Network's server monitoring and analysis using Nagios

Conference Paper · March 2017

DOI: 10.1109/WiSPNET.2017.8300092

2 authors:

Renita Johnson
Society for Electronic Transactions and Security
6 PUBLICATIONS **17** CITATIONS
SEE PROFILE

N. Edna Elizabeth
Sri Sivasubramaniya Nadar College of Engineering
30 PUBLICATIONS **205** CITATIONS
SEE PROFILE

This full-text paper was peer-reviewed and accepted to be presented at the IEEE WiSPNET 2017 conference.

Network's Server Monitoring and Analysis Using Nagios

J. Renita[1] and N. Edna Elizabeth[2]
Electronics and communication Engineering, SSN College of Engineering, Kalavakkam, Chennai-603110
Email: [1]renitajesther@gmail.com [2]ednaelizabethn@ssn.edu.in

***Abstract*—Network Monitoring is a procedure used to monitor a computer network system and notify the network administrator in case of any outages. It is necessary to diagnose and report the issues that would lead to failure or irregularity in the network. The performance and usage of a network can also be monitored. Network monitoring can be done as server and application monitoring. The process of monitoring server's system resources like CPU Usage, Memory Consumption, I/O, Network, Disk Usage, Bandwidth etc. is Server Monitoring. In this paper, server monitoring is done using Nagios, which is an open source tool. Several nodes are added to the network and the performance and status of the network are monitored. The data is collected and real time statistics is provided and the performance of the network is analyzed. The main motive is to alert the network administrator by methods like SMS or E-mail in case of any failure in the network. This helps in securing the network by alerting the potential issues in real time.**

***Index Terms*—Nagios, Server monitoring, CPU Usage, Memory consumption.**

I. Introduction

The external devices that are connected to the network have to be monitored at regular intervals in real time. Monitoring the network deals with the collection of data to provide real time statistics and to analyze the performance of the network. When an outage or failure occurs in the network, the network administrator has to be informed. The network has to be secured by alerting the potential issues before they become major problem. Methods like SMS, E-mail and Pager can be used to alert the network administrator regarding the failure in the network.

The term Network monitoring is used to describe a system that is helpful in monitoring the network topology continuously and finds if there is any jamming, slowdown of system or component failure and immediately notifies the network manager via E-mail, SMS or any other alarms in case of any problems. Network monitoring is found to be of no use unless the right things are tracked. The usual areas that are examined include bandwidth usage, Server performance and Application performance. Server monitoring is an important part of any data center monitoring architecture, but too often it becomes an essential process in successfully building out a holistic monitoring platform. Server monitoring consists of monitoring the operating system and its associated hardware metrics for servers that run the application. It's the view of the world from the perspective of the server, but never from inside the running processes. Basic server monitoring metrics include CPU system time, CPU wait time, used memory, free memory, disk queue length, disk usage, network collisions, adapter transmit rate, etc. Server monitoring is used by every IT organization in some shape or form. All Monitoring tools run on the SNMP protocol. Open source market includes many options like Nagios, Cacti, Zenoss, Zabbix, Open NMS etc. The basic need for monitoring depends on the type of business that is being carried out by the organization. There has been always a competition between open source and commercial solutions but many companies tend to acquire open source projects by introducing different version of projects for commercial and open source market. Various parameters based deployment, reporting, notifications; triggers, alerts, resource usage etc. are being tested [2]. Nagios is the most popular monitoring system and is made up with almost all linux distributions. There are several other plugins, add-on scripts that can be customized and used along with the tool. Nagios is a light weight program and provides a perfect monitoring tool that can be helpful to monitor all the active protocols and network devices connected to the network topology. It is also capable of providing real time comprehensive graphs and trend analysis. Cacti tool is found to be a performance monitoring tool based on a LAMP stack (Linux/Apache/MySQL/PHP) and has RRD (Round Robin Database). The process done in Cacti includes collection, management and display of graphs of the collected data. Some distributions (i.e., Fedora) also supply a version in their repositories. However, an important architecture plugin feature of cacti has to be patched in. Cacti use Round Robin Databases (RRD) and MySQL database technologies to store the collected information. MySQL and PHP are used to provide a graphical, web based interface to the RRD databases. Zenoss tool was developed by Bill, Erik Dahl and Mark Hinkle. The tool is accomplished of monitoring all devices, servers, network and application inside data center. The core database and the events are stored in My SQL database. The tool comes with an integrated package that contains all combined modules. Zabbix was developed by Alexei Vladishev, and was first released in 2001. The current stable version of Zabbix is 1.8.3. It can monitor the basic SMTP, HTTP, ICMP services without installation of agents. Zabbix has three core modules for its functioning i) Daemons ii) Agents iii) Web interface. As name suggests Open NMS, initially a Network Management System and one of the oldest monitoringsoftware in early 2000's open source leaders were only Nagios & Open NMS. Open NMS recognizes servers in data center and services are linked to the interfaces.

