ISSN 3032-3533
Vol 1, No.1 (2024)

Enhancing Network Performance Visibility with Grafana and Prometheus: A Case Study at P.T. Nata Digital Solution

1st Akhyar Lubis
Faculty of Science and Technology
Universitas Pembangunan Panca Budi
Medan, Indonesia
akhyarlbs@pancabudi.ac.id

2nd Muhammad Amal Giffari
Faculty of Science and Technology
Universitas Pembangunan Panca Budi
Medan, Indonesia
muhammadamal1337@gmail.com

3rd Sri Wahyuni
Faculty of Science and Technology
Universitas Pembangunan Panca Budi
Medan, Indonesia
sriwahyuni@dosen.pancabudi.ac.id

***Abstract*—This study presents a network monitoring system implementation using Prometheus and Grafana at P.T. Nata Digital Solution. The primary objective was to enhance network performance visibility and streamline network management by integrating Prometheus for data collection and Grafana for data visualisation. Various exporters, including Node, SNMP, and Blackbox, were configured to gather critical performance metrics such as CPU load, memory usage, disk space, and network traffic. The system also incorporated real-time alerting through Telegram, allowing for prompt responses to network issues. The implementation results showed significant improvements in network monitoring efficiency, enabling the I.T. team to proactively address performance bottlenecks and minimise downtime. The study highlights the effectiveness of using open-source tools to provide a scalable, cost-effective monitoring solution tailored to the organisation's needs. This approach facilitated proactive network management and served as a model for other organisations seeking to enhance their monitoring capabilities. Future work could integrate additional data sources and explore advanced analytics to optimise network management and operational resilience.**

Keywords—Network Monitoring, Prometheus, Grafana, Real-time Alerting, Open-source ToolsIntroduction

The rapid evolution of digital technologies has positioned computer networks as critical infrastructure across various sectors, including business, education, and government. Ensuring smooth network operations is essential for supporting daily activities and preventing disruptive incidents affecting performance and reliability. In this context, network monitoring is pivotal in maintaining optimal performance and availability by enabling proactive detection and resolution of potential issues [1]. However, traditional manual network monitoring methods often need to be more efficient and susceptible to human errors, highlighting the need for automated solutions.

Traditional network monitoring systems frequently need help with limitations such as high licensing costs, lack of scalability, and a user interface that can be cumbersome for administrators. These constraints have driven organisations like PT. Nata Digital Solution (NDS), a company specialising in information technology and internet services, seeks open-source monitoring solutions such as Grafana and Prometheus. These platforms offer cost-effective, scalable, and easy-to-implement alternatives that align well with NDS's operational needs, providing a reliable and comprehensive approach to network performance management [2].

As network infrastructures grow increasingly complex and the number of connected devices continues to rise, the demand for efficient and reliable monitoring systems has never been greater. PT. Nata Digital Solution faces challenges in maintaining visibility over its network performance, managing its infrastructure, and responding promptly to network anomalies. The main research problem addressed in this study is how to implement an effective network monitoring system using Grafana and Prometheus to enhance network performance visibility and streamline network management at PT. Nata Digital Solution.

The general solution proposed involves implementing a network monitoring system that integrates Grafana for data visualisation and Prometheus for metric collection. This system aims to provide real-time insights into the performance of network devices such as routers and switches, enabling proactive detection and resolution of network issues. By utilising open-source technologies, this solution is designed to be scalable, cost-efficient, and tailored to the specific needs of P.T. Nata Digital Solution.

Grafana is an open-source platform renowned for its robust data visualisation, monitoring, and alerting capabilities. It allows organisations to create interactive dashboards displaying real-time data, making it easier for network administrators to identify performance trends and potential issues [3]. On the other hand, Prometheus is a time-series database and monitoring system that collects metrics from configured targets at given intervals, providing robust data that can be queried to gain insights into network performance [4]. The combination of Grafana and Prometheus offers a flexible and comprehensive solution for network monitoring, particularly for environments that require real-time data analysis and alerting capabilities [5].

