WMI Based Real Time Agentless Enterprise Monitoring

Balaji Patil, Ankur Jain, Vinay Kumar Pathak

Abstract— Looking towards the complex, heterogeneous and dynamic nature of the networks, failures are unavoidable. Monitoring can be used for detection and reporting of failures. This underlines the need to develop a unified strategy for implementation and management of network resources in an enterprise.

This paper describes novel agentless system for real-time monitoring of windows based clients remotely by subscribing to those remote events. Monitoring is done using Windows Management Instrumentation (WMI) services. Results of service events are stored in Server. This system is called as Unified network resourse management system. We have demonstrated the system's capabilities and the results that are obtained from the clients using WMI services. These results include system hardware configuration, software configuration in terms of OS details, applications installed etc. This information is very useful to the administrator for maintenance of failures in the networks. Any change at the client system details, will be notified automatically by the clients to the server, so that server will have real-time updated information. This updated information will be very helpful incase of crashing of the remote client. Using this collected data, crashed clients can be restored in very short period of time. Real time monitoring of the clients is necessary for the maintaining the health of an enterprise network.

Index Terms— Agentless, Event, Enterprise monitoring, Passive Monitoring, Remote monitoring

1. INTRODUCTION

IN todays era of Information Technology (IT), technology is developing rapidly and introduction of new applications will further promote the IT development. Looking towards the complex, heterogeneous and dynamic nature of the thousand nodes of enterprise networks failures are unavoidable. So monitoring is used for detection and reporting of failures. In such a complex environment network administrators have to struggle a lot in order to solve the network problems rapidly and effectively ensuring their availability.

With the expansion of network scale, administrators can not complete these tasks manually. It becomes difficult to maintain the enterprise resourceses, monitor their availability and security of data. Administrators have to take the help of automated tools. In the management of enterprise network finding reasonable and feasible solution to improve the efficiency of system is a challenge.

So we propose a better and effective unified network management approach. In this approach we collect more and more remote data from clients in real-time. After collection and analysis of this data the network resources are managed.

Unified network resource management strategy is just seen as managing the changing resources in the networks or clients for example, the hardware configuration, options and strategies of the operating system etc. This dynamism underlines the need to develop a unified strategy for implementation and management of network resources in an enterprise.

Most of the remote network management systems are developed by the Windows-based component development i.e. COM as across Windows Management Instrumentation Commands (WMIC) provides very powerful functions for light weight implementation of remote network management. With this motivation we have developed a uniform standard remote resource management and monitoring enterprise system using WMIC services, consisting managing computer system resources, user resources and necessary alarming mechanisms.

So a better automated solution is developed using WMIC for remote management of components services that monitors resources without causing any distarbance in usual organization work.

This paper is organized in 5 sections. In section 1 we have tried to expain the need and motivation for development of unified resourse management system. Section 2 explains the technologies/techniques used for development of the system. Section 3 explains the proposed enterprise resource management system. In section 4 we have discussed the results and in section 5 we have written the conclusion.

2. RELETED WORK

In this section we are revising the technologies, techniques and existing tools available. In the past remote resourse management systems has been developed using various technologies like SNMP, COM, RMON etc.

The SNMP service is most widely used service for monitoring of networks. SNMP had a disadvantage of requirement of re-

- *Balaji Patil is currently pursuing his PhD from Uttarakhand Technical University, Dehradun, India. And working at Maharashtra Institute of technology, Pune, India. E-mail: balaji.patil@mitpune.edu.in*
- *Ankur Jain has completed his BE Computer Engineering from Maharashtra Institute of technology, Pune, India. E-mail: ankurjain2190@gmail.com*
- *Vinay Kumar Pathak is currently Vice chancellor, of V M O University, Kota, India. E-mail: vinay@vpathak.in*

mote agent. Another thing that needs to be mentioning is that being only a protocol, SNMP cannot offer the full management support that the typical enterprise system needs. While WMI provides the remote agentless monitoring of network. So we have used the WMI technology for development of automated unified resourse management system.

