Informant Systems, Inc.

Informant Systems, Inc.
11135-23A Avenue
Edmonton, AB   T6J4W5   Canada
p: 780.908.6669   f: 780.434.8991
www.informant-systems.com

SNMP Informant™

SNMP Informant, the default Microsoft SNMP extension agents and WMI

SNMP
Informant
"GET more out of Windows!"
Windows SNMP support for industry standard Network Management Systems
www.snmp-informant.com

Copyright

Restricted Rights Legend

Information in this document is subject to change without notice and does not represent a commitment on the part of Informant Systems. THE SOFTWARE AND DOCUMENTATION ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND INCLUDING WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. FURTHER, INFORMANT SYSTEMS DOES NOT WARRANT, GUARANTEE, OR MAKE ANY REPRESENTATIONS REGARDING THE USE, OR THE RESULTS OF THE USE, OF THE SOFTWARE OR WRITTEN MATERIAL IN TERMS OF CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE.

Informant Systems may make changes to specifications and product descriptions at any time, without notice.

Trademarks or Service Marks

Document Information

Version	Last Updated	Author	Edit Notes
1.0	February 27, 2016	GKW	Prepare document

Table of Contents

Table of Figures

About This Document

This short document describes the MS SNMP service, the SNMP extension agents included with a default SNMP service installation, how they differ from the SNMP Informant extension agents, and why you would want to use the SNMP Informant extension agents instead of or in addition to the default MS extension agents. It also discusses the Microsoft WMI (Windows Management Instrumentation) protocol, and how SNMP Informant bridges SNMP and WMI.

Brief SNMP Technical Overview

SNMP is the most popular network management protocol in the TCP/IP protocol suite. It is a simple request/response protocol that communicates management information between two types of SNMP software entities: SNMP applications (also called SNMP managers) and SNMP agents.

SNMP messages are based on the UDP (User Datagram Protocol), which is a fast, connectionless transport protocol. It is embedded within an IP packet within an Ethernet frame.

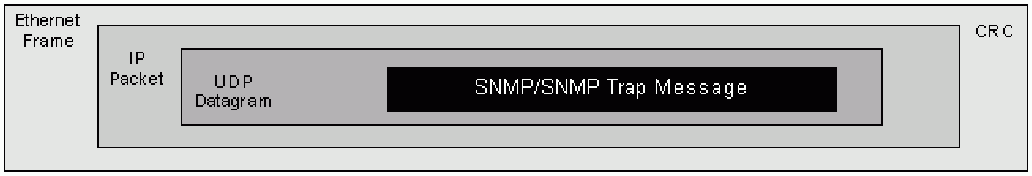

Figure 1: The SNMP UDP Packet

The Microsoft-Windows-SNMP-Agent-Service component (also called a “stack”) runs in a Windows OS enables Simple Network Management Protocol (SNMP) requests to be processed by the computer. The service (SNMP.EXE) receives the SNMP requests from the network, decodes them, and then dispatches them to the appropriate SNMP subagent (somename.dll). Microsoft provides several different subagents when the SNMP service is installed. These subagents are also called “extension agents”.

The SNMP Informant product line consists of several such extension agents.

Component Name	Associated Programs	Component Type	Description
Microsoft SNMP Service (also called a stack, a master agent or extendible agent)	Snmp.exe	Agent	Receives SNMP requests and delivers them to the appropriate SNMP subagent DLL for processing. The service is also responsible for intercepting events (traps) from the SNMP subagents and forwarding trap messages to the appropriate management systems.
SNMP Subagents (also called extension agents)	Lmmib2.dll, Inetmib1.dll, and others *(including SNMP Informant extension agents)*	Agent	Provides a set of entry points. When an SNMP request is received, the SNMP service delivers it to the appropriate subagent by calling one of these entry points. After the subagent processes the message, it passes the information back to the SNMP service, which then forwards the message to the SNMP manager.

How does SNMP Informant work?

