Network Monitoring

Network Design and Computer Management

December 2012

Author: Adekunle Matthew, Hasan Khan, Neelam Abdullah
Supervisor: Olga Torstensson, Malin Bornhager
Examiner: Nicolina Mansson
Network Project
School of Information Science, Computer and Electrical Engineering
Halmstad University
Abstract

Managing a network is a very big functional area along with performance, device maintenance, security, performance, monitoring, troubleshooting, plan of change and etc. Among all of these monitoring plays a vital role. It can cover a wide area of network management. Monitoring is the only way to find out whether the network is functioning according to plan. In order to know what is happening in a network, how its functioning at any given time, a network should have a logging system. Now a day this logging activity is done by Network monitoring tool. It lets user know the status of the network at any given time. This logging can give the user a wide view what can't be seen in general. For example the statistics of a week or month, even a year. Monitoring is a very important issue in an organization network which arose over the time.

In this project we are going to implement some well known network monitoring tools in a real world scenario and we will investigate how this monitoring tool can help network administrators to monitor a network. Moreover, what kind of information we can extract from a network by these tools.

The purpose of this project is to get an overall idea about the importance of network monitoring and what are the facts need to be considered while monitoring a network. There are lots of pros and cons in monitoring a network. So choosing the appropriate tool for monitoring is very important. Monitoring a network with the least effects on network performance is the best solution in case of monitoring.

The outcome from these monitoring tools is a wide range of useful data and integration of these data produces the status of the network at any give time. Moreover these data will be logged to create a statistical report. Different users such as a network admin and organization can use this information from different perspectives to make a network more efficient for users.
Abstract ........................................................................................................................................ II
1.0 Introduction ...................................................................................................................................... 1
2.0 Background ......................................................................................................................................... 2
  2.1 Project Scope ........................................................................................................................................ 2
  2.2 Project aim and goals ............................................................................................................................... 2
  2.3 Importance of monitoring for a company like “BIM Logiciel” .............................................................. 3
  2.4 What can “BIM Logiciel” monitor in their network? .............................................................................. 3
  2.5 Methodology ........................................................................................................................................... 3
  2.6 Social and ethnic issue ............................................................................................................................. 4
3.0 Basic Monitoring Tools ....................................................................................................................... 5
  3.1 PING ....................................................................................................................................................... 5
    3.1.1 When and why to use a ping test in Network monitoring ................................................................. 5
    3.1.2 Ping Response ..................................................................................................................................... 5
  3.2 SNMP .................................................................................................................................................... 5
    3.2.1 SNMP managed network components ............................................................................................. 6
    3.2.2 Protocol’s Communication ................................................................................................................. 6
    3.2.3 Different types of SNMP ................................................................................................................. 7
    3.2.4 Disadvantages of SNMP ................................................................................................................. 8
  3.3 SYSLOG ................................................................................................................................................. 8
4.0 Monitoring Softwares ......................................................................................................................... 10
  4.1 Monit ................................................................................................................................................... 10
    4.1.1 Features of Monit ............................................................................................................................... 10
    4.1.2 Overview .......................................................................................................................................... 10
  4.2 ZENOSS .............................................................................................................................................. 11
    4.2.1 How Zenoss work .............................................................................................................................. 12
    4.2.2 Zenoss Monitoring Solution ........................................................................................................... 12
    4.2.3 Zenoss Core is built on three layers which enable us to troubleshoot ............................................ 14
    4.3.4 How does Zenoss Core handle the Events and the activities? ...................................................... 15
  4.3 PRTG ................................................................................................................................................... 16
    4.3.1 Features of PRTG ............................................................................................................................ 16
5.0 Comparison ......................................................................................................................................... 20
6.0 Implementation ..................................................................................................................................... 22
7.0 Result .................................................................................................................................................. 25
8.0 Further enhancements ......................................................................................................................... 29
9.0 Conclusion ......................................................................................................................................... 30
10.0 References: ....................................................................................................................................... 31
Figures List

Figure 1: How SNMP works: Page: 7
Figure 2: Severity values: Page: 8
Figure 3: Monit Overview: Page: 11
Figure 4: monitoring activities with Zenoss Core: Page: 13
Figure 5: Architecture of Zenoss Core: Page: 14
Figure 6: Zenoss Core three layers: Page: 14
Figure 7: Severity Level of Zenoss: Page: 15
Figure 8: Status of Zenoss: Page: 15
Figure 9: PRTG monitoring a HP switch: Page: 18
Figure 10: PRTG monitoring bandwidth: Page: 19
Figure 11: Comparison: Page: 20
Figure 12: Configuring PRTG with auto feature: Page: 21
Figure 13: Adding customized sensor to the devices: Page: 23
Figure 14: Setting up a report: Page: 24
Figure 15: FTP server status: Page: 25
Figure 16: Status of E-mail server and VoIP server: Page: 26
Figure 17: Status of internet connection: Page: 26
Figure 18: Monitoring Facebook website: Page: 27
Figure 19: Monitoring Cloud, Printer and Printer: Page: 27
Figure 20: alarms issue of PRTG: Page: 28
Figure 21: Overview of whole network in a glance: Page: 28
### Abbreviations List

