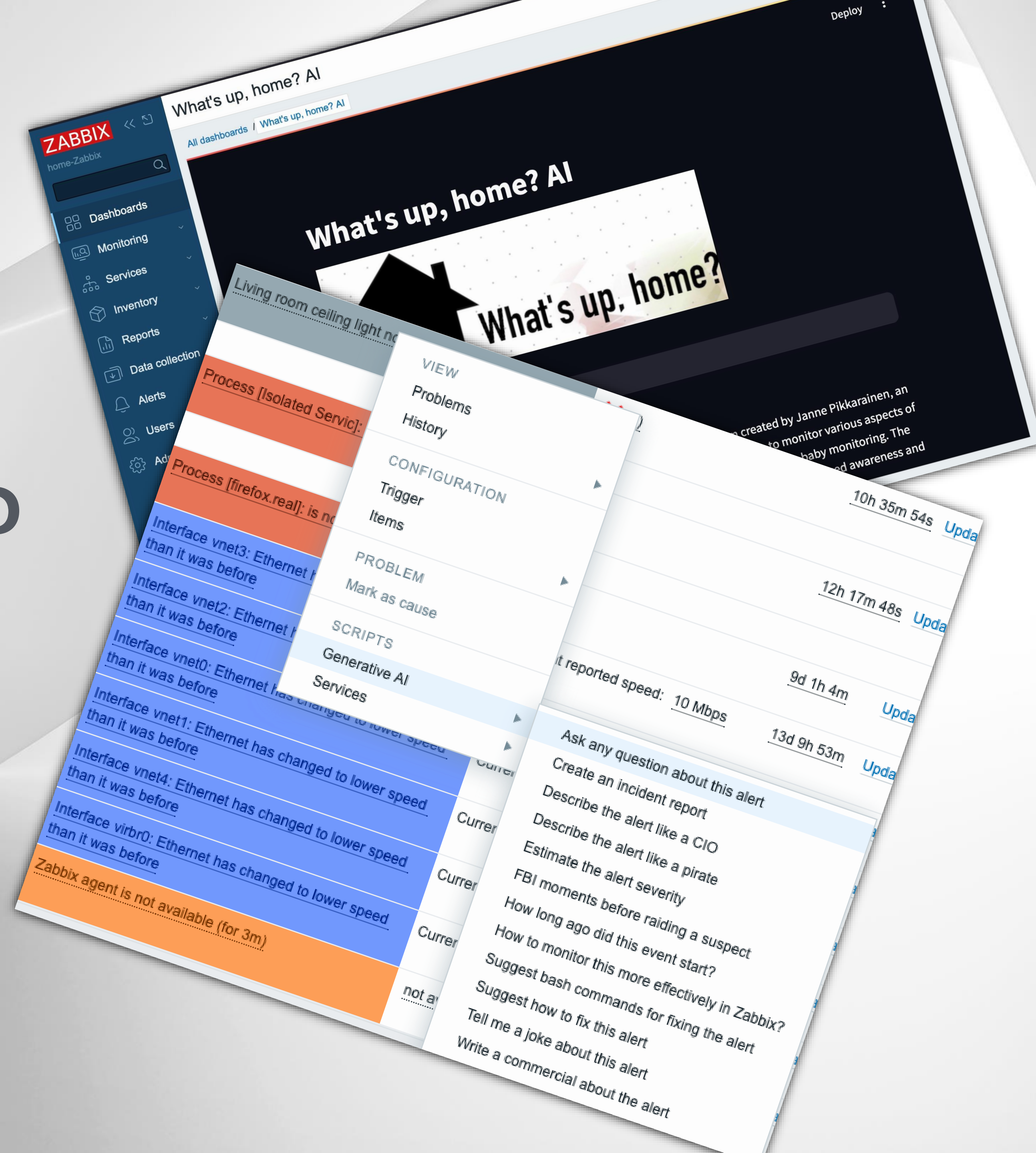


What's up, home?

Goes **Generative AI**



Who am I?

