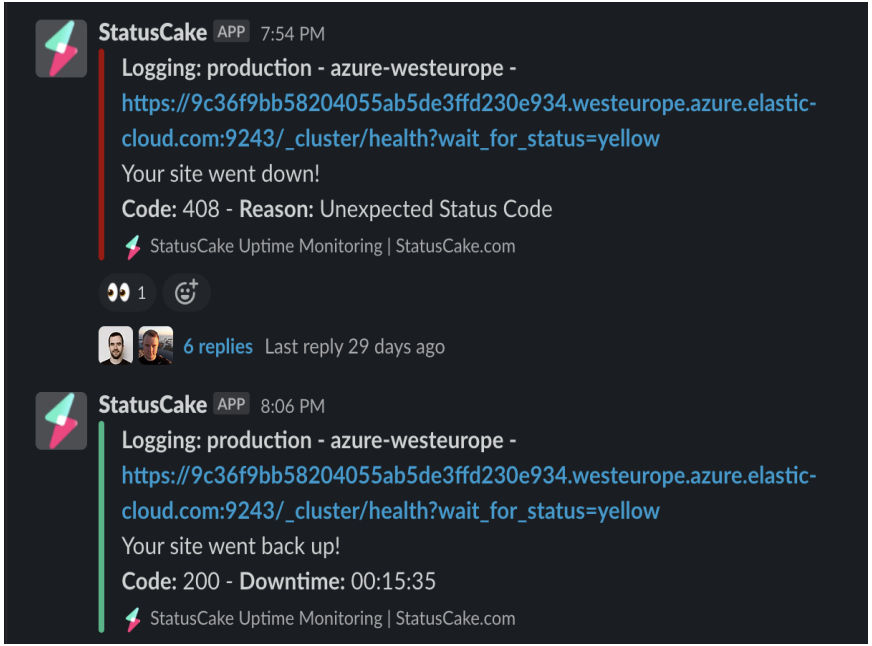
Pros:

fast alerting response (almost live)

Cons:

external tool>slower management

Can we use in-house alerting?



elastic

Proposal: Kibana alerting

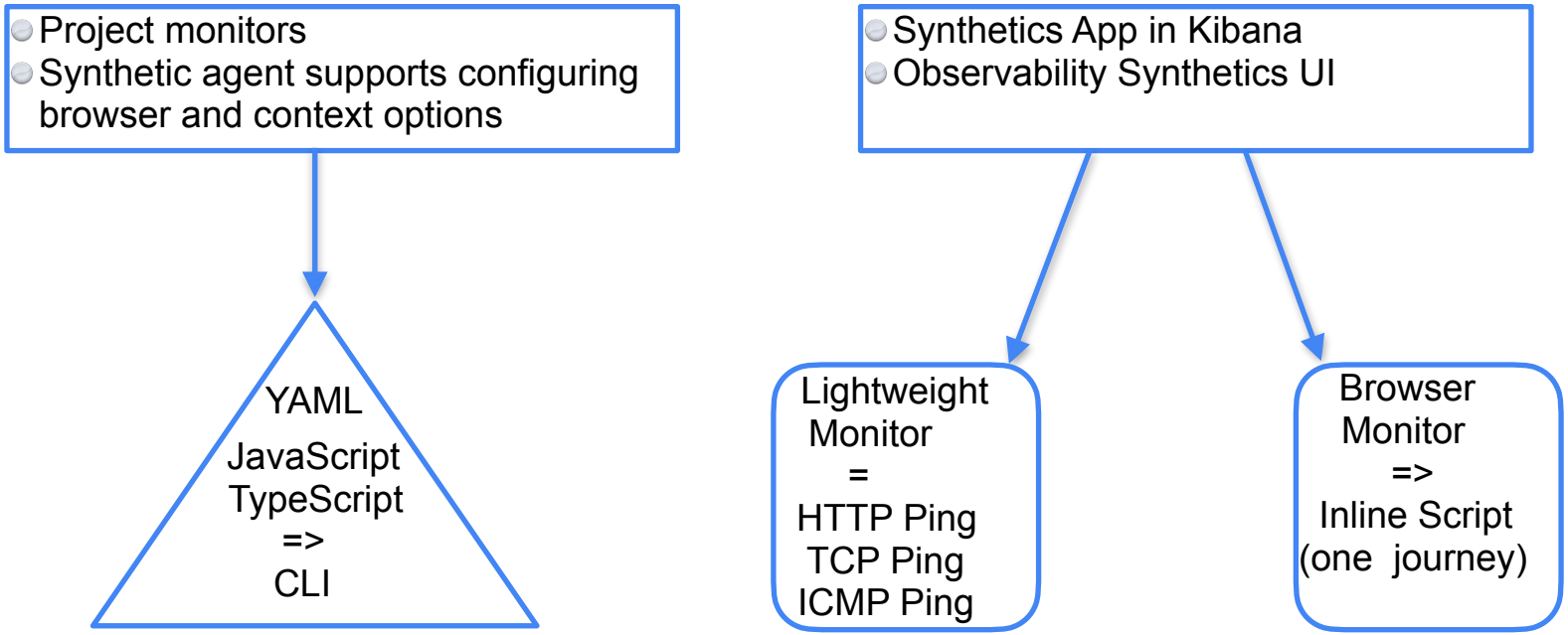
Pros:
in-house tool that has integration with synthetic monitoring