978-1-5090-4442-9/17/$31.00

In this paper, an approach is presented to monitor the devices in the network. A tool named Nagios is used to monitor the server and the applications that run in the network. The tool can monitor the status of the device and can perform status check and notifies when there occurs any problem in the network. The use of external plug-in helps in notifying the network manager about the problem in the network.

Section II includes the related works of different authors and their proposals. Section III deals with the details about the tool and the methodology used for server monitoring. Section IV shows the results and graphs obtained. Section V give the conclusion and further enhancement that can be done to this work.

II. Related Works

Network's Server monitoring helps us in understanding the System's resource usage which can help in improving the capacity planning and provides a better end-user performance.

Fung Po Tsoa et al., (2016) has presented a survey on managing the server and network resources. The survey also includes virtual machine allocation and its management to improve the utilization and cost efficiency of the physical servers. The author has used Software defined networking principles and has discussed about the challenges and opportunities for converged resource management [5].

Sihyung Lee et al., (2014) discussed the open problems in network monitoring and suggested guidelines for the future network monitoring system. The author has analyzed about the integration of the present technologies with the entire network monitoring operations and has also focused on network monitoring technologies [11].

Rafiullah Khan et al., (2013) have suggested an effective and automotive network monitoring system to monitor the network switches and informs the administrator when switch goes down. The presented network monitoring system can easily identify the network problem and its effect and is found to be efficient providing full control over the network [9].

Adam kucera et al., (2013) has suggested that different types of management are done with increasing size of the Building Management systems and has concluded that Nagios can be utilized for monitoring servers [1].

Ahmed D. Kora et al., (2012) has discussed about the open and adaptable platform that supports fault and configuration management for next generation network and also offers additional features for application and management function to enable easy and low cost management of new technologies and services [2].

T. Michael Silver, (2010) has discussed about the implementation of monitoring system using an Open Source software package to improve the availability of services and to reduce the response time when troubles occur. He author has also provided details about Nagios to monitor servers and WAN and has concluded that installation of software takes more time and computer resources [6].

Thomas Davis et al., (2009) has presented a comparative study on Nagios, Cacti and the method of installation and benefits by providing details on the system status in standardized way. The author has also concluded that the system provides data in a more proactive management style instead of reactive management style of system to be used and provides a valuable insight into the system's status in a standardized way and reduces staff training [12].

C.H. Philip Yuen et al., (2012) has done a study of the real time monitoring network with multiple monitors for large scale applications. A study based on the highly scalable monitoring devices for distributed applications was done. The problem is formulated to construct overlays which are used in minimizing monitoring delay. A Simple, efficient and scalable monitoring algorithm SMon was introduced in order to reduce the monitoring delay and reduces network diameter in real time and in a distributed manner [8].

Anshul kaushik, (2010) has covered the choice of monitoring of various servers using SNMP protocol and providing open source solutions. The author has also compared many open source tools like Zabbix, Zenoss, Nagios and Open NMS and has concluded that Nagios is a good package and is being used by masses [3].

Antonis Papadogiannakis et al., (2012) have proposed an approach for improving the runtime performance of a large class of CPU and memory intensive passive monitoring applications. The improvement of packet processing performance is done in this work by enhancing the locality of code and data access. The author has presented a new approach called locality buffering to improve the runtime performance of a large class of CPU and memory intensive passive monitoring applications [4].

TABLE I
Nagios Objects and Function.

Object	Purpose
Hosts	Servers or devices being monitored
Host groups	Groups of hosts
Services	Services being monitored
Service groups	Groups of services
Time periods	Scheduling of checks and notifications
Commands	Checking hosts and services notifying contacts processing performance data event handling contacts individuals to alert contact groups of contacts

III. Methodology

The selection of a specific software mainly depends on the services that are being monitored and the goals for monitoring. Nagios is found to have wide range of users and offers higher functionality than other open source tools. The software is found to have a good history of active development, a large and active user community and a significant number of included and user contributed extensions. Because of the flexibility of the software design that uses a plug-in architecture, service checks for library-specific applications can be implemented.