<table>
<thead>
<tr>
<th>Abbreviations</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Central Processing Unit.</td>
</tr>
<tr>
<td>GUI</td>
<td>Graphical User Interface</td>
</tr>
<tr>
<td>CLI</td>
<td>Command Line Interface</td>
</tr>
<tr>
<td>PING</td>
<td>Packet internet GroperPing</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>SIP</td>
<td>Session Initiation Protocol,</td>
</tr>
<tr>
<td>RDP</td>
<td>Remote Desktop Protocol</td>
</tr>
<tr>
<td>VoIP</td>
<td>Voice over Internet Protocol</td>
</tr>
<tr>
<td>MTBF</td>
<td>Mean time between failure</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SYSLOG</td>
<td>System logging</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>RFC</td>
<td>Request For Comments</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>OSI</td>
<td>Open Systems Interconnection</td>
</tr>
<tr>
<td>NMS</td>
<td>Network-Management Systems</td>
</tr>
<tr>
<td>SNMPv1</td>
<td>Simple Network Management Protocol version 1</td>
</tr>
<tr>
<td>UNIX</td>
<td>UNiplexed Information and Computing System.</td>
</tr>
<tr>
<td>HTTPs</td>
<td>Hyper Text Transfer Protocol secure</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>MD5</td>
<td>Message Digest 5</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hashing Algorithm</td>
</tr>
<tr>
<td>SSHD</td>
<td>Secure Shell Daemon</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hyper Text Transfer Protocol</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>CMDB</td>
<td>Configuration Management Data Base</td>
</tr>
<tr>
<td>ICMP</td>
<td>Internet Control Message Protocol</td>
</tr>
<tr>
<td>WMI</td>
<td>Windows Management Instrumentation</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>SQL</td>
<td>Structured Query Language</td>
</tr>
<tr>
<td>DOS</td>
<td>Disk Operating System</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>QOS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>WAN</td>
<td>Wireless Local Area Network</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>IPv4</td>
<td>Internet Protocol, version 4</td>
</tr>
<tr>
<td>IPv6</td>
<td>Internet Protocol, version 6</td>
</tr>
<tr>
<td>DMZ</td>
<td>Demilitarized zone</td>
</tr>
<tr>
<td>PDF</td>
<td>Portable Document Format</td>
</tr>
<tr>
<td>HTML</td>
<td>Hyper Text Markup Language</td>
</tr>
<tr>
<td>XML</td>
<td>Extensible Markup Language</td>
</tr>
<tr>
<td>CSV</td>
<td>Comma-Separated Value</td>
</tr>
<tr>
<td>MBPS</td>
<td>Megabits Per Seconds</td>
</tr>
</tbody>
</table>
1.0 Introduction

Monitoring a successfully fully functional network are the most important elements of a network nowadays. Network monitoring is referring to a system which continuously monitors a network. “A network monitoring system is capable of detecting and reporting failures of devices or connections. It normally measures the processor (CPU) utilization of hosts, the network bandwidth utilization of links, and other aspects of operation” [1]. In general, this monitoring task is performed by using third party software which is GUI based and easy to understand. But there is also some in built services in network hardware to perform this task which is CLI based such as PING. For example to determine the status of a DHCP server, monitoring software may send ping periodically, a text message could be sent to the company’s e-mail server to check whether e-mail server is up and working functionally. Commonly measured metrics are availability, response time, latency, jitter, packet loss.

In this Report, we are going to discuss about what advantages we can have from network monitoring, what areas are vital to monitor in a network, how we can do it and we going to implement monitoring tool in our proposed company “BIM Logiciel” to see how a fully functional network can be monitored.
2.0 Background

"BIM Logiciel" is a medium size software company in Halmstad. Around 50 employees work in this company. These users are divided into three groups such as sales, admin, tele-worker. The company has four servers such as email server, FTP server, SIP server, and Radius servers. The company has their own VoIP setup inside the company. There are all together 2 routers, 4 switches, and two wireless access points by which users are connected to the network. So it’s a medium size company along with these resources and they want to monitor their network.

2.1 Project Scope

Project scope of this project is to find out a monitoring solution for “BIM Logiciel” to monitor their network and how they can be benefited by monitoring their network.

“BIM Logiciel” is a small software development company in Halmstad. They have around 50 regular employees in their company. These users are continuing to use the company network for their job. The company has two internet connections from ISP in order to provide smooth speed to their user. Such as one connection from TELIA for users, who is downloading and browsing the internet. Another connection from TELENOR which provide the external users' service of web server, e-mail server.

“BIM Logiciel” doesn’t have any monitoring tools at this moment. For example few days before there was an incident of one hour network downtime. The company hired an external company to fix the problem but they couldn’t help much instantly as there was no proper monitoring system. So it was time consuming to fix the problem which cost “BIM Logiciel” a lot. To solve this issue company decided to implement a network monitoring system in their company.

