

Design and Build a Network Monitoring System Using Nagios at PT. Telkom Access


Muhammad Tri Madja Pandia¹, Fachrid Wadly²

^{1,2}Universitas Pembangunan Panca Budi

ABSTRACT

The implementation of an effective network monitoring system is very important for companies to maintain service performance and availability. This research aims to design and implement a network monitoring system using Nagios at PT. Telkom Access. The research methodology includes direct observation, interviews with related parties, and literature studies. The results of the study show that the implementation of Nagios in PT. Telkom Access enables real-time monitoring of network devices and servers, provides early notifications of potential problems, and facilitates rapid response to disruptions. The system is integrated with the Ubuntu Server 22.04 operating system and utilizes the Nagios plugin to monitor various performance parameters. In conclusion, Nagios provides reliable and effective solutions to increase service availability, optimize network performance, and ensure customer satisfaction at PT. Telkom Access.

Keyword : Nagios, Network Monitoring, Ubuntu Server, Nagios Plugin, PT. Telkom Access

 This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

Corresponding Author:

Muhammad Tri Madja Pandia,
Universitas Pembangunan Panca Budi
Jl. Gatot Subroto KM. 4.5 20122, Medan
Email : trimajapandia@gmail.com

Article history:

Received Jan 20, 2025
Revised Jan 27, 2025
Accepted Feb 04, 2025

1. INTRODUCTION (10 PT)

In the all-connected digital era, the availability and performance of computer networks are crucial for the continuity of company operations. Especially for telecommunication service providers such as PT. Telkom Akses, a reliable and stable network is the main backbone in providing quality services to customers (Sutiman & Gunawan, 2021). Network disruptions or downtime can have a significant impact, ranging from inhibited internal communications, disconnected customer service, to large financial losses. Therefore, it is important for PT. Telkom Access to have a sophisticated and responsive network monitoring system (Rizkiana et al., 2018).

Network monitoring systems allow real-time monitoring of various components of network infrastructure, such as servers, routers, switches, firewalls, and so on. With continuous monitoring, network administrators can quickly detect potential problems, analyze the root cause of the outage, and take preventive action before a broader impact occurs. The information obtained from the monitoring system can also be used to optimize network performance, improve efficiency, and plan future infrastructure development (Prayogo et al., 2012).

Nagios, as one of the popular open-source network monitoring software, offers a comprehensive solution for monitoring network health and performance (Shidhani et al., 2016). Nagios' superior features, such as real-time monitoring, flexible notification system, intuitive data visualization, and integration capabilities with various platforms, make it the right choice for PT. Telkom Access. With the implementation of Nagios, it is hoped that PT. Telkom Access can increase visibility into its network conditions, speed up response times to disruptions, and minimize negative impacts (Nugroho et al., 2018).

This research focuses on the design and development of a network monitoring system using Nagios in the environment of PT. Telkom Access. The research stages include needs analysis, system design, implementation, and testing. The results of this study are expected to provide an effective and efficient network monitoring solution for PT. Telkom Access, so that it can ensure service availability, increase customer satisfaction, and support the company's business growth. In addition, this research is also expected to contribute to the development of science and technology in the field of network monitoring.

2. LITERATURE REVIEW

Previous research related to the implementation of network monitoring systems has been carried out by several researchers. The study shows that the use of network monitoring software such as The Dude and OpenNMS can assist network administrators in monitoring network infrastructure in real-time, detecting potential problems, and improving network management efficiency (Elhaq et al., 2021) (Nugroho et al., 2018).

For example, research conducted by (Elhaq et al., 2021) shows that the implementation of The Dude as a network monitoring system in the Mikrotik environment can help network administrators to detect network problems or disturbances earlier and make it easier to solve them. In addition, other research reveals that the use of OpenNMS to monitor the performance of network devices can provide an overview of the response time of each running service as well as SNMP data to monitor device quality (Nugroho et al., 2018).

Meanwhile, research conducted by (Prayogo et al., 2012) revealed that a network monitoring system with notifications through SMS Gateway is able to assist network administrators in monitoring anytime and anywhere, so that it can maintain network stability and reduce downtime (Elhaq et al., 2021).

Types of Computer Networks

Computer networks can be classified based on various criteria, such as geographic reach, topology, and architecture. Here are some commonly used types of computer networks:

- **Personal Area Network:** A network that connects devices in close proximity, such as *smartphones, laptops, and printers*. Examples are Bluetooth and Wi-Fi Direct connections.
- **Local Area Network:** A network that connects computers and other devices within a confined area, such as a building or campus. LANs are typically used to share resources, such as *printers and file servers*.
- **Metropolitan Area Network:** A network that covers a larger geographic area than a LAN, such as a city. MAN is often used by large organizations or local governments.
- **Wide Area Network:** A network that covers a very large geographic area, such as a country or continent. The Internet is the most well-known example of a WAN.
- **Virtual Private Network:** A network that allows users to connect to a private network through a public network, such as the internet. VPNs are used to improve the security and privacy of data communications.

