HP Insight Management WBEM Providers

Dan Weiland

ISS SW Product Marketing

June 16, 2008

get connected PEOPLE. TECHNOLOGY. SOLUTIONS.

HP Technology Forum & Expo 2008

Produced in cooperation with: encompass ITUG

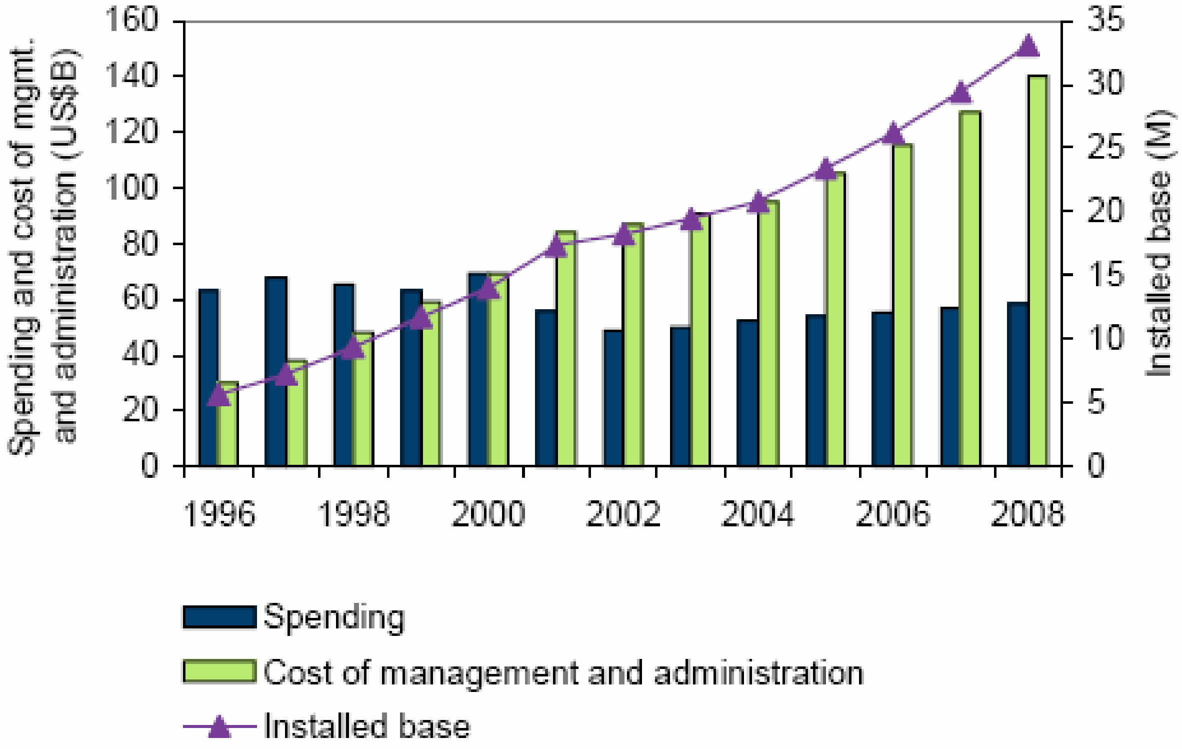
Agenda

- Customer Needs
- HP's Management Direction
  - Management Standards
  - Positioning
  - Benefits
  - Architecture overview
  - HP WBEM Providers overview
  - Deployment methods
  - Dependencies
  - Need to know
  - Usages Scenario
- Roadmap
- Conclusion

Voice of the Customer

Effective systems management is critically important…

Worldwide Server Spending, Cost of Server Management and Administration, and Server Unit Installed Base, 1996–2008

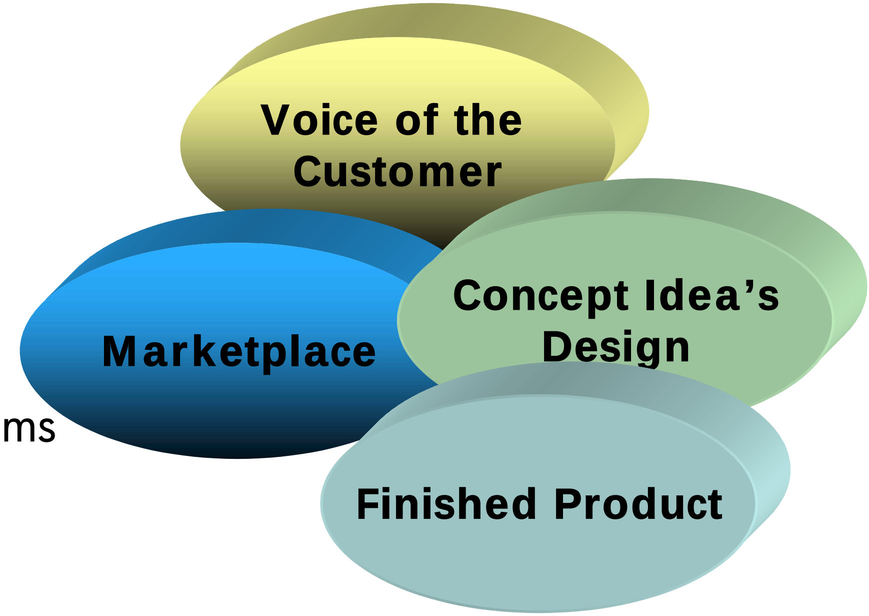


Systems management tools are designed to help reduce the costs of management and administration.

Source: IDC, 2004

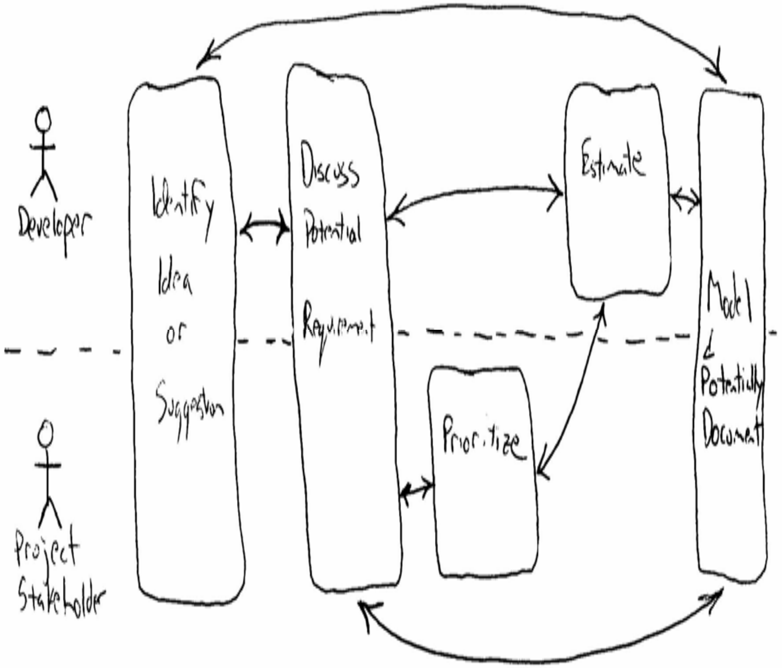
Voice of the Customer
Challenges

- Insecure legacy management protocols (SNMP)
- High cost of deploying, using and maintaining disparate management infrastructure on heterogeneous systems.
- Too many tools to perform commodity functions that fail to interoperate.
- Concern about performance impact of management agents and providers on systems being managed.
- Concern about the reliability of information
- Unable to build higher order IT policies due to the inability to correlate information across different types of devices and systems in the enterprise.



Voice of the Customer
Management Requirements

- Simple
  - Reduce installation and configuration complexity
  - Reduce agent footprint and maintenance burden
  - Reduce the number of proprietary management tools
- Secure
  - Single integrated Security Model
  - Built using industry standard secure protocols and encryption algorithms (SSL, SSH)
  - Reduce the number of entry points into internal network
- Standard
  - Ensure common data representations and transports through conformance to leading standards
  - Command Line and Programmatic interfaces on all enterprise components (Servers, Management Processors, Enclosures etc..).


Developer
Project Stakeholder
Identify Idea or Suggestion
Discuss Potential Requirement
Estimate
Prioritize
Model & Potentially Document

HP’s Management Direction

Management

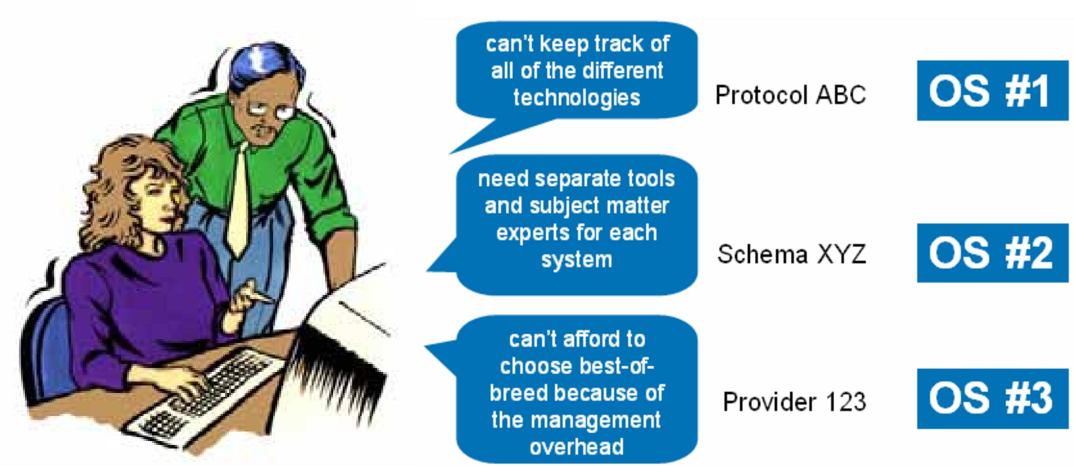
Industry Standards

Why Industry Standards?

- IT without industry standards is chaotic!
- IT without industry standards is too expensive!
- IT without industry standards limits choices!

ISS Standards Approach

- Invest in new standards only when there is clear superiority over existing standards
- Invest in standards that will enable significant product simplification or flexibility over time
- Invest in standards with clear industry and customer backing



can't keep track of all of the different technologies

need separate tools and subject matter experts for each system

can't afford to choose best-of-breed because of the management overhead

Protocol ABC

Schema XYZ

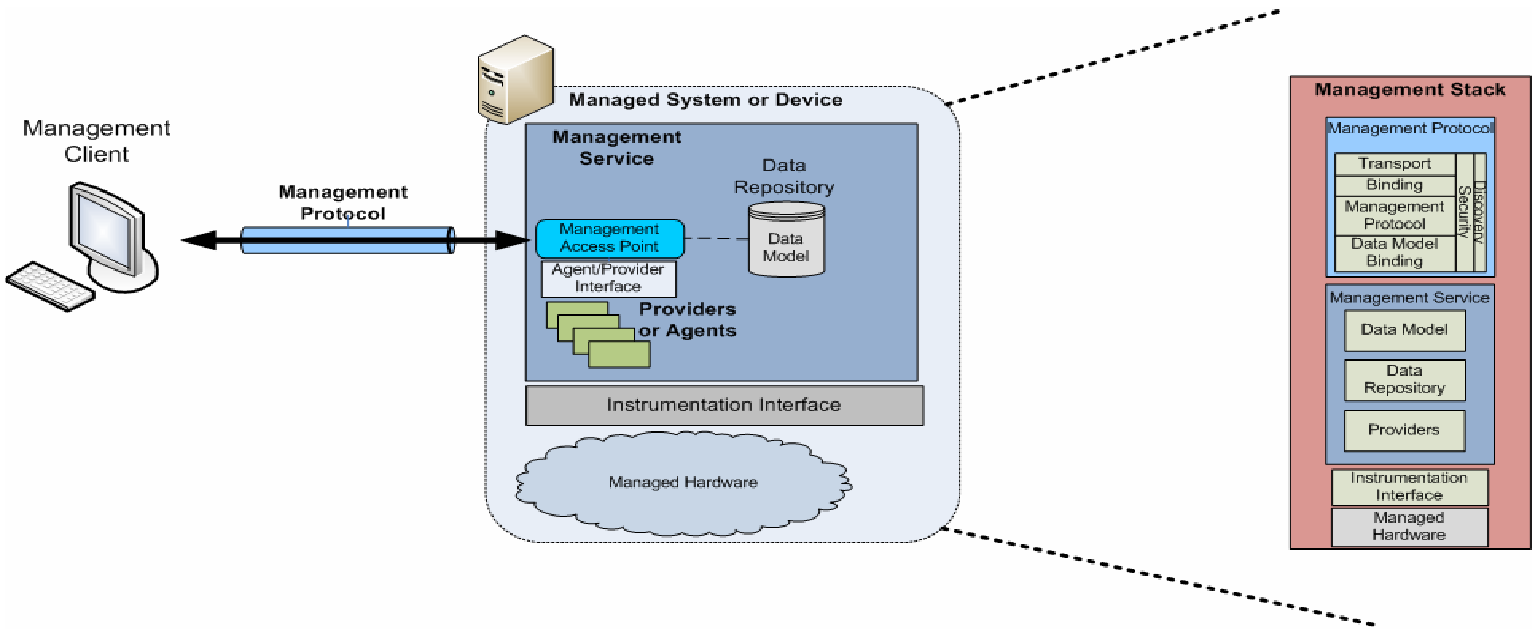
Provider 123

OS #1

OS #2

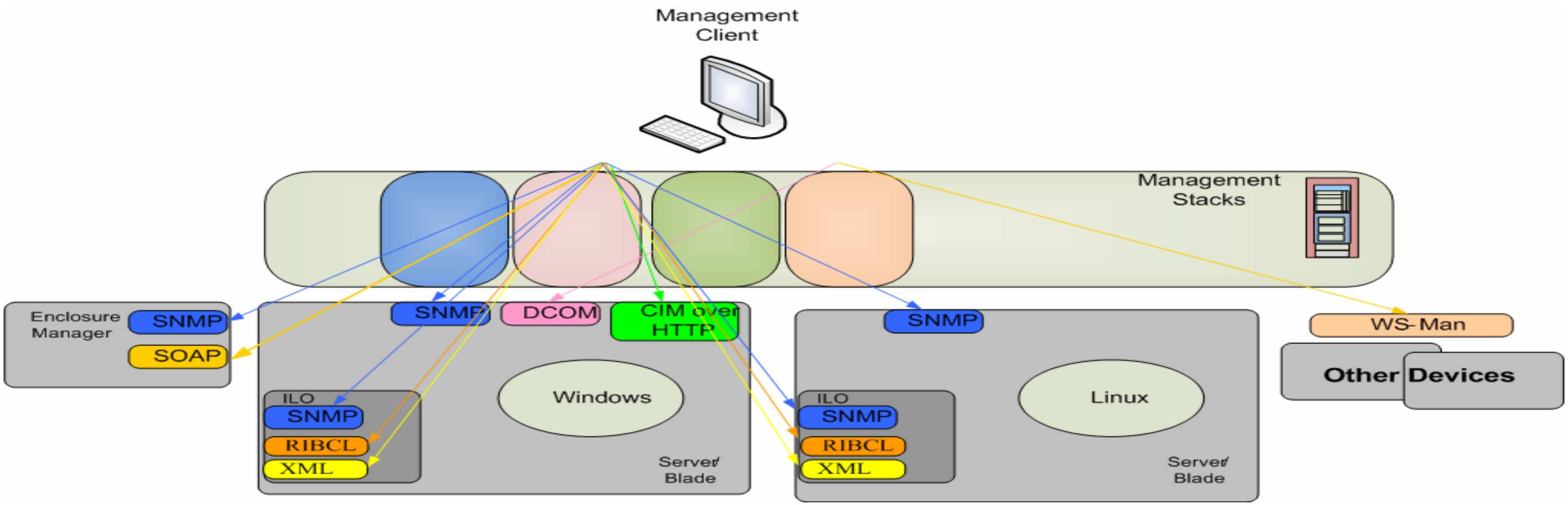
OS #3

Makeup of a Management Stack



- Management Client – Enabled IT professionals to manage devices in the enterprise.
- Management Protocol – enables managed server and client to exchange information in a common format.
- Management Service – implements the server side of the management protocol and supports a data model and corresponding semantics.
- Management Access Point (MAP) – Access point connected to by the management client to exchange information (ex: TCP Port)
- Data Repository – Stores the data model schema and instances much like a relational database stores table schemas and table instances.
- Providers/Agents – Extends management service for a particular managed devices. This allows the server to be extended to support new types of devices.
- Instrumentation Interface – Interface to the low-level hardware being managed (ex: IPMI, SMBIOS, e

