ZABBIX IDS SYSTEM DESIGN WITH PUSH NOTIFICATION BASED ON TELEGRAM BOT

Ahmad, Jakarta State Polytechnic

***Abstract*— Many companies have used servers for their company operations. As the company grows, the servers used are also increasing and increasing. So it is necessary to maintain and monitor the performance on the server and the need for information about server performance. Intrusion Detection System is one system to determine the performance on the server. In this study, the Zabbix IDS system was used with notifications using telegram bots, and testing was carried out whether notifications could be received if there was an intrusion on the server. The result of the test is that zabbix monitors the server in real time and sends notifications if there is an intrusion on the server.**

***Index Terms*— Zabbix, Telegram Notification, Monitoring server**

I. INTRODUCTION

NICT UIN Syarif Hidayatullah Jakarta, as one of the unstructured organizations, is responsible for implementing, developing and improving service performance in the field of information and communication technology. As a means of supporting education, NICT UIN Syarif Hidayatullah Jakarta will also carry out the function of training and expertise in the field of information and communication technology, so that it becomes the data service center of UIN Syarif Hidayatullah for the academic community. In relation to inventory maintenance, server equipment must be maintained as one of the assets assigned by the Ministry of Information and Communication (Kominfo) to NICT UIN Syarif Hidayatullah Jakarta.

II. LITERARY REVIEW

2.1.1. Monitoring

Monitoring is an element that can be implemented on network/server devices. This activity is usually carried out periodically to check the availability and performance status of each node. The monitoring system will automatically notify the responsible administrator when there are problems or unavailability of some resources. In some cases it is possible to actively manage the network/server using a monitoring system. (Sulasno & Saleh, 2020)

Server monitoring system is an important and necessary aspect for a datacenter. With a centralized server monitoring system, one system Administrator can know the condition of all servers without the need to run one remote process at a time each server to check the status of all servers in the data center.

Ideally a monitoring system, both free or paid, There are functions to monitor Disk capacity, memory usage, CPU usage, and services running on the server. (Yanto & Ruswanda, 2017)

2.1.2. IDS

Intrusion detection system (Intrusion Detection System) is a system that can detect attacks and threats that arise on computer networks that are connected to both local networks and the internet.

IDS provides early warning to network administrators in case of suspicious activity (abnormalities) on the computer network. In addition to providing early warning, IDS can also track and identify types of activities that harm computer network systems. (Dar & Harahap, 2018)

2.1.3. Zabbix

Zabbix is a highly effective zabbix network monitoring technology and monitoring system. Zabbix is an open source product that is available and easy to get. In addition, Zabbix has notification alerts that distinguish it from other monitoring applications. Zabbix monitoring agent can also be used to monitor or monitor the network, either monitoring network hardware or on servers or applications.

This paragraph of the first footnote will contain the date on which you submitted your paper for review, which is populated by IEEE. It is IEEE style to display support information, including sponsor and financial support acknowledgment, here and not in an acknowledgment section at the end of the article. For example, "This work was supported in part by the U.S. Department of Commerce under Grant BS123456." The name of the corresponding author appears after the financial information, e.g. *(Corresponding author: M. Smith).* Here you may also indicate if authors contributed equally or if there are co-first authors.

The next few paragraphs should contain the authors' current affiliations, including current address and e-mail. For example, First A. Author is with the National Institute of Standards and Technology, Boulder, CO 80305 USA (e-mail: author@ boulder.nist.gov).

Second B. Author, Jr., was with Rice University, Houston, TX 77005 USA. He is now with the Department of Physics, Colorado State University, Fort Collins, CO 80523 USA (e-mail: author@lamar.colostate.edu).

Third C. Author is with the Electrical Engineering Department, University of Colorado, Boulder, CO 80309 USA, on leave from the National Research Institute for Metals, Tsukuba 305-0047, Japan (e-mail: author@nrim.go.jp).

Mentions of supplemental materials and animal/human rights statements can be included here.

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org

With the Zabbix monitoring system, it can save human resources. Due to the system the company can use many servers and systems at the same time and with little administrator supervision. (Prasetyo & , 2021)

2.1.4. Servers

A server is a computer system that provides certain types of services on a computer network. Servers are supported by scalable processors and large amounts of RAM, and also have a dedicated operating system. This operating system is different from the usual operating system. Ordinary computers use the Windows operating system, Mac OS, etc., this server operating system may be different.