- Janne Pikkarainen from Finland FI
- Sitting in front of computers since 1986
- Doing IT for living for 25+ years now, out of that monitoring since 2001
- 10+ years at Forcepoint, currently as Lead Site Reliability Engineer
- Walking, talking Zabbix commercial



LIFE & SOCIETY FINNISHNESS

FOR SEVENTH YEAR RUNNING, FINLAND IS FIRST IN WORLD HAPPINESS REPORT – OTHER NORDICS IN TOP 7

Since 2018, the UN World Happiness Report has found that Finland is the happiest country in the world. How does happiness happen?

About Forcepoint

- Provides **cyber security** for the biggest **enterprises** you can imagine of, **hospitals**, **critical infrastructure** and so forth
- NGFW, SD-WAN, Web/e-mail protection, VPN, ZTNA, RBI, DLP, CASB, many other acronyms and products
- **Global footprint** with employees & customers spread all over the world

Forcepoint PARTNERS SERVICES & SUPPORT COMPANY ENGLISH

Why Forcepoint Data Security Everywhere Data-first SASE Resources [Talk to an Expert →](#)

Data Security That Knows No Bounds.

Forcepoint GenAI Security safely enables AI Transformation.

[See What's New →](#)

Data Security. Everywhere.

Unify Policy Enforcement and Reduce Risk Across the Enterprise.

[Find Out More →](#)

Safeguard Data in Cloud Apps, Web, Email, Network and Endpoint.

[Learn How →](#)

Discover and Secure Unstructured Data with AI.

[Read More →](#)

Forcepoint Named a Leader in Forrester Wave: SSE, Q1 2024.

[Learn Why →](#)

Quick recap of my blog

- Been doing my blog since **March 2022**
- I **monitor my home** with Zabbix
- In addition to home, I monitor and **do just about anything** with Zabbix
- During 2023, started to **integrate Zabbix with a locally run LLM, GPT4AI**
- See <https://whatsuphome.fi/>



I monitor **everything** with Zabbix

More info at <https://whatsuphome.fi/>

AdGuard Home

Air conditioner

Air humidifier

Airport departures/arrivals

Air quality index (outdoors)

Apple Watch

Baby sleep

Baby stroller temperature

BackupPC

“Banana” color

Car location

CCTV camera

CO2 levels (indoors)

Cozify

Countdown timer

Docker

Dog in bed?

Door sensors

Elasticsearch

Electricity price

Electricity consumption

Facial cream usage

FlightGear

HAProxy

HashiCorp Vault

Headset

Home router

HP LaserJet

Jenkins

Laptop webcam

Lights

Logs

Lunch menus

Maritime traffic

Mobile data usage

Motion sensors

MySQL

Northern Lights

Philips OneBlade

Power sockets

PostgreSQL

Product prices

Raspberry Pi 4

Roomba

RSS feeds

Selenium

Smoke/fire alarm

Sonos smart speaker

Thermometers

TV

Weather

whatsuphome.fi website

whatsuphome.fi visitors

Zabbix Security Advisories

Today's agenda

What is **GPT4All**?

Integrate GPT4All with Zabbix **context menus**

Let **GPT4All write its own blog** based on active Zabbix alerts

Embed your Zabbix data with GPT4All

Give Zabbix a personality through GPT4All

What is GPT4All?

- GPT4All is an **open-source project** to provide a **Generative AI** for almost any hardware
- Supports **1000+** different **language models**
- **Locally run**, no need for account or Internet, so **your data is safe**
- Has a GUI client, but also **Python/Node/other bindings**
- Through Python, very easy to **integrate with Zabbix**



Hello world in GPT4All

.. and Python

```
from gpt4all import GPT4All
```

```
model = GPT4All("orca-mini-3b-  
gguf2-q4_0.gguf")
```

