ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 8, August 2017

Server Monitoring Using Windows Management Instrumentation and SNMP

K.Bhagyasri[1], K.Velayudham[2], P. Srivyshnavi[3]

M.Tech Student, Computer Science Engineering(CSE), Department of CSE, School of Engineering & Technology, Sri Padmavati Mahila Viswavidyalayam (SPMVV), Tirupati, A.P, India[1]

Manager, Department of SPACE, SCOF, RO SDSC SHAR, ISRO, SRIHARIKOTA, India[2]

Senior Assistant Professor, Department of CSE, School of Engineering & Technology, Sri Padmavati Mahila Viswavidyalayam (SPMVV), Tirupati, A.P, India[3]

ABSTRACT: Large organizations flourish and grow in workforce, the size of network used by the organizations increases; different components of the network are located at geographically different locations. The idea is to monitor the status of different properties of applications running on remote servers and systems, all of which are connected in a network. The troubleshooting process becomes much easier, because the service and server at faulty can be detected remotely and the necessary actions like restarting the service can be done. To perform such monitoring we have mainly two protocols – Simple Network Management Protocol (SNMP) and Windows Management Instrumentation (WMI). WMI provides more information retrieving capabilities than SNMP, but it can be used only with Windows based systems.

In proposed work we designing an application that can query the state of the server, query the condition of any kind of service present on the system, record changes of the condition of the services. While WMI will be used to obtain information about the services, SNMP will be used to obtain the memory usage of the servers on a daily basis. This core part will be present in a timer, so that the servers will be queried at regular intervals. Features such as, which servers are to be monitored, adding and deleting new servers will be provided in the web application. Options such as which properties of the services are to be monitored, which services are to be monitored can be select in the web application as well.

KEYWORDS: Server, WMI, SNMP, Services.

I. INTRODUCTION

WMI consists of a set of extensions to the windows driver model that provides an operating system interface through which instrumented component provide information and notification. WMI is a Microsoft implementation of the web-based enterprise management(WBEM) and common information model (CIM) standards from distributed management task force(DMTF). Windows Management Instrumentation is a core WMI technology, you can use WMI to manage both local and remote computers. WMI provides a consistent approach to carrying out day-to-day management task with programming or scripting languages.

II. LITERATURE SURVEY

SERVER:

A Server is a computer program that provides services to other computer programs and their users in the same or other computers. The computer that a server program runs in frequently referred to as a server. Servers in terms of resources being used physical location of the server and available storage space and monitoring services/applications running on the server

For example, say MSSQL service working on the server, it would be helping if we had a system that could inform us when a vital service or application has stopped working unexpectedly. The necessary measures can be taken in a timely manner. If we did not have such system, any operation trying to invoke the MSSQL Service.

WMI:

WMI consists set of extensions to windows drive model that provides an operating system interface through which instrumented components provide information and notifications. Windows management instrumentation is a core WMI technology, you can use WMI to manage both local and remote computers. WMI provides a consistent approach to carrying out day- to- day management task with programming or scripting languages. WMI prescribes enterprise management standards and related technologies for windows that work with existing management standards , such as Desktop Management Interface (DMI) and SNMP.

SNMP:

SNMP is an internet standard protocol for collecting and organizing information about managed devices on IP network and for modifying that information to change device behavior. SNMP is widely used in network management for network monitoring. SNMP exposes management data in the form of variable on the managed system organized in a management information base (MIB) which describe the system status and configuration. These variables can be remotely queried by the managing applications. SNMP one or more administrative computers called managers have task of monitoring or managing a group of hosts or devices on a computer network. Managed system executes at all time software component called an agent which reports information via SNMP to manager. Using SNMP total memory usage of the server is estimated. Monitoring of the servers running on linux on operating system we can use SNMP.

SQLYog:

SQLYog is a GUI tool for the MySQL. SQLYog is distributed both as free software free of charge as well as several paid, propertary, versions. SQLYog works on the platform starting from windows XP/windows 2003 to Windows 8/Server 2008 R2.

