REAL TIME SERVER ALERT SYSTEM USING PORT SCANNING AND REACHABILITY TEST FUNCTIONS

MUHAMMAD HAFIZ BIN MUHAMAD HENDRI

THESIS SUBMITTED IN FULFILMENT OF THE DEGREE OF BACHELOR OF COMPUTER SCIENCE (COMPUTER SYSTEMS & NETWORKS) WITH HONOURS

FACULTY OF COMPUTER SYSTEMS AND SOFTWARE ENGINEERING

2013

ABSTRACT

Server Alert System is a monitoring tool that allows network administrator to monitor and being notified if there is issue related to the server. This system will take action by doing a quick scanning in a time cycle interval. What makes this Server Alert System possible to be developed as an effective tool is that failures in the server can be notified via SMS where the current state of the server can be determined by doing port scanning and sending the ICMP echo messages or can easily know as PING. This system is installed in the server where from the server it will send ICMP message to the gateway for connectivity checking. If the server receives a request time out message, it means the server has no connection with the gateway as well as the internet connection. This system provides several functionalities for keeping the administrator aware of problems in the server through SMS alert. When the system detects an issue, it will immediately send a warning message via SMS to the network administrator. This system will be used along with a modem to provide the SMS module. This system offers the notification that ensures the administrator to recognize there is an issue that needs attention. This Server Alert System is built using VB .Net programming language. The software that will be used is Microsoft Visual Studio 2008 to create a connection between the administrator and the server for monitoring purpose.

ABSTRAK

Sistem Pengawasan Pelayan adalah alat pemantauan yang membenarkan pentadbir rangkaian untuk memantau dan dimaklumkan jika terdapat isu yang berkaitan dengan pelayan. Sistem ini akan mengambil tindakan dengan melakukan imbasan secara pantas dalam tempoh kitaran masa. Apa yang membuatkan Sistem Pengawasan Pelayan ini dapat dibangunkan sebagai alat pemantauan yang berkesan adalah isu yang timbul pada pelayan boleh dimaklumkan melalui SMS di mana status semasa pelayan boleh ditentukan dengan menggunakan imbasan nombor “port” dan melalui mesej “ICMP Echo” atau boleh dikenali sebagai “PING”. Sistem ini dipasang pada pelayan di mana daripada pelayan ia akan menghantar mesej ICMP kepada “gateway” untuk pemeriksaan sambungan. Jika pelayan menerima mesej “request time out”, ia bermakna pelayan tidak mempunyai sambungan dengan gateway secara tdak langsung tiada sambungan internet. Sistem ini mempunyai beberapa fungsi untuk memastikan pentadbir menyedari masalah pada pelayan dengan menerima SMS. Apabila sistem mengesan sebarang isu, dengan segera ia akan menghantar mesej amaran melalui SMS kepada pentadbir rangkaian. Sistem ini akan digunakan bersama-sama dengan modem untuk menyediakan modul SMS. Sistem ini menawarkan pemberitahuan bagi memastikan pentadbir untuk mengenalpasti bahawa terdapat isu pada pelayan yang memerlukan perhatian. Sistem ini dibina menggunakan bahasa pengaturcaraan “VB .Net”. Perisian yang akan digunakan adalah Microsoft Visual Studio 2008 untuk mewujudkan sambungan antara pentadbir dan pelayan untuk tujuan memantau.

LIST OF FIGURES

LIST OF TABLES

CONTENTS

CHAPTER 1

INTRODUCTION

1.1 Overview

System is a group or parts of objects, often consisting of a principal part and a number of less important parts, working together according to a purpose (Concise Oxford Dictionary, 2012). According to Banathy(1997), system can be categorized into two major types which are Natural System and Designed System. The main focus of this study is about the Designed System. It is said to be the creation of the human itself which include the major type of system which is the human activity system. This human activity system should covers three elements such as it must serves the purpose of its collective entity, members, and environment of the larger system in which it is embedded.

Application software is a subclass of the computer software which can causes computer to do specific tasks besides conducting the computer itself (ScienceDaily, 2012). A particular example of specific software is known as application software. The term is applied to differentiate specific software with the software system, which manages and integrates the ability a computer but do not directly done the tasks which benefits the user. The system software serves the application, then it is also serves the user. There are many examples of application software that are used until now. The most popular application software is Microsoft Office, Mozilla Firefox, Adobe Photoshop and several others.

