Google CONF42

Actionable alerts

Fix problems quickly

June, 2024

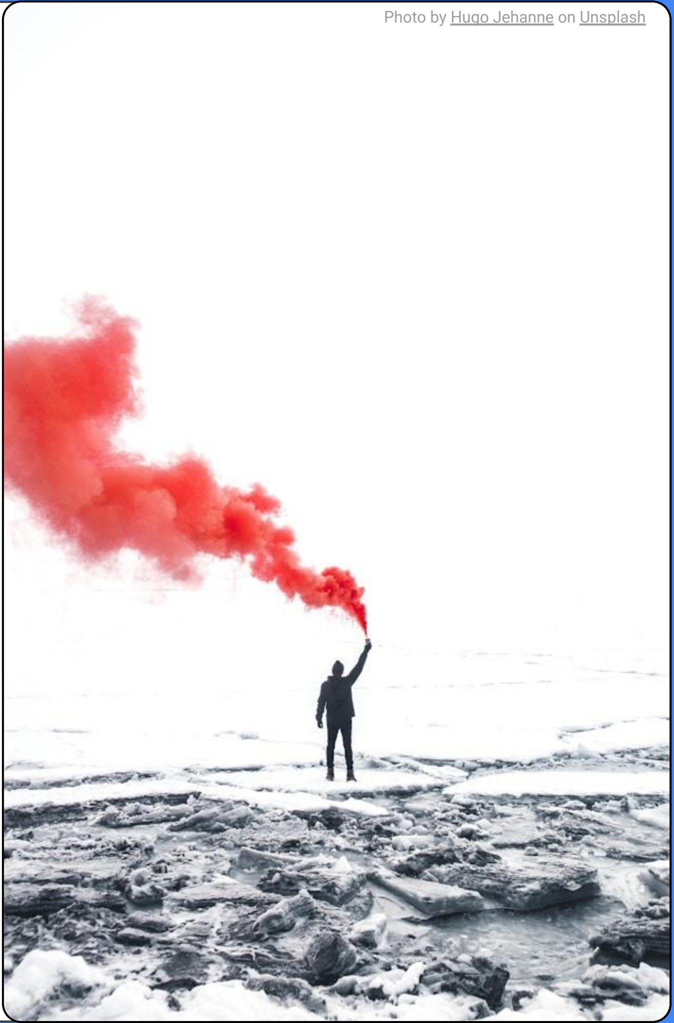


Photo by Hugo Jehanne on Unsplash

Nice to meet you

Leonid Yankulin
Senior Developer Relations Engineer
at Google Cloud

Over 5 years at Google Cloud. Started in Professional Services. For last 3 years work as DevRel Engineer in Cloud Advocacy with a focus on observability. Before Google I worked as DevOps architect for McKesson, developed healthcare software, interactive TV and gaming applications.

You can find me as **minherz** at in, and

Read my blog at https://leoy.blog

Agenda

- Efficient alerting
- Actionable alerting and automation
- Alert automation on Google Cloud (demo)

Praemonitus praemunitus

Forewarned is forearmed

Components of efficient alert

WHEN

Observe **relevant** metrics and conditions that affects system's purpose.

WHAT

Capture **relevant** information to ensure **outcome** of the alert response.

HOW

Notify response teams reliably to ensure timely alert processing.

WHEN to alert

WHEN

Observe **relevant** metrics and conditions that affects system's purpose.

WHAT

Capture **relevant** information to ensure **outcome** of the alert response.

HOW

Notify reliably to ensure **outcome** of the response.

WHAT to capture about alert

WHEN

Observe **relevant** metrics and conditions that affects system's purpose.

WHAT

Capture **relevant** information to ensure **outcome** of the alert response.

HOW

Notify reliably to ensure **outcome** of the response.

HOW to alert

WHEN

Observe **relevant** metrics and conditions that affects system's purpose.

