NETWORK MONITORING TOOLS: ENABLING THE MANAGEMENT OF NETWORK ASSETS, ENSURING HIGH AVAILABILITY

[1]Jefferson Gonçalves Coelho, [1]Bruno Pereira Gonçalves,[1]Mayre Vane Serafim da Silva,[1]Jaqueline Silva de Souza Pinheiro,[1]Jean Mark Lobo de Oliveira, [1]Victor da Silva Almeida and *[2]David Barbosa de Alencar

[1]Academic Department, University Center FAMETRO, Amazon-Brazil
[2]Institute of Technology and Education Galileo of Amazon (ITEGAM), Brazil

ARTICLE INFO

ABSTRACT

With the advancement of technology and communication systems as monitoring tools used to manage the network essential to ensure the continuous functioning of systems and devices on a company's network. Through bibliographic research, with studies on computer network and its communication protocols, experimental, considering procedures and manuals of installation, configuration, descriptive, to verify the data collected by the tools. It presents a comparison between Zabbix and Nagios, two open source tools very popular in the market, to conclude which tool is best suited to media and large companies' scenarios. In summary, Zabbix presents a more viable option for the growth and efficiency of network management in companies. Nagios, on the other hand, proved to be adaptable to different scenarios, with the availability of several plugins increased by the community.

INTRODUCTION

Communication of human beings is necessary for their own development. The advancement of technology, especially in communication and computer systems, makes globalization increasingly intense. For this communication to occur, computer networks have a fundamental role, as they interconnect these organizations by digital means. Any organization that has a computer network wants to have the means to maintain it in excellent performance, as the company's information travels over it. With this, there is a management that is responsible for monitoring assets, such as computers, servers, printers and any other connected devices, alerting the administrator with precision if any changes in the services provided. The good performance of a network requires that all its services are in full operation, so there is a greater guarantee of availability. Failures in systems can cause several damages, mainly when they affect the consumer, loss of productivity occurs, affecting their profits, costs and consequently the dissatisfaction to the users of the network. Currently, in network management there are several ways toguarantee the high availability of equipment, services and network, such as, for example, to implement redundancy mechanisms. With the repetition of critical components for the functioning of a service, its reliability is improved, because in the event of a failure that could disable the primary system, a secondary system assumes responsibility, that is, the objective of IT redundancy (information technology) and ensure the uninterrupted use of services and avoid data loss. For network administrators to have these characteristics in computer networks, tools are used that help in the network monitoring process, with which it is possible to improve fault management and performance management, with a view to a better solution for the corporate scenario in which the tools were used, comparing several criteria such as: installation, configuration and performance as a way to obtain more appropriate choices in management solutions.

BIBLIOGRAPHIC REVIEW

The theoretical framework of the research was structured in 3 topics, namely: VirtualBox: Performance, configuration; Zabbix: its features, Alerts and Notifications; Nagios.

Virtual Box: According to Oracle (2020, page 1) VirtualBox is an effective virtualization software for institutional and domestic use, it is not only a high performance software and excellent in resources for both corporate customers but also the only professional available for free as software for open source under the terms of the GNU General Public License. According to the official VirtualBox website, the software can be installed on the following operating systems:

> (...) on Windows, Linux, Macintosh and Solaris hosts and supports a large number of guest operating systems, including, among others, Windows (NT 4.0, 2000, XP, Server 2003, Vista, Windows 7, Windows 8, Windows 10), DOS / Windows 3.x, Linux (2.4, 2.6, 3.x and 4.x), Solaris and Open Solaris, OS / 2 and OpenBSD. (2020).

Main Features according to the VirtualBox Manual: "Portability, additions to guests: shared folders, continuous windows, 3D virtualization. multiprocessing guest (SMP). USB device support. Hardware compatibility and resolutions on multiple screens." (2020).