SNMP Informant is installed on a Windows server after the Microsoft SNMP service is installed and configured. As mentioned, SNMP Informant products are SNMP extension agents. Once SNMP Informant is installed, the SNMP Informant MIBS are copied to the Network Management System where they are used by the management application.

- *MIB (Management Information Base) files are "translation" files that cross references numeric OIDs (Object Identifiers) and target data types.*

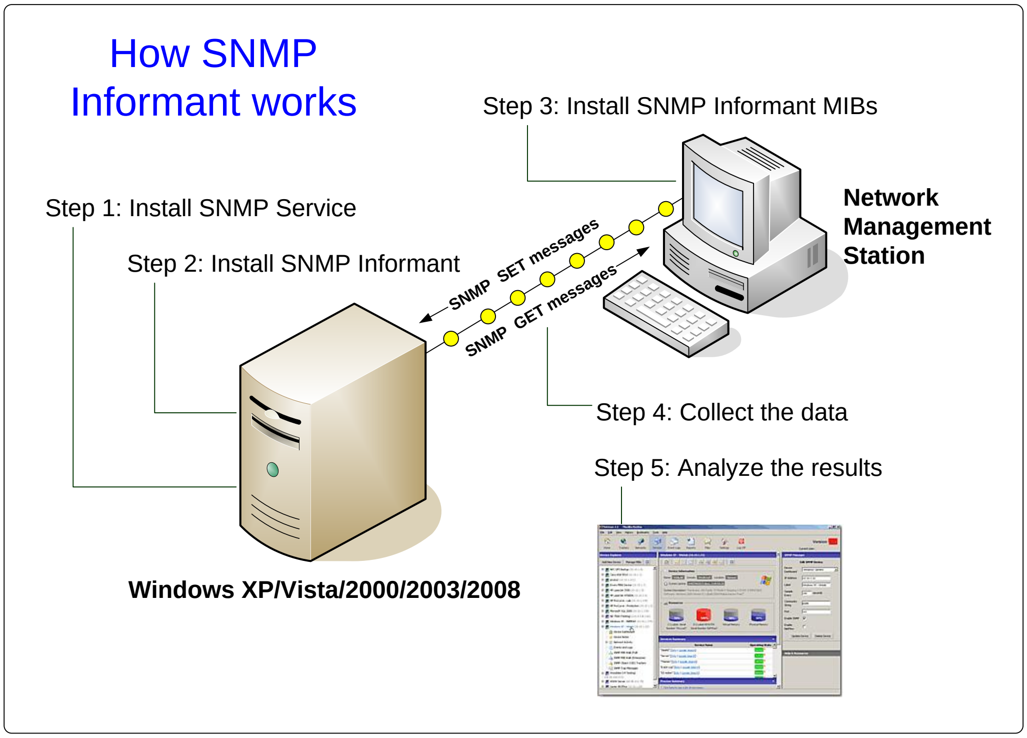
How SNMP Informant works
Step 3: Install SNMP Informant MIBs
Network Management Station
Step 1: Install SNMP Service
Step 2: Install SNMP Informant
SNMP SET messages
SNMP GET messages
Step 4: Collect the data
Step 5: Analyze the results
Windows XP/Vista/2000/2003/2008

Figure 2: SNMP Informant functional overview

Once SNMP Informant is installed on a server running the Microsoft SNMP service, no additional work is required to configure the product.

- *If the SNMP Informant-Exchange product is installed, then during installation, the Administrator is required to enter the name/password of an Exchange Management service account so that it can connect to the local Exchange WMI provider.*

Default Microsoft SNMP Extension Agents

As mentioned, when the Microsoft SNMP service is installed, it includes many extension agents, which provide information about various sub-systems within the host server. The following table identifies these default extension agents, and describes them (including a reference to the RFC document ID.

- Note how many of the 21 MS extension agents either have a dependency on the Routing and Remote Access service (8), or are otherwise network-oriented, and are not server performance based.

