# Role of IPMI, SMASH, and WS-Management in HP ProLiant remote server management

technology brief, 3rd edition

# Abstract

Since the introduction of remote server management, both the technology from vendors and requirements of IT organizations have changed dramatically. Management tools are being deployed today in much greater volumes to improve system availability and IT operational efficiency in data centers and remote server locations. Consequently, a wide variety of management tools are now part of server purchase decisions.

As server technologies have multiplied in the areas of auditing, security, remote access, automation, individual server management, and management of multiple systems, the need to converge on a consistent solution has emerged. Customers need standardization to improve operational efficiency in heterogeneous environments and to perform certain commodity functions in a common way.

Unfortunately, multiple server management specifications are in development and contending for industry standard status. The primary contenders are the Intelligent Platform Management Interface (IPMI) over LAN specifications, Systems Management Architecture for Server Hardware (SMASH), and Web Services for Management (WS-Management). After contributing significantly to the development of these specifications, HP is strategically incorporating the industry-wide initiatives of Systems Management Architecture for Server Hardware (SMASH) and WS-Management into its management tools to address customer requirements for security, interoperability, and ease-of-use.

This technology brief describes the IPMI, SMASH SM CLP, and WS-Management initiatives, how they relate to other management protocols, and why HP has chosen to implement these initiatives for remote server management.

# Acronyms in text

The following acronyms are used in the text of this document.

| Acronym | Acronym expansion |
|---|---|
| BMC | Baseboard Management Controller |
| CLP | Command Line Protocol |
| CIM | Common Information Model |
| DMTF | Distributed Management Task Force |
| HTTP | Hyper Text Transport Protocol |
| HTTPS | Hypertext Transfer Protocol over Secure Socket Layer |
| IAB | Internet Activities Board |
| IETF | Internet Engineering Task Force |
| iLO | integrated Lights-Out |
| IPMI | Intelligent Platform Management Interface |
| LAN | Local Area Network |
| MIB | Management Information Base |
| OS | Operating System |
| RFC | Request for Comments |
| RMCP | Remote Management Control Protocol |
| SSH | Secure Shell |
| SSL | Secure Socket Layer |
| SIM | HP Systems Insight Manager |
| SM CLP | Server Management Command Line Protocol |
| SMASH | Systems Management Architecture for Server Hardware |
| SMWG | Server Management Working Group |
| SNMP | Simple Network Management Protocol |
| TCP/IP | Transmission Control Protocol / Internet Protocol |
| UDP | User Datagram Protocol |
| WBEM | Web-Based Enterprise Management |
| WMI | Windows Management Instrumentation |
| WS-Management | Web Services for Management |
| XML | Extensible Markup Language |

# Customer requirements for management standards

Many customers might question why they should have any interest in the standards that HP chooses to use in its management tools such as HP Systems Insight Manager (SIM) and Integrated Lights-Out (iLO) processors. After all, this is technology that is not directly visible by the customer. However, as products have evolved and as management capabilities have become increasingly important, the reality is that current management applications rely on underlying software models and protocols that often do not meet the requirements of IT managers. Customers have a need for:

- Standardized ways of representing and transmitting management data independent of the server hardware, management console, or the state of the server. With current management tools, customers might have several different management consoles and tools to manage servers from different vendors, leading to confusion or an increased need for training.
- More secure and reliable protocols for communicating between management consoles and the managed devices. Administrators need to be able to manage servers regardless of their physical location. Administrators also need to ensure that their ability to access servers remotely does not increase the vulnerability of the server to viruses or other problems.
- Management applications that are easier to configure to reduce initial configuration times and the number of mistakes made.

# Components of a management standard

Management standards generally define either a data model (a schema), or a management protocol, or both.

## Data model

The type and structure of management information that describes a managed system is known as a data model. The data model standard used in many management applications is the Common Information Model, or (CIM),[1] which is defined by the Distributed Management Task Force (DMTF). CIM is a data model which is used to represent the elements of a system, including hardware, operating system (OS), and applications. It defines elements from network and storage hardware, as well as servers. It also defines the associations between those elements. Because it defines the management data in a common way, it enables management tools from a variety of vendors to be platform independent.

CIM is the underlying data model for management initiatives such as Web-based Enterprise Management (WBEM) and SMASH. CIM is also the data model that tools such as HP SIM and HP OpenView use.