Zabbix: In Lima's book. Zabbix is an open source monitoring software for companies. It is software that monitors various specifications of various assets on a computer network. It was created by Alexei Vladishev in 1998. The idea was born when he worked at a bank in Latvia as a system administrator, but he was not satisfied with the monitoring tools he was using at the time. (2014). Zabbix is a tool that monitors various processes on a network, the availability of services and all servers. It uses a versatile monitoring system that allows you to adjust alerts by e-mail and SMS, adapting to any IT scenario. Thus, notifications facilitate the quick reaction to difficulties in the work environment. Zabbix features several means of reporting and managing stored information, thus helping to provide high availability of network services. According to Horst; Pires and Déo (2015) Zabbix is a modern, Open Source engine and is also multiplatform (Web interface for any platform and the full version for different Linux distributions). There is only one option of the tool, which is aimed at companies, becoming applied to analyze the availability and performance of applications, assets and services on the network. In accordance with Olups (2010), Zabbix provides several ways to manage the most varied elements of your IT infrastructure, thus interacting with any asset that is connected to this network. It can be identified as a semi-distributed control system with centralized management. Although numerous devices have a single central database, it is possible to use distributed monitoring with proxies and network nodes, and most devices will use the Zabbix agent. According to Horst; Pires and Déo (2015), Zabbix is composed of a wide architecture, several software components, containing: Zabbix Server, Zabbix Agent, Zabbix Proxy, Java Gateway, Web Interface, Data Flow, Database.

Alerts and Event Notifications of Monitored Assets: Zabbix is able to display notifications on the web interface, using various colors, which can be adjusted according to the type or degree of importance of the difficulty, in addition to executing audible alerts. It issues alerts whenever critical parts of the network and infrastructure fail and also when they recover, thus generating managers a warning of important events. Zabbix allows you to configure the sending of alerts via SMS, e-mail, Gtalk and still have a very different, intuitive and personalized visual effect. According to Vladishev, through Zabbix it is allowed to monitor numerous procedures of the network and servers, as well as the performance of services. The notification system makes it possible to adjust alerts against approximately any event, facilitating the immediate response to the presented failures. According to Olups (2010), the most common notification method to be used is via email. Whenever something interesting happens in Zabbix, some action must be taken in case of a serious failure, then the configuration is made so that an email is sent to the administrator, manager or personnel responsible for the network. However, before deciding when and what should be sent, you will have to be "informed" to Zabbix how it will be done. According to Horst; Pires and Déo (2015), any form of contact with the world is carried out by a type of media. When installing Zabbix, it is prepared to operate with three types of media: E-mail, Jabber (an instant message) and SMS (via a modem connected to the server). In addition to all this, it is possible to create additional types of media, to integrate with third party tools and enhance Zabbix. In accordance with Horst; Pires and Déo (2015), it is possible that one day it will be necessary to configure the integration of Zabbix with third-party tools, such as demand software, ticket or workflow. When this need arises, it will be possible to use scripts and associate them with a new type of media. Thus, you can easily and simply insert incident data and notifications into temporary files.

Nagios: Nagios is a powerful monitoring system that allows organizations to identify and resolve IT infrastructure problems. In Silva's book Nagios: "(...) is a popular open source monitoring program written and maintained by Ethan Galstad". (2018). Created in 1999 by Nagios Enterprises. With it is possible to monitor the entire infrastructure of a network and ensure that hosts and services send event notifications. (NAGIOS, 2020). "It can be installed on several operating systems, in addition to Linux it also supports Solaris, Windows and HPUX. It supports integration with other tools, thereby extending its monitoring and control power.". (SILVA, 2018).

Nagios Core Overview: According to the Nagios Brazilian Community (2020) website, Nagios core offers organizations many benefits, including:

Monitoring Comprehensive: Provides monitoring of all components of the IT infrastructure, including applications, services, operating systems, network protocols, system metrics and network infrastructure.

Visibility: Provides a central view of your entire network of IT operations and business processes.