Computer Network Hardware

Some of the important hardware commonly used in building and managing computer networks include:

- **Router:** It serves to connect two or more networks, forward data packets between networks, and determine the best path for data to reach its destination. Routers are an important component in a network, especially for connecting a LAN to the internet.
- **Switch:** Functions to connect multiple devices in one LAN and forward data only to the destination device. Switches are more efficient than hubs because they reduce unnecessary data traffic.
- **Hub:** Serves as a central point of connection for devices within the LAN. The hub broadcasts the received data to all connected devices, making it less efficient than a switch. Nowadays, the use of hubs is getting less and less frequent.
- **Network Interface Card:** A card that is attached to a computer or other device to connect it to a network. NICs provide a physical interface for network connections, either via cable or wireless.
- **Modem:** It serves to modulate and demodulate the signal, thus allowing the computer to connect to the internet via telephone lines, cables, or fiber optics.
- **Cable/Connector:** Cables and connectors are used to physically connect network devices. The type of cable and connector used depends on the type of network and the standard applied. Examples are UTP cables, fiber optic cables, and RJ-45 connectors.
- **Firewall:** A hardware or software that serves to protect a network from unauthorized access. Firewalls can be specialized hardware or implemented as software on servers or *routers*.

- **Server:** A computer that provides services to other computers in the network, such as a *file server*, *print server*, or *web server*.
- **Access Point:** A device that allows wireless devices to connect to a wired network. Access points serve as a bridge between wireless networks and cable networks.

These hardware devices work together to form a reliable and efficient network infrastructure. Choosing the right hardware is essential to ensure network performance and security.

Nagios Monitoring Application

Nagios is an *open-source* system and network monitoring software. Nagios allows administrators to monitor their IT infrastructure, including servers, applications, services, and network devices, to ensure everything is functioning properly. Here are some Nagios monitoring applications:

- **Server Monitoring:** Nagios can monitor various server parameters, such as CPU usage, memory usage, disk space, temperature, and service status. This allows administrators to identify potential issues before they impact server performance.
- **Network Monitoring:** Nagios can monitor network devices such as *routers*, *switches*, and *firewalls*. This monitoring includes connection status, *bandwidth usage*, and *latency*. Nagios can also detect network device failures and provide notifications to administrators.
- **Application Monitoring:** Nagios can monitor the performance of web applications, databases, and other applications. This monitoring includes response time, availability, and resource usage. By monitoring the application, administrators can ensure that the application is running optimally and meeting *the service level agreement*.
- **Service Monitoring:** Nagios can monitor various services, such as email, DNS, and DHCP. This monitoring ensures that these services are available and functioning properly.
- **Notifications and Alerts:** Nagios may send notifications and alerts to administrators via email, SMS, or other methods in the event of a problem or anomaly. These notifications allow administrators to respond quickly to issues and minimize their impact.
- **Reporting and Analytics:** Nagios provides reporting and analytics features that allow administrators to monitor performance trends, identify areas for improvement, and make informed decisions based on data.

With its extensive and flexible capabilities, Nagios is a reliable and effective monitoring solution for various types of IT infrastructure. The implementation of Nagios at PT. Telkom Akses is expected to increase visibility and control over the network, so as to ensure service availability and customer satisfaction

3. RESULTS AND DISCUSSION (10 PT)

Previous research related to the implementation of network monitoring systems has been carried out by several researchers. The study shows that the use of network monitoring software such as The Dude and OpenNMS can assist network administrators in monitoring network infrastructure in real-time, detecting potential problems, and improving network management efficiency (Elhaq et al., 2021) (Nugroho et al., 2018).

For example, research conducted by (Elhaq et al., 2021) shows that the implementation of The Dude as a network monitoring system in the Mikrotik environment can help network administrators to detect network problems or disturbances earlier and make it easier to solve them. In addition, other research reveals that the use of OpenNMS to monitor the performance of network devices can provide an overview of the response time of each running service as well as SNMP data to monitor device quality (Nugroho et al., 2018).

Meanwhile, research conducted by (Prayogo et al., 2012) revealed that a network monitoring system with notifications through SMS Gateway is able to assist network administrators in monitoring anytime and anywhere, so that it can maintain network stability and reduce downtime (Elhaq et al., 2021).