IT Challenge

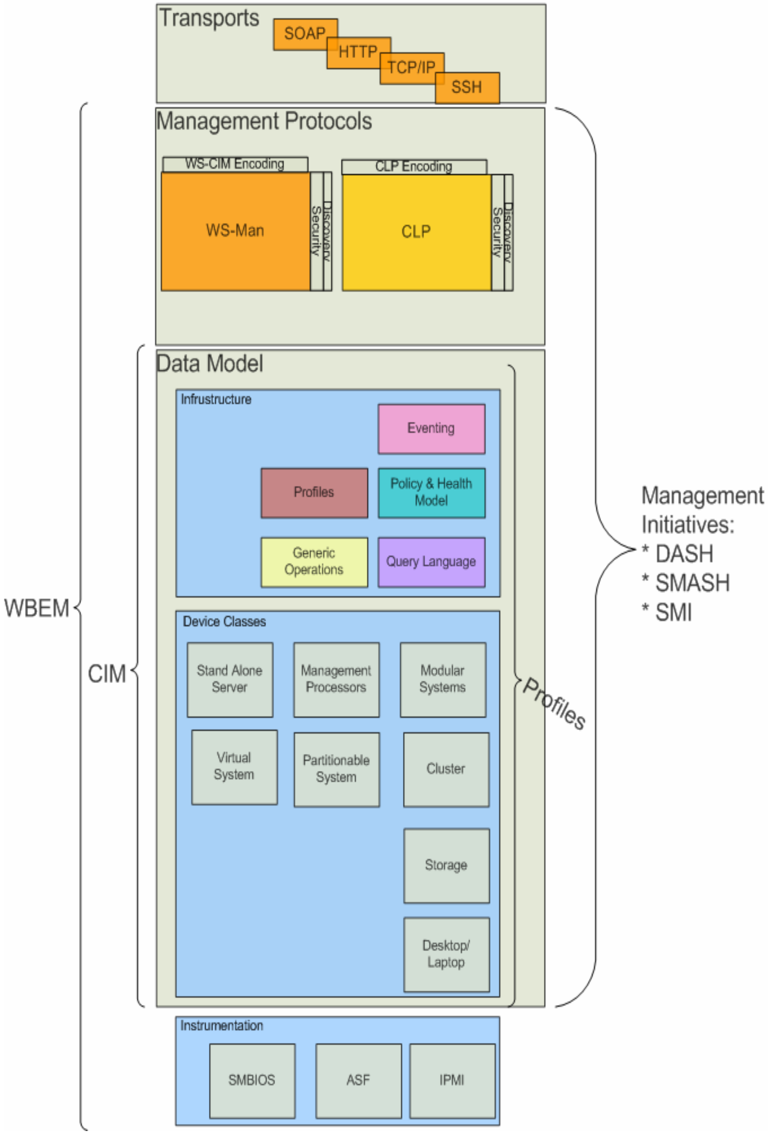


- Proliferation of management stacks complicates management client solutions.
- Deploying and supporting multiple management stacks adds to TCO.
- Unable to build higher order management solutions on top of infrastructure built on top of inconsistent management stacks.
- Different authenticating and authorization complicates single sign on.
- Problems gets worse as more hardware is virtualized.

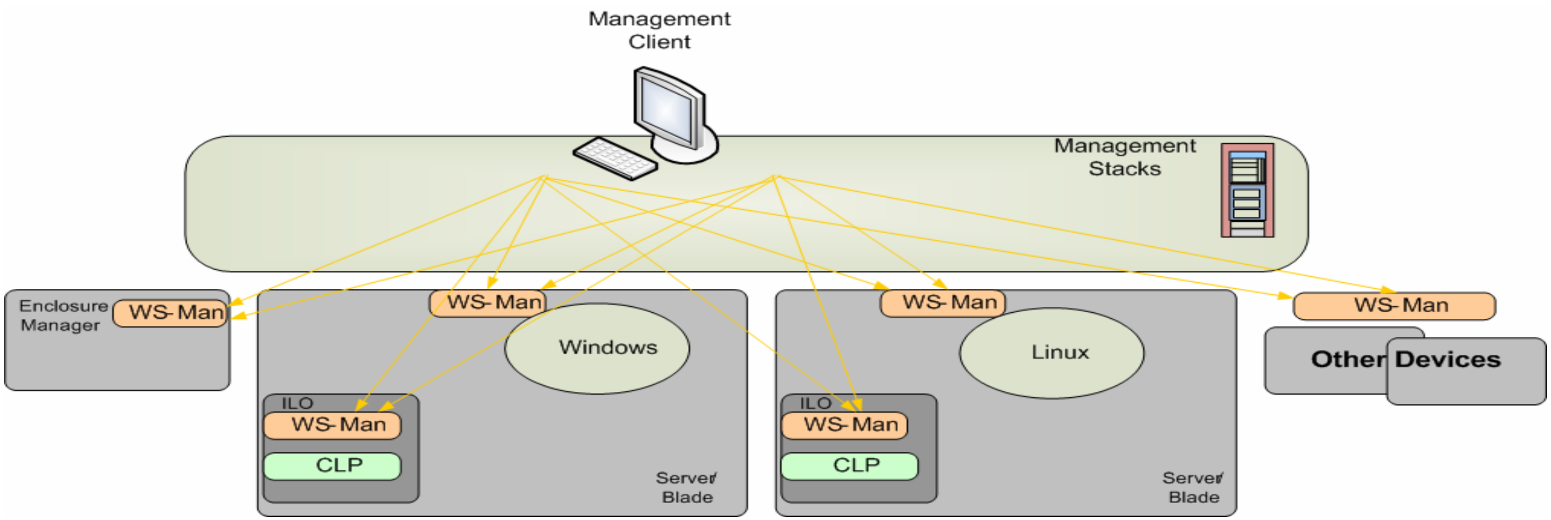
DMTF Technology Stack Map

WBEM – Web Based Enterprise Management

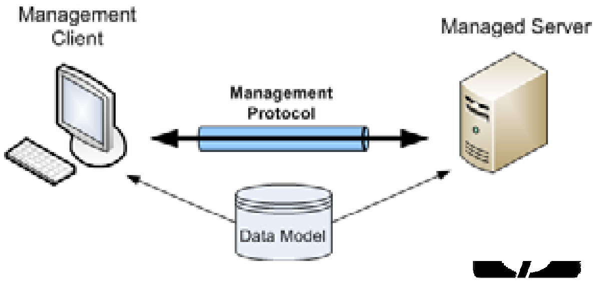
- Umbrella term for the set of internet-based standards defined by the DMTF for enterprise management, including:
  - **Standard Data Model**: CIM - Common Information Model
    - Core object-oriented schema managed by the DMTF. Used to define the data model used for WBEM enabled managed devices.
    - DMTF profiles define the data model and
    - CIM and profiles are the foundation for SMASH and SMI-S management initiatives.
  - **Standard Transport and API**: WS-Man – Web Services for Management
    - Routable, secure, interoperable, based on web service standards
    - Programmatic interface for both in-band and out-of-band management
  - **Standard Human Interface (CLP)** – Command Line Protocol defines a common and consistent command set for user facing command-line interface.
  - Management Initiatives – See Backup Slide.
  - *WBEM is not operating system or platform specific.*



IT Challenge – Solution



- Standards based management
  - Common and consistent management infrastructure built on top of well defined stack components.
  - Management protocol ensures interoperability between management client, managed server and managed devices
  - Consistent data model ensures the client can understand the semantics of the information supported by the managed server
- Reduces management client complexity
- Enabled higher order management solutions.
- Eases support of heterogeneous managed devices.
- Reduces TCO



HP WBEM Positioning

HP-UX

WBEM provides discovery, system, and reporting data to HP SIM that is more robust than SNMP with the HP-UX WBEM providers

OpenVMS 8.3-1H1

WBEM capability has been extended to OpenVMS on the BL860c and BL870c Server Blade systems and the rx3600 and rx6600 members of the HP Integrity server family.

Linux
Integrity Servers

WBEM provider modules enable access both local and remote, to key information about your Linux system using industry standard protocol

HP is aggressively driving industry standards based management across it's portfolio of products to provide secure, robust, and reliable data that enables customers to manage systems consistently across multiple platforms and operating systems. HP continues to lead the industry in server management providing integrated solutions that optimize infrastructure for greater operational efficiency.

Microsoft Windows Server
ISS Servers & Options

VMware ESX Server 3i

Linux
ISS Servers & Options

ProLiant Manageability

Future Direction

- Transition away from SNMP instrumentation to WBEM
- Adopt common data infrastructure defined by standards inside the DMTF and SNIA.
  - SMASH for server
  - SMI-S for storage
- Extend standards where there is significant HP value-add
- Adopt WS-Man as consistent programmatic protocol for in-band and out-of-band management
- Adopt SMASH CLP as out-of-band command-line interface

Management Direction
Benefits

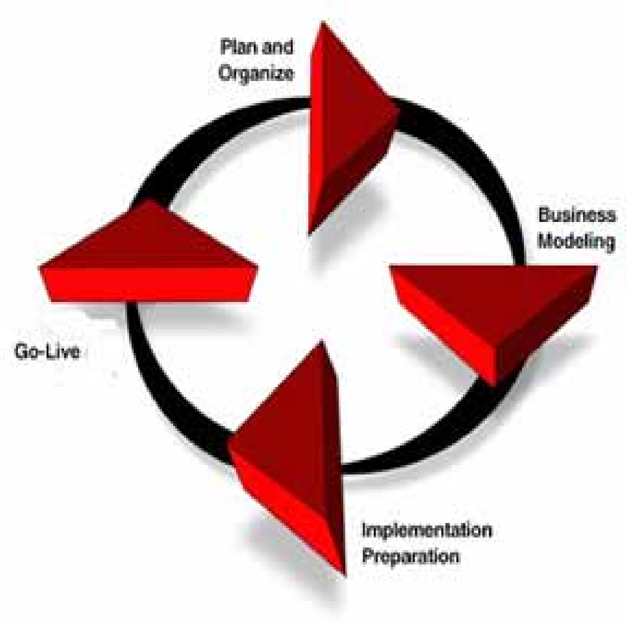
- Heightened security
- Reduced complexity of deployment, usability and maintainability
- Improved quality and usability of data
  - Consistency of information across OSs
- Guaranteed event delivery
- Common view of the system for both in-band and out-of-band management
- Delivers standards-based management across vendor platforms
- Facilitates the development of platform-neutral, reusable infrastructure, tools and applications
- Reduce TCO
  - Reducing the number of management applications required
- Lighter-weight
  - helps reduce the overall load on the server
- Improved SMH performance and updated UI
- Can co-exist with SNMP agents

Microsoft Windows Server Solution

HP Insight Management WBEM Providers

Solution Overview

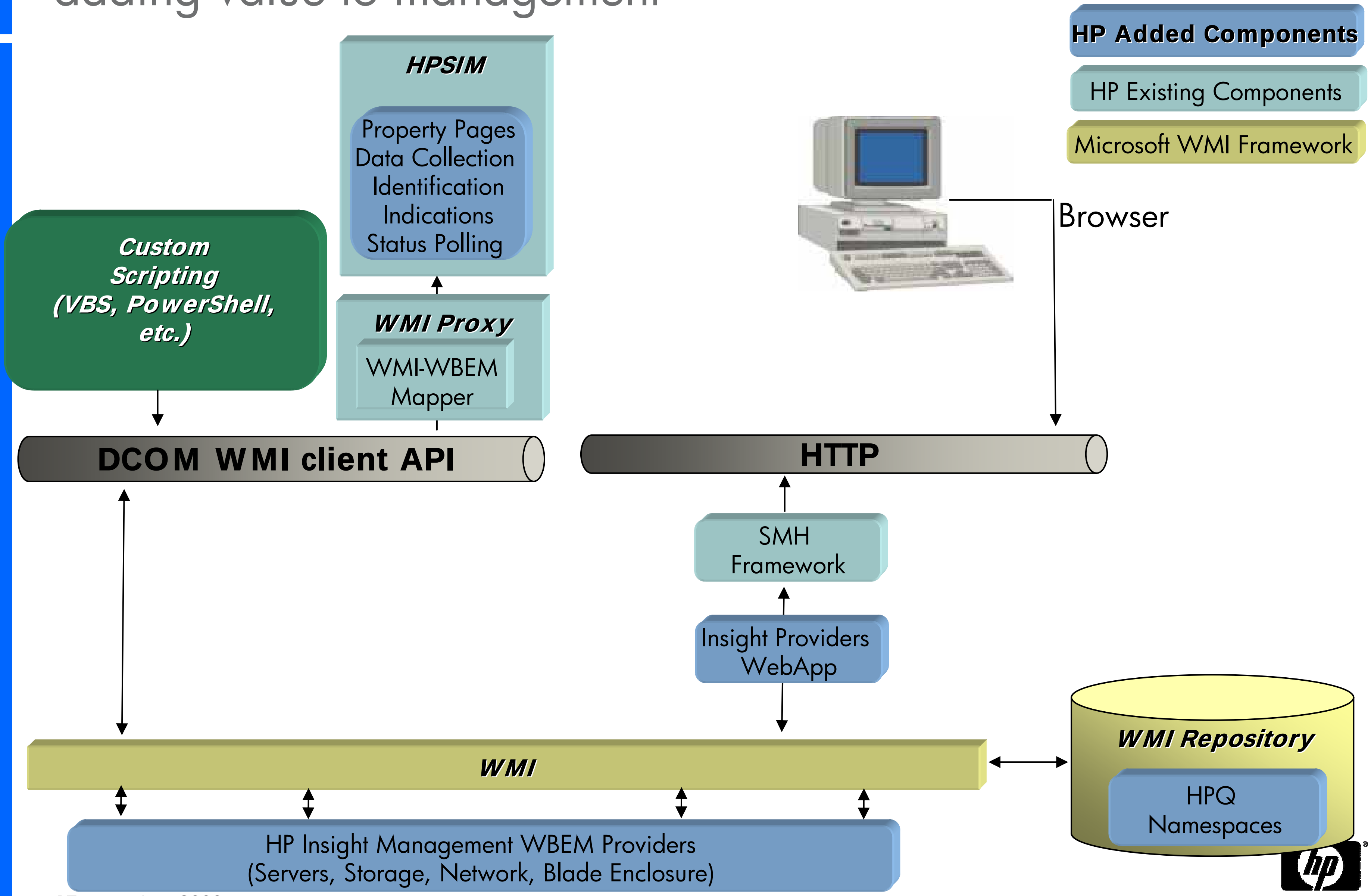
- HP Insight Management WBEM Providers for Windows
  - The HP Insight Management WBEM Providers for Windows extend CIM to make ProLiant-specific management data and events available to system administrators, enabling administrative tasks to be automated
    - The Providers leverage the rich set of base-level instrumentation provided by the system management controllers and drivers
    - Deliver in-depth hardware management, inventory data, system state, and event notifications
    - Secure encrypted data transmission
- Built on top of Windows Management Instrumentation (WMI)
- Enables IT to deliver a well-integrated set of standards-based management tools.
- First step towards a common consistent standards based management infrastructure across all HP managed devices.