Table I shows the Nagios objects and their purpose [6]. The network administrator has to ensure whether the server is

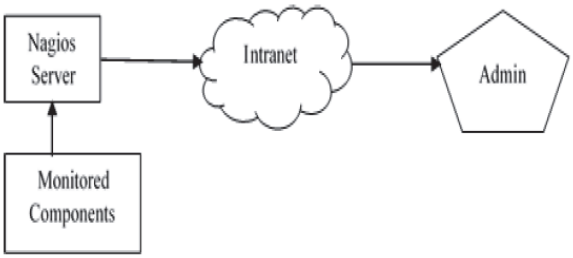

Fig. 1. Nagios monitoring.

functioning properly. If the border router or Internet connection goes down, Nagios will be unable to deliver email alerts to administrators. This allows an administrator to immediately begin investigating the problem and get the primary Nagios server back online.

Fig. 1 explains the process of Nagios monitoring where the status of the monitored components are collected by the server and the notifications are send to the administrator through intranet. The tool is installed in Ubuntu using VM Ware workstation in ISRO. The credentials have to be supplied in order to access Nagios. Using Nagios Mail server, SNMP server, Nagios server etc. can be easily monitored. Initially, the configuration wizard has to be uploaded and managed in core configuration manager. Fig. 2 explains the flow chart of server monitoring process done in Nagios tool. The IP address of the server is added. Four servers are added to the configured system of ISRO. The servers are 192.168.100.28, 192.168.100.88, 192.168.100.50 and 192.168.100.19. The IP address of the server is configured and the configuration wizard is made to run.

The address and the URL of the primary Nagios server are supplied. The authentication credentials used to login to the primary Nagios web interface is supplied. Host name has to be specified for identification purpose. Hence, a specific host name is provided to the server. The server metrics like ping, I/O Wait, Web interface etc. is selected for monitoring. The configuration is finished and new Servers (hosts) are created for monitoring. The servers are added in order to check their current working status at regular intervals. The representation of server in green indicates the server is Ok, Red indicates the server is Critical and orange indicates the status of the server is unknown.

The tool is configured in such a way that the error notification is send via e-mail. The SNMP address, IMAP address and the mail address of the network administrator has to be specified for mail alert to occur. The e-mail address of the network administrator is given and alert mail is received when the server is critical. A second notification mail is send to the network administrator from Nagios to recover the server that is critical. The e-mail alert is repeated until the server is recovered. Fig. 3 explains the proposed methodology. Initially, the IP address of the servers is added and the protocols for monitoring the server are chosen. The condition of the server is pinged to the administrator. In case when there is no ping

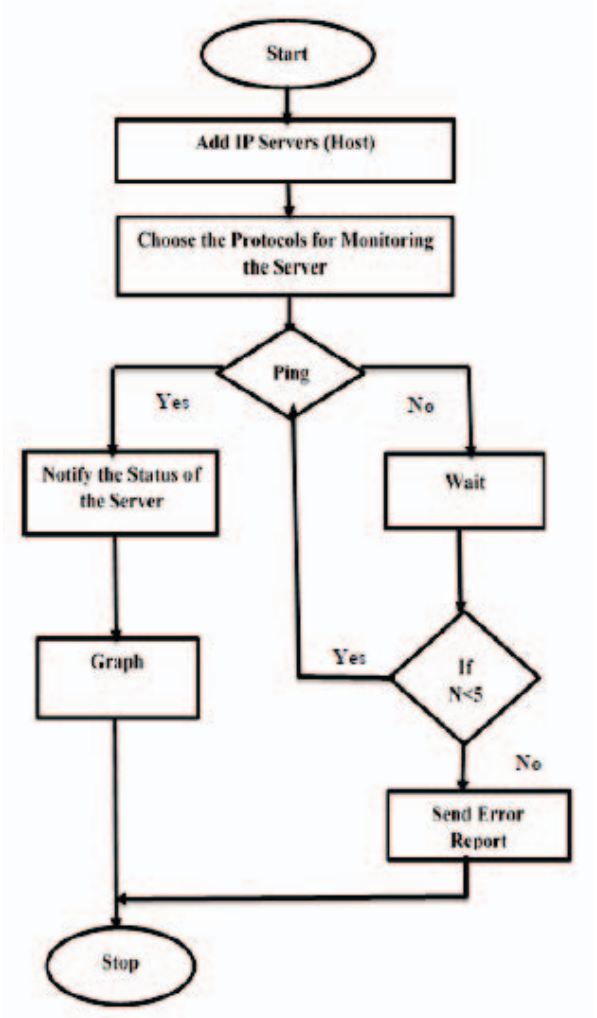

Fig. 2. Flow chart for server monitoring.