Cons:
slightly slower alerting response

elastic

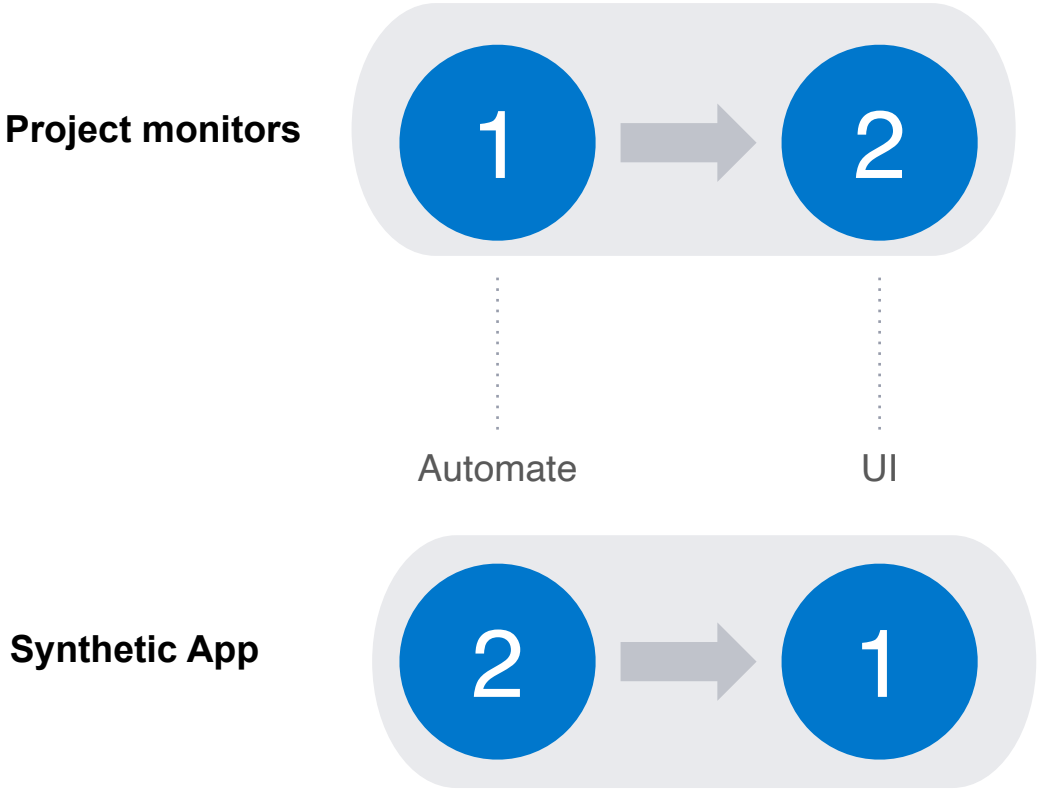
Synthetic monitoring

https://www.elastic.co/guide/en/observability/current/monitor-uptime-synthetics.html

