# Performance Analytics of Network Monitoring Tools

**Deepak Chahal, Latika Kharb, Deepanshu Choudhary**

***Abstract*: Network is considered to be one of the most critical resources in an organization, and managing the networks for high performance and reliability is a great challenge. Therefore a fast and smart network monitoring system is always required in different organizations, and for the purpose of monitoring and troubleshooting related issues, Network monitoring tools are often used. In this paper, we discuss some popular network monitoring tools such as Nagios, Zabbix, Hyperic, Capsa free, ganglia etc. We then present a comparison among all the considered monitoring tools based on the different parameters like license, data storage method, access control, platform, logical grouping and distributed monitoring.**

***Index Terms*: Network monitoring, Nagios, Zabbix, Kiwi Monitor, Ganglia, Wireshark.**

## I. INTRODUCTION

Network monitoring is considered to be an important part of network resource management, which is responsible for constantly monitoring computer network [1]. It can be achieved by monitoring the network problems that are caused due to over loaded and/or crashed servers, network connections or other devices. For monitoring the network, a ping is use to sent the system, and if there is any delay in responding back or it does not responds then network monitoring system takes the responsibility [2]. The monitoring depends upon three common parameters such as delay, jitter that is failure of synchronization, and bandwidth. If any of these problems get configured, the alerts go to the administrator via email, SMS, pager alerts, or by other alarming technique. Therefore using the concept of network monitoring, the network becomes efficient in use and also increases the performance and improves the reliability of the network. Network monitoring tools are necessary for the implementation of the concept of network monitoring. These monitoring tools are typically set up by the System Administrators, and helps in achieving a reliable and quick start in monitoring the network [3]. So it is necessary for a monitoring tool to run all the time. There are several network monitoring tools, and selection of a right monitoring tool can be based upon the alerting and integration with the existing system, functionality, scalability, deployment, maintenance and also the price which not only includes the software license cost but also includes the cost involved in staff training [4]. The objective of this paper is to present an overview of some commonly used networking monitoring tools. We also present a comparison based on the several parameters.

## II. MONITORING TOOLS

This section deals with the discussion of various monitoring tools, their features, advantages and disadvantages.

### *A. Nagios*

Nagios is a real time network monitoring tool created by Ethan Galstad, and was launched in 1999. It is licensed under GPL v2, and is an open source monitoring tool [5]. One of the best feature of Nagios is the great scalability of its configuration. One can configure the hosts, services, contact to groups, and alert escalation plan because of its feature of configuring with the text files. However this tool requires trained IT-staffs, and allows user for the customizations of the hosts and services checks. The tool not only monitors the services like SMTP, PING, HTTP but also the hardware resources like usage of memory or disk [6]. Nagios consists of Nagios library which makes a larger number of plug-ins available for the users expanding its monitoring capabilities, and also helps in adapting the updated technologies, applications and systems with no updates in it. Nagios supports the escalation, so that if the problem is not acknowledged by the administrator within a predefined frame then alerts are immediately sent to the second authorized person based on the priority for resolving the problem [7]. When Nagios is combined with Request Tracker (RT) it gives an efficient and automatic network monitoring which is intelligent enough to identify the problem location, and its effects on rest of the network. In fact the notifications sent by the Nagios generate ticket in RT, sent to the administrator via email. For resolving the network problem configured, the administrator can access the RT server remotely and just changes the ticket status to ‘resolve’ [1]. In a wireless environment, Nagios can also identify the size and the nodes located in the network [2]. It can monitor the hard drive, space, uptime and down time of each node present.

**Revised Manuscript Received on June 14, 2019**

**Deepak Chahal**, Professor, Jagan Institute of Management Studies, Sector-5, Rohini, Delhi, India.

**Latika Kharb**, Professor, Jagan Institute of Management Studies, Sector-5, Rohini, Delhi, India.

**Deepanshu Choudhary**, Student Scholar (MCA), Jagan Institute of Management Studies, Sector-5, Rohini, Delhi, India.

*Published By:*
*Blue Eyes Intelligence Engineering*
*& Sciences Publication*

The threshold can be set up by the network administrator. If the usage of bandwidth constantly arises and hits the threshold set by the administrator then an alert is sent by the Nagios. Nagios notification is based upon the internet connection, so if the internet goes down then emails to the administrator cannot be sent and log files gets generated which informs email cannot be send [2].