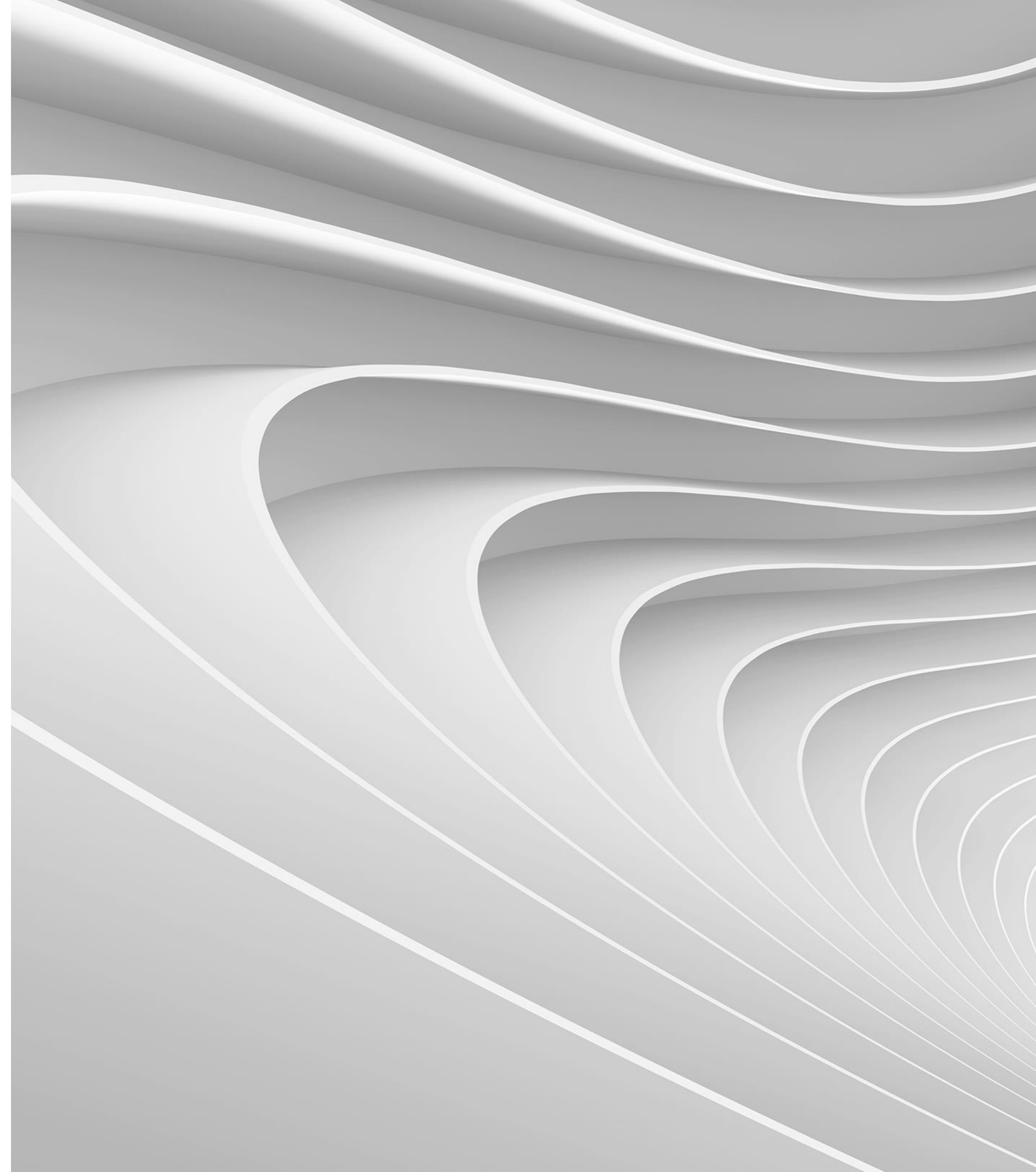
```
output = model.generate("Say hello  
to Zabbix Summit", max_tokens=3)
```

```
print(output)
```

- MacBook Pro M2 Pro 2023, 16 GB RAM, 512 GB SSD
 - Using it for configuring everything
 - Using it for writing my blog posts
 - Using it for AI experiments
 - Takes care of backups to iCloud
- Dell Latitude E7450, Intel i7, 16 GB RAM, 256 GB SSD
 - My old work laptop re-imaged for this project

GPT4All + Zabbix context menus

Let AI to help you inside Zabbix



Enrich your alerts dashboard

The screenshot shows a monitoring dashboard with several alerts. A context menu is open over the 'Zabbix agent is not available (for 3m)' alert. The menu options are:

- VIEW
- Problems
- History
- CONFIGURATION
- Trigger
- Items
- PROBLEM
- Mark as cause
- SCRIPTS
- Generative AI
- Services

The 'Generative AI' option is selected, showing a list of actions:

- Ask any question about this alert
- Create an incident report
- Describe the alert like a CIO
- Describe the alert like a pirate
- Estimate the alert severity
- FBI moments before raiding a suspect
- How long ago did this event start?
- How to monitor this more effectively in Zabbix
- Suggest bash commands for fixing the alert
- Suggest how to fix this alert
- Tell me a joke about this alert
- Write a commercial about the alert

Describe the alert like a CIO

Script execution successful.