WHAT

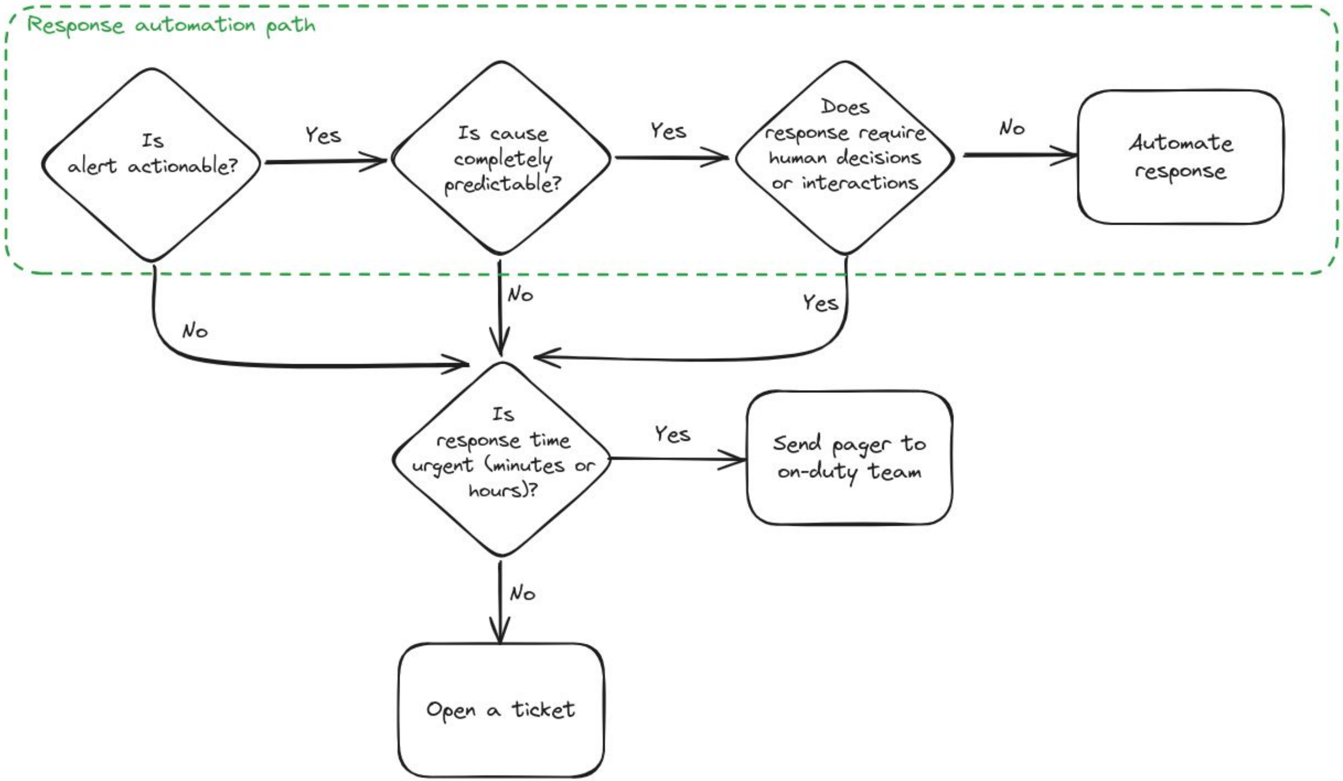
Capture **relevant** information to ensure **outcome** of the alert response.

HOW

Notify reliably to ensure **outcome** of the response.

Don't send an engineer to do a machine's job

Automate, Ticket, or Page?


Response automation path
Is alert actionable?
Yes
Is cause completely predictable?
Yes
Does response require human decisions or interactions
No
Automate response
No
No
Yes
Is response time urgent (minutes or hours)?
Yes
Send pager to on-duty team
No
Open a ticket

Components of automated alert

WHEN

Alert on individual resource(s) and not the service(s)
Use determinable cause
Approximate time windows

WHAT

Resource metadata
Service context
Detailed description of the alert conditions

HOW

System-to-system notification solutions such as API endpoint or async messaging solution
Adopt to automation data format (e.g. JSON)

