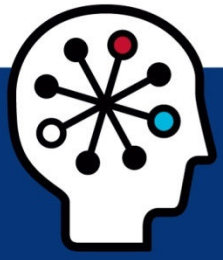
Managing HP servers through firewalls with Insight Software



Abstract

This paper identifies possible ways of managing HP servers with HP Systems Insight Manager and Insight Software deployed in the area of the network that is considered more secure than the standard production network. This is not a best practices document. This document provides information that can enable system administrators to create management solutions appropriate for specific computing environments.

Acronyms in text

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

Acronym	Acronym expansion
CLP	Command Line Protocol
CIM	Common Information Model
DIMM	Dual inline memory module
DCOM	Distributed Component Object Model
DMTF	Distributed Management Task Force
HP SIM	HP Systems Insight Manager
HTTP	Hyper Text Transport Protocol
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
ICMP	Internet Control Message Protocol.
IETF	Internet Engineering Task Force
iLO 2	Integrated Lights-Out 2
IPMI	Intelligent Platform Management Interface
MIB	Management Information Base
OS	Operating System
RMCP	Remote Management Control Protocol
RPC	Remote procedure call
SSH	Secure Shell
SSL	Secure Socket Layer
SM CLP	Server Management Command Line Protocol
SMASH	Systems Management Architecture for Server Hardware
SMI-S	Server Management Initiative - Specification
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol

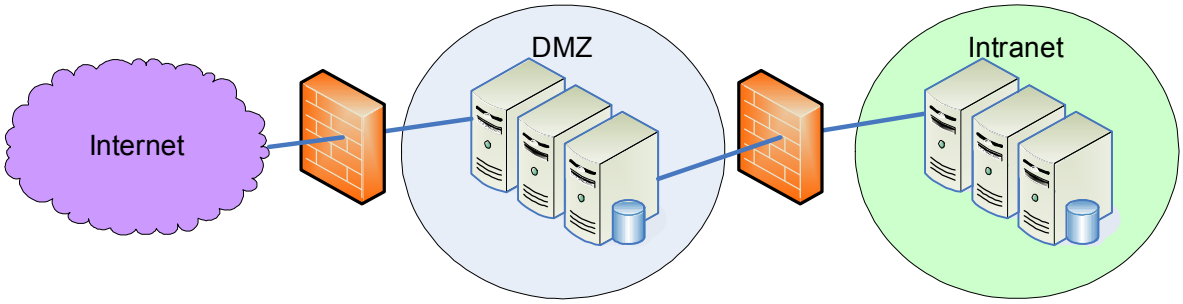
UDP	User Datagram Protocol
WBEM	Web-Based Enterprise Management
WMI	Windows Management Instrumentation
WS-Management	Web Services for Management
XML	Extensible Markup Language

Introduction

Managing systems in a secure environment is a challenge that most system administrators face. It requires a careful balance between critical security requirements and the need to effectively manage and maintain the systems.

Within an Internet connected architecture, there is typically a more secure zone, commonly referred to as the de-militarized zone (DMZ). This zone is positioned between the corporate servers and the Internet, usually separated from both by firewalls that restrict traffic flow. With this architecture, servers that provide publicly available Internet services can be accessed through a firewall, but these services are inaccessible on the internal network. This more secure zone provides an area that is isolated from the internal network and is hardened against external attack (Figure 1). The security challenges in the DMZ are similar to those in other areas of a network that require special security attention.

Figure 1 Block diagram of a generic corporate computing environment



Through three sample case studies, this paper explores options for managing HP systems in the DMZ. It explains the benefits and risks associated with each option. Information in this paper should allow system administrators to tailor solutions for their own computing environments, based on the levels of management they need and the security risk level they are willing to take.

In Case 1, the majority of management protocols are prohibited from the secure network, and the management solution will not be allowed to violate any security restrictions. This solution is not recommended, as the administrator is incapable of managing the hardware in the DMZ. It completely eliminates the use of HP management tools such as HP Systems Insight Manager.

In Case 2, a completely separate network is used for management. This solution has the benefit of completely segregating management traffic from the primary network and allowing a full spectrum of management capabilities (because management protocols can enter through the firewall). However, it is the most expensive option in terms of hardware and infrastructure costs. While it does increase cost due to additional hardware and infrastructure, this option allows the use of iLO 2 to securely manage hardware in the DMZ. Of the two options providing management capabilities in the DMZ (case 2 and 3), this one has the least risk of hackers or security breaches.

In Case 3, management protocols are allowed and management traffic is permitted to travel through the firewall to HP Systems Insight Manager. This results in a fully featured management solution at a measured risk. Because the infrastructure uses a single network for both management and production traffic, this option does increase the risk from hackers or security breaches.

The intended audience for this paper is engineers and system administrators familiar with existing HP technology and servers. The paper does not attempt to define and explain all the security concepts and topics mentioned. Instead, it refers readers to resources containing that information.

HP management products

The following HP products are possible management options for HP servers deployed in the DMZ:

- HP Insight Control Environment (ICE)-Linux
- HP Insight Management Agents (Agents)
- HP Insight Management WBEM Providers for Windows (Insight Providers)
- HP Insight Orchestration (HPIO)
- HP Insight Power Manager (IPM)
- HP Smart Update Manager (HP SUM)
- HP Systems Insight Manager (HP SIM)
- HP WEBM Services for HP-UX
- ProLiant Essentials Performance Management Pack (PMP)
- Rapid Deployment Pack (RDP)
- Server Migration Pack Universal Edition (SMP)
- Version Control Agent (VCA)
- Version Control Repository Manager (VCRM)
- Virtual Machine Management Pack (VMM)
- Virtual Server Environment (VSE)
- Vulnerability and Patch Management Pack (VPM)
- Management processors such as Integrated Lights-Out 2 (iLO 2)

For information about these HP management products, see the "For more information" section at the end of this paper. Appendix A gives port information related to these products.

