HP VMware ESXi management environment

integration note

Abstract

VMware virtualization technology has changed the computing landscape, transforming IT infrastructure with market-leading virtual machine products. VMware ESXi is a next-generation thin architecture, providing an efficient foundation for building a dynamic, automated data center. HP has tightly integrated ESXi into ProLiant platforms, simplifying virtualization deployments.

Introduction

VMware ESXi is a "thin" architecture that removes the traditional console OS, improving reliability by eliminating many common security vulnerabilities. The HP integrated VMware ESXi ultra-thin hypervisor software is shipped on a USB key pre-installed in the internal USB port of the HP ProLiant server. The system boots directly from the USB key, so new servers are ready to run VMware ESXi right out of the box, providing greater speed and simplicity for customers new to virtualization. A menu-driven interface eases host configuration and setup for VMware ESXi. This method of distributing virtualization technology removes time-consuming installation steps, simplifies host configuration, and increases capacity expansion for customers who already use VMware's data center virtualization and management suite, VMware Infrastructure (VI).

HP integrated VMware ESXi provides seamless, out-of-the box integration with HP Systems Insight Manager (HP SIM), the industry's only unified storage and server management platform. HP Systems Insight Manager 5.2, and later, software incorporates user-friendly features and an improved installation process, and it supports association and discovery for VMware ESXi. Enhanced hardware alerting and inventory management allows customers to actively receive information about the health of their ProLiant servers. This enables companies to eliminate risk, lower potential costs, and resolve server problems before they result in actual downtime.

HP implementation of WBEM in ESXi

On its own, VMware ESXi provides a simplified approach to managing server compute nodes with a robust set of standards-based management capabilities, freeing the administrator from day-to-day tasks. Administrators can also use the integrated remote command line interface (CLI) for storage, network, and host configuration, as well as for maintenance, patches and updates. VMware ESXi includes several key management components and approaches:

- Remote Command Line Interface (Remote CLI)
- Industry-standard monitoring protocols such as the Common Information Model (CIM)
- Independent Software Vendor (ISV) solutions that leverage standard interfaces, the VI application program interface (API) and VMware Consolidated Backup

HP adds to the manageability of VMware ESXi by integrating this thin architecture within ProLiant platforms, delivering active management and consolidated lifecycle management for a consistent, reliable experience. The integrated ESXi hypervisor incorporates HP Insight Management Web-based Enterprise Management (WBEM) providers. WBEM providers use the CIM standard to represent systems, networks, applications, devices, and other managed components in an object-oriented fashion. HP based its HP Insight Management WBEM Providers on the SMASH and SMI-S standards,[1] extending those data models as necessary to support features specific to ProLiant platforms.

HP Insight Management WBEM Providers (Insight Providers) are pre-installed along with integrated VMware ESXi on the internal USB key to provide active hardware management using HP SIM. These

---

[1] More information about CIM, Systems Management Architecture for Server Hardware (SMASH), and Storage Management Initiative Specification (SMI-S) is available in Appendix A.

WBEM-based providers report hardware monitoring data on a regular basis without prompting, providing the most up-to-date server state information possible.

Figure 1 shows the Systems Management software included with the HP integrated VMware ESXi. HP SIM and Virtual Center are available separately.

Figure 1. Software included with HP integrated VMware ESXi
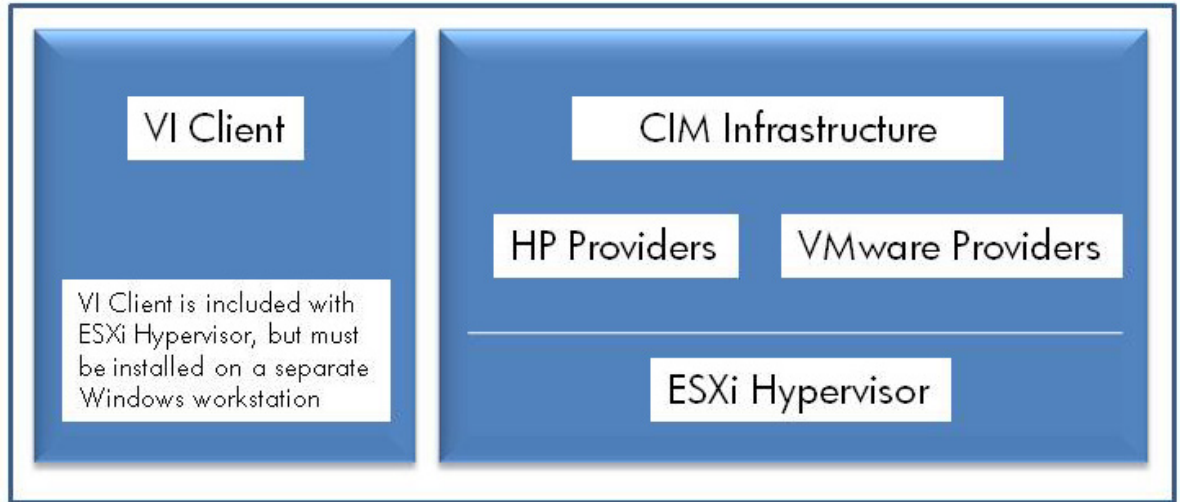
HP server information available using WBEM