2.1 WMI Technology

Windows Management Instrumentation (WMI) [4] is the Microsoft implementation of Web-Based Enterprise Management (WBEM), which is an industry initiative to develop a standard technology for accessing management information in an enterprise environment. WMI uses the Common Information Model (CIM), a industry standard to represent systems, applications, networks, devices, and other managed components. The ability to obtain management data from remote client-computers is what makes WMI useful. Remote WMI connections are made through DCOM. The WMI Architecture is as shown in the fig.1.

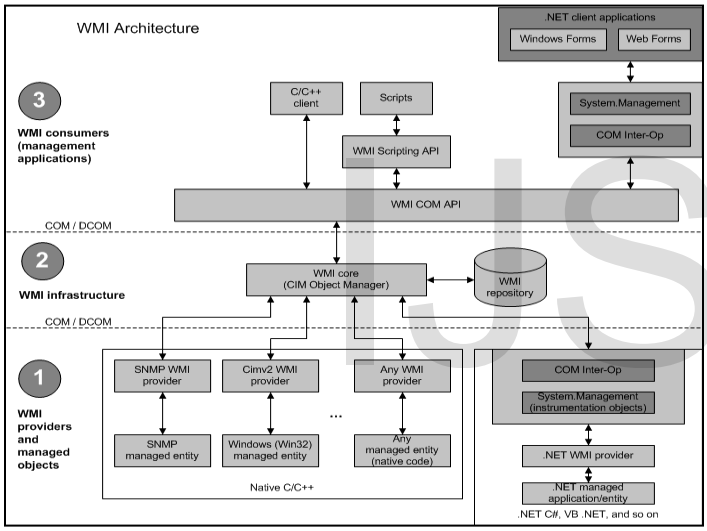


Fig. 1 WMI Architecture [4]

2.2 Types of Monitors

For monitoring of the networks various types of monitors are available. We have used the Active monitoring for real-time notification of the events or changes in the enterprise networks. Monitors are of following types-

Active Monitors - that track and alert you in real time when devices and services are down.

Passive Monitors – that listen for external signals (SNMP traps, log messages etc.) to identify and alert on infrastructure issues as they happen.

Performance Monitors – that track the health of network and application infrastructure over time and are key to proactive troubleshooting and planning.

Custom Monitors – that can be set up to track individual performance metrics as required.

Thresholds Monitors – that alert you when minimum or maximum thresholds are breached.

2.3 Passive Monitoring

The passive monitoring [5] approach uses devices to watch the traffic as it passes through it. These devices can be special purpose devices such as a sniffer or they can be built into other devices such as routers, switches or even end nodes. Examples of such built in techniques include Remote monitoring, SNMP and WMI devices. The passive monitoring devices are polled periodically and information is collected to assess network performance and its status.

The passive approach measures the real time traffic on the enterprise network without increasing overhead on the network.

2.4 Automated Monitoring Tools

There are various automated network monitoring tools are available in the market, few of them are mentioned below with their features.

PRTG Network Monitor

PRTG Network Monitor [9] monitors system availability using a variety of methods from simple ping through SNMP and WMI protocols to specific tasks such as HTTP, DNS and Remote Desktop availability using sensors. Using specific sensors for specific machines, an administrator can monitor service availability and reliability. Also, PRTG comes with some bandwidth monitoring sensors, which can trap the DOS attacks and performance of networks related issues. PRTG is easy to install & operate and it supports all Windows versions, XP/2003 or later. It has inbuilt number of graphical utilities for visual presentation of the collected monitoring information. A host of supported network services and protocols: SMTP, PING, HTTP, POP / POP3, FTP, PPP, etc.

IpSwitch Whatsup gold 14.2

Whatsup gold [10] is a network management suite. It can monitor devices using SNMP. Whatsup gold also features WMI support for Windows monitoring and agentless SSH monitoring for Linux/Unix systems monitoring everything on your network. A wide range of plugins are available for Whatsup gold. There are five main aspects to this software: Discovery, Mapping, Monitoring, Alerting, and Reporting. It provides Performance monitors (CPU utilization, Disk and space utilization, Interface utilization, Memory, Ping Latency etc). It supports application monitoring but requires polling at regular intervals and hence it consumes network bandwidth.

