Available on: http://gjetr.ep-journals.org/ E-ISSN: 3051-3782, P-ISSN: 3051-3774

Global Journal of Engineering and Technology Review

Volume: 01 Issue: 02 October 2025

Distributed Network Monitoring with Nagios

Frida Gjermeni

Aleksander Moisiu" University of Durres, Faculty of Information Technology, Albania

Elton Tata

SEE University, Faculty of Contemporary Sciences and Technologies, North Macedonia

Published Date: October 21, 2025 **Article DOI: 10.65150/EP-gjetr/V1E2/2025-01**

ABSTRACT: In information systems, data is collected, stored and processed, as well as information, knowledge and digital products are protected. The best solution for these requirements is an ISP network monitoring system. ISP networks are distributed and heterogeneous, which makes monitoring crucial for their health. For continuous monitoring, some monitoring systems use open-source software tools. It contributes to the monitoring of systems, applications, services, networks, and infrastructure. We can use these tools to detect network or server problems, share network services or devices among specific groups, generate alerts by simplifying the monitoring process, and save logs for creating reports. Our paper discusses how an ISP can monitor its network using a system such as Nagios. This open-source system provides real-time monitoring and alerts network administrators to anomalies as soon as they occur. We will also present the advantages that Nagios offers to an Internet Service Provider (ISP) for monitoring network equipment and services. We focus on using Nagios as a tool for automatic detection of anomalies occurring in the network topology as well as notification to the Network Monitoring Center (NMC) via email or web interface access.

KEYWORDS: Information system, Internet Service Provider (ISP), Monitoring System, Network, Nagios.

I. INTRODUCTION

In recent years' communication technologies have undergone a major revolution in the way they function and organize. The emergence of new technologies but also new manufacturers in the field of telecommunications equipment have led to the creation of a heterogeneous network. Given that each manufacturer creates its own protocols and its own way of managing equipment brings increased difficulty in managing and monitoring them in a heterogeneous and distributed network of an ISP. An ISP cannot have equipment from only one manufacturer for two reasons, the first should not become dependent on only one manufacturer and the second should adapt to the latest developments bringing new network technologies at a higher cost decreases to be competitive in the market. The network administrator of an ISP must find monitoring systems to suit the heterogeneity of the network at an appropriate cost to the company. One of the monitoring systems which is also open-source that best suits the topology of a heterogeneous network is Nagios. The monitoring system will be used to detect network connection failures, interface problems according to predefined policies, changes in configuration or congestion of lakes capacity due to increased traffic [14]. All monitoring systems to ensure continuous and real-time monitoring of servers, network equipment, services, etc. use the SNMP protocol. Efficient and fast monitoring is one of the basic requirements for any ISP network management system [15]. Most companies try to use open source software such as Nagios, Zabbix, Cacti etc. Nagios is one of the most popular tools used in ISP network monitoring. It provides continuous and real-time monitoring by notifying the monitoring center by generating alerts or sending e-mails on the problem that occurred in the network. Nagios has found wide use in many different fields such as monitoring a surveillance system or monitoring a computer network of an office or a company. In this paper we will focus on using Nagios as a tool for monitoring an ISP network. The main purpose is to detect anomalies in the network topology as soon as possible as well as notification through alerts displayed on the web interface or e-mail to notify the administrator to take the necessary measures to restore the service from the problem caused. Also in this paper we will see the benefits of the proposed system in relation to other monitoring systems but also the opportunities that Nagios offers us in facilitating this process during network monitoring in an ISP. The rest of the study is structured as follows: Section II presents the related work in the field of monitoring, which presents different ways and tools for the monitoring process. Section III presents a comparison between ten different tools used to monitor specific elements for each of them. Section IV presents the general architecture of how Nagios conducts the monitoring process. Section V presents the architecture of the ISP monitoring model. Section VI presents some data on how to work with Nagios for a more efficient and organized monitoring. In section VII we will present a discussion on the monitoring process in the ISP based mainly on Nagios. And in section VIII we will summarize the conclusions.

II. RELATED WORK

Network monitoring in an ISP is one of the most important elements to have a secure and healthy network. Monitoring allows us to be informed in real time of any changes that occur in the network. Every ISP attaches great importance to monitoring systems to be informed at all times about the state of the devices that make up the network. In this section we will present some of the efforts on usable monitoring systems.