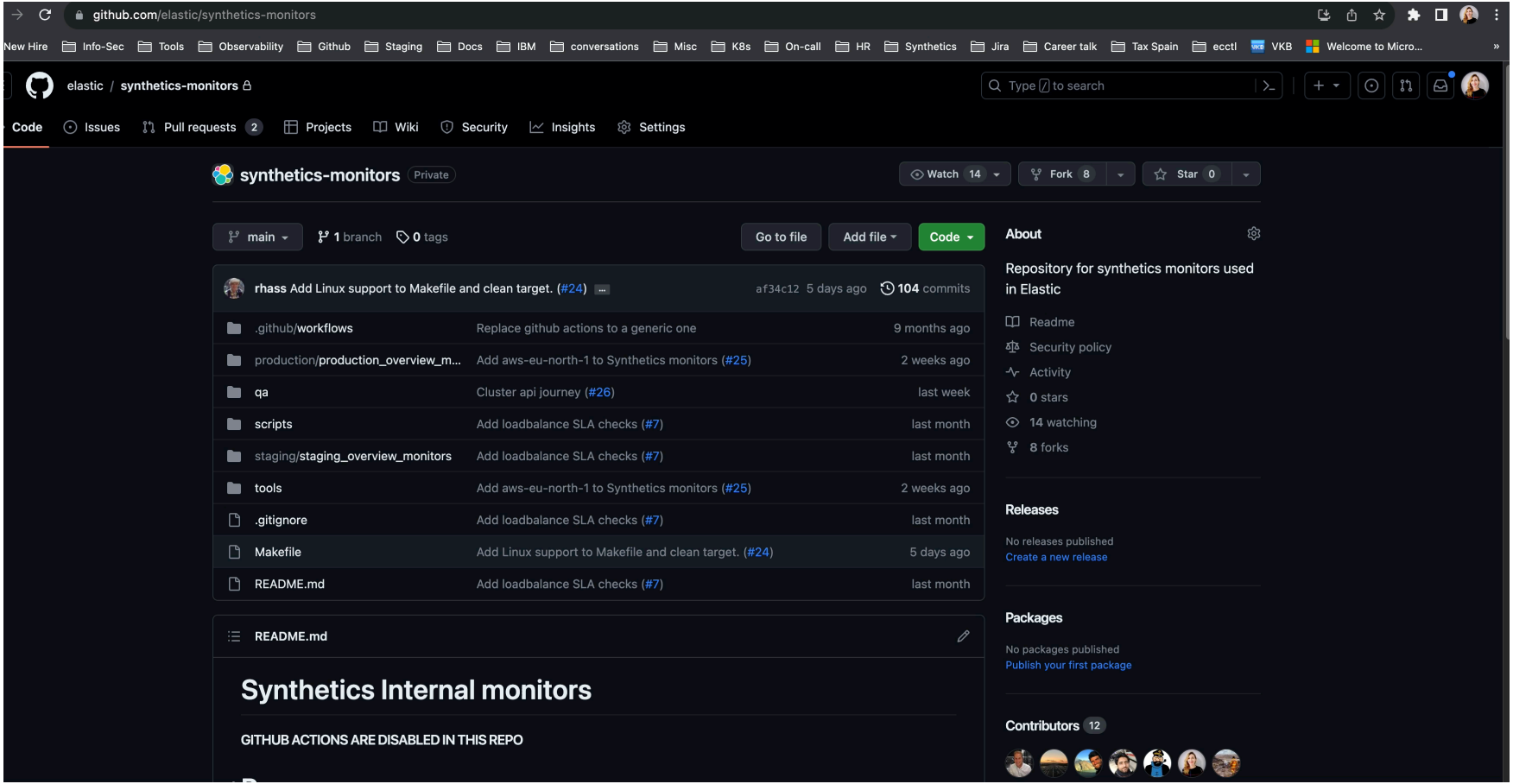


elastic

Workflow



elastic


github.com/elastic/synthetics-monitors
elastic / synthetics-monitors
Type / to search
Code
Issues
Pull requests 2
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
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

elastic

Find apps, content, and more. ⌘/

D Home

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.

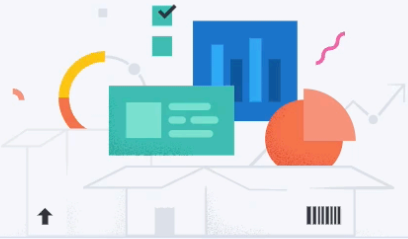
Analytics

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.

