

Automated NOC:
Zabbix as Code with
AI-Enriched Alerts

9.10.2026

axians



We are part of the Vinci Group

36

COUNTRIES

16.000

EXPERTS



Axians celebrates with Zabbix

axians

ZABBIX

PREMIUM DELIVERY
PARTNER

ZABBIX

TRAINING PARTNER

Axians Slovakia

10 years Premium Partner



Who am I?



Ing. Michal Owczarzy

AOC Architect & Pre-Sales, Axians

- Architect of AOC, our automated NOC platform
- Former Network Tools Technical Lead — ran the Riverbed monitoring stack for a global healthcare enterprise
- I also work with our sales team, turning the platform into something a customer can understand and buy

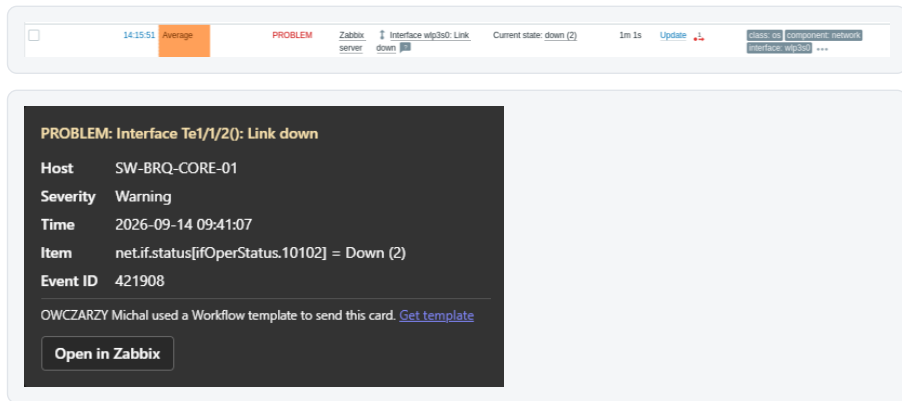


Zabbix Certified Specialist

Have you ever imagined that the moment a problem message arrives, you would already know why it happened and how to fix it?

The alert we all get

WHAT ARRIVES



The screenshot shows a Zabbix alert notification card. At the top, there's a status bar with a checkbox, a timestamp '14:15:51', an 'Average' label, a 'PROBLEM' status, the item name 'Interface wlp3s0: Link down', the current state 'Current state: down (2)', the time '1m 1s', an 'Update' button, and a dropdown menu showing 'class: go component: network interface: wlp3s0 ***'. Below this, the main content area has a dark background with the following text: **PROBLEM: Interface Te1/1/20: Link down**, Host: SW-BRQ-CORE-01, Severity: Warning, Time: 2026-09-14 09:41:07, Item: net.if.status[ifOperStatus.10102] = Down (2), Event ID: 421908. At the bottom, there's a note: 'OWCZARZY Michal used a Workflow template to send this card. [Get template](#)' and an 'Open in Zabbix' button.

WHAT IT DOES NOT SAY

- ? What actually happened
- ? Who touched it
- ? Whether anything is down
- ? Why it happened
- ? How to fix it

Zabbix knows what changed. Not why.

Everything after this line is a person, opening other tools.

The ideal ticket

What if the perfect ticket looked like this?

WHAT	Not a fault. The port was shut by hand at 09:41:03 — four seconds before Zabbix alerted.
WHO	A named engineer over SSH — confirmed twice, by Wazuh and by ServiceNow , independently.
IMPACT	Brno is up on one link. Redundancy is gone . Zero users affected right now.
WHY	A change was approved for today — but it names a different port .
FIX	One command, no outage — with the estimate marked as an estimate.

Same event. Same second. No other tool opened.

● SW-BRQ-CORE-01 Te1/1/2 shut down by michal.owczarzy at 09:41:03 — wrong port, Brno is up but has no spare link to the DC

Create subtask Link work item Create Checklist Clockwork Pro Response Templates

Key details

NOC-JSM-Access raised this request via API
[View request in portal](#)

Description • Unsaved changes

✗ SW-BRQ-CORE-01 Te1/1/2 — shut by hand, wrong port

What	Not a fault. Te1/1/2 was administratively shut at 09:41:03 , four seconds before Zabbix alerted.
Who	Michal Owczarzy (michal.owczarzy), SSH from 10.10.42.17 — named by Wazuh and by ServiceNow , independently
Impact	Brno is UP on one link. Redundancy is GONE . 0 users affected right now.
Why	Change CHG0041471 was approved and scheduled for today — but it names Te1/1/4 . Te1/1/2 is not in it.
Fix	no shutdown on Te1/1/2 — below, about 30 seconds, no outage

✓ **FIX IT — one command, no risk**

Bring Te1/1/2 back up. It rejoins Po1 automatically via **LACP**; no reconvergence, nothing drops.

```
1 interface TenGigabitEthernet1/1/2
2 no shutdown
3 end
4 write memory
5 I confirm it is back in the bundle:
6 show etherchannel 1 summary
```

Leave Te1/1/4 shut — that one was the intended change and it is correct.