Based on Internet technology growth, the client/server architecture in combination with the object-oriented approach has led the industry of software development and systems development into a new era. It is the architecture of client requesting and receiving specific services from centralized server or can be called as host computer (Encyclopaedia Britannica, 2013). A service request can be said as the need for the user and it depends on the server to decide how to resolve. According to the President of Performance Computing, Richard Finkelstain, the majority of today's client / server-based software can be found in the database, and it is here that the biggest challenge to which any corporation now located. One of the famous client/server architecture is the web where it requires the client to use browser to find any resources through Internet.

In addition, to maintain the performance of the server it requires a thorough monitoring and it is basically the job of the server administrator. According to Rose (2011), the function of monitoring the server is to check whether the website and server are in a good condition. A good monitoring application will always run a checking and send a warning to the admin if any problem should be found out. Therefore, with an immediate effect the admin could solve issue regarding the server.

In general, server could be monitored using traditional server monitoring system. However, specific information on the failures and errors may only be delivered to the administrator in monitoring room now. There is a room for further improvement with some kind of server monitoring system. Seen as a useful matter is a suitable method of informing person when the system failed instead of just generates a static message on the screen. If the system can notify the administrator directly rather than the operator may be necessary to wait for anything to occur, it will take a more pro-active in the way that it failed. However, a system which simply lost power may not communicate to such to inform anyone. Based on that situation, another tool is required to monitor or manage the system chosen for any problems. Action will be taken to inform service personnel or perhaps also take remedial action.

1.2 Problem Statement

The importance of the server availability has raised the dependence on technologies and computer jobs. In fact a small business can lose thousands of dollars of income per hour as their network service remains down. The increase within income lost giving the idea of monitoring system. Based on that reason, server monitoring system could make sure the network administrator personnel rapidly notified. That solution may accelerate to reduce the loss of income during the unforeseen time (Bertin, 2008).

Server performance is a key concern for the entire server administrator. Maintaining the server performance to optimum levels is a key challenge as the size of the network in the organization continuously grows. The duty of the server administrator is to assure that such issues related to server can be solved. Any alteration from the user is forbidden to retain reliability of the server (Masri, 2003). Sometimes, the server administrator does not have sufficient time to monitor entire server at one time, then the server monitoring system is beneficial to assure the server is always in good condition. Most important thing is notification of the server issues must be sent immediately due to any late notification may result in bigger problems on the server.

In an attempt to make sure smooth running of managing the server, the server administrator should select the appropriate and ideal method or mechanism of notifying the server problems as soon as possible. In addition, the server administrator must select the superb quality and good performance of server management system to handling the server availability. Server management system helps solving the problems or any alterations made and send instant notification to the administrator (DSG, 2000).

The importance of overcome this trouble is to make better server management. Increase in the awareness level of the server by using the Network Management System that the tool will set the system notifying to the administrator when there are any problems occurs. Urgent action may be taken to diagnose issue before the problem can result in the system disruption.

1.3 Goals & Objective

Generally, the goal of this project is to implement a Server Alert System. The objectives of the project are state as below:

i. To identify the specific requirements which are needed to develop a server monitoring system that can notify server issue to the server administrator.
ii. To design an application for a server monitoring system based on SMS alert architecture.
iii. To develop a system which able to send a notification of the server to administrator via SMS alert.

1.4 Project Scope

The scope of this project is that the system only functions as an alert system whereby if the server has a problem with the connectivity and service only. The proposed system can be used to notify the administrator. Then the administrator will take necessary steps to solve the problem. The system will use the GSM modem to send SMS to administrator. Only the person who used local service provider can receive alert notification. The system also will be implemented in a small networking environment and it will be installed inside the server that compatible with windows operating system.

The other scope of the project is; the system can only be run on Windows XP and above with. NET Framework has been included. Besides, the system will do a connection checking and port scanning to determine the current status of the server. The system will only monitor the web server which is only focusing on port 80 and other several ports. This system does not analyze the safety aspects of a computer such as a virus or worm. This system only monitors activity on the computer software. Control of hardware activity is ignored.