www.hp.com/go/HPwbem

HP WBEM Solution Overview

adding value to management



HP Insight Management WBEM Providers

- **Server providers**
  - –Processor information and indications
  - –Memory information and indications
  - –PCI devices and system slots information
  - –Sensor information and indications, support for redundancy, fans, temperature sensors, power supplies, ASR
  - –Unit ID visual indicator
  - –Computer system information, support for physical location, IML, system ROM, and aggregate status
  - –Status roll-up of all connected components and devices

- **Network providers**
  - –Network controller information and indications, support for 10/100 Mb Ethernet, Gb Ethernet
  - –NIC teaming
- **Storage providers**
  - –Storage controller information and indications, support for Ultra3 and Ultra320 SCSI, SmartArray 5x and 6x, SAS/SATA information, Fibre Channel
  - –Storage enclosure

Indications to event log apply to all providers

WMI Providers indications, which are logged to the Windows® system event log

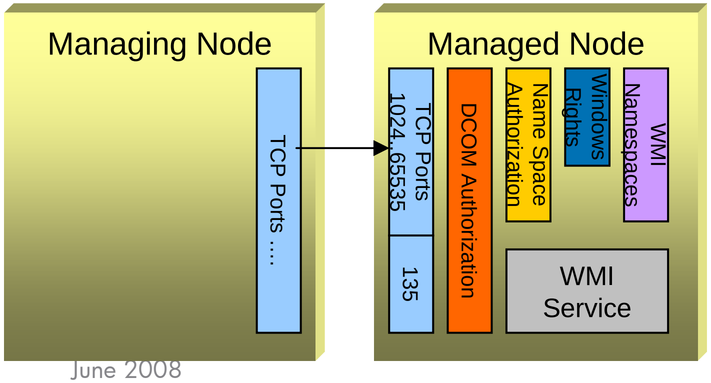
Security Comparison

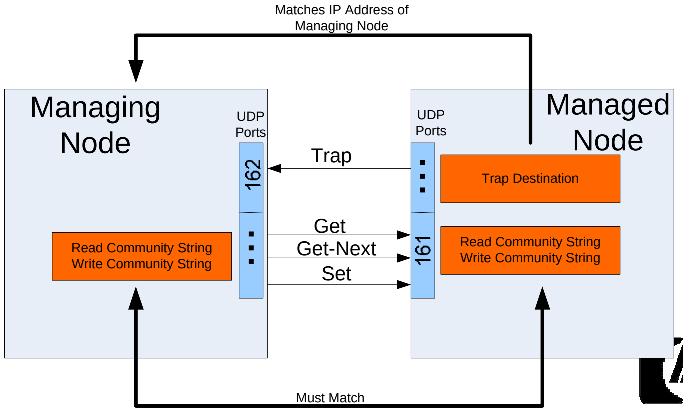
WBEM - WMI

- WMI security is built on top of existing Windows security
- WMI is built on top of DCOM security for remote access.
- DCOM leverages built-in Windows authentication services (NTLM or Kerberos)
- DCOM controls authorizing remote access to WMI namespaces.
- WMI namespace security is another level of security to control access to classes and instances for each namespace
- In the future, Windows will allow for secure management over HTTP/HTTPS with Windows Remote Management (WS Management protocol)

SNMP

- Windows SNMP security is based on SNMPv1
- By default, Windows SNMP support is not installed
- Uses an SNMP Community String over the network in clear text, which is inherently less secure
- SNMP security is not directly tied to Windows Local or Domain security credentials





HP Insight Management WBEM Providers

Security Deployment

Key Security Considerations

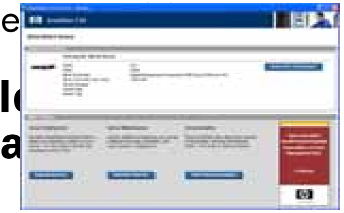
- WBEM Providers Use Existing OS Based Security on Windows.
- By Default, Only Administrators Have access to WBEM Provider Data Stored in WMI Namespaces.
- Enabling Non-Administrators (three ways)
  - PSP Component Configuration Parameter
  - SIM Configure and Repair Agents
  - Manually
    - Add User to "Distributed COM Users" on Managed Server
    - Give User/Group Access to root/HPQ namespace using Windows WMI Control applet.

HP Insight Management WBEM Providers
Deployment

- **SmartStart v8.x**
  - Begin the normal SmartStart installation process
  - Select ***HP Insight Management WBEM Providers*** for Windows at the Server Deployment – Management Instrumentation screen
  - The installation will continue and install the WBEM providers
- **ProLiant Support Pack v8.x**
  - Invoke HPSUM.exe
  - Select local or remote host at the Select Installation Host screen
  - Select bundles to install at the Select Bundle Filter screen
  - Next screen is where you can select the ***HP Insight Management WBEM Providers***.
  - Next steps follow the standard process

- **HP SIM v5.2**
  - From HPSIM select configure > configure or Repair Agents
  - Verify target systems
  - Enter credentials (ie. User name, password and domain)
  - Next step install Providers and Agents (Optional) page appears
  - Check box Install ***WBEM / WMI Provider (HP Insight Management WBEM Provider)***
  - Continue to standard next steps
- **Stand-Alone**
  - Using WBEM Providers Smart Component executable file
  - 32-bit Windows execute cp00xxxx.exe
  - 64-bit Windows exe

NOTE: The WBEM Providers can be uninstall using the Windows® Add or Remove Progra interface.



HP Insight Management WBEM Providers

Deployment

Dependencies

- Requires PSP 8.0 and higher
  - HP ProLiant Advanced and Enhanced System Management Controller driver
  - HP ProLiant iLO 2 Management Controller driver
  - HP ProLiant Remote Insight Lights-Out II Board driver
  - HP ProLiant Integrated Lights-Out Management Interface driver
  - Storage and Network drivers needed to support installed storage and network options

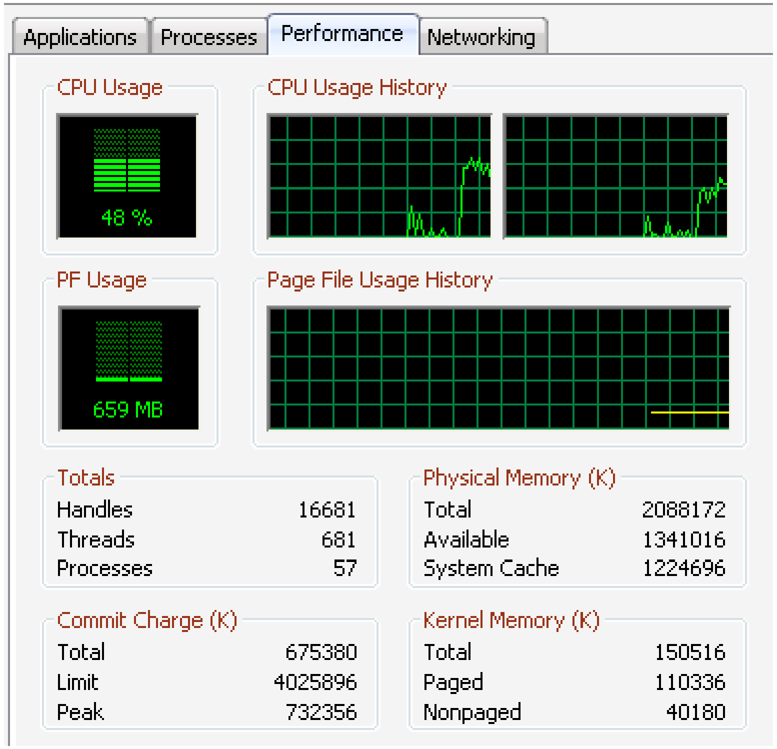
Need to know

- Blade enclosures
  - OA utilizes SNMP for out-of-band communication
- iLO
  - Can be configured to use SNMP but most customers do not utilize this function
  - Utilizes SNMP for out-of-band communication
- Host based fibre attached storage not supported
  - Future release
- NearLine tape not supported
  - Future release
- Insight Control Management Software updates required
- Remote Services support
  - Tools will be available 2h08
- Tivoli, MOM
  - Currently investigating requirements
- OpenView
  - Investigating
- SCOM
  - Future release 1h09

HP Insight Management WBEM Providers

Need to Know

- Most instance providers are loaded when needed, and unload automatically after several minutes of inactivity.
- All event (indication) providers are NOT unloaded automatically to insure events received from the drivers are handled correctly.
- Instrumentation comparable with SNMP-base Insight Management Agents
  - Indications (Alerting) and Event logging
  - Properties (Inventory)
- Can co-exist with SNMP agents
- No dependency on SNMP agents



Totals

Handles	16681
Threads	681
Processes	57

Physical Memory (K)

Total	2088172
Available	1341016
System Cache	1224696

Commit Charge (K)

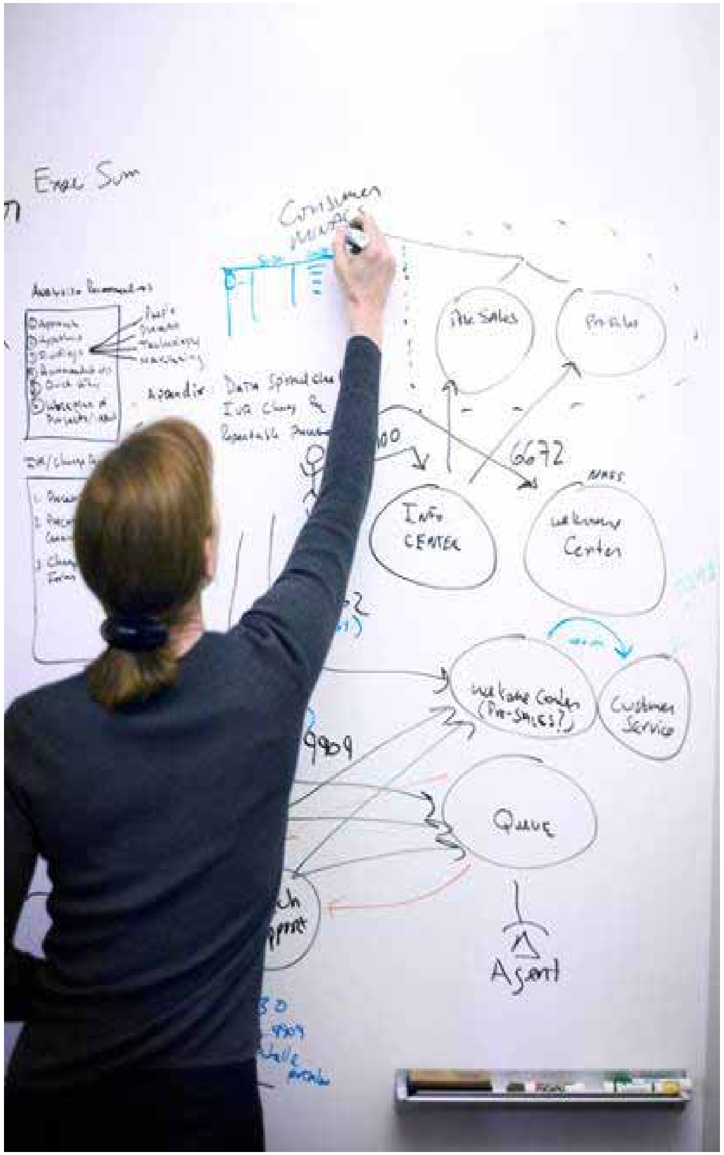
Total	675380
Limit	4025896
Peak	732356

Kernel Memory (K)

Total	150516
Paged	110336
Nonpaged	40180

Usage Scenarios

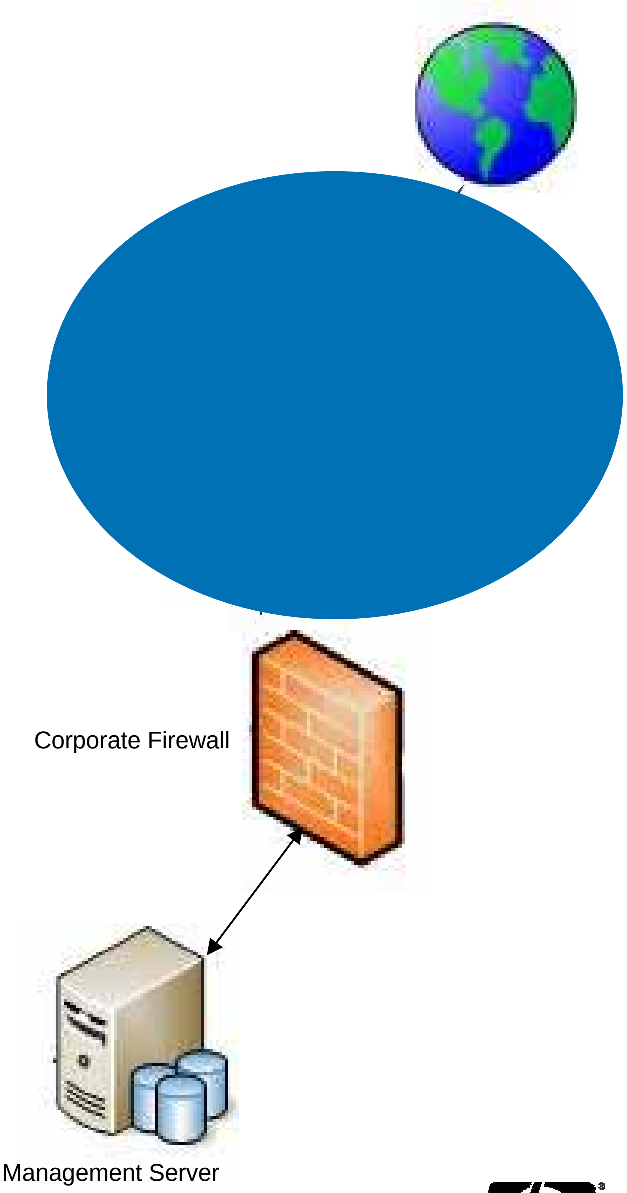
- Customers that have tighter security requirements
  - –Ability to securely manage servers in the DMZ
- Customers that are required to remove SNMP from their datacenter environment
- Multi-server management for ML, DL and BL using Enterprise Management applications
  - –Systems Insight Manager
  - –Custom applications



Usage Scenario

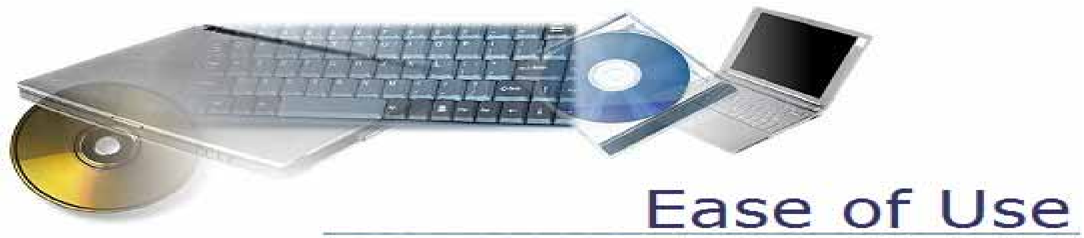
DMZ: As easy as 123

- Deploying a DMZ consists of several steps:
  - Determining the purpose of the DMZ
  - Selecting the servers to be placed in the DMZ
  - Considering other devices to be placed in the DMZ
  - Deciding on a method and strategy for monitoring servers in the DMZ
    - HP Insight Management WBEM Providers



