# Application Scanning and Ipv6 Assessment For MS-SQL Server

Shivi Garg
Information Systems
Delhi Technological University
Delhi, India
shivi1989@gmail.com

Manoj Kumar
Computer Engineering
Delhi Technological University
Delhi, India
mkg1109@rediffmail.com

***Abstract*—This paper attempts to present a solution that allows the users to scan the remote host machine on a network and to assess IPv6 enablement for MS-SQL. It aims to detect the hardware and the software installed on that machine. This goal is achieved by the use of Windows Application Programming Interface (API) through Windows Management Instrumentation (WMI) Scripts which handles the registry. WMI Scripts are used to connect to the registry of a remote host machine that reads the installed path of the software and hardware details of that machine. First, it will detect the underlying Operating System whether it can support IPv6 or not. If the underlying operating system can support IPv6, then only applications running on it can run on IPv6 enabled network. So for this the system also assesses the IPv6 enablement of MS-SQL Server.**

***Index Terms*—IPv6, API, WMI, MS-SQL**

## I. Introduction

In Microsoft Windows operating systems, an Application Programming Interface (API) defines the software in terms of its operations, inputs, outputs and underlying types. The main purpose of an API is to specify how different software components should interact with each other. It defines a set of functionalities that are independent of their respective implementation, thus allowing both definitions and implementation to vary without compromising each other [1]. The various functionalities provided by API can be divided into eight categories like- Security, Base Services, Graphics, User Interface, Multimedia, Windows Shell and Networking.

The Windows Registry is a hierarchical database. It stores configuration settings for systems, users, applications, hardware, and lot more different parameters. It contains settings for low-level operating system components and for applications processing on the platform that have opted to use the registry [2]. WMI Scripts are used to connect to the registry of a remote host machine, and reads the installed path of the software and hardware details of the machine. This application also assesses the IPv6 Enablement of MS-SQL Server. If the current version of MS-SQL is equal or higher than the minimum version supporting IPv6 then it needs to be checked for the IPv6 Enablement.

## II. WMI Scripts

Windows Management Instrumentation (WMI) helps to obtain information on how an Operating System operates, i.e. it gives an administrator a means to extract information about all aspects of an OS, and so we can consider WMI as [3]:

- A database that keeps information regarding system's disk, services, processor, and objects.
- A way to automate collection of data for hardware and software.
- A channel that interconnects various inner secrets of the Microsoft OS.
- A unique dialect of Visual Basic script (VBS) with its own WMI Query Language (WQL).
- An instrument that can be used to identify the properties of an operating system.

Windows Management Instrumentation (WMI) is the structure for management data and operations on Windows based operating systems. WMI Scripts can be written or can be applied to automate administrative tasks on remote computers, but WMI also provides management data to other parts of the operating system and products, for e.g. System Center Operations Manager, formerly known as Microsoft Operations Manager (MOM), or Windows Remote Management [4]. The major function of WMI is to describe a proprietary set of environment-independent specifications that allow management information to be shared between various management applications. WMI prescribes enterprise management standards and associated technologies for Windows that work with existing management standards, such as Desktop Management Interface (DMI) and SNMP. WMI supplements these standards by providing a uniform model. This model represents an environment through which management data can be accessed from any source in a common way [5].

Once the Operating System version which supports IPv6 is known, then hardware and software list is generated running on the host machine in a network. The minimum version of operating system to support IPv6 is Windows XP (SP2). Once all the software along with all the details are listed we need to look for MS-SQL for IPv6 assessment. If MS-SQL is installed, then we will check for its enablement.

## III. Migration from IPv4 to IPv6

The numbering space of IPv4 is very limited. Due to fast depletion rate of IPv4 Addresses there is a need to migrate towards IPv6. IPv6 has more numbering space and it also has other advantages over IPv4. IPv6 traffic on the Internet is still less than 1% of total traffic [6]. It provides End-to-End connectivity by eliminating the need for NAT hence resulting

IRJECE

in better connectivity in peer-to-peer networks. IPv6 provides interoperability between different IPv6 implementations [7].

## IV. Proposed System

This System checks the enablement of MS-SQL for IPv6. If the current version of MS-SQL installed on remote host machine is equal or higher than the IPv6_minimum_version then it needs to be checked for the IPv6 Enablement. The minimum version of MS-SQL which supports IPv6 is MS-SQL server 2005[8].