Extension agent (DLL) and MIB FILE	Description	Object Identifier	RFC	Dependency
acsmib.dll ACS.MIB	Microsoft-defined MIB for the Quality of Service Admission Control Service (QoS ACS)	1.3.6.1.4.1.311.1.15	(None)	(None)
iasperf.dll ACCSERV.MIB	RADIUS-ACC-Server-MIB contains object-types for monitoring accounting information between a network access server and a shared accounting server.	1.3.6.1.3.79	2139	Internet Authentication Service
iasperf.dll AUTHSERV.MIB	RADIUS-AUTH-Server-MIB contains object-types for monitoring authentication, authorization, and configuration information of a network access server.	1.3.6.1.3.79	2138	Internet Authentication Service
dhcpmib.dll DHCP.MIB	Microsoft-defined MIB contains object-types for monitoring the network traffic between remote hosts and the DHCP server.	1.3.6.1.4.1.311.1.3	(None)	DHCP service
ftpmib.dll FTP.MIB	Microsoft-defined MIB contains object-types for monitoring the File Transfer Protocol (FTP) service.	1.3.6.1.4.1.311.1.7.2	(None)	IIS Server
hostmib.dll HOSTMIB.MIB	Contains object-types for monitoring and managing host resources.	1.3.6.1.2.1.25	1514	(None)
httpmib.dll HTTP.MIB	Microsoft-defined MIB for the Hypertext Transfer Protocol (HTTP) service	1.3.6.1.4.1.311.1.7.3	(None)	IIS Server
igmpagnt.dll IGMPV2.MIB	Collects information on what groups are joined on the subnet.	1.3.6.1.359	(None)	Routing and Remote Access service

Extension agent (DLL) and MIB FILE	Description	Object Identifier	RFC	Dependency
inetmib1.dll IPFORWD.MIB	Defines objects for managing routes on the IP Internet.	1.3.6.1.2.1.2	1354 2096	(None)
lmmib2.dll LMMIB2.MIB	LAN Manager MIB-II covers workstation and server services.	1.3.6.1.4.1.77.1	(None)	(None)
mcastmib.dll MCASTMIB.MIB	MIB module for managing IP Multicast routing	1.3.6.1.3.60.1.1	(Pending)	Routing and Remote Access service
intermib1.dll MIB_II.MIB	Management Information Base (MIB-II) provides a simple, workable architecture and system for managing TCP/IP-based internets.	1.3.6.1.2.1.1 1.3.6.1.2.1.2 1.3.6.1.2.1.4 1.3.6.1.2.1.5 1.3.6.1.2.1.6 1.3.6.1.2.1.7	1213	(None)
snmpmib.dll MIB_II.MIB	Management Information Base (MIB-II) provides a simple, workable architecture and system for managing TCP/IP-based internets.	1.3.6.1.2.1.11	1213	(None)
rtipxmib.dll MIPX.MIB	Microsoft-defined MIB for the Internetwork Packet Exchange (IPX) Protocol	1.3.6.1.4.1.311.1.8	(None)	Routing and Remote Access service
rtipxmib.dll MRIPSAP.MIB	Microsoft-defined MIB for the Routing Information Protocol (RIP)	1.3.6.1.4.1.311.1.9	(None)	Routing and Remote Access service
btpagnt.dll MSIPBTP.MIB	Microsoft-defined MIB for the Boot Protocol (BOOTP) service	1.3.6.1.4.1.311.1.12	(None)	Routing and Remote Access service
ripagnt.dll MSIPRIP2.MIB	Microsoft-defined MIB for the Routing Information Protocol version 2 (RIP2)	1.3.6.1.4.1.311.1.11	(None)	Routing and Remote Access service
rtipxmib.dll NIPX.MIB	Novell-defined MIB for the IPX Protocol	1.3.6.1.4.1.23.2.5	(None)	Routing and Remote Access service