The server also runs management software that controls access to the network and its resources (such as files and printers) and provides access to network member workstations. (Hafid, et al., 2019)

2.1.5. Proxmox

Proxmox VE is a complete open source server management platform for enterprise virtualization. It tightly integrates the KVM hypervisor and Linux Containers (LXC), software-defined storage and network functionality, on a single platform. With the integrated web-based user interface, you can easily manage VMs and containers, high availability for clusters, or integrated disaster recovery tools. (Proxmox, 2022)

Proxmox VE is an open source comprehensive enterprise virtualization platform that fully integrates the KVM hypervisor and LXC containers, software-defined storage and networking capabilities into a single platform for high availability clusters and disaster recovery. (Siregar, 2020)

.1.6. Telegram bots

Bots are third-party applications that can be run inside Telegram. Users can send messages, commands, and inline requests. We can control bots using HTTPS to telegram API.

The uses of telegram bots according to (Mulyanto, 2020) include:

• The bot can be used as a smart newspaper that will provide news to the bot's subscribers.
• The bot can also be used as a bridge to other services such as Gmail, Images, GIF, IMDB, Wiki, Music, Youtube, GitHub.
• Bots can also be used to receive payments from Telegram users. Bots can offer paid services or work as virtual storefronts.
• Bots can also be used as special tools for example providing alerts, weather forecasts, translations, formatting, or other services.
• Bots can also be used as a single-player or multi-player game.
• Bots can be used as a social service that connects people who are looking for conversation partners based on similar interests or affinities.

Bots or robots are typically used to automate repetitive activities and can be used by administrators as monitoring tools.

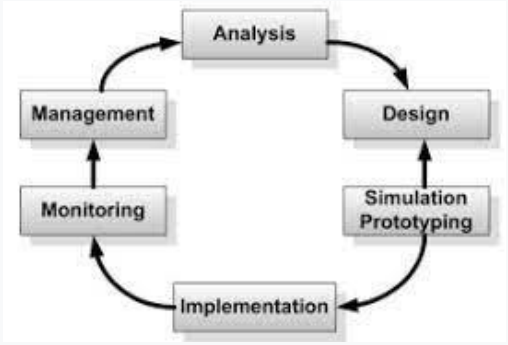
2.1.7. Bash

Bash Shell programming is programming a set of commands using scripts written in the Bash shell, so that later they can be run by the operating system. Apart from the Bash shell, there are many other shells you can use for programming, but using Bash is more flexible because the scripts written are more compatible to be read from different machines, different Linux or even different operating systems. (Maizi & Maizi, 2019)

The Bash shell uses standard posix as a specification of how features are implemented and basically bash implements grammar, parameters, variables, redirection , and quoting as it uses in the Bourne shell. On the GNU/Linux operating system, using Bash is the operating system's default shell program, although there are many other shell programs such as the Korn shell (ksh), C shell (csh). (Alfiandi, et al., 2020)

III. METHODOLOGY

A The research stages of this thesis use the Network Development Life Cycle (NDLC) methodology.



1. Analysis

This stage performs needs analysis, user analysis, and server analysis. In several ways, such as: field surveys and documentation for design materials.

2. Design

At this stage, it is necessary to design a system and server based on the results of the analysis that has been carried out, as well as an estimate of the costs that will be needed in conducting research.

3. Simulation Prototyping

Perform simulations using third-party applications to monitor possible errors and be able to assess the effectiveness of the system to be made.

4. Implementation

At this stage the data that has been collected and designed will be implemented in real terms.

5. Monitoring

At this stage, observations will be made on everything that has been implemented. Here are some that will be observed, namely:

a. Zabbix is doing well
b. New feature of bash on Zabbix can run and connect to servers that Zabbix monitors
c. Doing documentation

6. Management

In the following stage, management is carried out on users such as policies that can be used

C. Object of Research

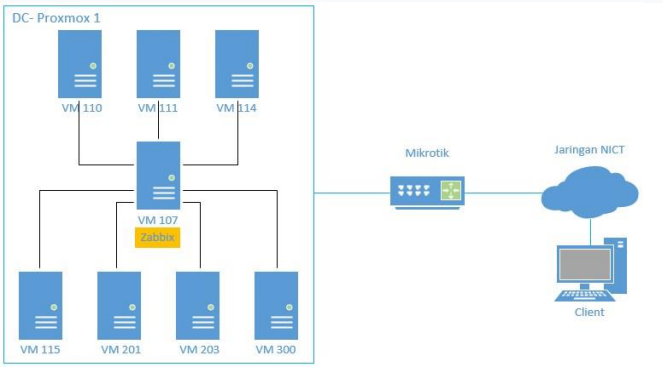
The object of research is a scientific target aimed at obtaining data and knowing what, who, when and where the research is carried out. The focus of this research is the result of testing Zabbix as a monitoring system and also new features of bash that can make monitoring servers easier. Which will later be compared with research related to the existing Zabbix monitoring system.