Tom-Cat:

Tomcat is an application server from the Apache Software foundation that executes java servlets and renders web pages include Java Server page coding. It can15 be used as a standalone product with its own internal web server or together with other web servers including Apache. It requires a Java Runtime Enterprise environment that conforms to JRE 1.1 or later.

High Charts:

High charts released in 2009. High charts is a charting library written in pure JavaScript, offering an easy way of adding interactive charts to your web site or web application. In modern browsers graphs are rendered in SVG with VML support for legacy browsers.

WMI Architecture:

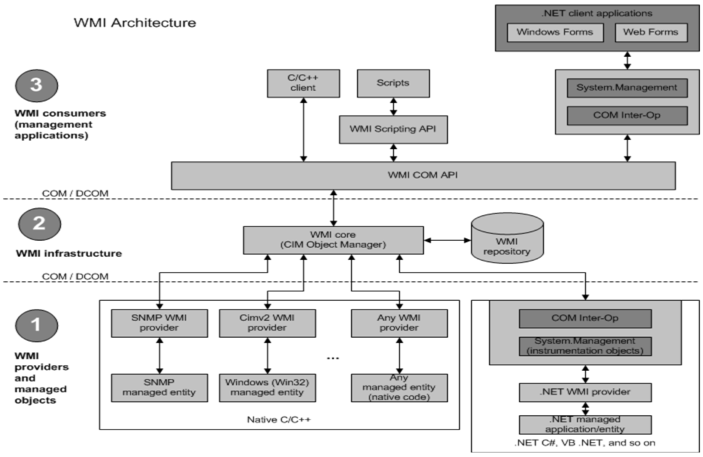


Fig: WMI Architecture

SNMP Architecture:

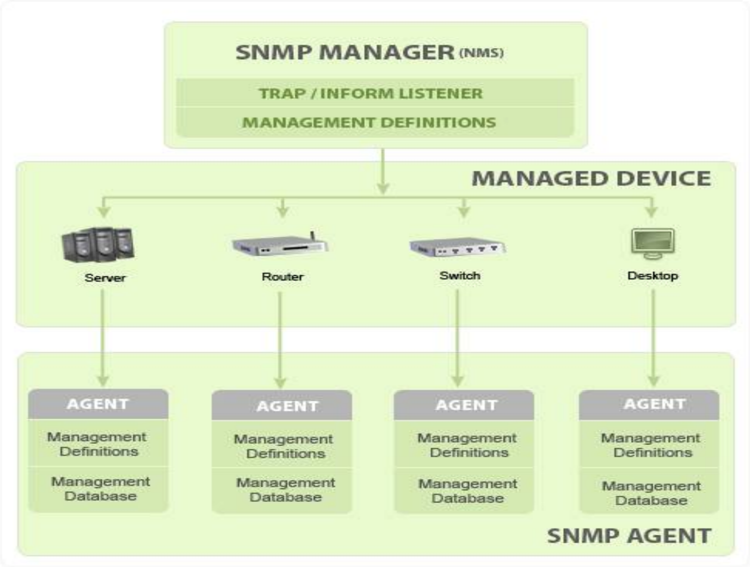


Fig: SNMP Protocol Architecture

III. PROPOSED METHODOLOGY

Server Monitoring:

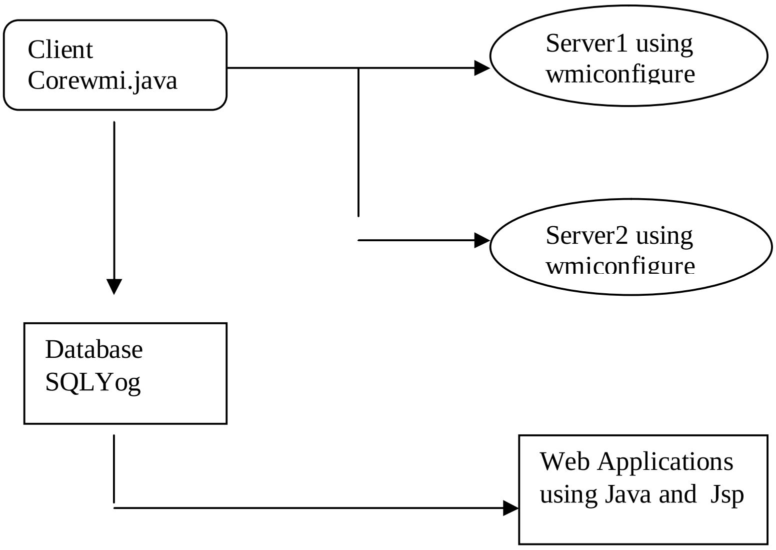


Fig: Block diagram of Server Monitoring

Server Monitoring Using WMI and SNMP:

