www.volsu.ru

DOI: https://doi.org/10.15688/mpcm.jvolsu.2018.3.4

UDC 004.414
LBC 32.973.202-018.2

NEXT-GENERATION NETWORK MONITORING SYSTEMS — CRITICAL REQUIREMENTS AND DESIGN

Alexander Maksimovich Natarov

Student, Volgograd State University
natarov.a.m@volsu.ru, kiem@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Alexander Alexandrovich Shirokii

Candidate of Physical and Mathematical Sciences, Senior Researcher,
Laboratory of Modular Information-Control Systems,
V. A. Trapeznikov Institute of Control Sciences Russian Academy of Sciences
shiroky@ipu.ru
Profsoyuznaya St., 65, 117997 Moscow, Russian Federation

Abstract. The article deals with the monitoring systems and their usage in IT-infrastructure. The first generation of monitoring systems grew up from instruments made by software companies for their internal needs. Such systems currently fail to meet the actual business requirements. The number of used by common enterprises business applications and software services grows vigorously. It led to depletion of legacy systems'' scaling abilities. Now business asks for new generation monitoring systems, which are flexible, able to process large-scale IT-infrastructures and has low operation costs. This article is devoted to revealing qualitative monitoring systems requirements by evaluation of several companies'' business requirements. Those companies have various level of IT infrastructure integration in their business processes. We interviewed more than 50 tech specialists and managers and grouped requirements by IT-infrastructure scale. We formulated critical requirements for new generation monitoring systems using previously collected data and also opened access to best-practices of such systems implementation and usage. We also proposed feasible architecture of next-generation monitoring system.

Key words: monitoring systems, monitoring system requirements, LAN monitoring, monitoring of computer networks, notification of network failures, monitoring system design.

Introduction

Information systems become more complicated due to IT development, namely, accumulating more and more information and improvement in collecting and analyzing algorithms. The "Internet of Things" and microservices architecture grow quickly and produce a lot of new data sources [12; 13]. When such number of sources incorporates into the certain information system the brand-new class of tasks appears. Now system administrator needs to keep a close eye on network resources availability and balance of their use.

The structure of digital content consumption has also changed significantly. Whereas 20 years ago most Internet sites contained only simple and small-sized HTML pages, today just the Netflix company, renting out films and serials, generates up to a third of a day traffic in the US [14]. Volumes of transmitted data are constantly grow up — for example, we prefer to watch video content in 4K, which requires 2.5x times more bandwidth than the same video in FullHD. Soon the network requirements will significantly increase again due to the introduction of the 8K standard.

This is why both internet providers and users need more and more computing resources. For instance, the Amazon company declares revenue from the AWS infrastructure, which provides virtual servers for rent, of nearly USD 5 billion [8]. The NSA of the US is also purchasing servers in large volumes [16].

The risks of computers and network failures are increasing with infrastructure complexity. It is necessary to use a new approach for the development of the organization and technical systems, allowing to minimize the number of failures by their forecasting and taking proactive measures, on the one hand, and to ensure the quick failure response of IT-department, on the other.

The solution is to deploy a monitoring system, that could rapidly detect infrastructural failures, predict a breakdown, reveal the inefficient and aberrant behavior of hardware. Let us define "monitoring" as continuous process of watching the specified parameters of certain object, registering their values, and comparing them with specified criteria. Accordingly, "monitoring system" is a specialized software that monitors parameters of software services and hardware, their compliance with the specified patterns and checks services availability. In the case of error, the monitoring system notifies the system administrator and, possibly, takes some actions automatically. It is possible to monitor infrastructural indicators (accessibility of nodes from the network, CPU load, RAM usage, free space on disks, etc.) [1; 6; 15], and service indicators (DB write queue, some changes at logs, etc.). Such systems allow not only to react to the problems swiftly but solve them proactively by revealing potential vulnerabilities. That is the way to minimize or completely eliminate infrastructure failures.

The first monitoring systems appeared in the late 1990s. At the beginning of the 2000s, there were three leading systems — MS SCOM, Zabbix, and Nagios. All of them were developed for the internal needs of the companies-creators and then grew up in the large projects for a wide range of business users. However, no one expected such an intensive infrastructures growth when designed these systems, and their scalability depleted quickly. System requirements become too high and operating costs of monitoring a bulk of nodes become comparable to those for basic IT services, such as domain controllers or data warehouses.