IV. DISCUSSIONS

A. Requirements Analysis

In the monitoring system on the proxmox server, the Zabbix application is used to implement a monitoring system on several

virtual machines. The monitoring system method is by adding a virtual machine as a Zabbix server that will monitor other virtual machines. Then the virtual machine that will be monitored is installed by the Zabbix agent, so that the virtual machine can be detected by Zabbix. Configuring the telegram bot is also done on Zabbix as a notification that will be sent if an intrusion occurs on one of the virtual machines. Bash scripts are also configured on Zabbix to monitor virtual machines. Bash script is used to monitor the history of commands on the server that have been carried out, so the user can monitor what commands are used and have data on the time and date the command was carried out.



Monitoring System Block Diagram on Proxmox Server

C. System Implementation

The realization of the monitoring system on the proxmox server is divided into several processes, namely Zabbix server installation, Zabbix agent installation, Zabbix web configuration, telegram bot configuration, and bash script configuration.

D. Data Analyze

The results of the first scenario testing conducted with the Zabbix agent. Testing is done by stopping the Zabbix agent service and restarting the service 4 times. And the calculation of the comparison of the notification time sent by the telegram bot is carried out. Here is the data from the test results

Below is the values of all test

Pengujian	Problem (Menit)	Resolved (Menit)
Notifikasi Bot Telegram 1	3 Menit	1 Menit
Notifikasi Bot Telegram 2	3 Menit	25 Detik
Notifikasi Bot Telegram 3	3 Menit	25 Detik
Notifikasi Bot Telegram 4	3 Menit	1 Menit 22 Detik

Based on the data in the table above, in the first test the telegram bot sent a problem notification within 3 minutes and sent a resolved time within 1 minute. In both tests the bot sent a problem notification within 3 minutes and sent a resolved notification within 25 seconds.

In the third test the bot sent a problem notification within 3 minutes and sent a resolved notification within 25 seconds. In the fourth test, the bot sent a problem notification within 3 minutes and sent a resolved notification within 1 minute 22 seconds.

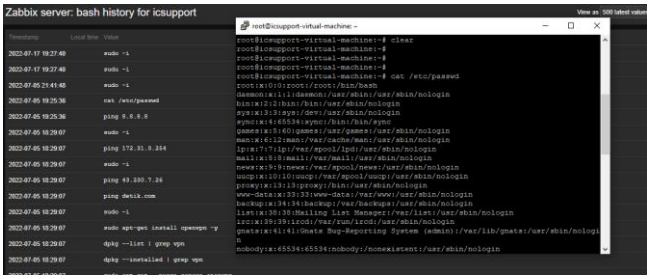


Figure 4. 31 First Test Results Command “cat /etc/passwd”

Figure 4.31 shows the results of the first test with the command "cat /etc/passwd". The results show that when the "cat /etc/passwd" command is executed, the log is read by the bash history in Zabbix web in the latest data menu. Included the date and time of use of the command.

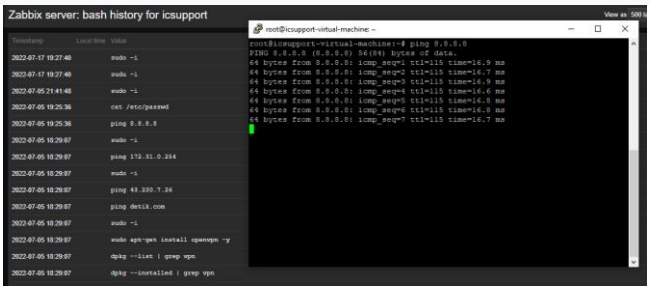


Figure 4. 32 Test Results of the Second Command "ping 8.8.8.8"

