Managing your HP servers through firewalls with HP SIM 5.2

Abstract

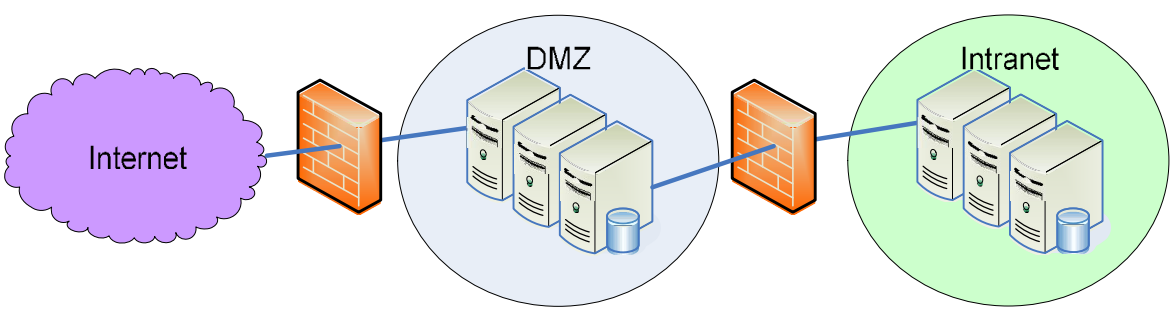
This paper identifies ways of managing HP servers with HP Systems Insight Manager (HP SIM) deployed in the area of the network that is considered more secure than the standard production network. This is not a best practices document. It provides information that can enable system administrators to create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

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.

In many sites, the secure environment is the area of the network that sits between the corporate servers and the Internet, usually separated from both by firewalls that restrict traffic flow. This environment (Figure 1) is commonly referred to as the demilitarized zone (DMZ). 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 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 enable 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 they need and the security restrictions.

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. However, it is the most expensive option in terms of hardware and infrastructure costs.

In Case 3, management protocols are allowed and management traffic is permitted to travel through the firewall to HP SIM. This results in a fully featured management solution of measured risk.

The intended audience for this paper is engineers and system administrators familiar with existing technology and servers. The paper does not attempt to define and explain all the security concepts and topics mentioned. Instead, it refers you to resources containing that information. A glossary at the end defines some of the terms used in the text.

HP management products

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

- HP SIM
- HP Insight Management Agents (Agents)
- HP ProLiant Essentials performance Management Pack (PMP)
- HP WBEM Services for HP-UX
- Management processors such as Remote Insight Lights-Out Edition II (RILOE UII) and Integrity Lights Out (iLO)
- HP System Management Homepage (which includes all agent pages, the HP Version Control Agents, and HP Version Control Repository Manager page, and the HP diagnostic pages)
- HP Virtual Machine Management Pack (VMM)

Case 1: Management protocols banned from DMZ

In some computing environments, IT security policies restrict management protocols in the secure environment. Security policies might permit other protocols (such as e-mail 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 systems in such an environment. Although managing ProLiant servers requires that SNMP be installed and running on the servers, SNMP can be set up to prevent access from off the platform. For information on how to configure SNMP, 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 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 management server (CMS) through the operating system file share. As a second option, administrators can browse to the web-based Agents at https://*servername*:2381/ and manually view the asset information.

Fault management

Administrators can configure ProLiant servers to send an e-mail (through 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, e-mails are automatically sent to the root e-mail on the managed system.

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

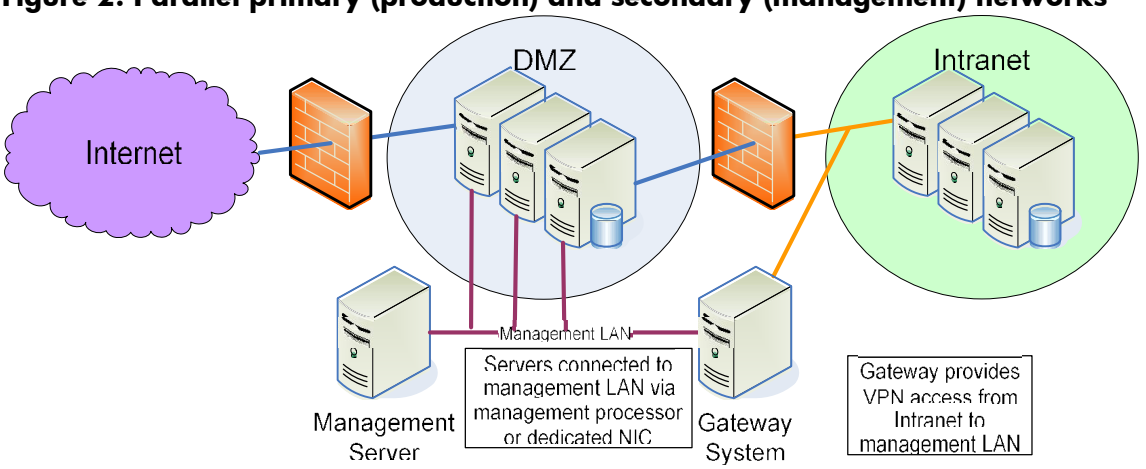
Case 2: Separate management network

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 SIM allows secure access to the systems in the DMZ.

