Intelligent monitoring system

*An integrated approach using Zabbix, Grafana, and Machine Learning*

Luís António Pinto de Barros

Polytechnic Institute of Guarda

**Abstract**— This paper presents the development and implementation of an integrated network monitoring infrastructure with enhanced security measures and intelligent event filtering capabilities. The project encompassed the establishment of a controlled laboratory environment featuring a demilitarized zone (DMZ), incorporating SFTP, SMTP, and HTTP servers to simulate enterprise-level network operations.

The implementation methodology followed a systematic approach, beginning with the configuration of network segmentation and DMZ architecture to ensure optimal security posture. Subsequently, the Zabbix monitoring system was deployed for comprehensive network resource supervision and anomaly detection. The system's capabilities were extended through strategic integration with GLPi asset management platform, facilitating automated inventory tracking and device relationship mapping.

Further enhancement was achieved through the integration of Grafana analytics platform, enabling sophisticated data visualization and real-time performance metrics analysis. To optimize operational efficiency, a cross-platform application was developed using React Native framework, providing unified access to monitoring systems through both web and mobile interfaces.

The final phase incorporated machine learning algorithms, specifically implementing the K-means clustering technique, to optimize event filtering and reduce false positives in the monitoring system. This approach resulted in a significant improvement in event classification accuracy, with a silhouette coefficient of 0.8491, demonstrating effective segregation of relevant network events from noise.

**Keywords** — Network Monitoring, Cybersecurity Infrastructure, DMZ Implementation, Zabbix Integration, Machine Learning, K-means Clustering, React Native

António Mário Ribeiro Martins

Polytechnic Institute of Guarda

1. MOTIVATION

The fundamental motivation for this project stemmed from the growing necessity to ensure comprehensive network monitoring, particularly within a technological landscape where cyber threats undergo continuous evolution. The establishment of a controlled laboratory environment incorporating a DMZ proved essential for simulating real-world scenarios, enabling the assessment of deployed tools' response capabilities and effectiveness. The integration of Zabbix with other platforms, specifically GLPi and Grafana, aims not only to enhance operational efficiency but also to optimize data analysis and presentation clarity. Furthermore, the incorporation of machine learning techniques reflects the pursuit of cutting-edge event filtering methodologies, reducing noise while maximizing the relevance of captured information. In essence, the motivation was to develop a robust infrastructure that, beyond ensuring security, would facilitate innovations in the cybersecurity domain.

1. OBJECTIVES

The project objectives are centered on establishing a robust and efficient monitoring environment, emphasizing the integration of multiple tools and innovative techniques. To achieve this goal, the following objectives were established:

* Configure and test the network laboratory with DMZ and associated servers;
* Implement and optimize the Zabbix monitoring system for continuous network supervision;
* Integrate Zabbix with the GLPi asset management system to achieve a consolidated view of devices;
* Establish connectivity between Zabbix and Grafana for the development of customized monitoring dashboards and advanced visual analytics;
* Develop a mobile and web application using React Native to centralize and streamline network monitoring access;
* Implement machine learning techniques on Zabbix data to filter and minimize non-pertinent events;
* Comprehensively test the system to ensure the effectiveness and efficiency of all implementations;
* Document all stages and configurations to facilitate future system expansions or modifications.

1. STATE OF THE ART

Network monitoring and optimization are imperative in the digital era, where security and efficiency are crucial. Understanding the technological landscape is fundamental for selecting the most appropriate tools to meet project requirements.

Initial analysis focused on evaluating existing network monitoring solutions, as detailed in Table 1. The comparison encompassed major platforms including Zabbix, Nagios, PRTG, SolarWinds, WireShark, Splunk, and Graylog, evaluating their capabilities across critical operational parameters.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Platform Features** | **Zabbix** | **Nagios** | **PRTG** | **SolarWinds** | **WireShark** | **Splunk** | **Graylog** |
| Real-time Monitoring | **✔** |  | **✔** | **✔** | **✔** |  |  |
| Integration Capabilities | **✔** | **✔** | **✔** |  |  | **✔** | **✔** |
| Configurable Alerts | **✔** | **✔** |  |  |  |  |  |
| Web Interface | **✔** | **✔** | **✔** | **✔** |  | **✔** | **✔** |
| Application Monitoring | **✔** |  |  | **✔** |  |  |  |
| Packet Analysis |  |  |  |  | **✔** |  |  |
| Log Centralization |  |  |  | **✔** |  | **✔** | **✔** |

Table 1- Comparison of Network Monitoring Platforms' Features

B. Critical Analysis of Monitoring Platforms

Zabbix demonstrates versatility and extensibility, providing an end-to-end solution for network monitoring. While Nagios offers robust functionality, it often requires more extensive manual configuration. PRTG distinguishes itself through its user-friendly interface and efficiency across various scenarios.

Notably, Zabbix offers valuable integrations with other tools, particularly GLPi and Grafana, although these integrations were not the primary focus of this project.

C. Machine Learning Solutions Analysis

A comprehensive evaluation of machine learning libraries was conducted, focusing on their applicability to network monitoring data analysis, as shown in Table 2.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Features** | TensorFlow | Scikit-learn | Keras | Pytorch |
| Open source | ✔ | ✔ | ✔ | ✔ |
| Neural Network Support | ✔ |  | ✔ | ✔ |
| Flexibility na Modularity | ✔ | ✔ | ✔ |  |
| Predefined  Algorithms |  | ✔ |  |  |
| Automatic  Differentiation | ✔ |  |  | ✔ |

Asd

Table 2 - Comparison of Python libraries

D. Critical Analysis of ML Libraries

TensorFlow, with its comprehensive library, presents a robust solution for complex analyses, despite its steeper learning curve. Scikit-learn proves ideal for more straightforward machine learning tasks.

The selection criteria for technologies centered on three key aspects:

1. Adaptability
2. Integration capabilities
3. Practical effectiveness in real-world scenarios

IV. NETWORK TOPOLOGY

In this work, we configured a network infrastructure that simulates the complexity found in real enterprise environments, encompassing not only device installation but also the construction of a digital ecosystem analogous to those utilized by modern organizations.

A. Network Configuration

The laboratory implementation involved the deployment of essential servers:

* Email server
* Web server
* SFTP server

Additionally, significant attention was given to the installation and configuration of critical security and connectivity components, specifically a firewall and managed switch infrastructure.

B. DMZ Implementation

Security measures were emphasized through the implementation of a Demilitarized Zone (DMZ). This architectural layer serves as a security barrier, positioning critical resources such as web and email servers in an intermediary zone between internal and external networks, thereby shielding sensitive assets from external threats.

A diagram of a computer network

AI-generated content may be incorrect.The implemented network architecture is illustrated in Figure 1, which depicts the logical separation of network segments and the placement of key infrastructure components.

Figure 1 - Network

C. Security Configuration

In the firewall configuration, rules were strictly defined to permit only protocols essential for:

1. Internal network communication
2. Secure internet access
3. Server operability

This restrictive approach ensures that only vital protocols for server operations, internal network communication, and secure internet access are authorized, thereby:

* Reducing potential attack vectors
* Ensuring network integrity
* Maintaining operational security

The implementation follows security best practices by isolating critical services in the DMZ while maintaining appropriate access controls through the firewall, as demonstrated in the network architecture diagram.