In this paper, we identify and describe the key requirements for new-gen monitoring systems that can be used in business.

1. Material and Methods

To specify the monitoring systems key requirements, we have to describe typical business customers of software of that kind.

Generally, all the companies which have complex IT infrastructure are potential users of monitoring systems. Large enterprises like banks or governmental structures and IT companies use such systems very often.

QUESTIONNAIRE

- Job title
- Scope of the company
- Number of employees in the company
- How many servers are used in company?
- How often do failures occur?
- How much does the company lose profits per hour of downtime?
- Is the monitoring system being used?
- If the system is not used, why? Were there any attempts at implementation?
- If the system is used, which one and what disadvantages it has?

Fig. 1. Questionnaire for IT manager

We have interviewed the support and infrastructure experts currently using monitoring systems to determine the key requirements for them. Figure 1 represents the questionnaire. On the basis of the analyzed interviews, we conclude that requirements vary depending on the scale of the IT infrastructure, but no association between industry types was found. This means that requirements grouping is not necessary.

In addition, the authors interviewed IT specialists of several companies that are not using monitoring systems in order to infer their opinion on such systems in general and on the applicability of them in specific business situations. There is publicly available data [2; 5; 7] describing monitoring systems use cases, typical difficulties in their implementation and support. Key requirements for a ready-for-production monitoring system were formulated on the basis of all the data analysis.

2. Requirements description

A contemporary enterprise-class monitoring system should satisfy at least four requirements in order of decreasing priority:

1. Robustness.
2. Low resource utilization.
3. High convenience and follow-on development possibility.
4. Low cost of ownership.

2.1. Robustness

In case of monitoring systems, robustness means not only the uninterrupted operation but, first of all, guarantee to respond to unfavorable changes of monitored parameters. The system can automatically react to events (e.g. restart the service in case of failure) and inform the IT staff about the failure. Reliable delivery of notices is an important factor for reducing the downtime of the service. But the most important function is to immediately notify IT staff when any parameter ??exceeds its regular range of values. It allows the IT service to predict a bottleneck formation and to resolve possible problems proactively [11]. It is paramount to balance the number of incoming notifications. If the system disturbs the system administrator too often, he will start to ignore its notifications and, as a result, could omit notification of a serious malfunction.

Enterprise-class monitoring systems collect a huge amount of data on the host: starting with the CPU load and ending with the number of processes running in the OS. Informing of all the changes in such parameters is redundant. Nevertheless, this information could be necessary to analyze load changes and plan the infrastructure development.

We suppose that it is necessary to allocate at least 3 levels of notifications:

- information level — shows all the messages;
- important only level — shows only messages about probable problems;
- critical only level — notifies only about the malfunctions occurred (inaccessibility of sites and services) and large deviations of critical parameters.

The monitoring system should be able to group messages in different ways and allow the administrator to manage groups and set up alerts. This makes configuration of the notification system flexible enough. For example, critical messages could be delivered through several communication channels simultaneously (SMS + Messengers + phone call + ...). Information messages do not need individual alerts — it is enough to view them at the web interface or include in the consolidated report.

2.2. Resource utilization

Typical IT infrastructure size constantly growth as well as the amount of data it serves. Accordingly, there are more failure points, which need to pay attention to — so, the monitoring system should monitor an increasing number of nodes.

Hence, the second critical requirement is the effective use of resources: network bandwidth, monitoring server CPU resources, etc. Operating costs on the monitoring system should not be excessive.

If the system needs to transmit and receive a vast amount of data every second, record it on a drive, and read it to notify about the problem, then such a system will certainly be ineffective — the costs of its running will exceed those for productive services.

To ensure minimum functionality of the monitoring system, it is necessary to transmit a status flag (1 byte) and a unique device identifier (GUID, 16 bytes). Thus, the minimum data packet size is 17 bytes. The volume packet will increase with the amount of information transmitted.

We will model the monitoring scenario of a typical medium-sized company. Suppose that there are one hundred monitored nodes. Let us calculate how much information will be transferred to the monitoring system server in various working modes.