Integrating Grafana with Prometheus enhances monitoring efficiency by providing detailed visualisations of key performance metrics such as CPU load, memory usage, and network traffic [6]. This system supports various data sources and can be extended with numerous plugins, making it adaptable to different monitoring needs. In addition, using Prometheus's query language (PromQL) allows administrators to perform complex queries on the collected metrics, enabling

more profound analysis and more precise alert configurations [7].

Several studies have demonstrated the effectiveness of Grafana and Prometheus in enhancing network monitoring capabilities. For example, a survey by Febriana [8] highlighted the advantages of using these tools in terms of scalability, flexibility, and the ability to provide real-time alerts through various channels, including Telegram [9], [10]. By leveraging these technologies, P.T. Nata Digital Solution can address network management challenges, improve visibility, and reduce response times to network incidents, leading to better network performance and reliability.

I. LITERATURE REVIEW

Grafana is an open-source platform renowned for its robust capabilities in data visualisation, monitoring, and alerting [11]. It allows organisations to create interactive dashboards displaying real-time data, making it easier for network administrators to identify performance trends and potential issues [3], [12]. On the other hand, Prometheus is a time-series database and monitoring system that collects metrics from configured targets at given intervals, providing robust data that can be queried to gain insights into network performance. The combination of Grafana and Prometheus offers a flexible and comprehensive solution for network monitoring, particularly for environments that require real-time data analysis and alerting capabilities [13].

Integrating Grafana with Prometheus enhances monitoring efficiency by providing detailed visualisations of key performance metrics such as CPU load, memory usage, and network traffic. This system supports various data sources and can be extended with numerous plugins, making it adaptable to different monitoring needs. In addition, the use of Prometheus's query language (PromQL) allows administrators to perform complex queries on the collected metrics, enabling more profound analysis and more precise alert configurations [9], [14], [15].

Several studies have demonstrated the effectiveness of Grafana and Prometheus in enhancing network monitoring capabilities. For example, a survey by Febriana (2020) highlighted the advantages of using these tools in terms of scalability, flexibility, and the ability to provide real-time alerts through various channels, including Telegram [16], by leveraging these technologies, PT. Nata Digital Solution can address network management challenges, improve visibility, and reduce response times to network incidents, leading to better performance and reliability. The existing literature on network monitoring using Grafana and Prometheus highlights numerous benefits, such as improved scalability, cost efficiency, and enhanced real-time data visualisation capabilities. Studies such as those by Darmawan [2] and Iqromullah [3] have shown that these tools are particularly effective in environments that require detailed insights into network performance metrics. However, while the integration of Grafana and Prometheus offers significant advantages, there are notable gaps in the literature regarding their application in specific contexts, such as in complex network environments like PT. Nata Digital Solution.

One significant gap is the lack of detailed case studies that explore the integration of Grafana and Prometheus with additional alerting tools, such as Telegram, to improve response times and facilitate proactive network management. Furthermore, while many studies have focused on the technical capabilities of these tools, fewer have examined the practical implementation challenges, including the setup and configuration complexities, that organisations may face when adopting these technologies [8]. These gaps underscore the need for further research to explore how Grafana and Prometheus can effectively implement and integrate with existing network infrastructure to maximise their benefits.

Additionally, limited research exists on the specific impact of these tools on operational efficiency and business outcomes in real-world scenarios. The current study aims to address these gaps by providing a detailed analysis of the implementation process, challenges, and outcomes of deploying Grafana and Prometheus at PT Nata Digital Solution. By doing so, it seeks to contribute to the body of knowledge on network monitoring solutions and offer practical insights for other organisations considering similar implementations.

The primary objective of this study is to implement a comprehensive network monitoring system using Grafana and Prometheus to enhance network performance visibility and optimise network management at P.T. Nata Digital Solution. The study aims to demonstrate how these tools can monitor critical performance metrics, such as bandwidth, latency, and packet loss, and provide real-time alerts through integration with Telegram. This will enable the I.T. team at P.T. Nata Digital Solution to detect and resolve network issues more rapidly, reducing downtime and improving overall network reliability.