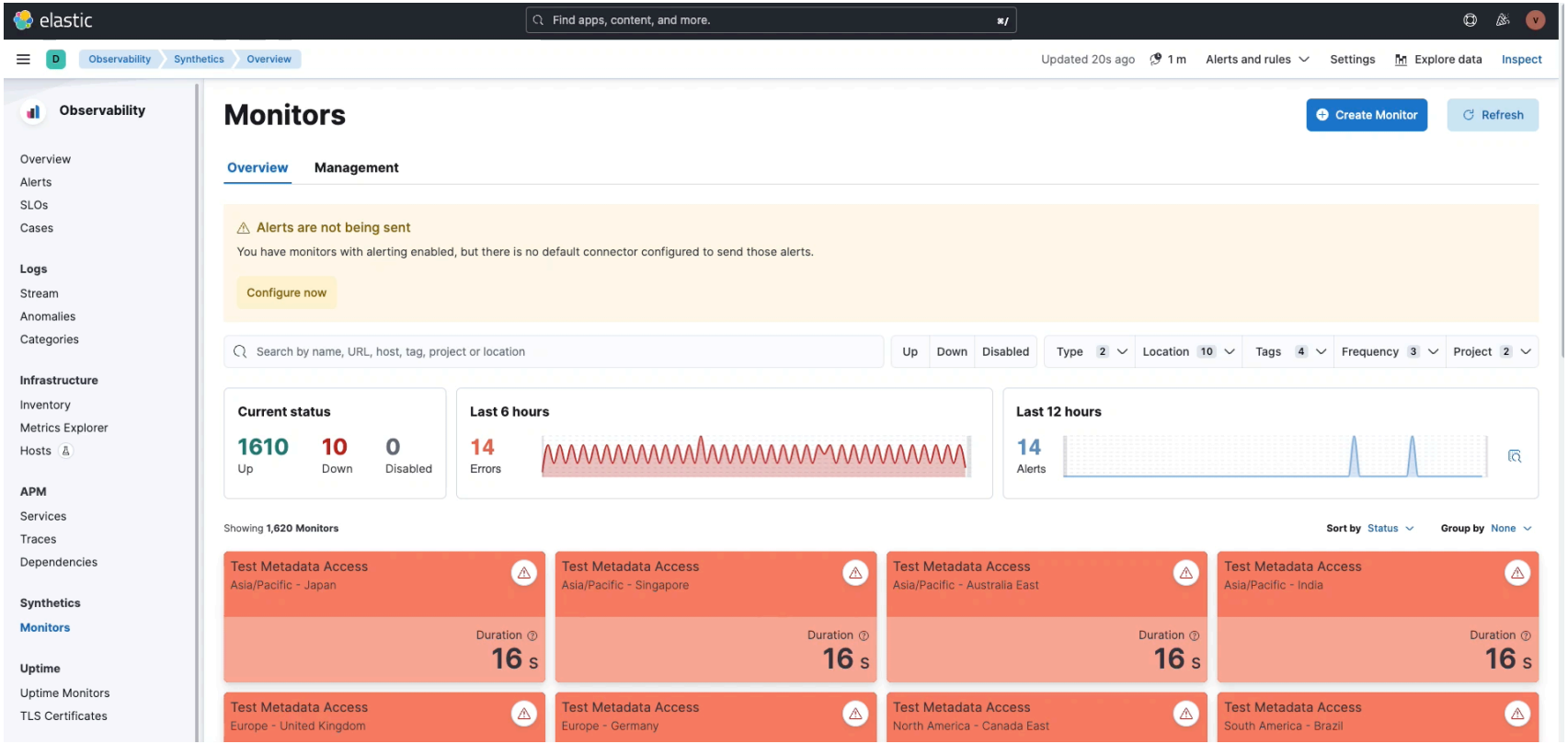
Setup guides | Add integrations | Try sample data | Upload a file



Management

Dev Tools | Stack Management

Manage permissions | Monitor the stack | Back up and restore | Manage index lifecycles


elastic
Find apps, content, and more.
Observability
Synthetics
Overview
Updated 20s ago
1 m
Alerts and rules
Settings
Explore data
Inspect
Observability
Overview
Alerts
SLOs
Cases
Logs
Stream
Anomalies
Categories
Infrastructure
Inventory
Metrics Explorer
Hosts
APM
Services
Traces
Dependencies
Synthetics
Monitors
Uptime
Uptime Monitors
TLS Certificates
Monitors
Create Monitor
Refresh
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
Asia/Pacific - Japan
Duration
16 s
Test Metadata Access
Asia/Pacific - Singapore
Duration
16 s
Test Metadata Access
Asia/Pacific - Australia East
Duration
16 s
Test Metadata Access
Asia/Pacific - India
Duration
16 s
Test Metadata Access
Europe - United Kingdom
Test Metadata Access
Europe - Germany
Test Metadata Access
North America - Canada East
Test Metadata Access
South America - Brazil

