

SRE Assessment Template

Prometheus and Grafana Screenshots

```

[ec2-user@ip-172-31-92-158 ~]$ cat /etc/ssh/sshd_config
# Using username "ec2-user".
# Authentication with public key "EC2_key_pairs"
Last login: Mon Jan 16 13:05:29 2023 from dslb-188-101-022-141.188.101.pools.vod
afone-ip.de

[ec2-user@ip-172-31-92-158 ~]$ curl -s https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-92-158 ~]$ sudo systemctl status node_exporter
Unit node_exporter.service could not be found.
[ec2-user@ip-172-31-92-158 ~]$ sudo systemctl status node_exporter
node-exporter.service - Prometheus Node Exporter Service
Loaded: loaded (/etc/systemd/system/node-exporter.service; enabled; vendor preset: disabled)
Active: active (running) since Mon 2023-01-16 20:25:58 UTC; 39s ago
Main PID: 2950 (node_exporter)
CGroup: /system.slice/node-exporter.service
└─2950 /usr/local/bin/node_exporter

Jan 16 20:25:58 ip-172-31-92-158.ec2.internal node_exporter[2950]: level=info ts=2023-01-16T20:25:58.494Z caller=node_exporter.go:112 collector=thermal_zone
Jan 16 20:25:58 ip-172-31-92-158.ec2.internal node_exporter[2950]: level=info ts=2023-01-16T20:25:58.494Z caller=node_exporter.go:112 collector=time
Jan 16 20:25:58 ip-172-31-92-158.ec2.internal node_exporter[2950]: level=info ts=2023-01-16T20:25:58.494Z caller=node_exporter.go:112 collector=timex
Jan 16 20:25:58 ip-172-31-92-158.ec2.internal node_exporter[2950]: level=info ts=2023-01-16T20:25:58.494Z caller=node_exporter.go:112 collector=udp_queues
Jan 16 20:25:58 ip-172-31-92-158.ec2.internal node_exporter[2950]: level=info ts=2023-01-16T20:25:58.494Z caller=node_exporter.go:112 collector=uname
Jan 16 20:25:58 ip-172-31-92-158.ec2.internal node_exporter[2950]: level=info ts=2023-01-16T20:25:58.494Z caller=node_exporter.go:112 collector=vmstat
Jan 16 20:25:58 ip-172-31-92-158.ec2.internal node_exporter[2950]: level=info ts=2023-01-16T20:25:58.494Z caller=node_exporter.go:112 collector=xfs
Jan 16 20:25:58 ip-172-31-92-158.ec2.internal node_exporter[2950]: level=info ts=2023-01-16T20:25:58.494Z caller=node_exporter.go:112 collector=zfs
Jan 16 20:25:58 ip-172-31-92-158.ec2.internal node_exporter[2950]: level=info ts=2023-01-16T20:25:58.494Z caller=node_exporter.go:191 msg="Listening on" address=:9100
Jan 16 20:25:58 ip-172-31-92-158.ec2.internal node_exporter[2950]: level=info ts=2023-01-16T20:25:58.494Z caller=tls_config.go:170 msg="TLS is disabled and it cannot be enabled on the fly." http2=false
[ec2-user@ip-172-31-92-158 ~]$

```

Dashboard

node_memory_MemAvailable_bytes	
node_disk_io_now	
node_network_receive_bytes:rate:sum	

Responsibilities

1. The development team wants to release an emergency hotfix to production. Identify two roles of the SRE team who would be involved in this and why.

SRE team would have provided incident response as well as contribution to post-mortem analysis of the case that finally resulted into the emergency hotfix..

2. The development team is in the early stages of planning to build a new product. Identify two roles of the SRE team that should be invited to the meeting and why.

SRE team would contribute to all activities related to capacity planning of required resources and in developing strategies in Monitoring & Alerting of the future system.

3. The emergency hotfix from question 1 was applied and is causing major issues in production. Which SRE role would primarily be involved in mitigating these issues?

Again incident response since the hotfix causes major production issues to be tackled together with affected teams.

Team Formation and Workflow Identification

API Monitoring and Notifications

Display the status of an API endpoint: Provide a screenshot of the Grafana dashboard that will show at which point the API is unhealthy (non-200 HTTP code), and when it becomes healthy again (200 HTTP code).