In the first case, agents will collect and send critical information only — the availability flag and the machine number. If the system requests host one time per 10 seconds, then for 1 hour will be sent to $17 \times 6 \times 60 = 6\,120$ bytes $= 6$ KB. Therefore, for 1 hour the system will receive about 600 KB of data at all, which is not so many.

In the second case, agents collect and transfer all possible parameters about the host: the number of processes and their list, CPU and RAM usage, free space on the drives. The operational experience of existing monitoring systems makes it possible to estimate the volume of such a package in 2 MB. Then each host will transfer about $2 \times 6 \times 60 = 720$ MB of data per hour. So, all the data processed within an hour will be sized in about 70 GB.

That volume is already quite large and we must remember that as the number of nodes increases the amount of data transferred will also increase. If we collect not only information about the host itself, but also detailed information about the work of programs on it, sending copies of log files, the amount of information will multiply.

Thus, the workload of the monitoring system is large enough and grows rapidly when scaling, so this system should use available resources as economically as possible.

2.3. Convenience and further development

Complex systems like a monitoring system require serious costs for implementation and maintenance. Therefore, it is important to make the system as convenient as possible in the process of installation and during everyday operation of its main user — a system administrator [4].

Another part of the monitoring system features is the possibility of its further development and adaptation for particular tasks. If the organization needs to monitor some specific indicators, e. g. the number of packets that come from a specific host over the network or the temperature at one of the sensors connected to a remote computer, a good monitoring system should allow this to be done with the minimal time and effort of technical staff [3; 9].

In addition, monitoring system should be universal. If system administrator needs one system to monitor hardware parameters and another one to monitor the status of web servers, then such a complex of systems will be quite difficult to administer.

Figure 2 shows an example of a flexible monitoring agent. Monitoring itself is implemented with the modular system that will allow configuring the agent for various tasks. As modern programming languages allow to make cross-platform code easily, so we design the architecture without binding to a particular operating system.

Figure 3 suggests the architecture of the server side of the enterprise-class monitoring system. The reporting subsystem generates reports in various formats and allows to automate their delivery. This subsystem should minimize interaction with the system interface.

2.4. Cost of ownership

This requirement describes not only the cost of the license but also the cost of the infrastructure for the system. We are addressing the point separately here because the cost of a license often exceeds the cost of the rest of the required infrastructure.