### B. *Zabbix*

Zabbix is an open source network monitoring tool created by Alexie Valdishev, and was released in 2005 [8]. The installation of Zabbix is easy but difficult to configure and maintain [5]. For storing the data Zabbix packages uses MySQL, SQLite or Oracle. This tool not only monitors the network services, servers and network hardware but also databases, applications and VMware by using agent-based and agentless approaches. It uses Intelligent Platform Management Interface (IPMI) for hardware monitoring and collects information about temperature, fan speed, chip voltage and disk state [4]. For host monitoring, agents can be used which can be installed on UNIX and Windows, and runs as native system process which does not require any specific environment unlike java or .NET [9]. For agentless monitoring of host simple checks are done which includes SNMP, TCP, ICMP, HTTP. Zabbix uses trigger and action events for monitoring. In trigger, a key is evaluated, if trigger's state changes on the key changes, the system is responsible to send an email to the administrator which is done by adding an action event. Zabbix consists of templates made up of several items and triggers but does not contain any action so any host is linked with these templates has to define their own actions [7]. Zabbix sends alert to the admin via email, jabber messages or text messages to the mobile phone.

### C. *Hyperic*

Hyperic is a monitoring and management software licensed under GPL which is optimized for physical environment as well as for virtual environment [5]. The installation and configuration of Hyperic monitoring tool is easy and takes very less time. Hyperic consist main components such as Hyperic agent which is lightweight java-based client and is responsible for discovering system metrics, Hyperic Use Interface where discovered resources are presented, Hyperic server and Hyperic database [10]. It can monitor applications on almost every operating system including Linux, Unix, Windows, Solaris, AIX, HPUX, VMware and also on Amazon Web Services. It has the ability for auto-discovering components required by virtual applications and the resources [11]. Hyperic monitoring tool reduces the operation workload and increases the IT management maturity level. It can also monitor the logs, configuration files and can remotely control the software resources. Hyperic is available in two version, Hyperic HQ and vFabric Hyperic. Hyperic HQ is an open source version and takes the responsibility of monitoring system components such as CPU [7], network interfaces and the file systems, whereas vFabric Hyperic is a paid version and has more features than Hyperic HQ such as automated corrective actions. Hyperic can send alerts to the network administrators via email, SMS and SNMP trap [4]. However Hyperic has disadvantage of the cost of resources by Java Virtual Machines (JVM).

### D. *IBM Tivoli*

IBM Tivoli monitoring tool supports many operating systems such as Windows, Linux and Unix. It is easy to install but need an IT expert for configuring, updating and refining the analytical and response features. It has a good and intuitive web interface. IBM Tivoli provides many software services which makes possible sharing information and collaboration which are required for achieving common business goals [12]. It is capable of utilizing the sensors present in the data centers for determining temperature, air flow, humidity, power, water leak, and security related problems easily and efficiently [13]. IBM Tivoli contains three major components, monitoring agent responsible for collecting the information which gets deployed in VMs, data collection server and ware house responsible for consolidating and managing the collected information and the portable presentation component which is responsible for presenting monitoring status and analyzing the collected information [14]. If any issue is configured, it is automatically gets repaired. It also helps the user in monitoring the hypervisor and the workload on it [13]. The network admins can be alerted by email and SMS using this tool.

