UDC - 519.72:517.977

COMPARATIVE ANALYSIS OF MONITORING SYSTEMS OF COMPUTER NETWORK

Hovhannes S. Abgaryan
National Polytechnic University of Armenia
105 Teryan St., Yerevan, RA
abgaryanhov@gmail.com
ORCID: 0000-0002-2300-2442
Republic of Armenia

Abstract

The article presents an analysis of the most common monitoring systems for computer networks, as a result of which new criteria for the effectiveness of choosing tools for monitoring computer networks have been developed, as well as criteria for choosing an effective tool for monitoring computer networks.

Key words: computer networks, monitoring, diagnostics, analysis, network protocol, control, programming.

Introduction

Nowadays it is hard to conceptualize an organization operating without computer networks. Companies are constantly dependent on Information Technologies (IT), particularly those on computer networks. Currently, it is exceptionally urgent and concurrent to apply network performance monitoring and diagnostics. As a matter of fact, it will enable network operators to upgrade network flows.

Literary review on the issue and analysis

The issues of computer network monitoring have been addressed by Olifer V.G. [4], Wakke A.D. [2], Wilson Ed. [5], Lavrov A. [3], Tadosyan A. [1] and others [6], [7], [8]. Diverse approaches and methods are presented in their works; however, no comparative analysis is available on the specific criteria of choosing and outlining appropriate monitoring tools.

Research objectives and novelty

This paper is aimed at devising new criteria for the effectiveness of the selection of computer network monitoring tools and conducting comparative analysis according to the devised criteria. Also, efficient tools of the computer network monitoring are advocated based on the activity type.

Content

Computer network monitoring is the use of a system that constantly monitors a computer network and quickly notifies in case of outages and other problems for further improvement.

Computer network management has two stages:

1. **Monitoring:** At this stage a simple operation is performed: the primary data on the operation of the networks is collected and statistics is made on the condition of all the personnel operating in the network, packages of different protocols, tablets, slots, switches and routers.

2. **Analysis:** At this stage an analysis is carried out which is a complex and intellectual operation. Thus, the information collected during the monitoring phase is interpreted, compared with previously obtained data, on the basis of which conclusions are made on the possible causes of network delays and operation processing failures. Monitoring tasks are determined by software and hardware, tests, network analyzers as well as by the management agent. The task of analysis requires an active participation of a human factor and the implementation of such complex tools as specialized systems and practical experience of network specialists.

The divergent tools applied for the analysis and diagnostics of telecommunication networks can be divided into several major categories:

Management system agents - They support one of the standard MIB functions and post information via SNMP or CMIP protocols. Receiving data from agents requires control systems that collect data automatically.

Embedded systems - It is implemented in the form of hardware system with software and is designed to perform a diagnostic function. To illustrate, take an example of Ethernet multi-segment control module.

Protocol analyzers - They are software or hardware systems that differ from the control system in their network flow monitoring and analysis of functions.

For cable system diagnostics and certification, devices can be conventionally divided into 4 major groups:

- Network monitors
- Materials for cable system certifications
- Cable scanners
- Testers

Network analyzers are applied to measure different levels of cable. In addition to the physical level, these devices operate at the channel and sometimes network level.

Cable system certification instruments carry out certification in accordance with the requirements of one of the international cable system standards.

Cable scanners are used to diagnose the cable system.

Moving on, now we represent the general characteristics of free and open-source computer monitoring software which are the basis for conducting a comparative analysis of their operation.

Zabbix – Open-source monitoring software

Zabbix is an open-source monitoring software tool (Fig. 1). Zabbix consists of Server, Proxy, Agent and Web Interface. Server, Proxy and Agent are written in C. Web Interface is written in PHP and JavaScript.

Zabbix offers several monitoring options:

Simple checks verify the availability of the host and responsiveness of standard services such as SMTP or HTTP without installing any software on the monitored host.

A Zabbix agent is installed on UNIX and Windows hosts to monitor statistics such as CPU load, network utilization, disk space and other information monitoring.

External check – monitoring is carried out via SNMP, TCP and ICMP checks.