Extension agent (DLL) and MIB FILE	Description	Object Identifier	RFC	Dependency
(No .dll) SMI.MIB	Provides the common definitions for the structure and identification of management information for TCP/IP-based internets.	(No object identifier available)	1155 1215 1902 1903 1904	(None)
ospfagnt.dll WFOSPF.MIB	Nortel Networks–defined MIB for the Open Shortest Path First (OSPF) routing	1.3.6.1.4.1.18	(None)	Routing and Remote Access service
winsmib.dll WINS.MIB	Microsoft-defined MIB for the Windows Internet Name Service (WINS)	1.3.6.1.4.1.311.1.2	(None)	WINS

SNMP Informant vs. the Default MS SNMP extension agents

While the SNMP support provided by Microsoft has improved substantially over the past few years, it still has limitations. The different MS extension agent DLLs installed with the SNMP service provide information on several specific subsystems, but **no MS SNMP extension agent provides access to the performance counter subsystem.**

SNMP Informant's Performance Provider product line accepts incoming SNMP messages, decodes them (determines what performance counter object is being asked for), then gets the data from the performance counter subsystem, and returns it to the system making the request.

Figure 1 on the following page show how SNMP Informant bridges SNMP and the Performance counter subsystem on the host server.

It is important to note that no modifications need to be made to the host SNMP service to support SNMP Informant.

Figure 2 is a more technical diagram showing how SNMP Informant integrates with the Microsoft SNMP stack.

