

Comparative Study on Network Monitoring Tools of Nagios Versus Hyperic

Isaac Sikubwabo¹, Mariam Usanase², Dr. Papias Niyigena³

^{1,2}Student at MSc. IT, Department of Information Technology, University of Lay Adventists of Kigali

³Lecturer, Department of Information Technology, University of Lay Adventists of Kigali

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 Those are Nagios and Hyperic we then present a comparison among the two tools Nagios and Hyperic as the considered monitoring tools based on the different parameters like license, data storage method, access control, platform, logical grouping and distributed monitoring.

INTRODUCTION/BACKGROUND

In today's world, the term network monitoring is widespread throughout the IT industry. Network monitoring is a critical IT process where all networking components like routers, switches, firewalls, servers, and VMs are monitored for fault and performance and evaluated continuously to maintain and optimize their availability. One important aspect of network monitoring is that it should be proactive. Finding performance issues and bottlenecks proactively helps in identifying issues at the initial stage. Efficient proactive monitoring can prevent network down time or failures.

Data becomes useful only when it is presented clearly to the right audience. It is important for IT administrators and users to know about critical metrics as soon as they log in. A network dashboard should provide an at-a-glance overview of the current status of your network, with critical metrics from routers, switches, firewalls, servers, services, application, URLs, printer, UPS and other Infrastructure devices. Support for widgets to monitor the required specifics and real-time performance graphs can help administrators quickly troubleshoot problems and monitor devices remotely.

When monitoring a network and its devices, a common good practice is to adopt a secure and non-bandwidth consuming network management protocol to minimize the impact it has on network performance. Most of the network devices and Linux servers support SNMP (Simple Network Management Protocol) and CLI protocols and Windows devices support WMI protocol. SNMP is one of the widely accepted protocols to manage and monitor network elements. Most of the network elements come bundled with a SNMP agent. They just need to be enabled and configured to communicate with the network management system (NMS). Allowing SNMP read-write access gives one complete control over the device. Using SNMP, one can replace the entire configuration of the device. A network monitoring system helps the administrator take charge of the network by setting SNMP read/write privileges and restricting control for other users. 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.

RELATED WORK

Computer networks can be viewed as a series of devices that are interconnected and able to communicate with each other. Most networked environments connect computers via switches and routers. Switches provide the forwarding capability that allows logically neighboring devices to communicate. Routers add the routing capability that provides the network with structure and allows communication between sub-networks. This project is interested mainly in the Internet Protocol (IP) networks (Information Sciences Institute, 1981). Computer networks vary significantly in size and importance. The larger and more important networks can cost organizations that are running them large sums of money for every minute that they are unavailable or malfunctioning.

The profiling of "social" behavior of hosts was studied in BLINC [1] for the purpose of traffic classification. BLINC, however, focuses only at the host level. In BLINC, the notion of a "graphlet" models a single host's flow patterns. By contrast, our work

on TDGs uses network-wide graphs. In some sense, a TDG is an aggregation of the graphlets of all hosts in a network for a particular key. To simplify the aggregation, TDGs use edges only between source and destination IP addresses unlike “graphlets” [1] which also have edges to nodes that represent port numbers. Apart from some notable exceptions, TDGs have not been used for network analysis and monitoring. The first work using TDG-like graphs for intrusion detection appeared in 1999 [2], but there has not been recent follow up. Recently, work by Ellis uses graph-based techniques to detect worm outbreaks within enterprise network environments [3]. These efforts only focus on worm detection, by trying to capture the tree-like structure of self-propagating code. In addition, companies like Mazu and Arbor Networks utilize graph-based techniques. Tan et al. [5] in collaboration with Mazu show how similarity between hosts, based on their connection patterns, can be used to group network users into related roles. In contrast to grouping hosts and calculating user similarity, the present work mainly focuses on characterizing the structure found in connection graphs of hosts based on a key (e.g., a common TCP or UDP port number). Graph based techniques are also used by Aiello et al. [6] in the field of Communities of Interest (CoI). Similar to [5], CoI research focuses on extracting communities and modeling “normal behavior” of hosts. Deviation from normal behavior can then be used to trigger an alarm. Moreover, the authors in [6] and [5] do not use the graph metrics we employ in this work and mainly focus on enterprise network environments. Finally, TDGs as defined here are significantly different than trust propagation networks [7]. The problem there is to identify intruders in social networks, which represent trust relationships (and not an exchange of packets), as discussed in Sybil Guard [7].

Tstat started as evolution of tcptrace [8], which was developed to track and analyze individual TCP flows, offering detailed statistics. Tstat initial design objective was to automate the collection of TCP statistics of traffic aggregate, adding real time traffic monitoring features. Over the years, Tstat evolved into a more complex tool offering rich statistics and functionalities. Developed in ANSI C for efficiency purposes, Tstat is today an Open Source tool that allows sophisticated multi-Gigabit per second traffic analysis to be run live using common hardware. Tstat design is highly flexible, with 2 Network to monitor (a) TCP/UDP Behavioral FSM DPI Pure DPI L7 L4 L3 IP. Tstat monitoring probe setup (a) and analysis workflow (b). Several plugin modules offering different capabilities that are briefly described in the following. In addition, plugins can be activated and deactivated on the fly, without interrupting the monitoring. Being a passive tool, live monitoring of Internet links, in which all flowing packets are observed, is the typical usage scenario.

Network management software can be divided into two categories: In a broad perspective, any network requires network management software, and is used in telecommunications, banking, finance and many other industries. In a narrow perspective, there are different divisions according to different angle. According to the management object, it can be divided into system management software and equipment management software. System management software is comprehensive and in-depth monitoring and management software (including server, network equipment and application system) for the whole network. The equipment management software is mainly introduced by the network equipment manufacturers to well manage their network equipment (for example, equipment management software introduced by Huawei).