Microsoft's Operations Manager -2012

Operations Manager [11], a component of Microsoft System

Center 2012, is software that helps you monitor services, devices, and operations for many computers from a single console. Operations Manager will tell you which monitored objects are not healthy, send alerts when problems are identified, and provide information to help you identify the cause of a problem and possible solutions. Administrator can configure what will be monitored by selecting computers and devices to be monitored and importing management packs that provide monitoring for specific features and applications. Major disadvantage of this tool is it has bugs in monitoring applications.

All these above mentioned tools have some advantages and shortcomings, so this study underlines need of developing a unified automated monitoring tool which will monitor the enterprise network. Table 1 shows the impact of monitoring method, which provides the reason for development of an agentless WMI based automated monitoring tool [11].

TABLE 1
Methods of Monitoring

Method of Monitoring	Impact of overheads
With Agent	Processor: 1% average increase in processor utilization Disk: 9% average increase in pages/second Space: 351 MB data Network: 02 MB/min additional traffic Memory: Requires 19-32 MB memory
Agentless	Processor: less than 1% average increase in processor utilization Disk: less than 1% average increase in pages/second Space: less than 10 MB Network: less than 1 MB/min additional traffic Memory: Required only 1MB memory

3. ENTERPRISE NETWORK RESOURCE MANAGEMENT

Considering the need of enterprise network management an automated tool is developed with required features. Real time agent less discovery of clients is basically monitoring the infrastructure, changes taking place in client's environment, etc. These changes are then notified to the server (administrator). This helps administrator to take necessary decisions accordingly and it ensures availability and reliability of enterprise network.

For developing the unified monitoring tool one has to decide the critical areas and devices, parameters to be monitored as per the need of enterprise.

For this to happen the administrator must first subscribe those events for which it requires notification from the clients. These events are subscribed using temporary event subscription. After the connection is established between the clients and server, once the server subscribes events to the clients, it receives notifications from the client in real time.

3.1 System Design Principles

In this section we have described principles [4] considered in the development of the system - i) Support for remote client monitoring and control of resources by reading the remote client data in real time ii) Support for heterogeneous operating systems iii) Single central server for storage and retrival of comprehensive client data iv) To provide a graphical user interface for collecting and presenting the data collected from the clients v) Easy to use, easy to expand, low-cost, high-performance enterprise resourse management system.

3.2 Realization of Remote Management Function

The remote CPU is able to be operated in the same way as local computer. Remotely performance monitoring and client availability is done. The performance measurement parameters are CPU utilization, memory utilization, free disk space, new software installation, network adapters and OS patches, etc. These results which are monitored will be outputted to web-based graphical user interface using dynamic HTML technology.

3.3 Design Architecture

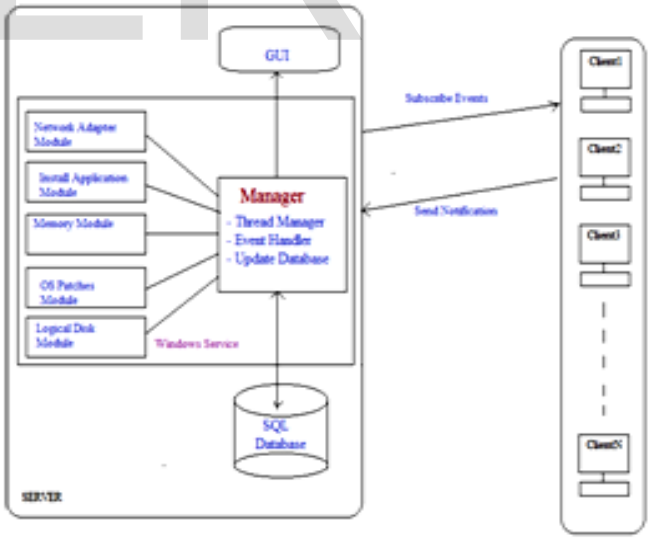


Fig. 2 System Architecture

The system architecture has following components-

Thread Manager - This is used to manage multiple clients connected in the network. These clients are having Windows operating system.