- The Management Server is monitoring the corporate DMZ
- Administrators have opened the port for “Providers” running in the DMZ to forward information to the management server inside the corporate network
- Communication from these “Providers” is ***securely encrypted*** to prevent interception

Conclusion



- HP provides seamless integration of management across it's portfolio of products providing consistent, secure, robust and reliable data for monitoring and management of their infrastructure
- Combining WBEM with HPSIM creates a more powerful, open standards-based management solution.
- Provides increased security over SNMP
- Ease of Use
  - Enterprise management can realistically become more centralized
- Time savings
  - Tracing faults to their origin now truly has the potential of Enterprise scope
- Manageable
  - Use SNMP agents and / or WBEM providers

backup

Management Initiatives

- Management initiatives
  - Wrap several specification defined inside the DMTF and SMI into a wrapper specification that defines a consistent management stack for a class of device.
  - SMASH – Systems Management Architecture for Server Hardware
    - Driven by the DMTF
    - Profiles – CIM-based data model for server hardware
    - Transports
      - CLP – Command Line Protocol interface (mainly out-of-band)
      - WS-Man – programmatic interface (both in-band and out-of-band)
      - Aligns in-band and out-of-band, in-service and out-of-service management
  - SMI – Storage Management Initiative
    - Driven by SNIA
    - Effort to define standard profiles based on CIM for storage management
    - SMI-S specification

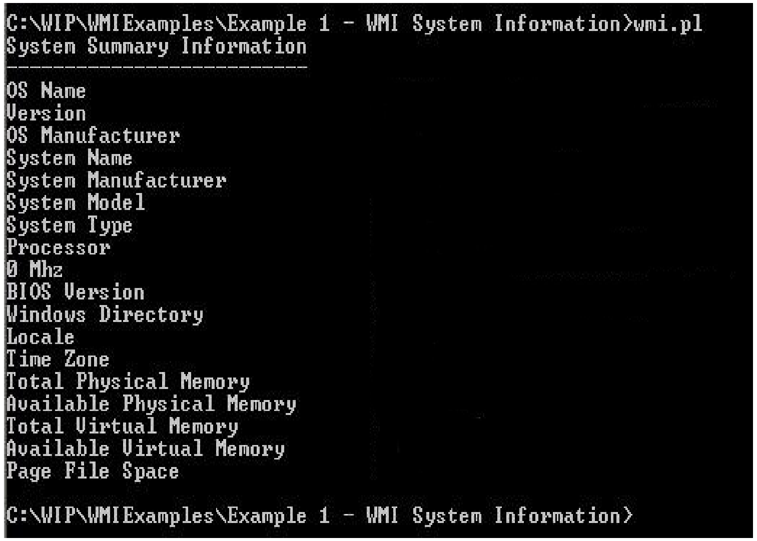
WBEM – SNMP Comparison

	WBEM	SNMP
Advantages	•Significant customer demand •Improved customer experience for initial setup and configuration •OS-based security and communications •Broad set of management information expose through standard classes (compared to SNMP) •Broad platform interoperability (SNMP /DMI/event logs, error logs, EMS, EVM) •OS independent (implementation on Windows, Unix, and Linux within HP)	•Well established, provides management today •Broad vendor implementation on wide range of platforms
Disadvantages	•Implementation not universal on enterprise platforms - growing •Linux implementation and distribution in development	•Insecure transport •Sensitive data in plain text •Limited to device discovery, status and events •Complex configuration for inexperienced users (non OS-based security) •Growing number of customers wanting to remove from their environment (largely security reasons)

Windows Management Instrumentation

WMI

- ***Definition***
  - Windows Management Instrumentation (WMI) is a component of the Windows operating system that provides management information and control in an enterprise environment. It is Microsoft’s implementation of Web Based Enterprise Management (WBEM).
- ***Usage Scenarios***
  - Administrators can use WMI to query and set information on desktop systems, applications, networks, and other enterprise components.
  - Developers can use WMI to create event monitoring applications that alert users when important incidents occur.
- WMI is a product of Microsoft and is only for Windows operating systems



```
C:\WIP\WMIExamples\Example 1 - WMI System Information>wmi.pl
System Summary Information
--------------------------

OS Name
Version
OS Manufacturer
System Name
System Manufacturer
System Model
System Type
Processor
0 Mhz
BIOS Version
Windows Directory
Locale
Time Zone
Total Physical Memory
Available Physical Memory
Total Virtual Memory
Available Virtual Memory
Page File Space

C:\WIP\WMIExamples\Example 1 - WMI System Information>
```

Windows Management Instrumentation (WMI)

WBEM Variant

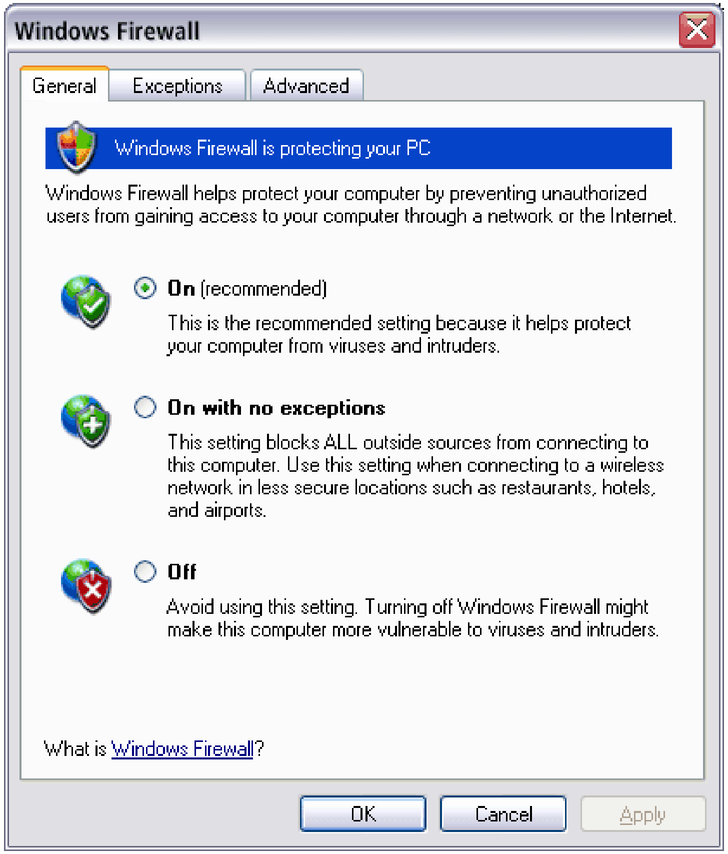
- Microsoft specific implementation of WBEM for Windows resources mgmt
- Leverages native OS comms transport (DCOM) and security model
- WMI management consists of following major elements:
  - WMI Providers
    - similar to element mgmt agents. Communicate with / monitor physical and logical components (e.g. OS services, applications and hardware)
  - CIM Object Manager (CIMOM)
    - manages communications and security between WMI providers, the CIM repository and management applications
    - Provides infrastructure for event monitoring
  - WMI Repository
    - Central storage used by CIMOM for registration data on WMI providers and apps
    - In some cases CIMOM derives dynamic data from the WMI Providers directly and not the WMI repository
  - WMI Scripting Library
    - Set of COM objects that allow scripts to interface with the WMI infrastructure (maintains security) and enumerates management data

HP Insight Management WBEM Providers

Windows Server 2008 Firewall

Configuration Overview

- Direct remote WMI access can be established running the Windows Server 2008 Firewall
- Default configuration will disallow remote WMI access
- Two commands executed locally on the Windows Server 2008 providing remote WMI access
  - netsh advfirewall firewall set rule group=”Windows Management Instrumentation (WMI)” new enable=yes
    - Output: Updated 4 rule(s).
    - Ok
  - netsh advfirewall firewall set rule name=”Network Discovery (NB-Name-In)” new enable=yes
    - Output: Updated 1 rule(s).
    - Ok



Windows Firewall is protecting your PC

Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through a network or the Internet.

● **On** (recommended)

This is the recommended setting because it helps protect your computer from viruses and intruders.

○ **On with no exceptions**

This setting blocks ALL outside sources from connecting to this computer. Use this setting when connecting to a wireless network in less secure locations such as restaurants, hotels, and airports.

○ **Off**

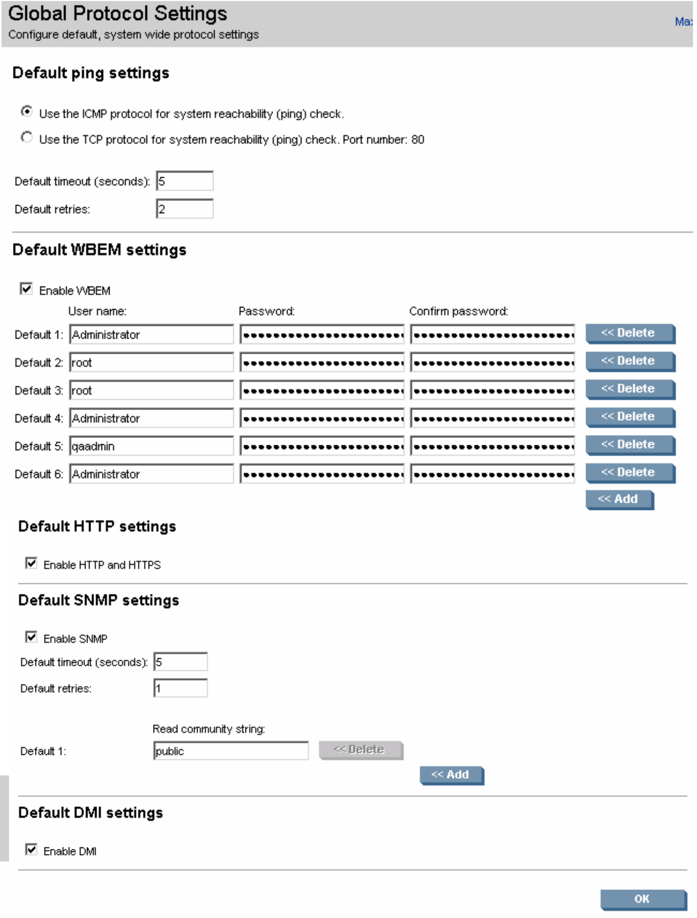
Avoid using this setting. Turning off Windows Firewall might make this computer more vulnerable to viruses and intruders.

What is Windows Firewall?

HP SIM v5.2

Configuring for use with WBEM Providers

- HP SIM can be configured to use the WBEM Providers on target systems for:
  - Discovering and identifying the target systems
  - Gathering management data for display in the HP SIM Property pages
  - Receiving event indications from target systems
- To configure HP SIM:
  - 1. Configure global protocol settings to specify the credentials for the system that is hosting the WMI Mapper.
  - 2. Configure the WMI Mapper proxy.
  - 3. Verify the settings.
  - 4. Rediscover the Windows® system so that WBEM is an identified protocol.
  - 5. Subscribe to WMI indications.



Global Protocol Settings

Configure default, system wide protocol settings

Default ping settings

● Use the ICMP protocol for system reachability (ping) check.

○ Use the TCP protocol for system reachability (ping) check. Port number: 80

Default timeout (seconds): 5

Default retries: 2

Default WBEM settings

☑ Enable WBEM

	User name:	Password:	Confirm password:	
Default 1:	Administrator	••••••••••••••••••••••	••••••••••••••••••••••	<< Delete
Default 2:	root	••••••••••••••••••••••	••••••••••••••••••••••	<< Delete
Default 3:	root	••••••••••••••••••••••	••••••••••••••••••••••	<< Delete
Default 4:	Administrator	••••••••••••••••••••••	••••••••••••••••••••••	<< Delete
Default 5:	qaadmin	••••••••••••••••••••••	••••••••••••••••••••••	<< Delete
Default 6:	Administrator	••••••••••••••••••••••	••••••••••••••••••••••	<< Delete

<< Add

Default HTTP settings

☑ Enable HTTP and HTTPS

Default SNMP settings

☑ Enable SNMP

Default timeout (seconds): 5

Default retries: 1

Read community string:

Default 1: public << Delete

<< Add

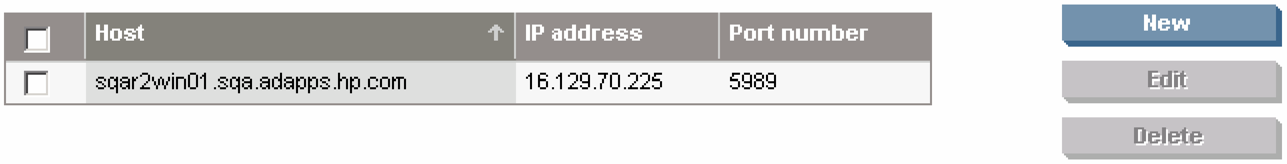
Default DMI settings

☑ Enable DMI

OK

WMI Mapper Proxy

Add, modify and configure WMI Mapper Proxy.



