A Survey on Open Source Tools - for Server Monitoring using SNMP

S. Priscilla Florence Persis, S. Bindiya
B.Tech IT – III year
SNS College of Engineering ,Coimbatore.

***Abstract:-* This paper covers the scope of monitoring various servers with SNMP protocol by using open source solutions available. It focuses on the Monitoring in enterprise using SNMP protocol & open source platforms for proactive server monitoring and data center management. It provides the solution for the case study using the open source server monitoring tools.**

Keywords: Open Source Monitoring , Data Center Monitoring , Performance Server Review , incident reporting , SNMP Protocol , Nagios , Hyperic HQ , Open NMS , Zabbix , Zenoss , Ground Works.

1. OVERVIEW

"The only constant thing in this world is change" and it implies very well to the science & technology domain. Industries are spending and investing a major capital for monitoring their servers, applications and network equipments,so this paper explains about the server monitoring using open source tools.

Open source tools is a phrase used to mean a program or tool that performs a very specific task, in which the source code is openly published for use and/or modification from its original design, free of charge. Open source tools are typically created as a collaborative effort in which programmers improve upon the code and share the changes within the community, and is usually available at no charge under a license defined by the open source initiative.

Server monitoring lets you get real-time internal statistics from the servers that you load test. By internal statistics, we mean things like CPU usage, number of cache hits in the database, number of open connections, amount of free memory, etc.

In this paper we will evaluate performance of different open-source options available for monitoring enterprise level data center operations using SNMP protocols.

2. MONITORING TYPES

Monitoring can be performed either by querying normal status of the application as up or down which does not require any special agents to be installed like in case of ICMP ping response. This kind of monitoring can be referred to as "agent less monitoring". Or it can be done with help of special installed tool agents which interact with the services of OS and applications and is also capable of sending vitals and other system info to the monitoring server, this kind of monitoring tool using some specialized developed agents is referred to as "agent based tools".

Reactive Approach is the only option available for system administrators after information passed about the system by end users. There is no mechanism for directly interacting with server vitals.

Industry is moving towards Pro Active approach where there is a layer between system administrator and datacenter that provides pro active measures to system administrators to act precisely and pass on information to upper management with help of reports. With help of SNMP we can able to track all performance related info in database for MIS reporting and can link with KPI (Key Performance Index).

3. SNMP Protocol

Simple Network Management Protocol (SNMP) is a popular protocol for network management. It is used for collecting information from, and configuring, network devices, such as servers, printers, hubs, switches, and routers on an Internet Protocol (IP) network. Microsoft Windows Server 2003 provides SNMP agent software that works with third-party SNMP management software to monitor the status of managed devices and applications.

SNMP is used for monitoring network devices and other data center equipments. It is part of the TCP/IP protocol suite. In a data center environment each server with an installed agent communicates with SNMP to broadcast the status of a device on which agent is installed. The manager (Monitoring Server) collects the data from various nodes.

SNMP manager:

The Windows Server 2003 SNMP service provides only the SNMP agent. Unless you develop your own SNMP management application, you must install third-party SNMP management software, such as HP Openview, Novell NMS, IBM NetView, or Sun Net Manager to work with the SNMP agent. You can install third-party SNMP management software on one or more hosts. Alternatively, you can develop your own SNMP management software application by using the two application programming interfaces (APIs) that Windows Server 2003 provides:

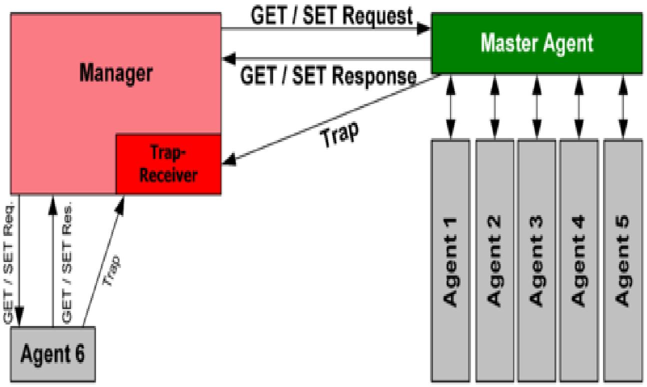
WinSNMP API (Wsnmp32.dll) provides a set of functions for encoding, decoding, sending, and receiving SNMP messages.