The designing an application that can query the state of the server, query the condition of any kind of service present on the system record changes of the condition of the services. The core part of the applications is WMI and SNMP. While WMI will be used to obtain information about the services, SNMP will be used to obtain the memory usage of the servers on daily basis. This core part will be present in a timer, so that the servers will be queried at regular intervals. To implement a modular and loosely coupled design information obtained through WMI and SNMP will be stored in a database and data available presented to the user through a web applications. This means that the web application and core logic will never actually interact directly with each other. The feature such as, which servers are to be monitored, adding and deleting new servers will be provided in the web application. Options such as which properties of the services are to be monitored, which services are monitored can be select in the web applications as well.

We have tried to design an easily modifiable system, where the users has the capability to decide what is to be monitored and what is not. The front end will also be using **Highcharts API**, which is written in pure JavaScript, to generate dynamic graphs showing the memory usage of servers for past twenty days.

DOI: 10.15680/IJIRCCE.2017. 0508033

Configure WMI for Windows Server2008:

The procedure below outlines the steps required to configure the server, Remote Registry, and WMI services for automatic startup.

Step1: To open Run menu text the **services.msc** and Enabling DCOM for Windows Server2008. Under Computer Services, expand

computers and then click My computer. Select the default Properties tab. Configure the following Default Properties.

step2: Configure DCOM communication for Windows Server 2008. From the DCOM configuration (**dcomcnfg**) windows, expand

computers and select My computer. On action menu Click Properties. Select Default Protocols tab. Configure the following details

a. If connection- oriented TCP/IP is listed in the DCOM Protocols windows, go to step5 in this row
b. If connection- oriented is not listed in the DCOM protocol window, select Add
c. From the protocol sequence list box, select Connection- oriented TC/IP. Click OK.

step3: Configure Windows 2008 user account for DCOM. On Action menu, click properties. select the COM Security tab. In

Access Permissions, click Edit Default. Select the user or group requiring DCOM access.

note: If the user or group requiring DCOM access is not listed in the permissions list, you must add the user to the configuration.

a. Local Access – Select the Allow check box
b. Remote Access – Select the Allow check box

Click OK.

step4: Configuring the Windows2008 Firewall. In Run menu type (**wf.msc**). Click OK. Select Inbound Rules. On the action

menu, click new Rule. Select Custom and click Next. The program windows is displayed.

a. select all programs, and click Next. The protocol and ports window is displayed.
b. From the Protocol type list box, select TCP and click Next
c. Under which remote IP address does this rule apply to field, select the radio button on these IP address. Click Add.

step5: Configuring DCOM Access for Windows Server2008. In Run menu type (**regedit**). You must be a system administrator

to edit registry settings.

a. Locate the following registry location:HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}
b. Right-click the entry {76A64158-CB41-11D1-8B02-00600806D9B6}, then click Permissions.
c. Click the Advanced button. The Advanced Security Settings are displayed.
d. In the Owner field, click Change. In the Enter the object name field, set the owner as Administrators.

Give Administration Full Control permission. Click OK In permission entries field select your user and click edit.

note: If the user is not listed in the permission list, you must click Add and define your user as a principal. to search for a user

name , click Check Names, then click OK to Add your user.