J. Renita and N. Edna Elizabeth [1] present a monitoring system in order to inform the network administrator of any anomalies occurring in the network topology. In this paper Nagios is used as a platform for network monitoring. The importance in this monitoring is given to the monitoring of servers in relation to CPU status, Memory usage etc. where their status is constantly checked and in case of any anomaly the network administrator is notified via e-mail. The software is configured in such a way that network monitoring is done every 10 s and Nagios after 5 attempts in case the device does not respond generates an alarm and notifies the administrator by e-mail about the anomaly.

Miguel Silva et al [2] presents a P2P Overlay system for detecting anomalies in a network to facilitate the work of the network administrator of an ISP to monitor the infrastructure and equipment connected to the network. This monitoring system through the realization of P2P connections generates traffic graphs allowing the administrator to detect the lack of
traffic, cases when there is traffic congestion depending on the defined parameters or other purposes related to the network. The process of communication between units is realized through the TCP / UDP protocol on which control packets, data transfer packets and all data on other network processes are exchanged.

Jianwu Zhang [3] presents an Internet Protocol (IP) based testing system based on SNMP. This monitoring system is able to monitor the status of the interface, the name of the interface, is also designed to monitor the CPU utilization of devices, memory in order to monitor network performance.

Watanakeesuntorn Wassapon [4] which for monitoring represents Opimon which monitors and visualizes SDF based on OpenFlow. This tool provides real-time monitoring of network topology as well as switching tables. In the OpenFlow network is separated into two parts namely: control plane and data plane. The data plan is responsible for sending packets from source to destination while the control plan has the task of controlling each switch in the network.

MingLi Wu [5] introduces a Hadoop network monitoring platform which integrates Ganglia and Nagios taking advantage of each platform. This platform is able to monitor various components in the network topology as well as device data to detect anomalies with the help of the network administrator. This system is also complete with a visualizing interface to make it easier to find where the network anomaly has occurred.

Marios Iliofotou et al [6] propose the use of Traffic Dispersion Graphs (TDGs) as a way to monitor, analyze and visualize network traffic. In a network, TDG nodes correspond to a unique IP address and the graph is constructed by capturing packets exchanged between sending and destination nodes. So this system by monitoring the gate traffic manages to understand through the behavior of this traffic anomalies that may occur in the network based on the policies set by the ISP. In this way, when there is an anomaly, it is noticed by the network administrator who makes decisions based on the analysis of the situation.

Andreea Cirneci et al [7] introduce a system called Netpy which to evaluate the performance of a network is based on monitoring the traffic generated in the network. NetFlow records are used to visualize traffic, which is analyzed by the network administrator to understand the anomalies and to take the necessary actions in each case. This tool consists of four modules: Storage Module, Intrusion Detection Module, Analysis Engine and User Interface. Netpy is mainly focused on performance and response time.

AN OVERVIEW OF NAGIOS AND OTHER MONITORING SYSTEMS.

An ISP with a wide and heterogeneous network where the main goal is to provide a continuous and quality service, an important role is given to the monitoring system. The monitoring system enables the monitoring of any device that has access to the network to detect possible anomalies and notify the network administrator of what has happened. An ISP which offers multiple services as well as on the network may have equipment from different vendors, such as cisco, juniper, alcatel, etc., the network administrator must carefully evaluate each element to decide which monitoring system is most appropriate. Some of the elements that should be considered are, a user friendly monitoring system, to notify by e-mail, SMS or any form of notification in cases where an anomaly is detected in the network, possibly be open-source, to adapt to a heterogeneous network and simple to implement. Below in Table 1. we present ten monitoring systems based on [8], [9], comparing some of the most important parameters of a monitoring system.

TABLE I. TEN MOST POPULAR MONITORING TOOLs.