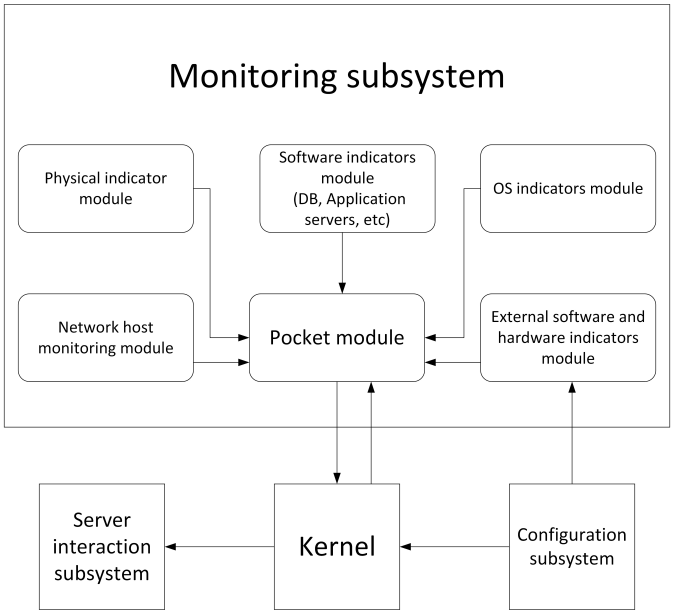

Fig. 2. Monitoring system agent architecture

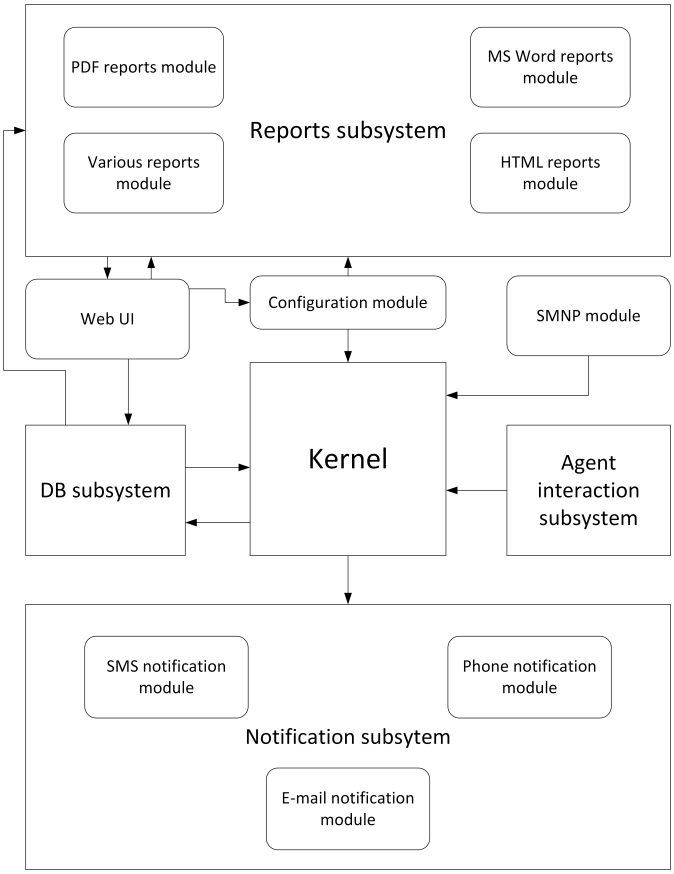

Fig. 3. Monitoring system server architecture

Most monitoring systems distribute under one of the free licenses but commercial solutions from HP, Microsoft or IBM brings the biggest part of the costs in the license, not in the cost of the infrastructure to deploy.

In addition to all the above, commercial licenses mostly prohibit the modification of software except the one already incorporated into it by the manufacturer. For example, DB monitoring module is not bundled in SCOM and it costs several thousands of USD to buy it from external suppliers [10]. The cost of developing one's own module is not much lower but depends on the skill level of the development team.

It is important to bear in mind that the main cost of monitoring systems is not the license cost, but the costs of a system running and support; not only at the time of implementation but also during subsequent operation. In the free monitoring systems, there are no expenses for licensing, but there are no less, and often even larger, costs of qualified specialists needed to implement and maintain the system. The server resources cost to deploy the system are relatively not significant in the long run, compared to the expenditures we were talking earlier.

Conclusion

This study presents the key requirements of the new generation monitoring systems. These systems should be robust, flexible and require low operating costs for use in production.

In addition, the authors proposed the system architecture that satisfies the identified requirements. Using this architecture helps to develop the system with the implementation of all requirements, including speed and cost of ownership.

REFERENCES

1. Barash L. Monitoring trafika v setyakh s kommutatsiey paketov [Traffic Monitoring in Packet-Switched Networks]. *Kompyuternoe obozrenie*, 2008, vol. 37 (654), pp. 20-25.

2. Veselukha G.L. Inzhenernyy vzglyad na monitoring oborudovaniya Tsentrov obrabotki dannykh [Engineering View on Monitoring of Data Center Equipment (Implementation Experience)]. *Elektronnyy nauchnyy zhurnal «Vek kachestva»*, 2017, vol. 2, pp. 100-111.

3. Vysochina O., Shmatkov S., Mukhsin S.A. Analiz sistem monitoringa telekommunikatsionnykh setey [Analysis of Telecommunications Networks Monitoring Systems]. *Radioelektronika, informatika, upravlinnya* [Radio Electronics, Computer Science, Control], 2010, vol. 2, pp. 139-142.

4. Gayfulin T., Kostomarov D. Analiz sovremennykh sistem monitoringa [Analysis of Modern Monitoring Systems]. *Izvestiya TulGU. Tekhnicheskie nauki*, 2013, vol. 9, iss. 2, pp. 51-55.

5. Kazmin D. *Opyt vnedreniya sistem IT-monitoringa. Forum IBM 2012* [Experience in Implementing IT Monitoring Systems. IBM Forum, 2012]. URL: https://www.ibm.com/ru/events/presentations/perm2012/kazmin.pdf.