Insight Providers collect data from sources such as drivers and system firmware to populate the CIM data model. HP SIM receives the system hardware inventory and hardware health monitoring data. Table B-1 in Appendix B lists the component information provided by the environment by data source.

Proactive notification of server issues

An indication is a Distributed Management Task Force (DMTF) concept that formalizes an event representation into an instance of a CIM class. An instrumentation provider or the CIM Object Manager (CIMOM) is written to monitor changes in a state and generate an instance of an indication to notify the management application, for instance HP SIM, of particular events. In order for the management application to receive event notification from the Insight Providers for ESXi, a subscription to WBEM events must be initiated from the management application. Once the subscription is made, the Insight Providers for ESXi will start delivering indications to the management application server as events occur. The server consolidated health status is updated as the indication is delivered. Every event or indication is delivered with the following information from the computer system generating the event:

- Event time
- Computer system name
- HP Insight Management WBEM Provider version
- Computer system IP address
- Computer system OS name
- Computer system serial number and Globally Unique Identifier (GUID)
- Computer system product ID and model name

3

- Severity
- Recommended action
- Probable cause

The Insight Providers deliver component information such as temperature, status (failed, repaired, degraded), and redundancy. This data comes from sources such as the main (base server) system, processor (CPU) subsystem, fan subsystem, power supply subsystem, and memory subsystem.

HP integrated VMware ESXi provider and profile summary

The Insight Providers for ESXi collect management data from the ProLiant base server system and its processor, fan, power supply, and memory subsystems. Information provided includes properties and health status for all individual devices and redundant sets per subsystem, plus real-time event notifications.

The Insight Providers deliver in-depth hardware management, inventory data, system state, and event notifications through HP SIM. The providers will report a range of server information such as server model, name, serial number, IP address, OS, and universal unique identifier (UUID), including overall server or consolidated health status through the HP SIM systems page. Each subsystem provider will report individual configuration and status information through the HP SIM property pages.

The Insight Providers conform to the Systems Management Architecture for Server Hardware (SMASH) and Storage Management Initiative Specification (SMI-S) standards. The Insight Providers extend the CIM data model to provide administrators with information specific to ProLiant platforms. The Insight Providers collect data from various sources such as drivers and system firmware to populate the data model. HP SIM 5.2 or later provides seamless integration with the Insight Providers for ESXi, including identification, inventory, event monitoring, and status polling.

ProLiant server information available using VMware's Virtual Infrastructure Client and Virtual Center

Two versions of management software are also available directly from VMware:

- VMware ESXi includes a client application utility named Virtual Infrastructure (VI) Client. VI Client is a system management program primarily focused on the management of virtual machines on individual servers with certain hardware management capabilities included. VI Client uses VMware CIM providers to retrieve server hardware component information.
- Virtual Center is another VMware management application available from the VMware website or from the installation CD. Virtual Center is a system management program primarily focused on the management of virtual machines with certain hardware management capabilities included. Virtual Center is capable of simultaneously managing multiple servers. It uses VI Client as its primary user interface to access each server.

Currently, VI Client can display certain ProLiant server information by retrieving and decoding data using the standard Intelligent Platform Management Interface (IPMI). However, this interface is limited and there is more detailed ProLiant server information available that VI Client may display incorrectly or not display at all (depending on VI Client version) due to the HP IPMI OEM-specific data implementation.