Based on the results of this comparison, the telegram bot sends problem notifications for 3 minutes during all stages of testing the Zabbix agent service is stopped. And sending notifications resolved in different times, between 25 seconds to 1 minute. Therefore, it can be concluded that the Telegram Bot notification system can run and function properly.

shows the results of testing several commands performed. In the first test, running the command "cat /etc/passwd" on the client host and the result was that the command was detected in the Bash history log in the Zabbix web latest data menu. In the second test, run the command "ping 8.8.8.8" on the client host. When the command is executed, it is detected in the bash history log in the Zabbix web latest data menu. The third test is to run the command "apt-get install openvpn -y" when the command is run, bash history successfully detects the command and enters the bash history log. In the fourth test, running the command "ping detik.com" when the command was run, bash history also managed to detect the command and enter the latest data log.

REFERENCES

[1] Alfiandi, T., Diansyah, T. & Liza, R., 2020. ANALISIS PERBANDINGAN MANAJEMEN KONFIGURASI MENGGUNAKAN ANSIBLE DAN SHELL SCRIPT PADA CLOUD SERVER DEPLOYMENT AWS. Volume 8, pp. 78-84.

A., S. & Hafid, A., 2019. OPTIMALISASI SUMBER DAYA KOMPUTER DENGAN VIRTUALISASI SERVER MENGGUNAKAN PROXMOX VE. Volume 9, pp. 369-376.

Aziz, F. I. & Ritzkal, B. A., 2018. Sistem Monitoring Jaringan Dan Optimalisasi Manajemen Bandwith Dengan Algoritma HTB(Hierarchical Token Bucket) Pada Zabbix Dengan Notifikasi SMS Gateway Dan Email (Studi Kasus Dinas Komunikasi Dan Informatika Kab.

Dar, M. H. & Harahap, S. Z., 2018. IMPLEMENTASI SNORT INTRUSION DETECTION SYSTEM(IDS)PADA SISTEM JARINGAN KOMPUTER. Volume 6, pp. 1-10.

Hamzah, A., Ismail, S. J. R. & Meis, L., 2019. Implementasi Sistem Monitoring Jaringan Menggunakan Zabbix dan Web Web Application Firewall di PT PLN (Persero) Transmisi Jawa Bagian Tengah..

Husna, M. A. & Rosyani, P., 2021. Implementasi Sistem Monitoring Jaringan dan Server Menggunakan Zabbix yang Terintegrasi dengan Grafana dan Telegram.

Mulyanto, A. D., 2020. Pemanfaatan Bot Telegram Untuk Media Informasi Penelitian. *MATICS*, Volume 12, pp. 49-54.

N. & Maizi, Z., 2019. PEMBUATAN PETA JARINGAN UNTUK MEMONITORING KONEKSI KOMPUTER MENGGUNAKAN PEMROGRAMAN BASH SCRIPT. Volume 5, pp. 164-174.

Nugraha, B. P. & Ratamaa, N., 2022. Implementasi Network Dan Server Monitoring Menggunakan Zabbix Berbasis Linux Integrasi Realtime Notifikasi Telegram di PT. Arsen Kusuma Indonesia.

P., 2022. *Proxmox.* [Online]
Available at: https://www.proxmox.com/en/proxmox-ve
[Accessed 26 Februari 2022].

Prasetyo, S. E. & H., 2021. Analısıs Dan Perancangan Monıtorıng Dan Notıfikası System Web Applıcatıon Fırewall Menggunakan Zabbıx. Volume 1, pp. 1-9.

Siregar, S. R., 2020. Efesiensi Fisik Komputer Serverdengan Menerapkan Proxmox Virtual Environment. *Journal of Computer System and Informatics* , Volume 1, pp. 83-87.

Situmorang, A. P., Wati, T. & A., 2022. Analisis Perbandingan Sistem Monitoring Jaringan Berbasis Web Menggunakan NTOPNG dan Zabbix di SMPN 1 Tamansari.

Sulasno, S. & Saleh, R., 2020. Monitoring merupakan elemen yang dapat diimplementasikan ke perangkat. *JUITA: Jurnal Informatika,* Volume 8, pp. 1-10.

Wijonarko, D., 2017. Zabbix Network Monitoring sebagai Perangkat Monitoring Jaringan Di SKPD Kota Malang.

Yanto, J. & Ruswanda, M., 2017. IMPLEMENTASI SISTEM MONITORING SERVER MENGGUNAKAN NAGIOS. pp. 1-10.