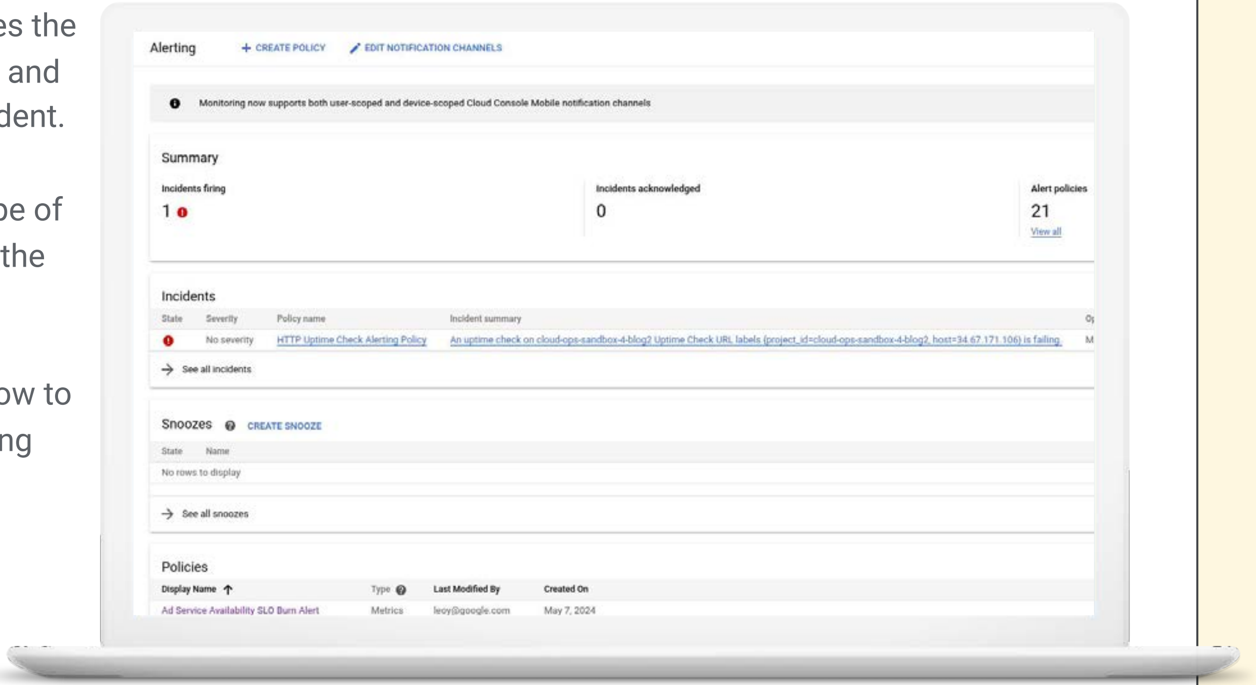
Demo time:
automate alert in Google Cloud

Cloud Monitoring Alerting

An alerting policy, which describes the circumstances under which to alert and the way to be notified about an incident.

Each incident is a record of the type of data that was monitored and when the conditions were met.

A notification channel defines how to receive notifications when Monitoring creates an incident.



Monitoring now supports both user-scoped and device-scoped Cloud Console Mobile notification channels

Summary

Incidents firing
1 ●

Incidents acknowledged
0

Alert policies
21
View all

Incidents

State	Severity	Policy name	Incident summary	Op
●	No severity	HTTP Uptime Check Alerting Policy	An uptime check on cloud-ops-sandbox-4-blog2 Uptime Check URL labels {project_id=cloud-ops-sandbox-4-blog2, host=34.67.171.106} is failing.	M