Comparison of HP SIM with HP Insight Providers and VC/VI Client with VMware providers

The optimum system management environment for HP ProLiant servers is HP SIM with the HP Insight Providers. This configuration gives HP ProLiant servers a superior set of management capabilities.

Table B-1 in Appendix B provides a side-by-side comparison of the information available in each environment, sorted by data source.

Managing HP integrated VMware ESXi

With HP integrated VMware ESXi, ProLiant customers can plug new servers directly into their existing VMware VI3 environments, while ensuring active hardware management using Insight Providers pre-installed on the USB key.

HP integrated VMware ESXi does not provide support for the System Management Homepage (SMH). In place of SMH, HP SIM should be used to view management information for ProLiant servers running ESXi.

VMware ESXi provides a simplified approach to managing server compute nodes, with a robust set of standards-based management capabilities. Administrators can also use the integrated remote CLI for storage, network, and host configuration, as well as for maintenance, patches, and updates. The automatic configuration capabilities in VMware ESXi provide detection, discovery, and intelligent-default configuration.

HP integrated VMware ESXi management capabilities are numerous:

- Remote Command Line Interface. It is possible to manage VMware ESXi through a remote execution environment that can run VMware ESXi command scripts.
- Advanced manageability and usability features. Users can manage the entire virtualized IT environment with VMware ESXi.
- Virtual Infrastructure Client. Users can manage VMware ESXi, virtual machines, and (optionally) VirtualCenter Server with a common user interface.
- Virtual Infrastructure Web Access. VMware ESXi can be managed with simple Web interface (formerly known as the Management User Interface, or MUI).
- Virtual machine shortcuts. For self help, users have direct access to virtual machines through a Web browser.
- Remote devices. It is possible to install software in a virtual machine running on a server from the CD-ROM of a desktop.
- Agent-less Hardware Management with CIM. CIM provides a protocol for monitoring hardware health and status through VirtualCenter or CIM-compatible 3rd party tools.

Using HP-SIM to manage servers running ESXi

HP SIM 5.2 or later and the Insight Providers are fully integrated to support identification, inventory, event monitoring, and status polling. In order for HP SIM to successfully identify a VMware ESXi managed node, the user must enter system level WBEM credentials. The WBEM credentials can be entered three ways:

The "First Time Wizard"

When HP SIM is started for the first time, it raises the First Time Wizard. The First Time Wizard allows the user to enter a variety of HP SIM configuration parameters. The WBEM credentials entered here are applied globally (see Figure 2).

Figure 2. HP SIM First Time Wizard credential screen

Global Protocol Settings page – Options-->Protocol Settings-->Global Protocol Settings

A user may enter credentials in the global protocol settings page at any time. When discovery runs (default schedule is once daily) or when new nodes are discovered, the global WBEM credentials are used to identify WBEM on the managed node (see Figure 3). If the ESXi managed node has already been discovered and does not have WBEM listed as a management protocol, then the user must run **Options**-->**Identify**.

Figure 3. HP SIM Global Protocol Settings page

System Protocol Settings page

If the user does not supply credentials at the global level, then the user can declare the credentials at the managed node level. From the System page the user selects the "Tools & Links" tab, "System Protocol Settings." Once the system credentials are entered, the user must run "Identify" so that the credentials are validated (see Figure 4). The credentials will only be applied to the managed node that is selected.

Figure 4. HP SIM System Protocol Settings page

During the identification process, HP SIM determines if a managed node is running an ESXi operating system. If an ESXi operating system is running, HP SIM attempts to contact both the VMware providers and HP Insight Providers. HP SIM identification will create a path to these providers so that it can immediately contact and collect data from the appropriate providers.

The HP SIM Systems page provides an overview of the managed node. The Systems page summary includes IP and DNS information, links to additional management tools such as property pages, and WBEM events list. Figure 5 provides examples of how the HP SIM Systems page integrates with HP Insight Providers.

Figure 5. HP SIM Systems Page for an ESXi host server

HP SIM can subscribe for and receive WBEM indications. These indications are asynchronous alerts that give HP SIM users a real-time status for hardware components that are experiencing problems. Figures 6 and 7 provide an example of how WBEM indications are activated and deactivated. Figure 6 depicts an example of how these indications are reported using the HP SIM interface. Each indication or event in the Events list contains a link that will provide a detailed display of the indication content.

To create a subscription in the user interface, click **Options** -->**Events** -->**Subscribe to WBEM Events**. The user does not have to supply any specific information; it is generated by HP SIM.