Output

```
1. Subject: Urgent - Living Room Ceiling Light Outage Alert
2. Dear Valued Users,
3. We are writing to inform you that we have encountered an unexpected
   issue with the living room ceiling light in our facility. As a result,
   this service is currently unavailable for use.
4. Our technical team has been immediately notified and is working
   diligently to resolve the situation as quickly as possible. We apologize
```

Ok

Suggest bash commands for fixing the alert

Script execution successful.

Output

```
1. Check if the Zabbix agent service is running by using the following
   command:
   ``bash
   sudo systemctl status zabbix-agent
   ``
   If it's not running, you can start it with this command:
   ``bash
```

Ok

How to do that?

Through Zabbix Scripts!

```
from gpt4all import GPT4All

import argparse

parser = argparse.ArgumentParser(description='Pass question to GPT4All')

parser.add_argument('-q', '--question')

args=parser.parse_args()

model = GPT4All('wizardlm-13b-v1.2.Q4_0.gguf')

system_template = 'A chat between a curious user and an artificial intelligence assistant.'

prompt_template = 'USER: {0}\nASSISTANT: '

with model.chat_session(system_template, prompt_template):

    response1 = model.generate(args.question)

    print(response1)
```

Script

Name	Suggest how to fix this alert					
Scope	Action operation	Manual host action	Manual event action			
Menu path	Generative AI/					
Type	URL	Webhook	Script	SSH	Telnet	IPMI
Execute on	Zabbix agent	Zabbix server (proxy)	Zabbix server			
Commands	ssh jpikkarainen@192.168.50.80 "cd /Users/jpikkarainen/Projects/HuggingFace;/opt/homebrew/bin/python3 ./zabbix_response_generator.py --question 'Tell me about this Zabbix alert. The alert is {EVENT.NAME}'"					

Pros and cons

- Very **easy** to **implement** and **extend**
- **Integrates** with Zabbix **menus** nicely
- ... but the **output** dialog is **tiny**
- ... **no** back and forth **chat**
- ... **does not** support the **interactive** ways of Zabbix 7.0's inter-widget communication framework



Time to **blog!**
Automatically, that is

Search

[My account](#) [Log out](#)

What's up, home?

Generative AI edition
All the stories generated by GPT4All

[HOME](#) [BACK TO MAIN WHAT'S UP, HOME?](#)

What am I reading?

All the blog posts here are generated by a locally run LLM, [GPT4All](#). The stories are based on current active alerts on my [What's up, home?](#) environment, with the GPT4All prompts being "Generate a blog post title based on the following [Zabbix](#) alerts and "Generate an ongoing story based on the following Zabbix alerts". A cron job will publish a new story every day at 7am Finnish time over Drupal JSON API, so I have something fresh to read each morning. Now, let's get to it, the content created by the little AI starts below.

"Monitoring Mayhem: Uncovering the Chaos in Your Home and Network" - a title that captures the essence of your ongoing Zabbix alerts. Would you like me to help you prioritize or investigate any specific issues?

[View](#) [Edit](#) [Outline](#) [Delete](#) [Revisions](#)

Published by [ZabGPT](#) - Thu, 09/12/2024 - 07:00

Good morning, everyone at Zabbix Summit conference! I'm excited to share with you the analysis of these interesting alerts from various sources.

Firstly, let's look at some infrastructure-related issues. We have a Jenkins job that's unhealthy on IP address `192.168.50.80`. This might be causing delays or failures in automated builds and deployments. Additionally, we're seeing containerd service restarts with an uptime of less than 10 minutes, which could indicate instability or configuration issues.

Moving on to home automation-related alerts, we have a hallway motion sensor that's not available, indicating potential connectivity problems or hardware malfunctions. The Home Assistant system is also experiencing some issues: it's been unresponsive for over two hours and the average noise level has exceeded 60 dB, which might be causing discomfort or disturbance.