1.5 Methodology

There are a several steps should be performed in this study to build the project successfully. Figure 1.1 shows the steps to complete this project:

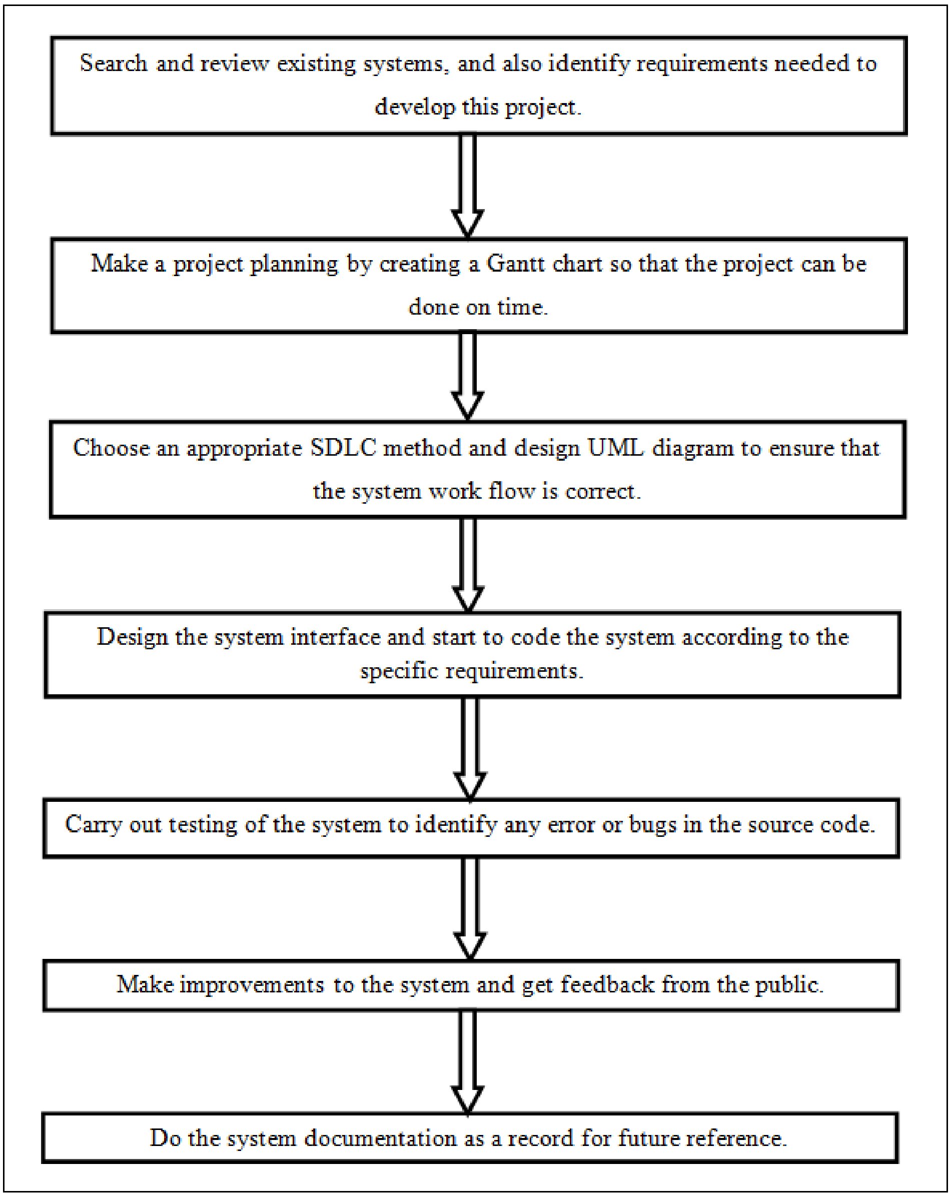

Search and review existing systems, and also identify requirements needed to develop this project.
Make a project planning by creating a Gantt chart so that the project can be done on time.
Choose an appropriate SDLC method and design UML diagram to ensure that the system work flow is correct.
Design the system interface and start to code the system according to the specific requirements.
Carry out testing of the system to identify any error or bugs in the source code.
Make improvements to the system and get feedback from the public.
Do the system documentation as a record for future reference.

Figure 1.1: Project development flow chart

1.6 Discussion

In fact, the server administrator is always responsible for making decisions about how to manage the server. Therefore, they have to make good decisions to select great quality performance in efforts to monitor the server for any existing issues associated to the server can be resolved. However, before developing new system for the server, depth study and research must be performed regarding the server and software. The system must also be tested for actual network environment whether it is ideal to use. That is what going to be done in the next chapter of literature review where a very detail of study and analysis regarding the system.

CHAPTER 2

LITERATURE REVIEW

2.1 Overview

The literature review is a study that has been done related to the equipment and other needs that are used during the development server monitoring system. Functions available in the project has been reviewed and clarified in each of its functionality. Purpose of this chapter is to explain about the selected project. Review consists of two parts which are existing system and method or technology used to develop this project. This chapter explain in detail regarding techniques or technologies which are suitable to be adapting into the project. This chapter mainly consist of five sections. The first section is regarding the system. In section 2.2 will be discussing about the existing system which related to this study. The existing system will be compared and analysed. The next section will be discussing about the server function. In this section, every detail will be explained regarding the server issue, monitoring, management, and notification. For section 2.4, the technologies used in this study are explained briefly which include the Email and SMS. In section 2.5 will be discussing about several internet protocol utilities which are very important in developing this study. Lastly, this chapter will explained about the software requirements used such as .Net Framework, Microsoft Visual Studio 2008, SQL Server and Microsoft Access.