## Management protocol

The protocol defines how the data is formatted when it is requested and transmitted across the network (for example, the format for a GET call or a SET call). The use of a standard protocol allows management applications to communicate, and the use of a common data model gives them a common language.

Command line protocols, such as the SMASH Server Management Command Line Protocol (SM CLP) are human-oriented. Command line protocols allow IT administrators to interrogate and control systems directly, such as reading the iLO system log to find server status or show the health of a

[1] This should not be confused with the HP Systems Insight Manager (SIM) management tool, which evolved from a tool called Compaq Insight Manager, or CIM.

server. Administrators can also use scripting with command-line protocols to directly manage a wide range of servers interactively.

Programmatic protocols, such as WS-Management,[2] are machine-oriented and enable applications to manage the systems. Applications use programmatic protocols to talk to each other and to the hardware instrumentation. For example, HP SIM uses WS-Management to interact with the iLO management processors.

## Management initiatives

Often, these management standards are bundled together as initiatives which address multiple facets of a management domain such as server management. For example, the SMASH initiative is actually a suite of specifications that includes SM CLP, SM Management Element Addressing, SM CLP-to-CIM Mapping specification, and so on. Initiatives such as SMASH and IPMI are specific to server management, while the Storage Management Initiative (SMI) is specific to storage. Table 1 gives examples of prevalent management initiatives, their associated protocols, and data models.

**Table 1.** Examples of prevalent management initiatives

| Initiative name | Protocol | Data model |
|---|---|---|
| Systems Management Architecture for Server Hardware (SMASH) | SMASH CLP | SMASH profiles (a subset of CIM) |
| Simple Network Management Protocol (SNMP) | User Datagram Protocol (UDP) over Internet Protocol (IP) | Management Information Base (MIB) |
| Web-based enterprise management (WBEM)<br>**NOTE:** WBEM is an umbrella term for several management technologies. This table shows a single example of protocol and data model. | CIM-Extensible Markup Language (XML) | CIM |
| Intelligent Platform Management Interface (IPMI) | Remote Management Control Protocol (RMCP) over UDP | IPMI data structures |
| Storage Management Initiative (SMI) | CIM-XML | SMI-S profiles (a subset of CIM) |
| Desktop and Mobile Architecture for Managing System Hardware (DASH) | WS-Management | CIM |

# Related industry standards and specifications

This section provides some background information about related management initiatives other than IPMI, WS-Management, and SMASH.

Simple Network Management Protocol (SNMP) and WBEM are existing standards used for some types of management. SNMP is a standard of the Internet Engineering Task Force (IETF), while many other management standards and initiatives, such as WBEM and SMASH, are specified by the DMTF.

[2] Microsoft provides a command-line tool named Windows Remote Management (WinRM) for use by administrators, allowing the WS-Management protocol to be used in a command-line manner. This is mentioned in the WS-Management section titled "Native OS operation" later in the paper.

The DMTF is a well recognized industry standards body for management-related technology that defines the data model and protocols for server management. HP is a member of the Board of Directors and is actively involved with DMTF in the development of various standards and specifications for managing enterprise environments.

## SNMP

SNMP is a management standard in widespread usage for a variety of management needs, especially for network management. The benefit of SNMP is that it is a lightweight, mature standard, is non-proprietary, and is broadly supported. SNMP was first approved in 1990 by the IETF.

SNMP provides a standard definition of the types and formats of messages transmitted to and from devices, using a transport protocol of User Datagram Protocol (UDP)/Internet Protocol (IP) and a data model known as the Management Information base (MIB). Most industry-standard servers support SNMP and MIBs today. The MIB data structures use discrete islands of information that are adequate for representing devices, but do not relate to other components such as applications, services or their associations to present a holistic system view. Most third-party vendors tend to loosely follow the industry standards for the development of MIBs. This may require the end user to change or customize the MIBs to properly integrate them with a management application such as HP SIM.

The UDP transport mechanism used with SNMP provides no guaranteed delivery of alerts, events, or queries. As a result, SNMP notifications may occasionally be lost or dropped completely. For this reason, many management applications implement device status polling as a supplement to alerts.

In addition, the most commonly used versions of SNMP, SNMP v1 and v2, do not provide security features such as message authentication and encryption. Version 3 adds more robust security but has not been widely adopted for server management.