Snoozes

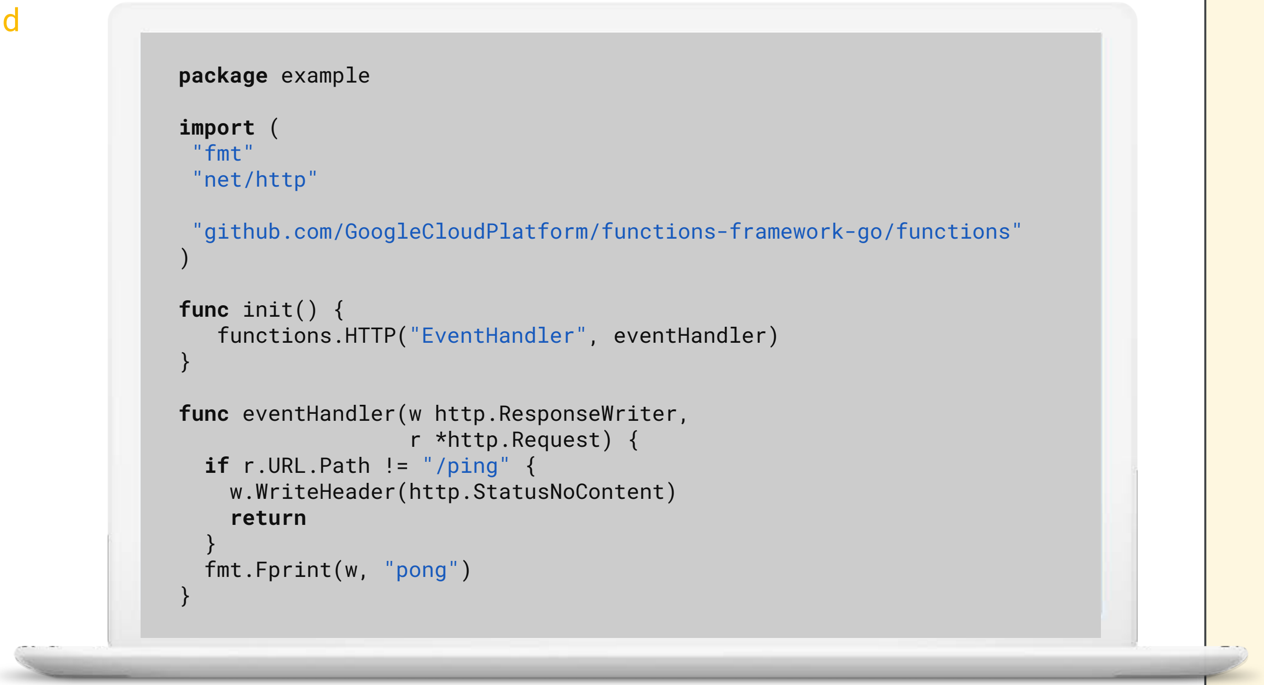
State	Name
No rows to display	

Policies

Display Name ↑	Type	Last Modified By	Created On
Ad Service Availability SLO Burn Alert	Metrics	leoy@google.com	May 7, 2024

Starting point: service and resource

A simple echo **endpoint** using Cloud Functions.

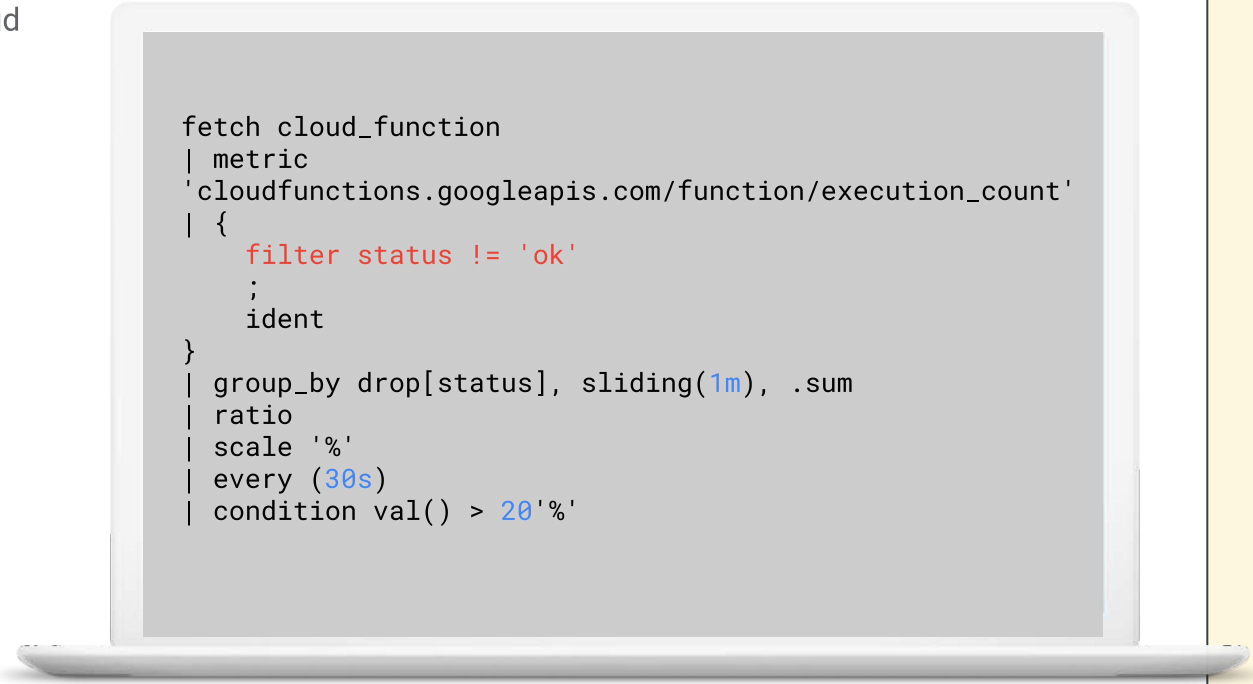


```
package example

import (
 "fmt"
 "net/http"

 "github.com/GoogleCloudPlatform/functions-framework-go/functions"
)

func init() {
   functions.HTTP("EventHandler", eventHandler)
}

func eventHandler(w http.ResponseWriter,
                  r *http.Request) {
  if r.URL.Path != "/ping" {
    w.WriteHeader(http.StatusNoContent)
    return
  }
  fmt.Fprint(w, "pong")
}
```

Starting point: WHEN

A simple echo endpoint using Cloud Functions.

Monitor **error rate** signal.



