

Comparative Study on Network Monitoring Tools

Vudipi Manohar¹

¹Student of B. Tech, Computer Science and Engineering, GITAM (Deemed to be University), Visakhapatnam, India

Abstract – Network monitoring systems serve all major technology companies around the world. The features of networks revolve around high performance and reliability. These are the essential features for systems to monitor and they become the points of comparison among several monitoring systems competing with each other in the market. Therefore, network monitoring systems must be selected keeping, the requirements of the businesses in mind, which brings us to this paper. In this paper, the comparisons among network monitoring systems, which are popular among network administrators, are shown. The features such as license, user interface, discovery, distributive monitoring and plugins compared and analyzed.

Key Words: monitoring system, network monitoring, comparison, networks, Nagios, Solar Winds, PRTG.

1. INTRODUCTION

We are in the golden age of technology as billions of devices are connected to the network. We must ensure that these networks are secure and monitored for safety purposes. Devices connected to networks have increased from millions to trillions. A network monitoring system is essential in this scenario for maintaining the network devices. It has become a necessity for every network irrespective of its size. These networks require a monitoring system which can provide a well-defined report on problems such as performance issues and bottlenecks.

The aspect of network monitoring has changed with systems, providing dashboards and graphical interfaces. Network administrators can monitor large networks with interfaces from a central location. Network monitoring systems can generate precise reports on connectivity and performance of devices on the network. Network management and many other tasks can be performed by a network monitoring system to provide a robust network with high performance. Monitoring systems have become the first level of security for most organizations now, ensuring that the devices connected are properly working.

1.1 Monitoring

There are several monitoring tools available on the market. These tools can be classified based on the scale of the organization they cater to, such as small and medium businesses to large enterprises. Small and medium businesses need a system which is easy to deploy and maintain due to their organizational constraints. These cannot maintain complex monitoring systems. The

enterprises, on the other hand, need a comprehensive and scalable variant of systems which they could customize based on their needs. Some of the popular ones with small and medium businesses are PRTG Network Monitor, Nagios Core and one of the comprehensive enterprise tools is SolarWinds.

1.2 Open Source and Proprietary Systems

The concept of open-source is revolutionary, and several companies are benefiting from them. The availability of source code is an advantage for security. The code which is not secure could be modified to achieve a secure application. The end product could be made better in many ways when the developers have the source code to build on. In network monitoring, open-source applications are well built. They have also provided a base for any modifications for the future. This system has some concerns as anybody could analyse the code and cause problems to systems, thus reducing the reliability of the system.

The concept of proprietary systems in network monitoring provides security through non-availability. The source code is not available, ensuring that no other system or entity could modify the code and cause problems. These systems are updated regularly, keeping in mind the latest exploits in the monitoring systems. The concept can be applied to open source systems such as Nagios Core. This open-source system is updated regularly and maintained to provide the same security as proprietary systems. Observations led to the conclusion that while open source makes code visible, we have found that source visibility does little to increase the security risks posed to a given project, in most cases [1].

2. MONITORING TOOLS

2.1 Nagios

Nagios is a monitoring system for computer networks and has an open-source license. Nagios is known for being the best server monitoring software on the market. It operates on the Linux environment and is platform-independent in terms of a monitoring system. It can monitor several resources such as application, network and server and can provide reports. Server monitoring can be agent-based and agentless, and Nagios provides this flexibility. It has a web interface containing all the real-time information being presented in the form of graphs and grouped based on the network [2].

Nagios provides monitoring of network services like HTTP, ICMP, SNMP, FTP, SSH. It also monitors resources of hosts such as processor load, their disk usage and system logs. It can also monitor hardware like IoT devices and sensors with the help of plugins which are written specifically for those devices. The monitoring system can generate reports for the data collected through monitoring, and it uses Round Robin Database to store the data. Nagios can send notifications in the form of email, SMS or through any user-defined method.

2.2 PRTG Network Monitor

Paessler Router Traffic Grapher Network Monitor is a network monitoring software with an open source license. The monitor can auto-discover hosts on the network, which helps to identify all the devices connected to the network. It also has a web interface which helps for real-time troubleshooting. This open-source version has monitoring of 100 integrated sensors.

This system is capable of monitoring bandwidth usage and uptime of connected devices and collects statistics from switches, routers, servers and other devices. The system uses a variety of communication protocols such as Ping, SNMP, NetFlow. The expansion of this system with a higher capacity which requires more sensors is not an open-source system which is a limitation the system possesses.

2.3 Solar Winds

SolarWinds is a system which has a simple setup to configure and deploy. This tool has a user-friendly interface with automatic network discovery. It is one of the easiest to use the system. It shows all devices, applications, networks, and vendors in single-page path analysis. It is useful to create more signal and less noise to quickly isolate network slowdowns.

SolarWinds Network Monitor has multi-vendor network monitoring for fault, performance, and availability. The Server and Application Monitor can monitor across private, public and hybrid cloud environments. It has a Database Performance Analyzer for optimization, a Network Bandwidth Analyzer for customizable traffic reports and a Security Event Manager to normalize log data to spot incidents.