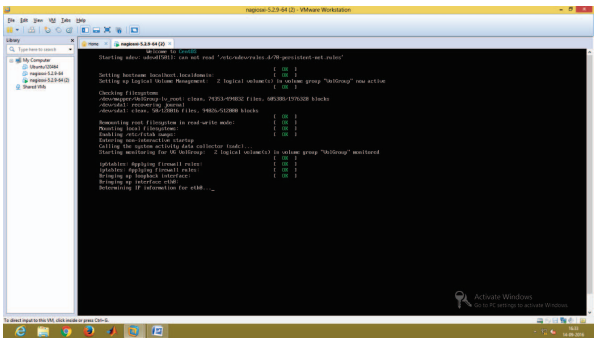

Fig. 3. Importing Nagios in VM ware and Nagios setup.

from Nagios the process is repeated up to five times. After that error report is send to the network administrator of ISRO saying that there is system failure.

IV. Results and Discussions

In this section we discuss about the results obtained when Network's Server was monitored in ISRO, Sriharikota. The interpretation to the results obtained is also discussed. Nagios

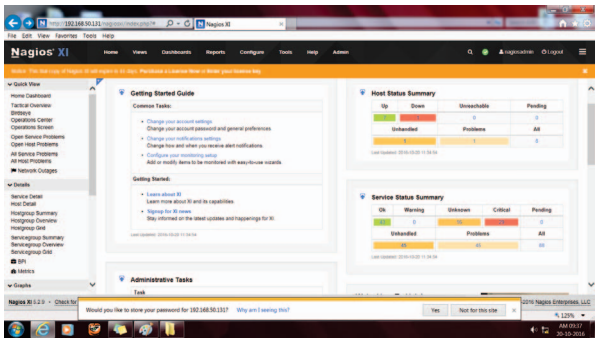

Fig. 4. Nagios-home.

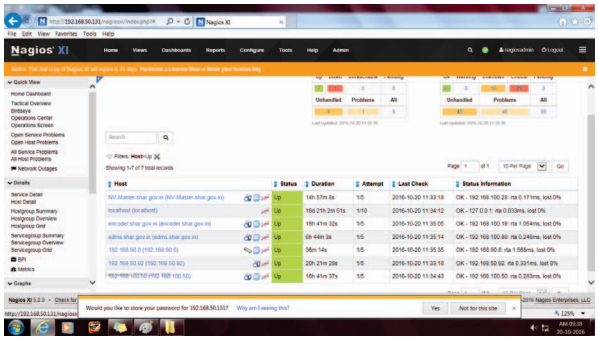

Fig. 5. Host-up.

was initially installed and configured and the following results were obtained.

Fig. 3 shows the initial procedure in which Nagios is imported in VM ware workstation using Ubuntu. The tool was accessed using the server 192.168.50.131. Username and password are given to login to Nagios home. The initial set up can be made in the Workstation. The network topology is made by defining the nodes in the directory.

The host and the host group have to be configured and the contacts are added. This is done in order to alert the contacts in case if there is any failure in the server. The software is configured in such a way that the entire network is monitored for every 10 s. Nagios can take 5 re-attempts when the service is unavailable. After that error state is updated in the status column. Fig. 4 shows the homepage of Nagios where the configuration wizard is made to run.

After the server (host) address is added, the monitoring is done at regular intervals. The servers that are in OK condition are represented in green. Fig. 5 shows the host up status. Fig. 6 shows the servers that are in critical condition. When the service is unavailable or if there is any error in the server it is represented as CRITICAL condition.

Fig. 7 shows the monitoring graph for 192.168.100.50 server. Here Round trip average, packet loss, round trip maximum and round trip minimum were monitored at an interval of 4 h.

When traffic is high, rtmax will be high (peak). The time duration taken for request and response will be high. Details are stored in a database. Packet loss is zero in this host because

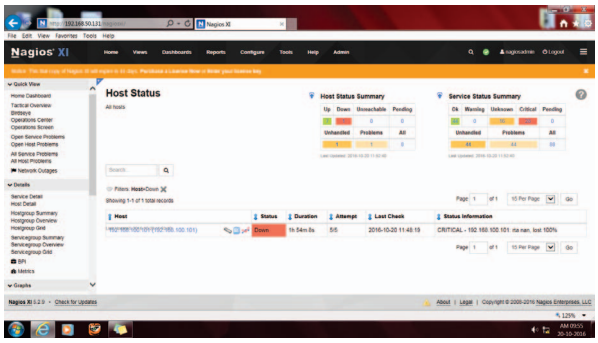

Fig. 6. Host-down.

