DB&L services

Bridging Networks: A Pioneering Fusion for Enhanced Network Oversight

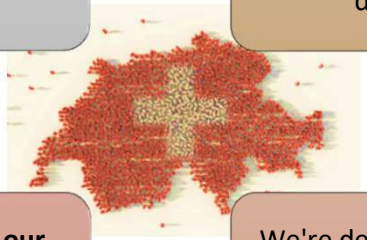
Combining Forces: ntop and Zabbix for Next-Level Network Insight

(2023-Sept)

About Us

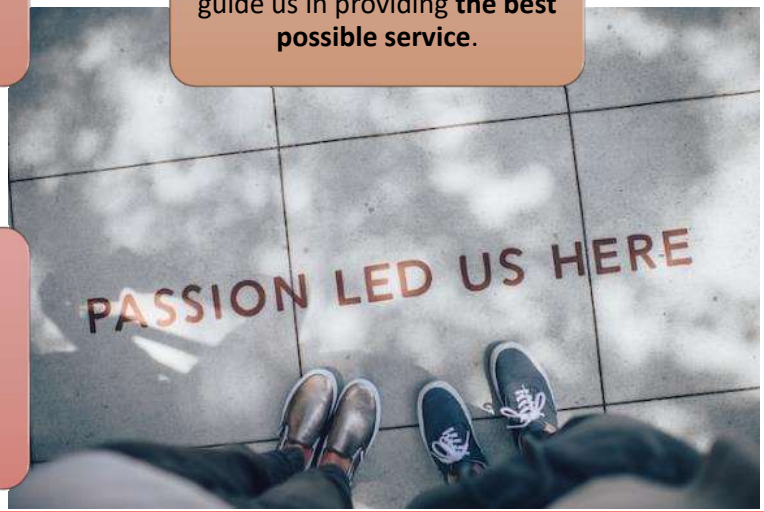
DB&L Services SA is a Swiss IT consulting firm founded in 2007.

Our team of experts has more than **20 years of experience** in project management, architecture, system engineering, and software development.



We're dedicated to delivering excellence and lasting success to our clients and our strong business values and ethics guide us in providing **the best possible service**.

We pride ourselves on our ability to build strong relationships with our clients, tailoring our solutions to meet their unique needs and exceeding their expectations.



Join us and experience the **DB&L Services SA** difference.

DB&L Service SA
tech@dblservices.ch
Via della posta 24, Bioggio

Combining Forces for Advanced Oversight

In today's IT landscape, network professionals and, more generally, system administrators are often overwhelmed with alerts and notifications.

Analyzing and resolving these alerts, especially those related to the network, can become complex and time-consuming.

But what if we could simplify this process?

Our primary focus is on the network domain, but we don't stop there.

Indeed, we recognize the challenges IT specialists face daily in trying to interpret and effectively respond to alerts and errors.

With these challenges in mind, we've developed a specific software.

This tool, **by merging the strengths of Zabbix and ntop**, activates upon the occurrence of certain events, seamlessly integrating Zabbix's data with ntop's analyses.

The result?

Our mission is to make life easier for IT professionals by providing the right tools for advanced analysis and timely response

Faster, more accurate analysis and a more effective resolution of alerts and errors.

DB&L Service SA
tech@dblservices.ch
Via della posta 24, Bioggio

Zabbix & ntop: The Key Players

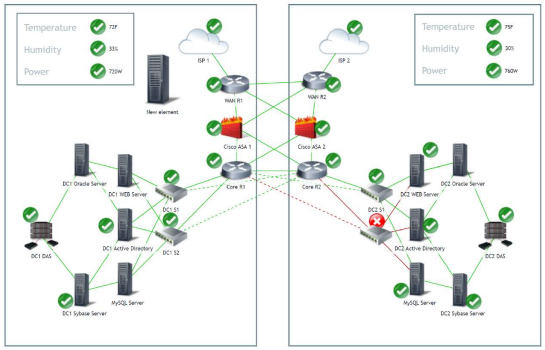
DB&L services

ZABBIX

- Zabbix is an enterprise-class open-source distributed monitoring solution. Designed to monitor and track the status, availability, and performance of network components and applications in complex IT infrastructures. It offers a wide range of features including automatic discovery, real-time viewing, and advanced reporting.

ntop

- ntop is a high-performance network traffic analysis tool. It provides a detailed view of network traffic by analyzing flows and allowing deep traffic introspection. With its capability to display real-time network metrics, ntop assists administrators in keeping network performance at its peak.