One interesting option with this solution is to leverage the SNMP pass-through capability of either the iLO or the RILOE II. While this SNMP pass-through option does not enable all management functions, it allows for passing status, inventory, and fault information to HP SIM or another SNMP capable management application. This option has the benefit of being very secure because the host operating system does not see the Lights-Out product as a network interface card (NIC).

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 might be beneficial to allow virtual private network (VPN(access to this network.

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



Asset management

With HP SIM installed on the secondary network, system administrators can collect system asset information from a ProLiant server on that secondary network through the iLO pass-through. As a second option, administrators can browse to the web-based Agents at https://*servername*:2381 and manually view the asset information.

The Appendix to this paper describes the procedure for configuring a separate management network. SNMP must 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 it. The Agents should be configured to allow access only from IP addresses on the management network. Windows Management Instrumentation (WMI), Web-Based Enterprise Management (WBEM), and Desktop Management Interface (DMI) can be disabled on the primary network by configuring a firewall on the system to disable each of the protocols oh 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 HPSIM or another management product, such as HP Network Node Manager).

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

If SNMP traps can be received by the CMS, then the Automatic Event Handling feature of the CMS can be used to send e-mails or forward traps to another CMS that manages the network.

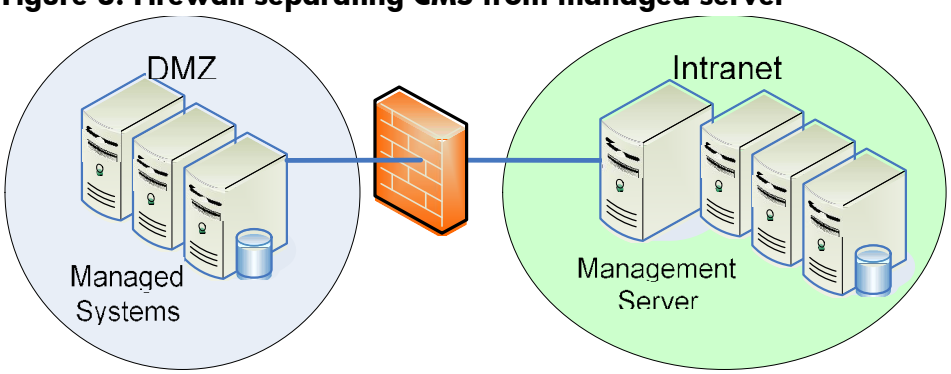
Case 3: Managing through a firewall

In other computing environments, a firewall commonly separates the CMS and the managed server. In such an environment (Figure 3), two networks are given different levels of trust. For example, the managed server might be 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 solutions, the firewall might restrict communication between specific IP addresses. For example, the firewall might allow exchange of any IP packets between the managed system and the CMS. However, because host names and IP addresses can be spotted, 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 does not permit User Datagram Protocol (UDP) traffic, as connectionless protocols cannot easily be configured to block incoming packets. Only specific Transmission Control Protocol (TCP) ports are opened, and they are possibly filtered for certain types of traffic.

Figure 3: Firewall separating CMS 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 an SQL database, and finally providing reporting capabilities on this gathered data. These steps require communication between the CMS and managed system as described below.

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 attempts to contact the managed system using a ping, if this fails, no further requests are sent to the system.

HP SIM normally uses an Internet Control Message Protocol (ICMP) echo to pint 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 can be specified in a configuration file. The target system does not need to be actively listening to the chosen port, but the firewall must be configured to allow these requests to pass.