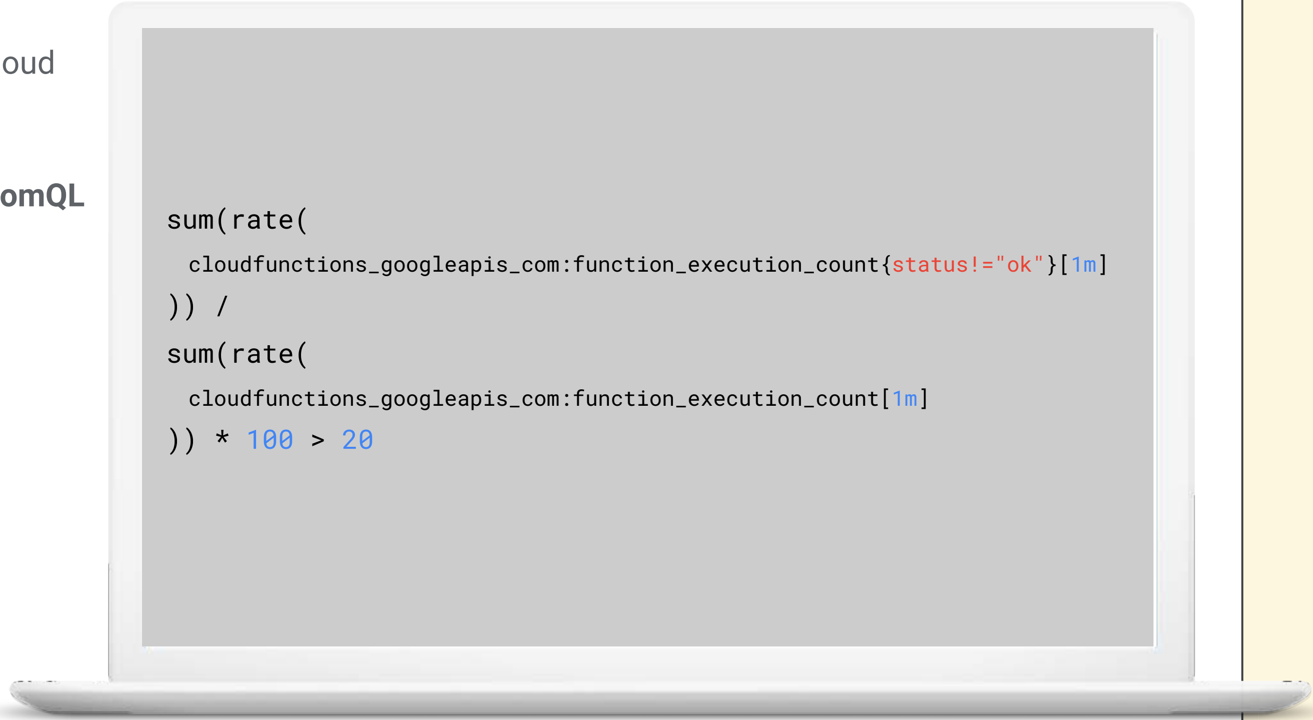
```
fetch cloud_function
| metric
'cloudfunctions.googleapis.com/function/execution_count'
| {
    filter status != 'ok'
    ;
    ident
}
| group_by drop[status], sliding(1m), .sum
| ratio
| scale '%'
| every (30s)
| condition val() > 20'%'
```

MQL reference: https://cloud.google.com/monitoring/mql/reference

Starting point: WHEN

A simple echo endpoint using Cloud Functions.