Tools	***License***	***Support***	***User Interface***	***Notifications***	***OS Support***	***Monitoring Abilities***	***Network Discovery***	***Reports system***	***Target business size***
Nagios	open-source	Active support community	Advance web interface	email and SMS	Linux/Unix	SNMP, ICMP	auto-discover devices	Yes	From SMB to large corporations
Solarwinds	No open-source	Active support community	Excelent GUI	email and SMS	Windows, Mac OS, and linux	SNMP, ICMP	auto-discover devices	Yes	Small and medium
PRTG	No open-source	Active support community	Advance web interface	email and SMS	Windows	SNMP, ICMP	auto-discover devices	Yes	From SMB to large enterprises

ManageEngine OpManager	No open-source	Active support community	Good interface	email and SMS	Windows and Linux	SNMP, ICMP	auto-discover devices	Yes	from SMB to large enterprises
WhatsUp Gold	No open-source	Active support community	Advance web interface	email and SMS	Windows	SNMP, ICMP	auto-discover devices	Yes	Small, medium and large
Zabbix	Open source	Active support community	Advance web interface	email and SMS	Windows, Mac,Linux, Unix	SNMP and IPMP	auto-discover devices	Yes	enterprises
Incinga	No open-source	community forum	Icinga Web	email and SMS	Linux/Unix and Windows	SNMP, ICMP	auto-discover devices	Yes	SMB and enterprise networks.
Datadog	No open-source	Active support community	Good interface	Notification	Windows, Mac OS, Linux	SNMP	auto-discover events	Yes	startups and small businesses
Cacti	open-source	community forum	Good interface	email	Linux/Unix and Windows	SNMP	auto-discover devices	Yes	From SMB to large corporations
Logic Monitor	No open-source	Active support community	Good interface	Notification	Windows, Linux/Unix	SNMP	auto-discover devices	Yes	Small, medium and large

IV. NAGIOS ARCHITECTURE

Network monitoring describes a system that continuously and real-time monitors every element of an ISP's network and notifies the network administrator through its notification methods. Notifications are generated in different forms and depending on the configurations that have been made in advance based on the options offered by the monitoring system. Network monitoring is implemented in order to notify the network administrator to indicate problems caused by overloaded systems, broken servers, lost network connections, virus or malware infections, and power outages, among others [10]. Below we present an architecture on how the Nagios monitoring system works shown in Fig. 1.

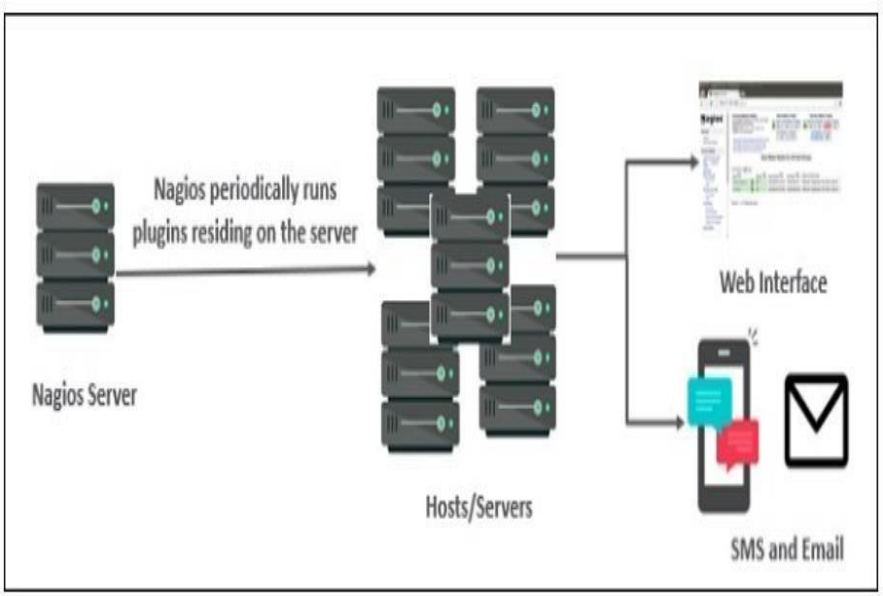

Fig. 1. Nagios operating architecture

As you can see, this architecture [11] consists of the server on which Nagios is installed, the hosts and services to be monitored (servers, routers, switches, etc.), the web interface as well as the notification elements. Nagios, is a free and open-source computer-software application that monitors systems, networks and infrastructure. Nagios offers monitoring and alerting services for servers, switches, applications and services. It alerts users when things go wrong and alerts them a second time when the problem has been resolved.

