Survey on Monitoring Of Network Using Open Source Software

[1]Prof. Amit Kore, [2]Mitali Bhat, [2]Ojaswini Gorana, [2]Anushree Ghugul, [2]Saumyak Saha

[1]Assistant Professor AISSMS's Institute of Information Technology, Pune, India

[2]Student AISSMS's Institute of Information Technology, Pune, India

Abstract: Network Monitoring is a basic requirement in an organization with enormous number of servers working within a network. To manually monitor those servers and their services is nearly impossible for an average human being. Thus, the concept of monitoring servers through software arose. One can monitor and analyze various servers and their services in one place i.e. on single main server. Nagios has been providing the same. However, Nagios does not complete the user's needs. Thus, software better than Nagios is required. The software will be open source, along with several nodes already added to it to monitor the performance of the servers in system in a better and less time-consuming way. The data will be collected, and real time statistics will be provided. Various reports can be generated to analyze the performance of the system offline. The main motive of the system is to make a better network monitoring open source software tool, by adding basics as well as important plugins, by making the GUI more interesting, reducing the back-end operations and making the system more efficient, and easy for layman.

Index Terms **– Network Monitoring, Computer Network, Open Source, MonIt, Data Visualization**

I. INTRODUCTION

In the 21st century, the need of Computers and Information Technology is increasing. Every organization across the globe are using computers and computer technologies. This increasing need of the technology also increases the security threats, or different types of failures. For the same reason, all the servers including the computers, switches and the routers need to be monitored around the clock. Hence the term monitoring of the computers comes into the picture.

In different organizations there are many servers working simultaneously. To individually check each server, when some failure occurs is a very hectic task. A software tool can help reduce the efforts by monitoring all the servers from a single main server.

Monitoring of a network is done based on different criterions, such as Up-time, Disk space, memory usage, traffic etc. Different tools are available to monitor a certain part of the servers and are modified as per the requirements. Instead of numerous modifications, a single tool covering all the important aspects can be built called as MonIt.

The main aim of the system is to provide the users with a software having much better specifications. MonIt has an improved Graphical User Interface, making it much more exciting to work with. Along with the GUI, the system is easy to be understood by anyone, even those who have no prior knowledge of networking. Data Visualization tool is also added in the system to give a pictorial representation of the network, making it much easier to understand the failures or the outages.

II. LITERATURE SURVEY

Paper [1] briefly discuss about the data centered monitoring of the network. Use of SNMP protocol and different open source protocols is done to monitor the systems effectively. It proves that the network monitoring tool is compatible and flexible for various open source platforms. The author explains that instead of focusing on different technologies, the users who are going to use the software should be taken into consideration first.

To monitor SNMP protocol, the devices, their agents and the servers are used. To use them effectively various technologies can be taken into consideration such as Nagios, Hyper HQ, Open NMS, Zabbix , Zenoss, etc. But not every user is well educated on these technologies. Hence the user's knowledge must be taken into consideration first. The author explains what type of software should be used by what type of the users. Nagios is mostly used software. It is open source software which gives basic virtual images. If the data needs to be handled manually then Hyper HQ can be used. Zabbix supports faster reporting capabilities. Whereas Zenoss is good at handling virtual networks.

All these tools were tested and it was concluded that every tool has its own drawbacks as well as advantages. For commercial use Hyper HQ makes more sense. But in most of the cases, open source software tools are preferable. These tools are more powerful due to their vast skill sets and lager community using them. Out of all the tools used, Hyper HQ is best one with most powerful results.

Paper [2] explains that the large organizations require a very efficient network monitoring system. They need fast reporting on the issues as soon as they arise. The author explains in these papers the continuous need of monitoring networks. It is also explained that these issues are reported to the administrator by using SMS or Email systems. This message contains the exact timing of the failure, where it is located, and how it can affect the rest of the system. To get this effectiveness the author recommends use of Nagios software along with the smart interaction Request Tracker.

In each network, there is a variety of people who are informed about these failures. Every person who is noted about the same has a priority, i.e. a certain person will work on a certain issue. Thus according to the problem, each individual is informed and called to resolve the issue.

Here Nagios is used to generate and monitor the network topology. It will send notifications about the issues. These notifications will create tickets in request tracker. Now the request tracker sends the emails or SMS to inform the individuals one by one.

