Monitoring of computer networks and applications using Nagios

MIROSLAV MATÝSEK, MILAN ADÁMEK, MAREK KUBALČÍK, MIROSLAV MIHOK
Tomas Bata University in Zlín
Department of Computer and Communication System
Nad Stráněmi 4511, 76005, Zlín
CZECH REPUBLIC
matysek@fai.utb.cz
http://web.fai.utb.cz/

Abstract: - The aim of this work was to test and prepare for common use a free supervisory system for monitoring of computer networks. The paper is focused on different methods and tools for monitoring. The Nagios monitoring tool is described comprehensively including its configuration. The paper also focuses on installation and application of its functionalities on the current most widely used operating systems. The system is able to send a notice by e-mail, SMS messages and generate statistical graphs of the measured values.

Key-Words: - Nagios, monitoring system, computer network, SNMP protocol, SAP, Linux, Microsoft Windows

1 Introduction

At the present electronic age there is probably no company or organization which can do without information technology. Most people perceive the computer as a tool for sending emails, surfing the Internet and using of the office application software. More technical skilled people use the computer for example for programming applications such as manufacturing tools or use the computers for data collection.

If a surveillance monitoring system is applied, most system administrators know about the problems that arise almost immediately. They have it exactly and immediately located and may solve it quickly. In most of cases then it is not necessary to argue with the user which largely is not an expert in the area of information technologies. Of course, the deployment of the monitoring system sharply reduces time of unavailability of systems and consequently caused damages. With help of these systems it is possible to prevent many problems such as stopping the server due to overfilling the disk array. This problem can be detected even earlier than it ever occurs.

With an appropriate monitoring system it can be supervised even non-critical devices such as network printers that are able to send information about the remaining amount of toner in its cartridge or information about the need of repairs.

If a company has a large number of systems and equipment, the deployment of a monitoring system is necessary. If the company also needs to save money, then the ideal choice is utilization of free software. One of the many options is the systems Nagios, Other possibilities are systems such as Zabbix or Cacti.

A typical example of a network administrator working day:
It is ten o'clock on Monday morning. Branch manager is furious because he is waiting for an important email which has not been delivered yet. The administrator finds by fast control that the messages are not stuck in the queue. There is also no reference in the log file and the email from the sender has arrived. So where's the problem? The central mail server is not also responding to the program Ping. This is probably the merit of the problem. But the IT department insists on the fact that the situation is not their fault and that the network is running properly at the headquarters and that the problem must be in the branch network. Searching of the error continues and finally it is found that that the VPN line to the head office was not operational because the back-up line did not set up routing rules. The final result is a lot of minutes spent on finding errors, edgy director (the action for which the email was necessary already expired) and sweaty administrator.

In case that a monitoring supervisory system is deployed, then system administrators mostly know about an arisen problem almost immediately. They have it precisely localized and they can it quickly remove. In most cases then it is not necessary to negotiate with a user who may not be an expert in

ISBN: 978-1-61804-118-0

information technology. Of course, deployment of a monitoring system sharply reduces the time of availability and reduces damages which can be consequently caused.

2 Nagios Monitoring System

2.1 System Description

The development of the program began in 1999. The original name of the project was Netsaint. It was finished in 2002 and it further continued under a new name - Nagios. The author is Mr. Ethan Galstad, who is currently also the president of Nagios Enterprises [1].

It is a very popular monitoring system. This fact also confirms a symposium which was released on the discussion forum for fans of Linux distributions.

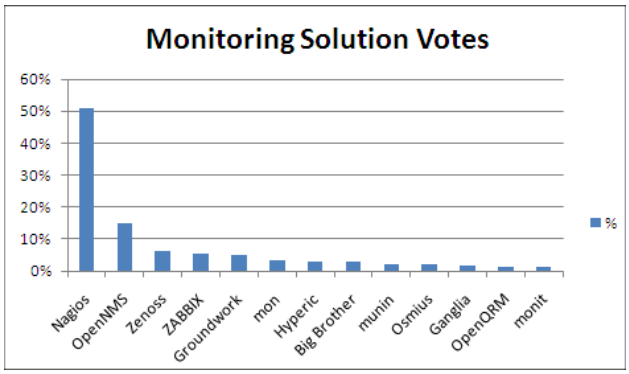

Fig. 1 Poll of the best monitoring tool

2.1.1 Hardware Requirements

According to discussion forums on the Internet the system with a standard dual core processor and 5 GB of RAM is able to process 2000 services per minute.