Nagios in the monitoring process is closely related to Simple Network Management Protocol (SNMP) which is a standard protocol used to communicate management information between network management stations (NMS) and agents (ex. Routers, switches, network devices) in the network elements. By conforming to this protocol, equipment assemblies that are produced by different manufacturers can be managed by a single program. SNMP protocol is widely used via Internet protocol (IP) and operates over UDP well- known ports of 161 and 162. SNMP was originally defined in RFC1098 and is now obsolete and updated by RFC1157. Fig.

Corresponding Author: Frida Gjermeni

2. show basic SNMP communication diagram. This figure shows the basic operation of simple network management protocol (SNMP).

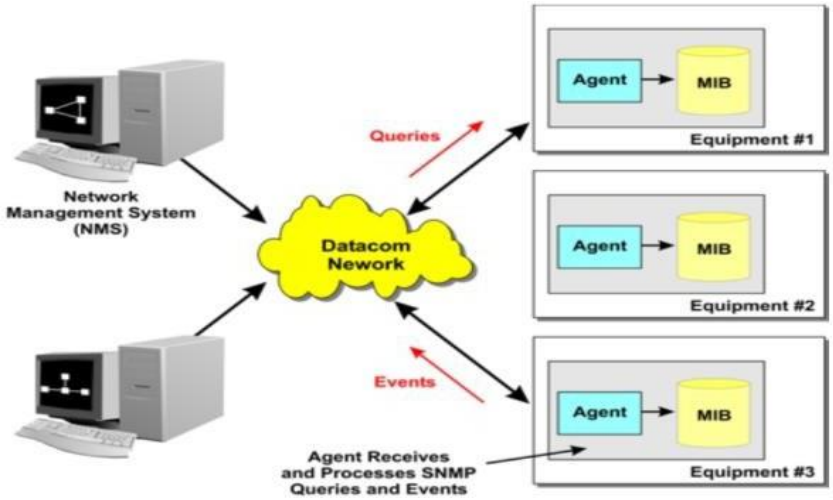

Fig. 2 Simple Network Management Protocol - SNMP Diagram

Agent management information base (MIB), Queries and Events. SNMP helps us to manage the network by: Enables the Read / Write option Gathers information about how much bandwidth is being consumed in a given interface. Monitors CPU usage, memory and generates alerts if a preset threshold is passed. Monitors the status of certain protocols (e.g. status of BGP, OSPF, IGMP) Sends SMS or e-mail if a device is down etc. There are two main components of SNMP that interact with Nagios to enable monitoring of network equipment and they are: OID (Object Identifier) MIB (Management Information Base) SNMP works by querying "Objects". An object is something from which we can obtain information about a network device. For example, an object could be the status of the interface. If we query the status of the gateway we will get a variable in response - the interface is UP or Down. SNMP identifies object via OID. MIB is like a "translator" which helps the Management Station understand the SNMP responses coming from the network device. Each SNMP agent maintains a database describing the device management parameters. SNMP manager uses this database to request specific information from the agent and then translates this information according to the requirements of the Network Management System (NMS). This shared database which is shared between Agent and Manager is called Management Information Base (MIB). MIB files are a set of questions that an SNMP Manager can ask an Agent. File MIB is a group of OIDs that provide information about an Interface, System, Protocol. Etc. Each measure, service or information measurable and included in the SNMP database has a corresponding OID, a concrete example is shown in Fig. 3.