### *A. Abbreviations and Acronyms*

IPv6: Internet Protocol Version 6
API: Application Programming Interface
WMI: Windows Management Instrumentation
MS-SQL: Microsoft SQL Server

## V. Embedding Algorithm

i. In this WMI script is made to run on the remote host machine so as to provide the hardware and the software listings installed on that machine.
ii. Check for the operating system version installed.
iii. If the operating system is higher than the windows XP (i.e. the minimum OS version to support IPv6), then check for the installed software applications.
iv. Check for the MS-SQL application.
v. If the current version of MS-SQL installed on the remote host machine is equivalent to or is higher than the IPv6_minimum_version then it needs to be checked for the IPv6 enablement. Else it does not support IPv6.
vi. For MS-SQL IPv6 enablement, installed registry path needs to be read.
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MicrosoftSQLServer\MS-SQL10.SQLEXPRESS\MS-SQLServer\SuperSocketNetLib\Tcp.
vii. In the TCP, check for the parameter "Enabled". If "Enabled" is 0, then it is IPv6 disabled.
viii. Else if it's 1, check for "ListenOnAllIPs", if its value is 1, then it is IPv6 enabled, If not, Check for all IP's one by one.

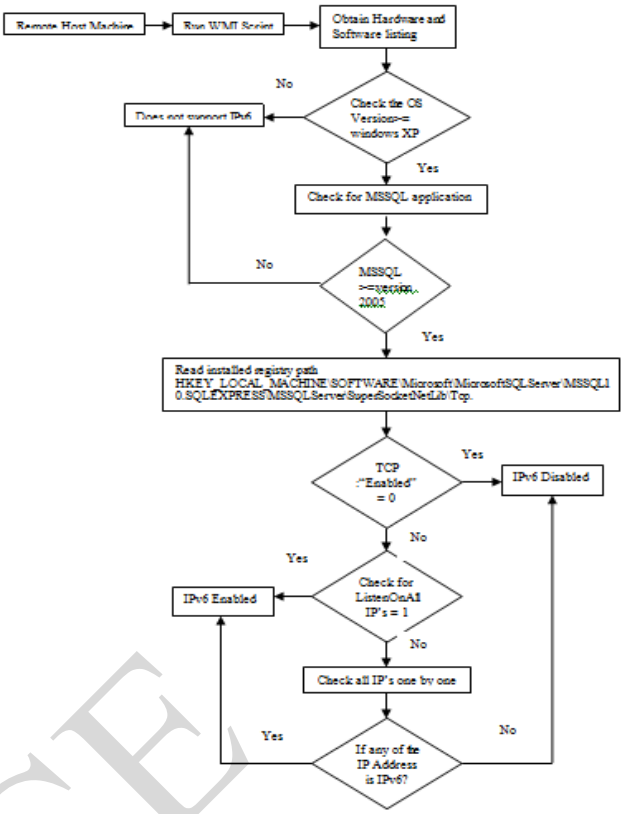



Fig. 1: Flowchart of Proposed Scheme

## VI. Research and Analysis

### *A. Input File*

An input file "InputFile.txt" is made with IP Address of the host machine, which is to be scanned on the first line. The second line contains the name of host machine. Figure 2 shows the "InputFile.txt" where first line indicates the IP Address of the host machine. Here, we are scanning on the local host. And second line indicates the User Name.

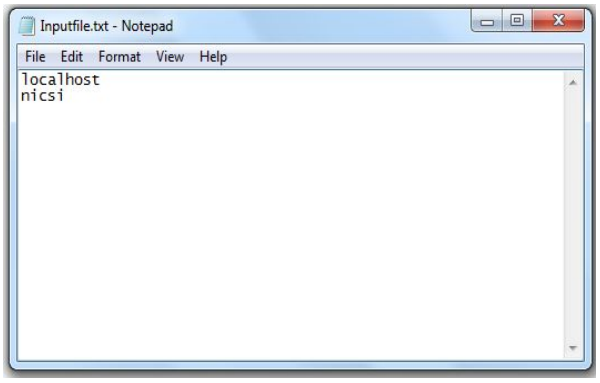



Fig. 2: InputFile.Txt showing IP Address and User Name

### *B. Operating System Version:*

WMI script is made to run on the remote host machine to get the hardware and the software listing installed on that machine. Operating System Version is checked for the IPv6 compatibility. OS is Windows 7 Professional 6.1, so it is

IRJECE

IPv6 compatible. The minimum version of Operating system which supports IPv6 is Windows XP service pack 2. Previous versions of Windows OS provide a limited support for IPv6 [9]. Figure 3 shows the Hardware Listing of remote host machine and the OS Version.