Figure 6. Subscribing for WBEM indications using the HP SIM user interface
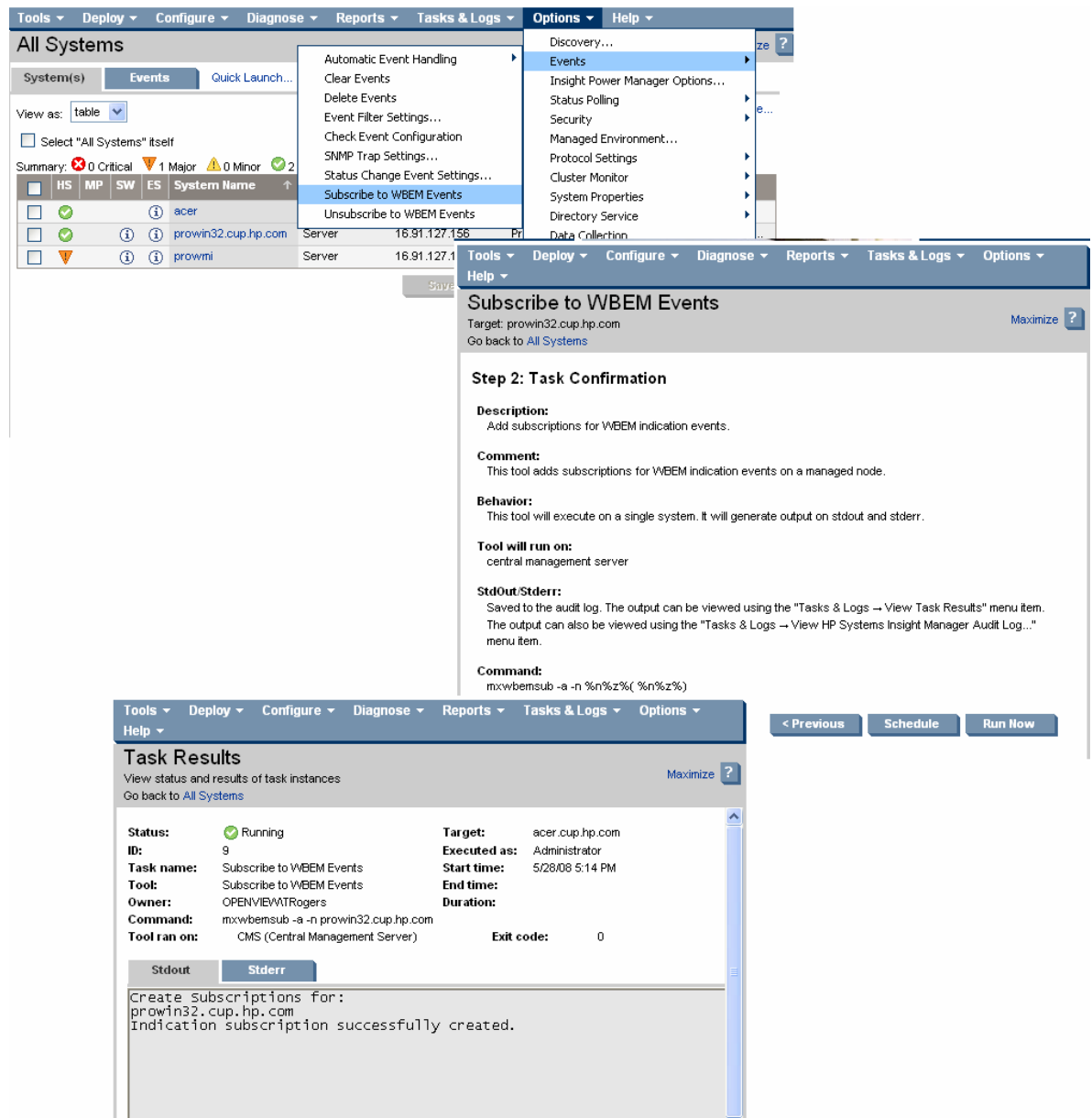
Alternatively, users may choose to create subscriptions using the CLI:

```
Mxwbemsub -a -n <node name>
```

Users can specify which HP SIM Central Management Server (CMS) is the destination address for the WBEM subscription. In the example shown in Figure 7, the HP SIM CMS is not declared and the local CMS is being used as the destination.