Case 1: management protocols banned from DMZ

In some computing environments, IT security policies restrict management protocols in the secure environment. Security policies may or may not permit other protocols (such as email or file sharing) in the DMZ. An acceptable management solution must conform to security restrictions of the environment.

Even if active management is not possible, some management information can flow from managed devices in such an environment. Either SNMP or WBEM/WMI can be used to manage ProLiant servers. These can be configured to prevent access from off the platform. For information on how to configure SNMP or WBEM, see the documentation for your operating system.

Asset management

In this type of computing environment, administrators can collect system asset information from a ProLiant server in the DMZ as long as the Agents or WBEM providers are running and an application is running that can get the data locally. For example, Microsoft® Systems Management Server can get asset information from the Agents and transfer that information to its central server via the operating system file share. As a second option, administrators can browse to the web-based System Management Homepage (https://servername:2381/) and manually view the asset information.

Fault management

Administrators can configure ProLiant servers to send an email (via SMTP) when a hardware problem occurs. In Microsoft Windows® operating systems, the Agent Event Notifier provides this optional

feature. Administrators can set up and configure the Agent Event Notifier during the agent deployment. In Linux® operating systems, if a hardware problem occurs, emails are automatically sent to the root email on the managed system.

The Insight Agents for Microsoft Windows also create Windows Event Log entries. A management tool such as HP OpenView Operations or Microsoft Operations Manager operating in the same environment can then collect the log entries and send them back to a centralized server. The Insight Agents for Linux also create entries in the syslog. Administrators can write a script to look for these entries and take appropriate action.

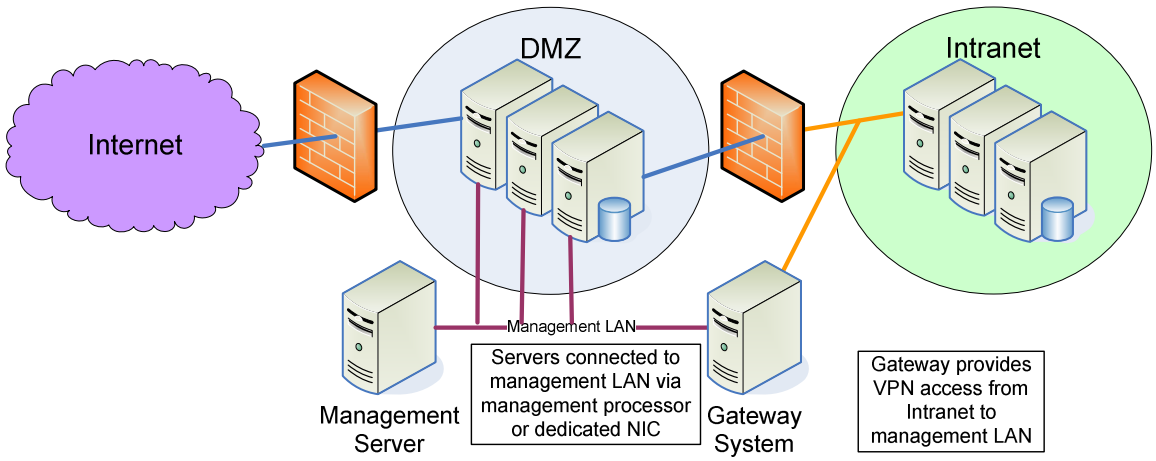
Case 2: separate management network

In some computing environments, system administrators create a separate, secondary network parallel to the primary or production network (Figure 2). The chief benefit to this approach is that management traffic flows through the secondary network, while the limited access from the production (primary) network maintains security. Configuring a separate management network using HP Systems Insight Manager allows secure access to the systems in the DMZ.

The secondary network can also be used for other operations that would be inappropriate for the primary network, such as tape backups, deployments using Rapid Deployment pack, or application maintenance.

Note:
Do not connect the management network to the corporate (internal) network. Compromising one of the systems in the DMZ could allow a hacker to get onto the management network. However, it may be beneficial to allow VPN access to the management network.

Figure 2 Parallel primary (production) and secondary (management) networks



Servers inside the DMZ and on the internal network can use iLO 2 processors. Because the network connection to iLO 2 is completely isolated from the network ports on the server, there is no possibility for data to flow from the DMZ network to the iLO management network, or vice-versa. Therefore, if

anyone compromises the DMZ network, he or she cannot compromise the iLO network. This architecture permits administrators to use iLO on servers located in the DMZ, or in the internal network, without the risk of compromising sensitive data. This separation is accomplished through the use of a dedicated NIC or the iLO 2 Shared Network Port with its Virtual Local Area Network (see the paper titled "HP Integrated Lights-Out security technology" available at http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00212796/c00212796.pdf for more information).

For best protection of the servers operating inside the DMZ, administrators should set the SNMP trap destinations to the loop back address and enable the SNMP pass-through in iLO 2 so that SNMP traps are routed onto the iLO management network. While this SNMP pass-through option does not enable all management functions, it allows for passing status, inventory, and fault information to HP Systems Insight Manager or another SNMP-capable management application. This option has the benefit of being very secure because the host operating system does not recognize the Lights-Out product as a NIC.

Asset Management

With HP Systems Insight Manager installed on the secondary management network, system administrators can collect system asset information from a ProLiant server on that management network through the iLO 2 pass-through. As a second option, administrators can browse to the System Management Homepage (https://servername:2381/) and manually view the asset information.

The Appendix to this paper describes the procedure for configuring a separate management network. When using SNMP management protocols, SNMP should be configured to accept packets only from the IP addresses used on the management network, or SNMP should be bound to the secondary network interface (if the operating system allows this.) The HP Insight Management Agents should be configured to allow access only from IP addresses on the management network. HP Systems Insight Manager should be configured to discover the systems on the secondary network. WMI and WBEM can be disabled on the primary network by configuring a firewall on the system to disable each of the protocols on the primary NIC.