Types of Computer Networks

Computer networks can be classified based on various criteria, such as geographic reach, topology, and architecture. Here are some commonly used types of computer networks:

- **Personal Area Network:** A network that connects devices in close proximity, such as *smartphones, laptops, and printers*. Examples are Bluetooth and Wi-Fi Direct connections.
- **Local Area Network:** A network that connects computers and other devices within a confined area, such as a building or campus. LANs are typically used to share resources, such as *printers and file servers*.
- **Metropolitan Area Network:** A network that covers a larger geographic area than a LAN, such as a city. MAN is often used by large organizations or local governments.
- **Wide Area Network:** A network that covers a very large geographic area, such as a country or continent. The Internet is the most well-known example of a WAN.
- **Virtual Private Network:** A network that allows users to connect to a private network through a public network, such as the internet. VPNs are used to improve the security and privacy of data communications.

Computer Network Hardware

Some of the important hardware commonly used in building and managing computer networks include:

- **Router:** It serves to connect two or more networks, forward data packets between networks, and determine the best path for data to reach its destination. Routers are an important component in a network, especially for connecting a LAN to the internet.
- **Switch:** Functions to connect multiple devices in one LAN and forward data only to the destination device. Switches are more efficient than hubs because they reduce unnecessary data traffic.
- **Hub:** Serves as a central point of connection for devices within the LAN. The hub broadcasts the received data to all connected devices, making it less efficient than a switch. Nowadays, the use of hubs is getting less and less frequent.
- **Network Interface Card:** A card that is attached to a computer or other device to connect it to a network. NICs provide a physical interface for network connections, either via cable or wireless.
- **Modem:** It serves to modulate and demodulate the signal, thus allowing the computer to connect to the internet via telephone lines, cables, or fiber optics.
- **Cable/Connector:** Cables and connectors are used to physically connect network devices. The type of cable and connector used depends on the type of network and the standard applied. Examples are UTP cables, fiber optic cables, and RJ-45 connectors.
- **Firewall:** A hardware or software that serves to protect a network from unauthorized access. Firewalls can be specialized hardware or implemented as software on servers or *routers*.
- **Server:** A computer that provides services to other computers in the network, such as a *file server, print server, or web server*.
- **Access Point:** A device that allows wireless devices to connect to a wired network. Access points serve as a bridge between wireless networks and cable networks.

These hardware devices work together to form a reliable and efficient network infrastructure. Choosing the right hardware is essential to ensure network performance and security.

Nagios Monitoring Application

Nagios is an *open-source* system and network monitoring software. Nagios allows administrators to monitor their IT infrastructure, including servers, applications, services, and network devices, to ensure everything is functioning properly. Here are some Nagios monitoring applications:

- **Server Monitoring:** Nagios can monitor various server parameters, such as CPU usage, memory usage, disk space, temperature, and service status. This allows administrators to identify potential issues before they impact server performance.
- **Network Monitoring:** Nagios can monitor network devices such as *routers, switches, and firewalls*. This monitoring includes connection status, *bandwidth usage, and latency*. Nagios can also detect network device failures and provide notifications to administrators.
- **Application Monitoring:** Nagios can monitor the performance of web applications, databases, and other applications. This monitoring includes response time, availability, and resource usage. By monitoring the application, administrators can ensure that the application is running optimally and meeting *the service level agreement*.

- **Service Monitoring:** Nagios can monitor various services, such as email, DNS, and DHCP. This monitoring ensures that these services are available and functioning properly.
- **Notifications and Alerts:** Nagios may send notifications and alerts to administrators via email, SMS, or other methods in the event of a problem or anomaly. These notifications allow administrators to respond quickly to issues and minimize their impact.
- **Reporting and Analytics:** Nagios provides reporting and analytics features that allow administrators to monitor performance trends, identify areas for improvement, and make informed decisions based on data.

With its extensive and flexible capabilities, Nagios is a reliable and effective monitoring solution for various types of IT infrastructure. The implementation of Nagios at PT. Telkom Akses is expected to increase visibility and control over the network, so as to ensure service availability and customer satisfaction.

Method

In this study, the methodology used is as follows:

Research Analysis

To build a network monitoring server at PT. Telkom Access with Nagios, required:

- **Hardware:** A server PC that is sufficient to run Ubuntu Server and Nagios applications. Hardware specifications need to be adjusted to the workload and the number of devices to be monitored.
- **Operating System:** Ubuntu Server as a platform for Nagios.
- **Software:**
 - Nagios Core as the main monitoring application.
 - Nagios plugins needed to monitor specific services and devices.
- **Dashboard:** A *dashboard* for visualization of monitoring data. Instead of NagVis (which has been removed on demand), consider using Nagios' built-in web interface or another compatible dashboard solution, such as Grafana.
-

Design

The implementation of Nagios at PT. Telkom Access will not change the existing network design. The Nagios server will be added to the network and configured to monitor the required devices and services. The IP Address for the monitoring server will be determined during the installation of Ubuntu Server.