Management API (Mgmtapi.dll) provides a basic set of functions for developing fast and simple SNMP management systems.

An SNMP-managed network consists of three key components:

- Managed device
- Agent — software which runs on managed devices
- Network management station (NMS) — software which runs on the manager

SNMP works on the layer 7 of OSI model (Application Layer) and uses UDP port 161 for communication reason being it does not need any acknowledgement and being used for monitoring purpose only. There are mainly 3 versions of SNMP protocol.



This PDU was introduced in SNMPv2 and was originally defined as manager to manager communication.

4. CASE STUDY

Let us assume that we have 64 servers in our data center with performance check sheet to fill daily for each server and the listed parameters are 10 in nos. then our system administration will be filling up 640 parameters daily for the complete data center.
Which is a repetitive task and is actually a man power wastage considering the fact that for 64 servers a system admin will take approx 10 minutes on each server he will be wasting 640 minutes approx 10 hours on this activity.

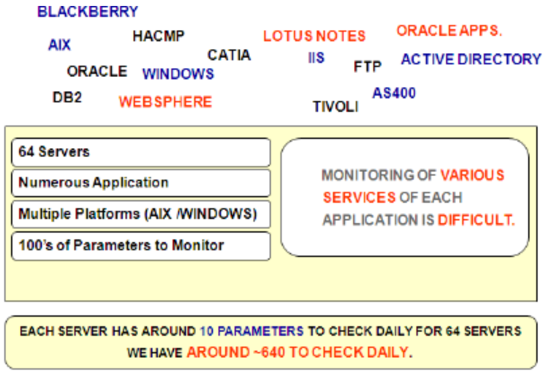

BLACKBERRY
HACMP
AIX
CATIA
LOTUS NOTES
ORACLE APPS.
IIS
FTP
ACTIVE DIRECTORY
ORACLE
WINDOWS
DB2
WEBSPHERE
AS400
TIVOLI
64 Servers
Numerous Application
Multiple Platforms (AIX /WINDOWS)
100's of Parameters to Monitor
MONITORING OF VARIOUS SERVICES OF EACH APPLICATION IS DIFFICULT.
EACH SERVER HAS AROUND 10 PARAMETERS TO CHECK DAILY FOR 64 SERVERS WE HAVE AROUND ~640 TO CHECK DAILY.

Fig : Number of Applications on 64 Servers each with 10 core parameters to check comes to 640 daily check.

The outcome of this case study suggests that there should be an automated system for monitoring resources inside data center.

Problems analyzed in case study:

- Non Availability of Automated System for Monitoring Data Center Events and Downtime
- Manual & long process of data collection in check sheets
- It is difficult to track data center 24X7

5. SOLUTION: OPEN SOURCE TOOLS

- Nagios
- Zabbix
- Zenoss
- Op5
- Icinga
- Cacti
- Munin

5.1. Nagios

Nagios is considered as one of the most popular if not the most popular open-source computer network monitoring software application available.The current version of Nagios is 4.0.8,introduced on August 12,2014. It was originally designed to run under Linux, but other Unix variants are also supported. Nagios provides monitoring of network services (SMTP, POP3, HTTP, NNTP, ICMP, SNMP, FTP, SSH) and host resources (processor load, disk usage, system logs) among others. Remote monitoring is managed through SSH or SSL encrypted tunnels. Nagios has a simple plugin design that gives users the freedom to effortlessly develop their own service checks based on needs and by using any of the supported tools that they would like. To detect and differentiate between hosts that are down and those that are unreachable, Nagios allows you to define network host hierarchy using 'parent' hosts. When services or host problems arises, notification will be sent to the one who is in charge of the network via e-mail, SMS, etc.

5.2. Zabbix

Zabbix was developed by Alexei Vladishev, and first released in 2001. Current stable version of Zabbix is 2.4.4.Zabbix is an enterprise-class monitoring tool that is full-featured and is commercially supported. It is capable of monitoring and tracking the status of different kinds of network services, servers, and other network hardware. Zabbix has great visualization functionalities including user-defined views, zooming, and mapping. It has a versatile communication method that allows quick and uncomplicated setup of different types of notifications for pre-defined events. Zabbix has three primary modules: server, agents, front-end. To store monitoring data, you can use MySQL, PostgreSQL, Oracle, or SQLite as your database. Without installing any software on the monitored host, Zabbix allows users to verify the availability and responsiveness of standard services such as SMTP or HTTP. To monitor statistics such as CPU load, network utilization and disk space, a Zabbix agent must be installed on host machine. Zabbix includes support for monitoring via SNMP, TCP and ICMP checks, IPMI and custom parameters as an option to installing an agent on hosts.