The novelty of this research lies in its focus on the practical implementation of Grafana and Prometheus in a real-world business environment, specifically within the context of P.T. Nata Digital Solution. Unlike previous studies that primarily focus on the theoretical aspects of isolated functionalities of these tools, this study provides a comprehensive case study that includes integrating alerting systems and addresses the challenges encountered during implementation. The scope of the study is limited to PT's network infrastructure. Nata Digital Solution, with an emphasis on the practical application, setup, and configuration of Grafana and Prometheus as a unified monitoring solution.

This research contributes to the field by offering detailed insights into the deployment process, the practical challenges, and the benefits of using Grafana and Prometheus for network monitoring. It aims to serve as a reference for other organisations facing similar network management challenges and considering adopting open-source monitoring solutions.

II. METHOD

A. Material

The materials used to implement the proposed monitoring system include hardware and software components. The hardware comprises a server equipped with an Intel Core i3-7100T processor, 8 GB of RAM, and a 256 GB SSD, running on the Ubuntu 24.04 LTS operating system. On the software side, the system utilises Prometheus (version 2.43) as the data collection tool, Grafana (version 11.1.0) for data visualisation, Node Exporter (version 1.8.2) for system-level metrics, SNMP Exporter (version 0.26.0) for network devices, and Blackbox Exporter (version 0.25.0) for service availability checks. Telegram is used for real-time alert notifications, ensuring that the I.T. team is immediately informed of any critical issues the monitoring system detects. This

combination of hardware and software provides a robust, scalable, and efficient solution for comprehensive network monitoring at P.T. Nata Digital Solution.

B. Monitoring of the Existing System

The current monitoring system at P.T. Nata Digital Solution primarily relies on traditional manual methods, often resulting in delayed responses to network issues, as problems are typically identified only after user complaints are received. This approach needs more real-time visibility and automation, making it efficient and prone to human error. A comprehensive analysis of the existing system was conducted to address these shortcomings, focusing on the essential network performance indicators, such as bandwidth utilisation, latency, and device resource usage. This analysis highlighted the need for an automated monitoring solution that could provide real-time alerts and performance insights, enabling quicker response times and proactive management of network resources.

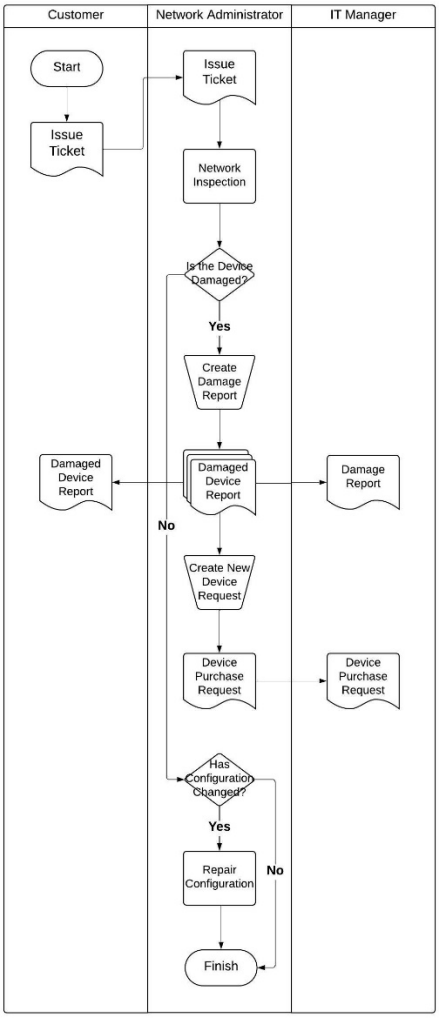

Fig. 1. Flowchart of the Existing Monitoring System

This flowchart illustrates the process flow of the current monitoring system. It starts with the customer reporting an issue, followed by network checks by the Network Administrator. A damage report is generated if a device is found to be faulty. The process involves creating reports and requesting new devices if necessary, followed by configuration checks and corrections as required.