Fault Management

SNMP traps can be forwarded through the Lights-Out interface on ProLiant servers. This allows full fault management data to flow into HP Systems Insight Manager or another management product (such as HP OpenView Network Node Manager).

The Insight Agents for Microsoft Windows also create Windows Event Log entries. A management tool such as HP OpenView Operations or Microsoft Operations Manager operating in the same environment can then collect the log entries and send them back to a centralized server. The Insight Agents for Linux also create entries in the syslog. Administrators can write a script to look for these entries and take appropriate action.

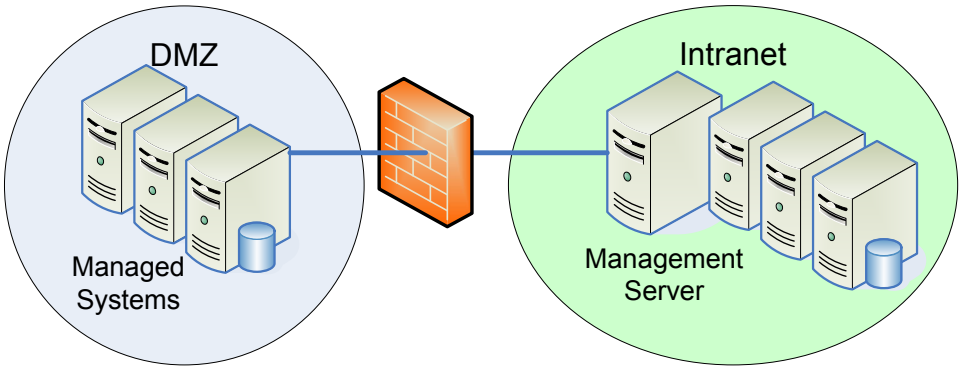
Case 3: managing through a firewall using a single network

In other computing environments, a firewall commonly separates the central management server (CMS) and the managed server. In such an environment (Figure 3), two networks are given different levels of trust. For example, the managed server may be in a DMZ, while the CMS resides in a more trusted portion of the intranet. The firewall is used to control traffic between these two networks. The firewall permits the exchange of only specific types of traffic between specific systems.

In some situations, the firewall may simply restrict communication between specific IP addresses. For example, the firewall may allow the exchange of any IP packets between the managed system and the CMS. However, because host names and IP addresses can be spoofed, a higher level of restriction can be imposed through the firewall; that is, the firewall can permit only non-spoofable protocols.

In this case study, we assume that the firewall is configured to allow only requests from the CMS to the managed server and returned responses. Typically, this means the firewall will not permit UDP traffic, as connectionless protocols cannot easily be configured to block incoming packets. Only specific TCP ports will be opened, and they will possibly be filtered for certain types of traffic.

Figure 3 Firewall separating central management server from managed server



Asset Management

HP SIM provides asset management services by first discovering and identifying the managed systems, gathering data from instrumentation running on each managed system, storing this data in a SQL database, and finally providing reporting capabilities on this gathered data. These steps require communication between the CMS and managed system as described in the following paragraphs.

First the managed systems and the instrumentation running on them must be identified. HP SIM offers an automatic discovery mechanism using IP ping sweep, or administrators can manually add systems by name or address. In either case, the CMS will attempt to contact the managed system using a ping; if this fails, then no further requests will be sent to the system.

HP SIM normally uses an ICMP echo to ping a system; however, some network administrators turn off ICMP through firewalls. In this situation, the administrator can configure HP SIM to use a TCP port to ping systems. Port 80 is used by default, but an alternative port may be specified in a configuration file. The target system need not be actively listening to the chosen port, but the firewall must be configured to allow these requests to pass.

Next, the CMS will attempt to identify a number of management protocols such as SNMP, HTTP, and WBEM. The protocols used for asset management depend on the types of systems being managed (Table 1):

- ProLiant servers provide management data through SNMP, giving complete coverage of the hardware instrumentation. Integrity servers running Windows also provide this SNMP instrumentation.
- ProLiant and Integrity servers running Microsoft Windows 2003 or 2008 also expose much data through the Insight Providers and WMI. The HP Insight Providers include server providers (information about processors, memory, peripheral devices, computer system information, and sensor information); network providers (network controller information and indications); and storage providers (storage controller information and indications). WMI on Integrity currently does not cover detailed hardware information such as controllers, DIMMs, and physical disks.
- ProLiant and Integrity servers running Linux may also provide management data through WBEM. While that data is not currently as rich as the SNMP information, WBEM provides basic hardware and operating system information today. WEBM will be expanded to provide full instrumentation in future.
- HP 9000 and Integrity servers running HP-UX provide management data with WBEM. HP recommends WBEM for asset management and makes it available on 11.x versions of HP-UX. (These systems also support SNMP, but SNMP is not required for asset management.)

Table 1 Protocols used for asset management of industry-standard servers

Server	OS	SNMP	WBEM	WMI	SSH	WS-MAN
ProLiant	Windows	Y	Y[1]	Y		
ProLiant	Linux	Y	Y		Y	
HP 9000	HP-UX	Y[2]	Y (11.x)			
HP Integrity	HP-UX	Y[2]	Y			
HP Integrity	Linux	Y	Y		Y	
HP Integrity	Windows	Y	Y[1]	Y		
Other devices		Y				Y

Notes:
[1] When WMI mapper is installed

[2] Not required for asset management

Selecting the protocols that must be enabled through the firewall depends on the types of system to be managed. Issues associated with each protocol are discussed below. Ideally, WBEM will be used to manage servers located through a firewall.