...About 30 seconds is an **AOC** estimate derived from the command set and typical LACP bundling time — a model output, not a measured value...

● Why it matters — Brno is online, but it has no spare link

Those are two different things, and only the second one changed. Po1 is one logical link built from two physical ones. Te1/1/2 is now shut, so Po1 runs on Te1/1/1 alone; traffic moved across instantly and **no service is degraded**.

What is gone is the spare. **There is nothing left to fail over to**, so the next optic, fibre or

Why this ticket is different



Everything is already in it

Zabbix, Wazuh, ServiceNow and the switch config, joined into one story.



Root cause on the first screen

You read why it happened before you decide whether to open anything.



It says what is still fine

The site is up. What is gone is the spare and that is the real risk.



The fix is a command

Ready to paste or to hand over, with the risk stated next to it.



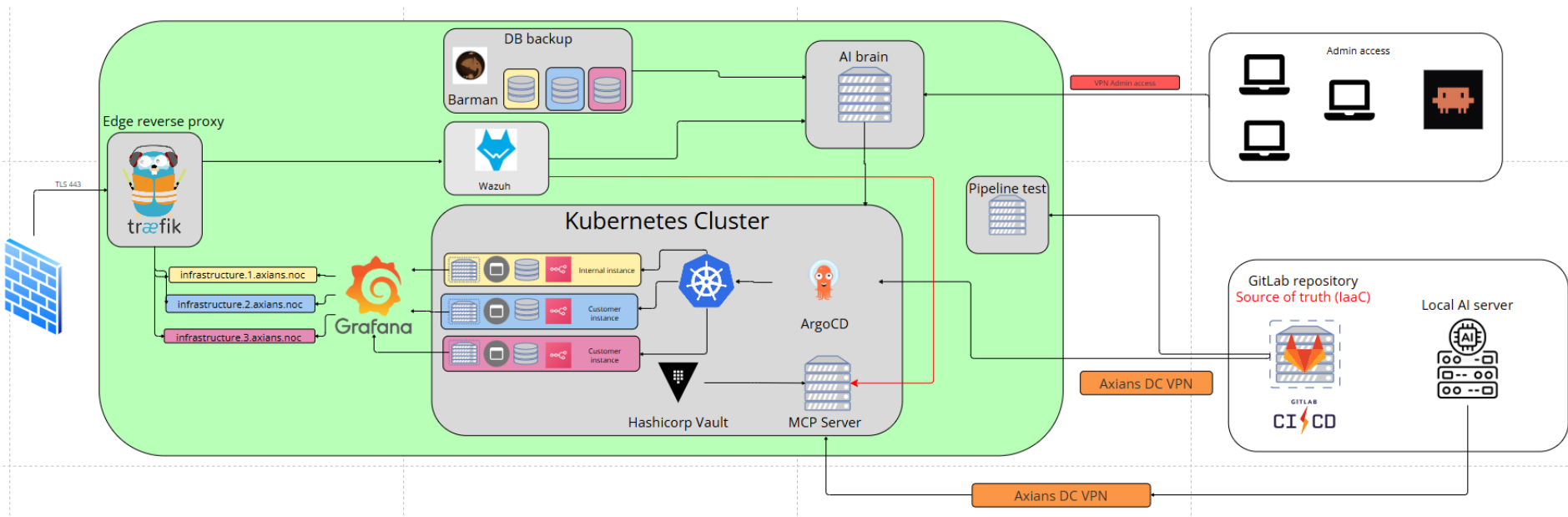
It marks its own guesses

An estimate is labelled an estimate. Facts and predictions never blur.



It learns from the shift

The engineer's fix goes back to GitLab — next time it is a known solution.



Every tool running as a code

One **namespace per tenant** -
n8n, Zabbix and its own
database

GitLab CI and ArgoCD are the
only way anything gets in

Wazuh for logs, an **MCP server**
integrations and for the AI layer

From event to ticket

01

A problem fires in Zabbix

02

Zabbix sends the event to n8n

03

n8n decides whether it is worth analyzing

04

Data is collected from the other tools

05

Correlation: cause or symptom?

06

The problem is identified

07

GitLab is checked for a known solution

08

A solution is proposed — rules first, AI only if needed

09

The output goes to GitLab, ITSM and Teams

10

The engineer's solution flows back into GitLab

The model is asked at step 8, and only when no known solution matches.

Demo time



Questions

Ask me the hard ones — what it costs, what it gets wrong, and what happens when the model is unavailable.

Thank you

Michał Owczarzy · AOC Architect & Pre-Sales,
Axians · michal.owczarzy@axians.com