Create a notification channel: Provide a screenshot of the Grafana notification which shows the summary of the issue and when it occurred.

The screenshot shows an email interface with MailHog on the left and a Grafana notification email in the center. The email is from 'Grafana' to 'example@email.com' with the subject '[FIRING:1] http200 webapps (http://52.202.41.59:5050 blackbox)'. The notification content includes the Grafana logo, the title 'Firing: 1 alert for alertname=http200 grafana_folder=webapps', a red 'Firing' status bar, the alert name 'http200', and details: 'Value: B=0, C=1' and 'Labels: alertname: http200, grafana_folder: webapps, instance: http://52.202.41.59:5050, job: blackbox'. There are buttons for 'Silence', 'Source', and 'Go to alerts page'. The footer indicates 'Sent by Grafana v9.3.2 © 2022 Grafana Labs'.

Configure alert rules: Provide a screenshot of the alert rules list in Grafana.

Alerting

Learn about problems in your systems moments after they occur

[Alert rules](#)
[Contact points](#)
[Notification policies](#)
[Silences](#)
[Alert groups](#)
[Admin](#)

Search by data source

All data sources

Search by label

Q Search

State

Firing Normal Pending

Rule type

Alert Recording

View as

Grouped List State

1 rule: 1 normal

+ New alert rule

Grafana

Alerts > webapps

1 rule | Edit

State	Name	Health	Summary	Actions
Normal	http200	ok		View Edit Delete

Silence

Show state history

Evaluate

Every 1m

Data source

Prometheus

For

5m

Matching instances

Search by label

Q Search

State

Normal 1 Alerting Pending NoData Error

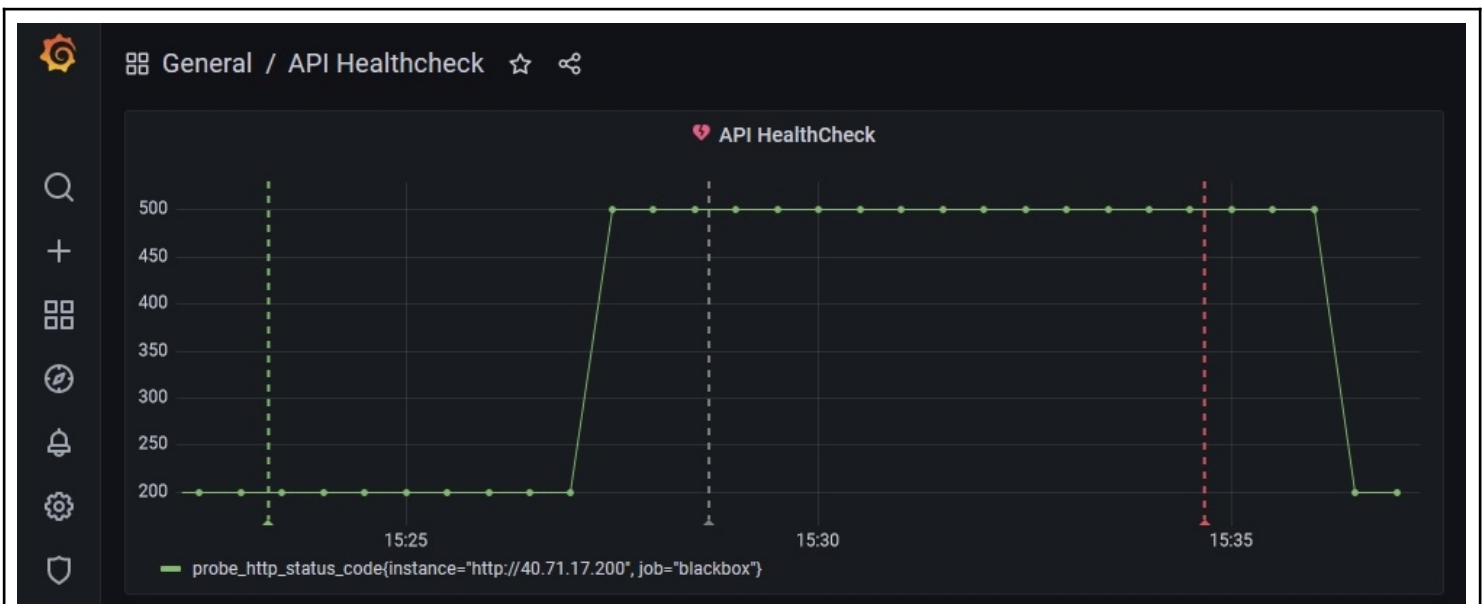
State	Labels	Created
Normal	<div>alertname=http200</div> <div>grafana_folder=Alerts</div> <div>instance=http://52.202.41.59:8080</div> <div>job=blackbox</div>	-