□	Host	IP address	Port number
□	sqar2win01.sqa.adapps.hp.com	16.129.70.225	5989

New

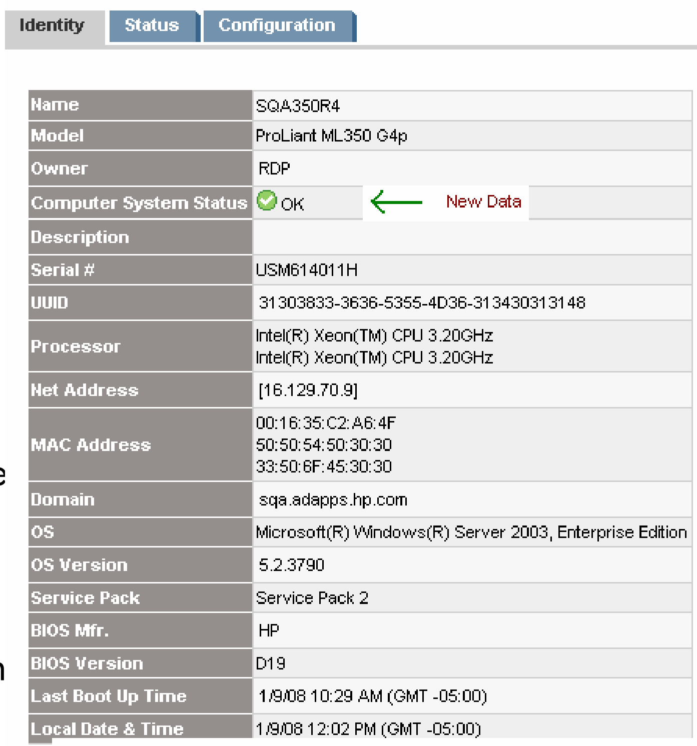
Edit

Delete

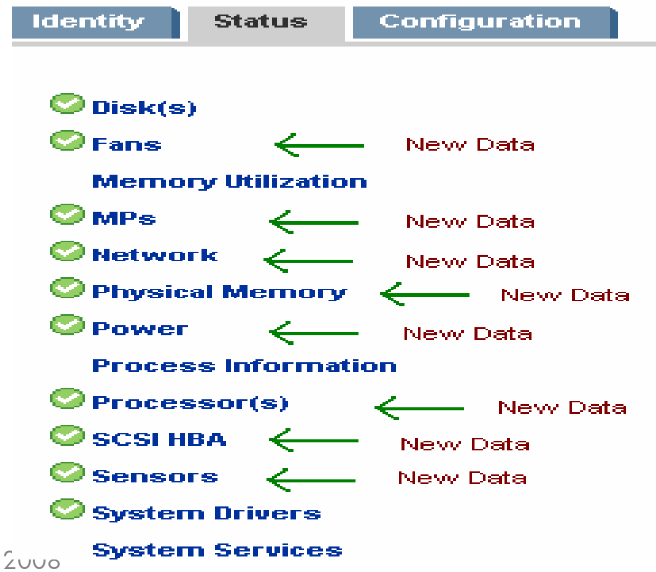
HP SIM v5.2

WBEM Provider Data

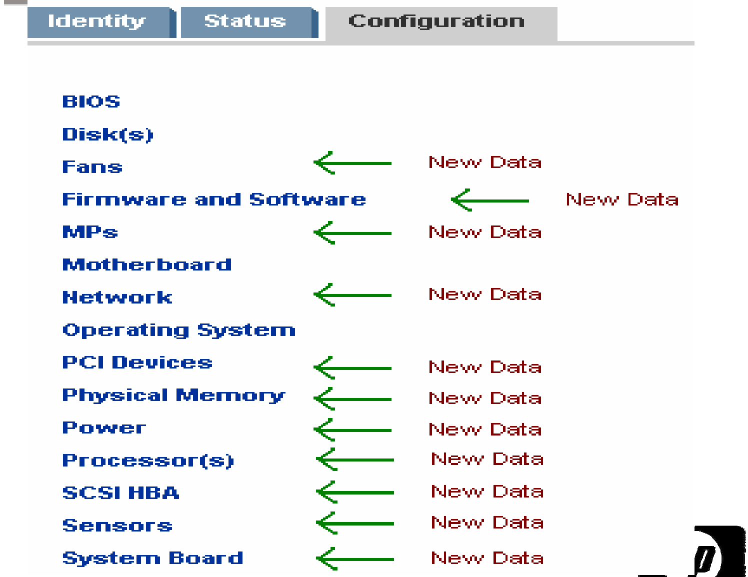
- Properties Page
  - Identity Tab
    - Displays WBEM properties that help describe the target system on the network.
  - Status Tab
    - Displays WBEM properties that help determine the status of the system, including status for all of the major computer subsystems.
  - Configuration Tab
    - This tab displays an inventory of the target system based on WBEM properties, including information on CPUs, disk drives, file systems, motherboards, software installations, and networks.



Name	SQA350R4
Model	ProLiant ML350 G4p
Owner	RDP
Computer System Status	✓ OK ← New Data
Description	
Serial #	USM614011H
UUID	31303833-3636-5355-4D36-313430313148
Processor	Intel(R) Xeon(TM) CPU 3.20GHz Intel(R) Xeon(TM) CPU 3.20GHz
Net Address	[16.129.70.9]
MAC Address	00:16:35:C2:A6:4F 50:50:54:50:30:30 33:50:6F:45:30:30
Domain	sqa.adapps.hp.com
OS	Microsoft(R) Windows(R) Server 2003, Enterprise Edition
OS Version	5.2.3790
Service Pack	Service Pack 2
BIOS Mfr.	HP
BIOS Version	D19
Last Boot Up Time	1/9/08 10:29 AM (GMT -05:00)
Local Date & Time	1/9/08 12:02 PM (GMT -05:00)



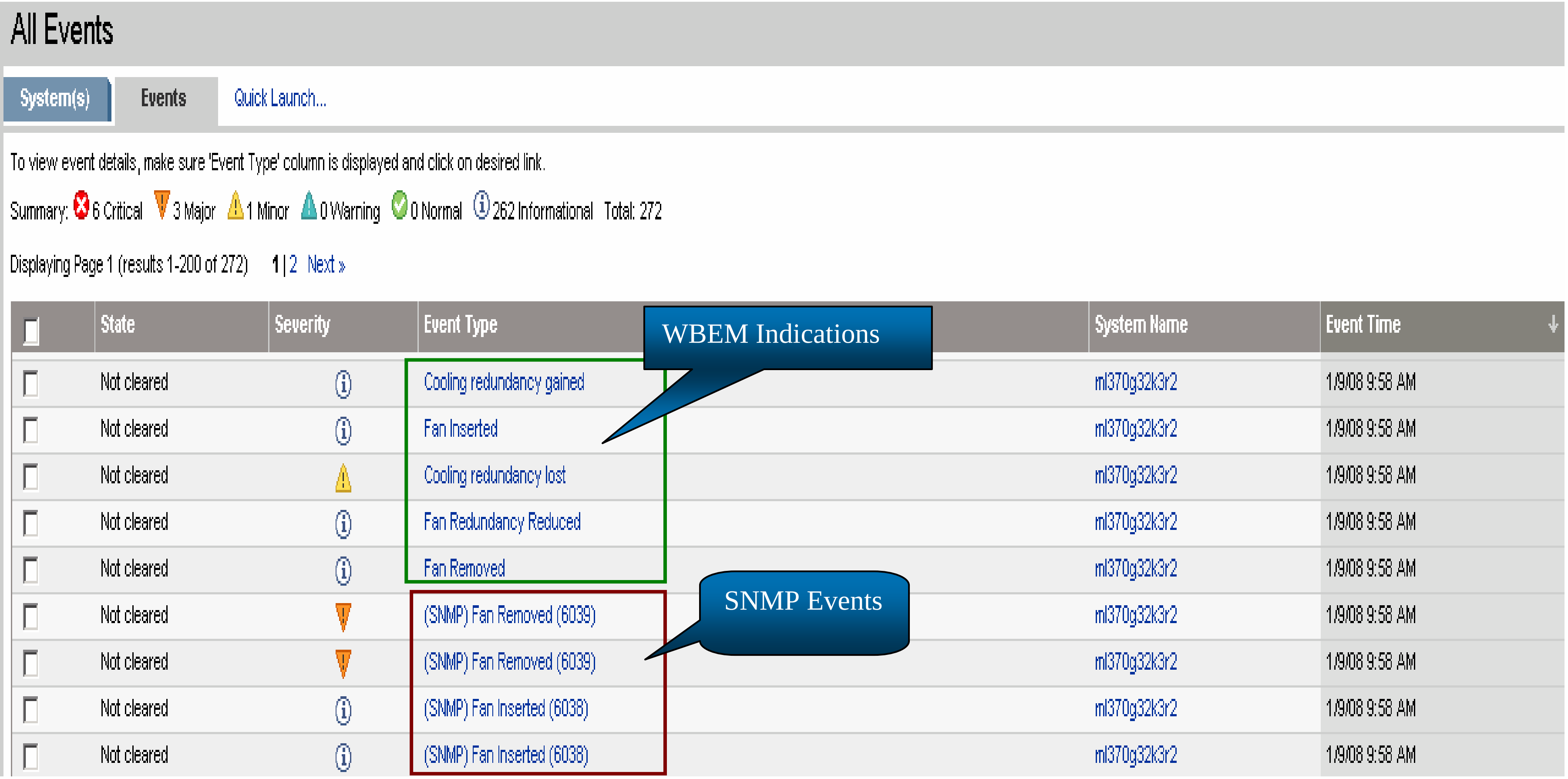
- ✓ Disk(s)
- ✓ Fans ← New Data
- Memory Utilization
- ✓ MPs ← New Data
- ✓ Network ← New Data
- ✓ Physical Memory ← New Data
- ✓ Power ← New Data
- Process Information
- ✓ Processor(s) ← New Data
- ✓ SCSI HBA ← New Data
- ✓ Sensors ← New Data
- ✓ System Drivers
- System Services



- BIOS
- Disk(s)
- Fans ← New Data
- Firmware and Software ← New Data
- MPs ← New Data
- Motherboard
- Network ← New Data
- Operating System
- PCI Devices ← New Data
- Physical Memory ← New Data
- Power ← New Data
- Processor(s) ← New Data
- SCSI HBA ← New Data
- Sensors ← New Data
- System Board ← New Data

HP SIM v5.2

WBEM / SNMP Event Comparison



All Events

System(s) | Events | Quick Launch...

To view event details, make sure 'Event Type' column is displayed and click on desired link.

Summary: ☒ 6 Critical ▼ 3 Major ⚠ 1 Minor ▲ 0 Warning ✓ 0 Normal ⓘ 262 Informational Total: 272

Displaying Page 1 (results 1-200 of 272) 1 | 2 Next »

□	State	Severity	Event Type	System Name	Event Time
□	Not cleared	ⓘ	Cooling redundancy gained	ml370g32k3r2	1/9/08 9:58 AM
□	Not cleared	ⓘ	Fan Inserted	ml370g32k3r2	1/9/08 9:58 AM
□	Not cleared	⚠	Cooling redundancy lost	ml370g32k3r2	1/9/08 9:58 AM
□	Not cleared	ⓘ	Fan Redundancy Reduced	ml370g32k3r2	1/9/08 9:58 AM
□	Not cleared	ⓘ	Fan Removed	ml370g32k3r2	1/9/08 9:58 AM
□	Not cleared	▼	(SNMP) Fan Removed (6039)	ml370g32k3r2	1/9/08 9:58 AM
□	Not cleared	▼	(SNMP) Fan Removed (6039)	ml370g32k3r2	1/9/08 9:58 AM
□	Not cleared	ⓘ	(SNMP) Fan Inserted (6038)	ml370g32k3r2	1/9/08 9:58 AM
□	Not cleared	ⓘ	(SNMP) Fan Inserted (6038)	ml370g32k3r2	1/9/08 9:58 AM

WBEM Indications

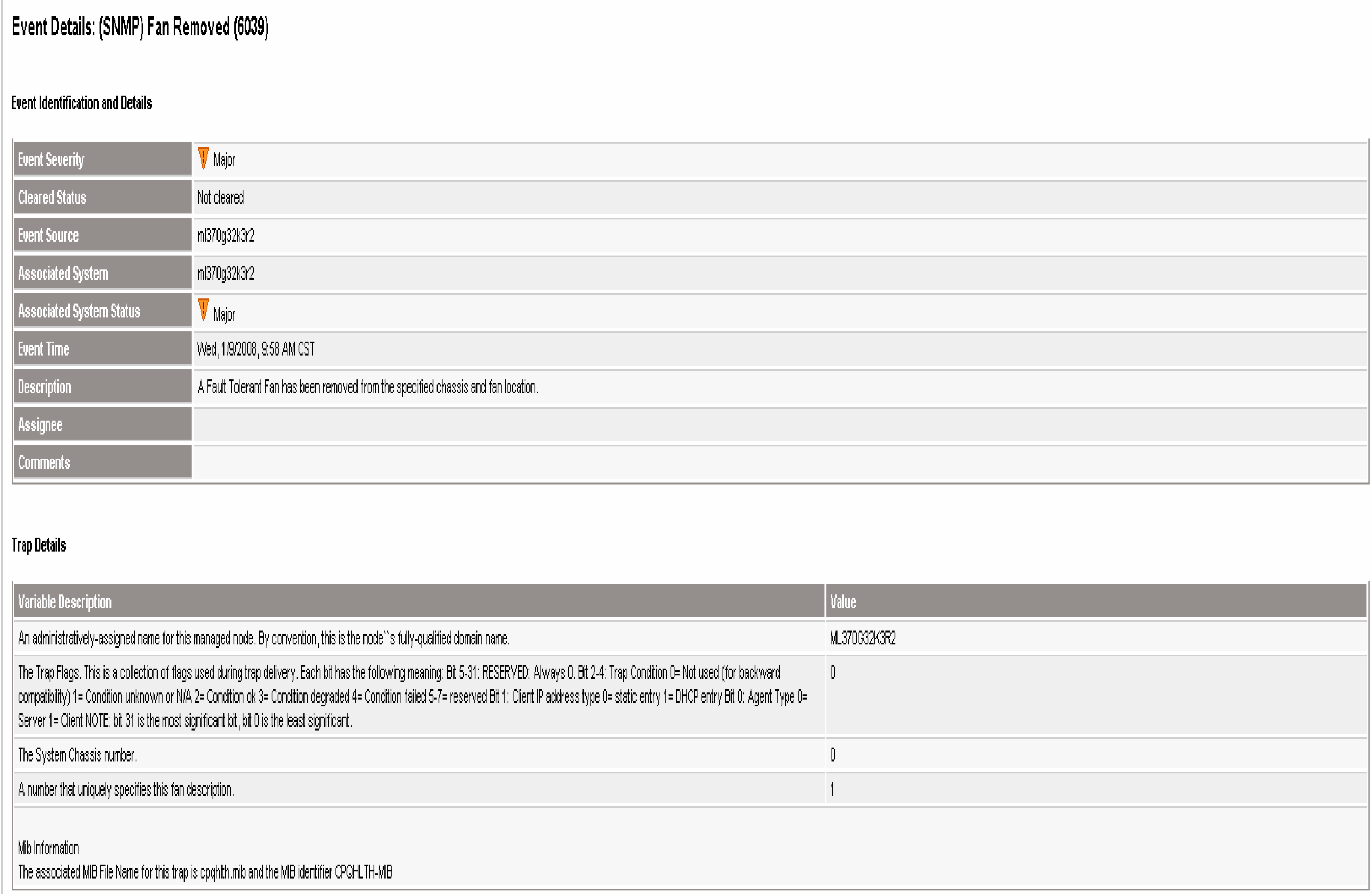
SNMP Events

HP-SIM receives SNMP and WBEM events from target node

Node generates events and events are listed in HP-SIM under All events list

HP SIM v5.2

SNMP Event Detail



Event Details: (SNMP) Fan Removed (6039)

Event Identification and Details

Event Severity	▼ Major
Cleared Status	Not cleared
Event Source	ml370g32k3r2
Associated System	ml370g32k3r2
Associated System Status	▼ Major
Event Time	Wed, 1/9/2008, 9:58 AM CST
Description	A Fault Tolerant Fan has been removed from the specified chassis and fan location.
Assignee	
Comments	