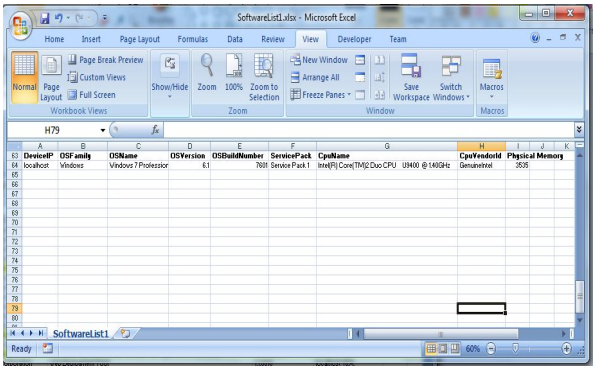


Fig. 3: Operating System Version for IPv6 Compatibility

*C. Software Listing:*

If the known version of Operating System is IPv6 compatible, then software listing installed on that machine is obtained and MS-SQL server is looked for. If the current version of MS-SQL installed on the remote host machine is equivalent or higher than the IPv6_minimum_version then it needs to be checked for the IPv6 Enablement. Else it does not support IPv6. Software Listing is shown in the Fig. 4.

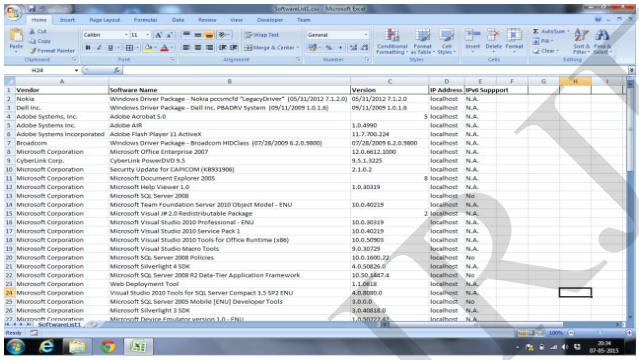


Fig. 4: Software Listing Obtained For The Remote Host Machine

Here, the current version of MS-SQL Server appears to be 2008, which is greater than the IPv6_minimum_version. Hence, now it is checked for the IPv6 Enablement.

*D. MS-SQL IPv6 Assessment:*

For MS-SQL IPv6 Enablement, installed Registry path needs to be read HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MicrosoftSQLServer\MS-SQL10.SQLEXPRESS\MS-SQLServer\SuperSocketNetLib\Tcp. In the TCP, we check for the parameter "Enabled". If Enabled is 0, then it is IPv6 Disabled. Figure 5 shows that Enabled parameter is 0, hence IPv6 is disabled.

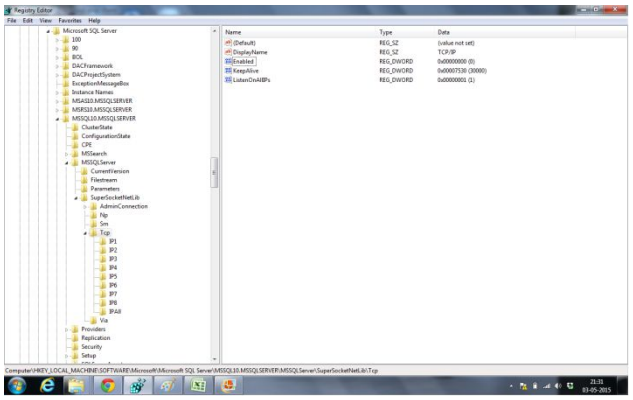


Fig. 5: 'Enabled' parameter is 0, showing IPv6 is disabled

If 'Enabled' parameter is set to, then we check for "ListenOnAllIPs" [10]. If its value is set to 1, then it is IPv6 enabled. Figure 6 shows IPv6 Enablement.

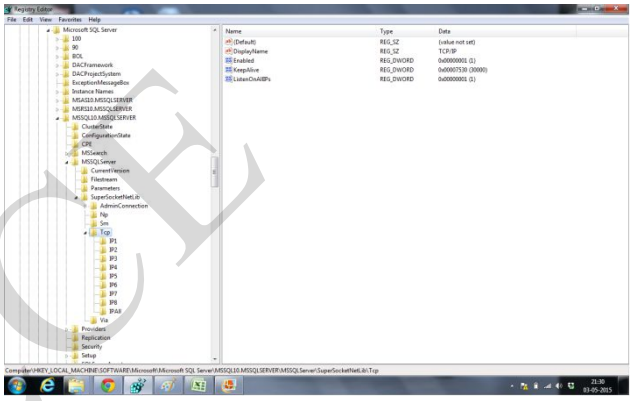


Fig. 6: Listenonallips Parameter Set To 1, Showing Ipv6 Is Enabled

If "ListenOnAllIPs "parameter is set to 0, then we have to check individual IPs separately. If we found any of IPv6 address, then it is IPv6 enabled else it is not. Figure 7 shows that the parameter "ListenOnAllIPs" is set to 0 and Figure 8 shows the verification of each individual IP Address as IPv6.