Figure 7. Subscribing for WBEM indications using the HP SIM CLI, and a list of existing subscriptions
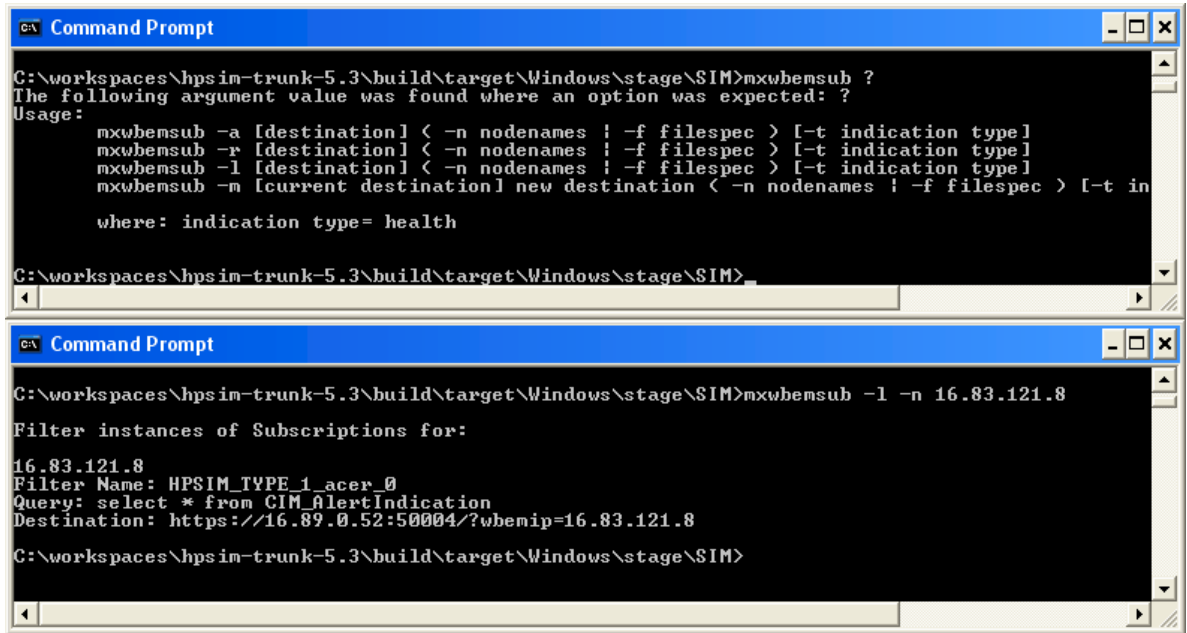
Status Polling

The Status Polling module allows HP SIM to keep status up to date and provides a timely and accurate depiction for users. The depiction uses status icons to indicate condition status; this allows the user to drill down through status screens following the top-level status through various levels to identify the specific instance of offending hardware. Figure 8 shows the status icons along with their associated severity level.

Figure 8. Status icons and their respective health status definitions
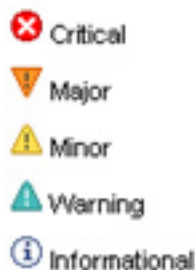
Every five minutes, HP SIM Status Polling collects an overall status value from the Insight Providers. This polling task collects the overall status from all WBEM protocol nodes. In Figure 9 the circled item shows the health status on the SIM systems page. This example indicates a Minor condition exists.

Figure 9. Health Status link

Identifying problems with hardware components

HP SIM, using HP Insight Providers, provides a way to identify malfunctioning hardware components. The Systems page Health Status link reflects the status reported by the providers. Select the Health Status link to navigate to the SIM Property Pages status tab. The following example illustrates an error status in HP SIM. Selecting the Health Status link launches the SIM property pages. The property page status tab then shows the error status is traceable to Power Supply 2, as shown in Figure 10.

Figure 10. Following a status to the offending hardware instance

Property pages

HP SIM Property pages (Figure 11) display overall server characteristics, status information, and configuration/inventory data. The Property page data, prepared and reported in real time, is exclusively WBEM data.

Figure 11. Property page examples

Indications in the HP SIM user interface

Indications are displayed in **All Events** or on an individual system basis under the System Page **Events** tab (Figure 12). Open an event to get more details.