elastic

PagerDuty integration

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

Errored Actions

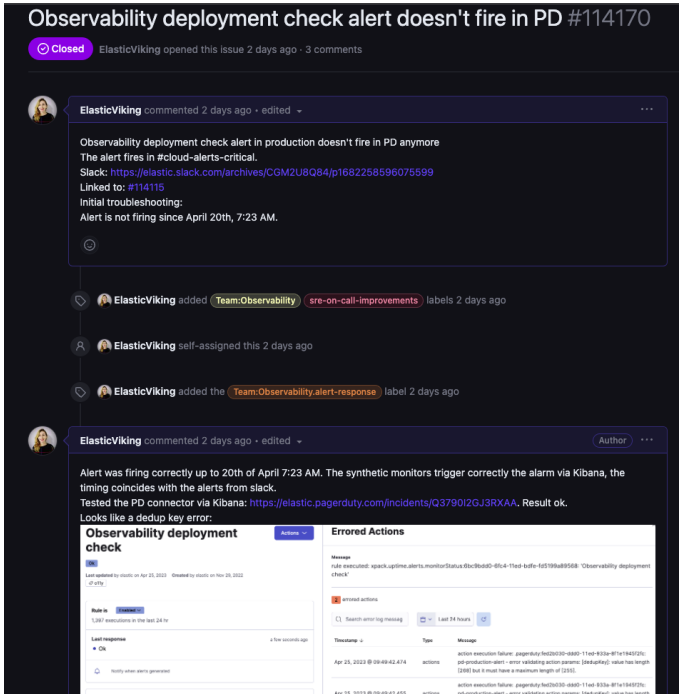
Message

rule executed: xpack.uptime.alerts.monitorStatus:6bc9bdd0-6fc4-11ed-bdfe-fd5199a89568: 'Observability deployment check'