We add two groups: performance Log user and Distributed COM User:

a. In the type field, select Allow
b. In the Applies to field, select this Key and Subkeys. Basic permissions fields, select Full control. By Default, selecting Full

Repeat this process for the following registry key: HKEY CLASSES_ROOT\Wow6432Node\CLSID\{76A64158-CB41-11DI-8B02-

00600806D9B6). Close the registry editor.

step6: Final step.

a. In regit, navigate to and click: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies \system.
b. Click LocalAccountTokenFilterPolicy and set the value to 1.
If LocalAccountTokenFilterPolicy does not exit, create this DWORD as follows:
- On the Edit menu, click new-> DWORD value
- Enter LocalAccountTokenFilterPolicy
- Right-click LocalAccountTokenFilterPolicy and click Modify. In the value data box, type 1, and click OK
-

IV. EXPERIMENTAL RESULTS

Web Applications: Web Applications using Java script pages created a server monitoring like services, server page, server status, server status history, service properties.

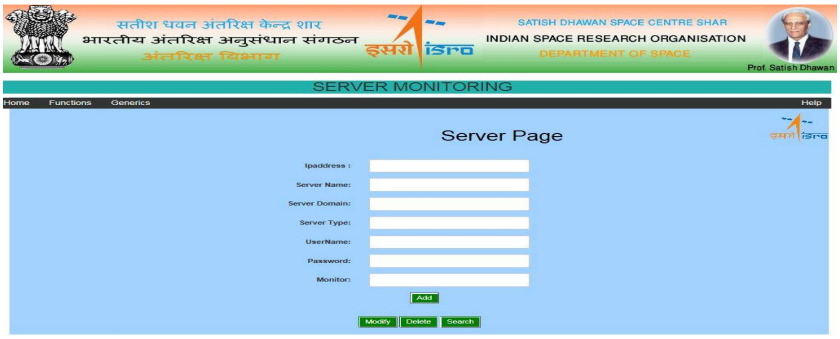
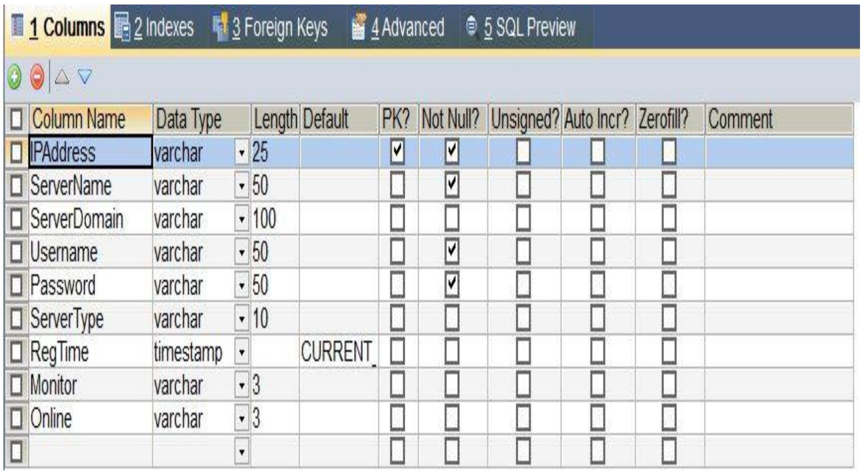