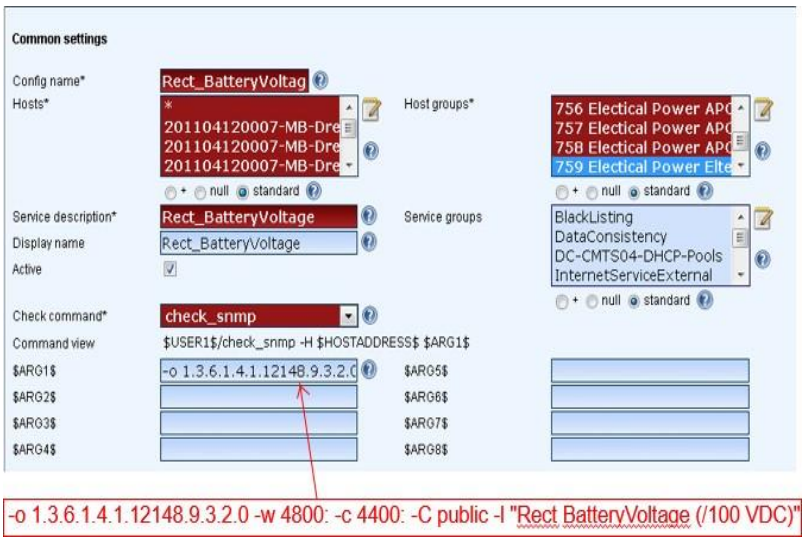

Fig. 3 Example of OID definition in Nagios

V. GENERAL MONITORING ARCHITECTURE IN ISP.

Given the ever-increasing amount of information generated by network equipment but also by those of the IoT, they increasingly require a more flexible monitoring system. A monitoring system in an ISP monitors the entire network topology to detect any potential problems by ensuring that all equipment and services are functional [13]. In an ISP with an extensive network topology and a heterogeneous network, the following model show in Fig. 4 is proposed to be implemented to provide real-time monitoring.

Corresponding Author: Frida Gjermeni

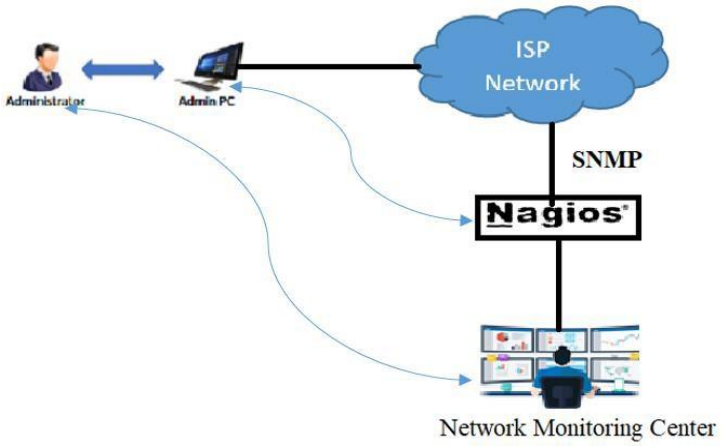

Fig. 4 General monitoring architecture at the ISP

Nagios is an open-source monitoring system, created specifically for monitoring the status of network equipment and services. He constantly checks the condition of services and equipment and at the moment when Nagios checks in case any device or service does not respond then he sends notification for anomalies with that device or service. Network Monitoring Center (NMC) conducts continuous network monitoring 24/7. Every NMC member is trained to interpret any alarm generated by Nagios. The NMC Team at the moment that in Nagios through the web interface a new anomaly appears, analyzes the situation and depending on the policies well defined by the ISP will notify the responsible departments to take the necessary measures to restore normalcy. The network administrator cannot do the network monitoring in an ISP for this purpose NMC Team has been created to cover the monitoring part 24/7. The network administrator is notified only in cases when the problem caused needs the intervention of the administrator to return to service in other cases other departments that take care of the complete maintenance of the network are notified, such as the maintainers for the physical part of the network, for problems energy etc. Given that most of the equipment is geographically distributed in the field and not directly supervised by natural persons, the management part becomes even more difficult. The network topology in ISP is divided into three levels: core layer, distribution layer and access layer. Each node in the network is important for this purpose at each Point of Presence (POP) continuous energy monitoring is done. It therefore helps Nagios to monitor and take precautions before the problem is caused. For this purpose, Nagios constantly monitors and in cases when the power is disconnected and POP switches to battery mode, an alarm is displayed on the interface or an e-mail is sent on this issue to take measures to prevent the outage of this node. Different services can also be defined in Nagios for each device that is part of the network topology. The types of services supported by Nagios include but are not limited to ICMP, PING, SNMP, HTTP, SMTP, NNTP, SSH etc.

VI. ORGANIZATION OF MONITORING IN ISP USING NAGIOS

As mentioned above Nagios is used in many areas of monitoring technology but we will focus on its use in network monitoring in a specific ISP. As it is known, network monitoring in ISP is one of the basic elements for providing a continuous service, this demonstrates the importance that Nagios has in the monitoring part. Nagios Core Version 4.4.6 is implemented on this Linux operating system in this ISP. An overview of it is shown below in Figs. 5.