6. Storozhuk D.O. *Metody i algoritmy dlya sistem monitoringa lokalnykh setey: dis. ... kand. fiz.-mat. nauk* [Methods and Algorithms for Local Area Network Monitoring Systems. PhD Dissertation]. Moscow, 2008. 97 p.

7. Chudinov V. *Opyt vnedreniya sistemy monitoringa informatsionnykh resursov na baze produktov IBM Tivoli v GVTs OAO RZhD. IBM PCTY 2011* [Experience in the Implementation of the Monitoring System for Information Resources on the

Basis of IBM Tivoli Products in the JSC Russian Railways. IBM PCTY, 2011]. URL: https://docplayer.ru/50463680-Opyt-vnedreniya-sistemy-monitoringa-informacionnyh-resursov-na-baze-produktov-ibm-tivoli-v-gvc-oao-rzhd.html.

8. *Amazon Report*. URL: https://aws.amazon.com/ru/resources/analyst-reports.

9. Croll A. *Complete Web Monitoring*. Sebastopol, O'Reilly Media, 2009. 672 p.

10. *Introduction to the Deployment Guide for Monitoring Server*. URL: http://technet.microsoft.com/ruru/library/dd630725(v=office.12).aspx.

11. Jones D. *Creating Unified IT Monitoring and Management in Your Environment*. San Francisco, Realtime Publishers, 2012. 92 p.

12. *Microservice architecture pattern language*. URL: http://microservices.io.

13. Fowler M., Lewis J. *Microservices — a definition of this new architectural term*. URL: http://martinfowler.com/articles/microservices.html.

14. *Washington Post: Netflix now accounts for almost 37 percent of our Internet traffic URL*. URL: https://www.washingtonpost.com/news/the-switch/wp/2015/05/28/netflix-now-accounts-for-almost-37-percent-of-our-internet-traffic.

15. Wilson E. *Network Monitoring and Analysis: A Protocol Approach to Troubleshooting*. Upper Saddle River, Prentice Hall, 2000. 350 p.

16. *Wired: The NSA Is Building the Countrys Biggest Spy Center*. URL: https://www.wired.com/2012/03/ff_nsadatacenter.

СИСТЕМЫ МОНИТОРИНГА СЛЕДУЮЩЕГО ПОКОЛЕНИЯ — КРИТИЧЕСКИЕ ТРЕБОВАНИЯ И АРХИТЕКТУРА

Александр Максимович Натаров

Студент, Волгоградский государственный университет
natarov.a.m@volsu.ru, kiem@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Александр Александрович Широкий

Кандидат физико-математических наук, старший научный сотрудник лаборатории модульных информационно-управляющих систем,
Институт проблем управления им. В. А. Трапезникова РАН
shiroky@ipu.ru
ул. Профсоюзная, 65, 117997 г. Москва, Российская Федерация

Аннотация. В статье рассматриваются вопросы применения систем мониторинга в IT-инфраструктурах реальных предприятий. Первое поколение систем мониторинга выросло из разработок для внутренних нужд компаний-разработчиков и в настоящий момент уже не удовлетворяют в полной мере актуальным бизнес-требованиям. Интенсивный рост числа применяемых на среднем предприятии корпоративных бизнес-приложений и сервисов привело к быстрому исчерпанию заложенных в старых системах возможностей масштабирования. В этих условиях актуализировалась задача создания систем мониторинга нового поколения: гибких, рассчитанных на крупные IT-инфраструктуры, требующих минимальных накладных расходов на функционирование. Настоящая работа посвящена выявлению качественных требований к системам мониторинга следующего поколения путем анализа

бизнес-требований ряда компаний с различным уровнем интеграции информационных технологий в деятельность. Авторы провели свыше 30 интервью технических специалистов и руководителей, объединив требования в группы, соответствующие различным масштабам IT-инфраструктуры. На основе этих сведений, а также анализа доступных в открытых источниках данных о сценариях использования систем мониторинга, типичных затруднениях при их внедрении и поддержки в компаниях различных направлений деятельности и размеров, авторами были сформулированы критические требования к системам мониторинга нового поколения. Также предложен вариант архитектуры такой системы.

Ключевые слова: системы мониторинга, требования к системе мониторинга, мониторинг ЛВС, мониторинг вычислительных сетей, оповещение о сбоях в сети, архитектура систем мониторинга.