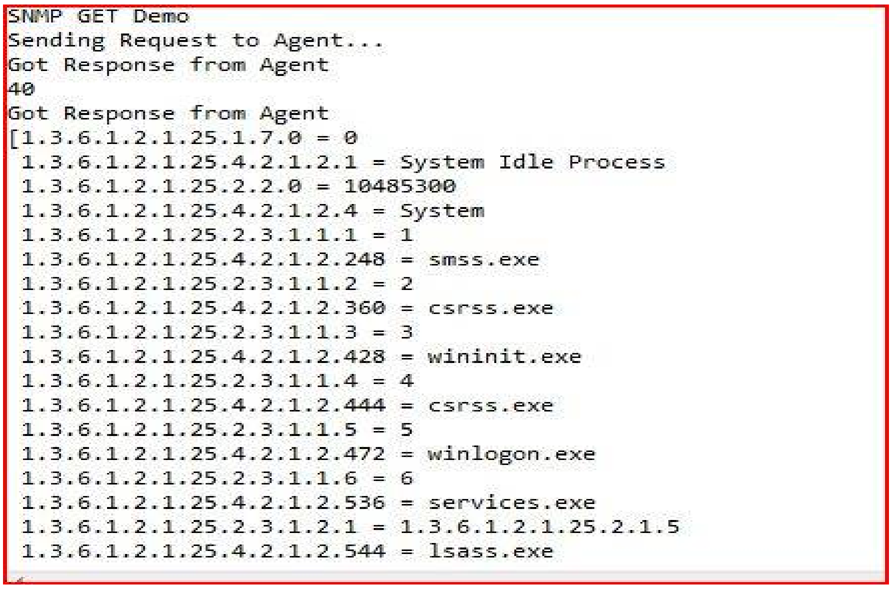
Fig: Result of Web Applications

SQL Database: SQL is used to communicate with a database. SQL can execute queries against a database, SQL can retrieve data from a database, SQL can insert records in a database. SQL is a standard language for accessing and manipulating database. create a tables, Create an entity in the table. We are using :
- SQLyog Community v11.52 (32 bit)
- MySQL - 5.1.52 : Database



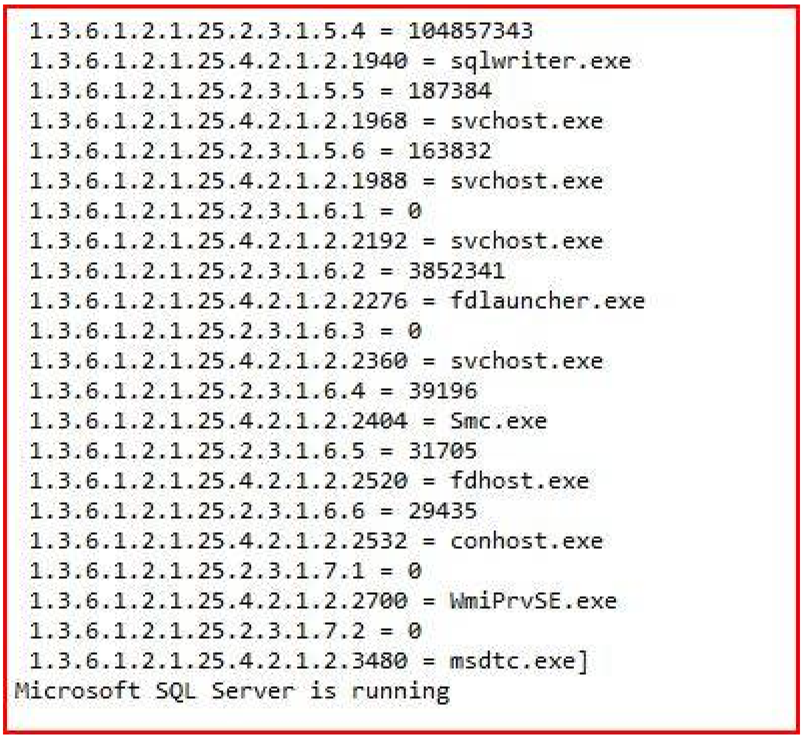
☐	Column Name	Data Type	Length	Default	PK?	Not Null?	Unsigned?	Auto Incr?	Zerofill?	Comment
☐	IPAddress	varchar	25		☑	☑	☐	☐	☐	
☐	ServerName	varchar	50		☐	☑	☐	☐	☐	
☐	ServerDomain	varchar	100		☐	☐	☐	☐	☐	
☐	Username	varchar	50		☐	☑	☐	☐	☐	
☐	Password	varchar	50		☐	☑	☐	☐	☐	
☐	ServerType	varchar	10		☐	☐	☐	☐	☐	
☐	RegTime	timestamp		CURRENT_	☐	☐	☐	☐	☐	
☐	Monitor	varchar	3		☐	☐	☐	☐	☐	
☐	Online	varchar	3		☐	☐	☐	☐	☐	
☐					☐	☐	☐	☐	☐	