C. System Architecture Design

The proposed system architecture integrates Prometheus for data collection and Grafana for data visualisation, offering a scalable and open-source solution for network monitoring. The architecture is designed to continuously collect metrics from various network devices, such as routers and switches, using Prometheus's scraping capabilities. Data is stored in Prometheus's time-series database and visualised in Grafana through interactive dashboards. Alerts are configured within Grafana to notify the I.T. team via Telegram whenever predefined thresholds are exceeded, such as high CPU usage or network latency. This architecture improves visibility into network performance and enhances the overall management and responsiveness of the I.T. team to network anomalies.

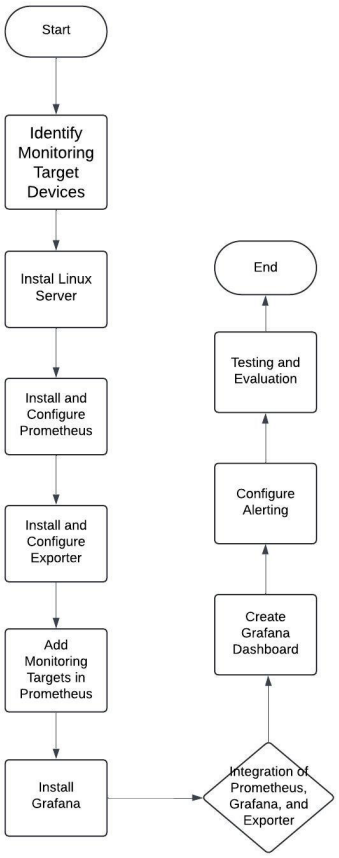

Fig. 2. Flowchart of Monitoring System Design

This flowchart depicts the design process for the proposed monitoring system. It begins with identifying and monitoring target devices, followed by installing a Linux server and setting up Prometheus and its exporters. Grafana is then installed and integrated with Prometheus, and dashboards are created. The final steps involve configuring alerting mechanisms and conducting testing.

D. Network Topology Design

The network topology for the monitoring system includes a centralised server configured to run Prometheus and Grafana, connected to various network devices that serve as monitoring targets. The topology facilitates efficient data flow from monitored devices to the server, which scrapes metrics at defined intervals. Each device in the network, including routers, switches, and servers, is configured to expose

necessary metrics through specific ports, such as SNMP for network devices and Node Exporter for system metrics. The server, positioned at I.P. address 10.99.99.2, acts as the core of the monitoring system, aggregating data and serving it to Grafana for visualisation. This structured topology ensures comprehensive coverage and monitoring of the entire network infrastructure at P.T. Nata Digital Solution.

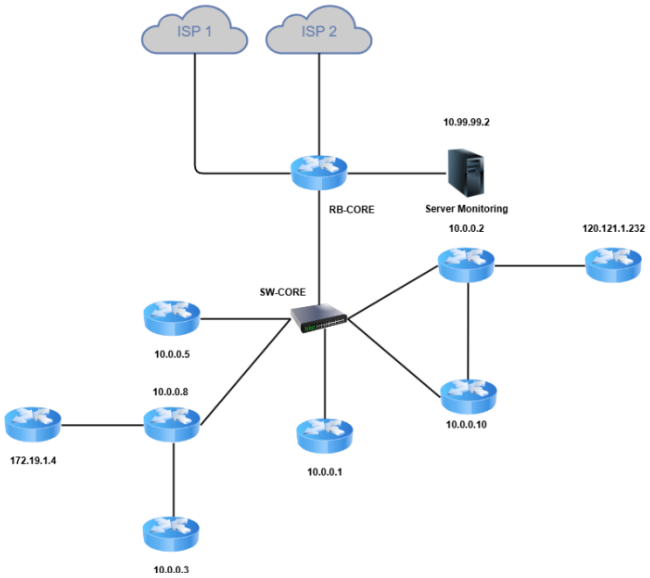

Fig. 3. Network Topology

The network topology diagram shows the monitoring system's infrastructure layout at PT. Nata Digital Solution. It includes connections between routers, switches, and the monitoring server, which operates on I.P. address 10.99.99.2. The diagram also highlights connections to external internet service providers (ISP1 and ISP2), illustrating the network's external linkages.