Awareness: Alerts are sent to the IT team via email and SMS. Multi-user notification escalation capabilities ensure to alert and reach the team responsible for the system.

Problem Correctors: Event handlers allow you to automatically restart failed applications, services, servers and devices when problems are detected.

Trends and Capacity Planning: Allows organizations to plan their infrastructure improvements before outdates systems are taken by surprise.

Reports: Check if SLAs are being met, provide records, fall histories, notifications and alert response for further analysis. Extensible Architecture: Offers easy integration with in-house software and third-party applications.

MATERIALS AND METHODS

The usage of Virtual Box Software, to create the virtual machines. Installation of the Zabbix and Nagios tool to monitor network devices with notebooks and routers, to be managed by the tools. According to the bibliographic research on computer network and monitoring concepts, focusing on the basis of the network protocols and on the monitoring tools used in the analyzes, an experimental research was carried out, where it was possible to have a knowledge base of the procedures performed to have the conclusion both in the installation manuals for the Zabbix and Nagios tools, understanding the SNMP protocol (Simple Network Management Protocol), used in the configuration of the assets that the tools will monitor. With the descriptive research it was possible to analyze the collected data, generate graphs and observe the alerts that the tools send in case of any intermittency in the monitored hosts.

DISCUSSION OF RESULTS

In this section is the main work of this research, where all the steps will be analyzed to define which of the Zabbix or Nagios tools is best suited in the evaluations.

Tool evaluation: In order to carry out a comparative assessment of its tools, several aspects of each were analyzed separately, such as: installation, configuration and data collection.

Installing the tools: Here you will see how each tool will be installed, each step and each command that it will use.

Zabbix: On the official Zabbix website, there is documentation on the installation step by step and various forms of installation such as: installation from repository packages, installation through containers, installation through executable sources, among others. For comparison purposes, installation using Zabbix repositories in version 4.4 was used. After running the virtual machine with the ubuntu system, the following commands were used for installation via the terminal:

To install the Zabbix repository:

```
# wget
https://repo.zabbix.com/zabbix/4.4/ubuntu/pool/main/z/zabbix-release/zabbix-release_4.4-1+bionic_all.deb
# dpkg -i zabbix-release_4.4-1+bionic_all.deb
# apt update
```

To install the Zabbix server, its database and its agent:

```
# apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-agent
```

To create the first access to the database:

```
# mysql -uroot -p password
mysql> create database zabbix character set utf8 collate utf8_bin;
mysql> grant all privileges on zabbix. * to zabbix@localhost identified by 'password';
mysql> quit;
```

Importing the created database:

```
# zcat /usr/share/doc/zabbix-server-mysql*/create.sql.gz | mysql -uzabbix -p Zabbix
```

Starting the Zabbix's server and agent services:

```
# systemctl restart zabbix-server zabbix-agent apache2
# systemctl enable zabbix-server zabbix-agent apache2
```

Configuring the Zabbix's Front End:

Opening the browser and entering the following address http://localhost/Zabbix, we have:

Source: The Authors, 2020.

Fig. 1. Home screen

Image 2 showing all installed services:

Source: The Authors, 2020.

Fig. 2. Installed prerequisites

Image 3 shows how the connection with the bank is being configured:
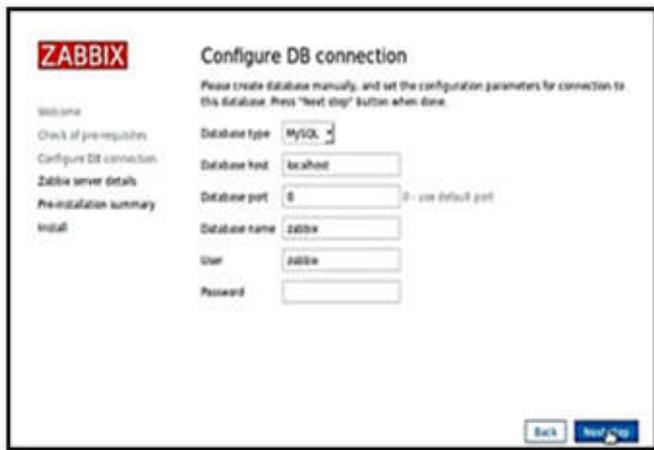
Source: The Authors, 2020.