Event Handler - For handling events from the clients.

Update Database - For storing the client's data from the events in the Database.

The services are first initialize using COM components. In order to receive asynchronous event notifications, WMI calls the *ProvideEvents()* method to notify the provider to start providing event notifications. One of the arguments of this method is a pointer to the *IWbemObjectSink* interface that is used by the provider to forward its events to a consumer.
Then WMI registers its event handling code (represented by the *IWbemObjectSink* pointer) with a provider, so that the provider calls the *IWbemObjectSink::Indicate* method each time an event is triggered which enumerates class properties. At the same time, database is updated and notification is popped up in the GUI. The system is implemented using in Microsoft Visual C++ and HTML.
The collected data can be used for various purposes such as managing network, handling security, identifying potential issues with client systems, illegal activities and installation of any unauthorized applications.

3.4 Algorithm for Remote Monitoring

Following is the algorithm for connecting to the remote client for subscribing to events and receiving events notifications within seconds of occurrence.

Algorithm: Remote Monitoring

Input: Client Nodes {N1, N2, … Nn}
Events {e1,e2,…en}

Output: Parameters {p1,p2….pn}

1. Read the credentials of users for connecting to remote client. [i.e., Domain\Username, Password, and Full ClientComputer Name]
2. Send connection request to each client.
3. If Connection succeeded, execute WQL query for subscribing to events. When subscribed, WMI service checks for event locally.
4. Whenever an event has occurred; client notifies it to WMI at server, where event sink handles the response and enumerate the result array.
5. The result array is compared with the previous result stored in the database and notifies the change to the User.

The events for which notifications are required are mentioned in the Table 2. For event notifications, event subscription query is generated and sent to the target client. As and when events occur, they are notified to the server.

The flowchart for monitoring the network is shown in fig. 3.