The paper gives detailed explanation on how to configure the Request Tracker for Nagios. This is a very effective system that monitors the network very efficiently and handles the issues quickly.

In Paper [3] Author Describes about the flexibility of Nagios network monitoring software. Nagios provides users with good quality of service, uptime-downtime data transfer rates, Service Level Agreements. Nagios is easy to install on the servers, but it is complex to optimize and configure. Nagios makes use of web pages, so the end users can access the software. But for configuration users need to access via the back end.

The paper further explains the architecture of Nagios. It tells how to install and configure Nagios on different operating systems such as Windows, Linux, Fedora, Android. The paper also explains the advantages of network administration. Along with this, the paper tells how to configure the SNMP agent on Nagios.

It can be concluded that Nagios was developed for run time applications. While doing the same it provides with a good quality of service. The system proves that, the number of processes running on the server is directly proportional to the transfer rates of the servers. It can also be said that in future Nagios can work on windows, iOS as well.

In the paper [4] author describes about the Nagios network monitoring tool. The author states that Nagios is an easy and simple monitoring software with many functionalities. But the disadvantages and the limitations of Nagios are also given in the paper. The paper further explains that Nagios can be used to develop a better software, which will give a better performance and functionalities than Nagios.

Now a days the networks are becoming more and more complex, and there are less tools that can administer these networks. For the same reason different tools need to be integrated together to obtain the required functionality. But this makes the task more tedious. So, the need of better software arises. Instead of using many softwares together, one single software needs to be built. Since Nagios provides with much more functionality than other softwares, the new tool can be based upon Nagios.

Nagios has flexible functionality; thus, it allows users to develop different tools or integrations to the same. As the user needs, he can add the modules in Nagios itself.

The user proposes a system based on Nagios which is user friendly, and more interactive. This paper gives a brief explanation how to build a system that can be more powerful than Nagios, using innovative plug-ins and modules. This results in a complete new software tool to monitor network.

Paper [5] discuss that monitoring of network involves the collection of data to provide real-time statistics and analyze the performance of the network. When any device in the network fails then the network administrator should be up to date about the device failure or network failure, for this problem this paper suggest that there should be a secured alerting system which will inform the network administrator by the methods like, SMS, E-mail, or any other communication method.

In this paper, an open source tool “Nagios” is a popular network monitoring tool which consists of several plug-ins, add-ons, and that can be customized. Nagios is a lightweight software which provides monitoring of active protocols and network devices in the network topology, it is also able to provide graphs and trend analysis. The tool can monitor the status of the device connected in the network and notifies when the problem occurs in the network. The monitoring of the network is done using parameters like CPU status, Memory usage, disk queue, network collisions, disk usage, adapter transmit rate, etc.

Paper [6] discuss the possibility of centralized monitoring provides not only significant benefits but also provides the basis for the prevention of potential problems and incidents. There is much software available in the market which provides monitoring of network, some of them provide exceptional options, but it is important that the monitoring of the network should be from one single platform. The open source is better choice in order to understand the parameters like low-cost, efficient and scalable system for monitoring and managing the network.

The open source software which is in use already has advantage and disadvantages, they all depend on the specific requirements.

This paper also explains the basic requirements of monitoring network and use of Zenoss core- open source platform. The paper mentions two methods that depend on the way of communication with devices and types of protocols and tools. The first method based on the ICMP (internet control message protocol), by, using the Ping tool and ICMP message, it is possible to detect whether the device is in operational mode.

The second method based on the use of SNMP (simple network Management protocol), the SNMP uses UDP at OSI transport layer, and SNMP is most commonly used protocols for monitoring devices in the computer network. This method specifies the communication between the user running the monitored device and server.

Paper [7] discuss the need for tools for monitoring the activities of the computer network, computer network monitoring system consist of:-

1) a set of monitors,
2) single PC control and data analysis software
3) a network traffic generator.

Each computer to be monitored should be connected the internet like via telephone lines.

The computer network consists of nodes (use to switch data), transmission links, and terminals. A computer which will not switch data, then that PC is called Host. The transmission link is used to connect PCs and through transmission links, all connected computer form a network.