Framework Implementation: An Integrated Solution

To manage and address the intricate challenges of the modern network environment, we've developed a framework that harnesses the strengths of existing tools, like Zabbix and ntop, and seamlessly integrates them.

This integration allows for a swift and effective response to network issues, cutting down analysis and resolution time.

Key features of our framework:

- **Efficiency**: Designed for quick response, fully leveraging the capabilities of Zabbix and ntop.
- **Extensibility**: The framework can be expanded to include more tools and address additional challenges.
- **Maintainability**: Crafted in a manner that eases updates and maintenance, ensuring the software remains up-to-date and reliable over time.

Practical Integration: Zabbix, ntop (and CMDB)

The heart of our solution lies in the hands-on integration of Zabbix and ntop.

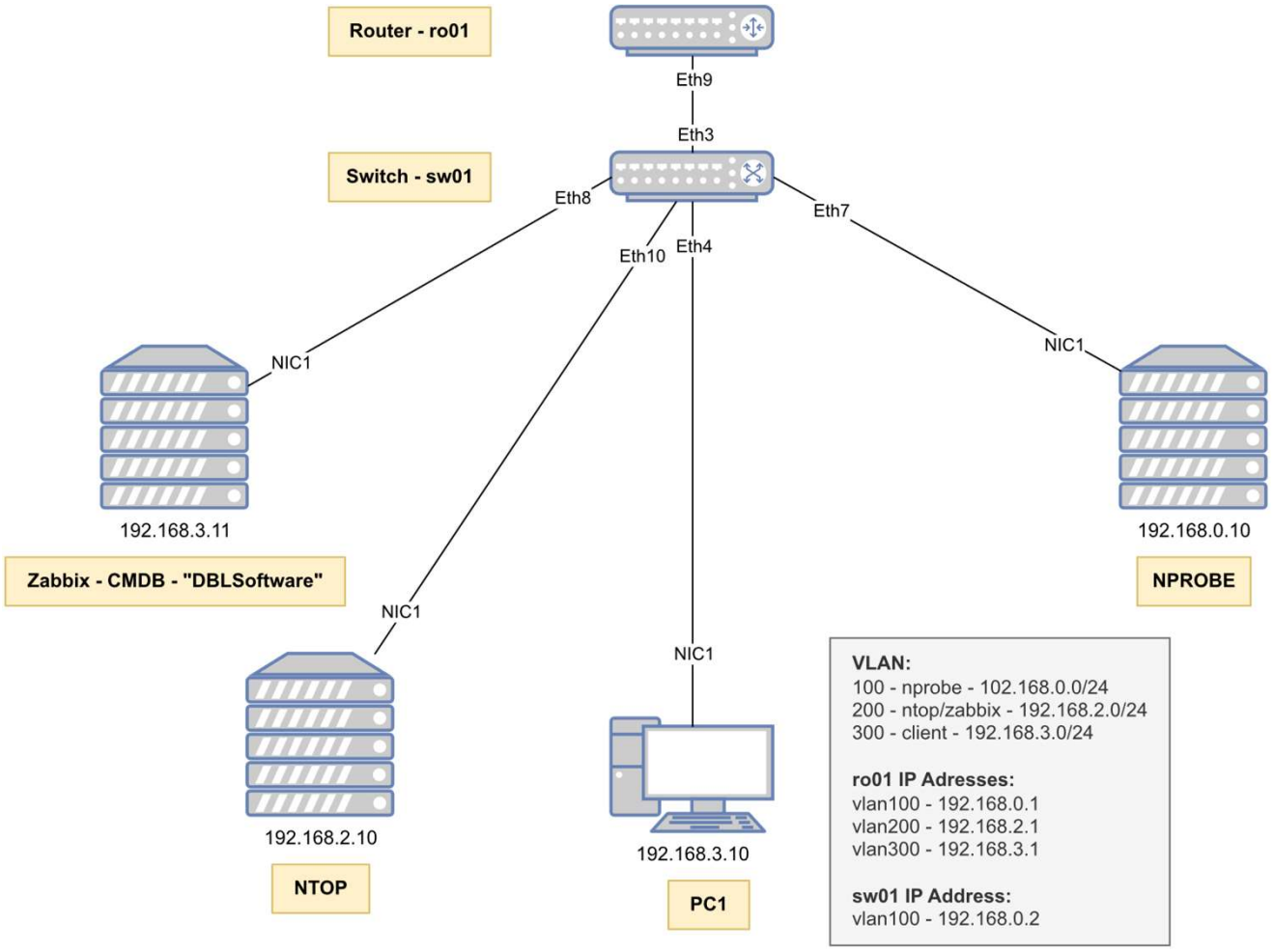
This synergy allows for efficient and timely monitoring, analysis, and response to network issues.