SNMP

SNMP gives the best management coverage but at the highest risk. While no "set" operations are required for asset management, SNMP is UDP-based; therefore, in many environments it is not considered a suitable protocol to pass through the firewall. Because SNMPv1 has a simple, clear-text "community," it provides a low level of security. However, SNMP may be suitable for some environments in which the network containing the managed systems is relatively controlled.

DMI

DMI is a remote procedure call (RPC)-based protocol. To operate, DMI requires opening a number of ports through a firewall. Therefore, DMI is not recommended for use through firewalls. It is largely being replaced by WBEM.

Note
DMI is not supported on HP-UX systems running HP-UX 11.23 (11iv2) and HP-UX 11.31 (11iv3). You must use WBEM for this operating system.

WBEM

WBEM uses HTTPS to provide a secure TCP connection from the CMS to the managed system. WBEM uses its own port (5989 for SSL connections) and is supported through firewalls. The CMS can use trusted certificates to authenticate the managed system, while the managed system uses user names and passwords to authenticate the CMS.

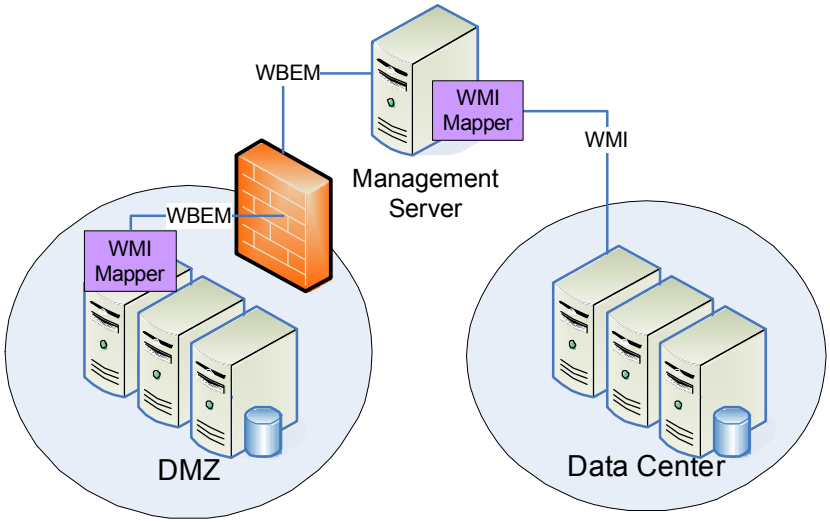
Note
Firewalls should be configured to allow the CMS to communicate with managed systems through default port 5989. If you have modified the default port setting for your WBEM provider, you must configure your firewall for the port number your WBEM provider on which it is actually configured."

WMI

WMI is Microsoft's implementation of WBEM. WMI runs over DCOM, which in turn, uses RPC.

The WMI Mapper is an application that provides translation from WMI (a DCOM-based interface) to a standardized WBEM interface (CIM XML/HTTP). This is a two-way translation. The WMI Mapper is required for HP SIM to manage Windows computers, including ProLiant servers running the Insight Providers for Windows. The WMI Mapper service runs separately from the HP SIM service. For Windows systems behind a firewall, HP recommends installing the WMI Mapper on a managed system in the secure network (Figure 4) and disabling direct remote access to WMI. This mapper allows standard WBEM requests through the firewall, and they are mapped to WMI requests on the managed system.

Figure 4 WMI Mapper on managed Windows system behind firewall



The WMI Mapper is included with the Windows version of HP SIM but can also be used with other versions. It is available with the HP SIM software or from the HP website at http://www.hp.com/go/hpsim. The mapper can be installed on a Windows system to allow WBEM access to that system.

If the mapper is to be used as a proxy to access other systems, as shown in the DMZ example above, then HP SIM must be configured to recognize the mapper as a proxy: Use the **Options** | **Security** | **WMI Proxy Settings** menu item and add the system on which the mapper is installed.

WS-MAN

WS-Management is a public standard SOAP-based protocol for sharing management data among all operating systems, computers, and devices. As of this writing, it is used to manage ILO2.

SSH

Secure Shell (SSH) allows logging in to another system over a network and executing commands on that system. It also enables administrators to move files from one system to another in an encrypted format. It provides authentication and secure communications over insecure channels, and uses TCP port 22 to communicate.

Fault management

The HP Agents have two means for communicating faults: SNMP traps and SMTP e-mail (Table 2). Both originate from the agents in the DMZ to the CMS or to the SMTP mail server. The HP Insight Management WBEM providers can communicate faults using WMI indications. It is recommended that the WMI Mapper be installed on the managed system so that these faults can be sent using WBEM (CIM-XML/HTTP) through the firewall.

Table 2 How HP agents communicate faults

CMS		Managed System		Port	Protocol[1]	Description
In[2]	Out	In	Out			
Y			Y	162	SNMP	SNMP Trap
	Y	Y		25	SMTP	SMTP E-mail
Y			Y	50004	HTTPS/HTTP	WBEM event receiver (configurable)

Notes:

[1] All ports are for TCP and UDP

[2] The CMS will normally have all managed system ports open, as the CMS is a managed system itself. Firewalls may be configured to block these ports if the CMS is not to be managed from another system.

Configuration Management

HP web agents on managed systems in a DMZ should first be configured to trust-by-certificate the HP SIM server. This will authenticate all Version Control (VC) commands and all Replicate Agent Settings (RAS) commands to the agent as coming from the specified CMS; these commands require HTTPS over port 2381.

Systems must be discoverable by the CMS. Refer to the "Asset Management" section for more information. Systems must also be identifiable, which minimally requires HTTP access over port 2301. Table 3 identifies the protocols used for configuration management when managing through a firewall.

Note
HP does not recommended enabling management protocols such as SNMP or DMI on systems outside the firewall or directly connected to the Internet.