2.2 Project aim and goals

The main objective of this project is to provide a complete monitoring system to “BIM Logiciel”. In order to do so certain goals needed to be met, such as:

- Find a cost effective monitoring solution.
- Should have good user interface.
- Implement a monitoring system.
2.3 Importance of monitoring

“Understanding the composition and complexity of your network, and having the capacity to be informed of how all the individual elements are performing at any given time, is a key success factor in maintaining the performance and integrity of the network – and often about the business – as a whole” [2]. Network admin feel very comfortable and confident when they know exactly what’s going on in their network at any given time and moreover in case of changing responsibilities new admin knows what has been happening for last certain period because of reports and documentation. For example teleworker can’t access to FTP server to upload field data, and for that reason developer in house can’t have raw data to work with, which means loss of productivity and missing deadlines. On the other hand if customers can’t reach the company by their e-mail, that means loss of potential customers. At the end loss of business. So it’s not only a simple network we talking here to reach to the internet. It’s very crucial in perspective of business. So in order to ensure all these devices working smoothly “BIM Logiciel” need to mount a network monitoring system in their company.

2.4 What can be monitored?

It is important for a company to know their network. That refers to each network device current status, such as disk space, availability of devices, and critical services, etc. Each existing running device in a network represents a risk of failure. Every device has an MTBF (Mean time between failure). But no one can guarantee when the device will fail. Monitoring tools can monitor which device is constantly failing or making trouble more often. It means, it’s time to change. So monitoring will help us to plan for changes or upgrades. The company has a great security solution. By monitoring this solution they want to make sure that security devices are functional. BIM Logiciel has several servers to internal and external users. All of a sudden there is a complain raise up that one of the server is down. Only by monitoring we can say whether it is actually an issue of server or users. Monitoring devices can log a report periodically and very user friendly such as with graph and chart. It is very important to have these reports to know the health and activity of a network. BIM Logiciel want to monitor some of the websites such as Facebook, twitter, mega upload, etc.

There are several basic tools can be used in order to monitor a network. Most of these resources are inbuilt and open source standard or proprietary, such as Ping, SYSLOG, SNMP, Netflow, Jflow, and Hflow. In this section some open source tools in monitoring will be described briefly.

2.5 Methodology

At the very beginning of this project very basic tools of network monitoring will be described. For example PING, SNMP, SYSLOG etc. These are the tools which are predefined in most of the system and open source. By these tools users can monitor a network. But skill and expertise in this area is important in order to do so as most
of the tools are command based without any graphical interface. After that an extensive research will be done on existing popular feasible monitoring software which will be able to fulfill BIM Logiciel requirements. A comparison will be done to choose the best among these tools. Finally the monitoring software will be implemented and results will be tested in order to check the usability and functionality of the software.

2.6 Social and ethnic issue

BIM logiciel is a small company in Halmstad, Sweden. They are trying to implement a monitoring tool in their company. Before starting, social aspect of the project need to consider. What kind of effect it will do on user and customer.

According to the rules employees should not use the company network for their personal use. It should solely use for the organization’s purpose. Communications with client can be monitored for quality assurance.

BIM Logiciel is going to monitor their network and their data. They are eligible to do so for the company’s well being. The user uses the network to check their Facebook or other social network where their personal info will be reviled by monitoring. Users aware of the issue as that is against company policy.

Moreover at this moment BIM Logiciel is monitoring the network devices, not everything such as emails, files, images etc. So this monitoring is not going to explore much in terms or privacy.

So in summary there will be some social issue raised by monitoring a network, but within a very limited area which can be considered for well being of the organization.
Network Monitor

3.0 Basic Monitoring Tools

3.1 Ping

The word Ping means "packet internet GroperPing". Ping is a basic Internet program that allows a user to verify that a particular IP address exists and can accept requests. Ping is used diagnostically to ensure that a host computer the user is trying to reach is actually operating. Ping works by sending an Internet Control Message Protocol (ICMP) Echo Request to a specified interface on the network and waiting for a reply. Ping can be used for troubleshooting to test connectivity and determine response time. Ping command is very useful in debugging and testing network and internet connection [3].

3.1.1 When and why use Ping

The user can verify connectivity between the devices by pinging the unique IP of the devices. This way the user can verify the connectivity to the internet and moreover, user can ping specific port in order to check some services of the devices. By using ping command user can determine how long it takes to send a packet to the destination device.

3.1.2 Ping Response

Every time the user ping a device user get a response back and it is very important to check the reply. Each response will help and guide the user to find the right troubleshooting path and it will be easy to find the exact device which is having problems and troubleshoot that device. Some common response that user can get from ping described below.

- **Reply From**: by getting this response from the address that the user has pinged it means the connection is working.
- **Request Timed out**: when the destination host down then pings will fail and the user will get this reply because that host doesn’t reply.
- **Unknown Host**: getting this reply means the user’s computer cannot recognize this address. Usually the IP address of the destination host is wrong or the host name.
- **Destination Host unreachable**: The destination that user is trying to ping is down or some ports may be down.
- **Hardware Error**: this means that user’s network adapter is shut down or the cables are unplugged.

3.2 SNMP

The Simple Network Management Protocol (SNMP) is a standard internet protocol, for maintaining devices and proactively let you know what’s going on your IP
Network Monitor

Network Monitor is often used in network management system for situations that warrant the attention of the administration. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol, hence is an Application Layer protocol, the Layer 7 of the OSI model.