Figure 12. Indications in the Events tab

Troubleshooting WBEM Indications in HP SIM

Follow these steps if a subscription fails:

1. Make sure WBEM is a discovered protocol on the managed node: **Systems Page**->**Product Description table**->**Management Protocols**.
2. Make sure the node is accessible: **Properties** link on the **Systems Page** or **Options**-> **Identify**.

Follow these steps if no indications display in HP SIM:

1. Select **Options**->**Events**->**Event Filter Settings**.
2. Select **Accept unregistered events** as highlighted in Figure 13. This option is not selected by default.
3. Try to list the known subscriptions: `Mxwbemsub -l -n <node name>`

Running the list command contacts the Small Footprint CIM Broker (SFCB) CIMOM on the ESXi managed node and searches for the subscription.

Figure 13. Event Filter Settings

Using HP Virtual Machine Manager to manage virtual machines running ESXi

HP integrated VMware ESXi can be managed in HP Virtual Machine Manager (VMM). Most of the VMM features that are currently supported for other hypervisors are also supported for ESXi. The following VMM features are supported for HP integrated VMware ESXi:

- Copy virtual machine
- Move virtual machine
- Create virtual machine guest template
- Deploy virtual machine guest template
- Create virtual machine guest back-up
- Restore virtual machine guest back-up
- Recover virtual machine of a failed host
- Setting alternate virtual machine hosts
- Start/Stop/Suspend/Resume virtual machine guests
- Performance data information of virtual machine hosts

Note:
For ESXi hypervisors, the Copy / Move operations require that the ESXi host be managed by Virtual Center and the Virtual Center credentials be specified through HP SIM.

Using VI Client and Virtual Center to manage ProLiant servers running ESXi

VMware offers VI Client and Virtual Center to manage servers running ESXi. VI Client is a simple, graphical interface that provides remote interactive configuration and management of ESXi servers. It has been enhanced to provide capabilities that were previously available only on the service console. VI client can also connect to Virtual Center, VMware's central management server application, to manage multiple ESXi host servers, including classic ESX servers. Figure 14 illustrates the relationship between VMware's virtual infrastructure components.

Figure 14. Relationships between VMware's virtual infrastructure components
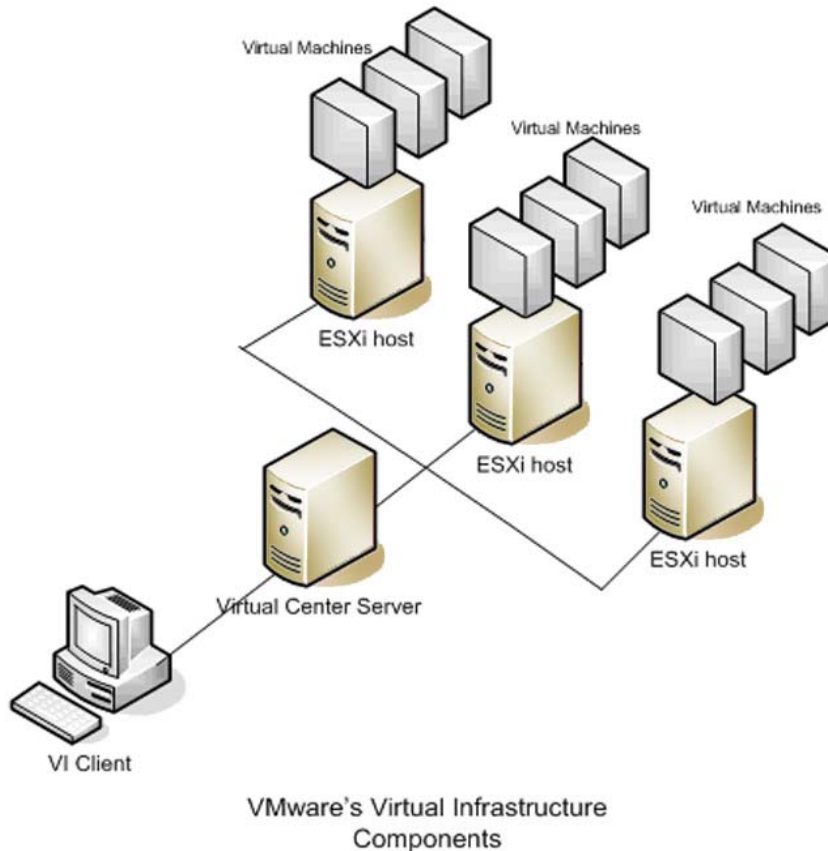
For more detailed information on how to install and configure VMware VI Client and VC, and how to manage ESXi hosts, please refer to VMware document "Getting Started with ESX Server 3i Embedded": http://www.vmware.com.