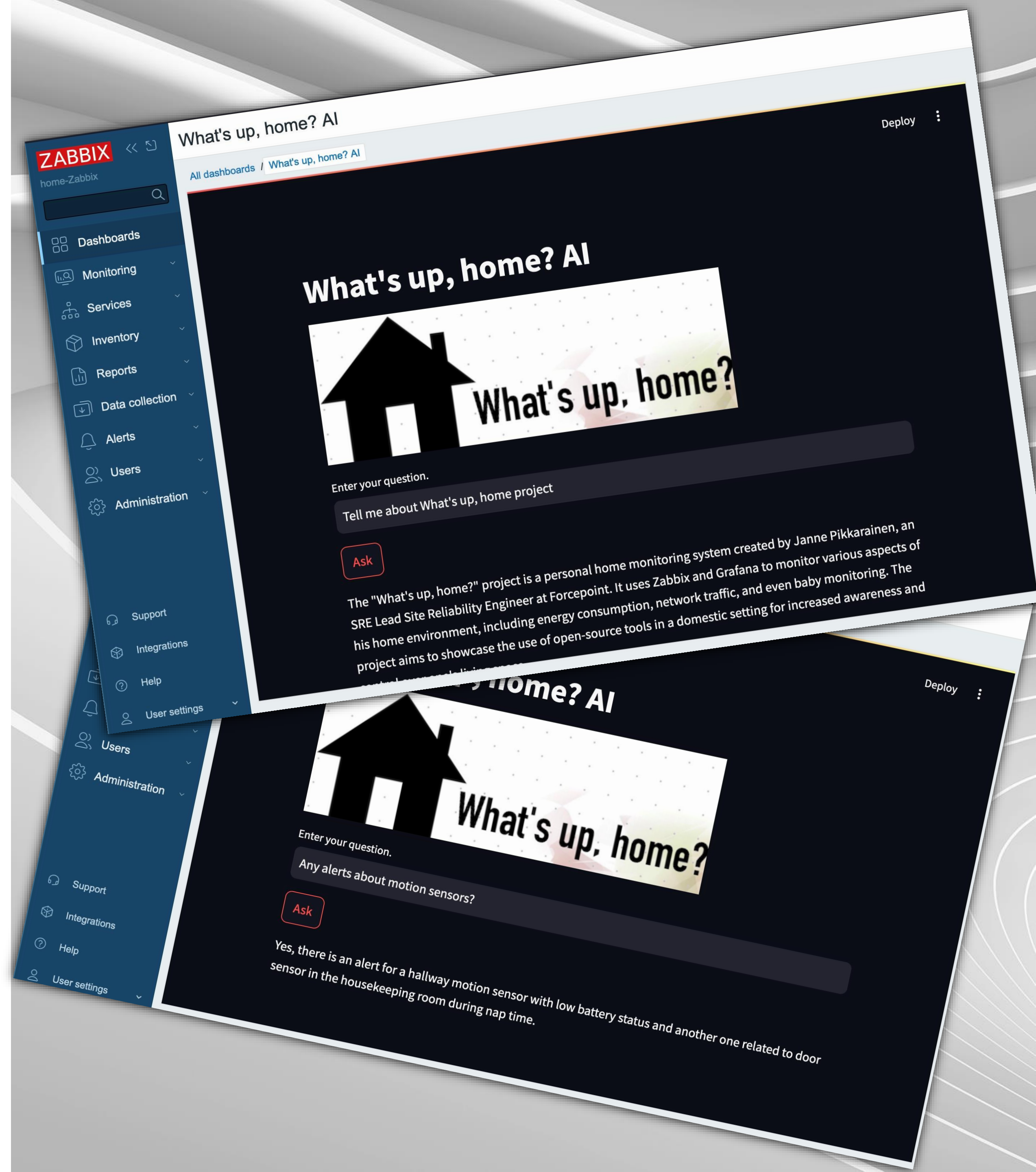
 What's up, home?