Fig. 5 Nagios Home Interface

In its Home interface we have an overview where you can see details on the installed version but also gives you the opportunity to access documents, tutorials that help to understand and help while working with it, offers the part of the Lab but also support. In an ISP with distributed but also heterogeneous network topology, the network administrator cannot do single monitoring at any time. Therefore, the Network Monitoring Team is responsible for the monitoring part, which monitors 24/7. Having such monitoring in the notification part in cases when an anomaly is detected, it is important to appear on the web interface where an alarm can be activated for any anomaly that occurs with network equipment or other services. Nagios also offers e-mail notification but in a network where services and equipment are numerous it is a waste of time for the monitoring staff to analyze the e-mails. In the web interface are displayed in real time every event that happens in the network, and after noticing such a thing is the Monitoring Team based on the escalation policies to notify the Network Administrator or other departments of the cases displayed. Below we present the main monitoring interface where the hosts are displayed in their respective state as shown in Fig. 6.

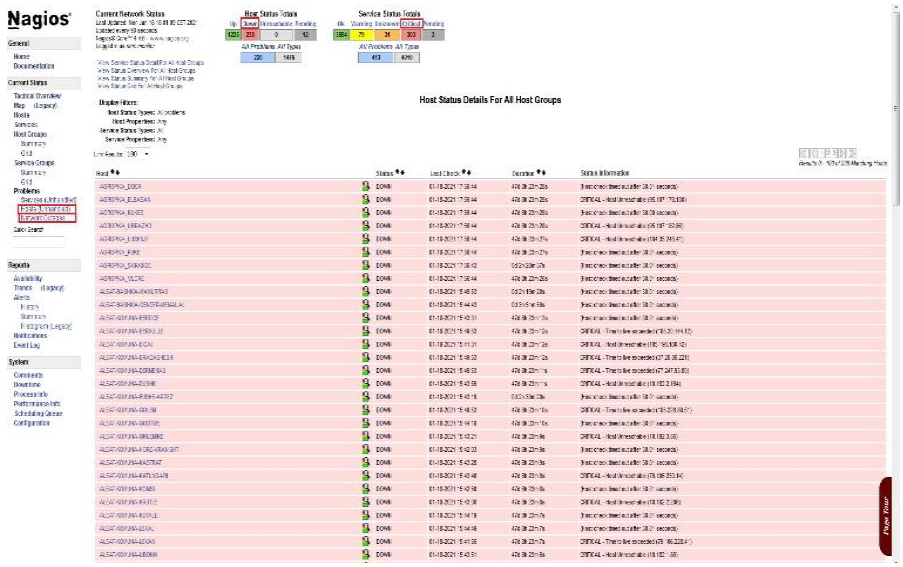

Fig. 6. Host monitoring interface

As you can see, the most important state of the hosts is the Down state when a certain host is out of work and the Up state that indicates that this host is functional. In the status of services, we see that there are some conditions that a service may have. Caution should be exercised in both the Warning and critical cases. The warning case shows a lower degree of risk, e.g. Mem Load has gone up to 50% of the capacity of a core router, in which case no immediate action should be taken but its performance should be kept under control and in case increases and crosses the threshold of 70% passes to critical then it should be looked at carefully as an increase in Memory consumption may cause this device to malfunction. Another convenience that Nagios offers is the division into Host Group. Show in Fig. 7.

Fig. 7 Host Group

Being a Heterogeneous network configuring each host or service on its own takes time and has no efficiency. Thus, in order to define common policies for a certain group, the division is made into host groups according to the technology, the manufacturer and the importance they have in the hierarchy of the network topology. This way when a new host or service is added there is no need to make the configurations from scratch but it is added to the respective group by taking the previous configurations that have been made for that group. Another important point for an ISP is to

Corresponding Author: Frida Gjermeni

generate reports on the availability of a particular host or service. Nagios is a very good tool in this regard because it offers the opportunity to generate reports in different periods and with a certain duration. After selecting the specified host or service, selects the time period for which the Nagios report should generate a detailed report with the time and period in which it was Up and Down by calculating availability as shown in Fig. 8.