It uses one or more administrative Computers, called managers. It has the feature of monitoring or managing a group of devices on a Computer Network, however there is a software component called an Agent installed on the managing system which reports information via SNMP to the manager, thus SNMP works using management Console and SNMP Agent.

One of the reasons why it is a very good protocol is that you can get full information about what is happening on your devices, at the exact time. It can see what’s going on with the hardware of the computer, take for instance in an organization with over 200 servers, and you as an administration want to keep track on them to make sure that they running fine however, before they can be up and running fine, all the advices should be in good working conditions. The fans, memory, and more SNMP help to keep track of all this and ensure to send information to the management console in case of any failure.

SNMP Agent exposes management data in the form of variable on the managed systems, you also can perform additional task, like modifying and applying new setting or configuration through the remote modification of these variables.

3.2.1 SNMP managed network components

Managed Device : this is a network node that contains an SNMP agent on a managed network. Management devices include Router, Switch it store the information collected and make it available on Network-Management Systems (NMS).

Agent: This is a software that is installed on a device that is being managed by SNMP.

Network Management System: This is software is installed on Manager

3.2.2 Protocol’s Communication

The agent uses UDP port 161 to receive a request from the manager, and the manager sends a request from any available source port to 161 which is the agent, however the agent response back to manager’s course port. The manager receives a notification (trap) on port 162. SNMP Agent is a software that able to read information from device and send this information to the Management console. The trap is an asynchronous notification from the agent to the manager it includes current system-up-time.
3.2.3 Different types of SNMP

SNMP v1, SNMP v2 and SNMP v3 versions 1 and 2 have some features in common, but SNMPv2 enhances the feature of SNMP v1, such as additional protocol operations. SNMP version 3 (SNMPv3) also enhances the feature of SNMP v1 and v2 by adding security and remote configuration feature to the previous versions.

- **SNMP v1** is the first implementation of the SNMP protocol. It operates over protocol such as UPD and IP SNMPv1 is widely used. SNMP is a request/response protocol. It uses get, GetNext, Set and Trap to accomplish this. The main drawback about Version 1 was the security issue. There is no authentication for protecting the message source from disclosure and placing access controls on the Logiciel database Management Interface Base.

- **SNMP v2** was designed to enhance the performance of Version 1, however the Get, GetNext, and set operation used in version is the same with those in version 2. Moreover Version 2 defines new feature GetBulk and inform. GetBulk enable the NMS to efficiently get or retrieve large blocks of Data. The basic idea was to address the security issue but with other features added to Version the security issue was not addressed.

- **SNMP v3**, it has the same feature as v1 and v2, but add additional feature which addressed the security issue that was lacking in v1 and v2. It adds security and remote configuration to v1 and v2, so many other features are added, like to dynamically configure the SNMP agent.

SNMP communicates in the following way, please see figure 1.

---

Figure 1: How SNMP works.
3.2.4 Disadvantages of SNMP

- The first SNMP revision’s simplistic management information model did not support a modern network’s detailed information requirements, but it was updated in SNMP 2c and SNMP 3 [4].
- The information is spread on the networking to many nodes.
- The information maintained is not till date.
- The SNMP lacks cohesion with other management paradigms.
- New security extensions in SNMP 3 may place an additional processing burden upon to manage objects [4].

3.3 SYSLOG

SYSLOG is a standard for system logging. In short we can say anything we configure to log from a system will be forwarded and will store like a typical log book. SYSLOG use UDP port 514 for communication between SYSLOG servers and clients. As its UDP we know that it doesn’t do reliable communication. SYSLOG packet contains information about the facility, Severity, Hostname, Timestamp, and Message. SYSLOG messages are categorized widely basis of the source generate them. For example it could be a router, switch, an operating system, process etc. These categories are called by the Facility. According to RFC there are eight standard severity levels which are shown in figure 2 below.

<table>
<thead>
<tr>
<th>Integer</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Emergency: System is unusable.</td>
</tr>
<tr>
<td>1</td>
<td>Alert: Action must be taken.</td>
</tr>
<tr>
<td>2</td>
<td>Critical: Critical conditions.</td>
</tr>
<tr>
<td>3</td>
<td>Error: Error conditions.</td>
</tr>
<tr>
<td>4</td>
<td>Warning: Warning conditions.</td>
</tr>
<tr>
<td>5</td>
<td>Notice: Normal but significant condition.</td>
</tr>
<tr>
<td>6</td>
<td>Informational: Information message.</td>
</tr>
<tr>
<td>7</td>
<td>Debug: Debugging message.</td>
</tr>
</tbody>
</table>

Figure 2: Severity values.
Network Monitor

Let see how SYSLOG works and it can help us in monitoring. SYSLOG has three components by which it performs logging. There are three SYSLOG components described below.

- Log device: devices which create log messages such as router, firewall, server or any device which can create an event message for SYSLOG.
- Log collector: These components collect SYSLOG data. SYSLOG server would be a typical log collector in this case.
- Log relay: sometime message need to forward through a log collector. These component forward messages which they receive from log devices.