The addition of a CMDB further enhances the process, providing a comprehensive view of network resources and related applications.

Key integration points:

- **Monitoring and Analysis**: Zabbix detects network issues, while ntop provides in-depth insight into the cause.
- **Correlation**: The CMDB assists in linking network issues to specific resources and applications, offering a holistic view of the issue.
- **Automation and Response**: Our software stands as a pivotal element in the detection and response process. Once an event is pinpointed by Zabbix, our software automatically springs into action, querying ntop for more in-depth details. This integrated process provides a comprehensive view of the event, blending high-level information from Zabbix with granular details from ntop. Moreover, the ability to respond in real-time to issues allows for more effective and timely management of network anomalies.

Practical Integration: Zabbix, ntop (and CMDB) - (4)



Practical Integration: the process

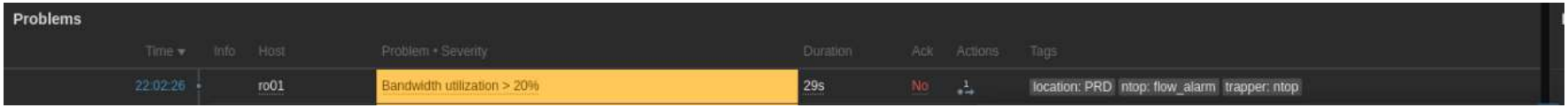
Phase 1:
Within our monitored environment, Zabbix spots a specific issue: "Bandwidth utilization > 20%". Recognizing this as a potential critical situation, it immediately triggers our software, initiating a direct query to ntop for more detailed insights regarding the nature of the bandwidth spike.

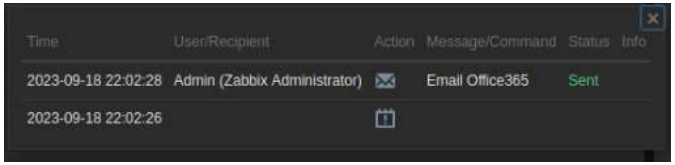
Phase 2:
Responding to the query, ntop examines the data flow of the interface that exhibited the excessive bandwidth usage.

Practical Integration: the process - (2)