Managing servers with SNMP-based agent configurations can be a labor intensive process without some level of automation within the management console.[3] For example, customers have to set community strings and trap destinations on each node. Component information using MIBs has to be identified and compiled into the server environment in advance, so IT administrators are limited to the information that the developer instrumented into the server. In addition, detailed MIBs are often vendor-specific, so the same information may vary from product to product or vendor to vendor. Also, managing servers through a firewall requires administrators to open up UDP ports, which is often prohibited by IT security policies, unlike opening TCP ports which are used by web protocols such as HTTP or HTTPS.

## WBEM

WBEM is a set of management and Internet standard technologies that have been brought together by the DMTF to unify the management of enterprise computing environments.[4] The core set of WBEM standards includes a data model (CIM) and a management protocol. The original WBEM protocol, CIM-XML, is in widespread use on Linux and Unix systems and is the foundation for the storage management initiative specification (SMI-S). WBEM has been broadened to include WS-Management as an alternative management protocol.

WBEM is extensible. HP provides WBEM implementations for a variety of server operating systems including HP-UX, Linux, Tru64, and OpenVMS. HP also provides SMI-S compliant storage instrumentation. There are many other implementations of WBEM including Windows Management Instrumentation (WMI), Pegasus, OpenWBEM, and Solaris WBEM Services.[5] Each implementation

[3] For example, HP Systems Insight Manager allows configuration of community strings and trap destinations for multiple ProLiant or BladeSystem servers through a feature named "Configure or Repair Agent Settings."
[4] DMTF WBEM Definition, 2005, www.dmtf.org/standards/wbem.
[5] More information about these implementations is available from the web pages listed in the "For more information section."

supports a set of standard classes defined in CIM and a set of proprietary extensions specific to the implementation.

WBEM is generally viewed as more versatile than previous management standards such as SNMP because of its richer data model, which includes associations and inheritance, and its web-based protocols. Security can be built into WBEM more simply than into SNMP, because it can leverage more secure, web-based protocols such as HTTPS.

# IPMI overview

IPMI is a management architecture focused on server hardware, originally developed jointly by HP and Intel in 1998; NEC and Dell became promoters soon thereafter. IPMI began as a specification to define instrumentation and management of key environmental elements such as fan, temperature, power supply, and other embedded health functions. IPMI 1.0 makes this information accessible locally from the OS or from an optional Baseboard Management Controller (BMC).[6] Interfaces for remote management were not within the scope of IPMI 1.0, which deals exclusively with internal server management.

IPMI 1.5 introduced IPMI over LAN in 2002. It defined some basic remote management capabilities such as remote control of system power, access to event logs, and alerting for environmental conditions. Because IPMI was designed for low-end, lowest-cost manageability controllers, rather than embrace the heavier-weight network standard protocol Transmission Control Protocol/Internet Protocol (TCP/IP), IPMI 1.5 introduced an entirely new network protocol known as Remote Management Control Protocol (RMCP). RMCP is a non-routable protocol that requires an IPMI proxy service to send messages beyond its own subnet. This requires additional network infrastructure to manage devices using IPMI, and provides relatively weak reliability and security using RCMP over UDP packets. RMCP is unique to IPMI and does not use industry standard protocols adopted for internet use, such as TCP/IP, or more secure protocols such as Secure Shell (SSH) or Secure Sockets Layer (SSL).

In 2004, IPMI 2.0 introduced Serial Over LAN console redirection which enabled remote access to the system's serial port console over the network. IPMI 2.0 provides for an IPMI remote console utility using RMCP for data encryption and authentication. IPMI protocols are only supported by a few management consoles, whereas web browser and Telnet/SSH utilities are widely available.

Each of these IPMI specifications includes a small number of mandatory features and a larger number of optional capabilities to claim IPMI compliance. A customer requirement referencing an IPMI specification will not necessarily ensure interoperability.

IPMI consists of a low-level internal interface and byte-oriented messages over the network. The local information access inside the server is well-supported via IPMI device drivers and providers in the OS to populate the server management information. To support access to IPMI information directly from the BMC over the network, special proxy applications must be developed and used in order to interface IPMI servers with more widely-adopted management protocols such as SNMP and WBEM.

# SMASH overview

SMASH is another standard architecture and set of management protocols from the DMTF. In late 2003, to address a need for cross-platform standards to manage servers from multiple vendors, the DMTF formed the Server Management Working Group (SMWG). HP, IBM, Intel, Dell, OSA Technologies and Newisys are among the founding members of the SMWG. Because of its acceptance by so many vendors and users, SMASH is expected to have wide industry adoption.