The fundamentals reasons for monitoring system- performance, detect malfunctions, diagnose the cause problems.

Paper [8], When there are several computers connected on the network then, a single PC monitor the whole network securely at the same time, personal computer safety is also important. This paper explains the problem with an example that if there is a network in the campus then there should be software that will effectively provide safety, reliability and steady running campus network, for the campus network.

The computer network is an important infrastructure in both aspects socially and officially. It is more important to keep the computer network secure from malicious attacks and unsafe factors.

The campus network is a distributed system. The network can cover large geographical area and the network is diverse since the usage of campus network consists of multiple domains which lead to large scale computing calculations, the CERNET platform needs fast speed can affect. Due to large structure is not complex then we should look for heterogeneity and dynamics in design. The main goal of network monitoring is to test the security of the network through inspection of the safety of the web server. It can detect suspicious activity and illegal activity to the system.

Paper [9], This reference link is the documentation of the existing Nagios Core tools. It provides all the installation guidelines, system requirements, and all other basic information. It also provides knowledge base for Nagios.

Overview of Linux and window monitoring is provided. It gives an idea about NRPE which is used to fetch the data from the hosts. The plug-ins are the base for the network monitoring. The plug-ins are nothing but the programs that are used to collect the performance data (for e.g. bandwidth, hardware information, etc) from the hosts.

Paper [10], Network monitoring is an important aspect to monitor and administer the network devices and services. Using network monitoring tools it is very easy to monitor the network devices, and also it reduces the burden on the network administrators as it uses automatic checking of the devices and gives the status and error reports accordingly.

Nagios- A network monitoring software, it's a flexible and extensible software used for monitoring of network, and also has a developer community. However, this software has many limitations, such as it is difficult to configure and it doesn't has an attractive user interface.

But, moreover there are some add-on's that are straight-forward and user-friendly. Administrator's still need to work on this to suit each network. Thus the adjustment of Nagios needs specific networks, demanding on expertise of network and system administrators.

Paper [11], nowadays it has become more important of Monitoring of Network in a modern complicated network. As now technology is increasing and network monitoring is becoming advanced, but as in past administrators was only used to monitor a few network devices or less than a 100 computers. In the past as the network bandwidth was only about 100Mbps; but nowadays for monitoring of network a larger bandwidth is required, and high speed networks more than 10 Gbps and also Wireless networks.

Nowadays, network administrators are constantly trying to maintain smooth operation of networks. Paper [11], it basically provides an overview of the network monitoring system used currently, the network architectures, their features, the network properties etc.

Paper [12], Network monitoring, is both inclusion of software and hardware, involving of both or a combination of both, which is used for constantly observing the status of the network devices and hosts, which is then gets notified to the network administrator via Email or via SMS or any other alarms in the case where there is an error occurred or failure of system. Status updates and error results are generated only when monitoring system speaks with the Networking devices or hosts by using different protocols.

The main aim of this paper is to develop a network monitoring tool, better than the previous versions. In the developing of monitoring tool, it is a combination of SNMP, ICMP and port scanning concept. It is a footstep of on how to develop a monitoring tool for the non-expertise network programmer for monitoring of network and host devices.

Paper [13], In spite of all the revolution one thing remains constant i.e. Network monitoring system software. By using network monitoring it is easy to keep an eye on the network, whether it is WAN, LAN, VoIP, and MPLS etc.

Before using network monitoring, it is very essential to understand it, as well as all the essentials about the Windows® Systems, which is used in general all over the globe. Here, Networks can be categorized based on the geo area such as LAN, WAN, or Internet. Topologies of the network can also differ based on the organizational requirements. Examples of topologies: Star, Bus, Ring etc.

Some of the general techniques of monitoring are as follows; these are the techniques which are used for the collection of data monitored from the network.

1. Ping
2. Simple network management protocol (SNMP)

Paper [14], Network monitoring is an important aspect in monitoring of network devices, Monitoring helps the network administrators to identify possible issues before affecting the business continuity, and before affecting find the solutions to it. Whether it is a small business with 100 nodes or a large scale business with 1000 nodes, continuous monitoring of network helps to maintain a high speed performing with a very small downtime.

For network monitoring, the design is also an important aspect; the design should adopt some basic principles. Such as it should be comprehensive and should cover all the aspects of an enterprise for i.e. Connectivity and networking as well as security.

