International Journal of Open Source Software and Processes
Volume 7 • Issue 2 • April-June 2016

A Comparative Analysis of Open Source Network Monitoring Tools

Ali Al Shidhani, The Research Council of Oman, Information and Communications Technology Research, Muscat, Oman
Khalil Al Maawali, Information Technology Authority, Seeb, Oman
Dawood Al Abri, Sultan Qaboos University, Department of Electrical and Computer Engineering, Muscat, Oman
Hadj Bourdoucen, Sultan Qaboos University, Communication and Information Research Center, Muscat, Oman

ABSTRACT

Nowadays, the heavy reliance on computer networks necessitates minimizing outage time, increasing the availability of services, and preventing network related problems. Such realization requires continuous monitoring and observation. This is not a trivial task. Thus, automatic network monitoring tools are deployed to monitor and analyze the traffic trespassing network devices. There is an increasing demand for automated network monitoring tools and selecting a suitable candidate can become a challenging task. Some computerized network monitoring tools and systems are available, including expensive proprietary/closed-source solutions and Free Open Source Software (FOSS) systems. Three of the most popular FOSS network monitoring systems are: Nagios, OpenNMS and Zabbix. They are solid competitors to the available proprietary solutions. This paper evaluates the strengths and weaknesses of these tools. A qualitative and quantitative evaluation of the tools were conducted through monitoring real-time network traffic. The paper presents a thorough comparison between the tools. The comparison results are vital for network administrators wishing to adopt the studied monitoring tools.

KEYWORDS

Computing Systems, FOSS, IP Networks, Network Management Systems, Network Monitoring, NMS, Open Source

INTRODUCTION

Information technology (IT) and computing systems are increasingly dependent on IP networks. Virtualization, cloud computing, grid computing, mobile computing and much more are based on IP networks. IP networks are also used as voice carrier and have changed the traditional telephonic systems considerably. Voice over IP (VoIP) is becoming the most preferred consumer solution for distance calling compared to using traditional circuit switched-based networks due to cost benefits. Gaming consoles are using IP Networks for online gaming, IPTV and other applications (Qadir & Adnan, 2010). Networks are rapidly getting large, complex and more heterogeneous. Maintaining and managing IP networks is challenging, and that raised the need for specialized Network Management Systems (NMS).

Depending on network requirements and solution providers (vendors), a NMS may consist of a combination of different software and hardware units. The functional areas of a NMS include: fault management, configuration management, performance management, security management, and

DOI: 10.4018/IJOSSP.2016040101

accounting management. NMS helps network administrators to handle fully or partially all functional areas of a network management system.

There are two main types of monitoring: real-time monitoring, which offers information on the present condition of services, and historical monitoring, which provides long-term data on status, utilization, and performance (Silver, 2010). Monitoring can consist of a variety of tests such as simple ping test to verify that a host or a service is alive and connected to the network. Other examples include establishing a connection on a specific port and evaluating service response time. A monitoring system can assist network administrators by reporting faults before receiving a complaint from end users. In addition, a monitoring system performs proactive fault monitoring and performance monitoring for optimization, supporting resource management, monitoring the resources accessed and monitoring security threats.

Several network monitoring tools exist; both proprietary and Free-Open Source Software (FOSS). These tools can be configured to monitor specific hardware components or conduct general network management and analysis. Services monitored and goals for monitoring are two main factors in the selection of a particular monitoring software package (Qadir & Adnan, 2010).

There are some commercial network monitoring products with proprietary license; some of them with freeware (limited time) versions and limited functionality or features. Tens of FOSS projects are listed under a General Public License (GPL) (Free Software Foundation, n.d.) or similar license; some with commercial support available but without different feature sets or licenses.

The competition between different NMS solutions is intense. Today many large IT companies such as Oracle and HP manufacture solid NMS products. However, these products are very expensive and usually used with restrictions because of licensing contracts. As a result, FOSS NMS projects are considered a reasonable substitute.

This paper analyzes and evaluates three commonly used FOSS NMS tools, namely; Nagios, OpenNMS and Zabbix. They are considered to be highly efficient and used in multiple research studies (Qadir & Adnan, 2010). Testing and evaluating the tools was conducted on a real production network to obtain the most realistic results. The major contribution of this paper is presenting a qualitative and quantitative analysis of the three abovementioned FOSS NMS tools thus eventually aiding network administrators and planners to decide on the most suitable tool to monitor the network they administer.

Nagios

Nagios (Nagios, n. d.) project started in 1999 and was released under General Public License (GNU) version 2 (GPLv2). It is a powerful FOSS monitoring tool that assists network administrators to detect and dissolve network infrastructure issues. Nagios has active development community that consists of large number of users. Multiple developed extensions and plugins were contributed by Nagios users' community. Nagios developers also provide commercial support with several solution providers. Monitoring extensions and probing sensors also exist; they are designed to interoperate efficiently with Nagios. The tool uses plug-in architecture, which provides flexibility to users to build their own service checks for specific applications. Notification service in Nagios alerts network managers with necessary information regarding any detected problem. This permits them to resolve the problem before it affects enterprise services or end users. It stores data via text files rather than using a dedicated database system.

OpenNMS

OpenNMS (OpenNMS, n. d.) is FOSS network management system started in 1999 and released under GPLv3. It is capable of managing a network with nearly 70,000 devices (Qadir & Adnan, 2010). It can perform auto device discovery, performance measurement, service monitoring and events, alarms and notifications management. It also provides assets management capacity. OpenNMS source code is based on Java and XML, where the management server is implemented as a multithreaded application and the user interface consists of number of Servlets and Java server pages (JSPs). It also requires PostgreSQL database.