Table 3 Summary of protocols used for configuration management

CMS		**Managed System**		**Port**	**Protocol**[1]	**Description**
In[2]	Out	In	Out		ICMP	Ping
	Y	Y		22	SSH	SSH server (for DTF)
	Y	Y		161	SNMP	SNMP Agent
Y			Y	162	SNMP Trap	Trap listener
	Y[4]	Y		80	HTTP	Management processor and other devices; standard Web server
Y	Y[4]	Y		280	HTTP	Web server for HP SIM; Web agent auto-start port
	Y[4]	Y		443	HTTPS	Management processor and other devices; standard Web server
	Y			1443	TCP	Microsoft SQL Server database
	Y	Y		2301	HTTP	Web agent Web server

Y[3]				2367	RMI	HP SIM RMI connection
	Y	Y		2381	HTTPS	Web agent Web server
	Y			5432		ProstgreSQL Server database
	Y	Y		5988	HTTP	WBEM service
	Y	Y		5989	HTTPS	WBEM service
Y				50000	HTTPS	HP SIM Web server
Y				50001	HTTPS	HP SIM SOAP (configurable[6])
Y				50002	HTTPS	HP SIM SOAP with client certificate authentication (configurable[7])
Y				50003	HTTP	HP SIM SOAP (configurable[8])
Y			Y	50004	HTTPS/HTTP	WBEM event receiver (configurable)
Y				50005	WBEM	WBEM Events
Y				50006	PostgreSQL	PostgreSQL
Y				50008	SIM JMS	JMS port
Y				50009	SIM JNDI	JNDI port
	Y	Y		50010	DMI[5]	DMI
				50013	RMI	Web Services RMI Loader
				50014	JRMP	JRMP Invoker
				50015	Pooled invoker	Pooled invoker
	Y[4]	Y		411	HTTP	IBM Director agent
	Y[4]	Y		1311	HTTPS	Server administrator
	Y[4]			2069	HTTP	OSEM
	Y[4]	Y		3202	HTTPS	StorageWorks NAS
	Y[4]	Y		3257	HTTPS	Rack & Power Manager
	Y[4]	Y		4095	HTTP	CommandView ESL
	Y[4]	Y		4096	HTTP	CommandView SDM
	Y[4]	Y		8000	HTTP	HP Web letAdmin
	Y[4]	Y		8008	HTTP	Default home page
	Y[4]	Y		8443	HTTPS	HP Web JetAdmin

Notes:

Outbound (out) – Request or response sent from a server is called outbound

Inbound (in) – Request or response received by a server is called inbound

[1] All ports are for TCP and UDP (except ICMP).

[2] The CMS will normally have all managed system ports open, as the CMS is a managed system itself. Firewalls may be configured to block these ports if the CMS is not to be managed from another system.

[3] RMI port is used within the CMS for inter-process communication. Connections from outside the CMS are not accepted, and firewalls may block this port.

[4] Many CMS outgoing ports are used for discovery.

[5] The exact UDP/TCP ports used by DMI are dynamic and vary from system to system, but they tend to be around 32,780 and higher.

[6] Port number is configurable in mx.properties using MX_SOAP_PORT.

[7] Port number is configurable in mx.properties using MX_SOAP_SSO_PORT.

[8] Port number is configurable in mx.properties using MX_SOAP_HTTP_PORT; port can be enabled/disabled in globalsettings.props using HTTP_SOAP_PORT_ENABLE with "true" or "false."

Version Control

This discussion is based on the assumption that the Version Control Repository (VCR) is behind the firewall with CMS, and likely on the CMS.

Discovering the software available on the managed system requires SNMP over port 161. After receiving a command to update some component, the system must retrieve the component from the VCR, which it does using HTTPS over port 2381 to the VCR. To communicate its update status back to the CMS, the agent uses HTTP over port 280. Additionally, the CMS polls the system for its status every 15 minutes for up to 2 hours.

Replicate Agent Settings

Replicate Agent Settings require a source system whose configuration is copied and stored at the CMS for duplicating to other target systems. This function relies on HTTPS traffic via port 2381 and can operate over the firewall as long as the firewall is configured to pass this traffic.

SSH

SSH is used both locally on the HP SIM central management server and remotely to manage systems for various tools. Normally, SSH servers listen on TCP port 22. If, for some reason, this must be changed, the SSH port that HP SIM uses is configurable.

Performance Management

This section is based on the assumption that PMP/PPA is behind the firewall with CMS. Systems must be discoverable by the CMS using ICMP echo or TCP to port 80.

Table 4 Performance management protocol

CMS		Managed System		Port	Protocol[1]	Description
In[2]	Out	In	Out		ICMP	Ping
	Y	Y		80	TCP	System Discovery[1]
	Y	Y		161	SNMP	PMP/PPA

Notes:

[1] Discovery protocol is configurable between ICMP or TCP and a configurable port; default is 80.

[2] The CMS will normally have all managed system ports open, as the CMS is a managed system itself. Firewalls may be configured to block these ports if the CMS is not to be managed from another system

Vulnerability and Patch Manager (VPM)

This section is based on the assumption that HP VPM is behind the firewall with the CMS.

Table 5 Ports that must be open on the server

CMS	Managed System	Port	Protocol[1]	Description

In[2]	Out	In	Out			
	Y	Y		280	TCP	HP SIM HTTP port
Y				50000	TCP	HP SIM HTTPS port
	Y	Y		22	TCP	HP SIM SSH port
Y				50001	TCP	HP SIM secure Simple Object Access Protocol (SOAP) port
	Y	Y		161	TCP/UDP	SNMP
Y				162	TCP/UDP	SNMP traps
	Y	Y		5989	TCP	HP SIM Web-Based Enterprise Management(WBEM)/WMI Mapper Secure port
	Y	Y		2301,2381,49400	TCP	HP ProLiant Agents
	Y	Y		445	TCP	MSDE Named Pipes Communications
	Y	Y		1434	UDP	MSDE Shared Instance Support

Notes:

[1] All ports are for TCP and UDP.