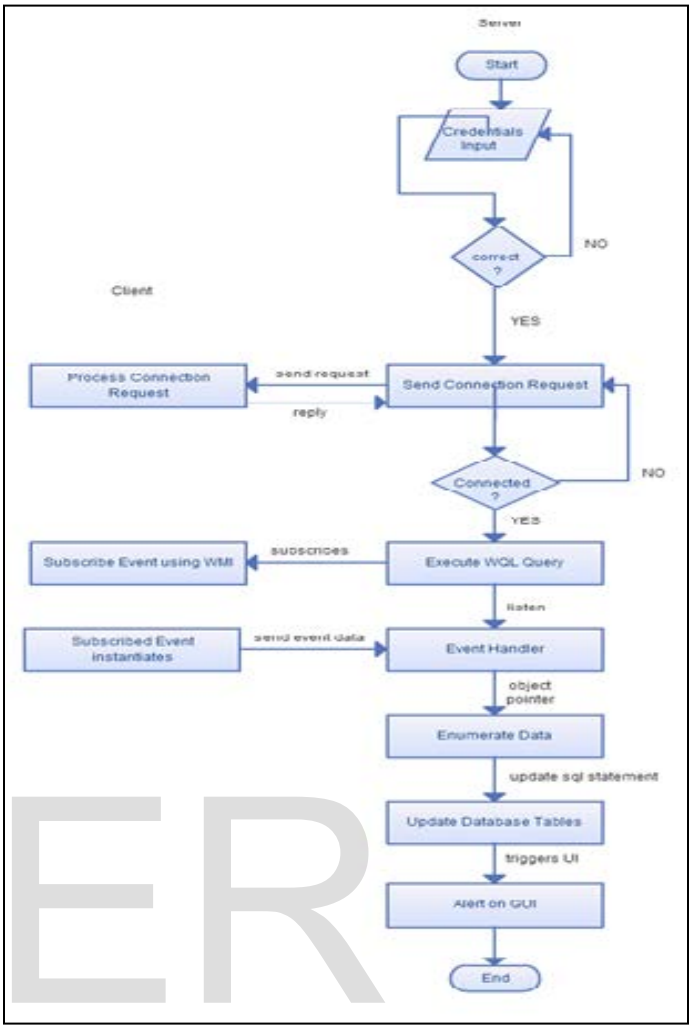


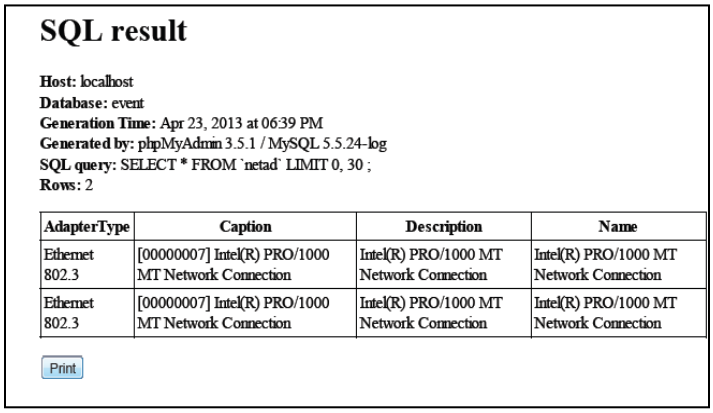
Fig. 3 Flowchart for Monitoring

TABLE 2
Event Notifications for Devices

Device Class	Event Parameters
Network Adapter - Win32_Network Adapter	Caption, AdapterSize, Availability, Time_Created, InstallDate, Network_Address, Status, ProductName, ServiceName, Change
Memory - Win32_PhysicalMemory	Caption, Capacity, BankLabel, DataWidth, Description, FormFactor, MemoryType, Model, PartNumber, Speed, Version, Change
Installed Applications - Win32_Product	Caption,Description,TimeCreated, InstallLocation, InstallSource, Name, PackageName, ProductID, RegCompany, Vendor, Version, Change
OS Patches - Win32_Patch	Caption, File, Patch Size, ProductCode, Sequence, TimeCreated, SettingID, Change
Logical Disk - Win32_LogicalDisk	Caption, Availability, Time_Created, BlockSize Access, DeviceID, DriveType, FileSystem, FreeSpace, Size, Change

4. RESULTS AND DISCUSSIONS

In this section we have discussed the results of our system, which shows the notifications received form the clients for changes happened. Fig. 4 shows events data received from client and is stored in database. Data includes information about Adapter Type, Caption, Description, name of the Network Adapter changes from Client. Similarly fig. 5 shows events received form clients it includes Caption, File System, Volume Name and what is the change in Logical Disk from Client.



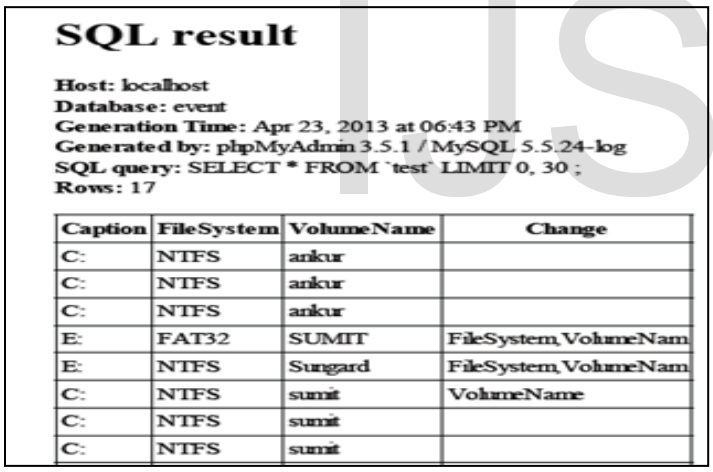
SQL result

Host: localhost
Database: event
Generation Time: Apr 23, 2013 at 06:39 PM
Generated by: phpMyAdmin 3.5.1 / MySQL 5.5.24-log
SQL query: SELECT * FROM `netad` LIMIT 0, 30 ;
Rows: 2