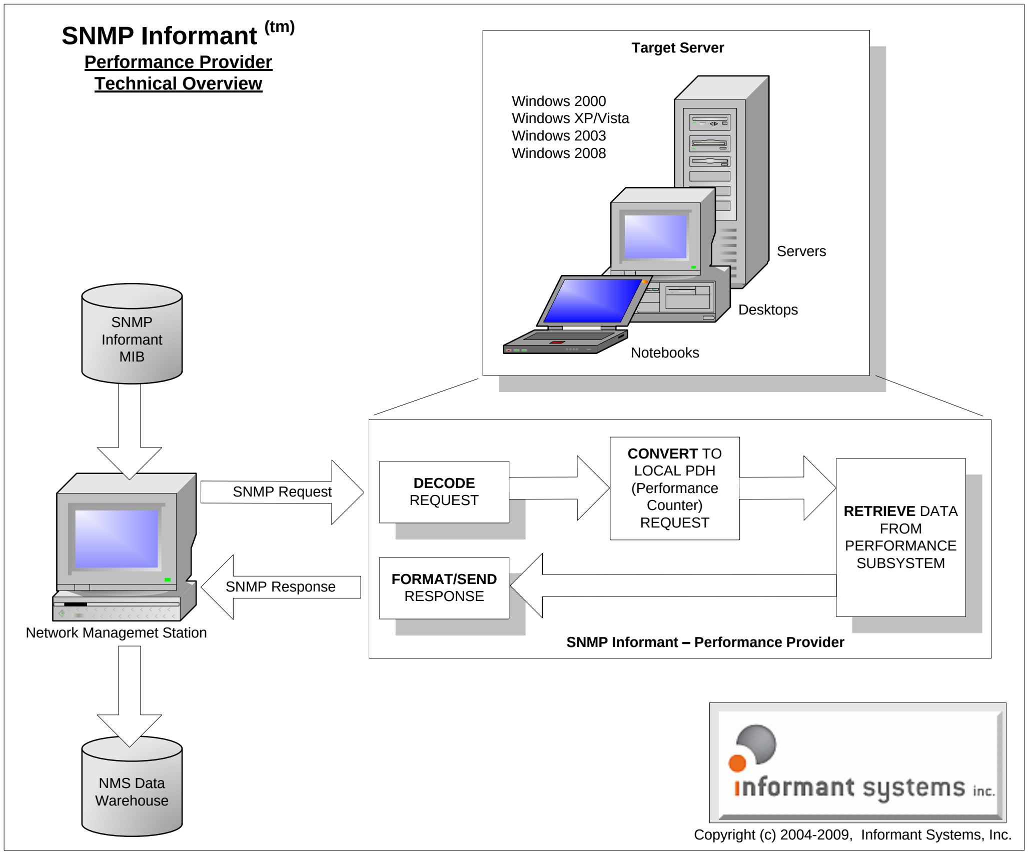

Figure 3: How SNMP Informant collects performance information

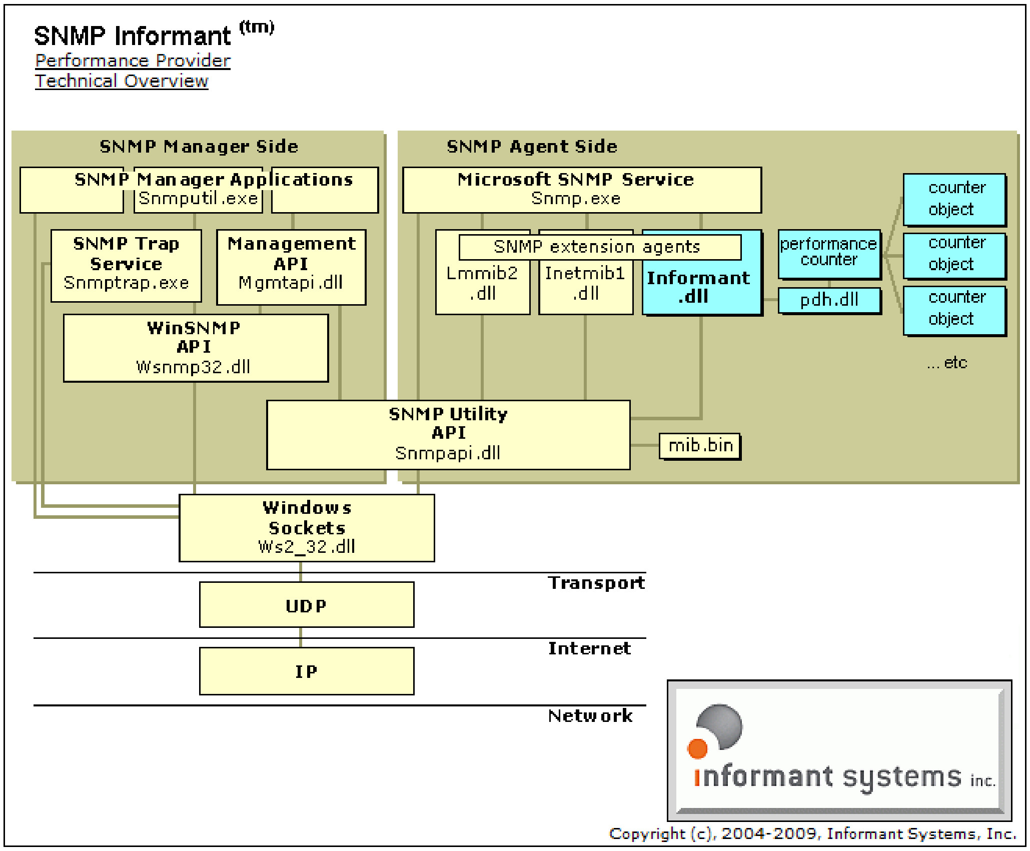

Figure 4: How SNMP Informant hooks into the Performance Subsystem

What about WMI?

WMI, or Windows Management Instrumentation is a proprietary Microsoft technology which allows Windows systems to connect to other Windows systems and collect an extensive amount of system configuration and state information as well as performance data.

One of the problems with WMI though, is that if you are running a Network Management System that is NOT Windows-based, then you can't collect WMI data from a remote Windows Server.

Plus, the WMI protocol is inherently slower than SNMP and requires Windows authentication. WMI also requires several ports to be opened up between the Network Management System and the target server. SNMP on the other hand, requires a single port (UDP 162).

The description below comes from the Zenoss FAQ, answering the question "What Ports does WMI use?"