Testing

The success of Nagios implementation depends on several factors, including:

- **Infrastructure and Hardware:** Server and network performance must be adequate to support Nagios' operations.
- **Software Configuration:** The configuration of Nagios must be done correctly, including the addition of *hosts* to be monitored and the setting of notifications.
- **Access Monitoring:** Nagios must have proper access to the devices and services to be monitored.

Implementation

Nagios implementation steps at PT. Telkom Access:

1. **Ubuntu Server Installation:** Install Ubuntu Server on the provided server PC. Specify a *static* IP address for the monitoring *server* during the installation process.
 2. **Nagios Core Installation:** Install Nagios Core on Ubuntu Server.
 3. **Nagios Plugin Installation:** Install *the* Nagios plugins needed to monitor the desired services and devices.
 4. **Nagios Configuration:** Configure Nagios to monitor predefined *hosts* (network devices and *servers*). This configuration includes settings for the services to be monitored, alert thresholds, and notification methods.
 5. **Dashboard Configuration:** Configure Nagios' built-in web interface or integrate with other *dashboard* solutions for data visualization monitoring.
 6. **Testing:** Conduct thorough testing to ensure that the Nagios is functioning properly and provides accurate monitoring information.
-

With the right implementation, Nagios can help PT. Telkom Access monitors its network infrastructure, improves service availability, and optimizes network performance.

Data Collection Methods

Data Collection Methods at PT. Telkom Access:

- **Observation:** Direct observation was made in the Information Technology Division of PT. Telkom Access to get an overview of the existing network infrastructure. The duration of observation is adjusted to the needs.
- **Interview:** Interviews were conducted with related parties in the Information Technology Division of PT. Telkom Access, such as managers and supervisors, to understand in detail the system that is running, the problems that often occur, as well as the needs and expectations related to the implementation of the monitoring system.
- **Literature Studies:** Literature studies are conducted by gathering information from various sources, such as the internet, journals, and reference books, to support the design and implementation of an effective monitoring system. Literature studies also aim to strengthen the theoretical and practical foundations used.

By using the right method, it is hoped that the data obtained can support the process of designing and implementing a network monitoring system with Nagios at PT. Telkom Access.

4. Results and Illumination

Proposed Network Topology

Based on the background of the existing problem and by implementing a device to do monitoring, it does not change the network topology that is already running.

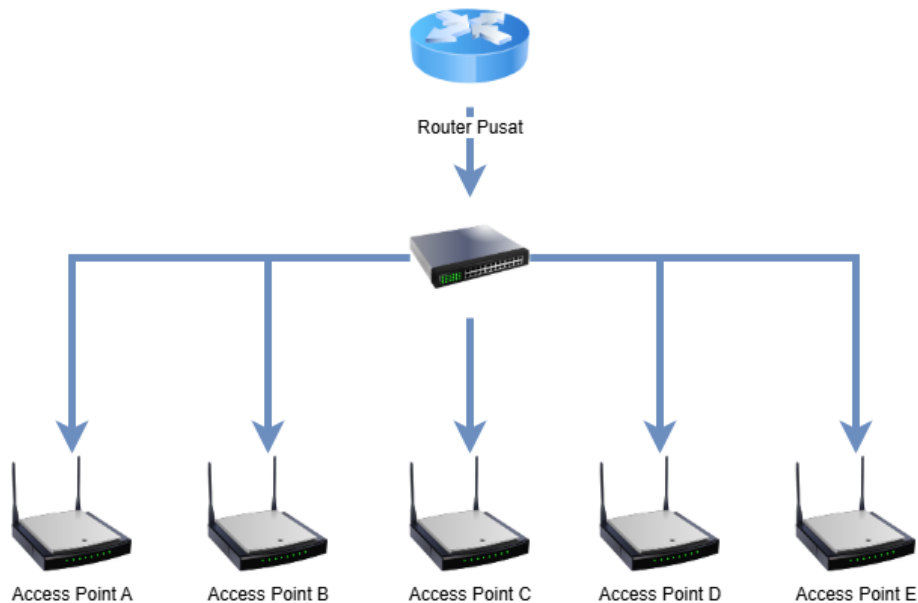


Figure 1. Current network topology

Network Schema

In the proposed network scheme, the author adds a device used to carry out monitoring. The proposed network scheme is as follows:

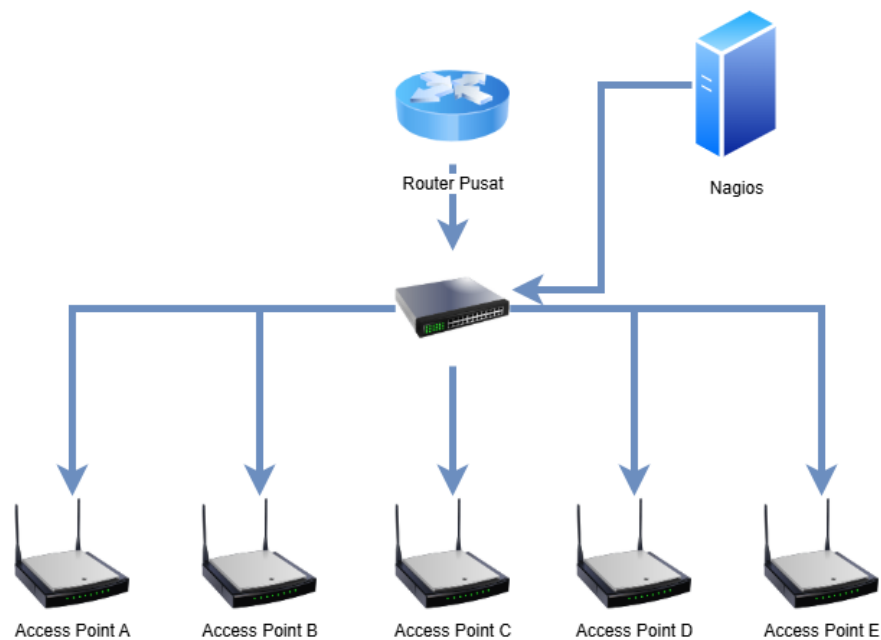


Figure 2. Proposed Network Scheme

Application Design

In building a monitoring system, a server device with an operating system installed is needed. The author uses the Linux operating system Ubuntu Server 22.04 with the Nagios Core 4.5 monitoring system and Nagios Plugin. Nagios cannot run on its own, so it requires elements involved in it such as Apache as a web server and MariaDB database.