Typical applications and OS are created in such a way that they are capable to give clues of their condition or any change of state. These clues help us to understand what is the application is doing? Individual applications and OS deliver message differently but SYSLOG is one of such application which is capable of accepting messages from different vendors at the same time.

Logging is a very important tool for network admin to identify unusual activity in the network. This can be used for debugging any problems also.

SYSLOG can be used as intrusion detection system. If any system is compromised, intruder tries to cover the footprint but with SYSLOG its really hard because it gives real time logging. So network admin actually can find out instantly or later how intruder compromised the system.

If any system is compromised, a proper investigation will be started in order to determine of severity and compromise. At that time SYSLOG played a great role in creating a picture of the system of that time.

Let say we monitoring one of the routers. What kind of info we can get by SYSLOG. Nay port failure will be logged. So we can instantly fix the problem by watching log message. Some time we need to see who logged remotely in our system. We can get that info also form SYSLOG.

SYSLOG provides us info of different severity level which helps us to understand how the system is healthy and what steps we need to take based on that severity level.
4.0 Monitoring Softwares

In this section there will be an extensive research on existing popular monitoring software. We can compare the most three popular software and justify whether they meeting the requirements of the company.

4.1 Monit

Monit is a utility for managing and monitoring processes, files, directories and devices on a Unix system. It is a daemon that wakes up every once in a while, goes through a list of things it is configured to check, and if something is not as it should be, takes a corrective action. Monit is a utility for controlling PC it can automatically maintain and repair the problems in the computer with executing meaningful actions in error situations. Monit is basically designed to monitor a daemon process or some other program running on the local host [5].

4.1.1 Features of Monit

Monit is free easy to use it has a human-readable configuration language, has good documentation and is a very lightweight monitoring package it can control and configure all the processes in a very easy and technical way it goes through all the problem and take steps to correct the problems. It can check PC usage and inform the user if a virus is deducted. E.g. It can stop those processes which are using too many resources.

Monit services in active, passive and manual mode. It can enable or disable service monitoring. It can also start, stop or restart processes. It Verify MD5 or SHA1 checksum of files, either on the local system or on a remote system it can do the connection test on the protocol level. It can test network connections to various servers such as TCP and UDP. Has built-in automatic tests for the main internet protocols. Its primary tasks are watching the processing for memory leaks, endless loops and all the other error it can be used to monitor other services and system parameters.

4.1.2 Overview

In the following figure 3 we can see how Monit Server is controlling all the files, directories device, remote host and all the processes if it finds any error, Monit solve the problem automatically and then inform user by sending an alert message via e-mail. We can access monit from a web browser it can provide us HTTPS interface can easily use a browser to to reach the monit server. The behavior of Monit is controlled by command-line option and a run control file monitor the default location for this file is ~/.monitrc. Through the console if monit find an error then it will print an error message to console, including the line number in the file from where error was found. Please see figure 3 below for monit overview.
Zenoss (Zenoss Core) is an open-source application, server, and network management platform based on the Zope (Community project Concerned with free an open-source server.) application server. Released under the GNU General Public License (GPL) version 2, Zenoss Core provides a web interface that allows system administrators to monitor availability, inventory/configuration, performance, and events [6].
4.2.1 How Zenoss work

To monitor your resources on a network, is by installing Zenoss Core to a server using virtual appliance like VMware on Windows, since Zenoss Core is to be installed on Linux Server. Hence is designed mostly for Linux, thanks for virtual appliance. Once you finish the installation on virtual appliances, it will ask you to logging which the default login is root and the password is root, then you will have a link to an IP address and port number similar to (http://198.162.17.285:8080) which will prompt you to choose a password for admin and redirect you to the management console immediately then is getting ready to go. From the management console you can configure it to what you need it to monitor.

The web Portal is friendly user interface, it enables drag and drop and it doesn’t require any operating system training before you can use it which make it easy and simple for users.

Zenoss is simple monitoring solution, easy to install, turn it on and start monitoring with friendly GUI; it can be complex as you need it to be.

4.2.2 Zenoss Monitoring Solution

Zenoss monitoring solution includes the following services:

**Device Management Capabilities:** it uses a configuration Management database, to store the events or activities on a network in an IT environment. You can manually add any devices to CMDB, or it can discover any active device on a network automatically using the routing table hence these devices can be manipulated remotely by Telnet or SSH for secure Modeling.

One of the coolest things about Zenoss Core is that you can configure the devices by user defined, location, also it has this powerful feature. Which allow us to define monitoring characteristics base one the hierarchical classification of the device.

**Availability Monitoring and Performance graphs:** using various protocols like ICMP and SNMP monitoring, are aware of the Layer 3 topology, hence it reports how available is the Network Devices, TCP/IP Services and Ports, URL, Windows Services and Processes, Linux/Unix Process.

The performance monitor collect the time series and provide the analysis of the following components for effective monitoring. File System Statistics. CPU and Memory Usage, negios and Cacti Plugin Support. Figure 4 below shows monitoring activities with Zenoss Core.
Fig 4: Monitoring activities with Zenoss Core [6].