- http://www.zenoss.com/community/docs/faqs/faq-english#WhatportsdoesWMIuse

> "WMI uses DCOM to communicate
>
> DCOM information from the Microsoft site...
>
> **Firewall and Registry Settings for DCOM**
>
> DCOM dynamically allocates one port per process. You need to decide how many ports you want to allocate to DCOM processes, which is equivalent to the number of simultaneous DCOM processes through the firewall. You must open all of the UDP and TCP ports corresponding to the port numbers you choose. You also need to open TCP/UDP 135, which is used for RPC End Point Mapping, among other things. In addition, you must edit the registry to tell DCOM which ports you reserved."

SNMP Informant's WMI Provider product line accepts incoming SNMP messages, decodes them (determines what WMI class/object is being referenced), then gets the data from the WMI CIM (Common Information Model) database and returns it to the system making the request.

Importantly, SNMP Informant allows you to collect Windows WMI data from a non Windows system (i.e. Linux or Unix) using SNMP.

Further, since SNMP Informant WMI Providers are SNMP to WMI "bridges", they do not require the authentication of a native WMI request.

In addition to providing a plethora of WMI data through SNMP GET commands, the SNMP Informant WMI-OS provider allows the NMS to send SET request messages to:

- ***Start, stop and pause Windows services***
    - ***Service state can be gathered through SNMP GET commands***
- ***Spawn remote programs and scripts***
- ***Initiate server reboots***

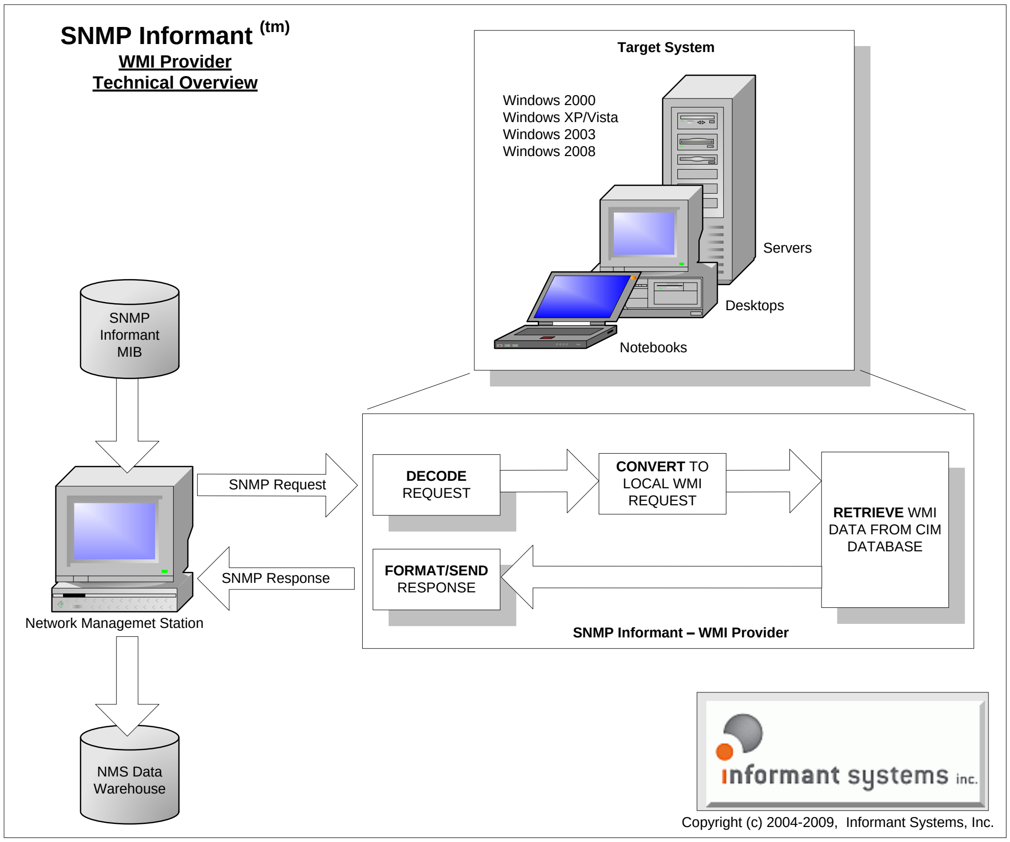

Figure 5: How SNMP Informant collects WMI information

Why Use SNMP Informant?