Next, the CMS attempts to identify a number of management protocols, such as SNMP, DMI, Hyper Text Transfer Protocol (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 today, giving complete coverage of the hardware instrumentation. Integrity servers running Windows also provide this SNMP instrumentation.
- ProLiant and Integrity servers running Microsoft Windows 2000 or 2003 also expose much data through WMI, giving extensive coverage of operating system information and basic hardware information such as server model and serial number. WMI currently does not cover detailed hardware information such as controllers, duel in-line memory modules DIMMs, and physical disks.
- ProLiant and Integrity servers running Linux can 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. WBEM is being expanded to provide full instrumentation in the future.
- HP 9000 and Integrity servers running HP-UX provide management data with WBEM. (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	DMI	WBEM	WMI
ProLiant	Windows	Y		Y	Y
ProLiant	Linux	Y		Y	
HP 9000	HP-UX	Y	Y	Y (11.x)	
HP Integrity	HP-UX	Y2		Y	
HP Integrity	Linux	Y		Y	
HP Integrity	Windows	Y		Y1	Y
Other devices		Y			

Notes:

[1] When WMI mapper is installed

[2] Not required for asset management

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

SNMP

SNMP provides the best management coverage but at the highest risk. While no set operations are required for asset management, SNMP is UDP-based. Therefore, in may environments it is not considered a suitable protocol to pass through the firewall. Because SNMP version 1 has a simple, clear-text community, it provides a low level of security. However, SNMP might be suitable for some environments in which the network containing the managed systems is relatively controlled.

DMI

DMI is an 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). 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 and gather information for data collection. 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. WBEM indications are delivered from the managed system to the CMS through HTTPS on port 50004.

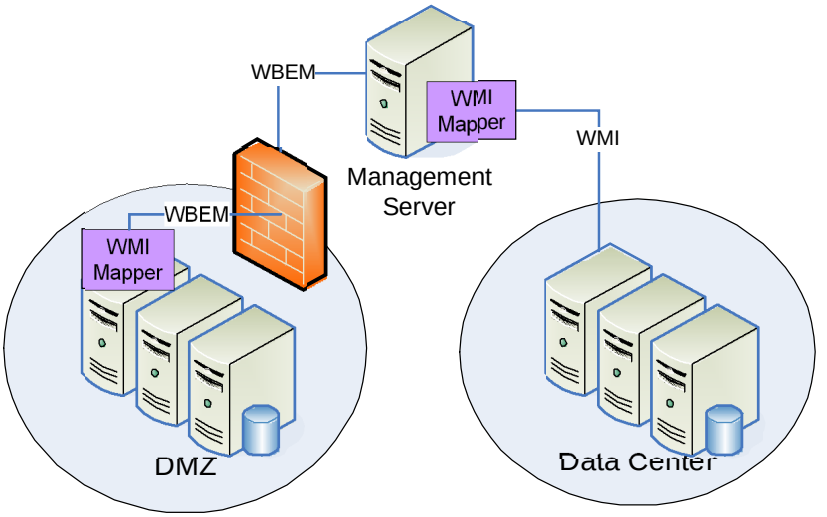
Note

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. WMI is generally not suitable through firewalls because a number of ports must be opened and the management traffic cannot be separated from other DCOM requests. For Windows systems behind a firewall, HP recommends installing the WMI Mapper on a managed system in the secure network (Figure 4). 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 systems 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. Select **Options → Protocol Settings → WMI Mapper Proxy** to add the system on which the mapper is installed.

Fault Management

The HP Agents have two means for communicating faults: SNMP traps and SMTP e-mail (Table 2). Both would originate from the agents in the DMZ to the CMS or to the SMTP mail server.

Table 2: How HP agents communicate faults

Usage	Protocol:port	Origin
SNMP Trap	SNMP:162	Agent (DMZ)
SMTP E-mail	SMTP:25	Agent (DMZ)

Configuration Management

HP web agents on managed systems in a DMZ should first be configured to trust-by-certificate the CMS server. This authenticates 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. See the **Error! Reference source not found.** 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.

Table 3: Summary of protocols used for configuration management

Usage	Feature	Protocol:port	Origin
System Discovery1	All	ICMP or TCP:80	CMS
System Identification	VC, RAS	HTTP:2301	CMS
Secure Requests	VC, RAS	HTTPS:2381	CMS
Software Identification	VC	SNMP:161	CMS
VCR Request2	VC	HTTPS:2381	System (DMZ)
Status Update3	VC	HTTP:280	System (DMZ)
SSH	SSH	SSH:22	CMS

Notes:

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

[2] If VCR is in DMZ, this is not necessary; the VCR can then be considered as any other managed system.

[3] Note that CMS polling could be used instead, but it is limited to 15-minute polls for 2 hours.

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 by way of 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 CMS and remotely to manage systems for various tools.

Performance management

This section is based on the assumption that HP ProLiant Essentials Performance Management Pack (PMP)/PPA is behind the firewall with CMS. Systems must be discoverable by the CMS using ICMP echo or TCP to port 80. All communication between PMP/PPA and managed systems occurs over SNMP.