This system is modular with separate products for monitoring networks and servers. Network Performance Monitor is made especially for networks and for server monitoring, there is Server and Application Monitor. The limitation of this system is that every module has to be bought and maintained separately.

3. METHODOLOGY

The research follows a qualitative approach to suggest the differences between open-source network monitoring tools

and the proprietary tools on the market and produces empirical results. The different kinds of research performed by other researchers have been taken into consideration while comparing these tools. The focus is not only on the tools but also on the pricing, which is a major factor in several studies which have compared tools. With the comparison of the tools taking in several factors related to the monitoring systems, this research is a comprehensive study to bring out a suitable monitoring system to be deployed. This research concludes with the selection of a system which is easy to use and is cost-effective for a user/organization.

4. COMPARISON OF TOOLS

The network monitoring tools are compared based on several factors which define the suitability of the systems for given businesses. The factors include automatic discovery, classification, performance monitoring, security management, alerts, scalability [3].

The comparison of the systems is shown individually in the form of tables given below, starting with the licensing and pricing of the systems. The license and price of the monitoring system are the factors which lead to cost-effective setups.

Table -1: Licensing and Pricing

Comparison of License and Pricing		
Tool	License	Pricing
Nagios	GNU General Public License version 2	Free (Core version) Paid (XI version)
PRTG Network Monitor	Perpetual License	Free (Until 100 sensors) Paid (+100 sensors)
SolarWinds	Perpetual License and Yearly License	Paid

Discovery and performance monitoring are important for large businesses. The comparison of these features is available in the table below. Table-2 compares the discovery, storage, configuration and classification features which are the main components of the monitoring system.

Table -2: Performance Monitoring

Comparison of Performance Monitoring				
Tool	Discovery	Logical Grouping	Configuration [4]	Storage

Nagios	Manual (Core) Auto (XI)	Yes [5]	Text Files	Flat File, SQL
PRTG Network Monitor	Auto	Yes [5]	Web Interface	SQL Database (Logs) Flat File (Monitoring)
Solar Winds	Separate Module for Auto Discovery	Yes [5]	Web Interface and Separate Module	SQL (Orion Database)

A network monitoring system should be scalable to accommodate the changes which occur in a business. There should be a support system in place to ensure that changes in the system do not cause any errors. Table-3 gives comparisons among these systems based on scalability and support.

Table -3: Scalability and Support

Comparison of Scalability and Support		
Tool	Scalability	Support
Nagios	Yes (Not effective for large businesses)	Paid Phone Support Support Forums
PRTG Network Monitor	Yes (Paid)	User Support Script Support Training Courses
SolarWinds	Yes	24/7 User Support Technical Support (Mail and Phone)

5. OBSERVATIONS

There are some observations made after comparing these network monitoring systems. These observations point out the differences in these systems and provide the suitability of systems to particular businesses.

The observations made are as follows,

- PRTG Network Monitor is free and based on the expansion of the business could be scaled to meet the demands.
- Nagios is free and provides only a base for the network monitoring system to be built on by the end-user.

- SolarWinds has a high price point for small business owners. The cost of maintaining the system is high, hence requiring lots of employees. Large organizations can maintain these systems designed for modularity.

The observations point out that small businesses could move towards PRTG network monitor, making it easy for them to monitor their limited devices for free and expanding if necessary. The feature of the web interface helps these businesses to maintain the system effectively.

Nagios provides a platform for the development of a customized network monitoring system. The small businesses can use the plugins as addons in Nagios to customize it.

SolarWinds is entirely modular, making it difficult for small businesses to buy each module and maintain it. SolarWinds is for large businesses with individual functions. The modules necessary for a particular function can be purchased and deployed.

6. CONCLUSION

This paper compared three network monitoring systems which are popular in their aspect. The suitability of the system, for small businesses and large organizations, has been presented. The tools compared are robust in monitoring systems these days. The differences in these tools have brought out the limitations and advantages of each of them. The importance, of pricing and open source, is also presented in the paper hence leading to the suitability of these systems for particular organizations.

REFERENCES

- [1] Clarke, Russell, David Dorwin, and Rob Nash. "Is open source software more secure?." Homeland Security/Cyber Security, 2009.
- [2] Nagios. The Industry Standard in IT Infrastructure Monitoring. <http://www.nagios.org>. Accessed March 24, 2020.
- [3] The must-haves of a network monitoring software. <https://www.manageengine.com/network-monitoring/whitepaper-network-monitoring-essentials.html>. Accessed March 28, 2020.
- [4] Isaac Sikubwabo, Mariam Usanase, Dr. Papias Niyigena. "Comparative Study on Network Monitoring Tools of Nagios Versus Hyperic", 2019.
- [5] Comparison of Network Monitoring Systems. https://en.wikipedia.org/wiki/Comparison_of_network_monitoring_systems.html. Accessed April 3, 2020.