[6] Baseboard Management Controller is the IPMI terminology for a management processor such as iLO.

SMASH is specifically designed to manage systems using a lightweight CIM object model. The first part of this standard, SM CLP, was finalized in 2005 and includes a direct mapping to a subset of the CIM Schema. SMASH also includes a set of profiles used to standardize the components of the DMTF's CIM object model, which represents system components such as fans, processors, memory, and blade enclosures. These profiles can be used by any DMTF protocol to represent different systems in a consistent and interoperable manner. The DMTF's Server Management Working Group plans to standardize on a programmatic interface based on the same lightweight CIM object models in a future SMASH release.

Most management tool vendors directly support CIM but do not support IPMI. A specification is being developed to define mapping of IPMI data to CIM objects. When this specification is complete, IPMI systems and non-IPMI systems will be manageable using the SM CLP and SMASH programmatic interfaces.

The SM CLP consists of human-oriented commands that are also suitable for use with scripts. SM CLP supports network access through Telnet and also SSHv2 for secure access. SMASH specifies only industry-standard routable protocols such as TCP/IP, which allow packets to be forwarded from one network to another, a key requirement for easy integration in most enterprise networks.

The SM CLP provides a lightweight command line syntax that allows systems from different vendors to be represented in similar ways. Products from server vendors, including standalone servers, blades, rack servers, and partitionable servers, will be able to support SM CLP commands. As a result, users on a management station or a client will be able to execute common operations such as system power-on and power-off, system log display, boot configuration, and text-based remote console using the same commands across disparate vendor platforms. Since SMASH standardizes only the messages exchanged with management applications, it provides a high degree of interoperability for performing functions, regardless of the actual feature implementation.

## WS-Management overview

WS-Management is emerging as the preferred programmatic interface for system management. Because it is a web services-based specification, WS-Management provides the security and routability characteristics inherent in web-based protocols and makes it possible to build distributed server management solutions that are OS-independent. It provides a common way for systems to access and exchange management information across the entire IT infrastructure—hardware, software, and applications.

The WS-Management specification[7] was originally developed by a small group of companies outside of the DMTF and was standardized and released by the DMTF in April 2006. A related specification, the WS-CIM specification,[8] was released in December 2006. These specifications allow management applications to standardize the way they access of CIM data, including operation, enumeration, and alerting. In other words, the WS-Management specification exposes CIM resources by means of a set of web-services protocols.

WS-Management is essentially structured XML (based on SOAP[9]) that can be sent to a web server to perform management functions. The nature of the structured SOAP protocol is such that it separates the functional aspects of *how* data is communicated *from the data itself* that is being transmitted (for example, CIM data).

---

[7] The WS-Management Specification is available on the DMTF website at www.dmtf.org/standards/published_documents/DSP0226.pdf

[8] The WS-CIM specification is available on the DMTF website at www.dmtf.org/standards/published_documents/DSP0230.pdf

[9] Originally SOAP was an acronym meaning Simple Object Access Protocol, however the full definition was dropped with Version 1.2 of the standard and it is now referred to only as SOAP.

There are several advantages to using WS-Management rather than other programmatic management protocols:

- Provides network security (authentication, integrity, and confidentiality) and reliable delivery
- Simpler and more versatile for vendors to implement than using CIM-XML with WBEM
- Allows subscription-based events to reduce administrative configuration tasks
- Supported by operating systems from Microsoft® and other vendors to provide maximum compatibility and to enable broad industry adoption

## Security and reliability

The WS-Management specification is not tied to any specific transport mechanism, so that any SOAP-enabled transport can be used as a carrier for WS-Management messages. However, the specification does establish common usages over either HTTP or HTTPS.

Because it uses the standard web services TCP ports—port 80 (HTTP port) and port 443 (HTTPS port)—it is a "firewall-friendly" protocol. For example, if IT administrators are using servers that can only have port 443 open because of firewall restrictions, the WS-Management protocol provides complete access between the server and the management application. Administrators can use the standard encrypted HTTP port without the need to open any additional ports on the managed server.

WS-Management supports mutual authentication, integrity, and encryption through the use of SSL. It also supports Kerberos, an authentication technology that is supported natively in many operating systems such as Windows Server 2003. The use of Kerberos enables single-sign-on capabilities to simplify security configuration.