2 errored actions

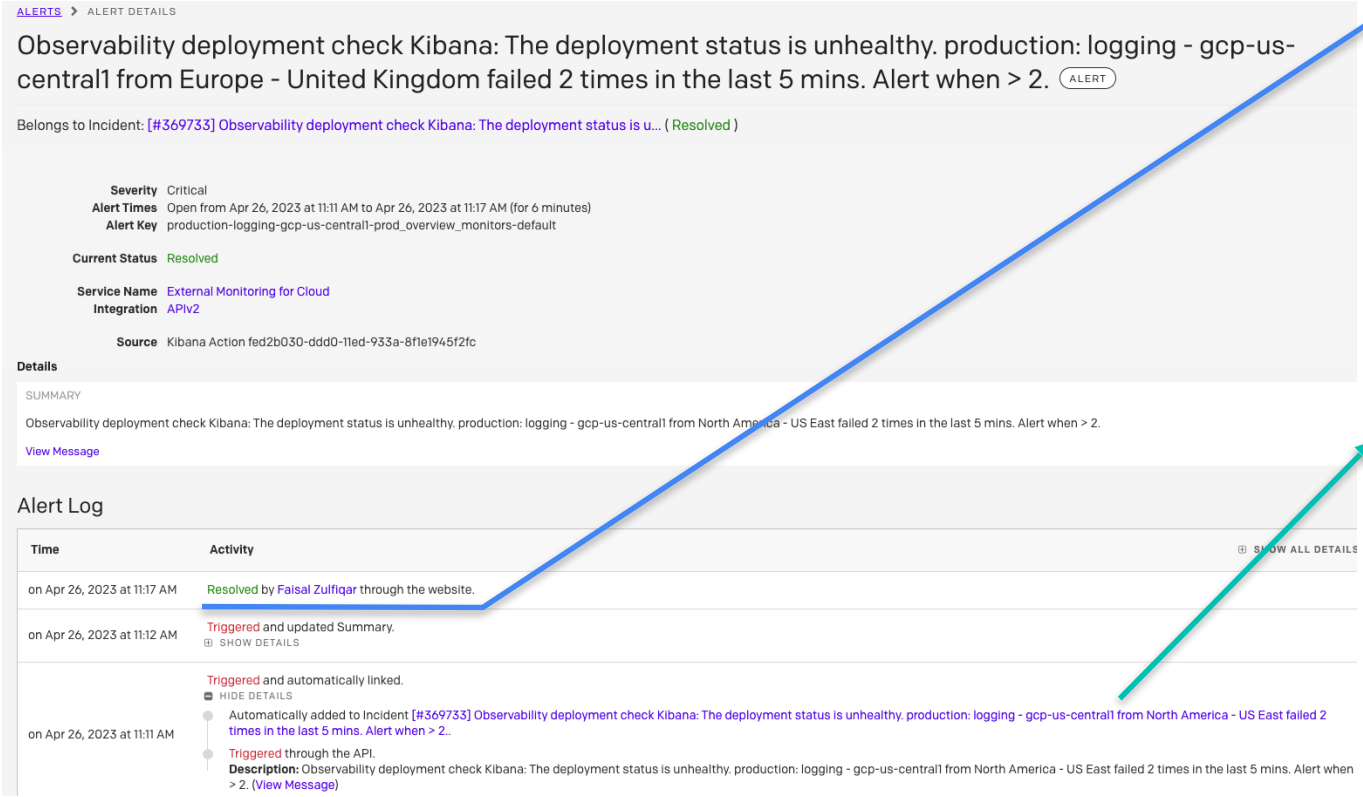
Search error log messag | Last 24 hours

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].