Fig. 3. Database

Image 4 shows a general summary of the front-end configurations:

Source: The Authors, 2020.

Fig. 4. Installation summary

In image 5, the message that the settings have been completed appears:
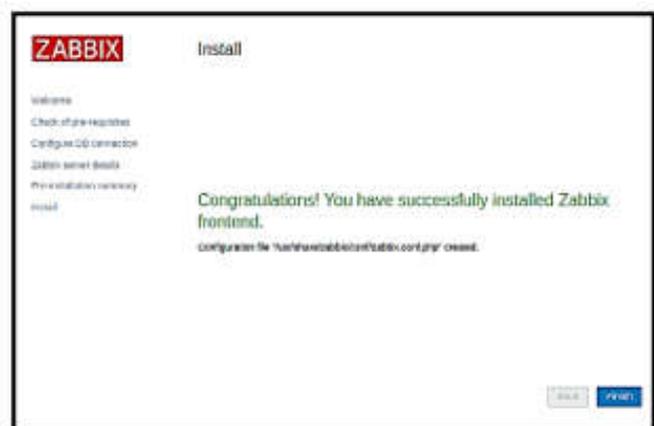
Source: The Authors, 2020.

Fig. 5. Finishing installation.

After completing the login screen is shown as shown in Image 6 below:

Source: The Authors, 2020.

Fig. 6. Login Screen

Nagios Core: When installing Nagios cores: we will use the official documentation to install the tool on the virtual machine with the ubuntu system installed. After running the virtual machine with the ubuntu system, the following steps were used for installation via the terminal:

1.   First we will update our packages with the command: "apt-get update".

2.   We will install the dependencies:
"apt-get install -y autoconf gcc libc6 make wget unzip apache2 php libapache2-mod-php7.0 libgd2-xpm-dev".

3.   Downloading Nagios: Accessing the directory cd/tmp:
wget   --no-check-certificate   -O   nagios-plugins.tar.gz
https://github.com/nagios-plugins/nagios-plugins/archive/release-2.2.1.tar.gz
And unzipping the downloaded file: tar zxf nagios -plugins.tar.gz

4.   Compiling the files and installing:

Accessing the unzipped file folder: cd /tmp/nagios-plugins-release-2.2.1/

Running ". /tools/setup ", "./configure", "make" and "make install".

5.   Installing additional nagios plug-ins, found on the Nagios page with the commands:

apt-get install -y autoconf gcc libc6 libmcrypt-dev make libssl-dev wget bc gawk dc build-essential snmp libnet-snmp-perl gettext.

5.1 installing additional plugins: accessing the temporary directory: "cd / tmp" and downloading through:

wget   --no-check-certificate   -O   nagios-plugins.tar.gz
https://github.com/nagios-plugins/nagios-plugins/archive/release-2.2.1.tar.gz

5.2 Unzipping the downloaded file: "tar zxf nagios - plugins.tar.gz".

6.   Commands to start services:

systemctl iniciar nagios.service
systemctl parar nagios.service
systemctl reiniciar nagios.service
systemctl status nagios.service

7.   Accessing the interface through the browser through the url: "localhost/nagios", as in image 7:
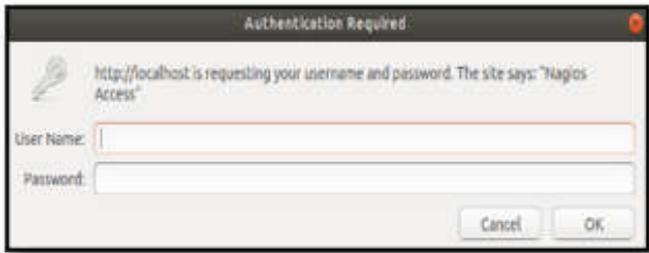
Source: The Authors, 2020.