### E. *SolarWinds*

SolarWinds monitoring tool has an excellent GUI and supports operating systems such as Windows, Mac, Linux and Unix. The installation time of SolarWinds depends upon the complexity of the configured data such as locations or tickets [5]. It can be customized by the user which helps to ease the monitoring, can be accessed by mobiles, and supports VMware. It can monitor wireless access points, the private, public as well as the hybrid clouds environment, and can identify the occurrence of the problems. It can automatically plan the storage capacity for best utilization. The file integrated as well as USB device monitoring can also be done using this tool [15]. SolarWinds presents the monitoring status such failures, performance and availability of the network in the form of detailed graphs. It provides SolarWinds Orion which is scalable, cost-effective and is built upon Simple Network Management Protocol (SNMP) [16]. It is designed for real-time monitoring of many network performance metrics such as availability and bandwidth utilization and can automatically discovers and configures the devices to be monitored [17]. In SolarWinds, alerts are based on simple and complex nested trigger conditions, and it notifies the network administrators via emails.

### *F. Kiwi Monitor*

Kiwi Monitor software allows the user to monitor their processes or applications, and records the data and creates an alert in accordance triggers which are pre-defined by the monitoring tool [18]. It is capable of showing the runtime of the window and activities of the users. It doesn't have any Spyware or Adware and it is a Freeware. It also allows the users for selection of applications from the build-in process viewer or enters an application's name. In kiwi monitor, small programs are used for starting with windows using small system resources in the background [19]. Kiwi Application Monitoring informs the user about many events so that the users can automate almost everything imaginable on their computer. It sends the user an alert at the start and close of the program. Kiwi Application Monitors can also tell the user a great deal of information at a glance like memory size of paged and non-paged systems, page able, private and virtual memory size, total processor time used etc.

### *G. Ganglia*

Ganglia monitoring software is considered to be a Distributed Monitoring System for high performance computing system such as Clusters and Grid. The design of this tool is based on hierarchy form targeted at the federation of clusters [20]. Ganglia depend upon multicast protocol for monitoring the state present in the clusters, and uses connection which is point to point. It consumes the information for data representation and for compact from technologies like XML, RRD tool, XDR, portable Data transport [21] and is implemented through Robust. It supports many operating systems like Windows, Mac, Linux, Unix and processors architecture. It is used for linking Clusters. Ganglia is BSD licensed open source project. The software is used to view live or recorded statistics covering metrics. Gmond is a part of Ganglia Monitoring tool which is a small service that needs to be installed and monitored in each server, also this is multithreaded. The other part is Gmetad which collects the data from other Gmetad Daemons in the form of Round Robin Database. Next is Round Robin Data tool (RRD) which is used to store its data and visualization. RRD is considered to be the heart of ganglia in graphing [22].

### *H. DAMS*

DAMS (**D**istributed **A**pplication **M**onitoring **S**ystem) is for monitoring the networks communications and distributed applications. It is capable of enhancing the distributed Java applications byte codes using ASM manipulation framework, and monitors the Application module and class methods at run time [23]. For monitoring, protocol adapter and connector are required so that the client can get connected to the application or server. The DAMS's architecture consists of three main layers; the System Agent Layer which is responsible for managing system resources, modifying the byte code of class and for generating new class files , the Monitoring Management Layer where the data gets classified and stored and gets the remote objects and the View Layer which displays the data and sets the layout [23]. In DAMS, Java Management Extensions (JMX) provides the architecture and the postulates for Distributed Monitoring System. By this solution, the DAMS become capble of monitoring the complexities of the business present in a large Distributed Systems. It also has good performance and scalability.

### *I. RDT*

R-OSGi Deployment Tool (RDT) is used to analyze OSGi applications and represents it in a graphical form to users. RDT is helpful in easy deploying and monitoring the distributed application on Eclipse. It analyses all the bundles present in the application. RDT has a customizable reporting which helps the user to understand the software easily. The real-time status and structure of an application which helps in identification of any network issue. It is also cable of finding the impacts of the network issues occurred across the network and troubleshoots them by finding the best solution. When RDT is used on an Eclipse platform then it is cable of capturing all the messages present across the network. These captured messages can be helpful in debugging and testing the distributed applications [24, 25]. When services gets combined with R-OSGi using R-Binders, the management of services present in the local or in distributed environment gets some good ways of solution on the occurrence of network problems. For the development of the distributed applications, RDT is responsible for collecting the credible dependencies information.