My blog flow

- <https://generativeai.whatsuphome.fi/> is 100% produced by GPT4All
- Python script asks Zabbix about the active alerts, and GPT4All writes a blog post about them
- Published to Drupal every morning 7am via Drupal API



Embed your Zabbix data with GPT4AI



Embedding data

- **General idea:** with GPT4All, it's easy to include custom data from **local directories** or **remote locations**
- GPT4All and Python **langchain** makes it easy
- **Feed it** Zabbix inventory, hosts, alerts, services, SLAs, playbooks, wiki...
- Create **your own web UI** with for example **Streamlit** and **embed** it with Zabbix **URL widget** or create a **custom Zabbix widget**



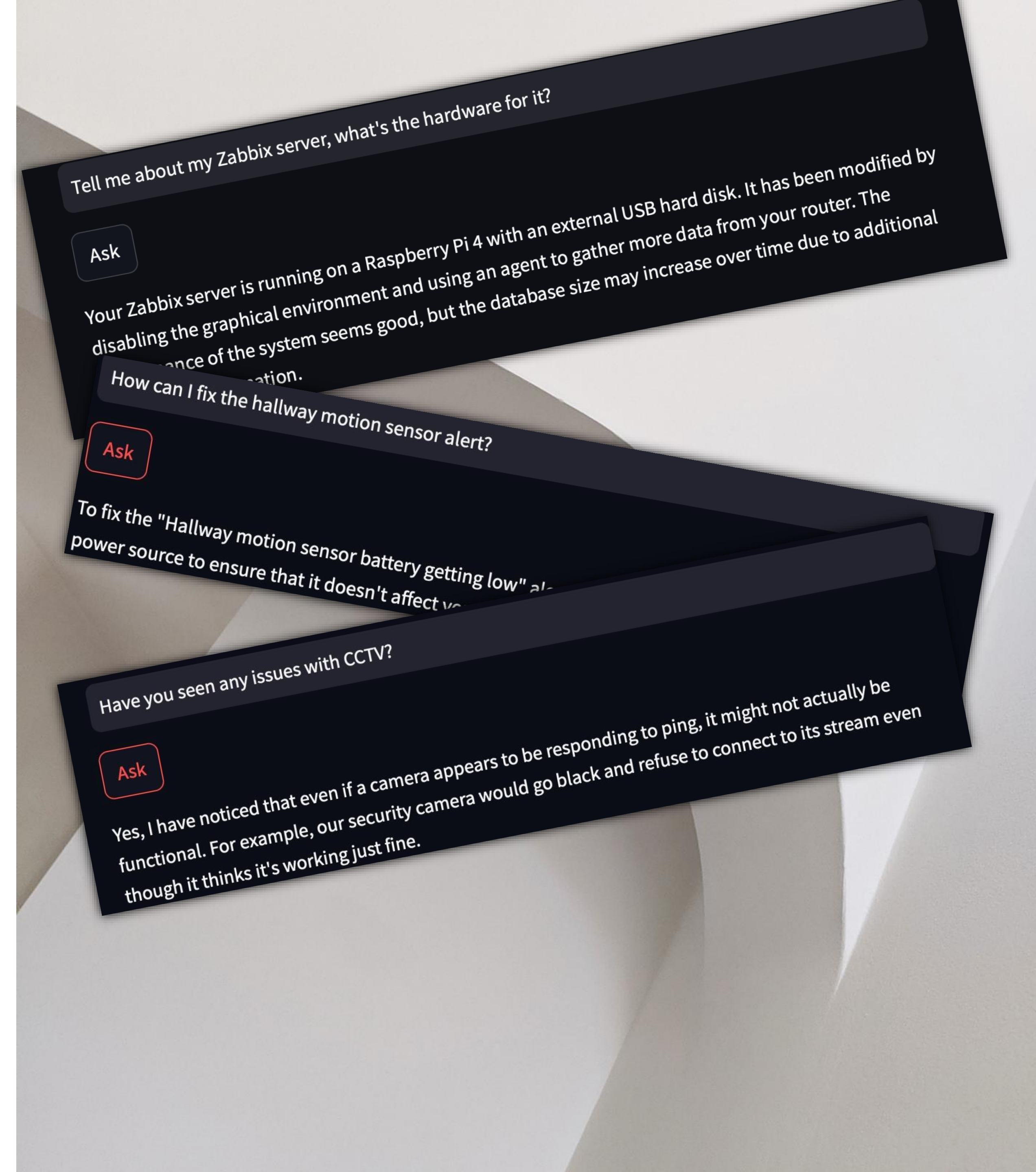
Additional data

- Zabbix **user manual**, other manuals you need
- In my case, my **blog entries**
- **CVEs**, Zabbix **release notes**
- **News/change log** etc about the **software you care** about
- This **helps GPT4All** to make its **responses** even better



Does it **work**?