Fig. 7. Nagios login screen

Accessing with the created user we have the Nagio Core home screens as in image 8:
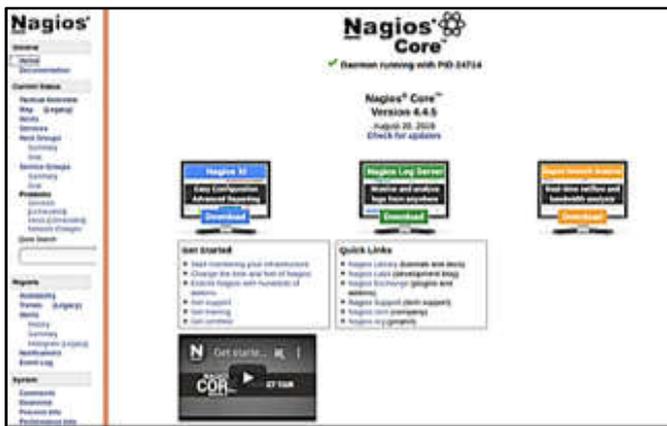
Source: The Authors, 2020.

Fig. 8. First nagios interface

Configuration and data collection of tools (hosts and services): This session will show you how to configure new hosts, graphics settings, and how the services of each tool will be viewed.

Zabbix: To configure an asset in the Zabbix web interface, follow the steps below:

Go to: Configuration > Hosts

Click create host in the upper right corner of the screen, or click on the link the name of the host you want to edit settings Enter the configuration parameters on the form.

The HOST tab includes the general attributes of a host:
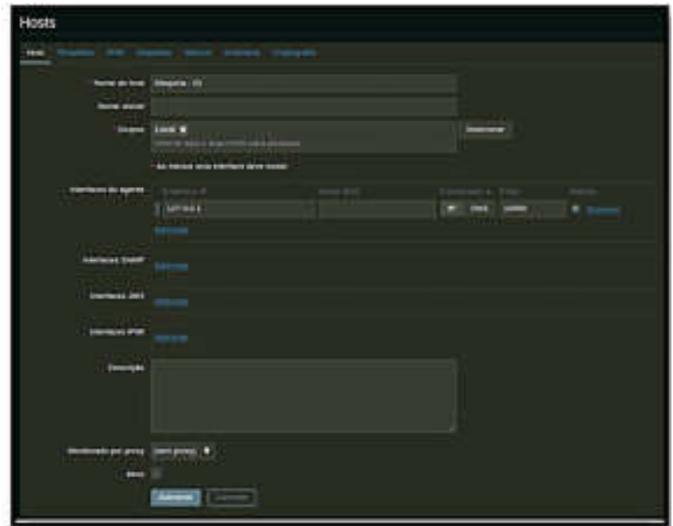
Source: The Authors, 2020.

Fig. 9. Host Creation Screen

Discovery Rule Configuration:

Access: configuration → Discovery
Click on the Create Discovery Rule button located at the top of the screen:

We have:
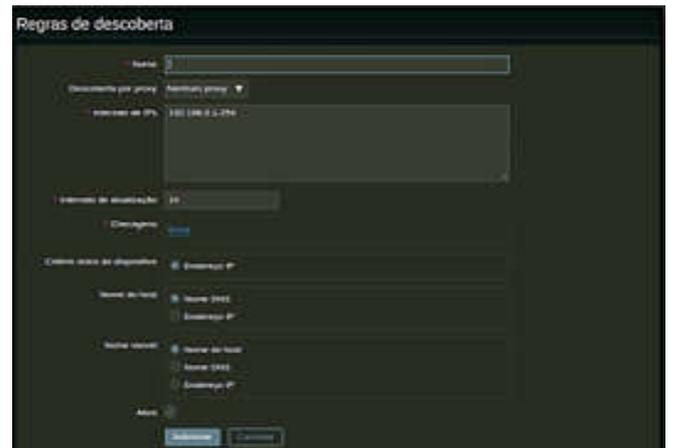
Source: The Authors, 2020.