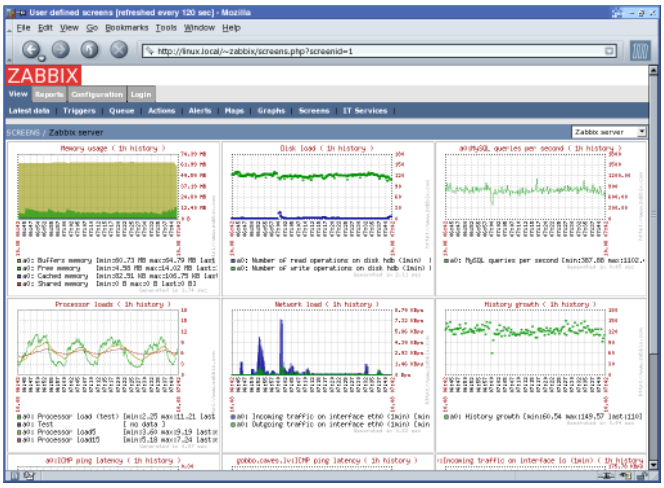

Fig. 1 ZABBIX monitoring software package

The following features are characteristic to Zabbix:

- ✓ High productivity and bandwidth, ability of 1000 and more hosts
- ✓ Automatic detection of servers and network instruments through centralized monitoring of log files, as well as through IPMI, JMX, SSH, Telnet
- ✓ Distributed monitoring with centralized web management
- ✓ Secure user identification
- ✓ Cook book
- ✓ Ability to create a network map
- ✓ Application of such database management systems as MySQL, PostgreSQL, SQLite and Oracle for data collection
- ✓ Zabbix server access on Linux, Solaris, HP-UX, AIX, FreeBSD, NetBSD, OpenBSD, Mac
- ✓ OS/ X operating systems;
- ✓ Zabbix Agent Access on Linux, Solaris, HP-UX, AIX, FreeBSD, OpenBSD, OS X, Tru64 / OSF1, Windows 2000, Windows Server 2003, Windows XP, Windows Vista, Windows Server 2008, Windows 7 operating systems
- ✓ JMX and SNMP v1, 2, 3 support
- ✓ Alerts / warnings via email, SMS and voice signals,
- ✓ Graphic representation of statistics

Nagios – Open-source monitoring program

Nagios is a free and open-source computer-software application that monitors computer systems (Fig. 2). Initially, Nagios has been intended for only being used on Linux operating systems. Then, it has been implemented on dealing with other operating systems (Sun Solaris, FreeBSD, AIX, and HP-UX) [9].

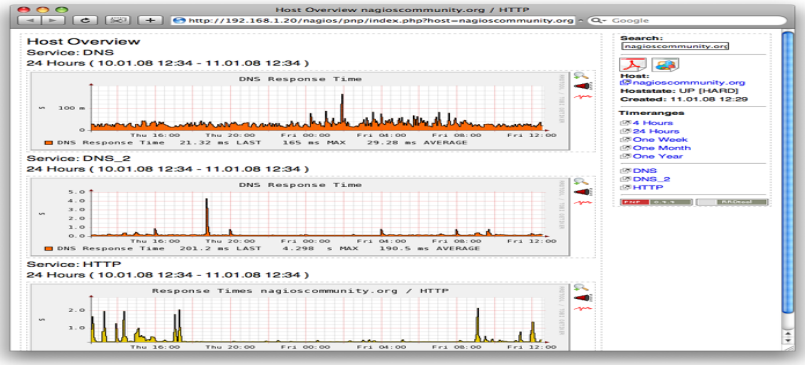

Fig. 2 Nagios monitoring sofware package

The features of Nagios include:

- ✓ Monitoring of network services (SMTP, HTTP, NNTP, ICMP, SNMP)
- ✓ Monitoring of host resources (processor load, disk usage, system log) in network operating systems
- ✓ Remote monitoring supported through SSH or SSL encrypted tunnels.
- ✓ A simple plugin design that allows users to easily develop their own service checks depending on needs (Fig. 3), by using their tools of choice (shell scripts, C++, Perl, Ruby, Python, PHP, C#, etc.)
- ✓ Parallelized service checks

Fig. 3 Nagios operation

- ✓ The ability to define network host using 'parent' hosts, allowing the detection of and distinction between hosts that are down or unreachable
- ✓ Contact notifications when service or host problems occur and get resolved (via e-mail, pager, SMS or any user-defined method through plugin system)
- ✓ Ability to define event handlers to be run during service or host events for proactive problem resolution
- ✓ Various software add-ons that provide a general overview of all hosts through which monitoring is performed.