2.1.2 Software Requirements

- Web server such as Apache and more.
- PHP 4.3 and more.
- MySQL 4.1.
- PEAR Module: HTML_Template_IT 1.1 and more.
- PHP Extension: gettext.
- PHP Extension: mysql.
- PHP Extension: ftp.
- Javascript enabled in your web browser.

2.1.3 Daemon

The Nagios daemon is a major part of the core. After its start are loaded settings from the configuration files and the monitoring of equipment and services begins. The communication of the daemon with the environment is implemented via files in which are stored the outputs as well as are read the input data.

2.1.4 Plugins

The core of Nagios is not able to control services as well as to notify their modifications. The control is performed by a plug. Plugs are incorporated between the core of Nagios and monitored hosts and services [2].

Plugs are small independent scripts that are used to control services on remote hosts. They can take a form of the Perl script or the Shell script. They run from the command line. The output of the plugs should always be directed to STDOUT (standard output). The output string should not have more than 80 characters.

Plugs are not distributed with the program core but they can be downloaded from the official website of the program or from pages of volunteer plug developers.

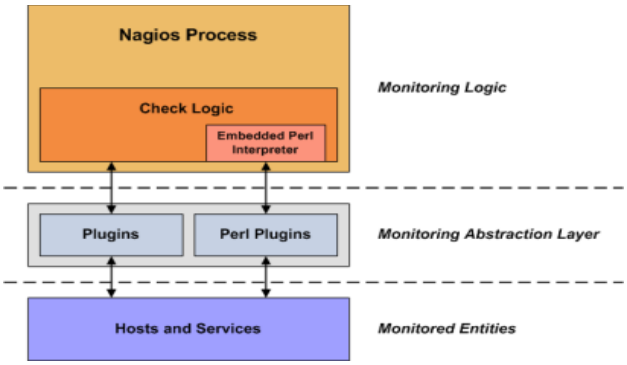

Fig. 2 Block diagram of the integration of plug-in architecture Nagios

2.1.5 Return Codes

Nagios evaluates the status of the host or his service via return codes from plug-ins. The following table contains a list of return codes along with the status of the service or host [3].

Table 1 Return codes from the plug

Return code	Status of service	Status of host
0	OK	UP
1	WARNING	UP or DOWN
2	CRITICAL	DOWN/UNREACHABLE
3	UNKNOWN	DOWN/UNREACHABLE

ISBN: 978-1-61804-118-0

2.2 Scheduling of Tests

Nagios core contains a very sophisticated scheduler with many user defined options.

2.2.1 Check Interval

All internal processes of Nagios, including host and service controls, are located in the global event queue. Schedule of control actions can be defined by a user, but not using the specified absolute date or time in cron (Unix/Linux) or Task Scheduler (Windows). This is caused by inability of Nagios to check how long it will be performed a monitoring program (plugin). Instead of it, Nagios can tell you how long to wait before it can run again after its finish.

It should be noted that the inspection interval is sufficient to define only for control of services. It is also possible to specify it during specification of the control interval of the target guest. But this is not necessary because host checks are usually carried out after failure of control service. If services are not working then it is assumed that the host is not accessible. The default interval length of control is 60 seconds [4].

2.3 SNMP Monitoring

The SNMP protocol was originally created for a remote control of devices of computer networks. It is an application protocol that provides services for management over the UDP protocol. The SNMP is based on the client/server model. The client program called network manager creates a virtual connection to the server. A SNMP agent is running on the monitored network device. The agent monitors the devices status and provides information about it by the manager. Information provided by the agent is arranged according to the MIB database (Management Information Base) that its the structure corresponding to the device.