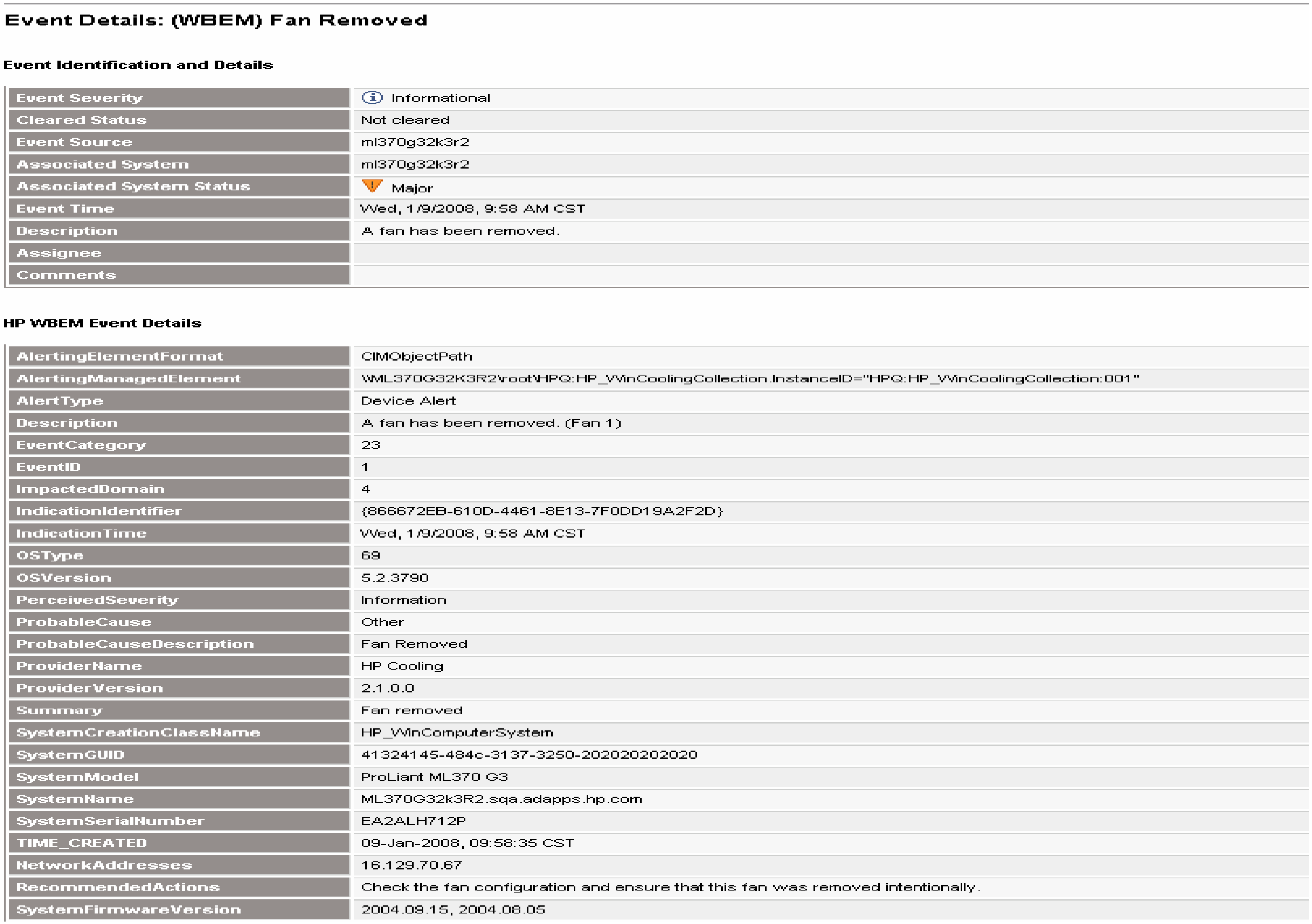
Trap Details

Variable Description	Value
An administratively-assigned name for this managed node. By convention, this is the node``s fully-qualified domain name.	ML370G32K3R2
The Trap Flags. This is a collection of flags used during trap delivery. Each bit has the following meaning: Bit 5-31: RESERVED: Always 0. Bit 2-4: Trap Condition 0= Not used (for backward compatibility) 1= Condition unknown or N/A 2= Condition ok 3= Condition degraded 4= Condition failed 5-7= reserved Bit 1: Client IP address type 0= static entry 1= DHCP entry Bit 0: Agent Type 0= Server 1= Client NOTE: bit 31 is the most significant bit, bit 0 is the least significant.	0
The System Chassis number.	0
A number that uniquely specifies this fan description.	1

Mib Information
The associated MIB File Name for this trap is cpqhlth.mib and the MIB identifier CPQHLTH-MIB

HP SIM v5.2

HP WBEM Event Detail



Event Details: (WBEM) Fan Removed

Event Identification and Details

Event Severity	ⓘ Informational
Cleared Status	Not cleared
Event Source	ml370g32k3r2
Associated System	ml370g32k3r2
Associated System Status	▼ Major
Event Time	Wed, 1/9/2008, 9:58 AM CST
Description	A fan has been removed.
Assignee	
Comments	

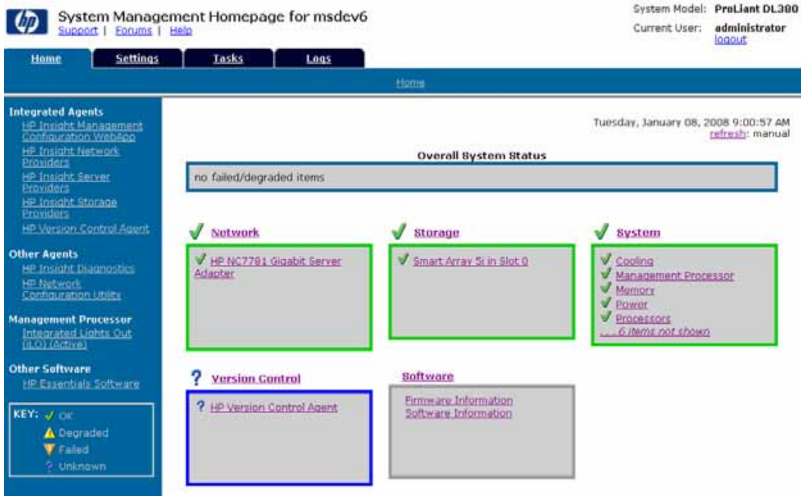
HP WBEM Event Details

AlertingElementFormat	CIMObjectPath
AlertingManagedElement	\\ML370G32K3R2\root\HPQ:HP_WinCoolingCollection.InstanceID="HPQ:HP_WinCoolingCollection:001"
AlertType	Device Alert
Description	A fan has been removed. (Fan 1)
EventCategory	23
EventID	1
ImpactedDomain	4
IndicationIdentifier	{866672EB-610D-4461-8E13-7F0DD19A2F2D}
IndicationTime	Wed, 1/9/2008, 9:58 AM CST
OSType	69
OSVersion	5.2.3790
PerceivedSeverity	Information
ProbableCause	Other
ProbableCauseDescription	Fan Removed
ProviderName	HP Cooling
ProviderVersion	2.1.0.0
Summary	Fan removed
SystemCreationClassName	HP_WinComputerSystem
SystemGUID	41324145-484c-3137-3250-202020202020
SystemModel	ProLiant ML370 G3
SystemName	ML370G32k3R2.sqa.adapps.hp.com
SystemSerialNumber	EA2ALH712P
TIME_CREATED	09-Jan-2008, 09:58:35 CST
NetworkAddresses	16.129.70.67
RecommendedActions	Check the fan configuration and ensure that this fan was removed intentionally.
SystemFirmwareVersion	2004.09.15, 2004.08.05

HP System Management Homepage

WBEM Provider Data

- The System Management Homepage now allows data collected from either the WBEM Providers or SNMP agents.
- After installation of the WBEM Providers, SMH will default to WBEM.
- To change this setting
  - –log into the SMH and go to the Settings Select SMH Data Source Select page.
  - –Choose the radio button for either WBEM or SNMP and click “Select.”
- One new feature is the “Auto Refresh” option.
  - –When SMH is using the SNMP data source, each page must be refreshed manually to retrieve the latest information.
  - –When using WBEM as the data source, the user can manually refresh the information or set an Auto Refresh interval to get updates.



System Management Homepage for msdev6
Support | Forums | Help

System Model: **ProLiant DL380**
Current User: **administrator**
logout

Home | Settings | Tasks | Logs

Home

Integrated Agents
HP Insight Management Configuration WebApp
HP Insight Network Providers
HP Insight Server Providers
HP Insight Storage Providers
HP Version Control Agent

Other Agents
HP Insight Diagnostics
HP Network Configuration Utility

Management Processor
Integrated Lights Out (iLO) (Active)

Other Software
HP Essentials Software

KEY: ✓ OK
⚠ Degraded
▼ Failed
? Unknown

Tuesday, January 08, 2008 9:00:57 AM
refresh: manual

Overall System Status
no failed/degraded items

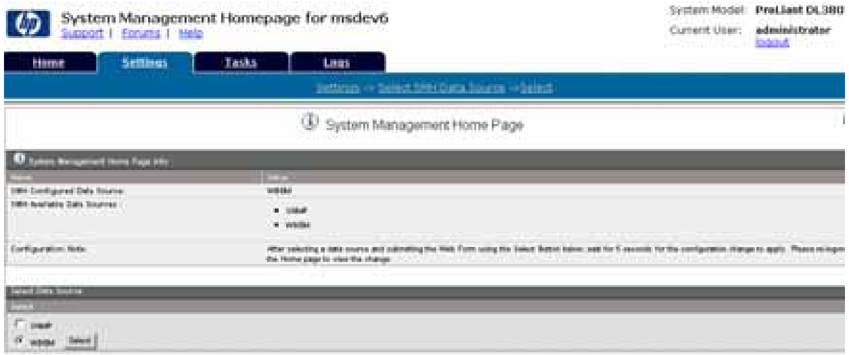
✓ **Network**
✓ HP NC7781 Gigabit Server Adapter

✓ **Storage**
✓ Smart Array 5i in Slot 0

✓ **System**
✓ Cooling
✓ Management Processor
✓ Memory
✓ Power
✓ Processors
... 6 items not shown

? **Version Control**
? HP Version Control Agent

Software
Firmware Information
Software Information



System Management Homepage for msdev6
Support | Forums | Help

System Model: **ProLiant DL380**
Current User: **administrator**
logout

Home | Settings | Tasks | Logs

Settings -> Select SMH Data Source ->Select

System Management Home Page

System Management Home Page Info

Name	Value
SMH Configured Data Source	WBEM
SMH Available Data Sources	• SNMP • WBEM
Configuration Note	After selecting a data source and submitting the Web Form using the Select Button below, wait for 5 seconds for the configuration change to apply. Please [illegible] the Home page to view the change.

Select Data Source

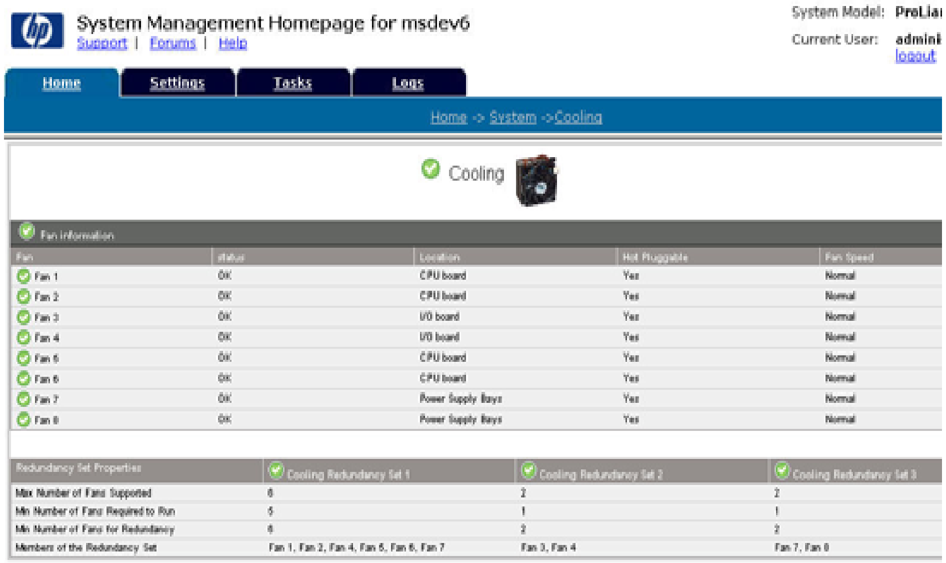
Option

○ SNMP
● WBEM [Select]

HP System Management Homepage

Enhancements

- Performance enhancements
- GUI enhancements
- Selectable data source for either SNMP or WBEM
- Cooling Page
  - Show empty fan slots (New)
  - Redundancy info (Enhanced)
- Power Page
  - Redundancy info (Enhanced)
- Memory Page
  - Data reorganized
  - Board Summary Table
    - No switching to different page, single page view for all information
    - Enhanced detail view
- Processor Page
  - Same enhancements as the memory page



System Management Homepage for msdev6
Support | Forums | Help

System Model: ProLiai
Current User: admini
logout

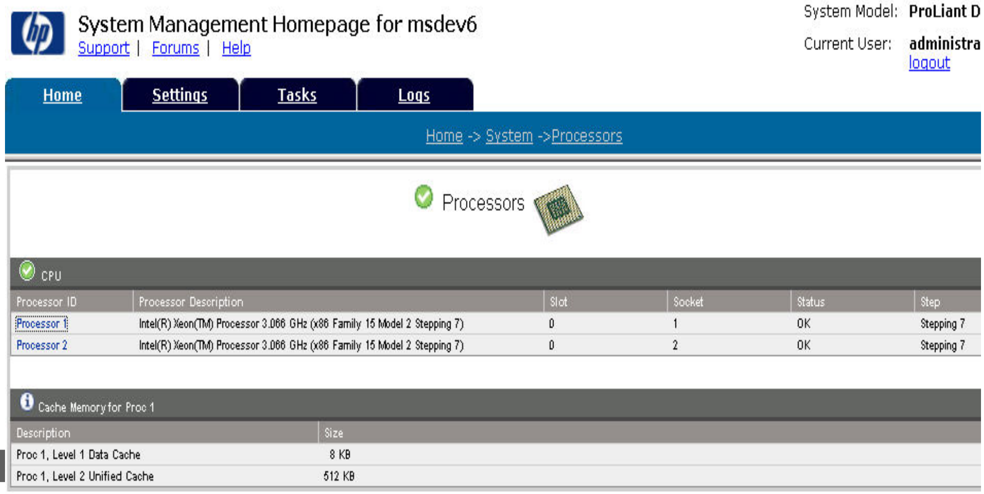
Home -> System ->Cooling

✓ Cooling

✓ Fan information

Fan	status	Location	Hot Pluggable	Fan Speed
✓ Fan 1	OK	CPU board	Yes	Normal
✓ Fan 2	OK	CPU board	Yes	Normal
✓ Fan 3	OK	I/O board	Yes	Normal
✓ Fan 4	OK	I/O board	Yes	Normal
✓ Fan 5	OK	CPU board	Yes	Normal
✓ Fan 6	OK	CPU board	Yes	Normal
✓ Fan 7	OK	Power Supply Bays	Yes	Normal
✓ Fan 8	OK	Power Supply Bays	Yes	Normal

Redundancy Set Properties	✓ Cooling Redundancy Set 1	✓ Cooling Redundancy Set 2	✓ Cooling Redundancy Set 3
Max Number of Fans Supported	6	2	2
Min Number of Fans Required to Run	5	1	1
Min Number of Fans for Redundancy	6	2	2
Members of the Redundancy Set	Fan 1, Fan 2, Fan 4, Fan 5, Fan 6, Fan 7	Fan 3, Fan 4	Fan 7, Fan 8



System Management Homepage for msdev6
Support | Forums | Help

System Model: ProLiant D
Current User: administra
logout

Home -> System ->Processors

✓ Processors

✓ CPU

Processor ID	Processor Description	Slot	Socket	Status	Step
Processor 1	Intel(R) Xeon(TM) Processor 3.066 GHz (x86 Family 15 Model 2 Stepping 7)	0	1	OK	Stepping 7
Processor 2	Intel(R) Xeon(TM) Processor 3.066 GHz (x86 Family 15 Model 2 Stepping 7)	0	2	OK	Stepping 7