E. Monitoring System Architecture with Grafana and Prometheus

The proposed system architecture significantly improves the current setup by introducing automation, scalability, and real-time monitoring capabilities. Prometheus acts as the primary data collection agent, interfacing with various exporters to gather metrics from both system and network levels. The collected data is then visualised in Grafana, which provides a user-friendly interface for monitoring network performance through customisable dashboards. This architecture also incorporates real-time alerting through Telegram, allowing the I.T. team to respond quickly to detected anomalies. The proposed system enhances operational efficiency and reduces downtime by enabling proactive management of network resources.

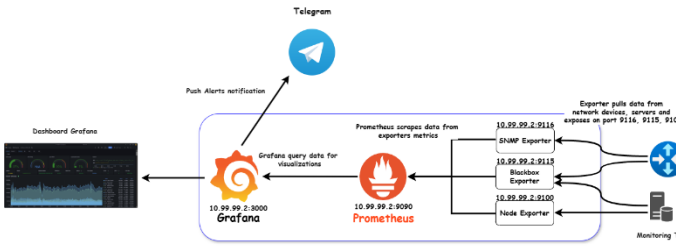

Fig. 4. Monitoring System Architecture with Grafana and Prometheus

This diagram illustrates the architecture of the monitoring system utilising Grafana and Prometheus. It shows how Prometheus collects metrics from various exporters (SNMP, Blackbox, and Node Exporter) connected to network devices. Grafana queries Prometheus for data visualisation, and the system is integrated with Telegram for real-time alert notifications.

III. RESULT AND DISCUSSION

The implementation of the network monitoring system using Prometheus and Grafana at P.T. Nata Digital Solution was successfully carried out with a series of structured steps, including the installation and configuration of Prometheus, SNMP Exporter, Blackbox Exporter, Node Exporter, and Grafana. Each component was meticulously set up to ensure accurate data collection and visualisation of network metrics, such as CPU load, memory usage, disk space, bandwidth, latency, and packet loss. The monitoring targets were configured with Prometheus using the prometheus.yml configuration file, which specifies the scrape intervals and targets to be monitored, including network devices like routers and switches. The Grafana dashboards provided a comprehensive visualisation of the metrics, enabling real-time monitoring and alerting through integrated Telegram notifications, enhancing the IT team's responsiveness to network issues.

```
Global:
  scrape_interval: 30s # Set the scrape interval to every 15 seconds. Default is every 1 minute.
#   evaluation_interval: 30s # Evaluate rules every 15 seconds. The default is every 1 minute.
  scrape_timeout: 20s
scrape_configs:
  - job_name: 'mikrotik-snmp'
    scrape_interval: 20s
    scrape_timeout: 20s
    static_configs:
      - targets:
        - 10.0.0.1 #
        - 10.0.0.2 #
        - 10.0.0.3 #
        - 10.0.0.8 #
        - 10.0.0.5 #
        - 10.0.0.7 #
        - 172.17.2.30 #
        - 120.121.1.231
        - 172.19.1.4
    metrics_path: /snmp
    params:
      module: [mikrotik]
    relabel_configs:
      - source_labels: [__address__]
        target_label: __param_target
      - source_labels: [__param_target]
        target_label: instance
      - target_label: __address__
        replacement: 127.0.0.1:9116

  # the case to use [icmp] module
  # any [job_name]
  - job_name: 'blackbox-icmp-ping'
    scrape_interval: 5s
    metrics_path: /probe
    params:
      module: [icmp]
    static_configs:
      - targets:
        # hostname or IP address of target Host
```

```
      - 1.1.1.1
      - 8.8.8.8
      - detik.com
      - 10.0.0.1
      - 10.0.0.7
      - 10.0.0.2 #
      - 10.0.0.3 #
      - 10.0.0.8 #
      - 10.0.0.5 #
      - 172.17.2.30 #
      - 120.121.1.232
      - 172.19.1.4

    relabel_configs:
      - source_labels: [__address__]
        target_label: __param_target
      - source_labels: [__param_target]
        target_label: instance
      - target_label: __address__
        # Blackbox exporter Host:Port
        replacement: 127.0.0.1:9115


  - job_name: 'node-exporter'
    static_configs:
      - targets:
        - 10.99.99.2:9100
```