WS-Management provides guaranteed event delivery and a response mechanism, unlike the UDP-based SNMP packets. It also uses a routable protocol, so that packets can be forwarded from one network to another.

## Versatility

WS-Management is a lightweight protocol, requiring less overhead to implement than using CIM-XML in a WBEM environment. Therefore, it can be easily implemented in a variety of environments from embedded management processors such as iLO to management applications such as HP SIM. The likely result is that WS-Management will be implemented across a wide variety of platforms and applications.

The WS-Management specification promotes interoperability between management applications and managed resources by identifying a core set of web-service specifications and usage requirements to expose a common set of operations that are central to all systems management. By using web services to manage IT systems, deployments that support WS-Management will enable IT managers to remotely access devices on their networks—everything from silicon components and handheld devices to PCs, servers and large-scale data centers. For instance, some of the open source versions of WBEM such as Pegasus have extensions available for WS-Management support, so that the same systems that have WBEM support can potentially be managed using the WS-Management protocol.

## Subscription-based events

The SNMP management standard requires MIBs to be pre-compiled in advance and requires management processors (such as iLO) to be configured individually for traps and alerts. WS-Management, on the other hand, includes the ability to subscribe to resources or services for events so that administrators can set different requirements or actions for each resource. For example, a management application such as HP SIM could include an event collector that uses the WS-Management protocol to collect events from multiple servers. The subscription capability simplifies the way that an administrator configures server management by eliminating the need for

administrators to configure community strings and trap destinations, one of the most problematic configuration issues with HP SIM.

### Native OS operation

Microsoft provides native support for WS-Management in Windows Server 2003 R2, Microsoft Windows Vista, and Longhorn (the upcoming version of Windows Server). Along with the native support for WS-Management in its operating systems, Microsoft also provides a command-line tool named Windows Remote Management (WinRM) for use by administrators. The WinRM is a front-end program that formats and sends WS-Management requests to the OS and displays the results in a command-line window, allowing administrators to perform scripting functions with WS-Management. Tools like this will allow server hardware vendors or third-party vendors to integrate WS-Management easily into their solutions.

Various Linux groups, such as Novell with SUSE Linux, are supporting WS-Management and developing open source implementations of it. Microsoft and Novell are working together to make it easier for customers to manage their mixed Windows and SUSE Linux Enterprise environments by collaborating on standards-based solutions. Novell ZENworks® Orchestrator and Microsoft System Center Operations Manager 2007 plan to incorporate WS-Management this year.[10]

## Implementation within HP ProLiant Essentials and iLO

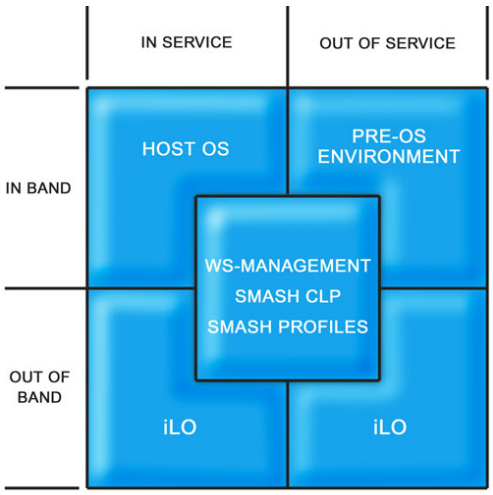
HP is committed to making ProLiant and BladeSystem the best-managed industry-standard servers available. To do this requires a consistent, standards-based approach that integrates protocols such as SMASH CLP and WS-Management with HP applications to provide easy-to-use, interoperable management tools.

HP believes that the SMASH CLP and the WS-Management standard are more robust than other emerging standards such as the IPMI over LAN specifications, fit well with technology standards that currently exist in customer environments, and will be supported on a wide range of systems and management applications.

HP expects to provide common access to instrumentation regardless of whether servers are in-band, out-of-band, in-service, or out-of-service (Figure 1). Through incorporating standards such as WS-Management and SMASH, HP expects to be able to provide this level of functionality.

[10] See the press release dated 12 Feb 2007, at www.novell.com/news/press/item.jsp?id=1284&locale=en_CA.

**Figure 1.** HP is moving toward an environment in which the same management protocols can be used regardless of the state of the server or how it is accessed.