Cacti - Open-source network monitoring program [11]

Cacti is an open-source and web-based network monitoring designed as a front-end application for the open-source, using RRDtool for data collection and graphing (Fig. 4). The program is written in PHP and the data is stored in a MySQL database.

The features of Cacti include:

- ✓ unlimited graph items
- ✓ built-in SNMP support
- ✓ templates of graphs, hosts and data sources
- ✓ data gathering on a non-standard timespan
- ✓ tree, list and preview views of graph data
- ✓ working with multiple users of their own graphs
- ✓ using additional scripts to monitor any type of data.

Fig. 4 Cacti network graffic monitoring software package

Research results

Considering the mentioned systems and their features, we represent comparative analysis in this section based on our own criteria (Table 1). Comparative analysis reveals the most effective tool for monitoring computer networks which is applicable by myriad organizations.

Table 1

Comparison of monitoring software packages

Criteria	Network monitoring software		
	ZABBIX	**NAGIOS**	**CACTI**
Charts	+	+	+
SLA report	+	Via Plugin	+
Logical grouping	+	+	-
Trending	+	+	+
Trend Prediction	+	-	-
Automatic detection	+	Via Plugin	-
Agent	+	+	+
SNMP	+	Via Plugin	+
Syslog	+	Via Plugin	-
External scripts	+	+	-
Plugins	+	+	+
Difficulty of creating plugin	Easy	Easy	Easy
Triggers	+	+	-
Web access	Full access	Viewing, reporting, managing	+
Distributed monitoring	+	+	-
Data storage method	SQLite, MySQL, PostgreSQL, Oracle	Non-dynamic, non-expandable database, SQL	MySQL
License	GNU GPL	GNU GPL	BSD
Cards	+	Dynamic and constructive	-
Language	C, PHP	C	C, Perl, PHP, Python

Conclusion

Sample and comparative analysis of computer network monitoring software packages has been revealed in this research that ZABBIX is more efficient than NAGIOS and CACTI systems. It is worth mentioning that ZABBIX provides support in different operating systems, has a perceptible,

easy and friendly interface, graphical capability of monitoring data with different parameters, combination of languages and so forth.

From now on, the presented comprehensive research enables users to make more conscious and efficient choices according to their own requirements.

References

1. Tadosyan A.A., Galstyan H.A. Building a school network model in CISCO Packet Tracker environment (2017) //Yerevan, 2017, ASPU Scientific Bulletin, No. 4 (33).- p. 47-53.
2. Wakke A.D. Zabbix A practical guide (2017) //DMK Press, 2017.- 356 p.
3. Lavrov A.A. Monitoring and administration of corporating networks (2013) //Monograph, S.A. Ivanovsky A.A. Lavrov, V.V. Yanovsky, SPb. Publishing house “SPbGETU” LETI”, 2013.- 160 p.
4. Olifer V.G., Olifer N.A. New technologies and equipment for IP networks (2000) //SPb.: BHV-Saint Petersburg, 2000.- 512 p.
5. Wilson Ed. Monitoring and analysis of networks. Troubleshooting methods (2002) //M:, LORI, 2002.- 364 p.
6. Aftimiei C. Recent evolutions of GridlCE: a monitoring tool for grid systems (2007) //C. Aftimiei, S. An-dreozzi, G. Cuscela, G. Donvito, V. Dudhalkar, S. Fantineli, E. Fattibene, G. Maggi, G. Misurelli, A. Pierro, Proceedings of the 2007 workshop on Grid monitoring, New York, 2007.- p. 1-8.
7. Gu J. Efficient Network Monitoring System (2012) //J. Gu, Y. Wu, Z. Gu, Communications in Computer and Information Science, 2012, Vol. 308.- p. 34-40.
8. McKellar J. Twisted Network Programming Essentials (2013) //J. McKellar. - O'Reilly Media, 2013.
9. Nagios: Nagios Documentation – http://www.nagios.org/ (available 31/03/2021)
10. Zabbix: What is Zabbix – http://www.zabbix.com (available 31/03/2021)
11. Cati: https://www.cacti.net/documentation.php (available 31/03/2021)