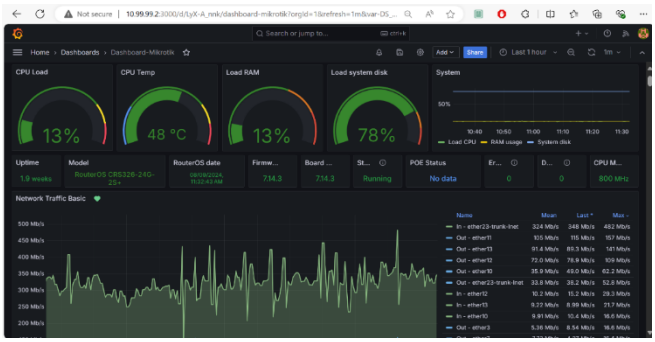

Fig. 5. Mikrotik Monitoring Dashboard Display

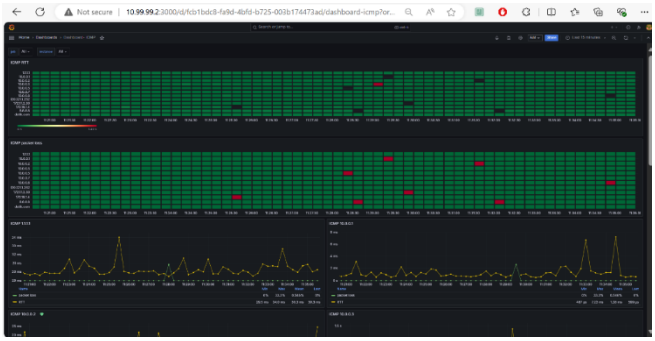

Fig. 6. ICMP Monitoring Dashboard Display

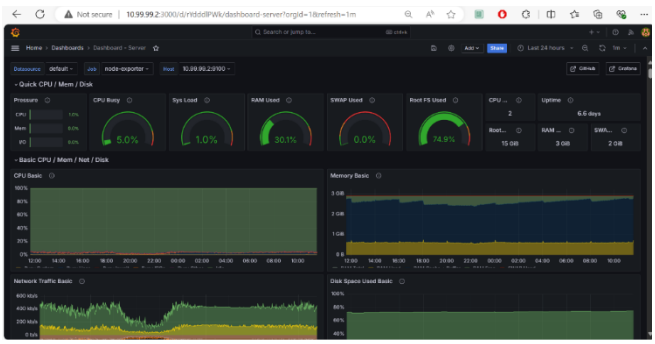

Fig. 7. Server Monitoring Dashboard Display

The monitoring system implemented at PT. Nata Digital Solution demonstrated significant improvements in network performance visibility using Prometheus and Grafana. The Mikrotik monitoring dashboard (Figure 5) provided real-time insights into key metrics such as CPU load, temperature, RAM usage, and system disk usage, with additional details on network traffic across various interfaces. The ICMP monitoring dashboard (Figure 6) effectively tracked metrics like ICMP RTT and packet loss for multiple targets, offering a clear visual representation of network stability and performance over time. Similarly, the server monitoring dashboard (Figure 7) displayed vital system metrics, including CPU, memory, and disk usage, allowing for comprehensive monitoring of server health and performance across different time intervals. The integration of these monitoring dashboards enabled a holistic view of the network's operational status, facilitating quicker identification and resolution of performance bottlenecks.