2.2 System

The system is a combination of components or elements that are linked together to carry out a process. The system is seen as having a connection block components. System is an assemblage of interrelated parts that work together by way of missing driving process (Pidwirny, 2006). Systems are often visualized or modelled as component blocks that has connections drawn between prototypes. Most systems share the same features. Features include the following; the system has a defined structure of the process and its parts; the system provides a generalization in reality; systems tend to work the same way. This involves input and output material which then processed to cause a change in some way.

2.2.1 Existing System

The study of the existing system was conducted at Faculty of Computer System and Software Engineering, Universiti Malaysia Pahang, Gambang. In general, this monitoring and control performed on computers that are available in the local area network is done manually. Based on interview session made between Adsoft Technology Server Administrators, they will check whether each of the servers is in good condition or got damaged by any virus infection and so forth. Server administrators are difficult to monitor server activity without being in the server room. There are also situations where the administrator only knows that the server is problematic if there are complaints from users.

Use of local area network (LAN) has helped to control this management problem. By using the power of the wireless LAN, the ability to control server activity increased. Systems of monitoring and management of server has been widely used for server monitoring. However, most of the server management system designed to check the network connection between the computer, opening port and address for Internet connection (IP Address) found on the server.

Monitoring server is part of the server management tasks which is particularly important for organizations that involve dealing with the public or in a business transaction. With a good server monitoring, disruption of the services is minimized and thus increasing uptime. The implementation of server monitoring function is dependent on server roles (Hairuddin, 2005). For example, for a Web server gets a high or process input from thousands or perhaps millions of users a day, server bandwidth and logs are the important aspect that need to be monitored. Bandwidth monitoring is to monitor the traffic handled by the server through activities such as read and write access on the server. This is important because the Web server has a limit in operating bandwidth. When there is a prohibitively high bandwidth at certain times, it can cause the server performance slowing down.

Each network monitoring system ought to be able to monitor lots of servers and many services. There is several software that can be used to monitor server. Among the software that can be used are Zabbix, Nagios, and Ping Tester. Both the software is open source which means this software does not support Microsoft windows but only Ping Tester support by Windows. This study is based on the comparison made by MAMPU during the Malaysian Public Sector Open Source Software (OSS) Programme.

