



derDACK
:: SIGNAL 4

ZABBIX '25

CONFERENCE

GERMANY

Mastering 24x7 IT Operations:
Smart Alerting &
Incident Response

Ronald Czachara

May 2025

Now that Zabbix got all the monitoring done...
How to get from issue detection to resolution?

Motivation

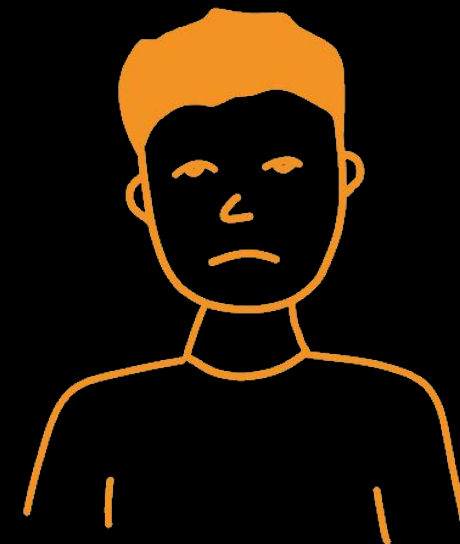
I already get SMS messages ...

- When email and SMS are not enough
- Real-life stories
- Best practices for 24x7 alerting
- Spark own ideas

???

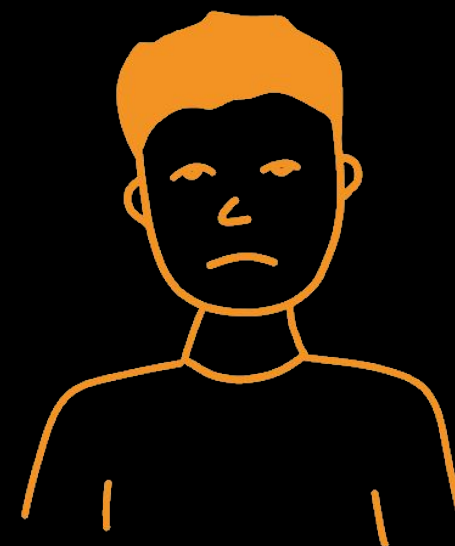
The Story of the On-Call Engineer

- IT Engineers, 24x7 on-call duty
 - Planning in Excel / print out
 - Phone hand over (configure forwarding)
 - Alerting via email and SMS text (modem)
 - Sometimes false or unimportant alerts
-
- Alert at night ...



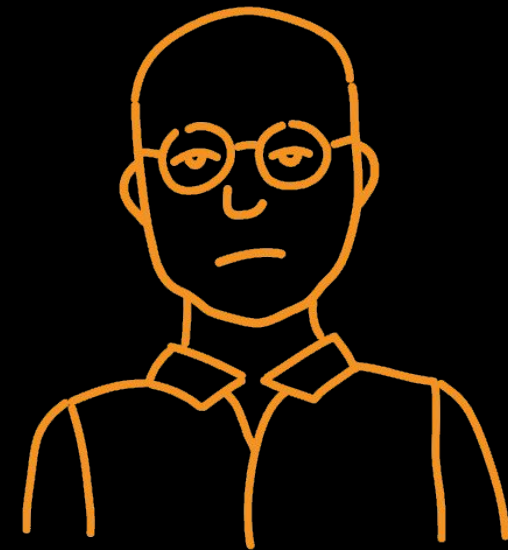
The Story of the On-Call Engineer

- Not the right contact ...