Fig: Result for Inserted values in SQLYog database



```
SNMP GET Demo
Sending Request to Agent...
Got Response from Agent
40
Got Response from Agent
[1.3.6.1.2.1.25.1.7.0 = 0
 1.3.6.1.2.1.25.4.2.1.2.1 = System Idle Process
 1.3.6.1.2.1.25.2.2.0 = 10485300
 1.3.6.1.2.1.25.4.2.1.2.4 = System
 1.3.6.1.2.1.25.2.3.1.1.1 = 1
 1.3.6.1.2.1.25.4.2.1.2.248 = smss.exe
 1.3.6.1.2.1.25.2.3.1.1.2 = 2
 1.3.6.1.2.1.25.4.2.1.2.360 = csrss.exe
 1.3.6.1.2.1.25.2.3.1.1.3 = 3
 1.3.6.1.2.1.25.4.2.1.2.428 = wininit.exe
 1.3.6.1.2.1.25.2.3.1.1.4 = 4
 1.3.6.1.2.1.25.4.2.1.2.444 = csrss.exe
 1.3.6.1.2.1.25.2.3.1.1.5 = 5
 1.3.6.1.2.1.25.4.2.1.2.472 = winlogon.exe
 1.3.6.1.2.1.25.2.3.1.1.6 = 6
 1.3.6.1.2.1.25.4.2.1.2.536 = services.exe
 1.3.6.1.2.1.25.2.3.1.2.1 = 1.3.6.1.2.1.25.2.1.5
 1.3.6.1.2.1.25.4.2.1.2.544 = lsass.exe
```

Fig: SNMP Request toAgent



```
 1.3.6.1.2.1.25.2.3.1.5.4 = 104857343
 1.3.6.1.2.1.25.4.2.1.2.1940 = sqlwriter.exe
 1.3.6.1.2.1.25.2.3.1.5.5 = 187384
 1.3.6.1.2.1.25.4.2.1.2.1968 = svchost.exe
 1.3.6.1.2.1.25.2.3.1.5.6 = 163832
 1.3.6.1.2.1.25.4.2.1.2.1988 = svchost.exe
 1.3.6.1.2.1.25.2.3.1.6.1 = 0
 1.3.6.1.2.1.25.4.2.1.2.2192 = svchost.exe
 1.3.6.1.2.1.25.2.3.1.6.2 = 3852341
 1.3.6.1.2.1.25.4.2.1.2.2276 = fdlauncher.exe
 1.3.6.1.2.1.25.2.3.1.6.3 = 0
 1.3.6.1.2.1.25.4.2.1.2.2360 = svchost.exe
 1.3.6.1.2.1.25.2.3.1.6.4 = 39196
 1.3.6.1.2.1.25.4.2.1.2.2404 = Smc.exe
 1.3.6.1.2.1.25.2.3.1.6.5 = 31705
 1.3.6.1.2.1.25.4.2.1.2.2520 = fdhost.exe
 1.3.6.1.2.1.25.2.3.1.6.6 = 29435
 1.3.6.1.2.1.25.4.2.1.2.2532 = conhost.exe
 1.3.6.1.2.1.25.2.3.1.7.1 = 0
 1.3.6.1.2.1.25.4.2.1.2.2700 = WmiPrvSE.exe
 1.3.6.1.2.1.25.2.3.1.7.2 = 0
 1.3.6.1.2.1.25.4.2.1.2.3480 = msdtc.exe]
Microsoft SQL Server is running
```

Fig: SQL Server is Running Using WMI Configuration

V. CONCLUSION

After a long time this application can successfully monitor the status of services of servers running on Windows operating system after regular intervals, it can record instances of status change of the properties. For the monitoring of servers running on Linux operating system, we can use SNMP. To obtain operational status of services on Linux servers, we need to configure an MIB file called HOST-RESOURCES mib. Efforts were made to do so, but we could not obtain the expected results. More effort is required to understand the configuring and access of MIB files on Linux systems. Although we could not use SNMP to obtain service status, we have used it to obtain the memory used by different services on a server. Integrating the information about the memory usage and Highcharts API, we were successfully able to generate dynamic graphs that show memory usage in a server over a period of time.

REFERENCES

1 K.Velayudham, Manager, ES&AS, SCOF.
2 http://www.paessler.com/support/videos
3 http://www.paessler.com/tools/wmitester
4 www.monitis.com
5 http://msdn.microsoft.com
6 http://www.w3schools.com
7 www.servermonitoring.com