## Integrated Lights-Out support

HP delivered the first implementation of SMASH-based technology with the ProLiant iLO firmware version 1.70. HP iLO currently provides complete support for the SM CLP specification for all iLO configuration and control functionality on HP ProLiant servers. It allows customers to use SM CLP to configure, update, and operate iLO features on HP ProLiant ML/DL 300 and 500 servers and on ProLiant BL server blades. HP is not planning any WS-Management support for iLO; however there will be WS-Management support for iLO 2.

The iLO 2 management processor supported the draft SM CLP specification in firmware version 1.00 and is SM CLP compliant in firmware version 1.30. The iLO 2 processor will incorporate WS-Management in its firmware release v1.30 (1H 2007). It will replace the existing XML interface for the iLO 2 processor and expose IPMI sensors. This will allow HP SIM to access any IPMI sensor through the WS-Management interface, such as sensors, fans, power switch operations, and the unit identification (UID) light. The exact type of and number of IPMI sensors depend on the server. Future firmware revisions are expected to broaden the WS-Management support to expose additional capabilities such as the ability to make iLO configuration changes and support single-sign on through the Kerberos authentication technology.

The iLO management processor on ProLiant servers and all management processors on Integrity servers currently offer technology that is superior to IPMI over LAN. However, because IPMI specifications are suitable for some internal server management functions, HP will use IPMI internally and over LAN selectively in HP servers that are already using IPMI.

## HP-SIM support

HP-SIM incorporates support for WS-Management in SIM v5.1. With this release, HP-SIM can access the operations that the updated iLO firmware has exposed by the WS-Management protocol. (As stated in the previous section, this includes fan information, the ability to power on, power off, restart, and toggle the UID light on or off.) HP plans to enhance the use of WS-Management significantly in future releases. It is expected that this will include expanded functionality such as additional iLO operations as well as the ability to expose its own management data and operations to other applications such as HP OpenView.

Other related management components, such as management agents, will also be incorporating the use of the WS-Management protocol (through WMI providers) in the near future. Over time, HP anticipates that SNMP will be phased out in agents and management processors, although applications such as HP SIM will support SNMP for an extended time to ensure compatibility with older, legacy hardware.

# Summary

The promise of industry standards is that they can lower vendor and end-user costs, allow vendors to innovate on a common foundation for improved value to the customer, and allow customers to choose the best solution for them while minimizing the chance of being locked in to a proprietary solution.

HP is incorporating the industry standards of SMASH SM CLP and WS-Management across their ProLiant and BladeSystem product lines and ProLiant Essentials management tools. HP is not alone in incorporating these standards: major operating system suppliers such as Microsoft and Novell are also incorporating these standards into their products.

The SMASH SM CLP and WS-Management standards were developed with a clear purpose and vision to be platform-independent, industry-standard management architectures that provide consistent management interfaces in heterogeneous environments. This allows customers to manage hardware from multiple vendors independent of OS state, system state, server system topology and access mechanism. It addresses environments common to data centers and centralized IT management of distributed systems. Customers will also benefit from the increased security, reliability, and reduced configuration times that are enabled through these standards.

# For more information

For additional information, refer to the resources listed below.

| Source | Hyperlink |
|---|---|
| DMTF webpage includes information about:<br>• SMASH initiative<br>• WS-Management<br>• WBEM | www.dmtf.org/home |
| Intelligent Platform Management Interface | http://developer.intel.com/design/servers/ipmi/index.htm |
| Integrated Lights-Out processors | www.hp.com/servers/iLO |
| Internet Engineering Task Force<br>• SNMP initiative | www.ietf.org |
| HP Systems Insight Manager | www.hp.com/go/hpsim |
| WBEM implementations | |
| • HP WBEM Services | www.hp.com/go/wbem |
| • Pegasus | www.openpegasus.org/ |
| • OpenWBEM | http://openwbem.org/ |
| • Solaris WBEM Services | www.sun.com/software/solaris/wbem/ |
| • Windows Management Instrumentation (WMI) | www.microsoft.com/whdc/system/pnppower/wmi/default.mspx |
| Storage: | |
| Storage Management Initiative | www.snia.org/smi/home |
| HP Storage Essentials | http://h18006.www1.hp.com/storage/smisproviders.html?jumpid=reg_R1002_USEN |

# Call to action

Send comments about this paper to TechCom@HP.com.



TC070402TB, April 2007