### *J. OpenNMS*

OpenNMS is a free and Java -based open source network management application platform. The main focus of OpenNMS is to be truly distributed. It is also a scalable software providing platform for all FCAPS network [26]. It can easily replace the large enterprise monitoring tool like HP OpenView and IBM Tivoli. It can easily detect outage of services and thresholds and is cable of monitoring applications remotely. It uses many services for collect of performance metrics and has an easy to integrate architecture. This software is portable to any platform supporting Java SDK as it is written in Java. This software is capable of managing large number of devices by using one server or clusters of servers. Main functional areas of OpenNMS are monitoring the services, collecting data using SNMP and JMX, and the other is Event management [27]. It provides **Meridian and Enterprises which** require **stability** uses **Meridian and Horizon is used by those who are** looking for such monitoring tools which can easily monitor new technologies. **It** can be accessed a web-based user interface built on jetty.

*K. Collectd*

Collectd is a Unix daemon which collects, transfers and stores performance data of computers and network equipments and makes it available for the network. The available resources are then overviewed and maintained by the system administrator which then helps to detect existing or looming bottlenecks. This software execute on the systems without even the help of scripting language, such as embedded systems as it is written in C for high performance. Everything in collectd comes in plug ins and so the daemon comes with over 100 plug ins. Daemon has been reported as working on Linux, Solaris, Mac OS X,AIX , FreeBSD , NetBSD, and OpenBSD. Collectd is actively developed and supported and well documented. Some limitations for collectd can be that it can write to RRD files but doesn't generate graphs [28]. It supports Microsoft Windows provided by SSC Serv which is a native Windows service and implements collectd's network protocol. There are many ways for increasing the collectd functionalities for the needs such as C-Plugins , Perl-plugins , Java-Plugins , Python-Plugins , UNIX domain socket and Execute binaries or scripts.

*L. Wireshark*

Wireshark is one the finest open source packet analyser and allows users to capture traffic from both wired and wireless data network at wire speed. It analyses VoIP calls, plot IO graphs for all traffic from an interface, decrypt many protocols, exports the output. It is portable in operating systems such as UNIX and windows. It import packets from text files, save, search packets on many criteria and create various statics. In wireshark packets which are in the grouped data form are sent through the network to certain designated system. In this way wireshark perform processes elimination which occurs because of improper management and bandwidth control for enhancing the Internet users. In wireshark, color-coding is used for identifying a particular type of packet. It is capable of processing thousands of IPs and tracks each IP individually as it provides database mode that supports sensors, customized intervals and reports. The data which is captured is in binary form, it convert that data in user readable form. It also has some disadvantages like it isn't an intrusion detection system because of which things on the network cannot get manipulated and can only measure them. It doesn't send packets on the network or do other active things [29].

*M. Capsafree*

Capsa provided by colasoft is a good solution to many network problems like low efficiency, trouble and even breakdown in networks. It captures packet in real-time, decodes them and diagnose them and display the result in views, visualized charts and reports. In a network communications when network adapter receives the traffic, it first matches it with the MAC address and then broadcasts it. For the detection and capturing the data core module are used which is present at the bottom-level of the Capsa and then it gets forwarded for summarization to the high-level modules for summarization. Some important features of Capsa: It can turn single-thread analysis to multi-thread analysis technology, which take advantage of using the computer resources like multi-core CPU to the full ability. It also recycles multiple cache buffers and decrease memory fragmentation. It creates dynamic tree structured protocols and identifies the type of protocols and sub-protocols. It supports for over 300 network protocols, MSN and Yahoo messengers filters, email monitor and auto save and customizable reports and dash boards, details are in graphs and numbers, provides auto-run packet captures and powerful customizable alarm. It has some disadvantages of being expensive, provides very less features of customization to the users and is portable only on Windows.