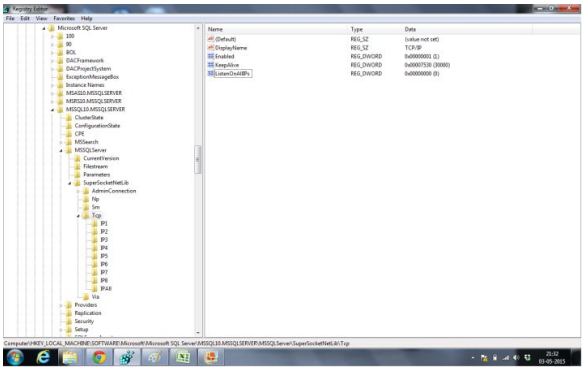


Fig. 7: Listenonallips Parameter Set To 0

IRJECE

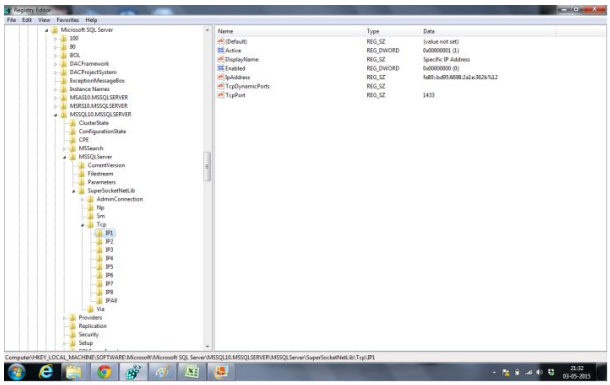


Fig. 8: Checking individual IPs for IPv6 Address

## VII. Conclusion

The proposed scheme is robust to all the other applications like MySQL. In this minimum version of operating system should be known which supports IPv6. If OS supports IPv6, then it will support all the underlying IPv6 applications. If MS-SQL is in installed list, it is assessed for the IPv6 enablement if it's higher than the minimum IPv6 version. MS-SQL assessment for IPv6 helps to port these database applications on the IPv6 network due to faster depletion of IPv4 addresses.

## Acknowledgment

This research was supported/partially supported by my co-author Mr. Manoj Kumar. We thank Dr. O.P. Verma, Head of the Department (HOD) of Information Technology (IT) department for assistance with database knowledge, and for comments that greatly improved the manuscript.

## References

[1] Wikimedia Foundation Inc. Wikipedia "Application Programming Interface", "http://en.wikipedia.org/wiki/Application_programming_interface"

[2] Pragati Pawar, P.S. Kulkarni, "Security for windows registry using carving," vol. 3, issue 4, April 2013.

[3] Julius Dizon, Lennard Galang and Marvin Cruz "Understanding WMI Malware", July 2010.

[4] Windows Management Instrumentation "https://msdn.microsoft.com/en-us/library/aa394582 (v=vs.85).aspx".

[5] Wikimedia Foundation Inc. Wikipedia "Windows Management Instrumentation", "http://en.wikipedia.org/wiki/Windows_Management_Instrumentation".

[6] Henten, Anders, Tadayoni and Reza, "Transition from IPv4 to IPv6," in European Regional ITS, 2012.

[7] Palukuru Venkata Praneeth Reddy, Kavali Mohammed Imran Ali, B. Sandeep and T.Ravi, "Importance and benefits of IPV6 over IPV4: A Study", vol 2, issue 12, Dec, 2012.

[8] IPv6 and SQL Server 2005, "https://blogs.msdn.microsoft.com/sql_protocols/2005/10/12/ipv6-and-sql-server-2005/".

[9] IPv6 support in Microsoft windows, "http://www.windowsnetworking.com/articles-tutorials/network-protocols/IPv6-Support-Microsoft-Windows.html".

[10] What IPs are you listening on SQL, "http://troubleshootingsql.com/2012/01/30/what-ip-are-you-listening-on-sql/".

IRJECE