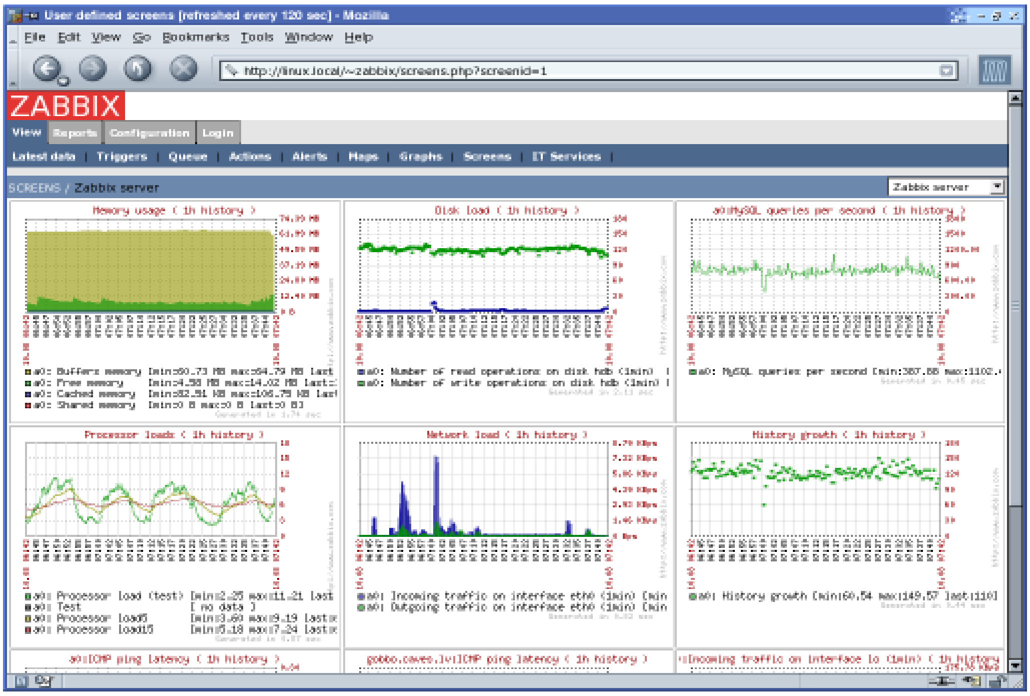
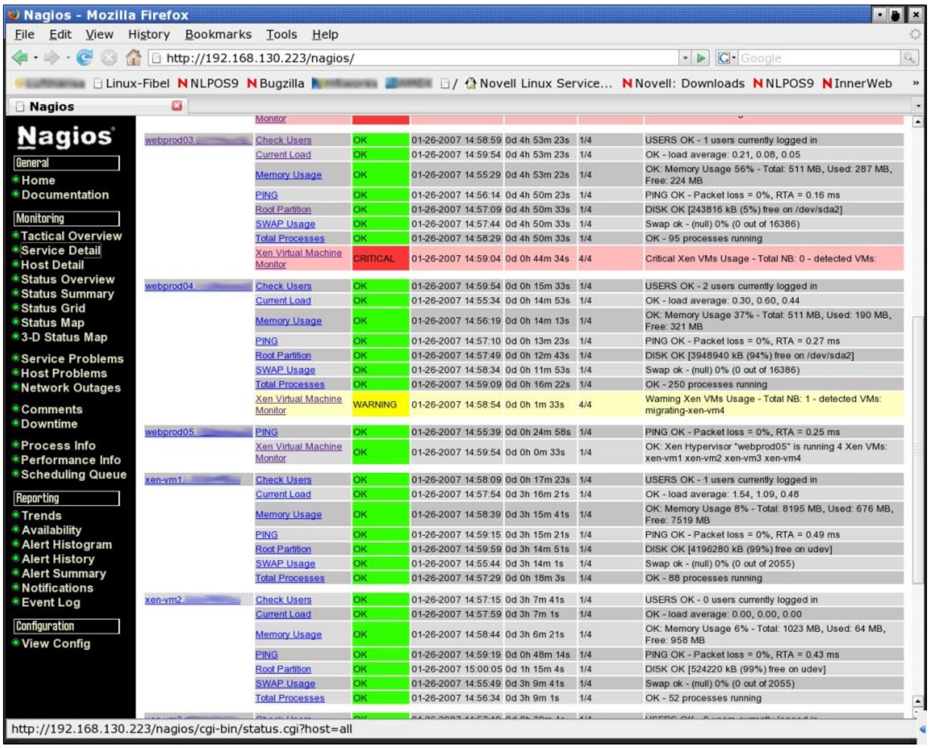

User defined screens [refreshed every 120 sec] - Mozilla
File Edit View Go Bookmarks Tools Window Help
http://linux.local/~zabbix/screens.php?screenid=1
ZABBIX
View
Reports
Configuration
Login
Latest data | Triggers | Queue | Actions | Alerts | Maps | Graphs | Screens | IT Services |
SCREENS / Zabbix server
Zabbix server
Memory usage (1h history)
Disk load (1h history)
a0:MySQL queries per second (1h history)
Processor loads (1h history)
Network load (1h history)
History growth (1h history)
a0:ICMP ping latency (1h history)
gobbo.caves.lv:ICMP ping latency (1h history)
:Incoming traffic on interface lo (1min) (1h history)