MONITORING TOOLS

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

Nagios

Nagios is an open source monitoring system for computer systems. It was designed to run on the Linux operating system and can monitor devices running Linux, Windows and UNIX operating systems (OS). **Nagios** software runs periodic checks on critical parameters of application, network and server resources

Nagios is powerful network monitoring tool that has been in active development for many years. It does almost anything that system and network administrators might need from a network monitoring utility. The web interface is fast and intuitive, and the server part is extremely reliable. Nagios is rather complex configuration can be a problem for beginners to learn, but it is also an advantage, since the tool can be adapted to almost any monitoring task. As with Cacti, a very active community supports Nagios core, so various plug-ins exist for a huge variety of hardware and software. Nagios enable you to continuously monitor the status of servers, services, network channels and everything else that has IP addresses. For example, you can monitor the use of disk space on the server, RAM and CPU usage, FLEXlm license usage (software license manager tool), server air temperature, WAN and internet connection latencies, net flow traffic, and much more.

No monitoring system for servers and networks would be complete without notifications. The Nagios software platform offers a customizable mechanism for notifications via e-mail, SMS and instant messaging via the most popular internet messengers, as well as an escalation scheme that can be used to make reasonable decisions about who should be notified when and in what circumstances. In addition, the display function shows all monitored devices in the logical representation of their placement on the network, with color coding that highlights problems as they arise.

The main disadvantage of Nagios is its configuration process, it is mostly done through the command line, which greatly complicates installation if you've never worked with it before. People familiar with standard Linux and UNIX configuration files, however, should not experience any particular problems. The possibilities of Nagios are huge, but the effort required to use some of them may not always be worth it. Nevertheless, the advantages of the early warning system metrics provided by this tool for so many aspects of the network are hard to overstate.

Hyperic

Hyperic is a monitoring and management software licensed under GPL which is optimized for physical environment as well as for virtual environment. 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. It can monitor applications on almost every operating system including Linux, UNIX, Windows, Solaris, AIX, HPUX, and VMware and also on Amazon Web Services. It has the ability for auto-discovering components required by virtual applications and the resources. 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, 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. However Hyperic has disadvantage of the cost of resources by Java Virtual Machines (JVM)

METHODOLOGY

The methodology for conducting this research is closely to the task of gathering information to be used, considering the duration and environment of research. This research is an empirical study, where information used is read from previous works, which means that we followed qualitative approach. As presented in the literature review section, different researchers discussed the performance of network monitoring such as Nagios,

Zabbix, Hyperic, Capsa free, ganglia etc. everyone from those researchers has mentioning on its own, the strength of the network simulator among the used ones in his/her study. Our main objective is to identify the main difference between those two tools in network monitoring based on different factors and conclude which is the best to use in a given organization or companies

COMPARISON OF NETWORKING MONITORING TOOL

The objective of this section is to compare all the considered network monitoring tools. According to their license, data storage method, access control, platform, logical grouping and distributive monitoring

Table that show the difference between Nagios and Hyperic based on different factors

Name of tool	License	Data storage method	Access control	platform	Logical grouping	Distributive monitoring
Nagios	Yes	Yes	yes	Yes	Yes	Yes
Hyperic	No	Yes	yes	Yes	Yes	No

Open source network management comparison : Support

Attribute / Project	Nagios	Hyperic
Forum	✓	✓
Mailing list	✓	✗
Support contract	✓	✓
Training	✓	✓
Consulting	✓	✓
Blog	✓	✓
Book(s)	✓	✗

Open source network management comparison: General comparison based on license, first released, development languages, external dependencies, configuration, User interface, reporting

Attribute / Project	Nagios	Hyperic
General		
Licence	GPL	GPL
First released	1998	2006
Development languages	C	Java/C
External dependencies	Net-SNMP / RRDTool	SNMP4J
Configuration	Text files	Web based

Attribute / Project	Nagios	Hyperic
Extensible	✓	✓
User interface	Web/WAP	Web
Reporting	✓	✓

CONCLUSION

In this paper, we have discussed about network monitoring, the bases on which a user or an organization can select a monitoring tool, and have also discussed 2 most widely used monitoring tools. These monitoring tools can be used for achieving the goal of high performance and reliable networks as they are capable of analyzing the resources for configuring the network problems and alert the administrator if any network issue occurs. Advantages, limitations and a comparison among all the considered monitoring tolls have also presented in this paper.

REFERENCES

1. Author Jack Hughes Posted on July 18, 2008CategoriesNetwork Management, Open Source Tags comparison, Hyperic, nagios, opennms, Zabbix, Zenoss10 Comments on Open source network management comparison: Support
2. Paul Bischoff - Paul Bischoff is a privacy advocate and the editor of Comparitech, a security-focused tech services review site. He's been covering IT-related subjects for multiple outlets since 2012 and is passionate about privacy, free speech and net neutrality
3. Nagios. The Industry Standard in IT Infrastructure Monitoring. <http://www.nagios.org>. Accessed June 3, 2015.
4. W. Aiello, C. Kalmanek, P. McDaniel, S. Sen, O. Spatscheck, and J. Merwe. Analysis of Communities of Interest in Data Networks. In Passive and Ac
5. M. Crovella and B. Krishnamurthy. Internet Measurement: Infrastructure, Traffic and Applications. John Wiley and Sons, Inc, 2006.
6. Yang Shangsen. Network management and maintenance technology. Electronic Industry Press Publication. 2004 2. Zhang Yan. Network management and maintenance master. Sichuan Electronic Audio Publishing Center. 2002