- **Good** for **general questions** about your hosts
- **Good** for telling if it **has seen any issues** with particular **host** or **service** if you feed it the past problems
- **Bad** with **exact timelines** or **other time-related data**
- **BEWARE!** As usual with GPTs, it can **hallucinate**



Give Zabbix a personality through
GPT4AI



Give Zabbix a **personality**

- Simple yet effective: define the personality through global Zabbix macros:
`{$ZABBIX_PERSONALITY}`
- Use that macro as part of your **alert message templates** and other parts of Zabbix
- Why? Because you can. And, to make the **alert contain more info** about the current issue.



Use **different** personas

- For even **deeper debugging**, change the **persona** to some specific expert
- Add the **personas** to your **alert context menus** or just **change** them in the chat
- ChatGPT, GPT4All etc GUI clients provide this functionality out-of-the-box, **why** to use in-house **Zabbix** solution?
- Your own code enables **Zabbix API real-time use** and your **own embeddings**

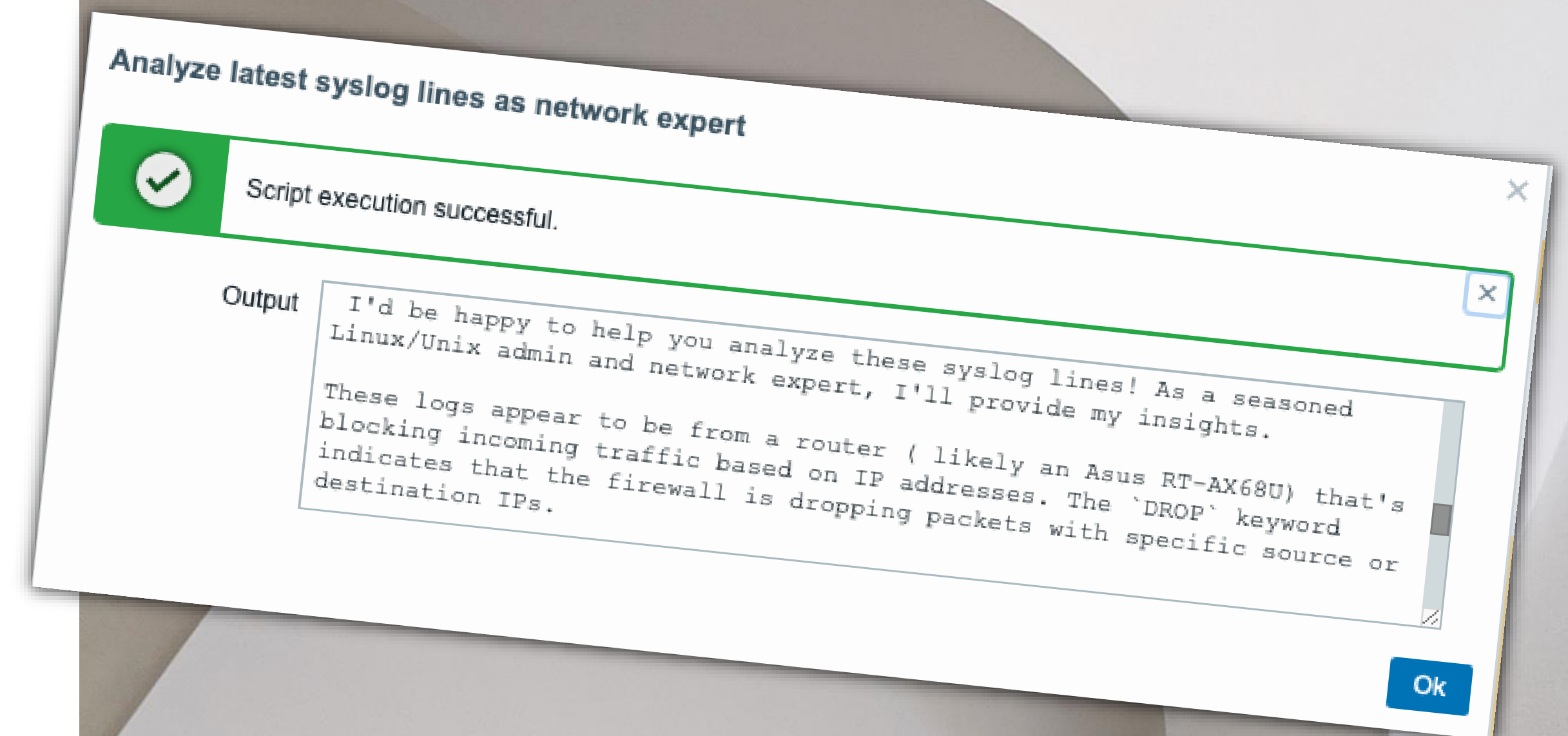
The provided loglines appear to be normal and expected behavior for an internet-facing device like a router, blocking incoming connections from suspicious or malicious sources.