Fig. 10. Discovery Rule Screen

Simple graphics setup

Access Monitoring → Recent data.

Use the filter to display the items you want.
Select the checkboxes of the items needed for the graph.

Click the View stacked graph or view graph button:
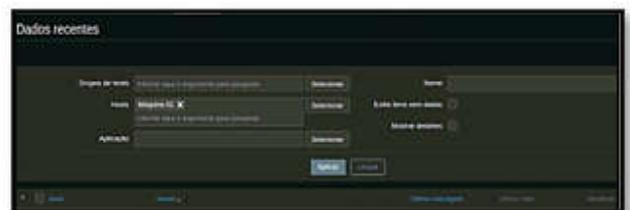
Source: The Authors, 2020.

Fig. 11. Configure Charts

Simple Chart
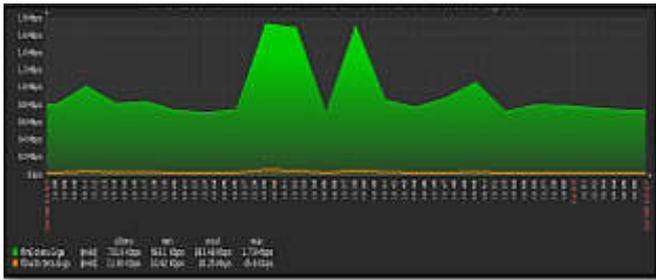
Source: The Authors, 2020.

Fig. 12. Chart

During data collection, Zabbix alerts incidents if you lose connectivity with the devices you are monitoring, as we can see in Image 13:
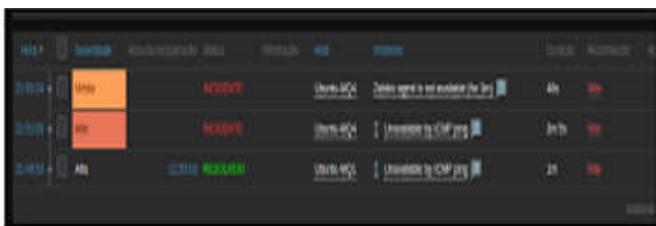
Source: The Authors, 2020.

Fig. 13. Incident alert screen

With the configured template it is possible to generate consumption graph, both of CPU, Memory and other attributes. As in image 14, we have the graph of memory consumption used on one of the hosts created in the experiment:
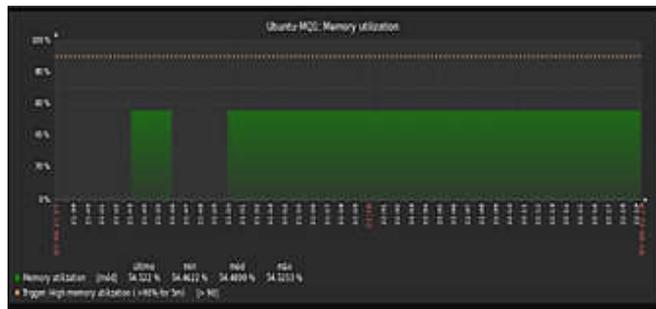
Source: The Authors, 2020.

Fig. 14. MQ1 memory consumption

Image 15 shows the CPU consumption of the monitored host:
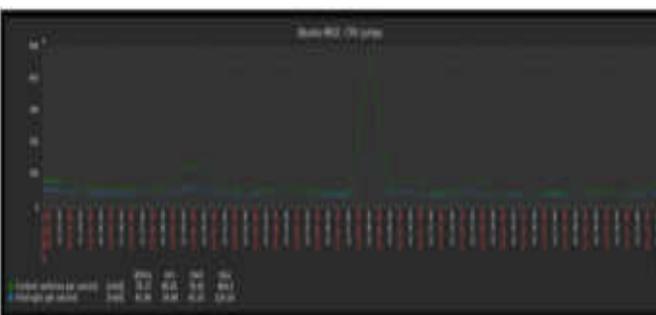
Source: The Authors, 2020.