References

1. Թադևոսյան Ա. Ա., Գալստյան Հ. Ա. Ուսումնական հաստատության լոկալ ցանցի մոդելի կառուցում CISCO Packet Tracker միջավայրում (2017) //Երևան, 2017թ.,ՀՊՄՀ գիտական տեղեկագիրը, թիվ 4 (33).- էջ 47-53:
2. Вакке А.Д. Zabbix. Практическое руководство (2017) //ДМК Пресс, 2017.- 356 с.
3. Лавров А.А. Мониторинг и администрирование в корпоративных вычислительных сетях (2013) // монография, С.А. Ивановский, А.А. Лавров, В.В. Яновский, СПб.: Изд-во «СПбГЭТУ «ЛЭТИ», 2013.- 160 с.
4. Олифер В.Г., Олифер Н.А. Новые технологии и оборудование IP-сетей (2000) //СПб.: БХВ-Санкт-Петербург, 2000.- 512 с.
5. Уилсон Эд. Мониторинг и анализ сетей. Методы выявления неисправностей (2002) //М.: ЛОРИ, 2002. - 364 с.
6. Aftimiei C. Recent evolutions of GridlCE: a monitoring tool for grid systems (2007) //C. Aftimiei, S. An-dreozzi, G. Cuscela, G. Donvito, V. Dudhalkar, S. Fantineli, E. Fattibene, G. Maggi, G. Misurelli, A. Pierro, Proceedings of the 2007 workshop on Grid monitoring, New York, 2007.- p. 1-8.
7. Gu J. Efficient Network Monitoring System (2012) //J. Gu, Y. Wu, Z. Gu, Communications in Computer and Information Science, 2012, Vol. 308.- p. 34-40.
8. McKellar J. Twisted Network Programming Essentials (2013) // J. McKellar. - O'Reilly Media, 2013.
9. Nagios: Nagios Documentation – http://www.nagios.org/ (հասանելի է 31/03/2021)
10. Zabbix: What is Zabbix – http://www.zabbix.com (հասանելի է 31/03/2021)
11. Cati: https://www.cacti.net/documentation.php (հասանելի է 31/03/2021)

ՀԱՄԱԿԱՐԳՉԱՅԻՆ ՑԱՆՑԵՐԻ ՄՇՏԱԴԻՏԱՐԿՄԱՆ ՀԱՄԱԿԱՐԳԵՐԻ ՀԱՄԵՄԱՏԱԿԱՆ ՎԵՐԼՈՒԾՈՒԹՅՈՒՆԸ

Հ.Ս. Աբգարյան
Հայաստանի ազգային պոլիտեխնիկական համալսարան

Հոդվածում ներկայացված են համակարգչային ցանցերի մշտադիտարկման առավել տարածված համակարգերի վերլուծությունը, որի արդյունքում մշակվել են նաև համակարգչային ցանցերի մշտադիտարկման գործիքակազմի ընտրության արդյունավետության նորովի չափանիշներ և առաջարկներ համակարգչային ցանցերի մշտադիտարկման արդյունավետ գործիքակազմ ընտրելու համար:

Բանալի բառեր. համակարգչային ցանցեր, մշտադիտարկում, արատորոշում, վերլուծություն, ցանցային արձանագրություն, կառավարում, ծրագրավորում:

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СИСТЕМ МОНИТОРИНГА КОМПЬЮТЕРНЫХ СЕТЕЙ

О.С. Абгарян
Национальный политехнический университет Армении

В статье представлен анализ наиболее распространенных систем мониторинга компьютерных сетей, в результате которого были разработаны новые критерии эффективности выбора инструментов мониторинга компьютерных сетей, а также предложена критерии по выбору эффективного инструмента мониторинга компьютерных сетей.

Ключевые слова: компьютерные сети, мониторинг, диагностика, анализ, сетевой протокол, управление, программирование.

Ներկայացվել է՝ 01.04.2021թ.
Գրախոսման է ուղարկվել՝ 13.04.2021թ.
Երաշխավորվել է տպագրության՝ 28.04.2021թ.