5.3. Zenoss

This tool was developed by Bill, Erik Dahl, Mark Hinkle and is capable of monitoring all devices, servers , network and application inside data center. The core database and the events are stored in My SQL database. Based on the Zope application server and written in Python, Zenoss (Zenoss Core) is a server and network management platform that combines original programming and several open source projects to integrate data storage and data collection processes via web-based user interface. It allows users to monitor availability, inventory/configuration, performance and events. Zenoss Core is capable of monitoring availability of network devices using SNMP, SSH, WMI, network services (HTTP, POP3, NNTP, SNMP, FTP) and host resources (processor, disk usage) on most network operating systems. A plug-in architecture provided by ZenPacks allows community members to extend its functionality. ZenPacks are encapsulated in Python eggs and supplies instrumentation and reports for monitored infrastructure units.Features are:

- Monitoring availability of network devices using SNMP, SSH, WMI
- Monitoring of network services (HTTP, POP3, NNTP, SNMP, FTP)
- Monitoring of host resources (processor, disk usage) on most network operating systems.
- Time-series performance monitoring of devices
- Event management tools to annotate system alerts
- Automatically discovers network resources and changes in network configuration
- Supports Nagios plug-in format

5.4. Op5

Op5 Monitor server monitoring capabilities enables gathering of performance, capacity and availability status data from all layers and parts of the server. Regardless if it is physical, virtual, cloud based servers or organizations with distributed data centers. op5 Monitor is an advanced server monitoring software which presents health and server performance metrics in a unified view where you can customize alerts, reports and dashboards for your organization needs. You have the ability to both check basic up-time and detailed usage on all types of servers.op5 Monitor is designed to make sure that a server is active, healthy, and responding to requests appropriately. We provide a easy to use server monitoring software that supports multiple hardware, virtual and cloud based servers vendors.Op5 Monitor server monitoring software makes it easy to quickly diagnose, correlate event and solve server performance issues instantly wherever they originate, regardless if it is at the server, network or application level.Some of the benefits are:

- Monitor physical, virtual and cloud servers in the same place
- Fast root cause identification and troubleshooting
- Alerts and reporting capabilities
- Cross-platform server monitoring
- Accurate server capacity planning
- Able to handle large volumes of monitored devices and services.

5.5. Icinga

Icinga is a scalable and extensible monitoring system which checks the availability of your resources, notifies users of outages and provides extensive BI data.Its initial release was on 15 May 2009.Current version of Icinga is Icinga 2 v2.1.0 on 29 August 2014.This version has the feature with enhanced configuration analysis, logging, cluster High Availability features. Icinga is an open source network and computer system monitoring application. It was originally created as a fork of the Nagios system monitoring application in 2009.Icinga is attempting to get past perceived short-comings in Nagios' development process, as well as adding new features such as a modern style user interface, additional database connectors. Icinga also maintains configuration and plug-in compatibility with Nagios, facilitating migration between the two monitoring software. Monitoring of network services (SNMP,SMTP,PING etc.), Monitoring of host resources (CPU load, disk usage, etc.), Monitoring of server components (switches, routers, temperature and humidity sensors, etc.), Simple plug-in design that allows users to easily develop their own service checks, Parallelized service checks are the features of monitoring using Icinga. Icinga is compatible with all plug-ins and the majority of add-ons written for Nagios, especially for users opting for the Icinga Classic UI. Popular add-ons to extend Icinga’s functionality include:

- Performance graphing (e.g. PNP4Nagios,NagiosGrapher, InGraph)
- Configuration interfaces and tools (e.g. Nconf (tool for configuring Nagios), NagiosQL, LConf)
- Business process monitoring (e.g. Business Process Addons)
- Network visualization (e.g. NagVis, Nagmap)
- Windows monitoring (e.g. NSClient++, Cygwin)
- SNMP trap monitoring (e.g. SNMPTT, NagTrap)