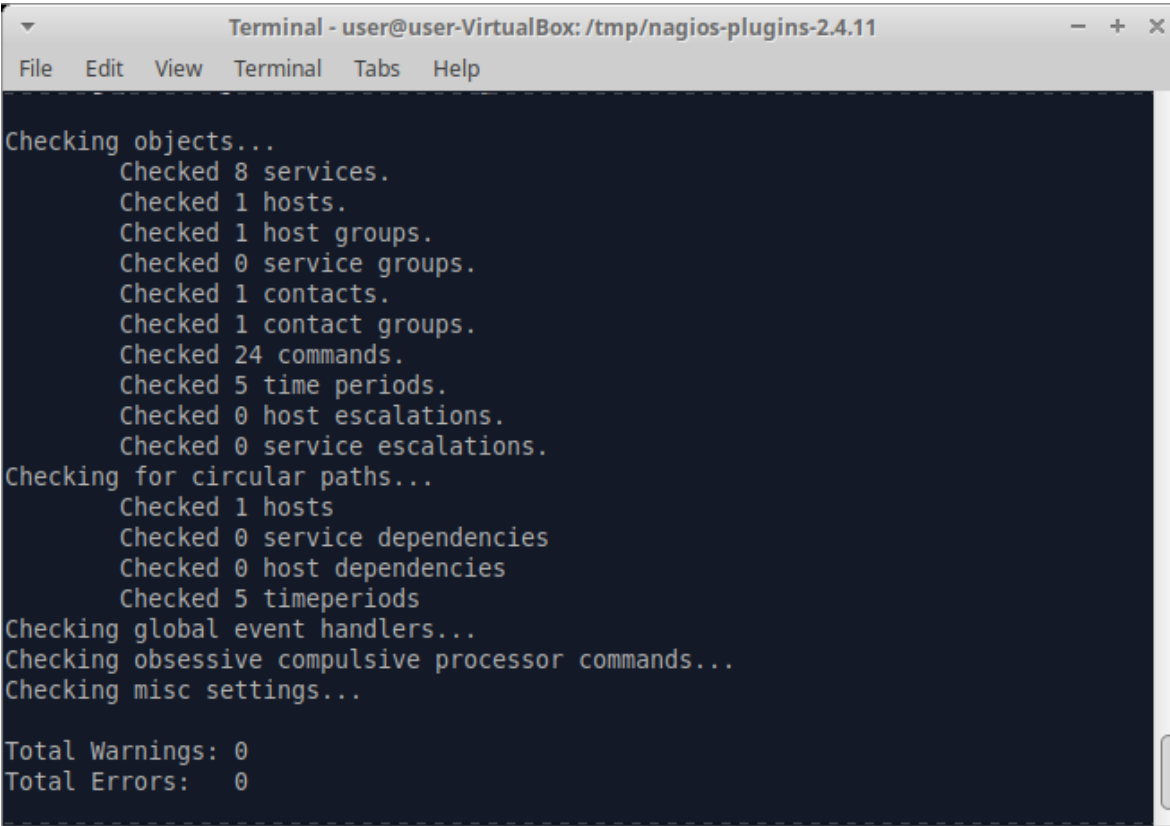
Nagios Installation

For the installation of Nagios Core 4.4, the first step is to download the installation file first and then perform the Nagios installation. Downloading can be done using the following command:

```
sudo apt update & sudo apt upgrade
sudo apt install -y wget build-essential apache2 php openssl perl make
php-gd libgd-dev libapache2-mod-php libperl-dev libssl-dev daemon
autoconf libc6-dev libmcrypt-dev libssl-dev libnet-snmp-perl gettext
unzip
cd /tmp
wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-
4.4.6.tar.gz
sudo useradd nagios
sudo groupadd nagcmd
sudo usermod -a -G nagcmd nagios
tar -xzf nagios-4.4.6.tar.gz
cd nagios-4.4.6
sudo ./configure --with-httpd-conf=/etc/apache2/sites-enabled
sudo make all
sudo make install
sudo make install-init
sudo make install-commandmode
sudo make install-config
```

```
sudo /usr/bin/install -c -m 644 sample-config/httpd.conf
/etc/apache2/sites-enabled/nagios.conf
sudo a2enmod rewrite
sudo a2enmod cgi
sudo systemctl restart apache2
cd /tmp
wget https://nagios-plugins.org/download/nagios-plugins-2.3.3.tar.gz
tar -xzf nagios-plugins-2.3.3.tar.gz
cd nagios-plugins-2.3.3
sudo ./configure --with-nagios-user=nagios --with-nagios-group=nagios --
with-openssl
sudo make
sudo make install
sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
sudo systemctl enable --now nagios.service
sudo systemctl restart apache2.service
```

By now, Nagios should be up and running on your Ubuntu 20.04 server. You can access the Nagios web interface by visiting your server's IP address or hostname in a web browser, followed by `"/nagios"`. From the downloaded Nagios Core file, it can be installed immediately. In this installation stage, a username and password will be added which will later be used to log in to the Nagios application.

A terminal window titled "Terminal - user@user-VirtualBox: /tmp/nagios-plugins-2.4.11" displays the output of the Nagios configuration process. The output shows a series of checks for various components, including services, hosts, groups, contacts, commands, and time periods. The final summary indicates zero warnings and zero errors.

```
Checking objects...
  Checked 8 services.
  Checked 1 hosts.
  Checked 1 host groups.
  Checked 0 service groups.
  Checked 1 contacts.
  Checked 1 contact groups.
  Checked 24 commands.
  Checked 5 time periods.
  Checked 0 host escalations.
  Checked 0 service escalations.
Checking for circular paths...
  Checked 1 hosts
  Checked 0 service dependencies
  Checked 0 host dependencies
  Checked 5 timeperiods
Checking global event handlers...
Checking obsessive compulsive processor commands...
Checking misc settings...

Total Warnings: 0
Total Errors: 0
```

Figure 3. Nagios Configuration

Once the installation process is complete, we can open the browser available to access the Nagios application by typing the IP address, which is `http://10.0.2.15/nagios`, as in the following image:

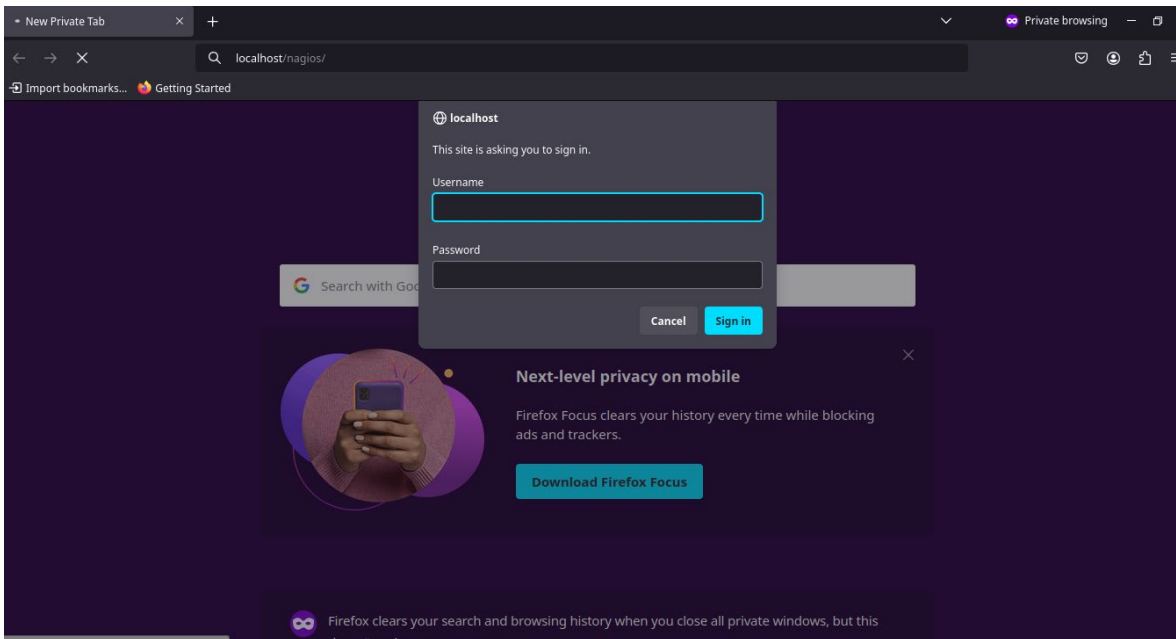
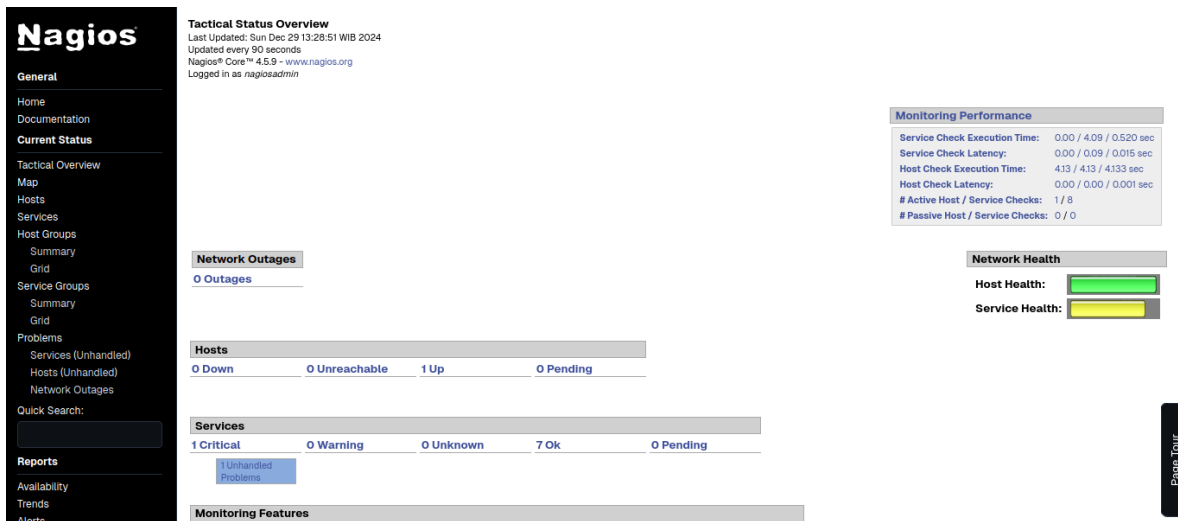


Figure 4. Nagios login

A username and password for the Nagios app have been created during the installation process. After entering the username and password correctly, Nagios is ready to be used for system monitoring. Here is the initial view of the Nagios app.



5. Conclusion

The implementation of Nagios at PT. Telkom Access enables real-time monitoring of network infrastructure, provides early notification of potential problems, and facilitates rapid response to outages. This contributes to increased service availability, optimized network performance, and operational efficiency. The Nagios monitoring system, which is integrated with the Ubuntu Server 22.04 operating system and utilizes the Nagios plugin, provides a reliable and effective solution to monitor the

health and performance of network and server devices in PT. Telkom Access. With proactive monitoring, PT. Telkom Access can minimize downtime, improve service quality, and ensure customer satisfaction.