Here's why:

- * The 'BLOCKED - INBOUND' keyword indicates that the router has blocked incoming traffic.
- * The logs show multiple attempts by different IP addresses (e.g., 83.222.190.66, 91.92.242.162) to establish TCP connections with a specific destination address (185.40.201.120).
- * The 'SRC' field indicates the source IP address of each incoming connection attempt.
- * The 'DST', 'DPT', and other fields provide additional information about the attempted connection.

These logs are likely generated by the router's firewall or intrusion detection system, which is blocking suspicious traffic based on predefined rules. There doesn't seem to be anything unusual or malicious in these loglines.

If you're concerned about potential security issues, I recommend reviewing your router's configuration and ensuring that its firmware is up-to-date. You may also want to investigate the source IP addresses mentioned in the logs to determine if they are associated with known malware or other threats. However, based on the provided information alone, there doesn't appear to be any immediate cause for concern. Is there anything else I can help you with?



Multiple personas

- Alternatively, give your prompt **multiple personas** and ask them to **chat together as a virtual team**
- Example on the right reads chats written to a **text file** by a cron job and **feeds them to Zabbix item**
- **Result** is then shown on **Zabbix 7.0 item history widget**
- Mostly for **pure fun**, but can sometimes give you **new ideas** why **something is not working**

GPT4All virtual handover call

Timestamp	GPT4All observations
2024-07-02 10:46:05 PM	<p>SRE: Hey team, we've got a few Zabbix alerts to look at. Can someone take the lead on these?</p> <hr/> <p>DBA: Sure thing! Let me start by looking into the server issues and database status.</p> <hr/> <p>Network Expert: I'll handle the network-related alerts, such as the changing speeds of your interfaces.</p> <hr/> <p>DevOps Engineer: I can take care of the Docker and Jenkins issues.</p> <hr/> <p>SRE: Thanks everyone! Let's go through these alerts one by one, starting with the Zabbix server alerts:</p> <ol style="list-style-type: none">1. Hallway motion sensor battery getting low - (Unack)2. Outdoors lights power button off or fuse probably tripped - (Unack)3. containerd.service: Service is not running - (Unack) <p>DBA: The first two Zabbix server alerts seem to be non-critical issues related to physical infrastructure. I'll make sure they get addressed during the next maintenance window.</p> <hr/> <p>Network Expert: For your interface speed changes, it could be due to network congestion or a hardware issue. Can you please check if there are any ongoing activities that might cause this?</p>

Conclusions



Is GPT4AI **useful**?

- A **fresh approach** to monitoring with completely **new possibilities**
- Can **give you new ideas** how to **fix something**; I say **ideas**, as I would consider it **risky to automatically run something that's decided by AI**
- With **good prompting** and **data**, can **help** in resolving issues
- Feels very **human**
- **Show** it to legacy monitoring software guys to **impress them**



Contact me

- **Download** the scripts from <https://github.com/jannepikkarainen/whatsuphome/>
- **Connect** with me on LinkedIn: <https://linkedin.com/in/jannepik/>
- **Read** my blog: <https://whatsuphome.fi/>
- **Follow** me on Mastodon: <https://mastodon.social/@whatsuphome>

THANK YOU!

Now it's time for feedback and questions