5.6. Cacti

Cacti is an open-source, web-based network monitoring and graphing tool designed as a front-end application for the open-source, industry-standard data logging tool RRDtool. Cacti allows a user to poll services at predetermined intervals and graph the resulting data. The Cacti project was first started by Ian Berry on September 2, 2001. Version 0.8.8c was released in August 2014 with numerous bug and security issues patched. It can be utilized to configure the data collection itself, enabling particular setups to be monitored without any manual configuration of RRDtool. Cacti allows you to poll services at preset period and graph the resulting data. It is mainly used to graph time-series data of metrics such as CPU load and network bandwidth utilization. Cacti can be expanded to monitor any source via shell scripts and executables. It also supports plugin architecture and has a large and active community that has gathered around the Cacti forums providing handy scripts, templates, and tips on writing plugins.The features of Cacti are:

- unlimited graph items
- auto-padding support for graphs
- graph data manipulation
- flexible data sources
- data gathering on a non-standard timespan
- custom data-gathering scripts
- built-in SNMP support
- graph templates
- data source templates
- host templates
- tree, list, and preview views of graph data
- user-based management and security

5.7 Munin

The current version of Munin is 2.0.24.Like Cacti, Munin utilizes RRDTool to present output in graphs through a web interface. It has a master/node architecture in which the master links to all the nodes at regular intervals and asks them for data. Using Munin, you can quickly and easily monitor the performance of your computers, networks, SANs, and applications. It makes it uncomplicated to spot the issue when a performance problem occurs and clearly see how you're doing capacity wise on all restricted resources. For Munin’s plugin, its main priority is on simple plug and play architecture. It has plenty of monitoring plugins available that will easily work without a lot of modification.

7. CONCLUSION

Out of all these open source solutions **Nagios** is the tool that is being used by the masses. Now we have option of virtual images appliances from nagios. **Zabbix** has quick reporting capabilities. **Zenoss** has an edge over monitoring virtualization platforms.**Op5** Monitor server monitoring software makes it easy to quickly diagnose, correlate event and solve server performance issues instantly wherever they originate, regardless if it is at the server, network or application level. **Icinga** is a scalable and extensible monitoring system which checks the availability of your resources, notifies users of outages and provides extensive BI data. **Cacti** can be utilized to configure the data collection itself, enabling particular setups to be monitored without any manual configuration of RRDtool. Cacti allows you to poll services at preset period and graph the resulting data. **Munin** makes it uncomplicated to spot the issue when a performance problem occurs and clearly see how you're doing capacity wise on all restricted resources.

Of all the open source tools Nagios is a optimal solution. Nagios is a powerful network monitoring tool that helps you to ensure that your critical systems, applications and services are always up and running. It provides features such as alerting, event handling and reporting. The Nagios Core is the heart of the application that contains the core monitoring engine and a basic web UI. On top of the Nagios Core, you are able to implement plugins that will allow you to monitor services, applications, and metrics, a chosen frontend as well as add-ons for data visualisation, graphs, load distribution, and MySQL database support, amongst others.

Icinga started out as a fork of Nagios, but has recently been rewritten as Icinga 2. Both versions are under active development and available today, and Icinga 1.x is backward-compatible with Nagios plug-ins and configurations. Icinga 2 has been developed to be smaller and sleeker, and it offers distributed monitoring and multithreading frameworks that aren’t present in Nagios or Icinga 1. You can migrate from Nagios to Icinga 1 and from Icinga 1 to Icinga 2.Like Nagios, Icinga can be used to monitor anything that speaks IP, as deep as you can go with SNMP and custom plug-ins and add-ons.

It can be concluded that each of the solution has its own advantages and drawbacks. SNMP protocol is widely used for developing latest monitoring solutions for network devices because of its lean structure and presence in mostly all operating systems. Open source is evolving as a major trend for the industries looking for scalable cost efficient solutions for their business operations.Nagios has a web interface that helps users check network health from anywhere; Creates reports on trends, availability, alerts, notifications — via the web interface;Monitors network redundancies and failure rates.

8. REFERENCES

[1] Use of open technologies for enterprise server monitoring using snmp from **International Journal on Computer Science & Engineering;2010, p2246**

[2] A Simple Network Management Protocol (SNMP) RFC 1157

[3] Management Information Base for network management of TCP/IPbased
Internet RFC 1066 – 1156

[4] Simple Network Management Protocol RFC 1067

[5] Structure and identification of management information for TCP/IPbased Internets RFC 1065