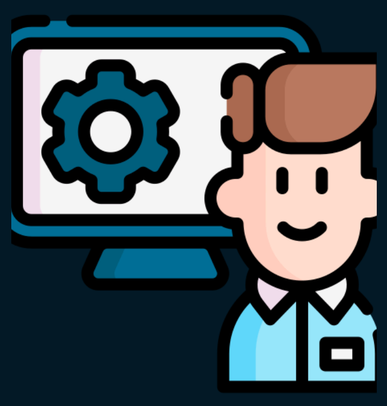

Assatulla Dias

Improvement of active network monitoring with explainable diagnostics

Supervisor: doc. Ing. **Petr Matoušek** Ph.D., M.A.

Active network monitoring

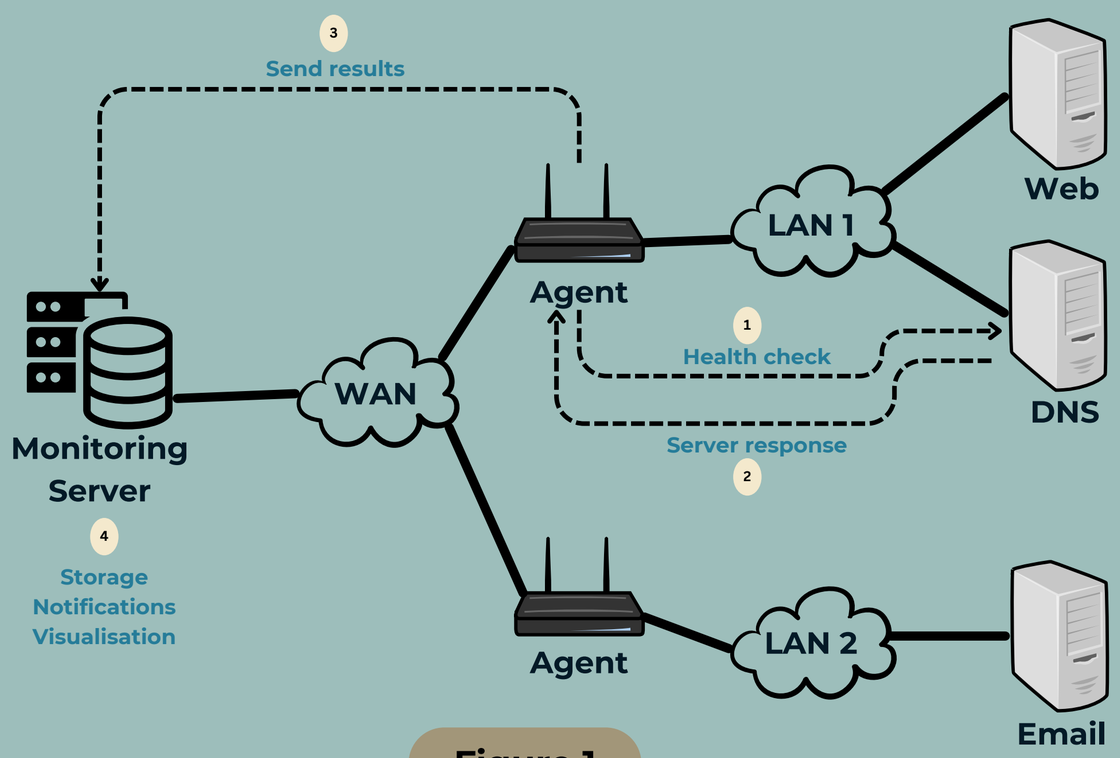

Figure 1

- A proactive method to monitor network infrastructure
- Simulates user journeys and network behaviors continuously
- Helps detect problems before they affect users

Design

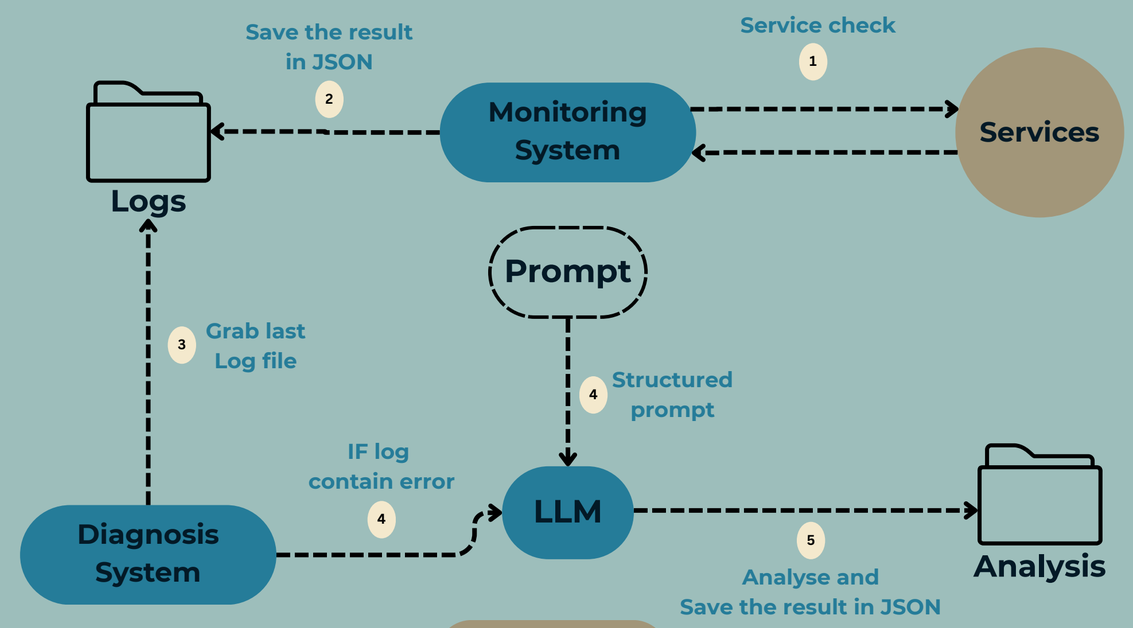

Figure 3

- Custom monitoring system
- Three Large Language Models:
  - Gemini
  - LLaMa
  - Nous Hermes 2