The advantage of this solution is that it is necessary to have a password to the privileged mode. The community string can be used for access to the device, which can be defined as read-only.

3 Monitoring Systems

3.1 SAP System Monitoring

There are several ways of monitoring the SAP (System Analyse und Programmentwicklung) systems. The simplest way is to control the ports on which the SAP system is running. It is usually running on ports 3200/3300 for numbers 00 and ports 3201/3301 for numbers 01, etc. This simple check can be made by check_tcp plug. In case that the internal services in SAP fail, the terminal user will not be able to sign to the system even if the ports will be available. If it is necessary to test complex interactions between components of the SAP then communication is needed at the application layer [5].

3.1.1 Control Using sapinfo

The program sapinfo is a part of an optional RFC-SDK package (Remote Function Call Software Development Kit) used in RFC interfaces. The package can be downloaded from SAP portal at http://service.sap.com, but for login it is necessary to have a customer number.

3.1.2 Control via Plug Check_sap.sh

Plug check_sap.sh is a script that is based on the program sapinfo. It is included in a package with plugins for Nagios in the contrib directory. Since it is not installed automatically it must be manually copied to the plugins directory.

3.1.3 Control via CCMS

The SAP system has its own monitoring system called CCMS (Computing Center Management System) in which local agents, determined for data collection, collect data from different hosts. CCMS is not just for SAP systems but it can monitor also external third-party applications.

Fortunately, the developers thought to the possibility of monitoring the CCMS and programmed plug-ins for the data collection system Nagios.

3.2 Monitoring of Linux/Unix

There are several different ways how to monitor attributes on remote Linux/Unix server. One of the possible approaches is a method with help of the SSH keys (Secure Shell), created SSL (Secure Sockets Layer) connection and plug modul Nagios check_by_ssh. The plugins are activated on a remote server. The disadvantage of this method is an extreme load on monitoring server in case we want to monitor hundreds of services or possible destruction of an encrypted SSH connection.

The second method uses NRPE (Nagios Remote Plugin Executor) which enables activating of plugins on a monitoring remote server [6].

ISBN: 978-1-61804-118-0

3.2.1 Direct Control Using the NRPE

Fig. 3 shows the most common use of the NRPE daemon. In this case, only local sources on a remote server are monitored, for example load of the CPU, availability of memory or disk array, swap, number of registered users etc.

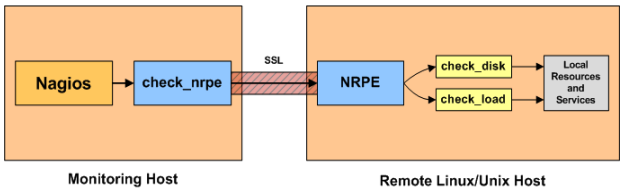

Fig. 3 Block diagram of the direct control of NRPE

3.2.2 Indirect Control Using the NRPE

Fig. 4 shows how to use the NRPE for control of services and resources on remote servers that are not accessible from the monitoring machine which is running Nagios.

In this case, the NRPE daemon acts as a proxy server.

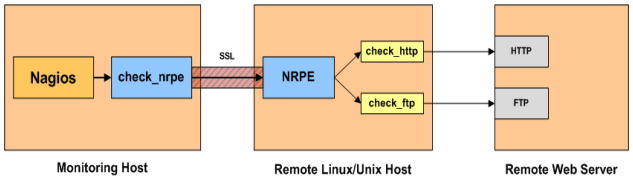

Fig. 4 Block diagram of indirect control NRPE

3.3 Monitoring of Microsoft Windows

Monitoring of running services on systems with the Microsoft Windows using Nagios is relatively easy to implement. One of the possibilities is utilization of the standard functionality of Windows and install the SNMP protocol support from the installation CD.

Another option is using of an agent NSCClient++.

3.3.1 Agent NSCClient++

It is a simple and secure monitoring agent written for Microsoft Windows operating systems. This agent serves as a proxy between the Nagios plug-in and a monitoring service or attribute on the Microsoft Windows server. Private services such as availability of the memory, disk space or CPU load can not be monitored without this client.