Monitor **error rate** signal with **PromQL**



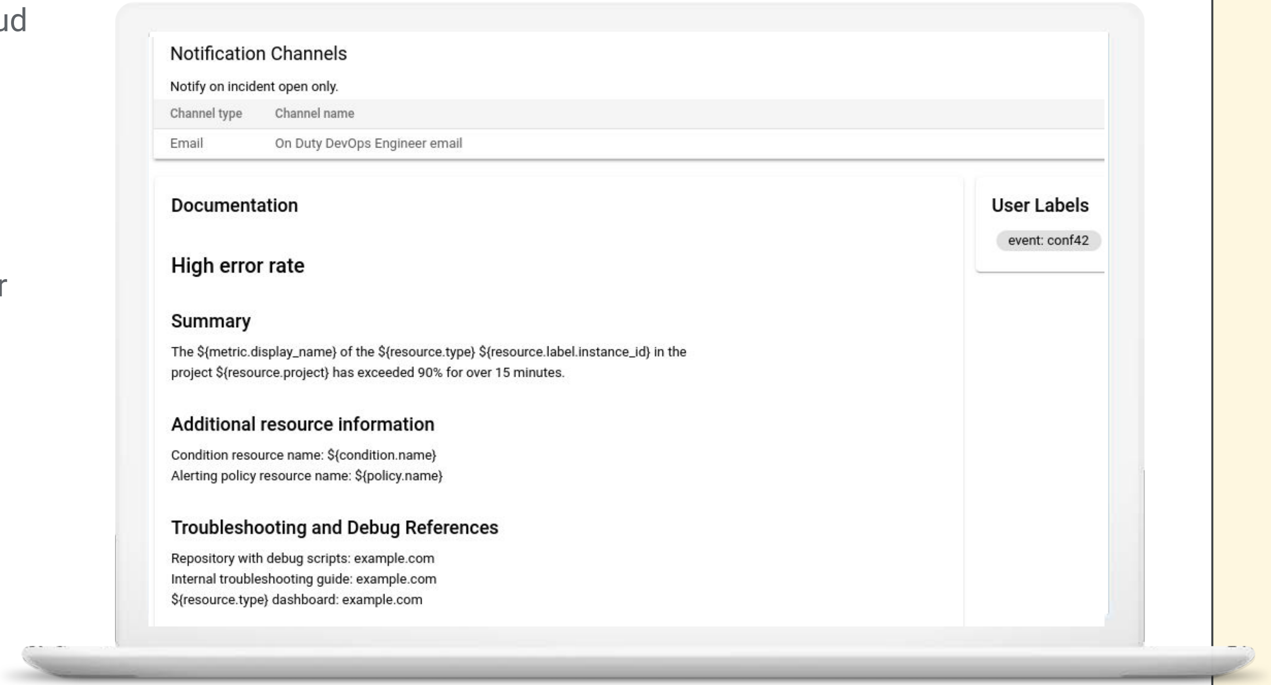
```
sum(rate(
  cloudfunctions_googleapis_com:function_execution_count{status!="ok"}[1m]
)) /
sum(rate(
  cloudfunctions_googleapis_com:function_execution_count[1m]
)) * 100 > 20
```

Starting point: WHAT and HOW

A simple echo **endpoint** using Cloud Functions.

Monitor **error rate** signal.

Capture **context**, human friendly **information** and **mail** it to engineer on-call.



Notification Channels

Notify on incident open only.

Channel type	Channel name
Email	On Duty DevOps Engineer email

Documentation

High error rate

Summary

The ${metric.display_name} of the ${resource.type} ${resource.label.instance_id} in the project ${resource.project} has exceeded 90% for over 15 minutes.

Additional resource information

Condition resource name: ${condition.name}
Alerting policy resource name: ${policy.name}