*N. Cacti*

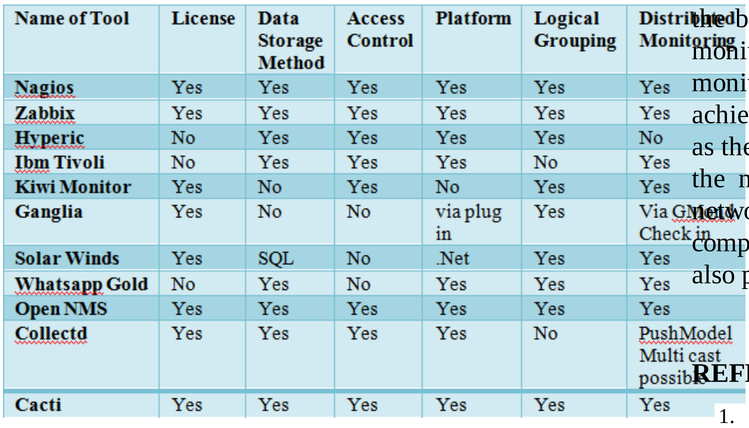
Cacti monitoring tool is an open source software and is useful to minimize downtime and collect relevant information about the network like log files. The multi technology adopted by cacti like PHP, MySQL, SNMP and RDDT have produced good interactive interface. Thus it is convenient to managers and also provides automatic display mechanisms for viewing graphs with web interface. Comparing with other monitoring tools Cacti is more robust and has more powerful functions [30]. The capabilities of Cacti can also be extended for collecting the data by using scripts, queries, or commands and then the data gets saved as templates. These templates are used so that other devices consist similar set of data can also use the feature of SNMP polling. Cacti consists RRD tool, a very strong and powerful open-source data logging and graphing system. Time-sharing data of metrics such as CPU load and network bandwidth utilization is being graphed by it. It is designed as front-end application as it is used to display bandwidth statics by web hosting providers for their customers [31]. It has some disadvantages like configuration of Interfaces is Tedious and configuration of Plug-in Architecture is non-trivial.

*O. WhatsUp Gold*

It is network monitoring solution that helps to run and grow networks. It uses standard protocols like TCP/IP, SNMP and IPX to map and monitor networks and continuously poll the mapped devices. It can alert the users using both visible and audible alarms. When it detects any problem in the network it immediately alert the user by beeper, pager, sound, e-mail, voice-messages etc. It offers clumsy user interface for simple functions such as reporting specific element and supports only windows. Installation of WhatsUp Gold monitoring software is unchallenging but for its configuration it needs web console. It provides more than 2000 configurable reports including real time reports, which are helpful for troubleshooting. Alerts in this monitoring tool are configured by emails, SMS, or custom scripts.

## III. COMPARISON OF NETWORKING MONITORING TOOLS

The objective of this section is to compare all the considered network monitoring tools.



| Name of Tool | License | Data Storage Method | Access Control | Platform | Logical Grouping | Distributed Monitoring |
|---|---|---|---|---|---|---|
| Nagios | Yes | Yes | Yes | Yes | Yes | Yes |
| Zabbix | Yes | Yes | Yes | Yes | Yes | Yes |
| Hyperic | No | Yes | Yes | Yes | Yes | No |
| Ibm Tivoli | No | Yes | Yes | Yes | No | Yes |
| Kiwi Monitor | Yes | No | Yes | No | Yes | Yes |
| Ganglia | Yes | No | No | via plug in | Yes | Via GMetad Check in |
| Solar Winds | Yes | SQL | No | .Net | Yes | Yes |
| Whatsapp Gold | No | Yes | No | Yes | Yes | Yes |
| Open NMS | Yes | Yes | Yes | Yes | Yes | Yes |
| Collectd | Yes | Yes | Yes | Yes | No | PushModel Multi cast possible |
| Cacti | Yes | Yes | Yes | Yes | Yes | Yes |