**Events, User and Alert Management**: it monitors various sources and keep track of the signs of any trouble, it keeps track on the syslog's, window events and more. The event management system includes: custom Events (allow us to customize which event to monitor and when to monitor it), automatic event prioritization (it automatically assigns which event is most critical) and Event Correlation. Another Coolest thing is that, you can configure Zenoss Core to send e-mail or pager alerts, to run any script or just to log the events. It depends on how we configure it; it really gives us flexibility for configuration and you can decide who can view or who is to receive the alert.

**Monitoring Reports**: It generates a detailed report which allows us to view what is happening right now and the activities on our network, which is the most important way we want to monitor our network.

Sometimes we are not really interested in the full report, not everyone should really know what is happening in the network or sometimes we need some additional report which is not included in the generated report, Zenoss is so cool that you can customize Device Report, it allows user to customize device reports from the web interface.

Sometimes, there could be a problem which we need to troubleshoot the System architecture is so simple and cool, which provide us a detailed understanding of
how Zenoss Core is built and can easily be troubleshooting. Fig 5 below shows the Architecture of Zenoss Core.

4.2.3 Zenoss architecture

**User Layer:** It is friendly user Interface, very flexible for the user to be able to work remotely or from command line. The user later enable you to Navigate around and organize how a network device are to be monitored. It also allows us to give administrative privileges to the user from the settings option.

**Data and Collection:** the collection later grabs all the events and data, which then store in the database. Please see Fig 6 below for the data collection.

Fig 6: Zenoss Core layers
4.2.4 How Zenoss handle the Events and the activities?

Events are stored in the database, and from the database it sends an alert such as e-mail or pager anytime a threshold is crossed.

Events Severities and Event Status: The figure 7 and figure 8 below is a table illustrate the available severities and the statues in Zenoss Core.

<table>
<thead>
<tr>
<th>Event Severity</th>
<th>Integer Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear</td>
<td>0</td>
<td>Correlates with previous down event and moves the event in history. Represented by green icon.</td>
</tr>
<tr>
<td>Debug</td>
<td>1</td>
<td>Used for troubleshooting. Does not indicate a problem Represented by gray Icon.</td>
</tr>
<tr>
<td>Info</td>
<td>2</td>
<td>Used for Mark event in the system for informational Purposes. Represented by a blue icon.</td>
</tr>
<tr>
<td>Warning</td>
<td>3</td>
<td>Indicates a potential problem. Represented by yellow icon.</td>
</tr>
<tr>
<td>Error</td>
<td>4</td>
<td>The device or component is unavailable or is operating at the dangerous performance levels. Represented by an orange icon.</td>
</tr>
<tr>
<td>Critical</td>
<td>5</td>
<td>The device or Component is down. Represented by a red icon.</td>
</tr>
</tbody>
</table>

Fig 7: Severity Level of Zenoss [7].

<table>
<thead>
<tr>
<th>Event Status</th>
<th>Integer Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suppressed</td>
<td>2</td>
<td>An event occurred, but it was sent directly to history.</td>
</tr>
<tr>
<td>Acknowledged</td>
<td>1</td>
<td>The event is still active and is being worked on by an admin</td>
</tr>
<tr>
<td>Unacknowledged</td>
<td>0</td>
<td>Represent a new event that has not been acknowledged and is presumably not being worked on.</td>
</tr>
</tbody>
</table>

Fig 8: Status of Zenoss [7].
4.3 PRTG

PRTG is a very popular network monitoring tool in the market. It has a freeware version of limited capability along with its enterprise level. It’s very user friendly and it can support any size of network. PRTG can help to critical system downtime by providing early notification of outages, so admin doesn’t have to wait for users to complain or outages.

This tool monitors of systems availability by using several methods such as ping, SNMP and protocols like WMI in order to specific tasks such as DNS, HTTP. PRTG comes with more than 130 types of pre-installed sensors for centralized, multi-system monitoring. Moreover there are custom made specific sensor can be modified in order to monitor specific system and service availability such as SQL and exchange. PRTG has bandwidth monitoring sensors which can ensure some of the traffic has a certain amount of bandwidth and it can ensure also that no DOS or overload activities is not available in our network. PRTG is one of the leading monitoring tools which is available on IPv6 network.

4.3.1 Features of PRTG

These features of the PRTG tool which makes this tool different and stronger than others.

- PRTG is very easy to use. It comes up with five different user interfaces. User can choose according to their device. For example in general it has HTTP and SSL base application which we can access from any PC. Then again it has apps if user chooses to use from iPad or notepad.

- PRTG provides comprehensive monitoring by following services.
  
  - More than 130 types of pre-configured sensor are covering all the aspects of monitoring a network.
  - Monitoring applications, services, QOS, SLA, LAN, WAN, VPN.
  - Supporting both ipv4 and ipv6 network.
  - Monitoring bandwidth.
  - Monitoring network uptime and downtime.

- PRTG gives us alert in a very flexible way. It’s got 9 different notification technologies such as e-mails, SMS and SNMP trap etc. To give status alerts such as up, down and warning. An alert can be configured on multiple vector such as if X and Y both down alerts should be issued.