[2] The CMS will normally have all managed system ports open, as the CMS is a managed system itself. Firewalls may be configured to block these ports if the CMS is not to be managed from another system.

Table 6 Harris STAT Scanner Engine

CMS		**Managed System**		**Port**	**Protocol[1]**	**Description**
In[2]	Out	In	Out			
	Y	Y		443	TCP	HTTPS port
	Y	Y		80	TCP	HTTP port
	Y	Y		135, 137, 138, 139, 445	TCP and UDP	File and Printer Sharing for Microsoft Networks

Notes:

[1] All ports are for TCP and UDP.

[2] The CMS will normally have all managed system ports open, as the CMS is a managed system itself. Firewalls may be configured to block these ports if the CMS is not to be managed from another system.

Table 7 Radia Patch Manager

CMS		**Managed System**		**Port**	**Protocol[1]**	**Description**
In[2]	Out	In	Out			
	Y	Y		3464	TCP	Configuration Server
	Y	Y		3466	TCP	Radia Management Portal
	Y	Y		3465	TCP	Radia agent

Notes:

[1] All ports are for TCP and UDP.

[2] The CMS will normally have all managed system ports open, as the CMS is a managed system itself. Firewalls may be configured to block these ports if the CMS is not to be managed from another system.

Table 8 Port that must be open on target nodes

CMS		Managed System		Port	Protocol[1]	Description
In[2]	Out	In	Out			
	Y	Y		135, 137, 138, 139, 445	TCP and UDP	File and Printer Sharing for Microsoft Networks
	Y	Y		135, 137, 138, 139, 445	TCP and UDP	Remote Registry service

Notes:

[1] All ports are for TCP and UDP.

[2] The CMS will normally have all managed system ports open, as the CMS is a managed system itself. Firewalls may be configured to block these ports if the CMS is not to be managed from another system.

Virtual Machine Management Pack Ports (VMM)

This section is based on the assumption that HP VMM is behind the firewall with the CMS.

Table 9 VMM Ports

CMS		Managed System		Port	Protocol[1]	Description
In[2]	**Out**	**In**	**Out**			
Y				1124	TCP and UDP	HP VMM Control **Note:** This port is applicable to CMS only. Communication between the VMM Web Service and the VMM Service (both on the HP SIM CMS) uses SSL.
	Y	Y		1125	TCP and UDP	HP VMM Agent **Note:** This port is applicable to CMS and managed systems. Communication between the VMM Service and VMM agent (on virtual machine hosts) uses SSL.
	Y	Y		1126	TCP and UDP	HP VMM Agent **Note:** This port is applicable to CMS and managed systems. Communication between the VMM Service and VMM agent (on virtual machine hosts) uses SSL. Communication between the VMM agents during a virtual machine move or copy operation uses SSL.
Y				50010	HTTPS	Communication between browsers and the VMM Web Service.

Notes:

[1] All ports are for TCP and UDP.

[2] The CMS will normally have all managed system ports open, as the CMS is a managed system itself. Firewalls may be configured to block these ports if the CMS is not to be managed from another system.

Insight Power Manager (IPM)

This section is based on the assumption that HP IPM is behind the firewall with the CMS.

Table 10 Port settings for IPM

CMS		**Managed System**		**Port**	**Protocol**[1]	**Description**
In[2]	**Out**	**In**	**Out**			
	Y	Y		2381	HTTPS	Web agent Web server
	Y	Y		2301	HTTP	Web agent Web server
	Y	Y		443	SSL	Communication with iLO

Notes:

[1] All ports are for TCP and UDP.

[2] The CMS will normally have all managed system ports open, as the CMS is a managed system itself. Firewalls may be configured to block these ports if the CMS is not to be managed from another system.

System Management Homepage

Table 11 Port settings for Systems management Homepage

CMS		**Managed System**		**Port**	**Protocol**[1]	Description
In[2]	Out	In	Out			
	Y	Y		2381	HTTPS	Web agent Web server
	Y	Y		2301	HTTP	Web agent Web server

Notes:

[1] All ports are for TCP and UDP.

[2] The CMS will normally have all managed system ports open, as the CMS is a managed system itself. Firewalls may be configured to block these ports if the CMS is not to be managed from another system.

HP Insight Orchestration (HPIO)

This section is based on the assumption that HP Insight Orchestration is behind the firewall with the CMS.

Table 12 HPIO ports

CMS		**Managed System**		**Port**	**Protocol**[1]	**Description**
In[2]	**Out**	**In**	**Out**			
Y				51443	HTTPS	XML or SOAP over HTTPS – LSU GUI's, API, and OO workflows to LSU Controller
Y				16443	HTTPS	XML or SOAP over HTTPS – Operations Orchestration (OO) GUI to OO Central

Y				50000	HTTPS	SOAP over HTTPS – LSU Controller to HP SIM
Y				40420	HTTPS	RMI over HTTPS – LSU Controller to VMM
Y				51001	HTTPS	RMI over HTTPS – LSU Controller to LSA (VSE logical server management)
Y				50000	HTTPS	SOAP over HTTPS – LSU Controller to LSU Deployment Service connector
Y				1433	TCP	JDBC over TCP – talk via JDBC to SQL Server

Notes:

[1] All ports are for TCP and UDP.

[2] The CMS will normally have all managed system ports open, as the CMS is a managed system itself. Firewalls may be configured to block these ports if the CMS is not to be managed from another system.