Mimir / Cortex / Loki

No rules found.

Applying the Concepts

Graph 1



4a. Given the above graph, where does it show that the API endpoint is down? Where on the graph does this show that the API is healthy again?

The service went down around 15:26 and was up again around 15:37.

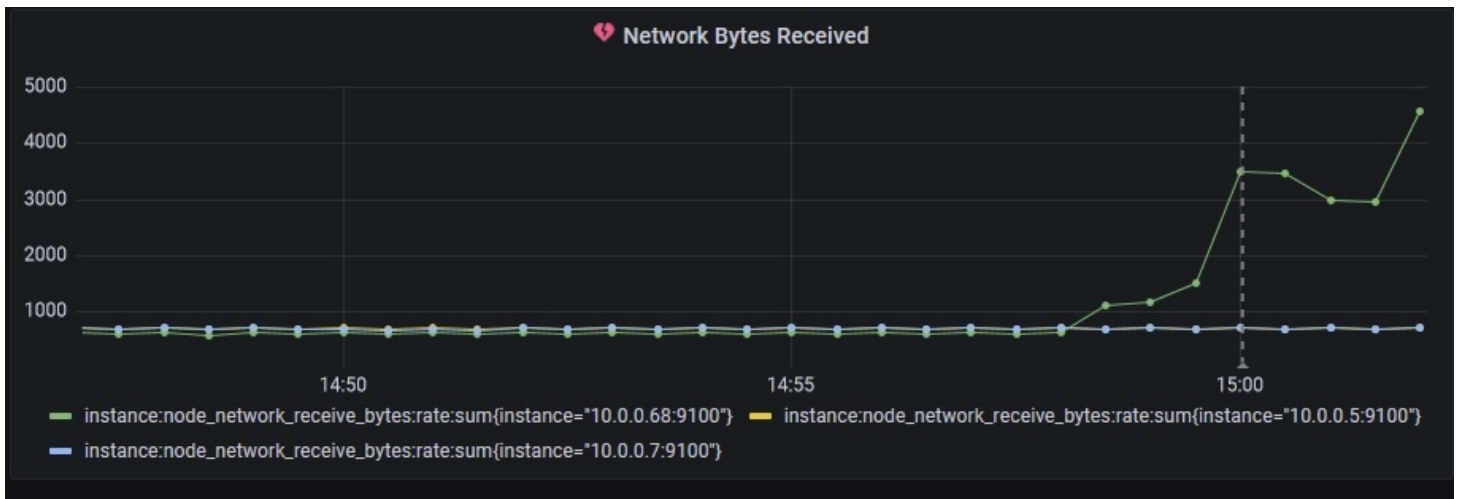
4b. If there was no SRE team, how would this outage affect customers?

Customers would have experienced a total service failure for around 11 minutes, since the server did not respond with 200 during that time.

4c. What could be put in place so that the SRE team could know of the outage before the customer does?

Setup blackbox exporter to test the endpoint continuously, then build grafana dashboards plus alerts on top.

Graph 2



5a. Given the above graph, which instance had the increase in traffic, and approximately how many bytes did it receive (feel free to round)?

10.0.0.68 showed increased traffic higher than 3kb.

5b. Which team members on the SRE team would be interested in this graph and why?

- SRE Monitoring Engineer, because he/she is responsible for the monitoring
- SRE Infrastructure Engineer, because he/she is responsible for the system infrastructure including network components
- optionally the SRE System Architect, since he/she might have a broader view with additional inputs