Figure 1: Comparison of Popular Tools

Next we first discuss parameter License. (i) License: The license of the software defines that whether the user can run, study, modify or share the software or not. The license can either be open sourced or closed source. (ii) Alerts: Alerts created by the monitoring tools must be sent to administrator for fast troubleshooting. It can be customized as per the user needs like having alerts only for critical network issues for reducing the unnecessary alerts. Monitoring tools can provide different alert techniques such as via emails, SMS and so on. (iii)Support:There are different supporting techniques such as active support community, webinars, email forums, help desks, phones, wiki and so on provided by the monitoring tools. These support techniques are for helping the users in case of any query about the software and for understanding the software easily. (iv) Monitoring Resources:The resources act as a reference model for a network and describes the communication happened among the applications installed on the devices or systems. There are many components that make a network enable communication between nodes like IP address, switching and routing, DNS (Domain Name System), Performance counters [32]. (v) Agent Language:It is a powerful way to describe the complex software entity. An agent is being defined in terms of its behavior rather than in attributes and functions. An agent is communicative and provides features like develop, run, display and monitor multi-agent based applications. For example Janus, an open source and multi-agent platform which is fully java implemented. (vi) User Interface:It can be defined as a space where human and machine commerce. This can be done by evaluating the tools that if it matches the needs.

Furthermore, with the dependence of user's skill and profile the user need to find the tool that matches with Web Interface to assures the access from heterogeneous clients and with the primarily use of mobile devices you can watch out for a Mobile User Interface [5]. (vii) OS Support : To debug processes and systems performance monitoring of operating system, management of the system resources is important, making decisions of the system and evaluating and examining the system. The division of the tool is primarily in the two main categories: Real Time and Log Based [33]. In a system, monitoring is done at the process level and this all data is used by operating systems to perform various decisions.

## IV. CONCLUSION

In this paper, we have discussed about network monitoring, the bases on which a user or an organisation can select a monitoring tool, and have also discussed 15 most widely used monitoring tools. These monitoring tools can be used for achieving the goal of high performance and reliable networks as they are capble of analysing the resources for configuring the network problems and alert the administrator if any network issue occurs. Adavnatges, limitations and a comparison among all the considered monitoring tolls have also presented in this paper.

## REFERENCES

1. R . Khan, S.U. Khan, ,R . Zaheer and M.I. Babar, "An efficient network monitoring and management system". International Journal of Information and Electronics Engineering, 3(1), 122, 2013.
2. B. M. Shuhaimi, M.A.A., I. Binti Roslan and S. B. Anawar, "The new services in Nagios: Network bandwidth utility, email notification and sms alert in improving the network performance". In Information Assurance and Security (IAS), 2011 7th International Conference on, IEEE, pp. 86-91, 2011, December.
3. M.K. Debbarma, D. Deb, N. Debbarma and P. De, "Performance analysis of network monitoring tool through automated software engineering approach". In Signal Processing And Communication Engineering Systems (SPACES), 2015 International Conference on, IEEE, pp. 402-406, 2015, January.
4. Kufel, "Tools for Distributed Systems Monitoring". Foundations of Computing and Decision Sciences, 41(4), 237-260, 2016.
5. J. Hernantes, G. Gallardo and N. Serrano, "IT infrastructure-monitoring tools". IEEE Software, 32(4), 88-93, 2015.
6. E. Luchian, P. Docolin and V. Dobrota, "Advanced monitoring of the OpenStack NFV infrastructure: A Nagios approach using SNMP". In Electronics and Telecommunications (ISETC), 2016 12th IEEE International Symposium on, IEEE, pp. 51-54, 2016, October.
7. K. Buytaert, T. De Cooman, F. Descamps and B. Verwilst, "Systems monitoring shootout". In Linux Symposium, pp 53, 2008, July.
8. Zabbix , https://en.wikipedia.org/wiki/Zabbix
9. Zabbix -The Enterprise -class monitoring solution for everyone, http://www.zabbix.com/.
10. v fabric documentation centre, https://pubs.vmware.com/vfabric5/index.jsp?topic=/com.vmware.vfabric.hyperic.4.6/Introduction_to_Hyperic_Monitoring.html.
11. Hyperic Application & System Monitoring, http://sourceforge.net/projects/hyperic-hq, Feb 2016.
12. IBM SmartCloud Monitoring, http://ibm.com/software/tivoli/products/smartcloudmonitoring, Feb 2016.
13. H. Chan and T. Kwok, " A policy-based sensor selection system with goal oriented singular value decomposition technique". In Policies for Distributed Systems and Networks, 2009. POLICY 2009. IEEE International Symposium on, pp. 95-97. 2009, July.
14. S.Durairajan and P. Sundararajan, "Portable service management deployment over cloud platforms to support production workloads". In Cloud Computing in Emerging Markets (CCEM), 2013 IEEE International Conference on, pp. 1-7. 2013, October.
15. IT Management Software, http://www.solarwinds.com/
16. P. Moceri, "SNMP and Beyond: A Survey of Network Performance Monitoring Tools", 2006.
17. J. Dissmeyer, "SolarWinds Orion Network Performance Monitor". Packt Publishing Ltd, 2013.