Version Control Agent (VCA)

Table 13 Ports for VCA

CMS		**Managed System**		**Port**	**Protocol**[1]	**Description**
In[2]	**Out**	**In**	**Out**			
	Y	Y		2381	HTTPS	Web agent Web server
	Y	Y		2301	HTTP	Web agent Web server

Notes:

[1] All ports are for TCP and UDP.

[2] The CMS will normally have all managed system ports open, as the CMS is a managed system itself. Firewalls may be configured to block these ports if the CMS is not to be managed from another system.

Version Control Repository Manager – VCRM

Table 14 Ports for VCRM

CMS		**Managed System**		**Port**	**Protocol**[1]	**Description**
In[2]	**Out**	**In**	**Out**			
	Y	Y		2381	HTTPS	Web agent Web server
	Y	Y		2301	HTTP	Web agent Web server

Notes:

[1] All ports are for TCP and UDP.

[2] The CMS will normally have all managed system ports open, as the CMS is a managed system itself. Firewalls may be configured to block these ports if the CMS is not to be managed from another system.

Insight Control Environment-Linux

Table 15 Ports for ICE-Linux

CMS		**Managed System**		**Port**	**Protocol**[1]	**Description**
In[2]	**Out**	**In**	**Out**			

	Y	Y		80	HTTP	SUSE deployment
	Y	Y		60000		RHEL deployment
	Y	Y		2709		Mond (On Managed node)
	Y	Y		514		Syslog-ng (On Managed node)
	Y	Y		5666		Nrpe (On Managed node)

Notes:

[1] All ports are for TCP and UDP.

[2] The CMS will normally have all managed system ports open, as the CMS is a managed system itself. Firewalls may be configured to block these ports if the CMS is not to be managed from another system.

Server Migration Pack Universal Edition

This section is based on the assumption that HP SMP is behind the firewall with the CMS.

Table 16 Ports for ICE-Linux

CMS		Managed System		Port	Protocol[1]	Description
In[2]	Out	In	Out			
	Y	Y		51124	SSL	For communication between the SMP Universal web service and the SMP Universal application service
	Y	Y		51125	SSL	For communication between the SMP Universal web service and iLO for auto destination boot. For communication between the SMP Universal application service and the SMP Universal Agent on the source server or source virtual machine host
	Y	Y		51126	SSL	For communication between the SMP Universal application service and the SMP Universal Agent on the source server or source virtual machine host For communication between the SMP Universal application service and the SMP Universal Agent on the destination server or destination virtual machine host For communication between the SMP Universal Agents on the source server or source virtual machine host and destination server or destination virtual machine host
Y				50000	HTTPS	Communication between browsers and the HP SMP Universal Web Service
Y				51127	HTTP	Default SMP web server port

Notes:

[1] All ports are for TCP and UDP.

[2] The CMS will normally have all managed system ports open, as the CMS is a managed system itself. Firewalls may be configured to block these ports if the CMS is not to be managed from another system.

Virtual Server Environment

This section is based on the assumption that HP VSE is behind the firewall with the CMS.

Table 17 Ports for communication between the CMS and managed nodes

CMS		Managed System		Port	Protocol[1]	Description
In[2]	Out	In	Out			
	Y	Y		5989	HTTPS	Used by WBEM.
	Y	Y		2381	HTTPS	Used by web agents.
	Y	Y		22	SSH-2	Used by the Distributed Task Facility (DTF).
	Y	Y		9143	OpenSSL	Used by Application Discovery.
Y				9617,9618		Global Workload Manager uses on CMS.
	Y	Y		280	HTTP	Web server for HP SIM; Web agent auto-start port
Y				50000	HTTPS	HPSIM Webserver

Notes:

[1] All ports are for TCP and UDP.

[2] The CMS will normally have all managed system ports open, as the CMS is a managed system itself. Firewalls may be configured to block these ports if the CMS is not to be managed from another system.

HP Smart Update Manager

Table 18 HP SUM ports for Windows

CMS		Managed System		Port	Protocol[1]	Description
In[2]	Out	In	Out			
	Y	Y		445 and 137/138/139	TCP and UDP	These ports are needed to connect to the remote ADMIN$ share on target servers (port 137 only if you are using NetBIOS naming service)
	Y	Y		60000-60007	SSL	Random ports are used in this range to pass messages back and forth between the local and remote systems via SSL
	Y	Y		80, 63000-63005	HTTPS	Used for passing files to the target and retrieving the logs via an internal mini-https server. Uses port 80 if it is available or a random port between 63000 and 63005 if it is not. Allows updates of the iLO firmware without the need to access the host server. This will allow servers running VMWare or other virtualization platforms to update their iLO without the need to reboot their server or migrate their VMs to other servers.
	Y	Y		50116	TCP	This is port is used in CMS
	Y	Y		51268	TCP	This port is used in target machine
	Y	Y		61000-61007		These ports are used from the target server back to the system running HP Smart Update Manager. The same mechanism is used by the remote access code as the 60000 ports, with the first trial port as 61000. There is no guarantee that the upper limit is 61007 when a conflict occurs. For the case of ipv4-only and one NIC, the lowest available one is used by HP Smart Update

						Manager to pass information between processes on the local workstation where HP Smart Update Manager is executed, and the next available one is used to receive messages from remote servers.
		Y		62000 and 62001		These ports (or the first two ports available after 62000) are used for internal process communications on the system running HPSUM on each target
		Y		62286		This port is the default for some internal communications. It is the listening on the remote side if there is no conflict. If a conflict occurs, the next available one is used.

Notes:

[1] All ports are for TCP and UDP.

[2] The CMS will normally have all managed system ports open, as the CMS is a managed system itself. Firewalls may be configured to block these ports if the CMS is not to be managed from another system.