- Using the Prompt engineering technique, LLM returns:
  - Explanation of what happened
  - Classification of the issue
  - Root cause analysis
  - Recommended steps to fix the issue

Explainable diagnostics using Large Langue Models

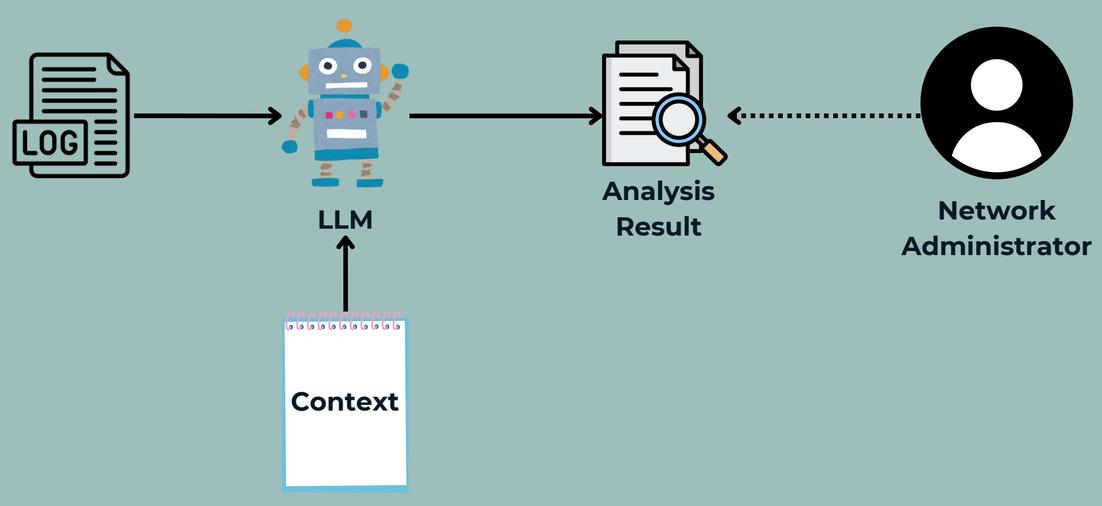

Figure 2

Goal:

- Automatically interpret network monitoring logs using LLM and generate human-readable explanations/analysis

Why do we need it?

1. Manual log analysis is time-consuming and requires deep expertise
2. Standard monitoring tools lack clear, actionable guidance
3. LLMs automate interpretation, enabling faster decision-making
4. Structured explanations simplify troubleshooting

Importance:

- Makes troubleshooting faster
- Helps non-experts understand issues
- Reduces workload

Application and Results


```
{
    "service": "SMTP",
    "status": "error",
    "datetime": "2025-03-29T19:33:35.848968",
    "target_host": "example.smtp.server",
    "port": 587,
    "ip_address": "192.168.0.100",
    "context": {
        "EHLO": "250 mail.example.local...",
        "NOOP": {
            "status": true,
            "smtp_code": "250",
            "smtp_msg": "b'2.0.0 OK'"
        },
        "AUTHENTICATE": {
            "status": false,
            "error_msg": "(535, b'5.7.0 authentication failed')"
        }
    },
    "response_time_ms": 223.0,
    "error_msg": "(535, b'5.7.0 authentication failed')"
},
{
    "service": "Connectivity Test",
    "status": "error",
    "datetime": "2025-03-29T19:37:20.558907",
    "target_host": "192.168.0.111",
    "is_alive": false,
    "error_msg": "Host is not reachable"
}
```


Listing 1

Log file example


```
[
    {
        "1. Explanation": "An attempt to authenticate with the SMTP server failed.",
        "2. Classification": "SMTP Authentication Failure",
        "3. Error Reason": "The SMTP server rejected the authentication attempt, likely due to incorrect
            username or password.",
        "4. Recommendation": "Verify the SMTP username and password. Ensure that the account is not locked or
            disabled. Check the SMTP server's logs for further details.",
        "service": "SMTP"
    },
    {
        "1. Explanation": "A connectivity test to host 192.168.0.111 failed.",
        "2. Classification": "Host Unreachable",
        "3. Error Reason": "The host 192.168.0.111 is either down, unreachable due to network issues, or a
            firewall is blocking the connection.",
        "4. Recommendation": "Verify that the host 192.168.0.111 is powered on and connected to the network.
            Check network connectivity (e.g., ping) to the host. Investigate any firewall rules that might
            be blocking the connection.",
        "service": "Connectivity Test"
    }
]
```


Listing 2

LLM response example

Possible deployment

- Internal IT support tool
- Real-time Chatbot Integration (Slack, Microsoft Teams, etc.)
- On-Call shift helper
- Dashboards and Analytics (Grafana, Zabbix, etc.)

BRNO FACULTY OF INFORMATION TECHNOLOGY
UNIVERSITY OF TECHNOLOGY

This work is part of the research project INVENTOR

Project code: FW10010040

Excel@FIT 2025