Figure 2.1: Zabbix



	Monitor					
webprod03.[redacted]	Check Users	OK	01-26-2007 14:58:59	0d 4h 53m 23s	1/4	USERS OK - 1 users currently logged in
	Current Load	OK	01-26-2007 14:59:54	0d 4h 53m 23s	1/4	OK - load average: 0.21, 0.08, 0.05
	Memory Usage	OK	01-26-2007 14:55:29	0d 4h 53m 23s	1/4	OK: Memory Usage 56% - Total: 511 MB, Used: 287 MB, Free: 224 MB
	PING	OK	01-26-2007 14:56:14	0d 4h 50m 23s	1/4	PING OK - Packet loss = 0%, RTA = 0.16 ms
	Root Partition	OK	01-26-2007 14:57:09	0d 4h 50m 33s	1/4	DISK OK [243816 kB (5%) free on /dev/sda2]
	SWAP Usage	OK	01-26-2007 14:57:44	0d 4h 50m 33s	1/4	Swap ok - (null) 0% (0 out of 16386)
	Total Processes	OK	01-26-2007 14:58:29	0d 4h 50m 33s	1/4	OK - 95 processes running
	Xen Virtual Machine Monitor	CRITICAL	01-26-2007 14:59:04	0d 0h 44m 34s	4/4	Critical Xen VMs Usage - Total NB: 0 - detected VMs:
webprod04.[redacted]	Check Users	OK	01-26-2007 14:59:54	0d 0h 15m 33s	1/4	USERS OK - 2 users currently logged in
	Current Load	OK	01-26-2007 14:55:34	0d 0h 14m 53s	1/4	OK - load average: 0.30, 0.60, 0.44
	Memory Usage	OK	01-26-2007 14:56:19	0d 0h 14m 13s	1/4	OK: Memory Usage 37% - Total: 511 MB, Used: 190 MB, Free: 321 MB
	PING	OK	01-26-2007 14:57:10	0d 0h 13m 23s	1/4	PING OK - Packet loss = 0%, RTA = 0.27 ms
	Root Partition	OK	01-26-2007 14:57:49	0d 0h 12m 43s	1/4	DISK OK [3948940 kB (94%) free on /dev/sda2]
	SWAP Usage	OK	01-26-2007 14:58:34	0d 0h 11m 53s	1/4	Swap ok - (null) 0% (0 out of 16386)
	Total Processes	OK	01-26-2007 14:59:09	0d 0h 16m 22s	1/4	OK - 250 processes running
	Xen Virtual Machine Monitor	WARNING	01-26-2007 14:58:54	0d 0h 1m 33s	4/4	Warning Xen VMs Usage - Total NB: 1 - detected VMs: migrating-xen-vm4
webprod05.[redacted]	PING	OK	01-26-2007 14:55:39	0d 0h 24m 58s	1/4	PING OK - Packet loss = 0%, RTA = 0.25 ms
	Xen Virtual Machine Monitor	OK	01-26-2007 14:59:54	0d 0h 0m 33s	1/4	OK: Xen Hypervisor "webprod05" is running 4 Xen VMs: xen-vm1 xen-vm2 xen-vm3 xen-vm4
xen-vm1.[redacted]	Check Users	OK	01-26-2007 14:58:09	0d 0h 17m 23s	1/4	USERS OK - 1 users currently logged in
	Current Load	OK	01-26-2007 14:57:54	0d 3h 16m 21s	1/4	OK - load average: 1.54, 1.09, 0.48
	Memory Usage	OK	01-26-2007 14:58:39	0d 3h 15m 41s	1/4	OK: Memory Usage 8% - Total: 8195 MB, Used: 676 MB, Free: 7519 MB
	PING	OK	01-26-2007 14:59:15	0d 3h 15m 21s	1/4	PING OK - Packet loss = 0%, RTA = 0.49 ms
	Root Partition	OK	01-26-2007 14:59:59	0d 3h 14m 51s	1/4	DISK OK [4196280 kB (99%) free on udev]
	SWAP Usage	OK	01-26-2007 14:55:44	0d 3h 14m 1s	1/4	Swap ok - (null) 0% (0 out of 2055)
	Total Processes	OK	01-26-2007 14:57:29	0d 0h 18m 3s	1/4	OK - 88 processes running
xen-vm2.[redacted]	Check Users	OK	01-26-2007 14:57:15	0d 3h 7m 41s	1/4	USERS OK - 0 users currently logged in
	Current Load	OK	01-26-2007 14:57:59	0d 3h 7m 1s	1/4	OK - load average: 0.00, 0.00, 0.00
	Memory Usage	OK	01-26-2007 14:58:44	0d 3h 6m 21s	1/4	OK: Memory Usage 6% - Total: 1023 MB, Used: 64 MB, Free: 958 MB
	PING	OK	01-26-2007 14:59:19	0d 0h 48m 14s	1/4	PING OK - Packet loss = 0%, RTA = 0.43 ms
	Root Partition	OK	01-26-2007 15:00:05	0d 1h 15m 4s	1/4	DISK OK [524220 kB (99%) free on udev]
	SWAP Usage	OK	01-26-2007 14:55:49	0d 3h 9m 41s	1/4	Swap ok - (null) 0% (0 out of 2055)
	Total Processes	OK	01-26-2007 14:56:34	0d 3h 9m 1s	1/4	OK - 52 processes running

Figure 2.2: Nagios

(a) Zabbix

Zabbix was created by Alexei Vladishev, and presently is actively developed and supported by Zabbix SIA. Zabbix is an enterprise-class open source distributed monitoring solution. Zabbix monitors varied parameters of a network and also the health and integrity of servers. Zabbix uses a versatile notification mechanism that enables users to piece e-mail based mostly alerts for nearly any event. This permits a quick reaction to server issues. Zabbix offers glorious news and knowledge image options supported the keep information. This makes Zabbix ideal for capability designing. Zabbix supports each polling and trappings.