Table 19 HP SUM ports for Linux

CMS		Managed System		Port	Protocol[1]	Description
In[2]	Out	In	Out			
	Y	Y		22	SSH	This port is needed to establish a connection to the remote Linux server through SSH
	Y	Y		60000-60007	SSL	Random ports are used in this range to pass messages back and forth between the local and remote systems via SSL
	Y	Y		80, 63000-63005	HTTPS	Used for passing files to the target and retrieving the logs via an internal mini-https server. Uses port 80 if it is available or a random port between 63000 and 63005 if it is not. Allows updates of the iLO firmware without the need to access the host server. This will allow servers running VMWare or other virtualization platforms to update their iLO without the need to reboot their server or migrate their VMs to other servers.
	Y	Y		61000-61007		These ports are used from the target server back to the system running HP Smart Update Manager. The same mechanism is used by the remote access code as the 60000 ports, with the first trial port as 61000. There is no guarantee that the upper limit is 61007 when a conflict occurs. For the case of ipv4-only and one NIC, the lowest available one is used by HP Smart Update Manager to pass information between processes on the local workstation where HP Smart Update Manager is executed, and the next available one is used to receive messages from remote servers.
		Y		62000 and 62001		These ports (or the first two ports available after 62000) are used for internal process communications on the system running HPSUM on each target
		Y		62286		This port is the default for some internal communications. It is the listening on the remote side if there is no conflict. If a conflict occurs, the

						next available one is used.
	Y	Y		7	ICMP	ICMP Echo Reply/Request is used to determine if target devices have successfully rebooted or not

Notes:

[1] All ports are for TCP and UDP.

[2] The CMS will normally have all managed system ports open, as the CMS is a managed system itself. Firewalls may be configured to block these ports if the CMS is not to be managed from another system.

Rapid Deployment Pack

This section is based on the assumption that RDP is behind the firewall with the CMS.

Table 20 RDP ports

CMS		**Managed System**		**Port**	**Protocol**[1]	**Description**
In[2]	**Out**	**In**	**Out**			
	Y	Y		69	UDP	PXE Client
	Y	Y		1758	UDP	PXE Client
	Y	Y		1759	UDP (Multi cast)	PXE Client
	Y	Y		67	UDP	PXE Client
	Y	Y		68	UDP	PXE Client
	Y	Y		4011	UDP	PXE Client
	Y	Y		405	TCP	PXEConfig
	Y	Y		406	TCP	PXECfg Service
	Y	Y		407	TCP	PXE Server and PXE MTFTP
	Y	Y		8081	HTTP	DSWeb
	Y	Y		8080	HTTP	DSWeb,Console Manager
	Y	Y		505	TCP	Win32 console,Axengine,PXEManager
	Y	Y		402	TCP/UDP	Agents,PXE Server,DataManager,PXEManager
	Y	Y		5001	TCP	Aclient
	Y	Y		5002	TCP	Aclient
	Y	Y		415	TCP	Remote Client
	Y	Y		402	UDP	Deployment Server
	Y	Y		401	UDP	Aclient (Wake-on-LAN Proxy)

Notes:

[1] All ports are for TCP and UDP.

[2] The CMS will normally have all managed system ports open, as the CMS is a managed system itself. Firewalls may be configured to block these ports if the CMS is not to be managed from another system.

Conclusion

This has paper identified various options available for managing HP systems in a secure environment. The solutions explained here are intended only as a framework for exploring the options. Each system administrator can and should tailor a solution for his network based on these options.

Appendix A: Configuring a separate management network

To configure a separate management network using HP Systems Insight Manager, install HP Systems Insight Manger on the secondary network by completing the following steps:

1. Configure SNMP to accept packets only from the IP addresses used on the management network, or bind SNMP to the secondary network interface (if the operating system allows this):
   - On Windows systems:

     From the Control Panel, open the **Services** menu.
     Open the **Properties** for the SNMP Service.
     Under the **Security** tab, add IP addresses to the list of IP Addresses that can accept SNMP packets.

   - On systems running Linux or HP-UX:

     Modify the configuration file "snmpd.conf" to accept SNMP packets only from the desired hosts.

     Do the same with any other OS service needed on the network.
2. If a firewall is used on the CMS or managed systems, configure the firewall rules to only allow SNMP WMI and WBEM requests from address in the management network. Use the ports in Appendix A to determine which rules to configure.

3. Configure the HP Insight Management Agents to allow access only from IP addresses on the management network:
   Log into the Agent with administrator privileges.
   Go to the **Settings/Options** page, and modify the IP Restricted Logins settings.

4. Configure HP Systems Insight Manager to discover the systems on the secondary network:
   In HP Insight Manager, go to **Options** | **Discovery** |**Automatic Discovery**.
   Add the IP addresses for the systems on the secondary network.

You can disable WMI, WBEM, and DMI on the primary network by configuring a firewall on the system to disable each of the protocols on the primary NIC. The method of accomplishing this varies for each firewall.

For more information

For additional information, refer to the resources listed below.

Source	Hyperlink
ProLiant server management	http://h18013.www1.hp.com/products/servers/management/index.html
HP Systems Insight Manager	http://www.hp.com/go/hpsim
Understanding HP Systems Insight Manager Security	http://h10018.www1.hp.com/wwsolutions/misc/hpsim-helpfiles/HPSIM_53_Security.pdf
WBEM Providers for HP SIM	www.hp.com/go/hpwbem/
ProLiant Essentials Performance Management Pack (PMP)	See the HP Insight Control Environnent User Guide located at http://www.hp.com/go/insight
HP WEBM Services for HP-UX	http://h18004.www1.hp.com/products/servers/management/hpsim/download.html
Integrated Lights-Out 2 (iLO)	www.hp.com/go/ilo
HP OpenView	www.openview.hp.com/

Call to action

To help us better understand and meet your needs for ISS technology information, send comments about this paper to: TechCom@HP.com.

481364-002, February 2009