- PRTG allows distributed monitoring which allows headquarter to monitor all remote sites in different locations. This tool allows monitoring even separated networks within a company such as DMZ and LAN.
Network Monitor

- PRTG is multilingual, so it comes in several international languages. User can switch into different languages even after installation.

- This tool provides in-depth reporting. We can get reports in HTML or PDF format. It can be configured to generate an automatic report periodically. Moreover monitoring data can be exported any given time in HTML, XML, CSV.

It's better if we get some sample output of PRTG. So we can see how it works in real life.

In figure 9 we can see how PRTG monitors a normal network device in detail. Here the monitored device is an HP switch. From this figure we can see that we can get information about CPU load, free memory, IP address and many other critical information. Moreover it shows the priority of that information. So we can modify it if we need it. On the left hand side it shows the graphical view of a certain period. On top there is a "to do" list, warnings, alerts and service is paused now. Please see Fig 9 Below
Figure 9: PRTG monitors an HP switch[8].

In figure 10 below show how PRTG monitoring bandwidth of a network. Let say a company got 100mbps network speed connection. By monitoring that we can see that how a company using the network over the time of the day. In this figure we can see that company using up to 93mbps in peak hour and down to 3mbps in the morning time. We can plan any kind of changes of network by this information.
Figure 10: PRTG monitoring bandwidth [8].
5.0 Comparison

At this stage information will be gathered about these tools which are preliminary chosen. We will see the strength and weakness of these tools. Moreover we need to find out which one of these tools will fulfill the requirement of our company.

Previous section we have worked with three tools Monit, PRTG and Zenoss. We showed their features, what are the area they covering and what are the benefits we getting from them. Preliminarily that’s the difference they have for each other but we can dig a bit further in this section and gather the difference in a table so that we can take a decision easily by looking at that. Figure 11 below shows the comparison.

<table>
<thead>
<tr>
<th>Name</th>
<th>IP SLA Reports</th>
<th>SNMP</th>
<th>SYSLOG</th>
<th>Access control</th>
<th>License</th>
<th>Auto discovery</th>
<th>Operating system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zenoss</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Commercial</td>
<td>Y</td>
<td>Linux and windows</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Demo for certain period</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PRTG</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Commercial</td>
<td>Y</td>
<td>Linux and windows</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Demo forever for 10 nodes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Monit  | Y              | Y    | Y      | N              | Free               | N              | Linux            

Fig 11. Comparing the three monitoring tools (Monit, Zenoss and PRTG)

This comparison of tools is based on user requirements. Monit is running only on Linux. But user requirement is that the tool should be platform independent. Moreover it doesn’t provide full access on devices and not user friendly. These are the reason for not choosing Monit.

Zenoss and PRTG have great flexibility and platform independent. They are easy to use and give full control of a network. Moreover, both of these products can discover a network automatically within a time period. So users don’t need to say what is where. Among these two PRTG has been chosen as its demo version gives a fully functional service of its commercial version for ten remote nodes for forever. On the other hand Zenoss gives us only a certain period of time to use freely and then user
Network Monitor

need to buy their commercial version. As “BIM Logiciel” has less than 10 nodes to monitor, so it is capable of monitoring the network.
6.0 Implementation

“PRTG” has been developed by a company named “Paessler”. The software can be downloaded from their homepage [http://www.paessler.com/prtg](http://www.paessler.com/prtg). There is an option to register the free version of the software. In order to get technical support, users need to register with “Paessler”. Appendix A shows how to get the key and installation of the software.

Now after installing the software, users have to configure their network segments and choose some pre-installed sensors or customize sensors in order to monitor the network. So, users can start with “Network Guru” which performs auto discovery in the network to find out the devices. Please see Fig 12 below.

Figure 12: Configuring PRTG with auto feature.

Above picture showing the automatic configuration of PRTG which is driven by “Network GURU”. Even though it’s an automatic feature to set up the configuration but still, some credentials such as our SNMP details, LAN server details, and internet connection details need to be provided. Appendix B and C show how to configure our LAN server and internet connection.
Well this far the discussion was about all automatic sensors which are pre-installed in PRTG. But there is some sensor can be customized for users. For example user choose to see disk space of our FTP server cause it is important for user to monitor. On below figure will show how to add a customized sensor for a device. First user has to choose their device. In this picture user has chosen their printer. Please see figure 13.

Once all these sensors have been set up, the user has to set up the report interval. There are several options whether user needs periodically such as weekly, monthly, or quarterly. User can have the report of live data as well. Below figure shows how to set up a report. The user chooses weekly for BIM Logiciel. Please see figure 14.
Figure 14: Setting up a report.

We can see in the above picture that, there are several options. But it depends on the user what they want to see from their report. We customized our one on term of summary with graph of all sensors.
7.0 Result

After implementing PRTG in network user would like to see how it’s functioning in their network. This result will prove that whether it's meet the user’s requirements or not.

BIM Logiciel wanted to monitor their servers. They wanted to see how much CPU load, Disk usage, Memory usage in some servers such as FTP server. FTP server plays an important role for internal employer and external tele-worker. The below figure shows us the status of our FTP server. Please see figure 15.