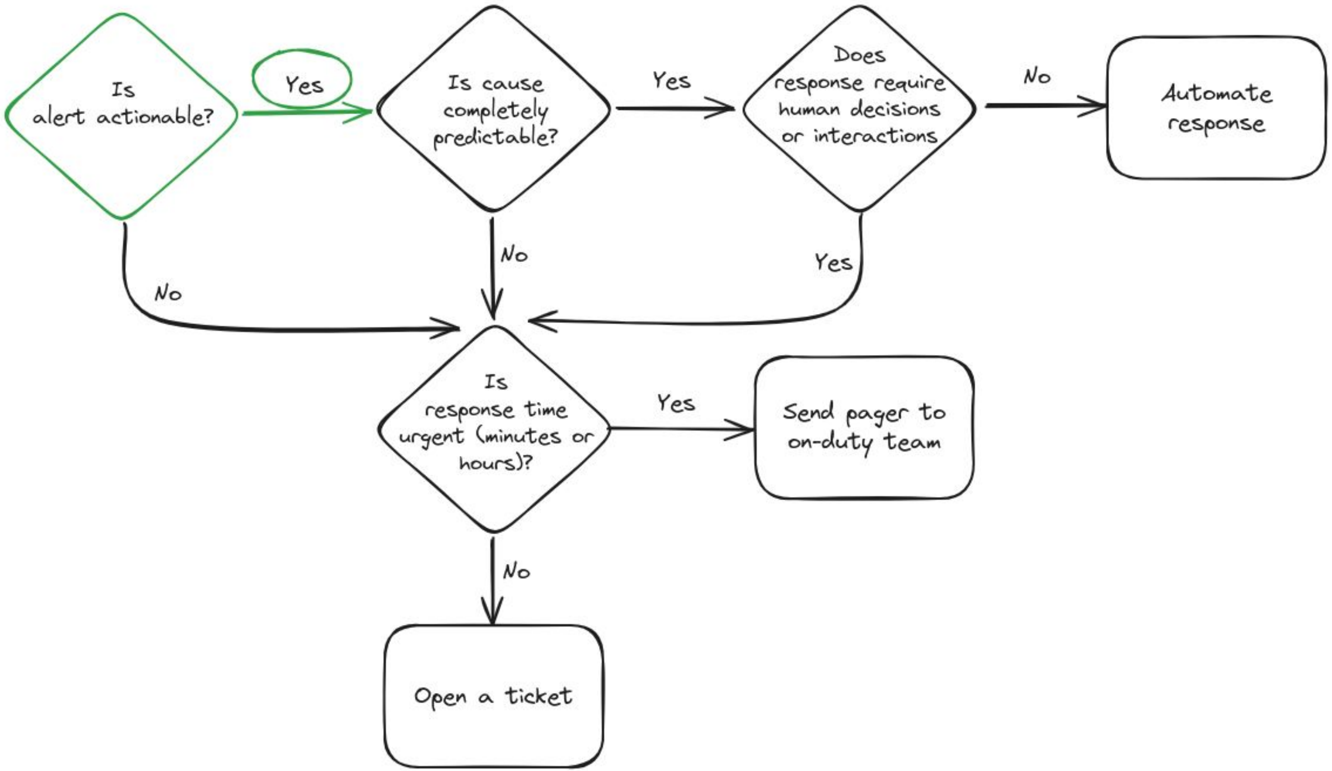
Troubleshooting and Debug References

Repository with debug scripts: example.com
Internal troubleshooting guide: example.com
${resource.type} dashboard: example.com

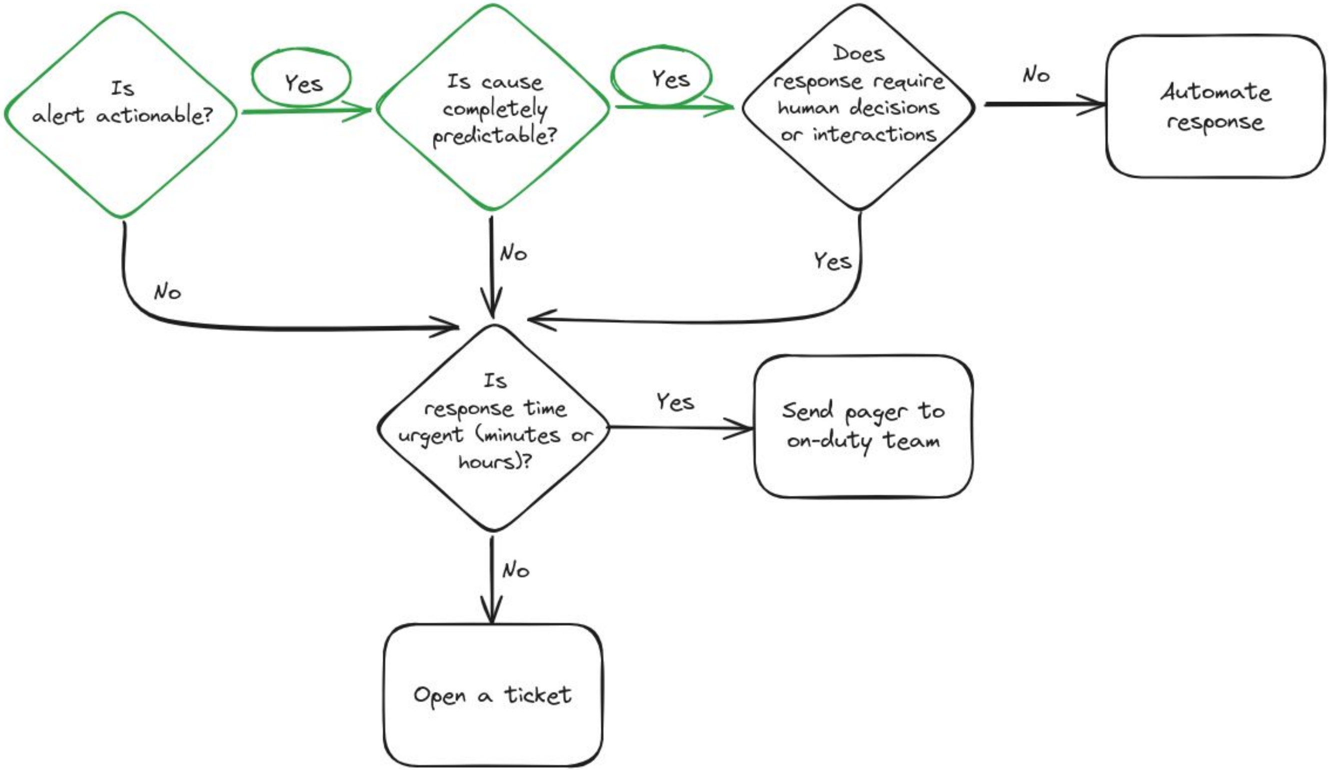
User Labels

event: conf42

Is alert actionable?