To manage a single ESXi host server, run the VI Client tool to connect to the ESXi host server by supplying the server's IP address and user root login credentials. The VI Client interface provides system hardware inventory and server administration functions.

Under the Inventory function, the VI Client has multiple tabs that group the server information being displayed, including management tasks that can be performed on the server. The Summary tab shows general information about the server and allows creation of new virtual machines, new resource pool, entry to maintenance mode, and reboot and shutdown of the ESXi server. Other tabs show the virtual machines created, CPU and memory allocation, real-time CPU performance chart, and user permissions. The Configuration tab displays all server hardware inventory data, some software

inventory, and updated overall server, subsystem and individual device health status. Figure 15 shows the Health Status page displayed by the VI Client.

Figure 15. Configuration tab Health Status data from an ESXi Update 1 server

The Events tab shows all management actions performed on the ESXi host. To view these events, the VI Client must be connected to the Virtual Center server. Figure 16 shows an example view of these events on an ESXi host.

Figure 16. Events on ESXi host using VMware's Virtual Center

Appendix A: Changing standards in the server management environment

The system management world is moving to standards other than Simple Network Management Protocol (SNMP) because SNMP-based management solutions have received increased scrutiny for their simple structure and weak security protocol relative to current alternatives. SNMP is a management standard in widespread use for a variety of management needs. It is a lightweight, mature, and non-proprietary standard. However, there are limitations to SNMP server management:

- No guaranteed delivery: The UDP transport mechanism used with SNMP does not provide guaranteed delivery of alerts, events, or queries
- Limited security: The most commonly used versions of SNMP, SNMP v1 and v2; do not provide security features such as message authentication and encryption. SNMP does not use Secure Socket Layer (SSL)
- Requires customization: The management information base (MIB) data structures use discrete islands of information that are adequate for representing devices but not other components such as applications, services, or their associations
- No automation: Managing servers with SNMP-based agent configurations can be a labor-intensive process

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. 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 have many needs:

- Standardized ways of representing and transmitting management data independent of the server hardware, management console, or the state of the server.
- More reliable, routable, and secure 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 server vulnerability to viruses or other problems.
- Management applications that are easily configured, thus reducing initial configuration times and the number of mistakes.

VMware ESXi for ProLiant uses the emerging standard and industry trend of provider-based, Common Information Model (CIM) management standards and infrastructure. WBEM uses the CIM standard to represent systems, networks, applications, devices, and other managed components in an object-oriented fashion. In addition, Systems Management Architecture for Server Hardware (SMASH) and Storage Management Initiative Specification (SMI-S), secure and robust standards being driven by the Distributed Management Task Force (DMTF) and Storage Networking Industry Association (SNIA) organizations, are quickly gaining momentum. The HP Insight Management WBEM Providers (Insight Providers) are based on the SMASH and SMI-S standards, and further extend them to support information that is specific to ProLiant platforms.

Web-based Enterprise Management

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.[2] 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 SMI-S.

---

[2] DMTF WBEM Definition, 2005, www.dmtf.org/standards/wbem

WBEM has been broadened to include Web Services for Management (WS-Management) as an alternative management protocol.

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.

Common Information Model

CIM is defined by the DMTF. It is the data model standard used in many management applications. A data model represents the elements of a system, including hardware, 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 a conceptual information model for describing management that is not bound to a particular implementation. This allows for the interchange of management information between management systems and applications. This can be either "agent-to-manager" or "manager-to-manager" communication that provides for Distributed System Management (DSM). CIM is the underlying data model for management initiatives such as SMASH and SMI-S. CIM is also the data model used by tools such as HP Systems Insight Manager (HP SIM) and HP OpenView.

Systems Management Architecture for Server Hardware

SMASH is a management initiative driven by the DMTF that specifies the data model (based on CIM) and protocols to be used for managing server hardware. It is a comprehensive management initiative, designed to address a need for cross-platform standards to manage servers from multiple vendors. It is routable, secure, and uses common industry-standard protocols. SMASH is specifically designed to manage servers using a lightweight CIM object model that is a subset of the CIM Schema.