![Device FTP_Server_BIM_Logicial](image)

Figure 15: FTP server status.

From above figure we can see that CPU load is 38%, Memory usage is 45% and free disk space is 45%. Overall this server is healthy at the moment.

There are other servers such as E-mail server and SIP server in the company. PRTG is going to cover them by continuous ping test and RDP test for E-mail server as in case user need to configure any changes in that server. Ping gives the status of availability of these servers and HTTP port 80 gives the functional status of “BIM_Voip” server as this SIP server can be configured by web interface. The next figure will show the status of these two servers. Please see figure 16.
Ping test is successful and we customized sensor RDP for “E-mail Server” is working fine. On the other hand “BIM_VoIP” is working fine with its ping test and http test.

From this example it is important to mention that the user should put the sensor in the devices what they need actually, because active monitoring cause extra overhead in the network which can decrease network performance.

At the very beginning it has been mentioned that, the company has two internet connections available. One connection is specially for browsing internet. Another one is used for downloading or uploading data to the company FTP server. Below figure shows the status of both internet connections along with DNS server from an ISP. Please see figure 17.

The company has an ISP connection from Telia and Telenor for internet. Telia is being used only for browsing. That’s why an HTTP sensor has been chosen in order to check the functionality. Connection from Telenor has been used for FTP server specially.

BIM Logiciel wanted to monitor some websites in order to make some rules for internet accessibility within the company. They wanted to see how much data have been used by these social network websites such as Facebook, Twitter, and YouTube. Facebook data has been chosen to show here as an example. Please see figure 18.
Figure 18: Monitoring Facebook website.

There are some extra services that have been added for BIM Logiciel which will help maintenance person’s job easier, such as monitoring the printer. From printer we can see how many pages we have printed, whether the network printer is on or not. Please see figure 19 below.

Fig 19: Monitoring Cloud, Printer.

Now let see how it issues alarm in case of failure. For this issue E-mail server has been disconnected from network for test purpose. And it immediately issues an alarm which stating that the email server is down. Figure 20 below shows the alarms issue of PRTG.
Fig 20: Alarm issue of PRTG.

Here one view of PRTG is missing, how it shows the overall view of the whole network in the summary. So let see how it gives a view to the peoples who are monitoring. Please see figure 21.

Figure 21: Overview of whole network at a glance.
8.0 Further enhancements

Due to limited time and context we showed how a small to middle size network can be monitored by the open source monitoring tool. But this tool can be further extended such as remote monitoring, where we can monitor branch network of a company from the main office. On the other hand we could implement in mobile devices such as the iPhone or Android phone for monitoring people so that they can monitor their network on mobility. SNMP could have been implemented in order to get more info from servers, routers and network printers. Servers with virtual machine could be monitored by PRTG. Cloud monitoring is not easy to implement but it’s possible to implement by this tool. We have already shown a little bit of cloud monitoring in this Report. But all of them are pre-defined by this software.
9.0 Conclusion

This report illustrates how very basic tools can be used to monitor the network. Knowing that simple tools can be so useful in monitoring our network, it gives details about all those tools work which most network administrators don't really take note, also with the details giving in this report reader can easily see which type of network monitoring to use and what it can monitor. And depends on those tools, companies are creating tailor made monitoring tools. These monitoring tools give us a great flexibility to monitor our network in order to tune the performance measurement in a great extent. Moreover they tell us what to monitor deeper, why should we monitor and what can be done with the result. Monitoring a network is very essential, intelligent management of the business. It helps the business grow and prevent them from un-necessary downtime due to inappropriate use of resources. Implementing the most essential Monitoring tools for BIM logiciel can prevent their network down age, they can take a decision about their company internet accessibility policy depends on available data. Finally one point can be proven by this report that by monitoring a network we can be benefited in many ways, some of them are tangible and some are intangible. We should know our network well by monitoring it.
Network Monitor

10.0 References:


[3] Ping Definition. [ONLINE] Available at: http://searchnetworking.techtarget.com/definition/ping This page was last reviewed on 20 November 2012


By: Craig Tunstall; Gwyn Cole ISBN-10: 0-201-61613-0

[5] What is Monit. [ONLINE] Available at: http://rubyworks.rubyforge.org/manual/monit.html This page was last reviewed on 9 December 2012

[6] http://en.wikipedia.org/wiki/Zope This page was last reviewed on 7 December 2012


Appendix A:

Setting up internet connection in PRTG
Appendix B:

Setting up internet connection in PRTG
Appendix C:

Setting up LAN server connection in PRTG

Guru: Set up monitoring for Server in your LAN

PTG has found the following servers in your LAN and will auto-discover them. Please review the list and add the DNS names or IP addresses of other servers, if desired.

<table>
<thead>
<tr>
<th>Servers</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory</td>
<td>Domain Controllers</td>
</tr>
<tr>
<td>Exchange &amp; E-Mail Servers</td>
<td>192.168.1.100</td>
</tr>
</tbody>
</table>

Other Servers in Your Network

Other Servers

*** Enter DNS names or IP's of your servers here ***