Network management is also an extensive field including various functions. Various objectives of management of network are classified and grouped into 5 major categories, which are as follows:

1. Fault tolerance (F),
2. Configuration Management(C),
3. Accounting Management, Performance Management (P), and
4. Security Management (S)

It is together known as FCAPS. Here, billing is not required only accounting is been replaced with administration.

III. Future Scope and Research Area

Large organizations need to be monitored consistently around the clock. But some organizations are large enough that they occupy a few floors of the building. In such organizations to monitor the network, a hierarchy of monitoring system can be used. A floor will be monitored using a sub main server on that floor. Then there will be another main server which will monitor these sub main servers. This will help in increasing the speed of the internet on the individual server, since we are using parallel networking.

IV. CONCLUSION

Monitoring of a network is done based on different criterions, such as Up-time, Disk space, memory usage, traffic etc. In different organizations there are many servers working simultaneously to individually check each server is a very tedious task. A software tool can help reduce the efforts by monitoring all the servers from a single main server. Different tools are available to monitor a certain part of the servers and are modified as per the requirements. So, in this system we have discussed in brief about the software tool to be designed, having the functionalities that can overcome the previous tools that were built such as, open source, easily understandable and with better performance. Thus, making it reliable and user-friendly. We also reviewed other methods which overcomes the traditional systems with higher accuracy possibility. We also discussed about scope and limitation of this systems. We hope our study paper help others in monitoring of the huge networks from a single main server and direction for future research and work.

V. REFERENCES

[1] A. KAUSHIK, "USE OF OPEN SOURCE TECHNOLOGIES FOR ENTERPRISE SERVER MONITORING USING SNMP," vol. 02, no. 07, pp. 2246–2252, 2010.

[2] R. Khan, S. U. Khan, R. Zaheer, and M. I. Babar, "An Efficient Network Monitoring and Management System," vol. 3, pp. 1–5, 2013. [Online].
Available: 10.7763/IJIEE.2013.V3.280

[3] C. Issariyapat, P. Pongpaibool, S. Mongkolluksame, and K. Meesublak, "Using Nagios as a Groundwork for Developing a Better Network Monitoring System," pp. 2771–2777, 2012.

[4] S. M. Magda, A. B. Rus, and V. Dobrota, "Nagios-Based Network Management for Android, Windows and Fedora Core Terminals Using Net- SNMP Agents," pp. 1–6, 2013.

[5] J. Renita and N. E. Elizabeth, "Network's Server Monitoring and Analysis Using Nagios," pp. 1904–1909, 2017.

[6] M. Ljubojević, A. Bajić, and D. Mijić, "Centralized monitoring of computer networks using Zenoss open source platform," 2018.

[7] D. E. MORGAN, W. BANKS, D. P. GOODSPEED, and R. KOLANKO, "A Computer Network Monitoring System," pp. 299–311, 1975.

[8] L. L Xingyu and J. Tingting, "Design and Implementation of the Campus Network Monitoring System," pp.117-119,2014.

[9] https://assets.nagios.com/downloads/nagioscore/docs/, 2012.

[10] S. Mongkolluksamee, P. Pongpaibool and C. Issariyapat ," Strengths and Limitations of Nagios as a Network Monitoring Solution," 2015. [Online].
Available:
https://www.researchgate.net/publication/267366269_Strengths_and_Limitations_of_Nagios_as_a_Network_Monitoring_Solution

[11] Jakub Svoboda, Ibrahim Ghafir, Vaclav Prenosil," Network Monitoring Approaches: An Overview," Oct 2015. [Online].
Available:
https://www.researchgate.net/publication/305957483_Network_Monitoring_Approaches_An_Overview

[12] Ahmed Kijazi, Kisangiri Michael," A Step on Developing Network Monitoring Tools," 2014. [Online].
Available:
https://www.researchgate.net/publication/283210566_A_Step_on_Developing_Network_Monitoring_Tool

[13] https://thwack.solarwinds.com/community/resources/guides/basics-of-network-monitoring

[14] https://thwack.solarwinds.com/community/resources/guides/network-monitoring-design-philosophy?CMP=ORG-BLG-THW