elastic

Grouped in PagerDuty but not resolved

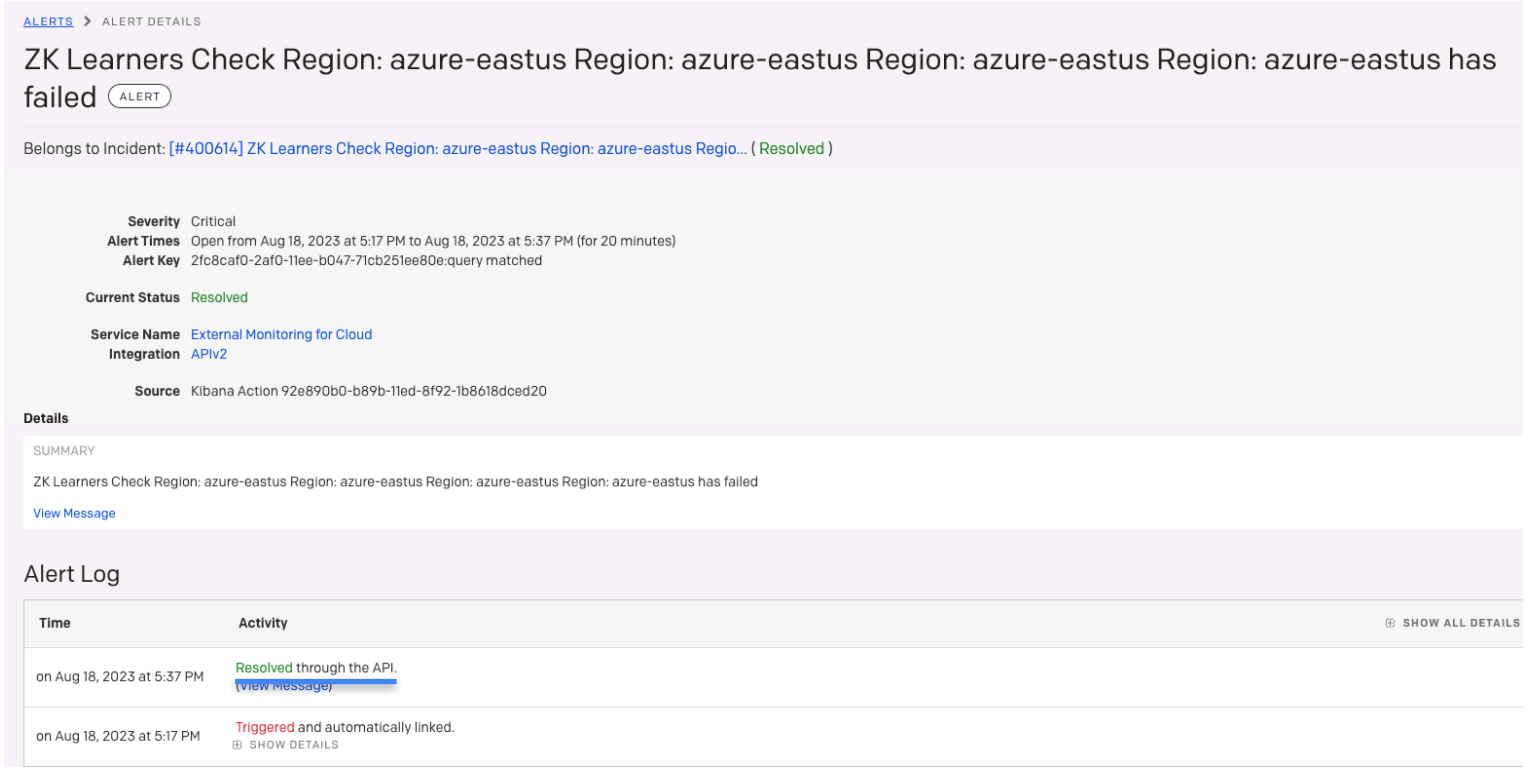


Manually resolved by the on-call SRE

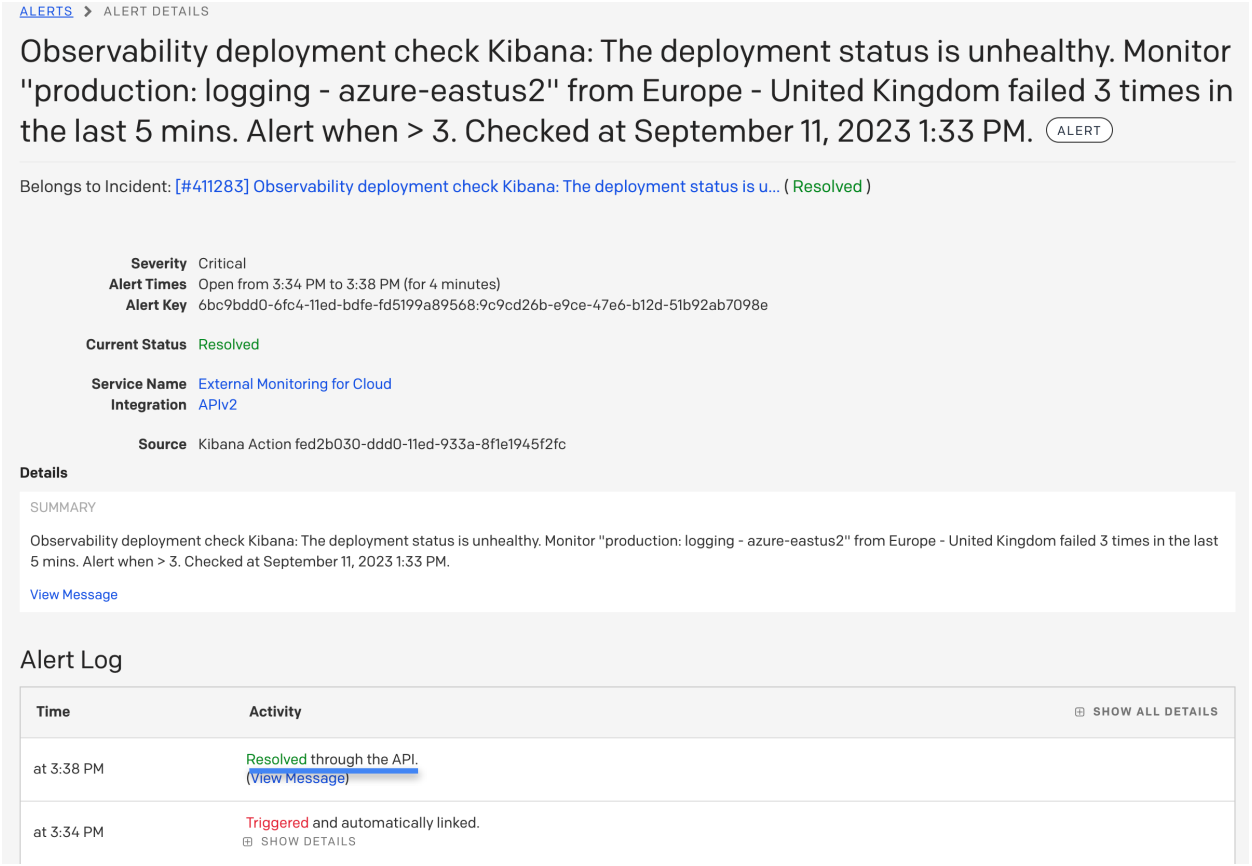
```
"dedupKey": "{{rule.id}}:{{alert.id}}"

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


elastic

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



Solution




```
"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.

elastic

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

elastic

Q&A