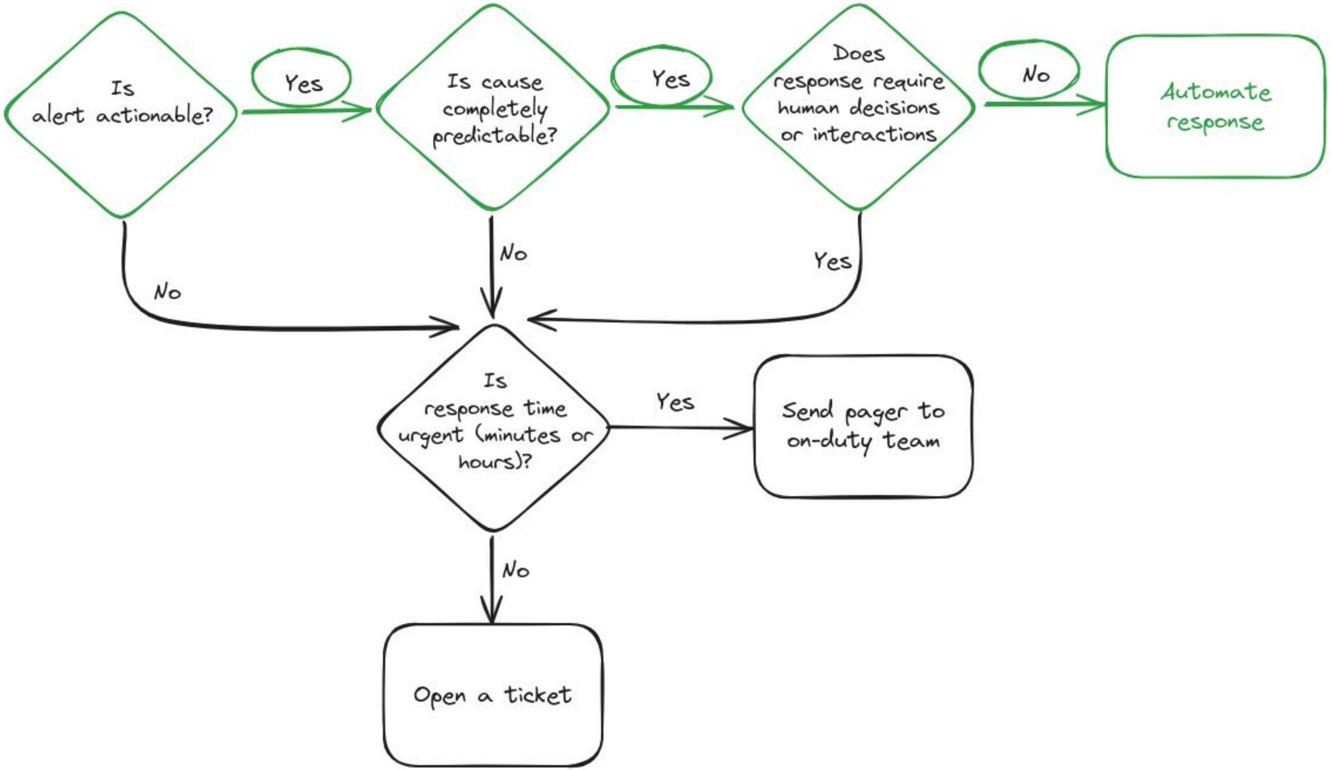

Is alert actionable?
Yes
No
Is cause completely predictable?
Yes
No
Does response require human decisions or interactions
No
Yes
Automate response
Is response time urgent (minutes or hours)?
Yes
No
Send pager to on-duty team
Open a ticket

Is cause deterministic?



Is alert actionable?
Yes
Is cause completely predictable?
Yes
Does response require human decisions or interactions
No
Automate response
No
No
Yes
Is response time urgent (minutes or hours)?
Yes
Send pager to on-duty team
No
Open a ticket

Does response require human intervention?


Is alert actionable?
Yes
Is cause completely predictable?
Yes
Does response require human decisions or interactions
No
Automate response
No
No
Yes
Is response time urgent (minutes or hours)?
Yes
Send pager to on-duty team
No
Open a ticket

Live demonstration on Google Cloud

Wrapping up

01 **Effective alerts vs. efficient alerts**
Not effective alerts = not working alerts; Make alerts efficient to decrease MTTR and MTTM

02 **Not all alerts can be automated but…**
Alerts can be automated. Automating actionable alerts increase efficiency further.

03 **Utilize service provider alerting capabilities**
Not every provider supports automation out-of-the-box. Use WHAT and HOW components to implement automation

Link to the post with source code bit.ly/automate-alerts

Thank You!

Share your feedback at bit.ly/feedback-to-leoy or scan QR code below