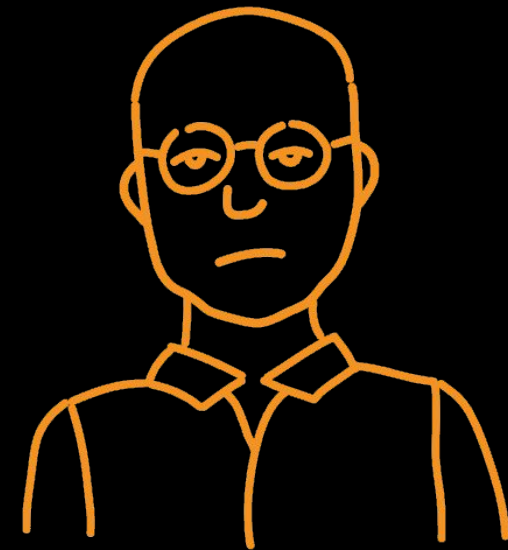
The Escalation

- Calls another engineer



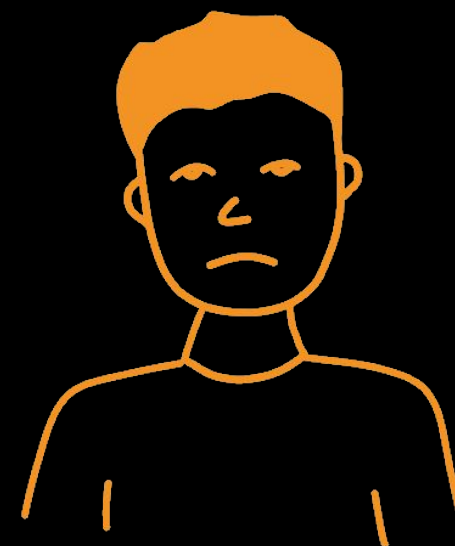
The Resolution

- Workaround implemented
- Back to sleep



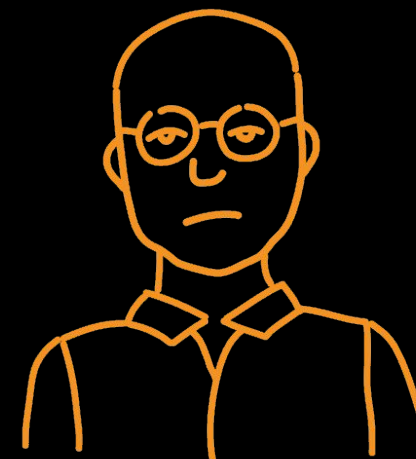
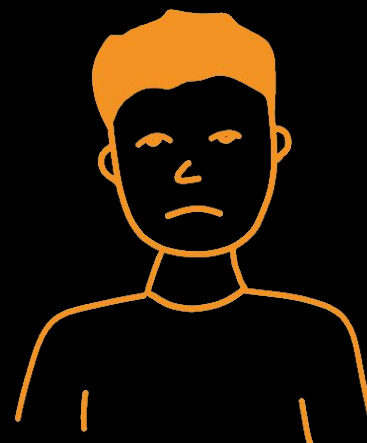
The Status

- Hm, the issue still seems to be there



No Sleep

- Call again
- No sleep for the rest of the night



Alert Fatigue – Causes

- Too many alerts
- False alerts
- Poor prioritization
- Duplicates
- Poor information



Alert Fatigue – Impact

- Missed alerts
- Late responses
- Decreased performance
- Higher operational costs
- Frustration
- Quitting
- Shocking statistics, e.g. 62% of SOC alerts ignored *
- Lose – Lose – Lose



* <https://smallbiztechnology.com/archive/2024/10/survey-shows-62-of-soc-alerts-ignored.html/>

Solution?

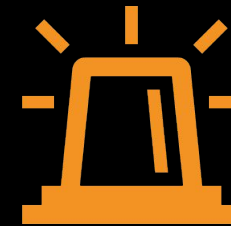


On-Call Scheduling and Responsibilities

- On-call calendar with dynamic alert routing
- Right information to the right people – clear responsibilities



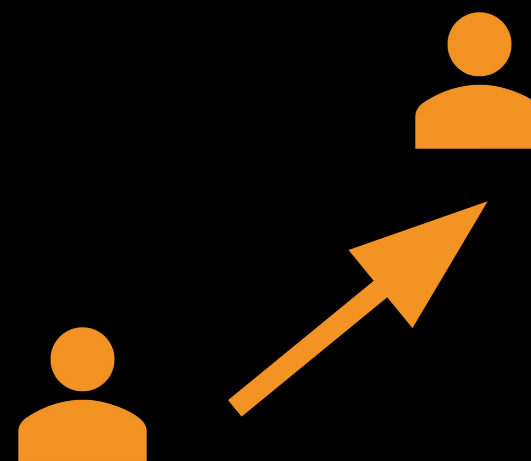
Better Notifications



- Multiple communication channels
- What is needed to resolve an issue
- Priority / severity: Wake up or let sleep
- E.g. soft / loud / vibrate (e.g. fitness band), DnD override
- Enrichment, e.g. color, icon, location, links to docs, kb, tickets, Zabbix portal (or app)
- Automation, no-code runbooks