In case of monitoring of public services such as HTTP, FTP, POP3, it is possible to use Nagios plugins check_http, check_ftp, check_pop.

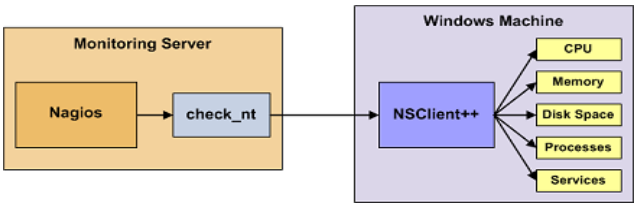

Fig. 5 Block diagram of the control agent using NSClient++

Fig. 5 shows the principle of collecting of the monitoring data using the Nagios plug-and check_nt agent NSClient++. During questioning about the data, NSClient++ will request for them. Further it will store the data in an internal stack and subsequently it will provide them to a plug-in check_nt for further processing.

3.4 Sending Notification

Only few computer network administrators are able constantly monitor changes in the monitoring tool. Therefore, also Nagios has the option of sending the notice by mail, SMS, pager or VoIP (connection to Asterisk). In order Nagios not to become a "spam server", it should be considered when the notifications will be sent, in what quantities and to how many recipients. It is not always needed to send a notification to the system administrator.

3.4.1 Sending Notification via E-mail Messages

In order to deliver alarm notifications from Nagios to the terminal recipient, it is necessary to use either a functional mail server or to install it on the server with Nagios. A possible solution is, for example, Postfix mail server that is simple to install and initially configure.

3.4.2 Sending Notification via SMS

Nowadays almost everyone owns a mobile phone and it would be a shame if the mobile phones are not used also for sending notifications from Nagios via SMS. Even if its length is limited to 160 characters, basic information about the host, failure, time and condition of devices or services fits to it just fine. This option provides a huge benefit to administrators who may be informed of any problems encountered anywhere, even if they are not directly at their computer.

There are many solutions how to send SMS messages from your computer to your mobile phone. On Linux distributions, we can implement SMS as an additional installation by utilities (Gnokii and Yaps) that communicate with a mobile phone which is connected to the computer.

ISBN: 978-1-61804-118-0

Another solution is using of SMS gateways available on the Internet. Clickatell Service Company service which provides SMS messages over HTTPS/API (Hypertext Transfer Protocol Secure/Application Programming Interface) was used in this work. It is necessary to create a login account on this page and enable communication HTTPS/API. Further it is necessary to make settings in the configuration file command.cfg, which defines a command which will be called when an alarm in the monitoring tool for sending notices occurs. This service is chargeable.

Some mobile operators provide a service through which you can send an email to their email account and it is automatically forwarded to your mobile phone.

4 Conclusion

The practical result of this work is the implementation of the Nagios monitoring system for an unnamed company, which will certainly be a great benefit for the company. The company management particularly appreciated network monitoring of the SAP system, which the previous pre-paid network monitoring system did not enable.

The only initial investment of the open-source Nagios product is its installation and configuration. The time spent on its launch will however quickly return in the form of a solid system for monitoring of computer networks from one central point.

References:

[1] C. Burgess, *The Nagios Book,* [online], 2005, [cit. 2010-02-02], Available from: http://www.nagiosbook.org/html/index.html

[2] M. Schubert, *Nagios 3 Enterprise Network Monitoring Including Plug-Ins and Hardware Devices,* Burlington, Syngress Publishing, Inc., 2008.

[3] E. Galstad, *Official Nagios Documentation,* [online], 2010, [cit. 2010-01-28], Available from: http://support.nagios.com/knowledgebase/officialdocs

[4] J. David, *Building A Monitoring Infrastructure With Nagios*, Boston, Pearson Education, Inc., 2007.

[5] W. Barth, *Nagios, System and Network Monitoring*, Munich, Open Source Press GmbH, 2006.

[6] J. Kretchmar, *Open Source Network Administratio,*. Upper Saddle River, Prentice Hall Professional, 2003.