All Zabbix reports and statistics, moreover as configuration parameters, are accessed through a web-based side that ensures that the standing of your network and also the health of your servers will be assessed from any location. Properly designed, Zabbix will play a vital role in monitoring IT infrastructure. This can be equally true for little organisations with a couple of servers and for big firms with multitudes of servers. Zabbix is freed from cost. Zabbix is written and distributed underneath the GPL General Public License version two. It means its coding is freely distributed and obtainable for the overall public.

(b) Nagios

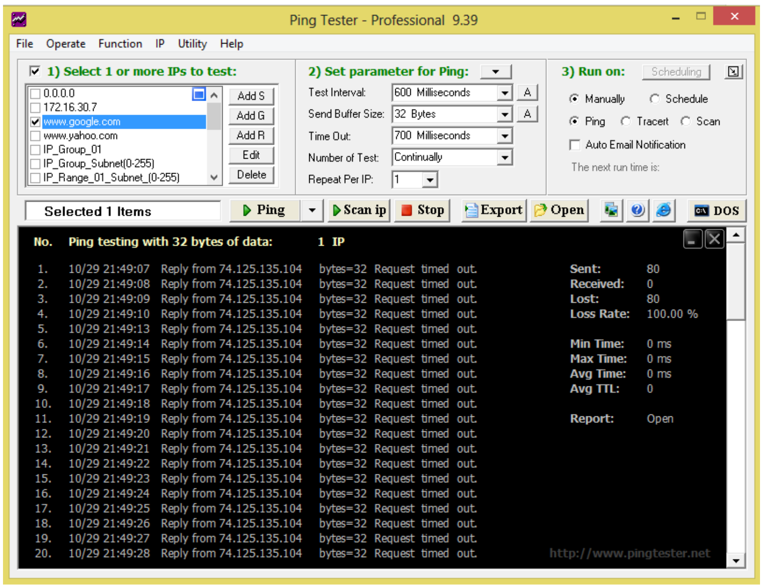
Nagios could be a free, open-source web-based network monitor developed by Ethan Galstad. Nagios is meant to run on UNIX operating system, however is even be used on UNIX variants. Nagios monitors the status of host systems and network services and notifies the user of issues. In common with several open source utilities, installation needs a degree of computer user expertise. Nagios is certainly not for the novice, unless people are ready to place the trouble in learning the fundamentals. However with a large vary of options, together with variety of internet interfaces, Nagios could be a terribly helpful, feature made monitoring tool. An oversized variety of plug-ins out there from the Nagios Library means that user will be able to design its capabilities to own necessities. Amongst others, Nagios monitors services like SMTP, POP3, HTTP, PING and resources like disk and memory usage, log files, processor load and then on and integrates with the Sensatronics IT Temperature Monitor to permit monitoring and alerting of server area and device temperature to own parameters.

Nagios will permit scheduling in order that as an example if user planned network outage user will suppress host and repair notifications. Nagios additionally permits users the flexibleness to develop custom host and service checks. All the plug-ins can be downloaded from the Nagios library. It’s additionally a potential to line up a hierarchy of alerts for example if alerts aren't skilful. The monitoring daemon runs intermittent checks on hosts and services user specify by using external plugins that return status data to Nagios. Once issues occur Nagios alerts user via email, instant message, SMS. Current status info, historical logs, and reports will all be accessed via an internet browser. Nagios runs on UNIX operating system and UNIX variants. Nagios doesn't support Microsoft Windows.

(c) Ping Tester

PingTesterPro comes together with all the basic functions that administrators need to monitor a given network. It is also easy to use and highly customizable. The generated reports provide users with a detailed and real-time state of the entire network, down to every machine. The almost $200 that need to be paid for the license might seem a little too much, especially if we take into consideration other applications that provide the same basic functionality. When pinging a certain IP address, there are other important parameters which are not even "mentioned" in PingTesterPro , such as offset, flag and packet checksum. Allowing users to customize them will certainly increase the application's usefulness.

PingTesterPro does a pretty good job when it comes to interrogating a certain network and includes more than the basic functionality needed by an administrator. While it lacks some more advanced functions that are needed to perform in-depth scans and analyses over a network environment, PingTesterPro comes with enough functionality under its hood to make a good job in the hands of a casual network administrator, even if the "pros" might dismiss it as incomplete and switch back to the dedicated tools that come with just any Linux distro.