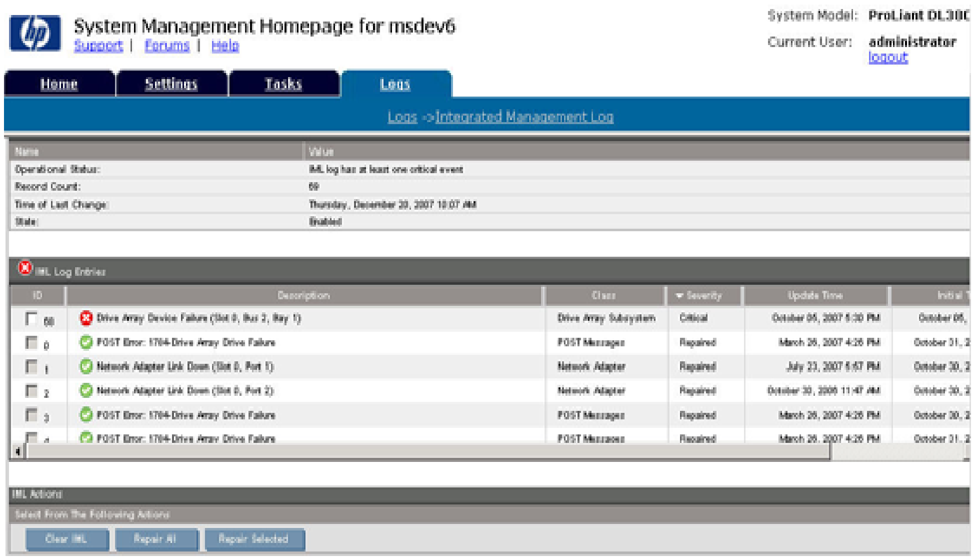
Cache Memory for Proc 1

Description	Size
Proc 1, Level 1 Data Cache	8 KB
Proc 1, Level 2 Unified Cache	512 KB

HP System Management Homepage

Enhancements

- Storage
  - Smart Array Link option to turn UID on/off on a drive
  - New frame design of pages allows easy drill down to additional details
  - Convent display of physical and logical drives info
- Logs
  - Integrated Management Log
    - Ability to sort by any column
    - Options to Clear IML, Repair All, Repair Selected
- Tasks
  - Server Configuration
    - Setting of primary and secondary owner info
    - Setting for processor, disk thresholds
- UID Page
  - Allows turning UID on/off



System Management Homepage for msdev6

System Model: ProLiant DL30

Current User: administrator

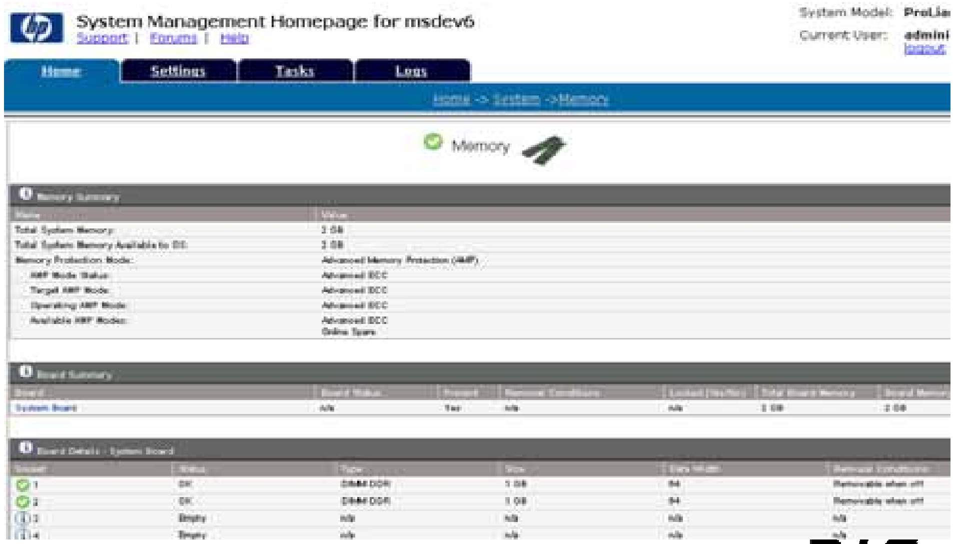
Name	Value
Operational Status:	IML log has at least one critical event
Record Count:	69
Time of Last Change:	Thursday, December 20, 2007 10:07 AM
State:	Enabled

IML Log Entries

ID	Description	Class	▼ Severity	Update Time	Initial
□ 68	☒ Drive Array Device Failure (Slot 0, Bus 2, Bay 1)	Drive Array Subsystem	Critical	October 05, 2007 5:30 PM	October 05,
□ 0	✓ POST Error: 1704-Drive Array Drive Failure	POST Messages	Repaired	March 26, 2007 4:26 PM	October 31, 2
□ 1	✓ Network Adapter Link Down (Slot 0, Port 1)	Network Adapter	Repaired	July 23, 2007 5:57 PM	October 30, 2
□ 2	✓ Network Adapter Link Down (Slot 0, Port 2)	Network Adapter	Repaired	October 30, 2006 11:47 AM	October 30, 2
□ 3	✓ POST Error: 1704-Drive Array Drive Failure	POST Messages	Repaired	March 26, 2007 4:26 PM	October 30, 2
□ 4	✓ POST Error: 1704-Drive Array Drive Failure	POST Messages	Repaired	March 26, 2007 4:26 PM	October 31, 2

IML Actions

Select From The Following Actions



System Management Homepage for msdev6

System Model: ProLia

Current User: admini

Memory Summary

Name	Value
Total System Memory:	2 GB
Total System Memory Available to OS:	2 GB
Memory Protection Mode:	Advanced Memory Protection (AMP)
AMP Mode Status:	Advanced ECC
Target AMP Mode:	Advanced ECC
Operating AMP Mode:	Advanced ECC
Available AMP Modes:	Advanced ECC Online Spare

Board Summary

Board	Board Status	Present	Removal Conditions	Locked (Yes/No)	Total Board Memory	Board Memor
System Board	n/a	Yes	n/a	n/a	2 GB	2 GB

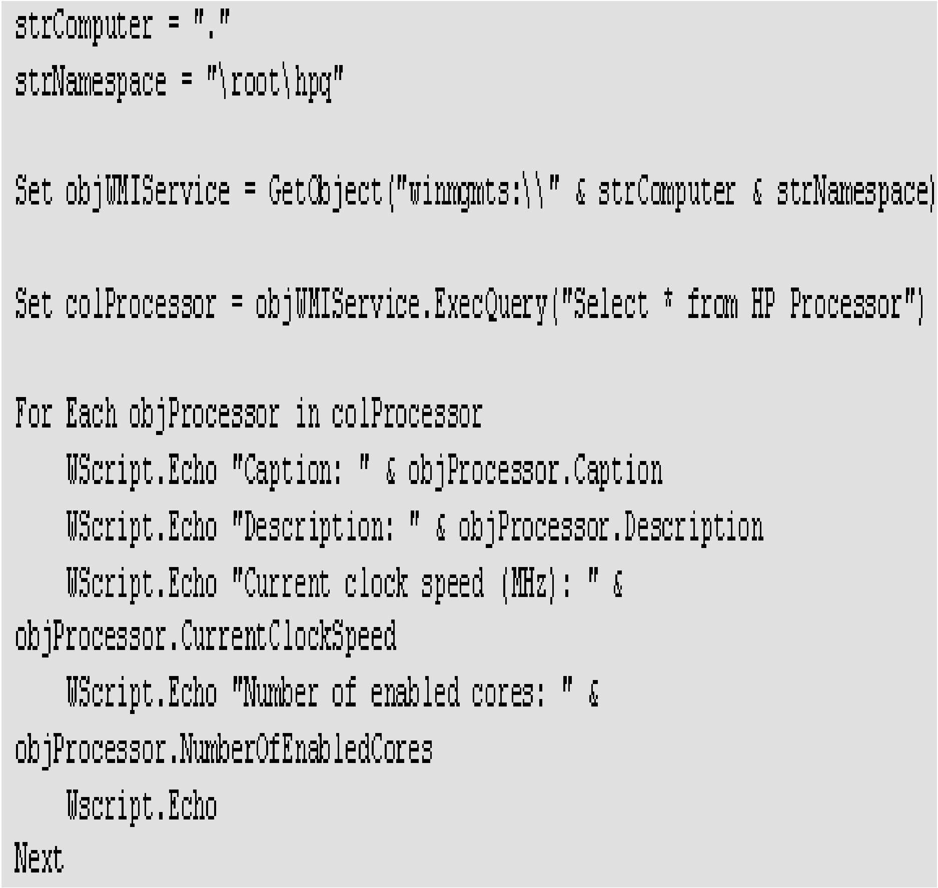
Board Details - System Board

Socket	Status	Type	Size	Data Width	Removal Conditions
✓ 1	OK	DIMM DDR	1 GB	64	Removable when off
✓ 2	OK	DIMM DDR	1 GB	64	Removable when off
ⓘ 3	Empty	n/a	n/a	n/a	n/a
ⓘ 4	Empty	n/a	n/a	n/a	n/a

HP Insight Management WBEM Providers

Scripting

- Scripts can be written to obtain data from the WBEM Providers via Microsoft Visual Basic
  - Display system status
  - Display server inventory
  - Receive alert indications
  - Evoke methods



```
strComputer = "."
strNamespace = "\root\hpq"

Set objWMIService = GetObject("winmgmts:\\" & strComputer & strNamespace)

Set colProcessor = objWMIService.ExecQuery("Select * from HP Processor")

For Each objProcessor in colProcessor
    WScript.Echo "Caption: " & objProcessor.Caption
    WScript.Echo "Description: " & objProcessor.Description
    WScript.Echo "Current clock speed (MHz): " &
objProcessor.CurrentClockSpeed
    WScript.Echo "Number of enabled cores: " &
objProcessor.NumberOfEnabledCores
    Wscript.Echo
Next
```

Resources

- HP Insight Management WBEM Providers – http://www.hp.com/HPwbem
- SNMP – http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm
- WBEM – http://www.dmtf.org/standards/wbem/
- WMI – http://www.microsoft.com/whdc/system/pnppwr/wmi/default.mspx
- IPMI – http://www.intel.com/design/servers/ipmi/
- SMASH – http://www.dmtf.org/standards/smash/
- CIM profiles – http://www.dmtf.org/standards/profiles/
- WS Management – http://www.dmtf.org/standards/wbem/wsman/
- DMTF website – http://www.dmtf.org
- SMI-S – http://www.snia.org/members/smis/ansi/

Backup

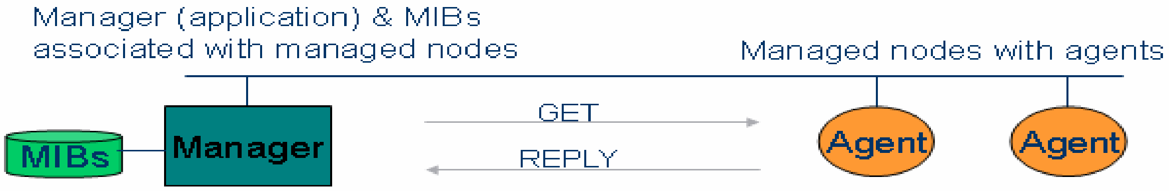
Simple Network Management Protocol

What is it SNMP?

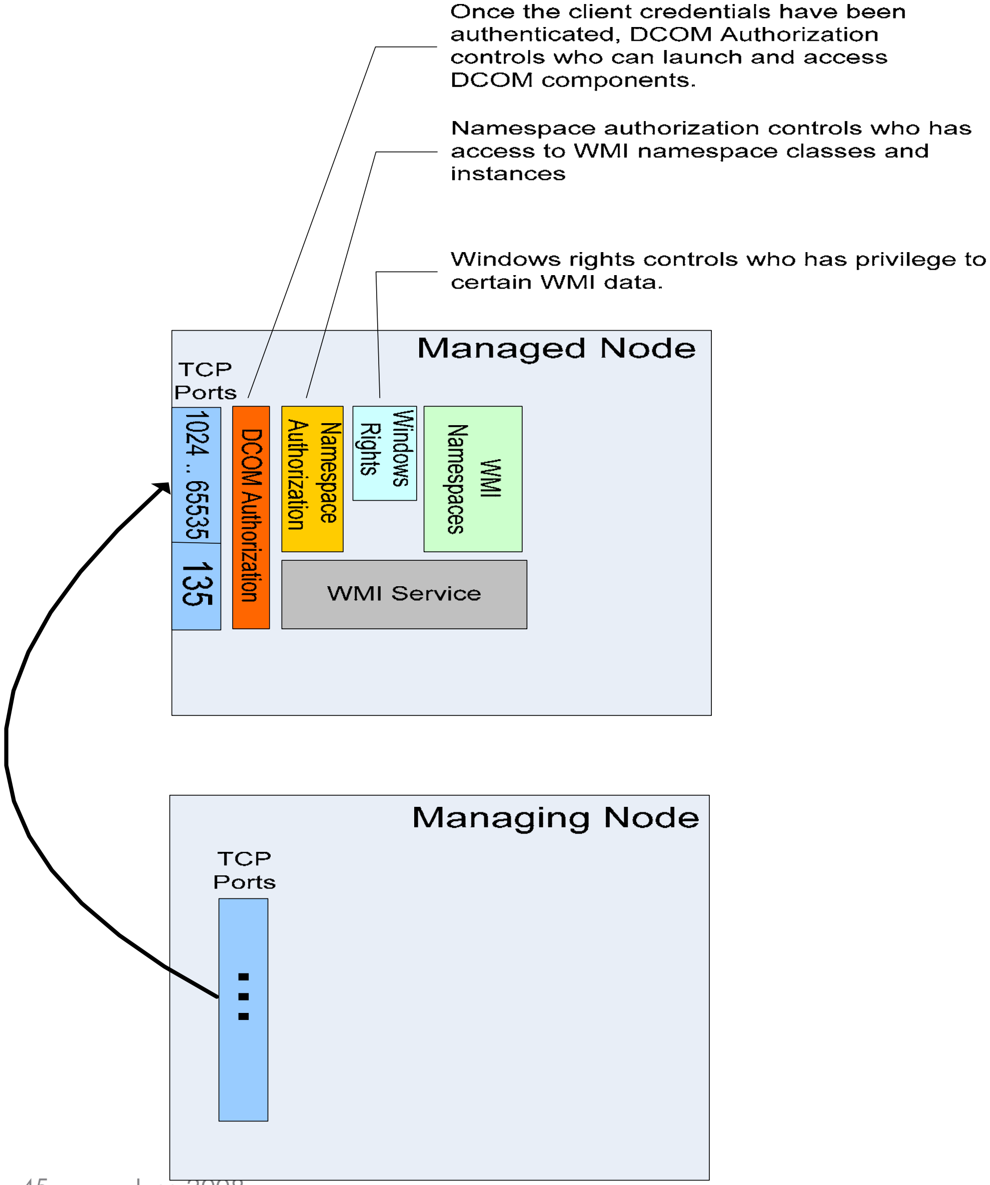
- Legacy standard for network device instrumentation and management
- Simple request/response protocol that communicates management information between two types of SNMP software entities: SNMP applications (also called SNMP managers) and SNMP agents.
  - –Manager polls managed nodes for requested data item(s) - (GET)
  - –Agent on managed node replies with data values (object identifier – OID)
  - –Information displayed based on content defined in associated MIB(s)
    - (Management Information base, defines managed items/conditions/variables)

Customer Benefits

- Provides management today
- Broad vendor implementation on wide range of platforms
- Considered insecure and unreliable
  - –Uses UDP (User Datagram Protocol) on top of IP
  - –Prone to collision and network noise
  - –No embedded authentication / confirmation of delivery
  - –Uses plain text passwords (SNMP v3 helps to address – but not widely adopted)
  - –Limited set of standards not rigidly enforced – vendor specific solutions / variations


Manager (application) & MIBs associated with managed nodes
Managed nodes with agents
MIBs
Manager
GET
REPLY
Agent
Agent

WMI Security Overview


Once the client credentials have been authenticated, DCOM Authorization controls who can launch and access DCOM components.
Namespace authorization controls who has access to WMI namespace classes and instances
Windows rights controls who has privilege to certain WMI data.
Managed Node
TCP Ports
1024 .. 65535
135
DCOM Authorization
Namespace Authorization
Windows Rights
WMI Namespaces
WMI Service
Managing Node
TCP Ports
...