The Server Management Command Line Protocol (SM CLP) is one of the protocols specified by SMASH. It consists of human-oriented commands that are also suitable for use with scripts. SM CLP supports network access through Telnet and also Secure Shell v2 (SSHv2) for secure access. 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, server blades, rack servers, and partitionable servers, can support SM CLP commands. As a result, users on a management station or a client can 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.

Appendix B: HP SIM with HP providers, VC/VIC with VMware providers comparison

Table B-1. Comparison of information provided by data source

Data source	HP SIM with HP providers	VC/VIC with VMware providers
Main System (Base Server) System	• System temperature exceeded normal operating range • System temperature has returned to normal operating range • Server model, serial number, product number and universal unique identifier (UUID) • System OS name, type, version number and description • Leverage VMware providers Host/Guest associations for virtual connections to blade servers • Leverage VMware providers for sensors • Computer System Consolidated health status	• Individual and overall temperature sensor health status, including temperature readings • System manufacturer, model, BIOS version and date
Processor (CPU) Subsystem	• Processor temperature exceeded normal operating range • Processor temperature has returned to normal operating range • Individual processor number, core and thread number, speed, physical socket location and health status • Individual processor chip model, manufacturer, version • Individual processor cache size, line size, cache level and type, read and write policy and health status • Processor collection health status	• Individual and overall processor health status • Individual processor model, speed, sockets, cores, logical processors
Fan Subsystem	• Individual fan type, variable speed support, physical fan location and health status • Fan module removal conditions and package type • Fan collection health status • Fan redundancy set, number of fans, associations with individual fan members, and redundancy status	• Individual and overall fan health status
Power Supply Subsystem	• Individual power supply type, physical power supply location and health status • Individual power supply module removal conditions and package type • Power supply collection health status • Power supply redundancy set, number of power supplies, associations with individual power supply members, and redundancy status	• Individual and overall power supply health status

Data source	HP SIM with HP providers	VC/VIC with VMware providers
	• Power supply temperature exceeded normal operating range • Power supply temperature returned to normal operating range	

Memory Subsystem, Version 2.0 only	• System memory capacity, starting and ending address, and health status
	• Individual memory module manufacturer, part number, serial number, removal conditions, data and total width, capacity, speed, type, position, form factor, bank label, SPD byte, location and health status
	• Individual memory board package type, removal conditions, hosting board, locked state, number of sockets, available memory size, total memory size, location and health status
	• Individual memory module slot connector layout, gender and description, location, and health status
	• Version2.0: memory redundancy set type, load balance algorithm, operating speed, available and total memory size, current, target and available configurations, and redundancy status
	• Version2.0: memory collection health status
	  – Memory module has failed or is predicted to fail
	  – Memory board error
	  – Memory redundancy degraded
	  – Memory recovered from degraded redundancy
		• Overall memory health status, and total physical system memory

For more information

For additional information, refer to the resources listed below.

Resource description	Web address
Distributed Management Task Force, Inc.	http://www.dmtf.org/standards/cim/
HP integrated VMware ESXi	http://h18004.www1.hp.com/products/servers/software/vmware-esx3i/index.html
HP Provider Architecture on ESXi	ftp://ftp.compaq.com/pub/products/servers/vmware/esx3i/HP%20WBEM%20Provider%20for%20ESXi%20Scripting%20Tools%20Guide.pdf
HP Systems Insight Manager	http://www.hp.com/go/hpsim
VMware resources:	
VMware ESXi	http://www.vmware.com/products/vi/esx/esx3i.html
VMware Documentation	http://www.vmware.com/support/pubs/
Architecture of ESXi Server	http://www.vmware.com/files/pdf/ESXServer3i_architecture.pdf
Basic System Administration - ESX Server 3.5, ESXi Server version 3.5, Virtual Center 2.5	http://www.vmware.com/pdf/vi3_35/esx_3/r35/vi3_35_25_admin_guide.pdf
ESXi Server Embedded Setup Guide	http://www.vmware.com/pdf/vi3_35/esx_3i_e/r35/vi3_35_25_3i_setup.pdf
Getting Started with ESXi Server Embedded	http://www.vmware.com/pdf/vi3_35/esx_3i_e/r35/vi3_35_25_3ie_get_start.pdf
Managing ESXi Server	http://www.vmware.com/files/pdf/ESXServer3i_management.pdf

Call to action

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