Table 4: Performance management protocol

Usage	Protocol:port	Origin
System Discovery1	ICMP or TCP:80	CMS
PMP/PPA	SNMP:161	CMS

Note:

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

Conclusion

This paper has 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.

Glossary

Desktop Management Interface (DMI) — a management system for PCs.
Source: High Tech Dictionary: http://www.computeruser.com/resources/dictionary/index.html.
See http://www.dmtf.org/standards/dmi.

DIMM — dual inline memory module.

Distributed Component Object Model (DCOM) — an extension of Component Object Model (COM), DCOM was developed by Microsoft for Windows operating systems. It supports objects distributed across a network, much like IBM's DSOM protocol, which is an implementation of Common Object Request Broker Architecture (CORBA).
Source: High Tech Dictionary:http://www.computeruser.com/resources/dictionary/index.html.

HyperText Transmission Protocol, Secure (HTTPS). HTTP over Secure Sockets Layer (SSL).

Internet Control Message Protocol (ICMP) — an extension to the Internet Protocol which is used to communicate between a gateway and a source host, to manage errors and generate control messages.
Source: High Tech Dictionary: http://www.computeruser.com/resources/dictionary/index.html.

RPC — remote procedure call.

Simple Mail Transfer Protocol (SMTP) — a server-to-server protocol for delivering electronic mail. The standard protocol used on the Internet; also used on other TCP/IP networks.
Source: High Tech Dictionary: http://www.computeruser.com/resources/dictionary/index.html.

Simple Network Management Protocol (SNMP) — the Internet standard protocol for network management software. Using SNMP, programs called agents monitor various devices on the network (hubs, routers, bridges, etc.). Another program collects the data from the agents. The database created by the monitoring operations is called a management information base (MIB). This data is used to check whether all devices on the network are operating properly.
Source: High Tech Dictionary: http://www.computeruser.com/resources/dictionary/index.html.

User Datagram Protocol (UDP) — a communications protocol for the Internet network layer, transport layer, and session layer, which makes it possible to send a datagram message from one computer to an application running in another computer. Like TCP, UDP is used with Internet Protocol (IP). Unlike TCP, UDP is connectionless and does not guarantee reliable communication; the application itself must process any errors and check for reliable delivery.
Source: High Tech Dictionary: http://www.computeruser.com/resources/dictionary/index.html.

Appendix: Configuring a Separate Management Network

To configure a separate management network using HP SIM, install HP SIM 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:
     1. From the Control Panel, open the **Services** menu.
     2. Open the **Properties** for the SNMP Service.
     3. 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:
     1. Modify the `snmpd.conf` configuration file to accept SNMP packets only from the desired hosts.
     2. Do the same with any other operating system service needed on the network.
2. Configure the Insight Management Agents to allow access only from IP addresses on the management network:
   a. Log into the Agent with administrator privileges.
   b. Go to the **Settings/Options** page, and modify the IP Restricted Logins settings.
3. Configure HP SIM to discover the systems on the secondary network:
   c. In HP Insight Manager, go to **Options** → **Discovery** → **Automatic Discovery**.
   d. 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 further considerations on enabling WMI, WBEM and DMI, see Table 5.

Table 5: Protocols used for asset management of industry-standard servers

Server	OS	SNMP	DMI	WBEM	WMI
ProLiant	Windows	Y		Y1	Y
ProLiant	Linux	Y		Y	
HP 9000	HP-UX	Y2	Y3	Y (11.x)	
HP Integrity	HP-UX	Y2		Y	
HP Integrity	Linux	Y		Y	
HP Integrity	Windows	Y		Y1	Y
Other devices		Y			

Notes:

[1] When WMI Mapper is installed

[2] Not required for asset management

[3] Not required if WBEM is installed

For more information

Topic	Link
ProLiant server management	http://h18013.www1.hp.com/products/servers/management/index.html
HP Systems Insight Manager	http://www.hp.com/go/hpsim
ProLiant Essentials Performance Management Pack (PMP)	http://h200002.www2.hp.com/bc/docs/support/SupportManual/c00291350/c00291350.pdf
HP WBEM Services for HP-UX	http://h18004.www1.hp.com/products/servers/management/hpsim/download.html
Integrated Lights-Out (iLO)	http://h18013.www1.hp.com/products/servers/management/iloadv/index.html
Remote Insight Lights-Out Edition II (RILOE II)	http://h18013.www1.hp.com/products/servers/management/riloe2/index.html
Main HP OpenView site	http://www.openview.hp.com/
ProLiant Essentials Vulnerability and Patch Management Pack Server Security Recommendations	http://h200002.www2.hp.com/bc/docs/support/SupportManual/c00291350/c00291350.pdf

Call to action

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

481364-001 02/2008

invent