REFERENCES

- Elhaq, M. K., Solehudin, A., & Juardi, D. (2021). Implementation of The Dude as a Monitoring System with Automatic Notifications Via Email, Telegram and SMS. In *Syntax Literate Indonesian Scientific Journal* (Vol. 6, Issue 7, p. 3380). <https://doi.org/10.36418/syntax-literate.v6i7.3640>
- Fachrurrozi, N. R., Wirabudi, A. A., & Rozano, S. A. (2023). Design of network monitoring system based on LibreNMS using Line Notify, Telegram, and Email notification. In *SINERGI* (Vol. 27, Issue 1, p. 111). Mercu Buana University. <https://doi.org/10.22441/sinergi.2023.1.013>
- Fahreza, F., & Rifqi, M. (2020). Nagios Core Optimization By Utilizing Telegram as Notification of Disturbance. In *Journal of Applied Science, Engineering, Technology, and Education* (Vol. 2, Issue 2, p. 121). <https://doi.org/10.35877/454ri.asci2259>
- Mardiyono, A., Sholihah, W., & Hakim, F. L. (2020). Mobile-based Network Monitoring System Using Zabbix and Telegram (p. 473). <https://doi.org/10.1109/ic2ie50715.2020.9274582>
- Nagios. (2023). Astiostech Saves Time and Money with Nagios Solutions | Nagios. <https://www.nagios.com/casestudies/astiostech/>
- Nugroho, Y. H., Sastra, N. P., & Wiharta, D. M. (2018). Analysis of OpenNMS (Open Network Monitoring System) Network Monitoring Performance on TCP/IP Network. In *SPECTRUM Journal* (Vol. 5, Issue 2, p. 158). <https://doi.org/10.24843/spektrum.2018.v05.i02.p20>
- Pratama, R., Orisa, M., & Ariwibisono, F. (2020). THE MONITORING AND CONTROLLING SERVER APPLICATION USES THE ICMP (INTERNET CONTROL MESSAGE PROTOCOL) AND SSH (SECURE SHELL) PROTOCOLS BASED ON THE WEBSITE. In *JATI (Informatics Engineering Student Journal)* (Vol. 4, Issue 1, p. 397). <https://doi.org/10.36040/jati.v4i1.2310>
- Prayogo, T. D., Kushartantya, K., & Wibawa, H. A. (2012). NETWORK MONITORING SYSTEM ON LINUX SERVERS USING SMS GATEWAY. In *JOURNAL OF INFORMATICS SOCIETY* (Vol. 2, Issue 3). <https://doi.org/10.14710/jmasif.2.3.63-72>
- Rivaldi, O., & Marpaung, N. L. (2023). The implementation of the network security system uses the Suricata-based intrusion prevention system. In *INOVTEK Polbeng - Informatics Series* (Vol. 8, Issue 1, p. 141). <https://doi.org/10.35314/isi.v8i1.3269>
- Rizal, R., Ruuhwan, R., & Nugraha, K. A. (2020). Network Security Implementation Using Port Blocking and Port Knocking Methods on Mikrotik RB-941. In *ICT Information Communication & Technology Journal* (Vol. 19, Issue 1, p. 1). <https://doi.org/10.36054/jict-ikmi.v19i1.119>
- Rizkiana, A., Sukiswo, S., & Widiyanto, E. D. (2018). ANALYSIS OF INTERNET NETWORK PERFORMANCE ON ASTINET SERVICES (CASE STUDY: PT TELKOM WITEL CENTRAL JAVA AND DIY). In *Transmission of the Scientific Journal of Electrical Engineering* (Vol. 20, Issue 1, p. 34). <https://doi.org/10.14710/transmisi.20.1.34-42>
- Rochman, S., Septiana, Y., & Mulyani, A. (2019). Designing a network architecture for a vocational high school by applying the concept of The Dude Server. In *Jurnal Algoritma* (Vol. 16, Issue 2, p. 126). <https://doi.org/10.33364/algoritma/v.16-2.126>
- Safitri, S. T. (2013). Analysis of Information Technology Governance at PT. Pertamina (Persero). In *JURNAL INFOTEL* (Vol. 5, Issue 1, p. 52). LPPM Telkom Institute of Technology Purwokerto. <https://doi.org/10.20895/infotel.v5i1.113>
- Telkom Digital Solution. (2023). <https://www.telkomdigitalsolution.com/>

Toland, C., Meenan, C., Warnock, M., & Nagy, P. (2007). Proactively Monitoring Departmental Clinical IT Systems with an Open Source Availability System. In *Journal of Digital Imaging* (Vol. 20, p. 119). Springer Science+Business Media. <https://doi.org/10.1007/s10278-007-9063-2>