Escalations

- Automatic escalations
- Manual escalations
- Who is on-call in other teams

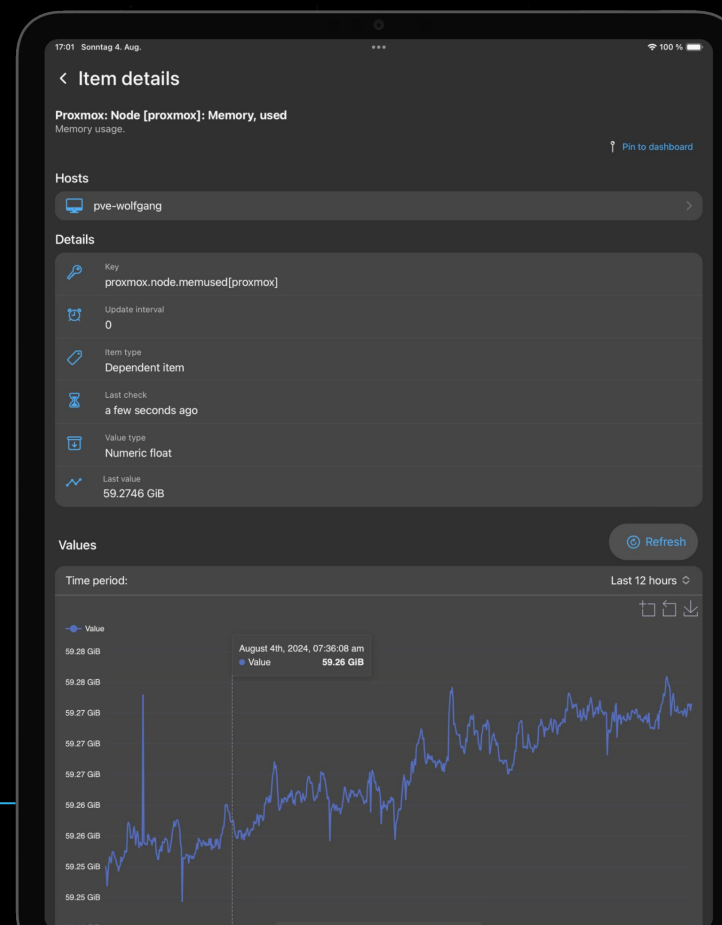
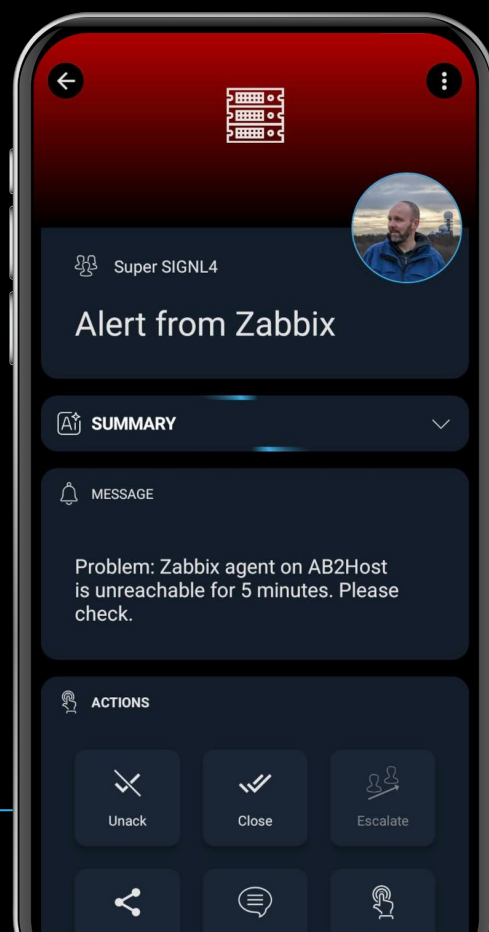


Collaboration and Two-Way Integration

- Ack, close, annotate, collaborate
- Two-way integration – transparency
- Make it convenient to get help (at night), e.g. mobile app



SIGNAL4 and IntelliTrend



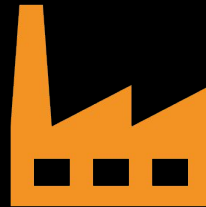
Bonus

- No SMS modem needed – heartbeats will do 🤔



Another story ...

- It is never too late ...
- until it is.



Happy Monitoring, Happy Alerting

Win – Win – Win



Happy Company, Happy On-Call Engineers



Questions? Comments?

LinkedIn: Ronald Czachara

