Enterprise Network Monitoring with Open-Source Zabbix

Lê Minh Hậu
Thai Nguyen University of Information and Communication Technology
Thai Nguyen University, Thai Nguyen, Vietnam
dtc1954802010100@ictu.edu.vn

***Abstract*—This undergraduate thesis implements a small enterprise-style network monitoring laboratory using Zabbix. The author reviews enterprise networks, common attacks, and monitoring methods before configuring the Zabbix server, web interface, agents, and templates. The practical model monitors Windows and Linux hosts, a ClearOS firewall through SNMP, and an Apache service through HTTP. Dashboard views cover resource use and service response, while triggers and notifications demonstrate operational and security alerts, including a denial-of-service scenario. The source provides setup screens and test observations showing that the selected hosts and services can be observed in one interface. It does not quantify performance on a large production network or prove that all security incidents can be detected. The author explicitly notes that the trial uses a small number of devices and does not exercise audit reporting, discovery, or all integration features. The thesis contributes a documented configuration and test workflow for a modest network and proposes a broader deployment procedure, with scalability and operational reliability remaining open for later assessment.**

***Index Terms*—Zabbix, network monitoring, SNMP, Apache, alerts, enterprise network**

I. Introduction

Enterprise networks contain multiple hosts, firewalls, and web services whose state must be monitored continuously. The thesis asks whether an open-source Zabbix installation can consolidate operational and security signals in a small representative network. It reviews network structure, attacks, and monitoring approaches before presenting an implementation. The reported work is a laboratory exercise intended to guide later enterprise deployment, rather than a measured trial in a large live environment [1]. Earlier ICTU student work on related designs is included here for context [3]. Related published studies provide context for the subject and methods [4], [5], [6], [7], [8], [9], [10]. These contextual works were selected for this English summary; they are not asserted to appear in the original thesis bibliography.

II. Methods

The author builds a network model and installs the Zabbix server and web interface. Monitoring is configured through Zabbix agents for computers, SNMP for a ClearOS firewall, and an HTTP template for Apache. The report describes hosts, items, triggers, dashboards, alerts, and notification channels. Practical scenarios inspect CPU, memory, disk use, firewall traffic, service response, security state, and a denial-of-service event. Screenshots and observations document the monitoring and alert behavior [1].

Supervisor: Lê Tuấn Anh, Thai Nguyen University of Information and Communication Technology (ltanh@ictu.edu.vn).

III. Results

The source shows dashboard widgets for host resource use, network traffic, and service responses, as well as alert examples for operational and security conditions. Its trial demonstrates that several protocol types can be presented through the same Zabbix interface and that configured triggers produce notices during the tested scenarios. The report does not measure alert latency systematically or test many devices. The findings therefore support feasibility in the small model, not a quantified claim of enterprise-scale performance [1].

IV. Discussion

The author identifies the small trial network as a major limitation. Additional hosts, stronger load conditions, and production access controls would be needed before scaling the monitoring system. The report proposes using audit logs, reports, low-level discovery, APIs, and selected third-party extensions in later work. It also recommends treating monitoring as one part of a wider security process rather than assuming that alerts alone prevent incidents. These proposals are not outcomes demonstrated in the current source [1].

V. Conclusion

The thesis documents the installation and trial of Zabbix for monitoring a small enterprise-style network. Agent, SNMP, and HTTP cases, dashboard screens, and alert examples support the reported functionality. The source does not establish performance or completeness for large deployments. It provides a practical setup record and a proposed deployment procedure, with scale testing and deeper security integration remaining future work [1].

References

[1] Lê Minh Hậu, ”Enterprise Network Monitoring with Open-Source Zabbix,” internal undergraduate thesis (original in Vietnamese), Thai Nguyen University of Information and Communication Technology, 2024.
[2] OWASP Foundation, ”Top 10 Web Application Security Risks,” https://owasp.org/www-project-top-ten/, cited in the source thesis.
[3] ICTU Student 90, ”SNMP Protocol and Its Application in Remote Network Management,” internal undergraduate thesis, Thai Nguyen University of Information and Communication Technology, 2009.

[4] I. V. Bilobrovets, ”Network threat detection technology using Zabbix software,” Modern Information Security, 2023. doi:10.31673/2409-7292.2023.020003.
[5] Mohd Faris Mohd Fuzi et al., ”Integrated Network Monitoring using Zabbix with Push Notification via Telegram,” Journal of Computing Research and Innovation, 2022. doi:10.24191/jcrinn.v7i1.282.
[6] Arya Pradana et al., ”Implementasi Sistem Monitoring Jaringan Menggunakan Zabbix Berbasis SNMP,” AITI, 2022. doi:10.24246/aiti.v19i2.248-262.
[7] Vreixo Formoso et al., ”Open Source Tool For Network Monitoring,” International Journal of Business Data Communications and Networking, 2009. doi:10.4018/jbdcn.2009010102.
[8] Ali Al Shidhani et al., ”A Comparative Analysis of Open Source Network Monitoring Tools,” International Journal of Open Source Software and Processes, 2016. doi:10.4018/ijossp.2016040101.
[9] E.S. Guznova et al., ”Zabbix monitoring system for analyzing and predicting events,” Achievements of Modern Radioelectronics, 2023. doi:10.18127/j20700784-202312-17.
[10] T. Michael Silver, ”Monitoring Network and Service Availability with Open-Source Software,” Information Technology and Libraries, 2010. doi:10.6017/ital.v29i1.3153.