Ping Tester - Professional 9.39
File Operate Function IP Utility Help
Add S
Add G
Add R
Edit
Delete
Scheduling
Ping
Scan ip
Stop
Export
Open
DOS
http://www.pingtester.net

☑ 1) Select 1 or more IPs to test:

- □ 0.0.0.0
- □ 172.16.30.7
- ☑ www.google.com
- □ www.yahoo.com
- □ IP_Group_01
- □ IP_Group_Subnet(0-255)
- □ IP_Range_01_Subnet_(0-255)

2) Set parameter for Ping:

Test Interval: 600 Milliseconds
Send Buffer Size: 32 Bytes
Time Out: 700 Milliseconds
Number of Test: Continually
Repeat Per IP: 1

3) Run on:

● Manually ○ Schedule
● Ping ○ Tracert ○ Scan
□ Auto Email Notification
The next run time is:

Selected 1 Items

```
No.   Ping testing with 32 bytes of data:        1  IP

1.    10/29 21:49:07  Reply from 74.125.135.104   bytes=32  Request  timed  out.        Sent:        80
2.    10/29 21:49:08  Reply from 74.125.135.104   bytes=32  Request  timed  out.        Received:    0
3.    10/29 21:49:09  Reply from 74.125.135.104   bytes=32  Request  timed  out.        Lost:        80
4.    10/29 21:49:10  Reply from 74.125.135.104   bytes=32  Request  timed  out.        Loss Rate:   100.00 %
5.    10/29 21:49:13  Reply from 74.125.135.104   bytes=32  Request  timed  out.
6.    10/29 21:49:14  Reply from 74.125.135.104   bytes=32  Request  timed  out.        Min Time:    0 ms
7.    10/29 21:49:15  Reply from 74.125.135.104   bytes=32  Request  timed  out.        Max Time:    0 ms
8.    10/29 21:49:16  Reply from 74.125.135.104   bytes=32  Request  timed  out.        Avg Time:    0 ms
9.    10/29 21:49:17  Reply from 74.125.135.104   bytes=32  Request  timed  out.        Avg TTL:     0
10.   10/29 21:49:18  Reply from 74.125.135.104   bytes=32  Request  timed  out.
11.   10/29 21:49:19  Reply from 74.125.135.104   bytes=32  Request  timed  out.        Report:      Open
12.   10/29 21:49:20  Reply from 74.125.135.104   bytes=32  Request  timed  out.
13.   10/29 21:49:21  Reply from 74.125.135.104   bytes=32  Request  timed  out.
14.   10/29 21:49:22  Reply from 74.125.135.104   bytes=32  Request  timed  out.
15.   10/29 21:49:23  Reply from 74.125.135.104   bytes=32  Request  timed  out.
16.   10/29 21:49:24  Reply from 74.125.135.104   bytes=32  Request  timed  out.
17.   10/29 21:49:25  Reply from 74.125.135.104   bytes=32  Request  timed  out.
18.   10/29 21:49:26  Reply from 74.125.135.104   bytes=32  Request  timed  out.
19.   10/29 21:49:27  Reply from 74.125.135.104   bytes=32  Request  timed  out.
20.   10/29 21:49:28  Reply from 74.125.135.104   bytes=32  Request  timed  out.
```

Figure 2.3: Ping Tester

2.2.2 Comparison

Table 2.1 shows the comparison between Nagios and Zabbix. The comparison of both systems is based on their configuration, scalability, reporting capability, and application interface.

Table 2.1: Comparison between Nagios and Zabbix

Software	Nagios	Zabbix
Developers	Ethan Galstad. Nagios	Zabbix SIA
OS	Unix / Linux	Cross-Platform
License	GNU General Public License	GNU General Public License
Data Store Configuration	• Saves configuration in flat files with a really straightforward format • permits to script the addition of latest service checks and create mass changes using varied scripting languages or basic shell script	• Use information to store configuration definitions, however doesn't encourage directly modifying it • Direct manipulation of the information doesn't seem to be a typical apply by Zabbix users • Having the configuration within the relational database might be used for ad-hoc reporting as well as updates
Scalability	• Has various data collection choices • The default technique doesn't scale well in any respect because it needs fork/exec's on the monitoring server for every check	• Works primarily via an agent that runs on every monitored host • user collects a huge set of data, that is then sent to the server on an everyday basis • Zabbix has the flexibility