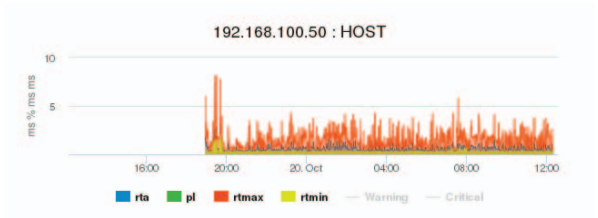

Fig. 7. Monitoring graph of 192.168.100.50.

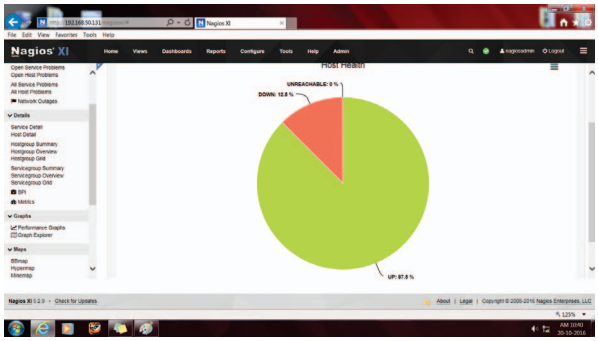

Fig. 8. Host health.

of sufficient bandwidth availability. The monitoring is done at an interval of four hours. The monitoring process continues and the status of the server is checked at regular intervals.

Fig. 8 shows the host health of the servers that are added to the network. The current status of the hosts and switches added to the server is shown in pie diagram. Fig. 9 shows the hyper map representing the servers that are OK and CRITICAL in the network. The location of servers and switches located in the network is plotted with respect to distance and their status (Ok or Critical).

Fig. 10 shows the mine map representing the servers that are added to the network topology. The status grid of Host is shown in tabulation form. Fig. 11 shows the notifications that are given by the Nagios monitoring tool along with the reason for the failure at a particular interval of time. In this case network admin is contacted.

Fig. 12 shows the status of the server that is being monitored. This includes load time, CPU status, memory and swap

Fig. 9. Hyper map.

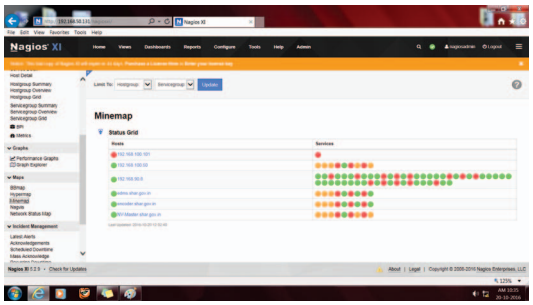

Fig. 10. Mine map.

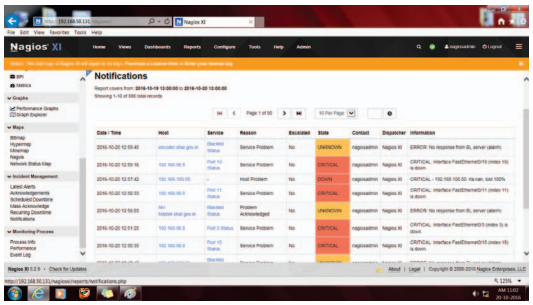

Fig. 11. Notifications.

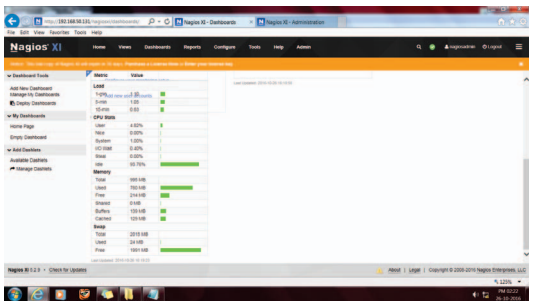

Fig. 12. Server status.

and their usage. Server monitoring uses the status of these server metrics for monitoring.

Fig. 13 shows the e-mail notification received from Nagios monitoring system. In case if there is any failure in the system the network administrator gets the notification e-mail.