In summary: ***The pre-installed MS extension agents are neither performance nor WMI agents, and are thus incapable of accessing performance counter or WMI class information. Neither can they control windows services or the server itself.***

Monitor System and Server Performance

When you install a Microsoft server product such Exchange, or SQL Server (or others like BizTalk Server and ISA Server), they will extend the performance counter subsystem by adding many additional performance objects and instances. You can see this for yourself by starting Performance Monitor (start/run/perfmon) and looking at the performance counters of a server *without* MS Exchange or SQL Server installed, then installing Exchange or SQL Server and running Performance Monitor again.

- ***The Microsoft SNMP extension agents will not allow access to this performance information.*** **SNMP Informant will.** In fact, SNMP Informant Performance providers allow you to use SNMP to access performance counter information for virtually every object and instance supported by a variety of Windows operating systems (XP/Vista/2000/2003/2008) and many Microsoft server products. There are over 4000 data points in the SNMP Informant-Advanced product alone! SNMP Informant also supports access to Citrix Presentation Server performance counters as part of the SNMP Informant-Citrix product.

- ***Translating Microsoft SNMP extension agent OIDs into equivalent performance counter objects can be difficult.*** **SNMP Informant OIDs can be directly translated to an equivalent performance counter.** *Many Microsoft troubleshooting white papers reference tracking performance counter objects and* instances. This is easy with SNMP Informant.

Collect Configuration and State Information

- ***Microsoft SNMP agents do not support collection of WMI data.*** **SNMP Informant does.** SNMP Informant WMI providers include support for the Microsoft operating system and hardware (good for ITIL CMDB population), Exchange 2003, Virtual Server and Hyper-V. Recently, with the release of the SNMP Informant-Citrix product, SNMP can now be used to extract Citrix Presentation Server WMI information.

Control your Windows Servers

- ***Microsoft SNMP extension agents do not support service control.*** **SNMP Informant does.** You can use SNMP Informant WMI providers to monitor and control Windows processes using SNMP. Start, stop or pause services. Spawn remote scripts, reboot servers. This can all be done with SNMP Informant (using SNMP SET commands).

Monitor MS Cluster Server and Citrix using SNMP

- ***Microsoft SNMP extension agents do not support monitoring Microsoft Cluster Services.*** **SNMP Informant does.** The SNMP Informant-Cluster product allows you to use SNMP to monitor your Microsoft Cluster server infrastructure.

- ***Microsoft SNMP extension agents do not support monitoring Citrix Presentation Server.*** **SNMP Informant does.** Recently released, the SNMP Informant-Citrix product allows you to use SNMP to monitor Citrix Presentation Server performance counters and WMI objects.

Product Maintenance and Product Development

- Informant Systems, Inc. is continuously improving SNMP Informant, and regularly adding support for other Microsoft and relevant server products.

About Informant Systems, Inc.

Informant Systems has been developing and providing the network management community with cost-effective SNMP extension agents for Windows operating systems and server applications since 1999. Our flagship product, SNMP Informant™ is in use by small, medium and large organizations around the world, including Universities, financial institutions, Fortune 500 companies and large multi-national organizations.

Informant Systems, Inc.

Informant Systems, Inc.
11135 – 23A Avenue
Edmonton, AB T6J4W5 Canada
Phone: 780-908-6669
Fax: 780-434-8991
Web: http://www.informant-systems.com

Product Information: product.info@informant-systems.com
Product Support: product.support@informant-systems.com

Primary Contact: **Garth K. Williams – President and Managing Director**
garth.williams@informant-systems.com