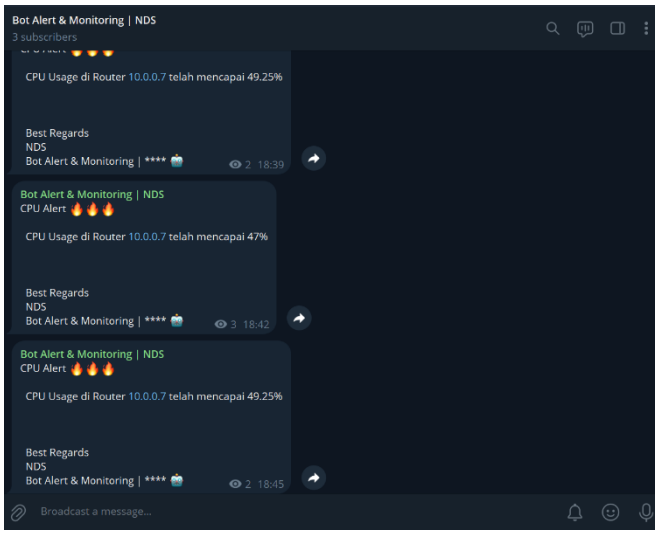

Fig. 8. Bot Alert Notification Display to Telegram Channel

The results align with previous studies highlighting the effectiveness of Prometheus and Grafana for network monitoring and management. Similar to findings by Darmawan [2], the system's use of customisable Grafana dashboards enhanced visibility and flexibility in monitoring various performance indicators, which is crucial for proactive network management. The deployment of Prometheus exporters, as Iqromullah et al. [3] notedClick or tap here to enter text., such as Node, SNMP, and Blackbox Exporters, allowed the system to capture a wide range of metrics from different sources, enhancing the depth and accuracy of monitoring. Furthermore, the integration of Telegram for real-time alerts (Figure 8) mirrored the approach discussed in Rahman & Amnur [1], emphasising the importance of timely notifications in maintaining network performance and reducing downtime through prompt responses to alerts.

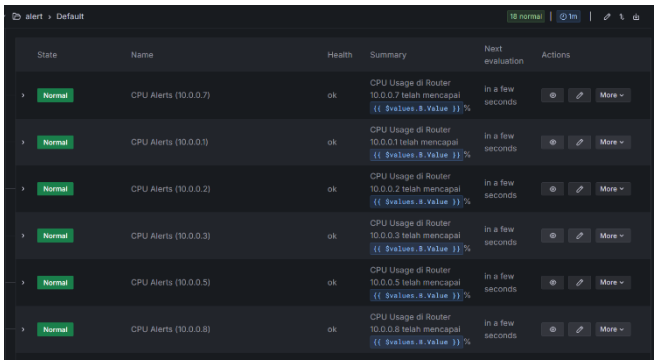

Fig. 9. CPU Alert Rule Display

The findings underscore the critical role of comprehensive monitoring systems in maintaining optimal network performance and reliability. By providing real-time data visualisation and alerting, the implemented system significantly enhanced the IT team's ability to manage and maintain the network infrastructure at PT. Nata Digital Solution. The deployment of CPU alert rules (Figure 9) exemplified the system's proactive approach to network management, where the IT team was promptly alerted via Telegram notifications (Figure 8) when CPU usage exceeded predefined thresholds. This capability reduced response times and minimised potential disruptions by allowing for immediate corrective actions. The practical application of this system demonstrates its potential to serve as a model for other organisations seeking to enhance their network monitoring capabilities using open-source tools, ultimately contributing to better operational efficiency and reduced operational risks in complex network environments.

IV. CONCLUSION

The implementation of a network monitoring system using Prometheus and Grafana at PT. Nata Digital Solution has proven to be effective in enhancing the visibility and management of network performance. By integrating Prometheus for data collection and Grafana for data visualisation, along with exporters such as Node, SNMP, and Blackbox, the system comprehensively monitors critical metrics, including CPU load, memory usage, disk space, and network traffic. The real-time alerting capabilities, integrated with Telegram, further enabled the IT team to respond swiftly to network issues, thereby minimising downtime and improving overall network reliability.

This study demonstrates the practical benefits of using open-source tools for network monitoring, offering a scalable and cost-effective solution that can be tailored to the organisation's specific needs. The deployment facilitated proactive management of network resources and served as a model for other organisations seeking to enhance their monitoring capabilities. Future research could explore integrating additional data sources and advanced analytics to refine the system's capabilities, ensuring even greater operational efficiency and resilience in network management.