AdapterType	Caption	Description	Name
Ethernet 802.3	[00000007] Intel(R) PRO/1000 MT Network Connection	Intel(R) PRO/1000 MT Network Connection	Intel(R) PRO/1000 MT Network Connection
Ethernet 802.3	[00000007] Intel(R) PRO/1000 MT Network Connection	Intel(R) PRO/1000 MT Network Connection	Intel(R) PRO/1000 MT Network Connection

Print

Fig. 4 Network Adapter Update in Database at Server



SQL result

Host: localhost
Database: event
Generation Time: Apr 23, 2013 at 06:43 PM
Generated by: phpMyAdmin 3.5.1 / MySQL 5.5.24-log
SQL query: SELECT * FROM `test` LIMIT 0, 30 ;
Rows: 17

Caption	FileSystem	VolumeName	Change
C:	NTFS	ankur	
C:	NTFS	ankur	
C:	NTFS	ankur	
E:	FAT32	SUMIT	FileSystem,VolumeNam
E:	NTFS	Sungard	FileSystem,VolumeNam
C:	NTFS	sumit	VolumeName
C:	NTFS	sumit	
C:	NTFS	sumit	

Fig. 5 Logical Disk Update in Database at Server

5. CONCLUSION AND FUTURE WORK

We have developed a monitoring service that will change the current monitoring techniques used in the enterprise monitoring. This system is helpful in pulling event notifications from remote clients in real time. It also monitors the infrastructure of the enterprise and generates necessary notifications periodically based on request. The developed system will be very useful to the administrator without any significant overheads on network traffic because of its angentless nature. This system can be used for-

i) Detection of failures in the functioning of complex enterprise networks.
ii) The collected information can be used for health monitoring of enterprise networks.
iii) The information can be used to create virtual environment and backup of the workspace in case of disaster recovery.
iv) This service helps in managing enterprise resources and making informed decisions by the administrator as well as manager.

As a part of the future work the system can be extended for non Windows OS. The modified and extended version of this system can be used for the replication and creating a virtual machines.

6. ACKNOWLEDGMENTS

I would like to thank Dr.Maitreya Natu from TRDDC, Pune for guiding me. I thank Dr. L. K. Kshirsagar, Principal, MIT Pune for helping me to publish this paper.

REFERENCES

[1] Patricio Domingues, Paulo Marques, Luis Silva ESTG, "Resource Usage of Windows Computer Laboratories" – Leiria, Portugal Univ. Coimbra, Portugal Univ. Coimbra – Portugal

[2] Matt Schnaidt ,Debra Hensgen, John Falby, Taylor Kidd, David St. John, "Passive, Domain-Independent, End-to-End Message Passing Performance Monitoring to Support Adaptive Applications in MSHN" Computer Science Department Naval Postgraduate School Monterey, CA 93943-5118

[3] Ammu Qudsiya, "Modeling Performance Monitoring Of It Infrastructure Components Using Timed Petri Nets". A* – Research Scholar, Department of Mathematics, Mother Theresa Women's University, Kodaikanal, India. Indian Journal of Computer Science and Engineering (IJCSE)

[4] Hui Peng and Yao Wang, "WMIC Realize Enterprise Remote Information Management ", Second Pacific-Asia Conference on Circuits, Communications and System (PACCS) -2010

[5] Genevieve Bartlett, John Heidemann, Christos Papadopoulos, "Understanding Passive and Active Service Discovery" http://www.sigcomm.org/events/sigcomm-conference

[6] Antonis Papadogiannakis, Demetres Antoniades, Michalis Polychronakis, and Evangelos P. Markatos, "Improving the Performance of Passive Network" www.ist-lobster.org/publications/papers

[7] Martin Friedrich, " Making WMI Queries in C++ ", www.codeproject.com

[8] http://msdn.microsoft.com.len-us/default.aspx

[9] http://www.paessler.com/prtg

[10] http://www.ipswitch.com/

[11] http://technet.microsoft.com/