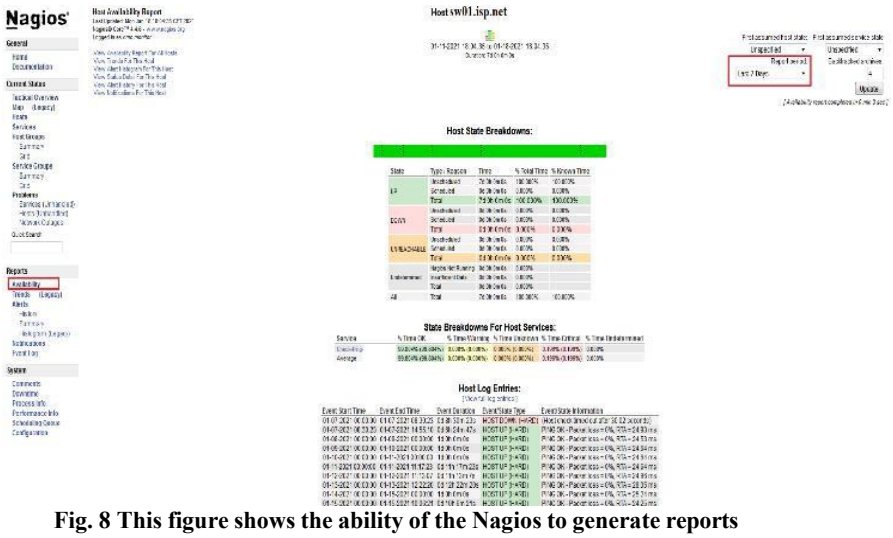

Fig. 8 This figure shows the ability of the Nagios to generate reports

What we mentioned above make Nagios a very important tool a part of monitoring for the detection of anomalies in the network topology. Also Nagios not only for the monitoring part but also offers many other advantages for the purposes of an ISP.

VI. DISCUSION

In an ISP with a wide and heterogeneous network there is always room for discussion about the monitoring process. Discussions relate to having a paid monitoring system or relying on open-source software. A monitoring system should be flexible and easy to use and implement. Nagios is an open-source monitoring system that best suits the monitoring requirements of an ISP. Nagios is a tool that is adapted to monitor any type of equipment produced by different manufacturers that make up the network topology. The types of services supported by Nagios include ICMP, PING, SNMP, HTTP etc. Nagios tests and obtains information in a continuous way on each device, certain interface or a certain service, thus detecting in a real way any anomaly that occurs in the network topology. At the moment of detecting an anomaly it appears and is updated in the web interface automatically to be seen by the Monitoring Team. In addition to the display in the web interface, any anomaly can be accompanied by an alert, sending an e-mail or SMS depending on the way chosen by the administrator to perform the monitoring. From the architecture presented, monitoring in an ISP, as we mentioned above, network monitoring cannot be monitored by the administrator but by the Monitoring Center that performs monitoring 24/7. Nagios monitors and notifies in cases when bandwidth utilization, memory consumption or CPU utilization is achieved, but for the visualization of this data as well as to see the progress in the form of graphs, a very good tool is Cacti. Cacti is open- source and one of the best network graphing tools which uses RRDTool's data storage for this purpose. Nagios but also Cacti are used to generate various reports regarding services or the history of various network devices. In the case presented Nagios is the best monitor used in monitoring ISP network.

VII. CONCLUSION

In an ISP where the network is wide and where many events occur at any time the network administrator cannot do network monitoring alone. So in this paper we have introduced a monitoring system implemented in an ISP where continuous monitoring is performed by the Monitoring Center 24/7 using Nagios. In this way the administrator will be notified by the monitoring center only in cases when his intervention is required for anomalies displayed in the network topology. Nagios as a tool used in monitoring has several advantages, it is open-source software, performs monitoring of various network devices regardless of their manufacturer, supports various technologies and displays in real time the detected anomalies. Nagios to determine the status of a device, interface or service performs continuous query via SNMP or PING. Nagios offers a web interface for monitoring but there are also other ways of notification such as e-mail or SMS. In an ISP where we are focused on the way of monitoring, the important thing is the display of anomalies detected in the web interface, it also offers the possibility of activating sound alarms when a new event appears.Facilitates the monitoring process by allowing you to sort by the time that each anomaly occurred in the network. Such a monitoring system facilitates the work of the network administrator, thus performing the other tasks in charge. Reduces the time to return to normal for any anomalies that occur as the monitoring center knows exactly according to predefined policies who should be notified of any problems that occur. Since Nagios monitors a variety of services including: memory utilization of each device, CPU utilization, monitors protocols such as BGP, OSPF, IGMP etc. It is also sensitive to the use of bandwidth based on preset restrictions, latency and link failure. Organizing Host Groups facilitates the monitoring process but also the addition of new monitoring equipment that has the same purpose as the pre- equipment of a certain group. Nagios is not just a monitoring tool but has the ability to adapt to the conditions of the organization. In the future Nagios will significantly influence the monitoring process in ISP by reducing the cost of this process but also the time in the recovery of anomalies by providing Quality of Services (QoS) of the network by implementing and using as efficiently as possible the advantages that it offers.