REFERENCES

[1] D. Rahman, H. Amnur, and I. Rahmayuni, “Monitoring Server dengan Prometheus dan Grafana serta Notifikasi Telegram,” *Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 1, no. 4, pp. 133–138, 2020, [Online]. Available: http://jurnal-itsi.org

[2] R. T. Darmawan, “Implementasi Grafana untuk Auto-Scaling pada NGINX Web-Server di Lingkungan Docker Container,” *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 7, no. 7, pp. 3163–3167, 2023, [Online]. Available: http://j-ptiik.ub.ac.id

[3] R. Iqromullah, Khairil, and E. Suryana, “Security System Implementation And Monitoring Networks At Sma N 10 City Of Bengkulu,” *Jurnal Media Computer Science*, vol. 2, no. 2, pp. 153–168, 2023.

[4] S. Dwiyatno, E. Rachmat, A. P. Sari, and O. Gustiawan, “Implementasi virtualisasi server berbasis docker container,” *PROSISKO: Jurnal Pengembangan Riset Dan Observasi Sistem Komputer*, vol. 7, no. 2, pp. 165–175, 2020.

[5] M. Z. Amirudin, R. Fahmi, E. Utami, M. S. Mustafa, and others, “Evaluasi Penggunaan Prometheus dan Grafana Untuk Monitoring Database Mongodb,” *Jurnal Informatika Polinema*, vol. 7, no. 2, pp. 43–50, 2021.

[6] R. Rahman, S. T. Agusriani, and R. Rina, “Meningkatkan Efisiensi Pengembangan Perangkat Lunak Melalui Transparansi dan Kolaborasi dengan Ubuntu,” *JURNAL PENELITIAN SISTEM INFORMASI (JPSI)*, vol. 2, no. 3, pp. 94–100, 2024.

[7] M. Y. E. Saputra, S. N. Arief, V. N. Wijayaningrum, Y. W. Syaifudin, and others, “Real-Time Server Monitoring and Notification System with Prometheus, Grafana, and Telegram Integration,” in *2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS)*, 2024, pp. 1808–1813.

[8] R. M. Febriana, “Implementasi Sistem Monitoring Menggunakan Prometheus Dan Grafana,” *Semin. Nas. Telekomun dan Inform*, vol. 13, pp. 164–169, 2020.

[9] A. Lubis and I. Sumartono, “Implementasi Layanan Akademik Berbasis Chatbot untuk Meningkatkan Interaksi Mahasiswa,” *RESOLUSI: Rekayasa Teknik Informatika dan Informasi*, vol. 3, no. 5, pp. 246–252, 2023.

[10] A. Lubis, I. Iskandar, and R. Septian, “Pengembangan Aplikasi Troubleshooting Jaringan Melalui Sistem Notifikasi dengan Integrasi Cacti dan Telegram,” *Brahmana: Jurnal Penerapan Kecerdasan Buatan*, vol. 4, no. 1A, pp. 104–109, 2022.

[11] M. Chakraborty and A. P. Kundan, “Grafana,” in *Monitoring cloud-native applications: Lead agile operations confidently using open source software*, Springer, 2021, pp. 187–240.

[12] W. W. Eckerson, *Performance dashboards: measuring, monitoring, and managing your business*. John Wiley & Sons, 2010.

[13] L. Chen, M. Xian, and J. Liu, “Monitoring system of openstack cloud platform based on prometheus,” in *2020 International Conference on Computer Vision, Image and Deep Learning (CVIDL)*, 2020, pp. 206–209.

[14] A. Lubis, I. Sumartono, and S. Lubis, “Panduan Praktis Pembangunan chatbot Interaktif dengan amazon Lex,” 2023.

[15] A. Lubis, I. Iskandar, R. S. Hardinata, and S. Lubis, “Design Thinking Approach in Building a Chatbot for Troubleshooting and Handling Disruption Complaints in Network Services,” in *International Conference on Sciences Development and Technology*, 2022, pp. 289–295.

[16] Akhyar. Iskandar. S. R. Lubis, *Membangun Server Monitoring Jaringan dengan Raspberry Pi . Panduan Implementasi dan Konfigurasi menggunakan Cacti*. Stindo Press, 2023.