*Published By:*
*Blue Eyes Intelligence Engineering*
*& Sciences Publication*

18. Kiwi Application Monitor, http://www.kiwimonitor.com/kiwi_application_monitor.php
19. Kiwi is a cool application monitoring and automation tool, http://www.guidingtech.com/2298/kiwi-application-monitoring-software/
20. Ganglia Monitoring System, http://ganglia.sourceforge.net/
21. M.L. Massie, B.N. Chun and D.E. Culler, "The ganglia distributed monitoring system: design, implementation, and experience". Parallel Computing, 30(7), 817-840, 2004.
22. Ganglia- a software , https://en.wikipedia.org/wiki/Ganglia_(software)
23. H. Jiang, H. Lv, N. Wang and R. Di "A performance monitoring solution for distributed application system based on JMX", In: Grid and Cooperative Computing (GCC), 2010 9th International Conference on, 2010, pp. 124 –127.http://dx.doi.org/10.1109/GCC.2010.35.
24. J.S. Rellermeyer, G. Alonso and T. Roscoe, "Building, deploying, and monitoring distributed applications with eclipse and r-osgi". In Proceedings of the 2007 OOPSLA workshop on eclipse technology eXchange, pp. 50-54, 2007, October. ACM.
25. Z. Feng and L. Huang, "R-binder: application of using service binder in R-OSGi". In Computer Science and Computational Technology, 2008. ISCSCT'08. International Symposium on, Vol. 2, pp. 34-39, 2008, December. IEEE. Chicago
26. openNMS | , https://www.opennms.org/en
27. C. Pape and R. Trommer, "Monitoring VMware-based virtual infrastructures with OpenNMS", 2012.
28. Collectd, https://en.wikipedia.org/wiki/Collectd
29. S. Mongkolluksamee, P. Pongpaibool and C. Issariyapat, "Strengths and limitations of Nagios as a network monitoring solution". In Proceedings of the 7th International Joint Conference on Computer Science and Software Engineering (JCSSE 2010), Vol. 7, 2009.
30. Thomas Urban, Cacti 0.8 Beginner's Guide, Packt Publishing Ltd, 32 Lincoln Road, Olton, Birmingham, B27 6PA UK, 2011.
31. P. Asrodia and H. Patel, "Analysis of Various Packet Sniffing Tools for Network Monitoring and Analysis", IEEE and Computer Engineering, pp: 56, 2012.
32. http://www.solarwinds.com/basics-of-network-monitoring.
33. Operating Systems and Process Monitoring Tools, https://www.cse.wustl.edu/~jain/cse567-06/ftp/os_monitors/

## AUTHORS PROFILE

Dr. Latika Kharb is working in Department of MCA as GGSIPU Faculty in JIMS: Jagan Institute of Management Studies, New Delhi. She has published over 85 research papers/ articles/ chapters in Peer-reviewed / Indexed International Publishers.

Dr. Deepak Chahal is working in Department of MCA as GGSIPU Faculty in JIMS: Jagan Institute of Management Studies, New Delhi. He has published over 25 research papers. He has been the convener of many Springer CCIS Conferences.