Corresponding Author: Frida Gjermeni

REFERENCES

1) J. Renita and N. E. Elizabeth, "Network's server monitoring and analysis using Nagios," 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET),Chennai, 2017, pp.1904-1909 ,doi:10.1109/WiSPNET.2017.8300092.
2) M. Silva, R. Mendonça and P. Sousa, "A P2P Overlay System for Network Anomaly Detection in ISP Infrastructures," 2019 14th Iberian Conference on Information Systems and Technologies (CISTI), Coimbra, Portugal, 2019, pp. 1-6, doi: 10.23919/CISTI.2019.8760780.
3) J. Zhang, "Design and implementation of test IP network intelligent monitoring system based on SNMP," 2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chongqing, 2017, pp. 2124-2127, doi: 10.1109/IAEAC.2017.8054392.
4) W. Wassapon, P. Uthayopas, C. Chantrapornchai and K. Ichikawa, "Real-time monitoring and visualization software for OpenFlow network," 2017 15th International Conference on ICT and Knowledge Engineering (ICT&KE), Bangkok, 2017, pp. 1-5, doi: 10.1109/ICTKE.2017.8259622.
5) MingLi Wu, Zhongmei Zhang and Yebai Li, "Application research of Hadoop resource monitoring system based on Ganglia and Nagios," 2013 IEEE 4th International Conference on Software Engineering and Service Science, Beijing, 2013, pp. 684-688, doi: 10.1109/ICSESS.2013.6615399.
6) Marios Iliofotou, Prashanth Pappu, Michalis Faloutsos, Michael Mitzenmacher, Sumeet Singh, and George Varghese. 2007. Network monitoring using traffic dispersion graphs (tdgs). In *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement* (*IMC '07*). Association for Computing Machinery, New York, NY, USA, 315–320. DOI:https://doi.org/10.1145/1298306.1298349
7) A. Cirneci, S. Boboc, C. Leordeanu, V. Cristea and C. Estan, "Netpy: Advanced Network Traffic Monitoring," 2009 International Conference on Intelligent Networking and Collaborative Systems, Barcelona, 2009, pp. 253-254, doi: 10.1109/INCOS.2009.13.
8) J. Hernantes, G. Gallardo and N. Serrano, "IT Infrastructure- Monitoring Tools," in IEEE Software, vol. 32, no. 4, pp. 88-93, July- Aug. 2015, doi: 10.1109/MS.2015.96
9) .https://www.pcwdld.com/best-network-monitoring-tools-and-software [14.01.2021]
10) M. A. A. bin Mohd Shuhaimi, Z. binti Zainal Abidin, I. binti Roslan and S. binti Anawar, "The new services in Nagios: Network bandwidth utility, email notification and sms alert in improving the network performance," 2011 7th International Conference on Information Assurance and Security (IAS), Melaka, 2011, pp. 86-91, doi: 10.1109/ISIAS.2011.6122800.
11) https://www.tutorialspoint.com/nagios/nagios_architecture.htm[15.01.2121]
12) http://www.telecomdictionary.com/telecom_dictionary_SNMP_definition.html [15.01.2021]
13) Rafiullah Khan, Sarmad Ullah Khan, Design and implementation of an automated network monitoring and reporting back system, Journal of Industrial Information Integration, Volume 9, 2018, Pages 24-34, ISSN 2452-414X, https://doi.org/10.1016/j.jii.2017.11.001.
14) Doliwa D, Frydrych M, Horzelski W. Network monitoring and management for company with hybrid and distributed infrastructure. Information Systems in Management. 2016;5(3):326-35.

Corresponding Author: Frida Gjermeni