A second mail is received that intimates the network administrator to recover the fault in the server. This e-mail alert is repeated until the system is recovered. The results show that

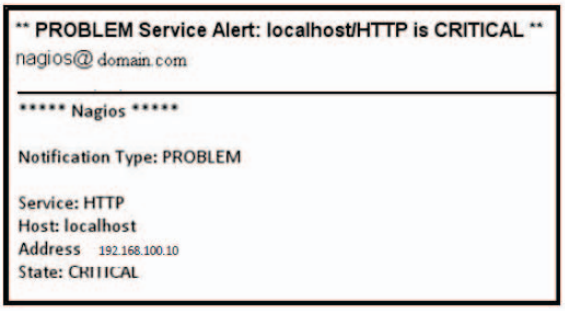

Fig. 13. E-mail notification.

Nagios monitoring can be easily done to the servers that are connected to the network topology and notifications are sent via e-mail to the network administrator in case if there is any network outage.

V. Conclusion and Future Enhancements

In this paper, a network monitoring system is presented that informs the network administrator in case of any failure in the network topology. Network monitoring was done in ISRO, Sriharikota. Server monitoring was given more importance and the server metrics like CPU status, Memory usage and load time etc. were continuously monitored and their corresponding status was checked at regular intervals. The tool was configured in such a way that the network administrator gets e-mail when there is any system failure. E-mail Notification is repeated until system recovery is done by the network administrator. Performance results were obtained for the servers that are being monitored.

The performance graphs for the server are obtained only with the help of plug-in. Hence for further development of the project, the logs or database of Nagios has to be checked. The database has to be built using MYSQL or any database. The display has to be designed based on the requirement of ISRO.

Acknowledgements: This work is a part of Network Monitoring used in Indian Space Research Organization, (ISRO), Sriharikota.

References

[1] Adam kucera, Petr Glos, and Tomas Pitner, "Fault detection in building management system networks," in *IFAC Proceedings*, 2013, pp. 416–421.

[2] Ahmed D. Kora and Moussa Moindze Soidridine, "Nagios based enhanced IT management system," *Interntional Journal of Engineering Science and Technology*, vol. 4, no. 3, pp. 818–822, 2012.

[3] Anshul kaushik, "Use of open source technologies for enterprise server monitoring using SNMP," *International Journal on Computer Science and Engineering*, vol. 02, no. 07, pp. 2246–2252, 2010.

[4] Antonis Papadogiannakis, Giorgos Vasiliadis, Demetres Antoniades, Michalis Polychronakis, and Evangelos P. Markatos, "Improving the performance of passive network monitoring applications with memory locality enhancements," *Computer Communications*, vol. 35, pp. 129–140, 2012.

[5] Fung Po Tsoa, Simon Jouet, and Dimitrios P. Pezaros, "Network and server resource management strategies for data centre infrastructures: a survey," *Computer Networks*, vol. 106, pp. 209–225, 2016.

[6] T. Michael Silver, *Monitoring network and service availability with open source software*, Information Technology and Libraries, pp. 8–15, 2010.

[7] Nicola Bonelli and Stefano Giordano, "Network traffic processing with PFQ," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 6, pp. 1819–1833, 2016.

[8] C. H. Philip Yuen and S. H. Gary Chan, "Scalable real-time monitoring for distributed applications," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 12, pp. 1226–1235, 2012.

[9] Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer, and Muhammad Inayatullah Babar, "An efficient network monitoring and management system," *International Journal of Information and Electronics Engineering*, vol. 3, no. 1, pp. 122–126, 2013.

[10] Roger Burton West, "Open source network monitoring software," *ITP Journals*, no. 124, pp. 3–6, 2000.

[11] Sihyung Lee, Kyriaki Levanti, and Hyong S. Kim, "Network monitoring: Present and future," *Computer Networks*, vol. 65, pp. 84–98, 2014.

[12] Thomas Davis and David skinnes, "Software monitoring using Nagios, Cacti and Prism," in *CUG Proceedings*, 2005, pp. 1–5.

[13] Zhenqi Wang, Yue Wang, Guangqiang Shao, and Ziyan Guo, "Research and design of network servers monitoring system based on SNMP," in *Education Technology and Computer Science, ETCS'09. First International Workshop*, 2009, vol. 3, pp. 857–860.

[14] Zhenqi Wang, Yue Wang, Guangqiang Shao, and Ziyan Guo, "Research and development of monitoring system for network servers," in *2008 4th International Conference on Wireless Communications, Networking and Mobile Computing*, 2008, pp. 1–3.