- WMI security is built on top of existing Windows security
- The WMI service exposes a DCOM component as a remote management interface
- DCOM leverages built-in windows authentication services (NTLM or Kerberos)
- Once authenticated, DCOM authorizes who has privilege to launch and access DCOM components
- WMI namespace security is another level of security to control access to classes and instances for each namespace
- Windows rights controls who has privileges to certain WMI data

HP Insight Management WBEM Providers

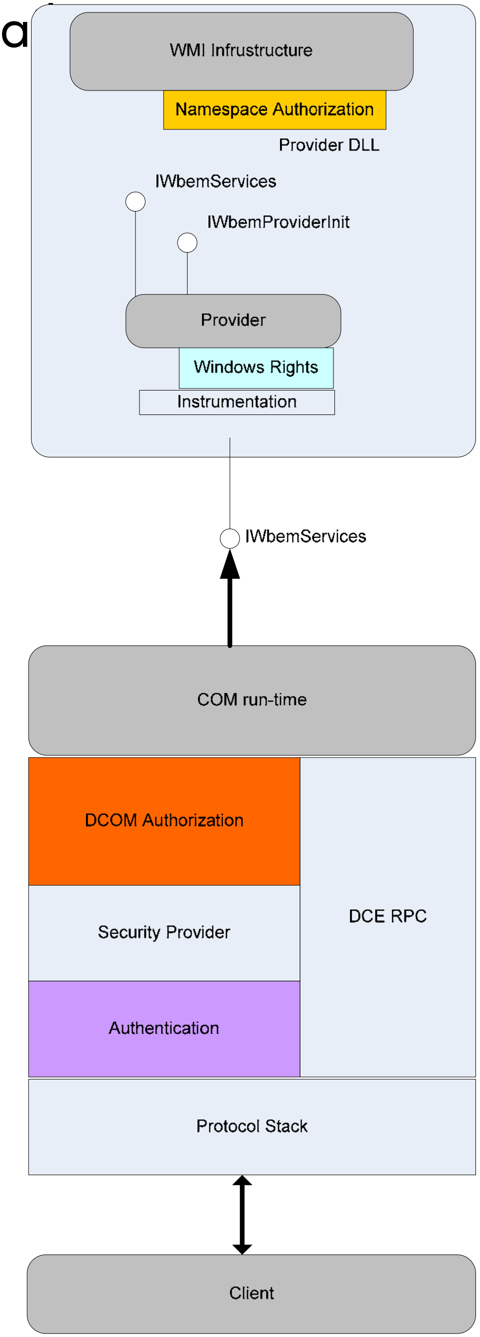
Security Deployment

Setup Overview

- The account (or accounts) to be used to access the WBEM providers' management information will need to be given sufficient access rights and security group memberships to allow remote access by HP Systems Insight Manager or other clients querying WMI data.
- To enable remote access of the WBEM Providers via WMI:
  - –Add the management account to the "Distributed DCOM Users" group.
  - –Add the management account to the namespace security of the following namespaces via WMI Control:
    - root\HPQ
    - root\HPQ\default
    - root\HPQ\TestEvent
    - root\Interop
    - root\CIMv2
  - –Each of the above namespaces will need the following permissions:
    - Execute Methods
    - Full Write
    - Partial Write
    - Provider Write
    - Enable Account
    - Remote Enable
    - Edit Security

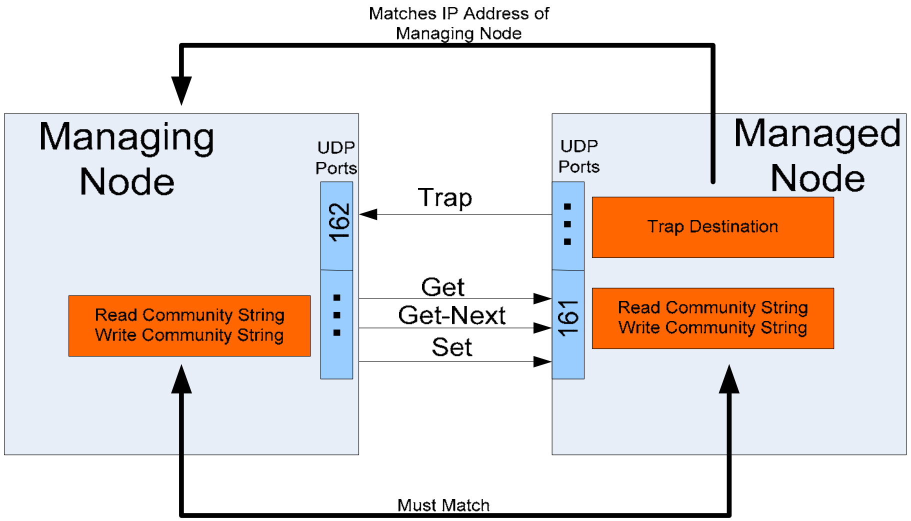
WMI/DCOM Security Deta

- Authentication
  - **Services:** NTLM, Kerberos
  - **Levels:** Default, None, Connect, Call, Packet, Packet Integrity, Packet Privacy
- DCOM Security
  - Authorization
  - Impersonation
- Namespace Security
  - **Execute Methods**: Permits methods that are exported from the WMI classes or instances to be run.
  - **Full Write**: Permits full read, write, and delete access to all WMI objects, classes, and instances.
  - **Partial Write**: Permits write access to static WMI objects.
  - **Provider Write**: Permits write access to objects that are provided by the provider.
  - **Enable Account**: Permits read access to WMI objects.
  - **Remote Enable**: Permits remote access to the namespace.
  - **Read Security**: Permits read-only access to WMI security information.
  - **Edit Security**: Permits read and write access to WMI security information.
- Hosting Model
  - LocalSystem
  - NetworkService
  - LocalService



Windows SNMP Security Overview

- Based on SNMPv1
- By default, Windows SNMP support is not installed
- Uses an SNMP Community String over the network in clear text, which is inherently less secure
- SNMP security is not directly tied to Windows Local or Domain security credentials



SNMP

SNMP v1	**Basic Operations and Features**
Get	Used by the NMS to retrieve the value of one or more object instances from an agent
GetNext	Used by the NMS to retrieve the value of the next object instance in a table or a list within an agent
Set	Used by the NMS to set the values of object instances within an agent.
Trap	Used by agents to asynchronously inform the NMS of a significant event.
SNMP v2	**Additional Operations and Features**
GetBulk	Used by the NMS to efficiently retrieve large blocks of data.
Inform	Allows one NMS to send trap information to another NMS and to then receive a response.
SNMP v3	**Security Enhancement**
	User-based Security Model (USM) for SNMP message security.
	View-based Access Control Model (VACM) for access control.
	Dynamically configure the SNMP agents using SNMP SET commands.

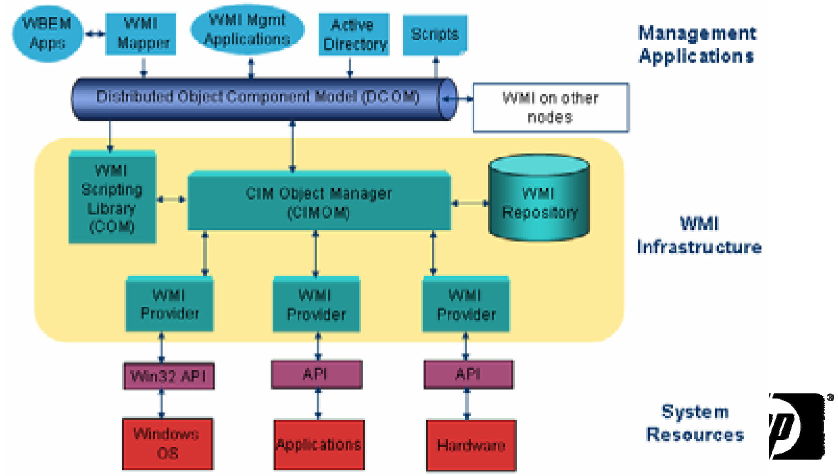
Windows Management Instrumentation

What is it WMI?

- Microsoft's framework for supporting WBEM standards
- Based on Windows OS security
- Supported by DCOM and WS-Management transports
- Part of Microsoft OSes and being established by Microsoft as their management standard

Customer Benefits

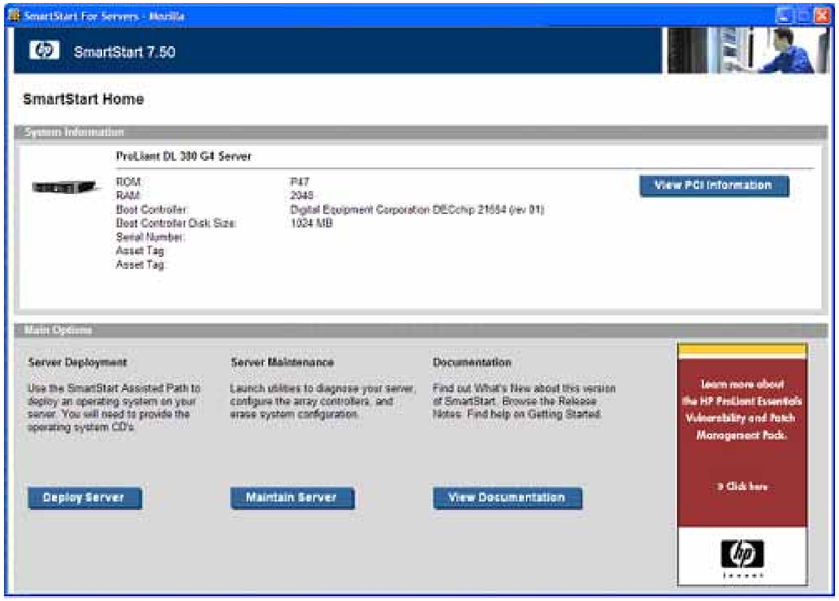
- Security integrated with Windows security
- Broad set of standard management information
- Integrated with Windows OSs



HP Insight Management WBEM Providers

Deployment

- **WBEM Providers Bundle**
  - –The WMI Providers—server, storage, and network—are packaged as a Smart Component that enables you to install, uninstall, and control the version of the WMI Providers as a single entity.
- **Perform pre-installation checks:**
  - – Be sure that the target server is on the supported hardware list.
  - – Be sure that the target server has a supported OS installed.
  - – Be sure that the target server has the appropriate HP software dependencies installed.
  - – The PSP must be installed before the WMI support bundle.
- **The WMI Providers can be uninstalled using the Windows® Add or Remove Programs interface.**



SmartStart For Servers - Mozilla

SmartStart 7.50

SmartStart Home

System Information

ProLiant DL 380 G4 Server

ROM:	P47
RAM:	2048
Boot Controller:	Digital Equipment Corporation DECchip 21554 (rev 01)
Boot Controller Disk Size:	1024 MB
Serial Number:	
Asset Tag:	
Asset Tag:	

View PCI Information

Main Options

Server Deployment

Use the SmartStart Assisted Path to deploy an operating system on your server. You will need to provide the operating system CD's.

Deploy Server

Server Maintenance

Launch utilities to diagnose your server, configure the array controllers, and erase system configuration.

Maintain Server

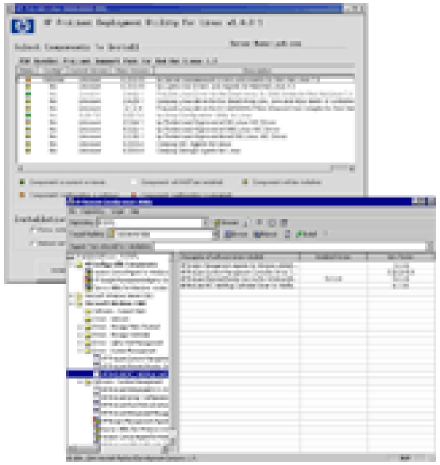
Documentation

Find out What's New about this version of SmartStart. Browse the Release Notes. Find help on Getting Started.

View Documentation

Learn more about the HP ProLiant Essentials Vulnerability and Patch Management Pack.

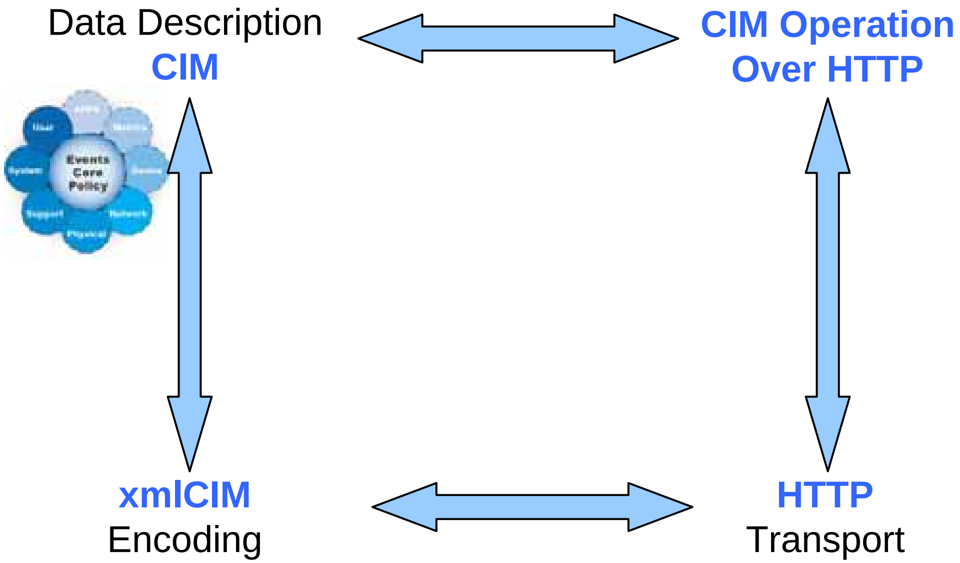
> Click here



WBEM Quick Overview

Web-Based Enterprise Management (WBEM) is a set of management and Internet standard technologies developed to unify the management of enterprise computing environments.

DMTF distributed management task force, inc.



Data Description
CIM

CIM Operation
Over HTTP

xmlCIM
Encoding

HTTP
Transport

WBEM is a set of technology specifications:

- CIM: The Common Information Model (CIM) is a conceptual information model for describing managed elements that are not specific to a particular implementation. Current version of CIM is version 2.8, version 2.9 pending.
- CIM Operations over HTTP: This specification defines a set of operations on the CIM data model (Query Properties, Receive Alerts, Control/configuration).
- xmlCIM: Specification for the encoding the CIM data model in XML. This specification also include operations performed on the data model (Query Properties, Receive Alerts, Control/configuration).
- HTTP: Defined as the standard transport for WBEM management data.

DMTF Board Members: 3Com, BMC, Cisco, Dell Computer Corp., Hewlett-Packard Company, IBM / Tivoli Systems, Inc., Intel Corporation, Microsoft Corporation, NEC Corporation, Novell, Oracle, Sun Microsystems, Inc., Symantec Corporation

Enterprise

One Voice

Solution