Fig. 15. CPU consumption of MQ1

Nagios Core: To add a new host for monitoring in Nagios, it was necessary to make a copy of the file that is already configured called "localhost.cfg" located in the directory: "/usr/local/nagios/etc/objects/localhost.cfg" and copy the data to the "mq2.cfg" file with the command: "cp localhost.cfg mq2.cfg", opening it for editing: "nano mq2.cfg". In image 16, the changes are made by substituting the hostname "localhost" field for the host name to be monitored.
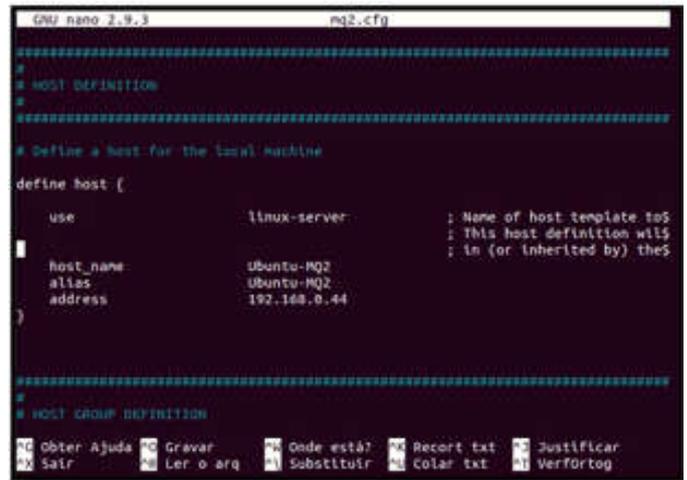
Source: The Authors, 2020.

Fig. 16. Configuring new host

After completing the changes to the file, it was necessary to perform a check with the command:

"/usr/local/nagios/bin/nagios -v
/usr/local/nagios/etc/nagios.cfg".

Image 17 shows a general summary of the error check:
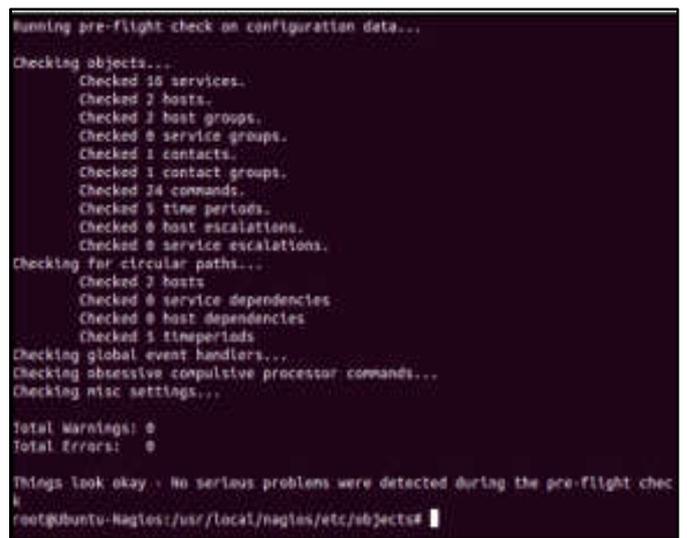
Source: The Authors, 2020.

Fig. 17. Error checking

Restarting the Nagios server to apply the changes:

"systemctl restart nagios.service".