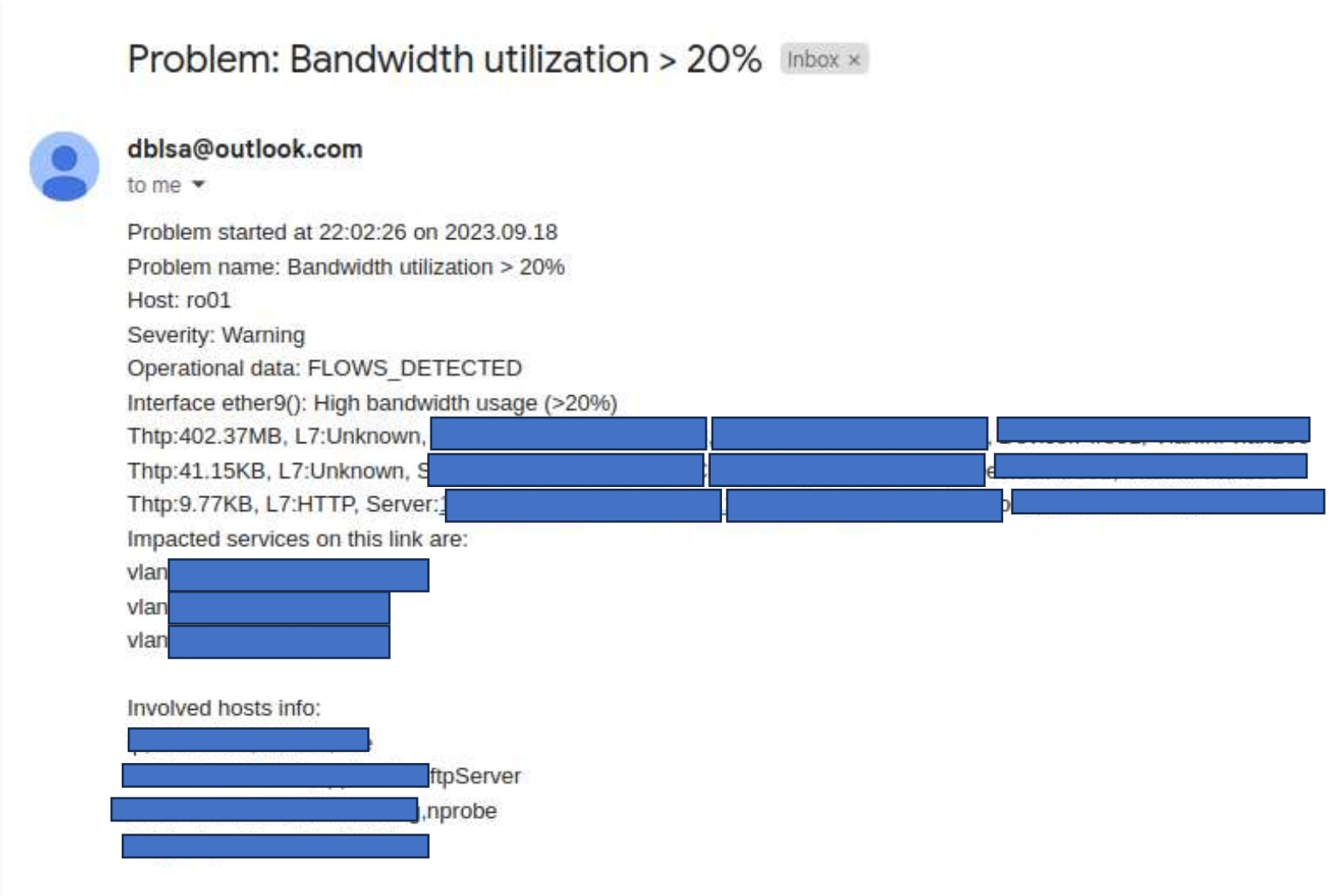
Phase 3:
Upon completing the analysis, ntop provides the detailed information requested.
Specifically, **it highlights the services most impacted** by the excessive bandwidth usage and **identifies the specific hosts involved**, thus offering a comprehensive overview of the elements responsible for the detected anomaly.

Phase 4:
After retrieving the detailed information from ntop, Zabbix integrates it within its platform and subsequently sends an automatic email to the responsible network technician or engineer. This communication facilitates a prompt reaction, providing all the necessary details for efficiently analyzing and resolving the issue





Practical Integration: the process – (3)



Problem: Bandwidth utilization > 20% Inbox ×

dblsa@outlook.com
to me

Problem started at 22:02:26 on 2023.09.18
Problem name: Bandwidth utilization > 20%
Host: ro01
Severity: Warning
Operational data: FLOWS_DETECTED
Interface ether9(): High bandwidth usage (>20%)
Thtp:402.37MB, L7:Unknown, [redacted]
Thtp:41.15KB, L7:Unknown, [redacted]
Thtp:9.77KB, L7:HTTP, Server:[redacted]
Impacted services on this link are:
vlan[redacted]
vlan[redacted]
vlan[redacted]

Involved hosts info:
[redacted]
[redacted]ftpServer
[redacted],nprobe
[redacted]

Next Steps and Future Vision

Feature Expansion and Use Cases: Beyond just Zabbix and ntop, we're actively exploring how to broaden our software's capabilities. This includes looking into other monitoring solutions and integrations, as well as introducing new use cases that align with the ever-evolving challenges of network management.

Advanced Automation, Data Retrieval, and Predictive Analysis: Our current system queries ntop upon detecting specific events. We aim to implement different logics for data retrieval and use artificial intelligence and machine learning to anticipate network issues before they escalate. The goal is to predict potential disruptions, allowing for proactive interventions.

Enhanced User Interface and Web GUI: Feedback-driven improvements to our user interface are underway. Additionally, we're planning to expand beyond the CLI and introduce a Web-based GUI, such as a Single Page Application (SPA), to offer users a more interactive and intuitive experience.

Database Integration: We also recognize the importance of supporting different Configuration Management Databases (CMDBs). Given that networks are fundamentally graph structures, we're considering graph-based databases. Such databases would simplify data storage, querying, and enrichment processes.

Data Collection and Advanced Processing: With an eye towards the future, we're aiming to not only collect but also leverage the data for advanced processing techniques, including machine learning. This data-driven approach will further enhance the capability of our software to provide predictive insights and actionable recommendations.

Paolo Rizzo

+41 79 460 75 38

paolo.rizzo@dblservices.ch

www.dblsa.ch