Showing the host previously added, with the services active, as in image 18.
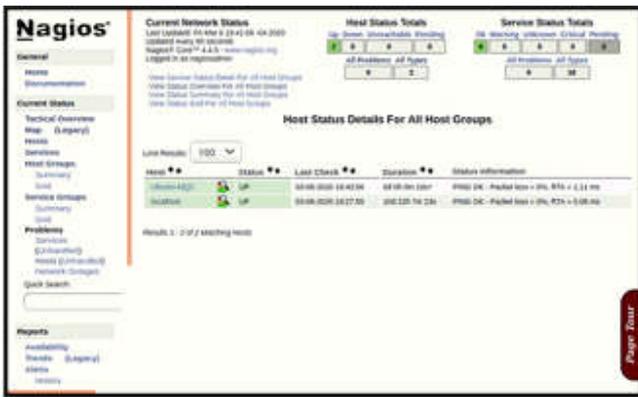
Source: The Authors, 2020.

Fig. 18. Home page with new Host

Nagios also has an area that shows all services being monitored on the machines, as in Image 19:

Source: The Authors, 2020.

Fig. 19. Active services

Comparison Resolution: Of the two tools used, Zabbix obtained a better performance in the processes carried out, its configuration had no difficulty due to the very clean documentation and there were no errors in any of the steps, the tool interface helps a lot both in the configuration of the hosts and in the additions groups and monitoring template and custom graphics. Device discovery is a great function for those who want to add multiple hosts automatically, the alerts shown are a guarantee in the network administrator's decision making. Nagios had a satisfactory performance, but the settings for adding new hosts and services need more time-consuming and detailed processes, as it is necessary to access files and modify them directly in the directories on the Linux system. However, this is not a problem for experienced users on the system..

Conclusion

The monitoring and management of the corporate network is essential due to the growth of technological systems making the network very decisive in decision making and important in the company's expenses and profits. Having the services and assets monitored in hand and having the best management tool according to the scenario of the company deployed, is an important choice for a more secure and long-lasting company life cycle.

The network security becomes more stable and reliable because with the use of monitoring tools it is possible to detect failures of essential systems in real time. With the results acquired in this comparative study between the tools such as characteristics, configurations and data analysis of the two software, it was possible to conclude that both Zabbix and nagios offer capacity, resources and solutions in the monitoring and management of networks, mainly corporate because both are free. Nagios showed that it is a complete tool and very adaptable in several network scenarios, as it has a high demand and it is very easy to receive plug-ins because it has a very active user community supporting the tool, however to configure Nagios it is necessary to have a high knowledge in handling files on the Linux system that for an advanced user does not make much difference. Zabbix precisely is more complete in all the processes covered, because its graphical interface and the way it operates, guarantees a more attractive form of usability, and can be used in several different ways, it has its agent for easy installation on devices and its main function of network discovery makes it more viable to implement the tools in networks with many devices.

Acknowledgments

REFERENCES

Adail, Horst; Aecio, Pires; Andre, Deo. DE A A ZABBIX. São Paulo: Novatec, 2015.

Bem-vindo ao VirtualBox.org! Available in: <https://www.virtualbox.org/>. Access in: fev 24th. 2020.

Lima, Janssen. Monitoramento de Redes com Zabbix. Rio de Janeiro: BRASPORT, 2014.

Nagios - brazilian Community. Available in: <http://nagios-br.com/nagios-core>. Access in: fev 21st. 2020.

Nagios O padrão da indústria em monitoramento de infraestrutura de TI. Disponível em: <https://www.nagios.org/about/overview/>. Access in: fev 20th. 2020.

Olups, Rihards. Zabbix 1.8 Network Monitoring. Birmingham: Packt Publishing, 2010.

Silva, Jeancarlo. nagios: Monitoração e Controle. Porto Alegre: Simplíssimo, 2018.

VirtualBox – Manual. Available in: < https://www.virtualbox.org/manual/ch01.html#virt-why-useful >. Access in: fev 24th. 2020.

Zabbix Documentation 4.4. Vladishev. Available in: <https://www.zabbix.com/documentation/current/pt/manual/introduction/about>. Access in: mar 05th. 2020.

****